|  |  |
| --- | --- |
| **Assemblée mondiale de normalisation des télécommunications (AMNT-20)Genève, 1er-9 mars 2022** |  |
|  |  |
|  |  |
| **SÉANCE PLÉNIÈRE** | Document 19-F |
|  | **Décembre 2021** |
|  | **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-20), PARTie I: ConsidÉrations gÉnÉrales |
|  |

|  |  |
| --- | --- |
| **Résumé:** | On trouvera dans la présente contribution le rapport de la Commission d'études 17 de l'UIT-T à l'AMNT-20 concernant les activités de cette commission pendant la période d'études 2017-2021. |
| **Contact:** | Heung Youl YoumPrésident de la CE 17 de l'UIT-TCorée (République de) | Courriel: hyyoum@sch.ac.kr |

**Note du TSB:**

Le rapport de la Commission d'études 17 à l'AMNT‑20 est présenté dans les documents suivants:

Partie I: **Document 19** **–** Considérations générales

Partie II: **Document 20 –** Questions qu'il est proposé d'étudier pendant la période d'études 2022‑2024

Table des matières

**Page**

[1 Introduction 4](#_Toc94524434)

[1.1 Domaine de compétence de la Commission d'études 17 4](#_Toc94524435)

[1.2 Équipe de direction et réunions de la Commission d'études 17 6](#_Toc94524436)

[2 Organisation des travaux 12](#_Toc94524437)

[2.1 Organisation des études et répartition des travaux 12](#_Toc94524438)

[2.2 Questions et Rapporteurs 14](#_Toc94524439)

[3 Résultats des travaux effectués pendant la période d'études 2017-2020 21](#_Toc94524440)

[3.1 Généralités 21](#_Toc94524441)

[3.2 Principaux résultats obtenus 22](#_Toc94524442)

[a) Question 1/17: Coordination en matière de sécurité des télécommunications/TIC
(2017-2020)/Stratégie et coordination en matière de normalisation de la sécurité (2021-) 22](#_Toc94524443)

[b) Question 2/17: Architecture et cadre de sécurité (2017-2020)/Architecture de sécurité et sécurité des réseaux (2021-) 23](#_Toc94524444)

[c) Question 3/17: Gestion de la sécurité des informations de télécommunication 2017‑2020)/Gestion de la sécurité des informations de télécommunication et services de sécurité (2021-) 24](#_Toc94524445)

[d) Question 4/17: Cybersécurité (2017-2020)/Cybersécurité et lutte contre le spam (2021-) 26](#_Toc94524446)

[e) Question 5/17: Lutte contre le spam par des moyens techniques (2017-2020) 29](#_Toc94524447)

[f) Question 6/17: Aspects relatifs à la sécurité des services et des réseaux de télécommunication et de l'Internet des objets (2017-2020)/Sécurité des services de télécommunication et de l'Internet des objets (2021-) 30](#_Toc94524448)

[g) Question 7/17: Services applicatifs sécurisés 33](#_Toc94524449)

[h) Question 8/17: Sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées 34](#_Toc94524450)

[i) Question 9/17: Télébiométrie (2017-2020) 36](#_Toc94524451)

[j) Question 10/17: Architecture et mécanismes de gestion d'identité (2017‑2020)/Architecture et mécanismes de gestion des identités et de télébiométrie (2021-) 37](#_Toc94524452)

[k) Question 11/17: Technologies génériques (Annuaire, infrastructure de clé publique (PKI), infrastructure de gestion des privilèges (PMI), notation de syntaxe abstraite numéro un (ASN.1), identificateurs d'objet (OID)) utilisées pour les applications sécurisées (2017-2020)/Technologies génériques (Annuaire, infrastructure de clé publique (PKI), langages formels et identificateurs d'objets par exemple) utilisées pour les applications sécurisées (2021-) 38](#_Toc94524453)

[l) Question 12/17: Langages formels pour les logiciels de télécommunication et les tests (2017-2020) 44](#_Toc94524454)

**Page**

[m) Question 13/17: Aspects sécurité des systèmes de transport intelligents (2017‑2020)/Sécurité des systèmes de transport intelligents (ITS) (2021-) 49](#_Toc94524455)

[n) Question 14/17: Aspects sécurité des technologies de registres distribués (2018‑2020)/Sécurité de la technologie des registres distribués (DLT) (2021-) 51](#_Toc94524456)

[o) Question 15/17: Sécurité relative aux nouvelles technologies, y compris la sécurité quantique 52](#_Toc94524457)

[3.3 Activités de la Commission d'études 17 en tant que commission d'études directrice, GSI, JCA, groupes régionaux et projets 53](#_Toc94524458)

[3.3.1 Activités de la Commission d'études 17 en tant que commission d'études directrice pour la sécurité 53](#_Toc94524459)

[3.3.2 Activités de la Commission d'études 17 en tant que commission d'études directrice pour la gestion d'identité 57](#_Toc94524461)

[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 58](#_Toc94524463)

[3.3.4 Activité conjointe de coordination sur la gestion d'identité (JCA-IdM) 59](#_Toc94524464)

[3.3.5 Groupe régional de la Commission d'études 17
pour l'Afrique (SG17 RG-AFR) 59](#_Toc94524465)

[3.3.6 Groupe régional de la Commission d'études 17 pour les États arabes (SG17 RG‑ARB) 60](#_Toc94524466)

[3.4 Projets 60](#_Toc94524467)

[3.4.1 Projet ASN.1 60](#_Toc94524468)

[3.4.2 Projet OID 60](#_Toc94524469)

[3.5 Réduire l'écart en matière de normalisation 61](#_Toc94524470)

[4 Observations concernant les travaux futurs 61](#_Toc94524471)

[5 Mises à jour de la Résolution 2 de l'AMNT pour la période d'études 2022-2024 63](#_Toc94524472)

[ANNEXE 1](#_Toc94524473) – [Liste des Recommandations, Suppléments et autres documents établis ou supprimés pendant la période d'études 64](#_Toc94524474)

[ANNEXE 2 – Propositions de révision de la Résolution 2 de l'AMNT
par la Commission d'études 17 82](#_Toc94524475)

# 1 Introduction

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

L'Assemblée mondiale de normalisation des télécommunications (Hammamet, 2016) a chargé la Commission d'études 17 d'étudier 12 Questions en vue de renforcer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC).

Conformément à l'Annexe A de la Résolution 2 de l'AMNT‑16, 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, 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 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 qu'aux langages de spécification de test à l'appui des tests de conformité en vue d'améliorer la qualité des Recommandations.*

Conformément à l'Annexe A de la Résolution 2 de l'AMNT‑16, la Commission d'études 17 (Sécurité) est la commission d'études directrice pour les domaines suivants:

*– 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‑16, les points de repère définis pour la CE 17 sont les suivants:

 *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, 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 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, des réseaux électriques intelligents, de l'Internet des objets, des réseaux pilotés par logiciel (SDN), des réseaux sociaux, de l'informatique en nuage, de l'analyse des mégadonnées, des téléphones intelligents, des services bancaires sur mobile et de 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, qui portent sur différents langages (ASN.1, SDL, MSC, URN et TTCN-3).*

 *Ces travaux seront menés en fonction des besoins des commissions d'études concernées (Commissions d'études 2, 9, 11, 13, 15, 16 et Commission d'études 20 pour les questions relatives à la sécurité de l'IoT et des villes et des communautés intelligentes) et en collaboration avec elles.*

 *La Commission d'études 17 étudiera les aspects pertinents de la gestion d'identité en collaboration avec la Commission d'études 20 pour l'IoT et avec la Commission d'études 2, conformément au mandat de chaque commission d'études.*

Conformément à l'Annexe C de la Résolution 2 de l'AMNT-16 (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 2017-2020 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 Équipe de direction et réunions de la Commission d'études 17

L'AMNT-16 a désigné M. YOUM Heung Youl (Corée, République de) en tant que Président de la Commission d'études 17 et a désigné les neuf Vice-Présidents ci-après: M. DOLMATOV Vasiliy (Fédération de Russie), M. ISHAG Muataz Elsadig (Soudan), M. EVREN Gökhan (Turquie), Mme FUREY Inette (états-Unis d'Amérique), Mme LATROUS Wala Turki (Tunisie), M. LIN Zhaoji (Chine), M. MIGUEL Hugo Darío (Argentine), M. MIYAKE Yutaka (Japon) et M. KETTIN ZANGA Patrick-Kennedy (République centrafricaine). M. KETTIN ZANGA Patrick‑Kennedy n'a participé à aucune réunion de la Commission d'études 17 au cours de cette période d'études.

En mars 2018, Mme FUREY Inette (états-Unis d'Amérique) a été remplacée par M. GONZALES Juan (états-Unis d'Amérique) à la vice-présidence de la Commission d'études 17. En mars 2020, M. MIGUEL Hugo Darío (Argentine) a été remplacé par Mme MOLINARI Lia (Argentine) à la vice-présidence de la Commission d'études 17. En août 2020, M. KETTIN ZANGA Patrick‑Kennedy (République centrafricaine) a été remplacé par M. MBATHAS Eric Anicet (République centrafricaine) à la vice-présidence de la Commission d'études 17.

La Commission d'études 17 s'est réunie à treize reprises en plénière 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 |
| --- | --- | --- |
| CE/GT 17 | Genève, 22-30 mars 2017 | CE 17-R1 à R9 |
| CE/GT 17 | Genève, 29 août – 6 septembre 2017 | CE 17-R10 à R17 |
| CE/GT 17 | Genève, 20-29 mars 2018 | CE 17-R18 à R24 |
| CE/GT 17 | Genève, 29 août – 7 septembre 2018 | CE 17-R25 à R32 |
| CE/GT 17 | Genève, 22-30 janvier 2019 | CE 17-R33 à R37 |
| CE/GT 17 | Genève, 27 août – 5 septembre 2019 | CE 17-R38 à R50 |
| CE/GT 17 | Virtuelle, 17-26 mars 2020 | CE 17-R51 à R66 |
| CE 17 | Virtuelle, 29 mai 2020 | CE 17-R67 |
| CE/GT 17 | Virtuelle, 24 août – 3 septembre 2020 | CE 17-R68 à R77 |
| CE 17 | Virtuelle, 7 janvier 2021 | CE 17-R78 |
| CE/GT 17 | Virtuelle, 20-30 avril 2021 | CE 17-R79 à R85 |
| CE/GT 17 | Virtuelle, 24 août – 3 septembre 2020 | CE 17-R86 à R102 |
| CE 17 | Virtuelle, 7 janvier 2022 | CE 17-R103 |

Des réunions de l'équipe de direction se sont tenues parallèlement à chaque réunion de la Commissions d'études 17.

De plus, un grand nombre de réunions de Groupes du 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 des Groupes du Rapporteur organisées dans le cadre de la Commission d'études 17
pendant la période d'études

| Dates | Place | Question(s) | Titre de l'événement |
| --- | --- | --- | --- |
| 12-12-2016-13-12-2016 | Chine [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5710&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0057)] | Réunion du Groupe du Rapporteur pendant la période intérimaire pour la Question 8/17  |
| 12-01-2017-13-01-2017 | Réunion électronique | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5711&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0054)] | Réunion électronique du Groupe du Rapporteur pendant la période intérimaire pour la Question 4/17 |
| 06-02-2017-10-02-2017 | Tunisie [Tunis] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5716&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0058)] | Réunion mixte des Groupes du Rapporteur pour la Question 11/17 conjointement avec l'ISO/CEI JTC 1/SC 6/WG10 |
| 08-02-2017-09-02-2017 | Corée (République de) [Séoul] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5712&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0053)] | Réunion du Groupe du Rapporteur pendant la période intérimaire pour la Question 3/17 |
| 08-02-2017-09-02-2017 | Corée (République de) [Séoul] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5713&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0056)] | Réunion du Groupe du Rapporteur pendant la période intérimaire pour la Question 6/17 |
| 22-06-2017-23-06-2017 | Corée (République de) [Séoul] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6903&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0392)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 22-06-2017-23-06-2017 | Corée (République de) [Séoul] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6904&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0393)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 27-06-2017-28-06-2017 | Chine [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6909&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0394)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 29-06-2017 | Japon [Tokyo] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6916&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0395)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 30-06-2017 | Japon [Tokyo] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6905&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)][Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6906&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)][Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6907&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)] | Réunion mixte des Groupes du Rapporteur pour les Questions 3/17 et 4/17 et 10/17 sur les services DFS |
| 03-07-2017 | Japon [Tokyo] | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=7916&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0396)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 14-07-2017 | Corée (République de) [Séoul] | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=8918&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0397)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 13/17 |
| 30-10-2017-03-11-2017 | Corée (République de) | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9047&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817)] | Réunion mixte sur la Question 11/17 conjointement avec l'ISO/CEI JTC1/SC6 |
| 30-11-2017-01-12-2017 | Corée (République de)[**Bundang]** | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9048&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817)] | Réunion du Groupe du Rapporteur pour la Question 14/17 |
| 13-12-2017-14-12-2017 | Chine [Beijing] | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9050&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0822)] | Réunion du Groupe du Rapporteur pour la Question 7/17 |
| 09-01-2018 | Canada [Vancouver] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9051&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0821)][Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9052&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-1006)] | Réunion mixte sur les Questions 4/17 et 10/17  |
| 22-01-2018-23-01-2018 | Chine [Beijing] | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9057&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0823)] | Réunion du Groupe du Rapporteur pour la Question 14/17 |
| 24-01-2018-25-01-2018 | Corée (République de) [Séoul] | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9056&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0818)] | Réunion du Groupe du Rapporteur pour la Question 13/17 |
| 25-01-2018-26-01-2018 | Corée (République de) [Séoul] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9054&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0820)] | Réunion du Groupe du Rapporteur pour la Question 3/17 |
| 25-01-2018-26-01-2018 | Corée (République de) [Séoul] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9055&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0819)] | Réunion du Groupe du Rapporteur pour la Question 6/17 |
| 04-06-2018-06-06-2018 | Chine [Beijing] | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9265&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1252)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 14/17 |
| 07-06-2018-08-06-2018 | Corée (République de) [Séoul] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9261&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1246)][Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9262&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1251)] | Réunions intérimaires du Groupe du Rapporteur pour les Questions 6/17 et 13/17 |
| 20-06-2018-21-06-2018 | Chine [Yinchuan] | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9259&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1247)] | Réunion du Groupe du Rapporteur pour la Question 7/17 |
| 26-06-2018-27-06-2018 | états-Unis [Seattle, Washington] | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9264&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1249)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 27-06-2018-28-06-2018 | Chine [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9263&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1248)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 27-08-2018-31-08-2018 | Japon [Tokyo] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9260&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1250)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 conjointement avec l'ISO/CEI JTC 1/SC 6/WG 10 |
| 08-11-2018- 09-11-2018 | Singapour | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9405&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1727)] | Réunions intérimaires du Groupe du Rapporteur pour la Question 13/17 |
| 12-11-2018- 13-11-2018 | Japon [Tokyo] | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9406&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726)] | Réunions intérimaires du Groupe du Rapporteur pour la Question 10/17 |
| 12-11-2018- 13-11-2018 | Japon [Tokyo] | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9407&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726)] | Réunions intérimaires du Groupe du Rapporteur pour la Question 14/17 |
| 22-04-2019- 26-04-2019 | Chine [Beijing] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9560&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2057)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 conjointement avec l'ISO/CEI JTC 1/SC 6/WG 10 |
| 04-06-2019- 05-06-2019 | Réunion électronique | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9559&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2056)] | Réunion électronique intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 04-06-2019- 05-06-2019 | Réunion électronique | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9563&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2059)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 14/17 |
| 10-06-2019- 12-06-2019 | Chine [Shanghai] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9574&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2051)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 11-06-2019- 12-06-2019 | Chine [Beijing] | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9561&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2058)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 13/17 |
| 18-06-2019- 19-06-2019 | Chine [Chongqing] | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9556&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2053)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 7/17 |
| 24-06-2019- 25-06-2019 | Chine [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9557&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2054)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 27-06-2019- 28-06-2019 | Japon [Tokyo] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9555&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2052)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 27-06-2019 | Réunion électronique | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9554&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2050)] | Réunion électroniqueintérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 22-10-2019- 23-10-2019 | Chine[Haikou] | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9763&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2564)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 7/17 |
| 05-12-2019- 06-12-2019 | Suisse [**Fribourg**] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9767&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762)][Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9768&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762)] | Réunion conjointe des responsables de l'étude des Questions 11/17 et 14/17 |
| 11-12-2019- 13-12-2019 | Chine[Jinan] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9882&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2562)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 11-12-2019 | Réunion électronique | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9766&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2567)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 |
| 11-12-2019 | Chine[Jinan] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9760&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2754)] | Réunions en parallèle des Groupes du Rapporteur pour les Questions 4/17 et 16/13 |
| 12-12-2019 | Japon[Tokyo] | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9765&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2566)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 13-12-2019 | Japon[Tokyo] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9759&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2561)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 07-01-2020- 08-01-2020 | Chine [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9764&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2565)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 07-01-2020- 08-01-2020 | Japon [Fukuoka] | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9769&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2569)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 13/17 |
| 08-01-2020 | Réunion électronique | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9771&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2570)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 14/17 |
| 13-01-2020- 14-01-2020 | Malaisie [Kuala Lumpur] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9783&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2563)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 03-02-2020- 07-02-2020 | Royaume-Uni [Londres] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9770&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2568)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 conjointement avec l'ISO/CEI JTC 1/SC 6/WG 10 |
| 17-04-2020 | Réunion électronique | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10081&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2963)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 22-04-2020 | Réunion électronique | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10087&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2966)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 |
| 11-05-2020- 12-05-2020 | Réunion électronique | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10083&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3093)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 13-05-2020 | Réunion électronique | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10088&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2979)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 13/17 |
| 02-06-2020- 03-06-2020 | Réunion électronique | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10080&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3090)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 10-06-2020- 11-06-2020 | Réunion électronique | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10089&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3096)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 13/17 |
| 19-06-2020 | Réunion électronique | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10347&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3091)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 22-06-2020- 23-06-2020 | Réunion électronique | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10090&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3097)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 14/17 |
| 13-07-2020 | Réunion électronique | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10086&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3095)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 16-07-2020- 17-07-2020 | Réunion électronique | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10084&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3094)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 19-10-2020- 30-10-2020 | Réunion électronique | [Q11/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11694&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3447)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 11/17 conjointement avec l'ISO/CEI JTC 1/SC 6/WG 10 |
| 18-11-2020 | Réunion électronique | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10081&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3462)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 25-11-2020 -26-11-2020 | Réunion électronique | [Q13/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11694&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3467)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 13/17 |
| 26-11-2020- 27-11-2020 | Réunion électronique | [Q4/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11570&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3460)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 07-12-2020-08-12-2020 | Réunion électronique | [Q2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11569&Group=17) [ [rapport de la réunion](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3459)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 2/17 |
| 09-12-2020- 10-12-2020 | Réunion électronique | [Q3/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11727&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3468)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 21-12-2020- 22-12-2020 | Réunion électronique | [Q6/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11571&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3463)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 04-01-2021- 05-01-2021 | Réunion électronique | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10084&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3469)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 14/17 |
| 01-02-2021-02-02-2021 | Réunion électronique | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10086&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210420-TD-PLEN-3547)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 01-02-2021-02-02-2021 | Réunion électronique | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11830&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3548)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 04-02-2021 | Réunion électronique | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11836&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3549)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 17-06-2021-18-06-2021 | Réunion électronique | [Q15/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12574&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3876)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 15/17 |
| 17-06-2021-18-06-2021 | Réunion électronique | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12539&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3875)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 8/17 |
| 24-06-202125-06-2021 | Réunion électronique | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12534&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3877)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 4/17 |
| 24-06-2021 | Réunion électronique | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12575&Group=17) [[rapport de la réunion](http://www.itu.int/md/T17-SG17-210824-TD-PLEN-3878)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 28-06-202129-06-2021 | Réunion électronique | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12592&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3879)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 14/17 |
| 01-07-202102-07-2021 | Réunion électronique | [Q2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12533&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3880)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 2/17 |
| 05-10-2021 | Réunion électronique | [Q3/17 [rapport de la réunion]](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4199/en) | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 19-11-2021 | Réunion électronique | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12744&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4178)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 24-11-202125-11-2021 | Réunion électronique | [Q2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12733&Group=17) [[rapport de la réunion](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4159)] | Réunion intérimaire du Groupe du Rapporteur pour la Question 2/17 |
| 20-01-202221-01-2022 | Réunion électronique | Q15/17 [rapport de la réunion] | Réunion intérimaire du Groupe du Rapporteur pour la Question 15/17 |
| 07-02-2022 | Réunion électronique | Q3/17 [rapport de la réunion] | Réunion intérimaire du Groupe du Rapporteur pour la Question 3/17 |
| 15-02-2022 | Réunion électronique | Q10/17 [rapport de la réunion] | Réunion intérimaire du Groupe du Rapporteur pour la Question 10/17 |
| 17-02-2022 | Réunion électronique | Q6/17 [rapport de la réunion] | Réunion intérimaire du Groupe du Rapporteur pour la Question 6/17 |
| 23-02-202224-02-2022 | Réunion électronique | Q2/17 [rapport de la réunion] | Réunion intérimaire du Groupe du Rapporteur pour la Question 2/17 |
| ??-02-2022 | Réunion électronique | Q4/17 [rapport de la réunion] | 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 quatre groupes de travail. Le Tableau 2 donne le numéro et le nom de chaque Groupe de travail, ainsi que les Questions qui lui ont été confiées et le nom de ses Président et Vice-Présidents entre 2017 et 2020.

TABLEau 2

Organisation de la Commission d'études 17 (2017-2020)

| Désignation | Questions à étudier | Nom du Groupe de travail | Présidentet Vice-Présidents |
| --- | --- | --- | --- |
| PLEN | Q1/17 |  |  |
| GT 1/17 | Q2/17; Q3/17; Q6/17; Q13/17 (7); | Sécurité des télécommunications/TIC | M. Miyake Yutaka (Président)M. Dolmatov Vasiliy (Vice‑Président)M. Evren Gökhan (Vice‑Président) |
| GT 2/17 | Q4/17; Q5/17; Q14/17 (8); | Sécurité du cyberespace | M. Nakao Koji (Président)Mme Furey Inette (Vice‑Présidente) (1) M. Gonzalez Juan (Vice‑Président) (2) |
| GT 3/17 | Q7/17; Q8/17; Q12/17; | Sécurité des applications | M. Taddei Arnaud (Président)M. Lin Zhaoji (Vice‑Président) (3)Mme Bai Xiaoyuan (Vice‑Présidente) (4) |
| GT 4/17 | Q9/17; Q10/17; Q11/17; | Gestion d'identité et d'authentification | M. Li Kepeng (Président) (5)M. Nah Jae Hoon (Vice‑Président/Coprésident) (5, 6)M. Lin Zhaoji (Coprésident) (6) |

Notes:

(1) Vice-Présidente jusqu'en septembre 2017.

(2) Vice-Président depuis mars 2018.

(3) Vice-Président jusqu'en septembre 2018.

(4) Vice-Présidente depuis janvier 2019.

(5) Président/Vice-Président jusqu'en septembre 2018.

(6) Coprésident depuis janvier 2019.

(7) La Question 13/17 a été établie par le CE 17 en septembre 2017.

(8) La Question 14/17 a été établie par le CE 17 en mars 2018.

**2.1.2** En raison de la pandémie mondiale de COVID-19, l'Assemblée mondiale de normalisation des télécommunications (AMNT-20), qui devait se tenir en 2020, a été reportée à 2022 et la période d'études 2017-2020 a été prolongée en conséquence pour tenir compte des nouvelles dates de l'AMNT-20. Lors de sa réunion tenue en août/septembre 2020, la CE 17 est convenue de soumettre une série de 12 Questions à l'AMNT-20 pour approbation (voir le paragraphe 2.2.) et d'établir un groupe spécial chargé des travaux préparatoires en vue de la prochaine période d'études.

Compte tenu du report de l'AMNT-20 à mars 2022, le GCNT, à sa réunion tenue du 11 au 18 janvier 2021, a approuvé cette nouvelle série de Questions de la CE 17 (voir la [Circulaire 295 du TSB](https://www.itu.int/md/T17-TSB-CIR-0295/en)). À sa réunion tenue du 20 au 30 avril 2021, la CE 17 a décidé d'adopter une nouvelle structure pour la série de 12 Questions, et en a confié l'étude à cinq groupes de travail.

Le Tableau 3 indique le numéro et le nom de chaque groupe de travail, ainsi que les Questions qui lui ont été confiées et le nom de son Président, à compter de 2021.

TABLEAU 3

Organisation de la Commission d'études 17 (2021-)

| Désignation | Questions à étudier | Nom du Groupe de travail | Président et Vice-Présidents |
| --- | --- | --- | --- |
| GT 1/17 | Q1/17; Q15/17 | Stratégie et coordination en matière de sécurité | Président:  M. Dolmatov Vasily (Russie)Vice-Président:  M. Kim Jonghyun (Corée)  |
| GT 2/17 | Q2/17; Q6/17; Q13/17; | Sécurité de la 5G, de l'Internet des objets (IoT) et des systèmes de transport intelligents (ITS) | Président:  M. Miyake Yutaka (KDDI)Vice-Présidente:  Mme Hu Zhiyuan (Nokia Shanghai Bell) M. Mills Philip (Royaume-Uni)  |
| GT 3/17 | Q3/17; Q4/17;  | Cybersécurité et gestion | Président:  M. Nakao Koji (NICT)Vice-Présidente:  Mme Molinari Lia (Argentine) |
| GT 4/17 | Q7/17; Q8/17; Q14/17 | Sécurité des services et applications | Président:  M. Nah Jae Hoon (ETRI)Vice-Présidente:  Mme Bai Xiaoyuan (Alibaba)  |
| GT 5/17 | Q10/17; Q11/17 | Technologies de sécurité fondamentales  | Président:  M. Lin Zhaoji (ZTE)Vice-Président:  *poste vacant* |

**2.1.3** Le Tableau 4 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-16, lors de sa réunion de mars 2017, le Groupe régional de la CE 17 pour la région des États arabes a été créé; voir le § 3.3.5.

**2.1.5** 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.

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

L'Activité conjointe de coordination sur la protection en ligne des enfants (JCA-COP), qui a poursuivi ses activités menées pendant la période d'études précédente, a été mise en sommeil lors de la première réunion de la CE 17 tenue en mars 2017.

**2.1.6** Pendant la période d'études, la Commission d'études 17 a poursuivi la mise en œuvre de 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 4

Autres groupes (le cas échéant)

| Nom du Groupe | Président | Vice-Présidents |
| --- | --- | --- |
| JCA-IdM | Coprésidents: M. Barbir Abbie (1), M. Park Keundug (1), M. Takechi Hiroshi (1), M. Youm Heung Youl (8) |  |
| JCA-COP | Sans objet |  |
| SG17 RG-AFR | M. Katundu Michael (2)Mme Njiraini Mwende (3) | M. Elhaj Mohamed (2),M. Mwesigwa Patrick (2),M. Touré Mohamed (2) |
| SG17 RG-ARB | Mme Latrous Wala Turki (4)**,**M. Al Salehi Badar Ali Said (5) | Mme Abdelkader Manel (6)**,**Mme Abouche Chehrazed (6)**,**Mme Almansoury Laial (7) |
| Projet ASN.1  | Chef de projet: Paul THORPE |  |
| Projet OID | Chef de projet: Olivier DUBUISSON |  |

Notes:

(1) Coprésident depuis mars 2017.

(2) Président Vice-Président jusqu'en septembre 2018.

(3) Présidente depuis avril 2019.

(4) Coprésidente de décembre 2017 à octobre 2018.

(5) (Co)président depuis décembre 2017.

(6) Vice-Présidente de décembre 2017 à octobre 2018.

(7) Vice-Présidente depuis décembre 2017.

(8) Coprésident a.i. depuis avril 2021.

## 2.2 Questions et Rapporteurs

**2.2.1** L'AMNT-16 a confié à la Commission d'études 17 les 12 Questions dont la liste figure dans le Tableau 5 et la CE 17 a désigné pendant cette période d'études les Rapporteurs et Rapporteurs associés dont les noms sont indiqués dans la liste.

TABLEau 5

Commission d'études 17 – Questions confiées par l'AMNT-16 et Rapporteurs (2017-2020)

| Question | Titre de la Question | GT | Rapporteur(19) |
| --- | --- | --- | --- |
| Q1/17 | Coordination en matière de sécurité des télécommunications/TIC | PLEN | Mme Latrous Wala (Rapporteur) (13)M. Elhaj Mohamed M. K. (Rapporteur) (1)Mme Ki Juhee (Rapporteur associé) (2)M. Najarian Paul (Rapporteur associé) (3)M. Senga Wataru (Rapporteur associé) (3)Mme Wang Yiwen (Rapporteur associé) (3) |
| Q2/17 | Architecture et cadre général de la sécurité | GT 1/17 | Mme Hu Zhiyuan (Corapporteur) (3)M. Oh Heung Ryong (Corapporteur) (3)Mme Chaabane Emna (Rapporteur associé) (10)M. Lee Jinmyung (Rapporteur associé) (16) |
| Q3/17 | Gestion de la sécurité des informations de télécommunication | GT 1/17 | Mme Naganuma Miho (Rapporteur) (3)M. Min Jinghua (Rapporteur associé) (7)M. Mustafa Thaib (Rapporteur associé) (5)M. Fischer Andres (Rapporteur associé) (4) |
| Q4/17 | Cybersecurité | GT 2/17 | M. Kadobayashi Youki (Rapporteur) (6)M. Kim Jong-Hyun (Rapporteur) (7)M. Sim Dong-Hi (Rapporteur associé) (2)M. Zhang Chen (Rapporteur associé) (15)M. Casanovas Eduardo (Rapporteur associé) (4) |
| Q5/17 | Lutte contre le spam par des moyens techniques | GT 2/17 | M. Zhang Yanbin (Rapporteur) (3)M. Kim ChangOh (Rapporteur associé) (3) |
| Q6/17 | Aspects relatifs à la sécurité des services et des réseaux de télécommunication et de l'Internet des objets (17)  | GT 1/17 | M. Baek Jonghyun (Corapporteur) (3)Mme Zuo Min (Corapporteur) (14)M. Yan Junzhi (Corapporteur) (8)M. Lee Gunhee (Rapporteur associé) (9)M. Takahashi Takeshi (Rapporteur associé) (3)M. Yu Bo (Rapporteur associé) (3)Mme Pazo Robles Maria Eugenia (Rapporteur associé) (4) |
| Q7/17 | Services applicatifs sécurisés | GT 3/17 | M. Nah Jae Hoon (Rapporteur) (3)Mme Gao Feng (Rapporteur associé) (7)M. Liu Lijun (Rapporteur associé) (3) |
| Q8/17 | Sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées (18)  | GT 3/17 | M. Wei Liang (Rapporteur) (3)M. Sang-Woo Lee (Rapporteur associé) (9)M. McFadden Mark (Rapporteur associé) (5) |
| Q9/17 | Télébiométrie | GT 4/17 | M. Caras John George (Rapporteur) (3)M. Li Kepeng (Rapporteur associé) (11)Mme Wang Mengxi (Rapporteur associé) (12) |
| Q10/17 | Architecture et mécanismes de gestion d'identité | GT 4/17 | M. Barbir Abbie (Rapporteur) (3)M. Park Keundug (Rapporteur associé) (3)M. Takechi Hiroshi (Rapporteur associé) (3)M. Xia Junjie (Rapporteur associé) (3) |
| Q11/17 | Technologies génériques (annuaire, infrastructure de clé publique (PKI), infrastructure de gestion des privilèges (PMI), notation de syntaxe abstraite numéro un (ASN.1), identificateurs d'objet (OID)) utilisées pour les applications sécurisées | GT 4/17 | M. Lemaire Jean-Paul (Rapporteur) (3)Mme Kaddachi Olfa (Rapporteur associé) (18) |
| Q12/17 | Langages formels pour les logiciels de télécommunication et les tests | GT 3/17 | M. Hogrefe Dieter (Rapporteur) (3)M. Mussbacher Gunter (Rapporteur associé) (5)M. Duhalde Enacom Martin (Rapporteur associé) (4) |

Notes:

(1) Désigné le 5septembre 2019.

(2) Désigné le 30 janvier 2019.

(3) Désignée le 30 mars 2017.

(4) Désigné le 30 mars 2017, révoqué le 29 mars 2018.

(5) Désigné le 6 septembre 2017.

(6) Désigné le 30 mars 2017, révoqué (nommé à un autre poste) le 29 mars 2018.

(7) Désigné le 29 mars 2018.

(8) Désigné le 30 janvier 2019.

(9) Désigné le 7 septembre 2018.

(10) Désignée le 30 mars 2017, révoqué le 7 septembre 2018.

(11) Désigné le 30 mars 2017, a démissionné le 7 septembre 2018.

(12) Désignée le 6 septembre 2017, révoqué le 7 septembre 2018.

(13) Désignée le 30 mars 2017, révoqué en janvier 2019.

(14) Désignée le 29 mars 2018, a démissionné le 30 janvier 2019.

(15) Désigné le 7 septembre 2018.

(16) Désigné le 6 septembre 2017, révoqué le 7 septembre 2018.

(17) Le titre de la Question 6/17 (Aspects relatifs à la sécurité des services et des réseaux de télécommunication) a été remplacé par le titre suivant: "Aspects relatifs à la sécurité des services et des réseaux de télécommunication et de l'Internet des objets".

(18) Le titre de la Question 8/17 (Sécurité de l'informatique en nuage) a été remplacé par le titre suivant: "Sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées".

(19) Désignation valable avant le 20 avril 2021.

**2.2.2** Compte tenu du report de l'AMNT-20 à mars 2022, le GCNT a approuvé, à sa réunion tenue du 11 au 18 janvier 2021, une nouvelle série de 12 Questions (voir la liste figurant dans le Tableau 5a), qui ont été approuvées par la CE 17 à sa réunion tenue en août/septembre 2020 (voir la [Circulaire 295 du TSB](https://www.itu.int/md/T17-TSB-CIR-0295/en)).

TABLEAU 5a

Commission d'études 17 – Questions approuvées par le GCNT (à compter du 18 janvier 2021)

| Nouveau numéro | Nouveau titre de la Question | Statut | Numéro précédent | Titre précédent de la Question | GT | Rapporteur (1) |
| --- | --- | --- | --- | --- | --- | --- |
| 1/17 | Stratégie et coordination en matière de normalisation de la sécurité | Suite | 1/17 | Coordination en matière de sécurité des télécommunications/TIC | GT 1/17 | Corapporteurs:– M. Elhaj Mohamed M. K– Mme Ki JuheeRapporteurs associés:– M. Najarian Paul– M. Senga Wataru– Mme Wang Yiwen**)** |
| 2/17 | Architecture de sécurité et sécurité des réseaux | Suite | 2/17 | Sécurité: architecture et cadre | GT 2/17 | Corapporteurs:– Mme Hu Zhiyuan– M. Oh Heung Ryong |
| 3/17 | Gestion de la sécurité des informations de télécommunication et services de sécurité | Suite | 3/17 | Gestion de la sécurité des informations de télécommunication | GT 3/17 | Rapporteur:– Mme Naganuma MihoRapporteurs associés:– M. Min Jinghua – M. Mustafa Thaib  |
| 4/17 | Cybersécurité et lutte contre le spam | Suite des Questions 4/17 et 5/17 | 4/17 | Cybersécurité | GT 3/17 | Corapporteurs:– M. Kim Jong-Hyun– M. Zhang YanbinRapporteur associé:– M. Kim ChangOh |
| 5/17 | Lutte contre le spam par des moyens techniques |  |  |
| 6/17 | Sécurité des services de télécommunication et de l'Internet des objets | Suite | 6/17 | Aspects relatifs à la sécurité des services et des réseaux de télécommunication et de l'Internet des objets | GT 2/17 | Corapporteurs:– M. Baek Jonghyun – M. Yan JunzhiRapporteurs associés:– M. Lee Gunhee– M. Takahashi Takeshi– M. Yu Bo  |
| 7/17 | Services applicatifs sécurisés | Suite | 7/17 | Services applicatifs sécurisés | GT 4/17 | Rapporteur:– Mme Nah Jae Hoon Rapporteurs associés:– Mme Gao Feng– M. Liu Lijun |
| 8/17 | Sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées | Suite | 8/17 | Sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées | GT 4/17 | Rapporteur:– M. Wei LiangRapporteur associé:– M. McFadden Mark |
| 10/17 | Architecture et mécanismes de gestion des identités et de télébiométrie | Suite des Questions 9/17 et 10/17 | 9/17 | Télébiométrie | GT 5/17 | Corapporteurs:– M. Barbir Abbie– M. Caras John GeorgeRapporteurs associés:– M. Kim Jason– M. Park Keundug– M. Takechi Hiroshi– M. Xia Junjie |
| 10/17 | Architecture et mécanismes de gestion d'identité |  |  |
| 11/17 | Technologies génériques (notamment: annuaire, infrastructure de clé publique (PKI), langages formels et identificateurs d'objets) utilisées pour les applications sécurisées | Suite des Questions 11/17 et 12/17 | 11/17 | Technologies génériques (annuaire, infrastructure de clé publique (PKI), infrastructure de gestion des privilèges (PMI), notation de syntaxe abstraite numéro un (ASN.1), identificateurs d'objet (OID)) utilisées pour les applications sécurisées | GT 5/17 | Rapporteur:– M. Lemaire Jean-Paul Rapporteur associé:– M. Hogrefe Dieter |
| 12/17 | Langages formels pour les logiciels de télécommunication et les tests |  |  |
| 13/17 | Sécurité des systèmes de transport intelligents (ITS) | Suite | 13/17 | Aspects de sécurité concernant les systèmes de transport intelligents | GT 2/17 | Rapporteur:– M. Lee Sang-Woo Rapporteurs associés:– M. Park Seungwook – Mme Zhang Yi  |
| 14/17 | Sécurité de la technologie des registres distribués (DLT) | Suite | 14/17 | Aspects de sécurité concernant les technologies des registres distribués | GT 4/17 | Corapporteurs:– M. Kadobayashi Youki– Mme Oh Kyeong HeeRapporteurs associés:– Mme Bai Xiaoyuan– Mme Wang Ke |
| 15/17 | Sécurité relative aux nouvelles technologies, y compris la sécurité quantique | Nouvelle | – | – | GT 1/17 | Rapporteur:– M. Sim DongheeRapporteurs associés:– M. Kenyoshi Kaoru– M. Yoon ChunSeok– M. Zhang Chen |

(1) désigné (ou reconduit dans ses fonctions) à la réunion de la CE 17 tenue du 20 au 30 avril 2021.

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

TABLEau 5b

Commission d'études 17 – Nouvelles Questions adoptées et Rapporteurs

| Question | Titre de la Question | GT | Rapporteur  |
| --- | --- | --- | --- |
| Q13/17 | Aspects relatifs à la sécurité des systèmes de transport intelligents(10)/sécurité des systèmes de transport intelligents (ITS)(11) | GT 1/17 (10)/GT 2/17 (11) | M. Lee Sang-Woo (Rapporteur) (1)M. Park Seungwook (Rapporteur associé) (1)Mme Zhang Yi (Rapporteur associé) (2) |
| Q14/17 | Aspects sécurité des technologies de registres numériques distribués(10) Sécurité des technologies de registres distribués (DLT) (11) | GT 2/17(10) /GT 3/17(11) | M. Kadobayashi Youki (Corapporteur) (3)Mme Oh Kyeong Hee (Corapporteur) (3)Mme Bai Xiaoyuan (Rapporteur associé) (4)Mme Wang Ke (Rapporteur associé) (4) Mme Zuo Min (Rapporteur associé) (5) |
| Q15/17 | Sécurité relative aux nouvelles technologies, y compris la sécurité quantique | GT 1/17(11) | M. Sim Dong-hi (Rapporteur) (6)M. Kenyoshi Kaoru (Rapporteur associé) (7)M. Yoon Chun Seok (Rapporteur associé) (8)M. Zhang Chen (Rapporteur associé) (9) |

Notes:

(1) Désigné le 30 mars 2017.

(2) Désignée le 7 septembre 2018.

(3) Désignée le 6 septembre 2017.

(4) Désignée le 29 mars 2018.

(5) Désignée le 6 septembre 2017, révoquée (nommée à un autre poste) le 29 mars 2018.

(6) Désigné le 20 avril 2021.

(7) Désigné le 20 avril 2021.

(8) Désigné le 20 avril 2021, responsable des tâches relatives à l'incubation.

(9) Désigné le 20 avril 2021.

(10) 2017-2020.

(11) 2021-2022.

**2.2.4** Les Questions dont la liste figure dans le Tableau 6 ont été fusionnées avec d'autres Questions de la CE 17 pendant cette période d'études.

TABLEau 6

Commission d'études 17 – Questions supprimées

|  |  |  |  |
| --- | --- | --- | --- |
| Question | Titre de la Question | Rapporteurs | Note |
| Q5/17 (supprimée) | Lutte contre le spam par des moyens techniques | M. Zhang Yanbin (Rapporteur)M. Kim ChangOh (Rapporteur associé) | La Question 5/17 a été fusionnée avec la Question 4/17 le 18 janvier 2021, après approbation par le GCNT. |
| Q9/17 (supprimée) | Télébiométrie | M. Caras John George (Rapporteur) | La Question 9/17 a été fusionnée avec la Question 10/17 le 18 janvier 2021, après approbation par le GCNT. |
| Q12/17 (supprimée) | Langages formels pour les logiciels de télécommunication et les tests | M. Hogrefe Dieter (Rapporteur)M. Mussbacher Gunter (Rapporteur associé) | La Question 12/17 a été fusionnée avec la Question 11/17 le 18 janvier 2021, après approbation par le GCNT. |

# 3 Résultats des travaux effectués pendant la période d'études 2017-2020

## 3.1 Généralités

Depuis le début de la période d'études et jusqu'à sa réunion électronique du 7 janvier 2022, la Commission d'études 17 a examiné un grand nombre de contributions et de documents temporaires (TD) ainsi que de notes de liaison.

Sur la base de ces documents, au 7 janvier 2022, la Commission d'études 17 avait:

– élaboré 53 nouvelles Recommandations selon la procédure AAP et 47 nouvelles Recommandations selon la procédure TAP (3 ont fait l'objet d'une détermination selon la procédure TAP);

– révisé 93 Recommandations existantes selon la procédure APP et 3 Recommandations existantes selon la procédure TAP;

– modifié 4 Recommandations;

– élaboré 8 nouveaux Suppléments, un Supplément révisé et un corrigendum à un Supplément existant;

– produit 17 Corrigenda techniques;

– élaboré 2 documents techniques et 6 rapports techniques révisés (aucun Manuel n'a été élaboré).

Pendant la période d'études jusqu'à la réunion électronique du 7 janvier 2022, la CE 17:

– a rassemblé 2 163 (2 063+100) participants (réunions précédentes: 100, 223, 231, 91, 262, 69, 225, 206, 178, 168, 130, 134, 146);

– a formulé 162 nouveaux sujets d'étude (réunions précédentes: 7, 15, 0, 15, 7, 26, 13, 25, 21, 26, 7);

– a reçu 1 179 contributions (réunions précédentes: 1, 98, 104, 2, 110, 121, 151, 118, 144, 113, 106, 78);

– a élaboré 4 220 documents temporaires (réunions précédentes: 106, 336, 305, 44, 434, 35, 439, 508, 380, 420, 395, 426, 368);

– a reçu 585 notes de liaison et envoyé 328 notes de liaison (réunions précédentes: 55+1, 51+23, 36+17, 21+0, 58+32, 1+2, 77+24, 64+42, 47+30, 40+37, 46+37, 49+40, 40+38).

## 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 présentés ci-dessous.

Les réponses officielles aux Questions sont indiquées dans un tableau synoptique figurant dans l'Annexe 1 du présent rapport.

a) Question 1/17: Coordination en matière de sécurité des télécommunications/TIC (2017-2020)/Stratégie et coordination en matière de normalisation de la sécurité (2021-)

La Question 1/17 sert de base à la CE 17 pour la coordination en matière de sécurité des télécommunications/TIC, tant au sein de la CE 17 qu'avec d'autres commissions d'études et des organisations extérieures. De plus, le groupe chargé de de la Question 1/17 élabore et met à jour plusieurs documents de sensibilisation et de référence que l'UIT-T considère comme autant d'outils précieux pour promouvoir ses travaux concernant la sécurité et les résultats qu'il a obtenus. 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 préparé la 7ème édition.

– Le rapport technique sur l'*utilisation efficace des normes de sécurité*, qui traite de la manière dont les Recommandations de l'UIT-T sur la sécurité qui ont été approuvées peuvent être mises en œuvre avec succès. Les différentes Recommandations (par exemple la Recommandation UIT-T X.805) et les familles de Recommandations (par exemple CYBEX) sont examinées et les avantages que l'on peut retirer de leur utilisation sont décrits. Au cours de cette période d'études, le groupe chargé de la Question 1/17 a préparé la 2ème édition.

– La *Feuille de route relative aux normes sur la sécurité des TIC*, qui contient une base de données consultable en ligne dans laquelle figurent plus de 2 600 normes approuvées sur la sécurité des TIC émanant des commissions d'études de l'UIT-T et d'organismes de normalisation extérieurs, notamment 3D@home, 3GPP, 3GPP2, ATIS, ETSI, IEEE, IETF, ISO/CEI JTC 1, OASIS, oneM2M, SmartBan et TETRA. Pendant l'actuelle période d'études, le groupe chargé de la Question 1/17 a approuvé de nombreuses mises à jour.

– Le *Recueil de Recommandations sur la sécurité*, qui comprend dans la Partie I un catalogue des Recommandations UIT-T approuvées relatives à la sécurité des télécommunications et, dans la Partie II, un extrait des définitions relatives à la sécurité approuvées par l'UIT-T. Au cours de l'actuelle période d'études, le Recueil a été mis à jour à chaque réunion consacrée à la Question 1/17.

Une coordination a été assurée avec tous les groupes chargés des Questions relevant de la Commission d'études 17, ainsi qu'avec 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.

Le groupe chargé de la Question 1/17 a également encouragé l'organisation d'ateliers sur la sécurité, a apporté une assistance aux deux groupes régionaux de la CE 17 (Afrique et États arabes) et a renforcé l'efficacité des travaux de la CE 17 en élaborant des modèles, des outils et des procédures. Au cours de l'actuelle période d'études, le groupe chargé de la Question 1/17 a aidé l'UIT à organiser 13 ateliers jusqu'à la fin de 2021.

b) Question 2/17: Architecture et cadre de sécurité (2017-2020)/Architecture de sécurité et sécurité des réseaux (2021-)

Le groupe chargé de la Question 2/17 a pour mission d'élaborer un ensemble complet de Recommandations relatives aux architectures et cadres de sécurité pour définir des solutions de sécurité normalisées pour les télécommunications, notamment des solutions de sécurité pour la 5G et des cadres de sécurité pour les réseaux pilotés par logiciel, la téléphonie utilisant la technologie LTE (évolution à long terme) et la virtualisation de réseau.

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

– Recommandation X.1011, *Lignes directrices relatives à la protection continue du processus d'accès aux services*; cette Recommandation contient une analyse des menaces de sécurité pour les processus d'accès aux services, indique des mesures de protection de la sécurité pour détecter les activités anormales en matière d'accès et présente un mécanisme d'autorisation amélioré pour l'accès aux services.

– Recommandation X.1040, *Architecture de référence de sécurité pour la gestion, tout au long de leur cycle de vie, des données sur les transactions de commerce électronique*; cette Recommandation analyse les principales caractéristiques des écosystèmes de services de commerce électronique ainsi que les menaces types rencontrées dans ces écosystèmes, et décrit une architecture de référence de sécurité pour la gestion, tout au long de leur cycle de vie, des données sur les transactions de commerce électronique.

– Recommandation X.1041, *Cadre de sécurité pour l'exploitation des réseaux de téléphonie utilisant la technologie LTE (évolution à long terme) (VoLTE)*;cette Recommandation analyse les menaces de sécurité qui pèsent sur le réseau VoLTE et préconise des mesures à l'intention des opérateurs de télécommunication afin de garantir la sécurité d'exploitation. Elle définit également un cadre de référence de sécurité pour les réseaux VoLTE*.*

– Recommandation X.1043, *Cadre et exigences de sécurité pour le chaînage de fonctions de service basé sur les réseaux pilotés par logiciel;* cette Recommandationanalyse les menaces qui pèsent sur la sécurité et indique les exigences de sécurité pour le chaînage de fonctions de service basé sur les réseaux pilotés par logiciel (SDN). Elle décrit en outre les mesures de sécurité correspondantes. La Recommandation X.1043 vise à mieux faire comprendre les risques en matière de sécurité rencontrés lors de l'utilisation du chaînage de fonctions de service SDN et à faciliter la mise en place de chaînes de fonctions de service SDN sécurisées.

– Recommandation X.1044, *Exigences de sécurité de la virtualisation de réseau;* cette Recommandationanalyse les problèmes et les menaces qui pèsent sur la sécurité de la virtualisation de réseau et indique les exigences de sécurité pour la couche des ressources physiques, la couche des ressources virtuelles et la couche des subdivisions de réseau isolées logiquement (LINP) de la virtualisation de réseau.

– Recommandation X.1045, *Architecture de la chaîne de services de sécurité pour les réseaux et les applications;* cette Recommandationvise à faciliter la fourniture de services de sécurité dynamiques et adaptatifs personnalisés pour les réseaux et les applications. Elle définit la chaîne de services de sécurité et un modèle d'architecture associé, et décrit l'utilisation de la chaîne de services de sécurité pour les réseaux et les applications. Cette Recommandation permet en outre d'identifier la source des attaques dans le réseau en utilisant un réseau superposé de chaîne de fonctions de service (SFC) à haute performance et de réduire/prévenir automatiquement ces attaques.

– Recommandation X.1046, *Cadre applicable à* la *sécurité définie par logiciel dans les réseaux pilotés par logiciel/réseaux avec virtualisation des fonctions de réseau*; cette Recommandationdéfinit un cadre applicable à la sécurité définie par logiciel – dans les réseaux pilotés par logiciel (SDN) et les réseaux avec virtualisation des fonctions de réseau (NFV). Elle contient une analyse des principaux problèmes de sécurité, y compris les aspects techniques et opérationnels, auxquels sont confrontés les réseaux SDN/NFV des opérateurs. Elle définit les exigences de sécurité à respecter pour remédier à ces problèmes dans les réseaux SDN/NFV. Cette Recommandation présente la notion de "sécurité définie par logiciel" et définit un cadre applicable à la "sécurité définie par logiciel". Elle permet d'assurer la sécurité définie par logiciel.

– Recommandation X.1047, *Exigences et architecture de sécurité pour la gestion et l'orchestration des tranches de réseau*; cette Recommandation définit des exigences et une architecture de sécurité pour la gestion et l'orchestration des tranches de réseau*,* ainsi que pour la création automatique de tranches de réseau de bout en bout avec des capacités de sécurité personnalisées, afin de déployer un découpage de réseau de bout en bout à grande échelle pour les segments des consommateurs, des entreprises et des pouvoirs publics.

– Le Supplément 30 à la Recommandation UIT-T X.805 *– Lignes directrices sur la sécurité pour les opérateurs de réseaux virtuels mobiles (MVNO)*, fournit des lignes directrices concernant la sécurité des opérateurs de réseaux virtuels mobiles (MVNO). La sécurité est très importante pour les MVNO et la plupart de ces opérateurs présentent de nombreuses similitudes sur le plan de la sécurité. Ce Supplément contient une analyse des principales caractéristiques des MVNO et des menaces types en matière de sécurité auxquels ils sont confrontés. Sur la base de la structure des MVNO, ce Supplément offre un cadre applicable à la sécurité des MVNO, qui comprend des objectifs et des exigences en matière de sécurité.

c) Question 3/17: Gestion de la sécurité des informations de télécommunication 2017‑2020)/Gestion de la sécurité des informations de télécommunication et services de sécurité (2021-)

Le groupe chargé de la Question 3/17 élabore des Recommandations sur la gestion de la sécurité des informations de télécommunication, par exemple le Code de bonnes pratiques pour les informations personnelles identifiables (PII) pour les organisations de télécommunication et les petites et moyennes organisations de télécommunication.

Pendant l'actuelle période d'études, le groupe chargé de la Question 3/17 a élaboré cinq nouvelles Recommandations, un corrigendum, deux Recommandations révisées et trois nouveaux Suppléments:

– Corrigendum 1 à la 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.*

– La Recommandation X.1052 (révisée), *Processus de gestion de la sécurité de l'information pour les organisations de télécommunication*, présente les bonnes pratiques en matière de gestion de la sécurité de l'information pour les organisations de télécommunication et complète la Recommandation UIT-T X.1051. Cette Recommandation est fondée sur une approche par processus pour décrire un ensemble de domaines de gestion de la sécurité et contient des lignes directrices à l'intention des organisations de télécommunication, pour qu'elles atteignent les objectifs de contrôle définis dans la Recommandation UIT-T X.1051. Une mise en correspondance est

 établie entre, d'une part les domaines de gestion de la sécurité tels que la gestion des actifs, la gestion des incidents, la gestion des risques et la gestion des politiques, et, d'autre part, les contrôles définis par la Recommandation UIT-T X.1051, pour mettre en place des méthodes.

– La Recommandation X.1053, *Code de bonne pratique pour les contrôles de sécurité de l'information sur la base de la Recommandation UIT-T X.1051 pour les petites et moyennes organisations de télécommunication,* établit des lignes directrices et des principes généraux pour instaurer, mettre en œuvre, maintenir et améliorer les contrôles de sécurité de l'information dans les petites et moyennes organisations de télécommunication (SMTO), sur la base de la Recommandation UIT-T X.1051. Elle donne en outre des indications de base relatives à la mise en œuvre des contrôles de sécurité de l'information pour les SMTO, 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.

– La Recommandation X.1058, *Technologie de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des informations d'identification personnelle,* définit un certain nombre de buts et de mesures de contrôle, et contient des directives permettant de mettre ces mesures en œuvre. Elle vise à répondre aux besoins recensés dans le cadre des évaluations de risque et d'impact effectuées dans le domaine de la protection des IIP. En particulier, cette spécification définit des directives qui sont fondées sur la norme ISO/CEI 27002, compte tenu des besoins de traitement des IIP et pouvant être pertinents au regard des risques de sécurité pesant sur les informations d'une organisation donnée.

– La Recommandation X.1059, *Guide de mise en œuvre à l'intention des organisations de télécommunication sur la gestion des risques liés à leurs actifs mondialement accessibles dans les réseaux IP,* fournit des orientations aux organisations de télécommunication sur la gestion des risques liés à leurs actifs mondialement accessibles dans les réseaux IP, actifs qui sont directement exposés aux pirates et auteurs d'attaques. Ces actifs peuvent en outre être reliés aux actifs traditionnels (voire à d'anciens actifs) de réseaux de télécommunication de générations antérieures, qui sont susceptibles de présenter certaines vulnérabilités au niveau de la conception qui pourraient être difficiles à corriger. Par conséquent, il serait utile de considérer comme un tout l'ensemble des actifs d'une organisation de télécommunication qui sont mondialement accessibles dans les réseaux IP, et de mettre en place certains contrôles de sécurité spécifiques pour réduire constamment les risques globaux et renforcer la sécurité globale des services et des réseaux de télécommunication.

– La Recommandation X.1060, *Cadre relatif à la création et à l'exploitation d'un centre de cyberdéfense,* définit le centre de cyberdéfense comme une entité jouant un rôle central dans le traitement des risques de cybersécurité au sein d'une organisation. Un centre de cyberdéfense s'articule autour de trois processus – mise en place, gestion et évaluation – qu'il doit mettre en œuvre concrètement et qui en forment le cadre. Cette Recommandation définit également les services dont l'organisation devrait être dotée pour mettre en œuvre des mesures de cybersécurité plus précises.

– Recommandation X.1061, *Lignes directrices relatives à l'acquisition d'une cyberassurance à l'intention des fournisseurs de services issus des technologies de l'information et de la communication (TIC)*

Ces lignes directrices relatives à l'acquisition d'une cyberassurance fournissent des explications sur la couverture d'une cyberassurance, les exigences applicables aux évaluations des risques de cybersécurité, le choix de l'assureur, les analyses effectuées par l'assureur et l'évaluation de l'assureur à l'intention des organisations qui optent pour une cyberassurance en tant que solution de traitement des risques pour gérer les conséquences d'un incident de cybersécurité.

– Supplément 13 (révisé) aux Recommandations de la série X – Supplément à la Recommandation *UIT-T X.1051 – Manuel d'utilisation pour les contrôles de sécurité de l'information*.

– Le Supplément 32 aux Recommandations de la série X – Supplément à la Recommandation *UIT-T X.1058 – Code de bonne pratique pour la protection des informations d'identification personnelle pour les organisations de télécommunication,* vient compléter les renseignements donnés dans la Recommandation UIT-T X.1058,en fournissant des orientations additionnelles relatives à la mise en œuvre pour la protection des informations d'identification personnelle (PII), qui ne sont pas décrites dans la Recommandation UIT-T X.1058 mais devraient également être applicables aux organisations de télécommunication pour assurer la protection des PII.

– Le Supplément 34 aux Recommandations de la série X – Supplément à la Recommandation UIT-T X.1051 *– Code de bonne pratique pour les contrôles de sécurité de l'information pour les organisations de télécommunication,* met l'accent et donne des informations sur un code de bonne pratique pour la gestion de la sécurité de l'information et des réseaux par le secteur des technologies de l'information de la Malaisie, sur la base de la Recommandation UIT-T X.1051.

– Le Supplément 36 aux Recommandations de la série X – Supplément à la Recommandation UIT-T X.1051 *– Contrôles critiques de la sécurité pour la gestion de la sécurité des réseaux et de l'information des organisations de télécommunication*, présente des bonnes pratiques en matière de cybersécurité pour la gestion de la sécurité au moyen de contrôles critiques de la sécurité dans le cadre de la Recommandation UIT‑T X.1051. L'utilisation du cadre des contrôles critiques de la sécurité (CSC) et des contrôles critiques de la sécurité connexes appuie et complète la Recommandation UIT‑T X.1051.

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.

d) Question 4/17: Cybersécurité (2017-2020)/Cybersécurité et lutte contre le spam (2021-)

Le groupe chargé de la Question 4/17 élabore des Recommandations sur les cadres et les exigences en matière de cybersécurité concernant la façon dont les fournisseurs de télécommunications/TIC peuvent sécuriser leur infrastructure, assurer un fonctionnement fiable et échanger des informations sur la cybersécurité. Au cours de l'actuelle période d'études, le groupe chargé de la Question 4/17 a également ajouté une fonction d'incubation pour tenir compte des nouveaux problèmes qui se font jour, par exemple la sécurité dans un environnement quantique, jusqu'en 2020, avant de confier cette fonction au groupe chargé de la Question 15/17 en janvier 2021. En janvier 2021 également, le groupe chargé de la Question 4/17 a repris les travaux en cours sur la lutte contre le spam, qui étaient menés auparavant au titre de la Question 5/17.

Pendant l'actuelle période d'études, 14 nouvelles Recommandations, une Recommandation révisée, deux nouveaux Amendements, deux nouveaux documents techniques et deux nouveaux rapports techniques ont été élaborés au titre de la Question 4/17:

– La Recommandation X.1212, *Considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité*, expose des considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité. Ses appendices décrivent des techniques représentatives servant à mesurer la perception par l'utilisateur final de ces indicateurs.

– La Recommandation X.1213, *Capacités requises en matière de sécurité pour lutter contre les réseaux zombies (ou botnets)* ciblant des smartphones, contient une analyse du contexte des réseaux zombies (ou botnets) ciblant des smartphones et les risques potentiels qu'ils représentent pour la sécurité et décrit les capacités requises en matière de sécurité.

– La Recommandation X.1214, *Techniques d'évaluation de la sécurité dans les réseaux de télécommunication/technologies de l'information et de la communication*, décrit une méthode d'évaluation de la sécuritépour les éléments logiciels des réseaux de télécommunication/technologies de l'information et de la communication (TIC) ainsi que les bonnes pratiques en la matière à l'intention des concepteurs, des constructeurs, des opérateurs et des spécialistes de la sécurité exerçant dans le domaine des télécommunications, en vue de l'examen de la sécurité de leurs éléments logiciels. Les réseaux traditionnels à commutation de circuits et les réseaux en mode paquet sont exposés à différentes menaces et attaques, internes et externes, qui ciblent les diverses parties d'un réseau de télécommunication/TIC. Dans les réseaux de télécommunication/TIC, cette Recommandation porte sur la détection des vulnérabilités et la méthode d'évaluation de la sécurité.

– La Recommandation X.1215, *Cas d'utilisation pour l'expression structurée d'informations sur les menaces,* présente divers cas d'utilisation dans lesquels le langage STIX (expression structurée d'informations sur les menaces) peut être utilisé pour faciliter l'échange d'informations et de renseignements (CTI) sur les cybermenaces.

– La Recommandation X.1216, *Exigences en matière de collecte et de conservation de preuves relatives aux incidents de cybersécurité,* décrit une procédure générale pour les interventions et les enquêtes en cas d'incident de cybersécurité. Elle contient aussi une analyse des sources des preuves relatives aux incidents de cybersécurité et précise les exigences relatives aux capacités des outils utilisés pour collecter et conserver ces preuves dans le cadre d'une procédure d'enquête. Cette Recommandation précise en outre les exigences relatives à la garantie de fiabilité des outils, qui serviront de lignes directrices aux concepteurs qui mettent au point des outils à cette fin.

– La Recommandation X.1217, *Lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication*. Du point de vue d'un opérateur de télécommunication, les renseignements sur les menaces constituent un ensemble d'informations organisées, analysées et affinées sur les attaques potentielles et actuelles qui peuvent menacer une organisation. Ces informations peuvent également comprendre les motivations, les intentions, les caractéristiques et les méthodes des auteurs d'attaques, ainsi que leur mode opératoire ou leurs techniques, leurs tactiques et leurs procédures. En ce qui concerne la sécurité des réseaux et de l'information, la survenue d'incidents de cybersécurité inattendus et à grande échelle a rendu urgente la nécessité de disposer de renseignements sur les menaces. Ces renseignements peuvent aider une organisation à réduire les risques et à améliorer sa sécurité globale. Une taxonomie, une grammaire et une présentation unifiées des renseignements sur les menaces ont été définies afin que différentes organisations puissent échanger ces renseignements. Cette Recommandation contient des lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication après une analyse d'ensemble.

– La Recommandation X.1218, *Exigences et lignes directrices pour l'analyse dynamique des logiciels malveillants dans un environnement de bac à sable*. Des logiciels malveillants inconnus sont couramment utilisés en cas d'attaques évoluées, en particulier de menaces persistantes avancées (APT), pour éviter d'être détectés. Par exemple, une attaque ciblée consistant à utiliser des courriels hameçons contenant des logiciels malveillants inconnus peut facilement aboutir à un premier compromis réussi. Ainsi, pour détecter des attaques évoluées et des logiciels malveillants inconnus, il convient d'accorder une attention particulière et d'appliquer des mesures de protection. La Recommandation UIT-T X.1218 vise à analyser les menaces liées à des logiciels malveillants inconnus et définit des exigences relatives à la détection des logiciels malveillants inconnus reposant sur l'analyse de comportement dynamique.

– La Recommandation X.1233, *Lignes directrices relatives à la lutte contre le spam par messagerie instantanée,* contient des lignes directrices à l'intention des fournisseurs et des utilisateurs de services de messagerie instantanée (IM), afin de lutter contre les spams par messagerie instantanée (SPIM). Elle traite des scénarios de spam par messagerie instantanée, des mesures techniques et des mécanismes de lutte contre les SPIM à l'intention des fournisseurs de services de messagerie instantanée, ainsi que des mesures d'intervention en cas d'urgence à l'intention des utilisateurs de services de messagerie instantanée afin de lutter contre les SPIM.

– La Recommandation X.1234, *Lignes directrices relatives à la lutte contre le spam envoyé par le service de messagerie multimédia (MMS)*, contient des lignes directrices relatives à la lutte contre le spam par MMS. Elle renferme une analyse des scénarios types, des caractéristiques et des méthodes de reconnaissance du spam par MMS et définit un cadre technique, des procédures à suivre et un certain nombre de technologies essentielles pour la reconnaissance des spams acheminés par MMS, afin d'aider les fournisseurs et les utilisateurs de MMS à lutter contre le spam.

– La Recommandation X.1235, *Technologies de lutte contre le piratage de sites web pour les organisations de télécommunication*, préconise à l'intention des organisations de télécommunication l'utilisation de certaines technologies permettant de repérer à temps des pirates de sites web et de protéger ces sites web contre le piratage.

– Les Amendements 11 et 12 à la Recommandation UIT-T X.1500, *Aperçu de l'échange d'informations sur la cybersécurité*, dressent une liste des techniques d'échange d'informations sur la cybersécurité structurées qui ont été mises au point afin de pouvoir les actualiser 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. Les Amendements rendent compte de la situation des techniques recommandées en mars 2017 et mars 2018 respectivement, y compris des références bibliographiques.

– La Recommandation X.1541 (révisée), *Format d'échange de description d'objet incident version 2*, décrit le modèle d'information pour le format d'échange de description d'objet incident (IODEF)) version 2 et définit un modèle de données associé, indiqué en XML L'IODEF indique une représentation de modèle de données destiné à être utilisé pour le partage des informations couramment échangées sur les incidents en matière de sécurité informatique ou d'autres types d'incidents. À cette fin, cette Recommandation énumère les dispositions pertinentes de la norme IETF RFC 7970 et indique si elles ont un caractère normatif ou informatif.

– La Recommandation X.1550, *Modèles de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents,* présente les approches existantes pour mettre en œuvre les politiques de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents. Elle expose divers modèles de contrôle d'accès qui ont fait leurs preuves, des modèles de partage d'informations ainsi que des critères pour évaluer la qualité de fonctionnement des réseaux d'échange d'informations sur les incidents. On considère que les solutions fondées sur des normes facilitent la mise en œuvre de différents modèles de contrôle d'accès dans le cadre de divers modèles de partage d'informations sur les questions de cybersécurité et dans différents environnements de confiance.

– La Recommandation X.1702, *Architecture d'un générateur de nombres aléatoires pour le bruit quantique,* définit l'architecture fonctionnelle générique d'une source d'entropie quantique, une méthode couramment utilisée pour évaluer et valider l'entropie d'une source de bruit à l'étude, et une méthode couramment utilisée pour définir les extracteurs d'éléments aléatoires lorsqu'ils font partie du système mis en œuvre.

– La Recommandation X.1710, *Cadre de sécurité pour les réseaux de distribution de clés quantiques*, définit un cadre comportant des exigences et des mesures visant à lutter contre les menaces en matière de sécurité pour les réseaux de distribution de clés quantiques (QKDN). Elle indique une structure de réseaux QKDN simplifiée pour l'analyse des menaces pertinentes pour la sécurité. Les exigences de sécurité et les mesures de sécurité correspondantes sont ensuite établies sur cette base.

– La Recommandation X.1714, *Combinaison de clés et fourniture de clés confidentielles pour les réseaux de distribution de clés quantiques*, décrit les méthodes de combinaison de clés pour un réseau de distribution de clé quantique (QKDN) et définit les exigences de sécurité applicables à la combinaison de clés et à la fourniture de clés pour les réseaux QKDN et les applications de cryptographie.

– Le Document technique TP.inno, *Description du mécanisme d'incubation et des moyens permettant de l'améliorer,* décrit dans son intégralité le mécanisme d'incubation créé par la CE 17. Elle recense d'autres moyens et mécanismes utilisés par l'UIT et d'autres organisations de normalisation pour favoriser l'innovation.

– Le Document technique TP.sgstruct, *Approches stratégiques concernant les études sur la transformation de la sécurité,* porte sur les aspects des études sur la transformation de la sécurité à court, moyen et long terme.

– Le rapport technique TR.sec-qkd, *Considérations de sécurité pour les réseaux de distribution de clés quantiques*, décrit un cadre QKD permettant de satisfaire aux exigences du point de vue du réseau de télécommunication.

– Le rapport technique TR.usm, *Modèle de sécurité unifié (USM) – une approche système intégrée neutre en matière de cybersécurité,* présente une architecture universelle selon laquelle "tout est lié à la sécurité" qui est neutre et indépendante. Elle permet de faciliter l'interopérabilité massive des contrôles de sécurité et l'automatisation des interventions dans le domaine de la sécurité.

Au cours de l'actuelle période d'études, le groupe chargé de la Question 4/17 a organisé à Genève, le 24 janvier 2019, un mini-atelier sur les communications quantiques sécurisés.

e) Question 5/17: Lutte contre le spam par des moyens techniques (2017-2020)

Le groupe chargé de la Question 5/17 élabore des Recommandations relatives à la lutte contre le spam par des moyens techniques, par exemple la lutte contre le spam publicitaire, la lutte contre le spam par messagerie instantanée, la lutte contre le spam publicitaire sur les applications mobiles, les mesures de rétorsion à prendre pour lutter contre les attaques par hameçonnage par le service de messages courts et la lutte contre les escroqueries par service téléphonique.

Pendant l'actuelle période d'études, trois nouvelles Recommandations et deux nouveaux Suppléments ont été élaborés au titre de la Question 5/17:

– La Recommandation X.1232, *Cadre technique de lutte contre le spam publicitaire dans les informations générées par les utilisateurs*, analyse les scénarios et les caractéristiques du spam publicitaire, et définit un cadre de référence et des flux de processus pour aider les fournisseurs de services Internet à lutter contre le spam publicitaire.

– La Recommandation X.1248, *Exigences techniques pour lutter contre le spam par messagerie instantanée,* définit les caractéristiques du spam par messagerie instantanée (SPIM) et indique les exigences techniques à respecter pour lutter contre ce phénomène. En raison du succès croissant de la messagerie instantanée (IM), la multiplication du SPIM est devenue un problème de plus en plus préoccupant. Les caractéristiques de la messagerie instantanée, outil largement répandu et gratuit qui repose sur le protocole Internet (IP), font que le SPIM est susceptible de se propager à grande échelle et de façon incontrôlable. Si les problèmes liés au SPIM ne sont pas traités avec le plus grand soin, ils risquent d'avoir des incidences négatives sur l'utilisation du service de messagerie instantanée lui-même.

– La Recommandation X.1249, *Cadre technique de lutte contre le spam publicitaire sur les applications mobiles,* propose un cadre technique pour lutter contre le spam publicitaire sur les applications mobiles. Le spam publicitaire sur les applications mobiles désigne l'envoi de publicités non sollicitées, qui s'affichent dans une application mobile. Ces publicités non sollicitées peuvent apparaître sur l'écran du dispositif mobile sous la forme d'un bandeau situé en haut ou en bas de l'écran, d'un interstitiel sur mobile ou d'une superposition.

– Le Supplément 29 aux Recommandations de la série X – Supplément à la Recommandation UIT-T X.1242 *– Lignes directrices sur les mesures de rétorsion à prendre pour lutter contre les attaques par hameçonnage par le service de messages courts (SMS),* fournit des lignes directrices universelles sur le hameçonnage des services de messages courts (SMS), technique frauduleuse sur téléphone mobile qui permet de commettre des fraudes par hameçonnage avec les smartphones, d'acquérir des informations personnelles sur les smartphones, ou d'obtenir l'approbation et le paiement de petites montants alors que le titulaire du compte n'est pas au courant de l'approbation.

– Le Supplément 33 aux Recommandations de la série X – Supplément à la Recommandation UIT-T X.1231*: Cadre technique de lutte contre les escroqueries par service téléphonique,* fournit un cadre technique et expose les bonnes pratiques connexes permettant de lutter contre les escroqueries par service téléphonique. Dans ce cadre, les fonctions des entités et les procédures de traitement sont définies. Les bonnes pratiques sont celles qui s'avèrent les plus efficaces pour mettre fin aux méthodes connues utilisées pour les escroqueries par service téléphonique.

f) Question 6/17: Aspects relatifs à la sécurité des services et des réseaux de télécommunication et de l'Internet des objets (2017-2020)/Sécurité des services de télécommunication et de l'Internet des objets (2021-)

Le Groupe chargé de l'étude de la Question 6/17 élabore des Recommandations sur les exigences et les cadres de sécurité applicables aux services de télécommunication, aux réseaux mobiles, aux réseaux électriques intelligents, à la TVIP et à l'Internet des objets.

Au cours de l'actuelle période d'études, 17 nouvelles Recommandations, un Amendement et un corrigendum à un Supplément existant ont été élaborés au titre de la Question 6/17:

– La Recommandation X.1042, *Services de sécurité utilisant les réseaux pilotés par logiciel*, porte sur la protection des ressources de réseau au moyen de services de sécurité fondés sur les réseaux pilotés par logiciel (SDN). Elle commence par établir une classification des ressources de réseau pour les services de sécurité fondés sur les réseaux SDN: application SDN, contrôleur SDN, commutateur SDN et gestionnaire de la sécurité (SM). Elle définit ensuite les services de sécurité fondés sur les réseaux SDN.

– La Recommandation X.1126, *Lignes directrices relatives à l'atténuation des effets négatifs des terminaux infectés dans les réseaux mobiles,* fournit aux opérateurs mobiles des lignes directrices visant à restreindre le nombre de terminaux infectés en utilisant, dans le réseau mobile, des technologies destinées à protéger à la fois les abonnés et les opérateurs mobiles.

– La Recommandation X.1127, *Lignes directrices révisées relatives aux critères de sélection d'algorithmes cryptographiques pour la protection de service et de contenu de TVIP,* traite essentiellement des exigences fonctionnelles de sécurité et de l'architecture fonctionnelle concernant les mécanismes de protection contre le vol de smartphones, compte tenu des exigences générales décrites par la Global System Mobile Association (GSMA).

– L'Amendement 1 à la Recommandation X.1197, *Lignes directrices relatives aux critères de sélection d'algorithmes cryptographiques pour la protection de service et de contenu de TVIP,* est une mise à jour des Appendices I et II visant à rendre compte de l'état actuel de la technique en août 2019, y compris des références bibliographiques.

– La Recommandation X.1331, *Lignes directrices relatives à la sécurité des dispositifs des réseaux domestiques (HAN) dans les réseaux électriques intelligents,* fournit une analyse des menaces auxquelles sont exposés les réseaux HAN dans les réseaux électriques intelligents, les exigences de sécurité et les fonctions de sécurité. Le rôle et les fonctions de chaque dispositif HAN étant différents, les exigences de sécurité et les fonctions de sécurité sont fournies pour chaque dispositif.

– La Recommandation X.1332*, Lignes directrices relatives à la sécurité des services de compteurs intelligents dans les réseaux électriques intelligents,* fournit des lignes directrices relatives à la sécurité des services de compteurs intelligents, afin de permettre aux fournisseurs de services de mettre en œuvre les mesures de sécurité appropriées pour garantir la sécurité de leurs services. Elle analyse le modèle général du service de compteurs intelligents du point de vue du niveau de service. À partir de ce modèle général, cette Recommandation examine les menaces de sécurité et les méthodes d'attaque contre les services de compteurs intelligents et définit les exigences de sécurité et les capacités permettant de faire face à ces attaques. En outre, cette Recommandation présente des normes de sécurité utiles qui peuvent être prises en considération lorsque le fournisseur de services met en œuvre les capacités de sécurité.

– La Recommandation X.1333, *Lignes directrices sur la sécurité pour l'utilisation d'outils d'accès à distance dans les systèmes de contrôle connectés à l'Internet*, décrit un ensemble de mesures visant à promouvoir l'utilisation des outils d'accès à distance (RAT) en toute sécurité pour les activités de surveillance, de contrôle et de maintenance.

– La Recommandation X.1361, *Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle,* décrit un cadre de sécurité applicable à l'Internet des objets (IoT) qui s'appuie sur des passerelles de sécurité. L'IoT est une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution. Cette Recommandation analyse les menaces et les problèmes de sécurité dans l'environnement de l'IoT et décrit les capacités qui pourraient permettre d'y faire face et de les atténuer. Elle présente une méthode générale permettant de déterminer quelles capacités de sécurité sont requises pour faire face à ces menaces et à ces problèmes et les atténuer dans le cadre de l'IoT.

– La Recommandation X.1362*, Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT),* définit la procédure de chiffrement avec données de gabarit associées (EAMD) pour les dispositifs de *l'Internet des objets (*IoT). Elle décrit la procédure EAMD et la façon dont elle assure un ensemble de services de sécurité pour le trafic qui utilise cette procédure.

– La Recommandation X.1363*, Cadre technique applicable au traitement des informations d'identification personnelle* *(PII) dans l'environnement de l'Internet des objets (*IoT),définit un cadre technique applicable au traitement des informations PII dans l'environnement de l'IoT avec un ou plusieurs fournisseurs de services.

– La Recommandation X.1364*, Exigences et cadre de sécurité applicables à l'Internet des objets à bande étroit,* indique les menaces pour la sécurité et les exigences de sécurité propres aux déploiements de l'IoT à bande étroite et établit un cadre de sécurité permettant aux opérateurs de protéger ces nouvelles applications technologiques.

– La Recommandation X.1365*, Méthode de sécurité applicable à l'utilisation de la cryptographie fondée sur l'identité à l'appui des services de l'Internet des objets fournis sur les réseaux de télécommunication,* décrit une méthode de sécurité applicable à l'utilisation de la technologie IBC de clé publique à l'appui des services IoT fournis sur les réseaux de télécommunication, y compris les mécanismes de gestion de l'identité, l'architecture de gestion des clés, les opérations de gestion des clés et l'authentification.

– La Recommandation X.1366*, Système d'authentification de messages agrégés pour l'environnement de l'Internet des objets,* définit deux systèmes d'authentification de messages. Le premier est un système d'authentification de messages agrégés (AMA) pour l'IoT en tant que mécanisme de base, tandis que le second est un système interactif d'authentification de messages agrégés (IAMA) doté d'un protocole interactif qui fonctionne de manière simple et sûre. Ces deux systèmes d'authentification de messages agrégés permettent d'assurer "l'authentification (de l'identité) des entités" ainsi que "l'authentification des messages".

– La Recommandation X.1367*, Format normalisé de journaux d'erreurs pour l'Internet des objets aux fins de la gestion des incidents de sécurité*, décrit un format de journal d'erreur normalisé qui peut être placé dans une charge utile de protocole, comme syslog (voir la norme IETF RFC 5424), afin de convertir les informations relatives au journal d'erreur provenant d'un dispositif d'extrémité dans le format normalisé de journal d'erreur. Cette Recommandation définit aussi un tableau normalisé de codes d'erreur qui permet de résoudre le second problème. De cette manière, les incidents de sécurité qui se produisent dans les réseaux informatiques et les réseaux de dispositifs d'extrémité de l'IoT peuvent être gérés dans leur intégralité.

– La Recommandation X.1368, *Mise à jour sécurisée des micrologiciels ou des logiciels des dispositifs de l'Internet des objets,* définit: 1) des modèles et des procédures de base pour la mise à jour sécurisée des micrologiciels ou des logiciels (FW/SW) des dispositifs de l'Internet des objets (IoT); et 2) les exigences et les capacités relatives à la mise à jour des micrologiciels de l'IoT.

– La Recommandation X.1369, *Exigences de sécurité pour la plate-forme de services IoT*, indique les exigences de sécurité applicables à la plate-forme de services de l'IoT. Elle permet d'évaluer les menaces et les problèmes de sécurité pour la plate-forme de services commerciaux IoT et décrit les mesures de sécurité permettant d'atténuer ces menaces et ces problèmes.

– La Recommandation X.1453, *Menaces et exigences de sécurité pour les systèmes de gestion vidéo*, contient une analyse des menaces de sécurité pour les systèmes de gestion vidéo (VMS) fondés sur la plate-forme de serveur fonctionnant sur un réseau IP et indique les exigences de sécurité permettant de remédier aux menaces de sécurité recensées.

– La Recommandation X.1811, *Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT*‑*2020*, identifie les menaces que l'informatique quantique fait peser sur les systèmes des Télécommunications mobiles internationales 2020 (IMT-2020) sur la base d'une évaluation du niveau de sécurité des algorithmes cryptographiques actuellement utilisés. Elle passe brièvement en revue les algorithmes à l'épreuve des attaques quantiques, de type symétrique ou asymétrique, et énonce des lignes directrices relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT-2020.

– Supplément 26, Corr. 1, aux Recommandations UIT-T de la série X *– 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*.

g) Question 7/17: Services applicatifs sécurisés

Le groupe chargé de la Question 7/17 élabore des Recommandations sur les exigences de sécurité relatives aux services applicatifs sécurisés, par exemple les services à valeur ajoutée et les services des technologies financières.

Au cours de l'actuelle période d'études, neuf nouvelles Recommandations ont été élaborées au titre de la Question 7/17:

– La Recommandation X.1145, *Cadre et exigences de sécurité pour les capacités ouvertes des services de télécommunication*, porte essentiellement sur une analyse des exigences de sécurité pour les capacités ouvertes des services de télécommunication et définit un cadre de sécurité.

– La Recommandation X.1146, *Lignes directrices pour garantir la protection des services à valeur ajoutée fournis par les opérateurs de télécommunication*,propose des lignes directrices pour garantir la protection des services à valeur ajoutée fournis par les opérateurs de télécommunication. Cette Recommandation analyse les scénarios de service types, les menaces pour la sécurité et les méthodes d'attaque, et définit aussi des mesures techniques pour lutter contre les menaces et les attaques, afin d'aider les opérateurs à garantir la sécurité des services à valeur ajoutée et de protéger les intérêts des utilisateurs.

– La Recommandation X.1147, *Exigences de sécurité et cadre pour l'analyse des mégadonnées dans les services Internet sur mobile*, renfermera une analyse des exigences de sécurité relatives à l'analyse des mégadonnées dans les services Internet sur mobile et une définition d'un cadre de sécurité.

– La Recommandation X.1148, *Cadre applicable au processus de désidentification à l'intention des fournisseurs de services de télécommunication*,décrit uncadre applicable au processus de désidentification comportant des mesures opérationnelles, et indique les

 modèles de diffusion des données ainsi que les différentes étapes du processus de désidentification des données à l'intention des fournisseurs de services de télécommunication, sur la base du modèle de cycle de vie des données et du rôle des parties prenantes.

– La Recommandation X.1149, *Cadre de sécurité d'une plate-forme ouverte pour les services des technologies financières,* décrit une architecture de plate-forme ouverte pour les services des technologies financières (FinTech). Elle précise en outre les menaces et les vulnérabilités relatives à la plate-forme ouverte et la procédure d'utilisation de l'interface de programmation d'application (API) ouverte pour les services des technologies financières. Elle indique également les différentes exigences de sécurité relatives à la plate-forme ouverte des services des technologies financières, en ce qui concerne les sociétés du secteur financier et les sociétés du secteur des technologies financières. L'Appendice de cette Recommandation présente certains cas d'utilisation de la plate-forme ouverte proposée.

– La Recommandation X.1450, *Lignes directrices sur les mécanismes d'authentification hybride et de gestion de clés dans le modèle client-serveur,* fournit des lignes directrices relatives aux mécanismes d'authentification hybride et d'échange de clés dans le modèle client-serveur. Le mécanisme sous-jacent propose d'utiliser des secrets partagés et de techniques de clé publique pour l'authentification et l'échange de clés. Cette Recommandation traite des scénarios de service, des menaces pour la sécurité et des méthodes permettant d'atténuer les effets de ces attaques*.*

– La Recommandation X.1451, *Identification des risques pour optimiser l'authentification,* décrit une fonction d'identification des risques dans un système de services TIC destinée à assurer un traitement préalable avant que la fonction d'authentification ne soit invoquée. Elle permet au système de services TIC d'optimiser l'authentification de l'utilisateur en fonction des risques identifiés. Cette fonction spécifique d'identification des risques permet au système de services TIC d'opter pour un mécanisme d'authentification en fonction de l'utilisateur et offre plusieurs avantages: 1) amélioration de l'expérience de l'utilisateur; 2) augmentation de la capacité et diminution du coût de l'authentification de l'utilisateur par transaction; et 3) réduction du risque de falsification de l'identité de l'utilisateur.

– La Recommandation X.1452, *Lignes directrices relatives aux services de sécurité fournis par les opérateurs*, classifie les cas d'utilisation potentiels des services de sécurité fournis par des opérateurs et renferme une analyse des exigences particulières applicables aux services de sécurité: Elle fournit ainsi des lignes directrices permettant aux opérateurs de protéger et d'améliorer leurs services de sécurité.

– La Recommandation X.1470, *Lignes directrices relatives à la sécurité des services à la clientèle en ligne fondés sur le web*, contient une analyse des menaces de sécurité des services à la clientèle en ligne fondés sur le web sous trois aspects: sécurité du réseau, sécurité du système et sécurité du service. Elle contient des lignes directrices relatives à la sécurité des services à la clientèle en ligne fondés sur le web et définit les mesures de sécurité correspondantes. Elle propose également des procédures de test permettant de vérifier la conformité des mesures de sécurité correspondantes aux exigences de sécurité définies.

h) Question 8/17: Sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées

Le Groupe chargé de la Question 8/17 élabore des Recommandations sur les menaces pour la sécurité et les exigences de sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées.

Au cours de l'actuelle période d'études, huit nouvelles Recommandations ont été élaborées au titre de la Question 8/17.

– La Recommandation X.1603, *Exigences de sécurité des données pour le service de surveillance de l'informatique en nuage,* analyse les exigences de sécurité des données pour le service de surveillance de l'informatique en nuage et traite notamment des exigences relatives à la portée des données de surveillance, du cycle de vie des données de surveillance, des exigences de sécurité concernant l'acquisition des données de surveillance et des exigences de sécurité concernant le stockage des données de surveillance.

– La Recommandation X.1604, *Exigences de sécurité relatives au réseau en tant que service (NaaS) dans l'informatique en nuage,* analyse les menaces et les problèmes de sécurité concernant le réseau en tant que service (NaaS) dans l'informatique en nuage, et précise les exigences de sécurité relatives aux aspects du NaaS, à savoir les applications NaaS, les plates-formes NaaS et la connectivité NaaS, sur la base des types de capacités de nuage correspondants.

– La Recommandation X.1605, *Exigences de sécurité pour les infrastructures publiques en tant que service (IaaS) dans l'informatique en nuage,* vise à fournir des informations concernant les exigences de sécurité pour les infrastructures IaaS publiques, afin d'aider les fournisseurs d'infrastructures IaaS à améliorer la sécurité des plates-formes IaaS au cours des étapes de planification, de construction et d'exploitation.

– La Recommandation X.1606, *Exigences de sécurité pour l'environnement des applications de "communication en tant que service",* recense les menaces de sécurité et contient des recommandations concernant les exigences de sécurité pour l'environnement des applications de communication en tant que service (CaaS). La Recommandation décrit les scénarios et les caractéristiques des applications CaaS dotées de capacités de multicommunication. Elle recense en outre les menaces qui découlent des caractéristiques uniques des applications CaaS et contient des recommandations relatives aux exigences de sécurité appropriées pour les applications CaaS.

– La Recommandation X.1643, *Exigences et lignes directrices sur la sécurité des conteneurs de virtualisation dans un environnement utilisant l'informatique en nuage*, contient une analyse des menaces et des problèmes de sécurité concernant les conteneurs de virtualisation dans un environnement utilisant l'informatique en nuage et décrit un cadre de référence assorti de lignes directrices relatives à la sécurité pour les conteneurs de virtualisation dans le nuage.

– La Recommandation X.1750, *Lignes directrices relatives à la sécurité des "mégadonnées en tant que service" pour les fournisseurs de services de mégadonnées*, analyse les problèmes de sécurité que rencontrent les mégadonnées en tant que service (BDaaS) et définit les rôles et les responsabilités liés à la sécurité dans la fourniture des services BDaaS, ainsi qu'un cadre de sécurité applicable à une infrastructure de mégadonnées. Elle précise en outre les mesures de protection de la sécurité à respecter pour les services et les composantes associés aux services BDaaS.

– La Recommandation X.1751, *Lignes directrices relatives à la sécurité pour la gestion du cycle de vie des mégadonnées par les opérateurs de télécommunication*, analyse les failles de sécurité et expose des lignes directrices relatives à la sécurité de la gestion du cycle de vie des mégadonnées par les opérateurs de télécommunication. On y trouvera une description de certaines caractéristiques des services de mégadonnées et des catégories de données de télécommunication, une analyse des failles de sécurité de la gestion du cycle de vie des mégadonnées ainsi que des lignes directrices à l'intention des opérateurs de télécommunication.

– La Recommandation X.1752, *Lignes directrices sur la sécurité pour l'infrastructure et la plate-forme de mégadonnées*, contient une analyse des menaces et des problèmes de sécurité concernant l'infrastructure et la plate-forme de mégadonnées et décrit un cadre de référence pour la mise en correspondance des lignes directrices sur la sécurité et des menaces recensées pour l'infrastructure et la plate-forme de mégadonnées.

– Le rapport technique TR.XAASL, *Cadre pour la normalisation de la sécurité des services virtualisés,* est un document pour examen qui porte sur l'établissement de considérations, d'exigences et de cadres normatifs pour les services virtualisés.

i) Question 9/17: Télébiométrie (2017-2020)

Le Groupe chargé de la Question 9/17 élabore des Recommandations sur la télébiométrie pour authentifier les utilisateurs à l'aide de la télébiométrie et pour protéger les informations télébiométriques contre l'accès non autorisé.

Pendant l'actuelle période d'études, trois nouvelles Recommandations, une Recommandation révisée et un corrigendum ont été élaborés au titre de la Question 9/17:

– La Recommandation X.1080.0 et X.1080.0 Cor.1, *Contrôle d'accès pour la protection des données télébiométriques,* indique comment protéger les informations télébiométriques contre l'accès non autorisé. Elle adopte un point de vue orienté services, selon lequel seules les informations nécessaires pour un but particulier sont fournies, c'est-à-dire que l'accès est accordé non seulement en fonction du droit de savoir, mais aussi en fonction du besoin de savoir. Cette Recommandation définit essentiellement une spécification d'attribut incluse dans un certificat d'attribut ou de clé publique qui décrit en détail les privilèges dont une entité particulière dispose pour un ou plusieurs types de service. La sécurité est assurée grâce à l'utilisation d'un profil de la syntaxe de message cryptographique (CMS). Le profil CMS permet d'assurer l'authentification, l'intégrité et, si nécessaire, la confidentialité (chiffrement). Il est destiné à fournir un appui en matière de sécurité pour les spécifications télébiométriques en général. Ce profil repose sur l'hypothèse et la condition du déploiement correct d'une infrastructure de clé publique (PKI). Cette Recommandation dépend aussi du déploiement d'une infrastructure de gestion des privilèges (PMI).

– La Recommandation X.1080.1 (révisée), *Cybersanté et systèmes mondiaux de télémédecine – Protocole générique de télécommunication,* définit le cadre pour les autres parties de la série de Recommandations UIT-T 1080.x en établissant le modèle global pour les aspects de la télébiométrie liés aux communications. Elle présente l'attribution de base des identificateurs d'objet pour identifier de manière univoque les informations lors du transfert de données et définit un protocole de télécommunication générique. Elle décrit une technique de spécification formelle des objets et définit un protocole générique prenant en charge les interactions entre une station médicale située à proximité du domicile d'un patient et un centre médical distant offrant de meilleures compétences. Ce protocole doit être utilisé et étendu par d'autres parties de la série de Recommandations UIT-T X.1080.x.

– La Recommandation X.1093, *Contrôle d'accès télébiométrique au moyen de cartes d'identification intelligentes*, décrit le mécanisme général de contrôle d'accès logique et/ou physique au moyen de cartes biométriques. Elle peut s'appliquer au tout nouveau domaine de la gestion d'accès nécessitant un contrôle d'accès physique et logique sécurisé.

– La Recommandation X.1094, *Authentification télébiométrique utilisant des biosignaux,* décrit de nouvelles méthodes d'authentification télébiométrique robuste et sécurisée utilisant des biosignaux.

j) Question 10/17: Architecture et mécanismes de gestion d'identité (2017‑2020)/Architecture et mécanismes de gestion des identités et de télébiométrie (2021-)

Le groupe chargé de la Question 10/17 élabore des Recommandations sur les sujets de gestion d'identité, y compris les cadres d'authentification. En janvier 2021, il a repris les travaux en cours sur la télébiométrie qui étaient menés auparavant au titre de la Question 9/17.

Pendant l'actuelle période d'études, cinq nouvelles Recommandations, deux Recommandations révisées et un nouveau Supplément ont été élaborés au titre de la Question 10/17:

– La Recommandation X.1080.2, *Protocole biologie-machine (B2M)*, définit un protocole général pour l'échange d'informations biométriques entre les équipements du patient et les équipements du médecin spécialiste pour qu'un centre médical puisse suivre un patient à distance et obtenir des informations en provenance de ce patient.

– La Recommandation X.1252 (révisée), *Termes et définitions de base relatifs à la gestion d'identité*, définit les principaux termes utilisés dans le domaine de la gestion d'identité (IdM). Ces termes, qui proviennent de nombreuses sources, sont tous employés couramment dans les travaux relatifs à la gestion d'identité. L'objectif de cette Recommandation n'est pas de proposer un recueil exhaustif de termes associés à la gestion d'identité. En revanche, les termes qui y sont définis sont limités à ceux considérés comme formant une liste de base des termes les plus importants et les plus couramment utilisés dans le domaine de la gestion d'identité. L'Annexe A de cette Recommandation contient des explications relatives à certains de ces termes clés.

– La Recommandation X.1254 (révisée), *Cadre de garantie d'authentification des entités*, définit trois niveaux de garantie d'authentification des entités (AAL) ainsi que les critères et menaces correspondant à chacun d'eux.

En outre, cette Recommandation:

• établit un cadre de gestion des niveaux de garantie AAL;

• fournit, d'après une évaluation des risques, des orientations concernant les techniques de contrôle à utiliser pour réduire les menaces qui pèsent sur l'authentification;

• donne des orientations relatives à l'application des trois niveaux AAL à d'autres systèmes de garantie d'authentification; et

• donne des orientations quant à l'échange des résultats d'authentification reposant sur les trois niveaux AAL.

– La Recommandation X.1276, *Protocole d'amélioration de l'authentification et métadonnées – Version 1.0*, propose des modèles architecturaux simples de renforcement de la confiance démontrant l'utilisation du renforcement de la confiance dans les architectures modernes de contrôle d'accès, décrit un ensemble commun de métadonnées, des mécanismes et des éléments de protocole pour les échanges d'informations en vue du renforcement de la confiance et encourage l'utilisation d'éléments de renforcement de la confiance pour faciliter la normalisation parmi les nombreuses technologies et approches actuellement utilisées pour atténuer les risques concernant les justificatifs et l'authentification.

– La Recommandation X.1277, *Cadre d'authentification universelle,* décrit le cadre d'authentification universelle (UAF) FIDO qui, pour les services en ligne et les sites web, que ce soit sur l'Internet ouvert ou au sein des entreprises, permet de tirer parti en toute transparence des fonctions de sécurité natives des dispositifs informatiques des utilisateurs finals pour assurer une authentification forte des utilisateurs et d'atténuer les problèmes associés à la création et à la mémorisation de nombreux identifiants en ligne.

– La Recommandation X.1278, *Protocole client-authentificateur/Cadre applicable au double facteur universel,* décrit un protocole de couche d'application pour la communication entre un authentificateur externe et un autre client/plate-forme, ainsi que les liens entre ce protocole d'application et divers protocoles de transport utilisant différents supports physiques.

– La Recommandation X.1279, *Cadre de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité,* fournit un cadre architectural pour l'authentification renforcée utilisant la télébiométrie et la détection d'usurpation d'identité. Cette Recommandation vise à analyser les menaces concernant les solutions traditionnelles d'authentification télébiométrique et définit un cadre architectural de même que les flux de processus d'authentification et les aspects liés à la sécurité de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité.

– Le Supplément 35 aux Recommandations de la série X – *Supplément à la Recommandation UIT-T X.1254 – Supplément sur les cas d'utilisation du cadre de garantie d'authentification des entités (EAA)*, expose trois cas d'utilisation relatifs à l'application du cadre de garantie d'authentification des entités lors de la mise en œuvre de la sécurité, y compris des considérations de sécurité détaillées dans l'évaluation des risques, le choix du niveau de garantie approprié et la sélection des technologies d'authentification.

La CE 17 a convenu, lors de sa séance plénière électronique du 29 mai 2020, d'attribuer le numéro X.1261 à la Recommandation UIT-T D.1140, *Cadre politique intégrant des principes applicables à l'infrastructure d'identité numérique*, pour qu'elle fasse partie des Recommandations UIT-T de la série D et des Recommandations UIT-T de la série X sur la gestion d'identité possédant un double numéro.

k) Question 11/17: Technologies génériques (Annuaire, infrastructure de clé publique (PKI), infrastructure de gestion des privilèges (PMI), notation de syntaxe abstraite numéro un (ASN.1), identificateurs d'objet (OID)) utilisées pour les applications sécurisées (2017-2020)/Technologies génériques (Annuaire, infrastructure de clé publique (PKI), langages formels et identificateurs d'objets par exemple) utilisées pour les applications sécurisées (2021-)

Le groupe chargé de la Question 11/17 élabore des Recommandations sur les services et systèmes d'annuaire, y compris les certificats d'attributs et de clés publiques dans les Recommandations de la série X.500. 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, système d'identification mondial basé sur des autorités d'enregistrement hiérarchiques, appelé "arborescence des identificateurs d'objet". En janvier 2021, le groupe chargé de la Question 11/17 a repris les travaux en cours sur les langages menés auparavant au titre de la Question 12/17.

Pendant l'actuelle période d'études, 5 nouvelles Recommandations, 20 Recommandations révisées, un Amendement et 14 Corrigenda techniques ((X.680 Cor.1, X.680 Cor.2, X.680 Amd.1, X.680 Cor.3, X.681 Cor.1, X.682 Cor.1, X.682 Cor.2, X.683 Cor.1, X.693 Cor.1, X.694 Cor.1, X.696 Cor.1, X.696 Cor.2, X.696 Cor.3, X.893 Cor.1, X.894 Cor.1) aux Recommandations des séries X.500-, X.680-, et X.690-, un Supplément et un nouveau Rapport technique ont été élaborés au titre de la Question 11/17:

– La Recommandation UIT‑T X.500 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services*, 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.

– La Recommandation UIT‑T X.501 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles*, décrit 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.

– L'Amendement 1 à la Recommandation X.501, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles*, met à jour le § 9.2 et l'Annexe A.

– La 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*, 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 indique 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 énonce 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.

– Le Corrigendum 1 à la Recommandation X.509, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadres pour les certificats de clé publique et d'attribut*, vise à corriger des erreurs au § 6.2.2 et dans l'Annexe B.

– La Recommandation X.510, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire:* *spécifications de protocole pour assurer des opérations sécurisées*, définit un protocole général, appelé protocole enveloppe, qui assure la cybersécurité des protocoles conçus pour la protection du protocole enveloppe en assurant l'authentification, l'intégrité et, à titre facultatif, la confidentialité (chiffrement). Le protocole enveloppe permet d'assurer la cybersécurité indépendamment des protocoles protégés, ce qui signifie que la sécurité peut être renforcée sans influer sur la spécification du protocole protégé.

– La Recommandation UIT‑T X.511 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: définition de service abstrait*, 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.

– La Recommandation UIT‑T X.518 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: procédures pour le fonctionnement réparti*, indique 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.

– La Recommandation UIT‑T X.519 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécification des protocoles*, indique 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 indiqués 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.

– La Recommandation UIT-T X.520 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attributs sélectionnés*, 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.

– La Recommandation UIT-T X.521 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: classes d'objets sélectionnées*, 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 indique les types d'attributs se rapportant aux objets de cette classe. La définition d'une forme de nom indique les attributs à utiliser pour former les noms des objets d'une classe donnée.

– La Recommandation UIT-T X.525 (révisée), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: duplication*, décrit 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.

– La Recommandation X.676, *Cadre de résolution basé sur les identificateurs d'objet pour les services groupés de l'IoT*, décrit un cadre de résolution basé sur les identificateurs d'objet (OID) permettant d'identifier différents services dans les environnements IoT. L'identificateur OID est un identificateur qui permet de nommer un objet avec un espace de noms attribué de façon hiérarchique. Dans l'Internet des objets (IoT), des milliers de services IoT basés sur des ressources hétérogènes seront fournis en tant que combinaisons de divers services. Dans un souci d'efficacité, diverses technologies, par exemple le rattachement au service, les services dynamiques ou les services à commutation fréquente, seront nécessaires, ainsi que la résolution et l'identification des services groupés. Cette Recommandation décrit les concepts de services groupés de l'IoT, les considérations, les architectures et les procédures relatives à un cadre de résolution basé sur l'IoT pour les services groupés l'IoT.

– La Recommandation X.677, *Mécanisme d'identification des aéronefs sans pilote à l'aide d'identificateurs d'objet*, analyse les exigences en matière de gestion du cycle de vie complet et de reconnaissance de l'identité d'exploitation des aéronefs sans pilote (UAV) et aborde les considérations relatives à la sécurité. Elle contient en outre les spécifications d'un mécanisme d'identification des aéronefs sans pilote au moyen d'identificateurs d'objet (OID), y compris les spécifications détaillées des règles d'attribution et des procédures d'enregistrement des identificateurs d'objet utilisés pour les aéronefs sans pilote.

– La Recommandation X.680 (révisée) (et son Amendement 1 ainsi que ses Corrigenda 1 à 3 avant la révision), *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1): – Spécification des objets informationnels,* fournit une notation dite notation de syntaxe abstraite numéro un (ASN.1) pour la définition de la syntaxe de données informationnelles. Elle définit un certain nombre de types de donnée simples et indique une notation pour y faire référence et en préciser les valeurs.

– La Recommandation X.681 (révisée) (et son Corrigendum 1 avant la révision), *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1): – Spécification des objets informationnels,* fournit 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. Une classe d'objets informationnels définit la forme d'un tableau conceptuel (un ensemble d'objets informationnels), une colonne étant attribuée à chaque champ de la classe d'objets informationnels, et chaque ligne complète définissant un objet informationnel.

– La Recommandation X.682 (révisée) (et son Corrigendum 2 avant la révision), *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1): spécification des contraintes*, décrit la notation ASN.1 à utiliser, dans le cas général, pour indiquer les contraintes et les exceptions par lesquelles on peut limiter les valeurs d'un type de données structuré. La notation permet aussi de signaler les cas de transgression d'une contrainte.

– La Recommandation X.683 (révisée) (et son Corrigendum 1 avant la révision), *Technologies de l'information – Notation de syntaxe abstraite numéro un(ASN.1): paramétrage des spécifications de la notation de syntaxe abstraite numéro un*, 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 de côté à certains stades du développement et sont définis ultérieurement pour aboutir à la définition complète d'une syntaxe abstraite.

– La Recommandation X.690 (révisée), *Technologies de l'information – Règles de codage de la notation de syntaxe abstraite numéro un(ASN.1): spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER),* définit un ensemble de règles de codage de base (BER) applicables aux valeurs des types définis au moyen de la notation ASN.1. L'application de ces règles de codage produit une syntaxe de transfert pour de telles valeurs. Il est implicitement entendu que ces règles de codage servent également au décodage. Cette Recommandation | Norme internationale définit également un ensemble de règles de codage distinctives (DER) et un ensemble de règles de codage canoniques (CER) qui permettent d'imposer des contraintes aux règles de codage de base (BER). La principale différence entre ces deux ensembles de règles est que les DER utilisent un codage de longueur définie alors que les CER utilisent un codage de longueur indéfinie. Les DER sont mieux adaptées au codage des petites valeurs, et les CER à celui des grandes valeurs. Il est implicitement entendu que ces règles de codage servent également au décodage.

– La Recommandation X.691 (révisée), *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact (PER)*, 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 Recommandation UIT‑T X.690 | ISO/CEI 8825-1).

– La Recommandation X.692 (révisée), *Technologies de l'information – Règles de codage ASN.1:* *spécification de la notation de contrôle de codage (ECN),* définit la notation de contrôle de codage (ECN) utilisée afin de décrire 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).

– La Recommandation X.693 (révisée) (et son Corrigendum 1 avant la révision), *Technologies de l'information – Règles de codage ASN.1:* *règles de codage XML (XER)*, indique les règles de codage utilisant le langage de balisage extensible (XML) applicables aux valeurs de types ASN.1.

– La Recommandation X.694 (révisée) (et son Corrigendum 1 avant la révision), *Technologies de l'information – Règles de codage ASN.1:* *mappage en ASN.1 des définitions de schéma XML du W3C,* définit des règles pour le mappage d'un schéma XSD (schéma conforme à la spécification du schéma XML du W3C) en un schéma ASN.1 (notation de syntaxe abstraite numéro un) , 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 (DER), les règles de codage compact (PER) ou les règles de codage XML (XER) pour le transfert des informations définies par le schéma XSD.

– La Recommandation X.695 (révisée), *Technologies de l'information – Règles de codage ASN.1:* *enregistrement et application des instructions de codage PER,* décrit les règles permettant d'appliquer des instructions de codage PER en utilisant des préfixes de type ou une section de contrôle de codage. Les instructions de codage permettent de modifier les codages de types ASN.1 pour certaines règles de codage spécifiées (dans ce cas PER). Elles peuvent être insérées dans une spécification ASN.1 entre crochets (à l'instar de l'étiquette utilisée dans les règles de codage de base, BER) immédiatement avant le type concerné (préfixes de type), ou rassemblées à la fin d'un module ASN.1 (section de contrôle de codage).

– La Recommandation X.696 (révisée) (et ses Corrigenda 1 à 3 avant la révision), *Technologies de l'information – Règles de codage ASN.1: Spécification des règles de codage des octets (OER),* indique 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).

– La Recommandation X.697, *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de la notation des objets Javascript (JER),* définit un ensemble de règles de codage de la notation des objets Javascript (JER) pouvant servir à produire une syntaxe de transfert pour des valeurs des types définis dans les Recommandations UIT-T X.680 | ISO/CEI 8824-1, UIT-T X.681 | ISO/CEI 8824-2, UIT-T X.682 | ISO/CEI 8824-3 et UIT-T X.683 | ISO/CEI 8824-4. Il est implicitement entendu que ces règles de codage servent également au décodage.

– Le Corrigendum 1 à la Recommandation X.893, *Technologies de l'information –* *Applications génériques de l'ASN.1: sécurité Fast Infoset,* a pour objet d'apporter des corrections aux annexes informatives et à la bibliographie afin de supprimer les références à l'algorithme triple DES obsolète.

– La Recommandation X.894 et ses Corrigenda 1 et 2, *Technologies de l'information – Applications génériques de l'ASN.1 – Syntaxe de message cryptographique*, contient des modules de notation de syntaxe abstraite numéro un (ASN.1) pour l'utilisation de la syntaxe de message cryptographique dans les Recommandations UIT-T. La syntaxe de message cryptographique (CMS) définit les services d'intégrité, de confidentialité, d'authenticité de l'origine et de non-répudiation des données, nécessaires pour échanger des informations de manière fiable et assurer une authentification forte. Elle contient en outre un ensemble de techniques de gestion des clés de chiffrement utilisées pour prendre en charge des mécanismes souples d'établissement de clés, comme la gestion de clé constructive, la concordance de clés, les échanges de clés, et le chiffrement à mot de passe. Ces techniques peuvent être utilisées pour éviter les fraudes et pour protéger les informations d'identification personnelles et d'autres informations sensibles. Cette Recommandation | Norme internationale prend en charge les techniques de signature numérique, de chiffrement et de chiffrement avec signature reposant sur les technologies de clé publique définies dans les Recommandations UIT-T de la série X.500 | les différentes parties de la norme ISO/CEI 9594. Toutes les règles de codage normalisées pour la notation ASN.1 sont prises en charge.

– La Recommandation Z.161 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): langage noyau de TTCN-3,* 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.

– La Recommandation Z.161.2 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage TTCN-3: prise en charge de la configuration et du déploiement,* 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). La notation TTCN-3 peut servir à la spécification de tous les types de test de systèmes réactifs, effectués en divers ports de communication.

– La Recommandation Z.161.3 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage TTCN-3:* *paramétrage évolué,* définit le paquetage "paramétrage évolué" 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.

– La Recommandation Z.161.4 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage TTCN-3: types de comportement,* définit le paquetage "types de comportement" 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.

– La Recommandation Z.161.7 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage TTCN-3:* *caractéristiques orientées objet,* définit la prise en charge de caractéristiques orientées objet dans 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.

– La Recommandation 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,* définit une façon normative d'utiliser la notation de syntaxe abstraite numéro un (ASN.1) définie dans les Recommandations UIT-T X.680, UIT-T X.681, UIT-T X.682 et UIT-T X.683 avec la notation TTCN-3.

– La Recommandation Z.168 (révisée), *Notation de test et de commande de test version 3 (TTCN-3):* *Mappage du langage IDL vers la notation TTCN-3,* définit les règles de mappage du langage de définition d'interface (IDL) de l'architecture de courtier commun de requête sur des objets (CORBA) 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. Les principes de ce mappage peuvent aussi être employés pour le mappage des langages de spécification d'interface d'autres technologies fondées sur les objets ou sur les composants.

– La Recommandation Z.169 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): utilisation des schémas XML avec TTCN-3*, définit les règles de mappage du schéma du World Wide Web Consortium (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 Recommandation Z.171 révisée, *Notation de test et de commande de test version 3 (TTCN-3): utilisation de la notation JSON avec la notation TTCN-3,* indique les règles à utiliser pour définir des schémas pour les structures de données JSON en notation TTCN-3 et permettre de tester les systèmes, interfaces et protocoles basés sur la notation JSON, ainsi que les règles de conversion entre la notation TTCN-3 et la notation JSON pour pouvoir échanger des données TTCN-3 au format JSON entre différents systèmes.

– Le Supplément 31 aux Recommandations de la série X – Supplément à la Recommandation UIT-T X.660 *– Lignes directrices relatives à l'utilisation des identificateurs d'objet pour l'Internet des objets*, fournit des lignes directrices sur la façon d'utiliser les identificateurs d'objet (OID) pour identifier les objets dans l'Internet des objets (IoT). Il comprend des lignes directrices sur la manière de structurer les OID, de mettre en œuvre des systèmes de résolution et d'établir des procédures de gestion fondées sur les Recommandations de l'UIT-T et les normes internationales existantes.

– Le document technique XSTP-OID-ORS, *Système de résolution des identificateurs OID: Problèmes, exigences et solutions possibles*, met en évidence les problèmes, les exigences et les solutions possibles pour la résolution des identificateurs OID. Au nombre des problèmes figurent la qualité de fonctionnement au niveau local et la résolution globale des sous-arborescences manquantes des identificateurs OID. Les exigences techniques relatives aux solutions possibles sont également examinées. Enfin, des solutions techniques possibles et des orientations d'ordre administratif et opérationnel sont fournies.

– Le Guide de mise en œuvre Z.Imp100 (révisé), *Guide de mise en œuvre du langage de description et de spécification – Version 4.0.1,* est une compilation deserreurs signalées et des problèmes de tenue à jour ainsi que des solutions correspondantes concernant les Recommandations UIT-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.111 et Z.119 relatives au langage de description et de spécification

l) Question 12/17: Langages formels pour les logiciels de télécommunication et les tests (2017-2020)

Le groupe chargé de la Question 12/17 élabore des Recommandations sur les langages formels (par exemple SDL, MSC, URN) pour définir les exigences, l'architecture et le comportement des systèmes de télécommunication: langages pour les besoins, langages de spécification et de mise en œuvre. De plus, le groupe chargé de la Question 12/17 élabore des Recommandations sur les langages pour les tests (par exemple TTCN-3) comme moyen pour assurer l'interopérabilité et la conformité.

Pendant l'actuelle période d'études, trois nouvelles Recommandations, 64 Recommandations révisées et deux guides de mise en œuvre révisés ont été élaborés au titre de la Question 12/17:

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

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

– La Recommandation UIT-T Z.100, Annexe F2 (révisée), *Définition formelle du langage SDL‑2010: Sémantique statique*, 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.

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

– La Recommandation UIT-T Z.101 (révisée), *Langage de description et de spécification – Langage SDL-2010 de base*, 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.

– La Recommandation UIT-T Z.102 (révisée), *Langage de description et de spécification – Langage SDL-2010 complet*, 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).

– La Recommandation UIT-T Z.103 (révisée), *Langage de description et de spécification – Notation abrégée et annotation dans le langage SDL-2010,* 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.

– La Recommandation UIT-T Z.104 (révisée), *Langage de description et de spécification – Caractéristiques du langage SDL‑2010 pour les données et les actions,* 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.

– La Recommandation UIT-T Z.105 (révisée), *Langage de description et de spécification – Langage SDL-2010 combiné avec des modules ASN.1,* 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 Recommandation 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).

– La Recommandation UIT-T Z.106 (révisée), *Langage de description et de spécification – Format d'échange commun pour le langage SDL-201,0* 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.

– La Recommandation UIT-T Z.107 (révisée), *Langage de description et de spécification – Données orientées objet en SDL‑2010,* 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.

– La Recommandation Z.151 (révisée), *Notation des prescriptions utilisateur – Définition du langage*, définit la notation *des prescriptions utilisateur (*URN) à utiliser pour l'acquisition, l'analyse, la spécification et la validation des prescriptions. La notation URN associe des concepts de modélisation et des notations pour les objectifs (principalement pour des prescriptions non fonctionnelles et des attributs de qualité) et les scénarios (principalement pour des prescriptions opérationnelles, des prescriptions fonctionnelles et pour des questions de qualité de fonctionnement et d'architecture). La sous-notation des objectifs est appelée langage des prescriptions orienté objectifs (GRL) et la sous-notation des scénarios est appelée représentation des scénarios d'utilisation (UCM).

– La Recommandation UIT-T Z.161 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): langage noyau,* 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 (architecture de courtier commun de requête sur des objets) et des interfaces de programmation d'applications (API).

– La 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*,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.

– La 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,* 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 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: paramétrage évolué,* définit le paquetage "paramétrage évolué" de la notation de test et de commande de test version 3 (TTCN-3).

– La 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*, définit le paquetage "types de comportement" de la notation de test et de commande de test version 3 (TTCN-3).

– La Recommandation UIT-T Z.161.6 (nouvelle et révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: Concordance évoluée*, définit la prise en charge de la concordance évoluée pour la notation de test et de commande de test version 3 (TTCN‑3).

– La Recommandation UIT-T Z.161.7 (nouvelle et révisée), *Notation de test et de commande de test version 3 (TTCN-3): extensions du langage: caractéristiques orientées objet,* définit la prise en charge de caractéristiques orientées objet dans la notation de test et de commande de test version 3 (TTCN-3).

– La Recommandation UIT-T Z.164 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): sémantique opérationnelle*, 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.

– La Recommandation UIT-T Z.165 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): interface d'exécution*, 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). L'interface d'exécution TTCN-3 (TRI) assure l'adaptation recommandée, en ce qui concerne la synchronisation et la communication, d'un système de test à une plate-forme de traitement particulière et au système testé, respectivement. Cette Recommandation définit l'interface comme étant un ensemble d'opérations indépendantes du langage cible.

 L'interface est définie de façon à être compatible avec la Recommandation UIT-T Z.161. Cette Recommandation utilise le langage de définition d'interface (IDL) de l'architecture de courtier commun de requête sur des objets (CORBA) pour spécifier complètement l'interface TRI. Les paragraphes 6, 7 et 8 de la norme ETSI ES 201 873‑5 V4.8.1 spécifient les mappages de la spécification abstraite vers les langages cibles Java et ANSI-C. Un résumé de la spécification de l'interface employant le langage IDL est donné à l'Appendice A de la norme ETSI ES 201 873-5 V4.8.1.

 Cette révision de la Recommandation contient des modifications, des précisions et des corrections de la forme et du fond.

– La Recommandation UIT-T Z.166 (révisée), *Notation de test et de commande de test version 3 (TTCN-3): interface de commande (TCI)*, spécifie les interfaces de commande pour les implémentations de système de test en notation de test et de commande de test version 3 (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 V4.11.1). La définition d'interface utilise le langage de définition d'interface (IDL) de l'architecture de courtier commun de requête sur des objets (CORBA) pour spécifier complètement l'interface TCI. Les paragraphes 8, 9 et 9.7 de la norme ETSI ES 201 873-6 V4.11.1 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.

– La 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*, 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. L'harmonisation d'autres langages avec la notation TTCN-3 n'est pas traitée dans cette Recommandation.

 La première révision de cette Recommandation 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.

 Cette révision de la Recommandation contient des modifications, des précisions et des corrections de la forme et du fond.

– La 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*, définit les règles de mappage du langage de définition d'interface (IDL) de l'architecture de courtier commun de requête sur des objets (CORBA) 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. Les principes de ce mappage du langage IDL de l'architecture CORBA vers *la notation TTCN-3* peuvent aussi être employés pour le mappage des langages de spécification d'interface d'autres technologies fondées sur les objets ou sur les composants. La spécification des autres mappages sort du cadre de cette Recommandation. Cette révision de la Recommandation contient des modifications, des précisions et des corrections de la forme et du fond.

– La 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*, 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.

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

– La Recommandation UIT-T Z.171 (nouvelle et révisée), *Notation de test et de commande de test version 3: Utilisation de la notation JSON avec la notation TTCN-3,* indique les règles à utiliser pour définir des schémas pour les structures de données JSON en notation TTCN-3 et permettre de tester les systèmes, interfaces et protocoles basés sur la notation JSON, ainsi que les règles de conversion entre la notation TTCN-3 et la notation JSON pour pouvoir échanger des données TTCN-3 au format JSON entre différents systèmes.

– Le Guide UIT-T Z.Imp100 (révisé), *Guide de mise en œuvre du langage de description et de spécification – Version 3.0.2,* est une compilation des erreurs signalées et des problèmes de tenue à jour , ainsi que des moyens d'y remédier, concernant les Recommandations UIT-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.111 et Z.119 relatives au langage de description et de spécification

– Le Guide UIT-T Z.Imp100 (révisé), *Guide de mise en œuvre du langage de description et de spécification* – *Version 4.0.0*, est une compilation des erreurs signalées et des problèmes de tenue à jour , ainsi que des moyens d'y remédier, concernant les Recommandations UIT-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.111 et Z.119 relatives au langage de description et de spécification

m) Question 13/17: Aspects sécurité des systèmes de transport intelligents (2017‑2020)/Sécurité des systèmes de transport intelligents (ITS) (2021-)

Le groupe chargé de la Question 13/17, qui a été mise à l'étude en septembre 2017, élabore des Recommandations sur les aspects sécurité concernant les systèmes de transport intelligents (ITS). Ces Recommandations portent sur différents types de communications à bord des véhicules, entre véhicules et entre un véhicule et un emplacement fixe.

Pendant l'actuelle période d'études, six nouvelles Recommandations ont été élaborées au titre de la Question 13/17:

– La Recommandation X.1371, *Menaces pour la sécurité des véhicules connectés*, décrit les menaces pour la sécurité des véhicules connectés et l'écosystème des véhicules.

– La Recommandation X.1372, *Lignes directrices relatives à la sécurité des communications de véhicule à tout autre élément (V2X)*, fournit des lignes directrices sur la sécurité des systèmes de communication de véhicule à tout autre élément (V2X).

 Elle recense les menaces existant dans l'environnement des communications V2X et définit des exigences de sécurité pour ce type de communications, afin de réduire ces menaces. Cette Recommandation présente en outre des cas d'utilisation de communications V2X sécurisées.

– La Recommandation X.1373, *Capacité de mise à jour sécurisée des logiciels pour les dispositifs de communication des systèmes de transport intelligents*, définit des procédures de mise à jour sécurisée des logiciels entre un serveur de mise à jour de logiciels et des véhicules moyennant des contrôles de sécurité appropriés. Concrètement, les constructeurs automobiles et les entreprises s'occupant de systèmes ITS peuvent utiliser cette Recommandation comme un ensemble normalisé de capacités pour les bonnes pratiques.

– La Recommandation X.1374, *Exigences de sécurité pour les interfaces et dispositifs externes disposant d'une capacité d'accès véhicule*, renferme une analyse des menaces de sécurité qui pèsent sur les véhicules connectés et comprend deux parties: la première porte sur les menaces qui pèsent sur les interfaces utilisées pour les communications entre un véhicule et les dispositifs externes connexes, tandis que la seconde traite des menaces auxquelles sont exposés les dispositifs externes qui communiquent avec le véhicule. La Recommandation UIT-T X.1374 définit les exigences de sécurité applicables à ces interfaces et dispositifs externes disposant d'une capacité d'accès véhicule dans les environnements des réseaux de télécommunication, pour faire face aux menaces identifiées en fonction des types d'interfaces d'accès. Les interfaces et dispositifs externes dotés d'une capacité d'accès au véhicule comprennent les systèmes de téléverrouillage sans clé (RKE) au moyen d'une clé intelligente, les outils et les clés électroniques sans fil de diagnostic utilisant le port II de diagnostic embarqué (OBD-II), les unités de commande télématiques dotées de dispositifs de communication sans fil, etc.

– La Recommandation X.1375, *Lignes directrices relatives à un système de détection des intrusions dans les réseaux embarqués*, expose des lignes directrices *relatives à* un système de détection des intrusions (IDS) dans les réseaux embarqués (IVN). Elle porte principalement sur les méthodes de détection des intrusions et des activités malveillantes dans les réseaux IVN, par exemple ceux utilisant un gestionnaire de réseau de communication (CAN) qui ne peut être pris en charge par les systèmes IDS classiques actuellement déployés sur l'Internet. La Recommandation UIT-T X.1375 comprend une classification et une analyse des attaques visant les réseaux IVN. Elle propose également des méthodes de détection des intrusions et des activités malveillantes dans les réseaux IVN fondés sur un gestionnaire CAN qui ne peuvent être pris en charge par les systèmes IDS classiques, ainsi que des lignes directrices concernant leur mise en œuvre.

– La Recommandation X.1376, *Mécanisme de détection des mauvais comportements liés à la sécurité des véhicules connectés utilisant les mégadonnées*, décrit un mécanisme de détection des mauvais comportements liés à la sécurité des véhicules connectés, afin d'aider les parties prenantes à utiliser les données automobiles pour améliorer la sécurité des véhicules. Plus la connectivité des véhicules augmente, plus les vulnérabilités sont nombreuses en raison du développement de technologies complexes. Ces vulnérabilités font peser davantage de menaces sur les véhicules connectés. L'analyse d'une grande quantité de données automobiles est très utile pour évaluer la sécurité des véhicules connectés.

Pendant l'actuelle période d'études, le groupe chargé de la Question 13/17 a organisé un mini-atelier sur les problèmes de cybersécurité que pose la conduite automatisée (Genève, 26 août 2019).

n) Question 14/17: Aspects sécurité des technologies de registres distribués (2018‑2020)/Sécurité de la technologie des registres distribués (DLT) (2021-)

Le groupe chargé de la Question 14/17, qui a été mise à l'étude en mars 2018, élabore des Recommandations sur les aspects sécurité des technologies de registres distribués (DLT), également appelées chaîne de blocs (blockchain). Ces Recommandations définissent notamment des solutions de sécurité complètes pour les applications et les services reposant sur la technologie DLT.

Pendant l'actuelle période d'études, neuf nouvelles Recommandations ont été élaborées au titre de la Question 14/17:

– La Recommandation X.1400, *Termes et définitions concernant la technologie des registres distribués*, contient un ensemble de base de termes et de définitions concernant la technologie des registres distribués (DLT). Les définitions donnent une caractérisation de base du terme et sont assorties, selon le cas, d'une note pour apporter des éclaircissements supplémentaires.

– La Recommandation X.1401, *Menaces de sécurité pour la technologie des registres distribués*, identifie les menaces qui peuvent viser diverses composantes fonctionnelles du système de registres distribués, par exemple le protocole, le réseau et les données. Cette recommandation peut être prise en compte comme document de référence lors de la conception ou de la mise en œuvre d'un système DLT.

– La Recommandation X.1402, *Cadre de sécurité pour la technologie des registres distribués*, décrit les capacités de sécurité susceptibles d'atténuer ces menaces et indique une méthode générale permettant de déterminer comment utiliser ces capacités de sécurité pour atténuer les menaces visant un système DLT donné.

– La Recommandation X.1403, *Lignes directrices sur la sécurité relatives à l'utilisation de la technologie des registres distribués pour la gestion décentralisée des identités*. La technologie des registres distribués et ses applications spécifiques, telles que la blockchain, offrent une occasion unique d'utiliser une infrastructure de confiance et une plate-forme qui pourraient s'avérer utiles en permettant à une fédération de confiance d'échanger des attributs d'identité et des informations d'identité. Cette Recommandation définit les aspects de confidentialité et de sécurité propres aux télécommunications dans l'utilisation de données DLT pour la gestion des identités.

– La Recommandation X.1404, *Garantie de sécurité pour la technologie des registres distribués*, définit trois niveaux de garantie de la sécurité pour la technologie des registres distribués (DLT), afin de faciliter la conception et la mise au point de mécanismes de garantie de la sécurité. Elle définit en outre dix composantes de garantie de la sécurité et indique les critères et les lignes directrices permettant d'atteindre chacun des trois niveaux d'une composante de garantie de la sécurité. Enfin, cette Recommandation fournit une mise en correspondance entre les menaces spécifiques et les composantes de garantie de la sécurité ainsi qu'une mise en correspondance entre les capacités de sécurité spécifiques et les composantes de garantie de la sécurité.

– La Recommandation X.1405, *Menaces et exigences de sécurité pour les services de paiement numérique basés sur la technologie des registres distribués,* décrit, sur la base de l'analyse des cas d'utilisation des services de paiement, un modèle de service, analyse les menaces et défis en matière de sécurité et définit des exigences de sécurité contre les menaces et les défis recensés.

– La Recommandation X.1406, *Menaces de sécurité contre le vote en ligne à l'aide de la technologie des registres distribués*, recense les menaces de sécurité qui pèsent sur les systèmes de vote en ligne recourant à la technologie DLT basée sur l'infrastructure des télécommunications/TIC. Elle propose un modèle de référence pour les systèmes de vote en ligne recourant à la technologie DLT basée sur l'infrastructure des télécommunications/TIC et contient une analyse des menaces de sécurité qui pèsent sur les processus de vote en ligne décrits dans les modèles.

– La Recommandation X.1407, *Exigences de sécurité applicables au service de vérification de l'intégrité numérique basé sur la technologie des registres distribués*, indique les menaces et les exigences de sécurité en ce qui concerne le service de vérification de l'intégrité numérique basé sur la technologie des registres distribués (DLT).

– La Recommandation X.1408, *Menaces et exigences de sécurité relatives à l'accès aux données et au partage de données reposant sur la technologie des registres distribués*, établit un modèle de référence permettant de décrire l'accès aux données et le partage des données reposant sur la technologie des registres distribués (DLT). Elle recense les entités et leurs rôles ainsi que les menaces de sécurité qui pèsent sur l'accès aux données et le partage des données reposant sur la technologie DLT. Elle définit également des exigences de sécurité visant à répondre aux menaces de sécurité recensées.

o) Question 15/17: Sécurité relative aux nouvelles technologies, y compris la sécurité quantique

Le groupe chargé de l'étude de la Question 15/17, qui a été formulée en janvier 2021, élabore des Recommandations sur la sécurité relative aux nouvelles technologies, y compris la sécurité quantique, et étudie également le mécanisme d'incubation (TP.inno) de la CE 17, qui permet d'aborder avec plus de souplesse les nouveaux domaines liés à la sécurité, le but étant de sécuriser les nouveaux services et les nouvelles applications reposant sur les télécommunications/TIC.

Pendant la période d'études actuelle, deux nouvelles Recommandations et un Corrigendum d'un rapport technique ont été élaborés au titre de la Question 15/17:

– La Recommandation X.1712, *Exigences de sécurité et conception des réseaux de distribution de clés quantiques – Gestion des clés*, recense les menaces et exigences de sécurité relatives à la gestion des clés dans les réseaux de distribution de clés quantiques (QKDN) et établit des mesures de sécurité en matière de gestion des clés pour respecter les exigences de sécurité.

– La Recommandation X.1770, *Lignes directrices techniques relatives aux calculs multi-parties sécurisés*, définit des lignes directrices techniques relatives aux calculs multi-parties sécurisés (MPC) et fournit les bases techniques normalisées permettant aux parties prenantes du secteur des TIC d'utiliser les calculs MPC pour protéger les données dans des scénarios de collaboration de données ou d'analyse des mégadonnées. Elle décrit également les applications dans lesquelles les calculs MPC peuvent être utilisés et la manière dont elles peuvent servir de référence aux parties prenantes du secteur des TIC pour concevoir des applications MPC.

– Le Corrigendum 1 du rapport technique TR.sec-qkd, *Considérations de sécurité concernant les réseaux de distribution de clés quantiques*, vise à modifier les expressions pertinentes concernant "*IT-secure*", à remplacer "*qubits*" par "*quantum states*" et "*co-fiber*" par "*co-propagation*" et à modifier les contenus connexes.

## 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, la gestion d'identité et 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 conjointement par le groupe chargé de la Question 11/17 et le groupe chargé de la Question 12/17 jusqu'en 2020, puis par le groupe chargé de la Question 11/17 à partir de 2021.

### 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‑16).

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 diversité d'organismes de normalisation et de forums s'occupant de la sécurité des TIC et des télécommunications. L'un des objectifs a été d'éviter les divergences éventuelles entre les travaux réalisés par les commissions d'études et les organismes extérieurs.

De plus, 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 comportent 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, UIT-D (CE 1, CE 2, GCDT) , UIT-R (CE 1, CE 5, CE 6, GT 4C, GT 5A, GT 5D, GT 6C), Initiative FIGI de l'UIT-T, groupes spécialisés de l'UIT-T (AI4EE, AI4H, AN, DFC, DLT, DPM, ML5G, NET2030, QIT4N, VM), JCA de l'UIT‑T (IMT2020, IoT et SC&C, MMeS, SDN), SCV de l'UIT‑T, commissions d'études de l'UIT-T (2, 3, 5, 9, 11, 12, 13, 15, 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 directrice, des notes de liaison ont été reçues des entités extérieures suivantes: 3GPP (SA3), BIPM, CEN-CENELEC JTC 19, ETSI ISG (CIM, ETI, F5G, IPE, NIN, QSC, SAI), ETSI SAGE, ETSI TC (CYBER, ITS, MTS), Alliance FIDO, IEEE 802.1, IETF WG TLS, ISO TC 307, ISO/CEI JTC 1/ SC (6, 27/WG 1-5, 29/WG1), MEF, NIST, OASIS, OMA, oneM2M, SAE et W3C, et ont été traitées.

La CE 17 a envoyé des notes de liaison aux entités internes suivantes: CITS de l'UIT, Groupe ad hoc IPR-AHG, UIT-D (CE 1, CE 2, GCDT), commissions d'études de l'UIT‑R (4, 5 (GT 5A, GT 5D)), Initiative FIGI de l'UIT-T, groupes spécialisés de l'UIT-T (AI4EE, DFC, DLT, NET2030, DPM, QIT4N, VM), JCA de l'UIT‑T (IMT2020, IoT et SC&C, MMeS, SDN), SCV de l'UIT‑T, commissions d'études de l'UIT-T (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), APT ASTAP, BSI, CEN-CENELEC JTC 19, CEI, ETSI (ISG CIM, MEC, QKD, ZSM, SAGE), ETSI TC (CYBER, ITS, MTS), Alliance FIDO, GSMA (FASG, SIM), OACI, IEEE Blockchain Initiative, IETF, IRTF, ISO TC (12, 20, 22, 37, 204, 307), ISO/CEI JTC 1/WG 9, ISO/CEI JTC 1/SC (6 (WG 10), 7, 27 (WG 1, WG 2, WG 3, WG 4, WG 5), 29, 38, 42), Kantara Initiative, MEF, MITRE, NGMN, NIST, OASIS TC (CTI, OpenC2, Trust Elevation), OIX, oneM2M, ONF, Fondation OPIX, Forum RAISE, SAE, UNECE, UPU, W3C, OMPI, OMS.

En application de la Résolution 7 de l'AMNT‑16, *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.

La CE 17 a organisé les ateliers suivants:

– [2ème atelier conjoint UIT-OMS sur le certificat COVID numérique](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/1126/Pages/default.aspx)

 Virtuel, 13 h 00-18 h 00 CEST, 26 novembre 2021

– [Atelier conjoint UIT-OMS sur le certificat de vaccination numérique](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/0811/Pages/default.aspx)

 Virtuel, 13 h 00-18 h 00 CEST, 11 août 2021

– "Identificateurs décentralisés et chaîne de blocs" dans le cadre de l'édition 2021 de la [Semaine du BDT sur le thème des technologies émergentes](https://www.itu.int/en/ITU-D/Conferences/ET/2021/Pages/Programme.aspx)

 Virtuel, 14 h 00-15 h 00, 8 juillet 2021

– [Mini-atelier de la CE 17 sur les problèmes de cybersécurité que pose la conduite automatisée](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx)
Genève, 14 h 30-17 h 30, 26 août 2019

– [Atelier de l'UIT sur la sécurité des technologies financières](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190826/Pages/default.aspx)
Genève, Suisse, 26 août 2019

– [Atelier de l'UIT sur les technologies de l'informatique quantique (QIT) pour les réseaux](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Pages/default.aspx)
Shanghai, Chine, 5-7 juin 2019

– [Mini-atelier de la CE 17 sur les communications quantiques sécurisés](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/Secure%20quantum%20communication.aspx)
Genève, 14 h 30-17 h 30, 24 janvier 2019

– [Atelier de l'UIT sur l'intelligence artificielle, l'apprentissage automatique et la sécurité](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190121/Pages/default.aspx)
Genève, Suisse, 21 janvier 2019

– [Atelier de l'UIT sur les attaques de cybersécurité avancées et les rançongiciels](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx)
Genève, Suisse, 28 août 2018

– [Atelier de l'UIT sur la sécurité de la 5G](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx)
Genève, Suisse, 19 mars 2018

– Atelier de l'UIT sur les aspects de sécurité concernant les systèmes de transport intelligents
Genève, Suisse, 28 août 2017

– [Atelier de l'UIT sur les aspects sécurité de la chaîne de blocs](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Pages/default.aspx)
Genève, Suisse, 21 mars 2017

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

– la mise en œuvre des Résolutions 7, 11, 18, 32, 40, 44, 50, 52, 54, 58, 64, 65, 67, 70, 73, 75, 76, 77, 78, 84, 86, 89, 90, 92, 93, 94, 96, 97 et 98 de l'AMNT‑16;

– la mise en œuvre des Résolutions 101, 123, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200 et 201 de la PP‑18;

– la mise en œuvre des Résolutions 23, 30, 34, 45, 47, 54, 63, 67, 69 et 80 de la CMDT‑17.

La Commission d'études 17 a élaboré un plan d'action fondé sur les Résolutions de la PP-14 et de la PP-18, de l'AMNT-16 et de la CMDT-17, qu'elle met à jour à chacune de ses réunions. Lors de la réunion de la CE 17 tenue en mars 2020, un éditeur de ces textes a été désigné pour faciliter les travaux.

De plus, 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.

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-T 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.

La seconde édition du Rapport technique sur l'utilisation efficace des normes de sécurité a été publiée. Ce rapport 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).

La 7ème édition du Manuel sur la sécurité en tant que Rapport technique a été publiée. 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 9 | J.1204 | Cadre de sécurité d'un système d'exploitation de télévision intelligente |
| CE 13 | Y.2241 | Cadre de service pour la prise en charge de l'apprentissage autodirigé ubiquitaire basé sur des objets web |
| CE 13 | Y.2774 | Exigences fonctionnelles de l'inspection approfondie des paquets dans les réseaux futurs |
| CE 13 | Y.3051 | Principes fondamentaux applicables à un environnement de confiance dans l'infrastructure TIC |
| CE 13 | Y.3052 | Aperçu de l'instauration de la confiance dans les infrastructures et les services TIC |
| CE 13 | Y.3053  | Cadre applicable aux réseaux de confiance ayant des domaines de réseau centrés sur la confiance |
| CE 13 | Y.3054 | Cadre pour les services médias basés sur la confiance |
| CE 13 | Y.3055 | Cadre de gestion des données personnelles fondée sur la confiance |
| CE 13 | Y.3056 | Cadre d'amorçage des dispositifs et des applications pour l'accès ouvert à des services de confiance dans des écosystèmes distribués |
| CE 13 | Y.3057 | Modèle d'indice de confiance dans les infrastructures et services TIC |
| CE 13 | Y.3302 | Architecture fonctionnelle des réseaux pilotés par logiciel |
| CE 13 | Y.3514 | Informatique en nuage – Cadre et exigences concernant la confiance pour les échanges inter-nuages |
| CE 13 | Y.3516 | Architecture fonctionnelle de l'interconnexion de nuages informatiques |
| CE 13 | Y.3517 | Informatique en nuage – Aperçu de la gestion de la confiance inter-nuages  |
| CE 13 | Y.3650 | Cadre applicable aux réseaux fondés sur les mégadonnées sur la base de l'inspection approfondie des paquets |
| CE 13 | Y.3802 | Réseaux de distribution de clés quantiques – Architecture fonctionnelle |
| CE 13 | Y.3803 | Réseaux de distribution de clés quantiques – Gestion des clés |
| CE 13 | Y.3804 | Réseaux de distribution de clés quantiques – Commande et gestion |
| CE 13 | Y.3805 | Réseaux de distribution de clés quantiques – Commande des réseaux pilotés par logiciel |
| CE 13 | Y.3806 | Réseaux de distribution de clés quantiques – Exigences de garantie de qualité de service |
| CE 15 | G.873.1 | Réseau de transport optique(OTN) – Protection linéaire |
| CE 15 | G.873.3  | Réseau de transport optique (OTN) – Protection partagée en anneau  |
| CE 15 | G.8132/ Y.1383 (révisée) | Protection partagée en anneau MPLS-TP |
| CE 15 | G.9978 | Émetteurs-récepteurs unifiés de réseau domestique filaire à haut débit – Admission sécurisée |
| CE 16 | H.248.77 | Protocole de commande de passerelle: paquetage et procédures de protocole de transport sécurisé en temps réel (SRTP) |
| CE 20 | Y.4457 | Cadre architectural pour la fourniture d'un service de sécurité des transports |
| CE 20 | Y.4808 | Cadre de l'architecture d'entité numérique pour la lutte contre la contrefaçon dans l'Internet des objets |
| CE 20 | Y.4810 | Exigences en matière de sécurité des données pour les dispositifs IoT hétérogènes |

Suppléments et Appendices approuvés

| CE | Numéro | Titre |
| --- | --- | --- |
| CE 13 | Supplément 44 à la série Y.3100  | Normalisation et activités sur le code source ouvert relatives à la logiciellisation des réseaux IMT-2020  |

Projets de Recommandations ayant fait l'objet d'un consentement

|  |  |  |
| --- | --- | --- |
| CE | Numéro | Titre |
| CE 13 | Y.2086 (Y.DNI-fr) | Cadre et exigences d'une infrastructure de réseau de confiance décentralisée *(a fait l'objet d'un consentement le 16 juillet 2021)* |
| CE 13 | Y.3807 (Y.QKDN-QoS-pa) | Réseaux de distribution de clés quantiques – Paramètres de qualité de service*(a fait l'objet d'un consentement le 10 décembre 2021)* |
| CE 13 | Y.3808 (Y.QKDN-frint) | Cadre pour l'intégration d'un réseau de distribution de clés quantiques et d'un réseau de stockage sécurisé*(a fait l'objet d'un consentement le 10 décembre 2021)* |
| CE 13 | Y.3809 (Y.QKDN-BM) | Réseaux de distribution de clés quantiques – Modèles basés sur les rôles opérationnels*(a fait l'objet d'un consentement le 10 décembre 2021)* |

### 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-16).

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 3CE 17 | D.1140X.1261\*\*\* | Cadre politique intégrant des principes applicables à l'infrastructure d'identité numérique |
| CE 2 | E.217rév | Communications maritimes – Identités des stations de navire |
| CE 11 | Q.4063 | Cadre applicable aux tests des systèmes d'identification utilisés dans l'Internet des objets |
| CE 11 | Q.5052 | Lutte contre les dispositifs mobiles ayant des identificateurs uniques dupliqués |
| CE 15 | L.207  | Éléments nodaux passifs avec détection automatique de l'étiquette d'identification |
| CE 16 | H.273 | Codes indépendants du codage pour l'identification du type de signal vidéo |
| CE 17 | X.1252rev | Termes et définitions de base relatifs à la gestion d'identité |
| CE 17 | X.1403 | Lignes directrices sur la sécurité relatives à l'utilisation de la technologie des registres distribués pour la gestion décentralisée des identités |
| CE 20 | Y.4805 | Exigences applicables aux services d'identification pour l'interopérabilité des applications des villes intelligentes |
| CE 20 | Y.4476 | Cadre de résolution fondé sur les identificateurs OID pour les transactions d'un registre distribué assigné aux ressources de l'Internet des objets (IoT) |
| CE 20 | Y.4809 | Identificateurs de l'Internet des objets pour les systèmes de transport intelligents |
| CE 20 | Y.4811 | Cadre de référence des services issus de la convergence pour l'identification et l'authentification des dispositifs IoT dans un environnement décentralisé |

\*\*\* Double numérotation de la Recommandation D.1140 (CE 3) en tant que Recommandation X.1261 (CE 17).

En outre, 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-16).

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.

Le groupe chargé des Questions 11/17 et 12/17 a été productif concernant les langages et techniques de description ASN.1, 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. La [base de données des modules ASN.1](http://www.itu.int/ITU-T/recommendations/fl.aspx?lang=1) continue d'être complétée et permet aux responsables de la mise en œuvre 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 900 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.

Le langage de spécification et de description (SDL-2010) est utilisé pour définir des systèmes à la fois comme modèles de référence dans des Recommandations et comme mises en œuvre. La grammaire SDL-2010 est définie dans les Recommandations Z.101 à Z.107 et il existe une définition formelle dans l'Annexe F de la Recommandation Z.100. Le groupe chargé de la Question 12/17 a mis à jour cette définition formelle. L'avantage de cette étude est qu'elle a permis de déceler et de supprimer les ambiguïtés, les erreurs et les incohérences dans les Recommandations Z.101 à Z.107. Une définition formelle parfaitement alignée sur le langage SDL‑2010 a fait l'objet d'un consentement selon la variante de la procédure d'approbation (AAP) le 5 septembre 2019. Parallèlement, les textes des Recommandations Z.100 à Z.107 mises à jour ont fait l'objet d'un consentement selon la procédure AAP, afin de supprimer les ambiguïtés, les erreurs et les incohérences. Une version révisée de la Recommandation Z.Imp100 a été approuvée le 5 septembre 2019, avec une liste vide de modifications apportées aux Recommandations Z.100 à Z.107 ayant fait l'objet d'un consentement selon la procédure AAP et une liste des textes précédents en vigueur. Par conséquent, le langage SDL-2010 est mieux défini et la définition formelle est cohérente. Aucune autre activité n'est prévue pour l'heure.

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. Trois nouveaux textes et 25 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.

### 3.3.4 Activité conjointe de coordination sur la gestion d'identité (JCA-IdM)

Pendant l'actuelle 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 tenu six réunions à l'occasion des réunions de la CE 17 tenues en août/septembre 2017, mars 2018, août/septembre 2018, août/septembre 2019, avril 2021 et août/septembre 2021, pour coordonner les travaux relatifs à la gestion d'identité (IdM) de l'UIT-T avec les groupes internes de l'UIT-T et les organisations extérieures compétentes, par exemple Decentralized Identify Foundation, FIDO Alliance, ISO/CEI JTC 1/SC 27/WG 5, ISO TC 307, Kantara Initiative, Mobile Driving Licence, groupe de travail sur l'identité NH-ISAC, OASIS, OpenIdD Foundation, Sovrin Fondation, SSI Open Standards et l'UPU.

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

Le Groupe régional pour l'Afrique de la CE 17 (SG17 RG-AFR), créé en avril 2015 lors de la dernière période d'études, a été reconduit au cours de l'actuelle période d'études. Il a tenu une réunion au cours de la période d'études actuelle à l'occasion d'une réunion conjointe avec le Groupe SG17 RG-ARB tenue les 2 et 3 avril 2019.

### 3.3.6 Groupe régional de la Commission d'études 17 pour les États arabes (SG17 RG‑ARB)

Le Groupe régional de la CE 17 pour les États arabes (SG17 RG-ARB), créé lors de la réunion de la CE 17 qui a eu lieu en mars 2017, a tenu sa première réunion à Mascate (Oman) en décembre 2017. Sa deuxième réunion a eu lieu au Koweït en octobre 2018 et sa troisième réunion s'est tenue à Tunis les 2 et 3 avril 2019. Ce groupe a tenu sa troisième réunion à l'occasion d'une réunion conjointe avec le Groupe SG17 RG-AFR.

Lors de toutes les réunions du groupe régional de la CE 17, le Conseiller de la CE 17 a présenté des tutoriels sur la réduction de l'écart en matière de normalisation et la CE 17. Les participants des pays des régions ont tenu des séances d'échanges d'idées sur des thèmes liés à la cybersécurité et ont recensé les sujets qui les intéressaient tout particulièrement et qui appellent un complément d'étude.

## 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 permettent de coordonner l'assistance aux utilisateurs pour ce qui est des outils ainsi que du 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 œuvre 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 les 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 œuvre 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 œuvre et peut introduire des erreurs. Le fait que tous les modules ASN.1 soient au même endroit facilite grandement la mise en œuvre 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 (OID) 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, qui comptait plus de 1 643 596 enregistrements au 16 novembre 2021 (<http://www.oid-info.com/cgi-bin/display?a=count_nodes>) dans le répertoire des identificateurs d'objet à l'adresse <http://www.oid-info.com>, 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).

En particulier, la Recommandation X.677, Mécanisme d'identification des aéronefs sans pilote à l'aide d'identificateurs d'objet, a été approuvée en vue d'analyser les exigences en matière de gestion du cycle de vie complet et de reconnaissance de l'identité d'exploitation des aéronefs sans pilote et aborde les considérations relatives à la sécurité. Elle contient en outre les spécifications d'un mécanisme d'identification des aéronefs sans pilote (UAV) au moyen d'identificateurs d'objet (OID).

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 à Bahreïn, au Bénin, en Équateur, en Jamaïque et au Viet Nam.

## 3.5 Réduire l'écart en matière de normalisation

Lors de toutes les réunions physiques tenue par la CE 17 au cours de l'actuelle période d'études, le TSB a organisé une réception de bienvenue et une visite des locaux de l'UIT à l'intention des nouveaux délégués de la CE 17. Le Président de la CE 17 a organisé une "séance d'orientation pour les nouveaux délégués et une discussion avec l'équipe de direction de la CE 17". En janvier 2019, le Conseiller de la CE 17 a organisé un "stage intensif en présence des Conseillers de la CE 17" pour répondre aux questions des délégués de la CE 17 sur les méthodes de travail de cette commission. En septembre 2019, le TSB a organisé une "une séance de formation à l'intention de la direction de l'UIT-T" conçue pour les Rapporteurs et les éditeurs de la CE 17.

Entre mars 2017 et septembre 2018, la CE 17 a organisé périodiquement, à l'occasion de ses réunions, une session de formation pratique pour les délégués des pays en développement 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.

Au cours de la période d'études actuelle, le CE 17 a organisé périodiquement des rencontres informelles (virtuelles) de délégués d'Afrique et des États arabes à l'occasion de ses réunions (virtuelles), pour faciliter les discussions sur la planification future des travaux des groupes SG17 RG-AFR et SG17 RG-ARB.

# 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. Un ensemble solide de Recommandations/normes sur la sécurité a été établi, des accords de collaboration et de coordination 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. Étant 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 enrichie, développée et renforcée, et non pas fragmentée.

Les menaces et les vulnérabilités existantes et futures qui nuisent à la sécurité devraient être traitées, afin de renforcer la confiance et la sécurité dans l'utilisation des TIC, compte tenu des nouveaux services et des nouvelles applications reposant sur les réseaux de télécommunication/TIC, moyennant l'élaboration de Recommandations et de rapports techniques. Les technologies de sécurité sont des éléments fondamentaux de la protection d'un système TIC contre les attaques ou les dommages causés à son matériel, ses logiciels ou ses informations, ainsi que contre les perturbations ou les erreurs d'orientation des services qu'il fournit.

De nouvelles approches et mesures en matière de sécurité sont nécessaires pour faire face comme il se doit aux menaces et aux risques dans le domaine de la sécurité. La Commission d'études 17 a un rôle décisif à jouer dans l'élaboration de normes internationales dans le domaine de la sécurité.

La sécurité des télécommunications et des TIC reste un domaine dans lequel des normes de sécurité seront nécessaires. La gestion des nouvelles menaces qui se font jour dans le domaine des télécommunications et des TIC, y compris les infrastructures de réseau, les systèmes, les applications et les services, est d'une importance vitale. Il est admis qu'il faut impérativement élaborer des normes et des lignes directrices sur la sécurité qui soient applicables en pratique et répondent aux besoins de tous les pays.

La gestion des nouvelles menaces qui se font jour dans le domaine des infrastructures de télécommunication et des TIC est d'une importance vitale. Les travaux de la Commission d'études 17 sur la sécurité (architecture générique de sécurité, cadre, exigences, mécanismes, protocoles et lignes directrices relatives à la gestion pour des réseaux/systèmes/services hétérogènes) doivent se poursuivre et il est nécessaire qu'une commission d'études directrice pour la sécurité coordonne les travaux effectués par l'UIT et les autres organisations de normalisation. La Commission d'études 17 est consciente du fait qu'il faut impérativement élaborer des normes et des lignes directrices sur la sécurité qui soient applicables en pratique et répondent aux besoins de tous les pays.

Le renforcement du cadre de sécurité et de la protection des informations d'identification personnelle (PII) est une condition préalable au développement d'une société de l'information très connectée et au renforcement de la confiance et de la sécurité parmi les utilisateurs des technologies de l'information et de la communication. Les données utilisées dans les applications et les services sont protégées par des technologies de sécurité et des mesures organisationnelles et physiques adaptées. La sécurité relative aux télécommunications et aux TIC reste un domaine dans lequel de nouvelles normes seront nécessaires. De nouvelles technologies émergentes comme l'informatique en nuage (y compris l'informatique en nuage en périphérie, l'informatique multi-nuage), les réseaux électriques intelligents, les usines intelligentes, les systèmes de transport intelligents, les réseaux cellulaires de 5ème génération, les réseaux pilotés par logiciel, la virtualisation des fonctions de réseau, le découpage de réseau, l'analyse des mégadonnées, l'Internet des objets, les technologies des registres distribués, les systèmes de transport intelligents et la sécurité quantique, appellent des mesures techniques et organisationnelles pour faire face à diverses menaces et divers risques et assurer la protection des informations PII des personnes, ainsi que des mesures techniques et organisationnelles pour assurer la protection en ligne des enfants. De nouvelles approches et mesures fondées sur l'évaluation des risques en matière de sécurité pour faire face efficacement aux menaces et aux risques qui pèsent sur la sécurité pourront être nécessaires. La Commission d'études 17 a un rôle essentiel à jouer dans l'élaboration de normes 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 jouer un rôle de coordination de premier plan et 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 des technologies financières, les OTT et 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, y compris l'identité décentralisée fondée sur la technologie DLT, 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.

Les nouveaux environnements des télécommunications/TIC, par exemple en ce qui concerne l'Internet des objets (IoT), les systèmes ITS, les usines intelligentes, les villes et les communautés intelligentes et les réseaux électriques intelligents, imposent des exigences de sécurité concernant l'utilisation de l'infrastructure PKI. L'infrastructure PKI a été conçue au départ pour sécuriser uniquement les services bancaires 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, des usines intelligentes et des réseaux électriques intelligents ne seront pas pris en compte, ce qui aura un impact considérable pour la société et la vie quotidienne, car la stabilité d'une partie importante des infrastructures essentielles sera affectée. Pendant la prochaine période d'études, il conviendra d'accorder une priorité élevée aux travaux visant à améliorer l'infrastructure PKI, afin de prendre en charge les nouveaux environnements.

Pour que la sécurité soit assurée, de nouvelles normes seront nécessaires. L'UIT a admis depuis longtemps qu'il est important de disposer d'outils 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).

# 5 Mises à jour de la Résolution 2 de l'AMNT pour la période d'études 2022-2024

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 le nom, les domaines d'étude généraux, les fonctions de commission d'études directrice, les points de repère et les Recommandations pour la prochaine période d'études.

ANNEXE 1

Liste des Recommandations, Suppléments et autres documents établis 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 corrigenda** approuvés pendant cette période d'études à la date du 7 janvier 2022 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 qui a eu lieu le 7 janvier 2022.

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‑20pour 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 du 7 janvier 2022 de l'établissement du tableau.

Tableau 7

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

| Recommandation | Approbation | Statut | TAP/AAP | Titre  |
| --- | --- | --- | --- | --- |
| [X.500](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14031&lang=fr) | 14-10-2019 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services |
| [X.501](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14032&lang=fr) | 14-10-2019 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Modèles |
| [X.501 (2019) Amd. 1](http://handle.itu.int/11.1002/1000/14790) | 14-10-2021 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire – Modèles – Amendement 1: Améliorations diverses |
| [X.509](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14033&lang=fr) | 14-10-2019 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut |
| [X.509 (2019) Cor. 1](http://handle.itu.int/11.1002/1000/14791) | 14-10-2021 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire – Cadre général des certificats de clé publique et d'attribut: Corrigendum 1 |
| [X.510](http://handle.itu.int/11.1002/1000/14320) | 22-08-2020 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécifications de protocole pour les opérations sécurisées |
| [X.511](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14034&lang=fr) | 14-10-2019 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: définition du service abstrait |
| [X.518](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14035&lang=fr) | 14-10-2019 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: procédures pour le fonctionnement réparti |
| [X.519](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14036&lang=fr) | 14-10-2019 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécifications de protocole |
| [X.520](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14037&lang=fr) | 14-10-2019 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attribut choisis |
| [X.521](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14038&lang=fr) | 14-10-2019 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: classes d'objets sélectionnées |
| [X.525](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14047&lang=fr) | 14-10-2019 | En vigueur | AAP | Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: duplication |
| [X.676](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13712&lang=fr) | 29-11-2018 | En vigueur | AAP | Cadre de résolution basé sur les identificateurs d'objet pour les services groupés de l'IoT |
| [X.677](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14039&lang=fr) | 08-03-2020 | En vigueur | AAP | Mécanisme d'identification des aéronefs sans pilote à l'aide d'identificateurs d'objet |
| [X.680 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13257) | 14-05-2017 | Remplacée | AAP |  |
| [X.680 (2015) Cor.2](http://handle.itu.int/11.1002/1000/13361) | 14-10-2017 | Remplacée | AAP |  |
| [X.680 (2015) Cor.3](http://handle.itu.int/11.1002/1000/13598) | 14-05-2018 | Remplacée | AAP |  |
| [X.680 (2015) Amd.1](http://handle.itu.int/11.1002/1000/13597) | 14-05-2018 | Remplacée | AAP | Assouplissement de la section IMPORTS pour permettre l'importation de définitions provenant de nouvelles versions d'un module donné |
| [X.680](http://handle.itu.int/11.1002/1000/14468) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Syntaxe abstraite numéro un (ASN.1): spécification de la notation de base |
| [X.681 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13599) | 14-05-2018 | Remplacée | AAP |  |
| [X.681](http://handle.itu.int/11.1002/1000/14469) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Syntaxe abstraite numéro un (ASN.1): spécification des objets informationnels |
| [X.682 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13362) | 14-10-2017 | Remplacée | AAP |  |
| [X.682 (2015) Cor.2](http://handle.itu.int/11.1002/1000/13600) | 14-05-2018 | Remplacée | AAP |  |
| [X.682](http://handle.itu.int/11.1002/1000/14470) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Syntaxe abstraite numéro un (ASN.1): spécification des contraintes |
| [X.683 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13601) | 14-05-2018 | Remplacée | AAP |  |
| [X.683](http://handle.itu.int/11.1002/1000/14471) | 13-02-2021 | En vigueur | AAP | Technologies de l'information - Syntaxe abstraite numéro un (ASN.1): paramétrage des spécifications de la notation de syntaxe abstraite numéro un |
| [X.690](http://handle.itu.int/11.1002/1000/14472) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base(BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER) |
| [X.691](http://handle.itu.int/11.1002/1000/14473) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact (PER) |
| [X.692](http://handle.itu.int/11.1002/1000/14474) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: spécification de la notation de contrôle de codage (ECN) |
| [X.693 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13363) | 14-10-2017 | Remplacée | AAP |  |
| [X.693](http://handle.itu.int/11.1002/1000/14475) | 13-02-2021 | En vigueur | AAP | Technologies de l'information Règles de codage ASN.1: règles de codage XML (XER) |
| [X.694 (2015) Cor.1](http://handle.itu.int/11.1002/1000/14040) | 14-10-2019 | Remplacée | AAP |  |
| [X.694](http://handle.itu.int/11.1002/1000/14476) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: mappage en ASN.1 des définitions de schéma XML du W3C |
| [X.695](http://handle.itu.int/11.1002/1000/14477) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: enregistrement et application des instructions de codage PER |
| [X.696 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13258) | 14-05-2017 | Remplacée | AAP |  |
| [X.696 (2015) Cor.2](http://handle.itu.int/11.1002/1000/13364) | 14-10-2017 | Remplacée | AAP |  |
| [X.696 (2015) Cor.3](http://handle.itu.int/11.1002/1000/13602) | 14-05-2018 | Remplacée | AAP |  |
| [X.696](http://handle.itu.int/11.1002/1000/14478) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage des octets (OER)  |
| [X.697](http://handle.itu.int/11.1002/1000/13365) | 14-10-2017 | Remplacée | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de la notation des objets Javascript (JER) |
| [X.697](http://handle.itu.int/11.1002/1000/14479) | 13-02-2021 | En vigueur | AAP | Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de la notation des objets Javascript (JER) |
| [X.893 (2007) Cor.1](http://handle.itu.int/11.1002/1000/14041) | 14-10-2019 | En vigueur | AAP |  |
| [X.894](http://handle.itu.int/11.1002/1000/12848) | 14-10-2018 | En vigueur | AAP | Technologies de l'information – Applications génériques de l'ASN.1 – Syntaxe de message cryptographique |
| [X.894 (2018) Cor.1](http://handle.itu.int/11.1002/1000/13871) | 16-03-2019 | En vigueur | AAP |  |
| [X.894 (2018) Cor. 2](http://handle.itu.int/11.1002/1000/14467) | 13-02-2021 | En vigueur | AAP | Applications génériques de l'ASN.1 – Syntaxe de message cryptographique – Corrigendum technique 2 |
| [X.1011](http://handle.itu.int/11.1002/1000/14793) | 29-10-2021 | En vigueur | AAP | Lignes directrices relatives à la protection continue du processus d'accès aux services |
| [X.1040](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13366&lang=fr) | 14-10-2017 | En vigueur | AAP | Architecture de référence de sécurité pour la gestion, tout au long de leur cycle de vie, des données sur les transactions de commerce électronique |
| [X.1041](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13603&lang=fr) | 14-05-2018 | En vigueur | AAP | Cadre de sécurité pour l'exploitation des réseaux vocaux LTE (VoLTE, voice-over-long-term-evolution)  |
| [X.1042](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13803&lang=fr) | 30-01-2019 | En vigueur | TAP | Services de sécurité utilisant les réseaux pilotés par logiciel |
| [X.1043](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13872&lang=fr) | 16-03-2019 | En vigueur | AAP | Cadre et exigences de sécurité pour le chaînage de fonctions de service fondé sur les réseaux pilotés par logiciel |
| [X.1044](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14042&lang=fr) | 29-10-2019 | En vigueur | AAP | Exigences de sécurité de la virtualisation de réseau |
| [X.1045](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14043&lang=fr) | 29-10-2019 | En vigueur | AAP | Architecture de la chaîne de services de sécurité pour les réseaux et les applications |
| [X.1046](http://handle.itu.int/11.1002/1000/14442) | 14-12-2020 | En vigueur | AAP | Cadre de sécurité définie par logiciel pour les réseaux pilotés par logiciel/la virtualisation des fonctions de réseau |
| [X.1047](http://handle.itu.int/11.1002/1000/14794) | 29-10-2021 | En vigueur | AAP | Exigences et architecture de sécurité pour la gestion et l'orchestration des tranches de réseau |
| [X.1051 (2016) Cor.1](http://handle.itu.int/11.1002/1000/13407) | 06-09-2017 | En vigueur | Accord |  |
| [X.1052](http://handle.itu.int/11.1002/1000/14044) | 29-10-2020 | En vigueur | AAP | Processus de gestion de la sécurité de l'information pour les organisations de télécommunication |
| [X.1053](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13367&lang=fr) | 13-11-2017 | En vigueur | AAP | Code de bonne pratique pour les contrôles de sécurité de l'information sur la base de la Recommandation UIT-T X.1051 pour les petites et moyennes organisations de télécommunication |
| [X.1058](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13182&lang=fr) | 30-03-2017 | En vigueur | TAP | Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des informations d'identification personnelle |
| [X.1059](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14045&lang=fr) | 29-10-2019 | En vigueur | AAP | Guide de mise en œuvre à l'intention des organisations de télécommunication sur la gestion des risques liés à leurs actifs mondialement accessibles dans les réseaux IP |
| [X.1060](http://handle.itu.int/11.1002/1000/14721) | 29-06-2021 | En vigueur | AAP | Cadre pour la création et l'exploitation d'un centre de cyberdéfense |
| [X.1061](http://handle.itu.int/11.1002/1000/14733) | 22-08-2021 | En vigueur | AAP | Lignes directrices relatives à l'acquisition d'une cyberassurance |
| [X.1080.0](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13193&lang=fr) | 30-03-2017 | En vigueur | TAP | Contrôle d'accès pour la protection des données télébiométriques |
| [X.1080.0 (2017) Cor.1](http://handle.itu.int/11.1002/1000/13591) | 29-03-2018 | En vigueur | Accord |  |
| [X.1080.1](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13604&lang=fr) | 14-05-2018 | En vigueur | AAP | Cybersanté et systèmes mondiaux de télémédecine – Protocole générique de télécommunication |
| [X.1080.2](http://handle.itu.int/11.1002/1000/14795) | 29-10-2021 | En vigueur | AAP | Protocole biologie-machine (B2M) |
| [X.1093](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13725&lang=fr) | 13-11-2018 | En vigueur | AAP | Contrôle d'accès télébiométrique au moyen de cartes d'identification intelligentes |
| [X.1094](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13873&lang=fr) | 16-03-2019 | En vigueur | AAP | Authentification télébiométrique utilisant des biosignaux |
| [X.1126](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13194&lang=fr) | 30-03-2017 | En vigueur | TAP | Lignes directrices relatives à l'atténuation des effets négatifs des terminaux infectés dans les réseaux mobiles |
| [X.1127](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13259&lang=fr) | 06-09-2017 | En vigueur | TAP | Exigences et architecture fonctionnelles de sécurité pour les mesures de protection contre le vol de téléphones mobiles |
| [X.1145](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13260&lang=fr) | 14-05-2017 | En vigueur | AAP | Cadre et exigences de sécurité pour les capacités ouvertes des services de télécommunication |
| [X.1146](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13368&lang=fr) | 14-10-2017 | En vigueur | AAP | Lignes directrices pour garantir la protection des services à valeur ajoutée fournis par les opérateurs de télécommunication |
| [X.1147](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13726&lang=fr) | 13-11-2018 | En vigueur | AAP | Exigences de sécurité et cadre pour l'analyse des mégadonnées dans les services Internet sur mobile |
| [X.1148](http://handle.itu.int/11.1002/1000/14249) | 03-09-2020 | En vigueur | TAP | Cadre applicable au processus de désidentification à l'intention des fournisseurs de services de télécommunication |
| [X.1149](http://handle.itu.int/11.1002/1000/14250) | 29-05-2020 | En vigueur | AAP | Cadre de sécurité d'une plate-forme ouverte pour les services des technologies financières |
| [X.1197 (2012) Amd.1](http://handle.itu.int/11.1002/1000/14046) | 05-09-2020 | En vigueur | Accord |  |
| [X.1212](http://handle.itu.int/11.1002/1000/13195) | 30-03-2017 | En vigueur | TAP | Considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité |
| [X.1213](http://handle.itu.int/11.1002/1000/13261) | 06-09-2017 | En vigueur | TAP | Capacités requises en matière de sécurité pour lutter contre les réseaux zombies (ou botnets) ciblant des smartphones |
| [X.1214](http://handle.itu.int/11.1002/1000/13404) | 29-03-2018 | En vigueur | TAP | Techniques d'évaluation de la sécurité dans les réseaux de télécommunication/technologies de l'information et de la communication |
| [X.1215](http://handle.itu.int/11.1002/1000/13849) | 30-01-2019 | En vigueur | TAP | Cas d'utilisation pour l'expression structurée d'informations sur les menaces |
| [X.1216](http://handle.itu.int/11.1002/1000/14259) | 03-09-2020 | En vigueur | TAP | Exigences en matière de collecte et de conservation de preuves relatives aux incidents de cybersécurité |
| [X.1217](http://handle.itu.int/11.1002/1000/14443) | 07-01-2021 | En vigueur | TAP | Lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication  |
| [X.1218](http://handle.itu.int/11.1002/1000/14444) | 29-10-2020 | En vigueur | AAP | Exigences et lignes directrices relatives à une analyse dynamique des logiciels malveillants dans un environnement de type "bac à sable" |
| [X.1232](http://handle.itu.int/11.1002/1000/14085) | 29-10-2019 | En vigueur | AAP | Cadre technique de lutte contre le spam publicitaire dans les informations générées par les utilisateurs |
| [X.1233](http://handle.itu.int/11.1002/1000/14773) | 03-09-2021 | En vigueur | TAP | Lignes directrices relatives à la lutte contre le spam par messagerie instantanée |
| X.1234 | 07-01-2022 | En vigueur | TAP | Lignes directrices relatives à la lutte contre le spam envoyé par le service de messagerie multimédia (MMS) |
| X.1235 | 07-01-2022 | En vigueur | TAP | Technologies de lutte contre le piratage de sites web pour les organisations de télécommunication |
| [X.1248](http://handle.itu.int/11.1002/1000/13262) | 06-09-2017 | En vigueur | TAP | Exigences techniques pour lutter contre le spam par messagerie instantanée (SPIM) |
| [X.1249](http://handle.itu.int/11.1002/1000/13605) | 30-01-2019 | En vigueur | TAP | Cadre technique de lutte contre le spam publicitaire sur les applications mobiles  |
| [X.1252](http://handle.itu.int/11.1002/1000/14642) | 30-04-2021 | En vigueur | TAP | Termes et définitions de base relatifs à la gestion d'identité |
| [X.1254](http://handle.itu.int/11.1002/1000/14260) | 03-09-2020 | En vigueur | TAP | Cadre de garantie d'authentification des entités |
| [X.1276](http://handle.itu.int/11.1002/1000/13606) | 14-05-2018 | En vigueur | AAP | Protocole d'amélioration de l'authentification et métadonnées – Version 1.0 |
| [X.1277](http://handle.itu.int/11.1002/1000/13727) | 29-11-2018 | En vigueur | AAP | Cadre d'authentification universelle |
| [X.1278](http://handle.itu.int/11.1002/1000/13728) | 29-11-2018 | En vigueur | AAP | Protocole client-authentificateur/Cadre applicable au double facteur universel |
| [X.1279](http://handle.itu.int/11.1002/1000/14261) | 03-09-2020 | En vigueur | TAP | Cadre de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité |
| [X.1331](http://handle.itu.int/11.1002/1000/13405) | 29-03-2018 | En vigueur | TAP | Lignes directrices relatives à la sécurité des dispositifs des réseaux domestiques (HAN) dans les réseaux électriques intelligents |
| [X.1332](http://handle.itu.int/11.1002/1000/14086) | 26-03-2020 | En vigueur | TAP | Lignes directrices relatives à la sécurité des services de compteurs intelligents dans les réseaux électriques intelligents |
| X.1333 | 07-01-2022 | En vigueur | TAP | Lignes directrices sur la sécurité pour l'utilisation d'outils d'accès à distance dans les systèmes de contrôle connectés à l'Internet |
| [X.1361](http://handle.itu.int/11.1002/1000/13607) | 07-09-2018 | En vigueur | TAP | Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle |
| [X.1362](http://handle.itu.int/11.1002/1000/13196) | 30-03-2017 | En vigueur | TAP | Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT) |
| [X.1363](http://handle.itu.int/11.1002/1000/14087) | 29-05-2020 | En vigueur | TAP | Cadre technique applicable au traitement des informations d'identification personnelle dans l'environnement de l'Internet des objets |
| [X.1364](http://handle.itu.int/11.1002/1000/14088) | 26-03-2020 | En vigueur | TAP | Exigences et cadre de sécurité applicables à l'Internet des objets à bande étroite |
| [X.1365](http://handle.itu.int/11.1002/1000/14089) | 26-03-2020 | En vigueur | TAP | Méthode de sécurité applicable à l'utilisation de la cryptographie fondée sur l'identité à l'appui des services de l'Internet des objets (IoT) fournis sur les réseaux de télécommunication |
| [X.1366](http://handle.itu.int/11.1002/1000/14262) | 03-09-2020 | En vigueur | TAP | Systèmes d'authentification de messages agrégés pour l'environnement de l'Internet des objets |
| [X.1367](http://handle.itu.int/11.1002/1000/14263) | 03-09-2020 | En vigueur | TAP | Format normalisé de journaux d'erreurs pour l'Internet des objets aux fins de la gestion des incidents de sécurité |
| [X.1368](http://handle.itu.int/11.1002/1000/14445) | 07-01-2021 | En vigueur | TAP | Mise à jour sécurisée des micrologiciels ou des logiciels des dispositifs de l'Internet des objets |
| X.1369 | 07-01-2022 | En vigueur | TAP | Exigences de sécurité applicables à la plate-forme de services IoT |
| [X.1371](http://handle.itu.int/11.1002/1000/14090) | 29-05-2020 | En vigueur | TAP | Menaces pour la sécurité des véhicules connectés et l'écosystème des véhicules |
| [X.1372](http://handle.itu.int/11.1002/1000/14091) | 26-03-2020 | En vigueur | TAP | Lignes directrices relatives à la sécurité des communications de véhicule à tout autre élément (V2X) |
| [X.1373](http://handle.itu.int/11.1002/1000/13197) | 30-03-2017 | En vigueur | TAP | Capacité de mise à jour sécurisée des logiciels pour les dispositifs de communication des systèmes de transport intelligents |
| [X.1374](http://handle.itu.int/11.1002/1000/14446) | 29-10-2020 | En vigueur | AAP | Exigences de sécurité applicables à des interfaces et des dispositifs externes équipés d'une capacité d'accès au véhicule |
| [X.1375](http://handle.itu.int/11.1002/1000/14447) | 29-10-2020 | En vigueur | AAP | Lignes directrices relatives à un système de détection des intrusions pour les réseaux embarqués |
| [X.1376](http://handle.itu.int/11.1002/1000/14448) | 07-01-2021 | En vigueur | TAP | Mécanisme de détection des mauvais comportements liés à la sécurité des véhicules connectés utilisant les mégadonnées  |
| [X.1400](http://handle.itu.int/11.1002/1000/14449) | 29-10-2020 | En vigueur | AAP | Termes et définitions concernant la technologie des registres distribués |
| [X.1401](http://handle.itu.int/11.1002/1000/14092) | 29-11-2019 | En vigueur | AAP | Menaces de sécurité pour la technologie des registres distribués |
| [X.1402](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14251&lang=fr) | 22-07-2020 | En vigueur | AAP | Cadre de sécurité pour la technologie des registres distribués |
| [X.1403](http://handle.itu.int/11.1002/1000/14264) | 03-09-2020 | En vigueur | TAP | Lignes directrices sur la sécurité relatives à l'utilisation de la technologie des registres distribués pour la gestion décentralisée des identités |
| [X.1404](http://handle.itu.int/11.1002/1000/14450) | 29-10-2020 | En vigueur | AAP | Garantie de sécurité pour la technologie des registres distribués |
| [X.1405](http://handle.itu.int/11.1002/1000/14722) | 29-06-2021 | En vigueur | AAP | Menaces et exigences de sécurité pour les services de paiement numérique basés sur la technologie des registres distribués  |
| [X.1406](http://handle.itu.int/11.1002/1000/14734) | 14-07-2021 | En vigueur | AAP | Menaces de sécurité contre les systèmes de vote en ligne recourant à la technologie des registres distribués  |
| X.1407 | 07-01-2022 | En vigueur | TAP | Exigences de sécurité applicables au service de vérification de l'intégrité numérique basé sur la technologie des registres distribués  |
| [X.1408](http://handle.itu.int/11.1002/1000/14801) | 29-10-2021 | En vigueur | AAP | Menaces et exigences de sécurité relatives à l'accès aux données et au partage de données reposant sur la technologie des registres distribués |
| [X.1450](http://handle.itu.int/11.1002/1000/13729) | 14-10-2018 | En vigueur | AAP | Lignes directrices sur les mécanismes d'authentification hybride et de gestion de clés dans le modèle client-serveur |
| [X.1451](http://handle.itu.int/11.1002/1000/14252) | 29-05-2020 | En vigueur | AAP | Identification des risques pour optimiser l'authentification |
| [X.1452](http://handle.itu.int/11.1002/1000/14451) | 29-10-2020 | En vigueur | AAP | Lignes directrices relatives aux services de sécurité fournis par les opérateurs |
| X.1453 | 07-01-2022 | En vigueur | TAP | Menaces et exigences de sécurité pour les systèmes de gestion vidéo |
| [X.1470](http://handle.itu.int/11.1002/1000/14803) | 13-11-2021 | En vigueur | AAP | Lignes directrices relatives à la sécurité des services à la clientèle en ligne fondés sur le web |
| [X.1500 (2011) Amd.11](http://handle.itu.int/11.1002/1000/13263) | 30-03-2017 | Remplacée | Accord | Techniques révisées d'échange d'informations sur la cybersécurité structurées |
| [X.1500 (2011) Amd.12](http://handle.itu.int/11.1002/1000/13590) | 29-03-2018 | En vigueur | Accord | Techniques révisées d'échange d'informations sur la cybersécurité structurées |
| [X.1541](http://handle.itu.int/11.1002/1000/13264) | 06-09-2017 | En vigueur | TAP | Format d'échange de description d'objet incident (version 2) |
| [X.1550](http://handle.itu.int/11.1002/1000/13198) | 30-03-2017 | En vigueur | TAP | Modèles de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents |
| [X.1603](http://handle.itu.int/11.1002/1000/13406) | 29-03-2018 | En vigueur | TAP | Exigences de sécurité des données approuvées pour le service de surveillance de l'informatique en nuage |
| [X.1604](http://handle.itu.int/11.1002/1000/14093) | 26-03-2020 | En vigueur | TAP | Exigences de sécurité relatives au réseau en tant que service (NaaS) dans l'informatique en nuage |
| [X.1605](http://handle.itu.int/11.1002/1000/14094) | 26-03-2020 | En vigueur | TAP | Exigences de sécurité pour les infrastructures en tant que service (IaaS) publiques dans l'informatique en nuage |
| [X.1606](http://handle.itu.int/11.1002/1000/14265) | 03-09-2020 | En vigueur | TAP | Exigences de sécurité pour l'environnement des applications de communication en tant que service |
| X.1643 | 07-01-2022 | En vigueur | TAP | Exigences et lignes directrices sur la sécurité des conteneurs de virtualisation dans un environnement utilisant l'informatique en nuage |
| [X.1702](http://handle.itu.int/11.1002/1000/14095) | 13-11-2019 | En vigueur | AAP | Architecture d'un générateur de nombres aléatoires pour le bruit quantique |
| [X.1710](http://handle.itu.int/11.1002/1000/14452) | 29-10-2020 | En vigueur | AAP | Cadre de sécurité pour les réseaux de distribution de clés quantiques |
| [X.1712](http://handle.itu.int/11.1002/1000/14805) | 29-10-2021 | En vigueur | AAP | Exigences et mesures de sécurité pour les réseaux de distribution de clés quantiques - gestion des clés |
| [X.1714](http://handle.itu.int/11.1002/1000/14453) | 29-10-2020 | En vigueur | AAP | Combinaison de clés et fourniture de clés confidentielles pour les réseaux de distribution de clés quantiques |
| [X.1750](http://handle.itu.int/11.1002/1000/14266) | 03-09-2020 | En vigueur | TAP | Lignes directrices relatives à la sécurité des mégadonnées en tant que service pour les fournisseurs de services de mégadonnées |
| [X.1751](http://handle.itu.int/11.1002/1000/14267) | 03-09-2020 | En vigueur | TAP | Lignes directrices relatives à la sécurité de la gestion du cycle de vie des mégadonnées par les opérateurs de télécommunication |
| X.1752 | 07-01-2022 | En vigueur | TAP | Lignes directrices sur la sécurité pour l'infrastructure et la plate-forme de mégadonnées  |
| [X.1770](http://handle.itu.int/11.1002/1000/14807) | 29-10-2022 | En vigueur | AAP | Lignes directrices techniques concernant les calculs multi-parties sécurisés |
| [X.1811](http://handle.itu.int/11.1002/1000/14454) | 30-04-2021 | En vigueur | TAP | Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT-2020 |
| [Z.100 Annexe F1](http://handle.itu.int/11.1002/1000/13732) | 13-11-2018 | Remplacée | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 |
| [Z.100 Annexe F2](http://handle.itu.int/11.1002/1000/13733) | 13-11-2018 | Remplacée | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 |
| [Z.100 Annexe F3](http://handle.itu.int/11.1002/1000/13734) | 13-11-2018 | Remplacée | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 |
| [Z.100](http://handle.itu.int/11.1002/1000/14048) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 |
| [Z.100 Annexe F2](http://handle.itu.int/11.1002/1000/14050) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Définition formelle du langage SDL-2010: Sémantique statique |
| [Z.100 Annexe F3](http://handle.itu.int/11.1002/1000/14051) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Définition formelle du langage SDL-2010: Sémantique dynamique  |
| [Z.100](http://handle.itu.int/11.1002/1000/14670) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification - Présentation générale de SDL-2010 |
| [Z.100 Annexe F1](http://handle.itu.int/11.1002/1000/14049) | 14-10-2019 | En vigueur | AAP | Langage de description et de spécification – Présentation générale de SDL 2010 – Définition formelle du langage SDL: Présentation générale |
| [Z.100 Annexe F2](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14702&lang=fr) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Définition formelle du langage SDL: sémantique statique |
| [Z.100 Annexe F3](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14703&lang=fr) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification – Présentation générale de SDL-2010 – Définition formelle du langage SDL: sémantique dynamique |
| [Z.101](http://handle.itu.int/11.1002/1000/14052) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Langage SDL‑2010 de base |
| [Z.101](http://handle.itu.int/11.1002/1000/14671) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification – Langage SDL‑2010 de base |
| [Z.102](http://handle.itu.int/11.1002/1000/14053) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Langage SDL‑2010 complet |
| [Z.102](http://handle.itu.int/11.1002/1000/14672) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification – Langage SDL‑2010 complet |
| [Z.103](http://handle.itu.int/11.1002/1000/14054) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Notation abrégée et annotation dans le langage SDL-2010 |
| [Z.103](http://handle.itu.int/11.1002/1000/14673) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification – Notation abrégée et annotation dans le langage SDL-2010 |
| [Z.104](http://handle.itu.int/11.1002/1000/14055) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Caractéristiques du langage SDL-2010 pour les données et les actions |
| [Z.104](http://handle.itu.int/11.1002/1000/14674) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification – Caractéristiques du langage SDL-2010 pour les données et les actions |
| [Z.105](http://handle.itu.int/11.1002/1000/14056) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Langage SDL‑2010 combiné avec des modules ASN.1 |
| [Z.105](http://handle.itu.int/11.1002/1000/14675) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification – Langage SDL‑2010 combiné avec des modules ASN.1 |
| [Z.106](http://handle.itu.int/11.1002/1000/14057) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Format d'échange commun pour le langage SDL-2010 |
| [Z.106](http://handle.itu.int/11.1002/1000/14676) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification – Format d'échange commun pour le langage SDL-2010 |
| [Z.107](http://handle.itu.int/11.1002/1000/14058) | 14-10-2019 | Remplacée | AAP | Langage de description et de spécification – Données orientées objet en SDL-2010 |
| [Z.107](http://handle.itu.int/11.1002/1000/14677) | 13-06-2021 | En vigueur | AAP | Langage de description et de spécification – Données orientées objet en SDL-2010 |
| [Z.151](http://handle.itu.int/11.1002/1000/13711) | 14-10-2018 | En vigueur | AAP | Notation de prescriptions d'utilisateur (URN) – Définition du langage |
| [Z.161](http://handle.itu.int/11.1002/1000/13369) | 14-10-2017 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): langage noyau de la notation TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/13703) | 14-10-2018 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): langage noyau de la notation TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/14059) | 14-10-2019 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): langage noyau de la notation TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/14480) | 29-10-2020 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): langage noyau de la notation TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/14781) | 14-10-2020 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): langage noyau de la notation TTCN-3 |
| [Z.161.1](http://handle.itu.int/11.1002/1000/13370) | 14-10-2017 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: prise en charge d'interfaces avec des signaux continus |
| [Z.161.2](http://handle.itu.int/11.1002/1000/13371) | 14-10-2017 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: prise en charge de la configuration et du déploiement |
| [Z.161.2](http://handle.itu.int/11.1002/1000/13704) | 14-10-2018 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: prise en charge de la configuration et du déploiement |
| [Z.161.2](http://handle.itu.int/11.1002/1000/14060) | 14-10-2019 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: prise en charge de la configuration et du déploiement |
| [Z.161.2](http://handle.itu.int/11.1002/1000/14782) | 14-10-2021 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: prise en charge de la configuration et du déploiement |
| [Z.161.3](http://handle.itu.int/11.1002/1000/13372) | 14-10-2017 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: paramétrage évolué |
| [Z.161.3](http://handle.itu.int/11.1002/1000/13373) | 29-10-2020 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: paramétrage évolué |
| [Z.161.3](http://handle.itu.int/11.1002/1000/13705) | 14-10-2021 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: paramétrage évolué |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13373) | 14-10-2017 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: types de comportement |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13705) | 14-10-2018 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: types de comportement |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14482) | 29-10-2020 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: types de comportement |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14784) | 14-10-2021 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: types de comportement |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13374) | 14-10-2017 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: concordance évoluée |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13706) | 14-10-2018 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: concordance évoluée |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14061) | 14-10-2019 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: concordance évoluée |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14483) | 29-10-2020 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: concordance évoluée |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14062) | 14-10-2019 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: caractéristiques orientées objet |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14062) | 29-10-2020 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: caractéristiques orientées objet |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14062) | 14-10-2021 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): Extensions du langage TTCN-3: caractéristiques orientées objet |
| [Z.164](http://handle.itu.int/11.1002/1000/13375) | 14-10-2017 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): sémantique opérationnelle TTCN-3  |
| [Z.165](http://handle.itu.int/11.1002/1000/13376) | 14-10-2017 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface d'exécution TTCN-3 (TRI) |
| [Z.165.1](http://handle.itu.int/11.1002/1000/14485) | 29-10-2020 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): paquetage d'extension de la TTCN-3: interface d'exécution étendue TTCN (TRI).  |
| [Z.166](http://handle.itu.int/11.1002/1000/13377) | 14-10-2017 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface de commande TTCN-3 (TCI) |
| [Z.166](http://handle.itu.int/11.1002/1000/13707) | 14-10-2018 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface de commande TTCN-3 (TCI) |
| [Z.166](http://handle.itu.int/11.1002/1000/14063) | 14-10-2019 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface de commande TTCN-3 (TCI) |
| [Z.166](http://handle.itu.int/11.1002/1000/14063) | 29-10-2020 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): interface de commande TTCN-3 (TCI) |
| [Z.167](http://handle.itu.int/11.1002/1000/13378) | 14-10-2017 | Remplacée | 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.167](http://handle.itu.int/11.1002/1000/13708) | 14-10-2018 | Remplacée | 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.167](http://handle.itu.int/11.1002/1000/13378) | 29-10-2020 | Remplacée | 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.167](http://handle.itu.int/11.1002/1000/13378) | 14-10-2021 | 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](http://handle.itu.int/11.1002/1000/13379) | 14-10-2017 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): mappage du langage IDL vers la notation TTCN-3 |
| [Z.168](http://handle.itu.int/11.1002/1000/13379) | 14-10-2021 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): mappage du langage IDL vers la notation TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/13380) | 14-10-2017 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): utilisation des schémas XML avec la notation TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/13709) | 14-10-2018 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): utilisation des schémas XML avec la notation TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14064) | 14-10-2019 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): utilisation des schémas XML avec la notation TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14488) | 29-10-2020 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): utilisation des schémas XML avec la notation TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14788) | 14-10-2021 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): utilisation des schémas XML avec la notation TTCN-3 |
| [Z.170](http://handle.itu.int/11.1002/1000/13381) | 14-10-2017 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): spécification des commentaires de documentation TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/13382) | 14-10-2017 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): utilisation de la notation JSON avec la notation TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/13710) | 14-10-2018 | Remplacée | AAP | Notation de test et de commande de test version 3 (TTCN-3): utilisation de la notation JSON avec la notation TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/13710) | 14-10-2021 | En vigueur | AAP | Notation de test et de commande de test version 3 (TTCN-3): utilisation de la notation JSON avec la notation TTCN-3 |

Tableau 8

Commission d'études 17 – Recommandations ayant fait l'objet d'un consentement/
d'une détermination, mais pas encore approuvées

| Recommandation | Consentement/détermination | TAP/AAP | Titre |
| --- | --- | --- | --- |
| X.672 | 03-09-2021 | AAP | Système de résolution d'identificateur d'objet |
| Amendement 1 à la Recommandation X.1246 | 03-09-2021 | TAP | Technologies intervenant dans la lutte contre le spam vocal dans les organisations de télécommunication |
| Amendement 1 à la Recommandation X.1247 | 03-09-2021 | TAP | Cadre technique de lutte contre le spam par messagerie mobile |
| Corrigendum à la Recommandation X.1712 | 07-01-2022 | AAP | Exigences et mesures de sécurité pour les réseaux de distribution de clés quantiques – gestion des clés  |
| X.1812 (X.5Gsec-t) | 03-09-2021 | TAP | Cadre de sécurité fondé sur des relations de confiance pour l'écosystème des IMT-2020 |

Tableau 9

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

|  |  |  |  |
| --- | --- | --- | --- |
| Recommandation | Dernière version | Date du retrait | Titre |
| Néant |  |  |  |

Tableau 10

Commission d'études 17 – Recommandations soumises à l'AMNT‑20

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

Tableau 11

Commission d'études 17 – Suppléments

| Recommandation | Approbation | Statut | Titre  |
| --- | --- | --- | --- |
| [X Suppl. 13](http://handle.itu.int/11.1002/1000/13730) | 07-09-2018 | En vigueur | UIT-T X.1051 – Supplément sur un guide de mise en œuvre de la Recommandation UIT-T X.1051 sur la gestion de la sécurité des informations |
| [X Suppl. 26 (2016) Cor.1](http://handle.itu.int/11.1002/1000/13592) | 29-03-2018 | En vigueur |  |
| [X Suppl. 29](http://handle.itu.int/11.1002/1000/13409) | 06-09-2017 | En vigueur | UIT-T X.1242 – Supplément sur les lignes directrices relatives aux mesures de rétorsion à prendre pour lutter contre les attaques par hameçonnage par le service de messages courts |
| [X Suppl. 30](http://handle.itu.int/11.1002/1000/13410) | 06-09-2017 | En vigueur | UIT-T X.805 – Supplément sur les lignes directrices relatives à la sécurité pour les opérateurs de réseaux virtuels mobiles |
| [X Suppl. 31](http://handle.itu.int/11.1002/1000/13411) | 06-09-2017 | En vigueur | UIT-T X.660 – Supplément sur les lignes directrices relatives à l'utilisation des identificateurs d'objet pour l'Internet des objets  |
| [X Suppl. 32](http://handle.itu.int/11.1002/1000/13593) | 29-03-2018 | En vigueur | UIT-T X.1058 – Supplément sur le code de bonne pratique pour la protection des informations d'identification personnelle (PII) à l'intention des organisations de télécommunication |
| [X Suppl. 33](http://handle.itu.int/11.1002/1000/13731) | 07-09-2018 | En vigueur | UIT-T X.1231 – Supplément sur le cadre technique de lutte contre les escroqueries par service téléphonique  |
| [X Suppl. 34](http://handle.itu.int/11.1002/1000/13869) | 30-01-2019 | En vigueur | UIT-T X.1051 – Supplément sur le code de bonne pratique pour les contrôles de sécurité de l'information pour les organisations de télécommunication |
| [X Suppl. 35](http://handle.itu.int/11.1002/1000/14066) | 05-09-2019 | En vigueur | UIT-T X.1254 – Supplément sur les cas d'utilisation du cadre de garantie d'authentification des entités (EAA) |
| [X Suppl. 36](http://handle.itu.int/11.1002/1000/14809) | 03-09-2021 | En vigueur | ITU-T X.1051 – Supplément sur les contrôles critiques de la sécurité pour la gestion de la sécurité de l'information et des réseaux des organisations de télécommunication |

Tableau 12

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

|  |  |  |  |
| --- | --- | --- | --- |
| Désignation | Date | Titre | Type de publication |
| [TP.inno](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15153) | 03/09/2020 | Description du mécanisme d'incubation et des moyens permettant de l'améliorer | Document technique |
| [TP.sgstruct](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15154) | 03/09/2020 | Approches stratégiques concernant les études sur la transformation de la sécurité | Document technique |
| [TR.ors](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15256) | 26/03/2020 | Système de résolution des identificateurs OID: Problèmes, exigences et solutions possibles | Rapport technique |
| [TR.sec-manual](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14367) | 03/09/2020 | Sécurité dans les télécommunications et les technologies de l'information: (7ème édition) | Rapport technique |
| [TR.sec-qkd](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14825) | 26/03/2020 | Considérations relatives à la sécurité des réseaux prenant en charge la distribution de clés quantiques  | Rapport technique |
| [TR.Suss](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14370) | 03/09/2020 | Utilisation efficace des normes de sécurité (2ème édition) | Rapport technique |
| [TR.usm](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15241) | 03/09/2020 | Modèle de sécurité unifié (USM) – Une approche système intégrée neutre en matière de cybersécurité | Rapport technique |
| [TR.XAASL](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16769) | 03-09-2021 | Rapport technique : Cadre pour la normalisation de la sécurité des services virtualisés | Rapport technique |
| [XSTR-SEC-QKD Cor.1](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16969) | 30-04-2021 | Considérations relatives à la sécurité des réseaux de distribution de clés quantiques – Corrigendum 1 | Rapport technique |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16983) | 30-04-2021 | Guide de mise en œuvre du langage de description et de spécification de la Recommandation UIT-T Z.100 – Version 4.0.1 | Guide de mise en œuvre |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14424) | 07/09/2018 | Guide de mise en œuvre du langage de description et de spécification de la Recommandation UIT-T Z.100 – Version 3.0.2 | Guide de mise en œuvre |
| [Z.Imp100rev](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14816) | 05/09/2019 | Guide de mise en œuvre du langage de description et de spécification de la Recommandation UIT-T Z.100 – Version 4.0.0 | Guide de mise en œuvre |

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 |
| --- | --- | --- | --- |
| Néant |  |  |  |

ANNEXE 2

Propositions de révision de la Résolution 2 de l'AMNT
par la Commission d'études 17

Annexe A

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).

Garantir la sécurité au moyen des TIC et assurer la sécurité des TIC sont les principaux sujets d'étude confiés à la Commission d'études 17 de l'UIT-T. Cette Commission d'études est notamment chargée de mener des études se rapportant à la cybersécurité, aux services de sécurité gérés, à la détection et à la réponse du point d'extrémité, à la gestion de la sécurité, à la lutte contre le spam et à la gestion d'identité. Elle est également chargée d'étudier l'architecture et le cadre général de la sécurité, la sécurité quantique, la sécurité des technologies de registres distribués (DLT), la sécurité des systèmes de transport intelligents, les aspects liés à la sécurité de l'IA et la sécurité des réseaux, des applications et des services tels que l'Internet des objets (IoT) et les villes intelligentes, divers types de réseaux tels que les réseaux IMT-2020/5G et au-delà, les réseaux électriques intelligents, les systèmes de contrôle industriel (ICS), la chaîne d'approvisionnement, les smartphones, les réseaux pilotés par logiciel (SDN), la virtualisation des fonctions de réseau (NFV), la télévision utilisant le protocole Internet (TVIP), les services web, les services over-the-top (OTT), les réseaux sociaux, l'informatique en nuage, l'analyse des mégadonnées, les services financiers numériques et la télébiométrie.

Le renforcement de la confiance et de la sécurité dans l'utilisation des TIC comprend également la protection des informations d'identification personnelle (PII), par exemple les aspects techniques et opérationnels de la protection des données pour ce qui est de garantir la confidentialité, l'intégrité et la disponibilité des informations PII.

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 2020

…

Commission d'études 17 de l'UIT-T

La Commission d'études 17 de l'UIT-T est chargée d'élaborer des Recommandations techniques essentielles visant à renforcer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC).

À cette fin, 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 et la sécurité des réseaux, des applications et des services tels que l'Internet des objets (IoT), les systèmes de transport intelligents, les services applicatifs sécurisés, les réseaux sociaux, l'informatique en nuage, la technologie des registres distribués, 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.

Le rôle de la Commission d'études 17 de l'UIT-T est de fournir des solutions techniques pour traiter les questions relatives à la sécurité des TIC et assurer la sécurité au moyen des TIC. Les études qui lui sont confiées portent tout particulièrement sur la sécurité dans de nouveaux domaines tels que la sécurité pour les réseaux IMT2020/5G et au-delà, l'Internet des objets (IoT), les villes intelligentes, les technologies de registres distribués (DLT), l'analyse des mégadonnées, les systèmes de transport intelligents, les aspects sécurité liés à l'IA et les technologies quantiques. En outre, la CE 17 est chargée de mener des études sur la gestion des informations d'identification personnelle (PII), par exemple les aspects techniques et opérationnels de la protection des données pour ce qui est de garantir la confidentialité, l'intégrité et la disponibilité des informations PII.

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), par exemple les aspects techniques et opérationnels de la protection des données; et la lutte contre le spam par des moyens techniques.

La Commission d'études 17 assure la coordination générale des travaux menés par l'UIT-T en sa qualité de commission d'études directrice pour la sécurité, la gestion des identités ainsi que les langages et les techniques de description.

En outre, la Commission d'études 17 est responsable de l'élaboration des principales Recommandations sur la sécurité des technologies de registres distribués (DLT), la sécurité des systèmes de transport intelligents, les aspects relatifs à la sécurité des applications et des services liés à la TVIP, de divers types de réseaux tels que les réseaux IMT-2020/5G et au-delà, des réseaux électriques intelligents, des systèmes de contrôle industriel (ICS), de la chaîne d'approvisionnement, de l'Internet des objets et des villes intelligentes, des réseaux pilotés par logiciel (SDN), de la virtualisation NFV, des réseaux sociaux, de l'informatique en nuage, de l'analyse des mégadonnées, des smartphones, des services financiers numériques et de 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, qui portent sur différents langages, par exemple ASN.1, SDL, MSC, URN et TTCN-3.

La Commission d'études 17 assure la coordination des travaux relatifs à la sécurité menés par toutes les commissions d'études de l'UIT-T. Ces travaux seront menés en fonction des besoins des commissions d'études concernées (Commissions d'études 2, 9, 11, 13, 15, 16 et 20) et en collaboration avec elles.

La Commission d'études 17 travaillera sur les aspects pertinents de la gestion d'identité en collaboration avec la Commission d'études 20 et avec la Commission d'études 2, conformément au mandat de chaque commission d'études.

…

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 2021-2024

…

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, 3, 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

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