

Serveur de sécurité UXP 1.25

Guide de l'Auditeur de transactions

UXP-UG-SSAUDIT

Table des matières

1. Introduction	1
1.1. Serveur de sécurité UXP	1
1.2. Concepts UXP	2
1.3. Références	6
2. Gérer mon compte	7
2.1. Affichage de mes rôles	7
2.2. Changer de mot de passe	7
2.3. Réinitialiser un mot de passe oublié	7
2.4. Tentatives de connexion et verrouillage	7
3. Messages	8
3.1. Rechercher des messages	8
3.1.1. Recherche de base	8
3.1.2. Recherche avancée	9
3.2. Vérifier la signature du message	10
3.2.1. États du message	10
3.2.2. Détails du message et résultat de la vérification	11
3.3. Télécharger un conteneur de signatures	13
3.4. Télécharger des certificats	13

1. Introduction

Ce guide s'adresse aux Auditeurs de transactions, qui sont chargés de vérifier les signatures des messages échangés par un serveur de sécurité sur la plate-forme d'échange unifiée (Unified eXchange Platform, UXP).

Ce guide explique comment :

- rechercher et visualiser les messages échangés avec succès par le serveur de sécurité ;
- vérifier les signatures des messages ;
- télécharger des conteneurs de signatures ;
- télécharger les certificats liés aux signatures.

Le serveur de sécurité ne stocke que les signatures des messages qu'il a traités avec succès. Par conséquent, la page Messages du serveur de sécurité ne permet pas d'obtenir une vue d'ensemble de tous les messages reçus par le serveur. Pour surveiller tous les messages qui arrivent au serveur (y compris les messages qui échouent en raison d'une erreur), il faut mettre en place la collecte des données de surveillance opérationnelle du serveur (voir [\[UXP-UG-PMA\]](#)).



L'Auditeur de transactions peut consulter les messages de tous les membres ou de certains d'entre eux, en fonction des privilèges qui lui ont été attribués. Vous pouvez vérifier vos privilèges dans **Mon compte**.

Ce guide n'explique pas comment faire fonctionner le Serveur de sécurité UXP, et il suppose que l'opération est déléguée à quelqu'un d'autre (un opérateur UXP). Adressez-vous à votre opérateur UXP pour obtenir de l'aide concernant :

- la gestion des utilisateurs ;
- la santé du serveur ;
- les journaux du système.

1.1. Serveur de sécurité UXP

La fonction principale d'un serveur de sécurité est de traiter les demandes de manière à préserver leur valeur probante.

Le serveur de sécurité est connecté à l'Internet public d'un côté et au système d'information au sein du réseau interne de l'organisation de l'autre côté. Dans un certain sens, le serveur de sécurité peut être considéré comme un pare-feu spécialisé au niveau de l'application, capable de servir d'intermédiaire entre les services Web SOAP et RESTful. Il doit donc être configuré en parallèle avec le pare-feu de l'organisation, qui sert d'intermédiaire pour les autres protocoles.

Le serveur de sécurité est doté de la fonctionnalité nécessaire pour sécuriser l'échange de

messages entre un client et un fournisseur de services.

- Les messages transmis sur l'Internet public sont sécurisés par des signatures numériques et le cryptage.
- Le serveur de sécurité du fournisseur de services applique un contrôle d'accès aux messages entrants, garantissant ainsi que seuls les utilisateurs ayant signé un accord approprié avec le fournisseur de services peuvent accéder aux données.

1.2. Concepts UXP

Instance UXP est une installation unique de l'infrastructure UXP.

Autorité de gouvernance UXP est une organisation chargée de la maintenance de l'instance UXP.

Membre UXP désigne toute personne physique ou morale ayant adhéré à UXP afin de fournir ou de consommer des services, ou les deux.

Sous-système représente une partie du système d'information d'un membre UXP. Les membres UXP doivent déclarer certaines parties de leurs systèmes d'information comme sous-systèmes afin d'utiliser ou de fournir des services UXP.

Les sous-systèmes sont autonomes en termes de fourniture et d'utilisation des services UXP.

- Les droits d'accès des sous-systèmes des membres UXP sont indépendants — les droits d'accès accordés à un sous-système n'ont aucune incidence sur les droits d'accès des autres sous-systèmes du membre.
- Les services fournis par un sous-système sont indépendants des services fournis par les autres sous-systèmes du membre.

Un membre UXP peut associer plusieurs sous-systèmes différents à un serveur de sécurité, et un sous-système peut être associé à plusieurs serveurs de sécurité.

Identifiant membre est l'identifiant unique d'un membre UXP. L'identifiant UXP du membre se compose de trois parties : un identifiant d'instance, une classe de membre et un code de membre. Un exemple d'identifiant de membre est EE/GOV/12345678.

Identifiant d'instance est un code unique attribué à une instance UXP. Par exemple, le code pour l'instance de développement estonienne est EE-DEV et le code pour l'instance de production est EE.

Classe de membre regroupe les membres UXP ayant des propriétés similaires sous une unité commune. Par exemple, les agences publiques sont regroupées sous la classe de membre GOV, les organisations privées sont regroupées sous la classe de membre COM.

Code membre est associé à un certain membre UXP et est unique au sein de la classe de membre. Le code membre reste inchangé pendant toute la durée de vie du membre UXP. Par exemple, le code membre pour les organisations et les agences gouvernementales en Estonie est le code du registre du commerce.

Code du sous-système est ajouté à l'identifiant du membre afin de distinguer les sous-systèmes individuels des membres.

Serveur de registre est un composant UXP exploité par l'autorité de gouvernance qui sert de registre des informations nécessaires au fonctionnement de l'instance UXP. Le serveur de registre UXP distribue ces informations aux serveurs de sécurité sous la forme d'une configuration globale.

Serveur de sécurité est un composant UXP qui connecte les sous-systèmes d'un membre UXP à l'infrastructure UXP.

Propriétaire du serveur de sécurité est un membre UXP légalement responsable d'un serveur de sécurité particulier.

Client du serveur de sécurité est un sous-système enregistré sur un serveur de sécurité. L'enregistrement doit être confirmé par l'Autorité de gouvernance et approuvé sur le serveur de registre.

Mutualisation est un modèle de fonctionnement du serveur de sécurité qui permet à plusieurs membres UXP de partager un seul serveur de sécurité tout en maintenant l'isolation des données et une gestion indépendante. Dans ce modèle, chaque membre opère dans son propre environnement logique, avec son propre ensemble d'utilisateurs, de rôles et de clés cryptographiques, ce qui garantit que les membres ne peuvent pas accéder aux informations des autres.

Configuration globale est un fichier qui contient les informations nécessaires au fonctionnement des serveurs de sécurité. Les serveurs de sécurité téléchargent régulièrement la configuration globale à partir du serveur de registre. Exemples d'informations dans la configuration globale :

- liste des membres UXP et de leurs sous-systèmes ;
- serveurs de sécurité enregistrés ;
- clients de serveurs de sécurité enregistrés ;
- certificat d'authentification enregistrés ;
- groupes globaux ;
- paramètres du système UXP ;
- adresses et clés publiques des services OCSP (si elles ne sont pas déjà disponibles via l'extension Authority Information Access des certificats) ;
- adresses et clés publiques des fournisseurs de services de certification agréés ;
- clés publiques des autorités de certification intermédiaires ;
- adresses et les clés publiques des prestataires de services d'horodatage agréés.

Groupe global est un groupe de droits d'accès géré au niveau du serveur de registre. Tous les sous-systèmes du groupe global disposent des droits d'accès attribués au groupe.

Groupe local est un groupe de droits d'accès géré au niveau du client du serveur de sécurité.

Autorité d'horodatage (TSA) est un fournisseur de services qui émet des horodatages.

Services d'horodatage sont des services fournis par la TSA afin de préserver la valeur probante des messages échangés via UXP.

Horodatage est une date et une heure accompagnées d'une signature délivrée par la TSA

pour prouver qu'un message a existé à un moment précis.

Autorité de certification (CA) est un fournisseur de services de certification qui émet des certificats numériques.

Services de certification sont des services fournis par CA aux membres UXP, offrant des certificats numériques qui vérifient la propriété d'une clé publique.

OCSP signifie Online Certificate Status Protocol (protocole d'état des certificats en ligne). Les répondeurs OCSP sont des serveurs exploités par l'autorité de certification afin de permettre la vérification de la validité des certificats.

Clés UXP sont des clés cryptographiques utilisées au sein de l'UXP. UXP utilise des paires de clés publiques et privées.

Une clé UXP est soit :

- une **clé de signature** — utilisée par les serveurs de sécurité pour signer numériquement les messages échangés, ou
- une **clé d'authentification** — utilisée par les serveurs de sécurité pour établir des canaux de communication sécurisés.

Certificats UXP sont des certificats délivrés par un fournisseur de services de certification agréé par l'autorité de gouvernance UXP.

Dispositif de création de signature est un mécanisme externe au serveur de sécurité permettant de protéger les clés cryptographiques que le serveur de sécurité utilise pour signer les messages. Les modules de sécurité matériels (HSM) et les jetons USB sont des exemples de dispositifs de création de signature.

Jeton est un espace de stockage destiné à protéger les clés cryptographiques utilisées par le serveur de sécurité. Le serveur de sécurité dispose de deux types de jetons :

- **jeton logiciel** — jeton logiciel intégré au serveur de sécurité,
- **jeton matériel** — jeton situé sur un dispositif de création de signature.

Services UXP sont des services fournis via l'infrastructure UXP.

Message UXP est un échange de données unidirectionnel entre un client et un fournisseur de services au sein de l'instance UXP. Selon son origine, un message peut être soit une demande, soit une réponse. Les messages UXP doivent être formés selon le protocole de message UXP ([\[UXP-PR-MESS\]](#)) et sont créés par les systèmes d'information des membres UXP.

Client du service est le sous-système d'un membre UXP qui a envoyé le message de demande.

Fournisseur de services est le sous-système du membre UXP qui a envoyé le message de réponse au client du service en réponse au message de demande.

Conteneur de signature est un fichier qui contient le message UXP signé, la signature numérique, l'horodatage et les certificats associés.

Transaction est la combinaison d'un message de demande et du message de réponse correspondant.

- **Identifiant de transaction** est un identifiant de transaction que le serveur de sécurité du client du service attribue lors du traitement d'un message de demande provenant du

système d'information. L'identifiant de transaction est généré automatiquement par le serveur de sécurité afin de contenir une valeur unique pour chaque message transmis par le serveur de sécurité.

L'identifiant de transaction est également enregistré dans le journal des messages et peut être utilisé pour identifier de manière unique les messages UXP.

Demande est un message de demande, les demandes sont initiées par le client du service.

- **Identifiant de demande** est un identifiant de transaction qui fait partie de l'en-tête du message (`id` dans les en-têtes SOAP ([\[UXP-PR-MESS\]](#)) et `Uxp-Queryid` dans les en-têtes HTTP). L'identifiant de demande est attribué par le système d'information du client du service.

En-têtes UXP ou en-têtes de message sont des en-têtes spécifiques utilisés pour inclure des méta-informations spécifiques UXP dans les messages UXP.

- Pour les services SOAP, voir les en-têtes dans [\[UXP-PR-MESS\]](#).
- Pour les services REST, les en-têtes UXP sont :
 - `Uxp-Client`
 - `Uxp-Service`
 - `Uxp-Queryid`
 - `Uxp-Transaction-Id`
 - `Uxp-Userid`
 - `Uxp-Consent-Ref`
 - `Uxp-Issue`

Instance UXP

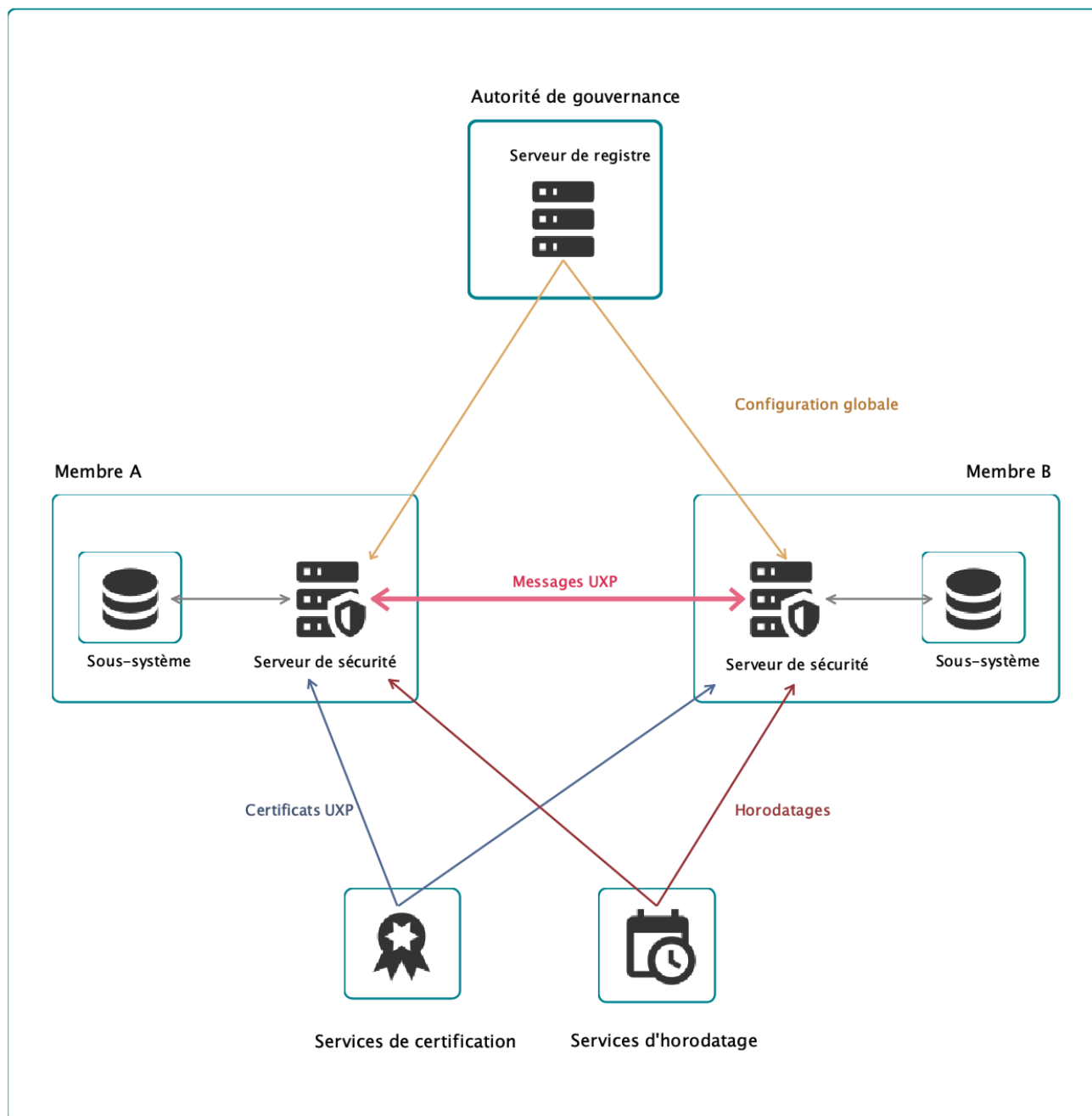


Figure 1. Schéma illustrant les composants d'une instance UXP

1.3. Références

- [\[UXP-PR-MESS\]](#) Cybernetica AS. UXP: Protocole de message v4.0. Identifiant du document : UXP-PR-MESS
- [\[UXP-UG-PMA\]](#) Cybernetica AS. Serveur de sécurité UXP : Configurer la surveillance du serveur de sécurité. Identifiant du document : UXP-UG-PMA

2. Gérer mon compte

2.1. Affichage de mes rôles

Pour voir quels rôles votre compte possède, procédez comme suit :

1. Survolez votre nom d'utilisateur dans le coin supérieur droit.
2. Cliquez sur **Mon compte**. Vous pouvez voir quels sont vos rôles.

Si vous ne voyez pas les rôles dont vous avez besoin, contactez votre administrateur.

2.2. Changer de mot de passe

Pour changer votre mot de passe, procédez comme suit :

1. Survolez votre nom d'utilisateur dans le coin supérieur droit.
2. Cliquez sur **Changer le mot de passe**.



Si vous ne voyez pas d'option pour changer votre mot de passe dans le menu, cette fonction n'est pas disponible pour votre type de compte. Veuillez contacter votre administrateur pour changer votre mot de passe.

3. Saisissez l'ancien et le nouveau mot de passe et cliquez sur **Changer le mot de passe**.

Après avoir changé votre mot de passe, vous serez déconnecté et devrez vous connecter à nouveau.

2.3. Réinitialiser un mot de passe oublié

Si vous avez oublié votre mot de passe, contactez votre administrateur et demandez-lui de réinitialiser votre mot de passe.

2.4. Tentatives de connexion et verrouillage

Pour limiter les attaques par force brute lors de la connexion, le compte d'un utilisateur sera temporairement verrouillé après un trop grand nombre d'essais infructueux. Si vous êtes sûr que votre mot de passe est correct mais que vous n'arrivez toujours pas à vous connecter, il se peut que votre compte soit temporairement bloqué en raison d'un trop grand nombre de tentatives infructueuses. Veuillez attendre 10 à 15 minutes et réessayer. Si vous ne parvenez toujours pas à vous connecter, veuillez contacter votre administrateur pour réinitialiser votre mot de passe.

3. Messages

Message UXP est un échange de données unidirectionnel entre un client et un fournisseur de services au sein de l'instance UXP. Selon son origine, un message peut être soit une demande, soit une réponse. Chaque message UXP est signé numériquement par l'expéditeur.

Le message de demande et le message de réponse forment ensemble une **transaction**. Une transaction implique deux participants :

- Le **Client du service** est le sous-système d'un membre UXP qui a envoyé le message de demande.
- Le **Fournisseur de services** est le sous-système du membre UXP qui a envoyé le message de réponse au client du service en réponse au message de demande.

Le **Conteneur de signature** est le fichier qui contient le message UXP signé, la signature numérique, l'horodatage et les certificats associés.

3.1. Rechercher des messages

Droits d'accès : Auditeur de transactions

Pour rechercher des messages, utilisez la **Recherche de base** ou la **Recherche avancée**. La **Recherche de base** permet une recherche plus rapide, tandis que la **Recherche avancée** offre des options plus fines.

Pour rechercher un message, procédez comme suit dans la page **Messages** :

1. Ouvrez la **Recherche de base** ou la **Recherche avancée**.
2. Remplissez les champs appropriés.
3. Cliquez sur **Rechercher**.
Le filtre affiche les messages qui correspondent aux critères de recherche.

Pour effacer le filtre actuel, cliquez sur **Effacer le filtre**.

Pour actualiser la liste des messages, cliquez sur **Rechercher** ou sur le bouton d'actualisation.



Les messages ne sont pas mis à jour en temps réel. Si vous attendez la mise à jour d'un message, **actualisez-le régulièrement**.

3.1.1. Recherche de base

La **Recherche de base** permet d'effectuer une recherche à l'aide des champs suivants :

- Champs du client :
 - Nom ;

- Sous-système ;



La recherche à partir du nom d'un client nécessite que ce dernier soit enregistré sur l'instance UXP. Si un client est absent ou retiré de l'instance UXP, ou si les informations sur les membres de l'instance UXP ne sont pas disponibles, utilisez la **Recherche avancée** pour saisir l'identifiant du client.

- Champs du service :

- Code ;
- Version ;

- Période :

- De ;
- À ;



La période et les délais de traitement sont indiqués dans le fuseau horaire de l'utilisateur.



Les champs **De** et **À** peuvent être spécifiés indépendamment l'un de l'autre. La spécification de l'heure nécessite également la spécification de la date.



Lors d'une recherche par dates (sans spécifier l'heure), le champ **De** définit l'heure du début de la journée 00:00:00 en heure locale, et le champ **À** définit l'heure de la fin de la journée 23:59:59 en heure locale.

- Type de message :

- Demande ;
- Réponse.

3.1.2. Recherche avancée

La **Recherche avancée** permet d'effectuer des recherches à l'aide des champs suivants :

- Identifiant de transaction ;
- Identifiant de demande ;
- Identifiant de l'utilisateur ;
- Champs du client :
 - Instance ;
 - Classe ;
 - Code ;
 - Sous-système ;
- Champs fournisseur :

- Instance ;
- Classe ;
- Code ;
- Sous-système ;
- Période :
 - De ;
 - À.



La période et les délais de traitement sont indiqués dans le fuseau horaire de l'utilisateur.



Les champs **De** et **À** peuvent être spécifiés indépendamment l'un de l'autre. La spécification de l'heure nécessite également la spécification de la date.



Lors d'une recherche par date (sans spécifier l'heure), **De** définit l'heure de début de journée 00:00:00 en heure locale, et **À** définit l'heure de fin de journée 23:59:59 en heure locale.

- Champs du service :
 - Code ;
 - Version ;
- Type de message :
 - Demande ;
 - Réponse.

3.2. Vérifier la signature du message

Droits d'accès : Auditeur de transactions

Pour vérifier la signature d'un message, ouvrez la page **Messages**. Recherchez le message et cliquez sur **Détails**. Le serveur tentera de vérifier la signature et affichera le résultat.

3.2.1. États du message

L'état du message détermine si la signature peut être vérifiée.

Un message peut se trouver dans l'un des quatre états suivants :

- **En attente d'horodatage** – Le conteneur de signature attend un horodatage. Il n'est pas possible de vérifier la signature ou de télécharger le conteneur de signature.
- **Horodaté** – Le conteneur de signature est horodaté mais n'est pas encore archivé. Il est possible de visualiser le résultat de la vérification et de télécharger le conteneur de

signature.

- **Archivé** – Le conteneur de signature est archivé, il est possible de le vérifier et de le télécharger uniquement si le conteneur est disponible sur le support d'archivage. Si le conteneur est disponible, tous les détails peuvent être consultés, y compris les détails de la signature.
- **Données manquantes** – Pas de conteneur de signature (par exemple, les données relatives à la signature ont été perdues à la suite d'une panne de courant). Il n'est pas possible de vérifier la signature ou de télécharger le conteneur.

3.2.2. Détails du message et résultat de la vérification



Toutes les heures affichées le sont dans le fuseau horaire de l'utilisateur.

Détails du message :

- Type de message ;
- Identifiant de transaction ;
- Identifiant de demande ;
- Identifiant de l'utilisateur ;
- Traité à (heure à laquelle le serveur de sécurité a traité le message entrant) ;
- Client du service ;
- Fournisseur de services ;
- Code de service ;
- Version du service ;
- Version du protocole.

Signature et son résultat de vérification :

- Si la signature est valide ;
 - Si le serveur de sécurité n'a pas pu vérifier la signature, la raison en est indiquée ;



Si la vérification de la signature échoue, il se peut que la signature soit toujours valide mais que le serveur de sécurité manque d'informations pour la vérifier.

- Heure de signature.
- **Certificat de signature :**
 - Si le certificat est valide ou non ;
 - Si le certificat n'est pas valide, la raison ;
 - Numéro de série ;
 - Sujet ;

- Émetteur ;
- Émis à ;
- Expire à ;
- Empreinte digitale (SHA-1).

Réponse OCSP du certificat de signature :

- Indique si la réponse OCSP est valide ou non ;
 - Si la réponse OCSP n'est pas valide, la raison ;
- Réponse OCSP ;
- Produite à.
- **Certificat de répondeur OCSP :**
 - Si le certificat est valide ou non ;
 - Si le certificat n'est pas valide, la raison ;
 - Numéro de série ;
 - Sujet ;
 - Émetteur ;
 - Émis à ;
 - Expire à ;
 - Empreinte digitale (SHA-1).

Horodatage :

- Indique si l'horodatage est valide ou non ;
 - Si l'horodatage n'est pas valide, la raison en est indiquée ;
- Valeur.
- **Certificat TSA :**
 - Si le certificat est valide ou non ;
 - Si le certificat n'est pas valide, la raison ;
 - Numéro de série ;
 - Sujet ;
 - Émetteur ;
 - Émis à ;
 - Expire à ;
 - Empreinte digitale (SHA-1).



Les certificats des répondeurs OCSP et TSA deviennent invalides si l'autorité de gouvernance retire ses certificats de la liste des répondeurs OCSP et des TSA

approuvés sur le serveur de registre.

3.3. Télécharger un conteneur de signatures

Droits d'accès : Auditeur de transactions

Une fois la signature horodatée, le conteneur de signature est disponible pour le téléchargement.

Pour télécharger un conteneur de signature, vous pouvez soit :

1. Accéder à la page **Messages**.
2. Rechercher le message.
3. Cliquer sur **Télécharger**.

ou

1. Ouvrir la page **Détails** du message.
2. Cliquer sur **Télécharger**.

Pour les signatures archivées, le serveur de sécurité ne peut renvoyer le conteneur de signature que si le conteneur est toujours disponible sur le stockage du serveur ou sur le stockage des archives.

3.4. Télécharger des certificats

Droits d'accès : Auditeur de transactions

Pour télécharger un certificat lié à la signature, accédez à la page **Détails du message** et choisissez le certificat à télécharger.

Les trois types de certificats qui peuvent être téléchargés sont les suivants :

- **Certificat de signature** de la clé de signature utilisée pour signer le message envoyé.
- **Certificat du répondeur OCSP** du répondeur OCSP qui a renvoyé la réponse OCSP du certificat de signature.
- **Certificat TSA** du service d'horodatage qui a émis un horodatage pour le message.