List of work items from the September 2012 SG 17 meeting

| Q(1) | Acronym | Title | New / Revised | Editor(s) | Location of Text (Date) | Equivalent e.g., ISO/IEC | Timing\*\*\* |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2/17 | X.gsiiso | Guidelines on security of the individual information service for operators | New | Yuanfei Huang, Lijun Liu, Ziqin Sang, Huirong Tian | TD 3156 (2012-09) |  | 2014-01 |
| 2/17, (7/17, 10/17) | X.hsn\* | Heterarchic architecture for secure distributed service networks | New | Yuri Pankratov | TD 2548 (2011-09) |  | 2014-01 |
| 2/17, (3/17) | X.ipv6-secguide | Technical guideline on deploying IPv6 | New | Masashi Eto, Koji Nakao | C 678, C 753 Rev.1 |  | 2013-04 |
| 2/17, (3/17) | X.mgv6\*\* | Supplement to ITU-T X.ipv6-secguide – Supplement on security management guideline for implementation of IPv6 environment in telecommunications organizations | New | Masashi Eto, Koji Nakao | TD 3182 (2012-09) |  | 2014-01 |
| 2/17 | X.vissec \* | Security of digital broadcasting and multimedia video information systems (VIS Security) | New | Dmitry Kostrov | COM 17 – R 48 Annex B Attachment 1 (2012-03) |  | 2014-01 |
| 3/17, (10/17) | X.gpim | Guideline for management of personally identifiable information for telecommunication organizations | New | Soonjoung Byun, Jungduk Kim, Lijun Liu Heung Youl Youm | TD 3186 Rev.1 (2012-09) |  | 2015 |
| 3/17 | X.sgsm | Information security management guidelines for small and medium telecommunication organizations | New | Ki-ho Lee, Junduk Kim, Wataru Senga | TD 3202 (2012-09) |  | 2013-04 |
| 3/17 | X.sup1056 \*\* | Supplement to ITU-T X.1056 – Related Recommendations, International Standards and documents for security incident management | New | Junduk Kim, Miho Naganuma, Damir Rajnovic | TD 3184 (2012-09) |  | 2014 |
| 4/17, (12/17) | X.1303 | Common alerting protocol (CAP 1.2) | Revised | Olivier Dubuisson, Youki Kadobayashi | TD 1629 (2011-04) |  | 2014-01 |
| 4/17 | X.1500 Amd.3 \*\* | Overview of cybersecurity information exchange – Amendment 3 – Revised structured cybersecurity information exchange techniques |  | Youki Kadobayashi | TD 3167 Rev.2 (2012-09) |  | 2013-04 |
| 4/17 | X.1526 (X.oval) | Open vulnerability and assessment language | New | Robert A. Martin | COM 17 – R 64 |  | 2012-09 |
| 4/17 | X.1544 (X.capec) | Common attack pattern enumeration and classification | New | Robert A. Martin | COM 17 – R 65 |  | 2012-09 |
| 4/17 | X.abnot \*\* | Supplement to ITU-T X.series Supplement on guidelines for abnormal traffic detection and control on IP-based networks | New | Xu Chen, Shen He, Lijun Liu, Lanfang Ren, Zhiguo Zhan, Min Zuo | TD 3155 (2012-09) |  | 2013-04 |
| 4/17 | X.bots\* | Centralized framework for botnet detection and response | New | Hyun Cheol Jeong, Mi Joo Kim, Joo Hyung Oh, Yoo Jae Won | TD 2756 Rev.1 (2011-09) |  | 2014-01 |
| 4/17 | X.cce\* | Common configuration enumeration | New | Robert A. Martin | TD 3094 (2012-09) |  | 2014-01 |
| 4/17 | X.cee\* | Common event expression | New | Robert A. Martin | TD 3104 (2012-09) |  | 2014-01 |
| 4/17 | X.cee.1\* | CEE architecture overview | New | Robert A. Martin | TD 3107 (2012-09) |  | 2014-01 |
| 4/17 | X.cee.2\* | CEE dictionary and event taxonomy (CDET) | New | Robert A. Martin | TD 3105 (2012-09) |  | 2014-01 |
| 4/17 | X.cee.3\* | CEE log syntax (CLS) encoding | New | Robert A. Martin | TD 3108 (2012-09) |  | 2014-01 |
| 4/17 | X.cee.4\* | CEE log recommendations (CELR) profile | New | Robert A. Martin | TD 3103 (2012-09) |  | 2014-01 |
| 4/17 | X.cee.5\* | CEE log transport (CLT) requirements | New | Robert A. Martin | TD 3106 (2012-09) |  | 2014-01 |
| 4/17 | X.csi\* | Guidelines for cybersecurity index | New | Damir Rajnovic, Heung Youl Youm | TD 3136 (2012-09) |  | 2013-04 |
| 4/17 | X.csmc\* | Continuous security monitoring using CYBEX techniques | New | Inette Furey, Youki Kadobayashi, Robert A. Martin, Kathleen Moriarty, Gregg Schudel, Takeshi Takahashi | TD 2569 Rev.1 (2011-09) |  | 2014-01 |
| 4/17 | X.cwss\* | Common weakness scoring system | New | Robert A. Martin | TD 3095 (2012-09) |  | 2014-01 |
| 4/17 | X.cybex-beep\* | A BEEP profile for cybersecurity information exchange techniques | New | Youki Kadobayashi | TD 2075 (2011-09) |  | 2014-01 |
| 4/17 | X.cybex-tp\* | Transport protocols supporting cybersecurity information exchange | New | Youki Kadobayashi, Damir Rajnovic | TD 2567 (2011-09) |  | 2014-01 |
| 4/17 | X.eipwa\* | Guideline on techniques for preventing web-based attacks | New | Xie Wei, Heung Youl Youm | TD 3134 (2012-09) |  | 2014-01 |
| 4/17 | X.maec\* | Malware attribute enumeration and classification | New | Robert A. Martin | TD 3093 (2012-09) |  | 2014-01 |
| 4/17 | X.sisnego\* | Framework of security information sharing negotiation | New | Gae-il An, Jong Hyun Kim, Kathleen Moriarty | TD 3165 (2012-09) |  | 2014-01 |
| 4/17 | X.trm\* | Overview of traceback mechanisms | New | Youki Kadobayashi, Huirong Tian, Heung Youl Youm | TD 3135 (2012-09) |  | 2013-04 |
| 5/17 | X.ticvs\* | Technologies involved in countering voice spam in telecommunication organizations | New | Xuetao Du, Tao Lou | TD 3228 (2012-09) |  | 2014-01 |
| 6/17 | X.1126 (X.msec-6) | Security aspects of smartphones | New | Hongwei Luo, Yutaka Miyake | COM 17 – R 67 |  | 2012-09 |
| 6/17 | X.1196 (X.iptvsec-6) | Framework for the downloadable service and content protection system in the mobile Internet Protocol Television (IPTV) environment | New | Heung-Youl Youm | TD 3188 Rev.1 (2012-09) Note (2) |  | 2012-09 |
| 6/17 | X.1313 (X.usnsec-3) | Security requirements for wireless sensor network routing | New | Mijoo Kim | TD 3185 Rev.1 (2012-09) |  | 2012-09 |
| 6/17 | X.iptvsec-8 | Virtual machine-based security platform for renewable IPTV service and content protection (SCP) | New | Yong Ho Hwang, Jongyoul Park | TD 3099 (2012-09) |  | 2013-04 |
| 6/17 | X.msec-7 | Guidelines on the management of infected terminals in mobile networks | New | Xuetao Du, Lou Tao, Chen Zhang, | TD 3243 (2012-09) |  | 2014-01 |
| 6/17 | X.msec-8 | Secure application distribution framework for communication devices | New | Mijoo Kim, Yutaka Miyake, Heung Youl Youm | TD 3203 (2012-09) |  | 2014-01 |
| 6/17 | X.sgsec-1 | Security functional architecture for smart grid services using telecommunication network | New | Tadashi Kaji, Mijoo Kim, Mi Yeon Yoon | TD 3189 Rev.1 (2012-09) |  | 2014-01 |
| 6/17 | X.unsec-1 | Security requirements and framework of ubiquitous networking | New | Xia Junjie, Lijun Liu, Wang Shitong | TD 2667 (2012-04) |  | 2014-01 |
| 7/17, (10/17) | X.1141 Amd.1 | Security Assertion Markup Language (SAML) 2.0 – Amendment 1: Errata |  | Abbie Barbir | TDs 1571, 1572, 1573, 1574, 1575, 1577, 1578, 1579, 1580, 1581, 1582, 1583, 1584, 1585, 1586, 1587, 1588 (2011-04) | OASIS SAML 2.0 | 2013-04 |
| 7/17, (10/17) | X.1142 Amd.1 | eXtensible Access Control Markup Language (XACML 2.0) – Amendment 1: Errata |  | Abbie Barbir | TDs 1556, 1557, 1569 (2011-04) | OASIS XACML 2.0 | 2013-04 |
| 7/17, (10/17) | X.1154 (X.sap-4) | General framework of combined authentication on multiple identity service provider environments | New | Tadashi Kaji, Hyung-jin Lim | COM 17 – R 68 |  | 2012-09 |
| 7/17 | X.1164 (X.p2p-4) | Use of service providers’ user authentication infrastructure to implement public key infrastructure for peer-to-peer networks | New | Ayumu Kubota, Yutaka Miyake | TD 3082 (2012-09) |  | 2012-09 |
| 7/17 | X.p2p-3 | Security requirements and mechanisms of peer-to-peer based telecommunication network | New | Lijin Liu | TD 2333 (2011-09) |  | 2014-09 |
| 7/17 | X.sap-6 | Non-repudiation framework based on a one time password | New | Keun-ok Kim, Hee-won Shim, Seong-Hyeon Song | TD 3177 (2012-09) |  | 2013-04 |
| 7/17 | X.sap-5 | Guideline on local linkable anonymous authentication for electronic services | New | Sok Joon Lee | TD 3151 (2012-09) |  | 2014-09 |
| 7/17 | X.sap-7 | Technical capabilities of fraud detection and response for services with high assurance level requirements | New | Tae Kyun Kim, Hyung-Jin Lim | TD 3145 (2012-09) |  | 2014-09 |
| 7/17, (10/17) | X.sap-8 | Efficient multi-factor authentication mechanisms using mobile devices | New | Heung-Youl Youm | TD 3157 (2012-09) |  | 2014-09 |
| 7/17 | X.sap-9 | Delegated non-repudiation architecture based on ITU-T X.813 | New | Keun-ok Kim, Hee-won Shim, Seong-Hyeon Song | TD 3142 Rev.1 (2012-09) |  | 2014-09 |
| 7/17 | X.websec-5 | Security architecture and operations for web mashup services | 7/17 | Jaehoon Nah, H.R. Oh | TD 2612 Rev.2 (2012-03) |  | 2014-09 |
| 7/17, (10/17) | X.xacml3 | eXtensible Access Control Markup Language (XACML) 3.0 | New | Abbie Barbir | TDs 1570, 1568, 1567, 1566, 1565, 1564, 1563, 1562, 1561, 1560, 1559, 1558 (2011-04) | OASIS XACML 3.0 | 2013-04 |
| 8/17 | X.ccsec\* | High-level security framework for cloud computing | New | Ruan He, Jun Shen Huirong Tian, Laifu Wang, Peng Zhao, Lin Zhaoji | TD 3191 Rev.1 (2012-09) |  | 2013-04 |
| 8/17, (7/17) | X.fsspvn\* | Framework for a secure service platform for virtual network | New | Min Huang, Jun Shen, Huirong Tian, Yuchen Wang | TD 3051 (2012-09) |  | 2014-01 |
| 8/17 | X.goscc\* | Guidelines of operational security for cloud computing | New | Ming Feng, Zhaoji Lin, Jun Shen, Huirong Tian, Laifu Wang | TD 3195 Rev.1 (2012-09) |  | 2014-01 |
| 8/17 | X.sfcse\* | Security functional requirements for Software as a Service (SaaS) application environment | New | Peng Zhao, Zhaoji Lin, Yanbing Zheng | TD 3060 (2012-09) |  | 2014-01 |
| 9/17, (11/17) | X.bhsm | Telebiometric authentication framework using biometric hardware security module | New | Myung Geun Chun, Yong Nyuo Shin | TD 3171 (2012-09) | ISO/IEC 17922 | 2014-09 |
| 9/17 | X.tam | A guideline to technical and operational countermeasures for telebiometric applications using mobile devices | New | Jae-Sung Kim, Yong Nyuo Shin | TD 3162 (2012-09) |  | 2015 |
| 9/17 | X.th2\* | Telebiometrics related to physics | New | Michele Peiry | TD 3055 (2012-09) | ISO 80003-2  Note (2) | 2014 |
| 9/17 | X.th3\* | Telebiometrics related to chemistry | New | Michele Peiry | TD 3056 (2012-09) | ISO 80003-3  Note (2) | 2014 |
| 9/17 | X.th4\* | Telebiometrics related to biology | New | Paul Gerome | TD 3043 (2012-09) | IEC 80003-4  Note (2) | 2014 |
| 9/17 | X.th5\* | Telebiometrics related to culturology | New | Paul Gerome | TD 3044 (2012-09) | IEC 80003-5  Note (2) | 2014 |
| 9/17 | X.th6\* | Telebiometrics related to psychology | New | Paul Gerome | TD 3045 (2012-09) | IEC 80003-6  Note (2) | 2014 |
| 9/17 | X.tif | Integrated framework for telebiometric data protection in e-health and worldwide telemedicines | New | Jae-Sung Kim, Yong Nyuo Shin, Seung Jai Yi | TD 3173 (2012-09) |  | 2013-04 |
| 10/17 | X.atag\* | Attribute aggregation framework | New | David W Chadwick, Ryu Watanabe | TD 2739 (2012-03) |  | 2014-01 |
| 10/17 | X.authi\* | Guideline to implement the authentication integration of the network layer and the service layer. | New | Lijun Liu | TD 3210 (2012-09) |  | 2014-01 |
| 10/17 | X.discovery\* | Discovery of identity management information | New | Robert Kahn | TD 3179 Rev.1 (2012-09) |  | 2013-04 |
| 10/17 | X.giim\* | Mechanisms to support interoperability across different IdM services | New | Jing Wu | TD 3039 Rev.2 (2012-09) |  | 2013-04 |
| 10/17 | X.iamt\* | Identity and access management taxonomy | New | Radu Marian | TD 3140 Rev.5 (2012-09) |  | 2016 |
| 10/17, (8/17) | X.idmcc\* | Requirement of IdM in cloud computing | New | Xiao Ming Guang, Jing Wu | TD 2228 (2011-09) |  | 2014-01 |
| 10/17 | X.mob-id\* | Baseline capabilities and mechanisms of identity management for mobile applications and environment | New | Sangrae Cho | TD 3164 (2012-09) |  | 2013-04 |
| 10/17 | X.oitf\* | Open identity trust framework | New | ZhaoJi Lin, David Turner | TD 3058 (2012-09) |  | 2014-01 |
| 10/17, 16/13 | X.scim-use\* | Application of system for cross identity management (SCIM) in telecommunication environments | New | Radu Marian, Zachary Zeltsan | TD 3242 Rev.1 (2012-09) |  | 2016 |
| 11/17 | E.115 (2010) Cor.1 | Computerized directory assistance – Corrigendum 1 |  | Erik Andersen | TD 3079 (2012-09) |  | 2012-09 |
| 11/17, (10/17) | F.5xx | Directory Service - Support of Tag-based Identification Services | New | Erik Andersen | TD 3222 (2012-09) |  | 2014-01 |
| 11/17 | X.500 (seventh edition) | Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services | Revised | Erik Andersen | TD 3070 (2012-09) | ISO/IEC 9594-1 | 2012-09 |
| 11/17 | X.501 (2008) Cor.3 | Information technology – Open Systems Interconnection – The Directory: models – Technical Corrigendum 3 |  | Erik Andersen | TD 3064 (2012-09) | ISO/IEC 9594-2:2008 Cor.3 | 2012-09 |
| 11/17 | X.501 (seventh edition) | Information technology – Open Systems Interconnection – The Directory – Models | Revised | Erik Andersen | TD 3071 Rev.1 (2012-09) | ISO/IEC 9594-2 | 2012-09 |
| 11/17 | X.509 (2008) Cor.3 | Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks – Technical Corrigendum 3 |  | Erik Andersen | TD 3068 (2012-09) | ISO/IEC 9594-8:2008 Cor.3 | 2012-09 |
| 11/17 | X.509 (seventh edition) | Information technology – Open Systems Interconnection – The Directory – Public-key and attribute certificate frameworks | Revised | Erik Andersen | TD 3072 Rev.1 (2012-09) | ISO/IEC 9594-8 | 2012-09 |
| 11/17 | X.511 (2008) Cor.3 | Information technology – Open systems interconnection – The Directory: Abstract service definition – Technical Corrigendum 3 |  | Erik Andersen | TD 3065 (2012-09) | ISO/IEC 9594-3:2008 Cor.3 | 2012-09 |
| 11/17 | X.511 (seventh edition) | Information technology – Open Systems Interconnection – The Directory – Abstract Service Definition | Revised | Erik Andersen | TD 3073 Rev.1 (2012-09) | ISO/IEC 9594-3 | 2012-09 |
| 11/17 | X.518 (2008) Cor.2 | Information technology – Open systems interconnection – The Directory: Procedures for distributed operation – Technical Corrigendum 2 |  | Erik Andersen | TD 3066 Rev.2 (2012-09) | ISO/IEC 9594-4:2008 Cor.2 | 2012-09 |
| 11/17 | X.518 (seventh edition) | Information technology – Open Systems Interconnection – The Directory – Procedures for Distributed Operations | Revised | Erik Andersen | TD 3074 Rev.1 (2012-09) | ISO/IEC 9594-4 | 2012-09 |
| 11/17 | X.519 (seventh edition) | Information technology – Open Systems Interconnection – The Directory – Protocols | Revised | Erik Andersen | TD 3075 Rev.1 (2012-09) | ISO/IEC 9594-5 | 2012-09 |
| 11/17 | X.520 (2008) Cor.3 | Information technology – Open systems interconnection – The Directory: Selected Attribute types – Technical Corrigendum 3 |  | Erik Andersen | TD 3067 (2012-09) | ISO/IEC 9594-6:2008 Cor.3 | 2012-09 |
| 11/17 | X.520 (seventh edition) | Information technology – Open Systems Interconnection – The Directory – Selected Attribute Types | Revised | Erik Andersen | TD 3076 Rev.1 (2012-09) | ISO/IEC 9594-6 | 2012-09 |
| 11/17 | X.521 (seventh edition) | Information technology – Open Systems Interconnection – The Directory – Selected object classes | Revised | Erik Andersen | TD 3077 Rev.1 (2012-09) | ISO/IEC 9594-7 | 2012-09 |
| 11/17 | X.525 (seventh edition) | Information technology – Open Systems Interconnection – The Directory – Replication | Revised | Erik Andersen | TD 3078 Rev.1 (2012-09) | ISO/IEC 9594-9 | 2012-09 |
| 11/17, (10/17) | X.pki-em | Information Technology - Public-Key Infrastructure: Establishment and maintenance | New | Erik Andersen | TD 3198 Rev.2 (2012-09) |  | 2016-09 |
| 11/17, (10/17) | X.pki-prof | Information Technology - Public-Key Infrastructure: Profile | New | Erik Andersen | TD 3199 Rev.2 (2012-09) |  | 2016-09 |
| 12/17 | X.667 | Information technology –Procedures for the operation of object identifiers registration authority: Generation of Universally Unique Identifiers (UUIDs) and their use in object identifiers | Revised | Olivier Dubuisson | TD 3083 Rev.3 (2012-09) | ISO/IEC 9834-8 | 2012-09 |
| 13/17 | X.906 | Open distributed processing – Use of UML for ODP system specification | Revised | Arve Meisingset | TD 2369 (2012-03) | ISO/IEC 19793 | 2014-09 |
| 13/17 | X.911 | Open distributed processing – Reference model – Enterprise language | Revised | Arve Meisingset | TD 2368 (2012-03) | ISO/IEC 15414 | 2014-01 |
| 13/17 | Z.100 Annex F1 | SDL formal definition: General overview | Revised | Edel Sherratt | TD 2980 (2012-09) |  | 2013-04 |
| 13/17 | Z.104 Amd.1 | Data and action language in SDL-2010 – Amendment 1: Annex C – Language Binding |  | Rick Reed | TD 2951 Rev.4 (2012-09) |  | 2012-09 |
| 13/17 | Z.109 Amd.1 | Unified modeling language (UML) profile for SDL-2010: Amendment 1: Appendix I – Example language specification |  | Thomas Weigert | TD 2984 Rev.5 (2012-09) |  | 2012-09 |
| 13/17 | Z.151 | User requirements notation (URN) – Language definition | Revised | Daniel Amyot | TD 3121 Rev.1 (2012-09) |  | 2012-09 |
| 13/17 | Z.Sup1\*\* | Supplement 1 to Z-series Recommendations – ITU-T Z.100-series – Supplement on methodology on the use of description techniques | Revised | Rick Reed, Thomas Weigert |  |  | 2013-04 |
| 14/17 | Z.161 | Testing and Test Control Notation version 3: TTCN-3 core language | Revised | Dieter Hogrefe |  | ETSI ES 201 873-1 | 2013-04 |
| 14/17 | Z.161.1 | The Testing and Test Control Notation version 3: TTCN-3 Language Extensions: Support of interfaces with continuous signals | Revised | Dieter Hogrefe |  | ETSI ES 202 786 | 2013-04 |
| 14/17 | Z.164 | Testing and Test Control Notation version 3: TTCN-3 operational semantics | Revised | Dieter Hogrefe |  | ETSI ES 201 873-4 | 2013-04 |
| 14/17 | Z.165 | Testing and Test Control Notation version 3: TTCN-3 runtime interface (TRI) | Revised | Dieter Hogrefe |  | ETSI ES 201 873-5 | 2013-04 |
| 14/17 | Z.165.1 | The Testing and Test Control Notation version 3: Extension Package: Extended TRI | Revised | Dieter Hogrefe |  | ETSI ES 202 789 | 2013-04 |
| 14/17 | Z.166 | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) | Revised | Dieter Hogrefe |  | ETSI ES 201 873-6 | 2013-04 |
| 14/17 | Z.167 | Testing and Test Control Notation version 3: TTCN-3 mapping from ASN.1 | Revised | Dieter Hogrefe |  | ETSI ES 201 873-7 | 2013-04 |
| 14/17 | Z.168 | Testing and Test Control Notation version 3: TTCN-3 mapping from CORBA IDL | Revised | Dieter Hogrefe |  | ETSI ES 201 873-8 | 2013-04 |
| 14/17 | Z.169 | Testing and Test Control Notation version 3: TTCN-3 mapping from XML data definition | Revised | Dieter Hogrefe |  | ETSI ES 201 873-9 | 2013-04 |
| 14/17 | Z.170 | Testing and Test Control Notation version 3: TTCN-3 documentation comment specification | Revised | Dieter Hogrefe |  | ETSI ES 201873-10 | 2013-04 |

Notes:

\* Marked draft Recommendations are for determination; all non-marked are for consent.

\*\* Texts for approval (AAP/TAP) not applicable)

\*\*\* Target date for consent or determination of Recommendations or for approval of Appendices, Supplements or Implementers’ Guides

(1) SG17 Question. In case of joint Question activity, the lead Question is given without parentheses and other Questions are shown in parentheses; such entries are only shown in the table against the lead Question.

(2) Complementary texts (neither common nor twin texts).

# Summaries for work items under development in Study Group 17

WORKING PARTY 1/17 - **NETWORK AND INFORMATION SECURITY**

Question 2/17 – Security architecture and framework

**X.gsiiso, *Guidelines on security of the individual information service for operators***

This Recommendation addresses the aspects of security of the information service provided by the telecommunication operators. In the transforming from traditional basic network operator to comprehensive information service provider, the operators expand their services to content service and ICT. The new services not only change the operational models, and they also bring new security issues to be resolved.

This Recommendation provides guidelines on security of the individual information service for operators. The scope covers the classification of individual information service, the security requirement, the mechanism, and the coordination.

**X.hsn, *Heterarchic architecture for secure distributed service networks***

This Recommendation describes heterarchic security architecture for distributed service networks (defined in Recommendation ITU-T Y.2206). The security architecture is based on the use of a system of network entity identifiers (or identity certificates) and a distributed system of storage and retrieval of information associated with these identifiers. Another aspect of the security architecture is a distributed trust management system and the security functions based on it. The security architecture is based on the use of an overlaying logical network and does not interfere with the basic service functionality.

**X.ipv6-secguide, *Technical security guideline on deploying IPv6***

IPv6 is intended to provide many built-in benefits such as large address space, mobility, and quality of service (QoS). Because it is a new protocol and operates in some different ways than IPv4, both foreseeable and unforeseeable security issues are likely to arise. Many new functions or requirements of IPv6, i.e., automatic configuration of interfaces, mandatory IPsec, mandatory multicast, multiple IP addresses and many new rules for routing, can be abused for compromising computer systems or networks.

Considering the above circumstance, this Recommendation provides a set of technical security guides for telecommunications organizations to implement and deploy IPv6 environment. This Recommendation focuses on how to securely deploy network facilities for telecommunications organizations and how to ensure security operations for IPv6 environment.

**X.mgv6, *Supplement to X-series Recommendations, ITU-T X.ipv6-secguide – Supplement on security management guideline for implementation of IPv6 environment in telecommunications organizations***

This Supplement provides a set of information security management guides for telecommunications organizations to develop and implement IPv6 telecommunication environment. Focusing on network facilities for telecommunications organizations, necessary security controls and implementation guidance for IPv6 implementation as an extension of ITU-T X.1051 are developed.

**X.vissec, *Security of digital broadcasting and multimedia video information systems (VIS Security)***

This Recommendation:

a) establishes baselines and general principles for assessing and analyzing security threats and requirements in digital broadcasting and multimedia video information systems (VIS) in telecommunication environments;

b) provides a baseline of security architecture for telecommunication members to ensure the confidentiality, integrity and availability of telecommunications facilities and services for video information systems.

Question 3/17 – Telecommunications information security management

**X.gpim, *Guideline for management of personally identifiable information for telecommunication organizations***

This Recommendation provides a guideline of management of personally identifiable information (PII) in the context of telecommunications. It also defines privacy controls and good practices for personally identifiable information protection. The objective of this Recommendation is to provide a common ground for the management of PII, for providing confidence in its management. It does not address the management system for protection of PII.

The Recommendation is applicable to an organization including a telecommunication organization throughout the life cycle of personally identifiable information. The Recommendation is also applicable to all types and sizes of telecommunication organizations, which collect, use, process personally identifiable information as part of information processing.

**X.sgsm, *Information security management guidelines for small and medium-sized telecommunication organizations***

This Recommendation provides guidelines for establishing and operating information security management for small and medium-sized telecommunication organizations (SMTOs) in the telecommunication industry.

It covers some of necessary security controls from Rec. ITU-T X.1051 | ISO/IEC 27011 for information security management in the context of small and medium telecommunication organizations without huge cost and human resources to implement its information security management system.

**X.sup1056 (Supplement to ITU-T X.1056), *Related Recommendations, International Standards and documents for security incident management***

Supplement to ITU-T X.1056 is to list up information on security incident management and a mapping with related international standards, Recommendations and other documents. Such information includes a general incident handling and how to establish incident response team, and also covers ICT readiness for business continuity and disaster recovery and particular information is also applicable to development countries.

Question 4/17 – Cybersecurity

**Draft X.1303 (X.cap), Common alerting protocol (CAP 1.2)**

The common alerting protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. CAP also provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

Recommendation ITU-T X.1303 also provides both an XSD specification and an equivalent ASN.1 specification (that permits a compact binary encoding) and allows the use of ASN.1 as well as XSD tools for the generation and processing of CAP messages. This Recommendation enables existing systems, such as systems based on Recommendation ITU-T H.323, to more readily encode, transport and decode CAP messages.

**X.1500 Amd.3, *Overview of cybersecurity information exchange – Amendment 3 – Revised structured cybersecurity information exchange techniques***

Amendment 3 to Recommendation ITU-T X.1500 (2011) provides a list of structured cybersecurity information techniques that have been created to be continually updated as these techniques evolve, expand, are newly identified or are replaced. The list follows the outline provided in the body of the Recommendation. This amendment reflects the situation of recommended techniques as of April 2013, including bibliographical references.

**Draft X.1526 (X.oval), *Open vulnerability and assessment language***

This Recommendation on the use of the Open Vulnerability and Assessment Language (OVAL), an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analysing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three schemas written in Extensible Markup Language (XML) to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process: an OVAL System Characteristics schema for representing system information, an OVAL Definition schema for expressing a specific machine state, and an OVAL Results schema for reporting the results of an assessment.

Content written in the OVAL Language is located in one of the many repositories found within the community. One such repository is known as the OVAL Repository. It is the central meeting place for the OVAL Community to discuss, analyse, store, and disseminate OVAL Definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developers Forum and by writing definitions for the OVAL Repository through the OVAL Community Forum. An OVAL Board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL Web site. This means that OVAL reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.

**Draft X.1544 (X.capec), *Common attack pattern enumeration and classification***

This Recommendation is an XML/XSD based specification for the identification, description, and enumeration of attack patterns. Attack patterns are a powerful mechanism to capture and communicate the attacker’s perspective. They are descriptions of common methods for exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. The objective of CAPEC is to provide a publicly available catalogue of attack patterns along with a comprehensive schema and classification taxonomy.

CAPEC enables:

• Standardizing the capture and description of attack patterns

• Collecting known attack patterns into an integrated enumeration that can be consistently and effectively leveraged by the community

• Classifying attack patterns such that users can easily identify the subset of the entire enumeration that is appropriate for their context

• Linking the attack patterns and the weaknesses (CWEs) that they are effective against through explicit references.

As many sources and examples as possible are leveraged from the CAPEC community and other interested parties, to develop the specific and succinct definitions of the CAPEC Dictionary elements and a variety of views and classification tree structures.

**X.abnot, Supplement *on guidelines for* *abnormal traffic detection and control on IP based networks***

This Supplement identifies abnormal traffic detection technologies and control measures for IP-based telecommunication network. The aim of this document is to provide telecommunication operators with a comprehensive guideline for monitoring, detecting and controlling of abnormal IP traffic.

**X.bots, *Centralized framework for botnet detection and response***

This Recommendation specifies a centralized framework for botnet detection and response. The Recommendation describes a definition, composition characteristics and behavior models of botnet. Also, it specifies various types of attack threat caused by botnet. The Recommendation also provides considerations required for botnet detection and response, defines functions and interfaces used in framework for botnet detection and response.

**X.cce, *Common configuration enumeration***

This Recommendation on common configuration enumeration (CCE) is a specification of configuration guidance statements and configuration controls to facilitate fast and accurate correlation of configuration statements present in disparate domains. A "configuration guidance statement" specifies a preferred or required setting or policy for a computer system. Configuration statements can be found in a variety of repositories such as security guides, benchmarks, vendor guidance and documentation, configuration assessment and management tools, and consolidated reporting systems. The objective of CCE is to provide a means for improving configuration management work processes by allowing people to quickly and accurately correlate configuration data across multiple information sources and tools.

**X.cee, *Common event expression***

This Recommendation on common event expression (CEE)standardizes the way computer events are described, logged, and exchanged. By using CEE’s common language and syntax, enterprise-wide log management, correlation, aggregation, auditing, and incident handling can be performed more efficiently and produce better results. The primary goal of the effort is to standardize the representation and exchange of logs from electronic systems. CEE breaks the recording and exchanging of logs into four (4) components: the event taxonomy, log syntax, log transport, and logging recommendations.

**X.cee.1, CEE architecture overview**

This Recommendation provides a high-level overview of common event expression (CEE) along with details on the overall architecture and introduces each of the CEE components including the data dictionary, syntax encodings, event taxonomies, and profiles. The CEE architecture is the first in a collection of documents and specifications, whose combination provides the necessary pieces to create the complete CEE event log standard.

**X.cee.2, CEE dictionary and event taxonomy**

This Recommendation defines the dictionary and taxonomy components of the common event expression (CEE) architecture. The CEE dictionary defines a common terminology, which can be used to describe the various properties of an event instance. The CEE taxonomy provides a common event classification system to help identify similar events. By combining the dictionary and taxonomy, end users and products can use the same terms to describe the same event characteristics, producing a more unified record of an event.

**X.cee.3, CEE log syntax (CLS) encoding**

This Recommendation defines the common log syntax (CLS) of the common event expression (CEE) architecture. CLS presents a common language for expressing event properties in the form of name-value fields. This Recommendation allows these details to be encoded using one of several formats, such as XML or structured text, which are designed for compatibility with existing event log protocols. Consistent event records representation allows users and products to use the similar terms to describe the similar events in compatible ways.

**X.cee.4, CEE log recommendations (CELR) profile**

This Recommendation defines the common event log recommendations (CELR) component of the common event expression (CEE) architecture. The intent of CELR is to provide guidance for vendors and end users on the events, including the event record contents, that should be logged by a device and to ensure device records contain sufficient details so that logs contain useful, actionable information.

**X.cee.5, CEE log transport (CLT) requirements**

This Recommendation on the common event expression (CEE) common log transport (CLT) requirements defines the capabilities for a log transport protocol. Such protocols enable CEE log syntax (CLS) encoded event records to be shared between parties in a universal, machine-readable manner. The intent of CLT is to provide guidance and requirements for vendors and end users regarding how event records should be reliably and securely shared.

**X.csi, *Guidelines for cybersecurity index***

This Recommendation provides a guideline to assist in the development, selection, and implementation of the measures or indicators that are basis to compute the cybersecurity index (CSI). To meet this objective, this Recommendation provides a list of potential indicators and describes a methodology used in computing the CSI from indicators on its different steps.

**X.csmc, *Continuous security monitoring using CYBEX techniques***

This Recommendation provides concepts, architectures, and requirements of continuous security monitoring using CYBEX techniques. It describes models of cybersecurity operations, with which it defines common terminology of the activities. Implementation using CYBEX techniques to gather information and verify controls for continuous monitoring is also introduced here. The common terminology aids in avoiding mis-communication among entities and facilitates communication and collaboration among entities.

**X.cwss, *Common weakness scoring system***

This Recommendation on the common weakness scoring system (CWSS)provides an open framework for communicating the characteristics and impacts of software weaknesses. The goal of CWSS is to enable ICT managers, software security vendors, application vendors and researchers to be able to reason and communicate about the relative importance of different weaknesses, whether in the architecture, design, code, or deployment.

**X.cybex-beep, *A BEEP profile for cybersecurity information exchange framework***

This Recommendation specifies a BEEP Profile for use within Cybersecurity Information Exchange Techniques (CYBEX). It utilizes BEEP, a generic application protocol kernel for connection-oriented, asynchronous interactions described in IETF RFC 3080. At BEEP's core is a framing mechanism that permits simultaneous and independent exchanges of messages between peers. All exchanges occur in the context of a channel – a binding to a well-defined aspect of the application, such as transport security, user authentication, or data exchange. Each channel has an associated "profile" that defines the syntax and semantics of the messages exchanged.

**X.cybex-tp, *Transport protocols supporting cybersecurity information exchange***

This Recommendation provides an overview of transport protocols that have been adopted and or adapted for use within the Cybersecurity Information Exchange (CYBEX). The Recommendation outlines applications of transport, transport protocol characteristics, as well as security considerations.

**X.eipwa, *Exchange of information for preventing web-based attacks***

This Recommendation describes the guideline on techniques for preventing web-based attacks. It describes the use scenarios for distributing malwares through the web, the functional capabilities, functional architecture for preventing web-based attacks.

**X.maec, *Malware attribute enumeration and classification***

This Recommendation on malware attribute enumeration and classification (MAEC) is an XML/XSD based specification for characterizing malware based on its behaviors, artifacts, and attack patterns. This will allow for the description and identification of malware based on distinct patterns of attributes rather than a single metadata entity (which is the method commonly employed in signature-based detection). MAEC’s focus on structured, attribute-based characterization provides several capabilities that the aforementioned methods do not possess. These capabilities stem from MAEC’s existence as a domain-specific language, with an encompassing and unambiguous vocabulary and grammar.

MAEC aims to: 1) improve human-to-human, human-to-tool, tool-to-tool, and tool-to-human communication about malware, 2) reduce potential duplication of malware analysis efforts by researchers, and 3) allow for the faster development of countermeasures by enabling the ability to leverage responses to previously observed malware instances. Threat analysis, intrusion detection, and incident management are processes that deal with all manners of cyber threats. MAEC, through its uniform encoding of malware attributes, provides a standardized format for the incorporation of actionable information regarding malware in these processes.

**X.sisnego, *Framework of security information sharing negotiation***

This Recommendation provides a framework of security information sharing negotiation on security information sharing between cybersecurity entities such as information requester and information provider. This Recommendation defines functional requirements and reference model for security information sharing negotiation, conceptual data modeling of security information sharing agreement (SSA) and security information sharing policy (SSP), and SSA negotiation process.

**X.trm, *Overview of traceback mechanisms***

This Recommendation describes various types of traceback mechanisms. This Recommendation also derives the evaluation criteria for comparing the traceback mechanisms.

Question 5/17 – Countering spam by technical means

**X.ticvs, *Technologies involved in countering voice spam in telecommunication organizations***

Voice communication is the fundamental function of telecommunication networks. However, voice spam has developed rapidly which has various kinds of harmful negative influences on effects to end users and network operators. The objective of this Recommendation is to develop technological solutions on countering voice spam for network operators and users.

This Recommendation introduces concept and characteristics of voice spam, analyses the current technologies and specifies a framework of countering voice spam. In addition, this Recommendation also provides practical countering solutions in both network-side and user-side along with some collaborations and co-operations will be discussed. Also, technical solutions are provided. This Recommendation can be used as a basis for further development of technological Recommendations on countering voice spam.

WORKING PARTY 2/17 - APPLICATION SECURITY

Question 6/17 ‑ Security aspects of ubiquitous telecommunication services

**Draft X.1126 (X.msec-6), *Security aspects of smartphones***

With the continuous development of functionalities and the expansion of applications, smartphones are facing many security threats, which can cause serious social and economic problems. The objectives of Recommendation ITU-T X.1126 are to protect the personal privacy of users and to improve information security of smartphones.

This Recommendation identifies smartphone threats which are categorized into vulnerabilities and attacks. In order to satisfy such security objectives, this Recommendation specifies a hierarchical security framework and relevant security requirements for smartphones. With regard to the security framework, this Recommendation provides necessary security solutions through system improvements and security tools.

**Draft X.1196 (X.iptvsec-6), *Framework for the downloadable service and content protection system in the mobile Internet Protocol Television (IPTV) environment***

Peer entity authentication is a mandatory requirement for securing peer-to-peer communications. However, especially in pure peer-to-peer (P2P) networks, it is difficult for peers to authenticate corresponding peer entities because there is no central server for authentication they can rely on. In addition, the existing public key infrastructure (PKI) has little use for this purpose because those peer entities rarely have public key certificates issued by well-known certification authorities.

The purpose of Recommendation ITU-T X.1164 is to define mechanisms to utilize service providers’ user authentication infrastructure to implement PKI for P2P networks, with which users who have a valid e-mail account managed by a service provider can issue certificates to their devices by themselves and make those certificates verifiable by corresponding peers in P2P networks.

**Draft X.1313 (X.usnsec-3), *Security requirements for wireless sensor network routing***

Recommendation ITU-T X.1313 provides the security requirements for wireless sensor network routing. It explains the general network topologies and routing protocols in ubiquitous sensor networks. In addition, this Recommendation analyses the security threats facing wireless sensor networks.

X.iptvsec-8, *Virtual machine-based security platform for renewable IPTV service and content protection (SCP)*

This Recommendation specifies a virtual machine-based security platform for the renewable service and content protection (SCP) system. The virtual machine supports an abstract function of hardware devices; hence this Recommendation defines a common interface and functional logics in the IPTV terminal device and includes data structure of SCP client and system components for a terminal device such as embedded SCP, media client, and control client.

X.msec-7, *Guidelines on the management of infected terminals in mobile networks*

This Recommendation guides mobile operators to manage infected terminals by utilizing technologies in the mobile network to protect both users and mobile operators. This Recommendation describes the features and effects of malicious software in the mobile environment. Based on the network-side technologies, this Recommendation focuses on mitigating the vicious effects caused by the terminals after they are infected. This Recommendation defines and organizes the management measures and corresponding technologies by discovery, governing and informing.

X.msec-8, *Secure application distribution framework for communication devices*

This Recommendation provides a secure application distribution framework for communication devices. The communication devices include smartphone, tablet PC, set-top-box (STB) and similar devices which have capability to download applications from managed application distribution sites (i.e. app store) and execute downloaded applications. This Recommendation includes guidelines for developing secure applications and security requirements for managing lifecycle of distributed applications.

X.sgsec-1, *Security functional architecture for smart grid services using telecommunication network*

This Recommendation describes a security functional architecture for smart grid services using telecommunication networks and also may specify the following:

- Security threats in smart grid services using telecommunication networks;

- Security requirements for smart grid services using telecommunication networks;

- Security functional architecture for smart grid services using telecommunication networks based on a functional model.

X.unsec-1, *Security requirements and framework of ubiquitous networking*

This Recommendation describes an overview of ubiquitous networking. It also describes the security threats and security requirements of ubiquitous networking. Security framework and functions that pertain to security of ubiquitous networking are provided in this Recommendation.

Question 7/17 ‑ Secure application services

**Draft X.1141, Amd.1, *Security Assertion Markup Language (SAML 2.0) - Amendment 1: Errata***

This Amendment amends Recommendation ITU-T X.1141 to reflect the official errata that have been approved by OASIS regarding the OASIS SAML 2.0 version.

**Draft X.1142, Amd.1, *eXtensible Access Control Markup Language (XACML 2.0) – Amendment 1: Errata***

This Amendment amends Recommendation ITU-T X.1142 to reflect the official errata that have been approved by OASIS regarding the OASIS XACML 2.0 version.

**Draft X.1154 (X.sap-4), *General framework of combined authentication on multiple identity service provider environments***

In recent, many application services, especially financial services, require more reliable or combined authentication method like multifactor authentication because of increasing of ID theft. For example, one time password authentication and other new authentication methods became to be used instead of traditional password based authentication.

The combination of authentication methods provided multiple IdSPs is able to enhance the assurance of authentication. Recommendation ITU-T X.1154 provides the general framework of combined authentication on multiple identity service providers (IdSPs) environment for service provider. In this Recommendation, three types of combined authentication methods are considered; multi-factor authentication, multi-methods authentication and multiple authentication.

The framework in this Recommendation describes models, basic operations and security requirements against each model components and each messages between model components to keep the total assurance of authentication in case of the combination of multiple IdSPs. In addition, the framework also describes models, basic operations and security requirements to support the authentication service that manages combination of multiple IdSPs.

**Draft X.1164 (X.p2p-4), *Use of service providers’ user authentication infrastructure to implement public key infrastructure for peer-to-peer networks***

Peer entity authentication is a mandatory requirement for securing peer-to-peer communications. However, especially in pure peer-to-peer (P2P) networks, it is difficult for peers to authenticate corresponding peer entities because there is no central server for authentication they can rely on. In addition, the existing public key infrastructure (PKI) has little use for this purpose because those peer entities rarely have public key certificates issued by well-known certification authorities.

The purpose of Recommendation ITU-T X.1164 is to define mechanisms to utilize service providers’ user authentication infrastructure to implement PKI for P2P networks, with which users who have a valid e-mail account managed by a service provider can issue certificates to their devices by themselves and make those certificates verifiable by corresponding peers in P2P networks.

**X.p2p-3, *Security requirements and mechanisms of peer-to-peer-based telecommunication network***

This Recommendation analyses the special security requirements in the peer-to-peer (P2P)-based telecommunication environment, designs the security technical framework for the new P2P-based telecom network architecture and service scenarios, and defines the security solutions and detailed mechanisms to assure the network and services security.

**X.sap-5, *Guideline on anonymous authentication for e-commerce services***

This Recommendation develops an anonymous authentication guideline and reference model for e-commerce because anonymous authentication can be used for providing privacy-preserving technology. This Recommendation describes privacy threats and security requirements for privacy enhanced e-commerce service. It also describes security functions that satisfy the security requirements and anonymous authentication reference models for e-commerce.

**X.sap-6, *Non-repudiation framework based on a one time password***

This Recommendation provides a non-repudiation framework based on one time password (OTP) to provide trust mechanisms between transaction entities. Also, this Recommendation describes the security requirements of OTP-based non-repudiation service as well as mechanisms for generating non-repudiation token. The sender may request a trusted third party (TTP) to generate the non-repudiation token of origin for the sender and also the recipient may request to verify the token of delivery for the recipient. Also, the TTP may generate the non-repudiation token of delivery for the recipient and verifies the token for the sender.

**X.sap-7, *Technical capabilities of fraud detection and response for services with high assurance level requirements***

This Recommendation provides the capabilities required to support fraud detection and response services for security sensitive ICT applications. Fraud detection and response services support the detection, analysis and management of fraud across users, accounts, products, processes and channels. It monitors and analyses user activity and behaviour at the application level (rather than at the system, database or network level) and watches what transpires inside and across accounts, using any channel available to a user. It also analyses behaviour among related users, accounts or other entities, looking for organized criminal activity, corruption or misuse. It is most commonly used in verticals managing customer money, such as e-banking, e-payment, e-government and enterprise remote access, etc., but is also commonly used to detection internal fraud and other types of unauthorized activities.

**X.sap-8, *Efficient multi-factor authentication mechanisms using mobile devices***

With a wide use of mobile devices, the amount of business transaction through mobile devices is drastically increasing. However, there are many weakness of a single-factor authentication for use in the mobile context, which requires the authentication to meet requirements in terms of the security and convenience. Therefore, there is a strong need for developing efficient and effective multifactor-factor authentication methods which are applicable to mobile context.

This Recommendation basically provides a multi factor authentication mechanism using mobile devices. It describes a weakness of a single-factor authentication mechanism, a need for multi factor authentication mechanism and various combinations of the multi factor authentication mechanism using mobile devices, and threats for the two-factor authentication mechanism. In addition, security requirements to reduce threats of a single-factor authentication are provided including potential typical multi factor authentication mechanisms. It is applicable for mobile devices with SIM card capability, and does not exclude virtual SIM cards. Specifically, it is applicable to all applications using mobile devices. This Recommendation uses the framework in Recommendation ITU-T X.1154 (X.sap-4).

**X.sap-9, *Delegated non-repudiation architecture based on ITU-T X.813***

Non-repudiation is to prevent entities from denying that they have sent or received electronic transaction data in the telecommunication network. This Recommendation will create an enhanced non-repudiation model based on Recommendation ITU-T X.813 in support of application services. The architecture can generate and verify the non-repudiation evidence for the transaction data by trusted third party (TTP) that is the central sign authority (CSA).

The architecture integrates multiple authentication devices to access the trusted third party that is the central signing authority (CSA). It also integrates multiple service providers to provide a non-repudiation service with a single authenticated device. The delegated non-repudiation architecture manages user authentication centrally. The service providers can provide the service of a user authentication and non-repudiation without additional construction of authentication systems.

This Recommendation describes the delegated non-repudiation service models and operations for each of the service models. This architecture also defines the security requirements of the delegated non-repudiation service.

The delegated non-repudiation architecture reduced the computation and operations of client aspects for user authentication and non-repudiation service. Thus this delegated non-repudiation architecture is more suitable for mobile devices.

**X.websec-5, *Security architecture and operations for web mashup services***

This Recommendation provides a security architecture and operations for web mashup services. It describes mashup models, security architecture and system operations. This Recommendation also analyses relationships between security requirements and operations.

**X.xacml3, *eXtensible Access Control Markup Language (XACML) 3.0***

This Recommendation defines core XACML including syntax of the language, models, context with policy language model, syntax and processing rules. This Recommendation specifies XACML core and hierarchical role based access control profile. A multiple resource profile of XACML and a SAML 2.0 profile of XACML are specified. To improve on the security of exchanging XACML based policies, this Recommendation also specifies an XACML XML digital signature profile for securing data. A privacy profile is specified in order to provide guidelines for implementers. This Recommendation is technically equivalent and compatible with the OASIS XACML 3.0 standard.

Question 8/17 – Cloud computing security

**X.ccsec, *High-level security framework for cloud computing***

This Recommendation provides a high-level security framework for cloud computing based on the analysis of cloud security threats, security requirements and security areas. This security framework provides the methodology for identifying the security functions that are required within each functional block of the reference architecture of cloud computing. This can then be used to guide the development of security controls, policies, and procedures for the specific cloud service models.

**X.fsspvn, *Framework for a secure service platform for virtual network***

This Recommendation defines the framework of service platform for virtual network (SPVN), which provides for establishing and managing virtual network. The service platform provides the functions of network connectivity (e.g. NAT transversal), security service (e.g. identity management in virtual network) and network management (e.g. security policy distribution, group management in virtual network). This Recommendation also describes the key technologies used in the service platform and the interfaces between the service platform and applications.

**X.goscc, *Guidelines of operational security for cloud computing***

This Recommendation provides guideline of operational security for cloud computing, which includes guidance of service level agreement (SLA) and daily security maintenance for cloud computing. The target audiences of this Recommendation are cloud service providers, such as traditional telecom operators, ISPs and ICPs.

**X.sfcse, *Security functional requirements for Software as a Service (SaaS) application environment***

This Recommendation provides a generic functional description for secure service oriented Software as a Service (SaaS) application environment that is independent of network types, operating system, middleware, vendor specific products or solutions. In addition, this Recommendation is independent of any service or scenarios specific model (e.g., web services, Parlay X or REST), assumptions or solutions. This Recommendation describes a structured approach for defining, designing, and implementing secure and manageable service oriented capabilities in telecommunication cloud computing environment.

Question 9/17 - Telebiometrics

**X.bhsm, *Telebiometric authentication framework using biometric hardware security module***

This Recommendation describes a telebiometric authentication scheme using biometric hardware security module (BHSM). For the telebiometric authentication of proving owner of X.509 registered at RA (Register Authority), BHSM has been considered. This Recommendation provides what are the requirements for deploying the BHSM scheme to securely operate the telebiometric authentication under PKI environments. The scheme focuses on providing how to assure the telebiometric authentication with biometric techniques and HSM and it also suggests ASN.1 standard format for including the proposed scheme in X.509 framework when telebiometric authentication and X.509 certificate are combined to prove the owner of the certificate.

**X.tam, *A guideline to technical and operational countermeasures for telebiometric applications using mobile devices***

This Recommendation defines the vulnerabilities and threats based on the mobile device in operating telebiometric systems and proposes a general guideline for security countermeasures from both technical and operational perspectives in order to establish a safe mobile environment for the use of telebiometric systems and to protect individual privacy. This Recommendation also describes countermeasures that allow the protection of mobile biometric devices as related to their installation, removal, and delivery. It is expected that the countermeasures will ensure security and reliability of the flow of biometric information using mobile devices.

**X.th2, *Telebiometrics related to physics***

This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.

It is applicable to both physics and biometrics (the measurement of physiological, biological, and behavioural characteristics limited to the field of physics). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

**X.th3, *Telebiometrics related to chemistry***

This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.

It is applicable to both chemistry and biometrics (the measurement of physiological, biological, and behavioural characteristics to the field of chemistry). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

**X.th4, *Telebiometrics related to biology***

This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.

It is applicable to both biology and biometrics (the measurement of physiological, biological, and behavioural characteristics to the field of biology). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

**X.th5, *Telebiometrics related to culturology***

This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.

It is applicable to both culturology and biometrics (the measurement of physiological, biological, and behavioural characteristics to the field of culturology). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

**X.th6, *Telebiometrics related to psychology***

This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.

It is applicable to both psychology and biometrics (the measurement of physiological, biological, and behavioral characteristics to the field of psychology). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

**X.tif, *Integrated framework for telebiometric data protection in e-health and telemedicines***

This Recommendation provides an integrated framework for protecting biometric data and private information protection in e-health and telemedicines. It defines a model of health services using telebiometrics for user identification and authentication. It identifies the threats in transmitting various sensory data related to human health and provides their countermeasures for secure transmission.

**WORKING PARTY 3/17 - IDENTITY MANAGEMENT AND LANGUAGES**

Question 10/17 ‑ Identity management architecture and mechanisms

**X.atag, *Attribute aggregation framework***

This Recommendation develops a framework for aggregating identity attributes from different identity providers, while identifying the resulting assurance level. The Recommendation also treats a secure attribute exchange under user control.

**X.authi, *Authentication integration in identity management***

This Recommendation provides a guideline for the telecom operators to implement the authentication integration of the network layer and the service layer, so that a user need not to be re-authenticated again in the service layer if (s)he has been strictly authenticated when accessing the operator's network. This Recommendation analyses the scenarios in which the authentication integration can be implemented well. It also provides the technical frameworks and solutions for the authentication integration in these scenarios.

**X.discovery, *Discovery of identity management information***

This Recommendation enables discovery:

• for relevant information about identifiers, including those utilizing e-mail address syntax and those that are URLs as well as persistent identifiers;

• of attributes about identity providers and relying parties, including, but not limited to visual logos and human-readable site names;

• supporting a spectrum of clients, ranging from passive clients to active clients with bootstrapping functionality;

• of authenticable attributes and add-on functionality of non-browser applications;

• of trust frameworks, policies and references.

**X.giim, *Generic identity management interoperability mechanisms***

Identity Management is becoming an essential basis for transaction, communication and governance; it has been an infrastructural brick in generalized convergence of telecommunication (specialized convergence of fixed and mobile network), information and Internet services as well. A lot of standard organizations have been working on offering a holistic approach on identity management of security, confidentiality and interoperability.

There are quite a few identity management (IdM) solutions, but most of them exist isolated and the interoperation among them is laborious. The existing interoperability mechanisms are often peer-to-peer based, for example, GBA to Liberty Alliance, GBA to OpenID and so on. In this way, one identity management (IdM) system should implement several mechanisms in order to communicate with other identity management (IdM) systems. It is always time-consuming and discouraging for unifying heterogeneous and distributed identity management (IdM) systems.

Generic identity management (IdM) interoperability mechanisms aim to simplify the complicated process of interaction among different identity management (IdM) systems. It should fill the gaps in the connection with currently deployed operator networks or services platforms within a trusted domain. Out of trust domain, this generic interoperability mechanism should fulfil interconnection with other identity management (IdM) technology, mostly in the world of IT based services.

This Recommendation describes the level of federation trust, trust framework for interoperability and introduces four typical identity management (IdM) interoperability scenarios in Appendix I.

**X.iamt, *Identity and access management taxonomy***

This Recommendation develops an identity and access management (IAM) taxonomy to improve the quality of IAM data element definitions, as well as improve the ability to find, analyse, and reference accurate and consistent IAM data elements throughout the IAM lifecycle.

**X.idmcc, *Requirement of IdM in cloud computing***

The Recommendation focuses on the harmonization of the telecommunication services in the cloud computing environment. This Recommendation starts from the use-case and requirements analysis in consideration of the existing industry efforts and it concentrates on how to harmonize the telecommunication services and the Internet services based on a common identity management infrastructure in the cloud computing environment.

**X.mob-id, *Baseline capabilities and mechanisms of identity management (IdM) for mobile applications and environment***

This Recommendation specifies baseline capabilities and mechanisms of identity management (IdM) for mobile applications and environment. The capabilities can include user requirements to meet user’s needs and functional aspects for IdM in mobile context. In addition, it specifies mechanisms for IdM in mobile context to be satisfied when an application in mobile environment is developed. It provides a reference framework that can incorporate specified baseline capabilities of IdM to be used in mobile applications and environment. The mechanisms specify mobile identity management and security to provide core mobile identity lifecycle management and security mechanisms. It also provides mobile identity operations that can provide functions required to build up secure and personalized mash-up applications in mobile environment.

**X.oitf, *Open identity trust framework***

This Recommendation addresses identity management technologies that reduce the friction of using the Web, much like credit cards reduce the friction of paying for goods and services. However, they also introduce a new problem: who do you trust? In other words, how does a relying party know it can trust credentials from an identity service provider without knowing if that provider’s security, privacy, and operational policies are strong enough to protect the relying party’s interests? A trust framework enables a party who accepts a digital identity credential (called the relying party) to trust the identity, security, and privacy policies of the party who issues the credential (called the identity service provider).

**X.scim-use (joint with Q16/13), *Application of system for cross identity management (SCIM) in telecommunication environments***

This Recommendation provides telecom specific uses cases and requirements based on the use of SCIM in IdM.

****Question 11/17 – Directory services, Directory systems, and public-key/attribute certificates****

**F.5xx, *Directory Service - Support of tag-based identification services***

This Recommendation provides guidance for providing directory services for tag-based identification applications by reference to the directory capabilities as specified in the ITU-T X.500 Series of Recommendations | ISO/IEC 9594-All Parts and in the Lightweight Directory Access Protocol (LDAP) specifications as developed within Internet Engineering Task Force (IETF).

**Draft X.500 (revised), *Information technology – Open Systems Interconnection –The Directory: Overview of concepts, models and services***

This Recommendation | International Standard introduces the concepts of the Directory and the DIB (Directory Information Base) and overviews the services and capabilities which they provide.

**Draft X.501 (revised), *Information technology – Open Systems Interconnection –The Directory – Models***

Recommendation ITU-T X.501 | ISO/IEC 9594-2 provides a number of different models for the Directory as a framework for the other ITU-T Recommendations in the X.500 series. The models are the overall (functional) model, the administrative authority model, generic Directory Information models providing Directory User and Administrative User views on Directory information, generic Directory System Agent (DSA) and DSA information models and operational framework and a security model.

**Draft X.509 (revised), *Information technology – Open Systems Interconnection –The Directory – Public-key and attribute certificate frameworks***

Recommendation ITU-T X.509 | ISO/IEC 9594-8 defines a framework for public-key certificates and attribute certificates. These frameworks may be used by other standards bodies to profile their application to Public Key Infrastructures (PKI) and Privilege Management Infrastructures (PMI). Also, this Recommendation | International Standard defines a framework for the provision of authentication services by Directory to its users. It describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services.

**Draft X.511 (revised), *Information technology – Open Systems Interconnection –The Directory – Abstract Service Definition***

Recommendation ITU-T X.511 | ISO/IEC 9594-3 defines in an abstract way the externally visible service provided by the Directory, including bind and unbind operations, read operations, search operations, modify operations and errors.

**Draft X.518 (revised), *Information technology – Open Systems Interconnection –The Directory – Procedures for Distributed Operations***

Recommendation ITU-T X.518 | ISO/IEC 9594-4 specifies the procedures required for a distributed directory consisting of a mix of Directory Systems Agents (DSAs) and LDAP severs acting together to provide a consistent service to its users independent of the point of access. It also describes procedures for protocol conversion between the DAP/DSP protocols and the LDAP protocol.

**Draft X.519 (revised), *Information technology – Open Systems Interconnection –The Directory – Protocols***

Recommendation ITU-T X.519 | ISO/IEC 9594-5 specifies the Directory Access Protocol, the Directory System Protocol, the Directory Information Shadowing Protocol and the Directory Operational Binding Management Protocol fulfilling the abstract services specified in Recommendation ITU-T X.501 | ISO/IEC 9594-2, Recommendation ITU-T X.511 | ISO/IEC 9594-3, Recommendation ITU-T X.518 | ISO/IEC 9594-4 and Recommendation ITU-T X.525 | ISO/IEC 9594-9. It includes specifications for supporting underlying protocols to reduce the dependency on external specifications.

**Draft X.520 (revised), *Information technology – Open Systems Interconnection –The Directory – Selected Attribute Types***

Recommendation ITU-T X.520 | ISO/IEC 9594-6 defines a number of attribute types and matching rules which may be found useful across a range of applications of the Directory. One particular use for many of the attributes defined is in the formation of names, particularly for the classes of object defined in Rec. ITU-T X.521 | ISO/IEC 9594-7. Other attributes types, called notification attributes, provide diagnostic information. This Recommendation | International Standard defines context types to supply characteristics associated with attribute values. It also includes definitions for LDAP syntaxes relevant for attribute types and matching rules.

**Draft X.521 (revised), *Information technology – Open Systems Interconnection –The Directory – Selected object classes***

Recommendation ITU-T X.521 | ISO/IEC 9594-7 defines a number of selected object classes and name forms which may be found useful across a range of applications of the Directory. An object class definition specifies the attribute types which are relevant to the objects of that class. A name form definition specifies the attributes to be used in forming names for the objects of a given class.

**Draft X.525 (revised), *Information technology – Open Systems Interconnection –The Directory – Replication***

Recommendation ITU-T X.525 | ISO/IEC 9594-9 specifies a shadow service which DSAs may use to replicate Directory information. The service allows Directory information to be replicated among DSAs to improve service to Directory users, and provides for the automatic updating of this information.

**X.pki-em, *Information Technology - Public-Key Infrastructure: Establishment and maintenance***

This Recommendation | International Standard specifies a procedures for establishing a Public-Key Infrastructure (PKI) in different environments. It specifies procedure for generation and distribution of asymmetric keys, distribution of public-key certificates, establishment of trust anchor information, etc.

**X.pki-prof, *Information Technology - Public-Key Infrastructure: Profile***

This Recommendation | International Standard specifies a profile and additional specification for how Public-key Infrastructure (PKI) is to be applied in different environments. It profiles the use of public-key certificates, suggested naming structure, what certificate extensions are relevant, details on validation of public-key certificates, revocation principles and the principle for strong authentication.

****Question 12/17 ‑**** Abstract Syntax Notation One (ASN.1), Object Identifiers (OIDs) and associated registration

**Draft X.667 (revised), *Information technology –Procedures for the operation of object identifiers registration authority: Generation of Universally Unique Identifiers (UUIDs) and their use in object identifiers***

Recommendation ITU-T X.667 | ISO/IEC 9834-8 specifies procedures for the generation of UUIDs and for their use in the international object identifier tree under the joint UUID arc.

****Question 13/17 ‑ Formal languages and telecommunication software****

**Draft X.906 (revised), *Open distributed processing – Use of UML for ODP system specifications***

This Recommendation | International Standard defines the use of the Unified Modeling Language (UML 2.1.1) for expressing the specifications of open distributed systems in terms of the viewpoint specifications defined by the Reference Model of Open Distributed Processing (RM-ODP). It defines a set of UML profiles for the expression of such specifications, and an approach for structuring them according to the RM-ODP principles. The purpose of this Recommendation | International Standard is to allow developers to use the UML profiles to write ODP specifications, and to allow UML tools to be used to process viewpoint specifications, thus facilitating the software design process. Annex A provides examples of the use of the UML profiles.

This revision enhances the ODP UML profiles to support the revision of the Enterprise language specified in Recommendation X.911 | ISO/IEC 15414.

**Draft X.911 (revised), *Open distributed processing – Reference model – Enterprise language***

This Recommendation | International Standard provides:

a) a language (the enterprise language) comprising concepts, structures, and rules for developing, representing, and reasoning about a specification of an Open Distributed Processing (ODP) system from the enterprise viewpoint (as defined in Recommendation ITU-T X.903 | ISO/IEC 10746-3);

b) rules which establish correspondences between the enterprise language and the other viewpoint languages (defined in Rec. ITU-T X.903 | ISO/IEC 10746-3) to ensure the overall consistency of a specification.

Previously, this language focused on allowed behaviour and does not distinguish the various different kinds of obligations relevant to enterprise design. This revision extends the language to make obligations and related concepts first class citizens.

**Draft Z.100 Annex F1 (revised), *SDL formal definition: General overview***

Annex F1 provides motivation, gives an overview of the structure of the formal semantics, and contains an introduction to the Abstract State Machine (ASM) formalism, which is used to define the SDL semantics. This update reflects the latest state of the art, in preparation for updating Z.100 Annex F2 and Z.100 Annex F3 for SDL-2010 instead of SDL-2000.

**Draft Z.104 Amd.1, *Data and action language in SDL-2010 – Amendment 1: Annex C - Language binding***

Amendment 1 updates Recommendation ITU-T Z.104 to incorporate binding to C language syntax as an alternative syntax for expressions and statements.

Amendment 1 replaces Annex C of Z.104 (2011).

**Draft Z.109 Amd.1, *Unified modeling language (UML) profile for SDL-2010: Amendment 1: Appendix I – Example language specification***

This new appendix provides an example syntax for the language described by an abstract grammar in Z.109.

**Draft Z.151 (revised), *User requirements notation (URN) – Language definition***

Recommendation ITU-T Z.151 defines the User Requirements Notation (URN) intended for the elicitation, analysis, specification, and validation of requirements and of business processes. URN combines modelling concepts and notations for goals (mainly for non-functional requirements and quality attributes) and scenarios (mainly for operational requirements, functional requirements, and performance and architectural reasoning). The goal sub-notation is called goal-oriented requirements language (GRL) and the scenario sub notation is called use case map (UCM).

**Draft Z Suppl.1 (revised), *Supplement 1 to Z-series Recommendations – ITU-T Z.100-series – Supplement on methodology on the use of description techniques***

This Supplement replaces ITU-T Z.100 Supplement 1 (10/1996) and includes a tutorial on the use of unified modeling language (UML) with ITU-T languages. It is intended that the document is suitable for incorporation by the users in their overall methodologies, tailored for their application systems and specific needs. In particular, this Supplement does not detail issues of derivation of an implementation from the specification or the testing of systems. In the case of testing, it is expected that this should be partially covered by a separate document dealing with the generation of tests for standards or products. In the case of product implementation, it is expected that manufacturers will have their own derivation guidelines and methodology.

Question 14/17 ‑ Testing languages, methodologies and framework

**Draft Z.161 (revised), *Testing and Test Control Notation version 3: TTCN 3 core language***

Recommendation ITU-T Z.161 defines TTCN-3 (Testing and Test Control Notation 3) intended for specification of test suites that are independent of platforms, test methods, protocol layers and protocols. TTCN-3 can be used for specification of all types of reactive system tests over a variety of communication ports. Typical areas of application are protocol testing (including mobile and Internet protocols), service testing (including supplementary services), module testing, testing of CORBA based platforms and APIs. The specification of test suites for physical layer protocols is outside the scope of this Recommendation.

The core language of TTCN-3 can be expressed in a variety of presentation formats. While this Recommendation defines the core language, Recommendation ITU-T Z.162 defines the tabular format for TTCN (TFT) and Recommendation ITU-T Z.163 defines the graphical format for TTCN (GFT). The specification of these formats is outside the scope of this Recommendation. The core language serves three purposes:

1) as a generalized text-based test language;

2) as a standardized interchange format of TTCN test suites between TTCN tools;

3) as the semantic basis (and where relevant, the syntactical basis) for the various presentation formats.

The core language may be used independently of the presentation formats. However, neither the tabular format nor the graphical format can be used without the core language. Use and implementation of these presentation formats shall be done on the basis of the core language.

**Draft Z.161.1 (revised), *The Testing and Test Control Notation version 3: TTCN-3 language extensions: Support of interfaces with continuous signals***

This Recommendation defines the "Continuous Signal support" package of TTCN‑3. It defines concepts for testing systems using continuous signals as opposed to discrete messages and the characterization of the progression of such signals by use of **streams**. For both the production as well as the evaluation of continuous signals the concept of **mode** is introduced. Also, the signals can be processed as **history**-traces. Finally, basic mathematical functions that are useful for analysing such traces are defined for TTCN-3. It is thus especially useful for testing systems which communicate with the physical world via sensors and actuators.

**Draft Z.162 (revised), *Testing and Test Control Notation version 3: TTCN-3 tabular presentation format (TFT)***

Recommendation ITU-T Z.162 defines TFT, the Tabular Format for TTCN-3. TFT is the tabular presentation format for TTCN‑3 (*Testing and Test Control Notation 3*) Core Language defined in Recommendation ITU-T Z.161. It is similar in appearance and functionality to TTCN-2 defined in Recommendation ITU-T X.292 for conformance testing. The tabular format provides an alternative way of displaying the core language as well as emphasizing those aspects that are particular to the requirements of a standardized conformance test suite. While the core language may be used independently of the tabular presentation format, the tabular format cannot be used without the core language. Use and implementation of the tabular presentation format shall be done on the basis of the core language. This Recommendation defines proformas, syntax mappings, additional static semantics, operational semantic restrictions, display and other attributes. Together, these characteristics form the tabular presentation format.

TFT inherits all the essential properties of the Core Language and is intended for specification of test suites that are independent of platforms, test methods, protocol layers and protocols. TTCN-3 can be used for specification of all types of reactive system tests over a variety of communication ports. Typical areas of application are protocol testing (including mobile and Internet protocols), service testing (including supplementary services), module testing, testing of CORBA-based platforms and APIs. The specification of test suites for physical layer protocols is outside the scope of this Recommendation.

**Draft Z.163 (revised), *Testing and Test Control Notation version 3: TTCN-3 graphical presentation format (GFT)***

Recommendation ITU-T Z.163 defines the graphical presentation format for the TTCN-3 core language as defined in Recommendation ITU-T Z.161. This presentation format uses a subset of Message Sequence Charts as defined in ITU-T Recommendation Z.120 with test specific extensions.

This Recommendation is based on the core TTCN-3 language defined in Recommendation ITU-T Z.161. It is particularly suited to display tests as GFTs. It is not limited to any particular kind of test specification.

The specification of other formats is outside the scope of this Recommendation.

**Draft Z.164 (revised), *Testing and Test Control Notation version 3: TTCN-3 operational semantics***

Recommendation ITU-T Z.164 defines the operational semantics of TTCN-3 (Testing and Test Control Notation 3). The operational semantics are necessary to unambiguously interpret the specifications made with TTCN-3. This Recommendation is based on the TTCN-3 core language defined in Recommendation ITU T Z.161.

**Draft Z.165 (revised), *Testing and Test Control Notation version 3: TTCN 3 runtime interface (TRI)***

Recommendation ITU-T Z.165 provides the specification of the runtime interface for TTCN-3 (Testing and Test Control Notation 3) test system implementations. The TTCN-3 Runtime Interface provides the recommended adaptation for timing and communication of a test system to a particular processing platform and the system under test, respectively. This Recommendation defines the interface as a set of operations independent of target language.

The interface is defined to be compatible with Recommendation ITU T Z.161. This Recommendation uses the CORBA Interface Definition Language (IDL) to specify the TRI completely. Clauses 6 and 7 specify language mappings of the abstract specification to the target languages Java and ANSI-C. A summary of the IDL-based interface specification is provided in Annex A.

**Draft Z.165.1 (revised), *Testing and Test Control Notation version 3: TTCN-3 extension package: Extended TRI***

This Recommendation defines the extended runtime interface (TRI) package of TTCN‑3. It defines a more efficient handling of software values by a version of TRI, that does not use binary encoded messages for the communication with the system under test (SUT), but uses the values as they are; meaning e.g. that software objects or serialized data can be passed directly between the SUT and the TTCN‑3 Executable (TE).

**Draft Z.166 (revised), *Testing and Test Control Notation version 3: TTCN-3 control interface (TCI)***

Recommendation ITU-T Z.166 specifies the control interfaces for TTCN-3 test system implementations. The TTCN-3 Control Interfaces provide a standardized adaptation for management, test component handling and encoding/decoding of a test system to a particular test platform. This Recommendation defines the interfaces as a set of operations independent of a target language.

The interfaces are defined to be compatible with the TTCN-3 standards (see clause 2). The interface definition uses the CORBA Interface Definition Language (IDL) to specify the TCI completely. Clauses 8 and 9 present language mappings for this abstract specification to the target languages Java and ANSI C. A summary of the IDL based interface specification is provided in Annex A.

**Draft Z.167 (revised), *Testing and Test Control Notation version 3: TTCN-3 mapping from ASN.1***

Recommendation ITU-T Z.167 defines a normative way of using ASN.1 as defined in Recommendations ITU-T X.680, X.681, X.682 and X.683 with TTCN-3. The harmonization of other languages with TTCN-3 is not covered by this Recommendation.

**Draft Z.168 (revised), *Testing and Test Control Notation version 3: TTCN-3 mapping from CORBA IDL***

Recommendation ITU-T Z.168 defines the mapping rules for CORBA IDL (as defined in chapter 3 in Draft Approved Specification ptc/06-05-01 (2006)) to TTCN-3 (as defined in Recommendation ITU-T Z.161) to enable testing of CORBA-based systems. The principles of mapping CORBA IDL to TTCN-3 can be also used for the mapping of interface specification languages of other object-/component-based technologies.

The specification of other mappings is outside the scope of this Recommendation.

**Draft Z.169 (revised), *Testing and Test Control Notation version 3: TTCN-3 mapping from XML data definition***

Recommendation ITU-T Z.169 defines the mapping rules for W3C Schema to TTCN-3 to enable testing of XML-based systems, interfaces and protocols.

**Draft Z.170 (revised), *Testing and Test Control Notation version 3: TTCN-3 documentation comment specification***

Recommendation ITU-T Z.170 defines a documentation of TTCN-3 source code using special documentation comments. The source code documentation can then be produced automatically from the TTCN-3 core language, e.g., in the form of hypertext web pages.

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