ITUPublications
Recommandations

Union Internationale des Télécommunications
Secteur de la Normalisation

Recommandation

UIT-T X.1410 (03/2023)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

Applications et services sécurisés (2) – Sécurité de la technologie des registres distribués (DLT)

Architecture de sécurité pour la gestion du partage de données reposant sur la technologie des registres distribués

RECOMMANDATIONS UIT-T DE LA SÉRIE X

Réseaux de données, communication entre systèmes ouverts et sécurité

RÉSEAUX PUBLICS DE DONNÉES	X.1-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	X.850-X.899
TRAITEMENT RÉPARTI OUVERT	X.900-X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	X.1000-X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	X.1100-X.1199
SÉCURITÉ DU CYBERESPACE	X.1200-X.1299
APPLICATIONS ET SERVICES SÉCURISÉS (2)	X.1300-X.1499
Communications d'urgence	X.1300-X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310-X.1319
Sécurité des réseaux électriques intelligents	X.1330-X.1339
Courrier certifié	X.1340-X.1349
Sécurité de l'Internet des objets (IoT)	X.1350-X.1369
Sécurité des systèmes de transport intelligents	X.1370-X.1399
Sécurité de la technologie des registres distribués (DLT)	**X.1400-X.1429**
Sécurité des applications (2)	X.1450-X.1459
Sécurité de la toile (2)	X.1470-X.1489
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	X.1500-X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	X.1600-X.1699
COMMUNICATIONS QUANTIQUES	X.1700-X.1729
SÉCURITÉ DES DONNÉES	X.1750-X.1799
SÉCURITÉ DES IMT-2020	X.1800-X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1410

Architecture de sécurité pour la gestion du partage de données reposant sur la technologie des registres distribués

Résumé

La Recommandation UIT-T X.1410 définit une architecture de sécurité pour la gestion du partage de données reposant sur les technologies de registres distribués (DLT). Sur la base de cette architecture, la présente Recommandation définit les interfaces entre les entités fonctionnelles, ainsi que les procédures applicables à la gestion du partage de données reposant sur la technologie DLT. La technologie des registres distribués (DLT) est en train de transformer les différents secteurs en offrant des solutions innovantes et de modifier le mode de fonctionnement des pouvoirs publics, des institutions et des entreprises. Cette technologie offre une solution pour répliquer, partager et synchroniser les données de manière sûre dans un réseau informatique distribué, compte tenu de ses fonctions de décentralisation et d'inviolabilité. Les approches actuelles en matière de partage de données opérationnelles et de données contenant des informations d'identification personnelle (PII) avec des entreprises et des plates-formes numériques entraînent des vulnérabilités en matière de respect de la vie privée, découlant du piratage ou d'une mauvaise gestion des données. L'adoption de la technologie DLT ou de la chaîne de blocs pour la gestion du partage de données permet aux particuliers, ou aux entreprises, de continuer d'exercer un contrôle plus direct sur leurs propres informations confidentielles. Dans le cas d'une solution basée sur la technologie DLT, seules les données ne contenant pas d'informations PII, par exemple les valeurs de données hachées, sont stockées dans la chaîne. Les données PII relatives au propriétaire des données sont stockées en dehors de la chaîne. Une solution basée sur la technologie DLT permet d'améliorer la traçabilité des données, la possibilité de vérifier les données ainsi que la possibilité de modifier leur statut.

Historique *

Édition	Recommandation	Approbation	Commission d'études	ID unique
1.0	UIT-T X.1410	03-03-2023	17	11.1002/1000/15109

Mots clés

Partage de données, technologie DLT, architecture de sécurité.

* Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1410

Architecture de sécurité pour la gestion du partage de données reposant sur la technologie des registres distribués

1 Domaine d'application

La présente Recommandation définit une architecture de sécurité pour le partage de données reposant sur les technologies de registres distribués (DLT), et comprend:

– la conception de l'architecture de sécurité pour le partage de données reposant sur la technologie DLT;

– la spécification des fonctions logiques de l'architecture de sécurité pour le partage de données;

– la spécification des interfaces entre les fonctions logiques de l'architecture de sécurité;

– la spécification des procédures pour le partage de données reposant sur la technologie DLT.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1408] Recommandation UIT-T X.1408 (2021), *Menaces et exigences de sécurité relatives à l'accès aux données et au partage de données reposant sur la technologie des registres distribués*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 adresse [b-UIT-T FG DLT D1.1]: identificateur utilisé pour désigner une ou plusieurs entités réalisant des transactions, ou d'autres actions, dans une chaîne de blocs ou un réseau de registres distribués.

3.1.2 chaîne de blocs [b-UIT-T X.1400]: type de registre distribué composé de données enregistrées numériquement structurées sous la forme d'une chaîne de blocs en expansion constante, où chaque bloc est lié de manière cryptographique et renforcé contre les altérations et les révisions.

3.1.3 autorité de certification (CA) [b-UIT-T X.509]: autorité jouissant de la confiance d'une ou de plusieurs entités, pour la création et la signature numérique de certificats de clé publique. L'autorité de certification peut, de manière optionnelle, créer les clés des utilisateurs.

3.1.4 fournisseur de données [b-ISO/CEI/IEEE 15939]: personne physique ou organisation à l'origine de données.

3.1.5 identité [b-ISO/CEI 29100]: ensemble d'attributs qui permettent d'identifier la personne concernée par des données à caractère personnel.

3.1.6 en dehors de la chaîne [b-ISO 22739]: concerne un système de blockchain, mais est situé, réalisé ou exécuté en dehors de ce système de blockchain.

3.1.7 dans la chaîne [b-ISO 22739]: situé, réalisé ou exécuté à l'intérieur d'un système de blockchain.

3.1.8 information d'identification personnelle (PII) [b-ISO/CEI 29100]: toute information qui a) peut être utilisée pour identifier la personne à laquelle elle se rapporte; ou b) est ou peut être directement ou indirectement liée à une personne.

NOTE – Pour déterminer si la personne à laquelle les informations PII se rapportent peut être identifiée, il convient de tenir compte de tous les moyens qui peuvent être raisonnablement utilisés par la partie intervenant dans la protection de la vie privée et détenant les données ou par toute autre partie pour identifier cette personne.

3.1.9 infrastructure de clé publique (PKI) [b-UIT-T X.509]: infrastructure pouvant prendre en charge la gestion de clés publiques afin de fournir des services d'authentification, de chiffrement, d'intégrité et de non-répudiation.

3.1.10 contrat intelligent [b-UIT-T X.1400]: programme écrit sur le système de registre distribué, qui codifie les règles pour des types particuliers de transactions de système de registre distribué, de telle manière que ces transactions peuvent être validées ou exécutées lorsque des conditions particulières sont réunies.

3.1.11 système de chiffrement symétrique [b-ISO/CEI 18033-1]: technique de chiffrement utilisée pour protéger la confidentialité des données et composée de trois processus constitutifs: un algorithme de chiffrement, un algorithme de déchiffrement, et une méthode de création des clés, où les algorithmes de chiffrement et de déchiffrement utilisent la même clé.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 consommateur de données: utilisateur qui lit des données puis les traite de manière à découvrir les limites lexicales ou de codage.

NOTE – Adapté de la norme [b-ISO/CEI 20944-1].

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'application (*application programming interface*)

CA autorité de certification (*certification authority*)

DLT technologie des registres distribués (*distributed ledger technology*)

PII information d'identification personnelle (*personally identifiable information*)

PKI infrastructure de clé publique (*public key infrastructure*)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

Les expressions "**peut**" et "**à titre d'option**" indiquent une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elles ne doivent pas être interprétées comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité avec la spécification.

Dans la présente Recommandation, les caractères en *italique* sont utilisés pour désigner des fonctions.

6 Architecture du partage de données reposant sur la technologie DLT

La technologie des registres distribués offre une solution pour répliquer, partager et synchroniser les données de manière sûre dans un réseau informatique distribué, compte tenu de ses fonctions de décentralisation et d'inviolabilité. Les approches actuelles en matière de partage de données opérationnelles et de données contenant des informations d'identification personnelle (PII) avec des entreprises et des plates-formes numériques entraînent des vulnérabilités en matière de respect de la vie privée, découlant du piratage ou d'une mauvaise gestion des données. L'adoption de la technologie DLT ou de la chaîne de blocs pour la gestion du partage de données permet aux particuliers, ou aux entreprises, de continuer d'exercer un contrôle plus direct sur leurs propres informations confidentielles. Dans le cas d'une solution basée sur la technologie DLT, seules les données ne contenant pas d'informations PII, par exemple les valeurs de données hachées, sont stockées dans la chaîne, tandis que les données PII relatives au propriétaire des données sont stockées en dehors de la chaîne. Une solution basée sur la technologie DLT permet d'améliorer la traçabilité des données, la possibilité de vérifier les données ainsi que la possibilité de modifier leur statut. Dans ce contexte, la présente Recommandation définit l'architecture de sécurité pour la gestion du partage de données reposant sur les technologies DLT. La gestion du partage de données fait appel à un système de chiffrement symétrique des donnés, dans lequel les algorithmes de chiffrement et de déchiffrement utilisent la même clé. Les menaces pour la sécurité sont décrites dans la Recommandation [UIT-T X.1408].

La présente Recommandation a été élaborée sur la base de la Recommandation [UIT-T X.1408]. Si la Recommandation [UIT-T X.1408] suit une approche conceptuelle, la présente Recommandation a été élaborée selon une approche axée sur la mise en œuvre. On trouvera dans le Tableau 1 la correspondance entre les termes utilisés dans la présente Recommandation et ceux utilisés dans la Recommandation [UIT-T X.1408].

Tableau 1 – Correspondance entre les termes utilisés dans la présente Recommandation et ceux utilisés dans la Recommandation [UIT-T X.1408]

Présente Recommandation	[UIT-T X.1408]
Fournisseur de données	Agent partageant des données (propriétaire des données)
Consommateur de données	Client du consommateur de données (responsable du traitement des données)
Serveur de stockage des clés	Serveur de gestion des clés
Serveur de stockage des données	Serveur de stockage des données (fournisseur du service de stockage des données)
Gestion du partage de données reposant sur la technologie DLT	Courtier en données

6.1 Vue d'ensemble de l'architecture fonctionnelle

La Figure 1 illustre l'architecture fonctionnelle de la gestion du partage de données reposant sur la technologie DLT, du point de vue de la mise en œuvre. Elle est conforme à l'architecture de l'accès aux données et du partage de données reposant sur la technologie DLT présentée dans la Figure B.1 de la Recommandation [UIT-T X.1408]. Cette dernière est imaginée d'un point de vue conceptuel et constitue une architecture de haut niveau. L'architecture fonctionnelle présentée dans la Figure 1 comprend cinq composantes fonctionnelles en bleu, et trois composantes fonctionnelles en gris.

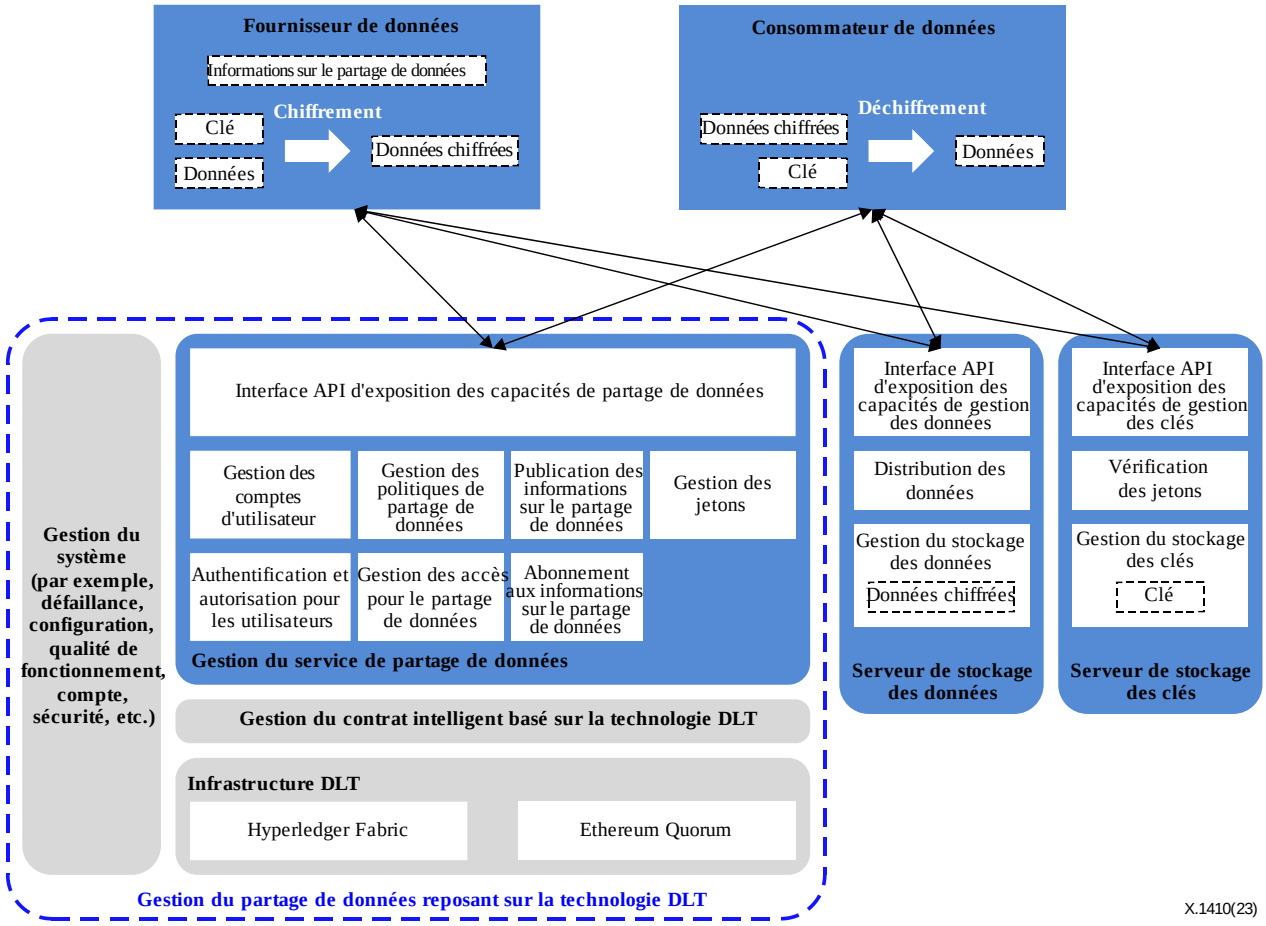

Figure 1 – Architecture fonctionnelle de la gestion du partage de données reposant sur la technologie DLT

Ces composantes sont décrites comme suit:

– Les cinq composantes fonctionnelles en bleu sont les suivantes: *fournisseur de données*, *consommateur de données*, *gestion du service de partage de données*, *serveur de stockage des clés* et *serveur de stockage des données*. Elles sont définies et décrites en détail au § 6.2.

– Les trois composantes fonctionnelles en gris sont les suivantes: *infrastructure DLT*, *gestion du contrat intelligent basé sur la technologie DLT* et *gestion du système (par exemple, défaillance, configuration, qualité de fonctionnement, compte, sécurité, etc.)*. Elles réutilisent les plates-formes DLT à code source ouvert existantes (par exemple Hyperledger Fabric), et n'entrent pas dans le cadre de la présente Recommandation.

Les procédures de gestion du partage de données reposant sur la technologie DLT sont décrites dans l'Annexe A.

6.2 Composantes fonctionnelles

6.2.1 Fournisseur de données et consommateur de données

La présente Recommandation introduit deux types d'utilisateur: le fournisseur de données (à savoir l'utilisateur qui partage ses données) et le consommateur de données (à savoir l'utilisateur qui consomme les données partagées par d'autres utilisateurs). Ces deux utilisateurs ont des capacités en commun:

1) obtenir des certificats numériques (y compris des clés publiques), ainsi que les clés privées correspondantes auprès de l'autorité de certification (CA);
2) stocker les certificats numériques obtenus et les clés privées correspondantes en toute sécurité;
3) communiquer avec le serveur de gestion du partage de données reposant sur la technologie DLT;
4) obtenir et stocker les certificats numériques, les paramètres de réseau et les configurations de réseau des nœuds du réseau DLT;
5) recevoir des notifications de la fonction de gestion de partage de données reposant sur la technologie DLT;
6) utiliser un système de chiffrement symétrique.

Le fournisseur de données et le consommateur de données ont des capacités qui leur sont propres, comme indiqué ci-après:

– Un *fournisseur de données* a les capacités suivantes:

  1) recueillir des données brutes et les rendre moins sensibles (par exemple en les rendant anonymes, en supprimant des informations sensibles telles que le nom, le numéro de téléphone mobile et les données de carte de crédit), sans porter atteinte à la qualité des données qui doivent être partagées;
  2) générer une clé pour un système de chiffrement symétrique;
  3) chiffrer des données avec la clé, en utilisant un système de chiffrement symétrique;
  4) stocker le cryptogramme et la clé de chiffrement correspondante de façon sécurisée sur le serveur local ou distant;
  5) effectuer l'authentification mutuelle auprès de la fonction de gestion de partage de données reposant sur la technologie DLT;
  6) fournir, à la fonction de gestion de partage de données reposant sur la technologie DLT des informations sur le partage de données, notamment l'identificateur du fournisseur de données, la clé publique du fournisseur de données, l'identificateur du cryptogramme et son adresse de stockage, l'identificateur de la clé de chiffrement et son adresse de stockage, les entreprises devant être autorisées à avoir accès, les utilisateurs devant être autorisés à avoir accès, ainsi que d'autres attributs des données (par exemple la catégorie de données, l'introduction des données, l'utilisation et le prix);
  7) combiner des informations sur le partage de données, ainsi que d'autres informations, pour créer une politique de partage de données, puis signer la politique de partage de données avec la clé privée;
  8) transmettre la politique de partage de données avec la signature numérique correspondante à la fonction de partage de données reposant sur la technologie DLT;
  9) recevoir la notification de la fonction de gestion de partage de données reposant sur la technologie DLT, qui indique que le contrat intelligent de partage de données a été créé;
  10) gérer la politique de partage de données, notamment en interrogeant et en mettant à jour les données.

– Un *consommateur de données* a les capacités suivantes:

1) s'abonner aux messages publiés concernant le partage de données;
2) effectuer l'authentification mutuelle auprès de la fonction de gestion de partage de données reposant sur la technologie DLT;
3) obtenir des informations sur le partage de données;
4) envoyer des informations sur le consommateur de données (par exemple l'identité du consommateur de données, la clé publique du consommateur de données) et les informations sur les données partagées (par exemple l'identité du fournisseur de données, la clé publique du fournisseur de données, l'identificateur du cryptogramme et l'identificateur de la clé de chiffrement), ainsi que la signature numérique (réalisée au moyen de la clé privée du consommateur de données) à la fonction de gestion de partage de données reposant sur la technologie DLT;
5) recevoir des notifications de la fonction de gestion de partage de données reposant sur la technologie DLT, comprenant les informations sur les données partagées, l'adresse de stockage de la clé, l'adresse de stockage du cryptogramme et le jeton d'accès;
6) envoyer le jeton d'accès au serveur de stockage des clés, afin d'obtenir la clé de chiffrement des données en fonction de l'adresse de stockage de la clé;
7) obtenir le cryptogramme en fonction de l'adresse de stockage des données;
8) déchiffrer le cryptogramme avec la clé du système de chiffrement symétrique obtenue, afin d'obtenir les données en clair;
9) gérer les enregistrements pour l'accès aux données partagées.

6.2.2 Gestion du service de partage de données

Les capacités de chaque composante de la gestion du service de partage de données sont décrites comme suit:

– La fonction ***gestion des comptes d'utilisateur*** a les capacités nécessaires pour gérer les comptes d'utilisateur, ce qui inclut la création, la mise à jour et la suppression des comptes, ainsi que l'interrogation des données.

– La fonction ***authentification et autorisation pour les utilisateurs*** a les capacités suivantes:

1) procéder à une authentification mutuelle auprès des utilisateurs (à savoir le fournisseur de données et le consommateur de données);
2) autoriser les utilisateurs à partager les données et à accéder aux données partagées.

– La fonction ***gestion des politiques de partage de données*** a les capacités suivantes:

1) recevoir des informations et des politiques sur le partage de données, ainsi que la signature numérique correspondante envoyées par le fournisseur de données;
2) créer une transaction DLT selon les informations transmises par le fournisseur de données;
3) soumettre la transaction DLT aux composantes sous-jacentes (à savoir les fonctions *infrastructure DLT* et *gestion du contrat intelligent basé sur la technologie DLT*), afin de créer un contrat intelligent pour le partage de données, qui sera transmis aux nœuds du réseau DLT;
4) informer les fonctions *fournisseur de données* et *publication des informations sur le partage de données* que le contrat intelligent pour le partage de données a été créé;
5) permettre aux fournisseurs de données de gérer les données qu'ils ont partagées.

– La fonction ***gestion des accès pour le partage de données*** a les capacités suivantes:

1) recevoir les demandes d'accès aux données (y compris les informations sur le consommateur de données, les informations sur les données partagées et la signature numérique correspondante) envoyées par le consommateur de données, et vérifier si ce dernier est autorisé à accéder aux données selon la politique de partage de données (dans certains cas, seul le consommateur de données issu d'un secteur ou d'un pays particulier peut accéder aux données partagées);
2) créer une transaction DLT selon les informations transmises par le consommateur de données;
3) soumettre la transaction DLT aux composantes sous-jacentes (par exemple à la fonction *infrastructure DLT*), afin d'enregistrer les accès aux données, qui seront ensuite transmis aux nœuds du réseau DLT;
4) informer la fonction *gestion des jetons* que la transaction relative à l'accès aux données a été créée et qu'un jeton d'accès va être généré;
5) recevoir le jeton d'accès transmis par la fonction *gestion des jetons*;
6) envoyer des informations sur l'accès pour le partage de données (par exemple le jeton d'accès, l'adresse de stockage de la clé et l'adresse de stockage des données) au consommateur de données;
7) permettre au consommateur de données de gérer les enregistrements de ses accès pour le partage de données.

– La fonction ***publication des informations sur le partage de données*** a les capacités suivantes:

1) recevoir des notifications de la fonction *gestion des politiques de partage de données*, qui contiennent de nouvelles informations sur le partage de données;
2) publier de nouvelles informations sur le partage de données;
3) informer la fonction *abonnement aux informations sur le partage de données* que de nouvelles informations sur le partage de données ont été publiées.

– La fonction ***abonnement aux informations sur le partage de données*** a les capacités suivantes:

1) recevoir des notifications de la fonction *gestion des informations sur le partage de données*, qui contiennent de nouvelles informations sur le partage de données;
2) envoyer de nouvelles informations sur le partage de données aux abonnés.

– La fonction ***gestion des jetons*** a les capacités suivantes:

1) recevoir des notifications de la fonction *gestion des accès pour le partage de données*, afin de générer un jeton d'accès;
2) générer le jeton d'accès;
3) envoyer le jeton d'accès généré à la fonction *gestion des accès pour le partage de données*.

– La fonction ***interface API d'exposition des capacités de partage de données*** permet aux utilisateurs de gérer les services de partage de données mentionnés ci-dessus, et d'y accéder.

6.2.3 Serveur de stockage des clés

Les capacités de chaque composante du serveur de stockage des clés sont décrites comme suit:

– La fonction ***gestion du stockage des clés*** a les capacités suivantes:

1) recevoir les demandes envoyées par le *fournisseur de données* pour stocker la clé;
2) authentifier le *fournisseur de données*;

3) stocker la clé en toute sécurité, par exemple stocker la clé sous la forme d'un cryptogramme ou dans un emplacement de stockage isolé;
4) informer le *fournisseur de données* que la clé est stockée;
5) recevoir des notifications de la fonction *vérification des jetons*, indiquant le résultat de la vérification du jeton d'accès;
6) envoyer la clé au *consommateur de données*.

– La fonction ***vérification des jetons*** a les capacités suivantes:
1) recevoir le jeton d'accès envoyé par le consommateur de données;
2) vérifier le jeton d'accès reçu;
3) envoyer le résultat de la vérification à la fonction *gestion du stockage des clés*.

– La fonction ***interface API d'exposition des capacités de gestion des clés*** permet aux utilisateurs de gérer une clé de chiffrement des données et d'y accéder.

6.2.4 Serveur de stockage des données

Les capacités de chaque composante du serveur de stockage des données sont décrites comme suit:

– La fonction ***gestion du stockage des données*** a les capacités suivantes:
1) recevoir la demande envoyer par le *fournisseur de données* pour stocker le cryptogramme;
2) authentifier le *fournisseur de données*;
3) stocker le cryptogramme;
4) informer le *fournisseur de données* que le cryptogramme est stocké.

– La fonction ***distribution des données*** a les capacités suivantes:
1) recevoir les demandes envoyées par un *consommateur de données*;
2) authentifier le *consommateur de données*;
3) envoyer le cryptogramme au *consommateur de données*.

– La fonction ***interface API d'exposition des capacités de gestion des données*** permet aux utilisateurs de gérer les données partagées et d'y accéder.

7 Architecture de sécurité pour la gestion du partage de données reposant sur la technologie DLT

Selon l'architecture fonctionnelle présentée dans la Figure 1, les consommateurs de données demandent et reçoivent une clé de chiffrement des données, qu'ils utilisent ensuite pour déchiffrer les données figurant dans le cryptogramme et ainsi obtenir les données partagées en clair. Après cela, les données partagées en clair ne peuvent pas être contrôlées par la fonction de gestion du partage de données reposant sur la technologie DLT. Les consommateurs de données peuvent transférer les données partagées en clair à d'autres utilisateurs qui ne sont pas autorisés à y accéder.

Afin de permettre aux fournisseurs de données de partager des données avec d'autres utilisateurs en toute sécurité et empêcher les consommateurs de données de transférer les données partagées en clair à d'autres utilisateurs, l'architecture fonctionnelle décrite dans la Figure 1 exige des caractéristiques de sécurité renforcées, qui sont présentées dans la Figure 2.

7.1 Vue d'ensemble de l'architecture de sécurité

La Figure 2 décrit l'architecture de sécurité pour la gestion du partage de données reposant sur la technologie DLT, qui permet de garantir les points suivants:

– les communications entre les composantes fonctionnelles illustrées dans la Figure 1 sont sécurisées;

– les fournisseurs de données chiffrent les données et définissent l'autorisation pour y accéder avant de les partager avec d'autres utilisateurs;

– les consommateurs de données déchiffrent les données partagées figurant dans le cryptogramme en fonction de l'autorisation d'accès avant d'y accéder;

– les consommateurs de données chiffrent les données partagées de la même manière que le font les fournisseurs de données après avoir accédé aux données; ainsi, les données partagées dans le cryptogramme sont stockées par les consommateurs de données;

– les consommateurs de données transfèrent uniquement les données partagées dans le cryptogramme à d'autres utilisateurs.

De cette manière, même si les utilisateurs reçoivent les données partagées qui leur ont été transférées par d'autres utilisateurs, ils doivent demander une autorisation à la fonction de gestion du partage de données reposant sur la technologie DLT pour accéder à ces données.

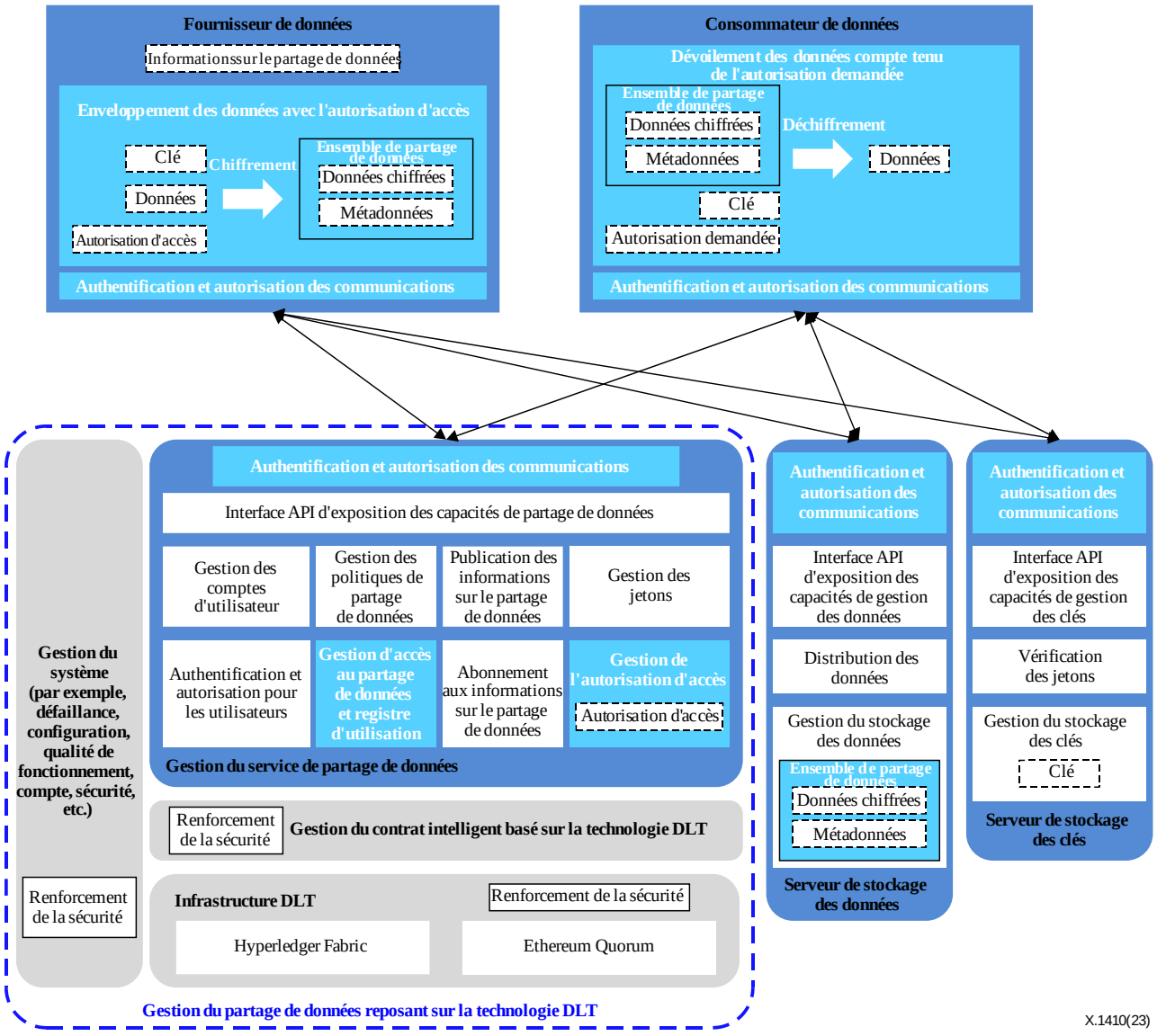

Figure 2 – Architecture de sécurité pour la gestion du partage de données reposant sur la technologie DLT

À la différence de la Figure 1, la Figure 2 présente des composantes fonctionnelles signalées sur fond bleu clair, qui constituent des fonctions de sécurité logiques, décrites en détail au § 7.2.

La présente Recommandation ne décrit pas le renforcement de la sécurité des trois composantes fonctionnelles en gris dans la Figure 2. Voir la Recommandation [b-UIT-T X.1402].

7.2 Composantes fonctionnelles de sécurité

7.2.1 Enveloppement des données avec autorisation d'accès

Pour que les utilisateurs puissent définir l'autorisation d'accès aux données à partager, le *fournisseur de données* dans la Figure 1 doit être renforcé grâce à l'introduction d'une nouvelle fonction logique de sécurité, à savoir *l'enveloppement des données avec autorisation d'accès*, dont les capacités sont les suivantes:

– générer la clé d'un système de chiffrement symétrique utilisée pour chiffrer les données à partager;

– communiquer avec le *serveur de stockage des clés* pour enregistrer l'identificateur de la clé et l'adresse permettant de l'obtenir;

– communiquer avec le *serveur de stockage des données* pour enregistrer l'identificateur de l'ensemble de partage de données et l'adresse permettant de l'obtenir;
– définir l'autorisation d'accès aux données à partager, y compris les temps d'accès, le délai d'expiration, la lecture seule, l'identificateur de la clé et son adresse de stockage, l'identificateur de l'ensemble de partage de données et son adresse de stockage;
– générer des métadonnées, y compris l'identificateur de l'ensemble de partage de données, l'identificateur du fournisseur de données, la clé publique du fournisseur de données et la signature correspondant aux informations précédentes;
– générer l'ensemble de partage de données, y compris les données chiffrées et les métadonnées;
– télécharger la clé sur le *serveur de stockage des clés* via un canal de transmission sécurisé;
– télécharger l'ensemble de partage de données sur le *serveur de stockage des données* via un canal de transmission sécurisé;
– télécharger l'autorisation d'accès dans la fonction *gestion du service de partage de données* via un canal de transmission sécurisé.

7.2.2 Dévoilement des données compte tenu de l'autorisation demandée

Pour que les utilisateurs puissent accéder aux données partagées selon l'autorisation demandée, le *consommateur de données* dans la Figure 1 doit être renforcé grâce à l'introduction d'une nouvelle fonction logique de sécurité, à savoir le *dévoilement des données selon l'autorisation demandée*, dont les capacités sont les suivantes:

– obtenir l'adresse permettant d'exécuter le contrat intelligent de partage de données;
– communiquer avec la fonction *gestion du service de partage de données*, exécuter le contrat intelligent de partage de données et obtenir l'autorisation demandée, y compris les temps d'accès, le délai d'expiration, la lecture seule, l'identificateur de la clé et son adresse de stockage, l'identificateur de l'ensemble de partage de données et son adresse de stockage;
– communiquer avec le *serveur de stockage des clés* pour obtenir la clé de chiffrement;
– communiquer avec le *serveur de stockage des données* pour obtenir l'ensemble de partage de données, y compris les données chiffrées et les métadonnées;
– valider l'ensemble de partage de données obtenu sur la base de la signature dans les métadonnées;
– déchiffrer les données chiffrées à l'aide de la clé de chiffrement;
– présenter les données partagées en clair aux utilisateurs en fonction de l'autorisation demandée;
– chiffrer les données partagées de la même manière que les fournisseurs de données le font une fois l'accès aux données terminé.

7.2.3 Gestion des autorisations d'accès

Pour que les utilisateurs puissent définir l'autorisation d'accès aux données partagées ou pour qu'ils puissent accéder aux données partagées compte tenu de l'autorisation demandée, la fonction *gestion du service de partage de données* dans la Figure 1 doit être renforcée par l'introduction d'une nouvelle fonction de sécurité logique, à savoir la *gestion des autorisations d'accès*, dont les capacités sont les suivantes:

– permettre aux utilisateurs de définir l'autorisation d'accès aux données à partager:
  • recevoir l'autorisation d'accès définie par le *fournisseur de données* à partir de la fonction *gestion de la politique de partage de données*;
  • stocker l'autorisation d'accès;

- envoyer la réponse à la fonction *gestion de la politique de partage de données*;

– permettre aux utilisateurs d'accéder aux données partagées compte tenu de l'autorisation demandée:
  - recevoir l'autorisation demandée par le *consommateur de données* à partir de la fonction *gestion de l'accès au partage de données et registre d'utilisations*;
  - générer l'autorisation demandée;
  - envoyer l'autorisation demandée à la fonction *gestion de l'accès au partage de données et registre d'utilisation*.

7.2.4 Gestion de l'accès au partage de données et registre d'utilisation

Pour que les utilisateurs puissent suivre l'utilisation de leurs données partagées, la fonction *gestion de l'accès au partage de données et registre d'utilisation* dans la Figure 2 doit être renforcée à l'aide des capacités suivantes:

– communiquer avec la fonction *gestion des autorisations d'accès* pour obtenir l'autorisation demandée;

– enregistrer les utilisations des données partagées compte tenu de l'autorisation demandée.

7.2.5 Authentification et autorisation des communications

Pour que les communications soient sûres, les cinq composantes fonctionnelles dans la Figure 1 (à savoir le *fournisseur de données*, le *consommateur de données*, la *gestion du service de partage de données*, le *serveur de stockage des clés* et le *serveur de stockage des données*) doivent être renforcées par l'introduction d'une nouvelle fonction logique de sécurité, à savoir l'*authentification et l'autorisation des communications*.

Lorsque le *fournisseur de données* ou le *consommateur de données* envoie la demande à la fonction *gestion du service de partage de données* ou au *serveur de stockage des clés* ou au *serveur de stockage des données*, la fonction *authentification et autorisation des communications* peut prendre en charge:

– la fonction *gestion du service de partage de données/serveur de stockage des clés*/*serveur de stockage des données* qui authentifie le *fournisseur de données/consommateur de données* compte tenu du certificat [b-IETF RFC 4306], [b-IETF RFC 5246] ou de la clé préalablement partagée [b-IETF RFC 4279], [b-IETF RFC 4306];

– le *fournisseur de données/consommateur de données* qui authentifie la fonction *gestion du service de partage de données*/le *serveur de stockage des clés*/le *serveur de stockage des données* compte tenu du certificat [b-IETF RFC 4306], [b-IETF RFC 5246];

– la fonction *gestion du service de partage de données/serveur de stockage des clés*/*serveur de stockage des données* qui autorise le *fournisseur de données/consommateur de données* sur la base de la liste blanche/liste noire [b-IETF RFC 5782], [b-IETF RFC 5851] ou de la liste de contrôle d'accès [b-IETF RFC 4314], [b-IETF RFC 4949];

– la création de la clé de la session, qui sera utilisée pour protéger les communications entre *le fournisseur de données/consommateur de données* et la fonction *gestion du service de partage de données*/le *serveur de stockage des clés*/le *serveur de stockage des données*.

7.3 Procédures de partage de données sécurisé

7.3.1 Procédure permettant aux fournisseurs de données de partager des données et de définir l'autorisation d'accès

La procédure permettant aux fournisseurs de données de partager des données en définissant une autorisation d'accès est décrite dans la Figure 3.

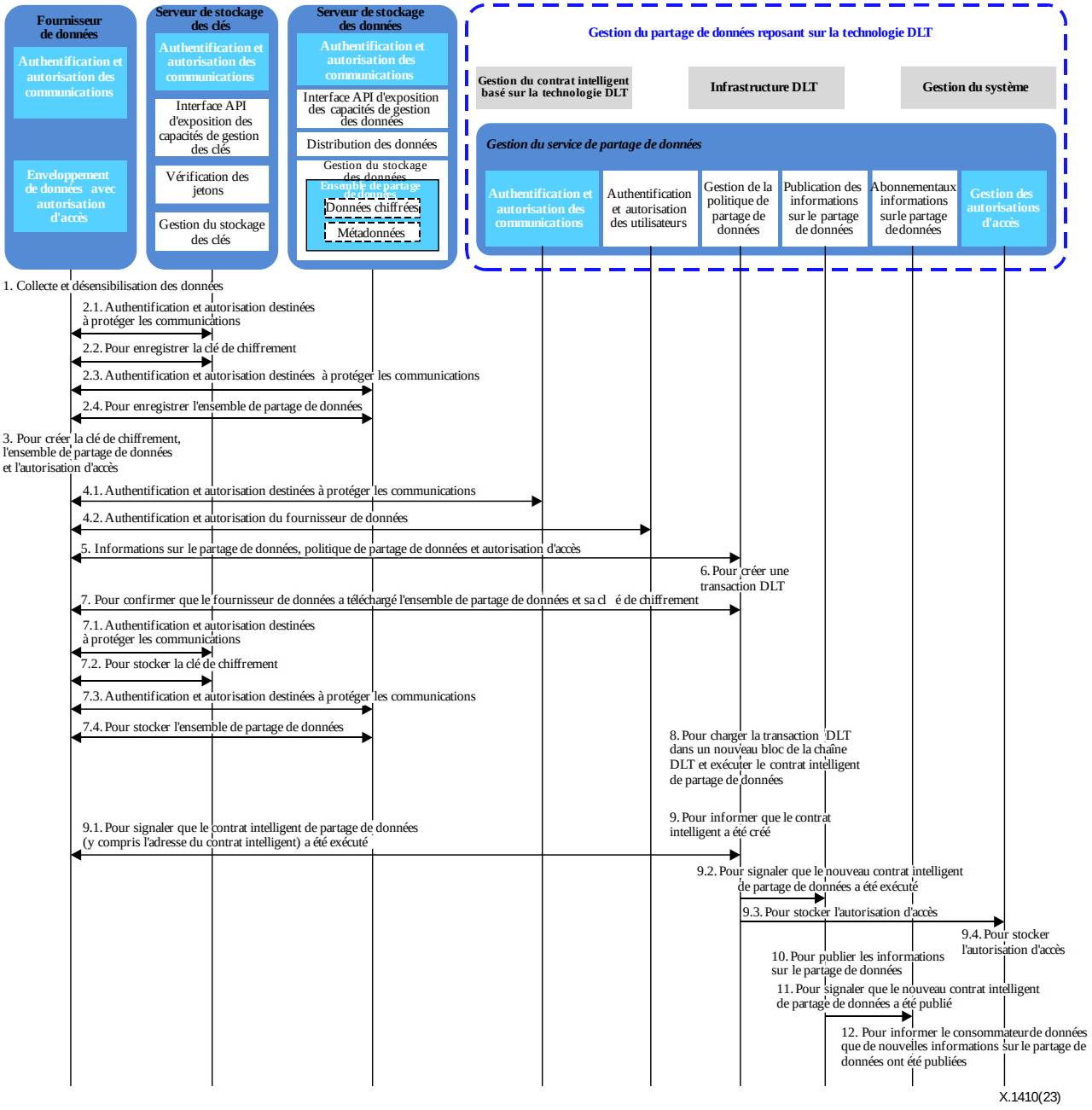

Figure 3 – Procédure permettant aux fournisseurs de données de partager des données en définissant une autorisation d'accès

Comme indiqué dans la Figure 3, la procédure est la suivante.

1) Le *fournisseur de données* recueille les données d'origine et les désensibilise sans altérer la qualité des données à partager.

2) Le *fournisseur de données* enregistre l'ensemble de partage de données et la clé correspondante sur le serveur de stockage des clés et le serveur de stockage des données, locaux ou distants, comme suit:

   2.1) le *fournisseur de données* et la fonction *authentification et autorisation des communications* du *serveur de stockage des clés* s'authentifient mutuellement et obtiennent une clé de session qui sera utilisée pour protéger les futures communications entre eux;

   2.2) le *fournisseur de données* se connecte au *serveur de stockage des clés* et enregistre l'identificateur de la clé et l'adresse permettant de l'obtenir;

2.3) le *fournisseur de données* et la fonction *authentification et autorisation des communications* du *serveur de stockage des données* s'authentifient mutuellement et obtiennent une clé de session qui sera utilisée pour protéger les futures communications entre eux;

2.4) le *fournisseur de données* se connecte au *serveur de stockage des données* et enregistre l'identificateur de l'ensemble de partage de données et l'adresse permettant de l'obtenir.

3) Le *fournisseur de données* crée des informations sur le partage de données, notamment l'identificateur et la clé publique du fournisseur de données, l'identificateur de l'ensemble de partage de données et son adresse de stockage, l'identificateur de la clé et son adresse de stockage, les entreprises qui devront bénéficier d'une autorisation d'accès, les utilisateurs qui devront bénéficier d'une autorisation d'accès ainsi que d'autres attributs des données (par exemple la catégorie de données, une présentation des données, leur utilisation, le prix).

Le *fournisseur de données* génère une clé utilisée pour chiffrer les données à partager.

Le *fournisseur de données* définit l'autorisation d'accès aux données, y compris les temps d'accès, le délai d'expiration, la lecture seule, l'identificateur de la clé et son adresse de stockage, l'identificateur de l'ensemble de partage de données et son adresse de stockage à partager;

Le *fournisseur de données* génère des métadonnées, notamment l'identificateur de l'ensemble de partage de données, l'identificateur du fournisseur de données, la clé publique du fournisseur de données et la signature des informations précédentes;

Le *fournisseur de données* génère un ensemble de partage de données, qui comprend les données chiffrées et les métadonnées.

4) Avant la publication des données à partager, il est nécessaire que:

4.1) le *fournisseur de données* et la fonction *authentification et autorisation des communications* de la fonction *gestion du service de partage de données* s'authentifient mutuellement et obtiennent une clé de session qui sera utilisée pour protéger les futures communications entre eux.

4.2) le *fournisseur de données* et la fonction *authentification et autorisation des utilisateurs* de la fonction *gestion du service de partage de données* s'authentifient mutuellement. Une fois l'authentification mutuelle réussie, la composante *authentification et autorisation des utilisateurs* vérifie si le fournisseur de données a le droit de publier les données à partager.

5) Le *fournisseur de données* fournit les informations sur le partage de données compte tenu des exigences de la fonction *gestion de la politique de partage de données* de la composante *gestion du service de partage de données*. Le *fournisseur de données* crée une politique de partage de données qui comprend des informations notamment sur le partage de données. Le *fournisseur de données* envoie les informations sur le partage de données, la politique de partage de données, l'autorisation d'accès et sa signature numérique à la fonction *gestion de la politique de partage de données*.

6) Une fois les informations sur le partage de données, la politique de partage de données, l'autorisation d'accès et la signature numérique correspondante envoyées par le *fournisseur de données* reçues, la fonction *gestion de la politique de partage de données* vérifie la signature numérique et crée une transaction DLT.

7) La fonction *gestion de la politique de partage de données* vérifie auprès du *fournisseur de données* que la clé et l'ensemble de partage de données sont stockés respectivement sur le *serveur de stockage des clés* et le *serveur de stockage des données*. Si tel n'est pas le cas, on procèdera comme suit:

7.1) le *fournisseur de données* et la fonction *authentification et autorisation des communications* du *serveur de stockage des clés* s'authentifient mutuellement et obtiennent une clé de session qui sera utilisée pour protéger les futures communications entre eux;

7.2) le *fournisseur de données* se connecte au *serveur de stockage des clés* et y stocke la clé;

7.3) le *fournisseur de données* et la fonction *authentification et autorisation des communications* du *serveur de stockage des données* s'authentifient mutuellement et obtiennent une clé de session qui sera utilisée pour protéger les futures communications entre eux;

7.4) le *fournisseur de données* se connecte au *serveur de stockage des données* et y stocke l'ensemble de partage de données.

8) La fonction *gestion de la politique de partage de données* envoie une ou plusieurs transactions DLT accompagnées de la signature numérique correspondante aux composantes sous-jacentes *infrastructure DLT* et *gestion du contrat intelligent basé sur la technologie DLT* pour former un nouveau bloc qui contient un ou plusieurs contrats intelligents de partage de données. Ces nouveaux blocs sont distribués aux nœuds DLT associés. Le chargement des transactions DLT dans la chaîne DLT dépend de la technologie sous-jacente utilisée pour la mise en œuvre (par exemple Hyperledger Fabric, Ethereum Quorum), laquelle n'entre pas dans le champ d'application de la présente Recommandation.

9) La fonction *gestion de la politique de partage de données* informe les composantes concernées que le contrat intelligent de partage de données a été créé.

9.1) La fonction *gestion de la politique de partage de données* notifie au *fournisseur de données* que le contrat intelligent de partage de données a été exécuté. Cette notification comprend l'adresse d'exécution du contrat intelligent.

9.2) La fonction *gestion de la politique de partage de données* notifie à la fonction *publication des informations sur le partage de données* que le contrat intelligent de partage de données a été exécuté. Cette notification comprend l'adresse d'exécution du contrat intelligent et les informations sur le partage de données.

9.3) La fonction *gestion de la politique de partage de données* notifie à la fonction *gestion des autorisations d'accès* que le contrat intelligent de partage de données a été exécuté. Cette notification comprend l'adresse d'exécution du contrat intelligent et l'autorisation d'accès.

9.4) La fonction *gestion des autorisations d'accès* stocke l'autorisation d'accès.

10) Une fois la notification envoyée par la fonction *gestion de la politique de partage de données* reçue, la fonction *publication des informations sur le partage de données* publie les nouvelles informations sur le partage de données reçues.

11) La fonction *publication des informations sur le partage de données* informe la fonction *abonnement aux informations sur le partage de données* que le contrat intelligent de partage de données a été exécuté. Cette notification comprend l'adresse d'exécution du contrat intelligent et les nouvelles informations sur le partage de données.

12) Une fois la notification envoyée par la fonction *publication des informations sur le partage de données* reçues, la fonction *abonnement aux informations sur le partage de données* envoie l'adresse d'exécution du contrat intelligent et les nouvelles informations sur le partage de données aux abonnés.

7.3.2 Procédure permettant aux consommateurs de données d'accéder aux données partagées compte tenu de l'autorisation demandée

La procédure permettant aux consommateurs de données d'accéder aux données partagées compte tenu de l'autorisation demandée est décrite dans la Figure 4.

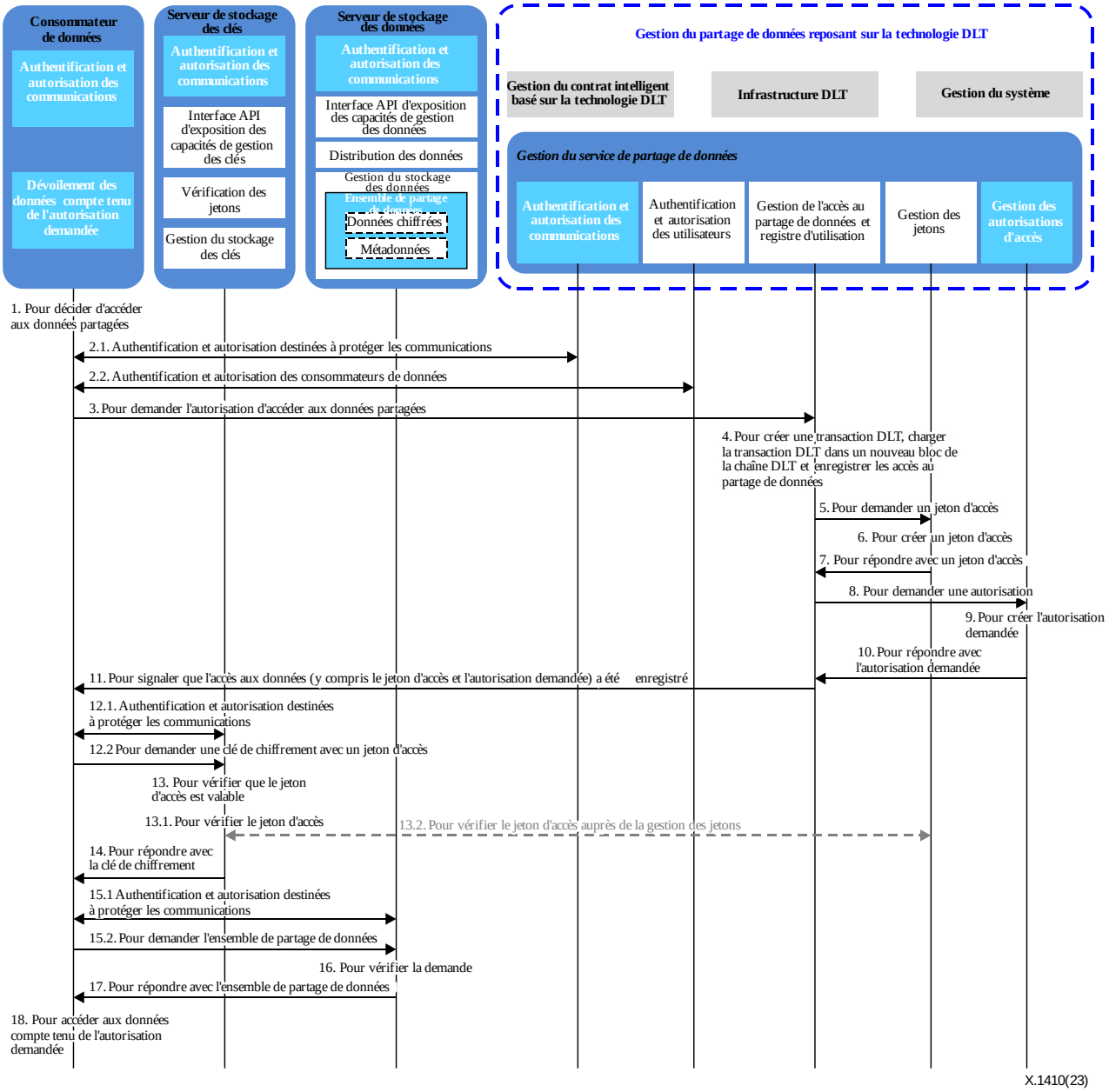

Figure 4 – Procédure permettant aux consommateurs de données d'accéder aux données partagées compte tenu de l'autorisation demandée

Comme indiqué dans la Figure 4, la procédure permettant aux consommateurs de données d'accéder aux données partagées compte tenu de l'autorisation demandée est la suivante:

1) Le *consommateur de données* obtient les informations sur le partage de données en recherchant la *publication des informations sur le partage de données*, en s'abonnant à la publication de ces informations ou en se faisant transférer ces informations par un tiers. Le consommateur de données décide d'accéder aux données partagées et exécute le contrat intelligent de partage de données.

2) Avant d'exécuter le contrat intelligent de partage de données pour accéder aux données partagées, les étapes ci-après doivent être suivies:

2.1) Le *consommateur de données* et la fonction *authentification et autorisation des communications* de la composante *gestion du service de partage de données* s'authentifient mutuellement et obtiennent une clé de session qui sera utilisée pour protéger les futures communications entre eux.

2.2) Le *consommateur de données* procède à l'authentification mutuelle avec la fonction *authentification et autorisation des utilisateurs* de la composante *gestion du service de partage de données*. Une fois l'authentification mutuelle réussie, la composante *authentification et autorisation des utilisateurs* vérifie que le consommateur de données ait le droit d'accéder aux données partagées.

3) Le *consommateur de données* envoie ses informations d'identité (par exemple l'identificateur, la clé publique) et les informations sur le partage de données ainsi que sa signature numérique à la fonction *gestion de l'accès au partage de données et registre d'utilisation*.

4) Une fois les informations d'identité, les informations sur le partage de données et la signature numérique du *consommateur de données* reçues, la fonction *gestion de l'accès au partage de données et registre d'utilisation* vérifie la signature numérique et s'assure que le consommateur de données est autorisé à accéder aux données compte tenu de la politique de partage de données (par exemple, seul un consommateur de données d'une entreprise ou d'un pays donné peut avoir accès aux données partagées). Si toutes les conditions d'accès aux données partagées sont réunies, la fonction *gestion de l'accès au partage de données et registre d'utilisation* crée une transaction DLT compte tenu des informations envoyées par le consommateur de données. La fonction *gestion de l'accès au partage de données et registre d'utilisation* envoie une ou plusieurs transactions DLT accompagnées de la signature numérique correspondante aux composantes sous-jacentes *infrastructure DLT* et *gestion du contrat intelligent basé sur la technologie DLT* pour créer un nouveau bloc contenant un ou plusieurs registres d'accès aux données. Le bloc nouvellement créé est distribué aux nœuds du réseau DLT associé. Le chargement des transactions DLT dans la chaîne DLT dépend de la technologie sous-jacente utilisée pour la mise en œuvre (par exemple Hyperledger Fabric, Ethereum Quorum), laquelle n'entre pas dans le champ d'application de la présente Recommandation.

5) La fonction *gestion de l'accès au partage de données et registre d'utilisation* demande à la fonction *gestion des jetons* de créer un jeton d'accès.

6) Une fois la notification envoyée par la fonction *gestion de l'accès au partage de données et registre d'utilisation* reçue, la fonction *gestion des jetons* crée un jeton d'accès.

7) La fonction *gestion des jetons* envoie le jeton d'accès créé à la fonction *gestion de l'accès au partage de données et registre d'utilisation*.

8) La fonction *gestion de l'accès au partage de données et registre d'utilisation* demande à la fonction *gestion des autorisations d'accès* de créer l'autorisation demandée.

9) Une fois la notification envoyée par la fonction *gestion de l'accès au partage de données et registre d'utilisation* reçue, la fonction *gestion des autorisations d'accès* crée l'autorisation demandée.

10) La fonction *gestion des autorisations d'accès* envoie l'autorisation demandée à la fonction *gestion de l'accès au partage de données et registre d'utilisation*.

11) Une fois le jeton d'accès et l'autorisation demandée reçus, la fonction *gestion de l'accès au partage de données et registre d'utilisation* enregistre l'utilisation des données partagées et envoie le jeton d'accès, l'autorisation demandée, les informations relatives à clé (par exemple l'identificateur et son adresse de stockage), les informations sur l'ensemble de partage de données (par exemple l'identificateur et son adresse de stockage), d'autres informations (par exemple les certificats numériques du *serveur de stockage des clés* et du *serveur de stockage des données*) au *consommateur de données*.

12) Une fois le jeton d'accès, l'autorisation demandée, les informations relatives à la clé et les informations sur l'ensemble de partage de données envoyés par la fonction *gestion de l'accès au partage de données et registre d'utilisation* reçus, le *consommateur de données* procède comme suit:

12.1) le *consommateur de données* et la fonction *authentification et autorisation des communications* du *serveur de stockage des clés* s'authentifient mutuellement et obtiennent une clé de session qui sera utilisée pour protéger les futures communications entre eux;

12.2) le *consommateur de données* envoie le jeton d'accès à la fonction *vérification des jetons* du *serveur de stockage des clés* compte tenu de l'adresse de stockage de la clé pour obtenir la clé de chiffrement.

13) La fonction *vérification des jetons* du *serveur de stockage des clés* vérifie que le jeton d'accès soit valable.

13.1) La fonction *vérification des jetons* du *serveur de stockage des clés* reçoit le jeton d'accès envoyé par le *consommateur de données* et vérifie ce jeton d'accès.

13.2) La fonction *vérification des jetons* peut, à titre d'option, être amenée à communiquer avec la fonction *gestion des jetons* de la fonction *gestion du partage de données reposant sur la technologie DLT* dans le cadre de la vérification du jeton d'accès.

14) La fonction *vérification des jetons* envoie le résultat de la vérification à la fonction *gestion du stockage des clés* du *serveur de stockage de la clé*. Une fois le résultat de la vérification envoyé par la fonction *vérification des jetons* reçu, la fonction *gestion du stockage des clés* du *serveur de stockage des clés* envoie la clé au *consommateur de données*.

15) Une fois la clé envoyée par la fonction *gestion du stockage des clés* du *serveur de stockage de la clé* reçue, le *consommateur de données* procède comme suit:

15.1) Le *consommateur de données* et la fonction *authentification et autorisation des communications* du *serveur de stockage des données* s'authentifient mutuellement et obtiennent une clé de session qui sera utilisée pour protéger les futures communications entre eux.

15.2) Le *consommateur de données* envoie une demande au *serveur de stockage des données* pour obtenir l'ensemble de partage de données.

16) Une fois la demande envoyée par le *consommateur de données* reçue, la fonction *distribution des données* du *serveur de stockage des données* authentifie le *consommateur de données*.

17) La fonction *distribution des données* du *serveur de stockage des données* envoie l'ensemble de partage de données au *consommateur de données*.

18) Le *consommateur de données* accède aux données compte tenu de l'autorisation demandée. Le *consommateur de données* chiffre les données partagées de la même manière que le *fournisseur de données* une fois que l'accès aux données prend fin.

Annexe A

Procédures de gestion du partage de données reposant sur la technologie DLT

(Cette Annexe fait partie intégrante de la présente Recommandation.)

On trouvera dans la présente annexe une description des deux principales procédures permettant: 1) au fournisseur de données de publier les données à partager à l'aide de la technologie DLT; 2) au consommateur de données d'accéder aux données partagées à l'aide de la technologie DLT.

Avant de procéder à la description des procédures de gestion du partage de données reposant sur la technologie DLT, on partira du principe que les conditions ci-dessous sont réunies:

– chaque utilisateur (par exemple le *fournisseur de données* et le *consommateur de données*) a obtenu un certificat numérique et la clé privée correspondante, générée automatiquement ou par une autorité de certification;
– chaque utilisateur a procédé aux bonnes configurations voulues (comme le certificat numérique du nœud DLT, les paramètres de connexion au réseau DLT, la mise à disposition du réseau);
– les utilisateurs (par exemple le fournisseur de données et le consommateur de données) ont accès à un système de chiffrement symétrique dont la puissance de chiffrement est suffisante pour garantir la confidentialité des données;
– les composantes *infrastructure DLT* et *gestion du contrat intelligent basé sur la technologie DLT* fonctionnent correctement;
– le réseau DLT fonctionne correctement;
– le *serveur de stockage des clés* et le *serveur de stockage des données* fonctionnent correctement.

A.1 Procédure permettant au fournisseur de données de publier les données à partager à l'aide de la technologie DLT

La procédure permettant au fournisseur de données de publier les données à partager à l'aide de la technologie DLT est décrite dans la Figure A.1.

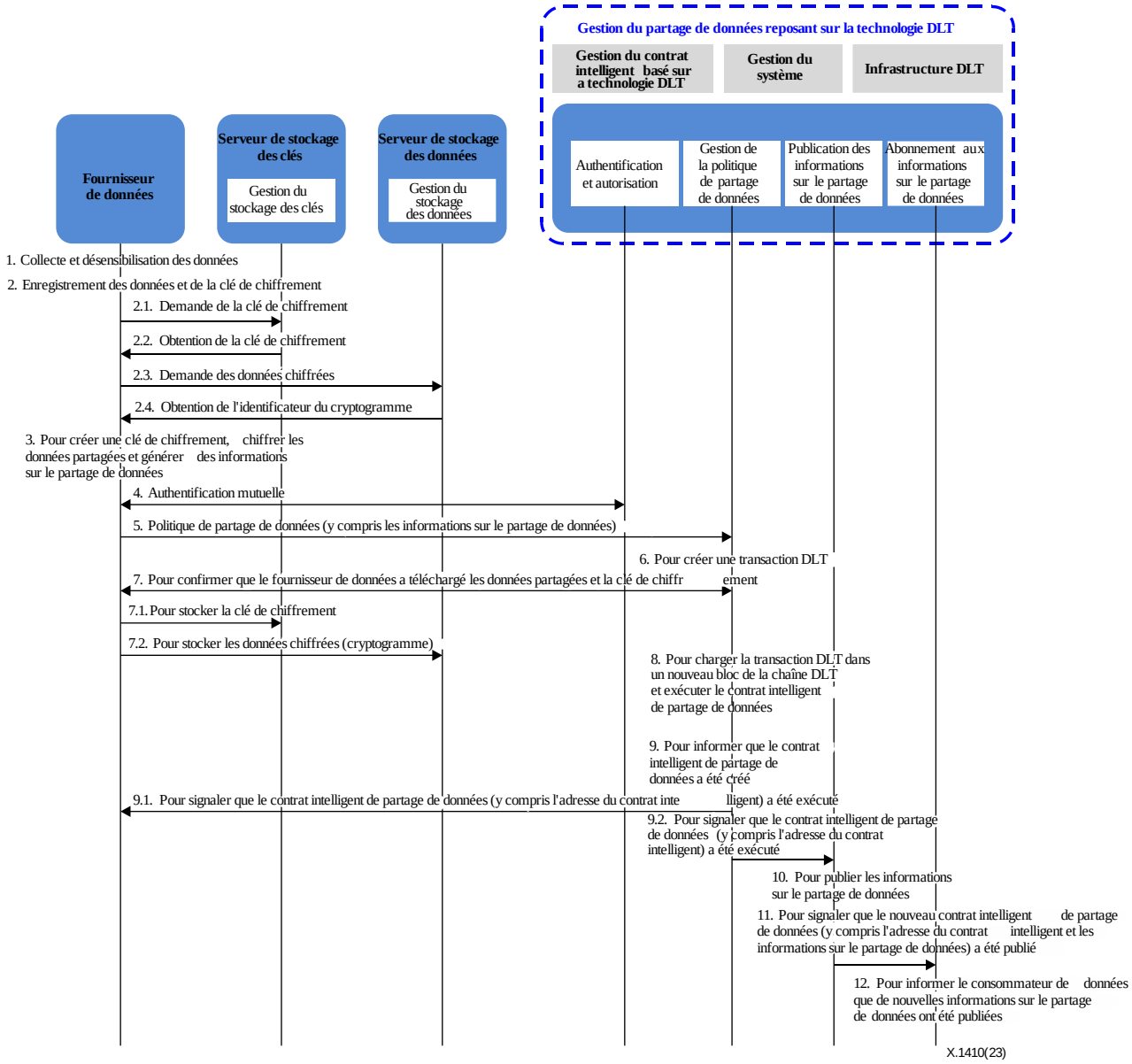

Figure A.1 – Procédure permettant au fournisseur d'accès de publier les données à partager à l'aide de la technologie DLT

Comme indiqué dans la Figure A.1, la procédure est la suivante:

1) Le *fournisseur de données* recueille les données d'origine et les désensibilise sans altérer la qualité des données à partager.

2) Le *fournisseur de données* enregistre les données à partager et la clé d'un système de chiffrement symétrique sur le serveur de stockage des clés et le serveur de stockage des données, locaux ou distants, comme suit:

   2.1) générer une clé de chiffrement des données utilisée pour un système de chiffrement symétrique;

   2.2) à partir du *serveur de stockage des clés*, le *fournisseur de données* obtient l'identificateur de la clé et son adresse de stockage;

   2.3) chiffrer les données avec la clé en utilisant le système de chiffrement symétrique, et enregistrer les données chiffrées, c'est-à-dire le cryptogramme;

   2.4) à partir du *serveur de stockage des données*, le *fournisseur de données* obtient l'identificateur du cryptogramme et son adresse de stockage.

3) Le *fournisseur de données* génère la clé de chiffrement des données et chiffre les données à partager à l'aide de la clé de chiffrement générée. Les données chiffrées constituent le cryptogramme. Le *fournisseur de données* crée des informations sur le partage de données, notamment l'identificateur et la clé publique du fournisseur de données, l'identificateur du cryptogramme et son adresse de stockage, l'identificateur de la clé de chiffrement des données et son adresse de stockage, les entreprises qui devront bénéficier d'une autorisation d'accès, les utilisateurs qui devront bénéficier d'une autorisation d'accès et d'autres attributs de données (par exemple la catégorie de données, une présentation des données, leur utilisation, le prix).

4) Avant de publier les données à partager, le *fournisseur de données* procède à l'authentification mutuelle avec la composante *authentification et autorisation des utilisateurs* de la *gestion du partage de données reposant sur la technologie DLT*. Un certificat numérique peut être utilisé à des fins d'authentification mutuelle. Une fois l'authentification mutuelle réussie, la composante *authentification et autorisation des utilisateurs* vérifie que le fournisseur de données ait le droit de publier les données à partager.

5) Une fois l'authentification et l'autorisation réussies, le *fournisseur de données* fournit les informations sur le partage de données compte tenu des spécifications de la fonction *gestion de la politique de partage de données* de la *gestion du partage de données reposant sur la technologie DLT*. Le *fournisseur de données* crée une politique de partage de données qui contient notamment des informations sur le partage de données. Le *fournisseur de données* envoie la politique de partage de données et la signature numérique correspondante à la fonction *gestion de la politique de partage de données*.

6) Une fois la politique de partage de données et la signature numérique correspondante envoyées par le *fournisseur de données* reçues, la fonction *gestion de la politique de partage de données* vérifie la signature numérique et crée une transaction DLT.

7) La fonction *gestion de la politique de partage de données* confirme auprès du *fournisseur de données* que la clé et le cryptogramme ont respectivement été stockés sur le *serveur de stockage des clés* et le *serveur de stockage des données*. Si tel n'est pas le cas, on procèdera comme suit:

   7.1) le *fournisseur de données* stocke la clé sur le *serveur de stockage des clés*;

   7.2) le *fournisseur de données* stocke le cryptogramme sur le *serveur de stockage des données*.

8) La fonction *gestion de la politique de partage de données* envoie une ou plusieurs transactions DLT accompagnées de la signature numérique correspondante aux composantes sous-jacentes *infrastructure DLT* et *gestion du contrat intelligent basé sur la technologie DLT* pour créer un nouveau bloc contenant un ou plusieurs contrats de partage de données. Le bloc nouvellement créé est distribué aux nœuds DLT associés. Le chargement des transactions DLT dans la chaîne DLT dépend de la technologie sous-jacente utilisée pour la mise en œuvre (par exemple Hyperledger Fabric, Ethereum Quorum), laquelle n'entre pas dans le champ d'application de la présente Recommandation.

9) La fonction *gestion de la politique de partage de données* informe les composantes concernées que le contrat intelligent de partage de données a été créé.

   9.1) La fonction *gestion de la politique de partage de données* notifie au *fournisseur de données* que le contrat intelligent de partage de données a été exécuté. Cette notification comprend l'adresse d'exécution du contrat intelligent.

   9.2) La fonction *gestion de la politique de partage de données* notifie à la fonction *publication des informations sur le partage de données* que le contrat intelligent de partage de données a été exécuté. Cette notification comprend l'adresse d'exécution du contrat intelligent et les informations sur le partage de données.

10) Une fois la notification envoyée par la fonction *gestion de la politique de partage de données* reçue, la fonction *publication des informations sur le partage de données* publie les nouvelles informations sur le partage de données reçues.

11) La fonction *publication des informations sur le partage de données* informe la fonction *abonnement aux informations sur le partage de données* que le contrat intelligent de partage de données a été exécuté. Cette notification comprend l'adresse d'exécution du contrat intelligent et les nouvelles informations sur le partage de données.

12) Une fois la notification envoyée par la fonction *publication des informations sur le partage de données* reçues, la fonction *abonnement aux informations sur le partage de données* envoie l'adresse d'exécution du contrat intelligent et les nouvelles informations sur le partage de données aux abonnés.

A.2 Procédure permettant au consommateur de données d'accéder aux données partagées à l'aide de la technologie DLT

La procédure permettant au consommateur de données d'accéder aux données partagées à l'aide de la technologie DLT est décrite dans la Figure A.2.

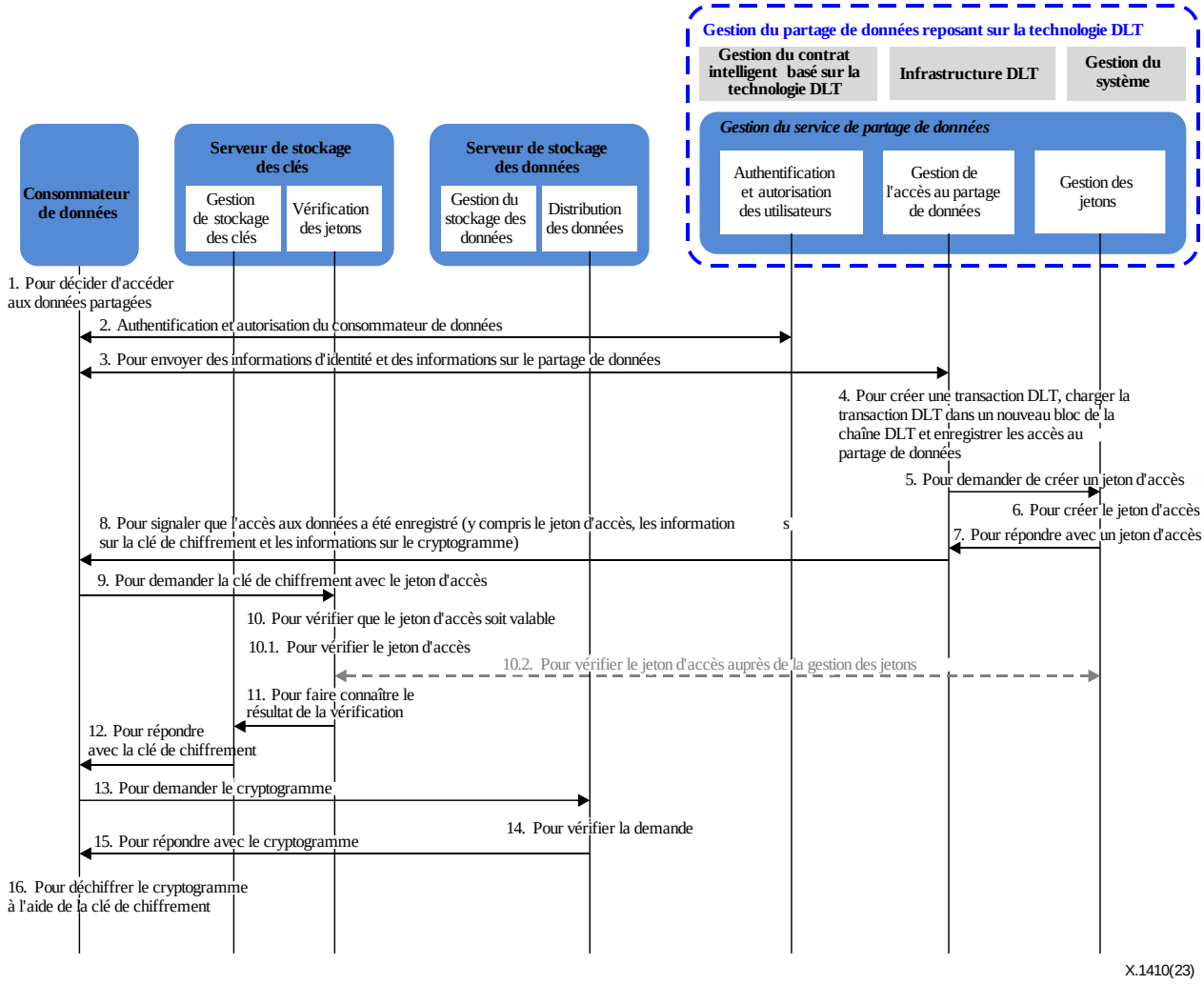

Figure A.2 – Procédure permettant au consommateur de données d'accéder aux données partagées à l'aide de la technologie DLT

Comme indiqué dans la Figure A.2, la procédure est la suivante:

1) Le *consommateur de données* obtient les informations sur le partage de données en recherchant la *publication des informations sur le partage de données*, en s'abonnant à la publication de ces informations ou en se faisant transférer ces informations par un tiers. Le consommateur de données décide d'accéder aux données partagées et exécute le contrat intelligent de partage de données.

2) Avant d'exécuter le contrat intelligent de partage de données pour accéder aux données partagées, le *consommateur de données* procède à l'authentification mutuelle avec la composante *authentification et autorisation des utilisateurs* de la *gestion du partage de données reposant sur la technologie DLT*. Il est recommandé d'utiliser un certificat numérique pour l'authentification mutuelle. Une fois l'authentification mutuelle réussie, la composante a*uthentification et autorisation des utilisateurs* vérifie que le consommateur de données ait le droit d'accéder aux données partagées.

3) Une fois l'authentification et l'autorisation réussies, le *consommateur de données* envoie ses informations d'identité (par exemple l'identificateur et sa clé publique), les informations sur le partage de données et sa signature numérique à la fonction *gestion de l'accès au partage de données*.

4) Une fois les informations d'identité, les informations sur le partage de données et la signature numérique du *consommateur de données* reçues, la fonction *gestion de l'accès au partage de données* vérifie la signature numérique et vérifie que le consommateur de données soit autorisé à accéder aux données compte tenu de la politique de partage de données (par exemple, seul un consommateur de données d'une entreprise ou d'un pays donné peut avoir accès aux données partagées). Si toutes les conditions d'accès aux données partagées sont réunies, la fonction *gestion de l'accès au partage de données* crée une transaction DLT compte tenu des informations envoyées par le consommateur de données. La fonction *gestion de l'accès au partage de données* envoie une ou plusieurs transactions DLT accompagnées de la signature numérique correspondante aux composantes sous-jacentes *infrastructure DLT* et *gestion du contrat intelligent basé sur la technologie DLT* pour créer un nouveau bloc contenant un ou plusieurs registres d'accès aux données. Le bloc nouvellement créé est distribué aux nœuds du réseau DLT associé. Le chargement des transactions DLT dans la chaîne DLT dépend de la technologie sous-jacente utilisée pour la mise en œuvre (par exemple Hyperledger Fabric, Ethereum Quorum), laquelle n'entre pas dans le champ d'application de la présente Recommandation.

5) La fonction *gestion de l'accès au partage de données* demande à la fonction *gestion des jetons* de créer un jeton d'accès.

6) Une fois la notification envoyée par la fonction *gestion de l'accès au partage de données* reçue, la fonction *gestion des jetons* crée un jeton d'accès.

7) La fonction *gestion des jetons* envoie le jeton d'accès créé à la fonction *gestion de l'accès au partage de données.*

8) Une fois le jeton d'accès reçu, la fonction *gestion de l'accès au partage de données* envoie le jeton d'accès, les informations relatives à la clé (par exemple l'identificateur et son adresse de stockage), les informations sur le cryptogramme (par exemple l'identificateur et son adresse de stockage) et d'autres informations (par exemple les certificats numériques du *serveur de stockage des clés* et du *serveur de stockage des données*) au *consommateur de données*.

9) Une fois le jeton d'accès, les informations relatives à la clé et les informations sur le cryptogramme envoyés par la fonction *gestion de l'accès au partage de données* reçus, le *consommateur de données* envoie le jeton d'accès à la fonction *vérification des jetons* du *serveur de stockage des clés* compte tenu de l'adresse de stockage de la clé pour obtenir le chiffrement, utilisé pour déchiffrer le cryptogramme.

10) La fonction *vérification des jetons* vérifie si le jeton d'accès est valable.

10.1) La fonction *vérification des jetons* du *serveur de stockage de la clé* reçoit le jeton d'accès envoyé par le *consommateur de données* et vérifie ce jeton d'accès.

10.2) La fonction *vérification des jetons* peut, à titre d'option, être amenée à communiquer avec la fonction *gestion des jetons* de la fonction *gestion du partage de données reposant sur la technologie DLT* dans le cadre de la vérification du jeton d'accès.

11) La fonction *vérification des jetons* envoie le résultat de la vérification à la fonction *gestion du stockage des clés*.

12) Une fois le résultat de la vérification envoyé par la fonction *vérification des jetons* reçu, la fonction *gestion du stockage des clés* envoie la clé de chiffrement au *consommateur de données*.

13) Une fois la clé de chiffrement envoyée par la fonction *gestion du stockage de la clé* reçue, le *consommateur de données* envoie une demande au *serveur de stockage des données* pour obtenir le cryptogramme.

14) Une fois la demande envoyée par le *consommateur de données* reçue, la fonction *distribution des données* du *serveur de stockage des données* authentifie le *consommateur de données*.

15) La fonction *distribution des données* du *serveur de stockage des données* envoie le cryptogramme au *consommateur de données*.

16) Le *consommateur de données* déchiffre le cryptogramme à l'aide de la clé de chiffrement puis accède aux données partagées en clair.

Bibliographie

[b-UIT-T X.509] Recommandation UIT-T X.509 (2019), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[b-UIT-T X.1400] Recommandation UIT-T X.1400 (2020), *Termes et définitions concernant la technologie des registres distribués*.

[b-UIT-T X.1402] Recommandation UIT-T X.1402 (2020), *Cadre de sécurité pour la technologie des registres distribués*.

[b-UIT-T FG DLT D1.1] Spécification technique UIT-T FG DLT D1.1 (2019), *Termes et définitions concernant la technologie des registres distribués*.

[b-ISO/CEI 18033-1] Recommandation ISO/CEI 18033-1(2021), *Sécurité de l'information – Algorithmes de chiffrement – Partie 1: Généralités.*

[b-ISO/CEI 20944-1] ISO/CEI 20944-1:2013, *Technologies de l'information – Interopérabilité et liaisons des registres de métadonnées (MDR-IB) – Partie 1: Cadre d'applications, vocabulaire commun et dispositions communes de conformité*.

[b-ISO/CEI 29100] ISO/CEI 29100: 2011, *Technologies de l'information – Techniques de sécurité – Cadre privé*.

[b-ISO/CEI/IEEE 15939] ISO/CEI/IEEE 15939:2017, *Ingénierie des systèmes et du logiciel – Processus de mesure*.

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-shared key ciphersuites for transport layer security (TLS)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet key exchange (IKEv2) protocol*.

[b-IETF RFC 4314] IETF RFC 4314 (2005), *IMAP4 access control list (ACL) extension*.

[b-IETF RFC 4949] IETF RFC 4949 (2007), *Internet security glossary, version 2*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol: Version 1.2*.

[b-IETF RFC 5782] IETF RFC 5782 (2010), *DNS blacklists and whitelists*.

[b-IETF RFC 5851] IETF RFC 5851 (2010), *Framework and requirements for an access node control mechanism in broadband multi-service networks*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Publié en Suisse
Genève, 2023