Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1752

(01/2022)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité des réseaux IMT-2020

Lignes directrices sur la sécurité pour l'infrastructure et la plate-forme de mégadonnées

Recommandation UIT-T X.1752

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	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile (1)	X.1140–X.1149
Sécurité des applications (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
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	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470-X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590-X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	**X.1750–X.1759**
Protection des données	X.1770-X.1789
SÉCURITÉ DES RÉSEAUX IMT-2020	X.1800–X.1819

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

Recommandation UIT-T X.1752

Lignes directrices sur la sécurité pour l'infrastructure et la plate-forme de mégadonnées

Résumé

La Recommandation UIT-T X.1752 contient une analyse des menaces et des problèmes de sécurité concernant l'infrastructure et la plate-forme de mégadonnées et décrit un cadre de référence pour la mise en correspondance des lignes directrices sur la sécurité et des menaces recensées pour l'infrastructure et la plate-forme de mégadonnées.

Historique

Édition	Recommandation	Approbation	Commission d'études*
1.0	UIT-T X.1752	07-01-2022	11.1002/1000/14806

Mots clés

Lignes directrices sur la sécurité, mégadonnées, infrastructure, plate-forme.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

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 responsables de la mise en œuvre 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.1752

Lignes directrices sur la sécurité pour l'infrastructure et la plate-forme de mégadonnées

1 Domaine d'application

La présente Recommandation décrit l'infrastructure et la plate-forme des mégadonnées en se fondant sur les activités de normalisation existantes sur les forums du secteur. Cette Recommandation définit une méthodologie d'évaluation des menaces et établit des lignes directrices de sécurité pour protéger l'infrastructure et la plate-forme de mégadonnées. Elle fournit également une cartographie mettant en correspondance les menaces et les lignes directrices en matière de sécurité.

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. Toutes les Recommandations et autres références étant sujettes 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. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T X.1279] Recommandation UIT-T X.1279 (2020), *Cadre de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité*.

[UIT-T X.1601] Recommandation UIT-T X.1601 (2015), *Cadre de sécurité applicable à l'informatique en nuage.*

[UIT-T X.1603] Recommandation UIT-T X.1603 (2018), *Exigences de sécurité des données pour le service de surveillance de l'informatique en nuage.*

[UIT-T X.1605] Recommandation UIT-T X.1605 (2020), *Exigences de sécurité pour les infrastructures en tant que service (IaaS) publiques dans l'informatique en nuage.*

[UIT-T Y.3600] Recommandation UIT-T Y.3600 (2015), *Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage.*

[UIT-T Y.3605] Recommandation UIT-T Y.3605 (2020), *Mégadonnées – Architecture de référence.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 contrôle d'accès [b-UIT-T X.800]: précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée.

3.1.2 audit [b-UIT-T X.800]: revue indépendante et examen des enregistrements et des activités du système afin de vérifier l'exactitude des contrôles du système pour s'assurer de leur concordance avec la politique de sécurité établie et les procédures d'exploitation, pour détecter les infractions à la sécurité et pour recommander les modifications appropriées des contrôles, de la politique et des procédures.

3.1.3 authentification [b-ISO/CEI 18014-2]: garantie donnée concernant l'identité d'une entité.

3.1.4 analyse des mégadonnées [b-UIT-T Y.2244]: contrôles effectués sur un volume important de données dans l'objectif d'obtenir des résultats significatifs, tels que des tendances ou des préférences.

3.1.5 désensibilisation des données [b-UIT-T X.1217]: processus consistant à dissimuler les données sensibles.

3.1.6 intégrité des données [b-UIT-T X.800]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.1.7 pare-feu [b-ISO/CEI 27033-1]: type de barrière de sécurité placée entre des environnements de réseau, qui se présente sous la forme d'un dispositif dédié ou d'un ensemble de plusieurs composants et techniques, à travers laquelle passe tout le trafic d'un environnement de réseau à un autre et vice versa. Seul le trafic autorisé défini dans le cadre d'une politique de sécurité locale est autorisé à passer.

3.1.8 équilibrage des charges [b-UIT-T Y.2052]: système permettant de séparer et d'équilibrer la charge de trafic afin d'utiliser efficacement les ressources du réseau (par exemple, largeur de bande de liaison).

3.1.9 système de détection des intrusions [b-ISO/CEI 27039]: systèmes d'information utilisés pour déterminer qu'une tentative d'intrusion a eu lieu ou qu'une intrusion est en cours ou a eu lieu.

3.1.10 système de prévention des intrusions [b-UIT-T X.1361]: variante des systèmes de détection des intrusions conçue précisément pour fournir une capacité de réponse active.

3.1.11 authentification multifacteur [b-UIT-T X.1158]: authentification au moyen de deux facteurs indépendants d'authentification au moins.

3.1.12 redondance [b-UIT-T E.800]: existence dans une entité de plus d'un moyen pour accomplir une fonction requise.

3.1.13 robustesse [b-UIT-T J.1014]: propriété de la mise en œuvre d'une fonction sécurisée ECI particulière, qui représente l'effort ou le coût à engager pour compromettre la sécurité de cette fonction.

3.1.14 paramètre de configuration de la sécurité [b-UIT-T X.1046]: ensemble de paramètres décrivant les caractéristiques de la fonction de sécurité, telles que la largeur de bande minimale, le nombre maximum de connexions, etc. prises en charge par la fonction de sécurité, l'objet protégé et les activités de sécurité de la fonction de sécurité.

3.1.15 signature unique [b-UIT-T Y.2201]: aptitude à utiliser une signature unique pour passer d'un opérateur de réseau/fournisseur de services à un autre opérateur/fournisseur de service dans le cas d'un utilisateur accédant à un service ou en itinérance dans un réseau visité.

3.1.16 menace [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

3.1.17 validation [b-UIT-T Z.450]: processus de vérification d'une spécification consistant à vérifier qu'elle est correcte sur le plan de la syntaxe et de la sémantique et qu'elle représente le comportement voulu.

3.1.18 vulnérabilité [b-UIT-T X.1524]: toute faille dans le logiciel qui peut être exploitée pour violer un système ou les informations qu'il contient.

3.1.19 liste blanche [b-UIT-T X.1245]: liste de personnes ou de sources utilisant des services de communication qui sont connus, fiables ou bénéficient d'une autorisation explicite.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 infrastructure de mégadonnées: système composé de dispositifs physiques de base et d'un environnement réseau dans un écosystème de mégadonnées visant à fournir des services de mégadonnées pour la collecte de données, le traitement de données, la gestion de données, etc.

3.2.2 plate-forme de mégadonnées: système ou ensemble de systèmes distribués dans un écosystème de mégadonnées visant à fournir des services d'analyse de données, de visualisation des données et autres fonctions.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

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

BDAP fournisseur d'applications de mégadonnées (*big data application provider*)

BDIP fournisseur d'infrastructure de mégadonnées (*big data infrastructure provider*)

DOS déni de service (*denial of service*)

DDOS déni de service réparti (*distributed denial of service*)

IAM gestion d'identité et d'accès (*identity and access management*)

IDS système de détection des intrusions (*intrusion detection system*)

IP protocole Internet (*Internet protocol*)

IPS système de prévention des intrusions (*intrusion prevention system*)

SSO authentification unique (*single sign-on*)

VM machine virtuelle (*virtual machine*)

5 Conventions

Dans la présente Recommandation:

L'expression "il est recommandé" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire.

6 Menaces et enjeux de sécurité recensés pour l'infrastructure et la plate-forme de mégadonnées

Conformément à la définition de la Recommandation [UIT-T Y.3600] et à la Figure 6-1 (c'est-à-dire, adaptée de la Figure 7-1 de [UIT-T Y.3600]), la plate-forme de mégadonnées est fournie par un fournisseur d'applications de mégadonnées (BDAP) pour réaliser l'analyse des données, la visualisation des données, ainsi que d'autres fonctions. L'infrastructure des mégadonnées est fournie par un fournisseur d'infrastructure de mégadonnées (BDIP) afin d'exécuter les services de mégadonnées y compris la collecte des données, le traitement des données, la gestion des données, etc.

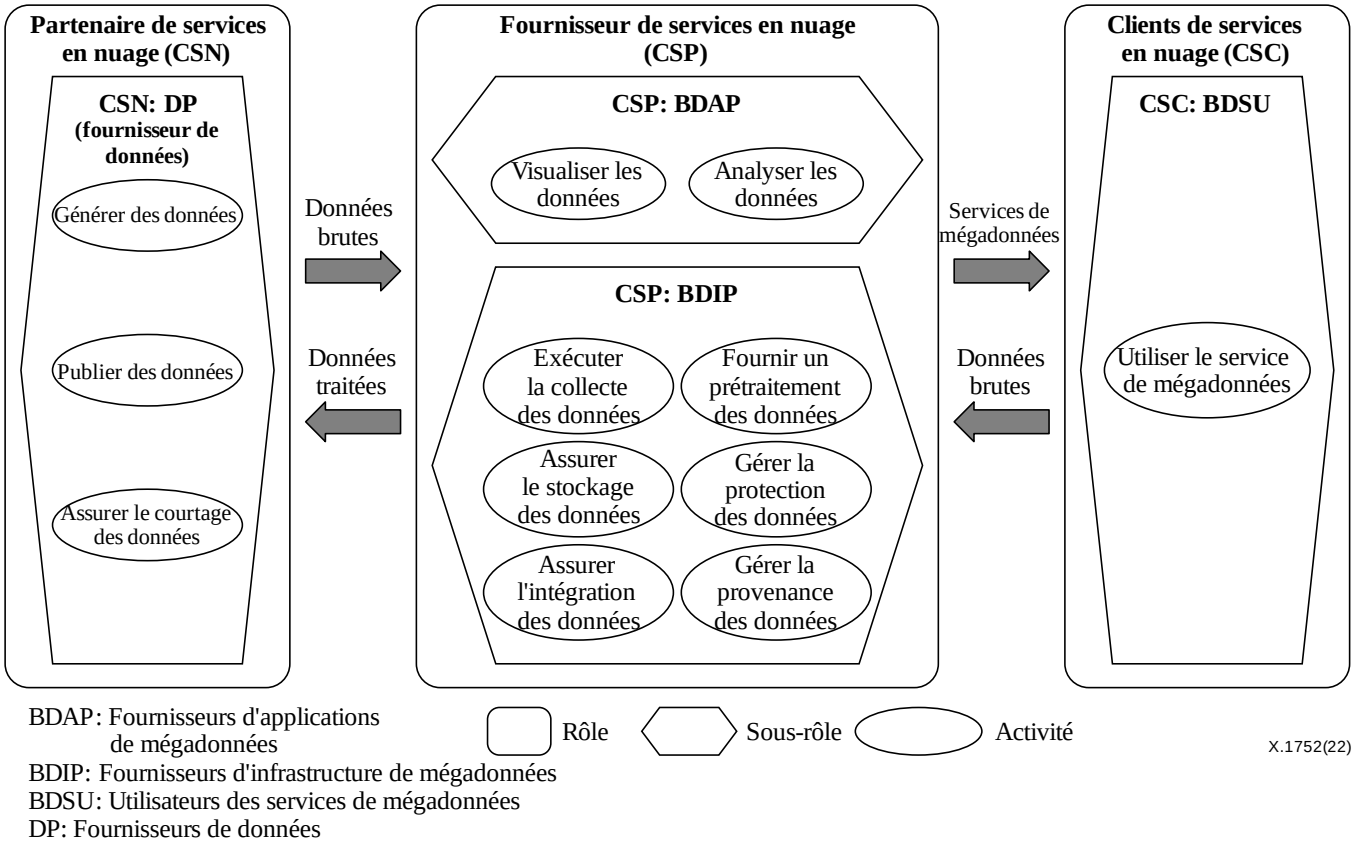

Figure 6-1 – Système de mégadonnées basées sur l'informatique en nuage

6.1 Enjeux et menaces de sécurité recensés pour l'infrastructure de mégadonnées

Les menaces et enjeux de sécurité recensés pour l'infrastructure des mégadonnées comprennent les menaces et enjeux de sécurité pesant sur la collecte des données, le stockage des données, l'intégration des données, le prétraitement des données et la gestion des données.

6.1.1 Enjeux et menaces de sécurité recensés pour la collecte des données

S'agissant de la sécurité lors de la collecte des données, les menaces et enjeux de sécurité comprennent:

a) la collecte de données sans autorisation: des auteurs d'attaques pourraient collecter les données sans permission ni autorisation;

b) la vulnérabilité de l'interface de collecte de données: des auteurs d'attaque pourraient utiliser la vulnérabilité de l'interface de collecte des données pour accéder au processus de collecte des données et entraîner une perte de données;

c) l'accès non autorisé aux fonctions d'administration: l'accès non autorisé aux fonctions d'administration au système de collecte de données pourrait entraîner la perte de données. L'auteur d'une attaque pourrait, par exemple, exploiter une vulnérabilité du système pour obtenir un accès non autorisé aux fonctions d'administration du système de collecte des données et remplacer l'adresse IP de destination de la collecte des données par sa propre adresse IP.

6.1.2 Enjeux et menaces de sécurité recensés pour le stockage des données

S'agissant de la sécurité du stockage des données, les menaces et enjeux de sécurité comprennent:

a) l'absence de gestion appropriée des informations cryptographiques, comme les clés de chiffrement, les codes d'authentification et le privilège d'accès, pourrait entraîner des préjudices considérables, tels que la perte de données ou une fuite inattendue de données vers l'extérieur. En outre, la convergence massive de données provenant de sources multiples augmente la difficulté de contrôler l'accès au stockage de données. La complexité des scénarios de stockage et de circulation des mégadonnées rend la mise en œuvre du chiffrement des données difficile;

b) l'indisponibilité des services: un serveur de stockage des données peut être visé par une attaque par déni de service (DoS) ou par déni de service réparti (DDoS); de plus, ces attaques peuvent entraîner une défaillance du matériel de stockage des données et, de ce fait, la perte ou la destruction de données;

c) des menaces et enjeux de sécurité pour les installations physiques de stockage des données: s'agissant des installations physiques, elles sont confrontées aux mêmes menaces et enjeux de sécurité que ceux détaillés au paragraphe 9.3 de la Recommandation [UIT-T X.1601] et au paragraphe 7 de la Recommandation [UIT-T X.1605];

d) des menaces et enjeux de sécurité portant sur le terminal de stockage de données: s'agissant du terminal de stockage de données, les menaces et enjeux de sécurité se concentrent sur les paramètres de configuration de sécurité des terminaux matériel et logiciel qui comprennent les paramètres de configuration de sécurité du système d'exploitation, le logiciel de bureau, le navigateur, le système de messagerie, etc. Les menaces et enjeux de sécurité principaux regroupent un faux jeu de paramètres de configuration de la sécurité, des mises à jour tardives des paramètres de configuration de la sécurité, des vulnérabilités des paramètres de configuration de la sécurité, etc.

6.1.3 Enjeux et menaces de sécurité recensés pour l'intégration des données

S'agissant de la sécurité de l'intégration des données, les menaces et enjeux de sécurité comprennent:

a) l'utilisation abusive des données: les données peuvent être déplacées entre différents emplacements physiques. Il est primordial de prendre des mesures pour prévenir l'utilisation abusive des données lors de la transmission des données vers différents emplacements;

b) l'usurpation d'identité: telle que définie dans [UIT-T X.1279], l'usurpation d'identité est la prétention supposée par une entité d'être une entité différente, en présentant une image enregistrée ou un autre échantillon de données biométriques, ou une caractéristique biométrique artificiellement reproduite, afin d'usurper l'identité d'un individu. Des auteurs d'attaques peuvent se substituer au système de gestion ou au serveur de stockage des données et provoquer la perte ou l'utilisation abusive de données lors de la phase d'intégration;

c) les menaces sur la sécurité des réseaux au cours de la phase d'intégration des données: ces menaces et enjeux de sécurité sont similaires à ceux mentionnés au paragraphe 9.5 de [UIT-T X.1601]. En outre, les enjeux particuliers en matière de sécurité de l'infrastructure de mégadonnées sont axés sur la gestion intégrée de la sécurité dans les réseaux physiques, les réseaux virtuels et les environnements en nuage.

6.1.4 Enjeux et menaces de sécurité recensés pour le prétraitement des données

S'agissant de la sécurité du prétraitement des données, les menaces et enjeux de sécurité comprennent:

a) des menaces internes: un employé du fournisseur d'applications de mégadonnées BDAP pourrait détourner les données à des fins autres que celles auxquelles elles sont destinées au cours de la phase de prétraitement des données sans l'autorisation de l'utilisateur;

b) la vulnérabilité du système: des données peuvent être perdues lors de la phase de prétraitement en raison de vulnérabilités du système.

6.1.5 Enjeux et menaces de sécurité recensés pour la gestion des données

S'agissant de la sécurité pesant sur la gestion des données, les menaces et enjeux de sécurité comprennent:

a) les vulnérabilités logicielles: de possibles vulnérabilités en matière de sécurité du logiciel utilisé dans la gestion des mégadonnées pourraient être exploitées par des auteurs d'attaques. Les défauts techniques de la virtualisation du système pourraient présenter plusieurs risques sur le plan de la sécurité; en outre, ces risques pourraient être aggravés si les techniques d'exploitation et de maintenance ne sont pas suffisamment au point. En outre, les modèles de stockage et de calcul d'infrastructure et de plate-forme de mégadonnées entraînent des risques plus élevés au niveau des paramètres de configuration de la sécurité sur le logiciel utilisé dans la gestion des mégadonnées;

b) la violation de contrôle d'accès: la violation de contrôle d'accès pour la gestion des données peut entraîner la perte, la fuite ou l'utilisation abusive de données;

c) l'accès non autorisé aux fonctions d'administration: l'accès non autorisé aux fonctions d'administration du système de gestion des mégadonnées pourrait entraîner la perte, la fuite ou l'utilisation abusive de données. L'auteur d'une attaque peut, par exemple, exploiter une vulnérabilité du système pour obtenir un accès non autorisé aux fonctions d'administration du système de gestion des mégadonnées et remplacer l'adresse IP de destination de la collecte des données par sa propre adresse IP;

d) menaces internes: les utilisateurs négligents ou mal formés (ou les membres d'une famille dans le cas d'une configuration chez des particuliers) ou encore des actions malveillantes de la part d'employés mécontents, représenteront toujours une menace importante.

6.2 Enjeux et menaces de sécurité recensés pour la plate-forme des mégadonnées

Les enjeux et menaces de sécurité recensés pour la plate-forme des mégadonnées comprennent ceux pesant sur la visualisation et l'analyse des données.

6.2.1 Enjeux et menaces de sécurité recensés pour l'analyse des données

S'agissant de la sécurité pesant sur l'analyse des données, les menaces et enjeux de sécurité incluent notamment:

a) la vulnérabilité du système: des données peuvent être perdues en raison d'une vulnérabilité du système d'analyse des données;

b) l'attaque par déni de service: un serveur d'analyse des données peut être visé par une attaque DoS ou DDoS;

c) l'utilisation partagée des applications d'analyse des données: les applications d'analyse des données sont normalement utilisées par différents utilisateurs, qui peuvent entraîner des évasions de machines virtuelles (VM), des fuites de données, etc.;

d) l'accès non sécurisé: l'accès non sécurisé à l'analyse des mégadonnées pourrait entraîner la perte, la fuite ou l'utilisation abusive de données des applications;

e) l'accès non autorisé aux fonctions d'administration: l'accès non autorisé aux fonctions d'administration de l'analyse des mégadonnées pourrait conduire à une perte de données.

6.2.2 Enjeux et menaces de sécurité recensés pour la visualisation des données

S'agissant de la sécurité pesant sur la visualisation des données, les menaces et enjeux de sécurité incluent notamment:

a) l'utilisation abusive des données: les données peuvent être utilisées de façon abusive (ou présentées sans la permission de l'utilisateur) par le fournisseur d'applications de mégadonnées lors de la visualisation des données;

b) la vulnérabilité du système: des données de rapports et des données d'analyse peuvent être perdues en raison d'une vulnérabilité du système de visualisation des données;

c) la représentation erronée: les données peuvent être représentées de façon erronée lors de la visualisation des données sans la permission de l'utilisateur en raison d'un accès défaillant aux politiques de contrôle d'accès.

7 Lignes directrices sur la sécurité relatives à l'infrastructure et à la plate-forme de mégadonnées

Selon la définition de la norme [UIT-T Y.3605], le cadre relatif à l'organisation en couche utilisé dans l'architecture de référence des mégadonnées comprend quatre couches, assorties d'un ensemble de fonctions qui s'étendent à l'ensemble des couches. Ces quatre couches sont:

– la couche d'accès;

– la couche d'application;

– la couche de traitement; et

– la couche source de données.

Les fonctions qui s'étendent à l'ensemble des couches sont appelées fonctions multicouches.

Le cadre relatif à l'organisation en couches est présenté à la Figure 7-1 (c'est-à-dire, adaptée de la Figure 8-2 de [UIT-T Y.3605]).

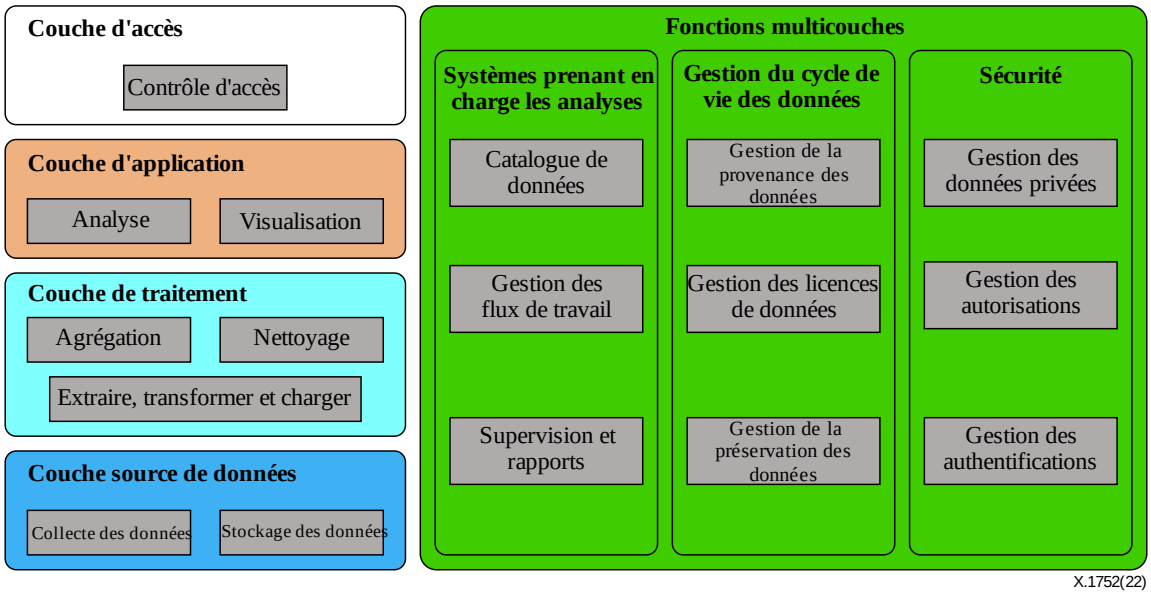

Figure 7-1 – Cadre relatif à l'organisation en couches des mégadonnées

A l'appui du cadre relatif à l'organisation en couches présenté à la Figure 7-1, la présente Recommandation utilise une architecture telle que présentée à la Figure 7-2 pour la sécurité de l'infrastructure et de la plate-forme des mégadonnées.

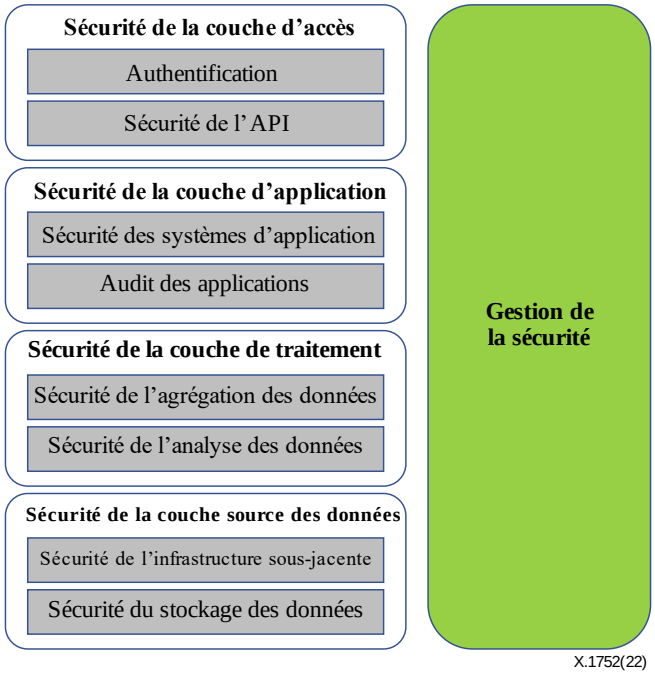

Figure 7-2 – Architecture destinée à la sécurité de l'infrastructure et de la plate-forme des mégadonnées

La présente Recommandation énonce les lignes directrices de sécurité relatives à l'infrastructure et à la plate-forme de mégadonnées suivantes:

a) lignes directrices de sécurité relatives à la couche source de données;

b) lignes directrices de sécurité relatives à la couche de traitement;

c) lignes directrices de sécurité relatives à la couche d'application;

d) lignes directrices de sécurité relatives à la couche d'accès;

e) lignes directrices relatives à la gestion de la sécurité.

7.1 Lignes directrices de sécurité relatives à la couche source de données

Les lignes directrices de sécurité relatives à la couche source de données sont axées sur la sécurité de l'infrastructure sous-jacente et la sécurité du stockage des données.

7.1.1 Les lignes directrices de sécurité relatives à l'infrastructure sous-jacente

Les lignes directrices de sécurité relatives à l'infrastructure sous-jacente sont les suivantes:

a) Il est recommandé de subdiviser les infrastructures virtuelles en domaines de sécurité interne et externe et de mettre en œuvre des politiques de sécurité sur demande. Il est recommandé de fournir des mécanismes d'isolement efficace entre les domaines de sécurité interne et externe.

b) Il est recommandé de mettre en œuvre des politiques de contrôle d'accès strictes entre les domaines de sécurité des infrastructures virtuelles. Il est recommandé d'utiliser le principe du moindre privilège, ainsi, l'authentification et l'autorisation des utilisateurs sont attribuées en fonction des responsabilités des rôles pour permettre le contrôle de l'accès aux infrastructures virtuelles.

c) Il est recommandé de mettre en œuvre des logiciels de sécurité, tels que des logiciels antivirus, sur les infrastructures virtuelles afin de renforcer la protection de la sécurité, et de mettre à jour périodiquement les bases de données de virus et de codes malveillants.

d) Il est recommandé de mettre en œuvre des équipements de détection et de protection contre les attaques réseau, par exemple un système de prévention des intrusions (IPS)/un système de détection des intrusions (IDS), un pare-feu, une protection contre les attaques par déni de service (DDoS), etc., à la frontière entre les réseaux internes et externes, et de mettre régulièrement à jour les bases de données de signatures d'attaques.

e) Il est recommandé de mettre en œuvre des politiques d'isolement et de contrôle d'accès strictes aux frontières des réseaux internes et externes afin d'empêcher les accès non autorisés aux infrastructures sous-jacentes.

f) Il est recommandé de surveiller le trafic réseau des infrastructures sous-jacentes et d'effectuer des inspections approfondies, y compris des informations clés telles que les statistiques de flux réseau, le trafic réseau anormal, etc.

g) Il est recommandé d'afficher les informations relatives aux attaques, telles que le type d'attaque, les adresses IP source/destination, l'horodatage, etc. lorsque des attaques ont été détectées.

h) Il est recommandé de procéder à une surveillance centralisée de la sécurité en temps réel, qui comprend l'état de fonctionnement de diverses ressources physiques et virtuelles.

7.1.2 Lignes directrices de sécurité relatives au stockage des données

Les lignes directrices de sécurité portant sur le stockage des données sont les suivantes:

a) Il est recommandé de mettre en œuvre des composants de stockage de données sécurisés, tels qu'un système de fichiers distribué sécurisé, un stockage indexé sécurisé, etc. afin d'assurer la sécurité de l'environnement de stockage.

b) Il est recommandé de prendre en charge des stratégies d'isolement pour les données de différents utilisateurs dans un environnement multi-locataires.

c) Il est recommandé de formuler des politiques de sécurité et des règles de gestion du stockage des données, telles que la politique de contrôle d'accès, la politique de transmission sécurisée des données, la politique d'intégrité des données, la politique de cohérence des copies multiples, la politique de chiffrement des informations personnelles et des données essentielles, etc.

d) Il est recommandé de prendre en charge une variété de mécanismes de désensibilisation des données.

e) Il est recommandé de prendre en charge le chiffrement du système de fichiers, afin d'éviter la corruption et la fuite des données. Il est en outre nécessaire de prendre en charge les chiffrements classés en fonction des niveaux de sensibilité des données: pas de chiffrement, chiffrement partiel, chiffrement complet, etc.

f) Il est recommandé de fournir des fonctions de détection des atteintes à l'intégrité des données de stockage et de restauration de l'intégrité des données après endommagement.

g) Il est recommandé de prendre en charge les paramètres de configuration de sécurité facultatifs du chiffrement que les utilisateurs peuvent choisir.

h) Il est recommandé de fournir une aide aux utilisateurs lors du choix du mécanisme de chiffrement d'une tierce partie pour chiffrer les données essentielles.

i) Il est recommandé de prendre en charge le chiffrement des données au moyen de clés sécurisées et de veiller au stockage et à la conservation de ces clés au niveau local.

j) Il est recommandé de prendre en charge un algorithme de chiffrement approprié pour la sauvegarde à long terme des supports de stockage (archivage), par exemple utiliser de longues clés de chiffrement et planifier le remplacement par un algorithme de chiffrement amélioré.

k) Il est recommandé de définir l'opportunité et les droits de partage des données, d'autorisation d'utilisation des données et de suppression des données.

l) Il est recommandé d'autoriser la période de validité de l'utilisation des données et de notifier les fournisseurs et les utilisateurs de mégadonnées associés.

m) Il est recommandé de prendre en charge les fonctions de suppression, de sauvegarde et de récupération des données.

7.2 Lignes directrices de sécurité relatives à la couche de traitement

Les lignes directrices de sécurité portant sur la couche de traitement sont axées sur la sécurité de l'agrégation des données et la sécurité de l'analyse des données.

7.2.1 Lignes directrices de sécurité relatives à l'agrégation des données

Les lignes directrices de sécurité relatives à l'agrégation des données sont les suivantes:

a) Il est recommandé que les composants d'agrégation de données prennent en charge un mécanisme d'authentification, et le terminal de la source de données et les opérateurs de la plate-forme de données volumineuses doivent être authentifiés et autorisés.

b) Il est recommandé de mettre en œuvre des règles de sécurité strictes dans le processus de regroupement des données, qui comprend la classification, la transmission et le stockage temporaire.

c) Il est recommandé que les différentes sources de données établissent une stratégie de classification des données avec une politique de gestion de la sécurité correspondante, qui doit couvrir le processus de transmission et de stockage temporaire. Pour chaque catégorie de sources de données, il est recommandé que la politique de gestion de la sécurité correspondante soit définie selon des critères de confidentialité, d'intégrité et de disponibilité.

d) Il est recommandé de prendre en charge les fonctions de contrôle d'accès restreint au dossier de stockage temporaire dans le processus d'agrégation des données, afin d'interdire l'accès à des processus ou à des données d'utilisateurs indésirables, ainsi que la modification non autorisée de l'adresse de stockage des composants d'agrégation des données.

e) Il est recommandé de fournir des fonctions d'équilibrage de charge pour les composants d'agrégation de données, de sorte que la pression de charge d'un flux de données important puisse être soulagée par plusieurs canaux.

f) Il est recommandé de fournir des fonctions de détection et de protection telles qu'un système de prévention ou de détection des intrusions (IPS/IDC) pour les composants d'agrégation de données, afin de pouvoir restreindre la collecte excessive ou indésirable de données.

g) Il est recommandé de prévoir des mécanismes de reprise sur défaillance et de récupération pour les composants d'agrégation de données, afin que les flux de données transmis puissent être transférés à un composant de secours.

h) Il est recommandé de fournir une journalisation pour l'agrégation des données et de transmettre des alertes en cas de situation anormale, notamment si les données ont été collectées de manière répétée, si les flux de données ont dépassé le seuil fixé, si les flux de données ont été interrompus ou si le plafond de stockage des données collectées a été dépassé.

7.2.2 Lignes directrices de sécurité relatives à l'analyse des données

Les lignes directrices de sécurité relatives à l'analyse des données sont les suivantes:

a) Il est recommandé de fournir des méthodes d'authentification pour s'assurer que seuls les utilisateurs ou les applications légitimes peuvent lancer des demandes d'analyse de données.

b) Il est recommandé de mettre en œuvre un module de contrôle d'accès pour l'analyse des données conformément à la politique d'identification des utilisateurs de mégadonnées et à la politique d'authentification des utilisateurs, y compris la gestion et la validation du respect des délais du contrôle d'accès, le mécanisme de validation de la légalité de l'accès aux données.

c) Il est recommandé de prendre en charge l'audit de sécurité portant sur l'analyse des données distribuées, les informations d'audit devant être stockées et contrôlées à titre conservatoire.

d) Il est recommandé de fournir un mécanisme de désensibilisation pour maintenir la sécurité et la robustesse de l'analyse des données, sachant que l'utilisation du mécanisme de désensibilisation ne doit pas affecter la continuité des activités ni affecter fortement la performance du système.

e) Il doit être possible de définir différents mécanismes de désensibilisation en fonction des demandes des différents utilisateurs et des différentes données.

f) Il est recommandé de pouvoir configurer l'algorithme de désensibilisation après une demande ou une requête des utilisateurs.

g) Il est recommandé que les mécanismes de désensibilisation puissent être ajoutés ou supprimés de manière dynamique, ce qui permettrait une mise à niveau du système en toute fluidité, sans interruption de l'activité.

7.3 Lignes directrices de sécurité relatives à la couche d'application

Les lignes directrices de sécurité relatives à la couche d'application sont axées sur le système de l'application et la vérification de l'application.

7.3.1 Lignes directrices de sécurité relatives au système des applications

Les lignes directrices de sécurité relatives au système des applications sont les suivantes:

a) Il est nécessaire de mettre en place des méthodes de détection et de protection du système des applications, telles que pare-feu, système antivirus, système de détection des intrusions/systèmes de prévention des intrusions (IDS/IPS).

b) Il est recommandé de mettre en place des mesures de protection contre les vulnérabilités du système des applications.

c) Il est recommandé de fournir des méthodes d'authentification pour empêcher l'accès non autorisé au système des applications.

d) Il est recommandé de maintenir une isolation entre les différentes applications, afin d'éviter les fuites de données causées par des analyses d'association de données lancées par différentes applications.

7.3.2 Lignes directrices de sécurité relatives à l'audit des applications

Les lignes directrices de sécurité relatives à l'audit des applications sont les suivantes:

a) Il est recommandé d'auditer les opérations réalisées par les administrateurs sur les applications, ce qui pourrait permettre de localiser des événements et d'extraire des preuves pour les incidents de sécurité.

b) Il est recommandé d'auditer les opérations réalisées par les utilisateurs sur les applications afin de favoriser la détection, l'alerte et la réponse rapide aux comportements malveillants.

c) Il est recommandé d'auditer la modification des paramètres de configuration de la sécurité concernant les alertes, la réponse rapide aux comportements malveillants, etc.

7.4 Lignes directrices de sécurité relatives à la couche d'accès

Les directives de sécurité relatives à la couche d'accès sont axées sur le mécanisme d'authentification et l'interface de programmation d'application (API).

7.4.1 Lignes directrices de sécurité relatives au mécanisme d'authentification

Les lignes directrices de sécurité relatives au mécanisme d'authentification sont les suivantes:

a) Il est recommandé de prendre en charge des services d'authentification améliorés, tels que l'authentification par authentification unique (SSO), l'authentification multifactorielle, etc.

b) Il est recommandé d'appliquer des politiques de mots de passe forts, comme l'augmentation de la complexité des mots de passe, la mise à jour régulière des mots de passe, etc.

c) Il est recommandé de prendre en charge le mécanisme d'authentification par liste blanche, tel que la liste blanche des adresses IP, etc.

7.4.2 Lignes directrices de sécurité relatives à l'interface de programmation d'application (API)

Les lignes directrices de sécurité relatives à l'interface de programmation d'application (API) sont les suivantes:

a) Il est recommandé de permettre aux administrateurs d'autoriser l'accès aux API, par exemple en configurant le nombre maximal d'accès aux API par un utilisateur, le nombre total de connexions que les API peuvent prendre en charge, etc.

b) Il est recommandé de prendre en charge les caractéristiques de surveillance en temps réel des flux réseau entre les clients et les interfaces API, de générer des alertes et de permettre une réponse aux incidents en cas de trafic réseau anormal.

c) Il est nécessaire de valider l'entrée des API pour éviter diverses attaques de sécurité.

d) Il est recommandé de prendre en charge le transfert de données essentielles sur un canal sécurisé, par exemple via un canal chiffré, etc.

e) Il est recommandé d'appliquer l'examen et la désensibilisation de manière bidirectionnelle entre les clients et les API avant le transfert des données.

f) Il est recommandé de prendre en charge la vérification de l'intégrité des données et de détecter la corruption ou la perte de données pendant les transmissions.

7.5 Lignes directrices de sécurité relatives à la gestion de la sécurité

Les lignes directrices de sécurité relatives à la gestion de la sécurité sont les suivantes:

a) Il est recommandé d'utiliser la gestion d'identité et d'accès (IAM) et l'audit du contrôle d'accès, notamment les dossiers d'exploitation et de maintenance, les journaux d'accès aux données, l'inspection du comportement d'accès, la gestion des clés et le chiffrement des données.

b) Il est recommandé d'utiliser des mécanismes de détection et de protection rationnels et efficaces, notamment la redondance de l'infrastructure de sécurité, l'analyse de la vulnérabilité, les systèmes de prévention des intrusions IPS / les systèmes de détection des intrusions IDS, les pare-feu et les dispositifs de sécurité de la virtualisation.

c) Il est recommandé d'utiliser des techniques de renforcement de la sécurité pour réduire la surface d'exposition aux attaques de l'infrastructure et de la plate-forme.

d) Il est recommandé de mettre régulièrement à jour les correctifs et les versions de l'infrastructure et de la plate-forme des mégadonnées.

Bibliographie

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[b-UIT-T X.810] Recommandation UIT-T X.810 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadre de sécurité pour les systèmes ouverts: Présentation générale*.

[b-UIT-T X.1158] Recommandation UIT-T X.1158 (2014), *Mécanismes d'authentification à plusieurs facteurs utilisant un dispositif mobile*.

[b-UIT-T X.1217] Recommandation UIT-T X.1217 (2021), *Lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication.*

[b-UIT-T X.1245] Recommandation UIT-T X.1245 (2010), *Aspects généraux de la lutte contre le pollupostage dans les applications multimédias sur les réseaux IP.*

[b-UIT-T X.1361] Recommandation UIT-T X.1361 (2018), *Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle.*

[b-UIT-T X.1524] Recommandation UIT-T X.1524 (2012), *Énumération des failles courantes.*

[b-UIT-T X.1631] Recommandation UIT-T X.1631 (2015), *Technologie de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information fondés sur la norme ISO/CEI 27002 pour les services en nuage.*

[b-UIT-T Y.2052] Recommandation UIT-T Y.2052 (2008), *Cadre du rattachement multiple dans les réseaux de prochaine génération utilisant le protocole IPv6.*

[b-UIT-T Y.2201] Recommandation UIT-T Y.2201 (2009), *Spécifications et capacités des réseaux de prochaine génération de l'UIT-T.*

[b-UIT-T Y.2244] Recommandation UIT-T Y.2244 (2019), *Modèle de service de planification des cultures en amont de la production.*

[b-UIT-T Y.3500] Recommandation UIT-T Y.3500 (2014), *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire.*

[b-UIT-T Y.3502] Recommandation UIT-T Y.3502 (2014), *Technologies de l'information – Informatique en nuage – architecture de référence.*

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Technologies de l'information – Techniques de sécurité – Services d'horodatage – Partie 2: Mécanismes produisant des jetons indépendants*.

[b-ISO/CEI 19440] ISO/CEI 19440:2007, *Entreprise intégrée – Constructions pour la modélisation d'entreprise.*

[b-ISO/CEI 19944] ISO/CEI 19944:2016, *Technologies de l'information – Services et dispositifs en nuage: débits, catégories et utilisation des données.*

[b-ISO/CEI 20000-1] ISO/CEI 20000-1:2011, *Technologies de l'information – Gestion des services – Cadre 1: Exigences du système de gestion des services*.

[b-ISO/CEI 27000] ISO/CEI 27000:2016, Technologies de l'information – *Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire.*

[b-ISO/CEI 27729] ISO/CEI 27729:2012, *Information et documentation – Code international normalisé des noms (ISNI).*

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

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

Imprimé en Suisse
Genève, 2022