

CEN

CWA 15535-1

WORKSHOP

April 2006

AGREEMENT

ICS 35.240.15

English version

Multi-application multi-issuer citizen card scheme standardisation - Part 1: Business model agreement

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

© 2006 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No.:CWA 15535-1:2006 E

Table of Contents

<i>Foreword</i>	4
1 Introduction	5
1.1 Scope and Objectives of the Document	5
1.1.1 Drivers	5
1.1.2 Scope	5
1.1.3 Enhanced Objectives	5
1.2 Informative References	6
1.2.1 SmartCities Deliverables Numbers:	6
1.2.2 English National Smart Card Project	6
1.2.3 EC Level	7
1.2.4 Others	7
1.3 Concepts, Definitions and Abbreviations	7
2 The Business of Deploying Cards and Services	13
2.1 The Classical Approach for Card Businesses: One Card Issuer and One Set of Services	13
2.1.1 Description	13
2.1.2 Limitations	13
2.2 The Multi-Application Approach	14
2.3 The Multi-Application, Multi-Partner Approach	14
2.4 The MMUSST Approach	14
2.5 eID like Approach	15
2.5.1 A Short Explanation of eID	16
2.5.2 Different Examples of National eID Cards	17
2.6 The MMUSST Approach and eID	18
2.7 Key business issues for the MMUSST approach	19
2.7.1 Business Issues to be addressed	21
3 Multi- Service/Multi-Issuer Schemes	22
3.1 Card scheme with Cards and Services communities	22
3.1.1 Card Community	22
3.1.2 Service Community	23
3.2 MMUSST Role Model	23
3.3 Potential Revenue Flows	27
4 MMUSST Business Cases	28
4.1 MMUSST Drivers	28
4.2 Typology of eServices	29
4.3 Methodology for Identifying Business Cases	31
4.3.1 Strategy for Card Scheme Deployment	31
4.3.2 Value Chain in a Card Scheme	33
4.3.3 Using the Value Chain method	34
5 Card Scheme Implementation Guidelines	35
5.1 Integration Methodology	35
5.2 Risk Assessment	36

5.2.1	Technology Risks	36
5.2.2	Financial and Commercial Risks	36
5.2.3	Legal Risks	36
5.3	Legal Framework	37
5.3.1	Specific Legal Characteristics of Multi-Application Cards	37
5.3.2	Data Protection and Privacy	37
5.3.3	Data Protection and Privacy - Practice	38
5.4	Privacy Code of Conduct	40
5.5	Cost Management and Transparency	41
5.5.1	Business Model versus Evaluation	43
5.5.2	Application Assumption	43
5.5.3	Model Driver Assumptions	43
5.5.4	Business Model Financial Inputs	44

Table of Figures

Figure 1 - The generic trust model	16
Figure 2 - Implementation of the trust model with e-ID cards	16
Figure 3 - Stakeholder Benefits	20
Figure 4 - Card and Service Community relationship	23
Figure 5 - MMUSST Role Model	24
Figure 6 - Potential Revenue Flows – Illustrative Example	27
Figure 7 - Deployment strategy for a card scheme	32
Figure 8 - Value Chain in a card scheme	33

Foreword

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which was supported by CEN following the public call for participation made in 2005.

A list of the individuals and organizations that supported the technical consensus represented by the CEN Workshop Agreement is available to purchasers from the CEN Management Centre.

The formal process followed by the Workshop in the development of the CEN Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of the CEN Workshop Agreement or possible conflict with standards or legislation. This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its members.

The final review/endorsement round for this CWA was started on 2005-12-20 and was successfully closed on 2006-03-13. The final text of this CWA was submitted to CEN for publication on 2006-04-05.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN: AENOR, AFNOR, ASRO, BSI, CSNI, CYS, DIN, DS, ELOT, EVS, IBN, IPQ, IST, LVS, LST, MSA, MSZT, NEN, NSAI, ON, PKN, SEE, SIS, SIST, SFS, SN, SNV, SUTN and UNI.

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN Management Centre.

1 Introduction

From its origins in the SmartCities project, MMUSST set out to deliver an overview of the methods and components for Multi-application Multi-issuer citizen card Scheme Standardisation. While this continues to be the case, initial work has identified the increasing importance of the single scheme, multiple service provider model, alongside the “multi-issuer” concept.

1.1 Scope and Objectives of the Document

1.1.1 Drivers

The principal “driver” for the MMUSST workshop is the SmartCities Interest Group, with members from across the European Union (city/regional councils) who share the belief and objective that multi-application, multi-issuer smart card schemes have a sustainable future in providing citizen access to electronic services.

Since the completion of the SmartCities Project a number of developments have taken place in the areas of eID, integrated transport and ePayment solutions. These provide even greater drivers for the development of multi-application, multi-issuer schemes.

1.1.2 Scope

Indeed, such developments present new opportunities that broaden the SmartCities concept so that it might better be described as:

“a multi-application, multi service provider card scheme with the possibility of multiple partners issuing cards”

1.1.3 Enhanced Objectives

Thus, the objective of MMUSST is to create an agreement whereby a card scheme operator can define minimum interoperability specifications for inviting service providers to offer services to one or several cards within a scheme, with these cards being issued by local, regional or national authorities or even by private organisations such as transport companies.

In this context, MMUSST addresses specific requirements:

- Potential card issuers are to be convinced that there will be service providers willing to offer eServices to their card holders (typical card issuers of citizen service cards are “Local Authorities/Town Hall”)
- Potential eService providers (both providers of core services for local functions and others within and beyond the public sector) are to be convinced that offering their services as eServices through different cards from different card issuers will provide an efficient and secure channel and an effective business proposition
- Typical eService providers are offering or developing:
 - On-card applications for eMoney & eTicketing
 - On-line access to eServices (including eServices requiring eAuthentication functions up to strong assurance) at local, regional and national level, and in the medium term possibly at pan-European level

CWA 15535-1:2006 (E)

- Suppliers of equipment, software and enabling services are to be convinced that there is a market in such schemes in order to invest and be competitive.

The intended audience includes development projects, implementers and suppliers, and CWA 1 seeks to build agreement on the scheme concept and on the implementation solution of a dynamic, interoperable, multi-application, multi-service provider, multi-issuer card scheme based on existing open standards.

CWA1 investigates local, regional and national functions in terms of scheme governance and management. The document includes examples and models from SmartCities and projects.

The aim of MMUSST is not to produce a prescription for locality based multi-application, multi-service provider, multi-issuer smart card schemes, but to provide a framework, based around existing standards, to help scheme designers develop a workable and sustainable solution.

1.2 Informative References

The principal source documentation for CWA1 is the outputs of the SmartCities project (IST Project Number 12252). It also utilises deliverable outputs from the English National Smart Card Project, which itself adopted the “SmartCities concept” of building local authority based multi-application smart card schemes encompassing multi-partner, multi-issuer involvement. It also draws heavily on material produced for and within eURI, eAuthentication and eEpoch

1.2.1 SmartCities Deliverables Numbers:

D1.6: Public Final Report
D11-1: SmartCities Sustainable business models and marketing study report
D12.4: Third SmartCities Interest Group Report
D12.6: Final Dissemination Report
D12.7: Report on Legal Aspects of Data exchange: Global Unique Identifiers and the Cross-Profiling of personal data
SIG: SmartCities Guidance Notes

1.2.2 English National Smart Card Project

WP2-01	Business Case including social political and commercial considerations
WP2-03	Sustainable Financial models
WP2-04	Financial Report Implementation/Set-up costs
WP2-05	Sustainable Business Models Final Report
WP3-01	Considerations for multi-application, multi-sector smartcard environments
WP3-02	Interoperability within the local authority sector
WP3-03	Applicable Standards
WP3-05	A standards sustainability report (for standards maintenance)
WP3-09	Trends in Smart Cards & Smart Card Technology
WP3-10	WP3-10 - Smart Card Technology Routemap
WP6-01	Report on Commercial Applications
WP7-01a	Definition and testing of clearing systems for transport and non transport transactions within a defined cross boundary environment
WP7-01b	Strategic LA smart card Architecture

WP7-02	Defining and testing the integration of token transfer between LA and non LA agencies.
WP7-03	E purse positioning paper
WP7-04	Existing e-Purse Scheme Analysis
WP7-05	Cross Regional e-Payments Requirements
WP7-06	Solutions Architecture Document
WP7-07	Clearing and Settlement Methodology
WP7-08	Local Authority Representation Framework
WP7-09	Authentication Policy Papers
WP7-10	Legal Agreement supporting bridging between certification authorities
WP7-11	Analysis of the potential for federating identities between schemes and role of third parties.
WP8-01	Financial Services Act
WP8-02	Card Governance Report
WP8-03	Security Issues
WP8-04	Information Law Report
WP8-07	Corporate Structures Report
WP8-08	Risk register
WP8-09	Commercial Conditions Checklist
WP8-13	Legal / Data Privacy - Introductory Report
WP9-01	Cardholder Database and Life Cycle Management System
WP9-02	Market Research Report

1.2.3 EC Level

CWA 13987:2003 (3 parts) (eURI)

CWA 15264:2004 (Part 1 & 2) (eAuth)

CEN TC224 WG15 : European Citizen Card

van Arkel J. "Towards an electronic ID for the European Citizen, a strategic vision"
Brussels, December 31, 2004

1.2.4 Others

The Next generation Ic Card System Study (NICCS) group

1.3 Concepts, Definitions and Abbreviations

The following Glossary of Terms uses Glossary and Abbreviations V0.07, delivered to CEN and the Work Shop in August 2005, with the terms followed by "*" having been updated.

Term	Acronym	Definition
Access Provider		<p>A Role that is responsible for managing infrastructure (e.g. card readers, terminals and necessary drivers, communication network and servers) used by card holders accessing the offered services.</p> <p>There may be more than one Access Provider within a Smart Card Scheme. Also other infrastructure, not controlled by the Card Scheme Operator, will be used by Card Holders.</p>

Term	Acronym	Definition
Actor		A User playing a coherent set of roles when interacting with the system within a particular Use Case An Actor may for instance be a human, an organisation or another (sub)system.
Applet		Java representation of software application. In a smart card normally uses the JavaCard variant.
Application Provider*	AP	An Entity that owns or is responsible for an on-card application offered by a Service Provider. The AP may also operate the Application Loader Role.
Authentication		The provision of assurance of the claimed identity of an entity or component ¹ . It may provide different level of assurance (from weak to strong) and may also be combined with authorisation to access or use a service or to participate in the provision of a service
Authorisation		The process by which entitlement of a requester to access or use a given service is determined.
Card Community Administrator		The general administrative Role operated by the Card Scheme Operator
Card Community Registrar		The Role for formal registration of other Role players and necessary information within the Smart Card Scheme
Card Holder		A physical person (in the legal sense, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer, and who may use the smart card for access to compliant applications
Card Issuer*	CI	An Entity that issues smart cards and other smart media to Card Holders, or to other organisations for further distribution, manages card level security information, and manages (possibly using agents) the population of cards
Card Scheme		(See Smart Card Scheme)
Card Scheme Operator	CSO	An Entity that operationally manages a Smart Card Scheme
Card Supplier		The person or organisation that manufactures smart cards and other smart media, or acts as agent or reseller of the same, providing Card Issuers with those smart cards and smart media
Certificate		In the context of a security scheme using public key cryptography: the public key of a user, together with some other information rendered unforgeable by encipherment with the private key of the issuing certification authority.

¹ May use a secure token (e.g. held in a smart card) and a method to securely link the real person to the secure token.

Term	Acronym	Definition
Certification Authority	CA	A trusted entity that creates and assigns certificates. Optionally the certification authority may create the user's keys.
Certification Service Provider	CSP	An entity that provides electronic certificates and related services
Digital signature		Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit, and protects against forgery (including forgery by the recipient). Digital signature is a special case of the more general concept of electronic signature.
Domain		Scope of action. (See Security Domain)
Electronic Identity (of a person)²		Identity data (of a person) usable in an electronic environment.
Electronic signature		Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that other data. Digital signature is a special case of the more general concept of electronic signature.
Entity		An abstract object performing one or more Roles within the set of linked Card Schemes. An entity can exist as an object in the real world (e.g. a service operator, a natural person), and then it is called a "legal entity". It can also be a model of this real world object (<i>abstract entity</i>).
eService		Service accessible to a card holder through an ICT system. Service delivery may be possible with or without the use of a smart card, although the scope of MMUSST concentrates on the use of the smart card in service delivery.
eService Community		All natural persons authorised to access and use a specific eService. Each eService community comprises those card holders whose on-card functions and data (including security data) are recognised by a given eService. eService Communities can be contained within, or span one or more Smart Card Communities.
eService Provider*		A role operated by a Service Provider: responsible for eServices and may also offer On-card Applications
Identification		The process of obtaining information about whom the requester claims to be without considering the "trustability" of this information.

² Other 'identity' definitions are in the Attribute class in this draft Glossary. This will be clarified in the final glossary.

Term	Acronym	Definition
Identification card		Card identifying its holder and issuer, which may carry data required as input for the intended use of the card and for transactions based thereon.
Identification, Authentication and electronic Signature	IAS	Within the scope of this CWA and documents referenced in this CWA, a related set of secure functions ³
Identity (of a person)		The common sense notion of personal identity. A person's name, personality, physical body and history, including such personal attributes as address etc, of an individual person ⁴ .
Interface		A standardised technical definition of the connection between two components
Interoperability		The ability of several independent systems or sub-system components to work together. In the context of this CWA, the ability of several systems or sub-system components to enable a cardholder to access eServices from different service providers and through different infrastructures.
Legal Identity (of a person)		Identity awarded by the relevant administration in a country. Since the legal names of persons (family names and given name(s)) are not necessarily unique, the identity of a person must include sufficient additional information (for example a unique identifier) to make the combination unique.
Multi-Application Card		A smart card that, with permission from the Card Issuer, may simultaneously host more than one application, each of which may be selected and used independently.
Personal data		any information relating to an identified or identifiable natural person ('data subject')
Personal Identification Number	PIN	A numeric security code used as a mechanism for local one-to-one verification with the purpose to ascertain whether the card holder is in fact the natural person authorised to access or use a specific service such as the right to unlock certain information on the card.
Personalisation		A set of processes for transforming a card that is in the card stock into a card that refers to a cardholder.
Platform		A specific hardware configuration, its supporting system software and device drivers.
Post-Issuance Load/Install		The process of downloading applications and/or data to the card after the card has been issued to the card holder.

³ See IAS Services

⁴ The separate concepts of Identity, Legal identity and Electronic Identity to be clarified

Term	Acronym	Definition
Registration (of a person)		Obtaining sufficient proof of the identity of the intended card holder by traditional means, possibly including attributes (e.g. as required for a specific eService). Registration is to a defined level of proof of identity.
Registration Authority*	RA	An entity whose primary role is registering the identities of persons (in the context of this CWA, persons who become Card Holders).
Role		A set of pre-defined functions required to provide a service to either the cardholder or the other stakeholders. A role will consume services from the other roles of the system and combine the consumed services with its own service function in order to offer other services.
Scheme		An organised set of Roles in the exchange between stakeholders (promoters, owners, users).
Security domain		The set of assets to be protected by a security system. When digital cryptographic techniques are used, normally uses a unique set of security keys.
Security Policy		The conditions for trust relationships agreed between the card scheme's stakeholders.
Service Provider*	SP	An entity whose primary role is to provide business services/goods. In the context of this CWA, operating in the role of eService Provider .
Signature		A mark uniquely and strongly linked to the bearer's identity and which, if applied to a contract and subject to certain other criteria specified by the applicable legal system, commits the bearer to its terms.
Smart Card		For the purposes of this CWA, an electronic device compliant with ISO/IEC 7810 and one or more of ISO/IEC 7816 (for contact interface cards), ISO/IEC 14443 (for Proximity contactless cards), and ISO/IEC 15693 (for Vicinity contactless cards). See also Smart Media .
Smart Card Application		See Card Application
Smart Card Community	SCC	An entity comprising one or more Card Issuers, and possibly other partner organizations, using some common technical and security methods, and responsible for provision of access by SCC card holders to contractually specified eService(s).
Smart Card Reader		Component of an ICT system that is capable of electronically reading the content of a contact/contactless smart card.
Smart Card Scheme*		A real world organisation or grouping of organisations promoting the development and operation of a Smart Card Community and one or more eService Communities .

Term	Acronym	Definition
Smart Card Terminal		Component of an ICT system that includes a smart card reader (CAD) and is capable of interpreting the data read by the reader
Smart Media		A token with the properties of a Smart Card but in a physical format different from that specified in ISO/IEC 7810.
System Integration		The process by which cardholder-facing, internal and partner-facing systems and applications are integrated with each other.
Trusted Third Party		A security authority or its agent that is trusted with respect to some security-relevant activities in the context of a security policy
Validation Authority	VA	An entity that validates and checks the status of credentials (e.g. a Certificate linking a smart card to the identity of the card holder).

2 The Business of Deploying Cards and Services

2.1 The Classical Approach for Card Businesses: One Card Issuer and One Set of Services

2.1.1 Description

Smart cards are used in increasing numbers as tokens for accessing off-line and on-line eServices. In the past, the card industry was focused on identifying the card, and thus the user of the card, through a magnetic-stripe, EAN-code etc. With these types of “dumb” cards functionality is limited and, unless a common number is used, different cards are needed to access separate services. Cards are also an important tool for customer and brand recognition.

With these technological developments, cards have been added with a micro-processor (chip) and they have become items with the capacity to store and process data, therefore called smart cards. The microchips are tamper resistant and form a good repository for storing high security information, such as identification information. Typical smart card applications include on-line and off-line eServices such as identification, mass transit and banking.

Currently, cards are issued by the organisation offering their own set of eServices to the card holders using its own infrastructure. Most typical example is the banking sector, which issues its own cards for the delivery of its own services. Technically, the cards today can be mono or multi-application ones, which mean that a single card can hold several applications.

2.1.2 Limitations

From the card holder point of view, having a number of single cards is not convenient. Since cards are becoming more and more used in the digital world, their number is increasing. From a card issuer point of view, the number of cards increases the cost. Especially from a local authority point of view, where a number of cards and tokens are used to access their services, multi-application cards are a tempting concept.

During recent years there has been development towards co-branding cards, e.g. credit card and frequent flyer card in single plastic and in the future, with the same chip. The development is still low in terms of sharing applications, but there is an increasing interest from a number of card issuers and service providers.

It should be remembered, that cards themselves only form the visible part of the whole infrastructure. Most of the investment and development for eServices is done in the back-office systems. **Without efficient eServices, cards themselves will not produce a sustainable business case.**

Identity and access control, whether strong or weak, on-line or off-line, are in the core of most of the eServices. Cards provide a convenient and secure mechanism for storing identity data and private keys.

2.2 The Multi-Application Approach

The mono-application card is characterised by a unique application personalised in the card memory. The card hardware and software resources are designed for the efficient and secure provision of the services linked to this unique card application. In particular the Operating System of the Card is not independent from the Card application. Both are intimately linked and are often a single program called the “mask”.

By contrast, the multi-application card is characterised by:

1. The co-existence of several applications on the same card chip which can be selected and executed by a card software stack, independent of other applications;
2. The dynamic evolution of the card content, making possible the independent management of the card and of the resident applications;
3. Potentially, the co-operation between applications to grant a final service to the end-user. This interaction is a potential source of contention which must be mitigated by an appropriate design of the card architecture.

2.3 The Multi-Application, Multi-Partner Approach

The successful roll-out and exploitation of such multi-application card scheme services depends on the presence of an infrastructure which incorporates support for card holders, card issuance, card management, service providers, and the necessary capabilities to manage data capture, security and privacy, standards compliance and basic business and process rules.

By offering the same card as a means to interact with different services, possibly provided by independent organisations, the multi-application approach offers a first step in openness. By adding the multi-issuer feature to this approach, MMUSST (see 2.4 below) is proposing to open up card schemes even more.

2.4 The MMUSST Approach

The MMUSST approach builds upon the initial multi-application rationale (the collapsing together of more than one service onto a single card) and takes it through logical steps:

1. Multi-application smart cards, where a single card replaces a number of cards and tokens issued by a single entity;

but takes this further in promoting the idea of

2. Allowing additional services, provided by other parties, to be accessed via the card;

and/or

3. Hosting applets/data on the card, provided by other parties;

and

4. Allowing partners other than the Card Scheme Operator to become card issuers, where a common card structure and scheme branding is defined (business and technical rules).

There is often very little difference inferred when describing “multi-application” and “multi-service” in the MMUSST context. However, as a point of definition, the following distinction can be made:

- Multi-application cards may simultaneously host more than one application, each of which may be selected and used independently (notwithstanding Point 3 at Section 2,2 above);
- Multi-service cards provide access to different services offered by different service providers; this can be technically achieved by using a multi-application card or a mono-application one using a common set of credentials

The diversity of the functions that a multi-application card can support; the different regulatory status of the entities issuing and using the cards; and the multiplicity of relationships involved in its operation, make this a complex concept from a legal and business point of view. Indeed, the complexity increases further when the facility for post-issuance application loading (by which individual cards, subject to prior agreement by the card issuer, can be loaded and updated with different applications) is also introduced.

In the context of this CWA, the multi-application card scheme is led by the Card Scheme Operator (typically, city or regional government). Initial partners negotiate contractual terms and conditions (e.g. liabilities, functions, resources, fees). Subject to the contractual terms, which may be varied from time to time, new partners (Card Issuers/Service Providers) can join the scheme and existing partners can leave.

The SmartCities project and other locality/city card schemes have tested this concept and, while delivery is not simple, it has been proven that:

- Multiple services can be accessed from a single card;
- eServices can be offered to a particular card holder by providers other than the issuer of the card;
- eServices can be offered for local use (i.e. in the area where the card has been issued), but also to be used elsewhere.

2.5 eID like Approach⁵

As indicated above, the SmartCities concept was motivated primarily by a “citizen-centric approach, while identifying the economies and business motivation for other parties to become stakeholders in a scheme. What it did not set to address was any requirement for a highly secure proof of identity (physical and electronic) or a full investigation of the system security required to deliver this.

However, both during and since the inception of the project, there has been a steady increase of interest in using smart cards as a secure way of determining citizen ID.

Indeed, both the conceptual area and even the terminology have become blurred so that an “entitlement card” (the original domain of SmartCities) is now synonymous with an “identity card” (a card traditionally provided and required by central government).

⁵ Drawing from CWA15264-1, April 2005

Thus, “eID like approach”, in the context of this paper, refers to centrally issued and controlled cards (like national ID cards) that can be the platform for implementing different applications.

2.5.1 A Short Explanation of eID

In the physical world, people are identified in face-to-face interactions either because they are already well known to others who require such identity or they are identified through recourse to trusted third parties (e.g. by reference to mutual colleagues, official papers or external referees). This implies a set of roles and relationship which can be represented by the trust model below.

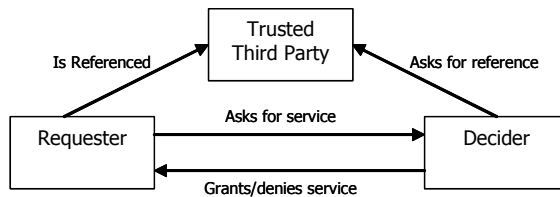


Figure 1 - The generic trust model

Electronic identity (e-ID) provides the secure mechanisms to assure knowledge of the real identity of a person, and confidence in the authenticity of who they claim to be, during an electronic transaction over a public network. This is particularly important if sensitive data is accessed or exchanged during an electronic transaction as in certain e-government or e-health services.

An e-ID card is a smart card which contains electronic identity information (i.e. data that identifies the card holder) and the logical capabilities to manage this information in a secure manner. e-ID cards are therefore implementing the trust model below.

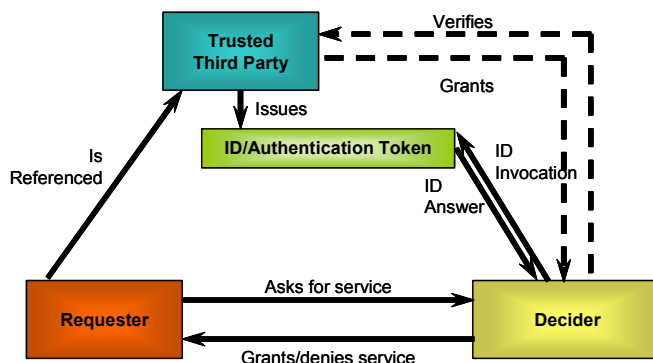


Figure 2 - Implementation of the trust model with e-ID cards

A special characteristic of the smart card format is that the e-ID card can combine an electronic identity capability with a physical identification card capability on the same support. It is hence able to address the needs for identification both in the electronic (“virtual”) and the physical (“real”) world. The plastic body contains the usual information needed to identify a person (e.g. name, photo). The electronic chip embedded on the card stores the personal data (e.g. public and private certificates, biometrics) needed to identify and authenticate the card-holder in public and private on-line transactions.

2.5.2 Different Examples of National eID Cards

Malaysia

An example of a heavily centralised eID multi-application card outside the EU is “MyKad” in Malaysia. This is a government instigated programme, initiated in 1999, which uses a powerful multi-application card for:

- ID card with thumbprint biometric;
- PKI for e-commerce transactions;
- E-Payments (including purse);
- Health Information;
- Driving Licence;
- Passport.

Other application areas including the payment of subsidies to farmers are also being piloted. The motivation behind the programme according to Datuk Azizan Ayob, Director General of the National Registration Department (NRD) is: “In Malaysia, by law, everyone must carry a national identification card once they reach the age of 12. Then there are driver’s licences, passports and bankcards, so people have too many cards to carry. We wanted one card that could perform multiple government and private sector applications, improving service to citizens and ensuring security of the information on the card”. The ubiquity of the card is also seen as a major contributor towards bridging the digital divide between rural and urban areas, which is a priority agenda of the Government. Malaysia is also keen to be at the forefront of technological advances. The target is for 20 million cardholders (full potential card base) in 2007. Cards are not compulsory, although they are issued as a matter of course to citizens over the age of twelve who apply for or renew their Identity Card.

Belgium

Within Europe, the Belgian eID card is a national card distributed by each municipality in replacement of the current plastic ID card. It gives access to e-services, e-portal functions and on-line tax declarations etc. Importantly, suppliers of payment terminals and banking readers have agreed to accept the card, which is also a travel document for “Schengen” countries.

Hong Kong

The Hong Kong Government is currently introducing a centrally driven scheme smart identity card⁶ (started August 2003 – target rollout, 4 years), with digital thumbprint biometric, as a completely separate implementation to the Octopus (commercial transit and payment card) Scheme. The card is free and is issued with optional library membership and free PKI certificate for one year. Driving Licence and e-purse applications are proposed for future years.

Consideration was given to hosting commercial applications (i.e. Octopus) on the card. The reasons cited for not doing so were:

- Security concerns
- Public perception issues

⁶ Site: <http://www.smartid.gov.hk/en/index.html>
Summary: <http://www.info.gov.hk/gia/general/200309/04/0904147.htm>

CWA 15535-1:2006 (E)

- Management issues.

Italy

The Italian national ID card project CIE (Carta Identità Elettronica, electronic identity card) is another centrally managed scheme, positioned to replace the 40 million existing paper based identity cards. The project was launched in 2001 and the first experimental phase ended in June 2003 with about 100,000 cards issued in 83 municipalities. The second experimental phase is running with 2 million cards in production of which 600,000 have already been dispatched to 56 municipalities. In the third phase (2005-2009) all municipalities will issue the cards to all citizens. The aim is to issue the cards in the next 5 years at a pace of eight million cards a year. The card is a travel document, but also positioned as an easy and efficient access to public services, in particular to health and social security services to be provided on-line (booking of hospital admissions, medical visits, medical tests, welfare requests filing).

Japan

A further relevant example on how to combine a locally issued card with an eID function is offered by Japan, with their Resident Registration Cards. These cards indeed are currently being issued by each municipality for their own purpose and are also used at national level as an eID card.

2.6 The MMUSST Approach and eID

The latter examples (in 2.5.2 above) show how the multi-application concept can be used with eID for access to services. Indeed, the Japanese example also provides a potential model for a local/central government issued card with some flexibility at local level.

Thus the question arises as to whether cities should even be considering issuing their own cards or whether they should wait until a regional/national card is being introduced. This touches on a number of cultural and philosophical issues that are not the concern of this paper, but also highlights two fundamental considerations which are, namely:

- Financial – that storing eID (possibly in its strongest form) on a locally issued multi-application card will significantly reduce the cost of delivery

And

- Security – that different forms of eID can co-exist with public and private applications on a locally issued multi-application card

What MMUSST is looking to prove is that there is a case for a local card and, subject to the motivation of the Card Scheme Operator, that card could be:

- Multi-application
- Multi-service provider

And

- Multi-issuer

The multi-issuer characteristic was born out of the economic drivers for a locally operated scheme (e.g. issues of funding, branding, ownership and, to a certain extent, control over the cardholder). Multi-issuer relationships might occur where, for example, a University or transport operator was part of a city scheme, with both requiring the facility to issue and re-issue cards according to local security or business needs. As with bank cards, SmartCities envisaged that common specification, and overt branding on cards, would allow a “family” of cards designs to be recognised within a single scheme and accepted at multiple outlets.

In the Hong Kong example (at 2.5.2 above) it has been suggested (anecdotally, at least) that none of the issues identified (arguing against the combination of a commercial transit/epayment card with national ID) was insurmountable, but that it was the pressure to proceed quickly with the programme of replacement for the existing ID Card that was the over-riding factor that drove the decision.

One idea that might be considered further is that of a multi-application citizen card carrying an electronic token that links the cardholder (voluntarily) to a second ID document or eID card. However, that the link is voluntary is fundamental to the concept of MMUSST.

Indeed, this point should be emphasised when discussing the relationship between eID and MMUSST: while eID itself is clearly a valuable card application, the premise must be that a citizen “requests” this service and not that it is a compulsory requirement in a card scheme.

2.7 Key business issues for the MMUSST approach

It is self-evident that MMUSST presents organisational complexity in partnership relationships and “sharing space” on a card. These overarch the issues developed below and are also addressed in CWA 2. Put simply, if an organisational and technical framework infrastructure can be agreed, then stakeholders will have a reference point for multi-application, multi-issuer schemes. Their challenge will be to deal with specific issues rather than those perceived or presented negatively as “show stoppers” in trying to move a scheme forward.

Equally, the MMUSST approach of a multi-issuer, multi-application environment and local eService interoperability must have a number of business advantages to make these efforts worthwhile. The benefits of the multi-application card, multi-partner/issuer model to the principal stakeholders were summarised by the SmartCities project and are updated and reproduced in the table below.

USER	
Reduced card ownership	By carrying more than one application on a card, the number of cards (smart or otherwise) which the public have to carry will be reduced
Pre-issuance Application choice	Within a multi-application scheme users will normally have the opportunity to choose which applications they would like on the card
Access & loading via remote media	It will usually be possible to access services via remote media such as kiosks and also load value onto the card at the same terminal (e.g e-purse value)
Co-branded offers	Basic co-branding offers (incentivising the use of one application by rewarding with value in another) should be possible within a multi-application scheme

Destigmatised services	If a user's card can carry a number of applications certain stigmatised services (e.g entitlements/concessions) can be concealed. With the service type hidden, other users are oblivious of the fact that a "stigmatised" transaction is taking place. This is also proven to foster service take-up.
APPLICATION/SERVICE PROVIDER	
Shared cost/risk	Depending upon the business model adopted it would usually be the case that there is an element of shared investment and operational risk within a basic multi-application scheme
Shared branding	Depending upon the marketing and branding policy of a multi-application scheme individual partners would benefits from promoting card usage <i>per se</i>
Access to wider markets	The marketing policy adopted should ensure that application providers within the scheme have at least the potential to obtain new customers from other application providers' markets
LOCAL AUTHORITY⁷	
Destigmatised public service provision	As noted above certain services can be hidden on the card within a multi-application scheme. This is particularly pertinent for public authorities in providing concessionary services that are linked to low income/disability.
Improved take-up of services	This is linked to the application provider benefit areas regarding access to wider markets and destigmatisation of services. In a local authority context this is measured by increasing the take-up of the public services it offers to eligible citizens whilst reducing fraud. This can include the automatic provision of benefits within certain transactions or the provision of information/incentives to card holders (at issuance or transaction) to use services.
Joined-up service provision	Currently citizens often have to authenticate themselves every time they interact with different departments of the authority. If more than one local authority application can be carried/accessed with the scheme smart card the local authority can make a major step to joining-up their services by understanding citizens' service use and needs and providing seamless services

Figure 3 - Stakeholder Benefits

While the motivation of scheme partners may be different (e.g. local authorities will value societal, intangible benefits accruing to their citizens, while other players will only be motivated by financial gain), collectively the core function of MMUSTT is to demonstrate a way of securely providing services electronically to a set of users who are both outside the control of the card and application issuer, yet at the same time need to be supported. It can be argued that without the users, the organisations involved will not continue to participate.

Multi-application on the cards is necessary as a foil to multiple databases, eServices and security methods, giving the flexibility to decouple eServices from each other and also to permit several transaction methods (function and security) to co-exist.

⁷ All supplier benefits will be realised by local authorities if they are an application provider within the scheme. The listed benefits within this category are local authority specific.

For MMUSST, the multi-issuer concept is the key, because entities, sometimes with very little in common will somehow have to work together for the user. Indeed, it might be argued that there are more sets of “issuers” than those who directly provide cards: e.g. multiple issuers of on-card applications, of PKI certificates. Even the suppliers of card readers and of support software for card readers and the developers of server-side (eService and database) functions could come into this category.

2.7.1 Business Issues to be addressed

The multi-application, multi-service, multi-issuer approach promoted by MMUSST is underpinned by a number of key business assumptions. These are listed below and developed within this document.

- The technical infrastructure is shared by multi-issuers and thus the generic approach is based upon marginal costs;
- There must be no significant barriers to entry for newcomers to the scheme;
- For a sustainable model to be developed there must be a win-win relationship between the multiple issuers. Ideally they will have complimentary customer bases;
- There will be an organisational framework established which can both foster trust between partners, manage conflict and establish clear operating rules.

3 Multi- Service/Multi-Issuer Schemes

A Card Scheme is usually designed by the Card Issuer, even when it is based on multi-application cards or intends to invite various service and eService Providers to join the scheme. A useful example for the design of such a Card Issuer centric scheme, including the role model and a high level architecture is provided by CWA 15267 on eAuthentication.

In a multi-issuer environment as defined by MMUSST, the situation is more complex. Depending from the business case used for setting up the scheme, it can be designed by

- an initiating Card Issuer (e.g. a municipality) who invites other card issuers to join the scheme
- a local, regional or national (and perhaps later a European) Authority which does not issue cards but invites potential Card Issuers and Service/eService Providers to join.
- A Service/eService Provider who is seeking to offer services to people holding cards issued by different card issuers.

The key issue raised here is in fact who is organising the relationship between each (potential) stakeholder of the scheme and how are they organised.

The role model below will provide the principles required for answering these business oriented questions.

3.1 Card scheme with Cards and Services communities

A preliminary distinction is of prime importance before setting up the Role Model of a Card Scheme: the role of the Card issuer is to be disconnected from the Service/eService Provider one and both roles are to be disconnected from the role of card Scheme Operator, in charge of managing.

From a business perspective in particular, the role of the Card Issuer and Service/eService Provider obey to different rules and principles; they are indeed at the two extremes of the above-mentioned value chain.

Once this disconnection is done, then there is a need to have another role, i.e. the card scheme operator (see below), in charge of arbitrating, coordinating the activities of the two others and, by doing so, taking care of the interest of the Card Scheme.

This disconnection leads us to organise two sub-entities within a single Card Scheme.

3.1.1 Card Community

A Card Community is a grouping of organisations, playing roles, established to oversee the operation of an interoperable environment for smart card operations. This environment includes the technical infrastructure needed to enable holders of compliant smart cards to access compliant applications via compliant terminals. A card Community is per essence Card Issuer centric.

In principle, there is one Card Community per Card Issuer, but there may be situations where several Card Issuers are applying common specifications and policies. In these situations one can consider that there are several Card Issuers which are federated within the same Card Scheme.

3.1.2 Service Community

A Service Community consists of all natural persons authorised to access and use Services/eService. It is therefore Service Provider centric. Some could say that it is Card Holder centric, since the person holding the card is using it for obtaining a particular service. At the level of the Role Model, this does not make much difference however.

Please note that an eService Community can be contained within, or span one or more Smart Card Communities. The relationship between Card Community and Service Community can be represented as in the below drawing.

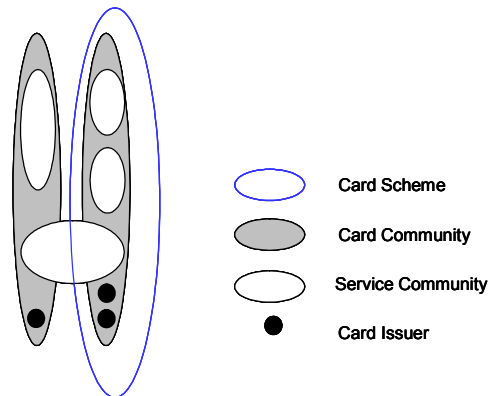


Figure 4 - Card and Service Community relationship

3.2 MMUSST Role Model

- In the MMUSST environment, the Smart Card Schemes include a number of Service Providers offering a number of Services/eServices to the Card Holders. Card Schemes can offer different levels of security within the scheme. It is up to the Service Providers to decide which level of security is required for their service and if the Smart Card Community they consider offers the required level of security. In the role model below, the possibility for the card community to offer strong authentication and eSignature services has been taken into consideration, but all the roles may not be relevant to schemes without these services being offered.
- The role model provides details on roles and responsibilities, but does not have to be considered as an entity model. An entity indeed is an object performing one or more Roles, depending from the implementation rules applicable in the card scheme. In other words, while in a Card Scheme "A", an entity "a" could combine the role of the Card Issuer with the one of eService Provider, one could have, in a Card Scheme "B", still in compliance with the same Role Model, and entity "b" acting as a Card Issuer and an entity "c" acting as service Provider. Therefore, the fact that several of these roles can be carried out directly by the same organization or subcontracted to a third party under the entitled organization responsibility does not affect the Role Model. Combining roles within the same entity may however have important consequences on the security policy of the card community.
- Some of the roles will/may be duplicated within the same Card Scheme.

- Operational tasks devoted to some of the roles may be delegated, but those implementers act as agents of the entity in charge of this role.
- The assumption is that each stakeholder will be liable for the aspects of the scheme that relate directly to the role that they play.

Card Scheme

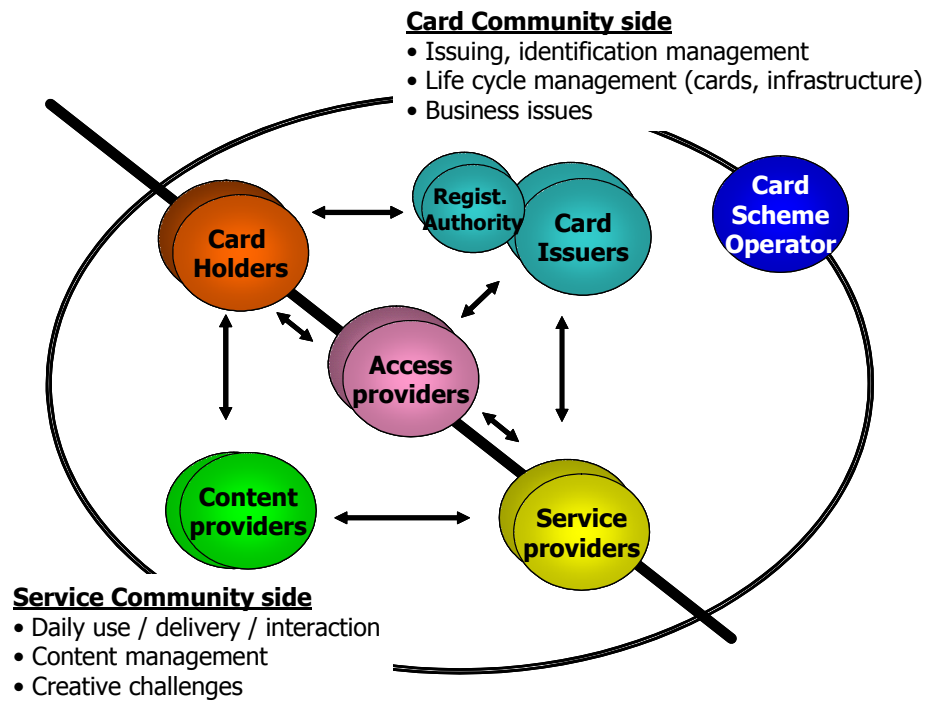


Figure 5 - MMUSST Role Model

The basic roles within a Card Scheme are exercised by the following stakeholders:

- **The Card Holder** (e.g. citizen, user) (CH) is a real person (in the legal sense, i.e. an individual human being, not a company or other legal structure) who has been issued with a smart card by a card issuer. The issued smart card is associated with and issued to the specific card holder and to him/her only. This association enables the card to be used by the card holder for IAS purposes and thus to enable him/her to access services provided by service providers.
- **The Card Issuer** (CI) roles are to manage personal identities with the support of the Registration Authority (RA), issue smart cards to card holders according to scheme policies and rules, and manage the issued cards throughout their lives (card population life cycle management). In case there are several card issuers in the same card scheme, they all have the same responsibilities, namely to:
 - Conform to card community security policies and rules
 - Ensure that the card holder has been registered according to its security policies
 - Physically issue the smart card (personalise it, generate security objects if the scheme requires (i.e. PIN key pairs), install certificates, enable them for use)
 - Securely deliver the smart card and, if any, the authentication mechanism (PIN or enrolment of biometrics) to the card holder
 - Operationally manage card security (including, if any, authorising application download/activation in the case of multi-application frameworks,

- monitoring the card community for security breaches, administrating cards by authorising post-issuance upload and activation of applications, blocking applications and cards, authorising card unlocking)
 - Operationally manage the card population (including maintaining a database of cards and their contents, providing a single point of contact for the card holder, and arranging for card and card content replacement in cases of lost/stolen/faulty cards)
- **The Registration Authority (RA)** registers card holders: i.e. obtains sufficient proof of the identity of the card holder by traditional means. Additional RA functionality (such as attributes of a real person, as required to implement the advanced electronic signature provision of E-sign) may be provided within the Card Community, possibly supplied by other RAs.
- The role of the **Card Scheme Operator (CSO)** is global and linked to the Card Scheme. It is to administer, monitor and support the relationships between the Card Issuer(s), the Access Provider(s) and Service Provider(s) in order to ensure the integrity of the Card Community.
 - In a MMUSST context, where the focus is on local authority schemes, the Card Scheme Operator is a role which fits well to local, regional, national or even European authorities. The basis for this logic is that, generally, citizens “trust” governmental organisations to behave in a way that is ethical and is not looking to excessively exploit the commercial aspects of the scheme.
 - That is not to say that another organisation could not take the role of the Card Scheme Operator, but there would then, probably be the further requirement for a formal “regulatory framework” as was envisaged by the SmartCities project as “SmartCities Global”.

The management and operational responsibilities of the CSO include:

- Definition and maintenance of scheme security policies and rules and ensure the coordination with the security policies and rules of the Card and Service Communities included in the Card Scheme.
 - Definition, maintenance and enforcement of internal card community interoperability specifications and rules of access (e.g. interoperability between the card issuer and a service provider, rules for using available space on the card for additional applications).
 - Registration of the different stakeholders of the Card Scheme and verification of their compliance to the specifications and rules of access (e.g. certification of the smart card readers towards the security specifications).
 - Definition, maintenance and enforcement of external interoperability specifications, and organisation of interoperability with other Card Schemes.
 - Provision of support of Card Holders (e.g. Help-Desk), Access Provider(s) and Service Provider(s)
- If any, the roles of **the Certificate Service Provider (CSP)** or the **Certification Authority (CA)**, is to:
 - Issue certificates under the responsibility of the stakeholder who ordered them: IAS certificates related to the card holder (including certificates containing attributes of the card holder)

CWA 15535-1:2006 (E)

- Any other certificates used for the functioning of the smart card information system (the scheme)
- Any other certificates required by a service provider for the functioning of its business service.
- Create and maintain a Certificate Revocation List or CRL, including creating and managing a repudiation policy in case of lost or stolen cards or misuse of cards
- Provide a service to validate certificates (in the present framework, this must be an on-line service). This service may be delegated to a Validation Authority (VA).
- If any, the roles of the card **Application Issuer** (AI), is to:
 - Issue on-card applications
 - Arrange with the card scheme operator (CSO) and card issuer (CI) for on-card applications to be registered and for downloads to the card to be authorized
 - Provide a mechanism for loading applications onto cards (this mechanism will usually be defined by the card issuer)
 - Manage security of the applications
 - Maintain (if required) backup accounts for the contents of the application on the cards, unless this is a function of the card management system
 - Provide recovery services for data when applications on the cards are replaced
- The role of the **Service/eService provider** (SP) within the model is to provide business services to the card holder using the smart card as a token and/or in conjunction with one or more other specific on-card applications.
 - It must register with the card scheme operator and comply with scheme policies and rules.
 - It concludes all the necessary contractual arrangements with the access provider and it also defines who may have access to the provided services and under which conditions.
 - Beyond that, the content of services is outside the scope of this CWA.
 - Card holders may be required to sign up (register) with service providers in order to use their services.
 - The service provider may offer services to more than one smart card community (smart card scheme), and therefore a Service Community expects to take advantage of the interoperability between smart card schemes in order to provide seamless services
- The **Access Provider** (AP) is the entity in charge of managing the infrastructure to be used by the card holder for accessing the offered services and managing card content. The infrastructure includes:
 - Terminals directly associated with card handling (e.g. card readers and necessary driver software);
 - Other terminal functions and equipment (e.g. where PCs are used as clients on the network);
 - Communication networks; and
 - Server systems.

- The **Content Provider (CP)** is the entity in charge of keeping the content of the service provider up-to-date. This will be in accordance with content service requirements and agreements.

3.3 Potential Revenue Flows

There are a number of potential revenue flows between actors within a scheme. Figure 7 presents an example of where these flows might occur in a mature scheme. It is worth noting that financial models of potential income streams to the scheme operator should also consider scenarios where:

- The Scheme Operator is also a Card Issuer;
- Service Providers are also Card Issuers.

Potential Revenue Streams

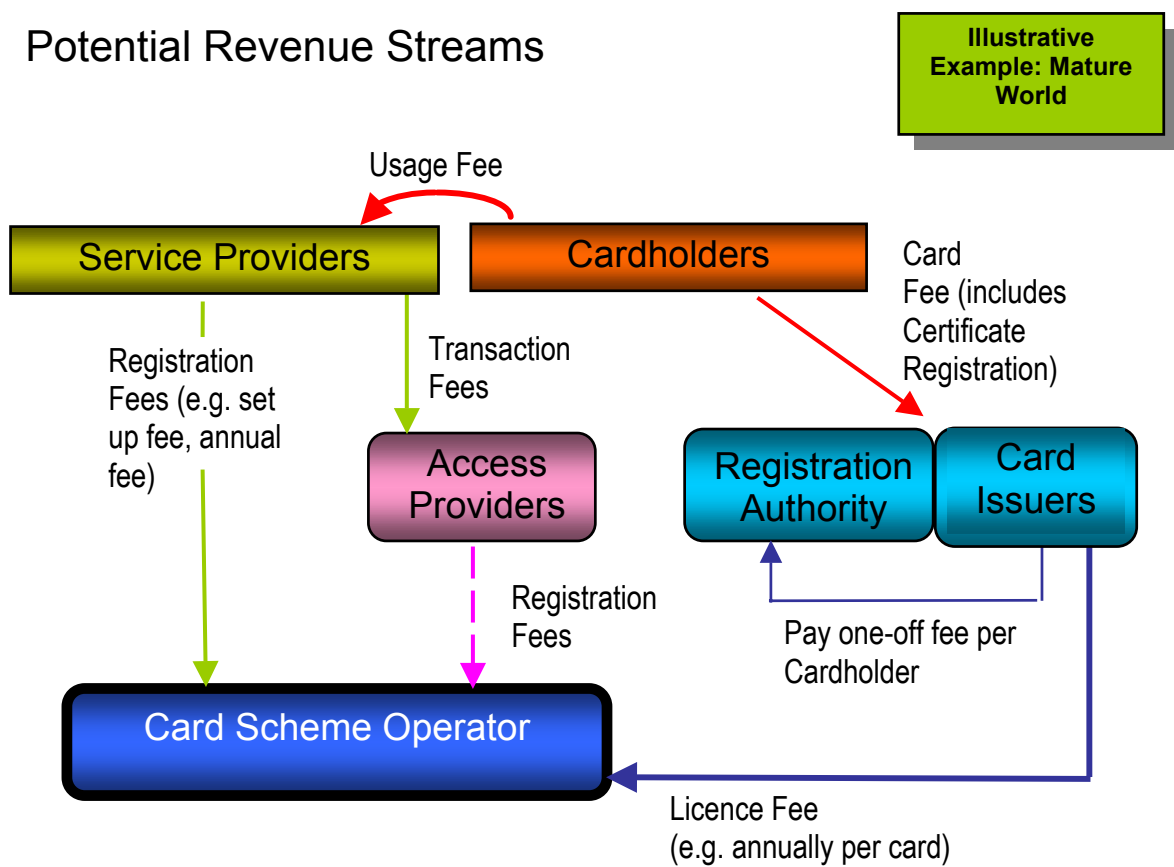


Figure 6 - Potential Revenue Flows – Illustrative Example

Clearly, where the Card Scheme Operator (CSO) is a local authority, the nature of the business arrangements that will be put in place will be focussed upon guaranteeing the income stream (fixed fees) and therefore minimising the risk to them within the scheme. If the CSO was a commercially oriented venture (e.g. joint company including the local authority or a different stakeholder), then the fee income could be more volume focussed.

4 MMUSST Business Cases

4.1 MMUSST Drivers

The SmartCities Interest Group, with its membership base made up of local authorities is primarily concerned with the following factors with regard to setting up a card scheme:

- access to services and facilities delivered by local authorities
- the management of concessionary entitlement to those services
- wider access to electronic government
- citizen benefits of multi-application cards that include services not provided by local authorities
- the improved business case and scheme sustainability that can be secured by hosting third party services on a local authority issued card
- the ability for the card to be used beyond local boundaries, by using accepted industry standards and conventions

These different factors encompass both single elements that have a financial and social justification for multi-application, multi-service cards, but also a number of inter-dependencies that underpin the central MMUSST business case.

Taking them in order:

- **access to services and facilities delivered by local authorities**

This is the internal business case based upon the rationalisation of token and card based services into one central scheme. There is significant cost of issuing and managing multiple cards and tokens to the same citizens from different service departments.

Similarly, there is a drive for local authorities to strive for better customer relationship management by providing a single point of contact for citizens and for access to diverse information to be available through different channels. Whether as an end module (“slave”) to a CRM system, or as a “master” database in itself, a centralised card management system can become a powerful tool in dealing with the citizen.

- **the management of concessionary entitlement to those services**

In categories such as: age (young and old); disability; economic circumstances; and geographical location, local authorities are legally (or by social policy) bound to provide concessions to certain groups. A multi-application card solution provides a portable proof of concession that might be applicable across a number of services and, importantly, using an electronic read can be made invisible, thus avoiding the social stigma of using “free tokens” of having a card with the age of the cardholder printed on the front.

- **wider access to electronic government**

Multi-application cards are an ideal platform for introducing citizens to services that are available with an electronic interface. Furthermore, as the number of “channels” for accessing electronic government increases, there is growing concern over security. Multi-application cards can be issued with security or trust levels and can hold applications to manage access based on that security/trust.

- **citizen benefits of multi-application cards that include services not provided by local authorities**

A considerable amount of feedback has been obtained from citizen consultation and validation exercises undertaken in the UK. Presented with the concept of a single card for accessing multiple services, citizens readily accept the benefits in terms of convenience.

Of particular interest to those surveyed are:

- The ability to register for multiple-services at one time and/or the ability to extend the number of services available without having to undergo full registration procedures and prove identity by producing documentation
- The use of a card bearing a photograph and electronic credentials as a form of ID
- The aggregation of access to chosen services on one card according to the “life-style” choices of the cardholder

The latter point in the above list is essential to the MMUSST, multi-issuer logic: for the citizen, “real” (or at least significant “added”) value is truly obtained where a multi-application card provides access to services from multiple partners. For the cardholder, the limitation of a local authority providing its own services is far less attractive than a card that can also be used for transportation and payment. However, it is essential to note that citizens do value the role of the local authority in managing the scheme as this engenders a feeling of trust that the regulations and laws regarding personal privacy will be strictly adhered to.

- **the ability for the card to be used (for desired services) beyond local boundaries, by using accepted industry specifications, standards and conventions**

The problem for individual schemes has been in trying to facilitate “value” card services without incurring significant set-up and operational costs (e.g. for a local e-purse scheme) and unwieldy organisational agreements (e.g. “public” transport schemes that cross local government boundaries).

These are overcome if sector based standards are applied to on-card applications and accessible services.

4.2 Typology of eServices

The following identification of potential services is taken from NSCP WP2-01. They have a UK focus which needs to be both rationalised and classified, perhaps into different tables (e.g. to identify services which may clustered with those offered by local authorities).

Table 1 - List of Applications, Services and Uses: Within Local Authority Control

LOCAL AUTHORITY PRODUCED	APPLICATIONS, SERVICES AND USES
Within Local Authority Control	
Employee	Visual/electronic ID
Employee	Access control/attendance
Employee	Parking
Employee	Closed electronic purse
Employee	Record of competencies (qualifications)
School	Attendance and access control
School	Catering
School	Reward
School	School library
School	Photocopier control
Education	Adult Education/Life-Long Learning
Licencing	Taxi
Licencing	Door staff registration
Licencing	Market traders
Citizen	Local Authority leisure
Citizen	Local Authority library (including mobile services)
Citizen	Other Local Authority services (e.g. activity mailing lists)
Citizen	Visual ID
Citizen	Single sign on/access/citizen account (PKI/Electronic Authentication)
Citizen	Financial transaction (both ways)
Citizen	Voting/Surveys (electronic authentication)
Citizen	Electronic purse
Citizen	Local payment token (including Parking)
Citizen	Loyalty/reward programmes (inc. incentives for behavioural change)
Citizen	Local benefits/entitlements (inc on street resident parking)
Citizen	Preferences (e.g. for kiosk)
Citizen	Proof of age
Citizen – Entitlement	Concessionary transport
Citizen – Education/Skills	Record of competencies (Qualifications)/Life-long learning
Citizen - Social Services	Community transport
Citizen - Social Services	Domicilliary Services front end for billing and timesheeting
Citizen – Housing	Rent payment – identification and account number
Citizen - Environment	Recycling and/or civic amenity site
Citizen - Community Safety	Neighbourhood watch
Tourism	Visitor access
Tourism	Event access
Tourism	Discounts
Transport	Tolls/charges
Transport	On and off street parking

Table 2 - List of Applications, Services and Uses: Other Local Public Sector

LOCAL AUTHORITY	APPLICATIONS, SERVICES AND USES
Other Local Public Sector	
Health	Prescription
Health	Emergency medical
Health	Appointment booking
Health	Tracking (date of medication etc)
Health	Mobile Services
Education	Student ID
Education	Access to campus facilities (including types of application above)
Education	Records of Competencies (qualifications)

Table 3 - List of Applications, Services and Uses: National Public Sector

LOCAL AUTHORITY	APPLICATIONS, SERVICES AND USES
National Public Sector	
Home Office	Passport
Home Office	Biometric
Home Office	Identity/entitlement
Vehicle Registration Authority	Driving licence/penalty points
Vehicle Registration Authority	Log book/MOT/tachograph
Transport Authority	National transport ticketing
Health	Number/record storage/access
Education	Youth Card (Connexions)
Education	Life Long Learning
Others	Benefits/Entitlements

Table 4 - List of Applications, Services and Uses: Private Sector

LOCAL AUTHORITY	APPLICATIONS, SERVICES AND USES
Private Sector	
Employee	Visual/electronic ID
Employee	Access control/attendance
Employee	Parking
Employee	Closed electronic purse
Employee	Record of competencies (qualifications)
Transport	Ferry
Transport	Rail
Transport	Bus
Transport	Underground
Transport	Trams
Transport	Taxis
Transport	Toll Bridge
Transport	Toll Roads
Transport	Parking – off street privately owned car parks (inc “Park and Ride”)
Transport	Parking – corporate
Financial	E-purse/e-payment
Telecoms	Phone cards
Telecoms	Conditional access to digital television channels
Retail	Loyalty/Reward
Retail	Tourism
Retail	Membership
Retail	Vending
Retail	Gambling/Gaming
Retail	Proof of age
Retail	Identity

4.3 Methodology for Identifying Business Cases

4.3.1 Strategy for Card Scheme Deployment

The Global Interoperability Framework for Identification, Authentication and Electronic Signature (IAS) with Smart Cards⁸, in its Part 4 “Deployment Strategy” provides the basic

⁸ See Part 03-4 of the “Open Smart Card Infrastructure for Europe” report of the eEurope Smart Card Charter issued in March 2003.

material for a deployment strategy for a card scheme which maximises the “creation of value”.

Such a strategy is developed along two axes:

- The card penetration, which is comparable with the channel strategy in traditional companies (see Figure 7, horizontal axes). It is the sum of dedicated terminals and kiosks plus the number of relations to Internet oriented tools to access the e-services.
- The value of the services, which is comparable to the merchandise strategy (concerning products and or services) in traditional organisations (see Figure 7, vertical axes).

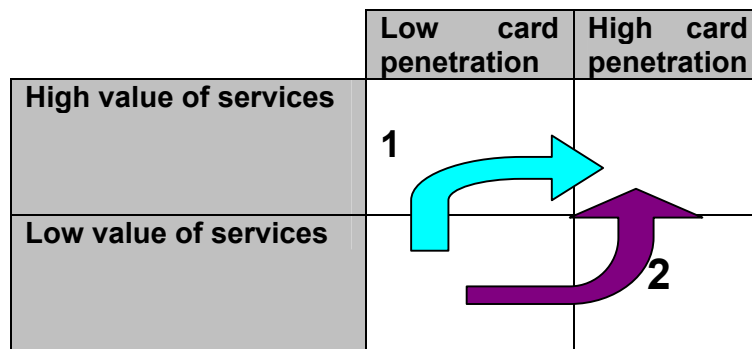


Figure 7 - Deployment strategy for a card scheme

Applying the concepts defined by Michel Porter, the well know specialist in business strategy, the strategy choices for winning strategies for value creation with a card scheme are:

- Exploiting high value dedicated services for dedicated target groups, i.e. differentiation strategy (see Figure 7, from lower left to upper left position)
- Exploiting cost effective services for larger markets, i.e. cost leadership strategy (see Figure 7, from lower left to lower right position)
- Aggressive channel strategy after having introduced and established brands for well accepted and cost effective e-Services (see Figure 7, to the upper right position)

The ultimate goal of the business strategy is to reach the high right position in Figure 7.

The classical problem is therefore:

- Does the card scheme first create the card base and infrastructure, and then add / invite the e-services later (curve # 2 in Figure 7), or
- Does the card scheme focus primarily on finding the successful e-services, and follow with the expansion of the card base and infrastructure (curve # 1 in Figure 7). In that case the strategy is much oriented to establishing a ‘brand’ of all the offered e- services.

From the above, it can be said that the MMUSST approach is a way to implement a deployment strategy which, by combining a multi-issuer approach with a multi-service provider one, aims at combining both the differentiation and the cost leadership strategies.

The business case is in finding somehow the right mix between card base and infrastructure on the one hand and the (number of) e-services using the card base on the other. The main method to balance this dynamically is the 'value chain' as explained below.

4.3.2 Value Chain in a Card Scheme

What does a value chain for a card scheme look like? The research company OVUM introduced a value chain for smart card centric services which divides the value creation process as follows:

1. Basic smart card services (smart cards, infrastructure)
2. Trust services (identification and authentication)
3. Electronic services (generic e-services, individualised/ interactive services)

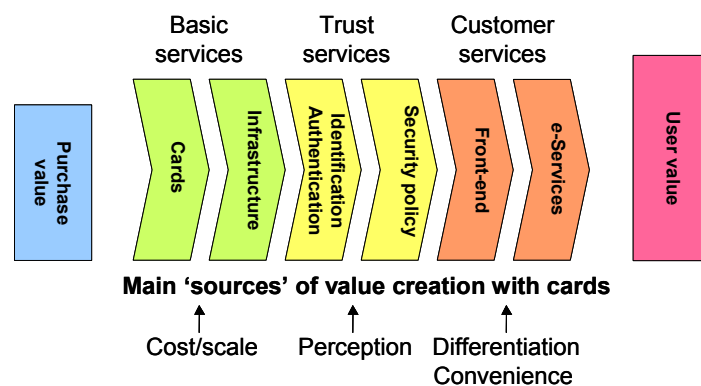


Figure 8 - Value Chain in a card scheme

Basic Services

Traditionally, the value chain was limited to smart cards and infrastructure. The issuer does not offer to the card holder any choice in the application or e-service. The application is ultimately aimed at providing benefits to the card issuer, for its own benefit (e.g. physical access to facilities, transport ticketing, payment, social protection or health insurance identification and entitlement, loyalty programmes). The value creation chain is mostly oriented to cost reduction for the card issuer and "creating more value" in this chain often means "lowering the cost of the smart card and the infrastructure by standardising and enlarging the scales".

Trust Services

When intended to provide high level trust, these services are often directed to special services with a limited amount of users, e.g. e-Market networks (purchasing, b2b ordering, etc.), closed subscriber groups, secure internal company (tele-) networks, secure e-mailing. They are indeed rather expensive with high interests and high risks. Mobile telecom is currently the only segment where some trust services (with the SIM-card) are applied on a large scale, but they are limited to identification without strong authentication.

In ALL other segments with low priced security products (via the internet), the offer and the acceptance seem to be fragmented. Therefore, "creating more value" in this context requires "disconnecting the trust services from the basic services". This is one of the key messages of CWA 15264 on eAuthentication.

High-end Customer services

These services come at the end of the chain and are therefore expensive to implement if the whole value chain has to be implemented by the same entity. In a large number of situations, this is a solid barrier to their deployment.

Currently, they are to be paid either by the customer (i.e. the card holder) or a card issuer which has a solid business case (e.g. governments). Therefore, similarly to the previous case, “creating more value” in this context requires “disconnecting the customer services from the trust services”. This would indeed open the door for sharing costs between all those who offers e-services to the same card holders. Again, this is one of the key messages of CWA 15264 on eAuthentication.

4.3.3 Using the Value Chain method

When using the value chain as a method to increase the user value by extending the eServices and the card base, the following statements are to be made:

1. Without customer appreciated e-services, smart card centric services have relatively low customer value. Or positively formulated: the most substantial user value is created by the eServices, and not by the card itself. For smart card oriented services, all strategies are possible:
 - Large scale / cheap services, competing on cost leadership
 - Small scale / dedicated services, competing on differentiation leadership
 - Brand / image oriented services, competing on perception

This applies to MMUSST

2. Parties involved in issuing cards and providing card access are probably not the best to maximise the user value by services. Their contribution in optimising the value creation is oriented to the cost reduction strategy:
 - Quality / cost ratios by large scales
 - Cost sharing

This applies only partially to MMUSST insomuch as a local municipality is likely to be the primary card issuer. However, other card issuers may also drive user value.

3. The perception of ‘trust’ by the customers is essential. For the acceptance of high-level services in a networked environment, quality and independence from commercial interests for this part of the chain could be the key. The applied technology must be perceived as superior, and / or generally accepted.

This key perception for MMUSST and was validated during the SmartCities Project and by Interest Group Members

4. The stakeholders have to follow their own strategy to maximise their contribution to the maximum user value, based on collective parameters of the final value for the user. It is important that the measures are shared.

This statement is implicit to the MMUSST concept,

5. The conditions that the parties have to fulfil together in organising themselves in a value chain for smart card centric eServices are:
 - Technical (standards, interfaces, handling common data flows)
 - Business (cost sharing, branding, business growing strategy)
 - Organisational (legal entities, responsibilities, common systems) with last, but not least, accepted common performance indicators.

This statement is implicit to the MMUSST concept.

5 Card Scheme Implementation Guidelines

5.1 Integration Methodology

The number of multi-owner, multi-application smart card schemes is expected to grow in coming years, as private and public sector organisations understand the potential benefits and opportunities that they can provide. One of the advantages of such a "universal" card is that the individual Card Holder could deal with one single issuing organisation, offering services from a number of different organisations, using a single card.

Implementing a MMUSST approach scheme involves many steps, including preparation, planning, organising, designing, developing, deploying, training and supporting the partners and educating final users. In particular meeting the business needs of the service providers has to be integrated into the scheme. This requires collaborative integration actions on technical systems, business objectives, legal constraints, revenue related parameters and migration strategies.

Thus, when integrating a multi-application system potential Card Scheme Operators should include all aspects of the following outline "Methodology for Multi-application System Integration":

1. Definition of Business Objectives both for the card scheme and each type of stakeholders (win-win approach)
2. Identification of user needs and constraints
3. Identification of Service Provider Requirements
4. Identification of Institutional and Legal constraints
5. Evaluation of Aggregation of Services for new revenue streams and other perceived benefits
6. Evaluation of service fulfilment and transaction completion (e.g. e-Payment Methodologies)
7. Methodology for Data Collection and Analysis
8. Migration path from existing technology, integration alternatives and data sources
9. Perform Initial Business Case Analysis
10. Compare and Recommend the Business Case
11. Develop Decision Choices
12. Consider possible partners
13. Planning, Deployment and Operation
14. Compilation of own and other best practice case studies and documentation for use in marketing, training and developments of the card scheme.

5.2 Risk Assessment

Such a methodology (as described above) is crucial to manage such a complex initiative. However, there remains a multitude of risks associated with setting up a scheme of this nature. When embarking upon a MMUSST type scheme, it is essential to establish a robust risk register. The three predominant areas of concern are:

5.2.1 Technology Risks

In fact, this will probably be the easiest risk to manage. The technology itself is mature and many technical standards are in place. However, it is essential that the technology choice is “fit for purpose” for both the initial scheme and forward proposals within a defined time horizon.

5.2.2 Financial and Commercial Risks

As suggested above, the scheme initiator, in a MMUSST scheme, is likely to be a (public) local or regional authority. Such entities are characterised by their regulator function and are risk averse, both by their nature and by the manner in which they are constituted. In fact, it is these elements which will determine the extent of their participation and boundaries for the scheme.

Local Authorities would therefore seek to avoid any commercial risk or at least limit it within their own responsibilities as a Card Issuer and/or Service Provider at scheme initiation. However, they are in an ideal position to fulfil the function of Card Scheme Operator both because of their regulator role, but also because they are trusted by scheme partners and card holders alike.

In proposing a scheme and adopting the role of CSO, the local or regional authority might accept that a level of “seed funding” must be provided to cover some of the initial costs (capital and operational). This acts both as an incentive for partners to join and to ensure that the future scheme is organised and constituted to an acceptable level.

If any public authority wishes to extend the commercial opportunities within the scheme, it might consider setting up a separate legal entity to manage the scheme (i.e. to become the Card Scheme Operator). This will, however, have the effect that they might lose an amount of control over the governance and direction of the scheme.

In either circumstance, the financial and political impact of entering into any commercial agreements must be assessed.

5.2.3 Legal Risks

The most far reaching (and often complex) area for risk management is associated with the legal relationship between different actors and the relationship with the Card Holder. While the sections below offer a comprehensive introduction to this area, further understanding is recommended⁹. A risk register of legal queries is essential.

⁹ The document prepared for the English National Smart Card Project entitled *WP8 – 08 – Risk Register* is an excellent starting point (although references primarily refer to English law) It is available at: <http://smartstore.scnf.org.uk/>

5.3 Legal Framework

5.3.1 Specific Legal Characteristics of Multi-Application Cards

The multi-application card is a personal physical document given to a Card Holder by a legal entity, the Card Issuer, in order for him/her to exercise the rights defined by one of more contracts existing at the time of the card delivery and optionally new ones concluded between Card Holder and a third entity, the Service Provider, usually subject to approval by the Card Issuer.

The rights represented by the card are not transferable to a third party. The multi-application card is intended for personal use, and the card supports the mechanisms to enable the card to provide services only to the entitled person. The general Proof of Rights contractually acquired by the Card holder, includes the following caveats/attributes:

1. There is no total transfer of Rights onto the Card as a result of delivery of the Card. If the card is lost there is no loss of the rights, just loss of the proof.
2. The Rights supported by the Card are only valid for a period of time after the Card Delivery. This period is contractually fixed. After that the Card Rights expire, and the Card Identifier must be put in a publicly available Revocation List.
3. Subject to established and applicable legislation and the specific contractual stipulations of the Contracts agreed between the Card Issuer and the Service providers and between the Card Issuer and the Card holder these Rights can be totally cancelled by the Card Issuer.
4. The Rights granted by a Service Provider can be revoked by the Service Provider, following the provisions of the contract signed between the Service provider and the Card Issuer and, optionally, between the Service provider and the Card holder.
5. Possibility of Priority Application Support: One of the applications can be activated by default; the other may require explicit selection and activation by the Card holder.

5.3.2 Data Protection and Privacy

The key legal issues surrounding the manipulation and use of personal data arising from MMUSST scheme, and the legal issues surrounding their establishment and operation are:

- Data protection and privacy
- Liability and security issues
- Scheme competition and procurement

The growth in the use of personal data has many benefits both for society, (for example: helping to fight crime), and for the individual, (for example swifter access to medical care). However, whenever personal data is collected and used, people's lives can be adversely affected if something goes wrong. For example, if details are not entered correctly people can be unjustly refused credit, benefits, housing, or even a job. If data is not kept securely, people's privacy can be affected. It is vital that those who collect and use personal data maintain the confidence of those who are asked to provide it.

The European Parliament has set Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data which

sets grounds for data legislation. Each country has their own data privacy acts and there are some minor differences between the specific acts within each country and these should be considered on a case by case basis. However, the fundamentals described are applicable to each country.

5.3.3 Data Protection and Privacy - Practice

Data Protection legislation applies to 'personal data', defined as being data about identifiable living individuals. Those who decide how and why personal data are processed (data controllers), must comply with the rules of good information handling, known as the data protection principles.

Principles of good information handling

Anyone processing personal data must comply with the eight enforceable principles of good practice. These state that data must be:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in line with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual. All aspects of the card scheme should be benchmarked against these eight principles at the outset of the scheme and during its development.

Legislative implications for the multi-owner multi-application scheme

From a data protection point of view, a key potential benefits, and also a new concern, would be the ability of a card issuer to **cross profile** a particular data subject in many fields of activity that were previously unconnected.

Such a cross profiling is not "per se" unlawful, but due to the potential for providing a global vision ("Big Brother") of an individual's activity, it is important that measures are taken to ensure that an individual's personal privacy is respected.

There are five further key fields within a multi-application scheme within which data protection and privacy legislation is particularly pertinent. These are presented below, together with the key questions arising. However, it should be noted that the principle of protection of citizens' rights with regard to data should pervade the whole culture of the schemes.

Data collection

- How is data collected?
- Are you collecting the data legitimately?
- Does the data subject know why they are giving you the data?

- Are you then storing and processing the data legally?
- You need to consider whether you are getting the data from existing databases or are you using application forms.

The card management system (CMS)

- Are you holding the data for a reasonable length of time?
- Are you sharing the data with another organisation or individual? Are there contracts in place between the different organisations?

The card architecture

- If the card is used by multiple organisations; what data are they allowed to access on the card?
- Have you created a 'shared area' on the card?
- Post issuance application download
- When you download an application will you adversely affect other applications or data residing on the card?

Liability and security issues

In order to comply to both the letter and spirit of the law, and indeed to ensure that users and application providers have full confidence in schemes, it is crucial that prior due regard is given to the limits of liability within a scheme, as well as the security of its internal systems.

Liability

- When a card is lost or stolen who does the card belong to?
- Who pays for a lost card?... the cardholder?
- If a card is damaged who pays for the card? ... the cardholder?
- If an application stops working whose responsibility is it?
- If there is a security breach who is liable? Issuer, application provider?
- If a digital certificate is used who is liable for its authenticity? Has a certificate policy been created?
- What contracts are in place between the various parties?

Security

Data Collection

- Are you confident that the data collected is valid? Is the person who they say they are, do they live where they say they live? Etc
- What authentication process has been used? (1 proof of address, 2 proof of id?)
- What mechanisms are used to secure the data transfer and avoid loss or changes in the data?

The Infrastructure

- Is there general card / terminal security?
- Could the security of the card and applications be compromised easily?
- Could a copy of the card be made easily?
- The cost of implementing security needs to be balanced with the potential risk?

CWA 15535-1:2006 (E)

- What security is in place to stop service providers accessing areas that are not relevant to them. For example is it reasonable to allow a train company to see medical details on the card?
- What is the impact of a breach in the security? Will this compromise all cards?
- How are all the communications protected against fraud?

5.4 Privacy Code of Conduct

Smart cards can store and process data. In the case of multi-application cards this may include personal data i.e. information relating to an identified or identifiable natural person. In order to stimulate the social acceptance of the cards and to promote their harmonised introduction general conditions derived from the European Directive 95/46/EC are specified in the following General Privacy Code of conduct for interoperable smart card systems.

The smart card offers possibilities to increase the transparency of the data operation process. By use of convenient card reader terminals the card user can view their own data (including data for identification, authentication and for a digital signature) in a relatively simple way and when enabled also view the data in the related registers of personal data.

The Code of Conduct provides a set of agreements within a smart card community that prevent uncontrolled and undesired use of personal data by card issuers and service providers. This is put into effect through a system of compartmentalization whereby individual service providers each acquire their own independent area or compartment of the electronic memory of the smart card. Every service provider has exclusive reading, writing and data operation authority for only his own field of application. Every application does have the possibility to consult and use but not to modify the general personal data recorded on the card by the card issuer. These separated responsibilities and possibilities for use are designed to remove the fear of data intentional or accidental misuse of personal data.

These Rules of Conduct are general rules which still need to be worked out in more detail in a specific sector. The health care sector for instance certainly needs detailed privacy rules in situations where there is a 'health card' with very sensitive personal data concerning medical care status and history. With these general codes of conduct, shape and content is given to the privacy principles mentioned above on the basic cross-sectoral level for smart cards.

GENERAL MODEL FOR A PRIVACY CODE OF CONDUCT

Taking into consideration:

- that the EU aims to accelerate and harmonise the development of smart cards across Europe and to establish them in all shapes and forms as the preferred intelligent mobile and secure access key to citizen and business e-services;
- that the smart card has many different applications and can be applied in many sectors in an interoperable way;
- that in these applications the interests of all parties involved must always be considered and sometimes weighed against one another;
- that due to the many different applications and equipment used, the data collection, recording and use can become non-transparent to the card holder;

- that on the other hand the smart card offers possibilities to guarantee the safety of the data that are stored and to make the data that are stored more transparent by a direct form of consultation;
- that the privacy protection concerning the use of the smart card would benefit from openness with regard to all aspects of the information operation process;
- that this openness can also lead to stimulation of the social acceptance of the smart card;
- that, furthermore, attention should be paid to principles on a legal basis for collection and use limitation, purpose specification, data quality, card holder rights, security and the existing legal frameworks;
- that finally the safety and reliability of the smart card should be guaranteed,

also in view of:

- the European Directive 95/46/EC on the Protection of individuals with regard to the processing of personal data and the free movement of such data;
- the European Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunication sector;
- National legislation in the Member States based on these Directives;

without prejudice to:

- the provisions of the national legislations and other formal and substantive legislation concerning data use and disclosure from the point of view of the smart card- related databases;
- (international) consumer conditions which have been set up in consultation with representative organizations;

and in so far as not yet provided for in sectoral privacy codes of conduct drawn up by representative organizations; The smart card constituency of the European Union subscribes to the following Rules of Conduct for the protection of the interests of the consumer, which includes his personal data with regard to the use of smart cards in both the public and the private sector.

5.5 Cost Management and Transparency

The best business models comprise simple propositions that provide a “win-win” situation for businesses and their users. This stands for all business models across all sectors. Business model development to underpin multi-application smart card schemes represents a strong challenge to this truism of simplicity. Within these schemes, suppliers (application providers) are numerous, users “consume” a variety of different applications (which can change over time within a dynamic environment), and schemes are managed to achieve a range of financial, social and public policy objectives.

Any participant in the system must be convinced of the benefit he will derive, and also be aware of the direct and indirect costs incurred.

This applies to users and all partners in a card scheme. Most investment decisions rely on the cost analysis as a significant factor in the final decision. The business case is incomplete without a well-documented section on costs. Therefore, when integrating a Multi-application System a life cycle cost estimate should be calculated for each alternative. This total cost should be expressed in constant monetary units and used to measure the value of purchased goods and services in terms of the price level in a given base year. The basic steps include:

CWA 15535-1:2006 (E)

- Identifying what the system will cost, the expected revenues for each partner, how the system will be financed, the expected other benefits and how risks and benefits will be shared among the participants.
- Considering the advantages and disadvantages of alternative management and financing options
- Finally creating/understanding the business case for each stakeholder partner

Because there are both subtle and large differences among the partners, a single model for determining the cost of integrating a MA system cannot be recommended:

- Certain Card Scheme Operators will have the capacity to include the cost of multi-application integration in their IT budgets, while others may not.
- Some will have the capacity to implement and maintain the system with their existing personnel, while others will have to outsource such expertise.
- Some Card Scheme Operators may already have the secure facilities needed to house the background sub-systems, while others will have to construct such a facility.

Even if the starting conditions are very different between Card Scheme Operators, commonalities sufficient to estimate the financial impact of the investment remain:

- A common factor is to decide whether existing operator resources can be leveraged for multi-application system integration and maintenance or whether these will have to be purchased or contracted out. The resource requirements associated with the planning, deployment operation, and on-going maintenance of the infrastructure must be defined.
- The software upgrades and purchases that will have to be made as a result of this implementation also factor into the overall cost.
- Policies and procedures necessary to support external users or external organisations must also be defined. The results of these and other analyses can help Scheme Operators budget for new MA system infrastructure costs as part of the normal IT upgrade budget.
- If the PKI is required to be interoperable, it is essential that a standards-based product and vendor be selected. Without the use of standards, interoperability problems may arise later and would be costly to correct. Liability protection is essential in many cases, especially when interoperability is required with external users or other PKI domains.
- Training costs for both end users and administrators may be substantial and will be an on-going cost that declines as the MA system knowledge within the user community increases. Other administrative costs like helpdesk and end entity registration procedures will be on-going and should be included in the cost.
- When considering the end user processes and interfaces, the “keep it simple” *dictum* applies

5.5.1 Business Model versus Evaluation

There are many tools open to the decision-maker in evaluating (*ex ante* and *ex post*) investment decisions. These can be monetary based, with all effects measured in monetary units (e.g. cost benefit analysis) or, where monetary effects cannot be measured, multidimensional (e.g. multi-criteria analyses). These evaluation techniques are complex tools, often resource intensive in their own right, yet have an important role within decision making.

These notes outline the structure and lessons learnt in determining a *financial* business model (termed business model). As such, it does not trade off the costs of the project with the monetary value of direct and indirect impacts of multi-application schemes. Instead, it outlines the steps taken within the Project to model a financially sustainable scheme (over 5 years), built around costs to establish and run the scheme, the revenues which can be achieved, as well as some very direct cost savings.

This does not preclude further (monetary/multi-dimensional) evaluation based work, though the business model approach presents a pragmatic approach to developing schemes, with the assumption that subsequent private sector applications on the card will make their own financial decisions to take part.

In developing the model it can become difficult if the Scheme is conceptualised as a formal organisation/partnership/joint venture, with it's own revenue apportionment rules and requirements. Rather, the MMUSST approach envisages the Scheme as merely a number of costs that had to be met, and revenues and savings that may be achieved. Building up from this basic level, individual partner organisations can disaggregate their own direct costs, revenues and savings, and potential indirect costs/revenues to make their own cases for involvement. This data can then be utilised in developing the formal partnerships/organisation and its financial apportionment rules.

5.5.2 Application Assumption

In establishing a business model for the Scheme it is necessary to make some initial assumptions regarding the application portfolio on the card. The SmartCities business model started with the following applications:

- Library borrowing;
- Leisure membership;
- Retail loyalty;
- Concessionary bus travel;
- Commercial bus travel.

This represented a mix of private sector and public sector applications. It is recommended that the initial assumptions reflect the probable mix in the first two years of the scheme, yet also recognise the potential for some private sector applications, to help assess potential revenue streams.

5.5.3 Model Driver Assumptions

Assumptions have to be made with regard to certain model drivers. These are dynamic variables that will determine the costs/revenues of scheme operation. As they are crucial in the financial analysis it is recommended that high and low estimates are made, and wherever possible, data is based on real experience¹⁰.

¹⁰ SIG members can provide useful data.

The MMUSST model is driven by changes in inputs in a number of these variables. The key drivers are:

- **Charging Variables:** application charges (if any) made to cardholders (by resident/non-resident number estimate of take-up)
- **Revenue Variables:** revenues paid to the scheme for management of certain applications (eg loyalty scheme)¹¹
- **Card Mix/Cost:** mix of card technology (and therefore cost of cards to the scheme) in circulation
- **Replacement/wastage:** cost to the scheme.

5.5.4 Business Model Financial Inputs

Data Elements

The key data elements of the model are listed below. The model should contain robust estimated cost/savings/revenue data for these elements:

- **COSTS: Set-up costs:** IT infrastructure; Card Production Facilities; Bureau; Set-up staff
- **COSTS: Operational:** consumables; maintenance; smart cards (mix); replacement cards
- **REVENUE: Revenue/income streams:** loyalty scheme revenue; handheld reader revenue;
- **SAVINGS: Potential savings:** direct quantifiable savings to partners (investors) from the scheme (e.g efficiency savings realised from move to centralised smart card production facility).

Additional Elements

The inputs described above give an indication of generic model inputs. However, model builders will need to assess what scope for other revenue/cost elements there are within their scheme. For example, the SmartCities Southampton scheme considered:

- Data warehouse costs to the scheme
- Data analysis: projected revenues from sale of anonymised data
- Costs (revenues/savings to scheme) of financial banking partner

Due to the complexity of the model, and the many assumptions that must be made, it is important to consider a range of scenarios for the development of the scheme. These should represent high/low cost/revenue mixes, and can subsequently be presented to decision-makers. In addition, scenarios could represent certain application biases (e.g transport/mobility led smart card). Scenarios under consideration within the SmartCities Project were as follows:

- **Baseline scenario:** Council core applications only (library, leisure, proof of age)
high cost/low revenue

¹¹ The revenue derived from selling space on the chip to application providers will naturally be limited by the space available on the card. Schemes and models should therefore consider the proportion of applications carried within the card and the back office, as this will determine the "ceiling" to application revenue. Dynamic loading of applications as well as the provision of core common applications on the card (eg e-purse) are related considerations.

- City Scheme scenario: Council applications above plus toll bridge, retail loyalty, concessionary bus, commercial bus route, University applications *high cost (expansive scheme)/medium revenue*
- Mobility scenario: commercial bus application, rail application, Integrated Transport Standards Organisation (ITSO) application
- *transport led: medium cost/high revenue*¹²
- Commercial scenario: sponsorship, Southampton Football Club ticketing
- *medium cost/high revenue option.*

The above discussion has provided pragmatic advice on the development of a business model for a local government Card Scheme. There are many time and place specific variations to the model, though the above provides a useful generic approach.

Business models behind such technological innovations will be constantly developed and refined. It is important to recognise that smart card scheme technology (card infrastructure and back office developments) and digital identity open up a range of new modes of service delivery and customer relationships and consumption. These developments may be hard to quantify, though should be addressed in the future.

These new models must include reference to the development of digital identity, and include scenarios built, not only upon smart cards as currently widely understood (i.e plastic, credit card sized cards), but also other media and mobile devices.

Successful business models are built upon a “win-win” principle for businesses and their customers. The real benefits of city card schemes, to businesses and users alike, may be realised by the business process improvements derived from new, cheaper and more effective ways of delivering their services which foster new ways of consumption. If schemes are merely seen (and measured) as technology projects which simply replace paper tickets with electronic tickets, some very real revenue and benefit areas will not be realised.

¹² Potentially high revenue given the privatised transport network in UK