|  |  |
| --- | --- |
| INTERNATIONAL TELECOMMUNICATION UNION | **STUDY GROUP 17** |
| **TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2013-2016 | **TD 0043 Rev.2**  |
| **English only****Original: English** |
| **Question(s):** | 11/17 | Geneva, 17 - 26 April 2013 |
| **TD** |
| **Source:** | Rapporteur Q.11/17 |
| **Title:** | Report on Question 11/17 |

Report on Question 11/17

1 Question 11/17 ‑ Generic technologies to support secure applications (<http://www.x500standard.com>)

2 Rapporteur

|  |  |
| --- | --- |
| Erik AndersenEIDQ | Tel.: +45 20 97 14 90Email: era@x500.eu |
| Jean-Paul LemaireUniversity Paris Diderot | Tel.:+33618473756Email: [jean-paul.lemaire@univ-paris-diderot.fr](file:///E%3A%5Cjean-paul.lemaire%40univ-paris-diderot.fr) |

3 Documents considered

3.1 Contributions

|  |  |  |
| --- | --- | --- |
| **Document Number** | **Source** | **Title** |
| [C 0003 Rev.1](http://www.itu.int/md/T13-SG17-C-0003/en) | EIDQ | Request for withdrawal of Rec. ITU-T X.530 |
| [C 0010 Rev.1](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-C-0010) | Iran (Islamic Republic of) | Generic technologies to support secure applications |
| [C 0012](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-C-0012) | Electronics and Telecommunications Research Institute (ETRI) | Proposal for a new ORS service in Recommendation ITU-T X.672 | ISO/IEC 29168-1 |
| [C 0013](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-C-0013) | Electronics and Telecommunications Research Institute (ETRI) | Proposal for a new work item - OID-based resolution framework for supporting interoperability between heterogeneous identifiers |
| [C 0091](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-C-0091) | LegalBox | Proposal of standardization for CMTP and CPOP protocols |

3.2 Temporary documents

| **Document Number** | **Source** | **Title** |
| --- | --- | --- |
| [TD 0020](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0020)[Rev. 1](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0020) | Q.11 Rapporteur | Q11/17 agenda |
| [TD 0064](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0064/en) | Q.11 | Report of collaborative meeting between ISO/IEC JTC 1/SC 6 /WG 8 and ITU-T Q11/17, 17 - 21 September 2012 in Gratkorn/Graz, Austria |
| [TD 0076 Rev. 1](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0076/en) | TSB | Summaries for work items under development in Study Group 17 |
| [TD 0080](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0080/en) | TSB | Organization of ITU-T X-series Recommendations |
| [TD 0084 Rev.1](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0084/en) | TSB | Planned actions on Recommendations and other texts at this SG17 meeting |
| [TD 0088 Rev. 1](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0088/en) | TSB | Relationships of ITU-T Study Group 17 with ISO, IEC and ISO/IEC JTC 1 |
| [TD 0089](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0089/en) | TSB | List of work items from last SG17 meeting or proposed in approved interim Rapporteur group, during this SG17 meeting, or in Correspondence Group activities |
| [TD 0093 Rev. 1](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0093/en) | TSB | Status of E and F-series Recommendations under the responsibility of SG 17 (revised 17 October 2012) |
| [TD 0094 Rev. 1](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0094/en) | TSB | Mapping between ISO/IEC Standards and ITU-T Recommendations (revised 17 October 2012) |
| [TD 0095 Rev. 2](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0095/en) | TSB | Listing of common and technically aligned Recommendations | International Standards (including technical reports and international standardized profiles) (revised 17 October 2012) |
| [TD 0096 Rev, 4](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0096/en) | TSB | Status of X-series Recommendations (revised 17 October 2012) |
| [TD 0099 Rev. 6](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0099/en) | TSB | Updated work plan for ITU-T Study Group 17 meeting, Geneva, 17 - 26 April 2013 |
| [TD 0101](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0101/en) | JCA-SG&HN | Incoming LS - Activities related to smart grid |
| [TD 0107 Rev.3](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0107/en) | TSB | Highlights of WTSA-12 of significance to SG17 |
| [TD 0108 Rev. 3](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0108/en) | TSB | Study Group 17 Questions responsibility for Recommendations and Supplements |
| [TD 0110](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0110/en) | OID project leader | Establishment of a national OID Registration Authority for Bulgaria |
| [TD 0111](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0111/en) | Q.11 Rapporteur | Summary of voting on NWIP ballot on Public-key infrastructure: Profile |
| [TD 0112](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0112/en) | Q.11 Rapporteur | Summary of voting on NWIP ballot on Public-key infrastructure: Establishment and maintenance  |
| [TD 0113](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0113/en) | ISO/IEC JTC1/SC27 | Incoming LS - Meeting Report - Study Period on Information Security within Smart Grid Environments |
| [TD 0131](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0131/en) | Q.11 Rapporteur | David Chadwick et al.: "Role of technical and juridical expert to the X.509 trust model" |
| [TD 0132](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0132/en) | ITU-T SG 16 | Incoming LS - LS to ITU-T SG 17 on request for comment on V2V security approach used by US DOT Safety Pilot Program |
| [TD 0140](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0140/en) | TSB | Draft WTPF IEG Opinion on Trust Frameworks and X.509 Certificates  |
| [TD 0158](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0158/en) | TSB | Draft work programme for Working Parties and Quest |
| [TD 0161 Rev.3](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0161/en) | TSB | List of proposed new work items for SG17 and list of work items to be deleted/modified |
| [TD 0163](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0163/en) | SG17 Working Party Chairmen | Timetable for Working Party Meetings Thursday 25 April 2013 |
| [TD 0173](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0173/en) | ITU-T SG13 | Incoming LS - Reply to your liaison on SG13 FN activities |
| [TD 0174](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0174/en) | ITU-T SG13 | Incoming LS - Reply to SG 13 liaison on draft Y.FNsdn-fm |
| [TD 0202 Rev.1](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0202/en)  | OID project leader | Establishment of a national OID Registration Authority for Thailand |
| [TD 0204](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0204/en) | Q.11 Rapporteur | Planned PKI activities for ITU-T Study Period 2013-2016 |
| [TD 0209](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0209/en) | TSB | ISO/IEC JTC 1/SC 7/WG19 Paris 2011 - Output Document from the November 2012 meeting in Paris - DAM for ITU-T Recommendation X.911 | ISO/IEC 15414 Amd 1 |
| [TD 0210](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0210/en) | TSB | ISO/IEC JTC 1/SC 7/WG19 Montreal 2013 - Input Document to the May 2013 meeting in Montréal - Information technology - Open distributed processing - Use of UML for ODP system specifications - ITU-T Recommendation X.906 | ISO/IEC CD 19793 |
| [TD 0214](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0214/en) | TSB | Plan of special joint sessions between ITU-T SG17 and ISO/IEC JTC 1/SC27 |
| [TD 0216](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0216/en) | ITU-T representative to the MoU/MG on e-business | Information and actions from the Management Group of the MoU on e-business |
| [TD 0218](http://www.itu.int/md/T13-SG17-130417-TD-PLEN-0218/en) | Q,11 Rapporteur | An OID-based Sensor node Identifier for Sensor Networks |

4 Meeting results

Mr. Erik Andersen, Q11/17 Rapporteur chaired the meeting. The meeting was collaborative with ISO/IEC JTC 1/SC 6/WG 8 and WG9.

**4.1 Highlight**

### 4.1.1 - Directory services, Directory systems, and public-key/attribute certificates

* + Contribution C 0091 was reviewed and found in line with the work on PKI in Q.11. A new proposed work item was created and may be found as TD 0239 Rev. 1. A first working draft was produced and may be found as TD 0240
	+ It was decided that the Rec. ITU-T X.509 should only contain PKI and PMI specifications and that directory related parts should be moved to other parts. A first working draft amendment to Rec. ITU-T X.509 may be found as TD 0241. A first working draft amendment for Rec. ITU-T X.511 may be found as TD 0242. A first working draft amendment for Rec. ITU-T X.520 may be found as TD 0243.
	+ TD 0131 proposing a new PKI component to be included in Rec. ITU-T X.509. The proposal was accepted and the result is also included in TD 0241.
	+ A discussion was conducted on how the Rec. ITU-T X.509 should be structured for the next edition.
	+ TD 0204 was reviewed. It is a presentation of Q.11 PKI plans for the study period. This presentation was updated and resulted in TD 0204 Rev. 1. It was intended for a presentation at the common ISO/IEC JTC1/SC27 - Q.11/17.
	+ TD 0168, LS to ITU-T SG 16 on V2V security approach used by US DOT, was reviewed and commented.
	+ A new draft for F.5xx was produced and may be found as TD 0331.

### 4.1.2 - ASN.1, OIDs, OSI and ODP

* + Contribution C12 was reviewed and the meeting proposes to define a new service type for Uniform Resource Identifier (URI) to enable an application specific ORS to use Web Service which provides dynamic contents generation, or service actions defined as follows:

# Proposed new service type for ITU-T X.672 | ISO/IEC 29168-1

|  |  |  |
| --- | --- | --- |
| Name of ORS service | Service type value | Specification of the service |
| URI | UINF | See below. |

# Specification of the Uniform Resource Identifier (URI) ORS service

All DNS zone files for an ORS-supported OID node shall contain a NAPTR resource record (see 6.3.2 of Recommendation ITU-T X.672 | ISO/IEC 29168-1) with ORS service type **UINF** and with the regular expression **information** containing a URI which indicates a service point for various service actions.

Any URI scheme which is officially registered to IANA can be used in the regular expression information.

According to the Rec. ITU-T | ISO/IEC 29168-1 Annex A, addition of a new service needs joint approval of ITU-T SG 17 of ISO/IEC JTC 1/SC 6 then has to be published on SG 17 web site.

* + Contribution C13 was discussed and a new work item proposal was prepared (TD 0297 Rev. 2). The first draft is in TD 0286. As the new work item is an innovative use of object identifiers, this work shall be done in collaboration with SG 2. So the meeting has prepared a liaison to SG 2 (TD 0332).
	+ TD 0218 was discussed and two solutions have been considered
	+ Extend Rec. ITU-T X.668 | ISO/IEC 9834-9, "Registration of object identifier arcs for applications and services using tag-based identification" to network sensors. This change needs an amendment with a new title.
	+ Create a new recommendation.

 The decision will be taken after ISO/IEC JTC1/SC6 meeting.

* + TD 216 (Information and actions from the Management Group of the MoU on e-business) has been reviewed and the meeting decides to send to liaison statements:
	+ One to ISO/TC 154 (TD 0334) about possible impacts of extensions of ISO 8601 on ASN.1 time types.
	+ One to OASIS (TD 0333) about possible usage of ASN.1 to describe the new MQTT protocol.
* The meeting has also reviewed the pending ASN.1 defects and it was decided to resolve them by email and then prepare technical corrigenda.

4.2 Agreements reached

4.2.1 ITU-T X.500 series of Recommendations

*Certified E-mail*

A new work item (TD 0239 Rev. 1) and associated draft recommendation (TD 0240) were agreed.

*Directory-IdM support:*

New Drafts for Amendment 2 to X.509 (TD 0241), X.511 (TD 0242) and X.520 (TD 0243) was created.

*X.500 Draft Technical Corrigenda:*

None.

*Implementors' Guide on the Web:*

Q11/17 is maintaining a web site, <http://www.x500standard.com/> acting as an online X.500 Implementers’ Guide. It has the advantage that new issues and their resolutions are made available in a timely fashion. Currently, the Q.11/17 Rapporteur maintains the site. There is a link from the SG17 Implementers’ Guide page into this online Implementers' Guide.

4.2.2 ITU-T E- and F-series Recommendation

A new revision of F.5xx was produced and may be found as TD 0331.

4.2.3 Collaboration with Q.10/17

Q.11 maintains its collaboration with Q10/17.

**4.2.4 ASN.1 and OID**

*New service for ORS:*

New service type for URI is proposed for Rec. ITU-T X.672 | ISO/IEC 29168-1.

*OID-based resolution framework for heterogeneous identifiers/locators:*

A new work item (TD 0297 Rev.1) and associated draft recommendation (TD 0286) were agreed.

*Progression of defects:*

Defects of ASN.1 will be progressed by email before the next SG 17 meeting.

*ASN.1 and OID projects:*

Term of references for the ASN.1 and the OID projects can be found in TD 0309 and TD 0308 respectively.

4.3 Action and plan on Recommendations

### 4.3.1 Supplement for approval at this SG 17 meeting

None

### 4.3.2 Recommendations for approval at this SG 17 meeting

None

### 4.3.3 Recommendations for consentor determination at this SG 17 meeting

None

### 4.3.4 Recommendations planned for consent or determination later in the study period

N/A

### 4.3.5 Recommendations planned for consent or determination at the next SG 17 meeting

Table 5 – Recommendations planned for consent(AAP) or determination(TAP)\*
in this study period

| Q. | Acronym | Title | Editor | Location of text | Equivalente.g., ISO/IEC | Timing |
| --- | --- | --- | --- | --- | --- | --- |
| 11 | F.5xx | Directory Service - Support of Tag-based Identification Services | Erik Andersen | TD 0331 |  | 3/2014 |
| 11 | X.500eightedition | Information technology – The Directory: Overview of concepts, models and services | Erik Andersen |  | ISO/IEC 9594-1 | 2016 |
| 11 | X.501,seventh edition | Information technology – The Directory – Models | Erik Andersen |  | ISO/IEC 9594-2 | 2016 |
| 11 | X.509seventh edition | Information technology – The Directory – Public-key and attribute certificate frameworks | Erik Andersen |  | ISO/IEC 9594-8 | 2016 |
| 11 | X.511seventh edition | Information technology – The Directory – Abstract Service Definition | Erik Andersen |  | ISO/IEC 9594-3 | 2016 |
| 11 | X.518seventh edition | Information technology – The Directory – Procedures for Distributed Operations | Erik Andersen |  | ISO/IEC 9594-4 | 2016 |
| 11 | X.519seventh edition | Information technology – The Directory – Protocols | Erik Andersen |  | ISO/IEC 9594-5 | 2016 |
| 11 | X.520seventh edition | Information technology – The Directory – Selected Attribute Types | Erik Andersen |  | ISO/IEC 9594-6 | 2016 |
| 11 | X.521seventh edition | Information technology – The Directory – Selected object classes | Erik Andersen |  | ISO/IEC 9594-7 | 2016 |
| 11 | X.525seventh edition | Information technology – The Directory – Replication | Erik Andersen |  | ISO/IEC 9594-9 | 2016 |
| 11(10) | x.pki-prof | Public-Key Infrastructure: Prolile | Erik Andersen |  |  | 2016 |
| 11(10) | x.pki-em | Public-Key Infrastructure: Establishment and maintenance | Erik Andersen |  |  | 2016 |
| 11 | x.cmail | CMTP and CPOP protocols | David Keller,Laura Prin  | TD 0240 |  | 2014 |
| 11 | X.orf | OID-based resolution framework for heterogeneous identifiers/locators | Younghwan CHOI | TD 0286 | ISO/IEC xxxxx | 2015 |
| 11 | X.906 | Information technology - Open distributed processing - Use of UML for ODP system specifications  | - | TD 0210 | ISO/IEC 19793 | 2016 |
| 11 | X.911 | Information technology - Open distributed processing - Reference model - Enterprise language  | - | TD 0209 | ISO/IEC 15414 | 2016 |

4.x National OID registrations

SG 17 is asked to note that letters have been received from Bulgaria (TD 110) and Thailand (TD 202) informing SG 17 that they are now operating a country registration authority under {joint iso-itu-t(2) country(16) bg(100)} and{joint iso-itu-t(2) country(16) th(764)} respectively.

4.x Response to TD 0076 Rev. 1, Summaries for work items under development in Study Group 17

Q.11 suggests the following replacement texts:

**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 frameworks for public-key certificates and attribute certificates. The Public-key certificate framework is the base specification for public-key certificates, for the different components going into a Public-Key Infrastructure (PKI), for validation procedures, for public-key certificate revocation, etc. The attribute certificate framework is the base specification for attribute certificates and the different components going into the Privilege Management Infrastructure (PMI). These frameworks may be used by standards bodies to profile their application to Public Key Infrastructures (PKI) and Privilege Management Infrastructures (PMI).

**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, operations to support password policies and operations to support interworking with LDAP. It also defines errors.

**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. The protocols may be encoded using all standard ASN.1 encoding rules.

4.x Response to TD 0096 Rev. 4, Status of X-series Recommendations (revised 27 February 2013)

The Abstract Syntax Notation One (ASN.1) tale should indicate Q.11 rather than Q.12.

4.4 Liaison statements

TD 0332: LS to ITU-T SG2

TD 0333: Liaison to OASIS regarding Message Queuing Telemetry Transport (MQTT)

TD 0334: Liaison to ISO/TC 154 regarding extensions to ISO 8601

TD 0362: Liaison to ISO/IEC JTC1/SC27 on ITU-T Study Group 17 Public-Key Infrastructure (PKI) activities

4.5 Action plan

4.5.1 Objectives

* Progress defects and produce technical corrigenda.
* To continue work on *Communication enhancement for the Directory* with the objective to improve the interworking capabilities with LDAP and to extend the support for other encoding rules than BER.
* To continue work on *Directory Support for IdM for the Directory* with the objective to adapt X.509 to new requirements.
* To initiate work on CMTP and CPOP.
* To initiate work on how to deploy Public-Key Infrastructure (PKI) in different environment.
* Work with RFID standards organization further to improve the RFID support.
* Follow the work on Biometric certificates.
* Provide guidance to relevant groups on the use of directories.

4.5.2 Relationship

Study groups: ITU-T SG 2, SG 13

Standardization bodies: ISO/IEC JTC 1/SC 6, ISO/IEC JTC 1/SC 27, ISO/IEC JTC 1/SC 31,
IETF working groups LDAP and PKIX

4.5.3 Work programme and milestones

|  |  |
| --- | --- |
| First edition of F.5xx | 2014-4 |
| Edition 8 of the X.500 Series | 2016 |
| Public-Key Infrastructure: Profile | 2016 |
| Public-Key Infrastructure: Establishment and Maintenance | 2016 |
| 2nd Edition of F.5xx | 2016 |

4.6 Summary of Recommendations

The updated summaries of draft Recommendations under Q.11/17 responsibility are reproduced in COM 17-R 1. Further updates will be posted at <http://www.itu.int/ITU-T/studygroups/com17/index.asp>.

5 Future meetings

Ongoing work will be progressed by correspondence and by email discussion.

An interim meeting, Paris, 9-10 July, 2013 (CMTP and CPOP only).

An interim meeting with ISO/IEC JTC1/SC6, Seoul, 17 -21 June, 2013

The Q11/17 will meet during the next SG17 meeting in Geneva, Switzerland in January 2014.

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