Question 11/17 – Generic technologies (such as Directory, PKI, formal languages, object identifiers) to support secure applications

(Continuation of Question 11/17)

1 Motivation

This Question supports the continued development of a variety of generic technologies that are in wide-spread use in support of secure applications. These include:

– Directory services (X.500 series)
– Public Key Infrastructures (PKI – X.509)
– Secure communication (X.510)
– Privilege Management Infrastructure (PMI – X.509)
– Abstract Syntax Notation One (ASN.1)
– Object Identifiers and their Registration Authorities
– Testing and Test Control Notation version 3 (TTCN-3)
– Maintenance of formal languages:
  - Specification and Description Language (SDL)
  - Unified Modelling Language (UML) Profile Design
  - Message Sequence Chart (MSC)
  - User Requirement Notation (URN)
  - CHILL, the ITU-T Programming Language
– Maintenance of OSI and ODP.

1.1.1.1 I.1.1 Motivation for the work on directories, PKI, and PMI

The ITU-T X.500-series of Recommendations has a significant impact in the industry. These Recommendations are major components of widely deployed technologies such as Public-Key Infrastructure (PKI) and lightweight directory access protocol (LDAP), and is used in many areas, e.g., financial, medical, and legal. Where high security directory services are required, e.g., in the military area, X.500 is the only answer.

X.500 provides elaborate access control and data privacy protection. It is an open-ended specification adaptable to many different applications. It is extendable to allow future requirements to be met. The widely used LDAP is built on the X.500 Directory model. Recommendation ITU-T X.500 has included capabilities for interworking with LDAP. X.500 and LDAP directory solutions are an important part of identity management (IdM).

X.509 is a significant ITU-T Recommendation. Public-key certificates are widely used.

In addition to being a major part of -e-business, e-banking, e-health, it now also being used other characterized by large networks with machine-to-machine communication and constrained entities e.g., Internet of Things (IoT) and intelligent electric networks (smart grid).

Public-key certificates are also for several IETF specification, e.g. Transport Layer Security (TLS).

Attribute certificates provide a secure method for conveying privileges important for access control. The OASIS SAML specifications are based on X.509 attribute certificates. Attribute certificates are also used in power systems Attribute certificates are in particular useful when privileges are assigned by other authorities than those issuing public-key certificates.

In collaboration with other groups X.509 needs to evolve and to be maintained to reflect and benefit from the experiences obtained within the Public-Key Infrastructure (PKI) area and in the Privilege

Management Infrastructure (PMI) area. X.509 needs to be enhanced to cope the new requirements such as Machine-to-Machine communications, smart-grid security, Internet of Things security, quantum safe algorithms and distributed ledger technologies. A Decentralized PKI mechanism using blockchains is under development.

Recommendations under responsibility of this Question as of 7 January 2022: E.104 (in conjunction with SG2), E.115 (in conjunction with SG2), F.500, F.510, F.511, F.515, X.500, X.501, X.509, X.510, X.511, X.518, X.519, X.520, X.521, X.525, X.530 and X.1341.

Texts under development as of 7 January 2022: X.510 Amd.1, X.pki-em.

1.1.1.2 I.1.2 Motivation for the work on ASN.1

Additional Recommendations, where needed, will be developed to accommodate advances in technology and additional requirements from users of the ASN.1 notation, its encoding rules.

ASN.1 has proved to be the notation-of-choice for many ITU-T standardization groups, many of which continue to produce requests for correction of residual ambiguities or lack of clarity.

There is a continuing requirement to provide advice and assistance to other study groups, external standards development organizations (SDOs) and countries on ASN.1.

Recommendations under responsibility of this Question as of 7 January 2022: X.680, X.681, X.682, X.683, X.690, X.691, X.692, X.693, X.694, X.695, X.696, X.697, X.891, X.892, X.893 and X.894.

Texts under development as of 7 January 2022: None.

1.1.1.3 I.1.3 Motivation for the work on object identifiers and their registration authorities

Object identifiers (OIDs) have proved a very popular namespace based primarily on a tree-structure of hierarchical registration authorities identified by integer value. Its recent extension to International OIDs allowing arcs to be identified by Unicode labels is also in demand for various applications and is likely to produce requirements for further development and extension, and allocations.

There is a continuing requirement to provide advice and assistance to other study groups, external standards development organizations (SDOs) and countries on the management of the OID namespace. It is expected that the need for help and advice will increase with the introduction of international OIDs and the increasing use of Country Registration Authorities by developing countries. There is therefore a continued need for an ITU-T "OID Project" with an appointed project leader to provide such advice and assistance.

Any innovative use of object identifiers is to be developed in conjunction with ITU-T Study Group 2.

Recommendations and Technical Papers under responsibility of this Question as of 7 January 2022: X.660, X.662, X.665, X.666, X.667, X.668, X.669, X.670, X.671, X.672, X.674, X.675, X.676, X.677 and Technical Paper XSTP-OID-ORS.

Texts under development as of 7 January 2022: revised X.672.

1.1.1.4 I.1.4 Motivation for the work on TTCN-3

The Testing and Test Control Notation version 3 (TTCN-3) allows tests for functionality and interoperability of systems to be specified and generic test suites to be written. TTCN-3 is being used in testing ITU-T Recommendations developed by the relevant ITU-T SGs and especially SG11, as the lead group on test specifications, conformance, and interoperability testing. ITU-T is producing a large number of Recommendations. To achieve interoperability, it is essential that implementations of these Recommendations conform to the Recommendations.

Recommendations under responsibility of this Question as of 7 January 2022: X.292, Z.161, Z.161.1, Z.161.2, Z.161.3, Z.161.4, Z.161.5, X.161.6, Z.161.7, Z.162, Z.163, Z.164, Z.165, Z.165.1, Z.166, Z.167, Z.168, Z.169, Z.170 and Z.171.

Texts under development as of 7 January 2022: None.

1.1.1.5 I.1.5 Motivation for the work on formal language maintenance

No further development is expected on the following formal languages:

– Specification and Description Language (SDL)
– Unified Modelling Language (UML) profile
– Message Sequence Chart (MSC)
– User Requirements Notation (URN)
– CHILL, the ITU-T programming language

But there is a need for on-going maintenance.

Recommendations, Supplements and Implementer's Guides under responsibility of this Question as of 7 January 2022: Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.110, Z.111, Z.119, Z.120, Z.121, Z.150, Z.151, Z.200, Z.450, and Supplement Z.Suppl.1, and Implementer's Guide Z.Imp100.

1.1.1.6 I.1.6 Motivation for the work on OSI maintenance

The work on the base Recommendations for Open Systems Interconnection (OSI) has been completed. Systems based on OSI Recommendations may be implemented over a relatively long period of time. Operational experience with implemented systems based on these Recommendations may lead to the discovery of technical errors or desirable enhancements to these Recommendations. Therefore, there is a need for on-going maintenance of X-series OSI Recommendations.

Recommendations and Implementer's Guides under responsibility of this Question as of 7 January 2022: F.400, F.401, F.410, F.415, F.420, F.421, F.423, F.435, F.440, F.471, F.472, X.200, X.207, X.210, X.211, X.212, X.213, X.214, X.215, X.216, X.217, X.217bis, X.218, X.219, X.220, X.222, X.223, X.224, X.225, X.226, X.227, X.227bis, X.228, X.229, X.233, X.234, X.235, X.236, X.237, X.237bis, X.245, X.246, X.247, X.248, X.249, X.255, X.256, X.257, X.260, X.263, X.264, X.273, X.274, X.281, X.282, X.283, X.284, X.287, X.400, X.402, X.404, X.408, X.411, X.412, X.413, X.419, X.420, X.421, X.435, X.440, X.445, X.446, X.460, X.462, X.467, X.481, X.482, X.483, X.484, X.485, X.486, X.487, X.488, X.610, X.612, X.613, X.614, X.622, X.623, X.625, X.630, X.633, X.634, X.637, X.638, X.639, X.641, X.642, X.650, X.851, X.852, X.853, X.860, X.861, X.862, X.863, X.880, X.881, X.882 and Implementer's Guide X.ImpOSI.

1.1.1.7 I.1.7 Motivation for the work on ODP maintenance

A key aspect of telecommunications systems development is the availability of software to support Open Distributed Processing (ODP). Provision of ODP requires standardization of reference models, architectures, functions, interfaces and languages (ITU-T X.900-series).

Recommendations under responsibility of this Question as of 7 January 2022: X.901, X.902, X.903, X.904, X.906, X.910, X.911, X.920, X.930, X.931, X.950, X.952 and X.960.

2 Question

Study items to be considered include, but are not limited to:

1.1.1.8 I.2.1 Study items related to the work on directories, PKI and PMI

In relation to directory services:

a) What new service definitions or modifications in the F-series are required to identify how current capabilities may be used and what new requirements there are on ITU-T X.500?

b) What enhancements to the E-series of Recommendations are necessary to cope with new service requirements?

c) What enhancements are required on the Directory to support new PKI requirements?

d) What new security and privacy requirements are there on directory information?

e) What other encoding rules for ITU-T X.500, such as XML, may be required to further improve the usefulness of ITU-T X.500?

f) What further enhancements are required to public-key and attribute certificates to allow their use in various environments, e.g., resource constrained environments machine-to-machine and large networks?

g) What further enhancements are required to public-key and attribute certificates to increase their usefulness in areas such as biometrics, authentication, access control and electronic commerce?

h) What changes to Recommendations ITU-T X.509 and ITU-T X.510 are required to support quantum safe algorithms and distributed leger technologies?

This work will be done in collaboration with ISO/IEC JTC 1/SC 6 in their work on extending ISO/IEC 9594. Cooperation will be maintained with the IETF particularly in the areas of LDAP and PKI.

1.1.1.9 I.2.2 Study items related to the work on ASN.1

a) What enhancements are required to the Abstract Syntax Notation One (ASN.1) and its associated encoding rules to meet the needs of future applications?

b) What collaboration, beyond current agreements, is required with other bodies producing de jure or de facto standards to ensure that ITU-T work on ASN.1 remains a leader in the area of provision of notations for protocol definition?

This work will be done in collaboration with ISO/IEC JTC 1/SC 6.

1.1.1.10 I.2.3 Study items related to the work on object identifiers and their registration authorities

a) What tutorial activity is needed to support the use of OIDs in a variety of environments?

b) What additional registration authorities or their procedures are needed to support the work of this and other Questions?

c) What collaboration, beyond current agreements, is required with other bodies producing de jure or de facto standards to ensure that ITU-T work on OIDs remain a leader for unambiguous naming?

This work will be done in collaboration with ISO/IEC JTC 1/SC 6.

1.1.1.11 I.2.4 Study items related to the work on TTCN

a) What enhancements are required to TTCN-3 to meet the needs of future applications?

This work will be done in collaboration with ETSI TC MTS.

1.1.1.12 I.2.5 Maintenance of formal languages

Continue maintenance of Recommendations related to SDL, UML profile, MSC, URN, and CHILL.

1.1.1.13 I.2.6 Maintenance of OSI

Continue maintenance of OSI architecture and individual layer Recommendations to provide any needed enhancements and to resolve any reported defects. Continue maintenance of OSI Message Handling Service and Systems, Reliable Transfer, Remote Operations, CCR, and Transaction Processing to provide any needed enhancements and to resolve any reported defects.

Close collaboration and liaison with other study groups and other international groups implementing OSI is highly desirable to ensure the widest applicability of resulting Recommendations.

This work is to be carried out in collaboration with ISO/IEC JTC 1 and its sub-committees.

1.1.1.14 I.2.7 Maintenance of ODP

Continue maintenance of ODP Recommendations.

Close collaboration and liaison with other study groups and other international groups implementing ODP is highly desirable to ensure the widest applicability of resulting Recommendations.

This work is to be carried out in collaboration with ISO/IEC JTC 1/SC 7/WG 19.

3 Tasks

Tasks include, but are not limited to:

1.1.1.15 I.3.1 Tasks related to the work on directories, PKI and PMI

a) Maintain the Directory by progressing Defect Reports and Technical Corrigenda.

b) Identify new directory requirements in support of new and current technologies.

c) Develop the ninth edition of the ITU-T X.500-series of Recommendations.

d) Develop enhancements to ITU-T X.509, X.510 and X.pki-em to support new requirements like automatic procedures for establishing and maintaining PKI.

1.1.1.16 I.3.2 Tasks related to the work on ASN.1

a) Provide updated Recommendations for ITU-T X.680- X.690- and X.890-series throughout the study period in response to user needs, producing new editions when appropriate.

b) When there is a need to improve data transfer, assist other Questions in all study groups in the provision of ASN.1 modules equivalent to XML schemas defined in ITU-T Recommendations (existing or under development), particularly in low bandwidth situations.

c) Monitor and assist with the publication process of approved Recommendations | International Standards and Technical Corrigenda.

d) Resolve all Defect Reports and progress Technical Corrigenda as necessary.

e) Ensure that all liaisons related to ASN.1 work are handled in a timely and appropriate manner.

f) Develop any additional tutorials or web pages that are likely to assist users of ASN.1.

1.1.1.17 I.3.3 Tasks related to the work on object identifiers and their registration authorities

a) Provide updated Recommendations for ITU-T X.660-and X.670-series throughout the study period in response to user needs, producing new editions when appropriate.

b) Monitor and assist with the publication process of approved Recommendations | International Standards and Technical Corrigenda.

c) Resolve all Defect Reports and progress Technical Corrigenda as necessary.

d) Ensure that all liaisons related to OID work are handled in a timely and appropriate manner.

e) Develop any additional tutorials or web pages that are likely to assist users of OIDs.

f) Obtain agreement in ISO/IEC JTC 1/SC 6 and SG17 on any additional OID allocations that are considered necessary.

g) Review candidacies for Registration Authorities for each kind of names covered by Rec. ITU-T X.660 | ISO/IEC 9834-1, propose to SG17 the organization to appoint, and inform ISO/IEC/JTC 1/SC 6 using Liaison Statement of the retained candidacy.

h) Under the responsibility of the OID Project Leader:

- Provide general advice to users of OIDs;
- Promote the use of international OIDs within other study groups and external standards development organizations (SDOs);
- Help countries with the establishment and maintenance of national registration authorities for OIDs (including international OIDs).

1.1.1.18 I.3.4 Tasks related to the work on TTCN

a) Maintain Recommendations under responsibility of this Question.

b) Promote the use of TTCN within other study groups and external SDOs.

1.1.1.19 I.3.5 Tasks related to the work on formal language maintenance

Develop corrections or enhancements, as needed, to Recommendations related to SDL, UML profile, MSC, URN, and CHILL. Maintain the SDL Implementers' Guide.

1.1.1.20 I.3.6 Tasks related to the work on OSI maintenance

Develop corrections or enhancements to OSI Recommendations, as needed, based on received contributions and to resolve any reported defects. Maintain the OSI Implementers' Guide.

1.1.1.21 I.3.7 Tasks related to the work on ODP maintenance

Develop corrections or enhancements to ODP Recommendations, as needed, based on received contributions and to resolve any reported defects.

An up-to-date status of work under this Question is contained in the SG 17 work programme at https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=17&sg=17.

4 Relationships

WSIS Action Lines:

– C5

Sustainable Development Goals:

– 8 (Decent Work and Economic Growth)

– 9 (Industry, Innovation and Infrastructure)

Recommendations:

– H.200-series, H.323, H.350-series, T.120, X.600-X.609 series, X.700-series, X.800-X.849 series, Z-series

Questions:

– All ITU-T Questions related to the above Recommendations and Q14/17 related to Distributed PKI

Study Groups:

– ITU-T SGs 2, 9, 11, 13, 15, 16, 20 and all study groups that use Directory, ASN.1, OIDs, conformance and interoperability testing, or that have need for them

Standardization bodies:

– Internet Engineering Steering Group (IESG); Internet Engineering Task Force (IETF); IEC/TC 57; ISO/IEC JTC 1/SCs 6, 7, 27 and 31; ISO TCs 68, 204; Organization for the Advancement of Structured Information Standards (OASIS); Object Management Group (OMG); World Wide Web Consortium (W3C); European Telecommunications Standards Institute (ETSI) TC MTS; ISO/IEC JTC 1 and its sub-committees that use the ITU system design languages

Other bodies:

– Universal Postal Union (UPU); SDL Forum Society