INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

COM 17 – LS 004 – E

English only

Original: English

Question(s): 1, 2/17 Geneva, 11-20 February 2009

Ref. : TD 0254 Rev.1

Source: ITU-T SG 17 (Geneva, 11-20 February 2009)

Title: Solicitation of interest in ITU-T SG 17 initiative on business use of telecommunications/ICT security standards

LIAISON STATEMENT

For action to: ITU-D Q.22/1, BDT programme 3; ITU Council Working Group on Resolution 149; ISO/IEC JTC 1/SC 27; IETF; ETSI; ENISA; IEEE; ATIS

For comment to:

For information to:

Approval: Agreed to at SG 17 meeting

Deadline: 15 September 2009

Contact:	Arkadiy Kremer Chairman, ITU-T SG 17	Tel: +7 495 673 3246 Email: kremer@rans.ru
Contact	Antonio Guimaraes Rapporteur, Q.1/17	Tel: +55 61 2312 2819 Email: ateixeira@anatel.gov.br
Contact:	Patrick Mwesigwa Rapporteur, Q.2/17	Tel:+256 414339004 Fax:+256 414348832 Email: pmwesigwa@ucc.co.ug

ITU-T Study Group 17 Question 1 (Telecommunications systems security project)) has initiated a new work activity called "Business use of telecommunications/ICT security standards." A description of the work activity is provided in the attachment. The output of the initiative would be of benefit primarily to organizations planning to deploy telecommunications/ICT security systems. ITU-T SG 17 sees developing countries and countries with economies in transition (DC/CET) to be especially interested in the results of this activity as they could better understand appropriate telecommunications/ICT security standards to consider.

ITU-T SG 17 seeks comment on the work activity from the ITU-D and other standards development organizations. Specifically, your views on the following would be appreciated:

- Do you agree that this work activity would be useful to organizations and/or DC/CETs planning to deploy telecommunications/ICT security systems?
- Does your organization have existing information that may be related to this work activity or that may be used to progress this work?

- Does your organization have contact with DC/CETs that may further elaborate on their needs and detail the information they may find most useful to capture in the activity output?
- Does your organization have any suggestions to provide additional detail regarding the proposed summary sheet elements (Section 1 in the attachment and in the examples) or criteria to select standards (Section 2 in the attachment)?
- Would your organization be willing to assist the ITU-T SG 17 in progressing this work?

ITU-T SG 17 welcomes your consideration and your response on this matter.

Attachment: 1

The attachment provides the scope of the proposed initiative on business use of top 100 security standards. Included are example texts for five standards that illustrate the proposal.

WSIS action Line C5 “Building confidence and security in the use of ICT”
Business use of Top 100 security standards

Scope

1. The report will consist of summary sheets for analysed security standards
    - Status and summary of standards
    - Who does the standard affect?
    - Business benefits
    - Technologies involved
    - Technical implications
2. Proposed criteria for Top 100 security standards list
    - **Readiness and abilities:** security standard contains measures of information security which pertain to the readiness and ability of operators or users to counter security threats
    - **Balance of interests:** in responding to threats the balance of stakeholder interests should be maintained
    - **Cost efficiency:** security standards and counter measures will be prioritised according to cost effectiveness and ranked according to their potential impact and their estimated implementation cost
    - **Controllability:** all standards in the report will be verifiable
    - **Variety of implementations:** consideration of various implementation options
3. Several examples:
    - ITU-T Recommendation X.509: Information technology – Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
    - The Common Criteria (ISO/IEC 15408)
    - EMV (version 3.1.1)
    - SIM and SIM Toolkit (GSM11.11, GSM11.14)
    - ISO/IEC 7816 - Smartcards with contacts

ITU-T Recommendation X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Who does this standard effect?

Anyone developing products, profiling application security, or deploying security solutions that are based on PKI or PMI, particularly for services such as authentication, encryption and confidentiality, digital signatures and nonrepudiation, and authorization.

Summary of standard

The standard defines frameworks for Public-Key Infrastructure (PKI) and for Privilege Management Infrastructure (PMI). These frameworks include:

- Infrastructure models
- Certificate and Certificate Revocation List (CRL) syntax definitions
- Directory schema object definitions
- Certificate path processing procedures

The standard also specifies use of these frameworks by Directory systems in their provision of secure services to Directory users.

Six editions of X.509 have been produced over the years, with the most recent being approved by ITU in September 2008. All editions have been developed cooperatively by ITU and ISO/IEC. The corresponding ISO/IEC standard is 9594-8.

Public Key Infrastructure

The basic PKI model consists of public-key certificates, being issued by Certification Authorities (CA) to end-entities for use in security services including authentication, confidentiality, and non-repudiation. CAs may also issue certificates to other CAs creating certificate paths between a given end-entity certificate and remote verifiers. A revocation scheme and mechanism for publishing information about certificates that are no longer considered trustworthy by their issuer is also defined.

The PKI framework has evolved from the 1st edition through the 6th edition. As additional requirements emerge, the basic PKI models have remained unchanged; however the syntaxes of both public-key certificates and CRLs have evolved. The versions, defined in the 3rd edition and maintained through the 6th edition, are public-key certificate (v3) and CRL (v2).

These syntaxes enable an unbounded set of extensions to be included in certificates and CRLs. The standard set of extensions, enables inclusion of additional information such as:

- Key and policy information
- Subject and Issuer details
- Certification path constraints
- CRL numbers and certificate revocation reasons
- CRL partitioning and delta information

Additional extensions can be defined by other industry groups.

The necessary Directory schema definitions to store and retrieve PKI data objects in LDAP and X.500 repositories are specified. These objects include Certification Authorities (CA), certificate subjects, CRLs, certification paths and policy objects.

Privilege Management Infrastructure

The PMI framework is more recent than its PKI counterpart. The 3rd edition of X.509 was the first to introduce a basic syntax for attribute certificates. The 4th edition, extended that structure, resulting in attribute certificate (v2) and defined the framework for privilege management, along the same basic models as for PKI. The 6th edition has further extended the framework by allowing privileges assigned in one PMI domain to be effective in another PMI domain.

The PMI model enables very basic implementations, where privilege is assigned directly by the Source of Authority (SOA) to the privilege holder through issuance of an attribute certificate. Privilege may also be assigned through public-key certificates but there are limitations to their use in PMI. The model also enables more complex infrastructures that include privilege delegation through intermediary Attribute Authorities (AA) as well as the use of roles. With roles, a role specification certificate would be issued to a role rather than an individual and contains the specific privileges of the role. Corresponding role assignment certificates are issued to individuals occupying a given role, thereby indirectly assigning the role privileges to those individuals. The same scheme for publishing revocation information about public-key certificates is adapted for use with attribute certificates that are no longer considered trustworthy.

Although the base syntax for attribute certificates was defined in the 3 rd edition, the syntax required extending and resulted in (v2) attribute certificate syntax. These revisions enable tighter binding between an attribute certificate and the corresponding public-key certificate used to authentication its holder, as well as issuance of attribute certificates to entities that do not participate in authentication protocols (e.g. software applets). A standard set of extensions was added for PMI to support:

- Basic privilege restrictions & limitations.
- Control of delegation & policy.
- Linking of certificates for role management.
- Identification of SOA entities and publication of privilege definitions.
- Revocation scheme extensions.

The necessary Directory schema definitions to store and retrieve PMI data objects in LDAP and X.500 repositories are specified. These objects include Source of Authority (SOA), Attribute Authority (AA), attribute certificate holders, CRLs, delegation paths, and privilege policy objects.

Directory use of PKI & PMI

The use of PKI, for Directory authentication and for the protection of directory operations and data objects, is outlined in X.509. However the details of how PKI relates to specific Directory functions are described within the other specifications in the X.500 series (primarily X.511 and X.518). Similarly, the use of attribute certificates for access control to directory information is described in other specifications in the series (primarily X.501).

Business benefits

PKI and PMI are being used as the foundation for securing transactions in Business to Business (B2B), Business to Customer (B2C) and Government to Citizen (G2C) environments. Profiles of X.509 are being defined for specific communities in the Internet, financial, government and other sectors. The basic data structures defined in X.509 for certificates and CRLs, through their extensibility schemes, enable application specific extensions, while still supporting fundamental interoperability.

Technologies involved

The standard is based on the use of pubic-key cryptography for digital signatures and encryption. The standard also makes use of Directory systems, as defined in related specifications within the X.500 Series and as defined in the IETF LDAP activities. This standard forms the basis upon which other standards are built.

Technical implications

This standard is based on the use of ASN.1.

The Common Criteria (ISO/IEC 15408)

Who does this standard effect?

The Common Criteria (also published as ISO15408) is the reference document for expressing security requirements on systems. Anyone who is involved with security in his organization (as designer, auditor, programmer or manager) should have a good understanding of this standard and use it as a reference document.

Summary of standard

The CC is presented as a set of distinct but related parts as identified below:

- **Part 1**: Introduction and general model, is the introduction to the CC. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high level specifications for products and systems. In addition, the usefulness of each part of the CC is described in terms of each of the target audiences.

- **Part 2**: Security functional requirements, establishes a set of security functional components as a standard way of expressing the security functional requirements for Targets of Evaluation (TOEs). Part 2 catalogues the set of functional components, families, and classes.

- **Part 3**: Security assurance requirements, establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance components, families, and classes. Part 3 also defines evaluation assurance levels that define the predefined CC scale for rating assurance for TOEs (Evaluation Assurance Level).

In support of the three parts of the CC listed above, other technical rationale material and guidance documents have been or are being prepared (e.g. the Common Methodology for Security Evaluation).

Business benefits

The advantages of using the common criteria are manifold:

- the common criteria is a methodology which is ***internationally accepted***

- the common criteria can be used as a ***security assurance methodology*** covering the different processes: development, evaluation and operation. The evaluation results help consumers gain confidence that the IT product is secure enough for their intended application and that the security risks implicit in its use are tolerable.

- the common criteria also describe an ***evaluation methodology*** which can be applied internally. The CC can be used as a basis for defining the internal audit methodology.

- the security assurance requirements defined in the common criteria cover ***other aspects*** than pure security or cryptographic requirements, such as configuration management, delivery and operation, documentation, testing, etc...

- it becomes possible to make ***assessments*** with international ***mutual recognition*** of certificates of the degree of security (Evaluation Assurance Level: from 1 to 7).

Many Protection Profiles are already defined (on smartcard hardware, on smartcard software, on PKI, on firewalls, etc...) and could be used as reference when expressing security requirements or comparing products.

Technical implications

The Common Criteria (CC) is a standard which aims to assist in evaluating the security of Information Technology (IT) products. The Common Criteria became an ISO standard (IS15408) in 1999 as a result of co-operation of different bodies from Europe (ITSEC), USA (TCSEC - Orange Book) and Canada (CTCPEC). By using such a common criteria base, the results of the evaluation is meaningful to a wider audience and during a wider time frame. They also permit comparability between the results of independent security evaluations. This is done by providing a common set of security requirements for the security functions of IT products and for assurance measures applied to them during the evaluation.

The CC describes security requirements in

• **functional requirements:** defining the actual security behaviour of the IT product. Part 2 gives a catalogue of possible requirements split in 11 classes : Security Audit, Communication, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Privacy, Protection of security Functions, Resource Utilization, Access, and Trusted Path/Channels.

• **assurance requirements:** defining how one can establish confidence in the defined security requirements. Part 3 defines different assurance classes: Configuration Management, Delivery and Operation, Development, Guidance Documents, Life Cycle Support, Test, Vulnerability Assessment and Maintenance of Assurance.

The CC also contains a set of pre-defined assurance levels (from 1 to 7) using components from Part 3. The higher the level of assurance, the higher the confidence that one will meet the expressed security objectives.

When applying the CC to a given application, a difference is made between Protection Profiles and Security Targets.

• **Protection Profiles:** are an implementation independent set of security objectives and requirements. They are valid for a category of IT products or systems that meet similar consumer needs. E.g. a "Firewall Protection Profile". They are normally agreed within an industry.

• **Security Targets:** are applied to an identified IT product (e.g. MilkyWay Firewall)

A Protection Profile describes:

- the product under evaluation (referred to as the Target of Evaluation - TOE)
- the security environment; including the assumptions being made, the identified threats and the organizational security policies.
- the security objectives, i.e. what one wants to protect
- the security requirements, which are a subset of the functional (Part 2) and assurance (Part 3) requirement catalogue as defined in the CC.

The Security Target is to a great extent similar to the protection profile, except it has been applied to a actual product.

For obtaining official evaluation, the Security Target becomes the basis for the agreement between the product vendor, evaluators and certification agencies as to what security functionality the product (TOE) offers and the scope of the evaluation. The Security Target and TOE are submitted to a third party certified laboratory that proceeds with the evaluation. The results of the evaluation confirm that the ST is satisfied with the TOE, in other words the functional and assurance security claimed in the ST has been verified. The certified laboratory facility produces a report documenting the findings. The report is submitted to a government agency acting as the Certification Body, which then proceeds with certification/validation of the product (i.e. TOE certification/validation).

EMV (version 3.1.1)

Who does this standard effect?

EMV is an acronym for a set of specifications. It stands for Europay International, MasterCard International, and Visa International. The EMV standard specifies debit/credit cards, the corresponding card acceptor devices (terminals), and the applications supported by them in order to perform debit and/or credit payments. Firstly, the standard should be known to financial organizations willing to issue EMV cards or to acquire EMV transactions. Secondly, since the EMV compliant cards can accommodate multiple applications, the standard should be known to anybody who wants to host additional applications on these cards (e.g. loyalty, security token,...).

Summary of standard

The EMV specifications consist of three documents:

- *EMV'96 Integrated Circuit Card Application Specification, shortly referred to as the EMV Application Specification.*

This part of the specifications deals with both physical and logical aspects of an EMV card. It details electromechanical characteristics, the logical interface of the card with data elements and commands, transmission protocol. Since the EMV cards are multi-application, this part of the standard specifies the selection application process in the card. All the security aspects related to the security services and their corresponding security mechanisms are also detailed in this part of the standard.

- *EMV'96 Integrated Circuit Card Specification, shortly referred to as EMV Card Specification.*

This part of the standard details the functional requirements of an EMV compatible terminal, its general physical characteristics, cardholder/acquirer interfaces, as well as the software architecture, including software and data management.

- *EMV'96 Integrated Circuit Card Terminal Specification, shortly referred to as EMV Terminal Specification.*

This part of the standard proposes the acceptable transaction profile of a debit/credit application. Each function used in the transaction process is explained, together with its acceptable execution place in the transaction flow.

Business benefits

The effort of the EMV consortium to elaborate a common set of specifications was intended to provide interoperability. The main benefit of this policy is the mutual support in operation of the organizations adopting this standard. Thus, terminals of one organization can support financial transactions initiated by cards issued by another organization, without the need of establishing business relations in advance. Another benefit of interoperability is the decrease of costs due to a better offer of smartcard and terminal providers. These specifications are intended to allow the migration of the actual debit/credit magnetic stripe cards to smartcards, which is believed to improve the security of the financial institutions against dishonest users. The direct result is the reduction of financial loss due to frauds in the system and the increasing confidence in payment products based on smartcards.

Moreover, the EMV opens new possibilities for multi-application smartcards.

Technologies involved

- Smart card technology (ISO/IEC 7816)
- Public key cryptography

- Certification authorities

Technical implications

From a technical point of view, the EMV standard is an important advance towards secure debit/credit transactions. Both issuers and acquirers have better possibilities to express their security policies and to choose the optimum balance between security and service availability.

Thus, the standard allows implementing advanced security mechanisms, as the dynamic data authentication and enciphered PIN, to the cost of using more powerful smart cards, which include crypto-coprocessors in their hardware architectures. This can sustain a secure debit/credit transaction involving small amounts even offline, in case the terminal cannot communicate online to the bank for a reason of network failure. In this case, the level of security for the issuer is kept high to a very good level of availability of the service for the client.

Contrarily, in an environment where reliable online connections can be established, a static data authentication could be enough for proving the authenticity of the card, the proof of transaction remaining completely at the responsibility of the issuer. This reflects in a lower price for the smart card, since it does not involve generation of signature, and consequently performing some long arithmetic requiring special resources.

The implementation of the EMV specifications leads also to important modifications of the payment networks run by payment systems operators. Authorization hosts must also be modified to support the new standard.

SIM and SIM Toolkit (GSM11.11, GSM11.14)

Who does this standard effect?

The SIM and especially the STK standard allows the issuer of GSM cards to personalize the handset towards its own application: menus can be added, SMS message can communicate, etc... SIM and STK are therefore of high importance for anybody considering m-Applications (m-Banking, m-Commerce, etc...)

Summary of standard:

A SIM (subscriber identification module) is a small-sized smartcard (ISO/IEC 17816-compatible) inserted in a GSM handset. The SIM task is to permit network access only to authorized persons, thus ensuring reliable billing. Next to this, the SIM stores some additional data, such as abbreviated numbers, last dialed number, etc.. The SIM is standardized in GSM11.11.

At the end of 1995, a new standard was issued: STK = the SIM ToolKit (GSM11.14). Contrary to the SIM which can be seen as a server application offering data storage and crypto-functionality, the STK is an active element. Using the STK, the issuer can control the handset:

- menus can be changed or added
- SMS messages with application data can be sent and received
- information can be displayed
- the user can be asked to select or enter data.

STK is therefore a very powerful instrument when designing m-Applications. In 1999, the first applications went live, supporting m-Banking, stock exchange information, travel and entertainment news, etc...

For the moment two new standards have been published: ETSI GSM03.19 which standardizes the STK API and ETSI GSM03.48 which standardizes how STK application can be downloaded over the air. Note that STK and WAP are complementary: the STK can be seen as a program residing in the handset, while WAP can be seen as an Internet Browser for handsets.

Business benefits

Although the business benefits for the classic SIM card is low (except for GSM operators), the SIM toolkit offers a lot more advantages. A commercial company issuing STK cards can fully control and adapt the menu of the handset. Using this feature, access to its services can become very user friendly.

Because all new GSM handsets on the market already support STK, this service can be made available today. Note that STK and WAP are complementary: the STK can be seen as a program residing in the handset, while WAP can be seen as an Internet Browser for handsets.

Technologies involved

- Smartcard technology (ISO/IEC 7816)
- SMS
- Cryptography

Technical implications

The SIM card is a classic smartcard whereby commands are sent by the handset (acting as client) and the smartcard responses (acting as a server). The commands used are mainly SELECT (to select the data file), READ (to read data on the smartcard) and UPDATE (to update the data). Next to these commands, commands are defined for protection (PIN verification, cryptograms, etc...). The SIM card application is (almost) completely standardized.

The STK is a more complex smartcard. Next to being a SIM, the smartcard is also so-called pro-active.

This implies that at application level, the smartcard (acting as a client) controls the handset (acting as a server). Because commands are always sent by the handset (ISO7816), this has been realized by implementing a FETCH command, which retrieves in the response from the smartcard the next "proactive command".

A complete set of pro-active commands have been defined, allowing one to control the menu and display, to send and receive SMS messages, to ask the user for input, etc... Defining a STK application requires therefore a good knowledge of the standard. Specifications are most of the time derived from the expected user interface (menu hierarchy, etc...).

STK applications are very powerful, both from a technical point of view as from a business point of view: controlling the user interface of a handset opens many possible applications. However because only GSM operators can issue SIM cards, an agreement with such a GSM operator needs to be found.

ISO/IEC 7816 - Smartcards with contacts

Who does this standard effect?

Anyone who wants to use smartcard (with contacts) technology within their organization.

Summary of standard

The physical and logical aspects of smartcards with contacts have been standardized by ISO/EIC within the ISO/IEC 7816 series. The following parts cover different aspects:

- ISO/IEC 7816-1:1987: physical characteristics and associated test methods
- ISO/IEC 7816-2:1988: dimensions and location of the contacts (including the small SIM size)
- ISO/IEC 7816-3:1989: electrical signals and transmission protocol. This standard explains how the smartcard and terminal need to "agree" on a protocol, based on the so-called Answer-to-Reset (ATR). Two transmission protocols exist: T=0 and T=1, the latter being superior in error recovery.
- ISO/IEC 7816-3 Amd1:1992: explains in detail the T=1 protocol
- ISO/IEC 7816-4:1995: inter-industry commands. It explains how data is organized on a smartcard (file structure) and lists most important commands (request/response).
- ISO/IEC 7816-5:1994: numbering system and registration procedure for application identifiers
- ISO/IEC 7816-6:1995: data elements (normally part of a TLV structure)
- ISO/IEC 7816-7:1995: enhanced inter-industry commands (incl. SQL commands to access data)
- ISO/IEC 7816-8:1995: detailed security architecture of smartcards

To acquire a general idea on how smartcards can be used, ISO/IEC 7816-4 is a very interesting document.

Business benefits

The ISO/IEC 7816 standard is the basic standard for smartcards. Any smartcard should at least be compatible with ISO/IEC 7816-1 to 4.

Anybody who needs to protect data in an application with multiple users should think of smartcards as an alternative offering (with the current state of the art) the highest protection. The major benefits of the smartcard as a security token are:

- (relatively) cheap (smartcard = 1-5 euro, smartcard readers = 40-100 euro)
- personal
- transportable (one normally carries it in their wallet)
- secure (data can be protected)
- useable as crypto-processor
- pre-loaded programs can be executed on the card itself.

Technologies involved

Note that the ISO/IEC 7816 is the reference standard on which other standards have been built, such as standards of smartcard operating system (proprietary, JavaCard, ...) or application standards (EMV, CEPS, GSM SIM, STK...). For contactless smartcards, other standards apply.

Technical implications

Smartcards are very useful as a security token. Indeed smartcards have the ability to store data where access to this data can be restricted (e.g. no access, access after PIN entry, access after mutual authentication, etc...). Furthermore smartcards have cryptographic power (DES, MAC, RSA, ...) and can thus be used as crypto-processors. Finally the issuer can write (small) programs and load them into the smartcard.

Therefore different kinds of application can be built upon the smartcard technology:

- Debit and credit card: the smartcard is used to protect user data and PIN

- Electronic purse and public transport card: because the smartcard is secure, one can store money or pseudo-money on the smartcard

- GSM SIM card: in a GSM handset, the SIM is used to personalize the handset to a specific user. The SIM card contains user data (identity, telephone book, last dialed number, etc...), but also some cryptographic data to authenticate the card and the operator.

- GSM SIM Toolkit card: in this case, the smartcard is not only used as a SIM card but also changes the behaviour of the handset

- PSAM card: the smartcard used as crypto-calculator in a payment terminal

- PKI user card: to store the user private key and generate digital signatures

When specifying smartcards, the following main steps need to be followed:

- Determine which data needs to be stored on the smartcard. For obvious reasons, one only needs to store data which is proprietary to the cardholder.

- Define the access conditions to this data. Based on these access conditions, one can determine the file structure of the card and the necessary PIN and keys.

- Determine how applications will access the card. If this can be implemented with standard commands, this should be preferred. Typical applications will read, update data, check PIN, encrypt/decrypt data, check MAC, etc... Mutual authentication whereby the application authenticates the card and vice versa, plays normally also a major role

- However in some cases, particular commands are needed to speed up the application or for security reasons. In this case, the specification of the command processing must be made and implemented.

Such commands used to be written in the manufacturers assembler language, but can nowadays be written in Java (JavaCards only).

Once the smartcard is specified, a manufacturer is selected who will implement the specifications. The necessary attention also needs to be paid to the personalization process, whereby application data (including cryptographic keys) needs to be written on the card.

Quality assurance is of particular importance in the case of smartcards. Because smartcards are normally issued in large quantities, the cards must be assured for high quality prior to distribution in order to avoid replacement costs.