INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

Ref. TD 0985 Rev.2

English only

Original: English

Question(s): 10/17 Geneva, 7 – 16 April 2010

TEMPORARY DOCUMENT

Source: Q.10/17 Rapporteur

Title: Q.10/17 Recommendations Summaries

Q10/17 Recommendations Summaries

Question 10 - Identity management architecture and mechanisms

X.1250, Baseline capabilities for enhanced global identity management trust and interoperability

This Recommendation describes baseline capabilities for global identity management (IdM) trust and interoperability (i.e., to enhance exchange and trust in the identities used by entities in telecommunication/ICT networks and services). The definitions and need for identity management trust are highly context dependent and often subject to very different policies and practices in different countries. The trust capabilities include the protection and control of personally identifiable information.

X.1251, A framework for user of digital identity

This Recommendation defines a framework to enhance user control and exchange of their digital identity related information. The Recommendation also defines user and functional capabilities of the digital identity information exchange. The work includes providing the user with the ability to control the release of personally identifiable information.

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

Contact: Abbie Barbir Email abarbir@live.ca
Canada

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.mobid, 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.eaa, Information technology – Security techniques – Entity authentication assurance

This Recommendation | International Standard " defines four levels of entity authentication assurance (i.e. LoA 1 – LoA 4); and the criteria and threats for each of the four levels of entity authentication assurance. Additionally it:

- Specifies a framework for managing the assurance levels
- Based on a risk assessment, provides guidance concerning control technologies that to be used to mitigate authentication threats to authentication;
- Provides guidance for mapping the four levels of assurance to other authentication assurance schemas; and
- Provides guidance for exchanging the results of authentication that are based on the four levels of assurance

Conformance testing and validation are out of scope.

X.EVcert, Extended validation certificate

This Recommendation adopts the CA Browser Forum specification to support very high assurance trust and security mechanisms for transactions between end users and organizations that provide high value or critical services or code. Based on ITU-T's X.509 digital certificate, it adds an array of identity proofing, technologies, and protocols to significantly enhance trust. This includes the creation of an encrypted transport layer path with the trusted party. Browser providers, and increasingly other client-based software vendors now support the capability on an estimated 60 percent of computers worldwide.

X.idm-dm, Common identity data model

This Recommendation develops a common data model for identity data that can be used to express identity related information among identity management (IdM) systems.

X.idm-ifa, Framework architecture for interoperable identity management systems

This Recommendation proposes a blueprint for a modular framework architecture for identity management systems. The architecture is expected to serve as a reference while discussing, designing and developing future interoperable identity management (IdM) systems. The architecture is intended to be generic in order to satisfy versatile requirements of user-centric, network-centric and service-centric IdM systems.

In addition, an informative mapping of the architecture on to next generation networks is included.

X.1252, Baseline identity management terms and definitions

This Recommendation provides a collection of terms and definitions used in identity management (IdM). They are drawn from many sources; all are believed to be in common use in IdM. These definitions are to be used as a baseline for IdM Recommendations throughout ITU-T; they may be expanded if necessary to provide greater clarity for a specific context. This will ensure the main features of IdM are consistent, aligned and understood.

X.idmsg, Security guidelines for identity management systems

This Recommendation proposes security guidelines for identity management (IdM) systems. The security guidelines provide how an IdM system should be deployed and operated for secure identity services in NGN (Next Generation Network) or cyberspace environment. The security guidelines will focus on providing official advice how to employ various security mechanisms to protect a general IdM system and it will also study proper security procedures required when two IdM systems are interoperated.

X.priva, Criteria for assessing the level of protection for personally identifiable information in identity management

This Recommendation defines the criteria for assessing the level of protection for personally identifiable information (PII) of the identity provider and the relying party concerned in identity service, depending on the protection for personally identifiable information requested by them to the requesting/asserting party, and the type and use purpose of PII and maintain period of PII, as well as the technical and administrative measures for protection for PII.

X.1275, Guidelines on protection of personally identifiable information in the application of RFID technology

This Recommendation recognizes that RFID technology renders information pertaining specifically to the merchandise worn or carried by individuals open to abuse even as it greatly facilitates access to and distribution of such information for useful purpose. The abuse can be manifest as tracking the location of the individual or invasion of his or her privacy in another malfeasant manner. For this reason the Recommendation provides guidelines regarding the RFID procedures that can be used to enjoy the benefits of RFID while attempting to protect personally identifiable information.

X.authi, Authentication integration in IDM

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 needn't to be re-authenticated again in the service layer if (s)he has been strictly authenticated when access the operator's network. This recommendation analyzes 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.giim, Generic IdM interoperability mechanisms

This Recommendation provides a generic framework for identity management (IdM) that is independent of network types, technology or vendor specific products used to provide solutions, and operating environment taking into consideration the need for large scale flexible and dynamic authentication systems

_____