Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1602

(03/2016)

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

Sécurité de l'informatique en nuage – Aperçu de la sécurité de l'informatique en nuage

Exigences de sécurité pour l'environnement des applications de logiciel en tant que service (SaaS)

Recommandation UIT-T X.1602

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	
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	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 pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange 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 oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

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

Recommandation UIT-T X.1602

Exigences de sécurité pour l'environnement des applications de logiciel en tant que service (SaaS)

Résumé

La Recommandation UIT-T X.1602 est une analyse du niveau de maturité des applications de logiciel en tant que service (SaaS). Elle propose la mise en place d'exigences de sécurité afin que l'exécution de ces applications se fasse dans un environnement cohérent et sûr. Des fournisseurs de services de nuage et des partenaires de services de nuage sont à l'initiative de ce projet, puisqu'ils doivent disposer d'un environnement pour les applications SaaS qui répond à leurs besoins en matière de sécurité. Ces exigences sont générales et indépendantes de tout modèle propre à un service, à un scénario particulier (comme les services web ou l'architecture REST), ou encore à des hypothèses ou solutions particulières.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1602	23-03-2016	17	11.1002/1000/12615

Mots clés

Exigences de sécurité, environnement des applications de logiciel en tant que service (SaaS), niveau de maturité SaaS.

* 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 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.1602

Exigences de sécurité pour l'environnement des applications de logiciel en tant que service (SaaS)

1 Domaine d'application

La présente Recommandation porte essentiellement sur les exigences de sécurité des environnements d'applications SaaS (logiciel en tant que service) exprimées en fonction du niveau de maturité des applications SaaS. Elle s'adresse aux fournisseurs de services de nuage et aux partenaires de services de nuage tels que les développeurs d'applications.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 service de nuage [b-UIT-T Y.3500]: une ou plusieurs capacités offertes via l'informatique en nuage invoquées à l'aide d'une interface définie.

3.1.2 catégorie de services de nuage [b-UIT-T Y.3500]: groupe de services qui possèdent un ensemble de qualités communes.

3.1.3 client de services de nuage [b-UIT-T Y.3500]: partie à une relation commerciale aux fins de l'utilisation de services de nuage.

3.1.4 partenaire de services de nuage [b-UIT-T Y.3500]: partie fournissant un appui ou une aide aux activités du fournisseur de services de nuage, du client de services de nuage, ou des deux.

3.1.5 fournisseur de services de nuage [b-UIT-T Y.3500]: partie qui met à disposition des services de nuage.

3.1.6 utilisateur de services de nuage [b-UIT-T Y.3500]: personne physique, ou entité agissant en son nom, associée à un client de services de nuage qui utilise des services de nuage.

3.1.7 bureau en tant que service [b-UIT-T Y.3500]: capacités offertes au client de services de nuage lui permettant de construire, de configurer, de gérer, de stocker, d'exécuter et de livrer à distance des fonctions de bureau d'utilisateurs.

3.1.8 infrastructure en tant que service [b-UIT-T Y.3500]: catégorie de services de nuage pour laquelle le type de capacité fourni au client de services de nuage correspond à des capacités d'infrastructure.

3.1.9 logiciel en tant que service (SaaS) [b-UIT-T Y.3500]: catégorie de services de nuage pour laquelle le type de capacité fourni au client de services d'informatique en nuage correspond à des capacités d'application.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ASP fournisseur de services d'application (*application service provider*)

CaaS communications en tant que service (*communications as a service*)

CRM gestion de la relation avec les clients (*customer relationship management*)

CSC client de services de nuage (*cloud service customer*)

CSN partenaire de services de nuage (*cloud service partner*)

CSP fournisseur de services de nuage (*cloud service provider*)

DaaS bureau en tant que service (*desktop as a service*)

IaaS infrastructure en tant que service (*infrastructure as a service*)

IAM gestion des identités et des accès (*identity and access management*)

IdM gestion des identités (*identity management*)

OLAP traitement analytique en ligne (*online analytical processing*)

OS système d'exploitation (*operating system*)

PaaS plate-forme en tant que service (*platform as a service*)

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

REST transfert d'état de représentation (*representational state transfer*)

SaaS logiciel en tant que service (*software as a service*)

SAP point d'accès au service (*service access point*)

SLA accord de niveau de service (*service level agreement*)

5 Conventions

Aucune.

6 Présentation générale

Un environnement des applications de logiciel en tant que service (SaaS) est un environnement de développement, de déploiement et d'exécution multi-locataires orienté vers les services, dans lequel le logiciel et ses données associées sont centralisés et normalement accessibles à la demande des utilisateurs au moyen d'un client (navigateur web par exemple) via internet.

Si la présente Recommandation concerne essentiellement l'environnement SaaS, certains de ses concepts peuvent aussi s'appliquer à d'autres catégories de services de nuage intégrant aussi le type de capacités d'application, par exemple la communication en tant que service (CaaS).

La Figure 1 illustre un modèle conceptuel d'environnement d'applications SaaS. Les capacités sous-jacentes de l'infrastructure en tant que service (IaaS), de la plate-forme en tant que service (PaaS) et du bureau en tant que service (DaaS) seront encapsulées dans des services; elles offriront un accès sûr et cohérent via un point d'accès au service exporté (SAP). Dans la présente Recommandation, IaaS peut offrir des services informatiques, de stockage et de réseaux, PaaS des services de plate-forme et DaaS des services de bureau pour un environnement d'applications SaaS. L'ensemble de ces services constitue les modules de base du développement d'une application.

L'environnement fournit aussi des fonctions de gestion de services nécessaires, notamment l'enregistrement des services, la configuration des services, l'orchestration des services, la vérification

de la dépendance des services, le contrôle d'accès aux services, l'isolation des services et d'autres fonctions de contrôle.

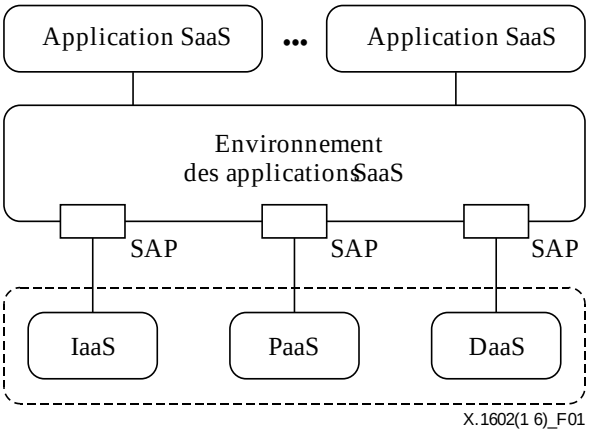
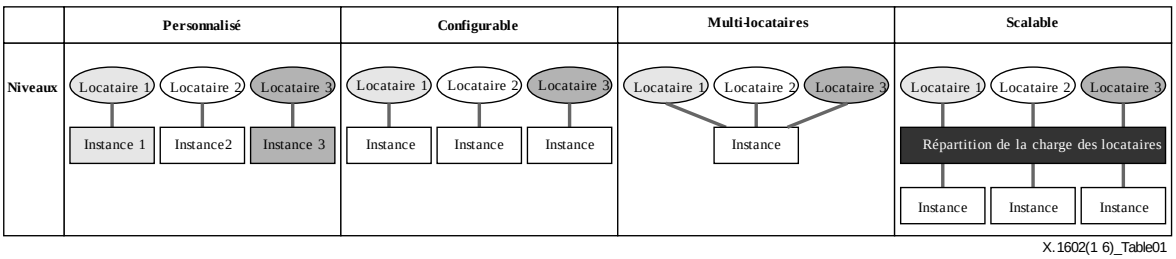


Figure 1 – Modèle conceptuel de l'environnement des applications SaaS

7 Niveaux de maturité d'application SaaS

Dans l'industrie, la maturité du SaaS est décrite en quatre niveaux que l'on peut désigner en abrégé: le niveau personnalisé (*custom level*), le niveau configurable (*configurable level*), le niveau multi-locataires (*multi-tenant level*) et le niveau modulable (*scalable level*). Chaque niveau possède les caractéristiques du niveau précédent et offre des fonctions supplémentaires. Le diagramme du Tableau 1 présente les caractéristiques des différents modèles de maturité SaaS.

Tableau 1 – Diagramme des niveaux de maturité d'application de l'environnement SaaS



Les exigences en matière de sécurité applicables aux environnements d'applications SaaS dépendent du niveau de maturité de l'application SaaS. Ces exigences sont illustrées du point de vue des CSP et des CSN au paragraphe 8.

7.1 Niveau 1: application SaaS personnalisée

L'application SaaS personnalisée est identique au modèle de fourniture de logiciels traditionnel appelé ASP (fournisseur de services d'application). Chaque client dispose de sa propre solution personnalisée d'application SaaS et exécute son instance d'application personnelle sur le serveur en nuage. Comme le montre la Figure 2, l'instance d'application personnalisée comprend l'ensemble de l'environnement d'exécution, y compris le système d'exploitation (OS), le système de gestion de données et l'intergiciel (*middleware*), qui sont spécifiques à chaque locataire. Le fournisseur d'environnements SaaS doit assurer le bon fonctionnement de multiples instances. Ce système est difficile à transposer à grande échelle pour répondre aux exigences toujours plus grandes des clients et son exploitation peut être coûteuse.

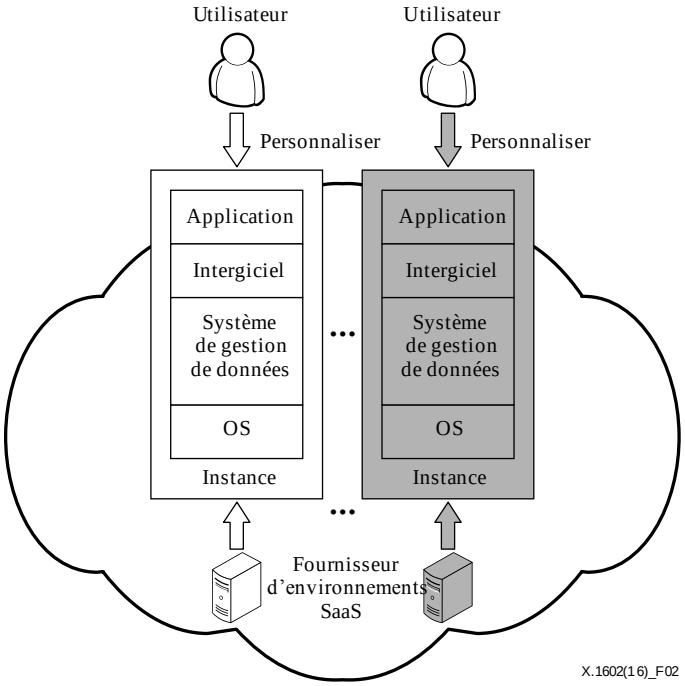


Figure 2 – Architecture d'application SaaS personnalisée

Les applications classiques de type client-serveur peuvent être facilement transformées en applications SaaS; il suffit pour cela de déplacer les serveurs dans le nuage et d'effectuer quelques modifications mineures. Les applications qui se prêtent bien à ce scénario sont généralement développées pour répondre à des besoins spéciaux de l'entreprise ou de l'organisation. La priorité est donnée à la sécurité au sein du système lui-même, une façon classique de procéder étant de regrouper un ensemble de machines physiques dans une zone privée et de déployer un système de gestion de données (qui offre des méthodes abstraites de persistance et des opérations pour les différents types de données) ainsi que le logiciel associé qui s'exécute sur ce système. Le système est conçu pour un usage interne exclusivement, avec contrôle d'accès strict. Le modèle d'instance d'application est le même pour tous les clients et les possibilités de configuration qu'il offre sont limitées. Cela étant, l'instance d'un client donné est totalement indépendante de toute autre instance.

7.2 Niveau 2: application SaaS configurable

Certaines applications courantes comme les logiciels de développement de sites web en libre-service ne sont pas personnalisées. Les fournisseurs d'environnements SaaS proposent des modèles communs pour ces applications et différents ensembles d'environnement d'exécution pour leurs instances. A partir d'un même modèle, les clients peuvent créer de multiples instances distinctes de l'application en configurant le visuel et le comportement de celle-ci. Ces instances sont déployées et exécutées sur des machines virtuelles ou physiques différentes pour répondre aux besoins de personnalisation. Les instances d'application sont isolées les unes des autres. La Figure 3 ci-dessous illustre cette architecture.

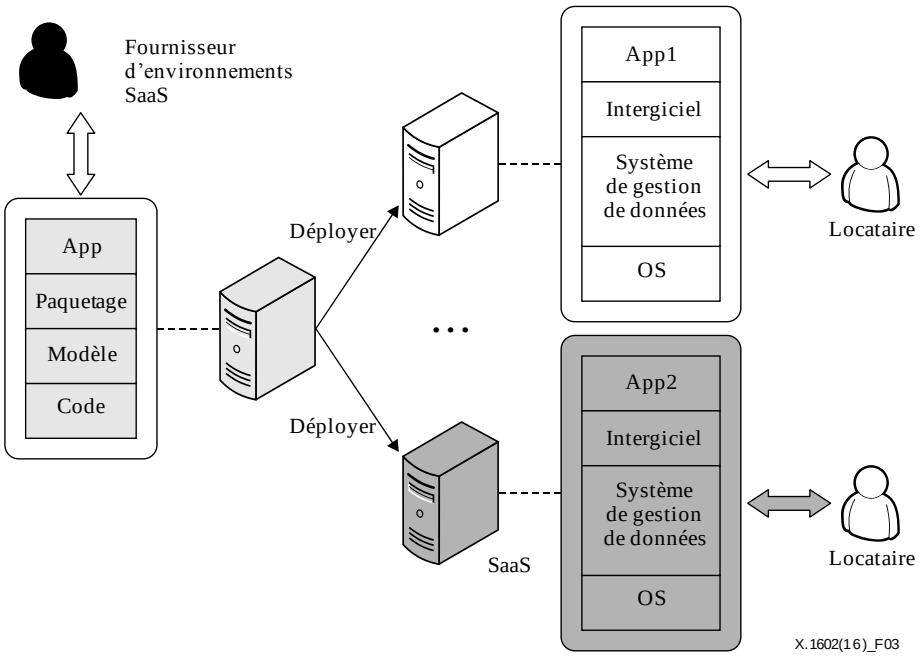


Figure 3 – Architecture d'application SaaS configurable

L'application SaaS configurable possède les caractéristiques suivantes:

1) Dans sa mise en service initiale, l'application est une copie d'un produit standard, puis les locataires configurent l'application selon leurs besoins. Toutefois, les possibilités de configuration du produit sont limitées.

2) Du côté du fournisseur d'applications SaaS, toute modification apportée au code du produit peut être facilement et immédiatement répercutée sur l'ensemble des locataires. Cela étant, seules des mises à jour ou des optimisations mineures du code de chaque instance sont possibles si l'on veut éviter les problèmes de compatibilité descendante.

3) Chaque locataire mémorise ses données dans sa propre machine virtuelle ou physique, les machines étant isolées les unes des autres. Les ressources offertes par le fournisseur d'environnements SaaS (stockage par exemple) doivent donc être suffisantes pour prendre en charge un nombre potentiellement élevé d'instances d'application qui s'exécutent en même temps.

L'évolution et l'amélioration des technologies logicielles permettront de fournir une application dotée d'options de configuration suffisantes pour répondre aux besoins de personnalisation des clients, et la configuration et l'utilisation devraient être plus intelligentes et automatisées. Les fournisseurs d'applications SaaS proposeront différentes versions de leurs produits pour s'adapter aux particularités des locataires.

7.3 Niveau 3: application SaaS multi-locataires

A ce niveau, le fournisseur d'applications SaaS est en mesure d'offrir une instance unique pour desservir en même temps plusieurs locataires. Il utilise pour ce faire des métadonnées configurables. La multi-location peut être activée au niveau de différentes couches: OS, système de gestion des données, intergiciel, application, etc. Un identifiant de locataire est mis en place pour distinguer les différents clients. Lorsqu'une base de données est utilisée dans un système de gestion de données, sa structure est étendue: un paramètre d'identité du locataire y est ajouté pour mémoriser toutes les données client dans un même ensemble de tables. L'identité du locataire doit aussi être ajoutée dans les requêtes de la base pour extraire les données correspondant à un client déterminé. La Figure 4 illustre l'architecture générale d'une application SaaS multi-locataires.

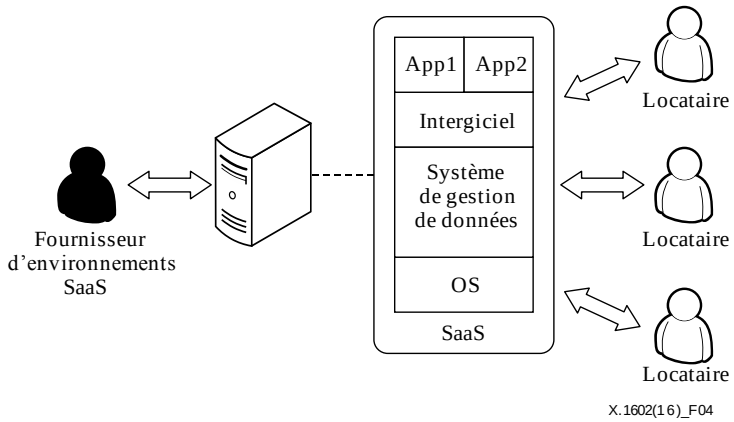


Figure 4 – Architecture d'application SaaS multi-locataires

On considère que le SaaS de veille économique (gestion des relations avec la clientèle par exemple) est une application type de ce niveau. Jusqu'ici, les efforts ont davantage porté sur la combinaison de l'entreposage de données/informatique en nuage et du SaaS en vue de fournir des applications de veille économique en ligne. L'entrepôt de données est hébergé par le centre de traitement de données; les applications de veille économique et les modèles de données sont prédéfinis et ne nécessitent qu'une personnalisation minimale. Les locataires n'ont qu'à choisir les éléments de données nécessaires à leurs applications de veille économique et à expliciter le mappage entre d'un côté les sources de données et, de l'autre, l'entrepôt et le modèle. Le système intègre ensuite les données provenant de multiples systèmes sources dans l'entrepôt, et ce dernier alimente les applications de traitement analytique en ligne, au moyen de scripts générés automatiquement. Habituellement, au moment de l'exécution, une seule instance de l'application de veille économique dessert plusieurs locataires en même temps, et ce au moyen de techniques de métadonnées. Les autorisations et les stratégies de sécurité garantissent que les données et les applications de l'un quelconque des clients ne sont pas accessibles aux autres clients.

Ce niveau, beaucoup plus efficace en termes d'utilisation des ressources de calcul et de stockage, peut prendre en charge davantage de locataires. Il est aussi possible d'atteindre ce degré de performance, d'extensibilité et d'élasticité en appliquant des techniques de partitionnement des données et de traitements parallèles.

Les traits distinctifs de ce niveau d'application SaaS sont la configurabilité et l'efficience multi-locataires.

7.4 Niveau 4: application SaaS modulable

La plupart des fournisseurs de services web desservent un nombre arbitrairement grand de clients comme autant de locataires multiples. En conséquence, chaque couche de l'architecture de la plate-forme sous-jacente, du matériel à l'application, doit être facile à moduler au niveau des applications et des services, comme illustré à la Figure 5. Ainsi est-il possible d'ajouter des locataires et des utilisateurs par locataire sans revoir l'architecture des applications.

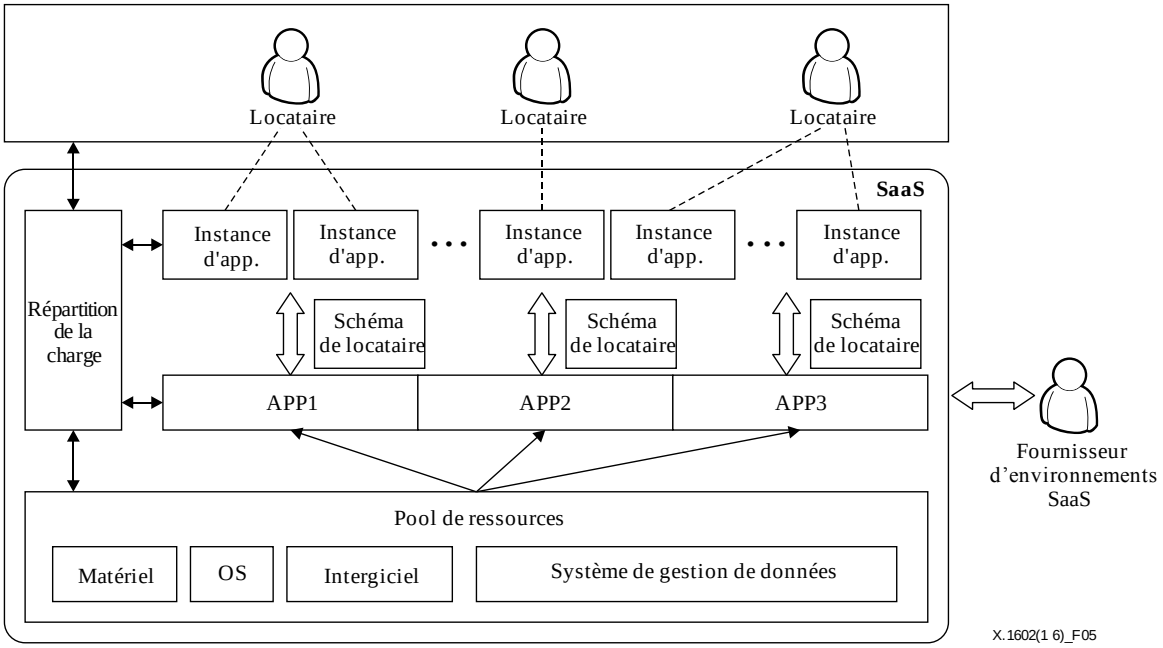


Figure 5 – Architecture d'application SaaS modulable

Lorsque le système doit prendre en charge un nouveau locataire, deux possibilités se présentent au niveau de la couche applicative: soit une ou plusieurs instances d'application sont créées en fonction des besoins spécifiques du locataire, soit une instance existante est choisie sur la base du mécanisme de répartition de la charge. Dans ce type d'environnement, toutes les instances d'applications doivent être créées de façon dynamique.

De même, les ressources sur lesquelles reposent les applications SaaS modulables doivent être configurables de façon très souple. Les matériels, intergiciels, logiciels et données doivent tous être gérés dans le pool de ressources. Les applications puisent dans le pool, de manière dynamique, toutes les ressources dont elles ont besoin. Lorsque cela est nécessaire, de nouvelles ressources peuvent être ajoutées sans recombinaison ni réarchitecture.

S'agissant des techniques de modulation dynamique, de multiples aspects touchant à la conception doivent être examinés: choix de la modulation, allocation des ressources, accord de niveau de service (SLA), etc. Un nouveau locataire peut être exécuté en tant qu'instance unique ou coexister avec d'autres locataires sur une instance partagée. Des instances exécutant chacune un type de locataires peuvent se voir allouer des ressources différentes. Si le fournisseur d'environnements SaaS met en place la répartition de la charge et le partage des ressources, il doit envisager de conclure des SLA différents selon les locataires.

8 Exigences de sécurité applicables à l'environnement des applications SaaS

La Figure 6 montre les relations entre le client de services de nuage (CSC), le fournisseur de services de nuage (CSP) et le partenaire de services de nuage (CSN) vis-à-vis de l'environnement des applications SaaS. Le CSP et le CSN exécutent différentes fonctions et jouent de ce fait différents rôles. Pour le CSP, le CSN peut être un fournisseur de contenus, un fournisseur de logiciels, un intégrateur système ou un vérificateur; le CSN et le CSP peuvent développer des applications pour le CSC. Le CSP et le CSN ont des interfaces avec l'environnement des applications SaaS, tandis que le CSC n'est en relation qu'avec les applications bâties sur cet environnement. Par conséquent, la présente Recommandation porte essentiellement sur les exigences de sécurité de l'environnement des applications SaaS dans le cas où le CSP et le CSN mettent en oeuvre un modèle de maturité différent. Le CSP et le CSN ont besoin d'un environnement qui soit en mesure de répondre à leurs demandes

en matière de sécurité; ils déterminent donc les exigences de sécurité de l'environnement des applications SaaS.

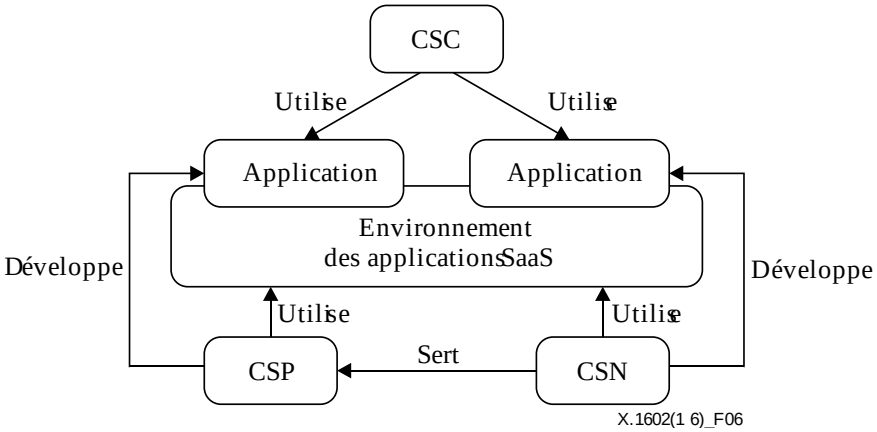


Figure 6 – Relations entre le CSC, le CSP et le CSN

Le CSP et le CSN ont chacun leurs exigences de sécurité vis-à-vis de l'environnement, à différents niveaux du SaaS. Le Tableau 2 décrit ces exigences dans l'environnement des applications SaaS. Les exigences dites "communes" s'appliquent à la fois au CSP et au CSN.

Tableau 2 – Exigences de sécurité du CSP et du CSN dans l'environnement des applications SaaS

	Environnement des applications SaaS
Exigences communes	Gestion des identités et des accès, sécurité des données, évaluation et audit de la sécurité, sécurité des interfaces, durcissement de la sécurité.
CSP	Disponibilité, garantie d'interopérabilité/de portabilité des services, protection des actifs logiciels, conformité juridique, vérification de la sécurité des codes sources.
CSN	Sécurité de l'audit, sécurité du logiciel, maintenabilité du logiciel.

8.1 Exigences communes de sécurité

Certaines exigences de sécurité concernant l'environnement des applications SaaS sont communes au CSP et au CSN.

8.1.1 Gestion des identités et des accès (IAM)

8.1.1.1 Gestion des identités (IdM)

Plusieurs administrateurs et utilisateurs interviennent dans l'environnement des applications SaaS. De plus, il est possible d'accéder à cet environnement et de l'utiliser depuis l'intérieur (CSP) ou depuis l'extérieur (CSC). La gestion des identités (IdM) est donc nécessaire non seulement pour protéger les identités, mais aussi pour faciliter les processus de gestion des accès, d'authentification, d'autorisation et d'audit des transactions dans cet environnement dynamique et ouvert.

Quel que soit le modèle de maturité, la gestion IdM devrait permettre de mettre en oeuvre l'authentification unique et/ou la fédération des identités pour l'environnement des applications SaaS au moyen de mécanismes d'authentification variés, répartis dans des domaines de sécurité différents.

8.1.1.2 Modèle de confiance

Les environnements des applications SaaS de niveau multi-locataires et de niveau modulable doivent comprendre un modèle de confiance global. Ce modèle permettra de créer des îlots et/ou des

fédérations d'entités de confiance. Ainsi, le système de gestion de l'environnement des applications SaaS, les ressources sous-jacentes, les hyperviseurs, les machines virtuelles et les applications bâties sur cet environnement seront en mesure d'authentifier l'identité et les droits autorisés des autres entités et éléments. Chaque îlot ou fédération de confiance reposera sur une ou plusieurs autorités de confiance (par exemple, une autorité délivrant des certificats d'infrastructure à clés publiques (PKI)).

8.1.1.3 Gestion des accès

Les administrateurs d'environnements d'applications SaaS sont tenus de fournir des mécanismes qui délèguent l'autorisation d'accès aux administrateurs des locataires. Ces derniers accordent des droits d'accès à leurs ressources correspondantes. La gestion des accès de ce type d'environnement doit prendre en charge de multiples modèles de contrôle d'accès: modèle fondé sur l'identité, modèle fondé sur la stratégie, modèle à base de rôles, modèle fondé sur la tâche, etc.

Dans le cas des applications SaaS de niveau personnalisé ou configurable, le minimum requis est le modèle de contrôle d'accès à base de rôles. Par exemple, un CSN qui aide un CSP à développer un service peut être chargé de certaines applications, mais n'a pas le droit d'administrer l'ensemble du système de services de nuage. En outre, il ne peut avoir accès qu'à une partie des ressources suivant les droits qui lui sont accordés. Cela étant, il peut partager ses ressources en fournissant aux autres CSN des interfaces d'application.

Dans le cas des niveaux multi-locataires et modulable, un modèle de contrôle d'accès est requis pour chaque utilisateur et chaque groupe. Pour le contrôle d'accès à base de rôles, il convient de partager des ressources entre plusieurs locataires en fonction des groupes de tâches d'un flux de travaux et des droits associés à ces tâches. Aussi, lorsque ces groupes de tâches sont exécutés, l'environnement des applications SaaS doit définir le mécanisme de contrôle d'accès fondé sur les tâches. Ce mécanisme permet de s'assurer que les droits d'accès des locataires aux ressources sous-jacentes peuvent être accordés et révoqués en temps voulu et qu'il n'est pas possible d'utiliser ces ressources sans autorisation.

8.1.2 Sécurité des interfaces

L'environnement des applications SaaS doit sécuriser les interfaces qui sont ouvertes aux CSP et aux CSN et par l'intermédiaire desquelles divers types de services d'informatique en nuage sont fournis ou développés. Il doit aussi sécuriser les communications qui s'appuient sur ces interfaces. Les mécanismes disponibles pour sécuriser les interfaces comprennent, sans s'y limiter, l'authentification unilatérale/mutuelle, la somme de contrôle d'intégrité (*integrity checksum*) et la signature numérique.

8.1.3 Sécurité des données

8.1.3.1 Isolation des données

Les données peuvent être isolées de deux façons: physiquement ou logiquement. L'isolation physique doit être réalisée par le contrôle d'accès aux stockages physiques. Pour ce faire, l'environnement des applications SaaS doit stocker les données de chaque locataire dans une zone de stockage physique isolée des autres ou mettre en place un contrôle d'accès aux données pour les différents locataires (autorisation d'accès, domaine de données ou toute autre méthode). L'isolation logique des données consiste à empêcher les locataires d'accéder aux données qui ne leur appartiennent pas, et ce au moyen de diverses techniques comme la virtualisation, même si toutes les données sont stockées ensemble.

Dans le cas des applications SaaS de niveau personnalisé ou configurable, les données de chaque locataire sont stockées séparément et isolées des autres au niveau physique.

Dans le cas des applications SaaS de niveau multi-locataires ou modulable, les données de tous les locataires sont stockées dans le nuage. L'environnement des applications SaaS doit donc être suffisamment intelligent pour isoler les données des différents locataires et pour maintenir cette isolation que ce soit en veille, en cours de traitement ou pendant les échanges. La frontière entre les locataires doit être mise en place au niveau physique ou au niveau logique, en fonction de la

granularité d'isolation requise et selon les modalités particulières de déploiement des logiciels et des équipements d'informatique en nuage.

8.1.3.2 Confidentialité des données

Le plus souvent, les données des locataires sont stockées et utilisées hors site et risquent donc d'être exposées. L'environnement des applications SaaS doit donc mettre en oeuvre des mécanismes de chiffrement pour garantir la confidentialité des données, et ce pendant la transmission, en cours de traitement et au repos, et prévenir les fuites de données imputables à des failles de sécurité dans l'application.

Le service de chiffrement des données est obligatoire pour tous les niveaux SaaS. Les données sensibles doivent être chiffrées pour éviter qu'elles ne soient exposées.

Dans le cas des environnements d'applications SaaS de niveau multi-locataires ou modulable, comme les données doivent être stockées dans une seule base ou dans une seule grande table, l'environnement doit fournir un mécanisme approprié de gestion de clés à même de garantir que les données ne peuvent pas être piratées par d'autres locataires.

8.1.3.3 Intégrité des données

L'environnement des applications SaaS doit mettre en oeuvre des mécanismes d'intégrité pour prévenir la falsification des données (données système et données d'utilisateur telles que les journaux d'exploitation et les données de configuration) pendant la transmission, en cours de traitement et au repos.

Il est impératif que les journaux système et applicatifs ne soient pas modifiables. Ainsi, en cas de dysfonctionnement ou d'utilisation frauduleuse, les CSP et les logiciels malveillants ne pourront pas y effacer leur trace.

Les applications SaaS doivent parfois être configurées par les CSC sur demande. Il importe que les données de configuration (fichier de configuration par exemple) ne soient pas modifiables sans autorisation.

Dans l'environnement des applications SaaS, les données d'utilisateur sont stockées dans le nuage géré par le CSP. La vérification de l'intégrité des données est donc une exigence de sécurité particulièrement importante. Il est, de plus, nécessaire de vérifier l'intégrité des données massives.

8.1.3.4 Fiabilité des données

La fiabilité des données doit être assurée. Pour cela, l'environnement des applications SaaS doit mettre en oeuvre des mécanismes de sauvegarde ou de redondance qui garantissent que les locataires ont toujours accès à leurs données même si une partie des noeuds de stockage du nuage devient inefficace.

Les données hébergées doivent être sauvegardées sur plusieurs sites, faute de quoi le bon fonctionnement du système ne pourra pas être assuré. L'environnement des applications SaaS doit être en mesure de restaurer l'ensemble des données en temps voulu. Pour assurer la cohérence des multiples copies, les données doivent être synchronisées.

8.1.3.5 Traçabilité et contrôle des données

L'environnement des applications SaaS doit être conçu de telle manière que l'emplacement physique des données soit conforme avec la législation et les règlements locaux en vigueur et avec les éventuelles restrictions figurant dans les accords juridiques. L'environnement doit fournir aux CSC des procédures leur permettant de préciser l'emplacement de stockage des données et de vérifier que leurs exigences à cet égard sont respectées.

Dans une infrastructure partagée et virtualisée, il est impératif non seulement que les utilisateurs gardent le contrôle de leurs données, mais aussi qu'ils puissent les localiser et contrôler leur cycle de vie sur toute sa durée. L'environnement des applications SaaS doit savoir très précisément, à tout

moment, où sont localisées et traitées les données système et les données d'utilisateur et offrir aux CSC un moyen de contrôler l'emplacement de leurs données. Il ne doit pas être possible pour des tiers non autorisés (y compris d'autres CSP) de suivre le mouvement des données pendant leur utilisation, ni de le reconstituer a posteriori.

8.1.4 Evaluation et audit de la sécurité

Lorsque des ressources sous-jacentes sont modifiées, piratées ou indûment traitées, l'environnement des applications SaaS doit être invoqué pour qu'une procédure d'évaluation de la sécurité soit engagée afin d'estimer si certains services de sécurité ou les stratégies appliquées sont en cause; si ces services ou stratégies ne satisfont pas à des conditions prédéfinies, des indications doivent être données ou des instructions préconisées. Un tiers habilité doit être mandaté pour s'assurer que l'environnement des applications SaaS respecte les exigences de sécurité qui s'appliquent. L'évaluation de la sécurité ou l'audit de sécurité pourrait être réalisé par le CSC, le CSP ou un tiers (CSN), tandis qu'un tiers habilité (CSN) pourrait effectuer la certification de sécurité.

On devra faire appel à des tiers de confiance indépendants pour évaluer la sécurité ou mener un audit de sécurité, et ce en toute fiabilité, indépendance et impartialité.

8.1.5 Durcissement de la sécurité

Fondamentalement, l'environnement des applications SaaS vise à offrir un environnement de développement, de déploiement et d'exécution d'applications SaaS, multi-locataires et orienté vers les services. Il arrive que les fonctions de sécurité des applications SaaS soient insuffisantes ou qu'elles ne soient pas mises en oeuvre correctement. L'environnement des applications SaaS doit être capable d'extraire et de vérifier les fonctions de sécurité défaillantes des applications Saas et doit offrir des mécanismes différenciés de durcissement de la sécurité qui permettent de corriger ces problèmes et ainsi de renforcer les applications pour que les exigences de sécurité des locataires dans les différents contextes soient satisfaites. Les fonctions de sécurité des applications se classent en deux catégories: d'un côté, les fonctions statiques, qui protègent les applications lorsqu'elles sont au repos, de l'autre, les fonctions dynamiques, qui assurent la sécurité des applications lorsqu'elles s'exécutent.

8.2 Exigences de sécurité du CSP

En termes de sécurité, outre les exigences générales, les CSP ont aussi des obligations spécifiques dans l'environnement des applications SaaS.

8.2.1 Disponibilité

Les CSP doivent garantir que l'environnement des applications SaaS est toujours opérationnel pour les CSC, ce qui suppose de gérer les éventuels problèmes (défaillances matérielles et logicielles, attaques par déni de service, etc.). Il est essentiel que la durée d'indisponibilité soit la plus courte possible.

8.2.2 Garantie d'interopérabilité/de portabilité des services

Dans le cas où un CSC souhaite faire migrer tout ou partie de son système vers un autre CSP, le CSP d'origine doit garantir l'interopérabilité et la portabilité des services de son environnement d'applications SaaS pour limiter au maximum les conséquences préjudiciables à l'activité du CSC en question. En outre, l'environnement doit garantir que les données du CSC gérées par le précédent CSP sont définitivement détruites et qu'elles ne pourront pas être récupérées par un tiers.

8.2.3 Protection des actifs logiciels

L'environnement des applications SaaS doit assurer la protection des actifs logiciels (applications, données internes aux applications, scripts, macros, bibliothèques de code des fonctions, licences logicielles, etc.).

Une exigence du CSP est que l'environnement des applications SaaS protège la confidentialité et l'intégrité de tous les actifs logiciels, ceux qu'il fournit et ceux qui sont apportés par le CSN. Cela suppose que ces actifs ne peuvent pas être copiés, détournés, piratés, divulgués ou, d'une autre façon, utilisés sans autorisation.

8.2.4 Conformité juridique

Même si le CSP peut utiliser des mécanismes de sauvegarde et de redondance pour garantir la fiabilité des données des CSC, l'environnement des applications SaaS doit garantir que les copies des données ne sont pas conservées plus longtemps que la durée de conservation autorisée par la législation en vigueur en matière de protection des données.

8.2.5 Vérification de la sécurité des codes sources

Etant donné que dans un environnement d'applications SaaS, un CSN peut fournir au CSP des codes applicatifs, des contenus et des logiciels, l'environnement doit fournir des mécanismes pour aider le CSP à vérifier les codes et à empêcher la mise en place de logiciels malveillants.

8.3 Exigences de sécurité du CSN

Dans l'environnement des applications SaaS, le CSN peut être un développeur d'applications, un fournisseur de contenus ou de logiciels, un intégrateur système ou un auditeur. En termes de sécurité, outre les exigences générales, les CSN ont aussi des obligations spécifiques dans l'environnement des applications SaaS.

8.3.1 Sécurité de l'audit

Lorsque le CSN est un auditeur, l'environnement des applications SaaS doit fournir des mécanismes pour l'aider à rassembler des informations liées à l'audit, à la consignation dans les journaux d'exploitation et aux rapports, avec une granularité correspondant au locataire et à l'application. Ces informations sont utilisées pour s'assurer que le service fourni par le CSP respecte les prescriptions réglementaires gouvernementales ainsi que les accords juridiques conclus avec les locataires. L'environnement des applications SaaS doit, de plus, fournir des mécanismes pour aider le CSN à vérifier que les informations réunies et transmises par les éléments d'audit du système CSP sont correctes et n'ont pas été falsifiées ou manipulées.

Par ailleurs, l'environnement doit offrir au CSN la possibilité de consigner les modifications de données importantes et de suivre, en ligne, la disponibilité des données pour envoyer une alarme de sécurité à temps et ainsi limiter les pertes.

8.3.2 Sécurité du logiciel

Lorsque le CSN est un développeur de logiciels ou de contenus de nuage, l'environnement des applications SaaS doit fournir des mécanismes pour l'aider à vérifier que les codes et autres composants qu'il fournit au CSP sont conformes aux éventuelles contraintes de programmation fixées par ce dernier. De plus, les codes et composants ne doivent contenir aucun logiciel malveillant ni violer l'intégrité des services de nuage du CSP.

8.3.3 Maintenabilité du logiciel

Lorsque le CSN est un développeur de logiciels de nuage, l'environnement des applications SaaS doit mettre en place des mécanismes pour l'aider à fournir des codes sources ou d'autres fonctionnalités pour le système CSP. Ces codes sources et ces fonctionnalités doivent contenir des indicateurs de version ou être gérés selon d'autres méthodes appropriées pour qu'ils puissent être maintenus pendant toute la durée de vie du service. Parmi ces méthodes figurent notamment la fourniture de mises à jour destinées à corriger les vulnérabilités connues, la suppression de la dépendance à d'autres composants connus pour être vulnérables et le renforcement de la sécurité globale du système.

Bibliographie

[b-UIT-T X.1601] Recommandation UIT-T X.1601 (2014), *Cadre de sécurité applicable à l'informatique en nuage*.

[b-UIT-T Y.3500] Recommandation UIT-T Y.3500 (2014) | ISO/CEI 17788:2014, *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire.*

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, 2017