

Open Smart Card Infrastructure for Europe

V2



Volume 9: Referenced Standards

Part: eURI Summary

NOTICE

This eESC Common Specification document supersedes all previous versions. Neither eEurope Smart Cards nor any of its participants accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this document. Latest version of OSCIE and any additions are available via www.eeurope-smartcards.org and www.eurosmart.com. For more information contact info@eeurope-smartcards.org.

Contents

Page

1	The eURI CEN/ISSS Workshop.....	1
1.1	Aim and Scope of the Workshop	1
1.2	Mandatory and Optional Data Fields	1
1.3	Implementation Method	2
1.4	Using the eURI to build interoperable networks	2
1.4.1	The case for interoperable networks	2
1.4.2	Actors.....	2
1.4.3	Card Communities	3
1.4.4	Levels of deployment	3
1.5	Relationship with existing standards	5
1.6	Privacy and data transparency.....	5
1.7	Title and Parts of the eURI CWA	5
1.8	Summary of content of the eURI CWA	6
1.9	Current Progress	6

1 The eURI CEN/ISSS Workshop

1.1 Aim and Scope of the Workshop

The URI specification was initially developed as CEN Workshop Agreement CWA 13987 : 2000.

URI stands for User Related Information, in this case stored on a smart card. The original URI project took as the scope of the data:

- a) such information as the user might otherwise be expected to type in at the terminal when using ICT services – typically this includes name, address, date of birth, name and/or address of the service that the user wishes to select (but *not* credit/debit card information)
- b) configuration information for the terminal, to be used by the terminal to adapt its user interface for users with special needs, such as requirements for large print on the display or for a longer period before the terminal times out when the user is requested to respond to a prompt
- c) optional additional information to be defined by the card scheme or by more than one card scheme acting in partnership

The terminal should read at least the configuration information as soon as the card is initialised, and immediately act on it.

Implementation of the URI, defined as an interface specification between card and terminal ('card edge'), was not part of the earlier CWA, and the Extended URI Workshop is developing the interface specification for contact cards conforming to ISO/IEC 7816 or for contactless cards conforming to ISO/IEC 14443 part 4, for use in a multi-application environment. The full title of the extended URI CWA (known as eURI, pronounced 'e U R I') is 'User Related Information Extended to Multi-application Smart Cards'. The CWA includes the card edge specification for the dataset, an access method, security methodology, and implementation information and guidelines.

The security level required for the URI is low, as release of the information is always controlled by the card holder (user). Thus the URI dataset should only be used to hold information which can be viewed by the user in a form which is readily understood.

The CWA consists of three Parts:

- CWA 13987-1 Smart Card Systems: Interoperable Citizen Services: User Related Information: Definition of User Related Information and Implementation
- CWA 13987-2 Smart Card Systems: Interoperable Citizen Services: User Related Information: Implementation Guidelines
- CWA 13987-3 Smart Card Systems: Interoperable Citizen Services: User Related Information: Guidelines to Creating, Operating and Maintaining an Interoperable Network

The specifications given in Part 1 are prescriptive, whereas Parts 2 and 3 are informative.

Publication of the new CWA is planned for early 2003.

1.2 Mandatory and Optional Data Fields

The eURI definition contained in Part 1 of the CWA 13987 specification includes both mandatory and optional items. The mandatory *data* is the minimum set that is required properly to support required eURI functionality. However, many implementations produced by eURI Issuers, with Card Holder approval where necessary, will include optional data. Such optional data will extend the usefulness of the eURI in providing inclusive operation and in making available a wider range of candidate interoperable applications at the terminal.

1.3 Implementation Method

The proposed implementation is as an application or applet in the smart card, with an Application Identifier (AID) as defined in ISO/IEC 7816, and selected by means of a 'SELECT' APDU using the AID as parameter. There will be one universal eURI AID, registered with ISO.

Data elements are encoded into data objects using TLV format (Tag, Length, Value), and the resulting data objects are combined into BER-TLV constructed data objects using tags and formats compliant with ISO/IEC 7816.

Where possible, the eURI uses existing standards to define the data elements, particularly EN 1332-4 for the special needs parameters used to configure terminals.

In addition:

- a) a format is proposed for transfer of data elements from the eURI across a network, using 7816-compliant methods for carrying identification of the source of the data element definition along with the data itself;
- b) the dataset specified in CWA 13987 : 2000 is being updated; and
- c) support for legacy datasets (CWA 13987 : 2000 and DISTINCT ID) continues until at least 2005.

1.4 Using the eURI to build interoperable networks

1.4.1 The case for interoperable networks

Smart card interoperability is a key requirement of the developing Information Society, especially as citizen mobility around Europe increases. This requirement is strongly supported by two factors:

- a) The growing use of smart cards as enabling tokens for products and services emanating from the Information Society, i.e. products and services based on Information and Communications Technologies (ICT)
- b) The usefulness of smart cards in the creation of an inclusive society by informing ICT applications and services of the requirements profile of the Card Holder.

An organisation wishing to deliver services by means of a smart card system may choose to invest in the issuing of its own smart cards and in the installation of its own equipment and provider network, or it may choose to share resources with other organisations. The effective and efficient sharing of resources among different organisations for service provision to the end user is what is intended in the eURI CWA by the term interoperability. The resources shared in an interoperable network using smart cards may include:

- a) the cards
- b) terminals supporting card readers
- c) data networks and network nodes used by Service Providers
- d) a Service Provider's customer base
- e) data and information.

The collective use of these resources for improving service delivery requires collaboration between Service Providers, Card Issuers, Card Acceptors and often also administrations or other regulatory bodies. Collaboration of this kind may be sought because the services offered by different providers are complementary or, indeed, they may be in direct competition. In any case, the benefits of participating in an interoperable network of this kind are considerable.

1.4.2 Actors

Deployment of the eURI is expected to benefit the various actors in the ICT service delivery value chain. The main actors identified in Part 3 of the CWA are:

- a) Card Holder
- b) Service Provider (both on and off card, including Application Loaders)
- c) Card Acceptor
- d) Card Issuer
- e) Certification and Registration Authorities
- f) Card Community Managers
- g) Regulatory Bodies

1.4.3 Card Communities

CWA 13987 provides specifications and guidelines that can enable the establishment of an interoperable network of actors. These organisations may form Card Communities¹ (CCs) in order to manage the eURI, provide authority for loading it onto a smart card, and controlling its format and contents.

The nature of a Card Community and its role are discussed in the informative parts (Parts 2 and 3) of the CWA specification. It is recognised that several Card Communities may exist side by side covering different geographical or other jurisdictional areas. It is also noted that Card Communities may co-operate with one another to widen yet further the scope of service interoperability.

1.4.4 Levels of deployment

The full benefits of eURI deployment will be achieved through the delivery of ICT services within an interoperable environment of ICT actors. The eURI specification is a key enabler for the establishment of this environment. However, it is recognised:

- a) that eURI implementations may be deployed at different levels, depending on the agreements made between members of the interoperable network and the technical restrictions of system terminals and
- b) that Card Community schemes other than those described in Part 3 of the CWA (an informative part) may be set up and that these Card Communities could nonetheless implement and make use of the eURI.

CWA 13987 provides guidelines for deployment up to the maximum level of interoperability, i.e. for service delivery involving on-line connection with a remote application. In practice, the following limitations to deployment at this level may apply:

- a) a Card Acceptor may choose to implement the eURI with restricted functionality, i.e. without providing access to on-line services
- b) the system terminal accepting the smart card may be restricted in its ability to adapt the human machine interface
- c) the system terminal accepting the smart card may not allow an on-line connection to a remote application
- d) the system terminal accepting the smart card may only be capable of offering a single service.

Where these restrictions apply, it is clear that many of the benefits of eURI, and the interoperable environment it supports, cannot be achieved. However, it is likely that some organisations may opt for phased deployment of the eURI, starting with a system offering restricted functionality and then gradually introducing additional on-line services at its terminals. Such organisations (who are likely to be both Card Issuers and Card Acceptors) are encouraged to use the CWA 13987 Part 1 specification, even though their current terminals offer restricted

¹ The eURI definition of a Card Community is 'a grouping of organisations established to oversee the operation of an interoperable network'; any number of Card Issuers may operate within a single Card Community.

functionality. Such organisations are also encouraged to form Card Communities (CCs) (or join existing CCs), making use of the guidelines set out in the CWA, if they wish.

The eURI can be implemented in Card Communities with different types of architecture. As an illustration of this, we could consider the proposed implementation of the eURI in a Card Community set up to meet the MAS Requirements proposed by NTT for EESCC TB7/WG4.

The following diagram illustrates how this implementation could be achieved.

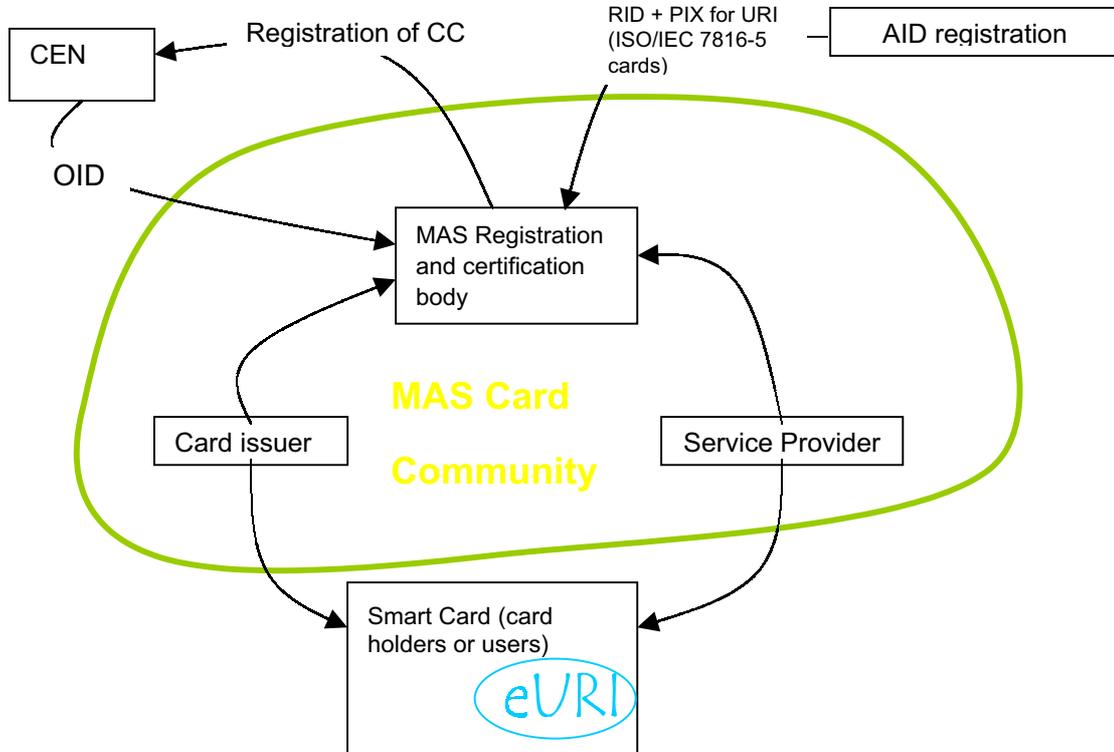


Figure 1 - Example of registration of the eURI as an application of a MAS Card Community

Once additional data elements not defined in the CWA are added to the eURI on the smart card, for interoperability the service provider or providers responsible for the definition of the additional data elements must be identifiable when accessing the smart card. For this purpose, compliance with the CWA requires those service providers, who together define and use an additional set of data elements, to form a Card Community (CC), register that CC with CEN, and obtain from CEN, and use on the smart card, a unique identifier for the CC. This identifier is formatted as an Object Identifier (OID) as defined in ISO/IEC 7816-6:1996 and ISO 8825-1.

At a lower level of deployment, the following parts of the eURI may be included on a smart card, and used, without the involvement of a Card Community:

- a) the mandatory component of the eURI, known as the Universal Card Holder Information (or UCI)
- b) the elements of the Personal Profile defined in the CWA
- c) management information (including pointers) supporting the above items

The UCI provides for the smart card to hold personal preference information, such as language preference and other terminal configuration preferences (e.g. large print).

At the lowest level of deployment, a Service Provider (who may well also be the Card Issuer) may load an eURI application and the UCI data structure without having any responsibility for the data held in the UCI. At a suitably configured terminal, the Card Holder may then load and manage personal preference information.

The following diagram illustrates how the UCI data set is structured and how the data objects are identified with specific tag values.

eURI Summary

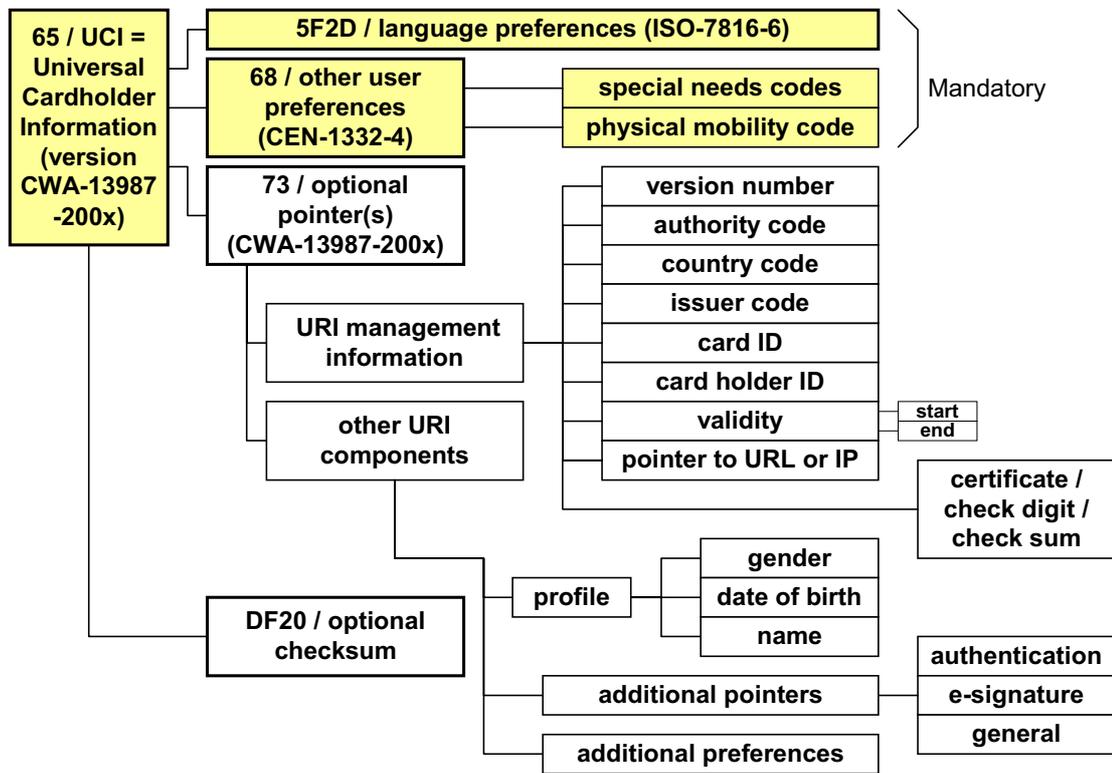


Figure 2 – Proposed structure of eURI data

1.5 Relationship with existing standards

The eURI CWA makes use of existing standards where appropriate and in particular conforms to ISO/IEC 7816 and to EN 1332-4:1999, *Identification card systems – Man-Machine Interface – Part 4: Coding of user requirements for people with special needs*. References to standards such as EN1332-4 which define coding of eURI data elements and objects indicate that those standards have priority over the CWA.

EN 1332-4 is of particular interest to citizens with special requirements and it also provides support for EU directives concerning Special Needs and Design For All which have been enacted by member countries. However, while EN 1332-4 specifies the data structures necessary to support the directive, it does not specify how this data may be used and accessed.

The eURI CWA provides a method to identify the presence of and method of access to a specific data set on the citizen's smart card, including EN 1332-4 data structures where appropriate. In addition, the eURI provides a single, common data set for all uses of the smart card and all ICT services where access is provided by the smart card. The solution proposed will permit the Card Holder to perceive a common interface to ICT services tailored specifically to their wishes and requirements.

Moreover, the eURI CWA also supports and conforms to EN 1332-1:1999, *Identification card systems – Man-Machine Interface – Part 1: Design principles for the user interface*.

1.6 Privacy and data transparency

The eURI CWA takes account of the requirements of EN1332-4 and ANEC98/ICT/007 with regard to the privacy of personal information, data security and data transparency. It also permits Card Communities to comply with applicable data protection legislation.

1.7 Title and Parts of the eURI CWA

The eURI CWA consists of three Parts:

- CWA 13987-1 Smart Card Systems: Interoperable Citizen Services: User Related Information: Definition of User Related Information and Implementation

- CWA 13987-2 Smart Card Systems: Interoperable Citizen Services: User Related Information: Implementation Guidelines
- CWA 13987-3 Smart Card Systems: Interoperable Citizen Services: User Related Information: Guidelines to Creating, Operating and Maintaining an Interoperable Network

The specifications given in Part 1 are prescriptive, whereas Parts 2 and 3 are informative.

Publication of the new CWA is planned for early 2003.

1.8 Summary of content of the eURI CWA

The new CWA 13987:200x specification includes:

- a) a normative definition of the eURI data set (Part 1);
- b) a card edge specification for access to the eURI (Part 1);
- c) supporting requirements, including logical message formatting for requesting and exchanging data elements (Part 1);
- d) informative guidelines on how the eURI may be implemented and deployed within an interoperable environment (Part 2); and
- e) an indication of the supporting organisational infrastructure necessary to maintain the ongoing operation of such an environment (Part 3).

The three parts of the CWA are mutually supportive. Hence, although Part 1 provides details of the fundamental requirements for implementing the open scheme, the reader will not gain a true understanding of the eURI's role as a mechanism for interoperability without reading the other two parts as well.

1.9 Current Progress

Full drafts of Part 1 (Normative) and Part 3 (Informative) of the new CWA have been produced, and are available, along with other documents, at the Workshop web site http://www.uninfo.polito.it/WS_URI/default.htm.

A full draft of Part 2 (Informative) is currently in preparation.