ETSI TS 102 350 V7.0.0 (2005-09)

Technical Specification

Smart cards;
Identity Files and Procedures on a UICC;
Stage 1
(Release 7)

Reference

DTS/SCP-R0287

Keywords

ID, security, smart card

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights 4

Foreword 4

Introduction 4

1 Scope 5

2 References 5

3 Definitions and abbreviations 5

3.1 Definitions 5

3.2 Abbreviations 6

4 Overview 6

4.1 Basic functionality of a TM 6

5 Requirements 7

5.1 Description of Requirements 7

5.1.1 Deployment Contexts for TMUICC 7

5.2 Secure Communications with the TMUICC 10

5.2.1 Basic Requirements 10

Annex A (informative): Liberty Alliance requirements 12

Annex B (informative): Change history 13

Annex C (informative): Bibliography 14

History 15

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Smart Card Platform (SCP).

The present document defines the stage 1 requirements for identity files and procedures on a UICC.

The contents of the present document are subject to continuing work within EP SCP and may change following formal EP SCP approval. If EP SCP modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

0 early working draft;

1 presented to EP SCP for information;

2 presented to EP SCP for approval;

3 or greater indicates EP SCP approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

There are a number of industry organizations producing authentication, privacy, and payment standards for the enterprise, mobile, financial, and services industries. For example the Liberty Alliance are creating specifications describing how a user's digital identity may be "federated", i.e. shared between (WEB) Service Providers and Identity Providers, to provide single sign-on and other services over mobile and wired networks in both online (connected) and offline (standalone) environments. Another example is that the Open Mobile Alliance has produced a set of requirements in order to create a single Identity Management enabler to be used by all OMA enablers.

The UICC platform is considered a candidate for a so-called Trusted Module for performing these identification, authentication, authorization and secure storage of personal data. Interoperability considerations require the standardization of the UICC/ME interface for the "identity" parameters on the card.

The present document is intended to collate the functional requirements from the Liberty Alliance and other "identity" forums that may have similar requirements.

1 Scope

The present document covers the client environment which typically includes an Identity User Agent (IdUA) and a secure hardware Trusted Module (TM).

Operation of the TM based on a UICC requires the use of existing standardized functions and applications on the UICC, as well as functions that are unique to the TM.

The present document focuses on the requirements for the TMUICC which has emerged from organizations such as Liberty Alliance and other relevant fora.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI TS 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

authentication assertion: proof of the authentication status of a user that is acceptable to the service provider for which access is requested

NOTE: An authentication assertion may include information describing the authentication context and cryptographic objects required for communication with the WSP.

Identity Provider: entity that creates, maintains and manages identity information for users and provides user authentication to other service providers within a federation of service providers and other identity providers that have business relationship and operational agreements

Identity Service: Internet-based service that is invoked by the user's identity

Identity User Agent (IdUA): software that allows users to retrieve and render web content, interact with an IdP, a web service provider (WSP) and has an abstracted logical interface to a Trusted Module

Signing: in TS 102 350, "signing" a message refers to the mechanism to create a proof of origin of a message by use of either Digital Signature or Cryptographic Checksum

Trusted Module: accessible storage and processing module available in association with an IdUA

NOTE: Functions include storage of personal data and credentials, client provisioning, authentication, secure messaging and application-layer security such as digital signature.

Trusted Module on a UICC: removable TM based on a UICC as defined in TS 102 221 [1] with at least one authentication application as they appear at its interface, including requirements for an end to end secure interface to the IdP and a secure local interface to the IdUA

Web Service: Generically, a service defined in terms of an XML-based protocol, often transported over SOAP, and/or a service whose instances, and possibly data objects managed therein, are concisely addressable via URIs

NOTE: Such a generic web service (gWS) may be defined in various proprietary and/or standardized terms, e.g. security paradigms.

Web Service Consumer: a role a system entity acts/performs when it makes a request to a web service

Web Service Provider: a role a system entity acts/performs when it provides a web service

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AP	Attribute Provider
CAD	Card Acceptance Device
IdP	Identity Provider
IdUA	Identity User Agent
MNO	Mobile Network Operator
OTA	Over The Air
SOAP	Simple Object Access Protocol
SSO	Single Sign On
TM	Trusted Module
TMUICC	Trusted Module implemented on a UICC
URI	Uniform Resource Identifier
WSC	Web Service Consumer
WSP	Web Service Provider
XML	eXtended Markup Language

4 Overview

A TM is a removable, personalized module containing files and executables that provides a secure storage and execution environment for certain operations required by an IdP and a IdUA in identity services. Functions include storage of personal data and credentials, IdUA provisioning, authentication, secure messaging and application-layer security such as digital signature.

The UICC requirements for identity files and procedures are designed to fully support the requirements of the Liberty Alliance and OMA. For clarity the relevant Liberty Alliance and OMA requirements are provided for information.

4.1 Basic functionality of a TM

Basic functionality of the interfaces between identity services and the TMUICC are to:

- Create and remotely manage Identity provisioning and credential storage files on a TMUICC.
- Use the TMUICC to provide identification, multiple levels of authentication and authorization i.e. signing (some schemes require the TM to sign authorization tokens for proof-of-presence of the user).
- Achieve end-to-end secure messaging between authorized entities (the IdP and the IdUA) and files and applications on the TMUICC in non-secure client environments and across insecure networks.

TMs shall be able to be deployed in environments where messages originating or terminating at the TMUICC can be subject to replay, eavesdropping or manipulation attacks that may not be feasible within a mobile phone or across mobile networks. Typical scenarios include deployment in a PC or in a PC peripheral device, as well as certain types of smart phone equipped with IdUA and an operating system with an open API.

Figure 1 shows some of the entities involved in a typical identity service. Only the IdP and the IdUA are allowed to directly interface to the TM. WSPs can interface to applications in the client environment and to the IdUA.

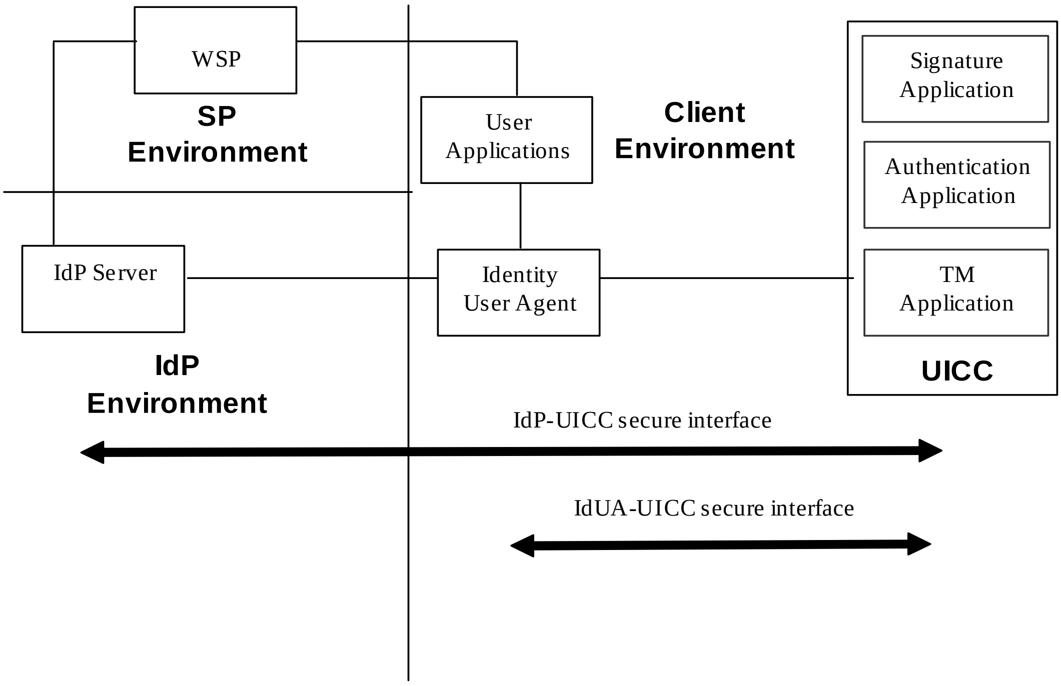

Figure 1: Standardized Interfaces Required to the TMUICC

5 Requirements

5.1 Description of Requirements

5.1.1 Deployment Contexts for TMUICC

The Card accepting device shall assume that the TMUICC will support all context(s) defined in this clause.

The simultaneous use of the TMUICC in different contexts at the same time is FFS.

(A single set of protocols and functions on the TMUICC that will meet the requirements of all deployment contexts implies a TMUICC-related protocol stack and command set that is common to all deployment contexts).

The figures and table below categorize and characterize the deployment contexts.

Context 1: TMUICC in a CAD connected to a PC

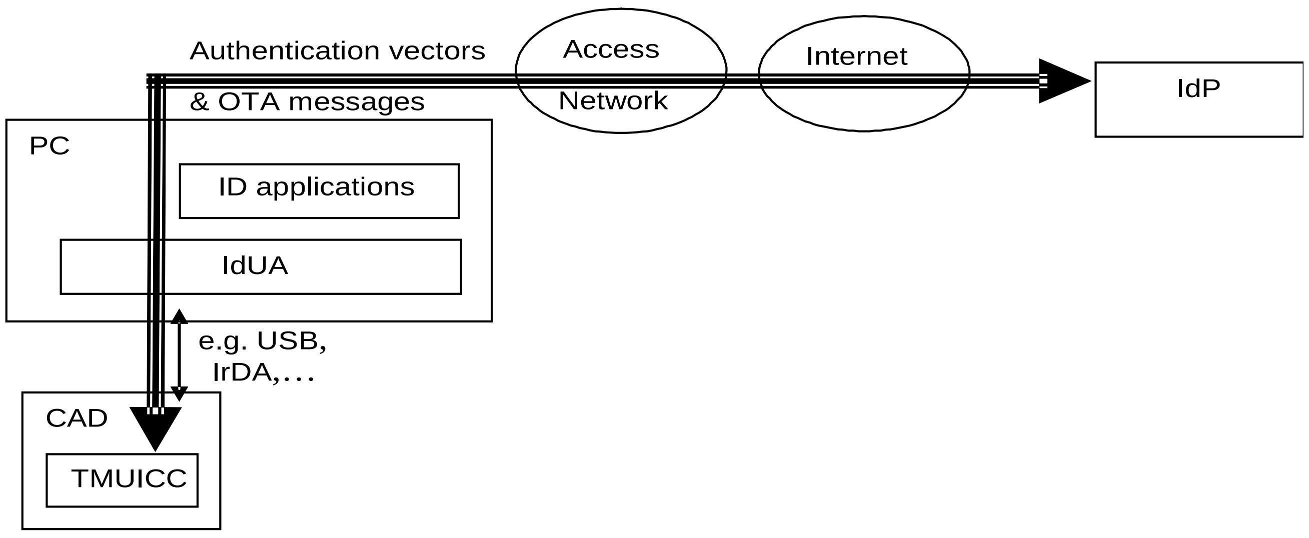

Figure 2: TMUICC in a CAD connected to a PC

Context 2: TMUICC in an non-ID-enabled Mobile Phone used as a PC Peripheral with a Local Interface

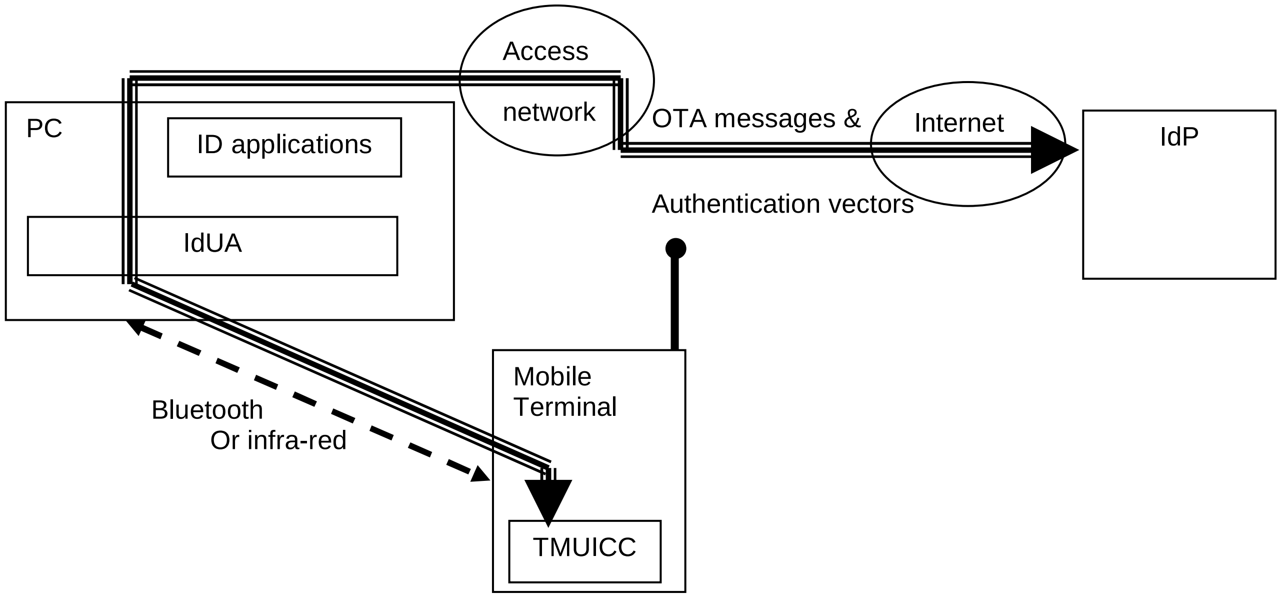

Figure 3: TMUICC in an nod-ID-enabled Mobile Phone used as a PC Peripheral with a Local Interface

Context 3: TMUICC in an ID-enabled mobile phone

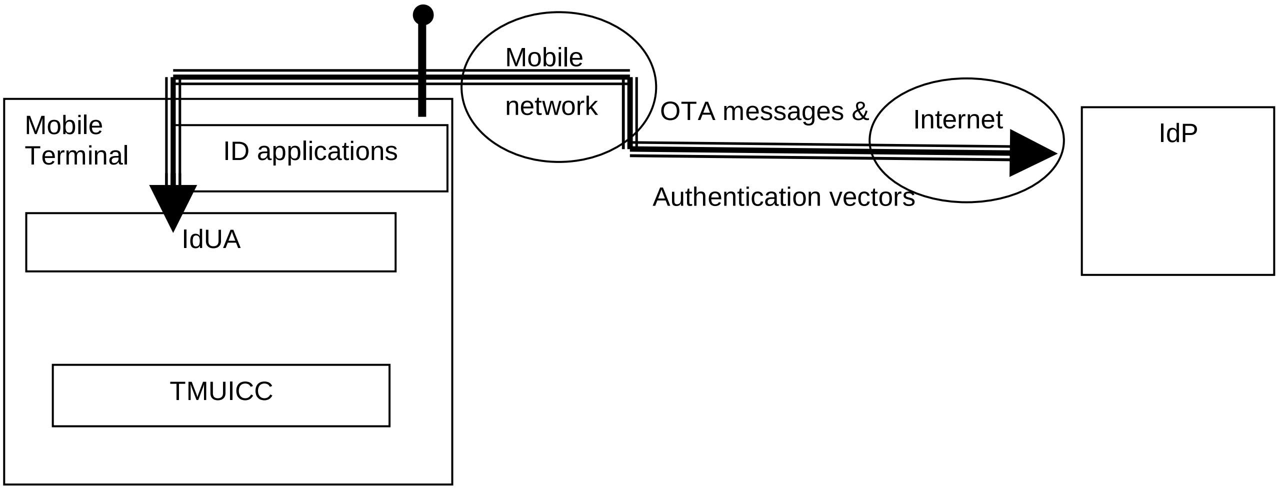

Figure 4: TMUICC in an ID-enabled mobile phone

Context 4: TMUICC not connected to the devices which has the IdUA

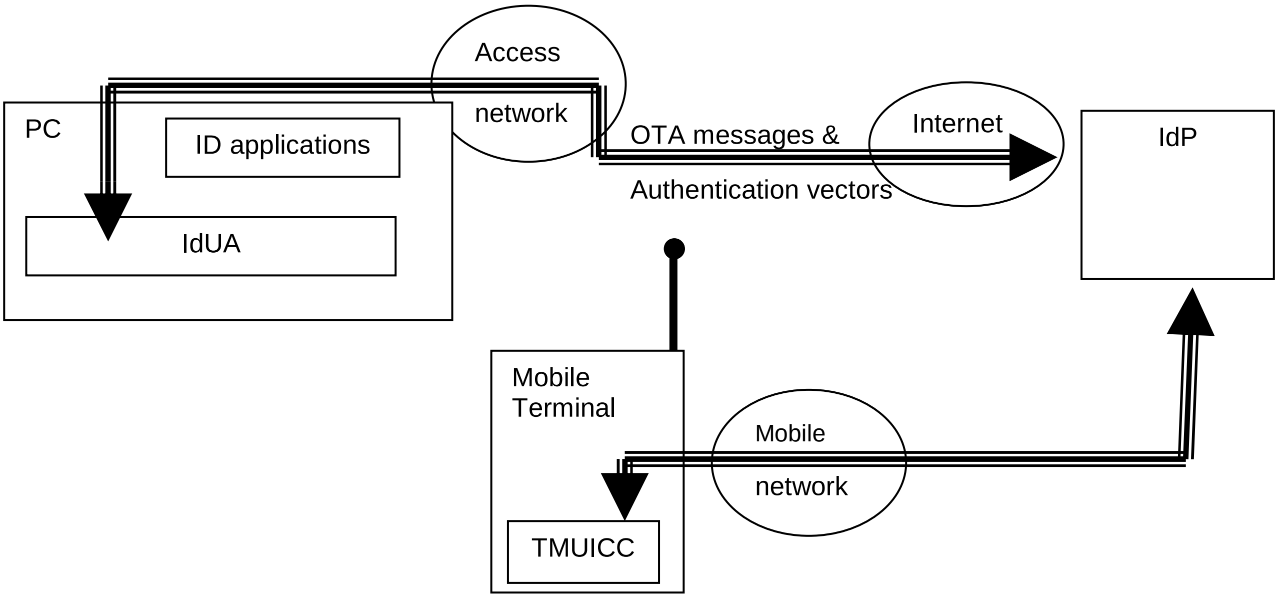

Figure 5: TMUICC not connected to the devices which has the IdUA

Different deployment contexts have different characteristics. Those characteristics that have the greatest bearing on the requirements of the TMUICC are shown in table 1.

Table 1: Characteristics of Deployment Contexts

	CONTEXTS			
CHARACTERISTICS	**1**	**2**	**3**	**4**
IdUA & TMUICC are co-located	no	no	yes	no
IdUA & TMUICC are in different devices	yes	yes	no	yes
Authentication vectors for TMUICC are sent end-end via MNO's "secure"mobile network	no	no	yes See note 4	yes
Authentication vectors for TMUICC are sent via open "insecure" network	yes	yes See note 2	no	no
IdP - TMUICC communication can be end-end via MNO's "secure" mobile network	no	no	yes See note 4	yes See note 4
IdP - TMUICC communication must be via open ("insecure") network	yes	yes See note 2	no	no
PIN entries can be electronically eavesdropped	yes See note 1	no See note 3	no	no
NOTE 1: PIN entries can be eavesdropped if the PC keyboard is used. A PIN pad on the CAD could prevent eavesdropping. NOTE 2: Although authentication of the TMUICC for mobile network access is achieved across the mobile network, authentication for identity services has to be bound to the specific PC being used. That would normally require the authentication vectors to be sent to the TMUICC via the PC and the open network to which it is connected. NOTE 3: This assumes that PIN entries will be via the mobile phone keypad and not the PC keyboard. NOTE 4: Smart phones may have internal environments where viruses and eavesdropping programmes can operate. This could enable sniffing keypad activity and of authentication vectors and manipulation of data across the "UICC/ME" interface.				

5.2 Secure Communications with the TMUICC

5.2.1 Basic Requirements

For Basic Requirements, the IdP and IdUA are required to communicate directly with the TMUICC for the following purposes:

- Secure storage, retrieval and management of client provisioning data;
- communication of an opaque identifier from the TMUICC to the IdP, to bootstrap the communications and authentication processes;
- secure distribution of dynamic session keys derived from shared secrets;
- secure processing of requests and responses for authentication assertions and for authorization assertions. These messages may need to be signed and verified by the TMUICC or IdP;
- secure transfer of application commands and responses, e.g. to invoke a challenge/response authentication application or a PIN verification application on the TMUICC;
- sending and receiving of authentication vectors inside the secure channels;
- requesting, sending and receiving of authentication assertions and authorization assertions. Some services require the assertions to be signed by the IdUA (i.e. the TM) before being passed to a WSP - the signatures being verified by either the IdP or WSP. These are:

1) Authentication.

2) Message integrity.

3) Replay detection and sequence integrity.

4) Proof of receipt and execution.

5) Message confidentiality.

6) Security management.

7) Exceptional procedures.

The TMUICC will also provide:

8) Signing of authorization assertions using symmetric techniques.

9) Secure storage and management functions for provisioned keys.

10) Secure generation, storage and deletion of temporary symmetric keys.

11) A secure environment for the execution of cryptographic algorithms, preventing unauthorized monitoring of or interference with such operations.

Annex A (informative):
Liberty Alliance requirements

Liberty Alliance requirements for identity services will create corresponding requirements on the TMUICC that will be taken into account for standardization in ETSI SCP:

- IdUA obtains and securely stores pre-issued assertions from the IdP and uses them to access services e.g. when the IdP is not accessible. This includes keeping records of assertions that have been issued and/or stored and reporting back to the IdP.
- IdUA acts as an attribute provider, i.e.:
    - Obtains (e.g. personal) attributes, validates them and stores them securely.
    - Allows controlled access to attributes by validating service authorization assertions from identity-consuming entities.
- IdUA acts as a Discovery Service by permitting discovery of its AP services, requiring validation of authorization assertions from WSCs.
- Pro-active SSO: Enables efficient SSO when the IdUA has behavioural knowledge that an WSP will require authentication in the near future.
- IdUA announces its authentication capabilities.
- Filter for dynamic data collection: users experience different environments and constraints that impact their willingness to allow others to access their information (voluntarily or not, i.e. Kids, Gamblers, Job interviews, Adult entertainment, etc.).
- ID services with zero-install client. This corresponds to deployment contexts where the IdUA and the TM are in different terminals.
- TM-driven dynamic session management and transfer: by binding the SSO sessions with the TM rather than the IdUA as a whole, this use case would allow to:
    - Automatically perform Single Log Off whenever the TM is disconnected or out or reach from the rest of the IdUA.
    - Transfer an existing session to another IdUA terminal whenever the user connects and/or acknowledges the new connection with the TM.

Annex B (informative): Change history

The table below indicates changes that have been incorporated into the present document since it was created by TC SCP.

Meeting	Plenary Tdoc	WG tdoc	VERS	CR	REV	CAT	SUBJECT	Resulting Version

Annex C (informative): Bibliography

Liberty ID-FF Implementation Guidelines, liberty-idff-guidelines version 1.2 www.projectliberty.org.

Liberty ID-FF Authentication Specification, liberty-authentication-context v1.2 www.projectliberty.org.

History

Document history		
V7.0.0	September 2005	Publication