An overview of ITU-T SG17

ITU Workshop on DLT security, identity management and privacy
Geneva, Switzerland
20 February 2023

Youki Kadobayashi

Co-Rapporteur, ITU-T SG17 Q.4

SG17 – Mission

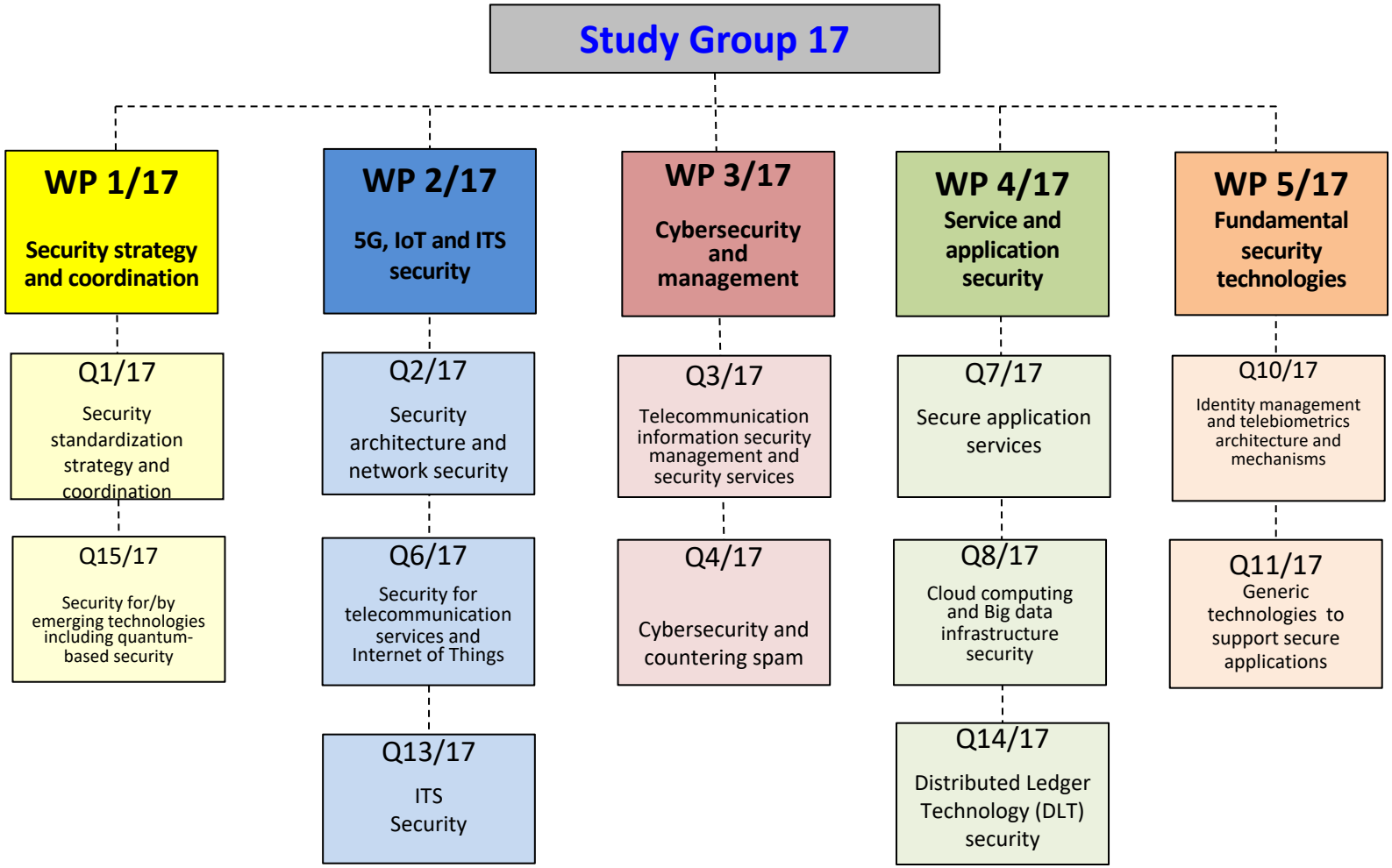
- **Building confidence and security in the use of information and communication technologies (ICTs) is one of the top priorities of the ITU (PP-Res. 130, WSIS Action Line C5).**
- New emerging technologies such as security for IMT-2020/5G and beyond, IoT, smart cities, DLT, big data analytics, ITS, security aspects related to artificial intelligence (AI) and quantum-related technologies., need technical, organizational, and physical measures to protect assets for the network, applications, and services.
- New security approaches to adequately address emerging security threats should be addressed.

ITU-T Study Group 17 Overview

- SG17 has 5 Working Parties with 12 Questions approved by WTSA-20 including one Question for strategy and coordination.
  - Q1 on Security standardization strategy and coordination
  - Q2 on Security architecture and network security
  - Q3 on Telecommunication information security management and security services
  - Q4 on Cybersecurity and countering spam
  - Q6 on Security for telecommunication services and Internet of Things (IoT)
  - Q7 on Secure application services
  - Q8 on Cloud computing and Big data infrastructure security
  - Q10 on Identity management and telebiometrics architecture and mechanisms
  - Q11 on Generic technologies to support secure applications
  - Q13 on Intelligent transport system (ITS) security
  - Q14 on Distributed Ledger Technology (DLT) security
  - Q15 on Security for/by emerging technologies including quantum-based security.

- See SG17 web page for more information https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx

ITU-T SG17, Security



SG17 Working Party Structure

- **WP 1 "Security strategy and coordination"**
  - Q1/17 Security standardization strategy and coordination
  - Q15/17 Security for/by emerging technologies including quantum-based security
- **WP 2 "Security technologies for 5G and their applications such as IoT and ITS"**
  - Q2/17 Security architecture and network security
  - Q6/17 Security for telecommunication services and Internet of Things (IoT)
  - Q13/17 Intelligent transport system (ITS) security
- **WP 3 "Cybersecurity technologies and its management"**
  - Q3/17 Telecommunication information security management and security services
  - Q4/17 Cybersecurity and countering spam
- **WP 4 "Service security technologies for secure applications"**
  - Q7/17 Secure application services
  - Q8/17 Cloud computing and Big data infrastructure security
  - Q14/17 Distributed Ledger Technology (DLT) security
- **WP 5 "Fundamental security technologies"**
  - Q10/17 Identity management and telebiometrics architecture and mechanisms
  - Q11/17 Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications

Question 3/17 - Telecommunication information security management and security services

- Responsible for telecommunication information security management
  - E.409 (joint responsibility with SG2), X.1051, X.1052, X.1053, X.1054, X.1055, X.1056, X.1057, X.1058, X.1059, X.1061; X.Suppl.13, X.Suppl.27, X.Suppl.32, X.Suppl.34, X.Suppl.36
- **7 Recommendations approved, and 4 Supplements agreed in last study period**
  - **X.1052**, Information security management processes for telecommunications organizations
  - **X.1053**, Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations
  - **X.1054| ISO/IEC 27014**, Information technology - Security techniques - Governance of information security
  - **X.1058 | ISO/IEC 29151,** Information technology - Security techniques - Code of practice for personally identifiable information protection
  - **X.1059, I**mplementation guidance for telecommunication organizations on risk management of their assets globally accessible in IP-based networks
  - **X.1060,** Framework of creation and operation for a Cyber Defence Centre
  - **X.1061,** Cyber insurance acquisition guideline for Information and Communication Technologies (ICT) services provider
  - **X.Suppl.13**, ITU-T X.1051 – Supplement on information security management users' guide for Recommendation ITU-T X.1051
  - **X.Suppl-32,** ITU-T X.1058 – Supplement on code of practice for personally identifiable information(PII) protection for telecommunications organizations
  - **X.Suppl.34,** ITU-T X.1051 – Supplement on code of practice for information security controls for telecommunication organizations
  - **X.Suppl.36**, ITU-T X.1051 – Supplement on critical security controls for telecommunication organization information and network security management in support of ITU-T X.1051
- **Texts currently under study include:**
  - **X.1051rev2**, Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations
  - **X.sup-cdc,** Supplement to X.1060: X.1060 Tutorial material
- Close collaboration with ISO/IEC JTC 1/SC 27/WG 1
- Rapporteur: Ms Miho NAGANUMA

For AAP consent

For agreement

Question 4/17 – Definition of Cybersecurity

- Definition of Cybersecurity
  (ref. Rec. ITU-T X.1205, Overview of cybersecurity):

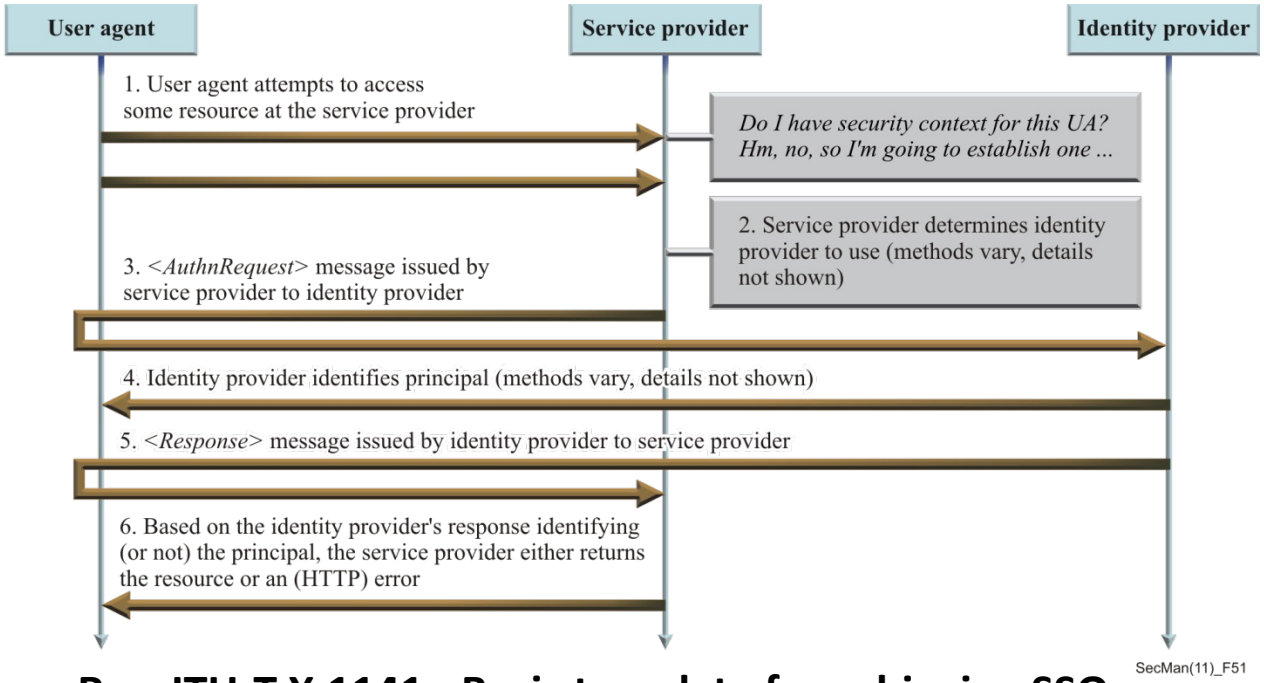
  Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

  The general security objectives comprise the following:

  – Availability
  – Integrity, which may include authenticity and non-repudiation
  – Confidentiality.

Question 7/17 – Security Assertion Markup Language (SAML) eXtensible Access Control Markup Language (XACML)

- Security Assertion Markup Language (Rec. ITU-T X.1141)
- eXtensible Access Control Markup Language (Recs. ITU-T X.1142, X.1144)
- Security architecture for message security in mobile web services (Rec. ITU-T X.1143)



Rec. ITU-T X.1141 - Basic template for achieving SSO

Question 14/17 – Distributed ledger technology security

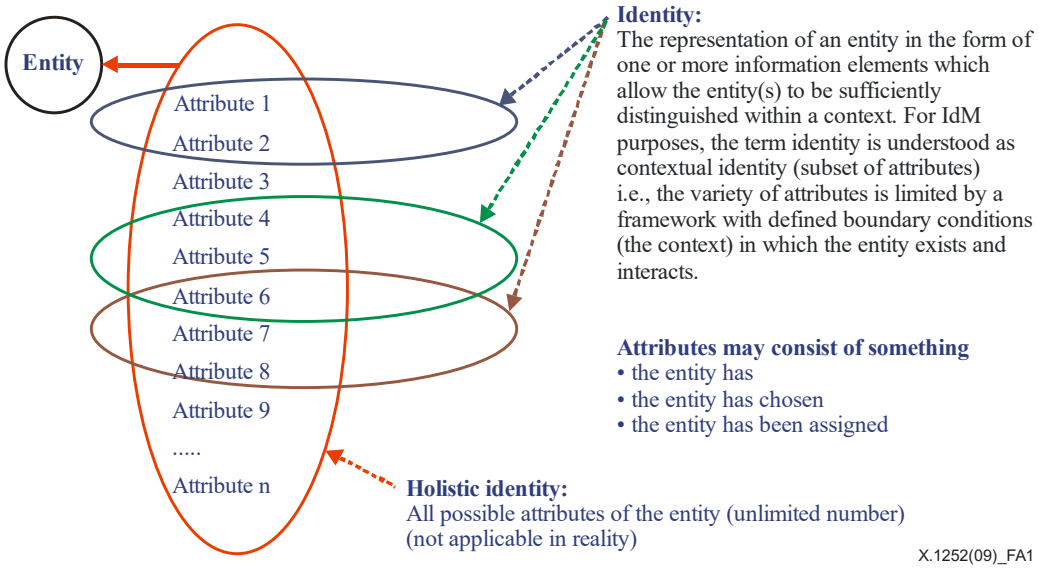
- In this study period, Q14/17 has 15 work items on DLT
- **9 Recommendations approved last study period:**
  - **X.1400**, Terms and definitions for distributed ledger technology
  - **X.1401,** Security threats of distributed ledger technology
  - **X.1402**, Security framework for distributed ledger technology
  - **X.1403,** Security guidelines for using distributed ledger technology for decentralized identity management
  - **X.1404**, Security assurance for distributed ledger technology
  - **X.1405**, Security threats and requirements for digital payment services based on distributed ledger technology
  - **X.1406**, Security threats to online voting system using distributed ledger technology
  - **X.1407**, Security requirements for intellectual property management based on distributed ledger technology
  - **X.1408**, Security framework for the data access and sharing management system based on the distributed ledger technology
- **Recommendations approved in this study period:**
  - **X.1409**, Security Services based on Distributed Ledger Technology
- **Recommendations and Technical Report currently under study include:**
  - For TAP approval: **X.1410(X.sa-dsm)**, Security architecture of data sharing management based on the distributed ledger technology
  - **X.sc-dlt**, Security controls for distributed ledger technology
  - For AAP consent: **X.srcsm-dlt**, Security Requirements for Smart Contract Management based on the distributed ledger technology
  - **TR.qs-dlt**, Technical Report: Guidelines for quantum-safe DLT system

Question 10/17 – Baseline identity management terms and definitions

- Provides 70 definitions of key terms used in identity management (IdM)

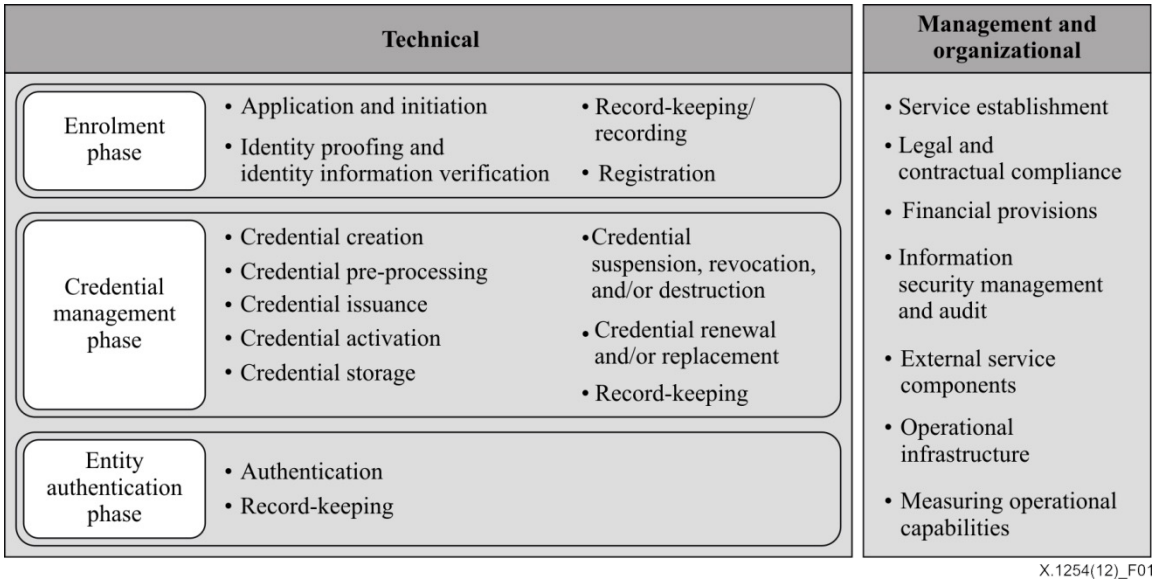
6.30 identity: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

NOTE – Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite



Rec. ITU-T X.1252 – Relationships between entity, identities and attributes

Question 10/17 – Entity authentication assurance framework



Rec. ITU-T X.1254 - Overview of the entity authentication assurance framework

Level	Description
1 – Low	Little or no confidence in the claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

Rec. ITU-T X.1254 - Levels of assurance

Question 11/17 - Generic technologies to support secure applications (parts: PKI, PMI)

- ITU-T X.509 on public-key/attribute certificates is the cornerstone for security:
  - Base specification for public-key certificates and for attribute certificates
  - Has a versatile extension feature allowing additions of new fields to certificates
  - Basic architecture for revocation
  - Base specification for Public-Key Infrastructure (PKI)
  - Base specifications for Privilege Management Infrastructure (PMI)
- ITU-T X.509 is used in many different areas:
  - Basis for eGovernment, eBusiness, etc. all over the world
  - Used for IPsec, cloud computing, and many other areas
  - Is the base specification for many other groups (PKIX in IETF, ESI in ETSI, CA Browser Forum, etc.)
- First X.509 event was held on May 9 2022 to celebrating 33 years of successful implementation and to identify future development directions.

Question 11/17 (cnt'd) - Generic technologies to support secure applications (parts: Directory, PKI, PMI)

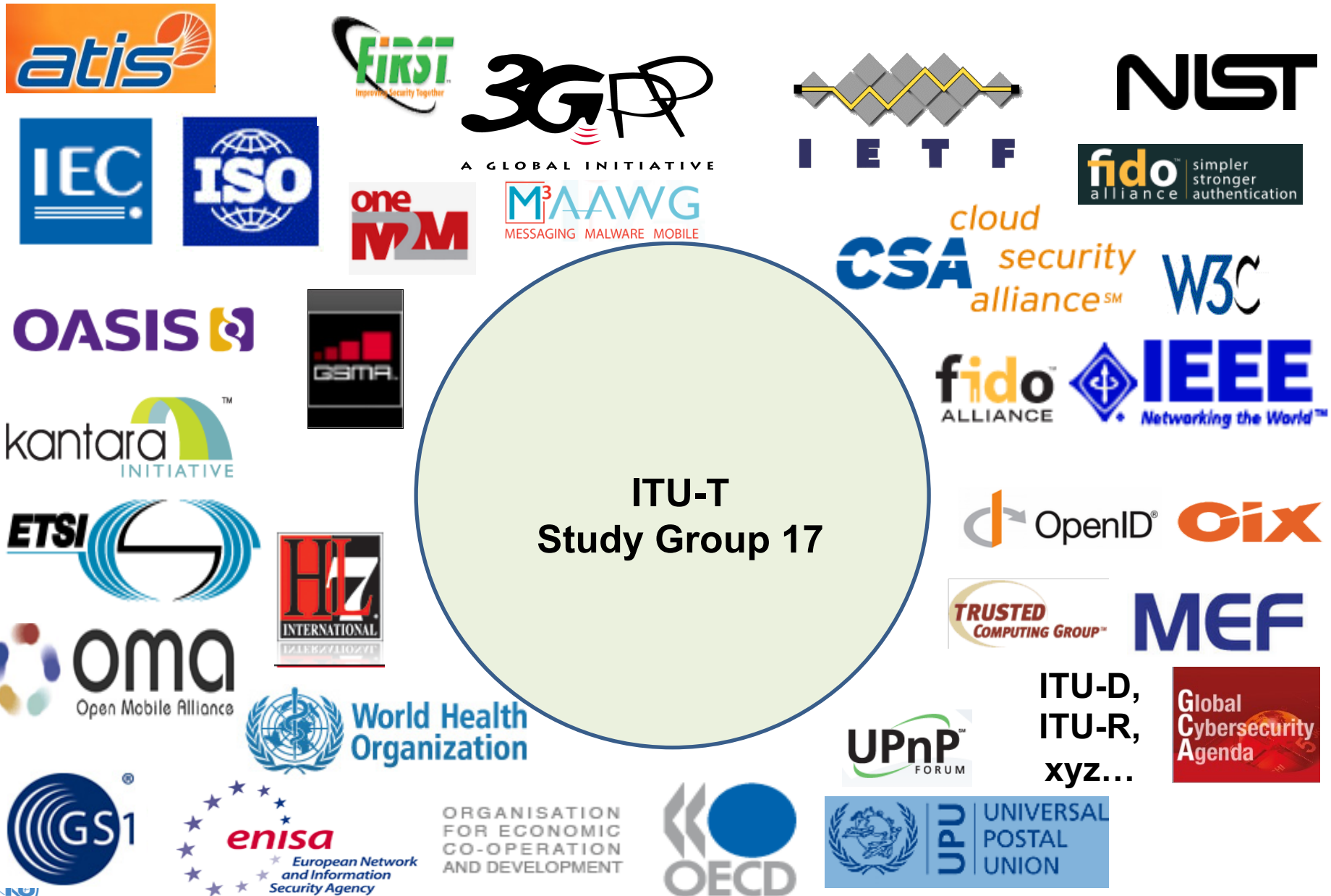
- **Recommendations approved in last study period**
  - **X.500 (revised),** Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services
  - **X.501 (revised**), Information technology – Open Systems Interconnection – The Directory: Models
  - **X.509 (revised),** Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
  - **X.510 (new):** Information technology – Open Systems Interconnection – The Directory: Protocol specifications for secure operations
  - **X.511 (revised),** Information technology – Open Systems Interconnection – The Directory: Abstract service definition
  - **X.518 (revised),** Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation,
  - **X.519 (revised),** Information technology – Open Systems Interconnection – The Directory: Protocol specifications
  - **X.520 (revised),** Information technology – Open Systems Interconnection – The Directory: Selected attribute types
  - **X.521 (revised),** Information technology – Open Systems Interconnection – The Directory: Selected object classes
  - **X.525 (revised)**, Information technology – Open Systems Interconnection – The Directory: Replication
- **Recommendations under development**
  - **X.510Amd.1,** Information technology – Open systems Interconnection - The Directory – Protocol specifications for secure operations
  - **X.508(X.pki-em)**, Information technology – Public key Infrastructure: Establishment and maintenance
  - **XSTR.x509ac4sc,** Technical Report: A use case of X.509 Attribute Certificate for Supply Chain
  - **X.dpki**, Decentralized Public-key infrastructure

r AAP consent
or AAP consent
VI at Aug 2022

SG17 relationship with other entities

Question	Entities	Topics
1/17	all	All topics
2/17	ISO/IEC JTC 1 SCs 27, 37, IEC TC 25, ISO TC 12, IETF, ATIS, ETSI, 3GPP,	Security architecture
3/17	Close collaboration with ISO/IEC JTC 1/SC 27	ISM, PII protection
4/17	Extensive relationships with many external bodies: IETF, IEEE, OASIS, NIST; ETSI; 3GPP; ISO/IEC JTC 1/SC 27; IEC TC 57, IEC TC 65/WG10; OMA; TCG Effective cooperation with ITU-D, IETF, ISO/IEC JTC 1, 3GPP, OECD, M3AAWG, ENISA and other orgs	Cybersecurity, CYBEX Anti-spam
6/17	ISO/IEC JTC 1/SCs 6, 25, 27 and 31; ISO TC 204, IEC SEG 6 (Micro Grid), IEC SMB WG3, IEC TCs 57 and 65; IETF; 3GPP; OMA; GSMA; ATIS; NIST; ETSI TC ITS, M2M; oneM2M; UPnP	Mobile security, IoT/USN security; smart grid security, ITS security; SDN security; IPTV security
7/17	OASIS, OMA, W3C, ISO/IEC JTC 1/SC 27, Kantara Initiative	Application security
8/17	Working closely with ITU-T SG13, ISO/IEC JTC 1/SCs 27 and 38, and Cloud Security Alliance	Cloud computing security
10/17	ISO/IEC JTC 1 SCs 6, 27 and 37; IETF; ATIS; ETSI INS ISG, OASIS; Kantara Initiative; OMA; NIST; 3GPP; 3GPP2; Eclipse; OpenID Foundation; OIX etc. ISO/IEC JTC 1/SCs 17, 27 and 37, ISO TCs 12, 68 and 215, IEC TC 25, IETF, IEEE	Identity management Telebiometrics
11/17	ISO/IEC JTC 1/SC 6/WG 10; IETF, ETSI TC ESI, CA Browser Forum SDL Forum Society, ETSI TC MTS; SG11, JCA-CIT	Directories, PKI, ASN.1, OID, ODP, OSI SDL-2010, URN, TTCN-3
13/17	ISO TCs 22 and 204, ISO/IEC JTC 1/SCs 6, and 27, IETF WG ITS, IEEE 802.11 WG and 1609 WG, SAE International, ETSI TC ITS, W3C Automotive WG, UNECE (UN Economic Commission for Europe) Working Party 29 and subsidiary bodies	ITS security
Q14/17	ISO TC 307, ISO/IEC JTC 1/SC 27, GSMA, W3C, ATIS, CCSA, TIA, TTA, TTC	DLT security
Q15/17	ETSI TC Cyber, ISG-QKD; ISO/IEC JTC 1/SC 27; OASIS; IETF	Quantum

Coordination with other bodies



Reference links

- Webpage for ITU-T Study Group 17
  - https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx
- Webpage on ICT security standard roadmap
  - https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/default.aspx
- Webpage for JCA on identity management
  - https://www.itu.int/en/ITU-T/jca/idm/Pages/default.aspx
- Webpage for JCA on child online protection
  - https://www.itu.int/en/ITU-T/jca/COP/Pages/default.aspx
- ITU Security Manual: Security in Telecommunications and Information Technology
  - https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-4-PDF-E.pdf

SAFE : Security is Absolutely First Everywhere

Thank you very much for your attention!