Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1751

(09/2020)

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

Applications et services sécurisés (2) – Sécurité de l'Internet des objets (IoT)

Lignes directrices relatives à la sécurité de la gestion du cycle de vie des mégadonnées par les opérateurs de télécommunication

Recommandation UIT-T X.1751

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	X.1140–X.1149
Protocoles de sécurité (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.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE 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
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**
SÉCURITÉ DE LA 5G	X.1800–X.1819

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

Recommandation UIT-T X.1751

Lignes directrices relatives à la sécurité de la gestion du cycle de vie des mégadonnées par les opérateurs de télécommunication

Résumé

La Recommandation UIT-T X.1751 contient une analyse des failles de sécurité et expose des lignes directrices relatives à la sécurité de la gestion du cycle de vie des mégadonnées pour les opérateurs de télécommunication.

L'évolution rapide de la technologie des mégadonnées est allée de pair avec une augmentation considérable de la valeur des données. Les mégadonnées ouvrent de nouvelles perspectives pour ce qui est des services de télécommunication. Les données étaient autrefois cloisonnées et gérées de manière indépendante dans différents systèmes fournissant des services de télécommunication. Les tendances à l'agrégation et à la fusion des données sont inévitables en raison de la mise en place de services de mégadonnées. Dans le cadre de la convergence vers la fusion des données, les données circulent sur des plates-formes et des processus de services et sont confrontées à plusieurs failles de sécurité à différents stades de leur cycle de vie.

On trouvera dans la Recommandation UIT-T X.1751 une description de certaines caractéristiques des services de mégadonnées et des catégories de données de télécommunication, une analyse des failles de sécurité de la gestion du cycle de vie des mégadonnées ainsi que des lignes directrices relatives à la sécurité à l'intention des opérateurs de télécommunication.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1751	03-09-2020	17	11.1002/1000/14267

Mots clés

Services de mégadonnées de télécommunication; gestion du cycle de vie des données.

* 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 on 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 à acquérir 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 la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

Table des matières

Recommandation UIT-T X.1751

Lignes directrices relatives à la sécurité de la gestion du cycle de vie des mégadonnées par les opérateurs de télécommunication

1 Domaine d'application

La présente Recommandation décrit les failles de sécurité et établit des lignes directrices relatives à la gestion du cycle de vie des services de mégadonnées de télécommunication. La présente Recommandation:

– expose les caractéristiques des services de mégadonnées et des catégories de données de télécommunication;

– analyse les failles de sécurité de la gestion du cycle de vie des services de mégadonnées de télécommunication;

– indique des lignes directrices relatives à la sécurité de la gestion du cycle de vie des données pour les services de mégadonnées de télécommunication.

Lorsque les opérateurs de télécommunication fournissent des services de mégadonnées, ils doivent impérativement obtenir au préalable l'accord exprès des abonnés. En outre, il est recommandé que ces opérateurs prennent les mesures nécessaires en matière de protection des données tout au long du processus de fourniture de services de mégadonnées.

Les mécanismes de protection pour diverses catégories de données n'entrent pas dans le cadre de la présente Recommandation.

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.1641] Recommandation UIT-T X.1641 (2016), *Lignes directrices pour la sécurité des données des clients de services en nuage.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 mégadonnées (big data) [b-UIT-T Y.3600]: modèle qui permet de collecter, stocker, gérer, analyser et visualiser des ensembles de données considérables présentant des caractéristiques hétérogènes, éventuellement en respectant des contraintes de temps réel.

3.1.2 mégadonnées en tant que service (BDaaS) [b-UIT-T Y.3600]: catégorie de service dans le nuage dans laquelle les capacités fournies au client du service en nuage sont celles qui lui permettent de collecter, de stocker, d'analyser, de visualiser et de gérer les données au moyen de mégadonnées.

3.1.3 associabilité [b-ISO/CEI 20889]: propriété d'un ensemble de données, selon laquelle il est possible d'associer (par rattachement) un dossier concernant une entité principale de donnée à un dossier concernant la même entité principale de données dans un ensemble de données séparé.

3.1.4 pseudonymisation [b-ISO/CEI 29100]: processus appliqué aux informations d'identification personnelle (PII) qui remplace l'identification des informations avec un alias.

3.1.5 politique de sécurité [b-UIT-T X.800]: ensemble des critères permettant de fournir des services de sécurité.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 cycle de vie des données: ensemble du processus de survie après la production des données, y compris la collecte, la transmission, le stockage, l'utilisation (qui englobe l'analyse et la visualisation des données), le partage et la destruction des données.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

2B	orienté entreprise (*to business*)
2C	orienté client (*to consumer*)
API	interface de programmation d'application (*application programming interface*)
APP	application
BDaaS	mégadonnées en tant que service (*big data as a service*)
BSS/OSS	système d'appui aux activités et système d'appui à l'exploitation (*business support system and operation support system*)
DB	base de données (*database*)
FTP	protocole de transfert de fichiers (*file transfer protocol*)
HDFS	système de fichiers distribués Hadoop (*Hadoop distributed file system*)
IoT	Internet des objets (*Internet of things*)
IP	protocole Internet (*Internet protocol*)
JDBC	connectivité de base de données Java (*Java database connectivity*)
LBS	service fondé sur la localisation (*location based service*)
LDAP	protocole rapide d'accès à l'annuaire (*lightweight directory access protocol*)
MPP	processeur massivement parallèle (*massive parallel processor*)
OSS	système d'appui à l'exploitation (*operation support system*)
PII	informations d'identification personnelle (*personally identifiable information*)
REST	transfert d'état représentationnel (*representational state transfer*)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à 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.

L'expression "**il est interdit**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**peut, à titre d'option**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de service 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 à la présente Recommandation.

6 Vue d'ensemble

Les mégadonnées, en raison de leur évolution rapide, ont pris beaucoup de valeur. Elles ouvrent de nouvelles perspectives aux opérateurs de télécommunication, qui disposent depuis longtemps de différents types de ressources de données, telles que les données d'appel et de localisation, les données personnelles, les données des consommateurs de services mobiles et les données du terminal, dans ce qu'il était convenu d'appeler les systèmes d'entrepôt de données. Étant donné qu'ils produisent rapidement des mégadonnées, les opérateurs de télécommunication innovent en permanence et investissent constamment dans la mise au point de services de mégadonnées.

Les services de mégadonnées de télécommunication concernent des volumes d'informations de l'ordre du téraoctet, voire du pétaoctet. Les données produites sont de différents types, par exemple les données structurées, semi-structurées et non structurées. Parmi les sources figurent les données privées, telles que les informations PII et les données des journaux d'accès. Ces données peuvent être la cible d'attaques.

Autrefois, les données étaient séparées et gérées indépendamment dans différents systèmes fournissant des services de télécommunication. De plus, ces systèmes pouvaient être situés dans différents emplacements et gérés par différents départements. Compte tenu de l'évolution des services de mégadonnées, les opérateurs de télécommunication ont éliminé les obstacles que constituaient les départements et recueillent des données auprès de plusieurs systèmes distincts. La convergence des données entraîne une augmentation considérable de la valeur des services de mégadonnées.

Lors du processus de fourniture des services de mégadonnées, les données circulent sur la plate-forme de mégadonnées et sont exposées, à chacun des différents stades de leur cycle de vie, à diverses menaces et à divers risques de sécurité. Ainsi, une erreur dans la collecte peut aboutir à ce que des données soient divulguées alors qu'elles n'auraient pas dû l'être. Il peut également y avoir un accès non autorisé au stade du stockage des données. L'utilisation de données à caractère sensible peut s'accompagner d'un risque de fuite de données lorsque des informations sont partagées. C'est pourquoi il est nécessaire d'analyser les failles de sécurité et de définir des lignes directrices sur la sécurité de la gestion du cycle de vie pour les services de mégadonnées de télécommunication.

On trouvera dans la présente Recommandation une analyse des risques et une description des lignes directrices relatives à la sécurité de la gestion du cycle de vie pour les mégadonnées de télécommunication.

7 Caractéristiques des services de mégadonnées de télécommunication et catégories de données

7.1 Caractéristiques des services de mégadonnées de télécommunication

De plus en plus d'opérateurs de télécommunication considèrent que les services de mégadonnées constituent une orientation stratégique importante pour l'innovation et le développement au sein de leur entreprise. En mettant en place par exemple des plates-formes dotées de capacités de

mégadonnées ou des équipes opérationnelles spécialisées, les opérateurs de télécommunication peuvent concevoir des services de mégadonnées.

Les opérateurs de télécommunication peuvent recueillir une large gamme de données sur les clients liées aux utilisateurs individuels, par exemple le profil de l'utilisateur, les dispositifs, l'utilisation et la localisation. Ils peuvent avoir recours à des techniques d'analyse des mégadonnées pour tirer parti de ces données, afin de mettre au point des services se rapportant à des applications très diverses, par exemple le commerce de détail, les soins de santé et les villes intelligentes. Les opérateurs de télécommunication peuvent utiliser ces services pour améliorer leurs propres activités ou les commercialiser auprès de fournisseurs de services tiers dans d'autres secteurs d'activité.

Toutefois, la gamme et les types de données que les opérateurs de télécommunication utilisent pour ces services de mégadonnées peuvent avoir pour conséquence de révéler une quantité considérable de données détaillées sur les personnes, y compris des informations PII, des données à caractère sensible, par exemple les croyances religieuses ou l'appartenance politique, et des secrets commerciaux. Cette considération est particulièrement importante si les opérateurs de télécommunication choisissent de partager ces données avec des tiers. Il est donc essentiel que les opérateurs de télécommunication reconnaissent les menaces qui peuvent surgir tout au long du cycle de vie des données de leurs services de mégadonnées et adoptent des mesures de sécurité pour protéger leurs utilisateurs.

7.2 Catégories de données

Les opérateurs de télécommunication disposent de quatre catégories principales de données d'utilisateur, qui sont présentés dans le paragraphe ci-dessous. En outre, compte tenu de l'essor de l'Internet des objets (IoT) et des services qui lui sont rattachés, les données prennent toujours plus d'ampleur et se caractérisent par une diversité toujours plus grande, ce qui fait peser de nouveaux risques sur la confiance et la sécurité des utilisateurs. Les opérateurs de télécommunication doivent donc tenir compte de ces risques.

1) Données produites par le système d'appui aux activités et le système d'appui à l'exploitation (BSS/OSS) de l'opérateur de télécommunication, qui comprennent l'identité de l'utilisateur, la longueur de l'appel, la cible de l'appel, la facture de communication, les types de services, voire le type de terminal.
2) Données produites par le système d'appui à l'exploitation (OSS) de l'opérateur de télécommunication, qui sont essentiellement des données relatives au comportement de l'utilisateur, y compris les données produites par l'intermédiaire de l'Internet mobile, des discussions sur messagerie instantanée, des jeux en ligne et de la navigation sur le web.
3) Données reposant sur les informations du service fondé sur la localisation (LBS) d'un utilisateur, qui sont étroitement liées, à la différence des catégories 1) et 2), à l'emplacement effectif de l'utilisateur et peuvent être utilisées pour le marketing commercial, la mobilité de la population, la sécurité du public et l'urbanisme.
4) Données entreprise (2B) ou données client (2C), produites dans un scénario IoT, qui sont des mégadonnées relatives aux "objets" et aux "personnes" – ces données sont particulièrement utiles dans le domaine des soins de santé, des dispositifs à porter sur soi et des maisons intelligentes.

Parmi les mégadonnées sur les objets, on citera les relevés d'eau, d'électricité et de gaz fournis par les compteurs, les données sur le climat et la pollution recueillies par les capteurs et les données de suivi des expéditions de biens.

Parmi les mégadonnées sur les personnes figurent les données sur la santé, les finances personnelles et l'historique des achats.

Il convient de noter que l'associabilité de certaines données peut avoir des conséquences plus importantes que prévu pour les utilisateurs, en fonction de la catégorie dans laquelle les données sont

classées initialement, par exemple les données anonymisées de la catégorie 4) qui sont analysées conjointement avec d'autres données peuvent rendre des personnes identifiables, comme les informations PII de la catégorie 1). Il est donc recommandé de tenir dûment compte de l'associabilité lors de la détermination de la façon de sécuriser les données, même dans les cas où les données ne sont pas immédiatement classées dans la catégorie des informations PII ou considérées comme d'autres données personnelles.

Dans la présente Recommandation, il est recommandé de sécuriser les données relevant de ces quatre catégories à toutes les étapes du cycle de vie des données en appliquant des lignes directrices en matière de sécurité.

8 Cycle de vie des données dans les services de mégadonnées de télécommunication

Le cycle de vie des données dans les services de mégadonnées de télécommunication comprend six grandes étapes: collecte des données; transmission des données; stockage des données; utilisation des données; partage des données; et destruction des données. La transmission des données peut se faire en plusieurs étapes.

Le cycle de vie des données dans les services de mégadonnées de télécommunication est illustré sur la Figure 1.

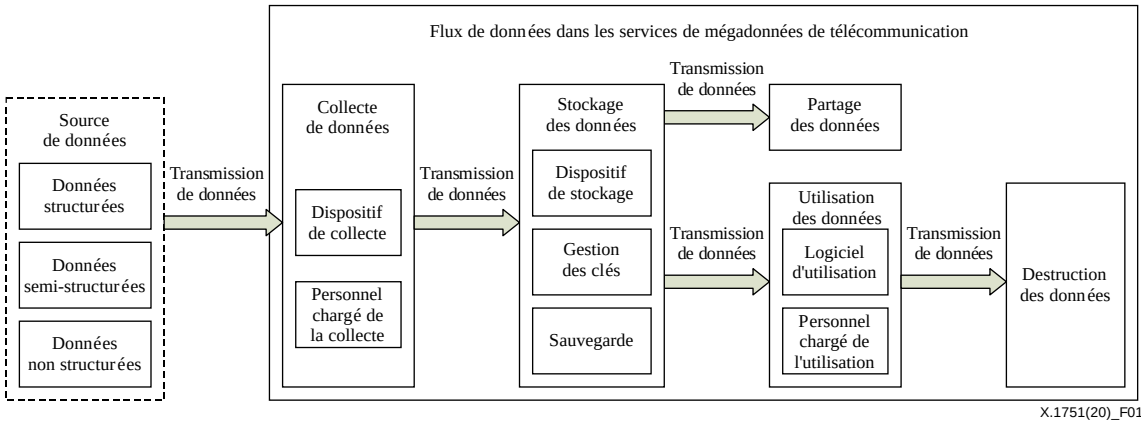

Figure 1 – Cycle de vie des données dans les services de mégadonnées de télécommunication

Le cycle de vie des services de mégadonnées de télécommunication commence par la collecte de données et se termine par la destruction de données. Après la collecte, les données peuvent être transmises, stockées, utilisées et partagées. La transmission des données peut avoir lieu entre différentes étapes, par exemple, après la collecte, les données peuvent être transmises à des dispositifs de stockage spécialisés; pendant l'utilisation, les données peuvent être transmises depuis les dispositifs de stockage vers le logiciel ou l'entité d'utilisation; après l'utilisation, les données ayant expiré ou devenues inutiles doivent être détruites.

Collecte de données: avec des dispositifs ou des entités spécialisés dans la collecte de données, différents types et diverses catégories de données sont rassemblés dans un répertoire spécifique ou un répertoire temporaire en vue d'être stockés.

Transmission de données: ce processus consiste à transférer des données d'un dispositif de collecte vers un dispositif de stockage et du stockage vers l'utilisation et le partage. Il arrive que l'étape de destruction des données s'accompagne également de la transmission de données.

Stockage de données: les données sont stockées dans des dispositifs spécialisés, par exemple des bases de données, des systèmes de fichiers répartis et des réseaux de disques. Le chiffrement et la sauvegarde des données sont également nécessaires pour les données importantes.

Utilisation de données: les logiciels et applications d'analyse des données accèdent aux données et les traitent pour fournir divers services de mégadonnées. Diverses données personnelles à caractère sensible peuvent être associées à ce processus.

Partage des données: le fournisseur de services de données ou le propriétaire des données partage ses propres résultats du traitement de l''analyse des données, voire les données sources, avec d'autres fournisseurs ou des tiers.

Destruction de données: les données ayant expiré, en particulier celles qui se trouvent dans des dispositifs qui stockent des informations importantes ou sensibles, doivent être entièrement détruites par un mécanisme de sécurité spécialement conçu à cet effet.

9 Failles de sécurité durant le cycle de vie des données des services de mégadonnées de télécommunication

Durant le processus des services de mégadonnées de télécommunication, les données circulent à chaque étape du service. Les failles de sécurité peuvent provenir de l'intérieur ou de l'extérieur du processus. Les failles de sécurité internes sont liées aux dispositifs et aux systèmes, tels que les dispositifs de collecte, les dispositifs de stockage et les dispositifs d'utilisation. Les failles de sécurité externes sont dues à une mauvaise configuration ou à une utilisation abusive. Les failles liées aux données sont décrites dans la Recommandation [b-UIT-T X.1040].

9.1 Étape de collecte des données

9.1.1 Faille de sécurité liée au dispositif et au système

Le dispositif et les systèmes sont vulnérables ou infectés par des virus ou des chevaux de Troie, ce qui pose des problèmes de sécurité.

9.1.2 Faille de sécurité liée à la configuration et à la gestion

1) Gestion du personnel

Il se peut que les dispositifs de collecte de données soient utilisés à mauvais escient ou sans autorisation, ce qui entraîne un risque de fuite de données.

2) Gestion des dispositifs

Une configuration à des fins malveillantes ou erronée des dispositifs de collecte peut entraîner la collecte non autorisée et une fuite de données.

Les données proviennent d'un certain nombre de systèmes commerciaux différents installés dans divers emplacements et gérés par différents départements. Un nœud malveillant peut s'introduire dans le groupe de dispositifs pour effectuer des opérations de collecte de données non autorisées.

3) Gestion des données

Les données qui sont sans rapport avec l'objectif d'utilisation déclaré sont collectées de manière excessive, ce qui peut entraîner une fuite de données.

Au stade de la collecte, un espace de stockage temporaire des données, par exemple le trajet aléatoire d'un serveur de protocole de transfert de fichiers (FTP), n'est pas contrôlé par le personnel chargé de la collecte, ce qui augmente le risque de divulgation ou d'altération non autorisée des données.

9.2 Étape de transmission des données

9.2.1 Faille de sécurité liée à la configuration et à la gestion

1) Gestion du personnel

L'administrateur modifie l'accès de transmission ou la configuration de la transmission sans autorisation, ce qui peut entraîner une fuite de données.

2) Gestion des dispositifs

Les données recueillies sont transmises sur un canal non sécurisé, d'où un risque d'écoute illicite ou d'altération des données.

L'interface de transmission n'est pas authentifiée, ce qui entraîne une erreur de connexion ou une connexion malveillante.

Un mécanisme de transmission entre différents nœuds ne protège pas la confidentialité et l'intégrité des données, ce qui entraîne des fuites de données et augmente le risque d'altération, d'écoute illicite et d'interception.

3) Gestion des données

L'absence de protection de la confidentialité pendant la transmission des données peut aboutir à l'interception des données ou à une fuite de données.

L'absence de protection de l'intégrité lors de la transmission des données peut se traduire par une manipulation malveillante des données ou endommager des données.

L'absence de protection de la disponibilité pendant la transmission peut entraîner l'interception ou l'altération volontaire des données.

9.3 Étape de stockage des données

9.3.1 Faille de sécurité liée au dispositif et au système

Le fait de ne déployer aucun logiciel antivirus, ou de déployer un logiciel de sécurité qui n'est plus valable, entraîne la divulgation et l'empoisonnement de données à caractère sensible.

Si un logiciel de sécurité est mal configuré ou n'est pas tenu à jour, les données ne sont plus protégées, ce qui peut conduire à la divulgation et à l'empoisonnement d'ensembles de données ainsi qu'à des attaques contradictoires contre ces ensembles de données.

9.3.2 Faille de sécurité liée à la configuration et à la gestion

1) Gestion du personnel

Les mesures de contrôle d'accès sont mal configurées, de sorte que les données stockées sont exposées au risque d'accès non autorisé ou d'altération. Les personnes autorisées à accéder à certains ensembles de données stockés sont en mesure de déduire des informations IIP ou d'autres données personnelles auxquelles elles ne sont pas autorisées à accéder, en raison de l'associabilité.

2) Gestion des dispositifs

Une base de données relationnelle, un système de fichiers réparti Hadoop (HDFS) et un entrepôt de données à processeur massivement parallèle (MPP) coexistent dans un environnement de stockage. Une gestion médiocre des autorisations a pour conséquence un accès non autorisé et la divulgation de données.

Un grand nombre de données non structurées sont stockées séparément dans différents nœuds, ce qui rend difficile l'application d'une même politique de sécurité. Des politiques de sécurité non homogènes ou des conflits peuvent se traduire par une protection insuffisante de la sécurité et par une fuite de données.

3) Gestion des données

Les données stockées ne sont pas chiffrées, que ce soit en totalité ou en partie, de sorte que les utilisateurs sont davantage exposés en cas de violation passive ou active des données.

Bien que les données stockées soient chiffrées, les failles liées à l'algorithme de chiffrement ou à la gestion des clés augmentent le risque d'accès non autorisé ou d'altération des données stockées.

L'intégrité des données n'est pas activement protégée pendant leur stockage, ce qui expose les données à des modifications non autorisées, même après leur collecte.

Les données stockées comprennent des données qui sont obsolètes ou ne se rapportent pas directement à l'objectif d'utilisation déclaré, ou encore qui ne sont pas nécessaires à cette fin. Plus le nombre de données stockées augmente, plus l'utilisateur est exposé en cas de violation passive ou active des données.

Si les mécanismes de sauvegarde et de récupération des données sont incomplets, les données risquent de ne pas être disponibles.

9.4 Étape d'utilisation des données

9.4.1 Faille de sécurité liée au dispositif et au système

Les logiciels d'analyse des données en réseau ou dans le nuage présentent des failles qui mettent en danger les données exposées aux logiciels.

L'application de visualisation des logiciels d'analyse des données pose des problèmes de sécurité qui peuvent être exploités par les auteurs d'attaques.

9.4.2 Faille de sécurité liée à la configuration et à la gestion

1) Gestion du personnel

En l'absence de capacités d'authentification et d'autorisation pour les utilisateurs ou d'applications de visualisation, un faux utilisateur ou une fausse application de visualisation peut obtenir des données visuelles, ce qui entraîne une fuite de données.

2) Gestion des dispositifs

Du fait de l'absence d'authentification de l'identité des dispositifs d'utilisation des données, un dispositif non autorisé rejoint la plate-forme de mégadonnées. Il en résulte une fuite de données ou une indisponibilité pour l'entreprise.

3) Gestion des données

Lorsqu'elles sont utilisées par des applications de visualisation, les données à caractère personnel, y compris les informations PII et les données sensibles, ne sont pas correctement anonymisées ou masquées et risquent davantage d'être identifiées.

Les données visualisées sont très faciles à relier entre elles, ce qui augmente le risque de déduction de l'identité ou d'autres données personnelles.

Les données de sortie issues des processus d'analyse des données ne sont pas stockées dans un environnement sécurisé, ou les données de sortie obsolètes ou qui ne se rapportent pas directement à l''utilisation recherchée, ou encore qui ne sont pas nécessaires pour cette utilisation, sont conservées. Plus le nombre de données conservées augmente, plus les utilisateurs sont exposés en cas de violation passive ou active des données.

Les journaux de données qui sont produits durant cette étape ne sont pas stockés de manière sécurisée, ce qui peut être mis à profit pour déduire des données personnelles en cas de violation des données.

9.5 Étape de partage des données

9.5.1 Faille de sécurité liée au dispositif et au système

Le dispositif et le système de partage des données sont vulnérables à des virus ou des chevaux de Troie ou infectés par ceux-ci, ce qui pose des problèmes de sécurité.

9.5.2 Faille de sécurité liée à la configuration et à la gestion

1) Gestion du personnel

Les responsabilités et les capacités des utilisateurs de données partagées en matière de sécurité ne sont pas suffisamment précisées, d'où une protection insuffisante des données et une fuite de données.

2) Gestion des dispositifs

La portée et les limites du partage des données sont mal définies; en outre, les mesures de contrôle de sécurité sont insuffisantes, de sorte que les données sensibles sont directement accessibles à des partenaires.

La protection de la sécurité d'un canal de partage de données n'est pas assurée, ce qui donne lieu à la divulgation ou à l'altération volontaire de données importantes.

3) Gestion des données

Les registres de consignation du partage des données sont incomplets, de sorte qu'il est difficile d'en déterminer la cause lorsqu'un incident de sécurité se produit.

9.6 Étapes de destruction des données

À la fin de cette étape, si les données n'ont pas été complètement détruites, des données sensibles peuvent être récupérées par du personnel malveillant, ce qui entraîne une fuite de données.

9.7 Relation entre les failles de sécurité et le cycle de vie des données

Les failles de sécurité apparaissent à différentes étapes du cycle de vie d'un service de mégadonnées. Le Tableau 1 donne un aperçu de la relation entre les failles de sécurité et le cycle de vie des données d'un service de mégadonnées.

Dans le Tableau 1, la lettre "O" (Oui) dans une cellule indique qu'il existe une faille de sécurité à ce stade.

Tableau 1 – Relation entre les failles de sécurité et l'étape du cycle de vie des données

Faille		**Étape du cycle de vie**					
		Collecte des données	**Transmission des données**	**Stockage des données**	**Utilisation des données**	**Partage des données**	**Destruction des données**
Faille du dispositif		O		O	O	O	
Faille de configuration et de gestion	Gestion du personnel	O	O	O	O	O	
	Gestion du dispositif	O	O	O	O	O	
	Gestion des données	O	O	O	O	O	O

10 Lignes directrices relatives à la sécurité du cycle de vie des données des services de mégadonnées de télécommunication

La présente Recommandation décrit des mécanismes détaillés qui conviennent pour toutes les catégories de données indiquées au § 7.2.

10.1 Étape de collecte des données

10.1.1 Lignes directrices relatives à la sécurité du dispositif et du système

Le logiciel du dispositif et le système utilisés pour la collecte des données doivent être à jour et être exempts de failles publiques.

Le dispositif et le système utilisés pour la collecte des données nécessitent l'installation de logiciels de sécurité, par exemple des logiciels antivirus et des logiciels de protection contre les logiciels malveillants, qui devront être compatibles avec le système d'exploitation du dispositif.

10.1.2 Lignes directrices relatives à la sécurité de la configuration et de la gestion

1) Gestion du personnel

Il est recommandé d'informer les utilisateurs des données qui sont collectées et des raisons pour lesquelles elles le sont, et d'obtenir leur accord exprès avant le début de la collecte.

Lors de la collecte de données, l'authentification et l'autorisation du personnel chargé de la collecte sont nécessaires.

2) Gestion des dispositifs

Il est recommandé de spécifier les mécanismes de sécurité et les mesures de protection de la sécurité pour la collecte des données, par exemple pour l'authentification et l'autorisation strictes des dispositifs de collecte. Il est recommandé que la catégorie de données soit conforme aux principes relatifs à la collecte.

Il est obligatoire de mettre en place un service de mégadonnées pour répondre au but recherché avec le service. Il est obligatoire de déterminer les données qui se rapportent strictement et sont strictement nécessaires à la collecte pour répondre à l'objectif de l'utilisation.

Le dispositif de collecte des données, les moyens de collecte, les formats de données, les processus de collecte et les méthodes de collecte doivent être précisés.

Il est obligatoire de mettre en application l'authentification d'accès du dispositif de collecte et du personnel chargé de la collecte; il est obligatoire d'assurer la détection d'un comportement anormal en matière de collecte et un avertissement signalant un tel comportement.

L'espace de stockage temporaire des données doit être soumis à de strictes restrictions, par exemple l'interdiction d'exporter sans autorisation des données depuis ce type d'espaces de stockage vers d'autres ressources de stockage, et il est recommandé d'autoriser la modification de l'espace de stockage.

Il est recommandé de protéger la transmission des données collectées, y compris les métadonnées, au moyen des algorithmes de chiffrement largement utilisés et testés par des tiers de confiance.

Gérer et stocker en toute sécurité les clés de chiffrement et, dans la mesure du possible, privilégier les protocoles cryptographiques dotés d'une fonction de confidentialité de transmission.

3) Gestion des données

Il est recommandé de déterminer les différentes classifications des données collectées, en fonction de leur importance et de leur sensibilité.

Il est nécessaire de consigner dans un journal les comportements anormaux suivants et de les signaler lorsque:

– la collecte et la transmission répétées dépassent le seuil fixé;
– la transmission est interrompue pendant le processus de collecte;
– le seuil fixé pour la capacité de stockage est dépassé.

10.2 Étape de transmission des données

10.2.1 Lignes directrices relatives à la sécurité de la configuration et de la gestion

1) Gestion du personnel

Empêcher les administrateurs de modifier arbitrairement les paramètres de configuration de l'accès ou de l'interface de transmission.

2) Gestion des dispositifs

La transmission des données via un canal chiffré de bout en bout est obligatoire.

L'interface de transport fournit des capacités d'authentification pour empêcher les connexions malveillantes.

3) Gestion des données

Il est recommandé de mettre en œuvre la protection de la confidentialité et de l'intégrité des données pendant l'étape de transmission des données.

Il est recommandé de détecter rapidement toute atteinte à l'intégrité des données pendant la transmission et de mettre en œuvre les mesures nécessaires pour rétablir l'intégrité des données après la détection d'erreurs.

10.3 Étape de stockage des données

10.3.1 Lignes directrices relatives à la sécurité du dispositif et du système

Il est obligatoire que le logiciel du dispositif de stockage et le système soient à jour et exempts de failles publiques.

Le dispositif de stockage nécessite l'installation d'un logiciel de sécurité à jour.

10.3.2 Lignes directrices relatives à la sécurité de la configuration et de la gestion

1) Gestion du personnel

Il est obligatoire d'appliquer un contrôle d'accès pour l'utilisateur ou l'application, comme le protocole d'authentification de réseau à clé secrète, le protocole Kerberos, et l'autorisation à granularité fine.

Il est recommandé d'intégrer les opérations relatives aux données importantes dans le mode commande de l'espace de stockage par plusieurs personnes, afin qu'une seule personne ne puisse pas disposer de tous les pouvoirs opérationnels pour les données importantes, par exemple leur sortie par lots, leur copie, leur destruction, leur publication et leur utilisation.

2) Gestion des dispositifs

Les méthodes d'autorisation doivent limiter l'accès aux personnes qui sont indispensables à la réalisation de l'objectif déclaré de l'utilisation pour laquelle les données sont collectées. Les autorisations doivent être accordées de façon à empêcher les personnes d'accéder à des données autres que celles absolument nécessaires à l'accomplissement des tâches concrètes qui leur ont été assignées et à tenir compte du fait que l'associabilité entre des ensembles de données stockés et des autorisations distinctes entre les personnes pourrait permettre de déduire des données à caractère personnel.

3) Gestion des données

a) Réduction des données au minimum

Il est recommandé de limiter le stockage des données, y compris les résultats des processus menés à bien pendant la phase d'utilisation des données, afin de ne conserver que les données qui se rapportent à l'objectif d'utilisation déclaré et sont nécessaires à cette fin.

Il est recommandé de fixer des périodes de conservation maximales précises pour toutes les données, sur la base de la durée minimale possible pendant laquelle les données doivent être conservées pour répondre à leur objectif d'utilisation déclaré.

b) Stockage des données chiffrées

Le stockage chiffré est nécessaire pour garantir la confidentialité des données importantes. Il est recommandé de prendre en charge un modèle hiérarchique de chiffrement des données; différents mécanismes de stockage de sécurité sont utilisés en fonction du niveau de confidentialité des données.

Il est recommandé d'utiliser des algorithmes de chiffrement largement déployés et testés par des tiers de confiance. Gérer et stocker les clés de chiffrement en toute sécurité et, dans la mesure du possible, utiliser de préférence des protocoles cryptographiques qui assurent la confidentialité de transmission.

c) Protection de l'intégrité des données

Il est recommandé de prévoir un mécanisme de détection de l'intégrité, afin de déterminer la détérioration ou la perte de données dues au stockage des données.

Il est recommandé de prendre les mesures nécessaires pour rétablir l'intégrité des données après la détection d'erreurs [UIT-T X.1641].

Les journaux d'audit qui documentent les modifications apportées aux données stockées doivent être tenus à jour. Les journaux doivent être stockés en toute sécurité et il est recommandé de mettre en évidence et de signaler les tentatives visant à les modifier.

d) Sauvegarde et récupération des données

Il est recommandé de prévoir des mécanismes complets de sauvegarde et de rétablissement des données, afin de garantir la capacité d'utilisation et l'intégrité des données.

10.4 Étape d'utilisation des données

10.4.1 Lignes directrices relatives à la sécurité du dispositif et du système

Il est recommandé que le logiciel du dispositif et du système soit à jour et exempt de failles publiques.

Il est recommandé d'installer un logiciel de sécurité à jour sur le dispositif et le système.

10.4.2 Lignes directrices relatives à la configuration et à la gestion

1) Gestion du personnel

Il est recommandé d'assurer une authentification unifiée pour permettre à différentes applications (utilisation des données) d'accéder à des plates-formes de mégadonnées, quel que soit le type d'interface utilisé par les applications, comme l'interface de programmation d'application de transfert d'état représentationnel des ressources (REST API) et la connectivité de base de données Java (JDBC). Le mécanisme d'authentification détaillé peut notamment être Kerberos, le protocole simple d'accès à l'annuaire (LDAP).

Il est recommandé de prévoir une autorisation à granularité fine en vue de son utilisation par différentes applications pour l'accès à des plates-formes de mégadonnées, qui repose sur les méthodes suivantes:

a) autorisation à granularité fine pour l'accès aux plates-formes de mégadonnées au moyen des noms d'utilisateur, des adresses du protocole Internet (IP) et des noms des applications (APP);

b) autorisation à granularité fine pour l'accès aux ressources de stockage, telles que le logiciel d'entrepôt de données Hive, la base de données répartie non relationnelle à code source ouvert Hbase, le système HDFS et les bases de données;

c) autorisation à granularité fine au moyen de différentes opérations de la base de données ou du système de fichiers (par exemple SELECT (SÉLECTIONNER), INSERT (INSÉRER) et CREATE (CRÉER));

d) autorisation à granularité fine pour les autorisations d'importer et d'exporter des données;

e) autorisation à granularité fine pour l'accès au fichier et à l'annuaire du système HDFS.

2) Gestion des dispositifs

Il est recommandé de prévoir des mécanismes de surveillance des activités malveillantes et de lutte contre ces activités au stade de l'utilisation des données.

Il est recommandé de prévoir des journaux d'audit de sécurité pour vérifier que les données sont utilisées de façon adéquate, assurer la conformité à la politique de sécurité et aux procédures opérationnelles établies, faciliter l'évaluation des dommages et recommander toute modification à apporter aux contrôles de sécurité, à la politique en matière de sécurité et aux procédures applicables à l'utilisation des données.

Il est recommandé d'envisager une politique d'audit de sécurité indiquant les informations sur l'utilisation des données qu'il est obligatoire d'enregistrer, les conditions ces informations sur l'utilisation des données doivent obligatoirement être enregistrées et la définition syntaxique et sémantique à utiliser pour l'échange des informations relatives à l'audit de sécurité.

3) Gestion des données

Afin de protéger les données sensibles, la pseudonymisation des données est nécessaire au stade de l'utilisation des données. Des lignes directrices détaillées pour la pseudonymisation des données seront unifiées et prises en compte lors de l'étape suivante de partage des données.

Il est recommandé de procéder à des audits de l'utilisation des données sensibles et des journaux d'audit devront être produits comme spécifié dans [UIT-T X.1641].

10.5 Étape de partage des données

10.5.1 Lignes directrices relatives à la sécurité du dispositif et du système

Il est recommandé que le logiciel du dispositif et du système de l'utilisateur soit à jour et exempt de failles publiques.

Il est recommandé d'installer un logiciel de sécurité à jour sur le dispositif et le système.

10.5.2 Lignes directrices relatives à la configuration et à la gestion

1) Gestion du personnel

Les utilisateurs doivent être informés des données, y compris des métadonnées et des données éventuelles résultant des processus menés à bien au cours de la phase d'utilisation des données, qui seront partagées avec des tiers et de l'identité de ces tiers. L'accord exprès de l'utilisateur doit être obtenu avant de partager des données, y compris des données en sortie.

2) Gestion des dispositifs

Il est recommandé de contrôler le comportement de l'exportation des données.

Lorsque des données sont partagées avec des services externes, il est recommandé de limiter l'utilisation des données afin d'éviter leur revente.

Il est recommandé que les mécanismes de protection de la sécurité soient négociés entre les parties prenantes concernées (par exemple, les opérateurs entre lesquels les données sont transférées) et qu'ils comprennent une politique de sécurité pour le transfert, le stockage, la destruction des données partagées et l'accès à ces données, ainsi qu'un plan de sauvegarde si les données partagées sont divulguées.

3) Gestion des données

La pseudonymisation des données est le processus qui consiste à masquer les informations PII d'origine et les données sensibles à l'aide de caractères ou de données. L'objectif est de protéger les informations PII et les données sensibles.

Différentes applications peuvent être configurées avec différents algorithmes de pseudonymisation. La pseudonymisation des données est recommandée pour:

a) prendre en charge l'adjonction et la suppression dynamiques d'algorithmes de pseudonymisation;

b) prendre en charge la pseudonymisation à granularité fine, ce qui signifie que la pseudonymisation peut être configurée par un administrateur pour une table ou des colonnes données d'une base de données;

c) utiliser des algorithmes publics, en évitant les algorithmes propriétaires de tiers;

d) ne pas affecter de façon significative la continuité des activités et la qualité de fonctionnement du système.

10.6 Étape de destruction des données

10.6.1 Lignes directrices relatives à la sécurité pour la gestion des données

Les données doivent être à la fois effacées et écrasées à l'état solide.

Une fois les données supprimées, il est recommandé que l'espace de stockage des ressources, par exemple les fichiers, les annuaires et les enregistrements de base de données, du système soit complètement nettoyé sans possibilité de restauration.

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.1040] Recommandation UIT-T X.1040 (2017), *Architecture de référence de sécurité pour la gestion, tout au long de leur cycle de vie, des données sur les transactions de commerce électronique.*

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

[b-ISO/CEI 20889] ISO/CEI 20889:2018, *Terminologie et classification des techniques de dé-identification de données pour la protection de la vie privée*

[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	Équipements 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, 2021