LABORATOIRE NATIONAL DE MÉTROLOGIE ET D'ESSAIS

CERTIFICATION NUMERIQUE

Référentiel ATTS

Certification d'une Architecture de délivrance d'une référence de Temps exacte, Tracée et Sécurisée.

Version 2

Novembre 2019

Mal employer le temps, autant ne rien faire.

Le philosophe bienfaisant (1764)

1. Révisions du document

Version	Date	Motif de la mise à jour
1	1/2019	Version initiale
2	11/2019	Modifications suite à relecture et commentaires des parties intéressées

2. Sommaire

3. Présentation du concept

3.1. Problématique actuelle liée à la diffusion du temps

Les solutions actuelles proposées sur le marché pour distribuer le temps le font avec exactitude mais sans traçabilité vis à vis la source (en particulier UTC).

Par ailleurs, les protocoles utilisés comme le NTP, le PTP, le GNSS, ou le Hertzien n'apportent pas d'éléments clés tels que :

- l'intégrité des messages temps transmis
- la traçabilité et l'exactitude des temps délivrés,

Les solutions faisant l'objet de ce référentiel de certification devront mettre en place une architecture de distribution et de diffusion permettant de répondre à ces besoins.

3.2. La certification d'une architecture de délivrance d'un temps exact, tracé et sécurisé

Une architecture certifiée permet de délivrer un **temps attesté** pour une exactitude donnée avec son origine et le cas échéant sa bonne utilisation par le matériel connecté (notion d'acquisition).

On parle d'une architecture de délivrance d'une référence de temps attesté exacte, tracée et sécurisée.

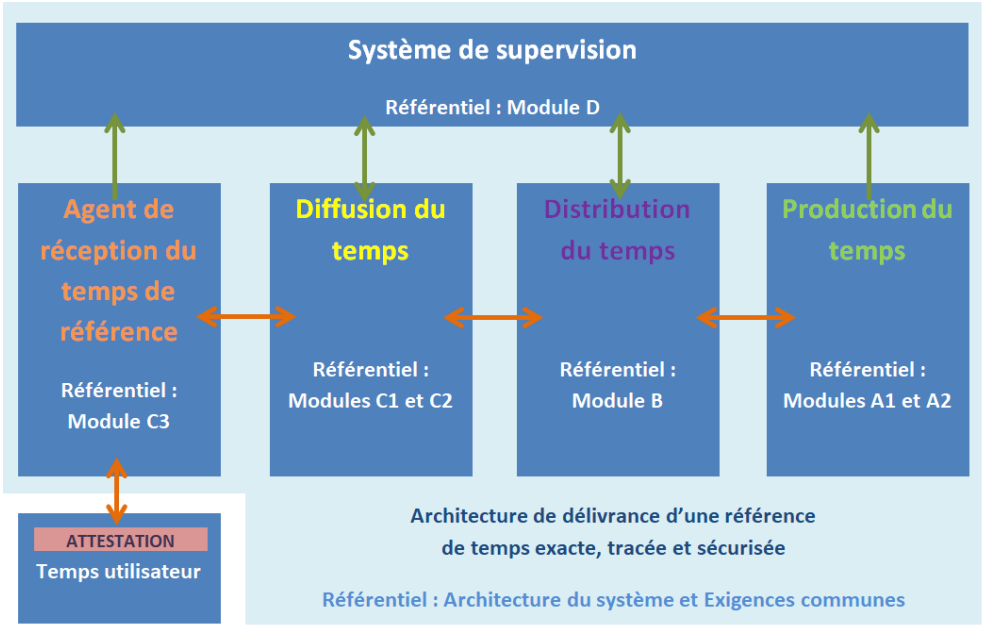

Figure 1 – Architecture, ses Systèmes et Modules du référentiel de certification

Rappel sur le temps légal

L'UTC (Universal Time Coordinated) est une échelle de temps adoptée comme base du temps international. Le Temps Universel Coordonné UTC est élaboré par le BIPM (Bureau International des Poids et Mesures). C'est la résultante d'une comparaison de plus de 400 horloges atomiques réparties dans plus de 70 laboratoires métrologiques dans le monde. **Le Temps légal ou Heure légale d'un pays est défini à partir de la référence internationale du Temps Universel Coordonné (UTC) à laquelle est ajouté ou retranché un nombre d'heures selon le fuseau horaire.**

4. Modalités d'élaboration et de validation du référentiel

La certification est une procédure par laquelle une tierce partie, l'organisme certificateur, donne une assurance écrite qu'un système d'organisation, un processus, une personne, un produit ou un service est conforme à des exigences spécifiées dans une norme ou un référentiel.

La certification est ici un acte volontaire qui peut procurer aux entreprises un avantage concurrentiel. C'est un outil de compétitivité qui renforce la confiance dans leurs relations avec leurs clients en leur garantissant, via le certificat, l'atteinte d'engagements de service et de conformité du produit. Elle doit donc être délivrée par des organismes certificateurs indépendants des entreprises certifiées ainsi que des pouvoirs publics. Elle est accessible à tout professionnel du secteur d'activité répondant aux critères des référentiels de certification.

Le présent référentiel a été élaboré à partir des documents de travail (cahiers des charges) issus des réunions du groupe d'experts du projet SCPTime® comprenant les fabricants des systèmes de l'architecture (production, distribution, diffusion), les laboratoires scientifiques (temps, métrologie, sécurité de l'information) et les clients industriels finaux.

Pour la validation de ce référentiel, le LNE a la responsabilité :

- d'identifier les parties prenantes concernées ;
- de s'assurer de la pertinence des parties prenantes sélectionnées ;
- de s'assurer de leur représentativité, sans prédominance de l'une d'entre elles ;
- de recueillir leur point de vue.

5. Architecture du système

5.1. Définition

Une architecture est certifiée pour une exactitude donnée. Cette architecture permet une traçabilité des opérations permettant, a posteriori, de démontrer que le temps a été diffusé :

- Avec une origine garantie (traçabilité vis-à-vis de la source)
- Avec une exactitude donnée
- Sans avoir été altéré

On parle alors de « **temps attesté** », objet de la certification de l'architecture.

Le tableau suivant définit les différents composants du système :

Nom du système	Description
Système de production du temps	Service en charge de la production du temps et de sa mise à disposition au système de distribution
Système de distribution du temps	Service en charge de la distribution du temps aux dispositifs de diffusion. Ce service s'appuie sur un réseau de serveurs en charge d'apporter le temps au plus près des clients.
Dispositif de diffusion	Dispositif permettant de diffuser le temps dans le périmètre client. Il peut s'agir : - D'un dispositif matériel installé dans le périmètre client ; - D'un service, on parle alors de dispositif de diffusion du temps de référence de type A.
Agent de réception du temps de référence	Dispositif logiciel optionnel, permettant d'obtenir une traçabilité du temps jusqu'à l'horloge locale du client (dispositif final recevant le temps exact, tracé et sécurisé qui sera attesté)
Système de supervision	Service permettant : - De contrôler la distribution et la diffusion du temps - De collecter les traces de distribution et de diffusion afin de reconstituer a posteriori la traçabilité.
Elément final du client	Interface/Elément du client final à synchroniser.

Le temps produit, distribué et diffusé est un temps attesté si :

- il est fourni par un système de production conforme aux exigences du présent référentiel (voir module A) ;
- il est transmis par des éléments certifiés reliés à la supervision jusqu'à un élément de fin de chaîne lui aussi certifié ;
- la conformité est vérifiée par un système de supervision certifié.

5.2. Exigences spécifiques de l'architecture du système

Une architecture est certifiée si :

- Tous ses composants faisant l'objet d'un module pouvant être certifié suivant ce référentiel sont effectivement certifiés.
- Si elle répond aux exigences spécifiques ci-après :

5.2.1. Organisation

ATTS-AR-010 - Entité responsable
Une entité (Personne morale) doit être responsable de la mise en place et du fonctionnement opérationnel de l'architecture du système. **Elle peut opérer directement ou faire sous-traiter tout ou partie des opérations.** **En cas de sous-traitance, celle-ci doit faire l'objet d'un contrat et spécifier les rôles et responsabilités de chacune des parties.**
Note de spécification :
La sous-traitance (ou délégation) ne supprime pas la responsabilité de l'entité mais peut prévoir une substitution partielle de responsabilité. L'attestation au client final ne peut faire l'objet d'une délégation.
Documentation à fournir à l'évaluateur :
- documentation de l'organisation et de la responsabilité ; - contrats de sous-traitance ou tout document contractuel définissant les délégations de responsabilité
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera : - qu'une entité a bien la responsabilité totale de l'architecture ; - que les substitutions de responsabilité des éventuelles entités délégataires sont cohérentes, continues et en relation avec le périmètre de la délégation ; - que l'entité existe ; l'existence de contrats de sous-traitance ou de délégation.

ATTS-AR-020 - Suivi des certifications
L'entité responsable doit mettre en place et appliquer une procédure de suivi des certifications des différents composants et services mis en œuvre.
Note de spécification :
N/A
Documentation à fournir :
- procédure de maîtrise de chacune des sous-traitances ; - inventaire des certifications des services et composants mis-en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera : - que la ou les procédures existent et sont adéquates ; - que l'inventaire est à jour.

5.2.2. Architecture

ATTS-AR-030 - Éléments communs de l'architecture
L'entité responsable doit mettre en place une architecture . Celle-ci doit comporter au moins : - **un système de production ;** - **un système de distribution ;** - **un système de diffusion ;** - **un système de supervision**
Note de spécification :
Les systèmes de production, de distribution, de diffusion et de supervision répondent aux exigences des modules du présent référentiel.
Documentation à fournir :
Documentation détaillée de l'architecture mise en place.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'architecture décrite comporte les systèmes et dispositifs précités
Exemple d'implémentation satisfaisant l'exigence
N/A

ATTS-AR-040 - Unicité du système de supervision
Pour une architecture donnée, le service de supervision doit être unique.
Note de spécification :
Documentation à fournir :
- Documentation de l'architecture du système de supervision
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'architecture est suffisamment décrite et que le service de supervision est unique.
Exemple d'implémentation satisfaisant l'exigence
N/A

ATTS-AR-050 - Mise en place d'agents
Si l'entité responsable met en place un dispositif de diffusion de type A, alors, les éléments finaux se synchronisant sur ce dispositif doivent utiliser obligatoirement des Agents de réception du temps de référence. **Si des dispositifs de diffusion de types B, C ou D sont uniquement en place, alors l'utilisation d'Agent de réception du temps de référence est optionnelle**
Note de spécification :
Voir module C3
Documentation à fournir :
- Document d'architecture du service.

Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'architecture décrite correspond à l'un de ces schémas.
Exemple d'implémentation satisfaisant l'exigence
N/A

ATTS-AR-060 - Modification d'architecture
En cas de modification majeure et/ou de mise en place d'une nouvelle architecture, l'entité responsable doit s'assurer qu'une demande de révision de la certification est réalisée avant la mise en production effective du composant.
Note de spécification :
Par majeur, on entend modification ou ajout d'un composant ou d'un service correspondant à un module certifié.
Documentation à fournir :
- Demande de révision de la certification incluant une description détaillée des modifications et des impacts.
Guide de validation :
[Évaluation documentaire] L'évaluateur réalisera une nouvelle évaluation en prenant en compte les exigences impactées.
Exemple d'implémentation satisfaisant l'exigence
N/A

5.2.3. Politique de synchronisation

ATTS-AR-070 - Politique de synchronisation

L'entité responsable de l'architecture du système doit définir et communiquer aux différents acteurs la politique de synchronisation de l'architecture. Celle-ci doit définir a minima :

- **L'exactitude cible de l'architecture (par exemple +/-50 microsecondes)**
- **Le taux de disponibilité cible (par exemple : 99,9% mensuel)**
- **Pour chaque élément de l'architecture, la fréquence de synchronisation nominale mise en œuvre. Cette fréquence de synchronisation nominale doit être conforme au tableau ci-dessous.**

Agent de réception du temps de référence	Dispositif matériel de diffusion de type B	Dispositif matériel de diffusion de type C	Dispositif matériel de diffusion de type D
A minima toutes les 60s	A minima toutes les 2^10s	A minima toutes les 2^10s	A minima toutes les 300s

Dispositif de diffusion de type A	Système de distribution du temps de référence	Serveur de production
A minima toutes les 2^10s	A minima toutes les 180s	A minima toutes les 1s

La politique de synchronisation doit également :
- préciser le niveau d'autonomie du système de diffusion en cas de panne de la production pour la précision. Ce niveau d'autonomie doit être a minima de 5 jours ;
- préciser la méthode de calcul de la disponibilité mise-en-œuvre.

Note de spécification :

Documentation à fournir :
- Politique de synchronisation.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si la politique est disponible, si elle est conforme à l'exigence et les méthodes employées pour vérifier sa bonne application. [Évaluation fonctionnelle] Vérification de la bonne application de la politique
Exemple d'implémentation satisfaisant l'exigence
Exemple de couple « exactitude cible / disponibilité cible » : exactitude cible 10ms / disponibilité cible : 99%

5.2.4. Exigences relatives à la mise en œuvre des Systèmes de production.

ATTS-AR-080 - Certification du système de production
L'architecture du système doit mettre en œuvre un ou des systèmes de production en conformité avec le module A – Production du temps
Note de spécification :
Documentation à fournir :
Voir module A – Production du temps
Guide de validation :
Voir module A – Production du temps

ATTS-AR-090 - Exactitude cible du système de production
Le système de production mis en œuvre doit produire un temps avec une exactitude cible au moins 10 fois supérieure à l'exactitude cible visée par l'architecture du système.
Note de spécification :
Documentation à fournir :
Voir module A – Production du temps
Guide de validation :
Voir module A – Production du temps

5.2.5. Exigences relatives à la mise en œuvre des Systèmes de supervision.

ATTS-AR-100 - Certification du système de supervision
L'architecture doit mettre en œuvre un système de supervision en conformité avec le module D - Supervision.
Note de spécification :
Documentation à fournir :
Voir module D – Supervision (Système de supervision)
Guide de validation :
Voir module D – Supervision (Système de supervision)

ATTS-AR-110 - Certification du système de supervision
Le système de supervision doit être indépendant des autres systèmes.
Note de spécification :
Par indépendant, il est entendu qu'il doit être opéré par une entité distincte des autres systèmes. Si cette entité a des liens juridiques avec d'autres entités de l'architecture (filiales, société mère commune), des mesures doivent être mises en œuvre contre les risques de conflits d'intérêts.
Documentation à fournir :
- Justification de l'indépendance.
Guide de validation :
L'évaluateur vérifiera les éléments démontrant l'indépendance et l'existence de règles de protection.

5.2.6. Exigences relatives à la mise en œuvre des Systèmes de distribution.

ATTS-AR-120 - Certification du système de distribution
L'architecture doit mettre en œuvre un ou des systèmes de distribution en conformité avec le module B – Système de distribution
Note de spécification :
Documentation à fournir :
Voir module B – Système de distribution
Guide de validation :
Voir module B – Système de distribution

ATTS-AR-130 - Exactitude cible du système de distribution
Le système de distribution mis en œuvre doit produire un temps avec une exactitude cible : - **a minima 5 fois meilleure que l'exactitude cible visée par l'architecture pour les exactitudes supérieures à 1 microseconde,** - **a minima 2 fois meilleure en dessous de 1 microseconde.**
Note de spécification :

Documentation à fournir :
Voir module B – Système de distribution
Guide de validation :
Voir module B – Système de distribution

ATTS-AR-140 - Compatibilité du système de distribution
Le système de distribution doit être compatible avec l'ensemble des autres éléments de l'architecture du système mis en œuvre.
Note de spécification :
Documentation à fournir :
- Présentation détaillée de l'architecture du système ; - Documentation des systèmes et produits mis en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les éléments sont bien déclarés compatibles par leurs constructeurs/ fournisseurs respectifs.

5.2.7. Exigences relatives à la mise en œuvre des dispositifs de diffusion.

ATTS-AR-150 - Certification des dispositifs de diffusion physique
Si l'architecture s'appuie sur des dispositifs matériels de diffusion du temps de référence, elle doit mettre en œuvre un ou des modèles de dispositifs de diffusion en conformité avec le module C1. **Si l'architecture s'appuie sur des dispositifs de diffusion du temps de référence de type A, elle doit mettre en œuvre un ou des modèles de dispositifs de diffusion en conformité avec le module C2.**
Note de spécification :
Documentation à fournir :
Voir module C – Diffusion du temps
Guide de validation :
Voir module C – Diffusion du temps

ATTS-AR-160 - Exactitude de dispositif de diffusion physique
L'exactitude du dispositif de diffusion doit être meilleure que l'exactitude cible de l'architecture du système.
Note de spécification :
Documentation à fournir :
- Description du dispositif utilisé et exactitude du dispositif ; - Précision de l'algorithme démontrant l'exactitude de calcul du dispositif de diffusion
Guide de validation :
[Évaluation documentaire] L'évaluateur s'assurera que les caractéristiques des modèles déclarés satisfont

l'exigence. La vérification s'appuie :

- d'une part, sur les caractéristiques déclarées pour le ou les dispositifs de diffusion mis-en-œuvre ;
- d'autre part, pour l'exactitude cible de l'architecture déclarée.

Nota : la vérification de l'exactitude du dispositif de diffusion n'est pas dans le périmètre du présent module. Celle-ci est vérifiée lors de l'évaluation du dispositif de diffusion

5.2.8. Exigences relatives aux sources et médias.

ATTS-AR-170 - Exigence relative au raccordement des dispositifs de diffusion
Afin d'assurer la disponibilité et la fiabilité du système, il est exigé, pour les dispositifs de diffusion disposant d'au moins deux entrées temps, que la seconde entrée ne soit pas reliée à la même source de temps. **L'entrée principale doit être raccordée à un dispositif de distribution de l'architecture.** **L'entrée secondaire doit avoir une exactitude égale ou supérieure à l'entrée principale.** **Il est recommandé que chaque entrée utilise un média différent.**
Note de spécification :
Il est exigé que : - soit chaque entrée logique du système de diffusion est reliée à sa source par un type de média différent ; - soit chaque entrée logique est reliée par le même type de média. Dans ce cas, il faudra des exigences sur les origines (exemple, fil et antennes GNSS différentes et séparées). Il est à noter que deux sources avec le même média sont considérées comme acceptables sous réserve de leur insensibilité aux brouillages externes.
Documentation à fournir :
- description des connexions mises en place ;
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si la description satisfait l'exigence. Rapport d'essais démontrant l'insensibilité aux brouillages externes

5.2.9. Exigences relatives à la remontée des traces.

ATTS-AR-180 - Raccordement du système de supervision
Les dispositifs de diffusion mis en œuvre doivent remonter des traces au système de supervision
Note de spécification :
Documentation à fournir :
Architecture du système mentionnant la remontée des traces
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si la description satisfait l'exigence.

5.2.10. Exigences relatives à la mise en œuvre des Agents de réception du temps de référence

ATTS-AR-190 - Certification des agents
Si l'architecture s'appuie sur des agents, elle doit mettre en œuvre version d'agents certifiés en

conformité avec le module C3
Note de spécification :
Documentation à fournir :
Voir module C3 – Agent de réception du temps de référence
Guide de validation :
Voir module C3 – Agent de réception du temps de référence

ATTS-AR-200 - Flux des agents des Agents de réception du temps de référence
L'entité opérant les Agents de réception du temps de référence doit ouvrir les flux permettant : - Aux agents de communiquer avec le système de supervision - Aux agents de se connecter aux systèmes de diffusion
Note de spécification :
Cette exigence doit être satisfaite par le client de l'architecture du système et est hors du périmètre d'évaluation. Cependant, il est demandé que cette exigence soit portée à la connaissance de l'entité mettant en œuvre les Agents de réception du temps de référence. Cela peut être réalisé à travers le guide d'installation.
Documentation à fournir :
Architecture du système mentionnant la remontée des traces
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si la description satisfait l'exigence.

ATTS-AR-210 - Compatibilité des Agents de réception du temps de référence
Les Agents de réception du temps de référence doivent être compatibles avec - Les dispositifs de diffusion mis en œuvre (matériels ou logiciels). - Le système de supervision mis en œuvre.
Note de spécification :
Documentation à fournir :
Rapports de compatibilité effectués
Guide de validation :
[Évaluation documentaire] Etudes des rapports de compatibilité

5.3. Système optionnel de calcul via GNSS

5.3.1. Description d'un un système de calcul via GNSS

L'ensemble des exigences suivantes s'appliquent à un système **optionnel** de calcul via GNSS compatible avec les modules de l'architecture du système.

Les sites d'exploitation du système de calcul doivent respecter les exigences communes du paragraphe 10.1.5.

Un système de calcul est un ensemble de site(s), de moyens humains, matériels, logiciels et réseaux, et de procédures permettant de :

- collecter l'ensemble des traces remontées par les éléments de l'architecture du système disposant de modules de calcul via GNSS.
- d'analyser les traces collectées pour produire une traçabilité.

Au sein de l'architecture du système, le système de calcul est installé au sein du SI de l'architecture et récupère l'ensemble des informations pertinentes liées aux mesures GNSS. Un calcul est réalisé sur les données afin de calculer une traçabilité à UTC. De ce fait, les exigences qui suivent portent principalement sur :

- le fonctionnement et les conditions d'opération du service ;
- le protocole d'échange avec les différents dispositifs déployés ;
- l'analyse des informations remontées ;
- la transmission de l'information de traçabilité à la supervision.

Le rôle du système de calcul est le calcul d'un écart de temps d'un dispositif par rapport à une source de temps. Cet écart est calculé à partir de mesures d'écart réalisées par rapport à une même source GNSS supposée non traçable à UTC. De ce fait, les principales fonctions attendues d'un service de calcul sont :

- La collecte sécurisée des écarts mesurés ;
- L'analyse des informations afin d'établir la traçabilité à UTC avec une exactitude cible ;
- La transmission sécurisée des informations au système de supervision via la sécurité physique, logique, réseau et organisationnelle du service.

Les exigences intègrent l'objectif de protéger le système de calcul contre les typologies d'attaque ou d'incidents pouvant compromettre la sécurité ou la traçabilité de l'architecture du système.

5.3.2. Exigences relatives à la collecte sécurisée des traces de synchronisation et statuts des éléments de l'architecture du système

ATTS-AR-220 - Capacité à collecter les informations de synchronisation
Le système de calcul doit être en mesure de collecter les mesures d'écarts produites par les modules de calcul via GNSS. Il doit être en mesure de prendre en compte : - **Une mesure globale GNSS** - **Une mesure par constellation** - **Une mesure par satellite**
Note de spécification :
Il est demandé à un système d'être capable de recueillir les informations de mesure pour au moins un type de produit.
Documentation à fournir à l'évaluateur :
- Listes des matériels compatibles avec le service - Description des dispositifs de collecte mis en œuvre - Test de collecte des informations de synchronisation
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie satisfait l'exigence. En particulier, il vérifiera qu'une gamme complète de produits est couverte. [Évaluation fonctionnelle] L'évaluateur demandera, pour chaque type d'élément de l'architecture du système, à constater la collecte effective des informations d'écarts.

5.3.3. Exigences relatives au dimensionnement

La plate-forme doit être dimensionnée en adéquation avec le volume de transactions.

ATTS-AR-230 - Dimensionnement
Les serveurs doivent être dimensionnés pour supporter la charge de collecte. L'entité opérant le calcul doit mettre en place une architecture dimensionnée en adéquation avec le nombre de transactions prévues.
Note de spécification :
En particulier, le pic d'activité et les variations saisonnières doivent être pris en compte.
Documentation à fournir à l'évaluateur :
- Description de la volumétrie cible ou mesure de volumétrie courante - Description de la volumétrie que la plate-forme est capable de supporter - Test de charge et résultat des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie satisfait l'exigence. En particulier, il s'assurera que la volumétrie que la plate-forme est capable de supporter est très supérieure à la volumétrie courante.

ATTS-AR-240 - Surveillance et prévision du dimensionnement
L'entité opérant le système de calcul a une obligation de surveillance du dimensionnement et de prévision de volumétrie à venir
Note de spécification :
La surveillance doit prendre en compte les déploiements prévus de nouveaux éléments de l'architecture du système.
Documentation à fournir à l'évaluateur :
- Description des mesures de surveillance mises en place
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie satisfait l'exigence. En particulier, il vérifiera que les mesures permettent bien d'estimer la volumétrie future de la plate-forme. [Évaluation fonctionnelle] L'évaluateur demandera à voir les projections et le plan de déploiement associé.

5.3.4. Exigences relatives à la sécurisation de la collecte

ATTS-AR-250 - Sécurisation de la collecte des synchronisations
Lorsqu'il échange avec un élément de l'architecture du système, le système de calcul doit mettre en œuvre un protocole de communication sécurisé conforme au paragraphe 10.1.8.
Note de spécification :
Documentation à fournir à l'évaluateur :
Voir paragraphe 10.1.8.
Guide de validation :
Voir paragraphe 10.1.8.

ATTS-AR-260 - Vérification de l'émetteur
Avant d'accepter la collecte d'un écart, le système de calcul doit s'assurer : • **que l'élément émetteur est bien identifié comme faisant partie de l'architecture du système (voir Module D - Supervision) ;** • **que l'élément émetteur a bien été authentifié avec succès** **Si l'une de ces vérifications échoue, une alerte doit être levée.** **Au niveau du calcul, un mécanisme anti attaque de type force brute doit être mis en en place.**
Note de spécification :
Documentation à fournir à l'évaluateur :
- Description du mécanisme mis en œuvre - Test du mécanisme et résultat des tests.
Guide de validation :
Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie satisfait l'exigence. En particulier, il vérifiera que les deux cas d'échec sont bien couverts par les tests. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests pour différents types d'équipements.

5.3.5. Conservation et protection des éléments collectés

Une fois les éléments collectés, le système de calcul doit assurer la protection et la conservation des informations de synchronisation collectées.

ATTS-AR-270 - Durée de rétention
Le système de calcul doit conserver les informations de synchronisation pour une durée de 6 mois.
Note de spécification :
Documentation à fournir à l'évaluateur :
- Description de la durée de conservation
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera si la durée de conservation est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la conservation effective des informations. La vérification se fera par échantillonnage.

ATTS-AR-280 - Protection des traces collectées
Le système de calcul doit mettre en œuvre de mesures permettant de s'assurer que les traces collectées ne puissent pas être altérées ou détruites.
Note de spécification :
Des mesures de droits d'accès appropriés sont jugées suffisantes pour se prémunir d'un effacement des données par une source humaine malveillante.
Documentation à fournir à l'évaluateur :
- Description des mesures mises en place
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera si les mesures décrites sont adéquates. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site la bonne implémentation des mesures décrites.

ATTS-AR-290 - Sauvegardes des traces collectées
Les traces collectées doivent faire l'objet de sauvegardes et/ou de réplication
Note de spécification :
Documentation à fournir à l'évaluateur :
- Description des mesures mises en place
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera si les mesures décrites sont adéquates. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site la bonne implémentation des mesures décrites.

5.3.6. Exigences relatives au calcul.

Le système de calcul doit être en mesure, à partir de mesures d'écarts par rapport à une référence GNSS, une mesure d'écart par rapport à une source UTC(k).

ATTS-AR-300 - Algorithme du calcul – données d'entrée
Le calcul doit être réalisé pour : • **un dispositif aval donné ;** • **un dispositif source donné ;** • **une date donnée.** **Selon le niveau du dispositif, les mesures fournies pourront être :** • **une mesure d'écart moyenne sur l'ensemble des satellites observés ;** • **une mesure d'écart moyenne par constellation de satellites ;** • **une mesure individuelle par satellite.**
Note de spécification :
Documentation à fournir :
- Description du format de sortie
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le format de sortie est décrit. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage que les résultats sont conformes à la description.

ATTS-AR-310 - Algorithme du calcul – fonctionnement
L'algorithme de calcul devra être décrit en détail. L'implémentation de l'algorithme pour des mesures individuelles par satellite (niveau 3) devra prendre en compte les préconisations du rapport BIPM 93/6. **Pour les autres niveaux, seules les recommandations applicables devront être prises en compte. En particulier, la description devra indiquer :** • **Les pondérations/exclusions éventuelles de satellite** • **La méthode de calcul** **Il doit notamment être démontré que la méthode de calcul permet d'obtenir un écart indépendant du temps satellite.**
Note de spécification :
Documentation à fournir :
- Description du format de sortie
Guide de validation :
[Evaluation documentaire] Etude de la description du fonctionnement de l'algorithme de calcul par rapport à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage que les résultats sont conformes à la description.
Exemple d'implémentation satisfaisant l'exigence

ATTS-AR-320 - Résultat du calcul
Le format de sortie doit être décrit. Celui-ci doit contenir : - **La date de mesure** - **L'écart calculé** - **L'identifiant du dispositif cible.** **Il est fait l'hypothèse que l'écart ne peut être supérieur à la seconde (si c'était le cas, l'écart serait détecté par la supervision). De ce fait, le résultat du calcul d'écart peut être donné modulo une seconde.**
Note de spécification :
Documentation à fournir :
- Description du format de sortie
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le format de sortie est décrit. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage que les résultats sont conformes à la description.

ATTS-AR-330 - Fréquence de l'analyse et écart à analyser
La fréquence de l'analyse mise en œuvre et les écarts à calculer devront être conformes à la politique de synchronisation décrite dans l'Architecture du système.
Note de spécification :
Documentation à fournir :
- Description des fréquences de traitements et des couples Source – Cible faisant l'objet d'un calcul.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que les fréquences et couples faisant l'objet d'un calcul sont conformes à la politique de synchronisation [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage que les résultats sont conformes à la description.

5.3.7. Exigences relatives à la mise à disposition des informations d'écart à la supervision

ATTS-AR-340 - Sécurisation de la transmission des écarts à la supervision
Lorsqu'il échange le résultat du calcul avec la supervision, le système de calcul doit mettre en œuvre un protocole de communication sécurisé conforme aux exigences du paragraphe 10.1.8.
Note de spécification :
Documentation à fournir à l'évaluateur :
Voir paragraphe 10.1.8.
Guide de validation :
Voir paragraphe 10.1.8.

5.3.8. Exigences relatives à la sécurité physique

ATTS-AR-350 - Exigences communes relatives à la sécurité physique
Les sites d'exploitation du système de calcul doivent respecter les exigences relatives à la sécurité physique du paragraphe 10.1.1.
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.1.
Guide de validation :
Voir paragraphe 10.1.1.

5.3.9. Exigences relatives aux ressources humaines

ATTS-AR-360 - Exigences communes aux ressources humaines

Les sites d'exploitation du système de calcul doivent respecter les exigences relatives aux ressources humaines du paragraphe 1.2 du chapitre 10. .
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.2.
Guide de validation :
Voir paragraphe 10.1.2.

5.3.10. Exigences relatives à la sécurité logique

ATTS-AR-370 - Exigences communes à la sécurité logique
Les sites d'exploitation du système de calcul doivent respecter les exigences relatives à la sécurité logique du paragraphe 10.1.3.
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.3.
Guide de validation :
Voir paragraphe 10.1.3.

ATTS-AR-380 - Protection des échanges réseau
Des mesures de protection des flux réseau doivent être mises en œuvre afin d'assurer la confidentialité et l'intégrité des données qui y transitent.
Note de spécification :
Certains flux peuvent ne pas nécessiter de mettre en place des mesures de protection, mais cela doit être justifié (par exemple : échange de données non sensibles, protection physique du matériel, besoin de performance …). Le cas échéant, des mesures de sécurité adéquate (protection physique) doivent être mises en place.
Documentation à fournir :
- Schéma des flux identifiant les flux sécurisés et non sécurisés - Description de la mesure de sécurisation mise en œuvre - Justification des flux non sécurisés.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, éventuellement par échantillonnage, que la mise en œuvre est conforme à la description fournie.

5.3.11. Module de calcul via GNSS

Les exigences ci-après sont applicables à un module de module de calcul via GNSS. Ces exigences sont uniquement applicables au module de calcul, embarqué sur certains éléments des systèmes de l'architecture (par exemple, un dispositif matériel de diffusion du temps de référence de type D).

Un autre système peut être déployé aux conditions qu'il puisse être démontré l'équivalence dans les résultats ponctuels ou sur la durée. D'un point de vue périmètre, l'antenne GNSS est hors du périmètre d'évaluation.

ATTS-AR-390 - Entrée horloge locale
L'entrée temps locale du module doit être connectée à l'horloge interne du dispositif autre. **La référence de temps doit être composée :** - **D'un TOD** - **D'un PPS**
Note de spécification :
Documentation à fournir :
- Description de l'entrée et du format.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que l'entrée décrite est conforme à l'exigence.
Exemple d'implémentation satisfaisant l'exigence
Une entrée filaire PTP ou NTP satisfait l'exigence.

ATTS-AR-400 - Entrée GNSS
L'entrée GNSS du module doit être connectée à un récepteur satellite **La documentation du produit doit décrire les caractéristiques du récepteur à utiliser.** **En particulier, le module doit correspondre a minima au niveau de mesure du module**

Niveau 1	Le récepteur de niveau 1 fournit une mesure d'écart moyenne sur l'ensemble des satellites observé. Il peut être mono ou multi-constellations.
Niveau 2	Le récepteur de niveau 2 fournit une mesure d'écart moyenne **par** constellation de satellites.
Niveau 3	Le récepteur de niveau 3 fournit une mesure individuelle par satellite.

Note de spécification :
Documentation à fournir :
- Guide utilisateur - Liste des constellations utilisées
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que l'entrée décrite est conforme à l'exigence.

ATTS-AR-410 - Données mesurées et transmises

La donnée mesurée doit être l'écart entre la date de l'horloge locale de l'hôte et l'heure GNSS.

Par convention, la mesure de l'écart doit avoir les caractéristiques suivantes :

- **La mesure doit démarrer sur le PPS local et se terminer sur le temps GNSS**
- **La date utilisée sera la date locale de l'équipement.**

Trois niveaux de mesures sont à prendre en compte :

Niveau 1	Mesure d'écart moyenne sur l'ensemble des satellites observés. Il peut être mono ou multi constellations.
Niveau 2	Mesure d'écart moyenne **par** constellation de satellites.
Niveau 3	Mesure individuelle par satellite.

La donnée remontée au module de calcul doit contenir :

- **l'heure de la mesure ;**
- **la ou les mesures d'écarts réalisées.**

Note de spécification :

Cet écart peut être mesuré modulo une seconde

Documentation à fournir :

- Description du dispositif de mesure.
- Test du dispositif de mesure

Guide de validation :

[Evaluation documentaire] L'évaluateur vérifiera que le dispositif de mesure décrit est conforme à l'exigence.

[Evaluation sur site] L'évaluateur demandera la réalisation d'essais de mesures et de transmission des données lors de l'évaluation et vérifiera l'écart

ATTS-AR-420 - Fréquence de remontée des mesures d'écarts
La documentation précisera les modalités de mise en œuvre, et éventuellement de paramétrage des éléments suivants : - **Fréquence des mesures d'écarts** - **Fréquence de remontées des mesures au module de calcul** - **Modalité de remontées des mesures au module de calcul** -
Note de spécification :
Les remontées pourront par exemple se faire à l'issue de chaque mesure ou de façon asynchrone, par « batch » regroupant toutes les mesures d'une période donnée.
Documentation à fournir :
- Description du dispositif de remontée des traces - Test du dispositif
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le dispositif de remontée décrit est conforme à l'exigence. **[Evaluation sur site] L'évaluateur demandera à réaliser les essais en sa présence.**

ATTS-AR-430 - Protection de la remontée des mesures d'écarts
La remontée des mesures d'écarts doit faire l'objet de mesure de protection conforme au paragraphe 10.1.8. *Exigences relatives à la remontée des traces de synchronisation au système de supervision et de contrôle*
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.8.
Guide de validation :
Voir paragraphe 10.1.8.

6. Module A : Production du temps

6.1. Module A1 : Système de production du temps

Ce module définit l'ensemble des exigences applicables à un système de production compatible avec l'architecture du système (Module A)

6.1.1. Définition

Dans l'architecture, le système de production est installé au sein du système d'information et fournit le temps à un système de distribution. De ce fait, les exigences qui suivent portent principalement sur :

- le fonctionnement et les conditions d'opération du service ;
- le protocole d'échange avec les dispositifs de diffusion ;
- le protocole d'échange avec le service de supervision et de contrôle ;
- les conditions de raccordement au système de production ;
- les matériels mis en œuvre.

Options possibles

Pour la production du temps, le présent module identifie deux types de systèmes de production :

- les systèmes de production utilisant comme source de temps un laboratoire UTC(k) ;
- les systèmes de production utilisant comme source de temps une ou plusieurs horloges GTS conformes au module A2.

6.1.2. Contexte et Fonctionnalités du système de production

Le rôle du système de production est la production d'un temps exact et sécurisé et dont la traçabilité à UTC est garantie. Le temps produit est fourni à un système de distribution chargé de l'acheminer jusqu'au client. De ce fait, les principales fonctions attendues d'un service de production sont :

- la production sécurisée d'un temps traçable à UTC(k) avec une exactitude cible ;
- la fourniture d'une interface sécurisée pour le système de distribution ;
- la sécurisation et la traçabilité des synchronisations ;
- la remontée des informations de synchronisation à la consolidation et analyse des traces de supervision de l'architecture en vue de fournir une attestation du temps fourni.

Afin de réaliser ces fonctionnalités, le système de production peut s'appuyer :

- soit sur un UTC(k) ;
- soit à partir d'horloge GTS répondant aux exigences du module A2.

6.1.3. Objectifs du système de production

- Capacité de fournir du temps à l'exactitude cible.
- Mise à disposition des informations temps auprès d'un système de distribution
- Assurer la traçabilité des opérations.
- Remontée à la supervision de l'historique de synchronisation
- Remonter à la supervision des alertes locales
- Assurer la sécurité physique, logique et organisationnelle du service.

Si le système de production s'appuie sur des horloges de type Module A2 -Horloge GTS, il doit également remplir l'objectif suivant :

- Objectif 7 : Raccordement sécurisé des sources de temps par rapport à UTC.

6.1.4. Exigences relatives à la capacité à fournir du temps à l'exactitude cible

ATTS-A1-010 - Source de temps
La source de temps utilisée doit être : - **Fournie par un UTC(k) ayant un écart inférieur à 100 nanosecondes par rapport à UTC sur les 6 derniers mois.** - **Un composant horloge GTS conforme au module A2 du présent référentiel.**
Note de spécification :
Cette exigence est une exigence documentaire.
Documentation à fournir à l'évaluateur :
- Dans le cas UTC(k), les données de la Circulaire T du BIPM. - Dans le cas Horloge GTS, la référence et le certificat du module A2 de l'horloge GTS utilisée.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que les données sont conformes ou que le certificat est bien fourni.

ATTS-A1-020 - Documentation du raccordement au système de production.
La méthode de raccordement des serveurs de production à la source de temps doit être documentée.
Note de spécification :
Cette exigence est une exigence documentaire. Le raccordement doit principalement assurer que : - Le système de production utilise une source de temps certifiée - Le système de production est synchronisé conformément à l'exactitude cible - L'information temps n'est pas altérée lorsque celle-ci est récupérée.
Documentation à fournir à l'évaluateur :
- Un document descriptif de la méthode de raccordement mise en œuvre. - [Cas UTC(k)] Validation d'un responsable de la source UTC(k) - [Cas GTS] Constat de l'installateur de l'horloge GTS.
Guide de validation :
[Évaluation documentaire] L'évaluateur : - S'assurera que la documentation est fournie - L'évaluateur analysera la méthode de raccordement. La documentation doit être complète et suffisante pour comprendre le mécanisme mis en œuvre sans ambiguïté. [Évaluation fonctionnelle] Vérification du raccordement

ATTS-A1-030 - Exactitude du raccordement
La méthode de raccordement doit permettre d'acquérir le temps en conformité avec une exactitude 10 fois inférieure à l'exactitude cible de l'architecture du système qui dépendra de cette source.
Note de spécification :

Documentation à fournir :
- Description de la méthode de raccordement mise en œuvre ; - Description des mesures réalisées, de la méthode de mesure utilisée et calcul de l'incertitude introduite par la méthode de mesure. Le retard de distribution de la source de temps vers chaque serveur doit être pris en compte, selon l'exactitude recherchée. - Rapport d'essais avec résultats des mesures effectuées.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la méthode de mesure est adéquate vis-à-vis de l'exactitude cible visée. **Nota : Pour le calcul de l'incertitude, les méthodes du GUM seront privilégiées.** L'évaluateur vérifiera que les résultats de mesure sont conformes à l'exactitude cible visée. [Évaluation fonctionnelle] L'évaluateur fera réaliser des mesures et vérifiera que celle-ci est en adéquation avec l'exactitude cible et les mesures préalablement réalisées.

ATTS-A1-040 - Sécurisation du raccordement au système de production.
La méthode de raccordement doit garantir que : - **Les serveurs de production sont raccordés à la source de temps** - **La sécurité de la communication est assurée (intégrité et origine)**
Note de spécification :
La sécurité de l'environnement peut être obtenue : - Soit par sécurisation logique du flux - Soit par sécurisation physique du média transportant le flux.
Documentation à fournir :
- Description du raccordement - Description des mesures de sécurité mise en œuvre
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la méthode de raccordement mise en place assure une sécurité suffisante du raccordement. En particulier : - Un tiers ne doit pas pouvoir altérer sans difficulté significative le flux - Un tiers ne doit pas pouvoir changer l'origine du flux sans difficulté significative. [Évaluation fonctionnelle] L'évaluateur vérifiera que les mesures de sécurité décrites sont bien mises en œuvre.
Exemple d'implémentation satisfaisant l'exigence
Les solutions suivantes satisfont l'exigence : - sécurisation du flux logique par des moyens cryptographiques à l'état de l'art garantissant l'origine et l'intégrité (par exemple, signature électronique ou scellement des données, sécurisation du flux à l'aide du protocole SSL…) ; - isolation physique et logique du média transportant l'information (par exemple : média dédié) et mise en place de mesures de contrôle d'accès physique.

6.1.5. Exigences relatives à la fourniture du temps au service de distribution

ATTS-A1-050 - Exactitude du transport du temps
Le temps est fourni par le système de production aux systèmes de distribution avec une exactitude de +/- 10 µs par rapport à sa source de temps.
Note de spécification :
Cette exigence est applicable à l'ensemble des serveurs, c'est-à-dire aux serveurs de production principaux et aux serveurs de secours. L'exactitude est mesurée par rapport à la source de temps (Horloge GTS ou UTC(k) par exemple) La mesure pourra être établie en mesurant séparément les composantes temps et fréquences.
Documentation à fournir :
- Mécanisme de mesure mis en œuvre ; - Méthode de mesure et mesures réalisées.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les résultats de mesure sont conformes à l'exactitude cible visée et qu'ils couvrent l'ensemble des serveurs mis en production. Cette exigence est applicable à tous les serveurs du système de production, y compris les serveurs de secours. [Évaluation fonctionnelle] L'évaluateur demandera à réaliser des mesures et vérifiera que celle-ci est en adéquation avec l'exactitude cible. L'évaluateur procédera par échantillonnage en appliquant la méthode de la racine carrée[1].
Exemple d'implémentation satisfaisant l'exigence
La mesure de la fréquence pourra être réalisée en s'appuyant sur un PPS de sortie.

ATTS-A1-060 - Fréquence de synchronisation
Afin d'assurer à la fois l'exactitude du temps et la non-surcharge des serveurs de production, les serveurs de production doivent être synchronisés a minima toutes les 5 minutes. **La fréquence maximale de synchronisation doit être documentée.**
Note de spécification :
Dans le cas où la fréquence de synchronisation n'est pas fixée, mais peut varier en fonction du temps, la méthode doit être documentée.
Documentation à fournir :
- Description de la fourchette de synchronisation configurée sur les serveurs ; - Description de l'algorithme permettant d'optimiser la fréquence de synchronisation, si applicable ; - Exemples de trace de synchronisation démontrant que la fréquence de synchronisation est respectée.
Guide de validation :
[Évaluation documentaire] L'évaluateur - vérifiera si la fourchette de fréquence de synchronisation choisie est compatible avec l'exigence ; - vérifiera si l'algorithme ne présente pas de contradiction avec l'exigence ; - vérifiera par échantillonnage, que les fréquences constatées sur les traces de synchronisation sont

[1] La méthode de la racine carrée consiste à réaliser la vérification sur la racine carrée du nombre total d'éléments. Par exemple, sur une population de 100 éléments, on réalisera la vérification sur un échantillon de 10 éléments. Sur une population de 2500 éléments, on réalisera la vérification sur un échantillon de 50 éléments.

conformes à l'exigence. - évaluera l'algorithme permettant d'optimiser la fréquence de synchronisation [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que : - la configuration des serveurs correspond à la description ; - les fréquences de synchronisation réelles apparaissant dans les traces correspondent à la description.

6.1.6. Exigences relatives à la traçabilité du temps produit

Le transport du temps doit faire l'objet d'une traçabilité.

ATTS-A1-070 - Traçabilité du transport du temps
Les synchronisations entre les serveurs de production et la source de temps doivent être surveillées.
Note de spécification :
Documentation à fournir :
- Documentation expliquant comment la traçabilité est réalisée ; Exemples de traces générées.
Guide de validation :
[Évaluation documentaire] L'évaluateur : - s'assurera que la documentation est fournie ; - s'assurera que les traces fournies sont conformes à la documentation. [Évaluation fonctionnelle] L'évaluateur vérifiera par échantillonnage que les logs ont bien été produits et archivés (l'évaluateur choisira de façon arbitraire des dates et heures de synchronisation et l'audité lui fournira les traces correspondantes)
Exemple d'implémentation satisfaisant l'exigence
L'enregistrement systématique de toutes les traces de synchronisation PPS du serveur de production permet de satisfaire cette exigence.

ATTS-A1-080 - Protection des traces de synchronisation
Le système de production doit assurer la protection des traces générées contre la perte et/ou la modification.
Note de spécification :
Documentation à fournir :
- Description des mesures mises en place pour parer aux pertes et/ou modifications intentionnelles ou accidentelles.
Guide de validation :
[Évaluation documentaire] L'évaluateur s'assurera: - que la documentation est fournie et ; - que les mesures décrites sont pertinentes. [Évaluation fonctionnelle] L'évaluateur vérifiera que les mesures décrites sont implémentées.
Exemple d'implémentation satisfaisant l'exigence
Des mesures de restriction d'accès en écriture et d'externalisation des sauvegardes satisfont cette exigence.

6.1.7. Exigences relatives à la Remontée des traces à la Supervision

L'ensemble des traces de synchronisation générées par les différents composants de production (voir Section précédente) doivent être remontées au système de supervision et de contrôle. Cette remontée doit être réalisée de façon sécurisée.

ATTS-A1-090 - Mécanisme de remontée de traces à la supervision des serveurs de temps
Le système de production doit mettre en place un mécanisme de remontée des traces de l'ensemble des serveurs du système de production conformément aux Exigences relatives à la remontée des traces de synchronisation au système de supervision et de contrôle ». **[Cas GTS] Dans le cas où des horloges GTS sont utilisées, les traces de synchronisations des horloges doivent également être remontées au système de supervision et de contrôle.**
Note de spécification :
Documentation à fournir :
- Description du mécanisme en place
Guide de validation :
[Évaluation documentaire] L'évaluateur s'assurera : - que la documentation est fournie ; - que la documentation est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera par échantillonnage que les traces sont remontées

6.1.8. Exigences relatives à la surveillance et à la gestion des alertes

Le système de production doit mettre en place un mécanisme interne de gestion des alertes.

ATTS-A1-100 - Gestion interne des alertes
Le système de production doit répondre aux exigences communes concernant les exigences relatives à la surveillance et à la gestion des alertes
Note de spécification :
En particulier, la surveillance et la gestion des alertes générées doivent couvrir les serveurs de production et, le cas échéant, les horloges GTS ou les défauts du signal UTC(k).
Documentation à fournir :
- description de l'organisation mise en place pour remonter les exigences au système de supervision et de contrôle ; - liste des incidents pris en compte.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera qu'une organisation est en place. [Évaluation fonctionnelle] L'évaluateur : - vérifiera que le mécanisme est bien implémenté et est conforme à sa description ; - demandera à consulter la liste des incidents remontés à la supervision

ATTS-A1-110 - Notification des incidents à la supervision

Tout incident interne impactant la production du temps doit être remonté sans délai au service de supervision et de contrôle.
Note de spécification :
En particulier, cette exigence est applicable aux incidents impactant : - l'intégrité ou l'origine du temps distribué ; - l'exactitude du temps distribué ; - la disponibilité du temps.
Documentation à fournir :
- Description de la procédure mise en place pour remonter les exigences au système de supervision et de contrôle ; - Liste des incidents pris en compte.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera la procédure et son application. [Évaluation fonctionnelle] L'évaluateur : - vérifiera que le mécanisme est bien implémenté et est conforme à sa description ; - demandera à consulter la liste des incidents remontés à la supervision.

ATTS-A1-120 - Action en cas d'incident critique
Dans le cas d'un incident critique, le système de production doit : - **notifier immédiatement et sans délai l'entité responsable de l'architecture du système ;** - **stopper la production du temps sur tous les systèmes impactés ;**
Note de spécification :
Les incidents critiques incluent a minima la suspicion de compromission ou la compromission d'un élément majeur du service, ou le soupçon de la production d'un temps erroné.
Documentation à fournir :
- Procédure de notification et traitement des incidents critiques.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la procédure existe si celle-ci respecte l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à voir la liste des incidents critiques survenus et si la procédure a bien été appliquée.

ATTS-A1-130 - Seconde intercalaire

Au sein du système de production, un processus doit être mis en place permettant:
- **de surveiller les secondes intercalaires à venir ;**
- **de réaliser les opérations nécessaires pour que les serveurs de production soient en mesure de prendre en compte la seconde intercalaire et ne pas la considérer comme une anomalie ;**
- **de notifier la seconde intercalaire :**
  ○ **au(x) système(s) de supervision ;**
  ○ **au(x) système(s) de distribution.**

Note de spécification :
Documentation à fournir :
- Description de la procédure mise en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - la manière dont est gérée la seconde intercalaire est précisée dans la procédure. [Évaluation fonctionnelle] L'évaluateur vérifiera : - qu'une surveillance de la seconde intercalaire est bien mise en œuvre ; - par échantillonnage, que la procédure d'intervention sur les serveurs de distribution a bien été réalisée sur les secondes intercalaires ayant eu lieu.

6.1.9. Exigences relatives à la sécurité physique

ATTS-A1-140 - Exigences communes
Les sites d'exploitation du système de production doivent respecter les exigences communes relatives à la sécurité physique.
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.1.
Guide de validation :
Voir paragraphe 10.1.1.

ATTS-A1-150 - Inventaire des composants
Les serveurs de production et les horloges GTS sont des composants critiques, de ce fait, ils doivent être identifiés et inventoriés.
Note de spécification :
Cette exigence vient compléter l'exigence commune « Inventaire des composants »
Documentation à fournir :
- Liste des serveurs de production et des horloges GTS à jour.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la liste est disponible. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que la liste est à jour.

ATTS-A1-160 - Manipulation des composants
Les opérations suivantes sur les serveurs de production et, le cas échéant, les horloges GTS doivent a minima faire l'objet d'une traçabilité : - **installation sur site ;** - **mise en route ;** - **opération de maintenance ;** - **désinstallation et fin de vie**
Note de spécification :
Cette exigence vient compléter l'exigence commune « Manipulation des composants »
Documentation à fournir :
- Procédure de suivi des opérations sur les composants critiques décrits plus haut.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la procédure est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que le suivi est réalisé conformément à la procédure.

6.1.10. Exigences relatives aux ressources humaines

ATTS-A1-170 - Exigences communes
Les sites d'exploitation du système de production doivent respecter les exigences communes relatives aux ressources humaines du paragraphe 10.1.2
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.2
Guide de validation :
- Voir paragraphe 10.1.2

6.1.11. Exigences relatives à la sécurité logique

ATTS-A1-180 - Exigences communes
Les sites d'exploitation du système de production doivent respecter les exigences communes 10.1.8 relatives à la sécurité logique.
Note de spécification :
Documentation à fournir :
- Voir exigences communes 10.1.8 relatives à la sécurité logique.
Guide de validation :
- Voir exigences communes 10.1.8 relatives à la sécurité logique.

ATTS-A1-190 - Protection des sources de temps
Les sources de temps doivent être logiquement isolées des autres systèmes : - **elles ne doivent pas pouvoir être accessibles hors du système de production.** - **un système de distribution du temps de référence ne doit pas pouvoir se synchroniser directement sur une source de temps, seuls les serveurs de production doivent pouvoir se synchroniser.**
Note de spécification :
Documentation à fournir :
- Description des mesures d'isolation mises en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les mesures mises en œuvre sont conformes à l'exigence et que seuls les accès strictement nécessaires sont ouverts. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, la mise en place des mesures décrites.

ATTS-A1-200 - Interconnexion Réseau
L'interconnexion entre réseaux de production et les autres réseaux hors système de production (par exemple l'interface avec la supervision) doivent être protégés par des systèmes de sécurité configurés pour n'accepter que les protocoles nécessaires au fonctionnement du système de production.
Note de spécification :
Documentation à fournir :
- Schéma réseau ; - Description de la stratégie de configuration des systèmes de sécurité.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera que la mise-en-œuvre est conforme à la documentation. Cette vérification pourra être réalisée par échantillonnage.

ATTS-A1-210 - Filtrage des flux sortants
Le système de production doit laisser passer le flux permettant aux serveurs de production de remonter les traces de synchronisation vers la supervision.
Note de spécification :
Documentation à fournir :
Description du mécanisme en place
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le mécanisme décrit est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera par échantillonnage que la configuration du pare-feu est conforme à la description.

6.1.12. Protection des matériels réseaux

ATTS-A1-220 - Environnement physique
Le système de production doit garantir que les composants matériels (hors câblage) du réseau de production (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé.
Note de spécification :
Documentation à fournir :
- Description de l'environnement.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le l'environnement décrit est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera par échantillonnage que l'environnement est conforme à la description.

6.1.13. Sécurisation des échanges réseau

ATTS-A1-230 - Protection des échanges réseau
Des mesures de protection des flux réseau doivent être mises en œuvre afin d'assurer la confidentialité et l'intégrité des données qui y transitent.
Note de spécification :
Certains flux peuvent ne pas nécessiter de mettre en place des mesures de protection, mais cela doit être justifié (par exemple : échange de données non sensibles, protection physique du matériel, besoin de performance …). Le cas échéant, des mesures de sécurité adéquate (protection physique) doivent être mises en place.
Documentation à fournir :
- schéma des flux identifiant les flux sécurisés et non sécurisés ; - description de la mesure de sécurisation mise en œuvre ; - justification des flux non sécurisés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera par échantillonnage que la mise en œuvre est conforme à la description fournie.
Exemple d'implémentation satisfaisant l'exigence

La mise en place de certificats SSL ou de VPN permet de répondre à cette exigence.

6.1.14. Dimensionnement réseau

ATTS-A1-240 - Dimensionnement des serveurs de production
Les serveurs de production, et le cas échéant, le nombre d'horloges GTS doivent être dimensionnés pour supporter la charge de transactions. L'entité opérant la production doit mettre en place une architecture dimensionnée en adéquation avec le nombre de transactions prévues.
Note de spécification :
Documentation à fournir :
- Estimation de la charge ; - Estimation du dimensionnement ; - Mesure courant de la charge.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera que la charge réseau fait l'objet des mesures régulières.

ATTS-A1-250 - Surveillance et prévision
L'entité opérant le système de production a une obligation de surveillance du dimensionnement et de prévision de volumétrie à venir.
Note de spécification :
Documentation à fournir :
- Plan de charge incluant l'estimation de charge à venir ; - Mesure de la charge actuelle et passée.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation est fournie et si les estimations semblent réalistes vis-à-vis de l'historique mesuré.
Exemple d'implémentation satisfaisant l'exigence

6.1.15. Exigences relatives à la journalisation des événements

ATTS-A1-260 - Exigences communes
Les sites d'exploitation du système de production doivent respecter les exigences communes relatives à la journalisation des évènements.
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.4.
Guide de validation :
- Voir paragraphe 10.1.4.

ATTS-A1-270 - Événements spécifiques à la gestion du temps
L'ensemble des traces de synchronisation et, le cas échéant, des opérations de raccordement des éléments doivent être tracées.
Note de spécification :
Documentation à fournir :
Politique de synchronisation
Guide de validation :
[Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que les traces sont conservées.

6.1.16. Exigences relatives à la continuité d'activité

ATTS-A1-280 - Exigences communes
Les sites d'exploitation du système de production doivent respecter les exigences communes relatives à la continuité d'activité du paragraphe 0
Note de spécification :
Documentation à fournir :
- Voir paragraphe 0
Guide de validation :
- Voir paragraphe 0

ATTS-A1-290 - Disponibilité
Le système de production doit mettre en place une architecture de haute disponibilité. L'architecture doit être mise en place de façon à atteindre un niveau de disponibilité de 99,5% de chacune des fonctions critiques.
Note de spécification :
Les fonctions critiques comportent a minima : - la production du temps à destination du système de production (sortie du système) ; - la remontée des incidents à la supervision ; - la remontée des traces de synchronisation à la supervision.
Documentation à fournir :
- Description détaillée de l'architecture de haute disponibilité mise en place ou certifications existantes
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'architecture décrite est adéquate. [Évaluation fonctionnelle] L'évaluateur : - Vérifiera par échantillonnage, l'architecture décrite est bien mise en place ; - vérifiera que les mesures réelles de disponibilité sont en ligne avec le niveau de disponibilité de l'exigence et, le cas échéant, si les mesures ne sont pas en adéquation, que des mesures correctives sont mises en place ou planifiées.

6.2. Module A2 : Système (horloge) GTS et raccordement à UTC(k)

6.2.1. Définition

Dans l'architecture du système, une horloge GTS (ou GTS) est installée au sein d'un système de production. Ses performances en termes d'exactitude et de stabilité permettent au système de production de fournir les performances requises au système de distribution.

Les exigences qui suivent portent :

- Sur le produit lui-même (parties matérielles et logicielles)
- Sur le cycle de vie du produit
- Sur les entrées/sorties, physiques et logiques, du produit
- Sur l'étalonnage de l'horloge GTS

Le produit étant destiné à être utilisé dans un environnement contrôlé, sa sécurité est principalement procurée par son environnement. Il pourra se présenter sous la forme d'un seul produit ou de plusieurs éléments, physiques et logiciels, physiquement séparés.

6.2.2. Description de l'horloge GTS

Ses **fonctionnalités** principales sont :

- Produire le temps avec l'exactitude cible
- Remonter les informations de synchronisation pour la consolidation et l'analyse des traces de supervision de l'architecture.
- Gérer les états d'alerte
- Remonter à la supervision du système de production des alertes locales
- Mettre à disposition du serveur de production, opéré par le système de production, l'information temps dans l'exactitude cible
- Fournir une Interface d'administration
- Fournir une interface d'étalonnage

Elle doit **être protégée** contre les typologies d'attaque ou d'incidents suivants, pouvant compromettre la sécurité ou la traçabilité de l'architecture du système :

- Un attaquant se substitue à la GTS et fournit un temps compromis au système de production
- L'information temps est indisponible
- La GTS ne trace pas l'ensemble des synchronisations
- La GTS fournit au système de distribution un temps qui n'est pas dans l'exactitude cible.
- La GTS ne remonte pas les informations de synchronisation ou l'état des éléments du système pour la consolidation et l'analyse des traces de supervision de l'architecture
- Un attaquant altère/a accès en lecture aux données remontées à la supervision
- Un attaquant altère les la production du temps
- Un attaquant crée un déni de service sur la GTS
- Un élément ou utilisateur non autorisé se connecte à la GTS.

En conséquence, la GTS de remplir les objectifs suivants :

- Produire le temps de façon sécurisé en conformité avec l'exactitude cible.
- Mettre à disposition des serveurs de production l'information temps en conformité avec l'exactitude cible.
- Tracer l'ensemble des synchronisations réalisées

- Remonter à la supervision l'historique de synchronisation (synchronisation en aval) de façon sécurisée (intégrité et authentification mutuelle)
- Etre en mesure, en cas de détection d'anomalies, de réaliser des actions réactives adéquates.
- Remonter à la supervision les alertes locales (par exemple anomalie de synchronisation; entité amont non atteignable) de façon sécurisée (intégrité et authentification) et réception et prise en compte d'un état l'alerte fournie par la supervision [intégrité et garantie de l'origine]
- Etre administrable de façon sécurisé (authentification des administrateurs, protection des données échangées)
- Fournir une interface permettant de réaliser le raccordement de façon sécurisée.

6.2.3. Exigences relatives à la Production du temps

Exigences visant à produire le temps de façon sécurisé en conformité avec l'exactitude cible.

ATTS-A2-010 - Oscillateurs internes

Les horloges et/ou oscillateurs internes doivent répondre aux exigences d'exactitude et de stabilité suivantes:

Exactitude	**< 100ns**
Stabilité	< 5.0 * 10^{-13} s par jour.

Note de spécification :

Le type de matériel et/ou de technologie mis en œuvre est laissé libre au choix du constructeur.

Documentation à fournir :

- Description de l'exactitude et de la stabilité cible du produit
- Description de la méthode de mesure utilisée et de la caractérisation de l'incertitude de mesure.
- Résultats des essais réalisés par le constructeur

Guide de validation :

[Evaluation documentaire] L'évaluateur vérifiera

- Que l'exactitude cible est conforme à l'exigence
- Que la méthode de mesure est adaptée
- Que les résultats des essais réalisés par le constructeur sont en ligne avec l'exigence.

6.2.4. Exigences relatives à la synchronisation Aval

Exigences relatives à la synchronisation de la GTS avec l'élément en aval (serveur de production). Ces exigences sont principalement attachées l'objectif de mettre à disposition des serveurs de production l'information temps en conformité avec l'exactitude cible. En particulier, la GTS doit être en mesure de fournir le temps avec une exactitude donnée.

ATTS-A2-020 - Protocoles à supporter

Les GTS doivent se synchroniser avec l'élément aval (UTC(k)) du système de production qui se synchronise à l'aide à minima d'une sortie PTP.

La documentation devra préciser quelles sorties permettent d'atteindre l'exactitude cible du produit.

Note de spécification :

Il est possible d'implémenter d'autres protocoles de sorties, cependant, la documentation devra :

- Préciser ces derniers

- Préciser si ces sorties permettent d'atteindre la précision cible.
Documentation à fournir :
- Description des sorties fournies.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que les sorties décrites sont conformes à l'exigence/ **[Evaluation sur site] Sur l'échantillon fourni, l'évaluateur réalisera ses propres tests de compatibilité avec les protocoles indiqués.**

ATTS-A2-030 - Exactitude du temps produit
La GTS doit être en mesure de fournir l'exactitude de sortie suivante : < 100 ms
Note de spécification :
Cette exigence est applicable à l'ensemble des sorties de la GTS identifiées dans l'exigence précédente.
Documentation à fournir :
- Description de l'exactitude cible du produit - Description de la méthode de mesure utilisée et de la caractérisation de l'incertitude de mesure. - Résultats d'essais réalisés par le constructeur
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera - Que l'exactitude cible est conforme à l'exigence - Que la méthode de mesure est adaptée - Que les résultats des essais réalisés par le constructeur sont en ligne avec l'exigence. La mesure doit être réalisée pour chaque entrée et pour chaque type de protocole supporté.

ATTS-A2-040 - Priorité du flux temps.
Si une priorisation des flux, en mise en place, alors les flux temps doivent être prioritaires sur les autres.
Note de spécification :
Documentation à fournir :
- Description de du mécanisme de priorisation des flux, s'il existe.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que si un mécanisme est décrit, celui-ci donne bien la priorité aux flux temps dans le traitement.

ATTS-A2-050 - Mesure d'écart
L'ensemble des composants GTS doit avoir fait l'objet d'une mesure d'écart avec UTC(k) réalisée par un organisme membre de l'Arrangement de Reconnaissance mutuelle ou accrédité conformément au cahier d'exigences 10 du présent référentiel.
Note de spécification :
L'exigence est applicable aux horloges principales et de secours.
Documentation à fournir :
- Certificat de mesure réalisé par l'organisme susvisé. - Inventaire des horloges GTS mises en place.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera qu'un certificat de mesure est fourni pour chaque horloge GTS.

6.2.5. Exigences relatives à la Traçabilité

La GTS doit être en mesure :

- De générer des traces de l'ensemble des synchronisations et de l'ensemble des éléments pertinents, en particulier les raccordements réalisés.
- D'assurer la protection de ces traces.

6.2.6. Génération de traces

Il est en attendu que la GTS génère des traces pour l'ensemble des éléments pertinents quant à la traçabilité et de générer des traces suffisamment détaillées pour être exploitées.

ATTS-A2-060 - Exigences de Traçabilité
Une GTS doit être conforme à l'ensemble des exigences communes aux systèmes de l'architecture concernant la traçabilité.
Note de spécification :
Documentation à fournir :
Voir chapitre 10.
Guide de validation :
Voir chapitre 10.

En complément des exigences communes, une GTS doit satisfaire les exigences suivantes :

ATTS-A2-070 - Liste minimale des traces devant être générées
Une GTS doit générer un enregistrement d'audit des événements suivants: **a) Utilisation de l'interface de raccordement** **b) Synchronisation élément(s) aval** **c) Synchronisation interne de l'horloge interne**
Note de spécification :
La documentation fonctionnelle et/ou technique de la GTS devra lister les types d'événements et décrire les formats des traces.
Documentation à fournir :

- Exemple de traces générées par la GTS, couvrant l'ensemble des événements - Spécification fonctionnelle décrivant le format des traces - Description des tests et résultats des tests correspondant à l'exigence.
Guide de validation :
-

ATTS-A2-080 - Dysfonctionnement de la génération de trace
En cas d'arrêt ou de dysfonctionnement des fonctions de génération de traces (exemple: espace de stockage plein), la GTS doit se mettre à minima dans un état d'alerte majeure (elle peut continuer à fournir le temps, mais n'est plus en mesure de l'attester).
Note de spécification :
N/A
Documentation à fournir :
- Description fonctionnelle du mécanisme - Description du test et résultat de l'exécution du test.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie.

ATTS-A2-090 - Désactivation de la génération de trace
La GTS ne doit pas permettre de désactiver la génération des traces.
Note de spécification :
Documentation à fournir :
- Description des mécanismes mis-en-œuvre pour empêcher la désactivation de la génération des traces.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fonctionnelle répond bien à l'exigence.
Exemple d'implémentation satisfaisant l'exigence
Les solutions suivantes satisfont l'exigence : - Absence de fonction de désactivation de la génération - Existence d'une fonction de désactivation de la génération, mais celle-ci est rendue inactive - Existence d'une fonction de désactivation et mise en alerte critique de la GTS en cas de déclenchement de cette dernière.

6.2.7. Protection des traces

Exigences relatives à la protection des traces. La GTS doit assurer la protection en intégrité et en confidentialité des traces générées.

ATTS-A2-100 - Intégrité des traces générées
La GTS doit mettre en place un mécanisme de protection de l'intégrité des traces pour empêcher leur modification.
Note de spécification :
Un mécanisme de contrôle d'accès est considéré comme suffisant pour remplir cette exigence.
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description du test et résultat de l'exécution du test.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie.
Exemple d'implémentation satisfaisant l'exigence
Les mécanismes suivants répondent à l'exigence : - Contrôle d'accès - Mécanisme cryptographique de protection de l'intégrité (hash, chaînage, signature électronique).

ATTS-A2-110 - Confidentialité des traces générées
La GTS doit interdire à tous les utilisateurs le droit d'accès en lecture aux enregistrements d'audit, à l'exception de ceux à qui l'on a accordé un droit de lecture explicite (les administrateurs de sécurité, administrateurs usine).
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme Les tests devront être réalisés pour chaque classe d'utilisateurs. [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie.

6.2.8. Exigences relatives à la Remontée des traces à la Supervision

L'ensemble des traces générées par la GTS (voir paragraphe Exigences relatives à la Traçabilité) doivent être remontées au service de supervision et de contrôle. Cette remontée doit être réalisée de façon sécurisée.

ATTS-A2-120 - Mécanisme de remontée des traces
Le mécanisme de remontée des traces implémenté sur la GTS doit être conforme aux exigences communes relatives à la remontée des traces à la supervision du paragraphe 10.1.8.
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.8.
Guide de validation :
Voir paragraphe 10.1.8.

En complément, la GTS doit satisfaire des exigences suivantes.

6.2.9. Mécanisme de remontée des traces

Il est nécessaire que le mécanisme de remontée des traces assure :

- Que celles-ci soient remontées dans leur intégralité
- Que le format et le protocole de transport soient bien compatibles avec celui du système de supervision et de contrôle.

ATTS-A2-130 - Périmètre de remontée des traces à la supervision (traces pertinentes)

La GTS doit remonter au système de supervision certifié les traces pertinentes de synchronisation dans leur intégralité. Les traces considérées comme pertinentes sont :
- **Trace d'utilisation de l'interface de raccordement**
- **Traces de synchronisation avec l'élément aval**
  o **Identifiant de l'élément aval ou origine de la requête,**
  o **date et heure de la synchronisation**
  o **valeurs transmises**

Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :

[Evaluation documentaire] L'évaluateur vérifiera que :

- la description fonctionnelle répond bien à l'exigence
- la description du test met bien en œuvre le mécanisme décrit
- le résultat du test démontre bien l'efficacité du mécanisme

[Evaluation sur site]

L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie.

Cette vérification pourra être réalisée sur site.

ATTS-A2-140 - Périmètre de remontée des traces à la supervision (effacement des traces)
Le mécanisme mis en place doit permettre de s'assurer que les traces de supervision ne sont pas perdues. En particulier, il est attendu que le mécanisme ne permet la destruction éventuelle des traces sur la GTS qu'après que celle-ci ait reçu la confirmation explicite que les traces ont bien été collectées par le système de contrôle et de supervision.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - la description fonctionnelle répond bien à l'exigence - la description du test met bien en œuvre le mécanisme décrit - le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie.
Exemple d'implémentation satisfaisant l'exigence
L'effacement des traces après avoir reçu un accusé de réception de la part de la supervision satisfait cette exigence.

ATTS-A2-150 - Identification de la source des traces
Le protocole de remontée des traces doit permettre d'identifier la GTS de façon non ambiguë de façon à rattacher les traces à la GTS dans le référentiel du système de supervision.
Note de spécification :
Cette identification peut être faîtes au niveau du protocole ou au niveau des données fournies.
Documentation à fournir :
- Description du mécanisme d'identification de la GTS et référentiel d'identification retenu. - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien - Comment la GTS est identifiée. - Si cette identification est bien non ambiguë

- Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre. En particulier, il s'assurera que les identifiants remontés correspondent bien aux identifiants des échantillons.
Exemple d'implémentation satisfaisant l'exigence
Une remontée du numéro de série unique de la GTS répond à cette exigence.

6.2.10. Sécurisation de la remontée des traces

La remontée des traces doit être réalisée de façon sécurisée.

ATTS-A2-160 - Sécurisation de la remontée des traces à la supervision
La GTS doit utiliser un canal sécurisé pour transmettre les traces de synchronisation à la supervision. Ce canal doit être conforme aux exigences communes du paragraphe 10.1.8.
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.8.
Guide de validation :
Voir paragraphe 10.1.8.
Exemple d'implémentation satisfaisant l'exigence

ATTS-A2-170 - Méthode d'authentification de la GTS
La GTS doit utiliser un certificat SSL client pour s'authentifier auprès de la supervision. L'authentification par couple identifiant/mot de passe n'est pas autorisée pour une GTS.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien lune authentification par certificat. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que l'authentification par certificat décrite est bien mise-en-œuvre.*

ATTS-A2-180 - Changement de certificat
Un niveau administrateur est requis pour modifier le certificat d'authentification
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre pour changer le certificat d'authentification - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit une procédure de changement de certificat conforme à l'exigence. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre.

ATTS-A2-190 - Protocole d'échange
La GTS doit implémenter a minima le protocole TLS/SSL pour établir des communications sécurisées avec la supervision.
Note de spécification :
D'autres protocoles peuvent être mis en œuvre, mais TLS/SSL doit a minima être supporté.
Documentation à fournir :
- Description des protocoles mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien le support de TLS/SSL. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le protocole est bien supporté.

ATTS-A2-200 - Identification des serveurs de supervision
La GTS ne doit fournir les traces de supervision qu'aux serveurs autorisés dans sa configuration.
Note de spécification :
Documentation à fournir :
- Description du mécanisme permettant de spécifier à la GTS la liste des serveurs autorisés - Description des tests relatifs à l'exigence et résultats de l'exécution des tests Nota : les tests doivent couvrir les cas où la connexion au serveur principal échoue et la connexion à un serveur de secours est mise en œuvre.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien - Comment paramétrer, le cas échéant, les serveurs autorisés. - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le mécanisme est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Un produit où la liste des serveurs est fixée définitivement répond à cette exigence Un produit où la liste des serveurs peut être paramétrée par un administrateur ou en usine satisfait cette exigence.

ATTS-A2-210 - Stockage des traces
L'espace de stockage local des GTS doit être dimensionné de telle façon qu'elle puisse conserver ses traces de synchronisation localement pendant une période de 24h en cas de panne de la supervision.
Note de spécification :
- .
Documentation à fournir :
- Description de l'espace prévu - Rationnel justifiant que cet espace est suffisant
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien les éléments demandés et que l'espace est effectivement suffisant [Evaluation sur site] L'évaluateur réalisera ses propres mesures et vérifiera si elles sont en ligne avec les données du constructeur.

6.2.11. Exigences relatives à la gestion des anomalies

L'ensemble des exigences suivantes ont pour objectif de permettre à la GTS d'être en mesure, en cas de détection d'anomalies, de réaliser des actions réactives adéquates.

En particulier, l'GTS doit être en mesure :

- De générer des alertes en cas de détection d'un élément anormal
- De prendre en compte des informations d'anomalie fournies par la supervision
- De notifier les alertes à l'utilisateur
- De réaliser automatiquement certaines actions en cas d'anomalie
- De revenir dans un état sûr après l'apparition d'une anomalie.

6.2.12. Génération et Gestion des alertes.

La génération des alertes peut survenir dans différents cas de figure. En particulier :

- En cas d'anomalie sur l'horloge GTS
- En cas d'anomalie lors d'autotest de la GTS.

ATTS-A2-220 - Alerte autonomie supervision
La GTS doit générer une alerte en cas d'incapacité à remonter les événements à la supervision pendant une durée supérieure à 2 heures.
Note de spécification :
Documentation à fournir :
- Description des anomalies - Description des tests et résultats de tests associés
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - la documentation décrit bien l'anomalie décrite dans cette l'exigence - la description des tests couvre bien cette anomalie - le résultat du test démontre bien l'implémentation du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

ATTS-A2-230 - Alerte en cas de tentative d'accès administrateur
En cas d'échecs successifs sur l'interface d'administration, la GTS doit lever une alerte.
Note de spécification :
Cette exigence est applicable à l'ensemble des interfaces d'administration.
Documentation à fournir :
- Description des anomalies - Description des tests et résultats de tests associés
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien - L'anomalie décrite dans cette l'exigence.

- que la description des tests couvre bien cette anomalie - que le résultat du test démontre bien l'implémentation du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. L'évaluateur réaliser un test indépendant en laboratoire sur un échantillon fourni.
Exemple d'implémentation satisfaisant l'exigence
Un mécanisme de levée d'alerte après 3 échecs successifs répond à l'exigence.

ATTS-A2-240 - Autotest de l'horloge interne
Diagnostic sur l'horloge interne: la GTS doit pouvoir diagnostiquer l'état de son horloge interne. En cas d'anomalie dans le diagnostic, une alerte critique doit être levée. **Le diagnostic doit être réalisé à la fréquence suivante: au moins une fois par jour et à chaque démarrage.**
Note de spécification :
Une fréquence plus élevée peut-être mise en œuvre.
Documentation à fournir :
- Description du diagnostic réalisé et de la fréquence
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien le diagnostic réalisé et la fréquence.
Exemple d'implémentation satisfaisant l'exigence
Un mécanisme qui vérifie toutes les 5 minutes un rapport de diagnostic généré par l'horloge satisfait l'exigence.

ATTS-A2-250 - Autotest du firmware au démarrage
La GTS doit réaliser un test d'intégrité du firmware à chaque démarrage. La méthode de vérification d'intégrité doit s'appuyer sur un algorithme cryptographique conforme à l'état de l'art.
Note de spécification :
L'état de l'art est établi par l'organisme national en charge de la sécurité des systèmes d'information.
Documentation à fournir :
- Description du test de firmware réalisé - Description des tests et résultats de tests associés
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien - le mécanisme de test du firmware. - que le mécanisme est conforme à l'état de l'art - que le résultat du test démontre bien l'implémentation du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre.
Exemple d'implémentation satisfaisant l'exigence
Pour la France, l'utilisation d'une signature électronique du firmware conforme aux recommandations de l'ANSSI satisfait l'exigence**.**

ATTS-A2-260 - Autotest des modules d'entrées et de sorties.
Diagnostic des modules de sortie: la GTS doit pouvoir diagnostiquer l'état de ses modules d'entrée et de sortie. En cas d'anomalie sur le module de sortie, une alerte critique doit être levée. **En cas d'anomalie sur le module d'entrée, une alerte majeure doit être levée et le module doit être exclu du calcul du temps.** **Le diagnostic doit être réalisé à la fréquence suivante: au moins une fois par heure pour chaque sortie.**
Note de spécification :
Documentation à fournir :
- Description du diagnostic réalisé et de la fréquence
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien le diagnostic réalisé et la fréquence.

6.2.13. Notification des anomalies

En cas d'anomalie, la GTS doit le notifier visuellement à l'utilisateur.

ATTS-A2-270 - Notification des anomalies
Un voyant visuel sur la GTS doit notifier l'utilisateur d'une anomalie.
Note de spécification :
Documentation à fournir :
- Documentation utilisateur décrivant la signification des anomalies visuelles - Description des tests du mécanisme et résultat d'exécution des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation utilisateur décrit bien le voyant d'anomalie. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme pour les différents types d'anomalies possibles (a minima mineure, majeure, critique) [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre.
Exemple d'implémentation satisfaisant l'exigence
Un voyant s'éclairant en cas d'anomalie satisfait cette exigence.

6.2.14. Actions réactives en cas d'anomalie

En cas d'anomalie, les GTS peuvent avoir une réaction automatique visant à corriger l'anomalie.

ATTS-A2-280 - Réactions automatiques aux alertes
Les GTS peuvent avoir des règles de réactions aux alertes. La documentation des GTS doit documenter l'ensemble de ces règles de réaction.
Note de spécification :
Documentation à fournir :
- Description des règles de réaction - Description des tests associés et résultats de tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien les règles de réaction et que chacune d'elle fait l'objet d'un test. Il vérifiera que le résultat du test démontre bien l'implémentation du mécanisme pour les différents types de règles. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre.

6.2.15. Retour en mode sûr en cas d'anomalie

Suite à une action corrective, qu'elle soit automatique ou manuelle, si l'anomalie est corrigée, la GTS retournera dans son état nominal. Les exigences qui suivent sont relatives à ce retour en mode sûr.

ATTS-A2-290 - Retour en mode sûr
Pour les alertes de niveau mineur à majeur, la GTS doit garantir le retour à un état sûr en utilisant des procédures automatisées. **Pour une alerte de niveau critique, une procédure manuelle doit être nécessaire.**
Note de spécification :
Documentation à fournir :
- Description du mécanisme de remise en état sûr - Description des tests associés et résultats de tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien les éventuelles règles de remise en état sûr pour les différents types d'anomalies et qu'ils sont conformes à l'exigence. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme pour les différents types de règles. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre.

6.2.16. Exigences relatives à la communication des anomalies avec la supervision

Une GTS doit remonter de façon sécurisée l'ensemble des alertes générées localement à la supervision.

ATTS-A2-300 - Canal sécurisé
La GTS doit utiliser le canal sécurisé pour transmettre les alertes à la supervision du système de production. Ce canal doit être conforme aux exigences décrites dans le paragraphe 10.1.8. concernant la remontée des traces
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.8.
Guide de validation :
Voir paragraphe 10.1.8.

ATTS-A2-310 - Complétude des alertes remontées
La GTS doit fournir à la supervision l'intégralité des alertes locales générées. Le mécanisme mis en place doit permettre de s'assurer qu'aucune alerte n'est perdue.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests associés et résultats de tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit le mécanisme et qu'il est conforme à l'exigence. Il vérifiera le résultat du test démontre l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. **[Essais]** **Des essais indépendants complémentaires peuvent être réalisés en laboratoire sur les échantillons fournis.**

ATTS-A2-320 - Délai de remontée des alertes
La GTS doit fournir à la supervision une alerte dans les meilleurs délais et au plus tard dans les 20 secondes après sa génération.
Note de spécification :
Ce délai n'est pas applicable en cas de non-disponibilité de la supervision.
Documentation à fournir :
- Mesure réalisée par le constructeur et description de la méthode de mesure.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit la méthode de mesure et que le résultat est conforme à

l'exigence. [Evaluation sur site] L'évaluateur rejouera le test afin de constater la conformité à la mesure fournie par le constructeur.

6.2.17. Exigences relatives à l'administration de la GTS

La GTS doit pouvoir être administrée de façon sécurisée. Les exigences qui suivent concernent l'authentification des administrateurs et la protection des données échangées.

6.2.18. Interface d'administration

La GTS doit fournir une ou plusieurs interfaces permettant de réaliser son administration.

ATTS-A2-330 - Présence d'une interface d'administration
La GTS doit fournir une ou plusieurs interfaces permettant d'administrer le produit. **Au moins une des interfaces doit permettre à un service de supervision d'administrer la GTS à distance.**
Note de spécification :
Si la GTS présente plusieurs interfaces d'administration (API, terminal physique sur la GTS, interface console…), ou permet d'accéder à l'interface d'administration de plusieurs méthodes différentes, les exigences de ce chapitre s'appliquent à chacune des interfaces et/ou chacune des méthodes.
Documentation à fournir :
- Description des interfaces
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien les interfaces d'administration et qu'il existe bien une interface d'administration à distance dédiée à la supervision [Evaluation sur site] L'évaluateur se connectera à chacune des interfaces de la GTS.
Exemple d'implémentation satisfaisant l'exigence
Un produit ne disposant que d'une seule interface à distance satisfait cette exigence.

6.2.19. Rôle permettant l'administration

La GTS peut mettre en place différents niveaux d'administration, de façon à ce que seuls des utilisateurs autorisés puissent réaliser certaines opérations.

ATTS-A2-340 - Niveau d'administration
La GTS doit gérer au moins un rôle d'administration
Note de spécification :
Si d'autres niveaux existent, le constructeur devra fournir une table de correspondance. A minima un niveau d'administrateur doit être en place.
Documentation à fournir :
- Description des niveaux d'administration
Guide de validation :
L'évaluateur vérifiera que les niveaux décrits sont conformes à l'exigence.

6.2.20. Authentification des administrateurs

Le rôle d'administrateur ne peut être obtenu qu'après une authentification. Cette section présente les exigences relatives à l'authentification des administrateurs.

ATTS-A2-350 - Authentification des rôles
Pour chacune des interfaces d'administration, les rôles permettant l'administration ne peuvent être obtenus qu'après une authentification
Note de spécification :
Documentation à fournir :
- Description du mécanisme d'authentification - Description des tests d'authentification et résultat des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation utilisateur décrit le mécanisme d'authentification pour chacune des interfaces et chacun des rôles. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre.

ATTS-A2-360 - Expiration des sessions
L'interface d'administration doit disposer d'un mécanisme de fermeture automatique de session à partir d'une durée d'inactivité.
Note de spécification :
La durée de session peut être paramétrable. Le mécanisme est applicable à toutes les interfaces.
Documentation à fournir :
- Description du mécanisme de fermeture de session - Description des tests d'authentification et résultat des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation utilisateur décrit le mécanisme de fermeture de session pour chacune des interfaces et la durée par défaut. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre.

ATTS-A2-370 - Sécurisation des sessions distantes
Si un administrateur se connecte à distance (via un protocole réseau par exemple), la connexion doit être sécurisée et assurer - **l'intégrité et la confidentialité des données échangées** - **l'authentification de la GTS.**
Note de spécification :
Si l'interface d'administration est obtenue via un terminal intégré à la GTS ou en branchant directement un écran et un clavier sur la GTS, cette exigence n'est pas applicable.
Documentation à fournir :
- Description du protocole réseau mis en œuvre.

- Description des tests d'authentification et résultat des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit le mécanisme mis en œuvre. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Un canal SSL avec chiffrement satisfait cette exigence.

ATTS-A2-380 - Authentification en échec
La GTS doit être en mesure de détecter les tentatives de connexion en échec. **En cas de tentative successive, la GTS doit mettre en place une contre-mesure la protégeant d'une attaque de type force brute.**
Note de spécification :
- Description de la contre-mesure mise en œuvre. - Description des tests et résultat des tests.
Documentation à fournir :
-
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit le mécanisme mis en œuvre. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Des contre-mesures, telles qu'un temps d'attente croissant entre chaque tentative ou l'apparition d'un captcha permet de se prémunir contre de telles attaques.

6.2.21. Paramètres d'administration

Exigences concernant les actions et modifications de configuration permises.

ATTS-A2-390 - Rôle public
La configuration ne peut être modifiée que par un administrateur
Note de spécification :
Documentation à fournir :
- Description de la liste des paramètres pouvant être modifiés par le rôle public
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la liste des paramètres satisfait l'exigence [Evaluation sur site] L'évaluateur vérifiera sur chaque interface que la liste des paramètres est conforme à la description.

ATTS-A2-400 - Configuration restrictive par défaut
La configuration par défaut de la GTS doit systématiquement prendre en compte, pour chaque paramètre, la valeur la plus restrictive.
Note de spécification :
Documentation à fournir :
- Description des valeurs par défaut
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que les valeurs par défaut sont bien restrictives. [Evaluation sur site] L'évaluateur vérifiera que les valeurs par défaut présentes sur l'échantillon sont bien celles décrites dans la documentation.

6.2.22. Gestion des mises à jour

La partie logicielle d'une GTS n'est pas figée au cours du temps. Elle peut être mise à jour, de façon à corriger ou faire évoluer le code du produit. La mise à jour est une opération critique qui doit pouvoir être réalisée en toute sécurité.

Afin de corriger dans un délai raisonnable les éventuelles failles de sécurité, la GTS doit pouvoir être mise à jour avec un mécanisme permettant le retour en arrière.

ATTS-A2-410 - Mise à jour de la GTS
La GTS doit pouvoir être mise à jour afin de corriger les éventuelles failles de sécurité.
Note de spécification :
Documentation à fournir :
- Description du processus de mise à jour.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le processus de mise à jour est bien décrit.

ATTS-A2-420 - Annulation de Mise à jour de la GTS
Toute mise à jour logicielle d'un élément de la GTS doit pouvoir être annulée de façon à revenir à la version précédente.
Note de spécification :
Documentation à fournir :
- Description du mécanisme de retour en arrière - Descriptions des tests et résultats des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le processus de retour en arrière est décrit. L'évaluateur vérifiera qu'un test permet de vérifier que le mécanisme de retour en arrière est effectif.

[Evaluation sur site] L'évaluateur rejouera les tests.

ATTS-A2-430 - Arrêt de la fourniture du temps lors d'une mise à jour de la GTS
La fourniture du temps doit être interrompue lors d'une mise à jour et jusqu'à la fin de celle-ci. En cas d'échec de mise à jour, la fourniture du temps ne doit pas être rétablie.
Note de spécification :
Il est important, lors de la mise à jour, que la question de la diffusion du temps soit prise en compte.
Documentation à fournir :
- Description du mécanisme d'arrêt de distribution du temps lors d'une mise à jour - Descriptions des tests et résultats des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le mécanisme est décrit. L'évaluateur vérifiera qu'un test permet de vérifier que le mécanisme est effectif. [Evaluation sur site] L'évaluateur rejouera les tests.

6.2.23. Exigence relative au raccordement

ATTS-A2-440 - Interface de raccordement
LA GTS doit disposer d'une interface de raccordement. Cette interface doit fournir a minima : **1. PPS de sortie** **2. Une interface d'ajustement du PPS de sortie** **3. Une interface de mise à l'heure (étalonnage en temps)**
Note de spécification :
Nota : l'interface PPS de sortie pourra être désactivée après raccordement.
Documentation à fournir :
- Description des mécanismes mis en œuvre. - Descriptions des tests et résultats des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le mécanisme est décrit. L'évaluateur vérifiera qu'un test permet de vérifier que le mécanisme est effectif. [Evaluation sur site] L'évaluateur rejouera les tests des interfaces.

ATTS-A2-450 - Authentification à l'interface de raccordement
Les actions d'ajustement en temps et en fréquence ne doivent être possibles que pour des administrateurs authentifiés.
Note de spécification :
Documentation à fournir :
- Description des mécanismes d'authentification mis en œuvre. - Descriptions des tests et résultats des tests.

Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le mécanisme est décrit. L'évaluateur vérifiera qu'un test permet de vérifier que le mécanisme est effectif. [Evaluation sur site] L'évaluateur rejouera les tests des interfaces**.**

6.2.24. Installation de la GTS

Une mauvaise installation et/ou configuration initiale de la GTS pourrait impacter la sécurité de l'architecture du système. De ce fait, l'installation de la GTS doit être réalisée de façon sécurisée.

ATTS-A2-460 - Installation et mise en œuvre opérationnelle de la GTS
L'installation initiale de la GTS doit être mise en œuvre par le fabricant et/ou une personne spécifiquement formée par le fabricant suivant la procédure d'installation. Un test de bon fonctionnement doit être réalisé conformément à une procédure préétablie et un PV de mise en fonction doit être rédigé, signé et archivé par le fabricant et par le client.
Note de spécification :
Seule la conservation de l'exemplaire du fabricant est dans le périmètre audité. Le PV peut-être sous forme papier ou sous forme électronique. S'il est sous forme électronique, des signatures électroniques conformes à la réglementation nationale doivent être utilisées.
Documentation à fournir :
- Modèle de PV - Exemplaires de PV remplis.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera par échantillonnage que les PV de mise en fonction sont effectivement rédigés.
Exemple d'implémentation satisfaisant l'exigence
Un PV sous forme papier satisfait l'exigence Au sein de l'Union européenne, un PV sous forme électronique muni de signature ou de cachet électronique conforme au Règlement eIDAS satisfait l'exigence.

ATTS-A2-470 - Conditions d'exploitation
Les horloges GTS doivent être exploitées conformément aux recommandations des guides d'installation et d'utilisation
Note de spécification :
L'exigence est applicable aux horloges principales et de secours.
Documentation à fournir :
- Procédures d'exploitation des horloges GTS
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera la présence des procédures d'exploitation. [Évaluation fonctionnelle] L'évaluateur vérifiera que les procédures sont connues et appliquées par les exploitants.

6.2.25. Maintenance et suivi

Après l'installation, il est nécessaire d'assurer un suivi et une maintenance de la GTS.

ATTS-A2-480 - Principe de maintenance
Le fabricant doit s'engager à maintenir son parc de GTS en condition opérationnelle. En particulier, il doit être en mesure de fournir pendant 5 ans des pièces de rechange ou de proposer un échange standard du matériel pour un matériel équivalent.
Note de spécification :
Documentation à fournir :
- Contrat type avec clause d'engagement, procédures internes
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera par échantillonnage que les clauses sont bien présentes dans les contrats.

ATTS-A2-490 - Vérification sur site
Le fabricant doit annuellement mettre en œuvre une vérification sur site du bon fonctionnement de la GTS. Toutes les GTS n'ayant pas fait l'objet d'un audit annuel ou présentant des anomalies devront être déconnectées.
Note de spécification :
Documentation à fournir :
- Procédure de vérification sur site de la GTS - Liste des éléments ayant été déconnectés. - Planning à venir et liste des GTS ayant fait l'objet d'une vérification annuelle.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera par échantillonnage que les clauses sont bien présentes dans les contrats.

6.2.26. Sécurité physique de la GTS

La GTS doit assurer sa sécurité physique.

ATTS-A2-500 - Intrusion physique
La GTS doit offrir la capacité de déterminer si une intrusion physique a eu lieu.
Note de spécification :
Documentation à fournir :
- Documentation de la solution mise en œuvre.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera dans la documentation qu'un dispositif est bien mis en place [Evaluation sur site] L'évaluateur vérifiera que le dispositif décrit est bien présent sur les échantillons.

6.2.27. Documentation

ATTS-A2-510 - Documentation à destination du client
La documentation de la GTS fournie au client doit contenir a minima: - **Un guide d'utilisation** - **Un guide d'installation**
Note de spécification :
Les deux guides peuvent être présentés sous la forme d'un seul document, ou sous la forme de plusieurs documents spécifiques.
Documentation à fournir :
- Guide d'utilisation - Guide d'installation - Description de la façon dont la documentation est remise au client
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que les documents existent pour le modèle évalué et évaluera si la façon de le mettre à disposition du client est appropriée
Exemple d'implémentation satisfaisant l'exigence
La remise au client sous forme papier en le livrant avec le produit satisfait l'exigence La mise à disposition du client par email ou par téléchargement satisfait l'exigence.

6.2.28. Exigences relatives à la sécurité physique

ATTS-A2-520 - Exigences communes
Les sites d'exploitation du système de production doivent respecter les exigences communes relatives à la sécurité physique.
Note de spécification :

Documentation à fournir :
Voir paragraphe 10.1.1.
Guide de validation :
Voir paragraphe 10.1.1.

6.2.29. Exigences relatives aux ressources humaines

ATTS-A2-530 - Exigences communes
Les sites d'exploitation du système de production doivent respecter les exigences communes relatives aux ressources humaines du paragraphe 10.1.2
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.2
Guide de validation :
- Voir paragraphe 10.1.2

6.2.30. Exigences relatives à la sécurité logique

ATTS-A2-540 - Exigences communes
Les sites d'exploitation du système de production doivent respecter les exigences communes 10.1.3 relatives à la sécurité logique.
Note de spécification :
Documentation à fournir :
- Voir exigences communes 10.1.3 relatives à la sécurité logique.
Guide de validation :
- Voir exigences communes 10.1.3 relatives à la sécurité logique.

6.2.31. Protection des environnements de développement, de test et de production de la GTS

ATTS-A2-550 - Environnement sécurisé
Les environnements de développement, de test et de production de la GTS doivent faire l'objet de mesures de protection physiques et logiques, en particulier de Contrôle d'accès physique et logiques permettant l'accès aux seules personnes autorisées.
Note de spécification :
Une certification ISO 27001 n'est pas requise, cependant, elle permet de justifier la mise en œuvre des mesures.
Documentation à fournir :
Description des mesures de protection physiques et logiques,
Guide de validation :
Exemple d'implémentation satisfaisant l'exigence
Une prise en compte des mesures dans le cadre d'une certification ISO 27001 satisfait l'exigence.

6.2.32. Gestion de configuration du produit

ATTS-A2-560 - Identification du modèle de GTS
Chaque modèle de GTS doit être clairement identifié par un identifiant unique.
Note de spécification :
L'identification du modèle de GTS peut-être composé d'un numéro de modèle et d'un numéro de version.
Documentation à fournir :
- Description de la nomenclature des numéros de version - Fourniture du numéro du modèle évalué
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fournie permet d'identifier de façon unique le modèle de GTS [Evaluation sur site] L'évaluateur vérifiera sur les échantillons fournis que le modèle correspond bien à la version fournie par le constructeur.

ATTS-A2-570 - Identification de la GTS
Pour chaque modèle de GTS donné, un numéro d'identifiant unique doit être assigné à chaque exemplaire de la GTS.
Note de spécification :
Documentation à fournir :
- Description de la méthodologie mise en place pour assurer l'unicité
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fournie permet de s'assurer que chaque GTS a un numéro unique. [Evaluation sur site] L'évaluateur vérifiera par échantillonnage que les numéros de série sont bien différents les uns des autres.

ATTS-A2-580 - Inventaire de configuration
Pour chaque modèle de GTS, l'ensemble des composants matériels et logiciels doivent être clairement identifiés, inventoriés, et tenus à jour. Un historique des changements de cet inventaire doit être conservé.
Note de spécification :
Documentation à fournir :
- Description de la méthode de gestion de configuration utilisée
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fournie permet de satisfaire l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que l'historique des changements est conservé.
Exemple d'implémentation satisfaisant l'exigence
Cela peut être réalisé par un checksum logiciel

6.2.33. Gestion des Failles de sécurité

ATTS-A2-590 - Veille technique
Le constructeur de la GTS doit effectuer une veille technique sur les vulnérabilités pouvant affecter les composants et doit mettre en œuvre, le cas échéant, des correctifs.
Note de spécification :
Documentation à fournir :
- Description de la procédure de veille technique mise en œuvre.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fournie permet de satisfaire l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à voir la liste des vulnérabilités identifiées et les actions correctives réalisées, le cas échéant. Selon le nombre de vulnérabilités, la vérification pourra être réalisée par échantillonnage.

ATTS-A2-600 - Remontée des failles de sécurité
Le constructeur doit mettre en place une procédure documentée permettant au client de remonter des vulnérabilités sur le produit et prendre en compte les éventuelles failles remontées.
Note de spécification :
Documentation à fournir :
- Description de la procédure de remontée des vulnérabilités.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fournie permet de satisfaire l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à voir la liste des vulnérabilités remontées par les clients, si celle-ci est applicable, et les actions correctives réalisées, le cas échéant. Selon le nombre de vulnérabilités, la vérification pourra être réalisée par échantillonnage.
Exemple d'implémentation satisfaisant l'exigence

Un suivi à l'aide d'un « bugtracker » type Mantis satisfait l'exigence.

6.2.34. Essai de la GTS par le fabricant

Avant délivrance au client et/ou mise en production, le constructeur doit tester les GTS.

ATTS-A2-610 - Vérification de la conformité du produit par le constructeur
Le constructeur doit mettre en place une procédure documentée de test permettant de couvrir fonctionnellement la GTS. Cette suite de test doit être exécutée sur un exemplaire représentatif du modèle de GTS. La suite de test et le processus de test doivent être documentés et un PV, spécifiant la liste des tests exécutés et leur résultat doit être conservé.
Note de spécification :
Documentation à fournir :
- Description de la procédure de test - Description des tests réalisés - Résultats des tests réalisés
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que - la procédure de test existe et est exécuté à chaque nouvelle version. - les résultats des tests sont conservés. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer l'ensemble ou un sous-ensemble des tests (selon le nombre de tests et leur durée d'exécution) et comparera aux résultats fournis et à la description de la procédure fournie.
Exemple d'implémentation satisfaisant l'exigence

ATTS-A2-620 - Test du produit avant délivrance au client
Le fabricant doit mettre en place une procédure documentée de test permettant de s'assurer que la GTS est conforme aux exigences du fabricant avant sa délivrance au client. La documentation devra préciser les tests réalisés et la méthode mise en œuvre.
Note de spécification :
Documentation à fournir :
- Description de la procédure de test - Description des tests réalisés - Résultats des tests réalisés
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que - la procédure de test existe. - la méthode mise en œuvre est adéquate. [Évaluation fonctionnelle] Par échantillonnage, l'évaluateur vérifiera que les tests sont bien réalisés.

6.2.35. Etalonnage de la GTS et raccordement à UTC(k)

Les exigences qui suivent sont applicables à un organisme accrédité chargé de valider le raccordement d'une horloge GTS.

Pour cela, l'étalonnage de la GTS doit être réalisé par un organisme accrédité. Les exigences suivantes sont relatives à l'accréditation de l'organisme et à la méthode d'étalonnage.

L'organisme en charge de la validation du raccordement doit :

- Avoir l'expertise pour réaliser l'étalonnage
- Réaliser l'opération de validation du raccordement de façon sécurisée
- Assurer la traçabilité de l'opération.

ATTS-A2-630 - Accréditation
L'organisme doit être accrédité ISO 17025 avec une portée pertinente ou être membre du CIPM MRA avec des CMS pertinents en cours de validité.
Note de spécification :
Documentation à fournir:
- Certificat ISO 17025 avec portée en cours de validité ou justificatif de la qualité de laboratoire membre du CIPM MRA avec CMC.
Guide de validation :
[Vérification documentaire] L'évaluateur vérifiera les documents fournies.

ATTS-A2-640 - Expertise requise
L'organisme doit être en mesure, préalablement à la réalisation de l'étalonnage, de démontrer son expertise technique: - **Pour la source UTC(k) choisie comme référence** - **Pour le matériel GTS cible** - **Pour la précision de synchronisation demandée**
Note de spécification :
Cette expertise doit être démontrée pour chaque expert individuel choisi. Si l'expertise individuelle n'est que partielle, alors une équipe combinant plusieurs experts doit être mise en œuvre.
Documentation à fournir:
- Liste des experts et justification de leur expertise.
Guide de validation :
[Vérification documentaire] L'évaluateur vérifiera les justifications fournies.
Exemple d'implémentation satisfaisant l'exigence
Les exemples suivants sont considérés comme suffisants : - Formation sur matériel GTS cible par le manufacturier et ; - Formation spécifique dispensée par l'organisme UTC(k) choisi comme référence ; - Expérience similaire sur des opérations de raccordement pour la précision visée (ou réalisation d'au moins un stage d'observation et un stage pratique supervisé sur une opération similaire. - Domaine couvert par la portée de l'accréditation 17025

ATTS-A2-650 - Maintien de l'expertise
L'organisme doit s'engager à maintenir les compétences au cours du temps. En cas d'incapacité à maintenir les compétences, l'organisme devra notifier à l'entité responsable de son incapacité, temporaire ou permanente, à réaliser les validations de raccordement.
Note de spécification :
Documentation à fournir:
- Justification de sa politique de maintenance de l'expertise et des compétences - Liste des incapacités temporaires notifiée
Guide de validation :
[Vérification documentaire] L'évaluateur vérifiera les justifications fournies.
Exemple d'implémentation satisfaisant l'exigence
La mise en place d'un plan de formation de nouveaux experts permet de satisfaire l'exigence Ce point peut être couvert par l'accréditation ISO17025.

ATTS-A2-660 - Etalonnage
L'organisme doit, préalablement à l'intervention, préparer un dossier présentant - **Le périmètre de l'intervention** - **L'exactitude cible visée** - **la méthode d'étalonnage choisie.** **Cette méthode doit faire l'objet d'une acceptation formelle par l'organisme opérant l'GTS**
Note de spécification :
Documentation à fournir:
- Plan d'intervention
Guide de validation :
[Vérification documentaire] L'évaluateur vérifiera par échantillonnage que les plans d'intervention sont bien conformes à l'exigence et ont bien fait l'objet de validation
Exemple d'implémentation satisfaisant l'exigence
Une signature du plan par les différentes parties satisfait l'exigence de validation et d'acceptation formelle.

ATTS-A2-670 - Intervention
L'intervention de raccordement doit comporter les étapes suivantes : - **Mesure, par l'organisme accrédité, de l'écart entre le système cible (l'instrument) et un étalon de référence (top d'un UTC(k)), sous couvert de son accréditation.** - **Si l'instrument est hors des spécifications, alors une opération d'ajustage doit être réalisée par l'opérateur du système de production.** - **Une nouvelle mesure est réalisée après opération d'ajustage.** **L'intervention doit également vérifier la date et l'heure (Heure, minute et second) de l'horloge.** **La délivrance d'un certificat d'étalonnage de la GTS avec mention de l'accréditation**
Note de spécification :
Pour la vérification de la date et de l'heure, il a été jugé suffisant de s'assurer de la conformité avec deux sources NTP.
Documentation à fournir:
- Procédure d'étalonnage ; Modèle de certificat d'étalonnage ou exemple de certificats déjà émis.
Guide de validation :
[Vérification documentaire] L'évaluateur étudiera la pertinence de la procédure d'étalonnage

ATTS-A2-680 - Rapport écrit de l'intervention
L'organisme ayant réalisé l'intervention doit réaliser un rapport écrit d'intervention. **Le rapport doit identifier :** - **La date et le lieu de l'intervention** - **L'organisme opérant le système de production et le nom du système de production** - **Le numéro de série de l'horloge GTS** - **L'étalon de référence utilisé** - **Le résultat de l'opération incluant l'écart en temps et en fréquence mesuré (avant et après l'opération d'ajustage le cas échéant)** - **Les écarts éventuels par rapport au plan d'intervention** - **Le plan d'intervention sera annexé au rapport.** - **Mentionner l'accréditation utilisée et l'organisme accréditeur** **Le rapport doit être signé.** **Le rapport doit être conservé au moins 5 ans après la réalisation de l'intervention.**
Note de spécification :
Le rapport peut être fourni sous forme papier ou électronique. Un rapport électronique doit être muni d'un sceau ou d'une signature électronique conforme au niveau avancé ou qualifié du Règlement eIDAS et permettant de s'assurer de l'origine de la signature avec un niveau de confiance substantiel.
Documentation à fournir:
- Modèle de rapport - Inventaires des interventions - Liste des rapports correspondants
Guide de validation :
[Vérification documentaire] L'évaluateur vérifiera par échantillonnage que les rapports sont bien rédigés et conforme à l'exigence.
Exemple d'implémentation satisfaisant l'exigence
Une signature ou un sceau électronique qualifié satisfait l'exigence Une signature ou un sceau électronique avancé conforme à la norme ETSI EN 319411-1 niveau NCP satisfait l'exigence.

ATTS-A2-690 - Indépendance
L'organisme doit être indépendant de l'organisme opérant le système de production.
Note de spécification :
Documentation à fournir:
- Justification de l'indépendance.
Guide de validation :
[Vérification documentaire] L'évaluateur vérifiera les justifications fournies.
Exemple d'implémentation satisfaisant l'exigence
L'absence de participation de l'organisme de production au capital de l'organisme de vérification est une condition nécessaire pour justifier l'indépendance.

7. Module B : Distribution du temps

Ce chapitre décrit les exigences applicables pour la certification d'un module nommé « Système de distribution » au sein de l'architecture du système.

Un système de distribution est un ensemble de site, de moyens humains, matériels, logiciels et réseaux, et de procédures permettant de fournir un temps attesté par l'architecture allant d'un système de distribution vers des dispositifs de diffusion et des Agents de réception du temps de référence.

Au niveau de l'architecture, le système de distribution est installé au sein du SI et diffuse aux dispositifs de diffusion le temps produit par le service de production. De ce fait, les exigences qui suivent portent principalement sur:

- Le fonctionnement et les conditions d'opération du service
- Le protocole d'échange avec les dispositifs de diffusion
- Le protocole d'échange avec le service de supervision et de contrôle
- Les conditions de raccordement au système de production
- Les matériels mis en œuvre.

Un système de distribution peut mettre optionnellement à disposition des clients un dispositif de diffusion de diffusion (Type A) permettant aux Agents de réception de ce client de se synchroniser sans installer de dispositif physique dans le périmètre client.

Le rôle du système de distribution est le transport sécurisé du temps d'un système de production et sa distribution à des éléments de l'architecture (dispositifs de diffusion matériel ou logiciel) se trouvant dans le périmètre du Système d'Information d'un client. De ce fait, les principales fonctions attendues d'un service de distribution sont :

- se synchroniser avec un système de production du temps
- sécuriser et tracer les synchronisations
- fournir du temps à des éléments certifiés en aval :
    - dispositif de diffusion physique dans le cas général ;
    - agent dans le cas de la mise d'un dispositif de diffusion du temps de référence de type A;
- remonter les informations de synchronisation au système de supervision et de contrôle à des fins de supervision et d'attestation du temps fourni.

Un système de distribution doit remplir les objectifs suivants :

- Récupérer de façon sécurisée les données temps auprès d'un système de production
- Assurer le transport du temps avec l'exactitude définie.
- Assurer la traçabilité des opérations.
- Remonter à la supervision de l'historique de synchronisation
- Gérer des états d'alerte et de la continuité d'activité
- Remonter à la supervision des alertes locales
- Assurer la sécurité physique, logique et organisationnelle du service.

Si le système de distribution opère un dispositif de diffusion de type A, celui-ci doit également remplir les objectifs suivants :

- Mise à disposition d'une interface de synchronisation sécurisée pour les Agents de réception du temps de référence.
- Diffuser d'un temps synchronisé avec les serveurs de l'infrastructure de distribution du temps de référence aux Agents de réception du temps de référence.
- Remonter à la supervision l'historique de synchronisation du dispositif de diffusion de type A de façon sécurisée.
- Remontée à la supervision des alertes locales du dispositif de diffusion de type A

7.1.1. Exigences relatives au raccordement au système de production

Les exigences relatives au raccordement du système de production avec le système de distribution ont pour objectif de récupérer de façon sécurisée des informations temps auprès d'un système de production.

Le raccordement doit principalement assurer que :

- Le système de distribution est effectivement synchronisé avec un système de production certifié au sein de l'architecture et non avec un autre système.
- Le système de distribution est synchronisé conformément à l'exactitude cible
- L'information temps n'est pas altérée lorsque celle-ci est récupérée.

ATTS-B0-010 - Documentation du raccordement au système de production.
La méthode de raccordement du système de distribution au système de production doit être documentée.
Note de spécification :
Cette exigence est une exigence documentaire.
Documentation à fournir à l'évaluateur :
- Un document descriptif de la méthode de raccordement mise en œuvre. - Un certificat de raccordement, signé a minima par un responsable du système de production et par le responsable du système de distribution
Guide de validation :
[Évaluation documentaire] L'évaluateur : - S'assurera que la documentation est fournie - L'évaluateur analysera la documentation fournie. La documentation doit être complète et suffisante pour comprendre le mécanisme mis en œuvre sans ambiguïté.

ATTS-B0-020 - Exactitude du raccordement
La méthode de raccordement doit permettre de récupérer le temps en conformité avec l'exactitude cible visée.
Note de spécification :
Documentation à fournir :
- Description de la méthode de raccordement mise en œuvre - Description des mesures réalisée, de la méthode de mesure utilisée **et de l'incertitude introduite par la méthode de mesure.** - Résultat des mesures constatées
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la méthode de mesure est adéquate vis-à-vis de l'exactitude cible visée. L'évaluateur vérifiera que les résultats de mesure sont conformes à l'exactitude cible visée. Une évaluation de l'incertitude devra être réalisée. [Évaluation fonctionnelle] L'évaluateur demandera à réaliser des mesures et vérifiera que celle-ci est en adéquation avec l'exactitude cible.

ATTS-B0-030 - Sécurisation du raccordement au système de production.
La méthode de raccordement doit garantir que : - **Le système de distribution est bien raccordé au serveur de production** - **La sécurité de la communication est assurée (intégrité et origine)**
Note de spécification :
La sécurité de l'environnement peut être obtenue : - Soit par sécurisation logique (chiffrement…) du flux - Soit par sécurisation physique (contrôle d'accès…) du média transportant le flux.
Documentation à fournir :
- Description du raccordement - Description des mesures de sécurité mise en œuvre
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la méthode de raccordement mise en place assure une sécurité suffisante du raccordement. En particulier : - Un tiers ne doit pas pouvoir altérer sans difficulté significative le flux - Un tiers ne doit pas pouvoir changer l'origine du flux sans difficulté significative. [Évaluation fonctionnelle] L'évaluateur vérifiera que les mesures de sécurité décrites sont bien mises en œuvre.
Exemple d'implémentation satisfaisant l'exigence
Les solutions suivantes satisfont l'exigence : - Sécurisation du flux logique par des moyens cryptographiques à l'état de l'art garantissant l'origine et l'intégrité (par exemple, signature électronique ou scellement des données. - Isolation physique et logique du média transportant l'information (par exemple : média dédié) et mise en place de mesures de contrôle d'accès physique.

7.1.2. Exigences relatives au transport du temps au sein du service de distribution

Le temps doit être transporté en conservant une exactitude conforme à l'exactitude cible visée.

ATTS-B0-040 - Exactitude du transport du temps
Le temps est transporté entre le système de production et le système de distribution avec une exactitude au moins cinq fois plus précise que l'exactitude de sortie ciblée.
Note de spécification :
Documentation à fournir :
- une documentation expliquant comment la méthode de transport permet d'assurer l'exactitude cible ainsi que l'incertitude introduite par la méthode de mesure. - Les tests de validation ayant permis d'établir que la méthode de transport permettait d'assurer cette exactitude.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la méthode de mesure est adéquate vis-à-vis de l'exactitude cible visée. L'évaluateur vérifiera que les résultats de mesure sont conformes à l'exactitude cible visée. Cette exigence est applicable à tous les serveurs de l'infrastructure de distribution, y compris les serveurs de

secours.

[Évaluation fonctionnelle] L'évaluateur demandera à réaliser des mesures et vérifiera que celle-ci sont en adéquation avec l'exactitude cible.

L'évaluateur procédera par échantillonnage en appliquant la méthode de la racine carrée.

ATTS-B0-050 - Fréquence de synchronisation
Afin d'assurer à la fois l'exactitude du temps et la non-surcharge des serveurs de production, les serveurs de l'infrastructure de distribution doivent être synchronisés a minima toutes les 5 minutes. **La fréquence maximale de synchronisation doit être documentée.**
Note de spécification :
Dans le cas où la fréquence de synchronisation n'est pas fixée, mais peut varier en fonction du temps, la méthode doit être documentée
Documentation à fournir :
- Description de la fourchette de synchronisation configurée sur les serveurs de distribution - Description de l'algorithme permettant d'optimiser la fréquence de synchronisation, si applicable - Exemples de trace de synchronisation démontrant que la fréquence de synchronisation est respectée.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera - si la fourchette de fréquence de synchronisation choisie est compatible avec l'exigence. - la description de l'algorithme ne présente pas de contradiction avec l'exigence - par échantillonnage que les fréquences constatées sur les traces de synchronisation sont conformes à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que : - la configuration des serveurs correspond à la description - Les fréquences de synchronisation réelles apparaissant dans les traces correspondent à la description.

Lors de son transport, l'information de synchronisation ne doit pouvoir être altérée.

ATTS-B0-060 - Intégrité du transport du temps
La méthode de transport du temps doit permettre de détecter toute atteinte à l'intégrité des informations temps transportés entre le serveur du système de production et le serveur du système de distribution.
Note de spécification :
Par intégrité, l'on entend que toute modification du flux temps doit pouvoir être détectée par une méthode robuste utilisant des algorithmes cryptographiques à l'état de l'art suivant les recommandations de l'ANSSI.
Documentation à fournir à l'évaluateur :
- Une documentation décrivant la méthode utilisée pour assurer l'intégrité. - Des traces démontrant le comportement du système (détection de l'altération et création d'alertes) en cas de manquement à l'intégrité du flux temps
Guide de validation :
L'évaluateur : - S'assurera que la documentation est fournie - Que la méthode décrite est conforme à l'état de l'art cryptographique - Que le test réalisé permet de s'assurer que la méthode est effectivement implémentée.
Exemple d'implémentation satisfaisant l'exigence

La mise en place d'une liaison privée combinée à l'utilisation de haché cryptographique lors du transport du temps permet de satisfaire cette exigence.

ATTS-B0-070 - Origine du transport du temps
La méthode de transport du temps doit permettre d'assurer l'origine du temps transporté
Note de spécification :
Par origine, on entend un élément de preuve fort démontrant que toute modification de l'origine flux temps doit pouvoir être détecté. Il est attendu d'utiliser une méthode une méthode robuste utilisant des algorithmes de chiffrement à l'état de l'art suivant les recommandations de l'ANSSI (pour la France) ou équivalent national pour un autre État, ou une méthode démontrée équivalente.
Documentation à fournir :
- Documentation décrivant la méthode utilisée pour garantir l'origine du flux temps. - Résultat de test démontrant le comportement du système (détection de l'usurpation de l'origine et alerte) en cas de tentative d'usurpation. U rapport de test démontrant le comportement du système en cas de manquement à l'intégrité du flux temps devra être fourni.
Guide de validation :
[Évaluation documentaire] L'évaluateur : - S'assurera que la documentation est fournie - Que la méthode décrite est conforme à l'état de l'art cryptographique, le cas échéant - Que le test réalisé permet de s'assurer que la méthode est effectivement implémentée.
Exemple d'implémentation satisfaisant l'exigence
La mise en place d'une liaison privée combinée à l'utilisation d'une signature électronique avancée sur le flux temps transmis avec algorithme et une longueur de clé privée conforme à l'état de l'art satisfait cette exigence. L'utilisation d'un flux sécurisé par des certificats SSL avec un certificat d'authentification serveur à l'état de l'art assure également la satisfaction de cette exigence.

ATTS-B0-080 - Délai de détection d'anomalie
Toute altération, perte de traçabilité ou d'origine du flux temps doit être détectée dans un délai inférieur à 10 secondes.
Note de spécification :
Cette exigence est une exigence technique. Il n'est pas obligatoirement demandé de réaliser en temps réel les vérifications de l'information temps transportée, cependant, ces vérifications doivent être réalisée dans un délai minimal afin d'assurer, en cas de détection d'un incident, une réponse à incident rapide et efficace.
Documentation à fournir :
Fournir une analyse de risque sur les anomalies détectables et démonstration sur leur délai de détection
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le test réalisé permet de s'assurer que la méthode est effectivement implémentée. [Évaluation fonctionnelle] L'évaluateur demandera à consulter l'historique des anomalies détectées et vérifiera si ces dernières sont en ligne avec l'exigence.
Exemple d'implémentation satisfaisant l'exigence
N/A

La distribution sécurisée s'appuie sur l'utilisation de serveurs de l'infrastructure de distribution

Ces serveurs sont des équipements destinés à être exploité par un système de distribution permettant de distribuer un temps attesté par l'architecture du système d'un système de distribution vers des dispositifs matériels ou logiciels de diffusion du temps de référence.

Dans l'architecture du système, le système de distribution est installé au sein du SI et diffuse aux dispositifs de diffusion le temps produit par le système de production. Pour réaliser cette distribution, il s'appuie sur des dispositifs matériels, appelés serveurs de l'infrastructure de distribution, chargés de communiquer avec les dispositifs de diffusion.

ATTS-B0-090 - Garantie d'intégrité du temps fourni
Le serveur de l'infrastructure de distribution doit être en mesure de mettre à disposition de l'élément aval un moyen cryptographique permettant, directement ou indirectement, à l'élément aval d'être assuré de *l'intégrité* du flux-temps fourni par le serveur.
Note de spécification :
Ce moyen cryptographique doit être fondé sur un algorithme cryptographique qui satisfait aux recommandations de l'organisme national en charge de la sécurité des systèmes d'information
Documentation à fournir :
- Description du mécanisme permettant à l'élément aval de vérifier l'intégrité des données fournies. - Description et résultats des tests correspondants.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - **La manière dont sont produites les données de vérification de l'intégrité des données diffusées est précisée dans la documentation fonctionnelle fournie** - **Le cahier de test couvre la production des données de vérification d'intégrité ainsi que leur vérification.** **[Evaluation sur site] L'évaluateur rejouera le test.**
Exemple d'implémentation satisfaisant l'exigence
Un mécanisme de hash (à l'état de l'art) sur les données satisfait à cette exigence. La diffusion des données à l'intérieur d'un canal sécurisé de type TLS avec les clés cryptographiques à l'état de l'art satisfait cette exigence.

ATTS-B0-100 - Protocoles à supporter
Les serveurs de l'infrastructure de distribution doivent fournir une interface de synchronisation pour les dispositifs matériels de diffusion. Les protocoles suivants doivent à minima être supportés : - **Protocole PTP** - **Protocole NTP**
Note de spécification :
Documentation à fournir :
- Description des sorties fournies.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que les sorties décrites sont conformes à l'exigence [Evaluation sur site] Sur l'échantillon fourni, l'évaluateur réalisera ses propres tests de compatibilité avec les protocoles indiqués.

ATTS-B0-110 - Éléments non certifiés ou non maîtrisés
Le système de distribution peut s'appuyer sur des éléments non maîtrisés (c'est à dire qui n'est pas sous le contrôle direct de l'organisme distributeur du temps) et non certifiés. L'opérateur de distribution doit assurer que ces éléments n'impactent pas la sécurité des données de temps échangées.
Note de spécification :
Documentation à fournir :
- Documentation qui justifie que les systèmes non maîtrisés n'impactent pas la sécurité des données échangées
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si les justificatifs donnés paraissent suffisants pour assurer la conformité à l'exigence. [Évaluation fonctionnelle] Si la documentation spécifie des mesures de sécurité spécifiques, l'évaluateur vérifiera que ces dernières sont implémentées.

ATTS-B0-120 - Maîtrise des éléments garantissant la sécurité du transport du temps
Les serveurs de l'infrastructure de distribution et tous éléments qui participent à garantir la sécurité de transport du temps doivent être maîtrisés.
Note de spécification :
Documentation à fournir :
- Un inventaire des serveurs et des éléments participant à garantir la sécurité de transport du temps, incluant les modèles et les numéros de série - Des éléments démontrant leur maîtrise.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description fournie satisfait l'exigence. [Évaluation fonctionnelle] l'évaluateur vérifiera que l'implémentation sur site est conforme à la description fournie. L'évaluation pourra se faire par échantillonnage.
Exemple d'implémentation satisfaisant l'exigence
Des serveurs, appartenant au système de distribution, hébergés dans un environnement privé du système de distribution et administrés par le service de distribution sont considérés comme maîtrisés.

7.1.3. Exigences relatives à la traçabilité du transport du temps

Le transport du temps doit faire l'objet d'une traçabilité.

ATTS-B0-130 - Traçabilité du transport du temps
Les synchronisations entre le système de production et le serveur de l'infrastructure de distribution doivent être tracées.
Note de spécification :
Cette exigence est une exigence technique.
Documentation à fournir :
- Documentation expliquant comment la traçabilité est réalisée. - Exemples de traces générées.
Guide de validation :

[Évaluation documentaire] L'évaluateur : - S'assurera que la documentation est fournie - S'assurera que les traces fournies sont conformes à la documentation. [Évaluation fonctionnelle] L'évaluateur vérifiera par échantillonnage que les logs ont bien été produits et archivés (l'évaluateur choisira de façon arbitraire des dates et heures de synchronisation et l'audité lui fournira les traces correspondantes)
Exemple d'implémentation satisfaisant l'exigence
L'enregistrement systématique de toutes les traces de synchronisation PTP/NTP des échanges entre les deux serveurs permet de satisfaire cette exigence.

ATTS-B0-140 - Protection des traces de synchronisation
Le système de distribution doit assurer la protection des traces générées contre la perte et/ou la modification.
Note de spécification :
-
Documentation à fournir :
- Description des mesures mises en place.
Guide de validation :
[Évaluation documentaire] L'évaluateur : - s'assurera que la documentation est fournie ; - s'assurera que les mesures décrites sont pertinentes. [Évaluation fonctionnelle] L'évaluateur vérifiera que les mesures décrites sont implémentées.
Exemple d'implémentation satisfaisant l'exigence
Des mesures de restriction d'accès en écriture et d'externalisation des sauvegardes satisfont cette exigence.

7.1.4. Exigences relatives à la Remontée des traces à la Supervision

L'ensemble des traces de synchronisation générées par les différents composants de distribution (voir Section précédente) doivent être remontées au service de supervision et de contrôle. Cette remontée doit être réalisée de façon sécurisée.

ATTS-B0-150 - Mécanisme de remontée de traces à la supervision
Le système de distribution doit mettre en place un mécanisme de remonté des traces de l'ensemble de serveurs de distribution conforme aux exigences communes du chapitre décrites dans le paragraphe 10.1.8. concernant la remontée des traces
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.8.
Guide de validation :
- Voir paragraphe 10.1.8.

7.1.5. Exigences relatives à la surveillance et à la gestion des alertes

Le système de distribution doit mettre en place un mécanisme interne de gestion des alertes.

ATTS-B0-160 - Gestion des alertes
Le système de distribution doit mettre en place une surveillance des éléments techniques mis en œuvre. En particulier, les alertes générées par les serveurs de l'infrastructure de distribution doivent être surveillées.
Note de spécification :
Documentation à fournir :
- Documentation du système de surveillance mis en œuvre
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera qu'un mécanisme de surveillance est en place [Évaluation fonctionnelle] l'évaluateur - vérifiera que le mécanisme est bien implémenté et est conforme à sa description - demandera à consulter la liste des alertes générées. Il s'attachera à vérifier : o par échantillonnage, que les alertes ont fait l'objet d'un traitement o que le nombre d'alertes généré est en adéquation avec le dimensionnement de l'équipe en charge de son traitement.

ATTS-B0-170 - Mécanisme de détection des vulnérabilités
Des mécanismes de détection de vulnérabilités doivent être mis en place.
Note de spécification :
Documentation à fournir :
- Fournir une analyse de risque
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera qu'un mécanisme de surveillance est en place. [Évaluation fonctionnelle] L'évaluateur - vérifiera que le mécanisme est bien implémenté et est conforme à sa description et pourra consulter les scans de vulnérabilité le cas échéant. -

ATTS-B0-180 - Notification des incidents à la supervision interne
Tout incident interne impactant la distribution du temps doit être remonté sans délai au système de supervision et de contrôle.
Note de spécification :
En particulier, cette exigence est applicable aux incidents impactant : - **l'intégrité ou l'origine du temps distribué** - **l'exactitude du temps distribué** - **la disponibilité du temps**
Documentation à fournir :
- Description de l'organisation mise en place pour remonter les exigences au système de supervision et

de contrôle - Liste des incidents pris en compte.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera qu'une organisation est en place. [Évaluation fonctionnelle] L'évaluateur - vérifiera que le mécanisme est bien implémenté et est conforme à sa description - demandera à consulter la liste des incidents remontés à la supervision

ATTS-B0-190 - Mise en place de procédures de remontée des incidents
Chaque entité opérant une composante du système de distribution doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.
Note de spécification :
Documentation à fournir :
- Description des procédures mises en place.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera qu'une organisation est en place et si celle-ci semble pertinente. [Évaluation fonctionnelle] L'évaluateur vérifiera que la procédure de remontée d'incident est connue des personnels. Cette vérification se fera lors d'une entrevue et par échantillonnage. L'évaluateur demandera à consulter la liste des incidents remontés par les personnels et vérifiera par échantillonnage qu'un traitement a été réalisé.

ATTS-B0-200 - Seconde intercalaire
Le système de distribution doit mettre en place une procédure afin - **De surveiller les secondes intercalaires à venir** - **De réaliser les opérations nécessaires pour que les serveurs de distribution soient en mesure de prendre en compte la seconde intercalaire et ne pas la considérer comme une anomalie.**
Note de spécification :
Documentation à fournir :
- Description de la procédure mise en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : **La manière dont est gérée la seconde intercalaire est précisée dans la procédure.** **[Évaluation fonctionnelle] L'évaluateur vérifiera :** - **Qu'une surveillance de la seconde intercalaire est bien mise en œuvre** - **Par échantillonnage, que la procédure d'intervention sur les serveurs de l'infrastructure de distribution a bien été réalisée sur les secondes intercalaires ayant eu lieu.**

7.1.6. Exigences relatives à la sécurité physique

ATTS-B0-210 - Exigences communes
Les sites d'exploitation du système de distribution doivent respecter les exigences communes relatives à la sécurité physique du paragraphe 10.1.1.
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.1.
Guide de validation :
Voir paragraphe 10.1.1.

ATTS-B0-220 - Inventaire des composants
Les serveurs de l'infrastructure de distribution sont des composants critiques, de ce fait, ils doivent être identifiés et inventoriés.
Note de spécification :
Cette exigence vient compléter l'exigence commune « Inventaire des composants »
Documentation à fournir :
Liste des serveurs à jour
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la liste est disponible. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que la liste est à jour.

ATTS-B0-230 - Manipulation des composants
Les opérations suivantes sur les serveurs de distribution doivent a minima faire l'objet d'une traçabilité : - **Installation sur site** - **Mise en route** - **Opération de maintenant** - **Désinstallation et fin de vie.**
Note de spécification :
Cette exigence vient compléter l'exigence commune « Manipulation des composants»
Documentation à fournir :
- Procédure de suivi des opérations sur les serveurs de distribution
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la procédure est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que le suivi est réalisé conformément à la procédure.
Exemple d'implémentation satisfaisant l'exigence

7.1.7. Exigences relatives aux ressources humaines

ATTS-B0-240 - Exigences communes
Les sites d'exploitation du système de distribution doivent respecter les exigences communes relatives aux ressources humaines du paragraphe 10.1.2.
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.2.
Guide de validation :
- Voir paragraphe 10.1.2.

7.1.8. Exigences relatives à la sécurité logique

ATTS-B0-250 - Exigences communes
Les sites d'exploitation du système de distribution doivent respecter les exigences communes relatives à la sécurité logique du paragraphe 10.1.3.
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.3.
Guide de validation :
- Voir paragraphe 10.1.3.

ATTS-B0-260 - Interconnexion Réseau
L'interconnexion entre réseaux de distribution et les autres réseaux hors système de production (par exemple, les éléments de diffusion ou de supervision) doivent être protégés par des systèmes de sécurité configurés pour n'accepter que les protocoles nécessaires au fonctionnement du système de distribution.
Note de spécification :
Documentation à fournir :
- Schéma réseau - Description de la stratégie de configuration des systèmes de sécurité.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera que la mise-en-œuvre est conforme à la documentation. Cette vérification pourra être réalisée par échantillonnage.

ATTS-B0-270 - Authentification des flux entrants
Le système de distribution doit mettre en œuvre un mécanisme permettant de s'assurer que les dispositifs de diffusion demandant à se synchroniser sur le serveur de distribution ont été préalablement authentifiés.
Note de spécification :
Documentation à fournir :
- Description du mécanisme d'authentification - Documentation et résultat de du test de synchronisation d'un dispositif de diffusion non authentifiée.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le mécanisme décrit est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera que la mise-en-œuvre est conforme à la documentation. L'évaluateur demandera à faire rejouer le test.

ATTS-B0-280 - Filtrage des flux entrants
Le système de distribution doit mettre en place un mécanisme de pare-feu entre les dispositifs de diffusion et les serveurs de distribution. Les pare-feu doivent être configurés de façon à ne laisser passer que les flux autorisés. Il est possible de mettre en place une configuration dynamique de l'ouverture des flux, mais dans ce cas, les règles d'ouverture et de fermeture automatique de flux devront être documentées. Dans tous les cas, les ouvertures et fermetures de port doivent faire l'objet d'une traçabilité.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en place
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le mécanisme décrit est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, éventuellement par échantillonnage - Que les pare-feu sont mis en œuvre conformément à la description fournie - que les traces d'ouverture et de fermeture de flux sont produites et conservées

ATTS-B0-290 - Filtrage des flux sortants
Le système de distribution doit laisser passer le flux permettant aux serveurs de distribution de remonter les traces de synchronisation vers la supervision.
Note de spécification :
Documentation à fournir :
Description du mécanisme en place
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le mécanisme décrit est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que la configuration du pare-feu est conforme à la description.

ATTS-B0-300 - Environnement physique
Le système de distribution doit garantir que les composants matériels (hors câblage) du réseau de distribution (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé.
Note de spécification :
Documentation à fournir :
- Description de l'environnement
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le l'environnement décrit est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que l'environnement est conforme à la description.

ATTS-B0-310 - Protection des échanges réseau
Des mesures de protection des flux réseau doivent être mises en œuvre afin d'assurer la confidentialité et l'intégrité des données qui y transitent.
Note de spécification :
Certains flux peuvent ne pas nécessiter de mettre en place des mesures de protection, mais cela doit être justifié (par exemple : échange de données non sensibles, protection physique du matériel …)
Documentation à fournir :
- Schéma des flux identifiant les flux sécurisés et non sécurisés - Description de la mesure de sécurisation mise en œuvre - Justification des flux non sécurisés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que la mise en œuvre est conforme à la description fournie.
Exemple d'implémentation satisfaisant l'exigence
La mise en place de certificats SSL ou de VPN permet de répondre à cette exigence.

ATTS-B0-320 - Dimensionnement des serveurs de l'infrastructure de distribution
Les serveurs de l'infrastructure de distribution doivent être dimensionnés pour supporter la charge de transactions. L'entité opérant la distribution doit mettre en place une architecture dimensionnée en adéquation avec le nombre de transactions prévues.
Note de spécification :
Documentation à fournir :
- Estimation de la charge - Estimation du dimensionnement - Mesure courant de la charge
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie est conforme à l'exigence.

[Évaluation fonctionnelle] L'évaluateur vérifiera que la charge réseau fait l'objet de mesure.

ATTS-B0-330 - Surveillance et prévision
L'entité opérant le système de distribution a une obligation de surveillance du dimensionnement et de prévision de volumétrie à venir
Note de spécification :
Documentation à fournir :
- Plan de charge incluant l'estimation de charge à venir. - Mesure de la charge actuelle et passée
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation est fournie et si les estimations sont réalistes vis-à-vis de l'historique mesuré.

7.1.9. Exigences relatives à la journalisation des événements

ATTS-B0-340 - Exigences communes
Les sites d'exploitation du système de distribution doivent respecter les exigences communes relatives à la journalisation des événements du paragraphe 10.1.4.
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.4.
Guide de validation :
- Voir paragraphe 10.1.4.

ATTS-B0-350 - Événements spécifiques à la gestion du temps
L'ensemble des traces de synchronisation et, le cas échéant, de calibrage des éléments doivent être tracées
Note de spécification :
Documentation à fournir :
N/A
Guide de validation :
[Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que les traces sont conservées.

ATTS-B0-360 - Champs obligatoires d'un enregistrement
Chaque enregistrement d'un événement dans un journal doit contenir au minimum les champs suivants : - **type de l'événement ;** - **nom de l'exécutant ou référence du système déclenchant l'événement ;** - **date et heure de l'événement** - **résultant de l'événement (échec ou réussite).**
Note de spécification :
Documentation à fournir :
- liste des journaux d'événements - exemple de chaque type de journal
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les exemples de journaux sont complets et conformes à l'exigence. En cas d'impossibilité de fournir l'ensemble des journaux, cette vérification pourra être réalisée sur site. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que les journaux générés sont conformes aux exemples fournis.

7.1.10. Exigences relatives à la continuité d'activité

ATTS-B0-370 - Exigences communes
Les sites d'exploitation du système de distribution doivent respecter les exigences communes relatives à la continuité d'activité du paragraphe 0
Note de spécification :
Documentation à fournir :
- Voir paragraphe 0
Guide de validation :
- Voir paragraphe 0

ATTS-B0-380 - Disponibilité
Le système de distribution doit mettre en place une architecture de haute disponibilité. L'architecture doit être mise en place de façon à atteindre un niveau de disponibilité de 99,5% de chacune des fonctions critiques.
Note de spécification :
Les fonctions critiques comportent à minima : - La distribution du temps - La remontée des incidents à la supervision - La remontée des traces de synchronisation à la supervision
Documentation à fournir :
- Description de l'architecture de haute disponibilité mise en place.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'architecture décrite est adéquate. [Évaluation fonctionnelle] L'évaluateur vérifiera, éventuellement par échantillonnage, l'architecture décrite est bien mise en place.

7.1.11. Exigences relatives l'utilisation de dispositifs de diffusion de Type A

Cette section contient l'ensemble des exigences complémentaires lorsque le système de distribution est raccordé à un dispositif de diffusion de Type A ».

L'objectif du dispositif de diffusion de type A est d'offrir les fonctionnalités d'un dispositif de diffusion à des clients qui ne possèdent pas de dispositif matériel de diffusion. L'objectif est de fournir une heure traçable à des Agents de réception du temps de référence authentifiés et autorisés à se connecter en garantissant un niveau d'exactitude donné.

ATTS-B0-390 - Séparation physique
Si le dispositif de diffusion de type A est opéré dans le même environnement que le système de distribution, les serveurs et matériels permettant d'opérer le dispositif de diffusion de type A doivent être physiquement séparés des serveurs de 'l'infrastructure opérés par le serveur de distribution
Note de spécification :
Le dispositif de diffusion de type A ne peut pas être hébergée à l'intérieur d'un serveur de l'infrastructure de diffusion. Les serveurs doivent être distincts.
Documentation à fournir :
La documentation d'architecture et un diagramme réseau seront fournis. Ces diagrammes devront identifier de façon non ambiguë les serveurs utilisés pour la distribution à destination des dispositifs de diffusion physiques et les serveurs utilisés dans le cadre de l'opération du dispositif de diffusion de type A.
Guide de validation :
[Évaluation documentaire] L'évaluateur s'assurera que l'exigence ci-dessus est bien remplie [Évaluation fonctionnelle] L'évaluateur s'assurera que la séparation est effective et correspond à la documentation. En particulier, il s'assurera o que les machines décrites se trouvent bien sur site o que les machines adressent bien des populations distinctes (cela pourra être constaté par échantillonnage sur les traces des machines).

ATTS-B0-400 - Protection du serveur de l'infrastructure de distribution
Le canal permettant la synchronisation entre le serveur et le dispositif de diffusion de type A doit offrir des mesures de sécurité permettant de s'assurer que : - **seul le dispositif de type A peut se synchroniser au serveur de l'infrastructure de distribution, en particulier, que les éléments se synchronisant au dispositif de diffusion (par exemple, les Agents) ne puissent se connecter au serveur de l'infrastructure de distribution** - **que les synchronisations entre le dispositif de type A et le serveur de l'infrastructure de distribution sont tracées.**
Note de spécification :
Documentation à fournir :
La documentation des mesures de sécurité doit être fournie.
Guide de validation :
[Évaluation documentaire] L'évaluateur s'assurera que l'exigence ci-dessus est bien remplie [Évaluation fonctionnelle] Revue de la mise en place des mesures décrites est effective.

8. Module C : Diffusion du temps

Ce chapitre décrit les exigences applicables pour la certification de systèmes de diffusion du temps intégrés dans une architecture certifiée nommés :

- Module C1 : Dispositif matériel de diffusion du temps de référence
- Module C2 : Dispositif de diffusion du temps de référence de type A
- Module C3 : Agent de réception du temps de référence

8.1. Module C1 : Dispositif matériel de diffusion du temps de référence

Dans l'architecture du système, le système de diffusion matériel est installé **au sein du SI du client** et diffuse aux éléments finaux du client directement ou via des Agents de réception, le temps fourni par le service de distribution. De ce fait, les exigences qui suivent portent :

- Sur le produit lui-même (parties matérielles et logicielles)
- Sur le cycle de vie du produit
- Sur les entrées/sorties, physiques et logiques, du produit
- Sur les protocoles d'échange avec :
    - Le système de distribution, placé en amont
    - L'Agent de réception ou l'élément final à synchroniser
    - Le service de supervision et de contrôle.

Il est prévu 4 types de profils de dispositifs matériels de diffusion pouvant être certifiés :

1. les dispositifs matériels de diffusion de type B ;
2. les dispositifs matériels de diffusion de type C ;
3. les dispositifs matériels de diffusion de type D.

Chaque type de dispositif matériel de diffusion permet d'atteindre un niveau d'exactitude et/ou d'assurance supplémentaire dans le processus de diffusion du temps attesté.

Les exigences qui suivent s'appliquent à tous les dispositifs matériels de diffusion. Lorsqu'une exigence n'est applicable qu'à un seul type de dispositif matériel de diffusion, cette exigence est précisée de façon explicite.

Les fonctionnalités principales d'un dispositif matériel de diffusion sont :

- Se synchroniser avec une source de temps en amont dans l'architecture du système
- Fournir du temps à des éléments en aval (Agents de réception du temps de référence).
- Sécuriser et tracer les synchronisations
  Remonter les informations de synchronisation au système de supervision (module dédié à la collecte des traces de synchronisation) à des fins de supervision et d'attestation du temps fourni.

Un dispositif matériel de diffusion du temps de référence doit remplir les objectifs suivants :

- Se connecter de façon sécurisée (intégrité et authentification) à l'élément amont pour réaliser une synchronisation temps
- Permettre à des éléments en aval (Agents) de se synchroniser
- Tracer l'ensemble des synchronisations réalisées
- Remonter à la supervision l'historique de synchronisation (synchronisation amont et aval) de façon sécurisée (intégrité et authentification mutuelle)
- Comparer différentes sources de temps et l'horloge interne, réaliser les éventuels arbitrages et lever des d'alertes en cas d'anomalies
- Être en mesure, en cas de détection d'anomalies, de réaliser des actions réactives adéquates.

- Remonter à la supervision les alertes locales (par exemple anomalie de synchronisation ; entité amont non atteignable) de façon sécurisée (intégrité et authentification) et réception et prise en compte d'un état l'alerte fournie par la supervision [intégrité et garantie de l'origine]
- Être administrable de façon sécurisé (authentification des administrateurs, protection des données)

8.1.1. Exigences relatives à la synchronisation Amont

Les exigences ci-après sont relatives à la synchronisation du dispositif matériel de diffusion avec le système de distribution. Ces exigences ont principalement pour objectif de se connecter de façon sécurisée (intégrité et authentification) à l'élément amont pour réaliser une synchronisation temps. En particulier, le dispositif doit être en mesure :

- De se synchroniser avec le service de distribution avec une précision donnée
- De s'assurer que la synchronisation a été réalisée de façon sécurisée.

8.1.2. Protocole de synchronisation et source de temps

ATTS-C1-010 - Protocoles à supporter
Les dispositifs doivent se synchroniser avec l'élément amont du système de distribution à l'aide notamment des protocoles suivants : - [Type D] le protocole utilisé doit être le protocole PTP accepté par le système de distribution permettant d'assurer le même niveau d'exactitude que le système de distribution ; - [Type B/C] les dispositifs matériels de diffusion doivent *à minima* supporter une diffusion sécurisée du protocole NTP.
Note de spécification :
Les dispositifs doivent *a minima* supporter le protocole spécifié ci-dessus. Il est possible pour un dispositif de supporter d'autres protocoles alternatifs permettant d'obtenir une exactitude similaire. Le fabricant du dispositif devra alors préciser si ces protocoles sont compatibles ou non avec l'architecture du système certifiée. (Ou protocole sécurisé, ou infrastructure sécurisée).
Documentation à fournir :
- spécification fonctionnelle du dispositif matériel de diffusion ; - programme et rapport de tests.
Guide de validation :
Concernant les protocoles obligatoires, l'évaluateur réalisera les vérifications suivantes : • L'évaluateur vérifiera dans la documentation que le protocole obligatoire est documenté. La version du protocole devra être précisée ainsi que les options éventuelles d'implémentation. • L'évaluateur demandera au fabricant les programmes et rapport de tests démontrant que le fabricant a bien testé l'implémentation du protocole • Sur site, l'évaluateur demandera à rejouer un sous-ensemble des tests. • Sur au moins un échantillon fourni, l'évaluateur réalisera un test indépendant des commandes principales du protocole pour s'assurer de la réalité de l'implémentation. Concernant les protocoles alternatifs : • le constructeur devra fournir la description du protocole ; • le constructeur devra faire la démonstration de l'équivalence du protocole alternatif proposé ; • les vérifications réalisées pour le protocole obligatoire sont applicables aux protocoles alternatifs.
Exemple d'implémentation satisfaisant l'exigence
Equivalence avec le protocole NTP en matière de traitement d'événement en particulier : • Conventions de notation • Procédure d'émission • Procédure de réception

- Procédure de paquet
- Procédure de mise à jour d'horloge
- Procédures d'initialisation.
- Procédure de libération
- Procédure de mise à jour de consultation.

ATTS-C1-020 - Nombre de sources de temps

[Type B] Le dispositif de type B doit pouvoir être connecté au minimum à un système de distribution certifié suivant le module B de ce référentiel.

[Type C et D] Les dispositifs de type C et D doivent pouvoir être connectés au minimum à deux sources de temps dont au moins une est un système de distribution certifié suivant le module B de ce référentiel

Note de spécification :

Documentation à fournir :

- spécification fonctionnelle du dispositif et/ou ;
- documentation d'administration du dispositif

Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera dans la documentation du dispositif que le nombre minimum de sources de temps est bien décrit et correspond bien à l'exigence.

[Evaluation sur site] Sur l'échantillon fourni, l'évaluateur vérifiera, en condition de laboratoire, s'il peut connecter avec succès le nombre de sources de temps décrits dans les spécifications.

Exemple d'implémentation satisfaisant l'exigence

Un dispositif de type B équipé d'une entrée lui permettant de se connecter à un système de distribution de l'architecture est conforme à l'exigence.

Un dispositif de type C ou D équipée des éléments suivants satisfait cette exigence :

- d'une entrée lui permettant de se connecter à un service de distribution de l'architecture est conforme à l'exigence ;
- d'une entrée lui permettant de récupérer un temps GNSS traçable à l'aide d'un module de calcul via GNSS.

ATTS-C1-030 - Exactitude de la synchronisation avec le temps reçu.

Le dispositif doit être en mesure de se synchroniser avec ses sources avec l'exactitude suivante :

Type B	Type C	Type D.
+/- 10 ms	+/- 50 microsecondes	+/-200 nanosecondes

Note de spécification :

Cette exigence est applicable à l'ensemble des entrées sources du dispositif.

Documentation à fournir :

- Description de l'exactitude cible du produit
- Description de la méthode de mesure utilisée et de la caractérisation de l'incertitude de mesure.
- Résultats des tests réalisés par le constructeur

Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera

- Que l'exactitude cible est conforme à l'exigence
- Que la méthode de mesure est adaptée

- **L'évaluateur réalisera une étude de la pertinence du calcul d'incertitudes**
- Que les résultats de test réalisés par le constructeur sont en ligne avec l'exigence.

La mesure doit être réalisée pour chaque entrée et pour chaque type de protocole supporté.

[Évaluation d'échantillon] Sur l'échantillon fourni, l'évaluateur réalisera ses propres mesures et les comparera aux résultats fournis par le fabricant.

ATTS-C1-040 - Exactitude de la source secondaire
[Type C et D] La source de temps secondaire doit avoir une exactitude au moins égale à celle de la source primaire (voir exigence précédente)
Note de spécification :
La nature des sources à mettre en œuvre au sein d'une architecture est spécifiée dans le chapitre « Architecture du système »
Documentation à fournir :
- Description de l'exactitude cible du produit - Description de la méthode de mesure utilisée et de la caractérisation de l'incertitude de mesure. - Résultats des tests réalisés par le fabricant
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si les résultats de test réalisés par le constructeur sont en ligne avec l'exigence. La mesure doit être réalisée pour chaque entrée et pour chaque type de protocole. [Phase laboratoire] Sur l'échantillon fourni, l'évaluateur réalisera ses propres mesures et les comparera aux résultats fournis par le constructeur.
Exemple d'implémentation satisfaisant l'exigence
Des sources primaires et secondaires d'exactitude identiques remplissent l'exigence. Une source primaire d'une exactitude de l'ordre de 5ms et une source secondaire de l'ordre de 10 ms remplissent l'exigence.

ATTS-C1-050 - Fréquence de synchronisation
Les fréquences de synchronisation du dispositif doivent être paramétrables. Des valeurs entre 8 et 1024 secondes doivent pouvoir être fixées.
Note de spécification :
Le paramétrage pourra assigner une valeur fixe de synchronisation ou un intervalle.
Documentation à fournir :
- Procédure de paramétrage (Documentation utilisateur/ administrateur) - Fréquences minimales et maximales autorisées
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera l'information est fournie, en particulier : - La documentation devra préciser comment le paramétrage de la fréquence est réalisé - Si la documentation précise des valeurs minimales et maximales autorisées. [Evaluation sur site] Sur l'échantillon fourni, l'évaluateur réalisera des paramétrages et vérifiera si les fréquences de synchronisation sont conformes au paramétrage. Il réalisera au moins 3 tests : - Un paramétrage avec une valeur de synchronisation maximale, ou à défaut, une valeur inférieure à la seconde. - Un paramétrage avec une valeur de l'ordre de 10 secondes, 30 secondes et 2 minutes - Un paramétrage avec une valeur de synchronisation maximale, ou à défaut, une valeur fixée à une

heure.
Exemple d'implémentation satisfaisant l'exigence
Un produit ne permettant pas de paramétrer la fréquence de synchronisation ne satisfait pas l'exigence. Un produit permettant de fixer, par configuration, une valeur fixe de synchronisation satisfait l'exigence. Un produit permettant de fixer des fréquences maximum et minimum de synchronisation satisfait l'exigence.

ATTS-C1-060 - Seconde intercalaire
Le dispositif doit être en mesure de prendre en compte la seconde intercalaire et ne pas la considérer comme une anomalie
Note de spécification :
Documentation à fournir :
- Description de la prise en compte de la seconde intercalaire dans la documentation utilisateur/ administrateur - Description du test de prise en compte de la seconde intercalaire dans le Cahier de test et résultats de tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - La manière dont est gérée la seconde intercalaire est précisée dans la documentation - Le cahier de test couvre le cas de la seconde intercalaire. [Evaluation sur site] L'évaluateur rejouera le test de la seconde intercalaire. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Un produit disposant d'un mécanisme permettant d'indiquer la date de la prochaine seconde intercalaire ou de l'obtenir automatiquement de la supervision satisfait l'exigence.

8.1.3. Sécurisation de la synchronisation amont

ATTS-C1-070 - Autorisation de connexion
Avant toute tentative de connexion au service de distribution, le dispositif doit demander une autorisation de connexion au service de supervision et de contrôle.
Note de spécification :
L'autorisation peut être une autorisation de connexion temporaire ou permanente à durée limitée à maximum 24h.
Documentation à fournir :
- Description fonctionnelle du type et mode d'autorisation obtenue de la supervision. - Description et résultat des tests correspondants
Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera que :
- La manière dont est gérée l'autorisation est précisée dans la documentation fonctionnelle fournie
- Le programme de test couvre la demande d'autorisation, en particulier :
  o Que le cas nominal est couvert.
  o Que dans les différents cas d'erreurs décrits dans la documentation (autorisation refusée, autorisation expirée…), la synchronisation avec le service de distribution n'est pas possible.

[Evaluation sur site] L'évaluateur rejouera le test.

ATTS-C1-080 - Authentification dans le protocole de connexion
Le protocole de connexion entre le dispositif et le système de distribution doit inclure une authentification mutuelle - **le service de distribution doit être authentifié ;** - **le dispositif doit être authentifié.** **Le niveau d'authentification attendu est le suivant :** - **L'authentification du service de distribution doit être réalisée par un certificat d'authentification ou un mécanisme démontré d'une robustesse équivalente.** - **L'authentification du dispositif peut être réalisée par l'utilisation d'un couple identifiant/mot de passe ou par un moyen d'authentification supérieur (par exemple, certificat d'authentification).** **Dans le cas de l'utilisation d'un certificat, celui-ci doit être conforme aux recommandations cryptographiques de l'organisme national en charge de la sécurité de l'information.** **Dans le cas de l'utilisation d'un mot de passe, celui-ci :** - **doit être généré de façon aléatoire ;** - **ne doit pas être dérivé de l'identifiant ou du numéro de série du dispositif ;** - **doit être conforme en termes de longueur et de complexité aux recommandations de l'organisme national en charge de la sécurité des systèmes d'information ;** - **ne doit pas être commun à plusieurs dispositifs ;** - **ne doit pas être accessible en lecture par le client ou modifiable par le client ;** - **s'il est conservé du côté constructeur, des mesures de sécurité doivent être mises en place, en particulier des mesures de chiffrement et de contrôle d'accès.**
Note de spécification :
L'authentification peut être réalisée soit de façon directe, soit de façon indirecte en confiant l'authentification à un service tiers dans lequel le système de distribution est lui-même authentifié. Le mécanisme cryptographique doit être conforme à l'état de l'art de la cryptographie tel que défini par l'organisme national en charge de la sécurité des systèmes d'information
Documentation à fournir :
- Description fonctionnelle du type d'authentification réalisé. - Description et résultat des tests correspondants
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - La manière dont est gérée la double authentification est précisée dans la documentation fonctionnelle fournie - Le programme de tests couvre l'authentification, en particulier que les cas de succès et d'échec sont couverts. [Evaluation sur site] L'évaluateur rejouera le test.

ATTS-C1-090 - Intégrité de l'information de temps reçue
Si le media transportant le flux de temps n'est pas sécurisé, Lle dispositif doit être en mesure de vérifier l'intégrité du temps fourni à l'aide d'un algorithme cryptographique Le dispositif ne doit pas synchroniser son horloge interne avant la réalisation de cette vérification.
Note de spécification :
Le mécanisme cryptographique doit être conforme à l'état de l'art de la cryptographie tel que défini par

l'organisme national en charge de la sécurité des systèmes d'information
Documentation à fournir :
- Description fonctionnelle du type de vérification réalisée. - Description et résultat des tests correspondants
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - **La manière dont est gérée la vérification de l'intégrité des données reçues est précisée dans la documentation fonctionnelle fournie** - **Le cahier de test couvre la vérification, en particulier que les cas de succès et d'échec sont couverts.** **[Evaluation sur site] L'évaluateur rejouera le test.**
Exemple d'implémentation satisfaisant l'exigence
Un mécanisme de hachage ou de signature électronique (conforme à l'état de l'art) des données de synchronisation reçues satisfait l'exigence.

ATTS-C1-100 - Origine de l'information de temps reçue
Le dispositif doit être en mesure de vérifier de façon fiable l'origine de la source de temps à l'aide d'un algorithme cryptographique ou d'un mécanisme dont la robustesse est démontrée équivalente.
Note de spécification :
Le mécanisme cryptographique doit être conforme à l'état de l'art de la cryptographie tel que défini par l'organisme national en charge de la sécurité des systèmes d'information
Documentation à fournir :
- Description fonctionnelle du type de vérification réalisée. - Description et résultat des tests correspondants
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - La manière dont est gérée la vérification de l'origine des données reçues est précisée dans la documentation fonctionnelle fournie - Le cahier de test couvre la vérification, en particulier que les cas de succès et d'échec sont couverts. [Evaluation sur site] L'évaluateur rejouera le test. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Le transport des données à travers un canal sécurisé SSL avec authentification du serveur de distribution satisfait cette exigence.

ATTS-C1-110 - Erreur de synchronisation due à l'asymétrie de la connexion réseau de l'utilisateur
[Type B] Le dispositif de diffusion doit inclure une méthode pour démontrer que la contribution à l'erreur de synchronisation due à l'asymétrie éventuelle du lien réseau vers la source de temps est inférieure à 80 ms en valeur absolue.
Note de spécification :
Le lien réseau de l'utilisateur peut comporter une asymétrie entre les temps de propagation des paquets du protocole de synchronisation de la source de temps vers le dispositif de diffusion et du dispositif de diffusion vers la source. Cette asymétrie, si elle n'est pas prise en compte, crée une erreur de synchronisation qui s'ajoute aux autres sources d'erreur. Les protocoles NTP et PTP ne pouvant mesurer l'erreur due à l'asymétrie, le dispositif doit inclure une méthode pour démontrer que cette erreur ne dépasse pas une limite acceptable.

Documentation à fournir :
• Description de la méthode • Résultats des mesures et calculs démontrant que l'erreur de synchronisation due à l'asymétrie est inférieure à 80 ms
Guide de validation :
L'évaluateur vérifiera que : - **La méthode proposée permet de s'assurer que l'asymétrie est inférieure à 80 ms.** - **Les tests confirment la bonne implémentation de la méthode et que le comportement du dispositif de diffusion est bien conforme à la description.**
Exemple d'implémentation satisfaisant l'exigence
Cette vérification peut être réalisée par une mesure du RTT. En effet, si le temps d'aller-retour (RTT) mesuré entre le dispositif de diffusion et la source du temps est inférieur à 160 ms, ce qui implique une limite supérieure à l'erreur de synchronisation due à l'asymétrie du lien de moins de 80 ms par la formule : erreur de synchronisation ≤ RTT/2.

8.1.4. Exigences relatives à la synchronisation Aval

Les exigences suivantes ont pour objectif de permettre à des éléments en aval (Agents de réception de temps de référence) de se synchroniser. En particulier, le dispositif matériel de diffusion doit être en mesure :

- De fournir le temps avec une exactitude donnée.
- De fournir les moyens de sécuriser la synchronisation.

8.1.5. Protocole de synchronisation

ATTS-C1-120 - Protocoles à supporter
- **Les dispositifs matériels de diffusion doivent se synchroniser avec l'élément aval du système de distribution à l'aide des protocoles suivants** - [Type D] le dispositif de type D doit fournir *a minima* une sortie PTP ; - [Type B/C] les dispositifs doivent *a minima* fournir une sortie avec le protocole NTP. **La documentation devra préciser quelles sorties permettent d'atteindre l'exactitude cible du produit.**
Note de spécification :
Documentation à fournir :
- Description des sorties fournies.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les sorties décrites sont conformes à l'exigence. [Evaluation sur site] Sur l'échantillon fourni, l'évaluateur réalisera ses propres tests de compatibilité avec les protocoles indiqués.

ATTS-C1-130 - Exactitude du temps diffusé

Le dispositif doit diffuser le temps avec l'exactitude suivante :

Type B	Type C	Type D.
+/- 10 millisecondes	+/- 50 microsecondes	+/- 200 nanosecondes

Note de spécification :

Cette exigence est applicable à l'ensemble des sorties du dispositif identifiées dans l'exigence précédente.

Documentation à fournir :

- Description de l'exactitude cible du produit
- Description de la méthode de mesure utilisée et de la caractérisation de l'incertitude de mesure.
- Résultats des tests réalisés par le constructeur

Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera

- **Que l'exactitude cible est conforme à l'exigence**
- **Que la méthode de mesure est adaptée**
- **Que les résultats de test réalisés par le constructeur sont en ligne avec l'exigence.**

La mesure doit être réalisée pour chaque entrée et pour chaque type de protocole supporté.

[Évaluation d'échantillon] Sur l'échantillon fourni, l'évaluateur réalisera ses propres mesures et les comparera aux résultats fournis par le constructeur.

ATTS-C1-140 - Priorité du flux temps.

Si une priorisation des flux, en mise en place, alors les flux temps doivent être prioritaires sur les autres.

Note de spécification :

Documentation à fournir :

- Description de du mécanisme de priorisation des flux, s'il existe.

Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera que si un mécanisme est décrit, celui-ci donne bien la priorité aux flux temps dans le traitement.

8.1.6. Sécurisation de la synchronisation aval

ATTS-C1-150 - Garantie d'intégrité du temps fourni

Le dispositif doit être en mesure de mettre à disposition de l'élément aval un moyen cryptographique permettant, directement ou indirectement, à l'élément aval d'être assuré de *l'intégrité* du flux-temps fourni par le dispositif.

Note de spécification :

Ce moyen cryptographique doit être fondé sur un algorithme cryptographique qui satisfait aux recommandations de l'organisme national en charge de la sécurité des systèmes d'information

Documentation à fournir :
- Description du mécanisme permettant à l'élément aval de vérifier l'intégrité des données fournies. - Description et résultats des tests correspondants.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - La manière dont sont produites les données de vérification de l'intégrité des données diffusées est précisée dans la documentation fonctionnelle fournie - Le cahier de test couvre la production des données de vérification d'intégrité ainsi que leur vérification. [Evaluation sur site] L'évaluateur rejouera le test.
Exemple d'implémentation satisfaisant l'exigence
Un mécanisme de haché (à l'état de l'art) sur les données satisfait à cette exigence. La diffusion des données à l'intérieur d'un canal sécurisé de type SSL avec les clés cryptographiques à l'état de l'art satisfait cette exigence.

ATTS-C1-160 - Garantie d'origine du temps fourni
Le dispositif doit être en mesure de mettre à disposition de l'élément aval un moyen cryptographique permettant, directement ou indirectement, à l'élément aval *d'authentifier* le dispositif.
Note de spécification :
Ce moyen cryptographique doit être fondé sur un algorithme cryptographique qui satisfait aux recommandations de l'organisme national en charge de la sécurité des systèmes d'information
Documentation à fournir :
- Description du mécanisme permettant à l'élément aval de vérifier l'origine des données fournies. - Description et résultats des tests correspondants.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - La manière dont sont produites les données de vérification de l'origine des données diffusées est précisée dans la documentation fonctionnelle fournie - Le cahier de test couvre la production des données de vérification de l'origine ainsi que leur vérification. [Evaluation sur site] L'évaluateur rejouera le test. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Un mécanisme de signature électronique (à l'état de l'art) par le dispositif sur les données diffusées satisfait à cette exigence. La diffusion des données à l'intérieur d'un canal sécurisé de type SSL avec authentification du dispositif par le client avec des clés cryptographiques à l'état de l'art satisfait cette exigence

8.1.7. Exigences relatives à la Traçabilité

Les exigences suivantes sont principalement attachées aux objectifs de :

- De générer des traces de l'ensemble des synchronisations et de l'ensemble des éléments pertinents.
- D'assurer la protection de ces traces.

8.1.8. Génération de traces

Il est en particulier attendu que le dispositif matériel de diffusion génère des traces pour l'ensemble des éléments pertinents quant à la traçabilité et de générer des traces suffisamment détaillées pour être exploitées.

ATTS-C1-170 - Exigences de Traçabilité
Un dispositif de diffusion doit être conforme à l'ensemble des exigences communes.
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.
Guide de validation :
Voir paragraphe 10.1.

En complément, un dispositif matériel de diffusion doit satisfaire aux exigences suivantes :

ATTS-C1-180 - Liste minimale des traces devant être générées
Un dispositif matériel de diffusion doit générer un enregistrement d'audit des événements suivants : **a) synchronisation élément(s) amont ;** **b) synchronisation élément(s) aval ;**
Note de spécification :
La documentation fonctionnelle et/ou technique du dispositif devra lister les types d'événements et décrire les formats des traces.
Documentation à fournir :
- Exemple de traces générées par le dispositif de diffusion, couvrant l'ensemble des événements - Spécification fonctionnelle décrivant le format des traces - Description des tests et résultats des tests correspondant à l'exigence.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - Que la spécification fonctionnelle décrit bien le contenu des traces. - Que l'exemple généré est bien conforme à la description de la spécification fonctionnelle - Que les tests couvrent bien l'ensemble des traces décrites dans l'exigence. [Evaluation sur site] - L'évaluateur rejouera les tests. - L'évaluateur récupérera des traces et d'assurera qu'elles sont conformes à la description et aux exemples fournis.

ATTS-C1-190 - Dysfonctionnement de la génération de trace
En cas d'arrêt ou de dysfonctionnement des fonctions de génération de logs (exemple : espace de stockage plein), le dispositif de diffusion doit se mettre dans un état d'alerte majeure (elle continue à fournir le temps, mais n'est plus en mesure de l'attester).
Note de spécification :
Documentation à fournir :
- Description fonctionnelle du mécanisme

- Description du test et résultat de l'exécution du test.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie. Cette vérification pourra être réalisée sur site.

ATTS-C1-200 - Désactivation de la génération de trace
Le dispositif de diffusion ne doit pas permettre de désactiver la génération des traces.
Note de spécification :
Documentation à fournir :
- Description des mécanismes mis-en-œuvre pour empêcher la désactivation de la génération des traces.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description fonctionnelle répond bien à l'exigence.
Exemple d'implémentation satisfaisant l'exigence
Les solutions suivantes satisfont l'exigence : - Absence de fonction de désactivation de la génération - Existence d'une fonction de désactivation de la génération, mais celle-ci est rendue inactive - Existence d'une fonction de désactivation et mise en alerte critique du dispositif de diffusion en cas de déclenchement de cette dernière.

8.1.9. Protection des traces

Le dispositif de diffusion doit en particulier assurer la protection en intégrité et en confidentialité des traces générées.

ATTS-C1-210 - Intégrité des traces générées
Le dispositif de diffusion doit mettre en place un mécanisme de protection de l'intégrité des traces pour empêcher leur modification.
Note de spécification :
Un mécanisme de contrôle d'accès est considéré comme suffisant pour remplir cette exigence.
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description du test et résultat de l'exécution du test.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme

[Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Les mécanismes suivants répondent à l'exigence : - Contrôle d'accès - Mécanisme cryptographique de protection de l'intégrité (hash, chaînage, signature électronique).

ATTS-C1-220 - Confidentialité des traces générées
Le dispositif de diffusion doit interdire à tous les utilisateurs le droit d'accès en lecture aux enregistrements d'audit, à l'exception de ceux à qui l'on a accordé un droit de lecture explicite (les administrateurs de sécurité, administrateurs usine).
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests et résultats de l'exécution des tests
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme Les tests devront être réalisés pour chaque classe d'utilisateurs. [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie. Cette vérification pourra être réalisée sur site.

8.1.10. Exigences relatives à la Remontée des traces à la Supervision

L'ensemble des traces générées par le dispositif de diffusion doivent être remontées au système de supervision et de contrôle. Cette remontée doit être réalisée de façon sécurisée.

ATTS-C1-230 - Mécanisme de remontée des traces
Le mécanisme de remontée des traces implémenté sur le dispositif de diffusion doit être conforme aux exigences communes du paragraphe 10.1.8.
Note de spécification :
Documentation à fournir :
Voir exigences communes du paragraphe 10.1.8.
Guide de validation :
Voir exigences communes du paragraphe 10.1.8.

En complément des exigences communes, le dispositif de diffusion doit satisfaire des exigences suivantes.

8.1.11. Mécanisme de remontée des traces

Il est nécessaire que le mécanisme de remontée des traces assure :

- Que celles-ci soient remontées dans leur intégralité
- Que le format et le protocole de transport soient bien compatibles avec celui du système de supervision et de contrôle.

ATTS-C1-240 - Périmètre de remontée des traces à la supervision (traces pertinentes)

Le dispositif de diffusion doit remonter au système de supervision certifié les traces pertinentes de synchronisation dans leur intégralité. Les traces considérées comme pertinentes sont :
- **Les traces de synchronisation avec l'élément amont :**
  o **identifiant du serveur de distribution**
  o **date et heure de synchronisation avec le serveur de distribution**
  o **valeur d'écart retenu après synchronisation avec le serveur de distribution**
- **Les traces de Synchronisation de l'horloge interne ;**
- **Les traces de Synchronisation avec l'élément aval :**
  o **identifiant de l'élément aval ou origine de la requête ;**
  o **date et heure de la synchronisation ;**
  o **valeurs transmises.**

Note de spécification :
Une synchronisation peut consister en l'échange de plusieurs jeux de données de synchronisation (réalisation de plusieurs mesures) et le calcul d'une moyenne des valeurs échangées. Seule la valeur retenue doit obligatoirement être remontée. Le détail de l'ensemble des mesures peut optionnellement être remonté.
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie. Cette vérification pourra être réalisée sur site.

ATTS-C1-250 - Périmètre de remontée des traces à la supervision (effacement des traces)
Le mécanisme mis en place doit permettre de s'assurer que les traces de supervision ne sont pas perdues. En particulier, il est attendu que le mécanisme ne permet la destruction éventuelle des traces sur le dispositif de diffusion qu'après que celle-ci ait reçu la confirmation explicite que les traces ont bien été collectées par le système de supervision.
Note de spécification :
Documentation à fournir :

- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
L'effacement des traces après avoir reçu un accusé de réception de la part de la supervision satisfait cette exigence.

ATTS-C1-260 - Identification de la source des traces
Le protocole de remontée des traces doit permettre d'identifier le dispositif de diffusion de façon non ambiguë de façon à rattacher les traces au dispositif de diffusion dans le système de supervision.
Note de spécification :
Cette identification peut être faîtes au niveau du protocole ou au niveau des données fournies.
Documentation à fournir :
- Description du mécanisme d'identification du dispositif de diffusion et référentiel d'identification retenu. - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien : - comment le dispositif de diffusion est identifié ; - si cette identification est bien non ambiguë ; - que la description du test met bien en œuvre le mécanisme décrit ; - que le résultat du test démontre bien l'efficacité du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre. En particulier, il s'assurera que les identifiants remontés correspondent bien aux identifiants des échantillons. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Une remontée du numéro de série unique du dispositif de diffusion répond à cette exigence.

8.1.12. Sécurisation de la remontée des traces

La remontée des traces doit être réalisée de façon sécurisée.

ATTS-C1-270 - Sécurisation de la remontée des traces à la supervision
Le dispositif de diffusion doit utiliser un canal sécurisé pour transmettre les traces de synchronisation à la supervision. Ce canal doit être conforme aux exigences décrites dans les exigences communes
Note de spécification :

Documentation à fournir :
Voir exigences communes
Guide de validation :
Voir exigences communes

ATTS-C1-280 - Méthode d'authentification du dispositif de diffusion
Le dispositif de diffusion doit utiliser un certificat SSL client pour s'authentifier auprès de la supervision. L'authentification par couple identifiant/mot de passe n'est pas autorisée pour un dispositif de diffusion.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien lune authentification par certificat. **[Evaluation sur site]** **L'évaluateur rejouera le test afin de s'assurer que l'authentification par certificat décrite est bien mise-en-œuvre.** **Cette vérification pourra être réalisée sur site.**

ATTS-C1-290 - Changement de certificat
Un niveau administrateur est requis pour modifier le certificat d'authentification
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre pour changer le certificat d'authentification - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit une procédure de changement de certificat conforme à l'exigence. **[Evaluation sur site]** **L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre.** **Cette vérification pourra être réalisée sur site.**

ATTS-C1-300 - Identification des serveurs de supervision
Le dispositif de diffusion ne doit fournir les traces de supervision qu'aux serveurs autorisés dans sa configuration.
Note de spécification :
Documentation à fournir :
- Description du mécanisme permettant de spécifier au dispositif de diffusion la liste des serveurs autorisés - Description des tests relatifs à l'exigence et résultats de l'exécution des tests Nota : les tests doivent couvrir les cas où la connexion au serveur principal échoue et la connexion à un serveur de secours est mise en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien - Comment paramétrer, le cas échéant, les serveurs autorisés. - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le mécanisme est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Un produit où la liste des serveurs est fixée définitivement répond à cette exigence Un produit où la liste des serveurs peut être paramétrée par un administrateur ou en usine satisfait cette exigence.

ATTS-C1-310 - Stockage des traces
L'espace de stockage local des dispositifs de diffusion doit être dimensionné de telle façon qu'elle puisse conserver ses traces de synchronisation localement pendant une période de 24h en cas de panne de la supervision.
Note de spécification :
- .
Documentation à fournir :
- Description de l'espace prévu - Rationnel justifiant que cet espace est suffisant
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien les éléments demandés et que l'espace est effectivement suffisant [Evaluation sur site] L'évaluateur réalisera ses propres mesures et vérifiera si elles sont en ligne avec les données du constructeur.

8.1.13. Exigences relatives à la comparaison des sources de temps

L'ensemble des exigences suivantes visent à comparer différentes sources de temps et l'horloge interne, réaliser les éventuels arbitrages et lever des d'alertes en cas d'anomalies.

Pour réaliser cet objectif, les dispositifs de diffusion s'appuient sur un oscillateur interne leur permettant de fonctionner de façon autonome entre les différentes phases de synchronisation. Lors d'une synchronisation, le dispositif de diffusion compare son temps interne avec les différentes sources disponibles pour déterminer, à l'aide d'un algorithme, le temps qu'elle diffusera. En cas d'incohérence entre le temps fourni par l'horloge interne et les sources de temps, le dispositif de diffusion doit appliquer des règles d'arbitrage.

8.1.14. Caractéristiques des oscillateurs internes

Les exigences suivantes sont relatives aux oscillateurs internes des dispositifs matériels de diffusion.

ATTS-C1-320 - Oscillateurs internes

Les horloges et/ou oscillateurs internes doivent répondre aux exigences de stabilité suivantes :

	Type B	Type C	Type D
Stabilité	**<300ms/j**	**<1ms/j**	**<1µs/j**

Note de spécification :

Le type de matériel et/ou de technologie mis en œuvre est laissé libre au choix du constructeur.

Documentation à fournir :

- Description de l'exactitude et de la stabilité cible du produit
- Description de la méthode de mesure utilisée et de la caractérisation de l'incertitude de mesure.
- Résultats des tests réalisés par le constructeur

Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera

- Que l'exactitude cible est conforme à l'exigence
- Que la méthode de mesure est adaptée
- Que les résultats de test réalisés par le constructeur sont en ligne avec l'exigence.

[Phase essai]

Sur l'échantillon fourni, l'évaluateur réalisera ses propres mesures et les comparera aux résultats fournis par le constructeur

8.1.15. Gestion des Sources de temps

Le dispositif de diffusion doit être en mesure de gérer les différentes sources de temps.

ATTS-C1-330 - Gestion des sources de temps

Le dispositif de diffusion doit être en mesure de gérer un statut de ces sources de temps interne et externe. A minima, le dispositif de diffusion doit pour chaque source :

- **Un état où la source est considérée comme fiable et de confiance**
- **Un état où la source n'est plus considérée comme fiable.**

Note de spécification :

D'autres états peuvent être gérés

Documentation à fournir :

-Description du mécanisme mis en œuvre.

Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera que la description est présente et satisfait l'exigence.

ATTS-C1-340 - Algorithme de calcul du temps
Le dispositif de diffusion doit mettre en œuvre un algorithme de synchronisation prenant en compte l'ensemble des sources de temps à sa disposition. Le principe de fonctionnement de cet algorithme doit être documenté.
Note de spécification :
Documentation à fournir :
- Description de l'algorithme de synchronisation implémenté - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien : - l'algorithme mis en œuvre ; - que la description des tests couvre bien les particularités de l'algorithme ; - que le résultat du test démontre bien l'efficacité du mécanisme (une étude de couverture de la suite de tests sera suffisante pour la démonstration). [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que l'algorithme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

ATTS-C1-350 - Éléments amont désynchronisés
Le dispositif de diffusion ne doit pas prendre en compte dans ces calculs temps un élément amont qui n'est pas considéré comme « fiable ».
Note de spécification :
Documentation à fournir :
- Description de l'algorithme de synchronisation implémenté - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation de l'algorithme prend bien en compte cette exigence pour chaque source de temps interne et externe. De plus, l'évaluateur vérifiera la description des tests pour s'assurer qu'elle couvre bien cette exigence pour chaque source et que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que l'algorithme répond bien à l'exigence. Cette vérification pourra être réalisée sur site.

8.1.16. Règles d'arbitrage

En cas d'inconsistances entre les valeurs fournies par les différentes sources de temps, le dispositif de diffusion doit réaliser un arbitrage. Ces règles d'arbitrage varient selon le type de dispositif de diffusion.

ATTS-C1-360 - Niveau d'alerte sur l'état de l'horloge
Un dispositif de diffusion doit être en mesure de gérer un état interne. Les quatre états suivants doivent être gérés par le dispositif de diffusion : - **état nominal : absence d'incohérence entre l'horloge interne du dispositif de diffusion et ces sources de temps. Fourniture du temps aux éléments aval ;** - **alerte mineure : une incohérence est détectée, mais l'horloge interne du dispositif de diffusion est synchronisée avec une source de confiance. Fourniture du temps aux éléments en aval ;** - **alerte majeure: une incohérence est détectée et l'horloge interne du dispositif de diffusion ne peut plus être synchronisée avec une source de confiance. Le temps est fourni en aval en mode dégradé sur le temps fourni par l'horloge interne ;** - **alerte critique : le dispositif de diffusion n'est plus en mesure de fournir un temps attesté par l'architecture du système.**
Note de spécification :
D'autres états peuvent être pris en compte, mais le lien avec ces 4 états doit être fourni et doit être non ambigu.
Documentation à fournir :
- Description de l'état interne du dispositif de diffusion.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation prend bien en compte cette exigence.

ATTS-C1-370 - Règles d'arbitrage (Type B)

Un dispositif matériel de diffusion de type B doit implanter les règles d'arbitrage suivantes :

Statut de l'horloge interne	Statut de l'élément amont primaire	Action devant être réalisée par le dispositif
Considéré comme de confiance	Considéré comme de confiance	État nominal : Fourniture du temps aux éléments aval
Dysfonctionnement de l'horloge interne	Considéré comme de confiance	Alerte critique : arrêt de fourniture du temps.
Considéré comme de confiance	Ne répond pas ou n'est plus de confiance	Alerte majeure : remonte son état à la supervision et synchronisation sur l'horloge interne.

Note de spécification :

Si un dispositif de diffusion implémente des règles d'arbitrage complémentaires, celles-ci devront être décrites dans un document afin d'être évaluées.

Documentation à fournir :

- Description de l'algorithme d'arbitrage
- Description des tests relatifs à l'exigence et résultats de l'exécution des tests

Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera que la documentation de l'algorithme prend bien en compte cette exigence.

De plus, l'évaluateur vérifiera la description des tests pour s'assurer qu'elle couvre bien cette exigence. En particulier, les tests doivent couvrir les 3 cas types de l'exigence.

[Evaluation sur site]

L'évaluateur rejouera le test afin de s'assurer que l'algorithme répond bien à l'exigence.

Cette vérification pourra être réalisée sur site.

[Phase laboratoire]

L'évaluateur réalisera des tests indépendants en laboratoire sur les échantillons fournis.

ATTS-C1-380 - Règles d'arbitrage (Types C et D)

Un dispositif de diffusion de type C ou D doit implanter *a minima* les règles d'arbitrage suivantes :

Statut de l'horloge interne	Statut de l'élément amont primaire	Statut de l'élément amont secondaire	Action devant être réalisée par le dispositif de diffusion
Considéré comme de confiance	Considéré comme de confiance	Considéré comme de confiance	État nominal : Fourniture du temps aux éléments aval
Dysfonctionnement de l'horloge interne (non-réponse ou écart avec les deux sources)	Considéré comme de confiance	Considéré comme de confiance	Alerte critique : arrêt de fourniture du temps.
Considéré comme de confiance	Le serveur principal ne répond pas ou n'est plus de confiance	Considéré comme de confiance	Alerte majeure : fourniture du temps aux éléments aval avec synchronisation à la source secondaire. Tentative de synchronisation au serveur de secours
Considéré comme de confiance	Absence de source amont répondant ou fiable	Considéré comme de confiance	Alerte majeure : fourniture du temps aux éléments aval avec synchronisation à la source secondaire.
Considéré comme de confiance	Considéré comme de confiance	Ne répond pas ou n'est plus de confiance	Alerte mineure : fourniture du temps aux éléments aval avec synchronisation de la source primaire.
Considéré comme de confiance	Ne répond pas ou n'est plus de confiance	Ne répond pas ou n'est plus de confiance	Alerte majeure : fourniture du temps en mode dégradée (mode autonome basé sur l'horloge interne)

Note de spécification :

Si un dispositif de diffusion implémente des règles d'arbitrage complémentaires, celles-ci devront être décrites dans un document afin d'être évaluées

Documentation à fournir :

- Description de l'algorithme d'arbitrage
- Description des tests relatifs à l'exigence et résultats de l'exécution des tests

Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera que la documentation de l'algorithme prend bien en compte cette exigence.

De plus, l'évaluateur vérifiera la description des tests pour s'assurer qu'elle couvre bien cette exigence. En particulier, les tests doivent couvrir les 3 cas types de l'exigence.

[Evaluation sur site]

L'évaluateur rejouera le test afin de s'assurer que l'algorithme répond bien à l'exigence. Cette vérification pourra être réalisée sur site.

[Phase laboratoire]

L'évaluateur réalisera des tests indépendants en laboratoire sur les échantillons fournis.

8.1.17. Exigences relatives à la gestion des anomalies

L'ensemble des exigences suivantes visent à être en mesure, en cas de détection d'anomalies, de réaliser des actions réactives adéquates.

En particulier, le dispositif de diffusion doit être en mesure :

- De générer des alertes en cas de détection d'un élément anormal
- De prendre en compte des informations d'anomalie fournies par la supervision
- De notifier les alertes à l'utilisateur
- De réaliser automatiquement certaines actions en cas d'anomalie
- De revenir dans un état sûr après l'apparition d'une anomalie.

8.1.18. Génération et Gestion des alertes.

La génération des alertes peut survenir dans différents cas de figure. En particulier :

- en cas d'anomalie lors de la synchronisation du dispositif de diffusion ;
- en cas d'anomalie lors d'autotest du dispositif de diffusion.

ATTS-C1-390 - Alerte de synchronisation
Le dispositif de diffusion doit générer des alertes lors des synchronisations : • **écart supérieur à l'exactitude nominale du dispositif de diffusion entre le temps reçu et l'horloge interne du dispositif de diffusion ;** • **incapacité à joindre l'élément amont pendant une durée supérieure à une valeur paramétrable. Cette valeur ne peut dépasser 15 min*.**
Note de spécification :
Si un dispositif de diffusion implémente d'autres règles d'alertes, celles-ci devront être décrites dans un document afin d'être auditées.
Documentation à fournir :
- Description des anomalies - Description des tests et résultats de tests associés
Guide de validation :
[Évaluation documentaire] Si la documentation décrit d'autres règles d'alertes, l'évaluateur vérifiera - que la description des tests couvre bien l'ensemble des anomalies décrites (si des anomalies ne peuvent être testées pour des raisons techniques, la documentation des tests devra le justifier) ; - que le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que l'algorithme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site. [Phase laboratoire] L'évaluateur réalisera, en laboratoire, des tests indépendants sur les anomalies décrites dans cette exigence. [1] **Ce point est déjà traité de manière implicite lorsque le dispositif n'arrive pas à se synchroniser avec la supervision.*

ATTS-C1-400 - Alerte sur la non-intégrité du temps fourni
Le dispositif de diffusion doit générer une alerte en cas d'échec de la vérification de l'intégrité de l'information de temps fournie par l'élément amont.
Note de spécification :
Documentation à fournir :
- Description des anomalies - Description des tests et résultats de tests associés
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien : - l'anomalie décrite dans cette l'exigence - que la description des tests couvre bien cette anomalie - que le résultat du test démontre bien l'implémentation du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

ATTS-C1-410 - Alerte autonomie supervision
Le dispositif de diffusion doit générer une alerte locale en cas d'incapacité à remonter les événements à la supervision pendant une durée supérieure à 15 minutes
Note de spécification :
Documentation à fournir :
- Description des anomalies - Description des tests et résultats de tests associés
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien : - **l'anomalie décrite dans cette l'exigence** - **que la description des tests couvre bien cette anomalie;** - **que le résultat du test démontre bien l'implémentation du mécanisme.** **[Evaluation sur site]** **L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre.** **Cette vérification pourra être réalisée sur site.**

ATTS-C1-420 - Alerte en cas de tentative d'accès administrateur
En cas d'échecs successifs sur l'interface d'administration, le dispositif de diffusion doit lever une alerte.
Note de spécification :
Cette exigence est applicable à l'ensemble des interfaces d'administration.
Documentation à fournir :
- Description des anomalies

- Description des tests et résultats de tests associés
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien : - l'anomalie décrite dans cette l'exigence. - que la description des tests couvre bien cette anomalie - que le résultat du test démontre bien l'implémentation du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site. L'évaluateur fera réaliser un test indépendant en laboratoire sur un échantillon fourni.
Exemple d'implémentation satisfaisant l'exigence
Un mécanisme de levée d'alerte après 3 échecs successifs répond à l'exigence.

ATTS-C1-430 - Autotest de l'horloge interne
Diagnostic sur l'horloge interne : le dispositif de diffusion doit pouvoir diagnostiquer l'état de son horloge interne. En cas d'anomalie dans le diagnostic, une alerte critique doit être levée. **Le diagnostic doit être réalisé à la fréquence suivante : au moins une fois toutes les 10 min.**
Note de spécification :
Une fréquence plus élevée peut-être mise en œuvre.
Documentation à fournir :
- Description du diagnostic réalisé et de la fréquence
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien le diagnostic réalisé et la fréquence.
Exemple d'implémentation satisfaisant l'exigence
Un mécanisme qui vérifie toutes les 5 minutes un rapport de diagnostic généré par l'horloge satisfait l'exigence.

ATTS-C1-440 - Autotest du firmware au démarrage
Le dispositif de diffusion doit réaliser un test d'intégrité du firmware à chaque démarrage. La méthode de vérification d'intégrité doit s'appuyer sur un algorithme cryptographique conforme à l'état de l'art.
Note de spécification :
L'état de l'art est établi par l'organisme national en charge de la sécurité des systèmes d'information.
Documentation à fournir :
- Description du test de firmware réalisé - Description des tests et résultats de tests associés
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien : - le mécanisme de test du firmware ; - que le mécanisme est conforme à l'état de l'art ; - que le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence

Pour la France, l'utilisation d'une signature électronique du firmware conforme aux recommandations de l'ANSSI satisfait l'exigence.

ATTS-C1-450 - Autotest des modules d'entrées et de sorties.
[Type C et D] Diagnostic des modules d'entrée et de sortie : le dispositif de diffusion doit pouvoir diagnostiquer l'état de ses modules d'entrée et de sortie. En cas d'anomalie sur le module de sortie, une alerte critique doit être levée. **En cas d'anomalie sur le module d'entrée, une alerte majeure doit être levée et le module doit être exclu du calcul du temps.** **Le diagnostic doit être réalisé à la fréquence suivante : au moins une fois par heure pour chaque entrée et chaque sortie.**
Note de spécification :
Documentation à fournir :
- Description du diagnostic réalisé et de la fréquence
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien le diagnostic réalisé et la fréquence.

8.1.19. Mise en état d'alerte par la supervision

Certaines anomalies peuvent être détectées localement par le dispositif de diffusion, mais d'autres anomalies ne peuvent être détectées que par le système de supervision, qui a une vision d'ensemble. De ce fait, ce service doit être en mesure de mettre en alerte un dispositif de diffusion en cas d'anomalie.

ATTS-C1-460 - Mise en alerte critique
Le dispositif de diffusion doit pouvoir être placé à distance depuis la supervision : - **en alerte critique (arrêt de la distribution d'un temps attesté) ;** - **en alerte majeure (perte de confiance dans l'ensemble des sources externes, fonctionnement en mode dégradé) ;** - **en alerte mineure (perte de confiance dans une source externe.** **Le message doit également permettre d'indiquer au dispositif que l'une des sources n'est plus de confiance.**
Note de spécification :
D'autres types de message ou d'actions peuvent être envoyés par la supervision, mais ils devront être documentés.
Documentation à fournir :
- Description du mécanisme de mise en alerte par la supervision - Description des tests du mécanisme et résultat d'exécution des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien - le mécanisme de mise en alerte par la supervision ; - que le mécanisme est conforme à l'exigence ; - que le résultat du test démontre bien l'implémentation du mécanisme. Nota : les trois niveaux d'alertes doivent *a minima* être testés. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre.

Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
L'envoi de l'alerte par un canal sécurisé avec authentification de la supervision répond à cette exigence.

ATTS-C1-470 - Contrôle d'accès relatif à la mise en alerte
Le dispositif de diffusion doit mettre en place une politique de contrôle d'accès : Le seul élément externe permettant de mettre le dispositif en état d'alerte doit être la supervision.
Note de spécification :
Documentation à fournir :
- Description du mécanisme permettant de garantir cette exigence - Description des tests du mécanisme et résultat d'exécution des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien - le mécanisme d'authentification de la supervision ; - que le mécanisme est conforme à l'exigence ; - que le résultat du test démontre bien l'implémentation du mécanisme. - Nota : les trois niveaux d'alertes doivent *à minima* être testés. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
L'envoi des commandes par un canal sécurisé assurant l'authentification de la supervision satisfait cette exigence.

ATTS-C1-480 - Canal sécurisé pour le transfert des alertes de supervision
Le dispositif de diffusion doit être en mesure de vérifier la nature des données envoyées par la supervision et lever une alerte si un message non cohérent est reçu.
Note de spécification :
La nature des vérifications doit être décrite par le constructeur.
Documentation à fournir :
- Description du mécanisme permettant de garantir cette exigence - Description des tests du mécanisme et résultat d'exécution des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien : - les vérifications effectuées et les éventuels mécanismes mis en place ; - que le résultat du test démontre bien l'implémentation du mécanisme pour les différents types de vérifications effectuées. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

8.1.20. Notification des anomalies

En cas d'anomalie, le dispositif de diffusion doit le notifier visuellement à l'utilisateur.

ATTS-C1-490 - Notification des anomalies
Un voyant visuel sur le dispositif de diffusion doit notifier l'utilisateur d'une anomalie.
Note de spécification :
Documentation à fournir :
- Documentation utilisateur décrivant la signification des anomalies visuelles - Description des tests du mécanisme et résultat d'exécution des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation utilisateur décrit bien le voyant d'anomalie. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme pour les différents types d'anomalies possibles (a minima mineure, majeure, critique). [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Un voyant s'éclairant en cas d'anomalie satisfait cette exigence.

8.1.21. Actions réactives en cas d'anomalie

En cas d'anomalie, les dispositifs de diffusion peuvent avoir une réaction automatique visant à corriger l'anomalie.

ATTS-C1-500 - Réactions automatiques aux alertes
[Type C &D] Les dispositifs matériels de diffusion de types C et D peuvent avoir des règles de réactions aux alertes. La documentation des dispositifs matériels de diffusion de types C et D doit documenter l'ensemble de ces règles de réaction.
Note de spécification :
Documentation à fournir :
- Description des règles de réaction - Description des tests associés et résultats de tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien les éventuelles règles de réaction et que chacune d'elle fait l'objet d'un test. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme pour les différents types de règles. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

8.1.22. Retour en mode sûr en cas d'anomalie

Suite à une action corrective, qu'elle soit automatique ou manuelle, si l'anomalie est corrigée, le dispositif de diffusion retournera dans son état nominal.

ATTS-C1-510 - Retour en mode sûr
Pour les alertes de niveau mineur à majeur, le dispositif de diffusion doit garantir le retour à un état sûr en utilisant des procédures automatisées.
Note de spécification :
Documentation à fournir :
- Description du mécanisme de remise en état sûr - Description des tests associés et résultats de tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien les éventuelles règles de remise en état sûr pour les différents types d'anomalies et qu'ils sont conformes à l'exigence. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme pour les différents types de règles. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

8.1.23. Exigences relatives à la communication des anomalies avec la supervision

Un dispositif de diffusion doit remonter de façon sécurisée l'ensemble des alertes générées localement à la supervision.

ATTS-C1-520 - Canal sécurisé
Le dispositif de diffusion doit utiliser le canal sécurisé pour transmettre les alertes à la supervision. Ce canal doit être conforme aux exigences communes.
Note de spécification :
Documentation à fournir :
Voir exigences communes
Guide de validation :
Voir exigences communes

ATTS-C1-530 - Complétude des alertes remontées
Le dispositif de diffusion doit fournir à la supervision l'intégralité des alertes locales générées. Le mécanisme mis en place doit permettre de s'assurer qu'aucune alerte n'est perdue.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests associés et résultats de tests.
Guide de validation :
[Évaluation documentaire]

L'évaluateur vérifiera que la documentation fournie décrit bien le mécanisme et qu'il est conforme à l'exigence. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site. [Phase laboratoire] Des tests indépendants complémentaires seront réalisés sur les échantillons fournis.

ATTS-C1-540 - Délai de remontée des alertes
Le dispositif de diffusion doit fournir à la supervision une alerte dans les meilleurs délais et au plus tard dans les 20 secondes après sa génération.
Note de spécification :
Ce délai n'est pas applicable en cas de non-disponibilité de la supervision.
Documentation à fournir :
- Mesure réalisée par le constructeur et description de la méthode de mesure.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien la méthode de mesure et que le résultat est conforme à l'exigence. [Evaluation sur site] L'évaluateur rejouera le test afin de constater la conformité à la mesure fournie par le constructeur. Cette vérification pourra être réalisée sur site.

8.1.24. Exigences relatives à l'administration du dispositif de diffusion

Le dispositif de diffusion doit pouvoir être administré de façon sécurisée. Il doit être administrable de façon sécurisée (authentification des administrateurs, protection des données échangées).

8.1.25. Interface d'administration

Le dispositif de diffusion doit fournir une ou plusieurs interfaces permettant de réaliser son administration.

ATTS-C1-550 - Présence d'une interface d'administration
Le dispositif de diffusion doit fournir une ou plusieurs interfaces permettant d'administrer le produit. **Au moins une des interfaces doit permettre à un service de supervision d'administrer le dispositif de diffusion à distance.**
Note de spécification :
Si le dispositif de diffusion présente plusieurs interfaces d'administration (API, terminal physique sur le dispositif, interface console…), ou permet d'accéder à l'interface d'administration de plusieurs méthodes différentes, les exigences de ce chapitre s'appliquent à chacune des interfaces et/ou chacune des méthodes.
Documentation à fournir :
- Description des interfaces
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien les interfaces d'administration et qu'il existe bien une interface d'administration à distance dédiée à la supervision [Evaluation sur site] L'évaluateur se connectera à chacune des interfaces du dispositif.
Exemple d'implémentation satisfaisant l'exigence
Un produit ne disposant que d'une seule interface à distance satisfait cette exigence.

8.1.26. Rôle permettant l'administration

Le dispositif de diffusion doit mettre en place différents niveaux d'administration, de façon à ce que seuls des utilisateurs autorisés puissent réaliser certaines opérations.

ATTS-C1-560 - Niveau d'administration
Le dispositif de diffusion doit gérer au moins 4 niveaux de rôle d'administration : - **Niveau Opérateur local** - **Niveau Administrateur** -
Note de spécification :
Si d'autres niveaux existent, le constructeur devra fournir une table de correspondance.
Documentation à fournir :
- Description des niveaux d'administration
Guide de validation :
L'évaluateur vérifiera que les niveaux décrits sont conformes à l'exigence.

ATTS-C1-570 - Administration à distance
La connexion avec le niveau administrateur doit être disponible à distance.
Note de spécification :
Cette exigence doit permettre au système de supervision d'administrer le dispositif de diffusion à distance.
Documentation à fournir :
- Description de l'interface d'administration à distance - Test de l'accès à distance par le système de supervision.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation utilisateur décrit l'accès à distance par la supervision. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

8.1.27. Authentification des administrateurs

Certains rôles ne doivent être obtenus qu'après une authentification. Les exigences suivantes sont relatives à l'authentification des administrateurs.

ATTS-C1-580 - Authentification des rôles
Pour chacune des interfaces d'administration, les rôles suivants ne peuvent être obtenus qu'après une authentification avec succès : - **Rôle administrateur** - **Rôle opérateur local**
Note de spécification :

Documentation à fournir :
- Description du mécanisme d'authentification - Description des tests d'authentification et résultat des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation utilisateur décrit le mécanisme d'authentification pour chacune des interfaces et chacun des rôles. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

ATTS-C1-590 - Expiration des sessions
L'interface d'administration doit disposer d'un mécanisme de fermeture automatique de session à partir d'une durée d'inactivité.
Note de spécification :
La durée de session peut être paramétrable. Le mécanisme est applicable à toutes les interfaces.
Documentation à fournir :
- Description du mécanisme de fermeture de session - Description des tests d'authentification et résultat des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation utilisateur décrit le mécanisme de fermeture de session pour chacune des interfaces et la durée par défaut. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

ATTS-C1-600 - Sécurisation des sessions distantes
Si un administrateur se connecte à distance (via un protocole réseau par exemple), la connexion doit être sécurisée et assurer : - **l'intégrité et la confidentialité des données échangées ;** - **l'authentification du dispositif de diffusion.**
Note de spécification :
Si l'interface d'administration est obtenue via un terminal intégré au dispositif de diffusion ou en branchant directement un écran et un clavier sur le dispositif de diffusion, cette exigence n'est pas applicable.
Documentation à fournir :
- Description du protocole réseau mis en œuvre. - Description des tests d'authentification et résultat des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit le mécanisme mis en œuvre. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Un canal SSL avec chiffrement satisfait cette exigence.

ATTS-C1-610 - Authentification en échec
Le dispositif de diffusion doit être en mesure de détecter les tentatives de connexion en échec. **En cas de tentatives successives, le dispositif de diffusion doit mettre en place une contre-mesure la protégeant d'une attaque de type force brute.**
Note de spécification :
- Description de la contre-mesure mise en œuvre. - Description des tests et résultat des tests.
Documentation à fournir :
-
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation décrit le mécanisme mis en œuvre. Il vérifiera le résultat du test démontre bien l'implémentation du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que mécanisme décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Des contre-mesures, telles qu'un temps d'attente croissant entre chaque tentative ou l'apparition d'un captcha permet de se prémunir contre de telles attaques.

8.1.28. **Paramètres d'administration**

Description des actions et modifications de configuration permises suivant les différents niveaux d'administration.

ATTS-C1-620 - Rôle Opérateur local
Le rôle opérateur doit permettre de faire la configuration IP statique ou dynamique du dispositif de diffusion.
Note de spécification :
Le service doit permettre éventuellement de configurer plusieurs adresses afin de spécifier des serveurs de secours.
Documentation à fournir :
- Description de la liste des actions possibles par le rôle opérateur - Description de la procédure, dans la documentation client, pour changer l'adresse du serveur de supervision. - Description des tests relatifs à cette exigence et résultat des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera • qu'un test permet de vérifier le changement effectif de ce paramètre. • qu'un test permet de vérifier que ce changement n'est pas accessible depuis le niveau public. [Evaluation sur site] L'évaluateur rejouera les tests. Cette vérification pourra être réalisée sur site.

ATTS-C1-630 - Rôle Administrateur
Le rôle administrateur doit permettre de configurer les paramètres opérateurs et l'ensemble des paramètres hors configuration usine. En particulier : - **Le rôle d'administrateur doit permettre de modifier le ou les serveurs de l'infrastructure de distribution de connexion.** - **Le rôle d'administration doit permettre de renouveler les moyens d'authentification opérateur** - **Le rôle d'administration doit permettre de changer le moyen d'authentification de l'administrateur.**
Note de spécification :
L'administrateur peut réaliser d'autres actions.
Documentation à fournir :
- Description de la liste des actions possibles par le rôle administrateur - Description des tests relatifs à cette exigence et résultat des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les actions décrites dans l'exigence sont également décrites dans la documentation fournie. L'évaluateur vérifiera qu'un test permet de vérifier que les actions décrites dans cette exigence sont possibles. L'évaluateur vérifiera qu'un test permet de vérifier que ce changement n'est pas accessible depuis le niveau public ou opérateur. [Evaluation sur site] L'évaluateur rejouera les tests. Cette vérification pourra être réalisée sur site.

ATTS-C1-640 - Configuration restrictive par défaut
La configuration par défaut du dispositif de diffusion doit systématiquement prendre en compte, pour chaque paramètre, la valeur la plus restrictive.
Note de spécification :
Documentation à fournir :
- Description des valeurs par défaut
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les valeurs par défaut sont bien restrictives. [Evaluation sur site] L'évaluateur vérifiera que les valeurs par défaut présentes sur l'échantillon sont bien celles décrites dans la documentation. Cette vérification pourra être réalisée sur site.

8.1.29. Gestion des mises à jour

La partie logicielle d'un dispositif de diffusion n'est pas figée au cours du temps. Elle peut être mise à jour, de façon à corriger ou faire évoluer le code du produit. La mise à jour est une opération critique qui doit pouvoir être réalisée en toute sécurité.

ATTS-C1-650 - Mise à jour du dispositif
Le dispositif de diffusion doit pouvoir être mis à jour afin de corriger les éventuelles failles de sécurité.
Note de spécification :
Afin de corriger dans un délai raisonnable les éventuelles failles de sécurité, le dispositif de diffusion doit pouvoir être mis à jour avec un mécanisme permettant le retour en arrière.
Documentation à fournir :
- Description du processus de mise à jour.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le processus de mise à jour est bien décrit.

ATTS-C1-660 - Annulation de Mise à jour du dispositif de diffusion
Toute mise à jour logicielle d'un élément du dispositif de diffusion doit pouvoir être annulée de façon à revenir à la version précédente.
Note de spécification :
Documentation à fournir :
- Description du mécanisme de retour en arrière - Descriptions des tests et résultats des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le processus de retour en arrière est décrit. L'évaluateur vérifiera qu'un test permet de vérifier que le mécanisme de retour en arrière est effectif. [Evaluation sur site] L'évaluateur rejouera les tests. Cette vérification pourra être réalisée sur site.

ATTS-C1-670 - Arrêt de la fourniture du temps lors d'une mise à jour du dispositif de diffusion
La fourniture du temps doit être interrompue lors d'une mise à jour et jusqu'à la fin de celle-ci. En cas d'échec de mise à jour, la fourniture du temps ne doit pas être rétablie.
Note de spécification :
Il est important, lors de la mise à jour, que la question de la diffusion du temps soit prise en compte.
Documentation à fournir :
- Description du mécanisme d'arrêt de distribution du temps lors d'une mise à jour - Descriptions des tests et résultats des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le mécanisme est décrit. L'évaluateur vérifiera qu'un test permet de vérifier que le mécanisme est effectif. [Evaluation sur site] L'évaluateur rejouera les tests. Cette vérification pourra être réalisée sur site.

ATTS-C1-680 - Origine de la mise à jour
Le dispositif de diffusion doit offrir par configuration : - **la possibilité à la supervision de forcer une mise à jour ;** - **de permettre au client, via son portail**
Note de spécification :
Le dispositif de diffusion étant hébergé dans un environnement client, le processus de mise à jour doit prendre en compte les contraintes de mise à jour
Documentation à fournir :
- Description du mode de configuration - Descriptions des tests et résultats des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le mécanisme est décrit. L'évaluateur vérifiera qu'un test permet de vérifier que le mécanisme est effectif dans chacune des deux options.

ATTS-C1-690 - Notification de mise à jour
[Type B] Dans le cas où la mise à jour est à l'initiative du client, les mises à jour doivent lui être notifiées sur le dispositif de diffusion.
Note de spécification :
Documentation à fournir :
- Description du mode de notification - Descriptions des tests et résultats des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le mécanisme de notification est décrit. L'évaluateur vérifiera qu'un test permet de vérifier que l'utilisateur est notifié en cas de disponibilité d'une mise à jour.

8.1.30. Autres exigences techniques de sécurité

8.1.31. Installation du dispositif de diffusion

Une mauvaise installation et/ou configuration initiale du dispositif de diffusion pourrait impacter la sécurité de l'ensemble de l'architecture du système. De ce fait, l'installation du dispositif de diffusion doit être réalisée de façon sécurisée.

ATTS-C1-700 - Installation et mise en œuvre opérationnelle du dispositif de diffusion
L'installation initiale du dispositif de diffusion doit être mise en œuvre par le fabricant et/ou une personne spécifiquement formée par le fabricant suivant la procédure d'installation. Un test de bon fonctionnement doit être réalisé conformément à une procédure préétablie et un constat de mise en fonction doit être rédigé, signé et archivé par le fabricant et par le client.
Note de spécification :
Seule la conservation de l'exemplaire du fabricant est dans le périmètre audité. Le constat peut-être sous forme papier ou sous forme électronique. S'il est sous forme électronique, des signatures électroniques conformes à la Réglementation nationale doivent être utilisées.
Documentation à fournir :
- La procédure d'installation - Modèle de constat - Exemplaires de constats remplis.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera par échantillonnage que les constats de mise en fonction sont effectivement rédigés.
Exemple d'implémentation satisfaisant l'exigence
Un constat sous forme papier satisfait l'exigence En Europe, un PV sous forme électronique muni de signature ou de cachet électronique conforme au Règlement eIDAS satisfait l'exigence.

8.1.32. Maintenance et suivi

Après l'installation, il est nécessaire d'assurer un suivi et une maintenance du dispositif de diffusion.

ATTS-C1-710 - Principe de maintenance
Le fabricant doit avoir un engagement d'être en mesure de maintenir son parc de dispositifs de diffusion en condition opérationnelle. En particulier, il doit être en mesure de fournir pendant 5 ans des pièces de rechange de ses dispositifs de diffusion ou de proposer un échange standard du matériel pour un matériel équivalent.
Note de spécification :
Documentation à fournir :
- Clause d'engagement présent dans les contrats.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera par échantillonnage que les clauses sont bien présentes dans les contrats.

8.1.33. Sécurité physique du dispositif de diffusion

Le dispositif de diffusion doit assurer sa sécurité physique.

ATTS-C1-720 - Intrusion physique
[Type C et D] Le dispositif de diffusion doit être protégé d'une intrusion physique (ouverture du dispositif de diffusion) a eu lieu.
Note de spécification :
Documentation à fournir :
- Documentation de la solution mise en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera dans la documentation qu'un dispositif est bien mis en place [Evaluation sur site] L'évaluateur vérifiera que le dispositif décrit est bien présent sur les échantillons.
Exemple d'implémentation satisfaisant l'exigence
Un scellement physique satisfait cette exigence.

ATTS-C1-730 - Capteur de température
[Type C, et D] Les dispositifs de diffusion de type C et D doivent être équipés de capteurs de températures. **Une alerte doit être générée par le dispositif de diffusion lorsque la température est hors de l'intervalle nominal.**
Note de spécification :
L'intervalle de fonctionnement nominal doit figurer dans le guide d'installation et dans le guide d'utilisation.
Documentation à fournir :
- Spécification des intervalles d'alertes décrite dans la documentation utilisateur - Description de la méthode de mesure utilisée pour les tests et de la caractérisation de l'incertitude de

mesure. - Résultats des tests réalisés par le constructeur
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera dans la documentation : - que les intervalles sont bien spécifiés ; - que le mode de notification de l'alerte est bien décrit ; - que la méthode de test est adaptée ; - que les résultats de test réalisés par le constructeur sont en ligne avec la description. [Phase laboratoire] Sur l'échantillon fourni, l'évaluateur réalisera ses propres mesures et les comparera aux résultats fournis par le constructeur.

8.1.34. **Entrée/Sorties**

ATTS-C1-740 - Mutualisation des entrées
[Type B] L'ensemble des entrées logiques du dispositif de diffusion (entrée temps, sortie temps, Supervision, Administration) peuvent être mutualisées sur la même entrée physique. **[Type C, et D] Le dispositif de diffusion doit séparer physiquement certains ports :** - **chaque port de synchronisation amont doit être distinct** - **chaque port de synchronisation aval doit être distinct des ports de synchronisation amont**
Note de spécification :
Documentation à fournir :
- Description des différents ports physiques et entrées logiques associées.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera dans la documentation : - que le lien entre les entrées physiques et logiques est décrit et est non ambiguë - qu'il est conforme à l'exigence selon le type de dispositif de diffusion visée. [Evaluation sur site] Sur l'échantillon fourni, l'évaluateur vérifiera que les ports physiques correspondent à la documentation.

ATTS-C1-750 - Bus de communication
[Type C et D] Le dispositif de diffusion doit mettre en place un bus de communication entre les entrées et les sorties. Ce bus ne peut pas être un bus réseau (IP) et il doit isoler le réseau amont (distribution) du dispositif de diffusion du réseau aval (réseau client). **Le bus doit être l'unique moyen permettant de faire transiter des informations du flux d'entrée du dispositif de diffusion vers le flux de sortie.**
Note de spécification :
Documentation à fournir :
- Description du mécanisme de Bus mis en place
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera dans la documentation que le mécanisme décrit est cohérent avec l'exigence.

8.1.35. Support du Système de calcul via GNSS

ATTS-C1-760 - Support du système de calcul via GNSS
[Type D] Les dispositifs de diffusion de type D doivent être équipés d'un module de calcul via GNSS mono-constellation ou équivalent. **Le module de calcul ou équivalent doit être conforme exigences communes des paragraphes 5.3.**
Note de spécification :
Ce module de calcul est optionnel pour un dispositif de diffusion de type B ou C. Si l'un de ces dispositifs de diffusion est équipé de ce module de calcul, alors le module doit être conforme aux exigences du paragraphe 5.3.
Documentation à fournir :
Voir paragraphes exigences du paragraphe 5.3. **Si un dispositif équivalent est proposé, le dossier d'étude démontrant l'équivalence**
Guide de validation :
Voir paragraphes exigences du paragraphe 5.3.

8.1.36. Documentation

ATTS-C1-770 - Documentation à destination du client
La documentation du dispositif de diffusion fournie au client doit contenir à minima : - **un guide d'utilisation ;** - **un guide d'installation.**
Note de spécification :
Les deux guides peuvent être présentés sous la forme d'un seul document, ou sous la forme de plusieurs documents spécifiques.
Documentation à fournir :
- Guide d'utilisation - Guide d'installation - Description de la façon dont la documentation est remise au client
Guide de validation :

[Evaluation documentaire] L'évaluateur vérifiera que les documents existent pour le modèle évalué et évaluera si la façon de le mettre à disposition du client est appropriée
Exemple d'implémentation satisfaisant l'exigence
La remise au client sous forme papier en le livrant avec le produit satisfait l'exigence La mise à disposition du client par email ou par téléchargement satisfait l'exigence.

8.1.37. Protection des environnements de développement, de test et de production du dispositif de diffusion

ATTS-C1-780 - Environnement sécurisé
Les environnements de développement, de test et de production du dispositif de diffusion doivent faire l'objet de mesures de protection physiques et logiques, en particulier de Contrôle d'accès physique et logiques permettant l'accès aux seules personnes autorisées.
Note de spécification :
Une certification ISO 27001 n'est pas requise, cependant, elle permet de justifier la mise en œuvre des mesures.
Documentation à fournir :
Description des mesures de protection physiques et logiques,
Guide de validation :
Une prise en compte des mesures dans le cadre d'une certification ISO 27001 satisfait l'exigence.

8.1.38. Gestion de configuration du produit

ATTS-C1-790 - Identification du modèle de dispositif de diffusion
Chaque modèle de dispositif de diffusion doit être clairement identifié par un identifiant unique.
Note de spécification :
L'identification du modèle de dispositif de diffusion peut être composée d'un numéro de modèle et d'un numéro de version.
Documentation à fournir :
- Description de la nomenclature des numéros de version - Fourniture du numéro du modèle évalué
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description fournie permet d'identifier de façon unique le modèle de dispositif de diffusion. [Evaluation sur site] L'évaluateur vérifiera sur les échantillons fournis que le modèle correspond bien à la version fournie par le constructeur.

ATTS-C1-800 - Identification du dispositif de diffusion
Pour chaque modèle de dispositif de diffusion donné, un numéro d'identifiant unique doit être assigné à chaque exemplaire du dispositif de diffusion.
Note de spécification :
Documentation à fournir :
- Description de la méthodologie mise en place pour assurer l'unicité
Guide de validation :

[Évaluation documentaire] L'évaluateur vérifiera que la description fournie permet de s'assurer que chaque dispositif de diffusion a un numéro unique. [Evaluation sur site] L'évaluateur vérifiera par échantillonnage que les numéros de série sont bien différents les uns des autres.

ATTS-C1-810 - Inventaire de configuration
Pour chaque modèle de dispositif de diffusion, l'ensemble des composants matériels et logiciels doivent être clairement identifiés, inventoriés, et tenus à jour. Un historique des changements de cet inventaire doit être conservé. **Une méthode de signature ou de hachage doit être mise en œuvre pour identifier les versions logiciel.**
Note de spécification :
Documentation à fournir :
- Description de la méthode de gestion de configuration utilisée
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description fournie permet de satisfaire l'exigence. **[Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que l'historique des changements est conservé.**
Exemple d'implémentation satisfaisant l'exigence
Un checksum sur tous les binaires permet de satisfaire l'exigence sur l'identification des versions logiciel.

8.1.39. Gestion des Failles de sécurité

ATTS-C1-820 - Veille technique
Le constructeur du dispositif de diffusion doit effectuer une veille technique sur les vulnérabilités pouvant affecter les composants et doit mettre en œuvre, le cas échéant, des correctifs.
Note de spécification :
Documentation à fournir :
- Description de la procédure de veille technique mise en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description fournie permet de satisfaire l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à voir la liste des vulnérabilités identifiées et les actions correctives réalisées, le cas échéant. Selon le nombre de vulnérabilités, la vérification pourra être réalisée par échantillonnage.

ATTS-C1-830 - Remontée des failles de sécurité
Le constructeur doit mettre en place une procédure documentée permettant au client de remonter des vulnérabilités sur le produit et prendre en compte les éventuelles failles remontées.
Note de spécification :
Documentation à fournir :
- Description de la procédure de remontée des vulnérabilités.

Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description fournie permet de satisfaire l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à voir la liste des vulnérabilités remontées par les clients, si cela est applicable, et les actions correctives réalisées, le cas échéant. Selon le nombre de vulnérabilités, la vérification pourra être réalisée par échantillonnage.
Exemple d'implémentation satisfaisant l'exigence
Un suivi à l'aide d'un « bugtracker » type Mantis satisfait l'exigence.

8.1.40. Tests de validation

Avant d'être délivrés au client et/ou mis en production, le fabricant doit tester les dispositifs de diffusion.

ATTS-C1-840 - Vérification de la conformité du produit par le constructeur
Le constructeur doit mettre en place une procédure documentée de test permettant de couvrir fonctionnellement le dispositif de diffusion. Cette suite de test doit être exécutée sur un exemplaire représentatif du modèle de dispositif de diffusion. La suite de test et le processus de test doivent être documentés et un constat, spécifiant la liste des tests exécutés et leur résultat doit être conservé.
Note de spécification :
Documentation à fournir :
- Description de la procédure de test - Description des tests réalisés - Résultats des tests réalisés
Guide de validation :
[Évaluation documentaire] L'évaluateur : - étudiera la pertinence de la procédure d'essais ; - vérifiera que la procédure de test existe et est exécutée à chaque nouvelle version; - vérifiera que les résultats des tests sont conservés. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer l'ensemble ou un sous-ensemble des tests (selon le nombre de tests et leur durée d'exécution) et comparera aux résultats fournis et à la description de la procédure fournie.

ATTS-C1-850 - Test du produit avant délivrance au client
Le constructeur doit mettre en place une procédure documentée de test permettant de s'assurer que le dispositif de diffusion est conforme aux exigences définies avant sa délivrance au client. La documentation devra préciser les tests réalisés et la méthode mise en œuvre.
Note de spécification :
Documentation à fournir :
- Description de la procédure de test - Description des tests réalisés - Résultats des tests réalisés
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que : - la procédure de test existe ; - que la méthode mise en œuvre est adéquate. - [Évaluation fonctionnelle] Par échantillonnage, l'évaluateur vérifiera que les tests sont bien réalisés.

8.2. Module C2 : Dispositif de diffusion du temps de référence (Type A)

Ce chapitre décrit les exigences applicables pour la certification d'un module nommé «Dispositif de diffusion du temps de référence (de Type A)» au sein de l'architecture du système.

Ce dispositif de diffusion est un ensemble de sites, de moyens humains, matériels, logiciels et réseaux, et de procédures permettant de diffuser un temps attesté par une architecture certifiée..

Contrairement aux dispositifs matériels de diffusion installés dans le périmètre client, le système de diffusion de type A est un système de diffusion :

- Potentiellement mutualisé entre plusieurs clients
- Opéré hors du périmètre du client.

Dans l'architecture, le système logiciel de diffusion de type A est installé au sein du SI de l'architecture (hors client) et diffuse aux Agents de réception le temps distribué par un dispositif spécifique relié au système de distribution. De ce fait, les exigences qui suivent portent principalement sur :

- Le fonctionnement et les conditions d'opération du service
- Le protocole d'échange avec les Agents
- Le protocole d'échange avec le service de supervision et de contrôle
- Les conditions de raccordement au système de distribution
- Les matériels mis en œuvre.

Le rôle du dispositif de type A est le transport sécurisé du temps d'un système de distribution vers des Agents de réception se trouvant dans le périmètre du SI client. De ce fait, ces principales fonctions sont :

- Se synchroniser avec un système de distribution du temps
- Sécuriser et tracer les synchronisations
- Fournir du temps à des Agents de réception certifiés en aval
- Remonter les informations de synchronisation au Service de consolidation et d'analyse des traces de supervision de l'architecture pour fournir une attestation du temps.

Un dispositif de diffusion du temps de référence de type A doit remplir les objectifs suivants :

- Récupérer de façon sécurisée des informations temps auprès d'un système de distribution
- Assurer le transport du temps dans l'exactitude cible
- Assurer la traçabilité des opérations.
- Remonter à la supervision de l'historique de synchronisation
- Gérer des états d'alerte et de la continuité d'activité
- Remonter à la supervision des alertes locales
- Assurer la sécurité physique, logique et organisationnelle du service.

8.2.1. Exigences relatives au raccordement au système de distribution

Les exigences ci-après sont relatives à la synchronisation du dispositif de diffusion avec le système de distribution. Ces exigences ont principalement pour objectif de récupérer de façon sécurisée des informations temps auprès d'un système de production.

Le raccordement doit principalement assurer que :

- Le système de diffusion est effectivement synchronisé avec un système de distribution certifié et non avec un autre système.
- Le système de distribution est synchronisé conformément à l'exactitude cible
- L'information temps n'est pas altérée lorsque celle-ci est récupérée.

ATTS-C2-010 - Documentation du raccordement au système de distribution.
La méthode de raccordement du système de diffusion de type A doit être documentée.
Note de spécification :
Elle peut s'appuyer sur des systèmes virtuels
Documentation à fournir à l'évaluateur :
- Un document descriptif de la méthode de raccordement mise en œuvre. - Un constat de raccordement, signé a minima par un responsable du système de distribution et par le responsable du système de diffusion
Guide de validation :
[Evaluation documentaire] L'évaluateur : - S'assurera que la documentation est fournie - L'évaluateur analysera la documentation fournie. La documentation doit être complète et suffisante pour comprendre le mécanisme mis en œuvre sans ambiguïté.

ATTS-C2-020 - Sécurisation du raccordement au système de distribution.
La méthode de raccordement doit garantir que : - **Le système de diffusion est bien raccordé au système de distribution** - **La sécurité de la communication est assurée (intégrité et origine)**
Note de spécification :
La sécurité de l'environnement peut être obtenue : - Soit par sécurisation logique (chiffrement…) du flux - Soit par sécurisation physique (contrôle d'accès…) du média transportant le flux.
Documentation à fournir :
- Description du raccordement - Description des mesures de sécurité mise en œuvre
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la méthode de raccordement mise en place assure une sécurité suffisante du raccordement. En particulier : - Un tiers ne doit pas pouvoir altérer sans difficulté significative le flux - Un tiers ne doit pas pouvoir changer l'origine du flux sans difficulté significative.

[Évaluation fonctionnelle] L'évaluateur vérifiera que les mesures de sécurité décrites sont bien mises en œuvre.
Exemple d'implémentation satisfaisant l'exigence
Les solutions suivantes satisfont l'exigence : - Sécurisation du flux logique par des moyens cryptographiques à l'état de l'art garantissant l'origine et l'intégrité (par exemple, signature électronique ou scellement des données. - Isolation physique et logique du média transportant l'information (par exemple : média dédié) et mise en place de mesures de contrôle d'accès physique.

ATTS-C2-030 - Fréquence de synchronisation avec le serveur de distribution
Le dispositif de diffusion de Type A doit être paramétré pour réaliser une synchronisation avec le serveur de distribution de distribution a minima une fois toutes les 30 17 min en fonctionnement nominal
Note de spécification :
Documentation à fournir :
- Documentation de la synchronisation -
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation est conforme. [Évaluation fonctionnelle] L'évaluateur vérifiera que les fréquences sont conformes à l'exigence.

ATTS-C2-040 - Source de temps
Le système de diffusion de type 1 ne doit pas prendre en compte dans ses calculs de temps un serveur de l'infrastructure de distribution du temps désigné comme « désynchronisé ».
Note de spécification :
Documentation à fournir :
Documentation technique intégrant cette exigence
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation est conforme. [Évaluation fonctionnelle] L'évaluateur vérifiera que la sécurité est bien implémentée.

ATTS-C2-050 - Seconde intercalaire
Le système de diffusion doit être en mesure de prendre en compte la seconde intercalaire.
Note de spécification :
Documentation à fournir :
Documentation technique intégrant cette exigence
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la manière dont est gérée la seconde intercalaire est précisée dans la procédure. [Évaluation fonctionnelle] L'évaluateur vérifiera qu'une surveillance de la seconde intercalaire est bien mise en œuvre

ATTS-C2-060 - Séparation physique
Si le système de diffusion de Type A est opérée dans le même environnement que le système de distribution, les serveurs et matériels permettant d'opérer le système de diffusion de Type A doivent être physiquement séparés de distribution
Note de spécification :
Le système de diffusion de Type A ne peut pas être hébergé à l'intérieur du serveur de distribution. Les serveurs doivent être distincts.
Documentation à fournir :
La documentation d'architecture et un diagramme réseau seront fournis à l'évaluateur. Ces diagrammes devront identifier de façon non ambiguë les serveurs utilisés pour la distribution (à destination des dispositifs de diffusion de type autre que A) et les serveurs utilisés dans le cadre de l'opération d'un dispositif de diffusion de Type A.
Guide de validation :
L'évaluateur vérifiera : - d'un point de vue documentaire, que l'exigence ci-dessus est bien remplie; - sur site, que la séparation est effective et correspond à la documentation. En particulier, il s'assurera : o que les machines décrites se trouvent bien sur site ; o que les machines adressent bien des populations distinctes (cela pourra être constaté par échantillonnage sur les traces des machines).

ATTS-C2-070 - Protection du serveur de distribution
Le canal permettant la synchronisation entre le serveur de distribution et le système de diffusion de Type A doit offrir des mesures de sécurité permettant de s'assurer que : **les agents se synchronisant au dispositif de diffusion de type A ne peuvent pas se connecter au serveur de distribution ;** - **les synchronisations entre le dispositif de diffusion de type A et le serveur de distribution sont tracées..**
Note de spécification :
Documentation à fournir :
La documentation des mesures de sécurité doit être fournie.
Guide de validation :
L'évaluateur vérifiera : - D'un point de vue documentaire, que l'exigence ci-dessus est bien remplie - Sur site, que la mise en place des mesures décrites est effective.

8.2.2. Exigences relatives à la diffusion aux Agents de réception du temps de référence

ATTS-C2-080 - Interface de synchronisation sécurisée pour le dispositif de diffusion de type A
Le système de diffusion A doit fournir une interface permettant aux Agents de se connecter.
Note de spécification :
Documentation à fournir :
- Description de l'interface - Résultats des tests réalisés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si les résultats des tests sont conformes.

ATTS-C2-090 - Garantie de l'exactitude du temps fourni par le dispositif de diffusion de type A
La Système de diffusion de type A doit être en mesure de fournir un temps avec une exactitude de 300 ms.
Note de spécification :
La mesure doit prendre en compte l'ensemble des erreurs à l'exclusion d'une erreur de synchronisation due à une asymétrie du lien réseau.
Documentation à fournir :
- Description de l'interface - Résultats des tests réalisés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si les résultats des tests sont conformes. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests.

ATTS-C2-100 - Protocole d'accès
Le système de diffusion de type A doit supporter le protocole NTP.
Note de spécification :
Documentation à fournir :
- Description de l'interface - Résultats des tests réalisés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si les résultats sont conformes. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests.

8.2.3. Sécurisation de l'interface

ATTS-C2-110 - Identification des Agents
Le système de diffusion de Type A doit être en mesure de n'accepter que des connexions entrantes venant d'Agents autorisés. **Un Agent de réception du temps de référence non identifié ou authentifié ne doit pas être en mesure de se connecter au système de diffusion**
Note de spécification :
Documentation à fournir :
Description du moyen mis en œuvre Tests réalisés
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si le moyen mis en œuvre est conforme à l'exigence. Il vérifiera également si les résultats des tests sont conformes. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests.

ATTS-C2-120 - Garantie de l'intégrité du temps fourni par le système de diffusion
Le système de diffusion de Type A doit être en mesure de mettre à disposition de l'élément aval (Agent) un moyen cryptographique permettant, directement ou indirectement, à l'élément aval d'être assuré de l'intégrité du flux-temps fourni par le système de diffusion. Ce moyen cryptographique doit être fondé sur

un algorithme cryptographique qui satisfait aux recommandations de l'ANSSI.
Note de spécification :
Documentation à fournir :
Description du moyen mis en œuvre Tests réalisés
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si le moyen mis en œuvre est conforme à l'exigence. Il vérifiera également si les résultats des tests sont conformes. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests.

8.2.4. Exigences relatives à la traçabilité du temps

Le transport du temps doit faire l'objet d'une traçabilité.

ATTS-C2-130 - Traçabilité du transport du temps
Les synchronisations entre le système de distribution et le système de diffusion de Type A doivent être tracées.
Note de spécification :
Cette exigence est une exigence technique.
Documentation à fournir :
- Documentation expliquant comment la traçabilité est réalisée. - Exemples de traces générées.
Guide de validation :
[Evaluation documentaire] L'évaluateur : - S'assurera que la documentation est fournie - S'assurera que les traces fournies sont conformes à la documentation. - [Évaluation fonctionnelle] L'évaluateur vérifiera par échantillonnage que les logs ont bien été produits et archivés (l'évaluateur choisira de façon arbitraire des dates et heures de synchronisation et l'audité lui fournira les traces correspondantes)
Exemple d'implémentation satisfaisant l'exigence
L'enregistrement systématique de toutes les traces de synchronisation PTP/NTP des échanges entre les deux serveurs permet de satisfaire cette exigence.

ATTS-C2-140 - Protection des traces de synchronisation
Le système de diffusion doit assurer la protection des traces générées contre la perte et/ou la modification.
Note de spécification :
La norme SOGIS satisfait l'exigence
Documentation à fournir :
- Description des mesures mises en place.
Guide de validation :
[Evaluation documentaire] L'évaluateur : - S'assurera que la documentation est fournie - S'assurera que les mesures décrites sont pertinentes.

- [Évaluation fonctionnelle] L'évaluateur vérifiera que les mesures décrites sont implémentées.
Exemple d'implémentation satisfaisant l'exigence
Des mesures de restriction d'accès en écriture et d'externalisation des sauvegardes satisfont cette exigence.

8.2.5. Exigences relatives à la Remontée des traces à la Supervision

L'ensemble des traces de synchronisation générées par les différents composants de diffusion doivent être remontées au service de supervision et de contrôle. Cette remontée doit être réalisée de façon sécurisée.

ATTS-C2-150 - Mécanisme de remontée de traces à la supervision
Le système de diffusion doit mettre en place un mécanisme de remontée des traces de l'ensemble des échanges avec le ou les serveur(s) de l'infrastructure de distribution aux exigences communes présente dans le paragraphe 10.1.8.
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.8.
Guide de validation :
- Voir paragraphe 10.1.8.

8.2.6. Exigences relatives à la surveillance et à la gestion des alertes

Le système de diffusion doit mettre en place un mécanisme interne de gestion des alertes.

ATTS-C2-160 - Gestion des alertes
Le système de diffusion doit mettre en place une surveillance des éléments techniques mis en œuvre. En particulier, les alertes générées par les serveurs de distribution doivent être surveillées.
Note de spécification :
Documentation à fournir :
- Documentation du système de surveillance mis en œuvre
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera qu'un mécanisme de surveillance est en place. [Évaluation fonctionnelle] l'évaluateur : - vérifiera que le mécanisme est bien implémenté et est conforme à sa description ; - demandera à consulter la liste des alertes générées. Il s'attachera à vérifier : o par échantillonnage, que les alertes ont fait l'objet d'un traitement ; o que le nombre d'alertes généré est en adéquation avec le dimensionnement de l'équipe en charge de son traitement.

ATTS-C2-170 - Mécanisme de détection des vulnérabilités
Des mécanismes de détection de vulnérabilités (
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera qu'un mécanisme de surveillance est en place. [Évaluation fonctionnelle] l'évaluateur - vérifiera que le mécanisme est bien implémenté et est conforme à sa description ; - demandera à consulter la liste des alertes générées. Il s'attachera à vérifier : o par échantillonnage, que les alertes ont fait l'objet d'un traitement ; - vérifiera que le nombre d'alertes généré est en adéquation avec le dimensionnement de l'équipe chargée de son traitement.

ATTS-C2-180 - Notification des incidents à la supervision interne
Tout incident interne impactant la diffusion du temps doit être remonté sans délai au service de supervision et de contrôle.
Note de spécification :
En particulier, cette exigence est applicable aux incidents impactant : - **l'intégrité ou l'origine du temps distribué ;** - **l'exactitude du temps distribué ;** - **la disponibilité du temps**
Documentation à fournir :
- Description de l'organisation mise en place pour remonter les exigences au système de supervision et de contrôle - Liste des incidents pris en compte.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera qu'une organisation est en place. [Évaluation fonctionnelle] L'évaluateur : - vérifiera que le mécanisme est bien implémenté et est conforme à sa description ; - demandera à consulter la liste des incidents remontés à la supervision.

ATTS-C2-190 - Mise en place de procédures de remontée des incidents
Chaque entité opérant une composante du système de diffusion doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.
Note de spécification :
Documentation à fournir :
- Description des procédures mises en place.

Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera qu'une organisation est en place et si celle-ci semble pertinente. [Évaluation fonctionnelle] L'évaluateur vérifiera que la procédure de remontée d'incident est connue des personnels. Cette vérification se fera lors d'une entrevue et par échantillonnage. L'évaluateur demandera à consulter la liste des incidents remontés par les personnels et vérifiera par échantillonnage qu'un traitement a été réalisé.

ATTS-C2-200 - Action en cas d'incident critique
Dans le cas d'un incident critique, comme la suspicion de compromission ou la compromission d'un élément majeur du système de diffusion, ou le soupçon de la diffusion d'un temps erroné, le système de diffusion doit : - **notifier immédiatement et sans délai l'entité responsable de l'architecture du système ;** - **stopper la diffusion du temps sur tous les systèmes impactés ;** - **traiter impérativement l'incident critique dès détection et dans les meilleurs délais.**
Note de spécification :
Documentation à fournir :
- Procédure de traitement des incidents critiques
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la procédure existe si celle-ci respecte l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à voir la liste des incidents critiques survenus et si la procédure a bien été appliquée.

8.2.7. Exigences relatives à la sécurité physique

ATTS-C2-210 - Exigences communes
Les sites d'exploitation du système de diffusion doivent respecter les exigences communes relatives à la sécurité physique du paragraphe 10.1.1.
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.1.
Guide de validation :
Voir paragraphe 10.1.1.

8.2.8. Exigences relatives aux ressources humaines

ATTS-C2-220 - Exigences communes
Les sites d'exploitation du système de diffusion doivent respecter les exigences relatives aux ressources humaines du paragraphe 10.1.2.
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.2.
Guide de validation :
- Voir paragraphe 10.1.2.

8.2.9. Exigences relatives à la sécurité logique

ATTS-C2-230 - Exigences communes
Les sites d'exploitation du système de diffusion doivent respecter les exigences communes relatives à la sécurité logique du paragraphe 10.1.3.
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.3.
Guide de validation :
- Voir paragraphe 10.1.3.

ATTS-C2-240 - Filtrage des flux entrants
Le système de diffusion doit mettre en place un mécanisme de pare-feu entre les Agents et le système de diffusion de type A. Les pare-feu doivent être configurés de façon à ne laisser passer que les flux autorisés. Il est possible de mettre en place une configuration dynamique de l'ouverture des flux, mais dans ce cas, les règles d'ouverture et de fermeture automatique de flux devront être documentées. Dans tous les cas, les ouvertures et fermetures de port doivent faire l'objet d'une traçabilité.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en place
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le mécanisme décrit est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, éventuellement par échantillonnage : - que les pare-feu sont mis en œuvre conformément à la description fournie ; - que les traces d'ouverture et de fermeture de flux sont produites et conservées

ATTS-C2-250 - Filtrage des flux sortants
Le système de diffusion doit laisser passer le flux permettant de remonter les traces de synchronisation vers la supervision.
Note de spécification :
Documentation à fournir :
Description du mécanisme en place
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le mécanisme décrit est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, éventuellement par échantillonnage, que la configuration du pare-feu est conforme à la description.

ATTS-C2-260 - Protection des matériels réseaux - Environnement physique
Le système de diffusion doit garantir que les composants matériels (hors câblage) du réseau de diffusion (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé.
Note de spécification :
Documentation à fournir :
- Description de l'environnement
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que l'environnement décrit est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, éventuellement par échantillonnage, que l'environnement est conforme à la description.

ATTS-C2-270 - Surveillance et prévision
L'entité opérant le système de diffusion a une obligation de surveillance du dimensionnement et de prévision de volumétrie à venir
Note de spécification :
Documentation à fournir :
- Plan de charge incluant l'estimation de charge à venir. - Mesure de la charge actuelle et passée
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation est fournie et si les estimations semblent réalistes vis-à-vis de l'historique mesuré.

ATTS-C2-280 - Journalisation des événements
Les sites d'exploitation du système de diffusion doivent respecter les exigences relatives à la journalisation des événements du paragraphe 10.1.4
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.4
Guide de validation :
Voir paragraphe 10.1.4

8.2.10. Exigences relatives à la continuité d'activité

ATTS-C2-290 - Continuité d'activité
Les sites d'exploitation du système de diffusion doivent respecter les exigences relatives à la journalisation des événements du paragraphe 0
Note de spécification :
Documentation à fournir :
Voir paragraphe 0
Guide de validation :
Voir paragraphe 0

Par ailleurs le système de diffusion doit respecter les exigences suivantes.

ATTS-C2-300 - Disponibilité
Le système de diffusion doit mettre en place une architecture de haute disponibilité. L'architecture doit être mise en place de façon à atteindre un niveau de disponibilité de 99,5% de chacune des fonctions critiques.
Note de spécification :
Les fonctions critiques comportent a minima : La diffusion du temps La remontée des incidents à la supervision La remontée des traces de synchronisation à la supervision
Documentation à fournir :
- Description de l'architecture de haute disponibilité mise en place.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que l'architecture décrite est adéquate. [Évaluation fonctionnelle] L'évaluateur vérifiera, éventuellement par échantillonnage, l'architecture décrite est bien mise en place.

8.3. Module C3 : Agent de réception du temps de référence

Ce chapitre décrit les exigences applicables pour la certification d'un module nommé « Agent de réception du temps de référence » (dit Agent) au sein de l'architecture du système.

Dans l'architecture du système, l'Agent est installé au sein du SI du client et surveille la synchronisation d'un élément final (L'Agent est un produit purement logiciel, installé sur une machine hôte). De ce fait, les exigences qui suivent :

- Sur le produit lui-même (parties matérielles et logicielles)
- Sur le cycle de vie du produit
- Sur l'environnement du produit
- Sur les protocoles d'échange avec :
    - Le système de diffusion, placé en amont (physique ou virtuel)
    - l'élément final à synchroniser
    - Le service de supervision et de contrôle.

Ses fonctionnalités principales sont :

- Sécuriser et tracer les synchronisations
- Remonter les informations de synchronisation à l'architecture du système à des fins de supervision et d'attestation du temps fourni.
- Remonter à la supervision des alertes locales (anomalie de synchronisation ; entité amont non atteignable)
- Gérer des états d'alerte
- Optionnellement, synchroniser l'élément final avec une source de temps en amont dans l'architecture du système

L'Agent de diffusion du temps de référence doit remplir les objectifs suivants :

- Se connecter de façon sécurisée (intégrité et authentification) à l'élément amont pour contribuer ou réaliser une synchronisation temps
- Contribuer au tracer de l'ensemble des synchronisations réalisées
- Dialoguer avec la supervision l'historique de synchronisation (synchronisation amont et aval) de façon sécurisée (intégrité et authentification mutuelle)
- Être en mesure, en cas de détection d'anomalies, de notifier l'utilisateur.
- Remonter à la supervision les alertes locales (par exemple anomalie de synchronisation ; entité amont non atteignable) de façon sécurisée (intégrité et authentification) et réception et prise en compte d'un état l'alerte fournie par la supervision [intégrité et garantie de l'origine]
- Être administrable de façon sécurisé (authentification des administrateurs, protection des données échangées)

8.3.1. Exigences relatives à la synchronisation Amont

Les exigences ci-après sont relatives à la synchronisation de l'Agent et de l'élément final du client avec un système de diffusion.

L'Agent doit être en mesure :

- De s'assurer que l'élément final (du client) est synchronisé avec le service de diffusion avec une précision donnée
- De s'assurer que la synchronisation a été réalisée de façon sécurisée.

ATTS-C3-010 - Type de système de diffusion
L'agent doit être en mesure d'effectuer des synchronisations avec des dispositifs de diffusion de tout type
Note de spécification :
Documentation à fournir :
- liste des dispositifs compatibles ; - cahier de test et résultats de test
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation est conforme à l'exigence. **[Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests sur chaque système de diffusion compatible.**

ATTS-C3-020 - Protocoles à supporter
L'agent doit se synchroniser avec l'élément amont du dispositif de diffusion à l'aide a minima du protocole sécurisé basé sur NTP.
Note de spécification :
Les agents doivent *a minima* supporter le protocole spécifié ci-dessus. Il est possible pour un agent de supporter d'autres protocoles équivalents permettant d'obtenir une exactitude similaire. Le développeur de l'Agent devra alors préciser si ces protocoles sont compatibles ou non avec l'architecture du système.
Documentation à fournir :
- Spécification fonctionnelle de l'agent. - La documentation de l'agent devra préciser les moyens de synchronisation avec l'élément final du client
Guide de validation :
Concernant les protocoles obligatoires, l'évaluateur réalisera les vérifications suivantes : • **L'évaluateur vérifiera dans la documentation que le protocole obligatoire est documenté. La version du protocole devra être précisée ainsi que les options éventuelles d'implémentation.** • **La liste des systèmes d'exploitation compatible et la politique de mise à jour de l'Agent.** **Concernant les protocoles alternatifs.** • **Le constructeur devra fournir la description du protocole et la liste des systèmes d'exploitation accueillants ;** • **Le constructeur devra faire la démonstration de l'équivalence du protocole alternatif proposé** • **Les vérifications réalisées pour le protocole obligatoire sont applicables aux protocoles alternatifs.**

ATTS-C3-030 - Observation de la dérive
L'Agent doit être en mesure de comparer le temps reçu (origine dispositif de diffusion du temps) et le temps de l'élément final du client cible afin de déterminer la dérive de cet élément. En cas d'écart supérieur à la tolérance de l'exactitude cible, l'Agent doit générer une alerte.
Note de spécification :
Documentation à fournir :
- Description fonctionnelle du mécanisme. - Description et résultat des tests correspondants
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - **La manière dont est gérée la comparaison est précisée dans la documentation fonctionnelle fournie** - **Le cahier de test couvre la vérification, en particulier que les cas de succès et d'échec sont couverts.** **[Evaluation sur site] L'évaluateur rejouera le test.** **Cette vérification pourra être réalisée sur site.**

ATTS-C3-040 - [Conditionnel] Synchronisation de l'élément final du client
Si l'élément final du client le permet et si la configuration de l'agent l'indique, l'agent doit déclencher périodiquement des synchronisations entre l'élément final du client et le dispositif de diffusion. **Le mécanisme doit être débrayable dans la configuration de l'élément final du client.**
Note de spécification :
Documentation à fournir :
- Description du mécanisme de synchronisation - Documentation et résultat des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - **la manière dont est gérée la comparaison est précisée dans la documentation fonctionnelle fournie ;** - **que le mécanisme est débrayable dans la configuration ;** - **le cahier de test couvre la vérification, en particulier que les cas de succès et d'échec sont couverts.** **[Evaluation sur site] L'évaluateur rejouera le test.** **Cette vérification pourra être réalisée sur site.** **L'évaluateur vérifiera sur une configuration type que les synchronisations sont bien effectives et permettent le maintien l'élément final du client à l'heure ou la possibilité de comparer les écarts.**

ATTS-C3-050 - Périodicité de Synchronisation
La périodicité minimale doit être conforme aux exigences fixées dans les exigences de l'architecture du système.
Note de spécification :
Documentation à fournir :
- Description de la périodicité minimale. - Description des tests et résultat des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la périodicité décrite est conforme au cahier d'exigence ou paramétrable. Si elle est paramétrable, il sera vérifié que la valeur cible est une valeur acceptée par l'agent et fait l'objet d'un test. **[Evaluation sur site] L'évaluateur rejouera le test.**

ATTS-C3-060 - Authentification de l'Agent
Si l'Agent se synchronise sur un dispositif de diffusion du temps de référence de type A de diffusion, l'Agent doit obtenir une autorisation préalable auprès de la supervision et doit être authentifié. Une authentification mutuelle doit être mise en place.
Note de spécification :
L'autorisation peut être une autorisation de connexion temporaire ou permanente.
Documentation à fournir :
- Description fonctionnelle du type et mode d'autorisation obtenue de la supervision. - Description et résultat des tests correspondants
Guide de validation :

[Evaluation documentaire] L'évaluateur vérifiera que :
- la manière dont est gérée l'autorisation est précisée dans la documentation fonctionnelle fournie ;
- le cahier de test couvre la demande d'autorisation, en particulier :
  o que le cas nominal est couvert ;
  o que dans les différents cas d'erreurs décrits dans la documentation (autorisation refusée, autorisation expirée, *etc*.), la synchronisation avec le service de distribution n'est pas possible.
[Evaluation sur site] L'évaluateur rejouera le test.
Cette vérification pourra être réalisée sur site.

ATTS-C3-070 - Authentification dans le protocole de connexion
Le protocole de connexion entre l'Agent et le dispositif de diffusion doit inclure une authentification double : - **Le dispositif de diffusion doit être authentifié** - **L'agent doit être authentifié.** **Le niveau d'authentification attendu est le suivant :** - **L'authentification du dispositif de diffusion doit être réalisée par un certificat d'authentification ou un mécanisme démontré d'une robustesse équivalente.**

- **L'authentification de l'agent peut être réalisée par l'utilisation d'un couple identifiant/mot de passe ou par un moyen d'authentification supérieur (par exemple, certificat d'authentification).** **Dans le cas de l'utilisation d'un certificat, celui-ci doit être conforme aux recommandations cryptographiques de l'organisme national en charge de la sécurité de l'information.** **Dans le cas de l'utilisation d'un mot de passe, celui-ci doit être conforme en termes de longueur et de complexité aux recommandations de l'organisme national en charge de la sécurité des systèmes d'information**
Note de spécification :
L'authentification peut être réalisée soit de façon directe, soit de façon indirecte en confiant l'authentification à un service tiers dans lequel le système de distribution est lui-même authentifié. **Le mécanisme cryptographique doit être conforme à l'état de l'art de la cryptographie tel que défini par l'organisme national en charge de la sécurité des systèmes d'information**
Documentation à fournir :
- Description fonctionnelle du type d'authentification réalisé. - Description et résultat des tests correspondants
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - La manière dont est gérée la double authentification est précisée dans la documentation fonctionnelle fournie - Le cahier de test couvre l'authentification, en particulier, les cas de succès et d'échec sont couverts. [Evaluation sur site] L'évaluateur rejouera le test. Cette vérification pourra être réalisée sur site.

ATTS-C3-080 - Intégrité de l'information de temps reçue
L'agent doit être en mesure de vérifier l'intégrité du temps fourni à l'aide d'un algorithme cryptographique.
Note de spécification :
Le mécanisme cryptographique doit être conforme à l'état de l'art de la cryptographie tel que défini par l'organisme national en charge de la sécurité des systèmes d'information
Documentation à fournir :
- Description fonctionnelle du type de vérification réalisée. - Description et résultat des tests correspondants
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - La manière dont est gérée la vérification de l'intégrité des données reçues est précisée dans la documentation fonctionnelle fournie - Le cahier de test couvre la vérification, en particulier, les cas de succès et d'échec sont couverts. [Evaluation sur site] L'évaluateur rejouera le test. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Un mécanisme de hachage ou de signature électronique (conforme à l'état de l'art) des données de synchronisation reçues satisfait l'exigence.

ATTS-C3-090 - Origine de l'information de temps reçue
L'agent doit être en mesure de vérifier de façon fiable l'origine de la source de temps à l'aide d'un algorithme cryptographique ou d'un mécanisme dont la robustesse est démontrée équivalente.
Note de spécification :
Le mécanisme cryptographique doit être conforme à l'état de l'art de la cryptographie tel que défini par l'organisme national en charge de la sécurité des systèmes d'information
Documentation à fournir :
- Description fonctionnelle du type de vérification réalisée. - Description et résultat des tests correspondants
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - La manière dont est gérée la vérification de l'origine des données reçues est précisée dans la documentation fonctionnelle fournie - Le cahier de test couvre la vérification, en particulier, les cas de succès et d'échec sont couverts. [Evaluation sur site] L'évaluateur rejouera le test. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Le transport des données à travers un canal sécurisé SSL avec authentification du serveur de distribution satisfait cette exigence.

8.3.2. Exigences relatives à la gestion des erreurs

ATTS-C3-100 - locale d'erreur
L'Agent doit être en mesure de détecter les erreurs suivantes : **-retour dans le temps ;** **-écart instantané supérieur à une valeur indiquée dans la configuration ;** **-dérive sur une période donnée supérieure à une certaine valeur indiquée dans la configuration ;** **-échec de connexion à un dispositif de diffusion.**
Note de spécification :
Documentation à fournir :
- Liste des erreurs détectées par l'agent. - Description et résultat des tests correspondants
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - La liste des erreurs contient a minima celles précisées dans l'exigence. - Le cahier de test couvre la vérification de l'exigence, en particulier que les cas d'erreur de l'exigence. [Evaluation sur site] L'évaluateur rejouera le test. Cette vérification pourra être réalisée sur site.

ATTS-C3-110 - Remontée des erreurs locales à la supervision
L'Agent doit être en mesure de remonter l'ensemble des erreurs locales à la supervision
Note de spécification :
Documentation à fournir :
- Mécanisme de remontée des erreurs - Description et résultat des tests correspondants
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - le mécanisme est décrit ; - le cahier de test couvre la vérification de l'exigence, en particulier que l'ensemble des alertes sont remontées. [Evaluation sur site] L'évaluateur rejouera le test. Cette vérification pourra être réalisée sur site.

ATTS-C3-120 - Réception d'erreurs détectées par la supervision
L'Agent doit être en mesure de recevoir des états d'erreurs détectés par la supervision
Note de spécification :
Documentation à fournir :
- Liste des erreurs pouvant être notifiées par la supervision - Description et résultat des tests correspondants
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - La liste des erreurs contient a minima celles précisées dans l'exigence. - Le cahier de test couvre la vérification de l'exigence, en particulier que les cas d'erreur de l'exigence. [Evaluation sur site] L'évaluateur rejouera le test. Cette vérification pourra être réalisée sur site.

ATTS-C3-130 - Sécurisation de la remontée des traces à la supervision
L'Agent doit utiliser un canal sécurisé pour transmettre et recevoir les alertes avec la supervision. Ce canal doit être conforme aux exigences communes.
Note de spécification :
Documentation à fournir :
Voir exigences communes
Guide de validation :
Voir exigences communes

ATTS-C3-140 - Notification
Sauf si l'utilisateur ou l'administrateur a désactivé les notifications, toutes les alertes de l'agent (alertes locales et alertes émises par la supervision) doivent être notifiées à l'utilisateur. Les alertes doivent en particulier indiquer explicitement si le temps n'est plus en mesure d'être attesté et/ou est soupçonné ne plus pouvoir être attesté.
Note de spécification :
Documentation à fournir :
- Description du mécanisme de notification - Guide utilisateur - Description et résultat des tests correspondants
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - Le mécanisme est décrit. - Le guide utilisateur décrit bien les différentes notifications et leur sens. - Les tests couvrent bien le cas d'une erreur envoyée depuis la supervision et les différents cas d'erreurs locales. [Evaluation sur site] L'évaluateur rejouera le test. Cette vérification pourra être réalisée sur site.

8.3.3. Exigences relatives à la Traçabilité

L'Agent doit être en mesure :

- De générer des traces de l'ensemble des synchronisations et de l'ensemble des éléments pertinents.
- D'assurer la protection de ces traces.

ATTS-C3-150 - Exigences de Traçabilité
L'agent doit être conforme à l'ensemble des exigences communes du chapitre 10.1. .7
Note de spécification :
Documentation à fournir :
Voir chapitre 10.1. .7
Guide de validation :
Voir chapitre 10.1. .7

ATTS-C3-160 - Liste minimale des traces devant être générées
En complément des exigences du chapitre 10.1. , un Agent doit générer un enregistrement d'audit des événements suivants : **a) synchronisation élément(s) amont** **b) synchronisation de l'élément final du client**
Note de spécification :
La documentation fonctionnelle et/ou technique de l'agent devra lister les types d'événements et décrire les formats des traces.
Documentation à fournir :
- Exemple de traces générées par l'agent, couvrant l'ensemble des événements - Spécification fonctionnelle décrivant le format des traces - Description des tests et résultats des tests correspondant à l'exigence.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - **que la spécification fonctionnelle décrit bien le contenu des traces ;** - **que l'exemple généré est bien conforme à la description de la spécification fonctionnelle ;** - **que les tests couvrent bien l'ensemble des traces décrites dans l'exigence.** **[Evaluation sur site]** - **l'évaluateur rejouera les tests ;** - **l'évaluateur récupérera des traces et d'assurera qu'elles sont conformes à la description et aux exemples fournis.** **Cette vérification pourra être réalisée sur site.**

ATTS-C3-170 - Dysfonctionnement de la génération de trace
En cas d'arrêt ou de dysfonctionnement des fonctions de génération de logs (exemple : espace de stockage plein, espace de stockage sur le disque placé en lecture seule, accès concurrent), l'agent doit se mettre dans un état d'alerte majeure (il continue à surveiller ou déclencher les synchronisations, mais n'est plus en mesure de l'attester).
Note de spécification :
N/A
Documentation à fournir :
- Description fonctionnelle du mécanisme - Description du test et résultat de l'exécution du test.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - **que la description fonctionnelle répond bien à l'exigence ;** - **que la description du test met bien en œuvre le mécanisme décrit ;** - **que le résultat du test démontre bien l'efficacité du mécanisme.** **[Evaluation sur site]** **L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie.** **Cette vérification pourra être réalisée sur site.**

ATTS-C3-180 - Désactivation de la génération de trace
L'agent ne doit pas permettre de désactiver la génération des traces.
Note de spécification :
Documentation à fournir :
- Description des mécanismes mis-en-œuvre pour empêcher la désactivation de la génération des traces.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fonctionnelle répond bien à l'exigence.
Exemple d'implémentation satisfaisant l'exigence
Les solutions suivantes satisfont l'exigence : - Absence de fonction de désactivation de la génération - Existence d'une fonction de désactivation de la génération, mais celle-ci est rendue inactive - Existence d'une fonction de désactivation et mise en alerte critique de l'agent en cas de déclenchement de cette dernière.

ATTS-C3-190 - Intégrité des traces générées
L'agent doit mettre en place un mécanisme de protection de l'intégrité des traces pour empêcher leur modification.
Note de spécification :
Un mécanisme de contrôle d'accès est considéré comme suffisant pour remplir cette exigence.
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description du test et résultat de l'exécution du test.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - que la description fonctionnelle répond bien à l'exigence ; - que la description du test met bien en œuvre le mécanisme décrit ; - que le résultat du test démontre bien l'efficacité du mécanisme. [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Les mécanismes suivants répondent à l'exigence : - Contrôle d'accès sur l'espace de stockage ne permettant pas aux utilisateurs sans privilège d'accéder en modification au dossier contenant les traces. - Mécanisme cryptographique de protection de l'intégrité (haché, chaînage, signature électronique). - Gestion des traces uniquement en mémoire vive.

L'ensemble des traces générées par l'agent doit être remonté au service de supervision et de contrôle. Cette remontée doit être réalisée de façon sécurisée.

ATTS-C3-200 - Mécanisme et Sécurisation de la remontée des traces à la supervision
L'Agent doit utiliser un canal sécurisé pour transmettre les traces de synchronisation à la supervision. Ce canal doit être conforme aux exigences communes du paragraphe 10.1.8.
Note de spécification :
La remontée des traces doit être réalisée de façon sécurisée. De plus il est nécessaire que le mécanisme de remontée des traces assure : • Que celles-ci soient remontées dans leur intégralité • Que le format et le protocole de transport soient bien compatibles avec celui du système de supervision et de contrôle.
Documentation à fournir :
Voir paragraphe 10.1.8.
Guide de validation :
Voir paragraphe 10.1.8.

ATTS-C3-210 - Périmètre de remontée des traces à la supervision (traces pertinentes)

L'Agent doit remonter au système de supervision certifié les traces pertinentes de synchronisation dans leur intégralité. Les traces considérées comme pertinentes sont :
- **traces de Synchronisation avec l'élément amont :**
  ○ **identifiant du dispositif de diffusion ;**
  ○ **date et heure de synchronisation avec le dispositif de diffusion ;**
  ○ **valeur d'écart retenu après synchronisation avec le dispositif de diffusion ;**
- **traces de Synchronisation de l'horloge de l'utilisateur final :**
  ○ **identifiant de l'utilisateur final ou origine de la requête ;**
  ○ **date et heure de la synchronisation ;**

Note de spécification :
Une synchronisation peut consister en l'échange de plusieurs jeux de données de synchronisation (réalisation de plusieurs mesures) et le calcul d'une moyenne des valeurs échangées. Seule la valeur retenue doit obligatoirement être remontée. Le détail de l'ensemble des mesures peut optionnellement être remonté.
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie. Cette vérification pourra être réalisée sur site.

ATTS-C3-220 - Périmètre de remontée des traces à la supervision (effacement des traces)
Le mécanisme mis en place doit permettre de s'assurer que les traces de supervision ne sont pas perdues. En particulier, il est attendu que le mécanisme ne permet la destruction éventuelle des traces sur l'agent qu'après que celle-ci ait reçu la confirmation explicite que les traces ont bien été collectées par le système de contrôle et de supervision.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
L'effacement des traces après avoir reçu un accusé de réception de la part de la supervision satisfait cette exigence.

ATTS-C3-230 - Identification de la source des traces
Le protocole de remontée des traces doit permettre d'identifier l'Agent de façon non ambiguë de façon à rattacher les traces à l'agent dans le référentiel du système de supervision.
Note de spécification :
Cette identification peut être faîtes au niveau du protocole ou au niveau des données fournies.
Documentation à fournir :
- Description du mécanisme d'identification de l'agent et référentiel d'identification retenu. - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien - Comment l'agent est identifié. - Si cette identification est bien non ambiguë - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre. En particulier, il s'assurera que les identifiants remontés correspondent bien aux identifiants des échantillons. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Une remontée du numéro d'identifiant unique de l'agent répond à cette exigence.

ATTS-C3-240 - Méthode d'authentification de l'agent
L'agent doit utiliser a minima un mot de passe pour s'authentifier auprès de la supervision. Le mot de passe doit être conforme aux exigences de l'ANSSI.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien lune authentification par mot de passe ou un mécanisme d'une robustesse supérieure. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que l'authentification par certificat décrit est bien mise-en-œuvre. Cette vérification pourra être réalisée sur site.

ATTS-C3-250 - Changement de certificat
Un niveau administrateur sur la machine hôte est requis pour modifier le mot de passe
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre pour changer le mot de passe - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit une procédure de changement de certificat conforme à l'exigence. **[Evaluation sur site]** **L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre.** **Cette vérification pourra être réalisée sur site.**

ATTS-C3-260 - Protocole d'échange
L'agent doit implémenter un protocole supportant TLS pour établir des communications sécurisées avec la supervision.
Note de spécification :
D'autres protocoles peuvent être mis en œuvre, mais TLS doit a minima être supporté.
Documentation à fournir :
- Description des protocoles mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :

[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien le support de TLS. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le protocole est bien supporté. Cette vérification pourra être réalisée sur site.

ATTS-C3-270 - Identification des serveurs de supervision
L'agent ne doit fournir les traces de supervision qu'aux serveurs autorisés dans sa configuration.
Note de spécification :
Documentation à fournir :
- Description du mécanisme permettant de spécifier à l'agent la liste des serveurs autorisés - Description des tests relatifs à l'exigence et résultats de l'exécution des tests Nota : les tests doivent couvrir les cas où la connexion au serveur principal échoue et la connexion à un serveur de secours est mise en œuvre.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien - Comment paramétrer, le cas échéant, les serveurs autorisés. - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le mécanisme est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Un produit où la liste des serveurs est fixée définitivement répond à cette exigence Un produit où la liste des serveurs peut être paramétrée par un administrateur ou en usine satisfait cette exigence.

8.3.4. Exigences relatives à l'administration de l'agent

L'agent doit fournir une interface permettant de réaliser son administration.

ATTS-C3-280 - Présence d'une interface d'administration
L'Agent doit fournir une ou plusieurs interfaces permettant d'administrer le produit.
Note de spécification :
Documentation à fournir :
- Description des interfaces
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit bien les interfaces d'administration et qu'il existe bien une interface d'administration à distance dédiée à la supervision [Evaluation sur site] L'évaluateur se connectera à chacune des interfaces de l'Agent.

ATTS-C3-290 - Rôle Administrateur
Seul le rôle administrateur doit pouvoir permettre de configurer les paramètres suivants : - **Association avec l'élément final du client** - **Configuration des serveurs de supervision (pour le dialogue avec l'Agent)** - **Configuration du mot de passe.**
Note de spécification :
L'administrateur peut réaliser d'autres actions.
Documentation à fournir :
- Description de la liste des actions possibles par le rôle administrateur - Description des tests relatifs à cette exigence et résultat des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que les actions décrites dans l'exigence sont également décrites dans la documentation fournie. L'évaluateur vérifiera qu'un test permet de vérifier que les actions décrites dans cette exigence sont possibles. L'évaluateur vérifiera qu'un test permet de vérifier que ce changement n'est pas accessible depuis le niveau public. [Evaluation sur site] L'évaluateur rejouera les tests. Cette vérification pourra être réalisée sur site.

8.3.5. Gestion des mises à jour

L'agent étant un logiciel, il n'est pas figé au cours du temps. Il peut être mis à jour, de façon à corriger ou faire évoluer le code du produit. La mise à jour est une opération critique qui doit pouvoir être réalisée en toute sécurité.

Afin de corriger dans un délai raisonnable les éventuelles failles de sécurité, l'agent doit pouvoir être mis à jour avec un mécanisme permettant le retour en arrière.

ATTS-C3-300 - Mise à jour de l'agent
L'agent doit pouvoir être mis à jour afin de corriger les éventuelles failles de sécurité. **Le mécanisme mis en œuvre doit assurer que la mise à jour soit protégée en origine et en intégrité.**
Note de spécification :
Documentation à fournir :
- Description du processus de mise à jour.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le processus de mise à jour est bien décrit.
Exemple d'implémentation satisfaisant l'exigence
La désinstallation de l'ancien logiciel et l'installation du nouveau satisfait l'exigence. Concernant la protection en origine et en intégrité, un mécanisme de signature de code ou un téléchargement à travers un canal sécurisé satisfait l'exigence.

ATTS-C3-310 - Annulation de Mise à jour de l'agent
Toute mise à jour logicielle d'un élément de l'agent doit pouvoir être annulée de façon à revenir à la version précédente.
Note de spécification :
Documentation à fournir :
- Description du mécanisme de retour en arrière - Descriptions des tests et résultats des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le processus de retour en arrière est décrit. **L'évaluateur vérifiera qu'un test permet de vérifier que le mécanisme de retour en arrière est effectif.** **[Evaluation sur site] L'évaluateur rejouera les tests. Cette vérification pourra être réalisée sur site.**
Exemple d'implémentation satisfaisant l'exigence
La désinstallation de la nouvelle version et la réinstallation de la version précédente satisfont l'exigence.

L'Agent étant hébergé dans un environnement client, le processus de mise à jour doit prendre en compte ces contraintes.

ATTS-C3-320 - Origine de la mise à jour
La mise à jour de l'agent doit pouvoir être réalisée par l'administrateur de la machine hôte.
Note de spécification :
Les mises à jour automatiques peuvent être mises en place, mais doivent pouvoir être désactivées.
Documentation à fournir :
- Description du mode de mise à jour - Descriptions des tests et résultats des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le mécanisme est décrit. **L'évaluateur vérifiera qu'un test permet de vérifier que le mécanisme est effectif dans chacune des deux options.**

ATTS-C3-330 - Notification de mise à jour disponible
Dans le cas où la mise à jour est à l'initiative du client, les mises à jour disponibles doivent lui être notifiées sur l'Agent.
Note de spécification :
Documentation à fournir :
- Description du mode de notification - Descriptions des tests et résultats des tests.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le mécanisme de notification est décrit. **L'évaluateur vérifiera qu'un test permet de vérifier que l'utilisateur est notifié en cas de disponibilité d'une mise à jour.**

8.3.6. Autres exigences techniques de sécurité

En plus des objectifs principaux de l'agent (voir section 6.1.3.), l'agent doit également répondre aux exigences de sécurité du présent chapitre.

Une mauvaise installation et/ou configuration initiale de l'agent pourrait impacter la sécurité de l'architecture. De ce fait, l'installation de l'agent doit être réalisée de façon sécurisée.

ATTS-C3-340 - Installation et mise en œuvre opérationnelle de l'Agent
L'installation initiale de l'agent doit être mise en œuvre par un administrateur habilité en suivant la procédure d'installation.
Note de spécification :
Documentation à fournir :
- Guide d'installation à l'attention du client

Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que le guide d'installation est fourni et décrit la procédure d'installation

ATTS-C3-350 - Intégrité du code de l'Agent
Le code exécutable de l'agent doit être signé afin de s'assurer de son intégrité lors de l'installation et du démarrage.
Note de spécification :
L'algorithme de signature de code et la taille de clé doivent être à l'état de l'art de la cryptographie.
Documentation à fournir :
- Type de signature mis en œuvre.
Guide de validation :
[Evaluation sur site] L'évaluateur vérifiera que le mécanisme de contrôle d'intégrité est bien en place.
Exemple d'implémentation satisfaisant l'exigence
Par exemple, pour un exécutable sous l'OS Windows, une signature de code reconnu par l'OS satisfait l'exigence.

ATTS-C3-360 - Documentation à destination du client
La documentation de l'agent fournie au client doit contenir *a minima* : - **Un guide d'utilisation** - **Un guide d'installation**
Note de spécification :
Les deux guides peuvent être présentés sous la forme d'un seul document, ou sous la forme de plusieurs documents spécifiques.
Documentation à fournir :
- Guide d'utilisation - Guide d'installation - Description de la façon dont la documentation est remise au client
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que les documents existent pour le modèle évalué et évaluera si la façon de le mettre à disposition du client est appropriée
Exemple d'implémentation satisfaisant l'exigence
La remise au client sous forme papier en le livrant avec le produit satisfait l'exigence La mise à disposition du client par email ou par téléchargement satisfait l'exigence.

ATTS-C3-370 - Documentation des mesures de sécurité et d'environnement à mettre en œuvre
La documentation de l'Agent devra décrire les mesures de sécurité devant être mises en œuvre par l'environnement de l'agent. En particulier, les mesures suivantes doivent être recommandées dans les guides et mise en place sur la machine hôtes d'un Agent : - doter les postes utilisateurs d'un pare-feu local et d'un antivirus ; - mettre en place une gestion des droits maîtrisés ;

- mettre en place une politique de durcissement de l'OS ; - activer et configurer le pare-feu local **De plus, la documentation doit indiquer les conditions nécessaires (droits, rôles) pour que l'agent puisse être en mesure de contrôler les synchronisations de l'élément final du client.**
Note de spécification :
Documentation à fournir :
- Guide d'utilisation - Guide d'installation
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que l'information est présente dans le document et que les conditions sont réunies pour une utilisation au sein de l'architecture.

ATTS-C3-380 - Documentation de la configuration minimale
Il est exigé que la documentation du produit décrive la configuration minimale conseillée.
Note de spécification :
Documentation à fournir :
- Guide d'utilisation - Guide d'installation
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que l'information est présente dans le document et que les conditions sont réalistes pour une utilisation au sein de l'architecture.

8.3.7. Exigences relatives au cycle de vie du produit

ATTS-C3-390 - Protection des environnements de développement et de test et de production de l'Agent de réception du temps de référence : Environnement sécurisé
Les environnements de développement, de test l'Agent doivent faire l'objet de mesures de protection physiques et logiques, en particulier de Contrôle d'accès physique et logiques permettant l'accès aux seules personnes autorisées.
Note de spécification :
Une certification ISO 27001 n'est pas requise, cependant, elle permet de justifier la mise en œuvre des mesures.
Documentation à fournir :
Description des mesures de protection physiques et logiques,
Exemple d'implémentation satisfaisant l'exigence
Une prise en compte des mesures dans le cadre d'une certification ISO 27001 satisfait l'exigence.

ATTS-C3-400 - Gestion de configuration du produit : Identification de la version de l'agent
Chaque version de l'agent doit être clairement identifiée par un identifiant unique.

Note de spécification :
L'identification du modèle d'agent peut être composée d'un numéro de version.
Documentation à fournir :
- Description de la nomenclature des numéros de version - Fourniture du numéro du modèle évalué
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fournie permet d'identifier de façon unique la version de l'agent. **[Evaluation sur site] L'évaluateur vérifiera sur les échantillons fournis que le logiciel correspond bien à la version fournie par le constructeur.**

ATTS-C3-410 - Gestion de configuration du produit : Identification de l'agent
Chaque instance de l'agent doit être identifiée de façon unique.
Note de spécification :
Documentation à fournir :
- Description du mécanisme d'identification.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description du mécanisme permet d'obtenir un identifiant unique par agent. **[Evaluation sur site] L'évaluateur vérifiera par échantillonnage que les identifiants sont uniques et qu'ils sont conformes au mécanisme.**
Exemple d'implémentation satisfaisant l'exigence
Techniquement, cela pourra se faire par une signature du matériel sous-jacent ou par l'utilisation de numéros de licence uniques.

ATTS-C3-420 - Gestion de configuration du produit : Inventaire de configuration
Pour chaque version d'agent, l'ensemble des composants logiciels doivent être clairement identifiés, inventoriés, et tenus à jour. Un historique des changements de cet inventaire doit être conservé. **Une méthode de signature ou de hachage logiciel doit être mise en œuvre pour identifier les versions.**
Note de spécification :
Documentation à fournir :
- Description de la méthode de gestion de configuration utilisée
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fournie permet de satisfaire l'exigence. **[Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que l'historique des changements est conservé.**
Exemple d'implémentation satisfaisant l'exigence
Un Checksum logiciel sur l'ensemble des sources permet de satisfaire l'exigence sur l'identification des versions.

ATTS-C3-430 - Gestion des Failles de sécurité : Veille technique
Le constructeur de l'agent doit effectuer une veille technique sur les vulnérabilités pouvant affecter les composants et doit mettre en œuvre, le cas échéant, des correctifs.
Note de spécification :
Documentation à fournir :
- Description de la procédure de veille technique mise en œuvre.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fournie permet de satisfaire l'exigence. **[Évaluation fonctionnelle] L'évaluateur demandera à voir la liste des vulnérabilités identifiées et les actions correctives réalisées, le cas échéant. Selon le nombre de vulnérabilités, la vérification pourra être réalisée par échantillonnage.**

ATTS-C3-440 - Gestion des Failles de sécurité : Remontée des failles de sécurité
Le constructeur doit mettre en place une procédure documentée permettant au client de remonter des vulnérabilités sur le produit et prendre en compte les éventuelles failles remontées.
Note de spécification :
Documentation à fournir :
- Description de la procédure de remontée des vulnérabilités.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la description fournie permet de satisfaire l'exigence. **[Évaluation fonctionnelle] L'évaluateur demandera à voir la liste des vulnérabilités remontées par les clients, si applicables, et les actions correctives réalisées, le cas échéant. Selon le nombre de vulnérabilités, la vérification pourra être réalisée par échantillonnage.**
Exemple d'implémentation satisfaisant l'exigence
Un suivi à l'aide d'un « bug tracker » type Mantis satisfait l'exigence.

8.3.8. **Tests**

Avant d'être délivré au client, le développeur doit tester les agents.

ATTS-C3-450 - Vérification de la conformité du produit par le constructeur
Le constructeur doit mettre en place une procédure documentée de test permettant de couvrir fonctionnellement l'agent. La suite de test et le processus de test doivent être documentés et un PV, spécifiant la liste des tests exécutés et leur résultat doit être conservé.
Note de spécification :
Documentation à fournir :
- Description de la procédure de test - Description des tests réalisés

- Résultats des tests réalisés
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - **la procédure de test existe et est exécutée à chaque nouvelle version ;** - **les résultats des tests sont conservés.** **[Évaluation fonctionnelle] L'évaluateur demandera à rejouer l'ensemble ou un sous-ensemble des tests (selon le nombre de tests et leur durée d'exécution) et comparera aux résultats fournis et à la description de la procédure fournie.**

9. Module D : Supervision (Système de supervision)

9.1. Système de supervision

Ce chapitre décrit les exigences applicables pour la certification d'un module nommé « Système de Supervision »

Un service de supervision est un ensemble de site, de moyens humains, matériels, logiciels et réseaux, et de procédures permettant de collecter l'ensemble des traces de production, distribution et diffusion du temps et D'analyser les traces collectées pour produire des attestations de synchronisation des dispositifs.

Au niveau de l'architecture, le système de supervision est installé au sein du SI et récupère l'ensemble des informations pertinentes liées à la distribution et diffusion du temps afin d'attester que les éléments du SI du client sont bien synchronisés avec une source UTC avec une exactitude donnée. De ce fait, les exigences qui suivent portent principalement sur:

- Le fonctionnement et les conditions d'opération du service ;
- Le protocole d'échange avec les différents dispositifs déployés ;
- L'analyse des informations remontées ;
- La génération des attestations de synchronisation de temps.

Le rôle du système de supervision est la production d'une attestation de synchronisation de temps à partir des traces remontées par les différents éléments de l'architecture du système, afin d'établir que la traçabilité à UTC était bien garantie pour une exactitude donnée. Le temps produit est fourni à un système de distribution chargé de l'acheminer jusqu'au SI client via un dispositif de diffusion. De ce fait, les principales fonctions attendues d'un service de supervision sont :

- La collecte sécurisée des informations de synchronisation à des fins de supervision et d'attestation de synchronisation de temps fourni ;
- L'analyse des informations de synchronisation afin d'établir la traçabilité à UTC avec une exactitude cible ;
- La production et la fourniture d'attestations de synchronisation de temps.

Un système de supervision de remplir les objectifs suivants :

- Collecter de façon sécurisée les traces de synchronisation et statuts des éléments de l'architecture du système ;
- Analyser de façon fiable les informations de synchronisation, générer les alertes et réagir
- Gérer le parc des éléments de l'architecture du système et leurs statuts ;
- Générer les attestations de synchronisation et de traçabilité de temps ;
- Assurer la sécurité physique, logique, réseau et organisationnelle du service.

9.1.1. Exigences relatives à la collecte sécurisée des traces de synchronisation et statuts des éléments du de l'architecture du système

ATTS-D0-010 - Capacité à collecter les informations de synchronisation
Le système de supervision doit être en mesure de collecter des informations de synchronisation et les alertes locales produites par les éléments suivants : - **Le système de production** - **Les serveurs de l'infrastructure de distribution du temps de référence** - **Les dispositifs matériels de diffusion du temps de référence (Type B, C, et D)** - **Les dispositifs de diffusion du temps de référence de Type A** - **Les Agents de réception du temps de référence**
Note de spécification :
Il est demandé à un système de supervision d'être capable de recueillir les informations de synchronisation avec au moins une chaîne complète de produits et services compatibles entre eux.
Documentation à fournir à l'évaluateur :
- Listes des matériels compatibles avec le service - Description des dispositifs de collecte mis en œuvre - Test de collecte des informations de synchronisation
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie satisfait l'exigence. En particulier, il vérifiera qu'une gamme complète de produits est couverte. [Évaluation fonctionnelle] L'évaluateur demandera, pour chaque type d'élément de l'architecture du système, à constater la collecte effective des informations de connexion.

9.1.2. Dimensionnement

La plate-forme doit être dimensionnée en adéquation avec le volume de transactions.

ATTS-D0-020 - Dimensionnement
Les serveurs doivent être dimensionnés pour supporter la charge de collecte. L'entité opérant la supervision doit mettre en place une architecture dimensionnée en adéquation avec le nombre de transactions prévues.
Note de spécification :
En particulier, le pic d'activité et les variations saisonnières doivent être pris en compte.
Documentation à fournir à l'évaluateur :
- Description de la volumétrie cible ou mesure de volumétrie courante - Description de la volumétrie que la plate-forme est capable de supporter - Test de charge et résultat des tests
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie satisfait l'exigence. En particulier, il vérifiera que la volumétrie que la plate-forme est capable de supporter est bien supérieure à la volumétrie courante.

ATTS-D0-030 - Surveillance et prévision du dimensionnement
L'entité opérant le système de supervision a une obligation de surveillance du dimensionnement et de prévision de volumétrie à venir
Note de spécification :
La surveillance doit prendre en compte les déploiements prévus de nouveaux éléments de l'architecture du système.
Documentation à fournir à l'évaluateur :
- Description des mesures de surveillance mises en place
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie satisfait l'exigence. En particulier, il vérifiera que les mesures permettent bien d'estimer la volumétrie future de la plate-forme. [Évaluation fonctionnelle] L'évaluateur demandera à voir les projections et le plan de déploiement associé.

9.1.3. Sécurisation de la Collecte

ATTS-D0-040 - Sécurisation de la collecte des synchronisations
Lorsqu'il échange avec un élément du réseau de l'architecture du système, le système de supervision doit mettre en œuvre un protocole de communication sécurisé conforme aux exigences communes du paragraphe 10.1.8.
Note de spécification :
Documentation à fournir à l'évaluateur :
Voir exigences communes du paragraphe 10.1.8.
Guide de validation :
Voir exigences communes du paragraphe 10.1.8.

ATTS-D0-050 - Vérification de l'émetteur
Avant d'accepter la collecte d'une trace de synchronisation, le système de supervision doit s'assurer: • **Que l'élément émetteur est bien identifié comme faisant partie de son parc** • **Que l'élément émetteur a bien été authentifié avec succès** **Si l'une de ces vérifications échoue, une alerte doit être levée. Au niveau de la supervision, un mécanisme anti attaque de type force brute doit être mis en en place.**
Note de spécification :
Documentation à fournir à l'évaluateur :
- Description du mécanisme mis en œuvre - Test du mécanisme et résultat des tests.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie satisfait l'exigence. En particulier, il vérifiera que les deux cas d'échec sont bien couverts par les tests. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests pour différents types d'équipements.

9.1.4. Conservation et protection des éléments collectés

Une fois les éléments collectés, le système doit assurer la protection et la conservation des informations de synchronisation collectées.

ATTS-D0-060 - Durée de rétention
Le système de supervision doit conserver les informations de synchronisation ayant permis d'établir une attestation de synchronisation de temps pour une durée de1 an minimale.
Note de spécification :
Documentation à fournir à l'évaluateur :
- Description des dispositifs de garantie de la durée de conservation
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si la durée de conservation est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la conservation effective des informations. La vérification se fera par échantillonnage.

ATTS-D0-070 - Protection des traces collectées
Le système de supervision doit mettre en œuvre des mesures permettant de s'assurer que les traces collectées ne puissent pas être altérées ou détruites sans laisser de traces.
Note de spécification :
Des mesures de droits d'accès appropriés sont jugées suffisantes pour se prémunir d'un effacement des données par une source humaine malveillante.
Documentation à fournir à l'évaluateur :
- Description des mesures mises en place
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si les mesures décrites sont adéquates. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site la bonne implémentation des mesures décrites.

ATTS-D0-080 - Sauvegardes des traces collectées
Les traces collectées doivent faire l'objet de sauvegardes et/ou de réplication
Note de spécification :
Documentation à fournir à l'évaluateur :
- Description des mesures mises en place
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera si les mesures décrites sont adéquates. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site la bonne implémentation des mesures décrites.

9.1.5. Exigences relatives à la gestion du parc des éléments de l'architecture du système et leurs statuts.

ATTS-D0-090 - Inventaire de parc
Le système de supervision doit gérer un inventaire du parc des éléments de l'architecture du système déployés. Seules les personnes et les systèmes autorisés peuvent ajouter, modifier ou supprimer des éléments dans le parc. **Toutes les actions sur le parc doivent être tracées.**
Note de spécification :
Documentation à fournir :
- Description de la gestion du parc.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description satisfait l'exigence [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage : - Que le parc est à jour et reflète le déploiement - Que la traçabilité des actions de modification est effective.

ATTS-D0-100 - Statut du parc
Le système de supervision doit gérer pour chaque élément du parc a minima : - **Un identifiant unique** - **Un niveau de synchronisation cible lorsque cela est applicable** - **Un statut (synchronisé ou non)**
Note de spécification :
Le système peut gérer un plus grand nombre d'états. Cependant, dans ce cas, une table de correspondance avec les états minimaux doit être fournie.
Documentation à fournir :
- Description de la gestion du statut.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description satisfait l'exigence [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage que le statut des éléments du parc est bien géré.

ATTS-D0-110 - Historique des changements de statut des éléments du parc
Le système de supervision doit conserver un historique des changements de statut.
Note de spécification :
Documentation à fournir :
- Description de la mise en œuvre
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description satisfait l'exigence [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage que les changements de statut sont bien historiés.

ATTS-D0-120 - Instance des Agents de réception
Deux instances avec le même numéro d'identification ne doivent pas pouvoir s'exécuter en parallèle sur deux matériels différents à un instant donné. Si la supervision détecte que deux Agents s'exécutent sur deux matériels différents, alors une alerte doit être levée.
Note de spécification :
Une analyse de l'alerte doit être faîte et, le cas échéant, une action correctrice doit être réalisée au niveau du périmètre client.
Documentation à fournir :
- Description de la mise en œuvre
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description satisfait l'exigence [Évaluation fonctionnelle] L'évaluateur demandera à rejouer le test sur site.

9.1.6. **Exigences relatives à l'analyse de traçabilité**

ATTS-D0-130 - Complétude de l'analyse
Le système doit analyser dans leur intégralité les informations pertinentes de synchronisation, événements et les alertes reçues.
Note de spécification :
Documentation à fournir :
- Description de l'algorithme d'analyse
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'algorithme d'analyse prend bien en compte toutes les traces considérées comme pertinentes.

ATTS-D0-140 - Règle d'analyse de la synchronisation

L'algorithme d'analyse doit intégrer les règles suivantes par analyse des traces:
 	
1. Un élément de l'architecture du système est démontré comme à l'heure à un temps t avec une exactitude donnée si :
 	
• **S'il ne présente pas à l'instant *t* d'alerte locale remontée incompatible avec le fait d'être synchronisé**
 	
• **Si l'instant t est compris entre deux synchronisations amont**
  ○ **réalisées avec un élément démontré comme à l'heure dans l'exactitude cible**
  ○ **présentant une mesure d'écart dans l'exactitude cible**
  ○ **réalisée durant la période d'autonomie du dispositif**
 	
2. Une source de l'architecture du système UTC(k) ou Horloge autonome est considérée comme à l'heure.
 	
3. Si un élément de l'architecture du système a remonté un statut d'alerte localement à un instant t, l'élément est considéré, par défaut, comme désynchronisé dans la période entre la dernière synchronisation avec succès précédent l'alerte et la première synchronisation après retour à l'état normal du dispositif.
 	
NOTA : la période peut être réduite s'il peut être déterminé avec certitude que l'élément était à l'heure entre la dernière synchronisation et l'occurrence de l'alerte. Tous ces cas devront alors être clairement identifiés et justifiés.
 	
4. Si la dernière synchronisation d'un élément a été réalisée avec un élément qui n'était pas à l'heure, alors son état est considéré comme non à l'heure jusqu'à la prochaine synchronisation réussie avec un élément à l'heure.
 	
5. Si la dernière synchronisation d'un élément a été réalisée avec écart supérieur à l'exactitude cible, alors son état est considéré comme non à l'heure depuis la synchronisation précédente.
 	
6. Si l'espace entre deux synchronisations dépasse la durée d'autonomie du produit, le produit est considéré comme désynchronisé a minima à partir du dépassement de la durée d'autonomie.

Note de spécification :
L'algorithme pourra avoir des optimisations, mais il sera demandé de démontrer le respect à ces six règles.
Documentation à fournir :
- Description de l'algorithme - Test de l'algorithme
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'algorithme d'analyse prend bien en compte toutes les règles ci-dessus et que les tests couvrent bien l'ensemble des règles. Cette analyse demande des compétences en évaluation logicielle [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests. L'évaluateur vérifiera également par échantillonnage que les règles sont bien appliquées.

ATTS-D0-150 - Seconde intercalaire
- **L'analyse doit prendre en compte la seconde intercalaire.**
Note de spécification :
Documentation à fournir :
- Description de la procédure mise en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la manière dont est gérée la seconde intercalaire est précisée dans la documentation

9.1.7. Gestion des états d'alerte et de la continuité d'activité

Le système de supervision ne doit pas simplement surveiller l'état du système, mais également, en fonction des alertes reçues et/ou des dysfonctionnements constatés de mettre en œuvre des réponses permettant d'assurer la continuité du service. En particulier, il est attendu du système de supervision :

- D'orchestrer les demandes de synchronisation des différents éléments
- D'envoyer des messages opérationnels à l'attention des éléments de l'architecture à l'exception des systèmes de production.

9.1.8. Gestion des demandes de synchronisation

C'est le rôle de la supervision de gérer les demandes de synchronisation et de les autoriser.

ATTS-D0-160 - Réception des demandes de synchronisation
Le système de supervision doit être en mesure de recevoir des demandes de synchronisation des éléments de l'architecture du système de fin de chaîne (Dispositifs matériels de distribution et de diffusion du temps et Agents de diffusion). **Le système demandeur doit être identifié dans la demande.**
Note de spécification :
Documentation à fournir :
- Documentation de l'interface des demandes de synchronisation. - Test de l'interface de demande.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera qu'une telle interface existe. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests.

ATTS-D0-170 - Traitement des demandes de synchronisation
Le système de supervision doit être en mesure de traiter les demandes de synchronisation en déterminant, à partir du statut de synchronisation des éléments du parc, un élément amont auquel se synchroniser. **La réponse doit indiquer a minima :** - **s'il est autorisé ou non à se synchroniser ;** - **le cas échéant, un identifiant d'un dispositif avec lequel l'élément doit de synchroniser ;**
Note de spécification :
Documentation à fournir :
- Documentation de l'algorithme de traitement de la demande - Test de l'algorithme.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation satisfait l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests.

ATTS-D0-180 - Sécurisation des demandes de synchronisation
Afin de sécuriser le canal de communication supportant les échanges concernant les demandes de synchronisation, le système de supervision doit mettre en œuvre un protocole de communication sécurisé conforme aux exigences communes.
Note de spécification :
Documentation à fournir à l'évaluateur :
Voir exigences communes.
Guide de validation :
Voir exigences communes.

9.1.9. Actions et Mises en alerte des éléments du réseau

ATTS-D0-190 - Action sur les éléments du réseau de l'architecture du système
Le service de supervision doit être en mesure d'envoyer ou de mettre à disposition d'un élément de l'architecture du système a minima les informations interprétables ou ordres suivants: - **Indication sur l'élément amont sur lequel se synchroniser** - **Autorisation de synchronisation** - **Arrêt/ démarrage de la distribution** - **Une mise à jour est disponible**
Note de spécification :
Documentation à fournir :
- Documentation de l'interface - Description des tests et résultats associés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation satisfait l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests.

ATTS-D0-200 - Information d'état
Le système de supervision doit être en mesure d'indiquer à un élément de la chaîne l'architecture du système son statut de synchronisation et s'il doit continuer à diffuser le temps
Note de spécification :
Documentation à fournir :
- Documentation de l'interface - Description des tests et résultats associés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation satisfait l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à rejouer les tests.

9.1.10. Production des attestations

ATTS-D0-210 - Contenu de l'attestation de synchronisation de temps

Les attestations de synchronisation de temps doivent fournir de façon non ambiguë:
- **L'identifiant et les caractéristiques de l'élément qui est synchronisé (identifiant unique, type de matériel, etc.).**
- **L'émetteur de l'attestation et son numéro de certification. L'émetteur de l'attestation doit être identifié par :**
  - **Le nom du service.**
  - **Le nom légal de l'entité opérant le service**
  - **Un numéro d'identifiant unique de l'entité.**
- **Le nom du client à qui est destinée l'attestation et un numéro d'identifiant unique du client.**
- **La précision/exactitude cible de la synchronisation.**
- **La précision/exactitude par rapport à UTC sur la période et le taux de synchronisation dans la précision cible.**
- **La source de temps utilisée et son écart maximal par rapport à UTC sur la période.**
- **La période pour laquelle elle s'applique (date de début et de fin).**
- **Les périodes pour lesquelles:**
  - **L'élément est attesté synchronisé**
  - **L'élément est non synchronisé.**
L'attestation devra également préciser toutes réserves éventuelles.

Note de spécification :
Ces éléments sont applicables à tous les formats cibles.
Documentation à fournir :
- Description du format d'attestation et du contenu - Exemples d'attestation
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation satisfait l'exigence. [Évaluation fonctionnelle] L'évaluateur demandera à obtenir des échantillons d'attestations.
Exemple d'implémentation satisfaisant l'exigence
En France, le numéro de SIRET peut être utilisé comme identifiant unique de l'émetteur.

ATTS-D0-220 - Lisibilité
Les attestations devront a minima être lisibles par un être humain. Il est possible également de les mettre en plus à disposition sous forme de fichier ou de service à destination d'une machine.
Note de spécification :
Documentation à fournir :
- Exemples d'attestations
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les attestations sont lisibles. [Évaluation fonctionnelle] L'évaluateur vérifiera par échantillonnage la lisibilité.

ATTS-D0-230 - Format
Les attestations devront a minima être fournies au format PDF
Note de spécification :
Documentation à fournir :
- Description des formats cible supportés. - Exemples d'attestations
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le format PDF est supporté. [Évaluation fonctionnelle] L'évaluateur vérifiera par échantillonnage les formats.

ATTS-D0-240 - Disponibilité
Les conditions générales du service devront décrire sous quelles conditions (à la demande …) les attestations pourront être obtenues (personnes pouvant les obtenir, délai d'obtention, mode d'obtention et de remise). Les attestations doivent a minima pouvoir être obtenues durant toute la durée de souscription du contrat : - **Par le souscripteur** - **Par les autorités compétentes dans le cadre d'une enquête judiciaire** **A minima :** - **La demande doit pouvoir être faîte par voie électronique ou papier** - **Une attestation doit pouvoir être obtenue a minima 10 jours après la fin de la période visée par l'attestation.** - **L'attestation doit pouvoir être générée sous 5 jours ouvrés suite à une demande.**
Note de spécification :
Documentation à fournir :
- Conditions générales - Description de l'architecture de production des attestations mises en place
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les conditions générales respectent l'exigence. L'évaluateur vérifiera que l'architecture en place est en adéquation avec les engagements des conditions générales. [Évaluation fonctionnelle] L'évaluateur réalisera par échantillonnage des demandes d'attestations et vérifiera que les exigences des conditions générales sont remplies.

ATTS-D0-250 - Garantie d'intégrité et d'origine
Le service de supervision doit garantir l'origine et l'intégrité de l'attestation fournie. La documentation du service doit préciser le mode de garantie et comment cette vérification peut être réalisée.
Note de spécification :
Documentation à fournir :
- Documentation du mécanisme mis en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera le mécanisme mis en œuvre. [Évaluation fonctionnelle] L'évaluateur réalisera par échantillonnage des demandes d'attestations et vérifiera que les exigences des conditions générales sont remplies.
Exemple d'implémentation satisfaisant l'exigence
Une signature ou un sceau électronique au sens du Règlement européen eIDAS permet de remplir cette exigence avec les types de signatures suivantes : - Signature ou sceau avancé à l'aide d'un certificat qualifié - Signature ou sceau qualifié. La fourniture de l'attestation au destinataire à travers un canal sécurisé protégé par un certificat d'authentification SSL qualifié eIDAS permet également de garantir cette exigence.

ATTS-D0-260 - Prise en compte de l'écart entre UTC et UTC(k) sur la période.
Le service de supervision doit prendre en compte l'écart entre UTC et UTC(k) sur la période.
Note de spécification :
Il est possible, en attente d'une publication de l'écart entre UTC et UTC(k) de produire des attestations temporaires sous réserve de l'écart entre UTC et UTC(k).
Documentation à fournir :
- Documentation du mécanisme mis en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera le mécanisme mis en œuvre. [Évaluation fonctionnelle] L'évaluateur réalisera par échantillonnage des demandes d'attestations et vérifiera le cas échéant que l'exigence est remplie.

9.1.11. Exigences relatives à la sécurité physique

ATTS-D0-270 - Exigences communes
Les sites d'exploitation du système de supervision doivent respecter les exigences relatives à la sécurité physique du paragraphe 10.1.1.
Note de spécification :
Documentation à fournir :
Voir paragraphe 10.1.1.
Guide de validation :
Voir paragraphe 10.1.1.

9.1.12. Exigences relatives aux ressources humaines

ATTS-D0-280 - Exigences communes
Les sites d'exploitation du système de supervision doivent respecter les exigences communes relatives aux ressources humaines du paragraphe 10.1.2.
Note de spécification :
Documentation à fournir :
- Voir paragraphe 10.1.2.
Guide de validation :
- Voir paragraphe 10.1.2.

9.1.13. Exigences relatives à la sécurité logique

ATTS-D0-290 - Exigences communes
Les sites d'exploitation du système de supervision doivent respecter les exigences communes relatives à la sécurité logique du paragraphe 10.1.3.
Note de spécification :
Documentation à fournir :
- Voir du paragraphe 10.1.3.
Guide de validation :
- Voir du paragraphe 10.1.3.

9.1.14. Protection des matériels réseaux

ATTS-D0-300 - Protection des échanges réseau
Des mesures de protection des flux réseau doivent être mises en œuvre afin d'assurer la confidentialité et l'intégrité des données qui y transitent.
Note de spécification :
Certains flux peuvent ne pas nécessiter de mettre en place des mesures de protection, mais cela doit être justifié (par exemple : échange de données non sensibles, protection physique du matériel, besoin de performance …). Le cas échéant, des mesures de sécurité adéquate (protection physique) doivent être mises en place.
Documentation à fournir :
- Schéma des flux identifiant les flux sécurisés et non sécurisés - Description de la mesure de sécurisation mise en œuvre - Justification des flux non sécurisés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, éventuellement par échantillonnage, que la mise en œuvre est conforme à la description fournie.
Exemple d'implémentation satisfaisant l'exigence
La mise en place de certificats SSL ou de VPN permet de répondre à cette exigence.

9.1.15. Exigences relatives à la journalisation des événements

ATTS-D0-310 - Journalisation des événements
Les sites d'exploitation du système de supervision doivent respecter les exigences communes relatives à la journalisation des événements du paragraphe 10.1.4. -
Note de spécification :
Documentation à fournir :
- Voir du paragraphe 10.1.4.
Guide de validation :
- Voir du paragraphe 10.1.4.

ATTS-D0-320 - Champs obligatoires d'un enregistrement
Chaque enregistrement d'un événement dans un journal doit contenir au minimum les champs suivants : - **type de l'événement ;** - **nom de l'exécutant ou référence du système déclenchant l'événement ;** - **date et heure de l'événement** - **résultant de l'événement (échec ou réussite).**
Note de spécification :
Documentation à fournir :
- liste des journaux d'événements - exemple de chaque type de journal
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les exemples de journaux sont complets et conformes à l'exigence. En cas d'impossibilité de fournir l'ensemble des journaux, cette vérification pourra être réalisée sur site. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que les journaux générés sont conformes aux exemples fournis.

9.1.16. Exigences relatives à la continuité d'activité

ATTS-D0-330 - Continuité d'activité
Les sites d'exploitation du système de supervision doivent respecter les exigences communes relatives à la continuité d'activité du paragraphe 0.
Note de spécification :
-
Documentation à fournir :
- Voir du paragraphe 0.
Guide de validation :
- Voir du paragraphe 0.

Ils doivent par ailleurs respecter les exigences spécifiques à la supervision suivantes :

ATTS-D0-340 - Disponibilité
Le système de supervision doit mettre en place une architecture de haute disponibilité. L'architecture doit être mise en place de façon à atteindre un niveau de disponibilité de 99,9% de chacune des fonctions critiques.
Note de spécification :
Les fonctions critiques comportent a minima : - La gestion des actions de synchronisation - La collecte des traces de synchronisation à la supervision
Documentation à fournir :
- Description de l'architecture de haute disponibilité mise en place.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'architecture décrite est adéquate. [Évaluation fonctionnelle] L'évaluateur vérifiera, éventuellement par échantillonnage, l'architecture décrite est bien mise en place.
Exemple d'implémentation satisfaisant l'exigence
Une architecture où chaque élément est redondé de façon active satisfait l'exigence. À ce titre, la solution peut s'appuyer, pour la partie datacenter, sur une certification Tier pour établir la démonstration. Une implémentation de niveau Tier 3 (circuits en redondance et disponibilité élevée) permet d'avoir un niveau satisfaisant l'exigence.

10. Exigences communes aux systèmes de l'architecture

La présente annexe définit un ensemble d'exigences de sécurité communes à certains éléments de l'architecture du système. Les différents modules du référentiel font appel à cette annexe.

10.1. Exigences communes

10.1.1. Exigences relatives à la sécurité physique

ATTS-EC-010 - Contrôle d'accès aux locaux
Afin d'éviter tous pertes, dommages et compromissions des ressources du système et l'interruption des services, les accès aux locaux des différents composants du service doivent être contrôlés.
Note de spécification :
Documentation à fournir :
- Description du mécanisme de contrôle d'accès - Liste des profils autorisés à accéder aux locaux.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit le mécanisme de contrôle d'accès et que la liste des profils est à jour. [Évaluation fonctionnelle] L'évaluateur vérifiera que le dispositif de contrôle décrit est bien appliqué.

ATTS-EC-020 - Accompagnement des visiteurs
Toute personne entrant dans une zone physiquement sécurisée ne doit pas être laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.
Note de spécification :
Documentation à fournir :
- Politique de contrôle d'accès.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie décrit la procédure d'accompagnement des personnels externes.

ATTS-EC-030 - Liste nominative des accès
L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux.
Note de spécification :
Documentation à fournir :
- Liste des personnes autorisées - Historique des accès.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera sur l'historique des accès que seules les personnes autorisées ont bien accès aux locaux.

ATTS-EC-040 - Accès physique aux machines
Afin d'assurer la disponibilité des systèmes, l'accès aux machines doit être limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.
Note de spécification :
Documentation à fournir :
- Liste des personnes autorisées - Fiche de poste/position des personnes ayant accès.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les postes des personnes ayant accès sont cohérents avec le besoin d'accéder aux machines.

ATTS-EC-050 - Revue de la liste nominative des accès
Une revue des accès physique doit être réalisée de manière périodique
Note de spécification :
Documentation à fournir :
- Compte-rendu des revues des accès.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la revue a bien été effectuée.

ATTS-EC-060 - Traçabilité des accès
La traçabilité des accès physiques doit être assurée
Note de spécification :
Documentation à fournir :
- Historique des accès physiques ou SLA confirmant que le prestataire trace les accès.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les accès physiques sont bien enregistrés. [Évaluation fonctionnelle] L'évaluateur demandera à accéder au site et vérifiera, après la visite, que les traces ont bien été générées.

ATTS-EC-070 - Détection d'intrusion
La sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique en particulier en dehors des heures ouvrables.
Note de spécification :
Documentation à fournir :
- Documentation des moyens de détection d'intrusion mis en œuvre

- Liste des alertes générées.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que des moyens sont bien décrits et sont adaptés. [Évaluation fonctionnelle] L'évaluateur vérifiera que les moyens décrits sont mis en œuvre et que les alertes générées sont bien traitées.

ATTS-EC-080 - Alimentation électrique et climatisation
Les caractéristiques des équipements d'alimentation électrique et de climatisation doivent permettre de respecter les conditions d'usage des équipements du service telles que fixées par leurs fournisseurs
Note de spécification :
Documentation à fournir :
- Description des conditions d'usage - Description de mise en œuvre des équipements
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie est bien conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera, par échantillonnage, que les équipements sont bien exploités dans des conditions décrites.

ATTS-EC-090 - Vulnérabilité aux dégâts des eaux
Les moyens de protection contre les dégâts des eaux doivent permettre de respecter les exigences de disponibilité du service.
Note de spécification :
Documentation à fournir :
- Description des moyens mis en œuvre
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie est bien conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site, la bonne implémentation des mesures décrites.

ATTS-EC-100 - Prévention et protection incendie
Les moyens de protection contre les incendies doivent permettre de respecter les exigences de disponibilité du service.
Note de spécification :
Documentation à fournir :
- Description des moyens mis en œuvre
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la documentation fournie est bien conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site, la bonne implémentation des mesures décrites.

ATTS-EC-110 - Inventaire des composants
Les composants critiques doivent être identifiés et inventoriés.
Note de spécification :
Les différents modules définissent la liste des composants considérés comme critiques.
Documentation à fournir :
- Listes des composants critiques
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la liste existe. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site, par échantillonnage, que la liste est à jour.

ATTS-EC-120 - Manipulation des composants
Les composants critiques doivent être gérés selon des procédures conformes à leurs besoins de sécurité. En particulier, ils doivent être manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés et les opérations doivent être tracées.
Note de spécification :
Les différents modules précisent l'interprétation de cette exigence dans un contexte précis.
Documentation à fournir :
- Procédure de gestion des éléments critiques
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que pour les différents types d'éléments critiques, des procédures d'exploitation existent. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site, par échantillonnage, le bon respect des procédures déclarées.

ATTS-EC-130 - Nécessité de sauvegarde
Chaque composante du service doit mettre en œuvre des sauvegardes de leurs applications et de leurs informations.
Note de spécification :
Documentation à fournir :
- Politique de sauvegarde
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la politique de sauvegarde est documentée et qu'elle couvre l'ensemble des éléments critiques. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site, par échantillonnage, que les sauvegardes sont réalisées et documentées.

ATTS-EC-140 - Export des sauvegardes hors site
En complément de sauvegardes sur sites, chaque composante du service doit mettre en œuvre des sauvegardes hors site.
Note de spécification :

Documentation à fournir :
- Politique de sauvegarde
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la politique de sauvegarde indique les mesures d'export des sauvegardes hors site. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site, par échantillonnage, que les sauvegardes sont bien exportées

ATTS-EC-150 - Disponibilité des sauvegardes
Ces sauvegardes doivent être organisées de façon à assurer une reprise des fonctions après incident le plus rapidement possible, et conformes aux exigences de disponibilité
Note de spécification :
Documentation à fournir :
- Politique de sauvegarde
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les conditions de disponibilité décrites dans la politique de sauvegarde sont conformes avec une reprise rapide sur incident. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site, par échantillonnage, que les sauvegardes sont bien disponibles.

ATTS-EC-160 - Intégrité des sauvegardes
Les sauvegardes doivent être testées régulièrement pour s'assurer de leur intégrité.
Note de spécification :
- Politique de sauvegarde - Traces des tests d'intégrité réalisés
Documentation à fournir :
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les conditions de disponibilité décrites dans la politique de sauvegarde sont conformes avec une reprise rapide sur incident. [Évaluation fonctionnelle] L'évaluateur vérifiera sur site, par échantillonnage, que les sauvegardes sont bien disponibles.

10.1.2. Exigences relatives aux ressources humaines

ATTS-EC-170 - Définition de rôle de confiance
L'organisation opérant le service doit distinguer les rôles de confiance. **Ces rôles doivent être décrits et définis dans la description des postes propre à chaque entité opérant une des composantes du système de distribution**
Note de spécification :
Les modules du présent référentiel des différents systèmes précisent les différents rôles de confiance.
Documentation à fournir :
- Description des rôles de confiance - Liste des personnes en rôle de confiance
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera : - qu'une liste descriptive des rôles de confiance est disponible ; - que la liste nominative des personnes en rôle de confiance est disponible.

ATTS-EC-180 - Séparation des rôles
Pour l'attribution des rôles, les principes de séparation des responsabilités et du moindre privilège doivent être appliqués. Par exemple, la personne effectuant une tâche ne peut pas être en charge de son contrôle.
Note de spécification :
Documentation à fournir :
- Description des rôles de confiance - Liste des personnes en rôle de confiance
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera qu'il ne constate pas d'attributions de rôle en contradiction avec l'exigence.

ATTS-EC-190 - Confidentialité
Tous les personnels amenés à travailler au sein de composantes du service doivent être soumis à une clause de confidentialité vis-à-vis de leur employeur.
Note de spécification :
Documentation à fournir :
- Clause de confidentialité signée
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera par échantillonnage que les rôles de confiance ont bien signé une clause de confidentialité.
Exemple d'implémentation satisfaisant l'exigence
Une clause présente dans les contrats ou un formulaire spécifique signé satisfont l'exigence.

ATTS-EC-200 - Nomination à un rôle de confiance
L'entité en charge du service doit informer toute personne intervenant dans des rôles de confiance : - **de ses responsabilités relatives aux services fournis,** - **des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.**
Note de spécification :
Documentation à fournir :
- Procédure d'information
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera qu'une procédure est en place pour informer les personnes en rôle de confiance. [Évaluation fonctionnelle] L'évaluateur interrogera une personne en rôle de confiance pour s'assurer qu'elle a été informée de ces responsabilités et des procédures à appliquer.

ATTS-EC-210 - Procédures de vérification des antécédents
Chaque entité opérant une composante d'un système de l'architecture doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. À ce titre, l'employeur peut demander à ces personnels la communication d'une copie du bulletin n°3 de leur casier judiciaire. **Ces vérifications doivent être menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).**
Note de spécification :
Documentation à fournir :
- Description des contrôles réalisés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les contrôles réalisés sont conformes à l'exigence. Cette vérification pourra se faire par échantillonnage.

ATTS-EC-220 - Formation initiale
Le personnel doit être préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.
Note de spécification :
Documentation à fournir :
- procédure et matériel de formation du personnel ; - preuve que les personnels ont bien été formés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les personnels ont bien été formés.
Exemple d'implémentation satisfaisant l'exigence
Les éléments suivants peuvent valoir comme preuve de formation :

- L'émargement à une session de formation - La participation active à la mise en place du projet (par exemple, la participation au développement d'un logiciel)

ATTS-EC-230 - Formation continue
Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.
Note de spécification :
Il s'agit d'évolutions majeures impactant les pratiques des personnels
Documentation à fournir :
- procédure et matériel de formation du personnel ; - preuve que les personnels ont bien été formés.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera par échantillonnage que les personnels ont bien été formés.
Exemple d'implémentation satisfaisant l'exigence

ATTS-EC-240 - Personnel extérieur
Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'infrastructure doit également respecter les exigences du présent chapitre. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.
Note de spécification :
Documentation à fournir :
- Clauses des contrats de sous-traitance
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que les clauses sont bien présentes dans les contrats de sous-traitance.

10.1.3. Exigences relatives à la sécurité logique

ATTS-EC-250 - Présence d'antivirus
Lorsque cela est applicable, des mesures de protection contre les virus et codes malveillants doivent être mises en œuvre.
Note de spécification :
Les outils et les librairies (par exemple, librairie de l'antivirus) doivent être à jour.
Documentation à fournir :
- Description des mesures mises en place.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que des mesures sont décrites. [Évaluation fonctionnelle] L'évaluateur vérifiera que les mesures décrites sont mises en place

ATTS-EC-260 - Protection contre les mises à jour non autorisées
Lorsque cela est applicable, des mesures de protection contre les mises à jour non autorisées doivent être en œuvre.
Note de spécification :
En particulier, seules les personnes autorisées doivent pouvoir mettre à jour les logiciels et librairie sur le SI.
Documentation à fournir :
- Description des mesures mises en place.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que des mesures sont décrites. [Évaluation fonctionnelle] L'évaluateur vérifiera que les mesures décrites sont mises en place

ATTS-EC-270 - Interconnexion Réseau
L'interconnexion entre réseaux doit être contrôlée et doit être, lorsque cela est nécessaire, protégée par des systèmes de sécurité configurés pour n'accepter que les protocoles nécessaires au fonctionnement du système opérant le service.
Note de spécification :
Des exigences complémentaires sont fournies dans les cahiers d'exigences spécifiques à chaque service.
Documentation à fournir :
Un diagramme réseau devra être fourni. La configuration des systèmes de sécurité doit être tenue à la disposition de l'évaluateur.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que des mesures sont décrites. [Évaluation fonctionnelle] L'évaluateur vérifiera que les mesures décrites sont mises en place

ATTS-EC-280 - Audit de la configuration des systèmes de sécurité
La configuration des systèmes de sécurité doit être périodiquement auditée.
Note de spécification :
L'audit de configuration doit être réalisé a minima une fois par an et après toute modification importante du réseau.
Documentation à fournir :
Le rapport du dernier audit.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'audit de configuration a été réalisé

ATTS-EC-290 - Traçabilité des actions sur les serveurs et composants réseau
Une traçabilité des actions réalisées sur les serveurs et les composants réseau doit être mise en œuvre
Note de spécification :
Documentation à fournir :

Historique des opérations
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que l'historique des opérations peut bien être consulté.

ATTS-EC-300 - Protection des échanges réseau
Des mesures de protection des flux réseau doivent être mises en œuvre afin d'assurer la confidentialité et l'intégrité des données qui y transitent.
Note de spécification :
Certains flux peuvent ne pas nécessiter de mettre en place des mesures de protection, mais cela doit être justifié (par exemple : échange de données non sensibles, protection physique du matériel …)
Documentation à fournir :
Matrice des flux et mesures mises en place
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la matrice des flux est documentée et qu'elle identifie les flux sécurisés. L'évaluateur vérifiera pour chaque flux non sécurisé qu'une justification est donnée.
Exemple d'implémentation satisfaisant l'exigence
La mise en place de certificats SSL ou de VPN permet de répondre à cette exigence.

ATTS-EC-310 - Surveillance et prévision
L'entité opérant le système de distribution a une obligation de surveillance du dimensionnement et de prévision de volumétrie à venir
Note de spécification :
Documentation à fournir :
- Mesure de surveillance du dimensionnement - Plan de montée en charge.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera l'existence d'une procédure de surveillance de la volumétrie et d'un plan de charge. [Évaluation documentaire] L'évaluateur vérifiera la mise en place effective de mesure de volumétrie.

ATTS-EC-320 - Authentification forte
Une authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) doit être mise en œuvre.
Note de spécification :
Documentation à fournir :
- Description du mécanisme d'authentification forte mis en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le mécanisme d'authentification décrit est conforme à l'exigence. [Évaluation documentaire] L'évaluateur vérifiera la mise en place effective des mesures décrites.

ATTS-EC-330 - Gestion des droits
Une gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) doit être mise en œuvre.
Note de spécification :
Documentation à fournir :
- Description de la politique de gestion des droits mis en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.

ATTS-EC-340 - Déconnexion des sessions
Une politique d'expiration de session doit être mise en œuvre afin que les sessions utilisateur se déconnectent automatiquement après un certain temps d'inactivité.
Note de spécification :
Documentation à fournir :
- Description de la politique de gestion des droits mis en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.

ATTS-EC-350 - Gestion des droits
Une gestion des comptes des utilisateurs doit être mise en œuvre.
Note de spécification :
En particulier, la modification et la suppression rapide des droits d'accès après un départ ou une réaffectation doivent être mises en œuvre.
Documentation à fournir :
- Description de la politique de gestion des droits mis en œuvre.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.

10.1.4. Exigences relatives à la journalisation des événements

ATTS-EC-360 - Événements à journaliser de façon automatique
Concernant les systèmes liés aux fonctions mises en œuvre dans le cadre de l'architecture du système, chaque entité opérant une composante du système de distribution doit au minimum journaliser les événements tels que décrits ci-dessous, sous forme électronique. La journalisation doit être automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système : - création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ; - démarrage et arrêt des systèmes informatiques et des applications ; - connexion / déconnexion des utilisateurs, en particulier des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.
Note de spécification :
Documentation à fournir :
- Description de la politique de journalisation.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.

ATTS-EC-370 - Autres événements à journaliser
Les événements suivants doivent également être journalisés, éventuellement de façon manuelle: - les accès physiques ; - les actions de maintenance et de changements de la configuration des systèmes ; - les changements apportés au personnel ;
Note de spécification :
Documentation à fournir :
- Description de la politique de journalisation.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.

ATTS-EC-380 - Champs obligatoires d'un enregistrement
Chaque enregistrement d'un événement dans un journal doit contenir au minimum les champs suivants : - type de l'événement ; - nom de l'exécutant ou référence du système déclenchant l'événement ; - date et heure de l'événement - résultant de l'événement (échec ou réussite).
Note de spécification :
Documentation à fournir :
- Description de la politique de journalisation.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.

ATTS-EC-390 - Délai de journalisation
Les opérations de journalisation doivent être effectuées au cours du processus. En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'événement.
Note de spécification :
Documentation à fournir :
- Description de la politique de journalisation.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.
Exemple d'implémentation satisfaisant l'exigence

ATTS-EC-400 - Archivage des journaux
Les journaux d'événements doivent être conservés sur site pendant au moins un (1) mois. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous dix (10) minutes après leur génération.
Note de spécification :
Documentation à fournir :
- Description de la politique de journalisation.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.

ATTS-EC-410 - Externalisation des journaux
Les journaux exportés doivent faire l'objet de sauvegarde pour assurer leur disponibilité.
Note de spécification :
Documentation à fournir :
- Description de la politique de journalisation.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.

ATTS-EC-420 - Protection des journaux
La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'événements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'événements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).
Note de spécification :
Documentation à fournir :
- Description de la politique de journalisation.
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que la description est conforme à l'exigence. [Évaluation fonctionnelle] L'évaluateur vérifiera la mise en place effective des mesures décrites.

10.1.5. Exigences relatives à la continuité d'activité

ATTS-EC-430 - Disponibilité
Le système opérant le service doit mettre en place une architecture de haute disponibilité pour ces fonctions critiques.
Note de spécification :
Les fonctions critiques et le taux de disponibilité minimale cible sont précisés dans chaque modules de chacun des systèmes.
Documentation à fournir :
- Taux de disponibilité cible
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera que le taux de disponibilité cible est décrit

ATTS-EC-440 - PCA/PRA
Chaque composante du service doit disposer d'un plan de continuité d'activité (PCA) permettant de répondre aux exigences de disponibilité des différentes fonctions fournies. **Un plan de reprise d'activité (PRA) doit également être mis en place en cas de sinistre majeur et doit préciser la durée estimée pour la reprise d'activité.**
Note de spécification :
Documentation à fournir :
- PCA/PRA
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera l'existence d'un PCA/PRA

ATTS-EC-450 - Test du PCA/PRA
Le PCA/PRA doit être testé dans son intégralité au moins une fois sur une durée de 2 ans. Un test partiel doit être réalisé chaque année.
Note de spécification :
Documentation à fournir :
- Rapport de test du PCA/PRA
Guide de validation :
[Évaluation documentaire] L'évaluateur vérifiera l'existence d'un rapport de test du PCA/PRA. Si le test n'est pas satisfaisant, l'évaluateur vérifiera : - qu'un plan d'action correctif a été mis en œuvre - qu'un nouveau test a été planifié.

10.1.6. Exigences relatives à la surveillance et à la gestion des alertes

ATTS-EC-460 - Gestion des alertes
Le service doit mettre en place une surveillance des éléments techniques mis en œuvre.
Note de spécification :
Les exigences spécifiques au sein des modules précisent les éléments techniques particuliers devant être surveillés.
Documentation à fournir :
- Documentation du système de surveillance mis en œuvre
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera qu'un mécanisme de surveillance est en place. [Évaluation fonctionnelle] l'évaluateur - vérifiera que le mécanisme est bien implémenté et est conforme à sa description ; - demandera à consulter la liste des alertes générées. Il s'attachera à vérifier : o par échantillonnage, que les alertes ont fait l'objet d'un traitement ; o que le nombre d'alertes généré est en adéquation avec le dimensionnement de l'équipe en charge de son traitement.

ATTS-EC-470 - Mécanisme de détection des vulnérabilités
Des mécanismes de détection de vulnérabilités (IDS, analyse automatique de journaux d'événements) doivent être mis en place.
Note de spécification :
Documentation à fournir :
- Description du mécanisme mis en œuvre.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera qu'un mécanisme de surveillance est en place. [Évaluation fonctionnelle] l'évaluateur - vérifiera que le mécanisme est bien implémenté et est conforme à sa description ; - demandera à consulter la liste des alertes générées. Il s'attachera à vérifier : o par échantillonnage, que les alertes ont fait l'objet d'un traitement ; - vérifiera que le nombre d'alertes généré est en adéquation avec le dimensionnement de l'équipe en charge de son traitement.

ATTS-EC-480 - Mise en place de procédures de remontée des incidents
Chaque entité opérant une composante du service doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers des sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.
Note de spécification :
Documentation à fournir :
- Description des procédures mises en place.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera qu'une organisation est en place et si celle-ci semble pertinente. [Évaluation fonctionnelle] L'évaluateur vérifiera que la procédure de remontée d'incident est connue des personnels. Cette vérification se fera lors d'une entrevue et par échantillonnage. L'évaluateur demandera à consulter la liste des incidents remontés par les personnels et vérifiera par échantillonnage qu'un traitement a été réalisé.

ATTS-EC-490 - Seconde intercalaire
Le système doit mettre en place une procédure afin - **de surveiller les secondes intercalaires à venir** - **de réaliser les opérations nécessaires pour que les serveurs soient en mesure de prendre en compte la seconde intercalaire et ne pas la considérer comme une anomalie.**
Note de spécification :
Une procédure manuelle de vérification régulière du bulletin C de l'IERS satisfait l'exigence
Documentation à fournir :
- Description de la procédure mise en œuvre.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : La manière dont est gérée la seconde intercalaire est précisée dans la procédure. [Évaluation fonctionnelle] L'évaluateur vérifiera : - qu'une surveillance de la seconde intercalaire est bien mise en œuvre ; - par échantillonnage, que la procédure d'intervention sur les serveurs a bien été réalisée sur les secondes intercalaires ayant eu lieu.

10.1.7. Exigences relatives à la génération des traces par un système de l'architecture du système

Un système appartenant à l'architecture doit être en mesure de générer un certain nombre de traces d'audit.

ATTS-EC-500 - Liste minimale des traces devant être générées
Le système/produit appartenant à l'architecture doit pouvoir générer un enregistrement des événements suivants : **a) démarrage et arrêt** **b) les connexions et actions des administrateurs de sécurité** **c) changement dans la configuration** **d) mises à jour**
Note de spécification :
La documentation fonctionnelle et technique du produit devra lister les types d'événements et décrire les formats des traces.
Documentation à fournir :
- Exemple de traces générées par le produit, couvrant l'ensemble des événements de cette exigence - Spécification fonctionnelle décrivant le format des traces - Description des tests et résultats des tests correspondant à l'exigence.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - Que la spécification fonctionnelle décrit bien le contenu des traces. - Que l'exemple généré est bien conforme à la description de la spécification fonctionnelle - Que les tests couvrent bien l'ensemble des traces décrites dans l'exigence. [Evaluation sur site] - L'évaluateur rejouera les tests. - L'évaluateur récupérera des traces et s'assurera qu'elles sont conformes à la description et aux exemples fournis.

ATTS-EC-510 - Identité de l'utilisateur ou du sous-composant qui est à l'origine d'un événement
Le système / produit doit pouvoir associer chaque événement pouvant être audité avec l'identité de l'utilisateur ou du sous-composant qui est à l'origine de l'événement
Note de spécification :
Documentation à fournir :
- Description fonctionnelle de la manière dont l'exigence est mise-en-œuvre - Un exemple de trace par sous-composant
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - Que la spécification du fonctionnement décrit bien comment chaque trace est associée à chaque sous-composant. - Que les exemples fournis sont bien conformes à la description de la spécification du fonctionnement [Evaluation sur site] - L'évaluateur récupérera pour chaque type de sous-composant de la Box le fichier de trace et s'assurera que o les traces sont bien produites ; o les traces peuvent bien être liées de façon non ambiguë avec le composant. Cette vérification pourra être réalisée sur site.

ATTS-EC-520 - Informations devant être enregistrées pour chaque événement
Le produit doit enregistrer au minimum les informations suivantes dans chaque enregistrement d'audit : - **date et heure de l'événement ;** - **type d'événement ;l'identité de l'utilisateur ou du sous-composantle résultat (succès ou échec) de l'événement.**
Note de spécification :
La structure des traces est libre et les traces peuvent contenir des éléments complémentaires. L'identité du sujet peut apparaître sur chaque événement ou être attachée à un ensemble d'éléments.
Documentation à fournir :
- Exemple de traces générées par le produit, couvrant l'ensemble des événements - Spécification fonctionnelle décrivant le format des traces - Description des tests et résultats des tests correspondant à l'exigence.
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - Que la spécification fonctionnelle décrit bien le contenu de l'événement et que l'ensemble des éléments de l'exigence sont présents. - Que l'exemple généré est bien conforme à la description de la spécification fonctionnelle - Que les tests couvrent bien l'ensemble l'exigence. [Evaluation sur site] - L'évaluateur rejouera les tests. - L'évaluateur récupérera des traces et d'assurera qu'elles sont conformes à la description et aux exemples fournis.

10.1.8. Exigences relatives à la remontée des traces de synchronisation au système de supervision et de contrôle.

Il est nécessaire que le mécanisme de remontée des traces assure :

- Que celles-ci soient remontées dans leur intégralité
- Que le format et le protocole de transport soient bien compatibles avec celui du système de supervision et de contrôle.

ATTS-EC-530 - Périmètre de remontée des traces à la supervision
Le produit doit remonter au système de supervision certifié les traces pertinentes de synchronisation dans leur intégralité. Le mécanisme mis en place doit permettre de s'assurer que les traces de supervision ne sont pas perdues.
Note de spécification :
Chaque module précise le type de trace à remonter.
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que : - Que la description fonctionnelle répond bien à l'exigence - Que la description du test met bien en œuvre le mécanisme décrit - Que le résultat du test démontre bien l'efficacité du mécanisme [Evaluation sur site] L'évaluateur rejouera le test et s'assurera que le résultat est cohérent avec la documentation fournie. Cette vérification est préférablement réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
L'effacement des traces après avoir reçu un accusé de réception de la part de la supervision satisfait cette exigence.

ATTS-EC-540 - Protocole de remontée des traces à la supervision
Le système de supervision de l'architecture doit remonter les traces dans un protocole supporté par le système de supervision et de contrôle. La documentation doit préciser le protocole utilisé et sa version et/ou les mécanismes de supervision compatibles.
Note de spécification :
Le mécanisme de remontée est libre, mais doit être documenté.
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien le protocole utilisé. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.

ATTS-EC-550 - Authentification du serveur de supervision
Le système/produit doit avoir authentifié avec succès le serveur de supervision avant tout échange de données.
Note de spécification :
Le mécanisme d'authentification mis en œuvre est libre, mais : - il doit être documenté ; - il doit être conforme à l'état de l'art et aux recommandations des organismes nationaux en charge de la sécurité de l'information.
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien le protocole utilisé et évaluera la pertinence du jeu de test fourni. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Une authentification du serveur par certificat SSL satisfait l'exigence.

ATTS-EC-560 - Authentification du produit
Le produit doit s'authentifier avec succès au serveur de supervision avant tout échange de données.
Note de spécification :
Le mécanisme d'authentification mis en œuvre est libre, mais : - il doit être documenté ; - il doit être conforme à l'état de l'art et aux recommandations des organismes nationaux en charge de la sécurité de l'information
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien le moyen d'authentification mis en œuvre. [Evaluation sur site] L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre. Cette vérification pourra être réalisée sur site.
Exemple d'implémentation satisfaisant l'exigence
Une authentification du serveur par certificat SSL satisfait l'exigence. Une authentification par couple identifiant/mot de passe satisfait cette exigence.

ATTS-EC-570 - Intégrité des données échangées
Le protocole de communication entre le système et la supervision doit assurer l'intégrité des données échangées.
Note de spécification :
Le mécanisme de vérification d'intégrité mis en œuvre est libre, mais : - il doit être documenté ; - il doit être conforme à l'état de l'art et aux recommandations des organismes nationaux en charge de la sécurité de l'information.
Documentation à fournir :
- Description du mécanisme mis en œuvre - Description des tests relatifs à l'exigence et résultats de l'exécution des tests
Guide de validation :
[Evaluation documentaire] L'évaluateur vérifiera que la documentation décrit bien le moyen de protection en intégrité mis en œuvre. **[Evaluation sur site]** **L'évaluateur rejouera le test afin de s'assurer que le protocole décrit est bien mis-en-œuvre.** **Cette vérification pourra être réalisée sur site.**
Exemple d'implémentation satisfaisant l'exigence
Une communication SSL satisfait l'exigence.

11. Règles de certification et modalités d'évaluation

11.1. Réalisation d'une offre et commande client

Après une première prise d'informations et d'échanges, le service commercial du LNE fait parvenir un questionnaire au demandeur de la certification qui doit être retourné rempli afin de pouvoir établir le devis. Le service commercial fait alors parvenir l'offre de certification au demandeur. Une fois la commande enregistrée, le processus de certification peut démarrer.

Chaque module du présent référentiel (A1, A2, B, C1, C2, C3 ou D) fait l'objet d'une certification à part entière par un demandeur spécifique. Ces certifications seront alors utilisées par le demandeur de la certification de l'architecture du système sous réserve de respect des exigences applicables.

11.2. Processus de certification

Le processus de certification se découpe en plusieurs étapes successives.

11.2.1. Certification des modules

1. L'instruction du dossier de demande : l'examen de recevabilité documentaire
2. Réalisation de l'évaluation de certification par module comportant :
   - l'évaluation de la conformité documentaire
   - l'évaluation de la conformité fonctionnelle si applicable selon l'exigence considérée
3. (Retour sur les fiches de non-conformité)
4. Proposition de décision de certification par un comité de lecture
5. Emission du certificat, le cas échéant

11.2.2. Certification de l'architecture du système

Processus identique à la certification d'un module décrit ci-dessus, uniquement réalisable à l'issue de la certification des modules.

11.2.3. Revue annuelle de la certification

A date anniversaire de la certification de l'architecture du système, l'entité responsable transmet au LNE une synthèse sur le fonctionnement de l'architecture et une revue est planifiée.

11.2.4. Description des étapes du processus

1. Examen de recevabilité documentaire

Une fois la prise de commande enregistrée, le demandeur envoie au LNE l'ensemble des documents applicables suivant le module considéré. Les documents attendus sont mentionnés dans la partie **« Documentation à fournir »** de chacune des exigences applicables.

Cette documentation doit être complète et décrire précisément l'ensemble des fonctionnalités et mécanismes mis en œuvre dans le cadre de la mise en conformité, permettant de répondre aux exigences du référentiel.

L'examen de recevabilité documentaire consiste donc à déterminer si l'évaluation de la conformité du module en question est possible, compte tenu du degré d'aboutissement du dossier technique transmis par le demandeur. Pour ce faire, il est constaté si des documents demandés sont manquants et si le principe des méthodes proposées pour répondre aux exigences est pertinent.

A l'issue de l'examen de recevabilité documentaire, le LNE informe le demandeur du résultat.

Dans le cas où cette étape conclut à l'irrecevabilité du dossier, il appartient au demandeur de la certification de répondre au LNE, en fournissant les documents manquants. Un devis complémentaire sera adressé par le service commercial du LNE, si un second examen de recevabilité documentaire est nécessaire.

2. Planification de l'évaluation de certification

Dans le cas où l'examen de recevabilité documentaire est satisfaisant, le dossier est recevable et le LNE prend contact avec le demandeur, afin de définir les dates de l'évaluation documentaire puis de l'Évaluation fonctionnelle si applicable.

La durée des évaluations (documentaire et site) est liée à sa complexité ; elle est fixée lors de la réalisation de l'offre de certification.

3. Evaluation documentaire

L'évaluation documentaire d'un module a pour objectif de vérifier le respect des dispositions documentaires définies dans chacune des exigences.

L'évaluation de certaines exigences requiert des compétences spécifiques en

- Métrologie et métrologie du temps
- Sécurité des systèmes d'information et cybersécurité
- Réseaux informatiques
- Evaluation logicielle
- Système de management de la qualité

4. Evaluation fonctionnelle

Elle complète l'évaluation documentaire, n'est pas applicable pour chaque exigence, et permet de s'assurer que les mesure proposées sont bien appliquées. Dans la majeure partie des cas, elle est réalisée sur les sites de l'architecture.

Les évaluations, une fois finalisées donnent lieu à un rapport d'évaluation concluant à la conformité ou à la non-conformité du module évalué.

5. Cas de non-conformités

Dans le cas où une non-conformité est constatée lors des évaluations, celle-ci est mentionnée et décrite dans le rapport d'évaluation. Toute non-conformité doit être corrigée avant la certification.

Après analyse des actions et corrections proposées par le demandeur de la certification, le le dossier de certification est présenté en comité de lecture pour avis.

6. Comité de lecture et décision

Le comité de lecture est chargé de rendre un avis sur la décision de certification dans le processus d'attribution, de surveillance, de retrait ou de suspension des certificats. Il est composé au minimum :

- d'un représentant de la direction du LNE (qui ne peut intervenir en tant que chef de projet certification et n'ayant pas participé à l'évaluation),
- d'un chef de projet certification n'étant pas en charge du dossier,
- d'un chef de projet certification en charge de présenter le dossier.

Le comité est présidé par le représentant de la direction du LNE.

Ce comité de lecture a pour mission :

- d'examiner les rapports d'évaluation et de formuler un avis et une recommandation sur les décisions à prendre,
- le cas échéant, d'examiner dans un premier temps les appels contre les décisions du LNE et de formuler un avis sur les suites à donner,
- d'évaluer la qualité des rapports d'évaluation.

La décision de certification s'appuie sur l'examen des éléments du dossier et du rapport d'évaluation de certification. Chaque décision de certification est matérialisée par l'enregistrement et le cas échéant l'émission d'un certificat.

Les certificats sont émis sans date limite de validité et restent valides tant qu'aucune modification majeure portant sur les caractéristiques certifiées n'est apportée. Il appartient au détenteur du certificat de signaler au LNE les modifications apportées au dispositif certifié, afin de faire réaliser les évaluations nécessaires à la révision du certificat.

7. Surveillance du certificat

Il est procédé à une évaluation de surveillance annuelle de la certification de l'architecture du système. Le contenu de l'évaluation annuelle varie suivant les modifications réalisées lors des douze derniers mois. Sa durée ne peut être inférieure à deux jours, avec a minima une journée d'évaluation documentaire et une journée d'évaluation fonctionnelle au sein de l'entité responsable.

11.3. Recours et traitement des plaintes

11.3.1. Recours contre décision

Le titulaire de la certification peut contester la décision prise par courrier avec accusé réception.

Dans un premier temps, le LNE procède au réexamen du dossier au vu des éléments factuels motivant le recours. Il notifie le maintien ou la nouvelle décision au demandeur dans un délai de 15 jours ouvrés à réception du recours.

Dans le cas où le demandeur désire maintenir son recours contre décision, il le notifie au LNE par lettre recommandée avec accusé réception dans un délai de 15 jours ouvrés. Ce recours, non suspensif de la décision du LNE, doit être motivé. Il est instruit par le LNE dans les 21 jours ouvrés suivant sa réception et donne lieu, lorsqu'il concerne la décision de certification, à examen par le comité de lecture. Le LNE informe l'auteur du recours, du maintien ou non de sa décision.

En cas de maintien du recours après instruction et soumission au comité de marque pour avis, le recours est présenté au Comité de Certification et de Préservation de l'Impartialité du LNE, qui après examen, propose ses conclusions. La décision finale est notifiée par le LNE à L'Entreprise.

11.3.2. Traitement des plaintes

Toute plainte concernant des produits fait l'objet d'un examen par le LNE afin de confirmer si la plainte concerne effectivement des produits certifiés. L'entité formulant une plainte doit étayer celle-ci en fournissant des preuves factuelles.

A réception de celles-ci, le LNE les examine et le cas échéant contacte l'entreprise concernée.

L'Entreprise concernée doit alors informer le LNE des suites apportées et tenir à disposition du LNE, les enregistrements relatifs à la plainte ainsi qu'aux actions entreprises pour la résoudre. La vérification de la mise en place des actions annoncées peut faire l'objet d'examens supplémentaires à la charge de l'Entreprise.

Dans le cadre du suivi de l'Entreprise, le LNE examine les enregistrements relatifs aux plaintes et réclamations et vérifie que les corrections et actions correctives appropriées ont été entreprises.

12. Glossaire

Terme	Définition
Agent de réception du temps de référence	Dispositif logiciel optionnel, permettant d'obtenir une traçabilité du temps jusqu'à l'horloge locale du client (dispositif final recevant le temps exact, tracé et sécurisé qui sera attesté)
Dispositif de diffusion	Dispositif permettant de diffuser le temps dans le périmètre client. Il peut s'agir : - D'un dispositif matériel installé dans le périmètre client ; - D'un service, on parle alors de dispositif de diffusion du temps de référence de type A.
Elément final du client	Interface/Elément du client final à synchroniser.
Horloge GTS	Système de production du temps avec exactitude et stabilité données
Seconde intercalaire	Une seconde intercalaire est un ajustement occasionnel d'une seconde du temps universel coordonné (UTC) lié au temps atomique international (TAI) pour que le temps universel coordonné demeure proche du temps solaire moyen donné par le temps universel lié à la rotation de la Terre et donc lentement variable.
Système de calcul via GNSS	Un système de calcul est un ensemble de site(s), de moyens humains, matériels, logiciels et réseaux, et de procédures permettant à la fois de collecter l'ensemble des traces remontées par les éléments de l'architecture du système disposant de modules de calcul via GNSS et également d'analyser les traces collectées pour produire une traçabilité.
Système de distribution du temps	Service en charge de la distribution du temps aux dispositifs de diffusion. Ce service s'appuie sur un réseau de serveurs en charge d'apporter le temps au plus près des clients.
Système de production du temps	Service en charge de la production du temps et de sa mise à disposition au système de distribution
Système de supervision	Service permettant : - De contrôler la distribution et la diffusion du temps - De collecter les traces de distribution et de diffusion afin de reconstituer a posteriori la traçabilité.
UTC	Temps atomique international (TAI) auquel est ajouté ou soustrait un nombre entier de secondes de manière à ce que UTC soit maintenu à moins de 0,9 s du temps universel (UT1) *« Le SI et la métrologie en France, éditions EDP Sciences, 2019 »*
UTC(k)	Prédiction en temps réel du temps UTC ou la réalisation physique locale réalisée dans un pays « k » *« Le SI et la métrologie en France, éditions EDP Sciences, 2019 »*
UTC(OP)	UTC(k) pour la France : Observatoire de Paris (Décret n° 2017-292 du 6 mars 2017 relatif au temps légal français)