|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Assemblée mondiale de normalisation  des télécommunications (AMNT-16) Hammamet, 25 octobre - 3 novembre 2016** | | CCITT/ITU-T 60th Anniversary logo |
|  | |  | |
|  | |  | |
| **SÉANCE PLÉNIÈRE** | | **Révision 1 du  Document 19-F** | |
|  | | **14 octobre 2016** | |
|  | | **Original: anglais** | |
|  | | | |
| Commission d'études 17 de l'UIT-T | | | |
| Sécurité | | | |
| rapport de la CE 17 de l'UIT-T À l'assemblÉe mondiale de normalisation des tÉlÉcommunications (AMNT-16),  PARTie I: ConsidÉrations gÉnÉrales | | | |
|  | | | |

|  |  |
| --- | --- |
| **Résumé:** | La présente contribution contient le rapport de la Commission d'études 17 de l'UIT-T à l'AMNT-16 concernant ses activités pendant la période d'études 2013-2016. |

**Note du TSB:**

Le rapport de la Commission d'études 17 à l'AMNT‑16 est présenté dans les documents suivants:

Partie I: **Document 19** **–** Considérations générales; y compris des propositions de modification de la Résolution 2 de l'AMNT (Annexe 2)

La Révision 1 de la Partie I constitue une mise à jour élaborée afin de tenir compte des résultats de la 8ème réunion de la Commission d’études 17.   
Etat: 14 octobre 2016.

Partie II: **Document 20 –** Questions qu'il est proposé d'étudier pendant la période d'études 2017‑2020

TABLE DES MATIÈRES

Page

[1 Introduction 3](#_Toc456595918)

[2 Organisation des travaux 8](#_Toc456595919)

[3 Résultats des travaux effectués pendant la période d'études 2013-2016 12](#_Toc456595920)

[4 Observations concernant les travaux futurs 42](#_Toc456595921)

[5 Mises à jour de la Résolution 2 de l'AMNT pour la période d'études 2017-2020 44](#_Toc456595922)

[ANNEXE 1 – Liste des Recommandations, Suppléments et autres documents   
produits ou supprimés pendant la période d'études 45](#_Toc456595923)

[ANNEXE 2 – Proposition de mises à jour du mandat de la Commission d'études 17   
et des rôles de Commission d'études directrice 58](#_Toc456595924)

# 1 Introduction

## 1.1 Domaine de compétence de la Commission d'études 17

L'Assemblée mondiale de normalisation des télécommunications (Dubaï, 2012) a chargé la Commission d'études 17 d'étudier 12 Questions relevant du domaine de la sécurité, y compris la cybersécurité, la lutte contre le spam et la gestion d'identité. La CE 17 est également responsable de l'application des communications entre systèmes ouverts y compris l'annuaire et les identificateurs d'objet, ainsi que des langages techniques, de leur méthode d'utilisation et d'autres problèmes connexes liés aux aspects logiciels des systèmes de télécommunication.

Conformément à l'Annexe A de la Résolution 2 de l'AMNT‑12, le mandat de la Commission d'études 17 (Sécurité) est le suivant:

*La Commission d'études 17 de l'UIT-T est chargée de renforcer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC). Elle est notamment chargée de mener des études se rapportant à la cybersécurité, la gestion de la sécurité, la lutte contre le spam et la gestion d'identité. Elle est également chargée d'étudier l'architecture et le cadre général de la sécurité, la protection des informations d'identification personnelle et la sécurité des applications et des services pour l'Internet des objets (IoT), les réseaux électriques intelligents, les téléphones intelligents, la télévision utilisant le protocole Internet (TVIP), les services web, les réseaux sociaux, l'informatique en nuage, les services bancaires sur mobile et la télébiométrie. La Commission d'études 17 est également responsable de l'application des communications entre systèmes ouverts, y compris l'annuaire et les identificateurs d'objet, des langages techniques, de leur méthode d'utilisation et d'autres problèmes connexes liés aux aspects logiciels des systèmes de télécommunication, ainsi que des tests de conformité en vue d'améliorer la qualité des Recommandations.*

Conformément à l'Annexe A de la Résolution 2 de l'AMNT‑12, la Commission d'études 17 (Sécurité) est la commission d'études directrice pour les domaines suivantes:

*– Commission d'études directrice pour la sécurité.*

*– Commission d'études directrice pour la gestion d'identité (IdM).*

*– Commission d'études directrice pour les langages et les techniques de description.*

Conformément à l'Annexe B de la Résolution 2 de l'AMNT‑12, le domaine de compétence de la CE 17 est le suivant:

*La Commission d'études 17 de l'UIT-T est chargée de renforcer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC). Elle est notamment chargée de mener des études relatives à la sécurité, y compris la cybersécurité, la lutte contre le spam et la gestion d'identité. Elle est également chargée d'étudier l'architecture et le cadre général de la sécurité, la gestion de la sécurité, la protection des informations d'identification personnelle (PII) et la sécurité des applications et des services pour l'Internet des objets (IoT), les réseaux électriques intelligents, les téléphones intelligents, la télévision utilisant le protocole Internet (TVIP), les services web, les réseaux sociaux, l'informatique en nuage, les services bancaires sur mobile et la télébiométrie. La Commission d'études 17 est également responsable de l'application des communications entre systèmes ouverts, y compris l'annuaire et les identificateurs d'objet, des langages techniques, de leur méthode d'utilisation et des autres problèmes connexes liées aux aspects logiciels des systèmes de télécommunication, ainsi que des tests de conformité en vue d'améliorer la qualité des Recommandations.*

*Dans le domaine de la sécurité, la Commission d'études 17 est responsable de l'élaboration des principales Recommandations sur la sécurité des TIC, telles que l'architecture et les cadres généraux de la sécurité; les aspects essentiels de la cybersécurité, y compris les menaces, les vulnérabilités et les risques, le traitement des incidents, l'intervention en cas d'incident et l'expertise numérique; la gestion de la sécurité, y compris la gestion des informations d'identification personnelle (PII); et la lutte contre le spam par des moyens techniques. En outre, cette commission assure la coordination générale des travaux menés par l'UIT-T dans le domaine de la sécurité.*

*En outre, la Commission d'études 17 est responsable de l'élaboration des principales Recommandations sur les aspects relatifs à la sécurité des applications et des services liés à la TVIP, aux réseaux électriques intelligents, à l'Internet des objets, aux réseaux sociaux, à l'informatique en nuage, aux téléphones intelligents, aux services bancaires sur mobile et à la télébiométrie.*

*La Commission d'études 17 est également chargée d'élaborer les principales Recommandations relatives à un modèle générique de gestion d'identité, indépendant des technologies de réseau et permettant l'échange sécurisé d'informations d'identité entre des entités. Il s'agira aussi d'étudier le processus de découverte des sources d'informations d'identité qui font autorité, les mécanismes génériques pour l'interopérabilité de divers formats d'informations d'identité, les menaces liées à la gestion d'identité, les mécanismes de lutte contre ces menaces et la protection des informations d'identification personnelle (PII) et d'élaborer des mécanismes garantissant que l'accès aux informations PII n'est autorisé que lorsque cet accès est approprié.*

*En ce qui concerne les communications entre systèmes ouverts, la Commission d'études 17 est responsable des Recommandations dans les domaines suivants:*

*• services et systèmes d'annuaire, y compris l'infrastructure de clé publique (PKI) (Recommandations UIT-T des séries F.500 et X.500);*

*• identificateurs d'objet (OID) et autorités d'enregistrement associées (Recommandations UIT-T des séries X.660 et X.670);*

*• interconnexion des systèmes ouverts (OSI), y compris la notation de syntaxe abstraite numéro un (ASN.1) (Recommandations UIT-T des séries F.400, X.200, X.400, X.600 et X.800);*

*• traitement réparti ouvert (ODP) (Recommandations UIT-T de la série X.900).*

*Dans le domaine des langages, la Commission d'études 17 est responsable des études relatives aux techniques de modélisation, de spécification et de description. Ces travaux, qui portent sur différents langages (ASN.1, SDL, MSC et URN), seront menés en fonction des besoins des commissions d'études concernées (Commissions d'études 2, 9, 11, 13, 15 et 16) et en collaboration avec elles.*

Conformément à l'Annexe C de la Résolution 2 de l'AMNT-12 (telle que modifiée par le GCNT), la liste des Recommandations relevant de la responsabilité de la Commission d'études 17 pendant la période d'études 2013-2016 est la suivante:

*• Recommandations UIT-T E.104, E.115, E.409 (conjointement avec la Commission d'études 2)*

*• Recommandations UIT-T de la série F.400; F.500-F.549*

*• Recommandations UIT-T de la série X, à l'exception des Recommandations UIT-T relevant de la responsabilité des Commissions d'études 2, 11, 13, 15 et 16*

*• Recommandations UIT-T de la série Z, à l'exception des Recommandations UIT-T de la série Z.300 et de la série Z.500.*

## 1.2 Equipe de direction et réunions de la Commission d'études 17

L'AMNT-12 a désigné M. Arkadiy KREMER (Fédération de Russie) en tant que Président de la Commission d'études 17 et a désigné neuf Vice-Présidents, à savoir: Khalid BELHOUL (Emirats arabes unis), Mohamed M.K. ELHAJ (Soudan), Mario German FROMOW RANGEL (Mexique), Antonio GUIMARAES (Brésil), Zhaoji LIN (Chine), Patrick MWESIGWA (Ouganda), Koji NAKAO (Japon), Sacid SARIKAYA (Turquie) et Heung Youl YOUM (Corée). M. FROMOW RANGEL n'a participé à aucune réunion de la Commission d'études 17.

La Commission d'études 17 a tenu huit réunions plénières pendant la période d'études (voir le Tableau 1).

TABLEau 1

Réunions de la Commission d'études 17 et de ses Groupes de travail

| Réunions | Date | Rapports |
| --- | --- | --- |
| Commission d'études 17 | Genève, 17-26 avril 2013 | COM 17-R 1 à R 6 |
| Commission d'études 17 | Genève, 28 août - 4 septembre 2013 | COM 17-R 9 à R 22 |
| Commission d'études 17 | Genève, 15-24 janvier 2014 | COM 17-R 23 à R 29 |
| Commission d'études 17 | Genève, 17-26 septembre 2014 | COM 17-R 30 à R 36 |
| Commission d'études 17 | Genève, 8-17 avril 2015 | COM 17-R 37 à R 45 |
| Commission d'études 17 | Genève, 8-17 septembre 2015 | COM 17-R 46 à R 57 |
| Commission d'études 17 | Genève, 14-23 mars 2016 | COM 17-R 58 à R 66 |
| Commission d'études 17 | Genève, 29 août - 7 septembre 2016 | COM 17-R 67 à R 80 |

L'équipe de direction s'est réunie à chaque réunion de la Commissions d'études 17.

Par ailleurs, un grand nombre de réunions de Rapporteur (y compris les réunions électroniques) ont été organisées en divers lieux pendant la période d'études (voir le Tableau 1-bis).

TABLEau 1-bis

Réunions de Rapporteur relevant de la Commission d'études 17 organisées pendant la période d'études

| Date | Lieu/Hôte | Question(s) | Titre de l'évènement |
| --- | --- | --- | --- |
| 14-01-2013 | Corée (Rép. de) [Séoul]/ Soonchunhyang University et KISA | 3/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 22-01-2013 -  24-01-2013 | Chine [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 23-01-2013 -  25-01-2013 | *Réunion électronique* | 4/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 19-02-2013 -  22-02-2013 | Suisse [Genève]/UIT | 8/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 17-06-2013 -  21-06-2013 | Corée (Rép. de) [Séoul]/Korean Agency for Technology and Standards (KATS) | 11/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 avec l'ISO/CEI JCT 1/SC 6 |
| 02-07-2013 -  03-07-2013 | *Réunion électronique* | 4/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 08-07-2013 -  10-07-2013 | Chine [Guangzhou]/China Telecom | 8/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 09-07-2013 -  10-07-2013 | France [Paris]/LegalBox | 11/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 |
| 04-12-2013 -  05-12-2013 | Corée (Rép. de) [Séoul]/TOZ | 3/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 17-02-2014 -  21-02-2014 | Canada [Ottawa]/Ericsson | 11/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 avec l'ISO/CEI JTC 1/SC 6/WG10 |
| 07-04-2014 -  11-04-2014 | Hongkong [Chine]/ISO/CEI JTC 1/SC 27 | 3/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 avec l'ISO/CEI JTC 1/SC 27/WG5 |
| 07-05-2014 -  08-05-2014 | *Réunion électronique* | 10/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 17-06-2014 -  18-06-2014 | Etats-Unis [Charlotte, Caroline du Nord]/Bank of America | 10/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 24-06-2014 -  26-06-2014 | Corée (Rép. de) [Séoul]/KR organizations | 6/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 25-06-2014 -  26-06-2014 | Corée (Rép. de) [Séoul]/KR organizations | 7/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 7/17 |
| 25-06-2014 -  26-06-2014 | Corée (Rép. de) [Séoul]/KR organizations | 3/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 01-07-2014 -  03-07-2014 | Chine [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 16-07-2014 -  17-07-2014 | *Réunion électronique* | 4/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 16-07-2014 | *Réunion électronique* | 11/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 |
| 20-10-2014 -  24-10-2014 | Royaume-Uni [Londres]/British Standards Institution | 11/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 avec l'ISO/CEI JTC 1/ SC 6/WG10 |
| 15-12-2014 -  17-12-2014 | Chine [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 15-01-2015 -  16-01-2015 | Corée (Rép. de) [Séoul]/Telecommunications Technology Association (TTA) | 3/17, 6/17 | Réunions intérimaires des Groupes du Rapporteur pour les Questions 6/17 et 3/17 |
| 27-01-2015 -  28-01-2015 | *Réunion électronique* | 4/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 29-01-2015 | *Réunion électronique* | 10/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 02-02-2015 | *Réunion électronique* | 10/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 05-02-2015 | *Réunion électronique* | 10/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 25-05-2015 -  29-05-2015 | Belgique [Gand]/Ghent University - iMinds | 11/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 avec l'ISO/CEI JTC 1/ SC 6/WG10 |
| 09-07-2015 -  10-07-2015 | *Réunion électronique* | 4/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 09-07-2015 -  10-07-2015 | Corée (Rép. de) [Séoul]/KISA | 6/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 09-07-2015 | Corée (Rép. de) [Séoul]/KISA | 3/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 16-07-2015 -  17-07-2015 | Chine [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 22-07-2015 -  24-07-2015 | Etats-Unis [New York]/Aetna | 10/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 07-01-2016 -  08-01-2016 | Corée (Rép. de) [Séoul]/TOZ | 10/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 07-01-2016 -  08-01-2016 | Corée (Rép. de) [Séoul]/TOZ | 3/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 07-01-2016 -  08-01-2016 | Corée (Rép. de) [Séoul]/TOZ | 6/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 18-01-2016 -  19-01-2016 | *Réunion électronique* | 4/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 29-02-2016 -  04-03-2016 | Chine [Xian]/Standardization Administration of the People's Republic of China (SAC) | 11/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 avec l'ISO/CEI JTC 1/SC 6/WG10 |
|  |  |  |  |
| 28-06-2016 -  29-06-2016 | Corée (Rép. de) [Séoul]/KISA | 3/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 28-06-2016 -  29-06-2016 | Corée (Rép. de) [Séoul]/KISA | 2/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 2/17 |
| 28-06-2016 -  29-06-2016 | Corée (Rép. de) [Séoul]/KISA | 7/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 7/17 |
| 28-06-2016 -  29-06-2016 | Corée (Rép. de) [Séoul]/KISA | 6/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 30-06-2016 -  01-07-2016 | Chine [Guangzhou]/China Telecom | 8/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 14-07-2016 -  15-07-2016 | Etats-Unis [New York]/Aetna | 10/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 18-07-2016 | *Réunion électronique* | 4/17 | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |

# 2 Organisation des travaux

## 2.1 Organisation des études et répartition des travaux

**2.1.1** A la première réunion qu'elle a tenue pendant la période d'études, la Commission d'études 17 a décidé d'établir cinq groupes de travail.

**2.1.2** Le Tableau 2 donne le numéro et le nom de chaque Groupe de travail, ainsi que le numéro des Questions qui lui ont été confiées et le nom de son Président.

**2.1.3** Le Tableau 3 fournit la liste des autres groupes créés par la Commission d'études 17 pendant la période d'études.

**2.1.4** Conformément à la Résolution 54 de l'AMNT-12, lors de sa réunion d'avril 2015, la CE 17 a créé le Groupe régional de la CE 17 pour l'Afrique; voir le § 3.3.5.

Pendant la période d'études, deux **Activités conjointes de coordination (JCA)** proposées par la Commission d'études 17 ont poursuivi leurs travaux, avec l'aval du GCNT.

– **Activité conjointe de coordination sur la gestion d'identité (JCA-IdM)**

La JCA-IdM a poursuivi ses activités menées pendant la période d'études précédente avec comme objectif de coordonner les travaux de l'UIT‑T sur la gestion d'identité (IdM) menés en collaboration avec des organismes extérieurs. Les principales réalisations de la JCA-IdM sont présentées au § 3.3.4.1.

**– Activité conjointe de coordination sur la protection en ligne des enfants (JCA‑COP)**

La JCA-COP a poursuivi ses activités menées pendant la période d'études précédente avec comme objectif de coordonner les travaux de l'UIT‑T sur la protection en ligne des enfants (COP) menés dans les différentes commissions d'études de l'UIT‑T, et d'assurer la liaison avec l'UIT‑R et l'UIT‑D ainsi qu'avec le Groupe de travail du Conseil sur la protection en ligne des enfants. Les principales réalisations de la JCA-COP sont présentées au § 3.3.4.2.

**2.1.5** Pendant la période d'études, la Commission d'études 17 a poursuivi deux **projets**.

– **Projet ASN.1**

Le projet ASN.1, établi pendant la période d'études 2001-2004, a permis de continuer d'apporter une assistance aux utilisateurs de l'ASN.1 (Recommandations UIT‑T des séries X.680, X.690 et X.890) à l'intérieur et à l'extérieur de l'UIT‑T et d'encourager l'utilisation de l'ASN.1 dans un grand nombre d'entités du secteur privé et d'organismes de normalisation. Les principaux résultats obtenus dans le cadre de ce projet sont présentés au § 3.4.1.

– **Projet OID**

Le projet OID, établi pendant la période d'études 2001-2004, a permis de continuer d'apporter une assistance et un soutien aux utilisateurs d'identificateurs d'objet (OID) enregistrés conformément aux Recommandations des séries X.660 et X.670 à l'intérieur et à l'extérieur de l'UIT‑T. Les principaux résultats obtenus dans le cadre de ce projet sont présentés au § 3.4.2.

TABLEau 2

Organisation de la Commission d'études 17

|  |  |  |  |
| --- | --- | --- | --- |
| Désignation | Questions  à étudier | Nom du Groupe de travail | Président du Groupe de travail |
| GT 1/17 | 1, 2, 3 | Sécurité de base | Koji NAKAO |
| GT 2/17 | 4, 5 | Sécurité des réseaux et des informations | Sacid SARIKAYA |
| GT 3/17 | 8, 10 | Gestion d'identité et sécurité de l'informatique en nuage | Heung Youl YOUM |
| GT 4/17 | 6, 7, 9 | Sécurité des applications | Antonio GUIMARAES |
| GT 5/17 | 11, 12 | Langages formels | Zhaoji LIN |

TABLEau 3

Autres groupes (le cas échéant)

|  |  |  |
| --- | --- | --- |
| Nom du Groupe | Président | Vice-Présidents |
| JCA-IdM | Coprésidents: Richard BRACKNEY(1), Jon SHAMAH(2), Hiroshi TAKECHI(3), Abbie BARBIR(4) |  |
| JCA-COP | Coprésidents: Ashley HEINEMAN(5), Philip RUSHTON |  |
| SG17-RG-AFR | Michael KATUNDU | Mohamed M. K. Elhaj, Patrick Mwesigwa, Mohamed Touré |
| Projet ASN.1 | Chef de projet: Paul THORPE |  |
| Projet OID | Chef de projet: Olivier DUBUISSON |  |

NOTES:

(1) Coprésident décédé le 12 septembre 2013.

(2) Coprésident jusqu'en septembre 2013.

(3) Coprésident depuis le 4 septembre 2013.

(4) Coprésident depuis le 24 janvier 2014.

(5) Coprésident jusqu'au 31 janvier 2016.

## 2.2 Questions et Rapporteurs

**2.2.1** L'AMNT-12 a confié à la Commission d'études 17 les 12 Questions dont la liste figure dans le Tableau 4 et la CE 17 a désigné les Rapporteurs et Rapporteurs associés dont les noms sont indiqués.

**2.2.2** Les Questions dont la liste figure dans le Tableau 5 ont été adoptées pendant cette période d'études.

Note – Aucune nouvelle Question n'a été adoptée, mais les Questions 6/17, 8/17 et 12/17 ont été modifiées pendant la période d'études.

**2.2.3** Les Questions dont la liste figure dans le Tableau 6 ont été supprimées pendant cette période d'études.

TABLEau 4

Commission d'études 17 – Questions confiées par l'AMNT-12 et Rapporteurs

| Question | Titre de la Question | GT | Rapporteur |
| --- | --- | --- | --- |
| 1/17 | Coordination en matière de sécurité des télécommunications/TIC | 1/17 | Mohamed M. K. ELHAJ  Rapporteurs associés: Hua JIANG(7), Young Wha KIM(2), Cai CHEN(13), Isaac Kobina KWARKO, Yiwen WANG(12) |
| 2/17 | Architecture et cadre de sécurité | 1/17 | Patrick Mwesigwa  Rapporteurs associés: Zhiyuan HU(1), Dmitry V. KOSTROV(7), Heung Ryong Oh |
| 3/17 | Gestion de la sécurité des informations de télécommunication | 1/17 | Miho Naganuma  Rapporteur associé: Kyeong Hee OH |
| 4/17 | Cybersécurité | 2/17 | Youki Kadobayashi  Rapporteurs associés: Michael KATUNDU(1), Jong Hyun Kim, Ibrahim Hamza AL MALLOUHI |
| 5/17 | Lutte contre le spam par des moyens techniques | 2/17 | Hongwei Luo(10)  Yanbin ZHANG(11)  Rapporteur associé: Seokung YOON(3) |
| 6/17 | Aspects relatifs à la sécurité des services de télécommunication ubiquitaires | 4/17 | Jonghyun Baek  Rapporteurs associés: Yutaka Miyake, Bo YU(12) |
| 7/17 | Services applicatifs sécurisés | 4/17 | Jae Hoon Nah  Rapporteurs associés: Lijun LIU(5) Huirong TIAN(8) |
| 8/17 | Sécurité de l'informatique en nuage | 3/17 | Liang Wei  Rapporteurs associés: Mark JEFFREY(9), Victor KUTUKOV |
| 9/17 | Télébiométrie | 4/17 | John George CARAS  Rapporteur associé: Yong Nyuo SHIN |
| 10/17 | Architecture et mécanismes de gestion d'identité | 3/17 | Abbie Barbir  Rapporteurs associés: Richard BRACKNEY(6), Hiroshi TAKECHI(4), Junjie XIA(3) |
| 11/17 | Technologies génériques utilisées pour les applications sécurisées | 5/17 | Erik Andersen  Rapporteur associé: Jean-Paul LEMAIRE |
| 12/17 | Langages formels pour les logiciels de télécommunication et les tests | 5/17 | Dieter Hogrefe  Rapporteurs associés: Gunter MUSSBACHER,  Rick Reed |

Note:

(1) Rapporteur associé désigné le 17 avril 2015

(2) Rapporteur associé désigné le 8 avril 2015

(3) Rapporteur associé désigné le 24 janvier 2014

(4) Rapporteur associé désigné le 4 septembre 2013

(5) Rapporteur associé désigné le 9 octobre 2015

(6) Rapporteur associé décédé le 12 septembre 2013

(7) Rapporteur associé jusqu'en mars 2015

(8) Rapporteur associé ayant quitté ses fonctions le 27 septembre 2015

(9) Rapporteur associé ayant quitté ses fonctions le 26 février 2016

(10) Rapporteur jusqu'au 17 septembre 2015

(11) Rapporteur désigné le 14 mars 2016

(12) Rapporteur associé désigné le 23 mars 2016

(13) Rapporteur associé désigné le 17 septembre 2015.

TABLEau 5

Commission d'études 17 – Nouvelles Questions adoptées et Rapporteurs

|  |  |  |  |
| --- | --- | --- | --- |
| Question | Titre de la Question | GT | Rapporteur |
| Néant |  |  |  |

TABLEau 6

Commission d'études 17 – Questions supprimées

|  |  |  |  |
| --- | --- | --- | --- |
| Question | Titre de la Question | Rapporteur | Résultats |
| Néant |  |  |  |

# 3 Résultats des travaux effectués pendant la période d'études 2013-2016

## 3.1 Généralités

Depuis le début de la période d'études et jusqu'à sa réunion de septembre 2016, la Commission d'études 17 a examiné 592 contributions et un grand nombre de documents temporaires (TD) et de notes de liaison.

Sur la base de ces documents, au 7 septembre 2016, la Commission d'études 17 a:

– élaboré 49 nouvelles Recommandations;

– révisé 69 Recommandations existantes;

– modifié 8 Recommandations;

– supprimé 3 Recommandations;

– élaboré 13 Suppléments;

– produit 19 Corrigenda techniques;

– élaboré 3 Rapports techniques (aucun Manuel n'a été élaboré).

## 3.2 Principaux résultats obtenus

Les principaux résultats obtenus par la Commission d'études 17 au titre des diverses Questions qu'elle devait étudier sont brièvement résumés ci-dessous (voir le Tableau 6a). Les réponses officielles aux Questions sont données dans un tableau synoptique figurant dans l'Annexe 1 du présent rapport.

**Tableau 6a – Résumé des résultats obtenus pendant cette période d’études**

| **Question** | **Recomman­dations** | | **Amen-dements** | **Corri­genda** | **Suppléments** | | **Autres publica­tions** | **Projets de Recommandation ayant fait l’objet d’un consentement/d’une détermination à la dernière réunion**  **(voir le Tableau 8)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nou-velles** | **Révi­sées** | **Nou-veaux** | **Révi­sés** |
| **1/17** | --- | --- | --- | --- | --- | --- | 1 TR | --- |
| **2/17** | 4 |  |  |  | 1 |  |  |  |
| **3/17** |  | 1 |  |  | 1 |  |  | X.1058 (X.gpim)\* |
| **4/17** | 9 | 3 | 8 |  | 2 | 1 |  | X.1212 (X.cogent)\*  X.1550 (X.nessa)\* |
| **5/17** | 2 |  |  | 1 | 2 |  |  |  |
| **6/17** | 2 |  |  | 2 | 3 |  |  | X.1126 (X.msec-11)\*  X.1362 (X.iotsec-1)\*  X.1373 (X.itssec-1)\* |
| **7/17** | 8 |  |  |  | 2 |  |  |  |
| **8/17** | 5 | 1 |  |  |  |  |  |  |
| **9/17** | 3 |  |  |  |  |  |  | X.1080.0 (X.pbact)\* |
| **10/17** | 4 |  |  |  |  |  |  |  |
| **11/17** | 4 | 23 |  | 14 |  |  | 1 TR |  |
| **12/17** | 6 | 30 |  |  |  | 1 | 4 IG | Z.100 Annexe F1 (révisée)  Z.100 Annexe F2 (révisée)  Z.100 Annexe F3 (révisée) |

Notes:

\* Projet de Recommandation relevant de la procédure TAP, les autres relèvent de la procédure AAP

TR Rapport technique

IG Guide de mise en oeuvre.

a) Question 1/17: Coordination en matière de sécurité des télécommunications/TIC

L'objectif de cette Question était toujours de coordonner et d'organiser toutes les activités relatives à la sécurité au sein de l'UIT-T, ainsi que d'élaborer et de mettre à jour des documents pour faciliter la coordination et la sensibilisation. Avant tout, le groupe chargé de la Question 1/17 fait office de contact de la CE 17 pour les questions de coordination en matière de sécurité.

Aucune Recommandation ne relève de la Question 1/17.

Pendant la présente période d'études, le groupe chargé de la Question 1/17 a élaboré et mis à jour plusieurs documents de sensibilisation, de promotion et de référence, que l'UIT-T considère comme utiles pour promouvoir ses travaux concernant la sécurité et les résultats de ces travaux. Ces documents sont par exemple:

– Le manuel sur la sécurité, *Sécurité dans les télécommunications et les technologies de l'information – Aperçu des problèmes et présentation des Recommandations UIT‑T existantes sur la sécurité dans les télécommunications*, qui présente les principaux travaux réalisés par les commissions d'études de l'UIT-T dans le domaine de la sécurité. Pendant la période d'études, le groupe chargé de la Question 1/17 a aidé le TSB à réaliser une mise à jour de ce manuel. La 6ème édition a été publiée en tant que Rapport technique.

– Le *Recueil de Recommandations sur la sécurité*, qui est un document en ligne en cinq parties comportant: un catalogue des Recommandations UIT‑T approuvées relatives à la sécurité des télécommunications, un extrait des définitions relatives à la sécurité approuvées par l'UIT‑T, un récapitulatif des commissions d'études de l'UIT-T menant des activités liées à la sécurité, un récapitulatif des textes relatifs à la sécurité approuvés récemment ou en cours d'approbation et un récapitulatif des autres activités de l'UIT liées à la sécurité.

– La *Feuille de route sur les normes de sécurité*, qui est une ressource en ligne qui donne des informations sur les normes de sécurité des technologies de l'information et de la communication (TIC) existantes et sur les travaux en cours dans les principales organisations de normalisation. La feuille de route comprend six parties:

– Organisations de normalisation des TIC et leurs travaux: cette partie contient des informations sur la structure de la Feuille de route et sur chaque organisation de normalisation citée. Elle comprend en outre des liens vers les glossaires et sites terminologiques existants concernant la sécurité;

– Normes approuvées sur la sécurité des TIC: cette partie contient une base de données consultable des normes de sécurité approuvées;

– Normes de sécurité en cours d'élaboration;

– Besoins futurs et propositions de nouvelle norme de sécurité;

– Bonnes pratiques; et

– Situation en matière de gestion d'identité (IdM): normes sur la gestion d'identité, organisations et analyse des lacunes.

Outre les informations sur les Recommandations UIT‑T relatives à la sécurité et sur les travaux associés, la feuille de route contient actuellement des informations sur les activités de normalisation des organismes suivants: ISO/CEI, ATIS, ENISA, ETSI, IEEE, IETF, OASIS, 3GPP et 3GPP2.

– Un Rapport technique sur l'*utilisation efficace des normes de sécurité*, qui vise à aider les utilisateurs, en particulier ceux des pays en développement, à mieux comprendre les avantages que présente l'utilisation des Recommandations UIT-T relatives à la sécurité dans divers contextes (par exemple pour les affaires ou le commerce, dans le secteur public ou le secteur privé). Il traite de l'utilisation des normes relatives à la sécurité dans diverses applications et sensibilise le lecteur à l'utilité et à l'importance des normes fondamentales dans le domaine de la sécurité, par exemple les normes sur l'architecture. On y trouve aussi une méthodologie, des définitions et d'autres orientations de haut niveau. D'une manière générale, l'objectif est d'encourager une utilisation efficace de ces normes.

Un mini-atelier organisé par l'Union postale universelle (UPU) et l'UIT a eu lieu le 21 janvier 2014 pendant une réunion de la CE 17 de l'UIT‑T. La Résolution 11 de l'AMNT-12 définit la collaboration, mise en place il y a longtemps, entre l'UIT-T et l'UPU. Les participants à l'atelier se sont penchés sur plusieurs sujets d'intérêt mutuel, notamment: .PostID, architecture des objets numériques, financement des télécommunications, paiement sur mobile sécurisé, messagerie électronique sécurisée et collaboration UIT-UPU.

L'UIT a accueilli un atelier sur le thème: "Enjeux de la normalisation, dans le domaine de la sécurité des TIC, pour les pays en développement" à Genève (Suisse), les 15 et 16 septembre 2014. L'objectif principal de cet atelier était de présenter et d'examiner les enjeux liés à la sécurité des TIC, en particulier pour les pays en développement. L'analyse des enjeux liés à la sécurité des TIC et le renforcement des capacités pour la mise en oeuvre des normes internationales sur la sécurité des TIC ont été au coeur des débats. L'atelier visait à renforcer les compétences en matière de normalisation en donnant des conseils concernant le contenu technique des normes internationales sur la sécurité des TIC et les bonnes pratiques associées. Il visait aussi à renforcer la collaboration entre les secteurs de la normalisation et du développement de l'UIT (UIT‑T et UIT‑D) concernant les activités liées à la sécurité, en plus de tirer parti de la collaboration entre l'UIT-T et d'autres organismes de normalisation. Les principaux sujets examinés lors de l'atelier ont été les suivants: cybersécurité, protection des données, services de confiance et informatique en nuage y compris les mégadonnées, l'accent ayant été mis sur la normalisation et le rôle joué par les TIC dans la protection des infrastructures essentielles.

L'UIT a accueilli un atelier sur le thème *Les enjeux de la cybersécurité mondiale et la collaboration pour un renforcement efficace de la cybersécurité dans les pays en développement*(le 8 septembre 2015 après-midi), organisé en collaboration avec la CE 2 de l'UIT‑D, à l'occasion de réunions de la CE 17 de l'UIT-T et de la CE 2 de l'UIT-D. Des représentants de premier plan de la CE 17 ont participé activement à l'atelier: Mme Miho Naganuma (modérateur de l'atelier), M. Mohamad Elhaj et M. Patrick Mwesigwa (modérateurs des deux principales sessions). Cet atelier a permis de fournir plusieurs indications importantes sur les problèmes de cybersécurité que rencontrent les pays en développement et de mettre en évidence les bonnes pratiques à suivre pour faire face à ces problèmes. Il a été l'occasion de montrer qu'il existe un bon esprit de collaboration entre l'UIT‑T et l'UIT‑D, et il s'est achevé sur un engagement des participants à élargir cette collaboration. La CE 17 a transmis le rapport commun de l'atelier à toutes les organisations régionales.

Un atelier UIT-UAT sur la stratégie relative à la cybersécurité dans les pays africains s’est tenu à Khartoum (Soudan) du 24 au 26 juillet 2016. Cet atelier régional a été organisé par l’Union internationale des télécommunications (UIT) en collaboration avec l’Union africaine des télécommunications (UAT), à l’invitation de la National Telecommunication Corporation (NTC) du Soudan. Le principal objectif de l’atelier était de permettre aux pays de renforcer leurs capacités et d’échanger des données d’expérience et de bonnes pratiques ainsi que de fournir des informations sur l’état de la mise en oeuvre des stratégies existantes relatives à la cybersécurité, d’identifier les éventuels besoins et de présenter une marche à suivre. Ont assisté à cet atelier plus de 110 participants issus de 19 pays, d’organisations régionales ou internationales, d’entreprises du secteur privé et d’acteurs nationaux du Soudan.

Enfin, une coordination active a été établie avec tous les groupes chargés des Questions de la Commission d'études 17, toutes les autres commissions d'études concernées par la sécurité et les organisations de normalisation extérieures participant aux travaux de normalisation de la sécurité des TIC.

b) Question 2/17: Architecture et cadre de sécurité

Les Recommandations UIT-T X.800, X.802 et X.803 traitent de la sécurité dans le contexte des systèmes ouverts. L'architecture de sécurité des systèmes assurant des communications de bout en bout est décrite dans la Recommandation UIT-T X.805. Un ensemble complet de cadres de sécurité détaillés, couvrant des aspects tels que l'authentification, le contrôle d'accès, la non-répudiation, la confidentialité, l'intégrité, l'audit et les alarmes de sécurité, a été établi (Recommandations UIT-T X.810, X.811, X.812, X.813, X.814, X.815 et X.816). Pour assurer la sécurité générique des couches supérieures (GULS), les Recommandations UIT-T X.830, X.831, X.832, X.833, X.834 et X.835 ont été élaborées. En coopération avec l'ISO/CEI JTC 1/SC 27, les Recommandations UIT-T X.841, X.842 et X.843 relatives aux objets d'information de sécurité et aux services de tiers de confiance ont été également établies.

Pendant la présente période d'études, quatre nouvelles Recommandations et un nouveau Supplément ont été élaborés au titre de la Question 2/17:

• Recommandation UIT‑T X.1033, *Lignes directrices sur la sécurité des différents services d'information fournis par les opérateurs*, qui donne des lignes directrices sur la sécurité des différents services d'information fournis par les opérateurs de télécommunication. Elle porte sur la classification des différents services d'information, les exigences liées à la sécurité, les mécanismes et la coordination.

• Recommandation UIT‑T X.1037, *Lignes directrices techniques concernant la sécurité dans le cadre du déploiement du protocole IPv6,* qui fournit un ensemble de lignes directrices techniques concernant la sécurité à l'intention des organisations de télécommunication qui déploieront et exploiteront des réseaux et services IPv6. Cette Recommandation traite de la question de savoir comment les organisations de télécommunications peuvent déployer en toute sécurité des installations de réseau et comment garantir un fonctionnement sûr dans l'environnement IPv6.

• Recommandation UIT-T X.1038, *Exigences de sécurité et architecture de référence pour les réseaux pilotés par logiciel*, qui définit des exigences de sécurité et une architecture de référence pour les réseaux pilotés par logiciel (SDN) afin de protéger ces réseaux. Cette Recommandation identifie les nouvelles menaces de sécurité ainsi que les menaces sur la sécurité des réseaux traditionnels qui pèsent sur les réseaux SDN, définit des exigences de sécurité, propose des mesures de protection possibles face aux nouvelles menaces de sécurité et présente une architecture de référence pour la sécurité des réseaux SDN.

• Recommandation UIT-T X.1039, *Mesures de sécurité techniques pour la mise en oeuvre des dimensions de sécurité UIT-T X.805*, qui vise à définir un ensemble de mesures de sécurité pour la mise en oeuvre des dimensions de haut niveau. Elle fournit en outre des orientations pour la mise en oeuvre de mesures de sécurité sur le plan technique qui peuvent être utilisées pour améliorer les capacités des organisations en matière de sécurité. L'ensemble des mesures de sécurité décrites dans cette Recommandation pourrait aider les organisations à gérer les risques pour la sécurité de l'information et à mettre en oeuvre les dimensions sur le plan technique. Cette Recommandation s'adresse notamment, mais non exclusivement, aux responsables de la mise en oeuvre des dimensions de sécurité de l'information dans une organisation.

• Supplément X.Suppl.23, *Supplément à la Recommandation UIT-T X.1037 sur des lignes directrices concernant la gestion de la sécurité dans le cadre de la mise en place d'un environnement IPv6 dans les organisations de télécommunication*, qui fournit des lignes directrices concernant la gestion de la sécurité dans le cadre de la mise en place d'un environnement IPv6 dans les organisations de télécommunication afin de garantir la protection des informations dans les réseaux et la protection de l'infrastructure réseau d'appui lors du passage du protocole IPv4 au protocole IPv6 et de la mise en place d'un environnement IPv6.

c) Question 3/17: Gestion de la sécurité des informations de télécommunication

Le groupe chargé de la Question 3/17 étudie la gestion de la sécurité des informations de télécommunication, sachant que pour les organisations de télécommunication, les informations et les processus d'appui, les installations de télécommunication, les réseaux et les supports de transmission constituent des actifs de télécommunication importants pour leurs activités. La Recommandation UIT‑T X.1051, qui contient des lignes directrices pour la gestion de la sécurité de l'information, est une Recommandation essentielle qui a été révisée en collaboration avec l'ISO/CEI.

Pendant la présente période d'études, une Recommandation révisée et un nouveau Supplément ont été élaborés au titre de la Question 3/17:

• Recommandation UIT‑T X.1051 (révisée)*, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information fondés sur la norme ISO/CEI 27002 pour les organisations de télécommunication*, qui établit des lignes directrices et des principes généraux pour instaurer, mettre en oeuvre, maintenir et améliorer les contrôles de sécurité de l'information fondés sur la norme ISO/CEI 27002 au sein d'organisations de télécommunication et donne des indications de base pour la mise en oeuvre des contrôles de sécurité de l'information au sein des organisations de télécommunication, afin de garantir la confidentialité, l'intégrité et la disponibilité des installations et services de télécommunication ainsi que des informations gérées, traitées ou stockées par ces installations et services.

• Supplément X.Suppl.27, *Supplément à la Recommandation UIT-T X.1054 sur les bonnes pratiques pour la mise en oeuvre de la Recommandation UIT-T X.1054 | ISO /CEI 27014 sur la gouvernance de la sécurité de l'information – Le cas du Burkina Faso*, qui décrit la mise en oeuvre de la Recommandation UIT-T X.1054 | ISO /CEI 27014 pour la gouvernance de la sécurité de l’information du Conseil des Ministres électronique du Burkina Faso, et présente un exemple de bonnes pratiques dans la mise en oeuvre de la Recommandation UIT-T X.1054 | ISO /CEI 27014.

Le groupe chargé de la Question 3/17 travaille en étroite collaboration avec l'ISO/CEI JTC 1/SC 27/WG 1 sur la gestion de la sécurité de l'information.

Cette Question diffère de celles confiées à la Commission d'études 2 en ce que la CE 2 s'occupe de l'échange d'informations de gestion du réseau entre les éléments du réseau et les systèmes de gestion et entre les systèmes de gestion dans un environnement de réseau de gestion des télécommunications (RGT) alors que la Question 3/17 porte principalement sur la protection des actifs de l'entreprise, y compris les informations et les processus, en vue de la gestion de la sécurité de l'information.

d) Question 4/17: Cybersécurité

Le groupe chargé de la Question 4/17 étudie la cybersécurité, sachant que le paysage des télécommunications évolue constamment, tout comme les exigences associées relatives à la sécurité des télécommunications/TIC. Dans le cyberenvironnement, il existe un fort besoin de sécurisation des protocoles, infrastructures et applications qui sont utilisés pour nos communications quotidiennes. La cybersécurité repose sur la sécurisation et la protection des services et des informations personnelles, sur la protection des informations d'identification personnelle et sur la fourniture d'une garantie des informations entre les entités en interaction. Le groupe chargé de la Question 4/17 a élaboré un ensemble de spécifications de premier plan pour l'échange sécurisé d'informations sur la cybersécurité, qui est nécessaire pour pouvoir mesurer et suivre en permanence la sécurité. Ces spécifications sont appelées CYBEX (Cybersecurity Information Exchange, en français échange d'informations sur la cybersécurité). Le groupe chargé de la Question 4/17 étudie également d'autres questions liées à la cybersécurité, par exemple la détection du trafic anormal, l'atténuation des effets des botnets et la détermination de l'origine des attaques (y compris le retraçage).

Le groupe chargé de la Question 4/17 a assumé la responsabilité première de la mise en oeuvre de la Résolution 50 de l'AMNT-12 (Cybersécurité) et a partagé avec le groupe chargé de la Question 3/17 la responsabilité de la mise en oeuvre de la Résolution 58 de l'AMNT‑12 (Encourager la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement).

Pendant la présente période d'études, neuf nouvelles Recommandations, trois Recommandations révisées, huit nouveaux Amendements, deux nouveaux Suppléments et un Supplément révisé ont été élaborés au titre de la Question 4/17:

• Recommandation UIT-T X.1208, *Indicateur de risque de cybersécurité en vue de renforcer la confiance et la sécurité dans l'utilisation des télécommunications/technologies de l'information et de la communication*, qui décrit une méthode destinée à être utilisée par les organisations pour calculer une mesure de risque à partir d'indicateurs de cybersécurité et qui dresse une liste d'indicateurs potentiels de cybersécurité. La Recommandation UIT‑T X.1208 ne propose pas l'utilisation d'un indice ou d'un seul indicateur pour exprimer les capacités d'une organisation en matière de cybersécurité.

• Recommandation UIT-T X.1210, *Description générale des mécanismes de résolution des problèmes de sécurité à la source dans les réseaux fondés sur le protocole Internet*, qui décrit les mécanismes de résolution des problèmes de sécurité à la source ainsi que les critères de sélection et les lignes directrices de base en matière de sécurité concernant ces mécanismes.

• Recommandation UIT-T X.1211, *Techniques pour prévenir les attaques sur le web*, qui décrit les techniques pouvant atténuer les attaques sur le web qui se produisent lorsque les vulnérabilités des serveurs d'hébergement de site web sont exploitées et que des codes malveillants sont injectés, lesquels peuvent ensuite infecter les ordinateurs des utilisateurs.

• Recommandation UIT-T X.1303*bis*, *Protocole d'alerte commun (CAP 1.2)*, qui définit un format simple mais général pour échanger, sur tout type de réseau, des alertes d'urgence pour tous les risques et des alertes destinées au public. Le protocole CAP permet de diffuser simultanément un message d'alerte cohérent sur un grand nombre de systèmes d'alerte différents, ce qui augmente l'efficacité de l'alerte tout en simplifiant la tâche d'alerte.

• Amendements 3, 4, 5, 6, 7, 8, 9, 10 à la Recommandation UIT‑T X.1500: *Techniques révisées d'échange d'informations sur la cybersécurité structurées*, qui dressent une liste des techniques structurées révisées d'échange d'informations sur la cybersécurité, qui a été créée afin d'être actualisée en permanence, au fur et à mesure de l'évolution et du développement de ces techniques et pour tenir compte de l'identification de nouvelles techniques ou du remplacement de certaines d'entre elles. Cette liste est conforme au plan figurant dans le corps de la Recommandation. Ces amendements rendent compte de la situation des techniques recommandées en avril 2013, septembre 2013, janvier 2014, septembre 2014, avril 2015, septembre 2015, mars 2016 et septembre 2016, y compris des références bibliographiques.

• Recommandation UIT-T X.1520 (révisée), *Vulnérabilités et expositions courantes, qui traite d'un moyen structuré d'échange d'informations sur les vulnérabilités et les expositions courantes en matière de sécurité de l'information*, qui fournit des dénominations communes pour les problèmes connus du public rencontrés dans les logiciels commerciaux ou libres utilisés dans les réseaux de communication, dans les dispositifs d'utilisateur final, ou dans tout autre type de dispositif des technologies de l'information et de la communication (TIC) capable d'utiliser des logiciels. Ces dénominations communes permettent de faciliter l'échange de données sur les vulnérabilités entre différentes capacités (outils, répertoires et services).

• Recommandation UIT-T X.1521 (révisée), *Système de notation des vulnérabilités courantes version 3.0*, qui définit un cadre ouvert pour la communication des caractéristiques et des incidences des vulnérabilités, s'agissant des technologies de l'information et de la communication (TIC), rencontrées dans les logiciels commerciaux ou libres utilisés dans les réseaux de communication, dans les dispositifs d'utilisateur final, ou dans tout autre type de dispositif TIC capable d'utiliser des logiciels.

• Recommandation UIT-T X.1525, *Système commun de notation des failles*, qui définit un cadre ouvert pour la communication des caractéristiques et des incidences des failles en matière de technologies de l'information et de la communication (TIC) rencontrées au moment du développement des fonctionnalités des logiciels.

• Recommandation UIT-T X.1526 (révisée), *Langage pour la définition ouverte des vulnérabilités et pour l'évaluation de l'état d'un système*, qui englobe les trois principales étapes du processus d'évaluation: la représentation des informations de configuration des points d'extrémité à tester; l'analyse du point d'extrémité en vue de détecter un état précis de la machine (en ce qui concerne la vulnérabilité, la configuration, un correctif, etc.); et le compte-rendu des résultats de cette évaluation. OVAL a pour objet de fournir une norme communautaire internationale en matière de sécurité de l'information, qui vise à promouvoir des contenus ouverts et publiquement accessibles sur la sécurité et à normaliser le transfert de ces informations à l'ensemble des outils et des services de sécurité. Par OVAL, on entend le langage employé pour coder des informations précises sur les points d'extrémité, mais aussi un ensemble de divers répertoires de contenus, tenus dans l'ensemble de la communauté.

• Recommandation UIT-T X.1542, *Format d'échange de messages sur les informations de session*, qui décrit le modèle d'information pour le format d'échange de messages sur les informations de session (SIMEF) et fournit un modèle de données associé, spécifié en langage de balisage extensible (XML). Le format SIMEF définit une représentation de modèle de données permettant de partager les informations enregistrées des sessions de couche transport concernant la gestion centralisée de la sécurité du réseau et le système d'échange d'informations sur la sécurité.

• Recommandation UIT-T X.1544, *Enumération et classification des schémas d'attaque courants*, qui est une spécification fondée sur le langage XML/XSD pour l'identification, la description et l'énumération des schémas d'attaque.

• Recommandation UIT-T X.1546, *Enumération et caractérisation des attributs de logiciels malveillants*, qui porte sur la création de l'énumération des attributs de logiciels malveillants de bas niveau et comprend des énumérations d'attributs de logiciels malveillants et un comportement qui fournit un vocabulaire commun.

• Recommandation UIT-T X.1582, *Protocoles de transport prenant en charge l'échange  
d'informations sur la cybersécurité*, qui donne un aperçu des protocoles de transport ayant été choisis et adaptés afin d'être utilisés dans le cadre du modèle d'échange d'informations de cybersécurité (CYBEX). La Recommandation UIT‑T X.1582 traite des applications de transport et des caractéristiques des protocoles de transport, ainsi que des questions de sécurité.

• Supplément X.Suppl.10 (révisé), *Supplément à la Recommandation UIT‑T X.1205* *sur les possibilités d'utilisation du retraçage dans les réseaux*, qui présente un aperçu du retraçage en vue de l'application de mesures visant à faire face à certains problèmes de réseau dans un environnement à un seul fournisseur de services ou dans un environnement plus complexe. Le retraçage peut aider à découvrir les points d'entrée, les trajets complets ou partiels et l'origine d'événements réseau problématiques. Ces informations pourront aider les fournisseurs de service à limiter les effets de ces événements.

• Supplément X.Suppl.18*, Supplément à la Recommandation UIT-T X.1205 sur des lignes directrices pour la détection et la limitation du trafic anormal sur les réseaux de télécommunication IP*, qui recense les technologies de détection du trafic anormal et les mesures propres à limiter ce trafic pour les réseaux de télécommunication IP. Le Supplément X.Suppl.18 a pour objet de fournir aux opérateurs de télécommunication des lignes directrices complètes pour la surveillance, la détection et la limitation du trafic IP anormal.

• Supplément X.Suppl.20, *Supplément à la Recommandation UIT-T X.1205 sur un cadre de négociation pour le partage d'informations de sécurité*, qui définit un cadre pour la négociation d'un accord sur le partage d'informations de sécurité entre entités de cybersécurité, par exemple un demandeur d'informations et un fournisseur d'informations. Le Supplément X.Suppl.20 définit des capacités fonctionnelles et un modèle de référence de négociation pour le partage d'informations de sécurité, la modélisation conceptuelle des données pour l'accord sur le partage d'informations de sécurité (SSA), la politique de partage d'informations de sécurité (SSP) et le processus de négociation de l'accord SSA.

e) Question 5/17: Lutte contre le spam par des moyens techniques

Le groupe chargé de la Question 5/17 étudie les mesures techniques de lutte contre le spam afin d'assurer la stabilité et la fiabilité du réseau de télécommunication. Le spam est devenu un problème de grande ampleur, qui occasionne nombre de difficultés aux utilisateurs, aux fournisseurs de service et aux opérateurs de réseau dans le monde entier. L'étude de la Question 5/17 contribue directement à l'application des Résolutions 52 et 50 de l'AMNT‑12.

Le groupe chargé de la Question 5/17 a suivi la structure à trois niveaux qu'il avait définie pour la série de Recommandations sur la lutte contre le spam, couvrant la plupart des types de spam, actuels ou futurs. Le premier niveau correspond aux stratégies techniques de lutte contre le spam. Le deuxième niveau porte sur des domaines spécifiques de lutte contre le spam (SMS, messagerie électronique et applications multimédias IP). Enfin, le troisième niveau porte sur les technologies générales à utiliser pour lutter contre le spam.

Pendant la présente période d'études, deux nouvelles Recommandations, deux nouveaux Suppléments et un Corrigendum (X.1243 Cor.1) ont été élaborés au titre de la Question 5/17:

• Recommandation UIT-T X.1246, *Technologies intervenant dans la lutte contre le spam vocal dans les organisations de télécommunication*, qui donne un aperçu du spam vocal, présente les technologies antispam existantes qui sont utilisées par les utilisateurs et les réseaux de télécommunication et décrit le mécanisme de collaboration entre elles.

• Recommandation UIT-T X.1247, *Cadre technique de lutte contre le spam par messagerie mobile*, qui donne un aperçu des méthodes de lutte contre le spam par messagerie mobile et propose un cadre technique de lutte contre ce phénomène. Dans ce cadre sont définies les fonctions incombant aux entités et les procédures de traitement à suivre. En outre, cette Recommandation décrit des mécanismes d'échange d'informations pour lutter contre le spam par messagerie mobile dans le domaine du traitement antispam ou entre plusieurs domaines de traitement antispam.

• Supplément X.Suppl.25, *Supplément à la Recommandation UIT-T X.1231 sur des orientations pour faciliter la lutte contre le spam à l'intention des concepteurs de téléphones mobiles*, qui donne aux concepteurs de téléphones mobiles des orientations pour faciliter la lutte contre le spam. En outre, ce Supplément décrit les menaces qui pèsent sur la sécurité des téléphones mobiles, en particulier au niveau des applications, et donne aux concepteurs de téléphones mobiles des orientations pour faciliter la lutte contre le spam.

• Supplément X.Suppl.28, *Supplément à la Recommandation UIT-T X.1245 sur des mesures techniques et des mécanismes de lutte contre l'usurpation de numéro dans le réseau de terminaison du service VoLTE*, qui analyse les menaces et recommande des mesures techniques et des mécanismes permettant de lutter contre l'usurpation de numéro dans le réseau de terminaison du service VoLTE si l'identité des appels entrants ne peut être protégée de manière fiable par le réseau de terminaison. Après une analyse des menaces liées à l'usurpation de numéro, ce Supplément porte essentiellement sur la protection des utilisateurs VoLTE, l'objectif étant de leur éviter de recevoir des appels utilisant un numéro usurpé ou de les prévenir en cas d'appel présumé utiliser un numéro usurpé, grâce au déploiement de procédures à la fois côté réseau et côté utilisateur (smartphone).

f) Question 6/17: Aspects relatifs à la sécurité des services de télécommunication ubiquitaires

Le groupe chargé de la Question 6/17 étudie les aspects relatifs à la sécurité des services de télécommunication ubiquitaires. Un service de télécommunication ubiquitaire désigne un service qui permet à n'importe qui d'accéder à n'importe quelle information souhaitée de façon conviviale, à tout moment, en tout lieu et avec n'importe quel dispositif. Le groupe chargé de la Question 6/17 s'intéresse en particulier à la sécurité des télécommunications ubiquitaires propres à un domaine assurées entre des dispositifs hétérogènes utilisant des technologies au niveau application (par exemple le web ubiquitaire pour un réseau de capteurs ubiquitaire, un réseau domestique, un réseau mobile, un réseau de multidiffusion, un réseau de TVIP, l'Internet des objets, un réseau SDN, un réseau électrique intelligent et un système ITS). Pendant la période d'études, le texte de la Question 6/17 a été modifié par l'intermédiaire du GCNT.

Pendant la présente période d'études, deux nouvelles Recommandations, deux Corrigenda techniques (X.1311 Cor.1, X.1314 Cor.1) et trois nouveaux Suppléments ont été élaborés au titre de la Question 6/17:

• Recommandation UIT-T X.1198, *Plate-forme de sécurité basée sur une machine virtuelle pour une protection de service et de contenu de TVIP renouvelable*, qui spécifie une plate-forme de sécurité basée sur une machine virtuelle pour le système de protection de service et de contenu renouvelable, définit une interface commune et une logique fonctionnelle dans le dispositif terminal de télévision utilisant le protocole Internet (TVIP) et décrit la structure de données du client SCP et les éléments de système d'un dispositif terminal (entité SCP intégrée, client de média et client de commande).

• Recommandation UIT-T X.1314, *Exigences et cadre de sécurité applicables aux réseaux ubiquitaires*, qui définit un cadre de sécurité de haut niveau pour les réseaux ubiquitaires, analyse les menaces pour la sécurité et définit les exigences de sécurité afin d'atténuer ces menaces dans l'environnement des réseaux ubiquitaires.

• Supplément X.Suppl.19, *Supplément aux Recommandations de la série UIT‑T X.1120‑X.1139 sur les aspects relatifs à la sécurité des smartphones*, qui vise à protéger la vie privée des utilisateurs et à améliorer la sécurité des informations dans les smartphones. Pour répondre à ces objectifs de sécurité, ce Supplément définit un cadre de sécurité hiérarchique et présente des considérations relatives à la sécurité pour les smartphones. Le Supplément X.Suppl.19 recense les menaces qui pèsent sur les smartphones, qui sont classées dans deux catégories, à savoir les vulnérabilités et les attaques. En ce qui concerne le cadre de sécurité, le Supplément X.Suppl.19 définit les solutions de sécurité nécessaires moyennant des améliorations du système et des outils de sécurité.

• Supplément X.Suppl.24, *Supplément aux Recommandations de la série UIT‑T X.1120‑X.1139 sur un cadre sécurisé de distribution des applications pour les dispositifs de communication*, qui définit un cadre sécurisé de distribution des applications pour les dispositifs de communication et les exigences de sécurité pour les sites de distribution d'applications afin d'offrir aux utilisateurs un environnement de communication plus sûr.

• Supplément X.Suppl.26, *Supplément à la Recommandation UIT-T X.1111 sur l'architecture fonctionnelle de sécurité pour les services de réseau électrique intelligent utilisant les réseaux de télécommunication*, qui décrit une architecture fonctionnelle de sécurité pour les services de réseau électrique intelligent utilisant les réseaux de télécommunication. Ce Supplément recense les risques et les exigences en matière de sécurité et définit en outre une architecture fonctionnelle de sécurité pour les services de réseau électrique intelligent utilisant les réseaux de télécommunication sur la base d'un modèle fonctionnel général.

Le groupe chargé de la Question 6/17 travaille en collaboration avec l'ISO/CEI JTC 1/SC 6, 25, 27 et 31 sur la sécurité des réseaux USN.

g) Question 7/17: Services applicatifs sécurisés

Le groupe chargé de la Question 7/17 étudie les services applicatifs sécurisés, par exemple la sécurité des services entre homologues (P2P), l'authentification sûre fondée sur un mot de passe avec échange de clés et divers services de tiers de confiance, et les services web.

Pendant la présente période d'études, huit nouvelles Recommandations et deux nouveaux Suppléments ont été élaborés au titre de la Question 7/17:

• Recommandation UIT-T X.1144, *Langage de balisage extensible de contrôle d'accès (XACML) 3.0*, qui définit la version 3.0 du langage de balisage extensible de contrôle d'accès (XACML 3.0) – version actualisée par rapport à celle définie dans la Recommandation UIT-T X.1142 (qui est équivalente à la norme XACML 2.0 d'OASIS (06/2006)) – et définit le langage XACML de base, y compris la syntaxe du langage, les modèles, le contexte avec le modèle de langage, la syntaxe et les règles de traitement pour les politiques.

• Recommandation UIT-T X.1154, *Cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité*, qui définit, à l'intention d'un fournisseur de services, le cadre général de l'authentification combinée dans des environnements multifournisseurs IdSP. Dans cette Recommandation, trois types de méthodes d'authentification combinée sont examinés: l'authentification multifacteur, l'authentification multiméthode et les authentifications multiples.

• Recommandation UIT-T X.1155, *Lignes directrices relatives à l'authentification anonyme reliable locale pour les services électroniques*, qui contient des lignes directrices sur l'authentification anonyme reliable locale pour les cyberservices. Elle traite des menaces que font peser les cyberservices sur la vie privée, des exigences en matière d'authentification anonyme reliable locale, des fonctions permettant de satisfaire ces exigences et d'un modèle général d'authentification anonyme reliable locale pour les cyberservices.

• Recommandation UIT-T X.1156, *Cadre de non-répudiation basé sur un mot de passe à usage unique*, qui définit un cadre de non-répudiation basé sur un mot de passe à usage unique pour améliorer la confiance entre les entités d'une transaction.

• Recommandation UIT-T X.1157, *Capacités techniques de détection des fraudes et de réponse pour les services exigeant un niveau de garantie élevé*, qui définit les capacités nécessaires pour assurer une détection des fraudes et une réponse pour les applications des technologies de l'information et de la communication (TIC) sensibles sur le plan de la sécurité**.**

• Recommandation UIT-T X.1158, *Mécanismes d'authentification à plusieurs facteurs utilisant un dispositif mobile*, qui décrit les failles des mécanismes d'authentification à un seul facteur, la nécessité de disposer de mécanismes d'authentification à plusieurs facteurs, diverses combinaisons de mécanismes d'authentification à plusieurs facteurs utilisant un dispositif mobile et les menaces liées aux mécanismes d'authentification à deux facteurs.

• Recommandation UIT-T X.1159, *Architecture de non-répudiation déléguée fondée sur la Recommandation UIT-T X.813*, qui décrit les modèles et opérations du service de non-répudiation déléguée.

• Recommandation UIT-T X.1163, *Exigences et mécanismes de sécurité des réseaux de télécommunication pair à pair*, qui donne des directives relatives à la sécurité pour un réseau de télécommunication basé sur la technologie P2P, présente brièvement les caractéristiques du réseau, analyse les exigences de sécurité pour le réseau et les services, et spécifie les mécanismes de sécurité permettant de répondre à ces exigences.

• Supplément X.Suppl.21, *Supplément à la Recommandation UIT‑T X.1143 sur le cadre de sécurité pour les services de mixage web*, qui décrit le cadre de sécurité pour les services de mixage web ainsi que les types de mixage web et une architecture de référence.

• Supplément X.Suppl.22, *Supplément à la Recommandation UIT-T X.1144 sur les améliorations et les nouvelles fonctionnalités offertes dans le langage de balisage extensible de contrôle d'accès (XACML 3.0)*, qui présente les améliorations et les nouvelles fonctionnalités définies dans la Recommandation UIT-T X.1144 (XACML 3.0) par rapport à la Recommandation UIT‑T X.1142 (XACML 2.0).

h) Question 8/17: Sécurité de l'informatique en nuage

Le groupe chargé de la Question 8/17 étudie la sécurité de l'informatique en nuage. La CE 17, avec l'aide des Présidents de la CE 13 et de la CE 17, a établi des principes de haut niveau pour la répartition des travaux sur la sécurité de l'informatique en nuage. Pendant la présente période d'études, le texte de la Question 8/17 a été modifié par l'intermédiaire du GCNT.

Pendant la présente période d'études, cinq nouvelles Recommandations et une Recommandation révisées ont été élaborées au titre de la Question 8/17:

• Recommandation UIT-T X.1601 et Recommandation UIT‑T X.1601 (révisée), *Cadre de sécurité applicable à l'informatique en nuage*, qui décrit le cadre de sécurité applicable à l'informatique en nuage. Cette Recommandation présente une analyse des menaces et des problèmes de sécurité dans l'environnement de l'informatique en nuage et décrit les capacités de sécurité qui pourraient atténuer ces menaces et résoudre les problèmes de sécurité. On y trouve une méthode générale permettant de déterminer, parmi ces capacités de sécurité, celles qu'il faudra préciser pour atténuer les menaces et résoudre les problèmes de sécurité dans le cadre de l'informatique en nuage.

• Recommandation UIT-T X.1602, *Exigences de sécurité pour l'environnement des applications de logiciel en tant que service*, qui analyse les niveaux de maturité des applications de logiciel en tant que service (SaaS) et propose des exigences de sécurité afin que l'exécution de ces applications s'effectue dans un environnement homogène et sécurisé. Des fournisseurs de services en nuage (CSP) et des partenaires de services dans le nuage (CSN) sont à l'initiative de ce projet, étant donné qu'ils ont besoin d'un environnement pour les applications SaaS qui réponde à leurs besoins de sécurité. Ces exigences sont générales et indépendantes de tout modèle propre à un service ou à un scénario particulier (comme les services web ou l'architecture de transfert d'état de représentation REST), ou encore de toute hypothèse ou solution.

• Recommandation UIT-T X.1631, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information fondés sur la norme ISO/CEI 27002 pour les services en nuage*, qui contient des lignes directrices relatives à la mise en place de contrôles de sécurité de l'information applicables à la fourniture et à l'utilisation de services en nuage, des orientations additionnelles relatives à la mise en oeuvre pour les contrôles pertinents définis dans la norme ISO/CEI 27002 et des contrôles additionnels et des orientations relatives à la mise en oeuvre qui se rapportent expressément aux services en nuage. Cette Recommandation | Norme internationale fournit des contrôles et des orientations pour la mise en oeuvre à l'intention des fournisseurs de services en nuage et des clients des services en nuage.

• Recommandation UIT-T X.1641, *Lignes directrices relatives à la sécurité des données des clients de services de nuage*, qui fournit des lignes directrices génériques concernant la sécurité des données des clients de services de nuage (CSC) dans le contexte de l'informatique en nuage. Elle analyse le cycle de vie de la sécurité des données CSC et propose des exigences de sécurité à chaque étape du cycle de vie des données. En outre, la Recommandation donne des lignes directrices concernant le moment auquel chaque contrôle devrait être appliqué pour assurer au mieux la sécurité.

• Recommandation UIT-T X.1642, *Lignes directrices relatives à la sécurité opérationnelle de l'informatique en nuage,* qui donne des lignes directrices générales sur la sécurité opérationnelle pour l'informatique en nuage du point de vue des fournisseurs de services en nuage (CSP). Cette Recommandation analyse les exigences de sécurité et les indicateurs pour le fonctionnement de l'informatique en nuage. On y trouve également un ensemble de mesures et d'activités détaillées en matière de sécurité pour l'exploitation et la maintenance courantes de ces services, destinées à aider les fournisseurs CSP à atténuer les risques liés à la sécurité et à résoudre les problèmes de sécurité pour le fonctionnement de l'informatique en nuage.

i) Question 9/17: Télébiométrie

Le groupe chargé de la Question 9/17 étudie la télébiométrie ainsi que les exigences de sécurité et les lignes directrices pour les applications de la télébiométrie, en particulier les exigences pour les protocoles génériques appropriés concernant la sûreté, la sécurité, la protection de la vie privée et l'accord "pour la manipulation de données biométriques" dans les applications de la télébiométrie, par exemple la cybersanté et la télémédecine.

Pendant la présente période d'études, trois nouvelles Recommandations ont été élaborées au titre de la Question 9/17:

• Recommandation UIT-T X.1085, *Technologies de l'information – Techniques de sécurité – Cadre d'authentification télébiométrique utilisant un module matériel de sécurité biométrique*. La Recommandation UIT-T X.1085 | ISO/CEI 17992 décrit un système d'authentification télébiométrique utilisant un module matériel de sécurité biométrique (BHSM) pour l'authentification télébiométrique du titulaire d'un certificat X.509 enregistré de manière individuelle auprès de l'autorité d'enregistrement. Cette Recommandation | Norme internationale définit les exigences relatives au déploiement du système BHSM de manière à procéder en toute sécurité à l'authentification télébiométrique dans les environnements PKI. Elle porte essentiellement sur la question de savoir comment assurer l'authentification télébiométrique au moyen du module matériel de sécurité et de techniques biométriques et elle propose en outre un format standard ASN.1 à utiliser pour inclure le système proposé dans le cadre X.509 lorsque l'authentification télébiométrique et le certificat X.509 sont associés pour authentifier le titulaire du certificat.

• Recommandation UIT-T X.1087, *Contremesures techniques et opérationnelles pour les applications de la télébiométrie utilisant des dispositifs mobiles*, qui définit le modèle de mise en oeuvre des systèmes télébiométriques fonctionnant dans les dispositifs mobiles et les menaces qui pèsent sur ces systèmes, et fournit des lignes directrices générales relatives aux contremesures de sécurité, des points de vue technique et opérationnel, afin d'établir un environnement mobile sûr pour l'utilisation des systèmes télébiométriques.

• Recommandation UIT-T X.1092, *Cadre intégré pour la protection des données de télébiométrie dans les domaines de la cybersanté et de la télémédecine*, qui définit un cadre intégré pour la protection des données biométriques et des informations privées dans les domaines de la cybersanté et de la télémédecine.

j) Question 10/17: Architecture et mécanismes de gestion d'identité

Cette Question vise à définir la vision ainsi qu'à coordonner et à organiser toutes les activités relatives à la gestion d'identité (IdM) au sein de l'UIT‑T. Une méthode descendante relative à la gestion d'identité est utilisée en collaboration avec d'autres commissions d'études et organisations de normalisation. Certains aspects de l'IdM (protocoles, exigences, identificateurs de dispositif de réseau, etc.) relèvent d'autres Questions.

Pendant la présente période d'études, quatre nouvelles Recommandations ont été élaborées au titre de la Question 10/17:

• Recommandation UIT-T X.1255, *Cadre pour la découverte des informations relatives à la gestion d'identité*, qui définit un cadre d'architecture ouverte dans lequel il est possible de découvrir des informations relatives à la gestion d'identité (IdM). Les éléments principaux du cadre présenté dans cette Recommandation sont: 1) un modèle de données d'entité numérique; 2) un protocole d'interface d'entité numérique; 3) un ou plusieurs système(s) de résolution/d'identificateur; et 4) un ou plusieurs registres de métadonnées. Ces éléments constituent la base du cadre d'architecture ouverte.

• Recommandation UIT-T X.1256, *Lignes directrices et cadre pour le partage des résultats d'authentification réseau avec des applications de services*, qui présente des lignes directrices à l'intention des opérateurs de réseau et des fournisseurs de services pour le partage des résultats d'authentification réseau, et offre un cadre pour permettre le partage d'un nombre minimal d'attributs entre de multiples services, le tout dans une relation de confiance solide.

• Recommandation UIT-T X.1257, *Taxonomie de la gestion d'identité et d'accès*, qui présente des spécifications qui visent à faire en sorte que la signification opérationnelle nécessaire soit assignée aux rôles et aux permissions de gestion d'identité et d'accès (IAM) et que cette signification opérationnelle puisse être tracée et référencée tout au long du cycle de vie des processus IAM, autrement dit que des permissions puissent être assignées efficacement aux utilisateurs, que des contrôles liés à la séparation des fonctions (SoD) puissent être mis en oeuvre avec succès dans différentes applications, et que des processus d'examen et d'actualisation d'accès puissent être effectués d'une manière efficace.

• Recommandation UIT-T X.1258, *Authentification d'entité améliorée basée sur des attributs agrégés*, qui présente le concept d'agrégation d'attributs en vue de permettre à une entité d'agréger des attributs provenant de multiples fournisseurs de services d'identité (IdSP). L'agrégation d'attributs est le mécanisme consistant à recueillir les attributs d'une entité obtenus auprès de multiples fournisseurs IdSP. Elle est nécessaire pour agréger les attributs de manière dynamique à la demande. Le fournisseur IdSP peut effectuer la demande d'agrégation lorsqu'une entité veut obtenir un service. Par la suite, un mécanisme d'agrégation des attributs centrés sur l'entité pourrait être appliqué à l'authentification afin de limiter les fuites de données confidentielles.

k) Question 11/17: Technologies génériques utilisées pour les applications sécurisées

Le groupe chargé de la Question 11/17 étudie les services et systèmes d'annuaire, y compris les certificats d'attributs et de clés publiques. La mise à jour des Recommandations de la série X.500 occupe une large part des travaux menés conjointement avec l'ISO/CEI JTC 1/SC 6/WG 10.

Des travaux importants ont été entrepris concernant la Recommandation UIT-T X.509 pendant la période d'études actuelle, en particulier:

a) La Recommandation UIT‑T X.509 est devenue une spécification épurée sur les infrastructures PKI et PMI, avec le transfert des sections relatives à l'annuaire X.500 dans d'autres parties de la série X.500, de sorte que la Recommandation UIT-T X.509 est devenue un document autonome.

b) Le style et la terminologie ont été alignés sur l'usage actuel dans l'industrie et une distinction claire a été établie entre les infrastructures PKI et PMI.

c) Une liste de capacités d'autorisation et de validation a été ajoutée, comme demandé et mentionné dans la norme CEI 62351-9, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance*.

d) Plusieurs autres modifications ont été apportées à la Recommandation UIT-T X.509 en vue de la prise en charge des futures exigences imposées par la sécurité des réseaux électriques intelligents et l'Internet des objets.

Par ailleurs, le groupe chargé de la Question 11/17 tient à jour les Recommandations relatives à la notation ASN.1 et poursuit l'élaboration de Recommandations sur les identificateurs d'objet. Ce travail est également effectué en collaboration avec l'ISO/CEI JTC 1/SC 6/WG10. La notation ASN.1 est stable avec la révision approuvée en septembre 2015. La base de données des modules ASN.1 continue d'être complétée et permet aux responsables de la mise en oeuvre d'accéder aux spécifications ASN.1 publiées, vérifiées du point de vue de la syntaxe et lisibles par un ordinateur.

Pendant plusieurs périodes d'études, la Commission d'études 17 a élaboré un système d'identification mondial basé sur des autorités d'enregistrement hiérarchiques, appelé "arborescence des identificateurs d'objet", qui est largement utilisée à la fois dans des Recommandations UIT‑R et UIT‑T et dans des Normes internationales de l'ISO/CEI pour de nombreuses applications. Plus de 954 046 identifications ont été enregistrées publiquement et beaucoup d'autres ont été délivrées pour une utilisation interne par diverses organisations. Au départ, les arcs de l'arborescence des identificateurs d'objet étaient identifiés au moyen de numéros et de noms utilisant l'alphabet latin.

Le groupe chargé de la Question 11/17, en collaboration avec l'ISO/CEI JTC 1/SC 7/WG19, a élaboré deux révisions des Recommandations UIT-T X.906 et UIT‑T X.911 sur le traitement réparti ouvert (ODP).

Le groupe chargé de la Question 11/17 tient à jour les Recommandations de la série X sur l'interconnexion des systèmes ouverts (OSI). Pendant la présente période d'études, aucune Recommandation OSI nouvelle ou révisée n'a été élaborée au titre de la Question 11/17 mais deux Corrigenda techniques ont été élaborés (X.226 Cor.1et X.227*bis* Cor.1).

Pendant la présente période d'études, 4 nouvelles Recommandations, 23 Recommandations révisées, 14 Corrigenda techniques (X.226 Cor.1, X.227*bis* Cor.1, X.509 Cor.1, X.509 Cor.2, X.509 Cor.3, X.680 Cor.2, X.682 Cor.1, X.683 Cor.1, X.690 Cor.2, X.694 Cor.2, X.520 Cor.1, X.691 Cor.1, X.691 Cor.3, X.691 Cor.4) aux Recommandations des séries X.500, X.680 et X.690 et un Rapport technique ont été élaborés au titre de la Question 11/17:

• Recommandation UIT‑T X.500 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services*, qui introduit les concepts d'annuaire et de base d'informations d'annuaire (DIB), et donne un aperçu général des services et capacités qu'ils fournissent.

• Recommandation UIT‑T X.501 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles*, qui spécifie un certain nombre de modèles différents relatifs à l'annuaire comme cadre pour les autres Recommandations UIT‑T de la série X.500. Ces modèles sont le modèle (fonctionnel) général, le modèle d'autorité administrative, les modèles génériques d'informations d'annuaire fournissant à l'utilisateur d'annuaire et à l'utilisateur administratif des vues sur les informations d'annuaire, les modèles génériques d'agent de système d'annuaire (DSA) et d'informations d'agent DSA, un cadre opérationnel et un modèle de sécurité.

• Recommandation UIT‑T X.509 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadres pour les certificats de clé publique et d'attribut*, qui définit des cadres pour l’infrastructure de clé publique (PKI) et l’infrastructure de gestion de privilège (PMI). Elle introduit le concept de base de techniques de chiffrement asymétrique. Elle spécifie les types de données suivants: certificat de clé publique, certificat d’attribut, liste de révocation de certificats (CRL) et liste de révocation de certificats d’attribut (ACRL). Elle définit aussi plusieurs certificats et extensions de liste CRL, ainsi que les informations relatives au schéma d’annuaire permettant de stocker dans un annuaire les données relatives aux infrastructures PKI et PMI. Elle définit en outre des types d’entité, tels que l’autorité de certification, l’autorité d’attribut, la partie utilisatrice, le vérificateur de privilège, le courtier de confiance et l’ancre de confiance. Elle spécifie les principes régissant la validation de certificat, le trajet de validation, la politique de certificat, etc. Elle inclut une spécification des listes de validation d’autorisation qui permettent d’effectuer une validation rapide et d’imposer des restrictions aux communications. Enfin, elle inclut les protocoles nécessaires pour tenir à jour les listes de validation d’autorisation et un protocole permettant d’accéder à un courtier de confiance.

• Recommandation UIT‑T X.511 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: définition de service abstrait*, qui définit de manière abstraite les services fournis par l'annuaire tels que ces services sont vus de l'extérieur, y compris les opérations de rattachement et de détachement, les opérations de lecture, les opérations de recherche, les opérations de modification, les opérations permettant de prendre en charge les politiques relatives aux mots de passe et les opérations permettant de prendre en charge l’interfonctionnement avec le protocole LDAP. Elle définit aussi les erreurs.

• Recommandation UIT‑T X.518 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: procédures pour le fonctionnement réparti*, qui spécifie les procédures nécessaires pour qu'un annuaire réparti constitué de différents agents de système d'annuaire (DSA) et serveurs utilisant le protocole simple d'accès à l'annuaire (LDAP) en interaction puisse fournir un service cohérent à ses utilisateurs, indépendamment du point d'accès. Elle décrit aussi les procédures de conversion entre les protocoles d'accès à l'annuaire et de système d'annuaire (DAP/DSP) et le protocole LDAP.

• Recommandation UIT‑T X.519 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécification des protocoles*, qui spécifie le protocole d'accès à l'annuaire, le protocole de système d'annuaire, le protocole de duplication miroir d'informations de l'annuaire et le protocole de gestion des liens opérationnels avec l'annuaire, pour la réalisation des services abstraits spécifiés dans les Recommandations UIT-T X.501 | ISO/CEI 9594-2, UIT-T X.511 | ISO/CEI 9594-3, UIT-T X.518 | ISO/CEI 9594-4 et UIT-T X.525 | ISO/CEI 9594-9. Elle contient des spécifications relatives à la prise en charge des protocoles sous-jacents afin de réduire la dépendance à l'égard de spécifications externes. Les protocoles peuvent être codés au moyen de toutes les règles de codage ASN.1 standards.

• Recommandation UIT-T X.520 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attributs sélectionnés*, qui définit un certain nombre de types d'attributs et de règles de concordance pouvant s'avérer utiles dans différentes applications de l'annuaire. Nombre de ces attributs ainsi définis peuvent notamment servir à la formation de noms, en particulier pour les classes d'objets définies dans la Recommandation UIT-T X.521 | ISO/CEI 9594-7. D'autres types d'attributs, appelés attributs de notification, donnent des informations de diagnostic. Cette Recommandation | Norme internationale définit des types de contexte qui donnent des caractéristiques associées à des valeurs d'attribut. Elle contient aussi des définitions relatives aux syntaxes LDAP appropriées pour les types d'attribut et les règles de concordance.

• Recommandation UIT-T X.521 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: classes d'objets sélectionnées*, qui définit un certain nombre de classes d'objets et de formes de noms sélectionnées pouvant servir dans différentes applications de l'annuaire. La définition d'une classe d'objets spécifie les types d'attributs se rapportant aux objets de cette classe. La définition d'une forme de nom spécifie les attributs à utiliser pour former les noms des objets d'une classe donnée.

• Recommandation UIT-T X.525 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: duplication*, qui spécifie un service de duplication miroir que les agents de système d'annuaire (DSA) peuvent utiliser pour copier les informations d'annuaire. Ce service permet de dupliquer, tout en les mettant à jour automatiquement, des informations d'annuaire entre agents DSA pour améliorer le service fourni aux utilisateurs de l'annuaire.

• Recommandation UIT-T F.511, *Service d'annuaire – Prise en charge des services d'identification par étiquette*, qui fournit des indications relatives à l'utilisation des services d'annuaire pour la prise en charge des applications d'identification par étiquette, sur la base des capacités d'annuaire définies dans la série de Recommandations UIT‑T X.500 | ISO/CEI 9594 (toutes les parties), et dans les spécifications du protocole simple d'accès à l'annuaire (LDAP) élaborées au sein de l'Internet Engineering Task Force (IETF).

• Recommandation UIT-T X.667 (révisée), *Technologies de l'information – Procédures opérationnelles des autorités d'enregistrement des identificateurs d'objet: génération des identificateurs uniques universels et utilisation de ces identificateurs dans les identificateurs d'objet*, qui spécifie des procédures pour la génération d'identificateurs uniques universels (UUID), ainsi que pour leur utilisation dans l'arborescence des identificateurs d'objet internationaux sous l'arc commun des UUID.

• Recommandation UIT-T X.675, *Cadre de résolution basé sur les identificateurs d'objet pour les identificateurs et localisateurs hétérogènes*, qui analyse les exigences, par exemple l'indépendance des identificateurs, la séparation des identificateurs, la compatibilité, l'unicité, la tolérance, la stabilité et la sécurité. L'architecture générale du cadre de résolution basé sur les identificateurs d'objet est spécifiée avec plusieurs scénarios. Ces scénarios montrent comment utiliser le cadre de résolution pour des identificateurs et des localisateurs hétérogènes.

• Recommandation UIT-T X.680 (révisée), *Technologies de l'information – Notation de syntaxe abstraite numéro un:* *spécification de la notation de base*, qui spécifie une notation dite notation de syntaxe abstraite numéro un (ASN.1) pour la définition de la syntaxe des données informationnelles. Cette Recommandation définit un certain nombre de types de donnée simples et spécifie une notation pour y faire référence et en spécifier les valeurs. La notation ASN.1 peut être utilisée chaque fois que cela est nécessaire pour définir la syntaxe abstraite d'informations, sans que cela impose une contrainte quelconque sur la manière de coder ces informations en vue de leur transmission.

• Recommandation UIT-T X.681 (révisée), *Technologies de l'information – Notation de syntaxe abstraite numéro un:* *spécification des objets informationnels,* qui spécifie la notation ASN.1 qui permet de définir les classes d'objets informationnels ainsi que les objets informationnels proprement dits et de leur donner des noms de référence.

• Recommandation UIT-T X.682 (révisée), *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes*, qui décrit la notation ASN.1 à utiliser, dans le cas général, pour spécifier les contraintes et les exceptions par lesquelles on peut limiter les valeurs des données d'un type de données structuré.

• Recommandation UIT-T X.683 (révisée), *Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un**,* qui définit les dispositions relatives aux noms de référence paramétrés et à l'affectation paramétrée pour des types de données qui sont utiles au concepteur quand il établit des spécifications dont certains aspects sont laissés indéfinis à certains stades du développement et sont définis ultérieurement pour aboutir à la définition complète d'une syntaxe abstraite.

• Recommandation UIT-T X.690 (révisée), *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives*, qui définit un ensemble de règles de codage de base (BER) applicables aux valeurs des types définis au moyen de la notation ASN.1 et qui définit également un ensemble de règles de codage distinctives (DER) et un ensemble de règles de codage canoniques (CER) qui permettent tous deux d'imposer des contraintes aux règles de codage de base (BER).

• Recommandation UIT-T X.691 (révisée), *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact*, qui décrit un ensemble de règles de codage applicables aux valeurs de tous les types ASN.1. Ces règles donnent une représentation beaucoup plus compacte que celle que l'on peut obtenir au moyen des règles de codage de base et de leurs dérivées (décrites dans la Rec. UIT-T X.690 | ISO/CEI 8825-1).

• Recommandation UIT-T X.692 (révisée), *Technologies de l'information – Règles de codage ASN.1: spécification de la notation de contrôle de codage (ECN)*, qui définit la notation de contrôle de codage (ECN) utilisée afin de spécifier les codages (de types ASN.1) qui diffèrent de ceux qui sont fournis par les règles de codage normalisées telles que les règles de codage de base (BER) et les règles de codage compact (PER).

• Recommandation UIT-T X.693 (révisée), *Technologies de l'information – Règles de codage ASN.1: règles de codage XML (XER)*, qui spécifie les règles de codage utilisant le langage de balisage extensible (XML) applicables aux valeurs de types ASN.1.

• Recommandation UIT-T X.694 (révisée), *Technologies de l'information – Règles de codage ASN.1: mappage en ASN.1 des définitions de schéma XML du W3C*, qui définit des règles pour le mappage d'un schéma XSD (un schéma conforme à la spécification du schéma XML du W3C) en un schéma ASN.1 afin d'utiliser les règles de codage de l'ASN.1 telles que les règles de codage de base (BER), les règles de codage distinctives de la notation ASN.1 (DER), les règles de codage compact (PER) ou les règles de codage XML (XER) pour le transfert des informations définies par le schéma XSD.

• Recommandation UIT-T X.695 (révisée), *Technologies de l'information – Règles de codage ASN.1: enregistrement et application des instructions de codage PER*, qui spécifie les règles permettant d'appliquer des instructions de codage PER en utilisant des préfixes de type ou une section de contrôle de codage.

• Recommandation UIT-T X.696, *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage des octets (OER)*, qui spécifie deux ensembles de règles de codage binaire applicables aux valeurs de tous les types ASN.1, qui utilisent moins de ressources de traitement que les règles de codage de base et leurs dérivées.

• Recommandation UIT-T X.696 (révisée), *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage des octets (OER)*, qui spécifie deux ensembles de règles de codage binaire applicables aux valeurs de tous les types ASN.1, qui utilisent moins de ressources de traitement que les règles de codage de base et leurs dérivées (décrites dans la Recommandation UIT-T X.690 | ISO/CEI 8825-1) et les règles de codage compactes (décrites dans la Recommandation UIT-T X.691 | ISO/CEI 8825-2).

• Recommandation UIT-T X.906 (révisée), *Technologies de l'information – Traitement réparti ouvert – Utilisation du langage UML pour les spécifications de systèmes ODP*, qui précise et étend la définition de la manière dont les systèmes de traitement réparti ouvert (ODP) sont spécifiés en définissant l'utilisation du langage de modélisation unifié pour l'expression des spécifications des systèmes ODP.

• Recommandation UIT-T X.911 (révisée), *Technologies de l'information – Traitement réparti ouvert – Modèle de référence – Langage d'entreprise*, qui précise et étend la définition de la façon dont les systèmes ODP sont spécifiés du point de vue entreprise. Elle est destinée à être utilisée pour l'élaboration ou l'utilisation de spécifications de systèmes ODP en langage d'entreprise.

• Recommandation UIT-T X.1341, *Protocoles de transport de courrier certifié et de bureau de poste certifié*, qui définit le protocole de transfert de courrier certifié (CMTP) et le protocole de bureau de poste certifié (CPOP) afin de favoriser l'échange de courriers électroniques certifiés dans le monde de manière sécurisée en assurant la confidentialité, l'identification des correspondants, l'intégrité et la non-répudiation.

• Rapport technique: *Enjeux existants et nouveaux de la normalisation de l'infrastructure de clé publique*, qui examine les problèmes et les menaces actuellement rencontrés lors du déploiement de l'infrastructure de clé publique (PKI), et les nouveaux enjeux pour l'infrastructure PKI notamment en ce qui concerne l'infrastructure PKI sans fil (WPKI), l'informatique en nuage, les réseaux électriques intelligents, et les communications de machine à machine (M2M) en général.

l) Question 12/17: Langages formels pour les logiciels de télécommunication et les tests

La Question 12/17 porte sur les langages formels utilisés pour définir les exigences, l'architecture et le comportement des systèmes de télécommunication: langages pour les besoins, langages de spécification et de mise en oeuvre. De plus, le groupe chargé de la Question 12/17 étudie les langages pour les tests comme outil pour assurer l'interopérabilité et la conformité.

Pendant la présente période d'études, la CE 11 et la CE 17 ont approuvé, par l'intermédiaire du GCNT:

– une révision de la Question 11/11 pour ajouter des travaux sur les méthodologies et le cadre des tests de conformité et d'interopérabilité;

– une révision de la Question 12/17 pour supprimer les travaux sur les méthodologies et le cadre des tests de conformité et ajouter des travaux sur la notation TTCN-3;

– une révision de l'Annexe C de la Résolution 2 afin d'indiquer que les séries Z.160/Z.170 relèvent de la CE 17 et que la série X.290 (sauf la Recommandation X.292), les Suppléments X.Suppl.4 et X.Suppl.5 et la Recommandation Z.500 relèvent de la CE 11.

Pendant la présente période d'études, six nouvelles Recommandations, 30 Recommandations révisées, quatre guides de mise en oeuvre révisés et un Supplément révisé ont été élaborés au titre de la Question 12/17:

• Recommandation UIT-T Z.100 (révisée), *Langage de description et de spécification – Présentation générale de SDL-2010,* qui présente le langage de description et de spécification destiné à être utilisé pour spécifier et décrire sans ambiguïté les systèmes de télécommunication.

• Recommandation UIT-T Z.100, Annexe F1 (révisée), *Définition formelle du langage SDL‑2010: Présentation générale*, qui donne la justification, donne un aperçu général de la structure de la sémantique formelle, et contient une introduction au formalisme de l'automate abstrait à états finis qui est utilisé pour définir la sémantique du langage SDL-2010.

• Recommandation UIT-T Z.100, Annexe F2 (révisée), *Définition formelle du langage SDL‑2010: Sémantique statique*, qui décrit les contraintes relatives à la sémantique statique et les transformations identifiées dans les paragraphes relatifs au modèle figurant dans les Recommandations UIT-T Z.101, Z.102, Z.103, Z.104, Z.105 et Z.107, qui font l'objet d'une inclusion par référence dans la Recommandation UIT-T Z.100.

• Recommandation UIT-T Z.100, Annexe F3 (révisée), *Définition formelle du langage SDL‑2010: Sémantique dynamique*, qui définit la sémantique dynamique du langage SDL-2010.

• Recommandation UIT-T Z.101 (révisée), *Langage de description et de spécification – Langage SDL-2010 de base*, qui définit les caractéristiques de base du langage de description et de spécification. Ce document donne les caractéristiques de base du langage, dont la définition est complétée dans les autres Recommandations UIT-T de la série Z.100.

• Recommandation UIT-T Z.102 (révisée), *Langage de description et de spécification – Langage SDL-2010 complet*, qui définit les caractéristiques complètes du langage de description et de spécification. Ce document donne des caractéristiques du langage qui ne figurent pas dans le langage SDL-2010 de base défini dans la Recommandation UIT‑T Z.101. Ces caractéristiques donnent la grammaire abstraite complète du langage à l'exception de certaines caractéristiques relatives aux données qui font l'objet de la Recommandation UIT-T Z.104 (et de la Recommandation UIT-T Z.107 pour les données orientées objet).

• Recommandation UIT-T Z.103 (révisée), *Langage de description et de spécification – Notation abrégée et annotation dans le langage SDL-2010*, qui définit les caractéristiques des notations abrégées et des annotations du langage de spécification et de description. Ce document donne des caractéristiques qui ne figurent ni dans le langage SDL-2010 de base de la Recommandation UIT-T Z.101, ni dans le langage SDL-2010 complet de la Recommandation UIT‑T Z.102. Les caractéristiques définies dans cette Recommandation, ou bien n'ont pas leur propre grammaire abstraite et sont transcrites dans une grammaire concrète, définie dans les Recommandations UIT‑T Z.101, UIT-T Z.102 et UIT-T Z.104 (et dans la Recommandation UIT-T Z.107 pour les données orientées objets), ou bien sont des annotations sans signification formelle.

• Recommandation UIT-T Z.104 (révisée), *Langage de description et de spécification – Caractéristiques du langage SDL‑2010 pour les données et les actions*, qui définit les caractéristiques concernant les données du langage de description et de spécification, afin que les définitions et les expressions de données soient bien définies. Les caractéristiques définies dans ce document chevauchent en partie les caractéristiques du langage incluses dans le langage SDL-2010 de base de la Recommandation UIT‑T Z.101 et utilisées dans le langage SDL-2010 complet de la Recommandation UIT-T Z.102 et les caractéristiques de la Recommandation UIT‑T Z.103.

• Recommandation UIT-T Z.105 (révisée), *Langage de description et de spécification – Langage SDL-2010 combiné avec des modules ASN.1*, qui définit la façon de combiner les modules de notation de syntaxe abstraite numéro un (ASN.1) avec le langage de spécification et de description 2010 (SDL-2010). Le texte remplace la Recommandation UIT-T Z.105 (2003) dans un souci d'alignement sur les Recommandations UIT‑T Z.100, UIT-T Z.101, UIT-T Z.102, UIT-T Z.103, UIT-T Z.104, UIT-T Z.106 et UIT‑T Z.107 pour le langage SDL-2010. La Recommandation UIT-T Z.105 (2003) remplaçait les mappages sémantiques de la notation ASN.1 vers le langage SDL-2000 définis dans la Recommandation UIT-T Z.105 (1999).

• Recommandation UIT-T Z.106 (révisée), *Langage de description et de spécification – Format d'échange commun pour le langage SDL-2010*, qui définit le format d'échange commun du langage de spécification et de description (SDL-CIF). Le format SDL-CIF doit permettre l'échange de spécifications SDL-2010 graphiques (SDL-GR) entre outils différents qui n'utilisent pas le même format d'archivage. Cette Recommandation introduit deux autres nouveaux niveaux de format SDL-CIF. Deux autres niveaux de conformité sont définis, le premier à un niveau de format SDL-PR plus libre et le second incorporant l'information graphique.

• Recommandation UIT-T Z.107 (révisée), *Langage de description et de spécification – Données orientées objet en SDL‑2010*, qui définit les caractéristiques concernant les données orientées objet du langage de spécification et de description, qui reposent sur les fondements des définitions et des expressions de données établies dans la Recommandation UIT-T Z.104. Les caractéristiques définies dans cette Recommandation chevauchent en partie les caractéristiques du langage incluses dans le langage SDL-2010 de base de la Recommandation UIT-T Z.101 et utilisées dans le langage SDL-2010 complet de la Recommandation UIT-T Z.102, et les caractéristiques des Recommandations UIT-T Z.103 et UIT-T Z.104.

• Recommandation UIT-T Z.109 (révisée), *Langage de description et de spécification – Profil du langage de modélisation unifié pour le SDL-2010*, qui définit un profil de langage de modélisation unifié (UML), correspondant à la sémantique du langage SDL‑2010 de manière à ce que le langage UML puisse être utilisé avec le langage SDL. L'emploi conjoint des deux langages SDL-2010 et UML fournit un outil cohérent permettant de spécifier la structure et le comportement des systèmes de télécommunication, ainsi que les données. La Recommandation UIT‑T Z.109 a été révisée dans un souci de cohérence avec le reste des Recommandations UIT‑T de la série Z.100 relatives au langage SDL‑2010.

• Recommandation UIT-T Z.109 (révisée), *Langage de description et de spécification – Profil du langage de modélisation unifié pour le SDL-2010*, qui définit un profil de langage de modélisation unifié (UML), correspondant à la sémantique du langage SDL‑2010 de manière à ce que le langage UML puisse être utilisé avec le langage de description et de spécification de l'UIT-T. L'Appendice I contient un exemple de spécification de langage (à titre d'information), avec une grammaire concrète et son mappage vers le profil UML.

• Recommandation UIT-T Z.111 (révisée), *Définition des langages de l'UIT-T: notations et lignes directrices*, qui présente les métagrammaires à utiliser dans les Recommandations UIT-T définissant des langages UIT-T de la série X.680 et de la série Z sur les langages de spécification, de mise en oeuvre, de modélisation et de test. Il est ainsi possible de décrire ces métagrammaires qui définissent la grammaire abstraite ou concrète (syntaxe, contraintes et sémantique) des langages sans avoir à répéter la métagrammaire (comme les règles de nommage lexical ou la description de la syntaxe au moyen du formalisme de Backus-Naur) en introduction ou en annexe pour chaque langage défini.

• Recommandation UIT-T Z.161 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): langage noyau*, qui définit la notation de test et de commande de test version 3 (TTCN-3), destinée à la spécification de suites de tests indépendantes des plates-formes, des méthodes de test, des couches de protocole et des protocoles. La première révision de la Recommandation contient de nombreuses extensions du langage (les valeurs par défaut des paramètres, le paramétrage des types, transféré dans un autre document (paramétrage avancé), les valeurs réelles spéciales et les limites d'intervalle exclusives, les restrictions en matière de visibilité des définitions importées, les restrictions de gabarits, l'omission implicite des champs de valeurs et de gabarits, les instructions break/continue, les nouvelles fonctions prédéfinies, etc.) et contient de nombreuses précisions (par exemple sur le sous-typage des types structurés, la compatibilité des types, l'exécution de l'instruction alt, etc.) et des corrections de forme et de fond.

Recommandation UIT-T Z.161 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): langage noyau*, qui définit la notation de test et de commande de test version 3 (TTCN-3), destinée à la spécification de suites de tests indépendantes des plates-formes, des méthodes de test, des couches de protocole et des protocoles. La notation TTCN-3 peut servir à la spécification de tous les types de test de systèmes réactifs, effectués en divers ports de communication. Elle s'applique en général aux tests des protocoles (y compris les protocoles de communication mobile et Internet), aux tests des services (y compris les services complémentaires), aux tests des modules, ainsi qu'aux tests des plates-formes employant l'architecture CORBA et des interfaces de programmation d'applications (API). Cette révision de la Recommandation contient des modifications, des précisions et des corrections de la forme et du fond.

• Recommandation UIT-T Z.161.1, Recommandation UIT-T Z.161.1 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage, prise en charge d'interfaces avec des signaux continus,* qui définit le paquetage "prise en charge de signaux continus" de la notation de test et de commande de test version 3 (TTCN-3). Cette notation peut servir à la spécification de tous les types de test de systèmes réactifs, effectués en divers ports de communication. Elle s'applique en général aux tests des protocoles (y compris les protocoles de communication mobile et Internet), aux tests des services (y compris les services complémentaires), aux tests des modules, aux tests des plates-formes employant l'architecture CORBA, aux tests des interfaces de programmation d'application (API), etc. La notation TTCN-3 n'est pas limitée aux tests de conformité et peut servir à de nombreux autres types de test, y compris ceux de l'interopérabilité, de la robustesse, de la régression, du système et de l'intégration. La spécification de suites de tests pour les protocoles de la couche physique sort du cadre de cette Recommandation.

• Recommandation UIT-T Z.161.2, Recommandation UIT-T Z.161.2 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: prise en charge de la configuration et du déploiement*, qui définit le paquetage "prise en charge de la configuration et du déploiement" de la notation de test et de commande de test version 3 (TTCN-3).

• Recommandation UIT-T Z.161.3, Recommandation UIT-T Z.161.3 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: paramétrage évolué*, qui définit le paquetage "paramétrage évolué" de la notation de test et de commande de test version 3 (TTCN-3).

• Recommandation UIT-T Z.161.4, Recommandation UIT-T Z.161.4 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: types de comportement*, qui définit le paquetage "types de comportement" de la notation de test et de commande de test version 3 (TTCN-3).

• Recommandation UIT-T Z.161.5, Recommandation UIT-T Z.161.5 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: tests d'exécution et en temps réel*, qui définit le paquetage "tests d'exécution et en temps réel" de la notation de test et de commande de test version 3 (TTCN-3).

• Recommandation UIT-T Z.164 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): sémantique opérationnelle*, qui définit la sémantique opérationnelle de la notation de test et de commande de test version 3 (TTCN-3). La sémantique opérationnelle est nécessaire pour pouvoir interpréter sans ambiguïté les spécifications en notation TTCN-3. Cette Recommandation est fondée sur le langage noyau de la notation TTCN-3, qui est défini dans la Recommandation UIT‑T Z.161. Cette révision de la Recommandation contient des modifications, des précisions et des corrections de la forme et du fond.

• Recommandation UIT-T Z.165 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): interface d'exécution*, qui contient la spécification de l'interface d'exécution pour la mise en place de systèmes de test employant la notation de test et de commande de test version 3 (TTCN-3). La deuxième révision de la Recommandation UIT‑T Z.165 contient des modifications, des précisions et des corrections de la forme et du fond.

• Recommandation UIT-T Z.165.1, Recommandation UIT-T Z.165.1 (révisée), *Notation de test et de commande de test version 3: Extension du langage TTCN-3: interface d'exécution étendue*, qui définit le paquetage "interface d'exécution TRI étendue" de la notation de test et de commande de test version 3 (TTCN-3). La notation TTCN-3 peut servir à la spécification de tous les types de test de systèmes réactifs, effectués en divers ports de communication. Elle s'applique en général aux tests des protocoles (y compris les protocoles de communication mobile et Internet), aux tests des services (y compris les services complémentaires), aux tests des modules ainsi qu'aux tests des plates-formes employant l'architecture CORBA, des interfaces de programmation d'application (API), etc. La notation TTCN-3 n'est pas limitée aux tests de conformité et peut servir à de nombreux autres types de tests, portant par exemple sur l'interopérabilité, la robustesse, la régression, le système et l'intégration. La spécification de suites de tests pour les protocoles de la couche physique sort du cadre de cette Recommandation.

• Recommandation UIT-T Z.166 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): interface de commande*, quispécifie les interfaces de commande pour les implémentations de système de test en notation TTCN-3. La deuxième révision de la Recommandation UIT‑T Z.166 contient des modifications, des précisions et des corrections de la forme et du fond.

• Recommandation UIT-T Z.166 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): interface de commande*, quispécifie les interfaces de commande pour les implémentations de système de test en notation TTCN-3. Les interfaces de commande TTCN-3 (TCI) assurent une adaptation normalisée, en ce qui concerne la gestion, le traitement des composants de test et le codage/décodage, d'un système de test à une plate-forme de test particulière. Cette Recommandation définit les interfaces comme étant un ensemble d'opérations indépendantes du langage cible. Les interfaces sont définies de façon à être compatibles avec les normes relatives à la notation TTCN-3 (voir le § 2 de la norme ETSI ES 201 873-6 V4.8.1). La définition d'interface utilise le langage de définition d'interface (IDL) CORBA pour spécifier complètement l'interface TCI. Les paragraphes 8, 9 et 9.7 de la norme ETSI ES 201 873-6 V4.8.1 présentent les mappages de cette spécification abstraite vers les langages cibles Java et ANSI-C. Cette révision de la Recommandation contient des modifications, des précisions et des corrections de la forme et du fond.

• Recommandation UIT-T Z.167 (révisée*),* *Notation de test et de commande de test version 3 (TTCN-3): utilisation de la notation ASN.1 avec la notation TTCN-3*, qui définit une façon normative d'utiliser, avec la notation de test et de commande de test version 3 (TTCN-3), la notation ASN.1 définie dans les Recommandations UIT-T X.680, UIT-T X.681, UIT-T X.682 et UIT-T X.683. La deuxième révision de la Recommandation UIT‑T Z.167 contient des modifications (conformité et compatibilité, les spécifications et les descriptions liées au type identificateur d'objet qui figuraient dans toutes les autres Recommandations UIT-T Z.16x ont été transférées dans cette Recommandation, prise en charge des valeurs XML dans les modules ASN.1, conversion des types OID-IRI et RELATIVE-OID-IRI, valeurs réelles spéciales et sous-types contenant des valeurs spéciales et des limites exclusives, mise à jour des chaînes de langages prédéfinies, etc.), des précisions (par exemple sur la visibilité des définitions ASN.1 importées ou sur les règles de transformation) et des corrections de la forme et du fond.

• Recommandation UIT-T Z.168 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): mappage du langage CORBA IDL vers la notation TTCN-3*, qui définit les règles de mappage du langage CORBA IDL (défini dans le Chapitre 3 de la spécification ptc/06-05-01 (2006)) vers la notation de test et de commande de test version 3 (TTCN-3) (définie dans la Recommandation UIT-T Z.161) en vue de permettre les tests des systèmes employant l'architecture CORBA. La deuxième révision de la Recommandation UIT‑T Z.168 contient des modifications, des précisions et des corrections de la forme et du fond.

• Recommandation UIT-T Z.169 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): Utilisation des schémas XML avec TTCN-3*, qui définit les règles de mappage du schéma W3C vers la notation de test et de commande de test version 3 (TTCN-3) en vue de permettre les tests des systèmes, des interfaces et des protocoles XML. La troisième révision de la Recommandation UIT‑T Z.169 contient des modifications, des précisions et des corrections de la forme et du fond.

• Recommandation UIT-T Z.169 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): Utilisation des schémas XML avec TTCN-3*, qui définit les règles de mappage du schéma W3C vers la notation de test et de commande de test version 3 (TTCN-3) en vue de permettre les tests des systèmes, des interfaces et des protocoles XML. Cette révision de la Recommandation contient des modifications, des précisions et des corrections de la forme et du fond.

• Recommandation UIT-T Z.170 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): spécification des commentaires de documentation TTCN-3*, qui définit une documentation du code source en notation de test et de commande de test version 3 (TTCN-3), utilisant des commentaires particuliers. La deuxième révision de la Recommandation UIT‑T Z.170 contient des modifications, des précisions et des corrections de la forme et du fond.

• Supplément Z.Sup1(révisé), *Supplément aux Recommandations UIT‑T de la série Z.100 sur la méthodologie d'utilisation des techniques de description*,(c'est-à-dire les Recommandations UIT-T Z.100 à Z.107, Z.109, Z.110, Z.120, Z.121, Z.150, Z.151 et Z.160 à Z.170), qui présente les grandes lignes d'une méthodologie (appelée SDL+) relative à l'utilisation combinée de ces langages, en particulier lorsque le langage de spécification et de description de l'UIT est utilisé.

• Guide UIT-T Z.Imp100 (révisé), *Guide de mise en oeuvre du langage de description et de spécification – Version 2.0.1*, qui est une compilation des erreurs signalées concernant les Recommandations UIT-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 et Z.119 relatives au langage de description et de spécification et des corrections apportées. Ce Guide se veut une autre source d'informations faisant autorité à l'intention des responsables de la mise en oeuvre à lire en association avec les Recommandations proprement dites. Il n'est pas en lui-même une Recommandation UIT‑T. Toutefois, il rend compte des corrections qu'il a été convenu d'apporter aux erreurs signalées. Ce guide concerne la version SDL-2010 du langage.

• Guide UIT-T Z.Imp100 (révisé), *Guide de mise en oeuvre du langage de description et de spécification – Version 2.0.2*, qui est une compilation des erreurs signalées concernant les Recommandations UIT-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 et Z.119 relatives au langage de description et de spécification et des corrections apportées. Ce Guide se veut une autre source d'informations faisant autorité à l'intention des responsables de la mise en oeuvre à lire en association avec les Recommandations proprement dites. Il n'est pas en lui-même une Recommandation UIT‑T. Toutefois, il rend compte des corrections qu'il a été convenu d'apporter aux erreurs signalées. Ce guide concerne la version SDL-2010 du langage.

• Guide UIT-T Z.Imp100 (révisé), *Guide de mise en oeuvre du langage de description et de spécification* – *Version 3.0.0*, qui comprend toutes les modifications que le groupe chargé de la Question 12/17 a accepté d'apporter au texte des Recommandations pertinentes ayant fait l'objet d'un consentement ou en vigueur à la date d'approbation du Guide par la CE 17. Il sera applicable jusqu'à la publication de sa version suivante ou jusqu'à ce que toutes les modifications aient été intégrées dans les Recommandations pertinentes et jusqu'à ce que le Guide de mise en oeuvre ait été mis à jour en vue de la version 3.0.1.

• Guide UIT-T Z.Imp100 (révisé), *Guide de mise en oeuvre du langage de description et de spécification* – *Version 3.0.1*, qui comprend toutes les modifications que le groupe chargé de la Question 12/17 a accepté d'apporter au texte des Recommandations pertinentes ayant fait l'objet d'un consentement ou en vigueur à la date d'approbation du Guide par la CE 17. Il sera applicable jusqu'à la publication de sa version suivante ou jusqu'à ce que toutes les modifications aient été intégrées dans les Recommandations pertinentes et jusqu'à ce que le Guide de mise en oeuvre ait été mis à jour en vue de la version 3.0.2.

## 3.3 Activités de la Commission d'études 17 en tant que Commission d'études directrice, GSI, JCA, groupes régionaux et projets

La Commission d'études 17 est la Commission d'études directrice pour la sécurité des télécommunications, pour la gestion d'identité et pour les langages et les techniques de description. Les activités de la commission d'études en tant que commission d'études directrice sont réparties comme suit:

– Sécurité – activités gérées par le groupe chargé de la Question 1/17.

– Gestion d'identité – activités gérées par le groupe chargé de la Question 10/17.

– Langages et techniques de description – activités gérées par le GT 5/17.

### 3.3.1 Activités de la Commission d'études 17 en tant que Commission d'études directrice pour la sécurité

La Commission d'études 17 a été désignée Commission d'études directrice pour la sécurité conformément à la Résolution 2 de l'Assemblée mondiale de normalisation des télécommunications (AMNT‑12).

En tant que commission d'études directrice pour la sécurité des télécommunications, la Commission d'études 17 est chargée d'étudier les Questions essentielles appropriées sur la sécurité. En outre, en concertation avec les autres commissions d'études concernées et en collaboration, le cas échéant, avec d'autres organismes de normalisation, la Commission d'études 17 est chargée de définir et de tenir à jour le cadre général et de coordonner et d'attribuer (compte tenu des mandats des commissions d'études) les études devant être menées par les commissions d'études, d'établir des priorités parmi ces études, et de faire en sorte que des Recommandations cohérentes et complètes soient élaborées en temps voulu.

Au sein de la CE 17, le groupe chargé de la Question 1/17 est le coordonnateur des activités sur la sécurité pour la Commission d'études directrice. Cette coordination est assurée en étroite collaboration avec les autres commissions d'études afin d'identifier et de mettre au point des solutions de sécurité. Toutefois, pour l'intégration de ces solutions avec les différentes technologies en cours de développement, il est nécessaire de faire appel aux compétences spécifiques du groupe chargé de la Question au titre de laquelle le développement est effectué.

En tant que Commission d'études directrice pour la sécurité, la Commission d'études 17 a établi une liaison permanente avec toutes les commissions d'études de l'UIT-T dont les travaux intègrent des aspects de sécurité. La CE 17 collabore aussi avec une grande variété d'organismes de normalisation et de forums s'occupant de sécurité des TIC et des télécommunications. Un des objectifs a été d'éviter les conflits potentiels entre les travaux réalisés par les commissions d'études et les organismes extérieurs.

Par ailleurs, des réunions de coordination sur la sécurité ont eu lieu pendant chaque réunion de la Commission d'études 17 et une liste de contacts pour la sécurité a été dressée pour toutes les commissions d'études dont les travaux intègrent des aspects de sécurité.

En ce qui concerne les activités de la CE 17 en tant que commission d'études directrices, des notes de liaison sur des questions de sécurité ont été reçues des entités internes suivantes: CITS de l'UIT, CT-CCVOCAB, SCV de l'UIT, UIT‑D (Question 26/2), CE 1 de l'UIT-D (Question 22-1/1), CE 2 de l'UIT‑D (Question 3/2, Question 5/2), CE 6 de l'UIT-R, groupes de travail de l'UIT-R (GT 4B, 5A, 5B, 5C, 5D, 7C), groupes spécialisés de l'UIT-T (FG-AC, DFS, DR&NRR, Innovation, SmartCable, SSC), JCA de l'UIT‑T (JCA-AHF, CIT, Cloud, COP, IoT, Res178, SDN, SG&HN), RevCom de l'UIT‑T, commissions d'études de l'UIT-T (CE 2, 3, 5, 9, 11, 12, 13 (GT 3/13), 15, 16 (Questions 14/16, 27/16, 28/16), 20) et GCNT de l'UIT-T, et ont été traitées.

En ce qui concerne les activités de la CE 17 en tant que commission d'études directrices, des notes de liaison ont été reçues des entités extérieures suivantes: 3GPP (SA3, TSG GERAN), CSA, ETSI ISG (ISI, QSC), ETSI TC (CYBER, ITS, M2M, MTS), GSMA SG, ICANN SSAC, CEI TC (25 (JWG 1, WG 5, WG 6), 57/WG15), IETF (IAB, Security Area, STIR WG), ISO TC 12 (JWG 20, WG 18), ISO/CEI JTC 1/SC (6/WG 7, 7/WG 19, 27 (SC27/WG 1, WG 2), 37, 38), ISO/CEI JTC 1/WG 10, MEF, OASIS, oneM2M WG4 et UPU, et ont été traitées.

La CE 17 a envoyé des notes de liaison aux entités internes suivantes: CITS de l'UIT, commissions d'études de l'UIT-D (CE 1 (Question 22-1/1), 2 (Questions 3/2, 5/2)), commissions d'études de l'UIT‑R (CE 4 (GT 4A, 4B, 4C), 5 (GT 5A), 7), groupes spécialisés de l'UIT-T (FG-DFS, Innovation, SSC), JCA de l'UIT‑T (JCA-AHF, CIT, Cloud, COP, IoT, Res178, SDN, SG&HN), RevCom de l'UIT‑T, SCV de l'UIT‑T, commissions d'études de l'UIT-T (CE 2, 3, 5, 9, 11, 12, 13, 15, 16, 20) et GCNT de l'UIT‑T.

La CE 17 a envoyé des notes de liaison aux entités extérieures suivantes: 3GPP (SA3, TSG GERAN), CSA, ENISA, ETSI (ISG ISI, SAGE, TC (CYBER, ITS (WG2, WG5), M2M, MTS, SmartM2M)), BIPM, FIDO Alliance, GSMA (MMG, FASG, SG), ICRU, CEI SEG, CEI TC (25 (JWG 1), 57 WG 15, 65/WG10), IESG, IETF (SEC Area, ACE WG, CORE WG, DICE WG, STIR WG), ISO SAG-S, ISO TC (12 (JWG 20, WG 18), TC 68/SC2, 154, 204, 215, 292), ISO TMB, ISO/CEI JTC 1/SC (6 (WG 10), 27 (SG sur l'IoT, WG 1, WG 2, WG 3, WG 4, WG 5), 37 (WG 4)), JTC 1/WG 9, M3AAWG, NIST, NSTIC, OASIS TC (Identity in the cloud, IBOPS, MQTT, Trust Elevation), OIDF, OMA, oneM2M (WG4), UPnP, UPU.

En application de la Résolution 7 de l'AMNT‑12, *Collaboration avec l'Organisation internationale de normalisation et la Commission électrotechnique internationale*, la Commission d'études 17 tient à jour un tableau en ligne qui contient la liste de ses relations avec des comités techniques (TC) de l'ISO et de la CEI et des sous-comités (SC) de l'ISO/CEI JTC 1 et qui indique également la nature de la relation: travaux conjoints (par exemple textes communs ou textes jumeaux), collaboration technique par un mécanisme de liaison, ou liaison informationnelle.

En 2013, au nom de l'UIT, la CE 17 a participé à deux ateliers sur la lutte contre le spam (Atelier de l'UIT sur le thème "Lutter contre le spam", Durban (République sudafricaine), le 8 juillet 2013, et Atelier commun de la CITEL (PCC.I), de l'UIT et de l'Internet Society sur la lutte contre le spam, Mendoza (Argentine), le 7 octobre 2013), qui tous deux ont été productifs et ont eu un impact remarquable.

En 2014, la CE 17 a organisé un atelier de l'UIT d'une journée et demi sur le thème "Enjeux de la normalisation, dans le domaine de la sécurité des TIC, pour les pays en développement" à Genève les 15 et 16 septembre 2014. Plus de 90 participants ont participé à l'atelier, dont une majorité issus de pays en développement. L'atelier a permis de renforcer les compétences en matière de normalisation grâce à la fourniture de conseils concernant le contenu technique des normes internationales relatives à la sécurité des TIC et les bonnes pratiques associées. Il a aussi permis de renforcer la collaboration entre les Secteurs de la normalisation et du développement de l'UIT (UIT‑T et UIT‑D) concernant les activités dans le domaine de la sécurité, en plus de tirer parti de la collaboration entre l'UIT‑T et d'autres organismes de normalisation. Cet atelier sur la sécurité a notamment abouti à la création d'un groupe de travail par correspondance chargé de déterminer de nouveaux sujets de normalisation pour la CE 17.

En 2015, un atelier de l'UIT sur la cybersécurité ayant pour thème "[Les enjeux de la cybersécurité mondiale et la collaboration pour un renforcement efficace de la cybersécurité dans les pays en développement](http://www.itu.int/en/ITU-D/Study-Groups/2014-2018/Pages/side-events/2015/cybersecurity-workshop.aspx)" a eu lieu le 8 septembre 2015 après-midi, à l'occasion de réunions de la Commission d'études 2 de l'UIT‑D et de la Commission d'études 17 de l'UIT-T. Cet atelier a permis de fournir plusieurs indications importantes sur les problèmes de cybersécurité que rencontrent les pays en développement et de mettre en évidence les bonnes pratiques à suivre pour faire face à ces problèmes. Il a été l'occasion de montrer qu'il existe un bon esprit de collaboration entre l'UIT-T et l'UIT-D, et il s'est achevé sur un engagement des participants à élargir cette collaboration.

En particulier, le programme de travail de la CE 17 sur la sécurité inclut:

• la mise en oeuvre des Résolutions 7, 11, 40, 50, 52, 58, 64, 65, 67, 70, 73, 75, 76 et 78 de l'AMNT‑12;

• la mise en oeuvre des Résolutions 101, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200 et 201 de la PP‑10 et de la PP-14; et

• la mise en oeuvre des Résolutions 23, 30, 34, 45, 47, 54, 63, 67, 69, 79 et 80 de la CMDT‑10 et de la CMDT-14.

La Commission d'études 17 a élaboré un plan d'action fondé sur les Résolutions de l'AMNT-12, qu'elle met à jour à chacune de ses réunions.

Par ailleurs, une page d'accueil de la commission d'études directrice pour la sécurité est tenue à jour sur le site web de la Commission d'études 17, avec des liens directs vers les principaux produits et services sur la sécurité.

La CE 17 met à jour activement la base de données des normes sur la sécurité des TIC approuvées, dans le cadre de la Feuille de route relative aux normes sur la sécurité des TIC, qui représente un outil important pour les organismes de normalisation afin d'éviter toute redondance. Les pages web des Parties 1, 2 et 3 de la Feuille de route ont été mises à jour.

La CE 17 a également mis à jour le Recueil relatif à la sécurité, qui donne des informations sur les activités de normalisation menées par l'UIT dans le domaine de la sécurité et comprend le catalogue des Recommandations UIT-T portant sur la sécurité et le catalogue des définitions et abréviations approuvées par l'UIT-T en matière de sécurité.

Les travaux sur le sujet X.TRsuss ont été achevés et ont débouché sur l’élaboration d’un Rapport technique sur l'utilisation efficace des normes de sécurité, qui vise à aider les utilisateurs, en particulier ceux des pays en développement, à mieux comprendre les avantages que présente l'utilisation des Recommandations UIT‑T relatives à la sécurité dans divers contextes (par exemple pour les affaires ou le commerce, dans le secteur public ou le secteur privé). Le Rapport technique traite de l'utilisation des normes relatives à la sécurité dans diverses applications et sensibilise le lecteur à l'utilité et à l'importance des normes fondamentales dans le domaine de la sécurité, par exemple les normes sur l'architecture. On y trouve aussi une méthodologie, des définitions et d'autres orientations de haut niveau. D'une manière générale, l'objectif est d'encourager une utilisation efficace de ces normes.

Les travaux d'élaboration de la 6ème édition du Manuel sur la sécurité en tant que Rapport technique ont été achevés. Ce Manuel constitue un outil de promotion essentiel de l'UIT-T, qui présente de façon simple les travaux importants menés par toutes les commissions d'études de l'UIT-T en matière de sécurité.

Les commissions d'études de l'UIT‑T (autres que la CE 17) ont obtenu les résultats suivants concernant leurs travaux sur les Recommandations relatives à la sécurité:

Recommandations approuvées:

| CE | Recommandation | Titre |
| --- | --- | --- |
| CE 5 | K.58 | Exigences de compatibilité électromagnétique, d'immunité et de sécurité pour les équipements des technologies de l'information et de la communication installés dans un même local et lignes directrices pour la détermination des responsabilités |
| CE 5 | K.87 | Guide pour l'application des exigences de sécurité électromagnétique – Vue d'ensemble |
| CE 9 | J.1002 | Spécification du protocole d'appariement pour le système renouvelable à accès conditionnel |
| CE 9 | J.1003 | Spécifications du protocole de réseau pour le système d'accès conditionnel renouvelable |
| CE 9 | J.1004 | Spécification des interfaces avec le centre d'autorisation pour le système d'accès conditionnel renouvelable |
| CE 9 | J.1005 | Architecture et exigences applicables à la gestion des droits numériques pour les écrans multiples de télévision par câble |
| CE 13 | Y.2705 | Exigences minimales de sécurité de l'interconnexion pour le service de télécommunications d'urgence (ETS) |
| CE 13 | Y.2725 | Prise en charge du protocole OpenID dans les réseaux de prochaine génération |
| CE 13 | Y.2770 | Spécifications relatives au contrôle approfondi des paquets dans les réseaux de prochaine génération |
| CE 13 | Y.2771 | Cadre pour l'inspection approfondie des paquets |
| CE 13 | Y.2772 | Mécanismes applicables aux éléments de réseau prenant en charge l'inspection approfondie des paquets |
| CE 13 | Y.3032 | Configurations des identificateurs de noeud et mise en correspondance de ces identificateurs avec les localisateurs dans les réseaux futurs |
| CE 13 | Y.3520 (révisée) | Cadre de l'informatique en nuage pour la gestion des ressources de bout en bout |
| CE 15 | G.808.1 | Commutation de protection générique – Protection linéaire des chemins et des sous-réseaux |
| CE 15 | G.808.3 | Commutation de protection générique – Protection maillée partagée |
| CE 15 | G.873.1 | Réseau de transport optique: protection linéaire |
| CE 15 | G.873.1 Amd.1 | Réseau de transport optique: protection linéaire – Amendement 1: Nouvel Appendice III – Protection de la couche optique |
| CE 15 | G.873.2 | Protection partagée en anneau des unités ODUk |
| CE 15 | G.8031/Y.1342 (révisée) | Commutation de protection linéaire Ethernet |
| CE 16 | F.748.1 | Exigences et caractéristiques communes de l'identificateur IoT pour le service IoT |
| CE 16 | F.771 Amd.1 | Description et spécifications du service d'accès aux informations multimédias déclenché par l'identification à base d'étiquettes – Amendement 1: Prise en charge d'interfaces radioélectriques multiples |
| CE 16 | H.235.0 (révisée) | Cadre de sécurité H.323: cadre de sécurité pour les systèmes multimédias de la série UIT-T H (systèmes UIT-T H.323 et autres systèmes de type UIT-T H.245) |
| CE 16 | H.235.6 (révisée) | Sécurité H.323: Profil pour le chiffrement avec gestion de clés native dans les systèmes UIT-T H.235/H.245 |
| CE 16 | H.248.50 | Protocole de commande de passerelle: paquetages de kits pratiques pour le franchissement NAT |
| CE 16 | H.248.84 | Protocole de commande de passerelle: traversée de dispositif NAT pour les services entre homologues |
| CE 16 | H.248.86 | Protocole de commande de passerelle: Prise en charge par les systèmes UIT-T H.248 de l'inspection approfondie des paquets |
| CE 16 | H.248.90 | Protocole de commande de passerelle: Paquetages UIT-T H.248 pour le contrôle de la sécurité du transport au moyen du protocole de sécurité de la couche transport (TLS) |
| CE 16 | H.248.91 | Protocole de commande de passerelle: Lignes directrices relatives à l'utilisation des capacités UIT-T H.248 permettant d'assurer la sécurité du transport dans les réseaux TLS dans les profils UIT-T H.248 |
| CE 16 | H.248.93 | Protocole de commande de passerelle: Prise en charge UIT-T H.248 du contrôle de la sécurité du transport au moyen du protocole de sécurité de la couche transport en mode datagramme (DTLS) |
| CE 16 | H.460.18 | Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de signalisation UIT-T H.323 |
| CE 16 | H.460.19 | Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de média UIT‑T H.323 |
| CE 16 | H.460.22 | Négociation des protocoles de sécurité pour protéger les messages de signalisation d'appel UIT-T H.225.0 |
| CE 16 | H.621 Amd.1 | Architecture du système d'accès aux informations multimédias déclenché par l'identification à base d'étiquettes: Amendement 1: Prise en charge d'interfaces radioélectriques multiples |
| CE 16 | H.751 | Métadonnées pour l'interopérabilité des informations relatives aux droits dans les services de TVIP |
| CE 16 | H.810 | Directives de conception visant à assurer l'interopérabilité des systèmes de santé individuels |
| CE 16 | H.812.4 | Directives de conception visant à assurer l'interopérabilité des systèmes de santé individuels: Interface WAN: Classe de dispositifs pour une session authentifiée persistante |

**Note:**

\* Recommandations approuvées selon la procédure TAP.

**Suppléments et Appendices approuvés**

| **CE** | **Numéro** | **Titre** |
| --- | --- | --- |
| CE 13 | Y.Sup19 | Série UIT-T Y.2200 – Supplément sur le service d'analyse des risques dans les réseaux de prochaine génération |
| CE 13 | Y.Sup18 | Série UIT-T Y.2200 – Supplément sur la gestion des certificats dans les réseaux de prochaine génération |
| CE 13 | Supplément 23 à la série Y.2770 | Série UIT-T Y.2200 – Supplément sur la terminologie relative à l'inspection approfondie des paquets |
| CE 13 | Supplément 25 | Série UIT-T Y.2200 – Supplément sur les cas d'utilisation et les scénarios d'application de l'inspection DPI |
| CE 15 | G.Suppl.52 | Recommandations UIT-T de la série G – Supplément sur la commutation de protection Ethernet en anneau |
| CE 15 | G.sup54 | Recommandations UIT-T de la série G – Supplément sur la commutation de protection linéaire Ethernet |
| CE 16 | H.460.24 (2009) Amd.2 | Transmission point à point de médias via des traducteurs d'adresse réseau et des pare‑feu dans les systèmes UIT-T H.323: Prise en charge du mode média multiplex UIT‑T H.460.19 pour les flux de médias point à point |

### 3.3.2 Activités de la Commission d'études 17 en tant que commission d'études directrice pour la gestion d'identité

La Commission d'études 17 a été désignée commission d'études directrice pour la gestion d'identité (IdM) conformément à la Résolution 2 de l'Assemblée mondiale de normalisation des télécommunications (AMNT-12).

En tant que commission d'études directrice pour la gestion d'identité, la Commission d'études 17 est chargée d'étudier les Questions essentielles appropriées sur la gestion d'identité. En outre, en concertation avec les autres commissions d'études concernées et en collaboration, le cas échéant, avec d'autres organismes de normalisation, la Commission d'études 17 est chargée de définir et de tenir à jour le cadre général et de coordonner et d'attribuer (compte tenu des mandats des commissions d'études) les études devant être menées par les commissions d'études, d'établir des priorités parmi ces études, et de faire en sorte que des Recommandations cohérentes et complètes soient élaborées en temps voulu.

En particulier, la Commission d'études 17 est chargée de mener des études relatives à l'élaboration d'un modèle générique de gestion d'identité, indépendant des technologies de réseau et prenant en charge l'échange sécurisé d'informations d'identité entre des entités. Elle doit aussi étudier le processus de découverte des sources d'informations d'identité qui font autorité, les mécanismes génériques pour l'interopérabilité de divers formats d'informations d'identité, les menaces liées à la gestion d'identité, les mécanismes de lutte contre ces menaces et la protection des informations d'identification personnelle (PII) et définir des mécanismes garantissant que l'accès aux informations PII n'est autorisé que lorsque cet accès est approprié.

L'état d'avancement des travaux sur la gestion d'identité au sein des commissions d'études de l'UIT‑T est le suivant:

Les commissions d'études de l'UIT‑T (autres que la CE 17) ont obtenu les résultats suivants concernant leurs travaux sur les Recommandations relatives à la gestion d'identité:

Recommandations approuvées

| CE | Recommandation | Titre |
| --- | --- | --- |
| CE 13 | Y.2084 | Fonctions de distribution de contenus dans les réseaux de services répartis |
| CE 13 | Y.2723 | Prise en charge d'OAuth dans les réseaux de prochaine génération |
| CE 13 | Y.2724 | Cadre pour la prise en charge d'OAuth et d'OpenID dans les réseaux de prochaine génération |
| CE 13 | Y.2725 | Prise en charge du protocole OpenID dans les réseaux de prochaine génération |
| CE 13 | Y.3031 | Cadre d'identification dans les réseaux futurs |
| CE 13 | Y.3032 | Configurations des identificateurs de noeud et mise en correspondance de ces identificateurs avec les localisateurs dans les réseaux futurs |
| CE 13 | Y.3034 | Architecture d'interfonctionnement de réseaux-éléments hétérogènes dans les réseaux futurs utilisant la séparation identifiant/localisateur |
| CE 16 | F.748.1 | Exigences et caractéristiques communes de l'identificateur IoT pour le service IoT |
| CE 16 | F.771 Amd.1 | Description et spécifications du service d'accès aux informations multimédias déclenché par l'identification à base d'étiquettes – Amendement 1: Prise en charge d'interfaces radioélectriques multiples |
| CE 16 | H.621 Amd.1 | Architecture du système d'accès aux informations multimédias déclenché par l'identification à base d'étiquettes: Amendement 1: Prise en charge d'interfaces radioélectriques multiples |
| CE 16 | H.642.1 | Accès à des informations multimédias basée en identification par étiquettes – Mécanisme d'identification |
| CE 16 | H.642.2 | Accès à des informations multimédias basée en identification par étiquettes – Procédures d'enregistrement des identificateurs |
| CE 16 | H.642.3 | Technologies de l'information – Technique d'identification automatique et de saisie des données – Protocole de résolution d'identificateur pour l'accès à des informations multimédias déclenché par une identification basée sur une étiquette |
| CE 16 | H.642.2 | Accès à des informations multimédias basée en identification par étiquettes – Procédures d'enregistrement des identificateurs |

**Suppléments approuvés**

| CE | Supplément | Titre |
| --- | --- | --- |
| CE 13 | Y.Suppl.18 | Série UIT-T Y.2200 – Supplément sur la gestion des certificats dans les réseaux de prochaine génération |

Un wiki contenant la feuille de route sur la gestion d'identité a été créé sur la page web de la CE 17 afin de présenter une compilation des normes sur la gestion d'identité qui existent ou qui sont en cours d'élaboration à l'échelle mondiale. Cette feuille de route sur la gestion d'identité rend compte de la coordination avec les autres organismes de normalisation et forums travaillant dans le domaine de la gestion d'identité afin d'éviter toute redondance de tâches.

Par ailleurs, une page d'accueil de la Commission d'études directrice pour la gestion d'identité est tenue à jour sur le site web de la Commission d'études 17, avec des liens directs vers les principales ressources.

### 3.3.3 Activités de la Commission d'études 17 en tant que Commission d'études directrice pour les langages et les techniques de description

La Commission d'études 17 a été désignée Commission d'études directrice pour les langages et les techniques de description conformément à la Résolution 2 de l'Assemblée mondiale de normalisation des télécommunications (AMNT-12).

En tant que Commission d'études directrice pour les langages et les techniques de description, la Commission d'études 17 est chargée, en ce qui concerne les langages et les techniques de description pour les télécommunications:

– de fournir des indications sur l'utilisation des langages et des techniques de description aux membres et aux autres commissions d'études de l'UIT‑T;

– de tenir à jour l'ensemble des Recommandations UIT‑T et autres lignes directrices relatives aux langages et aux techniques de description utilisés pour les télécommunications;

– de fournir des conseils sur les langages appropriés disponibles par ailleurs, à utiliser si aucun langage approprié n'est défini dans une Recommandation UIT‑T;

– d'interagir avec d'autres organismes reconnus tels que l'IETF et l'OMG qui utilisent ou définissent des langages et techniques de description complémentaires.

S'agissant des Questions 11/17 et 12/17, le GT 5/17 a été productif concernant les langages et techniques de description ASN.1, ODP, SDL, MSC, URN et TTCN. Une collaboration étroite avec d'autres commissions d'études et organisations a permis de faire avancer les travaux.

Le groupe chargé de la Question 11/17 travaille en collaboration avec l'ISO/CEI JTC 1/SC 6/ WG 10 concernant la notation de syntaxe abstraite numéro un (ASN.1), avec la publication de textes communs dans les séries X.680/X.690/X.890. L'ensemble des Recommandations des séries X.680/X.690 sur la notation ASN.1 a été révisé en 2015.

Le groupe chargé de la Question 11/17 travaille aussi en collaboration avec l'ISO/CEI JTC 1/SC 7/ WG 19 à l'élaboration de textes communs sur le traitement réparti ouvert (ODP). Les Recommandations UIT‑T X.906 (UML pour ODP) et X.911 (Langage d'entreprise) ont été révisées.

Les Rapporteurs pour la Question 12/17 se sont mobilisés pour organiser des ateliers afin de faire participer davantage le secteur privé et les établissements universitaires à l'élaboration de Recommandations sur les langages et à la mise au point d'outils d'appui. Pendant cette période d'études, les ateliers suivants ont eu lieu:

– 16ème Forum international sur les langages de conception de systèmes, Ingénierie de fiabilité fondée sur des modèles, 26-28 juin 2013, Montréal (Canada).

– 8ème Conférence sur l'analyse et la modélisation des systèmes (SAM-2014), dans le cadre de la Conférence MODELS-2014, 29-30 septembre 2014, Valence (Espagne).

– 17ème Forum international sur les langages de conception de systèmes – 12‑14 octobre 2015, Berlin (Allemagne).

– 9ème Conférence sur l'analyse et la modélisation des systèmes (SAM-2016), 3‑4 octobre 2016, Saint Malo (France).

Ces manifestations approuvées par la CE 17 sont organisées avec l'appui de l'UIT, qui contribue à leur publicité. Les membres de la SDL Forum Society participent aux travaux en cours menés au titre de la Question 12/17 sur la révision du langage de description et de spécification (SDL-2010) dans la série Z.100.

Concernant la Question 12/17, les travaux se font en relation étroite avec l'ETSI TC MTS, notamment pour la tenue à jour des Recommandations des séries Z.160 et Z.170 sur la notation TTCN‑3. Six nouveaux textes et 24 textes révisés ont été approuvés.

Par ailleurs, une page d'accueil de la Commission d'études directrice pour les langages et les techniques de description est tenue à jour sur le site web de la Commission d'études 17, avec une présentation générale de chacun des langages.

Les commissions d'études de l'UIT-T (autres que la CE 17) ont obtenu les résultats suivants concernant leurs travaux sur les Recommandations relatives aux langages:

Recommandations approuvées

| CE | Recommandation | Titre |
| --- | --- | --- |
| CE 13 | Y.3320 | Exigences relatives à l'application de méthodes formelles pour les réseaux pilotés par logiciel |

### 3.3.4 GSI et JCA

La CE 17 n'a chapeauté aucune initiative de normalisation mondiale (GSI) pendant cette période d'études. Deux activités conjointes de coordination (JCA) placées sous les auspices de la CE 17 permettent de soutenir la CE 17 dans ses fonctions de commission d'études directrice.

#### 3.3.4.1 JCA-IdM

Pendant cette période d'études, l'Activité conjointe de coordination sur la gestion d'identité (JCA‑IdM) a poursuivi ses activités menées pendant la période d'études précédente, tel que proposé au GCNT qui a donné son aval. La JCA-IdM a pour objet de coordonner le bon déroulement des travaux de l'UIT-T sur la gestion d'identité entre les commissions d'études (en particulier avec les CE 2, 13, 17 et 20) et de faire office de point de contact au sein de l'UIT-T et avec les autres organisations de normalisation/forums/consortiums sur la gestion d'identité afin d'éviter toute répétition des travaux et de faciliter la réalisation des tâches sur la gestion d'identité attribuées par l'AMNT‑12 dans sa Résolution 2 et la mise en oeuvre de la Résolution 4 du GSC-16 sur la gestion d'identité. La JCA-IdM a convenu de changer de cap dans ses activités, en particulier de s'intéresser davantage aux obstacles qui entravent la normalisation de la gestion d'identité, et de mieux tirer parti de la collaboration.

Des représentants des Commissions d'études 13 et 17 ainsi que d'un certain nombre d'organismes extérieurs concernés de premier plan ont participé aux dix réunions de la JCA-IdM, durant lesquelles 44 documents ont été traités, et d'importants efforts de coordination ont été accomplis entre les commissions d'études et divers organismes de normalisation extérieurs. Dans l'ensemble, la participation aux réunions de la JCA-IdM a été excellente et d'importants progrès ont été réalisés. Les organismes de normalisation extérieurs qui ont participé à ces réunions de la JCA-IdM étaient notamment les suivants: ISO/CEI JTC 1/SC 27/WG 5, ETSI/ISG, ENISA, OASIS/IdCloud TC, OASIS Trust Elevation TC, OASIS IBOPS, OpenID Foundation, FIDO Alliance, OASIS TC IBOPS, Kantara Initiative, American Bar Association, GLEIF, STORK 2.0 project et UPU.

La CE 17 a approuvé l'habilitation de l'OpenID Foundation conformément aux Recommandations UIT-T A.4 et A.5 et a lancé les procédures d'habilitation A.4 et A.5 concernant la FIDO Alliance.

Un wiki contenant la feuille de route sur la gestion d'identité a été créé sur la page web de la CE 17 afin de présenter une compilation des normes sur la gestion d'identité qui existent ou qui sont en cours d'élaboration à l'échelle mondiale. Cette feuille de route sur la gestion d'identité rend compte de la coordination avec les autres organismes de normalisation et forums travaillant dans le domaine de la gestion d'identité afin d'éviter toute redondance de tâches.

#### 3.3.4.2 JCA‑COP

La JCA‑COP a pour objet de coordonner les travaux sur la protection en ligne des enfants (COP) menés au sein des commissions d'études de l'UIT‑T et d'assurer la liaison avec l'UIT‑R et l'UIT‑D, ainsi qu'avec le Groupe de travail du Conseil sur la protection en ligne des enfants. La JCA-COP réunit diverses parties prenantes afin d'obtenir des informations sur les activités et les bonnes pratiques, mais aussi d'identifier les lacunes et d'élaborer une feuille de route pour les futures normes en matière de protection en ligne des enfants.

La JCA-COP a tenu huit réunions (dont six réunions traditionnelles, colocalisées avec les réunions de la CE 17, et deux réunions électroniques) pendant la présente période d'études; toutes les réunions de la JCA-COP ont rassemblé de nombreux participants.

Des présentations ont été soumises par les entités suivantes: ISO/CEI JTC 1/SC 27/WG5, IETF/ISOC, UIT‑D (Question 3/2), DeafKidzInternational, ECPAT, EFC, FCACP, FOSI, GSMA, ICMEC, I-KiZ et Iran (République islamique d').

Des notes de liaison ont été reçues des entités suivantes: CE 1 de l'UIT-D (Question 22-1/1), groupes spécialisés de l'UIT-T (FG-SSC, DR&NRR), JCA de l'UIT-T (JCA-AHF, SG&HN), commissions d'études de l'UIT-T (CE 2, 3, 9, 16, 17 et 20), RevCom de l'UIT‑T et GTC-COP de l'UIT, qui a soumis régulièrement des rapports.

Des notes de liaison ont été envoyées aux entités suivantes: FG-SSC de l'UIT‑T, JCA-AHF de l'UIT‑T et UIT-D (Question 22-1/1).

### 3.3.5 Groupe régional de la Commission d'études 17 pour l'Afrique (SG17-RG-AFR)

Lors de sa réunion d'avril 2015, la CE 17 a créé le Groupe régional de la CE 17 pour l'Afrique. M. Michael KATUNDU (Kenya) est le Président du Groupe et M. Mohamed ELHAJ (Soudan), M. Patrick MWESIGWA (Ouganda) et M. Mohamed TOURÉ (Guinée) en sont les Vice‑Présidents. Le Groupe SG17-RG-AFR a tenu deux réunions, l’une à Abidjan (Côte d'Ivoire) les 21 et 22 janvier 2016 et l’autre à Khartoum (République du Soudan) les 27 et 28 juillet 2016. A la première réunion, les participants ont identifié un certain nombre de questions d'actualité intéressant l'Afrique. Ils ont en outre fait part de plusieurs idées concernant la structure du groupe régional et les sujets qui pourraient être confiés aux coordonnateurs. Les participants ont examiné trois contributions et élaboré deux documents destinés à être examinés à la réunion de la CE 17 de mars 2016. A la deuxième réunion, les participants se sont mis d’accord sur une structure du groupe régional comportant trois groupes de travail:

GT 1: Cybersécurité, co-présidé par M. Adetunji BASORUN (Nigéria) et M. N’takpe Ernest ’OKA (République de Côte d’Ivoire).

GT 2: Sécurité des transactions électroniques sur mobile, co-présidé par M. Abubakar MAINA (Nigéria) et M. William K’DIO (République de Côte d’Ivoire).

GT 3: Sécurité de l’infrastructure Internet, co-présidé par M. Mutaz ISHAG (République du Soudan), M. Egide NDAYIZEYE (Burundi) et M. Bertrand Kisito NGA (Cameroun).

## 3.4 Projets

Dans le cadre des projets ASN.1 et OID, la CE 17 continue d'apporter une assistance:

• aux utilisateurs existants de l'ASN.1 et d'identificateurs d'objet (OID), à l'intérieur et à l'extérieur de l'UIT‑T (par exemple CE 16 de l'UIT‑T, ISO/CEI JTC 1/SC 27, ISO TC 215, 3GPP, etc.);

• aux pays et en particulier aux pays en développement pour la mise en place d'une autorité nationale d'enregistrement des identificateurs d'objet.

Ces projets rassemblent des intervenants et des tutoriels et coordonnent par ailleurs l'assistance aux utilisateurs pour ce qui est des outils ainsi que le contenu des sites web associés.

### 3.4.1 Projet ASN.1

Le projet ASN.1, placé sous la direction de M. Paul Thorpe, offre une assistance aux utilisateurs de la notation ASN.1 (Rec. UIT-T des séries X.680, X.690 et X.890), à l'intérieur et à l'extérieur de l'UIT-T (par exemple CE 16 de l'UIT‑T, ISO/CEI JTC 1/SC27, ISO/TC 215, ETSI LI, 3GPP, etc.). Par ailleurs, une aide est fournie au TSB pour la tenue à jour d'une base de données des modules ASN.1 exempts d'erreurs. La base de données des modules ASN.1 continue d'être complétée et permet aux responsables de la mise en oeuvre d'accéder aux spécifications ASN.1 publiées, vérifiées du point de vue de la syntaxe et lisibles par un ordinateur. Cette base de données contient plus de 840 modules définis dans plus de 200 Recommandations UIT-T et les modules définis par d'autres organismes de normalisation auxquels il est fait référence dans lesdites Recommandations.

En coopération avec le TSB, une base de données contenant une copie exploitable par machine de la version actuelle de tous les modules ASN.1 inclus dans les Recommandations de l'UIT‑T est tenue à jour. La fourniture d'une base de données en ligne des modules ASN.1 est un outil à forte valeur ajoutée pour l'UIT‑T par rapport aux autres organisations de normalisation. Elle permet d'améliorer l'efficacité des entreprises grâce à un gain de temps et d'argent. Les mises en oeuvre des Recommandations associées de l'UIT‑T nécessitent un format électronique (utilisant le codage ASCII) pour pouvoir traiter directement les définitions formelles avec les outils existants. L'obtention d'un codage ASCII à partir d'un document imprimé ou post-script nécessite une nouvelle frappe, ce qui ralentit la mise en oeuvre et peut introduire des erreurs. Le fait que tous les modules ASN.1 soient au même endroit facilite grandement la mise en oeuvre des protocoles correspondants. La base de données ASN.1 contient aussi certains modules provenant de plusieurs autres organismes de normalisation.

### 3.4.2 Projet OID

Les identificateurs d'objets permettent de référencer de façon universelle et univoque des objets utilisés ou définis dans des normes. Les travaux menés au titre de la Question 11/17 sur l'enregistrement hiérarchique des identificateurs d'objet de l'UIT‑T (séries UIT-T X.660 et X.670) se sont poursuivis activement en collaboration avec l'ISO/CEI JTC 1/SC 6.

L'arborescence des identificateurs d'objet internationaux compte plus de 966 000 enregistrements dans le répertoire des identificateurs d'objet à l'adresse <http://www.oid-info.com>, et permet d'identifier des objets (de toute sorte) via un système d'attribution hiérarchique contrôlé conjointement par l'UIT‑T et l'ISO/CEI. Les identificateurs d'objet permettent d'identifier des objets au moyen de n'importe quelle langue du monde entier (de manière structurée et hiérarchique).

Le projet OID, placé sous la direction de M. Olivier Dubuisson, aide les administrations nationales et les organismes nationaux relevant de l'ISO/CEI à mettre en place une autorité d'enregistrement pour l'identificateur d'objet de leur pays, par exemple dans les pays suivants: Algérie, Andorre, Argentine, Bolivie, Bosnie-Herzégovine, Brésil, Honduras, Lituanie, Malaisie, Mongolie, Nicaragua, Oman, Philippines, Rwanda et Sri Lanka.

## 3.5 Autres activités

### 3.5.1 Réduire l'écart en matière de normalisation

Depuis septembre 2013, la CE 17 organise régulièrement une session sur la réduction de l'écart en matière de normalisation pendant ses réunions. Ces sessions ont apportéd'innombrables informations sur le programme, les activités et les projets de l'UIT consacrés à la réduction de l'écart en matière de normalisation, et constituent une excellente occasion pour les pays en développement de faire part de leurs suggestions à la CE 17. Les sessions permettent aux pays en développement d'exprimer leurs intérêts et leurs besoins.

### 3.5.2 Mémorandum d'accord sur le commerce électronique

Le mémorandum d'accord sur le commerce électronique a été signé entre la Commission électrotechnique internationale (CEI), l'Organisation internationale de normalisation (ISO), l'UIT‑T et la Commission économique des Nations Unies pour l'Europe (CEE/ONU). Des groupes d'utilisateurs internationaux ainsi que certains forums et consortiums participent également à la mise en oeuvre du mémorandum d'accord. L'objet du mémorandum d'accord est de réduire autant que possible le risque d'approches divergentes et contradictoires concernant la normalisation, d'éviter la redondance des efforts et d'éviter la confusion parmi les utilisateurs.

La participation au groupe chargé de la gestion du mémorandum d'accord a permis de mieux coordonner et de mieux partager les informations sur les activités de la Commission d'études 17 concernant la sécurité, la télébiométrie, la gestion d'identité, les réseaux de capteurs ubiquitaires (USN), l'ASN.1, les identificateurs d'objet (OID) ainsi que sur des travaux connexes réalisés par d'autres commissions d'études.

### 3.5.3 Groupe consultatif stratégique de l'UIT-T/ISO/CEI sur la sécurité (SAG-S)

Le groupe SAG-S reconstitué était un groupe qui relevait du Bureau de gestion technique de l'ISO. La CE 17 de l'UIT‑T, en sa qualité de Commission d'études directrice de l'UIT‑T pour la sécurité, a participé aux réunions électroniques du groupe SAG-S tout au long de 2013 et a fourni à ce groupe des contributions concernant les Recommandations publiées par l'UIT‑T sur la sécurité et des projets, comme indiqué dans le document "Threat Collection". Le groupe SAG-S reconstitué était axé sur l'ISO et, malheureusement, n'a joué aucun rôle de coordination entre l'ISO, la CEI et l'UIT‑T, comme il le faisait auparavant. Le Bureau de gestion technique de l'ISO a mis fin aux activités du groupe SAG-S en 2014.

# 4 Observations concernant les travaux futurs

Les travaux de la Commission d'études 17 sur la sécurité n'ont cessé de prendre de l'ampleur tout au long de cette période d'études, faisant de cette commission un centre d'excellence spécialisé dans le domaine de la sécurité. La Commission d'études 17 est la commission d'études directrice de l'UIT‑T pour la sécurité. Les travaux de la CE 17 se sont poursuivis tout au long de cette période d'étude. Un ensemble solide de Recommandations sur la sécurité a été établi, des accords de collaboration avec d'autres organismes sont en place et un programme de travail sur des Questions relatives à la sécurité pour la prochaine période d'études est proposé dans la Partie II du rapport de la Commission d'études 17. Etant donné que le renforcement de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC) fait partie des premières priorités de l'UIT, il est essentiel que cette compétence de l'UIT‑T en matière de sécurité soit développée et renforcée, et non pas fragmentée.

La distinction entre réseaux de télécommunication et réseaux et applications informatiques continue de s'estomper. Les activités de la Commission d'études 17 sur la sécurité (architecture générique de sécurité, cadre, mécanismes et lignes directrices relatives à la gestion pour des réseaux/systèmes/services hétérogènes) doivent être poursuivies et il est nécessaire qu'une commission d'études directrice pour la sécurité coordonne les travaux réalisés par l'UIT et par les autres organisations de normalisation. La Commission d'études 17 estime en outre qu'il sera de plus en plus nécessaire d'élaborer des lignes directrices sur la sécurité qui répondent aux besoins de tous les pays.

Le renforcement du cadre de confiance, de l'authentification et de la protection des informations d'identification personnelle est une condition préalable au développement de la société de l'information et au renforcement de la confiance parmi les utilisateurs des TIC. La sécurité des télécommunications et des technologies de l'information et de la communication (sécurité des TIC) reste un domaine dans lequel de nouvelles normes seront nécessaires. De nouvelles technologies émergentes comme l'informatique en nuage, les réseaux électriques intelligents, les systèmes de transport intelligents, les réseaux cellulaires de 5ème génération, les réseaux pilotés par logiciel, l'analyse des mégadonnées, l'Internet des objets, nécessitent que des mesures techniques soient prises pour assurer la protection des informations d'identification personnelles (PII) des citoyens ainsi que la protection en ligne des enfants. De nouvelles approches en matière de sécurité pour faire face efficacement aux menaces qui pèsent sur la sécurité pourront être nécessaires. La Commission d'études 17 a un rôle essentiel à jouer dans l'élaboration de Recommandations internationales dans ces domaines. Pour définir les approches en matière de sécurité nécessaires pour les nouvelles technologies, le mieux est de faire appel à la commission d'études experte en ce qui concerne les approches existantes en matière de sécurité.

Les activités de la Commission d'études 17 en tant que commission d'études directrice pour la sécurité et ses activités de liaison et de coordination lui permettent de se tenir au courant des activités sur la sécurité menées par les autres commissions d'études ainsi que des travaux menés par les autres organismes de normalisation et consortiums. Les activités de liaison et de coordination de la CE 17 devraient continuer d'être importantes à l'avenir. La CE 17 travaille depuis longtemps en collaboration avec d'autres organismes de normalisation à l'élaboration conjointe de Recommandations/normes. D'une manière générale, en tant que commission d'études directrice et afin de mieux soutenir ses activités de normalisation dans le domaine de la sécurité, la CE 17 a recours à des mécanismes de liaison (correspondance, coopération officielle conformément aux Recommandations UIT‑T A.4/A.5/A.6) ainsi qu'à la citation de textes en référence et à l'élaboration de textes en commun (Recommandations UIT‑T A.23/A.25).

La CE 17 est également la commission d'études directrice pour la gestion d'identité (IdM), essentielle à l'échelle mondiale pour la gestion des identités numériques, l'établissement de la confiance, la protection des informations d'identification personnelles, l'exploitation des réseaux et le contrôle d'accès à un réseau ou à un service, la réalisation de transactions électroniques en ligne, les services financiers numériques, etc. Comme la gestion d'identité est extrêmement importante pour renforcer la confiance et la sécurité dans l'utilisation des TIC, les activités sur la gestion d'identité sont menées dans le cadre de la Commission d'études 17 en tant que commission d'études directrice de l'UIT‑T pour la sécurité. La CE 17 continue de coordonner les activités relatives à la gestion d'identité menées par l'UIT et par d'autres organisations de normalisation. Ses travaux concernant l'infrastructure PKI, la notation ASN.1 et les identificateurs d'objet ont été utiles dans plusieurs secteurs liés aux TIC.

Pour que la sécurité soit assurée, de nouvelles normes seront nécessaires. L'UIT a admis depuis longtemps qu'il est important de disposer de moyens d'expression structurés tels que la notation de syntaxe abstraite numéro un (ASN.1). Dans le cas de l'ASN.1, une étape importante a été franchie lorsqu'il a été décidé de faire en sorte que les déclarations ASN.1 figurant dans les Recommandations UIT‑T soient conformes à la définition de l'ASN.1 et soient mises à disposition sous forme de fichiers lisibles par machine. Le recours à cette approche (et aux ressources d'appui de l'UIT) pour les autres langages de spécification (par exemple le langage de spécification et de description (SDL)) pourrait encore améliorer la sécurité inhérente aux Recommandations de bonne qualité. Le fait d'utiliser ces Recommandations pourra être utile pour les produits. Outre les langages formels à utiliser pour rédiger les Recommandations, l'UIT a aussi spécifié la notation de test et de commande de test (TTCN) pour rédiger des tests de conformité (et d'autres tests).

Les nouveaux environnements, par exemple en ce qui concerne la sécurité de l'Internet des objets (IoT) et des réseaux électriques intelligents, entraînent des exigences pour l'infrastructure PKI qui ne sont pas encore prises en compte dans l'actuelle Recommandation UIT-T X.509. L'actuelle infrastructure PKI a été conçue au départ pour sécuriser uniquement les services bancaires et d'administration publique en ligne, mais pas pour prendre en charge des environnements comportant des entités aux capacités limitées, des millions ou des milliards d'entités sans interaction humaine. En l'absence d'amélioration de l'infrastructure PKI pour l'adapter à ces nouveaux environnements, des aspects importants de la sécurité de l'IoT et des réseaux électriques intelligents ne seront pas pris en compte, ce qui aura un impact considérable pour la société car la stabilité d'une partie importante des infrastructures essentielles sera affectée. Pendant la prochaine période d'études, il convient d'accorder une grande priorité aux travaux visant à améliorer l'infrastructure PKI afin de prendre en charge les nouveaux environnements.

# 5 Mises à jour de la Résolution 2 de l'AMNT pour la période d'études 2017-2020

L'Annexe 2 contient les mises à jour de la Résolution 2 de l'AMNT proposées par la Commission d'études 17 en ce qui concerne les domaines d'étude généraux, le nom, le mandat, les rôles de commission d'études directrice et les points de repère pour la prochaine période d'études.

ANNEXE 1

Liste des Recommandations, Suppléments et autres documents produits ou supprimés pendant la période d'études

La liste des Recommandations nouvelles ou révisées approuvées pendant la période d'études figure dans le Tableau 7.

Le Tableau 7 énumère les **Recommandations, amendements et corrigendums** approuvés pendant cette période d'études **à la date** de l'établissement du tableau. Les textes sont classés par Recommandation (ordre alphanumérique) puis par date d'approbation (versions les plus anciennes en premier). Une Recommandation portant un double numéro apparaît une seule fois. Une Recommandation qui a été suivie par d'autres commissions d'études n'apparaît que dans le cadre de la commission d'études qui l'a approuvée.

La liste des Recommandations ayant fait l'objet d'une détermination/d'un consentement à la dernière réunion de la Commission d'études 17 figure dans le Tableau 8.

Les textes sont classés par Recommandation (ordre alphanumérique). Une Recommandation portant un double numéro apparaît une seule fois. Une Recommandation qui a été suivie par d'autres commissions d'études n'apparaît que dans le cadre de la commission d'études qui a procédé à son consentement ou à sa détermination.

NOTE – Dans le présent rapport, on entend par dernière réunion celle du 7 septembre 2016.

La Liste des Recommandations supprimées par la Commission d'études 17 pendant la période d'études figure dans le Tableau 9. Les textes sont classés par Recommandation (ordre alphanumérique). Une Recommandation portant un double numéro apparaît une seule fois.

Le Tableau 10 contient la liste des Recommandations soumises par la Commission d'études 17 à l'AMNT‑16pour approbation.

Les Tableaux 11 et suivants présentent la liste des autres publications approuvées ou supprimées par la Commission d'études 17 pendant la période d'études.

Le Tableau 11 contient la liste des suppléments approuvés pendant cette période d'études, **à la date** de l'établissement du tableau.

Tableau 7

Commission d'études 17 – Recommandations approuvées pendant la période d'études

| Recommandation | Approbation | N/R | Statut | TAP/ AAP | Titre |
| --- | --- | --- | --- | --- | --- |
| F.511 | 06-04-2014 | Nouvelle | En vigueur | AAP | Service d'annuaire – Prise en charge des services d'identification par étiquette |
| X.226 Cor.1 | 16-07-2015 |  | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – Protocole de présentation en mode connexion: spécification du protocole – Corrigendum technique 1 |
| X.227*bis* Cor.1 | 16-07-2015 |  | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode connexion pour l'élément de service de contrôle d'association des objets de service d'application – Corrigendum technique 1 |
| X.500 | 14-10-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services |
| X.501 | 14-10-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles |
| X.509 (2012) Cor.1 | 28-05-2015 |  | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut – Corrigendum technique 1 |
| X.509 (2012) Cor.2 | 29-04-2016 |  | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut – Corrigendum technique 2 |
| X.509 (2012) Cor.3 | 14-10-2016 |  | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut – Corrigendum technique 3 |
| X.509 | 14-10-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadres pour les certificats de clé publique et d'attribut |
| X.511 | 14-10-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: définition de service abstrait |
| X.518 | 14-10-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: procédures pour le fonctionnement réparti |
| X.519 | 14-10-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécification des protocoles |
| X.520 (2012) Cor.1 | 13-11-2014 |  | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attributs sélectionnés – Corrigendum technique 1 |
| X.520 | 14-10-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attributs sélectionnés |
| X.521 | 14-10-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: classes d'objets sélectionnées |
| X.525 | 14-10-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: duplication |
| X.667 | 14-10-2012 | Révisée | En vigueur | AAP | Technologies de l'information – Procédures opérationnelles des autorités d'enregistrement des identificateurs d'objet: génération des identificateurs uniques universels et utilisation de ces identificateurs dans les identificateurs d'objet |
| X.675 | 15-06-2015 | Nouvelle | En vigueur | AAP | Cadre de résolution basé sur les identificateurs d'objet pour les identificateurs et localisateurs hétérogènes |
| X.680 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base |
| X.680 (2008) Cor.2 | 01-03-2014 |  | Supprimé | AAP | Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base – Corrigendum technique 2 |
| X.681 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels |
| X.682 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes |
| X.682 (2008) Cor.1 | 01-03-2014 |  | Obsolète | AAP | Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes – Corrigendum technique 1 |
| X.683 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un |
| X.683 (2008) Cor.1 | 01-03-2014 |  | Obsolète | AAP | Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un – Corrigendum technique 1 |
| X.690 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives |
| X.690 (2008) Cor.2 | 01-03-2014 |  | Obsolète | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives – Corrigendum technique 2 |
| X.691 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact |
| X.691 (2008) Cor.3 | 13-11-2014 |  | Obsolète | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact – Corrigendum technique 3 |
| X.691 (2008) Cor.4 | 13-11-2014 |  | Obsolète | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact – Corrigendum technique 4 |
| X.691 (2015) Cor.1 | 14-10-2016 |  | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact – Corrigendum technique 1 |
| X.692 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: spécification de la notation de contrôle de codage (ECN) |
| X.693 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: règles de codage XML (XER) |
| X.693 (2008) Cor.2 | 01-03-2014 |  | Obsolète | AAP | Technologies de l'information – Règles de codage ASN.1: règles de codage XML (XER) – Corrigendum technique 2 |
| X.694 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: mappage en ASN.1 des définitions de schéma XML du W3C |
| X.694 (2008) Cor.2 | 01-03-2014 |  | Obsolète | AAP | Technologies de l'information – Règles de codage ASN.1: mappage en ASN.1 des définitions de schéma XML du W3C – Corrigendum technique 2 |
| X.695 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: enregistrement et application des instructions de codage PER |
| X.696 | 29-08-2014 | Nouvelle | Obsolète | AAP | Technologies de l'information – Spécification des règles de codage des octets (OER) |
| X.696 | 13-08-2015 | Révisée | En vigueur | AAP | Technologies de l'information – Spécification des règles de codage des octets (OER) |
| X.906 | 07-10-2014 | Révisée | En vigueur | AAP | Technologies de l'information – Traitement réparti ouvert – Utilisation du langage UML pour les spécifications de systèmes ODP |
| X.911 | 13-09-2014 | Révisée | En vigueur | AAP | Technologies de l'information – Traitement réparti ouvert – Modèle de référence – Langage d'entreprise |
| X.1033 | 29-04-2016 | Nouvelle | En vigueur | AAP | Lignes directrices sur la sécurité des différents services d'information fournis par les opérateurs |
| X.1037 | 07-10-2013 | Nouvelle | En vigueur | AAP | Lignes directrices techniques concernant la sécurité dans le cadre du déploiement du protocole IPv6 |
| X.1038 | 14-10-2016 | Nouvelle | En vigueur | AAP | Exigences de sécurité et architecture de référence pour les réseaux pilotés par logiciel |
| X.1039 | 14-10-2016 | Nouvelle | En vigueur | AAP | Mesures de sécurité techniques pour la mise en oeuvre des dimensions de sécurité UIT-T X.805 |
| X.1051 | 29-04-2016 | Révisée | En vigueur | AAP | Technologies de l'information – Techniques de sécurité – Lignes directrices basées sur la norme ISO/CEI 27002 pour la gestion de la sécurité des informations pour les organisations de télécommunication |
| X.1085 | 14-10-2016 | Nouvelle | En vigueur | AAP | Technologies de l'information – Techniques de sécurité – Cadre d'authentification télébiométrique utilisant un module matériel de sécurité biométrique |
| X.1087 | 14-10-2016 | Nouvelle | En vigueur | AAP | Contremesures techniques et opérationnelles pour les applications de la télébiométrie utilisant des dispositifs mobiles |
| X.1092 | 13-06-2013 | Nouvelle | En vigueur | AAP | Cadre intégré pour la protection des données de télébiométrie dans les domaines de la cybersanté et de la télémédecine |
| X.1144 | 14-10-2013 | Nouvelle | En vigueur | AAP | Langage de balisage extensible de contrôle d'accès (XACML) 3.0 |
| X.1154 | 26-04-2013 | Nouvelle | En vigueur | TAP | Cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité |
| X.1155 | 29-10-2015 | Nouvelle | En vigueur | AAP | Lignes directrices relatives à l'authentification anonyme reliable locale pour les services électroniques |
| X.1156 | 13-06-2013 | Nouvelle | En vigueur | AAP | Cadre de non–répudiation basé sur un mot de passe à usage unique |
| X.1157 | 17-09-2015 | Nouvelle | En vigueur | TAP | Capacités techniques de détection des fraudes et de réponse pour les services exigeant un niveau de garantie élevé |
| X.1158 | 13-11-2014 | Nouvelle | En vigueur | AAP | Mécanismes d'authentification à plusieurs facteurs utilisant un dispositif mobile |
| X.1159 | 13-11-2014 | Nouvelle | En vigueur | AAP | Architecture de non–répudiation déléguée fondée sur la Recommandation UIT–T X.813 |
| X.1163 | 28-05-2014 | Nouvelle | En vigueur | AAP | Exigences et mécanismes de sécurité des réseaux de télécommunication pair à pair |
| X.1198 | 13-06-2013 | Nouvelle | En vigueur | AAP | Plate–forme de sécurité basée sur une machine virtuelle pour une protection de service et de contenu de TVIP renouvelable |
| X.1208 | 24-01-2014 | Nouvelle | En vigueur | TAP | Indicateur de risque de cybersécurité en vue de renforcer la confiance et la sécurité dans l'utilisation des télécommunications/technologies de l'information et de la communication |
| X.1210 | 24-01-2014 | Nouvelle | En vigueur | TAP | Description générale des mécanismes de résolution des problèmes de sécurité à la source dans les réseaux fondés sur le protocole Internet |
| X.1211 | 26-09-2014 | Nouvelle | En vigueur | TAP | Techniques pour prévenir les attaques sur le web |
| X.1243 (2010) Cor.1 | 24-01-2014 |  | En vigueur | TAP | Système de passerelle interactive pour la lutte contre le spam: Corrigendum 1 |
| X.1246 | 17-09-2015 | Nouvelle | En vigueur | TAP | Technologies intervenant dans la lutte contre le spam vocal dans les organisations de télécommunication |
| X.1247 | 23-03-2016 | Nouvelle | En vigueur | TAP | Cadre technique de lutte contre le spam par messagerie mobile |
| X.1255 | 04-09-2013 | Nouvelle | En vigueur | TAP | Cadre pour la découverte des informations relatives à la gestion d'identité |
| X.1256 | 23-03-2016 | Nouvelle | En vigueur | TAP | Lignes directrices et cadre pour le partage des résultats d'authentification réseau avec des applications de services |
| X.1257 | 23-03-2016 | Nouvelle | En vigueur | TAP | Taxonomie de la gestion d'identité et d'accès |
| X.1258 | 07-09-2016 | Nouvelle | En vigueur | TAP | Authentification d'entité améliorée basée sur des attributs agrégés |
| X.1303 *bis* | 01-03-2014 | Nouvelle | En vigueur | AAP | Protocole d'alerte commun (CAP 1.2) |
| X.1311 (2011) Cor.1 | 29-11-2014 |  | En vigueur | AAP | Technologies de l'information – Cadre de sécurité des réseaux de capteurs ubiquitaires – Corrigendum technique 1 |
| X.1314 | 13-11-2014 | Nouvelle | En vigueur | AAP | Exigences et cadre de sécurité applicables aux réseaux ubiquitaires |
| X.1314 Cor.1 | 29-10-2015 |  | En vigueur | AAP | Exigences et cadre de sécurité applicables aux réseaux ubiquitaires – Corrigendum 1 |
| X.1341 | 17-09-2015 | Nouvelle | En vigueur | TAP | Protocoles de transport de courrier certifié et de bureau de poste certifié |
| X.1500 Amd.3 | 26-04-2013 | Nouveau | Obsolète | Accord | Techniques d'échange d'informations sur la cybersécurité – Amendement 3 – Techniques structurées révisées d'échange d'informations sur la cybersécurité |
| X.1500 Amd.4 | 04-09-2013 | Nouveau | Obsolète | Accord | Techniques d'échange d'informations sur la cybersécurité – Amendement 4 – Techniques structurées révisées d'échange d'informations sur la cybersécurité |
| X.1500 Amd.5 | 24-01-2014 | Nouveau | Obsolète | Accord | Techniques d'échange d'informations sur la cybersécurité – Amendement 5 – Techniques structurées révisées d'échange d'informations sur la cybersécurité |
| X.1500 Amd.6 | 26-09-2014 | Nouveau | Obsolète | Accord | Techniques d'échange d'informations sur la cybersécurité – Amendement 6 – Techniques structurées révisées d'échange d'informations sur la cybersécurité |
| X.1500 Amd.7 | 17-04-2015 | Nouveau | Obsolète | Accord | Techniques d'échange d'informations sur la cybersécurité – Amendement 7 – Techniques structurées révisées d'échange d'informations sur la cybersécurité |
| X.1500 Amd.8 | 17-09-2015 | Nouveau | Obsolète | Accord | Techniques d'échange d'informations sur la cybersécurité – Amendement 8 – Techniques structurées révisées d'échange d'informations sur la cybersécurité |
| X.1500 Amd.9 | 23-03-2016 | Nouveau | Obsolète | Accord | Techniques d'échange d'informations sur la cybersécurité – Amendement 9 – Techniques structurées révisées d'échange d'informations sur la cybersécurité |
| X.1500 Amd.10 | 23-03-2016 | Nouveau | En vigueur | Accord | Techniques d'échange d'informations sur la cybersécurité – Amendement 10 – Techniques structurées révisées d'échange d'informations sur la cybersécurité |
| X.1520 | 24-01-2014 | Révisée | En vigueur | TAP | Vulnérabilités et expositions courantes |
| X.1521 | 23-03-2016 | Révisée | En vigueur | TAP | Système de notation des vulnérabilités courantes version 3.0 |
| X.1525 | 17-04-2015 | Nouvelle | En vigueur | TAP | Système commun de notation des failles |
| X.1526 | 26-04-2013 | Nouvelle | Obsolète | TAP | Langage ouvert d'évaluation des vulnérabilités |
| X.1526 | 24-01-2014 | Révisée | En vigueur | TAP | Langage pour la définition ouverte de vulnérabilités et pour l'évaluation de l'état d'un système |
| X.1542 | 07-09-2016 | Nouvelle | En vigueur | TAP | Format d'échange de messages sur les informations de session |
| X.1544 | 26-04-2013 | Nouvelle | En vigueur | TAP | Enumération et classification des schémas d'attaque courants |
| X.1546 | 24-01-2014 | Nouvelle | En vigueur | TAP | Enumération et caractérisation des attributs de logiciels malveillants |
| X.1582 | 24-01-2014 | Nouvelle | En vigueur | TAP | Protocoles de transport prenant en charge l'échange d'informations sur la cybersécurité |
| X.1601 | 24-01-2014 | Nouvelle | Obsolète | TAP | Cadre de sécurité applicable à l'informatique en nuage |
| X.1601 | 29-10-2015 | Révisée | En vigueur | AAP | Cadre de sécurité applicable à l'informatique en nuage |
| X.1602 | 23-03-2016 | Nouvelle | En vigueur | TAP | Exigences de sécurité pour l'environnement des applications de logiciel en tant que service |
| X.1631 | 15-07-2015 | Nouvelle | En vigueur | AAP | Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information fondés sur la norme ISO/CEI 27002 pour les services en nuage |
| X.1641 | 07-09-2016 | Nouvelle | En vigueur | AAP | Lignes directrices relatives à la sécurité des données des clients de services de nuage |
| X.1642 | 23-03-2016 | Nouvelle | En vigueur | TAP | Lignes directrices relatives à la sécurité opérationnelle de l'informatique en nuage |
| Z.100 | 29-04-2016 | Révisée | En vigueur | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 |
| Z.100 Annexe F1 | 13-01-2015 | Révisée | En vigueur | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Annexe F1 – Définition formelle du langage SDL-2010: Présentation générale |
| Z.100 Annexe F2 | 13-01-2015 | Révisée | En vigueur | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Annexe F2 – Définition formelle du langage SDL-2010: Sémantique statique |
| Z.100 Annexe F3 | 13-01-2015 | Révisée | En vigueur | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Annexe F3 – Définition formelle du langage SDL-2010: Sémantique dynamique |
| Z.101 | 29-04-2016 | Révisée | En vigueur | AAP | Langage de description et de spécification – Langage SDL-2010 de base |
| Z.102 | 29-04-2016 | Révisée | En vigueur | AAP | Langage de description et de spécification – Langage SDL-2010 complet |
| Z.103 | 29-04-2016 | Révisée | En vigueur | AAP | Langage de description et de spécification – Notation abrégée et annotation dans le langage SDL-2010 |
| Z.104 | 29-04-2016 | Révisée | En vigueur | AAP | Langage de description et de spécification – Caractéristiques du langage SDL-2010 pour les données et les actions |
| Z.105 | 29-04-2016 | Révisée | En vigueur | AAP | Langage de description et de spécification – Langage SDL-2010 combiné avec des modules ASN.1 |
| Z.106 | 29-04-2016 | Révisée | En vigueur | AAP | Langage de description et de spécification – Format d'échange commun pour le langage SDL-2010 |
| Z.107 | 29-04-2016 | Révisée | En vigueur | AAP | Langage de description et de spécification – Données orientées objet en SDL-2010 |
| Z.109 | 14-10-2013 | Révisée | Obsolète | AAP | Langage de description et de spécification – Profil du langage de modélisation unifié pour le SDL-2010 |
| Z.109 | 14-10-2016 | Révisée | En vigueur | AAP | Langage de description et de spécification – Profil du langage de modélisation unifié pour le SDL-2010 |
| Z.111 | 29-04-2016 | Révisée | En vigueur | AAP | Définition des langages de l'UIT-T: notations et lignes directrices |
| Z.161 | 14-07-2013 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): langage noyau |
| Z.161 | 13-11-2014 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): langage noyau |
| Z.161 | 29-10-2015 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): langage noyau |
| Z.161 | 14-10-2016 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): langage noyau |
| Z.161.1 | 13-11-2014 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage, prise en charge d'interfaces avec des signaux continus |
| Z.161.1 | 29-10-2015 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage, prise en charge d'interfaces avec des signaux continus |
| Z.161.2 | 13-11-2014 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: prise en charge de la configuration et du déploiement |
| Z.161.2 | 14-07-2013 | Nouvelle | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: prise en charge de la configuration et du déploiement |
| Z.161.2 | 29-10-2015 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: prise en charge de la configuration et du déploiement |
| Z.161.3 | 14-07-2013 | Nouvelle | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: paramétrage évolué |
| Z.161.3 | 13-11-2014 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: paramétrage évolué |
| Z.161.3 | 29-10-2015 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: paramétrage évolué |
| Z.161.4 | 14-07-2013 | Nouvelle | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: types de comportement |
| Z.161.4 | 29-10-2015 | Nouvelle | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: types de comportement |
| Z.161.5 | 13-11-2014 | Nouvelle | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: tests d'exécution et en temps réel |
| Z.161.5 | 29-10-2015 | Nouvelle | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: tests d'exécution et en temps réel |
| Z.164 | 14-10-2016 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): sémantique opérationnelle |
| Z.165 | 14-07-2013 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface d'exécution |
| Z.165 | 13-11-2014 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface d'exécution |
| Z.165 | 29-10-2015 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface d'exécution |
| Z.165.1 | 14-07-2013 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3: Extensions du langage TTCN-3: Interface d'exécution étendue |
| Z.165.1 | 13-11-2014 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3: Extensions du langage TTCN-3: Interface d'exécution étendue |
| Z.165.1 | 29-10-2015 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3: Extensions du langage TTCN-3: Interface d'exécution étendue |
| Z.166 | 14-07-2013 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface de commande |
| Z.166 | 13-11-2014 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface de commande |
| Z.166 | 29-10-2015 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface de commande |
| Z.166 | 14-10-2016 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface de commande |
| Z.167 | 14-07-2013 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): utilisation de la notation ASN.1 avec la notation TTCN-3 |
| Z.168 | 14-07-2013 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): mappage du langage CORBA IDL vers la notation TTCN-3 |
| Z.168 | 29-10-2015 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): mappage du langage CORBA IDL vers la notation TTCN-3 |
| Z.169 | 14-07-2013 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): Utilisation des schémas XML avec TTCN-3 |
| Z.169 | 29-10-2015 | Révisée | Obsolète | AAP | Notation de test et de commande de test version 3 (TTCN-3): Utilisation des schémas XML avec TTCN-3 |
| Z.169 | 14-10-2016 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): Utilisation des schémas XML avec TTCN-3 |
| Z.170 | 14-07-2013 | Révisée | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): spécification des commentaires de documentation TTCN-3 |

Tableau 8

Commission d'études 17 – Recommandations ayant fait l'objet d'un consentement/  
d'une détermination à la dernière réunion (et pas encore approuvées)

|  |  |  |  |
| --- | --- | --- | --- |
| **Recommandation** | **Consentement/ détermination** | **TAP/ AAP** | **Titre** |
| X.1058 (X.gpim) | 07-09-2016 | TAP | Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des informations d'identification personnelle |
| X.1080.0 (X.pbact) | 07-09-2016 | TAP | Contrôle d'accès pour la protection des données télébiométriques |
| X.1126 (X.msec-11) | 07-09-2016 | TAP | Lignes directrices relatives à l'atténuation des effets négatifs des terminaux infectés dans les réseaux mobiles |
| X.1212 (X.cogent) | 07-09-2016 | TAP | Considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité |
| X.1362 (X.iotsec-1) | 07-09-2016 | TAP | Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT) |
| X.1373 (X.itssec-1) | 07-09-2016 | TAP | Capacité de mise à jour sécurisée des logiciels pour les dispositifs de communication des systèmes de transport intelligents |
| X.1550 (X.nessa) | 07-09-2016 | TAP | Modèles de contrôle d'accès pour les réseaux d'échanges en cas d'incident |
| Z.100 Annexe F1 (révisée) | 07-09-2016 | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Annexe F1: Définition formelle du langage SDL: Présentation générale |
| Z.100 Annexe F2 (révisée) | 07-09-2016 | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Annexe F2: Définition formelle du langage SDL: Sémantique statique |
| Z.100 Annexe F3 (révisée) | 07-09-2016 | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Annexe F3: Définition formelle du langage SDL: Sémantique dynamique |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tableau 9

Commission d'études 17 – Recommandations supprimées pendant la période d'études

|  |  |  |  |
| --- | --- | --- | --- |
| **Recommandation** | **Dernière version** | **Date du retrait** | **Titre** |
| Z.400 | Mars 1993 | 24 décembre 2015 | Structure et format des manuels de qualité pour le logiciel de télécommunication |
| Z.600 | Novembre 2000 | 24 décembre 2015 | Architecture de l'environnement de traitement réparti |
| Z.601 | Février 2007 | 24 décembre 2015 | Architecture des données d'un système logiciel |

Tableau 10

Commission d'études 17 – Recommandations soumises à l'AMNT‑16

|  |  |  |  |
| --- | --- | --- | --- |
| **Recommandation** | **Proposition** | **Titre** | **Référence** |
| Néant |  |  |  |

Tableau 11

Commission d'études 17 – Suppléments

| Supplément | Approbation | Statut | Titre |
| --- | --- | --- | --- |
| X.Suppl.10 (09/2011) (révisé) | 24-01-2014 | En vigueur | UIT-T X.1205 – Supplément sur les possibilités d'utilisation du retraçage dans les réseaux |
| X.Suppl.18 | 26-04-2013 | En vigueur | UIT-T X.1205 – Supplément sur des lignes directrices pour la détection et la limitation du trafic anormal sur les réseaux de télécommunication IP |
| X.Suppl.19 | 26-04-2013 | En vigueur | Série UIT-T X.1120 – Supplément sur les aspects relatifs à la sécurité des smartphones |
| X.Suppl.20 | 26-04-2013 | En vigueur | UIT-T X.1205 – Supplément sur un cadre de négociation pour le partage d'informations de sécurité |
| X.Suppl.21 | 24-01-2014 | En vigueur | UIT-T X.1143 – Supplément sur le cadre de sécurité pour les services de mixage web |
| X.Suppl.22 | 24-01-2014 | En vigueur | UIT-T X.1144 – Supplément sur les améliorations et les nouvelles fonctionnalités offertes dans le langage de balisage extensible de contrôle d'accès (XACML 3.0) |
| X.Suppl.23 | 26-09-2014 | En vigueur | UIT-T X.1037 – Supplément sur des lignes directrices concernant la gestion de la sécurité dans le cadre de la mise en place d'un environnement IPv6 dans les organisations de télécommunication |
| X.Suppl.24 | 26-09-2014 | En vigueur | Série UIT-T X.1120-X.1139 – Supplément sur un cadre sécurisé de distribution des applications pour les dispositifs de communication |
| X.Suppl.25 | 23-03-2016 | En vigueur | UIT-T X.1231 – Supplément concernant des orientations pour faciliter la lutte contre le spam à l'intention des concepteurs de téléphones mobiles |
| X.Suppl.26 | 23-03-2016 | En vigueur | UIT-T X.1111 – Supplément sur l'architecture fonctionnelle de sécurité pour les services de réseau électrique intelligent utilisant les réseaux de télécommunication |
| X.Suppl.27 | 07-09-2016 | En vigueur | UIT‑T X.1054 – Supplément sur les bonnes pratiques pour la mise en oeuvre de la Recommandation UIT-T X.1054 | ISO /CEI 27014 sur la gouvernance de la sécurité de l'information – Le cas du Burkina Faso |
| X.Suppl.28 | 07-09-2016 | En vigueur | UIT-T X.1245 – Supplément sur des mesures techniques et des mécanismes de lutte contre l'usurpation de numéro dans le réseau de terminaison du service VoLTE |
| Z.Sup1 (révisé) | 17-04-2015 | En vigueur | Série UIT-T Z.100 – Supplément sur la méthodologie d'utilisation des techniques de description |

Tableau 12

Commission d'études 17 – Publications non normatives   
(manuels, etc.) approuvées

| Publication | Approbation | Statut | Titre |
| --- | --- | --- | --- |
| Rapport technique | 26-09-2014 | Publié | Enjeux existants et nouveaux de la normalisation de l'infrastructure de clé publique |
| Rapport technique | 17-09-2015 | Publié | Sécurité dans les télécommunications et technologies de l'information: Aperçu des problèmes et présentation des Recommandations UIT-T existantes sur la sécurité dans les télécommunications; 6ème édition |
| Rapport technique | 07-09-2016 | Publié | Utilisation efficace des normes de sécurité |

Tableau 13

Commission d'études 17 – Recommandations ayant fait l'objet d'une détermination/  
d'un consentement puis ayant été rejetées

| Recommandation | | Consentement/ détermination | TAP/ AAP | Titre |
| --- | --- | --- | --- | --- |
| Projet de Recommandation UIT‑T X.1126 (ex-X.msec-6)  (Note 1) | | Avril 2013 | TAP | Aspects relatifs à la sécurité des smartphones |
| Projet de Recommandation UIT-T X.894 (ex X.cms)  (Note 2) | | 23-03-2016 | AAP | Technologies de l'information – Applications génériques de l'ASN.1 – Syntaxe de message cryptographique |
| NOTE 1 – La CE 17 a cessé (avril 2013) ses activités de normalisation concernant la Recommandation UIT‑T X.1126 (ex‑X.msec-6), qui est devenue le Supplément X.Suppl.19.  NOTE 2 – Le 15 septembre 2016, faute d'approbation, il a été décidé, après le dernier appel, de transférer le projet de Recommandation UIT-T X.894 (X.cms) à la réunion suivante de la CE 17; un nouveau sujet d'étude X.CMS-prof est en cours de mise au point. | | | |

ANNEXE 2

Proposition de mises à jour du mandat de la Commission d'études 17   
et des rôles de Commission d'études directrice   
(Résolution 2 de l'AMNT)

On trouvera ci-après les propositions de modification du mandat de la Commission d'études 17 et des rôles de Commission d'études directrice, convenues lors de la dernière réunion de la Commission d'études 17 de la période d'études, sur la base des parties pertinentes de la [Résolution 2 de l'AMNT‑12](http://www.itu.int/en/ITU-T/wtsa16/Documents/CPI/ITU-T_Res2_2016-F.DOCX).

PARTIE 1 – Domaines d'étude généraux

**…**

**Commission d'études 17 de l'UIT-T  
Sécurité**

La Commission d'études 17 de l'UIT-T est chargée de renforcer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC). Elle est notamment chargée de mener des études se rapportant à la cybersécurité, la gestion de la sécurité, la lutte contre le spam et la gestion d'identité. Elle est également chargée d'étudier l'architecture et le cadre général de la sécurité, la protection des informations d'identification personnelle et la sécurité des applications et des services pour l'Internet des objets (IoT), les réseaux électriques intelligents, les smartphones, les réseaux pilotés par logiciel (SDN), la télévision utilisant le protocole Internet (TVIP), les services web, les réseaux sociaux, l'informatique en nuage, l'analyse des mégadonnées, les services financiers sur mobile et la télébiométrie. La Commission d'études 17 est également responsable de l'application des communications entre systèmes ouverts, y compris l'annuaire et les identificateurs d'objet, des langages techniques, de leur méthode d'utilisation et d'autres problèmes connexes liés aux aspects logiciels des systèmes de télécommunication, ainsi que des tests de conformité en vue d'améliorer la qualité des Recommandations.

**…**

PARTIE 2 – Commissions d'études directrices de l'UIT-T selon les domaines d'étude

**…**

CE 17 Commission d'études directrice pour la sécurité  
Commission d'études directrice pour la gestion d'identité (IdM)  
Commission d'études directrice pour les langages et les techniques de description

**…**

**Annexe B**(de la Résolution 2) **Points de repère à l'intention des Commissions d'études pour la mise au point   
du programme de travail postérieur à 2016**

**…**

**Commission d'études 17 de l'UIT-T**

La Commission d'études 17 de l'UIT-T est chargée de renforcer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC). Elle est notamment chargée de mener des études relatives à la sécurité, y compris la cybersécurité, la lutte contre le spam et la gestion d'identité. Elle est également chargée d'étudier l'architecture et le cadre général de la sécurité, la gestion de la sécurité, la protection des informations d'identification personnelle (PII) et la sécurité des applications et des services pour l'Internet des objets (IoT), les réseaux électriques intelligents, les smartphones, les réseaux pilotés par logiciel (SDN), la télévision utilisant le protocole Internet (TVIP), les services web, les réseaux sociaux, l'informatique en nuage, les services financiers sur mobile et la télébiométrie. La Commission d'études 17 est également responsable de l'application des communications entre systèmes ouverts, y compris l'annuaire et les identificateurs d'objet, des langages techniques, de leur méthode d'utilisation et des autres problèmes connexes liées aux aspects logiciels des systèmes de télécommunication, ainsi que des tests de conformité en vue d'améliorer la qualité des Recommandations.

Dans le domaine de la sécurité, la Commission d'études 17 est responsable de l'élaboration des principales Recommandations sur la sécurité des TIC, telles que l'architecture et les cadres généraux de la sécurité; les aspects essentiels de la cybersécurité, y compris les menaces, les vulnérabilités et les risques, le traitement des incidents, l'intervention en cas d'incident et l'expertise numérique; la gestion de la sécurité, y compris la gestion des informations d'identification personnelle (PII); et la lutte contre le spam par des moyens techniques. En outre, cette commission assure la coordination générale des travaux menés par l'UIT-T dans le domaine de la sécurité.

En outre, la Commission d'études 17 est responsable de l'élaboration des principales Recommandations sur les aspects relatifs à la sécurité des applications et des services liés à la TVIP, aux réseaux électriques intelligents, à l'Internet des objets, aux réseaux pilotés par logiciel (SDN), aux réseaux sociaux, à l'informatique en nuage, à l'analyse des mégadonnées, aux smartphones, aux services financiers sur mobile et à la télébiométrie.

La Commission d'études 17 est également chargée d'élaborer les principales Recommandations relatives à un modèle générique de gestion d'identité, indépendant des technologies de réseau et permettant l'échange sécurisé d'informations d'identité entre des entités. Il s'agira aussi d'étudier le processus de découverte des sources d'informations d'identité qui font autorité, les mécanismes génériques pour l'interopérabilité de divers formats d'informations d'identité, les menaces liées à la gestion d'identité, les mécanismes de lutte contre ces menaces et la protection des informations d'identification personnelle (PII) et d'élaborer des mécanismes garantissant que l'accès aux informations PII n'est autorisé que lorsque cet accès est approprié.

En ce qui concerne les communications entre systèmes ouverts, la Commission d'études 17 est responsable des Recommandations dans les domaines suivants:

• services et systèmes d'annuaire, y compris l'infrastructure de clé publique (PKI) (Recommandations UIT-T des séries F.500 et X.500);

• identificateurs d'objet (OID) et autorités d'enregistrement associées (Recommandations UIT-T des séries X.660 et X.670);

• interconnexion des systèmes ouverts (OSI), y compris la notation de syntaxe abstraite numéro un (ASN.1) (Recommandations UIT-T des séries F.400, X.200, X.400, X.600 et X.800);

• traitement réparti ouvert (ODP) (Recommandations UIT-T de la série X.900).

Dans le domaine des langages, la Commission d'études 17 est responsable des études relatives aux techniques de modélisation, de spécification et de description. Ces travaux, qui portent sur différents langages (ASN.1, SDL, MSC et URN), seront menés en fonction des besoins des commissions d'études concernées (Commissions d'études 2, 9, 11, 13, 15 et 16) et en collaboration avec elles.

**…**

**Annexe C**(de la Résolution 2) **Liste des Recommandations relevant de la compétence des  
différentes commissions d'études et du GCNT au cours  
de la période d'études 2013-2016**

**…**

**Commission d'études 17 de l'UIT-T**

Recommandations UIT-T E.104, E.115, E.409 (conjointement avec la Commission d'études 2)

Recommandations UIT-T de la série F.400; F.500-F.549

Recommandations UIT-T de la série X, à l'exception des Recommandations UIT-T relevant de la responsabilité des Commissions d'études 2, 11, 13, 15 et 16

Recommandations UIT-T de la série Z, à l'exception des Recommandations UIT-T de la série Z.300 et de la série Z.500

NOTE 1 – Les changements dans l'attribution des Recommandations de la série Z ont été décidés par le GCNT après l'AMNT-12.

**…**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_