Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1541

(09/2017)

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

Echange d'informations sur la cybersécurité – Echange concernant les événements/les incidents/l'heuristique

Format d'échange de description d'objet incident version 2

Recommandation UIT-T X.1541

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.1429
Protocoles de sécurité (2)	X.1450–X.1459
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.1541

Format d'échange de description d'objet incident version 2

Résumé

La Recommandation UIT T X.1541 décrit le modèle d'information pour le format d'échange de description d'objet incident (IODEF, *incident object description exchange format*) version 2 et définit un modèle de données associé, spécifié en XML. Ce modèle est destiné à être utilisé pour le partage des informations couramment échangées sur les incidents en matière de sécurité informatique ou d'autres types d'incidents. Pour cela, la présente Recommandation énumère les dispositions pertinentes de la norme IETF RFC 7970 et indique si elles ont un caractère normatif ou informatif.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1541	07-09-2012	17	11.1002/1000/11375
2.0	UIT-T X.1541	06-09-2017	17	11.1002/1000/13264

* 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 oeuvre 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 oeuvre 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

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
	3.1 Termes définis ailleurs	1
	3.2 Termes définis dans la présente Recommandation	1
4	Abréviations et acronymes	1
5	Conventions	2
6	Description d'objet incident et format d'échange	2
	6.1 Introduction	2
	6.2 Types de données IODEF	2
	6.3 Modèle d'information IODEF	3
	6.4 Considérations relatives au traitement	5
	6.5 Extension du format IODEF	5
	6.6 Questions liées à l'internationalisation	5
	6.7 Exemples	5
	6.8 Le modèle de données IODEF (Schéma XML)	5
	6.9 Considérations relatives à la sécurité	6
	6.10 Considérations de l'autorité IANA	6
	6.11 Références	6
Bibliographie		7

Introduction

La Recommandation UIT-T X.1500 "Techniques d'échange d'informations sur la cybersécurité" fournit des lignes directrices relatives à l'échange d'informations sur la cybersécurité, y compris d'informations sur les incidents et les indicateurs, telles que celles fournies dans la présente Recommandation. Le format d'échange de description d'objet incident (IODEF, *incident object description exchange format*) est un modèle de données permettant de représenter les informations sur la sécurité informatique couramment échangées. Il définit une représentation de modèle de données XML permettant d'acheminer des informations sur les incidents entre des entités qui, sur le plan opérationnel, sont chargées de mettre en place des parades préventives, de mener des activités de remise en état ou d'assurer un service de veille et d'alerte pour un public donné. Le modèle de données offre une méthode permettant de coder les informations sur les serveurs, les réseaux et les services exploités sur ces systèmes, sur la méthodologie d'exploitation et les données associées, sur les conséquences de l'incident et sur les démarches plus restrictives visant à documenter le déroulement des opérations.

L'objectif prioritaire du format IODEF est d'améliorer les capacités opérationnelles et les capacités d'évaluation d'une situation. L'adoption de ce format IODEF par la communauté renforce ses capacités de résoudre les incidents et d'acheminer des avertissements concernant les différentes menaces pour une situation donnée, en simplifiant la collaboration et le partage d'informations. Le format structuré IODEF permet:

– de renforcer l'automatisation du traitement des informations sur les incidents grâce à l'échange d'informations structurées sur les incidents, ce qui évite aux analystes de la sécurité d'avoir à examiner les textes de forme libre;
– de faciliter la mise en corrélation des données semblables (même très structurées) en provenance de sources différentes pour avoir une meilleure connaissance de la situation;
– de disposer d'un format commun à partir duquel il sera possible d'assurer l'interopérabilité des outils de traitement des incidents et d'analyse, en particulier lorsque les informations proviennent de plusieurs entités.

De nombreuses considérations politiques et juridiques liées aux procédures et à la confiance peuvent limiter ou empêcher l'échange d'informations. Le format IODEF est une spécification technique et n'a pas pour objet de traiter ces questions. La mise en oeuvre opérationnelle du format IODEF et des formats et protocoles associés devrait néanmoins tenir compte de ce contexte plus général lors de la conclusion d'accords d'échange d'informations.

Recommandation UIT-T X.1541

Format d'échange de description d'objet incident version 2

1 Domaine d'application

Le format d'échange de description d'objet incident (IODEF, *incident object description exchange format*) définit une représentation de modèle de données pour le partage des informations couramment échangées concernant les incidents en matière de sécurité informatique et d'autres types d'incidents (CSIRT, *computer security incident response team*). La présente Recommandation décrit le modèle d'information pour le format IODEF et fournit un modèle de données associé, spécifié pour le format XML.

Une représentation de modèle de données ou un cadre permettant l'échange d'informations sur des incidents relatifs à la sécurité informatique ou d'autres types d'incidents doit comprendre les fonctionnalités permettant de respecter toutes les législations, réglementations et politiques nationales ou régionales applicables.

Les responsables de la mise en oeuvre et les utilisateurs de toutes les Recommandations UIT-T, y compris la présente Recommandation et les techniques sous-jacentes, doivent se conformer à toutes les législations, réglementations et politiques nationales ou régionales applicables.

2 Références

Les Recommandations UIT-T suivantes et les autres références contiennent des dispositions qui, en référence à ce texte, constituent les dispositions de cette Recommandation. A la date de publication de cette Recommandation, les éditions indiquées sont valides. Toutes les Recommandations et autres références sont susceptibles d'être révisées; les utilisateurs de la présente Recommandation sont donc encouragés à envisager la possibilité d'utiliser l'édition la plus récente des Recommandations et des autres références dont la liste figure ci-après. Une liste des Recommandations UIT-T actuellement en vigueur est publiée régulièrement. Toute référence à un document cité dans la présente Recommandation, considéré comme un document autonome, ne lui confère pas le statut de Recommandation.

[IETF RFC 7970] IETF RFC 7970 (2016), *The Incident Object Description Exchange Format Version 2*.
<https://datatracker.ietf.org/doc/rfc7970/>

3 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

IANA autorité chargée de l'assignation des numéros Internet (*Internet assigned numbers authority*)

IODEF format d'échange de description d'objet incident (*incident object description exchange format*)

5 Conventions

Les termes suivants sont considérés comme équivalents:

– A l'UIT, l'emploi du futur d'obligation ("shall" en anglais) est équivalent à celui d'autres moyens d'expression de l'obligation (comme "must" en anglais), la même chose valant pour leurs formes négatives.

– A l'UIT, l'emploi du futur d'obligation ("shall" en anglais) est équivalent à l'emploi à l'IETF du mot "MUST" en anglais.

– A l'UIT, l'emploi de la forme négative du futur d'obligation ("shall not" en anglais) est équivalent à l'emploi à l'IETF des mots "MUST NOT" en anglais.

NOTE – A l'IETF, les mots "shall" et "must" (en caractères minuscules) sont employés dans les textes informatifs.

6 Description d'objet incident et format d'échange

Le paragraphe 6 définit le format d'échange de description d'objet incident (IODEF) version 2, en faisant directement référence aux sections de la norme [IETF RFC 7970] et en faisant correspondre les numéros des paragraphes et ceux des sections. Ainsi, par exemple, le paragraphe 6.x correspond à la section x de la norme [IETF RFC 7970] et leurs titres concordent aussi.

6.1 Introduction

La section 1 de la norme [IETF RFC 7970] est informative.

6.1.1 Terminologie

La section 1.1 de la norme [IETF RFC 7970] est informative.

6.1.2 Notations

La section 1.2 de la norme [IETF RFC 7970] est informative.

6.1.3 Concernant le modèle de données IODEF

La section 1.3 de la norme [IETF RFC 7970] est informative.

6.1.4 Modifications par rapport à la norme RFC 5070

La section 1.4 de la norme [IETF RFC 7970] est informative.

6.2 Types de données IODEF

La section 2 de la norme [IETF RFC 7970] est informative, mais ses sous-sections, c'est-à-dire les sections 2.1 à 2.15, sont normatives. Elles définissent les types de données suivants:

– Entiers (définis dans la section 2.1 de la norme [IETF RFC 7970])

– Nombres réels (définis dans la section 2.2 de la norme [IETF RFC 7970])

– Caractères et chaînes (définis dans la section 2.3 de la norme [IETF RFC 7970])

– Chaînes multilingues (définies dans la section 2.4 de la norme [IETF RFC 7970])

– Chaînes binaires (définies dans la section 2.5 de la norme [IETF RFC 7970])

  – Octets en Base64 (définis dans la section 2.5.1 de la norme [IETF RFC 7970])

  – Octets hexadécimaux (définis dans la section 2.5.2 de la norme [IETF RFC 7970])

– Types énumérés (définis dans la section 2.6 de la norme [IETF RFC 7970])

– Chaîne d'horodatage (définie dans la section 2.7 de la norme [IETF RFC 7970])

– Chaîne de fuseau horaire (définie dans la section 2.8 de la norme [IETF RFC 7970])

- Listes de ports (définies dans la section 2.9 de la norme [IETF RFC 7970])
- Adresse postale (définie dans la section 2.10 de la norme [IETF RFC 7970])
- Numéro de téléphone (défini dans la section 2.11 de la norme [IETF RFC 7970])
- Chaîne d'adresse électronique (définie dans la section 2.12 de la norme [IETF RFC 7970])
- Chaînes d'adresses URL (définies dans la section 2.13 de la norme [IETF RFC 7970])
- Identificateurs et références par identifiant (définis dans la section 2.14 de la norme [IETF RFC 7970])
- Logiciel (défini dans la section 2.15 de la norme [IETF RFC 7970])
  - Classe SoftwareReference (définie dans la section 2.15.1 de la norme [IETF RFC 7970])
- Extension (définie dans la section 2.16 de la norme [IETF RFC 7970])

6.3 Modèle d'information IODEF

La section 3 de la norme [IETF RFC 7970] est informative, mais ses sous-sections, c'est-à-dire de 3.1 à 3.29, sont normatives. Dans ces sous-sections sont déterminés les modèles de données suivants:

- Classe IODEF-Document (définie dans la section 3.1 de la norme [IETF RFC 7970])
- Classe Incident (définie dans la section 3.2 de la norme [IETF RFC 7970])
- Attributs communs (définis dans la section 3.3 de la norme [IETF RFC 7970])
  - attribut de restriction (défini dans la section 3.3.1 de la norme [IETF RFC 7970])
  - attribut observable-id (défini dans la section 3.3.2 de la norme [IETF RFC 7970])
- Classe IncidentID (définie dans la section 3.4 de la norme [IETF RFC 7970])
- Classe AlternativeID (définie dans la section 3.5 de la norme [IETF RFC 7970])
- Classe RelatedActivity (définie dans la section 3.6 de la norme [IETF RFC 7970])
- Classe ThreatActor (définie dans la section 3.7 de la norme [IETF RFC 7970])
- Classe Campaign (définie dans la section 3.8 de la norme [IETF RFC 7970])
- Classe Contact (définie dans la section 3.9 de la norme [IETF RFC 7970])
  - Classe RegistryHandle (définie dans la section 3.9.1 de la norme [IETF RFC 7970])
  - Classe PostalAddress (définie dans la section 3.9.2 de la norme [IETF RFC 7970])
  - Classe Email (définie dans la section 3.9.3 de la norme [IETF RFC 7970])
  - Classe Telephone (définie dans la section 3.9.4 de la norme [IETF RFC 7970])
- Classe Discovery (définie dans la section 3.10 de la norme [IETF RFC 7970])
  - Classe DetectionPattern (définie dans la section 3.10.1 de la norme [IETF RFC 7970])
- Classe Method (définie dans la section 3.11 de la norme [IETF RFC 7970])
  - Classe Reference (définie dans la section 3.11.1 de la norme [IETF RFC 7970])
- Classe Assessment (définie dans la section 3.12 de la norme [IETF RFC 7970])
  - Classe SystemImpact (définie dans la section 3.12.1 de la norme [IETF RFC 7970])
  - Classe BusinessImpact (définie dans la section 3.12.2 de la norme [IETF RFC 7970])
  - Classe TimeImpact (définie dans la section 3.12.3 de la norme [IETF RFC 7970])
  - Classe MonetaryImpact (définie dans la section 3.12.4 de la norme [IETF RFC 7970])
  - Classe Confidence (définie dans la section 3.12.5 de la norme [IETF RFC 7970])

- Classe History (définie dans la section 3.13 de la norme [IETF RFC 7970])
  - Classe HistoryItem (définie dans la section 3.13.1 de la norme [IETF RFC 7970])
- Classe EventData (définie dans la section 3.14 de la norme [IETF RFC 7970])
  - Mettre en relation les classes Incident et EventData (définies dans la section 3.14.1 de la norme [IETF RFC 7970])
  - Définition récursive d'EventData (définie dans la section 3.14.2 de la norme [IETF RFC 7970])
- Classe Expectation (définie dans la section 3.15 de la norme [IETF RFC 7970])
- Classe Flow (définie dans la section 3.16 de la norme [IETF RFC 7970])
- Classe System (définie dans la section 3.17 de la norme [IETF RFC 7970])
- Classe Node (définie dans la section 3.18 de la norme [IETF RFC 7970])
  - Classe Address (définie dans la section 3.18.1 de la norme [IETF RFC 7970])
  - Classe NodeRole (définie dans la section 3.18.2 de la norme [IETF RFC 7970])
  - Classe Counter (définie dans la section 3.18.3 de la norme [IETF RFC 7970])
- Classe DomainData (définie dans la section 3.19 de la norme [IETF RFC 7970])
  - Classe Nameservers (définie dans la section 3.19.1 de la norme [IETF RFC 7970])
  - Classe DomainContacts (définie dans la section 3.19.2 de la norme [IETF RFC 7970])
- Classe Service (définie dans la section 3.20 de la norme [IETF RFC 7970])
  - Classe ServiceName (définie dans la section 3.20.1 de la norme [IETF RFC 7970])
  - Classe ApplicationHeader (définie dans la section 3.20.2 de la norme [IETF RFC 7970])
- Classe EmailData (définie dans la section 3.21 de la norme [IETF RFC 7970])
- Classe Record (définie dans la section 3.22 de la norme [IETF RFC 7970])
  - Classe RecordData (définie dans la section 3.22.1 de la norme [IETF RFC 7970])
  - Classe RecordPattern (définie dans la section 3.22.2 de la norme [IETF RFC 7970])
- Classe WindowsRegistryKeysModified (définie dans la section 3.23 de la norme [IETF RFC 7970])
  - Classe Key (définie dans la section 3.23.1 de la norme [IETF RFC 7970])
- Classe CertificateData (définie dans la section 3.24 de la norme [IETF RFC 7970])
  - Classe Certificate (définie dans la section 3.24.1 de la norme [IETF RFC 7970])
- Classe FileData (définie dans la section 3.25 de la norme [IETF RFC 7970])
  - Classe File (définie dans la section 3.25.1 de la norme [IETF RFC 7970])
- Classe HashData (définie dans la section 3.26 de la norme [IETF RFC 7970])
  - Classe Hash (définie dans la section 3.26.1 de la norme [IETF RFC 7970])
  - Classe FuzzyHash (définie dans la section 3.26.2 de la norme [IETF RFC 7970])
- Classe SignatureData (définie dans la section 3.27 de la norme [IETF RFC 7970])
- Classe IndicatorData (définie dans la section 3.28 de la norme [IETF RFC 7970])
- Classe Indicator (définie dans la section 3.29 de la norme [IETF RFC 7970])
  - Classe IndicatorID (définie dans la section 3.29.1 de la norme [IETF RFC 7970])
  - Classe AlternativeIndicatorID (définie dans la section 3.29.2 de la norme [IETF RFC 7970])
  - Classe Observable (définie dans la section 3.29.3 de la norme [IETF RFC 7970])

- Classe IndicatorExpression (définie dans la section 3.29.4 de la norme [IETF RFC 7970])
- Expressions avec IndicatorExpression (définies dans la section 3.29.5 de la norme [IETF RFC 7970])
- Classe ObservableReference (définie dans la section 3.29.6 de la norme [IETF RFC 7970])
- Classe IndicatorReference (définie dans la section 3.29.7 de la norme [IETF RFC 7970])
- Classe AttackPhase (définie dans la section 3.29.8 de la norme [IETF RFC 7970])

6.4 Considérations relatives au traitement

La section 4 de la norme [IETF RFC 7970] est normative, bien que certaines de ses sous-sections soient informatives, comme l'indiquent les sous-sections suivantes.

6.4.1 Codage

La section 4.1 de la norme [IETF RFC 7970] est normative.

6.4.2 Espace de nom IODEF

La section 4.2 de la norme [IETF RFC 7970] est normative.

6.4.3 Validation

La section 4.3 de la norme [IETF RFC 7970] est normative.

6.4.4 Incompatibilités avec la version 1

La section 4.4 de la norme [IETF RFC 7970] est informative.

6.5 Extension du format IODEF

La section 5 de la norme [IETF RFC 7970] est informative.

La Recommandation [b-UIT-T X.1500] "Techniques d'échange d'informations sur la cybersécurité" fournit des lignes directrices relatives à l'échange d'informations sur les incidents et les indicateurs, telles que celles fournies dans la présente Recommandation (UIT-T X.1541). La présente Recommandation (UIT-T X.1541) donne le format de base pour l'échange d'informations sur les incidents, mais ne couvre pas tous les types d'utilisation conformément à la Recommandation [b-UIT-T X.1500]. Il faudra peut-être définir des extensions pour couvrir les types d'utilisation requis.

6.5.1 Extension des valeurs énumérées des attributs

La section 5.1 de la norme [IETF RFC 7970] et ses sous-sections sont normatives.

6.5.2 Extension des classes

La section 5.2 de la norme [IETF RFC 7970] et ses sous-sections sont normatives.

6.6 Questions liées à l'internationalisation

La section 6 de la norme [IETF RFC 7970] est normative.

6.7 Exemples

La section 7 de la norme [IETF RFC 7970] et ses sous-sections, qui décrivent les documents d'exemple IODEF, sont informatives.

6.8 Le modèle de données IODEF (Schéma XML)

La section 8 de la norme [IETF RFC 7970] est normative.

6.9 Considérations relatives à la sécurité

La section 9 de la norme [IETF RFC 7970] et ses sous-sections sont normatives.

Dans les mises en oeuvre conformes aux normes de l'UIT-T, le format de messagerie et le protocole sous-jacents utilisés pour l'échange d'instances du format IODEF doivent offrir les garanties nécessaires de confidentialité, d'intégrité et d'authenticité.

NOTE – A l'IETF, le mot "must" (en caractères minuscules) est employé dans les textes informatifs.

6.10 Considérations de l'autorité IANA

La section 10 de la norme [IETF RFC 7970] et ses sous-sections sont normatives.

6.11 Références

6.11.1 Références normatives

La section 11.1 de la norme [IETF RFC 7970] est informative.

Selon la présente Recommandation UIT-T, la section 11.1 de la norme [IETF RFC 7970] est informative, car l'UIT-T n'a pas arrêté de position sur ces références en ce qui concerne la présente Recommandation. Toutefois, il est admis que l'IETF a identifié un ensemble de références normatives pour la norme [IETF RFC 7970].

6.11.2 Références informatives

La section 11.2 de la norme [IETF RFC 7970] est informative.

Bibliographie

[b-UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité*.

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 téléphonique
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, 2018