Open Smart Card Infrastructure for Europe

V2

Volume 5: **Multi-applications**

Part 1: **Legal Framework for multi-application cards and systems**

Authors: **eESC TB7 Multi-application Smart Cards**

NOTICE

This eESC Common Specification document supersedes all previous versions.

Neither eEurope Smart Cards nor any of its participants accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this document.

Latest version of OSCIE and any additions are available via www.eeurope-smartcards.org and www.eurosmart.com. For more information contact info@eeurope-smartcards.org.

EDITED BY: LORENZO GASTON

Table of Contents

EXECUTIVE SUMMARY

The diversity of the functions that a multi-applicative card can support, the different regulatory status of the industries issuing these cards, and the multiplicity of entities and business relationships involved in its operation, make the multi-applicative card a complex object from a legal point of view. This deliverable is intended to provide some insight concerning the following issues:

1. Identification of the Legal Nature of the Card
2. Identification of Legal Issues specific to the Multi-application Card
3. Analysis of the Current legislation and Contractual Practices relevant for Smart Cards
4. Identification of Scenarios for Multi-application Practice: How to define some rules of « good practice » to help Card Issuers to feel comfortable with the legal consequences of disputes resulting from multi-application card anomalous operation.

NOTE: Legal issues such as specific Multi-applicative e-Privacy concerns and Tax management for e-commerce transactions are out of the scope of this document.

1 BASIC PRINCIPLES

1.The Objective of the TB7/WG2 is to provide guidance for a possible legal framework regulating the operation of the multi-application card business cases identified by the TB7/WG3:

Case 1.Multi-application card not issued by a financial institution
Case 2.Multi-application card not issued by a financial institution with an e-purse
Case 3.Multi-application bank card (issued by a financial institution)
Case 4.White Card

and leading to « good multi-application card management practices »

2. These four different operational scenarios may be implemented with an Intersectorial Multi-application Architecture to be specified by TB7/WG4. Depending on the nature of the applications resident in the card, specific signature services (e-signature) must be provided by the System and will be liable to the specific legislation supporting this technology (burden of proof law). E-signature is specially relevant for electronic commerce support, payment orders and agreement on on-line concluded contracts.

3. The Multi-application System is defined as the hardware and software Infrastructure which enables the management and operation of the multi-application card. It is made up of Server Computers, Telecommunication Networks, Terminals accepting cards and the multi-application cards themselves. The Multi-application **Scheme** refers to the legal entity that operates the Multi-application System.

4. The Multi-application Scheme is a business partnership of different organizations, playing one/several roles as defined by the business model. This multi-application scheme is usually led by the Card Issuer, but other models are also possible. The commercial relationships between the Scheme's partners are subject to contract agreements

5. The Multi-application System is run through a cooperative effort of several stakeholders, each one ensuring one or several roles within the System. A role consists of a set of predefined functions required to provide a service to either the cardholder or the other stakeholders.
Basic roles in a Multi-application Scheme include:

1. The Card Issuer
2. The Service Provider
3. The Application Provider
4. The Registration and Certification Authority
5. The Card Operator
6. The Cardholder

Several of these roles can be carried out directly by the same organization or subcontracted to a third under the entitled organization responsibility. 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 again other services to its environment.

6. The contracted services are provided by the Service Provider after explicit selection and subsequent activation of one of the applications resident in the card by the Cardholder. This activation initiates the corresponding transaction which is executed under the control of the data resident in the card. These data (usually cryptographic keys) are also used to certify the transaction. The certified data transaction can later be identified as being legitimate by the application provider and any other entity involved in the transaction.

7. The set of distributed data, partially stored in a card file, owned by an application provider, which are required to:

(1) Initiate a transaction that when successfully completed renders a pre-defined service to the cardholder with or without modification of the card file data and/or
(2) Generate and store a digital proof of the transaction

is known as Card Application.

8. In some scenarios, the transaction requires access to other data resident either in the card memory or a different device, but owned by a third party. The use of the non-proprietary data is subject to a previous contractual agreement between the owner of the

data (usually another application provider), the Application Provider and the Card Issuer responsible for the Security Policy of the card. The security policy is supported by the set of hardware and software mechanisms implement in the card after a Risk analysis. The security policy provides a pre-defined level of protection to the sensitive data resident in the card.

9. The fundamental equation is the following: Providing more freedom to the cardholder involves a greater financial risk for the Card Issuer (extra-cost for the Card Infrastructure. This increased security risk linked to the card extra-use, card security mechanisms to be implemented which add to the procuring cost) is to be quantified. On the other hand, the multi-application card is expected to be a source of extra-revenue for the Card Issuer. A compromise must be found to enable the Card Issuer to set the limits of the liability defined in the contract with the Cardholder.

10. Some of MA card cases identified in #1 (payment cards) are already operated under sectorial legislation, which is specific to each member state depending on the nature of the payment card commonly accepted (Credit, Debit, Debit/Credit or E-Purse), the national regulation applicable to the financial sector and the card technology currently used.

11. A legal framework provides the regulatory mechanisms necessary to protect the interest of the players involved and to ensure the smooth and secure development of the market. From a competitive perspective, barriers to entry resulting from legal regulation must be kept to the minimum necessary not to hamper innovation. However, in the past EC has recognized the need to protect the cardholder, felt as the weakest partner in card-based schemes, specially in the payment industry. As an exemple, Recommendation 97/489/EC was issued by the EC concerning the the transactions carried out by electronic payment instruments and, in particular, the relationships between cardholder and card issuer The multi-applicative card involves active participation of the Application/Service Provider. A balance between the interests of these different players has to be found.

2 OBJECTIVES AND METHODOLOGY

1. To identify recommendations to set up a legal framework stimulating Card Issuers to start the secure deployment and operation of the Multi-application card This deliverable is in no way intended to recommend a restricting frame for players, but just a minimum of rules to provide trust. This approach is justified because:

    a. There is no rational ground to recommend a restricted frame setting when no specific legal environment exists at this time for the MA card
    b. The main TB7 objective is the promotion of the MA cards and systems. A restricting frame is felt to adversely impact industry initiatives.
    c. TB7/WG2 is in line with the unification policy driven by EC legislation intended to minimize the legal frame, and just to be limited to the strictly required measures to enhance trust demanded by the industry.

2. To provide legal grounds to sustain the identified business models for the MA card identified by TB7. In particular TB7/WG2 shall pay special attention to the White Card Case. In addition, TB7/WG2 shall support the Service Provider and the Cardholder rights in a way compatible with the business model of the Card Issuer. The business objective is to stimulate the Application Providers to create and market new card applications, by protecting them from excessive dependence on Card Issuer.

3. To provide a consistent frame based on existing laws, extended when required to consider specific characteristics of the multi-applicative environment. This frame should be flexible enough to support a diversity of scenarios Starting points include the existing laws and Directives in complementary areas as well as for specific cards (financial)

4. To promote **trust** for the three main participants required for the MA system operation, Card Issuers, Application Providers and Cardholders, by taking into consideration and making compatible to a maximum extent their legitimate rights and business interests. In particular it is important to fix the Card Issuer Liability.

5. To guarantee the cardholder appropriate claim management procedures and fair contractual terms when disputing a card transaction.The basic assumption is that any of the contracting parties is only willing to accept its responsibilities when the responsibilities and duties of the other parties are clearly set and accepted and the proof of their accomplishment can be provided.

6. Finally, TB7/WG2 intends to contribute to the building-up of a consistent unified legal frame for e-commerce which can be easily transposed into national laws and provide effective protection and trust to the card industry. The authentication and burden of proof provided by the smart card seems to match the security requirements for e/m-commerce business. In addition, a smart card compliant with the e-Sign requirements has the legal support of the European Directive on Electronic Signature transposed in the national legislations.

In order to achieve the aforementioned objectives the following methodology shall be followed:

1. Identification and Analysis of the existing and relevant applicable legislation
2. Identification and Analysis of the existing standards for implementation of European Directives and Recommendations
3. Analysis of the Contractual Terms and Conditions currently applied for the provision of mono-applicative cards
4. Selection of multi-applicative scenarios requiring contractual support based on TB7/WG3 models
5. Investigation of ways to extent the existing contractual practices to the multi-application case by analizing the basic operations and the roles involved when performing a multi-applicative card transaction

6. Initial Draft Circulation for Comments according to point 7.
7. Initial evaluation of the Draft Recommendations in relation to:
    - Cardholder Protection (cardholder protective measures compatible with business models, effective e-privacy protection and real empowerment for application choice by the cardholder)
    - Support of Stakeholder Business Models (Liability Share, Appropriate Risk Apportionment)
    - Card and System Architecture Design
    - Consistency with current applicable legislation
8. Validation by major multi-applicative card issuers representating the Card Industry
9. Final Deliverable Publication.

The above objectives can be summarized as follows:

1. To create a Trust Environment for Cross-Industry Business agreements implemented through the issuance and operation of a multi-application card in a way that is independent of the specific Card Issuers and their partners in the MA scheme
2. To promote informed and effective relationships between Cardholders and Card Issuers as well as between Card Issuers, Service Providers, Application Providers and any other part involved in the operation of the multi-application scheme
3. To describe guidelines for good practice and service

3 DEFINITIONS

ACCEPTOR: Entity which accepts the MA card as a counterparty for the provision of a service or goods to the cardholder. Several scenarios are possible:

- The card generates a certificate which allows the acceptor to claim for a settlement which will cancel the debt created by the provision of the goods or service.
- The rights for the provision of the goods/service have already been acquired and the card prooves the right of the cardholder to obtain the service/ good from the acceptor. In this case the acceptor has to sign his conformity by writing some data into the card. This data shall then be read out by the acceptor, when the cardholder wishes to use the pre-acquired rights. (Static authentication in EMV / Transport Card)
- The card allows for cancellation of the debt created by the provision of the goods or service

ACQUIRER: Entity (usually a Bank, in this case referred to as Acquirer Bank) having signed a contract with the Acceptor, by which it accepts the transactions certified by a multi-application card and in exchange charges the Acceptor with a commission previously agreed. Therefore there is competition between Acquirers to capture acceptors (merchants or service providers)

APPLICATION PROVIDER (AP): Entity owner of a card application. The AP can in principle market their applications by issuing their own card or negotiate with the card issuer the downloading of their applications in an existing card. In the second case, the Card Issuer and the Application provider are linked by a contract. The Application provider takes a business risk by deciding to load their data into the card and in turn the card issuer takes a risk to accept the loading of data potentially jeopardizing the security of the card.
In a competitive scheme, the APs must have a choice between different CIs to negotiate the best terms for the loading of their applications.

CARD ISSUER (CI): Entity proprietary of the Card. It negotiates the rental of some memory space to other Application Providers. The multi-application card is a device allowing the Card Issuer to gain an additional revenue. The CI in particular defines the Security Policy of the card and supports the cost of the card Certification Process. The Card Issuer can block the card and then originate a financial loss to the other AP.

CERTIFICATION AUTHORITY, legal entity in the MA scheme, usually under the direct control of the Card Issuer in charge of certifying the partners themselves as well as the devices involved in the operation of the MA system as being compliant with the Security Policy of the Multi-application Scheme.

The CA is also an element of the marketing strategy of the Card Issuer, which in addition might facilitate major freedom for the provision of applications by the cardholder.

DOMAIN OPERATOR Entity subcontracted by the Card Operator to manage some card resources. It aggregates content and services from third-party partners and provides these services directly to their subscribers.

APPLICATION OPERATOR: entity that can grant access to a card application or to some of their proprietary data. The Application Operator can be either the Application Provider itself or a third party which exploits the Application on behalf of the Application Provider. The AP loads into the card the list of AO that it trusts. An AO may be a Service Provider with a business relationship with the AP. An AO might also be an Application Loader, in charge of application downloading on behalf of an Application Provider, a set of application Provider or the Card Issuer itself.

CARD OPERATOR Entity that manages the multi-application scheme on behalf of the Card Issuer. In this context, management refers to the support of the following system functions:

Card Management System of the MA Scheme
Cardholder and Application Provider Support
Data Capture and Exploitation
Terminal Management System when applicable
Authority of Certification control

All these roles can be directly played by the Card Operator or subcontracted to a third party under its direct control.

CLOSED MULTI-APPLICATION SYSTEM: In this context refers to the Multi-application scheme where the Card Issuer directly authorizes the Application Providers to load their application, whilst being the only entity having a billing relationship with the cardholder. For mono-application cards, the term refers to schemes where the Acquirer and the Card Issuer are the same entity (eg American Express cards)

OPEN MULTI-APPLICATION SYSTEM: In this context refers to the Multi-application Scheme where an Application Provider can negotiate with an entity other than the Card Issuer (including directly with the Cardholder) the downloading of applications in the card.
For mono-application Cards, the term refers to the scheme where the Acquirer is not necessarily the Card Issuer. A Clearing and Settlement infrastructure is then required to manage the payment transactions resulting from the operation of the card

MULTI-APPLICATION SCHEME: Refers to the legal entity in charge of the operation of the multi-application system. It is usually led by the Card Issuer. Initial partners negotiate contractual terms and conditions (liabilities, functions, resources, fees). The scheme is dynamic in nature: New Incomers (AP) can come into the scheme whilst former partners can leave it.

MULTI-APPLICATION SCHEME MODEL Model for the operation of the multi-application scheme usually designed by the Card Issuer. It includes the roles to operate the system, the functions provided by each role, and the interfaces linking the different functional blocks of the system.

MULTI-APPLICATION SCHEME PARTNER Any legal entity playing a role in the multi-application scheme.

INFORMATION SOCIETY SERVICE any service provided through a telecommunication network, against an agreed price and means of payment, at a distance, on request of an individual or legal entity. In our context, ISS applies to eg, the downloading of an applet into a multi-applicative card from a Web Server managed by an Application Provider.

TRUSTED RELATIONSHIP An entity A trusts an entity B when B behaves exactly as A expects. The Security Policy of the Card reflects the trust relationships between the Application Providers of the Multi-application Scheme.

TRUSTED THIRD PARTY Legal entity recognized by all the participants involved in a transaction enabled by the card and who initially do not trust each other ("enabled" because the card grants the required guarantees to all the participants necessary to conduct the transaction). The TTP guarantees that the transaction is performed following a pre-defined protocol, and that all the elements certifying the transaction are produced in a timely way with the required level of confidence. One of the responsibilities of the TTP is to provide the Burden of Proof. From a practical point of view, the TTP cannot forge any element of the transaction without being identified. The basic assumption is that this proof cannot be built by the TTP itself. Any attempt at collusion between the participants and the TTP can thus be identified.

WRONGFUL CARD ACT: Any actual or alleged act, error or omission, misstatement, misleading statement, neglect or breach of duty committed in connection with the provision of multi-applicative card services

4 ECONOMIC RATIONALE FOR LEGAL FRAMEWORK

4.1 Introduction

The economic models currently applied supporting the card operation requier some equity between the card partners (card issuers, service providers) to enable external network effects to work. The multi-application card represents an extrapolation for each card resident pair (Card Issuer, Application Provider) of the external network effect observed for the payment card.

Effective competition between CIs for the provision of applications from different APs is generally recognized as a condition for profitable operation of the MA system and effective payback for initial investment by the Card Issuer. This means that even if the card issuer takes up an oustanding position within the MA scheme, the regulatory framework should enable the AP a real negotiating capability and protect the SP against abusive contractual clauses In this context « abusive clauses » means:

- Excessive Interchange fees /Commissions/ Indemnities
- Risk apportionment and control
- Liabilities and Guarantees
- Execution Conditions
- Cancellation, Resolution and Repudiation of Agreements

The objective is the development of a stable « Application Provider Market » providing Card Issuers with an Offer of Value Added Services for the Card Issuer's customers. This means that we dissociate the « card-community » (cards issued by the same entity) from the « e-community » (cards accepting the same application, issued by different entities). An application provider may then operate competitively between different multi-application schemes willing to offer its application to their cardholders.

4.2 Business Models and Legal Framework

1.The MA scheme is built around three main players: Card Issuers, Service Providers and Cardholders, with other participants ensuring supportive roles as defined in

§. The set of legal relationships linking the entities participating in the management and operation of the Multi-application card system is the Multi-application Scheme.

2. The MA scheme represents a legal system since:

- It allows for multilateral/bilateral contractual agreements between different participating entities
- These contractual agreements within the scheme are independent: The nature of a contractual agreement between two entities impact the nature of the contract between any of the contracting parts and a third
- It is dynamic: The members of the system, legally organized as a MA scheme, can change over time, as well as the roles they play

3. The operation of the Multi-applicative system generates a flow of value between the members of the system.in compensation for the services provided as contractually stated. The payment terms and conditions as well as the modes of payment are outside the scope of the present document. Depending on their nature these payments be subject to the applicable legislation. Tax management linked to the eventual e-commerce activity of the system over the Internet are also outside the scope.

4. Business Models may be centered on the Card Issuer, the Service Providers, the Cardholder or any combination of two out of the three of them. These different interests involve shifting and limiting the respective liabilities between the Multi-applicative scheme partners.

5. A Business Model focused on the Card Issuer will shift the responsibility to the other two sides. That approach shall be contractually formalized. Because the co-operative effort required to launch and operate the MA scheme appears to be asymetric, this chapter identifies the major issues and expectancies from each of the major players.

6. Three basic operating modes of the multi-application scheme can be differentiated:

- Only the Card Issuer has a direct business relationship with the cardholder. The CI charges and bills directly the cardholder following terms and conditions contractually agreed. No contract is set between the Cardholder and the Application Providers. This system is comfortable for the Cardholder but empowers him less for personalisation purposes. Card Issuer and their agreed AP are linked by bilateral private agreements. The Card Issuer is the only player responsible from the perspective of the Cardholder.

- The Application Providers are authorized to bill the cardholder directly following bilateral terms and conditions. This model is suitable for the Domain Service division of the card resources.

A hybrid model, where some AP have direct billing capabilities with the cardholder whereas others do not

7. The Card Issuer is usually expected to manage and own the Multi-application System and, then, to define the corresponding legal scheme. But other models are possible: A joint venture between different stakeholders, each one playing a role within the scheme. This joint venture shall in particular define (1) the terms and conditions for the admission of a new incomer as well as (2) for a former member to leave the scheme and (3) governing the rules with any external entity to the scheme

4.3 Initial considerations for the multi-application scenarios

CASE 1:MULTI-APPLICATION CARD NOT ISSUED BY A FINANCIAL INSTITUTION

From a legal point of view, four different situations are relevant

1. The MA Medical Health, because of the ePrivacy concerns and specific protection for personal data.
2. The Multi-applicative SIM card, because of the importance of the SIM card for the Card Industry and the relevant business model for the coexistence of a payment application within a SIM card.
3. The MA with Betting Applications, because Gaming is outside the Scope of the Directive on Electronic Commerce and subject to its own legislation
4. The MA Identity Card, because as it is issued by a Public Administration, it is subject to Public Law.
5. The MA intended to support Multimedia access applications for the legislation relevant to copyright protection.

CASE 2: MULTI-APPLICATION CARD INCLUDING AN E-PURSE NOT ISSUED BY A FINANCIAL INSTITUTION

General Discussion

The integration of an e-purse changes the legal nature of the payment card, which becomes the secure repository of electronic money, and no longer a tool for mobilizing funds from a bank account to which the card is associated.
Irrespective of the other applications resident in the card, the card is subject to the applicable law for e-money.

The reasoning can rationalised by interpreting the concept of off-line transaction.

CASE 3: MULTI-APPLICATION CARDS ISSUED BY FINANCIAL INSTITUTIONS

Several scenarios for this business model can be identified around a primary payment application:

1.Multi-application card supporting different Payment methods
2.Multi-application Card supporting one/several Payment methods and application for the provision of only Financial Services

1.1 By Financial Application Downloading
1.2 By Bank IAS module

3. Multi-application Card supporting at least a Payment application and other non-financial applications

Each of these cases, is related to a particular legislation framework

Payment Bank Cards Ownership

Card ownership is an important issue when defining the legal framework for cards. The ownership of payment cards issued by financial institutions has produced extensive discussion amongst lawyers and researchers in the past.

Even if it is suggested that the card remains the property of the bank, this is probably not true. The contentious issue is the right of the card issuer to block card usage.
We could say that by blocking the card, the Bank do not forbid the usage of the card, (it actually cannot do this because the card remains the property of the holder), but the Card ID is put on the Revocation Card List. That is a pre-emptive procedure for the bank to stop someone using the card.

From the bank point of view, the card is the portable object which is delivered to a cardholder, and which acts as TTP (the Issuer Bank authorization is the guarantee for the merchant bank (acquirer) that the payment shall be on presentation of the transaction certificate signed by the card). The Requester (the cardholder) requests the Decider (the Merchant) to pay by card. From the merchant's point of view, the card is the representative from the Issuer Bank,as long as certain verifications take place (Validity, Card Authentication). These verifications serve as the Payment Authorization,
It is clear that the card final objective is to obtain a commitment for settlement from the Issuer Bank. From this point of view the card can be considered as owned by the Issuer.

We can consider whether the Issuer grants a Token (or rather the data element required for the card to create the token, which is the proof). On presentation by Bank B of the Token signed by a card issued by Bank A. What may happen is that the payment was accepted by the Issuer (or the Merchant) without authorization request by the Issuer (to save communication costs). Probably the Issuer may refuse the payment in this case. This is the concept of Risk Policy by the Merchant (and of its Bank).

The Provision of on-line financial services

1. Protection against Fraud

The use of the Internet has many advantages for the provision of products and financial services as well as to capture new clients. However, usage of the Internet distribution channel brings new risks of fraud and therefore puts some legal constraints on the effective protection of the parties involved.

An interesting case is that of broker-dealers providing customers with the ability to place trades through the Internet. These on-line trading systems were introduced in 1995. Since then they have grown dramatically and simultaneously there has been a surge in investors' complaints about delays and errors in processing on-line orders.

On-line brokers face similar legal constraints in connection with

1.Obligation of Information provided to Customers

Identification of Financial Service Providers (FSP)

The FSP is responsible for the implementation of on-line tools, enabling the Multi-application Cardholder (MC) to identify and verify the capacity of the FSP to propose these services and specially in handling customer trading volume

Execution of Customer's transactions

The FSP is responsible for providing to customers on-line information about how orders are executed, how the margin works and the possibility of system's delay, including notification of operational difficulties

Terms and Provisions for downloading of Digital Information

Case 1 Downloading of Application Information: This is a generic term covering different types of information useful for the customer, and in particular, real-time financial information, requirig integrity and authentication protection.

Case 2 Downloading of Executable Application Software, the provisions are the same as those defined in §, *Customer Consent for Stock Purchase*

CASE 4: LEGAL FRAMEWORK FOR A WHITE CARD SCENARIO
Card Issuer: Cardholder
Two different scenarios

1. Card Sold with an IAS module compliant with GIF Specification (for example)
   Liability of the IAS provider can be engaged.
2. Card Sold with just the ability to support the IAS

5 INTRODUCTION TO MULTI-APPLICATION CARDS

5.1 Mono-application vs Multi-application Cards

The mono-applicative card is characterized by a unique application personalized in the card memory. The card hardware and software resources are designed for the efficient and secure provision to the cardholder 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 often make a single program called the mask.

By contrast, the multi-applicative card is characterized by:

1. The coexistence of several applications on the same support which can be selected and executed by a card software stack ideally irrespective of the applications
2. The dynamic evolution of the card content, making possible the independent managemenent of the card and of the resident applications
3. The cooperation between applications, to grant a final service to the end-user. This cooperation, is a potential source of contentious situations to be minimized by an appropriate design of the card architecture.

This operational flexibility raises specific security and performance problems, which have an impact on the identified risks and the subsequent contractual clauses linking the entities involved in the design, personalization, issuance and operation of the card.

The sharing of liability between the Card Issuer and the Service Providers is a fundamental legal problem in a multi-applicative scheme. The agreed liability can only be assumed when the card security functions are trusted by each stakeholder. It follows that the card architecture and the protection profile required for the MA card are the grounds for the acceptance of any legal responsibility by the contracting parts. All the stakeholders must trust the security functionalities of the card, which must guarantee the secure execution of any application (as if it was the only resident application in the card) with no leakage of information other than that explicitely enabled.

This confidence is obtained from a certification process of the card by an independent organization which actually is a Trusted Third Party between the Card Issuer and the

Service Provider (with no business case for issuance of their own card, but looking for a card issuer operating a card held by a large community)

The MA cards have the business objective to increase the total number of transactions for any of the Service Providers compared with the figures that could be obtained by the individual card's issuance (Synergy between card applications). Obviously, this expected extra-revenue must not be counterbalanced by an increase in the number of claims and the subsequent economic losses because of increased fraud (Service granted against no revenue to an individual not having the required rights).

From the design point of view, specific counter-measures on the card hardware and operating system have to be implemented and their efficacity demonstrated by a certification process. This costly procedure is financed by the Card Issuer and then payed-back by an (1) Extra cost of the card sale, (2) a higher potential to capture interesting AP and (3) the ability to transfer the responsibility to a third party (possibly the cardholder) whilst limiting their own liability.

After setting out these points, it remains that the Specification of Protection Profiles for cards supporting critical applications is the responsibility of eEurope/SCC/TB3 and, as a consequence, out of the scope of the present document. However, some guidance to perform Risk Analysis is provided in Appendix 3. For further details please consult the standard ISO 13335.

5.2 Modes of Operation of the Multi-applicative Card and Legal Support

The basic assumption is the following: Organizations will issue cards with much more processing power and storage space than is required for their own purposes. Then the remaining memory space can be:

Either proposed to other organizations, in a rental contract for the loading and exploitation of their data (on-card application) and those organizations become business partners of the Card Issuer Organization

or the cardholder is given the opportunity to personalize the card with the content of his choice from a third organization, not necessarily a business partner of the Card Issuer. The card can then be used in schemes operated by different organizations

For the broadest operational capability of such a system it is necessary that the research, selection, downloading and later execution of the on-card application be done through a series of standard messages exchanged between the MA System components. The structure,coding and integrity of these messages must provide the different players with digital storable proof that the transaction has taken place as planned.

Depending on the Multi-application scheme arrangements, different procedures and functional modes of the multi-application system infrastructure card are possible. Because of the complexity of the MA System and associated operational costs, the delegation of the contractual obligations between the different partners is expected to become a common practice. However, delegation support has a direct impact on the system design, requiring a clear definition of the interfaces for interoperability, the harmonization of the protocols executed as well as the implementation of synchronisation mechanismes, to guarantee the consistency of real-time information, available in the different databases managed by the System Stakeholders, Card Issuers, Service Domain Operators, Application Providers and Certification Authorities.

The legal concept of Delegation

The legal concept of Delegation involves the following roles: *

1.The Delegator individual: Transfers one obligation of service to the Delegated
2.The Delegatee: Juridicial entity having an initial right over the Delegator, that is now transferred to the Delegator
3.The Delegated entity, has an obligation towards the Delegatee after the Delegation takes place.

Example Delegation in the Payment by Card

When authorizing the payment, there is a Delegation of the Obligation of Payment from the Cardholder (Delegator) to the Issuer Bank (Delegated Entity). This Delegation is said to be « promitori », because it definitively cancels the obligation of the Cardholder in front of the Merchant. The Cardholder obligation is shifted to the Card Issuer. By accepting the card, the Merchant implicitly accepts the Issuer Bank as its creditor. The Merchant's Bank (The Acquirer) will therefore claim the Issuer Bank for the amount of the transaction concluded with the Cardholder, with or without previous authorization by the Card Issuer.

The Delegation applied to the Multi-applicative Card Management

Service Domain Operator

The Card Issuer can delegate some of his obligations to other partners of the MA Scheme

The Delegated Management for Application Downloading

The Card Issuer is the Delegator who delegates the obligation of the Application Downloading on the Application Provider (Delegated Entity)

The Delegatee/Creditor is the Cardholder, who has acquired a right to the application downloading, to be executed by the CI. The Card Issuer

The Delegated Management for Application downloading is not of « promitori » type, because in case of unsuccesful execution of the procedure, the Card Issuer is liable directly to the Cardholder, unless otherwise contractually stated.

In addition we should differentiate between:

2. Liability when the card is active: After card RESET and during the execution of a command/response pair of a card command, or during the WAIT state of the card (the card, is powered, it has been successfully identified by the external world and is waiting for a command sent by the Terminal)
3. Liability when the card is inactive, and the fraud takes place after data processing by the card. The transaction is over, but the data retrieved from the multi-applicative card can be used to forge another card or to initiate an illegitimate transaction.

5.3 Cardholder Responsibilies to the Service Provider

The Service Provider Offer

In several business models, the Service Provider is an intermediate player, marketing the services and goods produced by itself or more frequently by a third entity. The SP signs a contract with the Card Issuer. By this contract, the SP accepts to grant a defined set of services to the cardholder.

The SP may in turn, have commercial relationships with

(1) Digital Content Providers, willing to distribute everything in digital form from computer programs, text, data, online databases and audio/video works (graphics, images, photos, video clips, music, interactive games and web pages) usually subject to copyright or
(2) Merchants offering physical goods but marketing their products through a Web Site, as the additional/ only distribution channel

The SP acts as the visible partner of those entites for the cardholder. This means that the Service Provider may be liable for any damage/security flaw introduced in the card by the loaded digital contents of their representees. The liability is actually restricted by the provisions of the contract between the Card Issuer and the Service Provider.

The responsibilities of the Cardholder relative to the Service Provider, is dependent on the contract signed between the Card Issuer and the Service Provider, in connection with the specific method (application personalized in the card or not) jointly decided.

The Access to the Services by the Multi-applicative Card

This document proposes to differentiate the usage of the multi-applicative capabilities of the card following the way the applications are personalized and then selected by the cardholder.

The Services accesed by the Card can be delivered in three ways:

Case 1.On card presentation, either physically or at-a-distance, followed by the succesful card authentication, cardholder authentication, and optionally the retrieval and verification of Card Specific Information (ie a Certificate issued by a CA trusted by the Service Provider). However, this mode of operation is associated with the Multiservice card, rather than the actual Multi-application Card.

Case 2. By the requirement of the Service Provider to download its own application on the card.. Access to the Services requires then not only the card presentation, card authentication and cardholder authentication, ***but also the explicit selection of the application*** by the cardholder and, optionally, the execution of other security mechanismes defined by the AP.

Case 3. On card presentation, an application (the main application) is automatically selected by default. Any other application resident in the card must be explicitely selected by the cardholder. Case 3 introduces a hierarchy between the applications in the card. and the concept of ***Application Priority***. This case is relevant when the Card Issuer provides also its own application, which becomes the Main Application in the Card.

Rationale for the proposed classification

1. Cases 2 and 3 apply when the Service Provider wants to use its own security policy. In this case, this policy must be compatible with the Security Policy of the Card as defined by the Card Issuer.

2. Case 1 is compatible with the existence of an application on the card, usually owned by the Card Issuer

3. Hybrid schemes are possible: Resident applications can coexist with a Card Security Module able to provide a Service Provider with an Authentication generic service for the cardholder (requester of the service)

4. Case 2 is close to the Personal Computer mode of Operation, where all the applications are put on the same level of hierarchy in relation to the Operating System.The White Card is a specific scenario for Case 2, with no Card Issuer (The Card Issuer is the Cardholder).

5. The four business models identified by TB7/WG3 can be implemented using any of the above cases for Service Provisioning

6. In all the cases, the Card acts as a Trusted Third Party (TTP) between the Requestor of the Service (The cardholder) and the Decider (The SP have to decide whether or not to grant the service depending on the guarantees represented by the Card).

7. This concept of Prioritary Application is intended to facilitate the transition between the current Mono-applicative Card (Payment, SIM) and a first generation of real mutiapplicative cards around the main application which remains basically unchanged.

8. Case 1, is intended to empower the role of the Service Provider, by taking advantage of the Card as a means to access their services, whilst avoiding the costly process of Application Development and Certification

6 THE LEGAL NATURE OF THE MULTI-APPLICATION CARD

6.1 Legal Characterization of the Multi-applicative Card

6.1.1 A proposal for a legal definition

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

6.1.2 Specific Legal Characteristics of the Multi-application Card.

Personal: The rights represented by the card are not transferable to a third party. The multi-applicative card is intended for personal use, and the card supports the mechanisms to enable the card to provide services only to the entitled person.

Represents the Proof of Rights contractually acquired by the Cardholder, with the following 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 lose of the rights, just lose of the proof)

2. These rights are to some extent under the control of the cardholder who can add new rights to the card or cancel some existing ones, using the infrastructure that the Card Issuer has to put at his/her disposal. These rights can be granted by a third entity, the Application Provider.

3. 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 Revocation List publicly available.

4. These Rights can be totally cancelled by the Card Issuer according to the provisions of the Contracts agreed between the Card Issuer and the Application Providers and between the Card Issuer and the Cardholder.

5. The Rights granted by an Application Provider can be revoked by the Application Provider, following the provisions of the contract signed

between the AP and the Card Issuer and, optionally, between the AP and the Cardholder

Possibility of Priority Application Support: One of the applications can be activated by default, the other may require explicit selection and activation by the Cardholder

Variable Legal Nature, depending on the nature of the application being executed, referred to as the active application, and the legislation relevant for the active application

Share of Responsibility for Card Failure or Card Fraud between the Card Issuer, the Application Provider, the Authority of Certification and the Cardholder.

6.1.3 Responsibility linked to Issuance and Operation of the Multi-applicative Card

6.1.3.1 Responsibility of the Certification Authority (CA)

The CA is in charge of the issuance and distribution of the Cryptographic Keys and associated Electronic Certificates required for Cardholder Authentication and Electronic Signature Purposes.

Two situations can be distinguished:

1.The CA is one of the Stakeholders of the Multi-application Scheme.

The MA Scheme shall define its internal Registration and Certification Policy depending on the Authentication and Non Repudiation practices required by their offer of Applications. The CA shall be responsible for the implementation of this Policy. Because of the different security requirements of each application, the CA may implement different Certification Policies.

This/These policy/ies shall include:

1.Certification Practices Statement, including Pair of Keys Generation, Private Key Protection, Numbering of Certificates
2.Registration Procedures for Internal Users and Other Certificate Requesters like Application and Card Management Servers
3.Renewal Procedures for Expiring Certificates, including Archival Copies of expired certificates
4.Certification Revocation List Management, Periodicity
5.Certification Revocation Procedures on Card Issuer request
6.On-line support for CRL verification by Service Providers external to the MA scheme

2.The CA is an external legal entity to the MA Scheme.

The MA scheme shall define its own Certification Policy and then proceed to the choice of the appropriate Certification Authority after Verification and Validation of its Certification Practices Statement.

The contract signed between the Card Issuer and the CA shall specify obligations and rights of the parties. When either a Service Provider/Application Provider or the Cardholder disputes a transaction with a Certificate issued by the CA, and requiring legal adjudication, the CA may be required to submit evidence about its Internal Policy. Because Legal Dispute may occur after the Certification Expiry, the Card Issuer shall contractually require the Archival Policy concerning Expiring Certificates.

6.1.3.2 Duties and responsibility of the Card Issuer

In principle, the Card Issuer can only accept full responsibility if:

- It absolutely trusts the card technology by submitting the card to the appropriate certification process.
- It can control the content of any issued card and in particular it is the only legal entity empowered to block the card usage.
- Its Card Security Policy guarantees firewalling to the Domain Operators, if any, and to the Services Provides.
- It trusts the Certification Authority(CA) when the CAis not under its direct control.
- The MA system under which the card is operated enables real-time fast Card Revocation Management.
- There is an efficient synchronisation mechanism with the databases managed by the other business partners (Application, Card and Terminal Management Systems, according to MAS Prerequisites Deliverables of TB7/WG4).
- The responsibility of the other business partners is limited and well defined

6.3.1.3 Responsibility of the Service Provider

- Must be compensated for losses if the card is revoked by the Card Issuer
- Can only install their applets in a card with the appropiate Security. Mechanisms, in particular, guaranteeing that the confidential data stored in the card cannot be accessed by another entity, unless contractually stated.
- The applications they provide must be certified by a CA under the control of the Card Issuer or by the Card Issuer itself

- Can manage their own applications life cycle independently from the Card Life cycle using its own Application Management System, which is managed by the Card Issuer.
- The Card can protect its Property Rights on Digital Content stored in the card, or in another device secured by the card.
- In case of Delegated Management, the procedures must comply with the Security Policy of the Scheme.
- Shares responsibility with the Card Issuer in the case of wrong execution, non-execution and card failure during a transaction initiated with its own application.

6.1.3.3 Responsibility of the Cardholder

The responsibility of the Cardholder is not in principle different than in the case of the mono-applicative card.

6.2 The Right of Property of the Multi-applicative Card

6.2.1 The Problem

The card remains the property of the Card Issuer in so far as ownership is not assigned to the card holder. The basic assumption is that the Card is a document representative of a contract for a period of time from the card delivery. Once this contract expires, the Cardholder becomes the unique owner of the physical support. The problem to be solved is to specify to what extent the physical delivery of the card involves the transfer of property rights to the Cardholder. As usual, there are competing conditions when trying to make compatible the Control of the Card Contents by the Card Issuer and a major freedom for the Cardholder to personalize the card.

6.2.2 Scenarios for the MA Card Ownership

The Card owned by the Card Issuer

The ownership of the card is claimed by the Banks. However as discussed, there are solid legal arguments against this opinion.

1.The main right is the possibility to require the cardholder to give his card back to the Card Issuer without necessarily invoking a break of the contractual obligations by the cardholder. In practice, it is easier and faster just to add the Blocked Card Identifier on a Black List. In this case, the Cardholder may claim a new card at no extra-cost and even expect compensation because he/she can no longer exercise the rights contractually guaranteed. This point clearly highlights the difference between the rights and the proof of the rights. The rights cannot be exercised by the customer without their proof. This proof consists of presentation of the card along with the demonstration of the right to use the presented card (usually PIN code + Card Authentication and Verification by the Acceptor that the Card is not on a Black List).

2. The second advantage is the possibility to rent to a third entity some of the card resources (usually memory) for exploitation. This third entity may then directly bill the cardholder through the application.

3. Finally, the Card Issuer completely controls the content of the card, by certifying only the Application Providers compliant with its security and marketing objectives

The Card owned by the Cardholder

This approach is consistent with the objective of the multi-applicative card to provide a major freedom for the card content, and avoid the problems linked to the eventual co-issuance. A typical scenario may be the White Card.

The Joint Ownership Card Issuer

(To be analyzed)

7 GOVERNING LAWS & JURISDICTION APPLICABLE TO THE MA CARD

7.1 Generic Considerations

It is generally assumed that the legal regulation of an economic activity only makes sense when the volume of this activity has generated a number of conflicting situations between the economic partners which could be avoided with the existence of the appropriate legislation. From a purely business point of view, these conflicts are the source of economic losses. In one sense, the legal framework also supports the future development and the efficient operation of the economic activity it regulates.

In the current context, with actual limited deployment of multi-application cards, the lack of field experience may indicate that the requirement for legislation is not an urgent issue. However, experience with the mono-applicative card, specially for payment purposes, proves that despite the easy-to-use handling of the card, the result of the card operation is a complex mixture of economic relationships generating a series of rights and duties for all the parties involved.

These problems become more complex in the multi-applicative context, where the number of stakeholders and bilateral/multilateral relationships is thus increased. In addition the multi-application card gives rise to a series of specific issues related to card ownership, liability share and application priority. This legal uncertainty seems to hinder the growth of multi-application cards and systems. Therefore, some card issuers have been reflecting on recommendations to deal with some expected conflicting scenarios in the operation of MA systems.

To conclude we can summarize that:

1. The Legislation applicable to the MA smart card relies heavily on the legal nature of the Issuer entity, which directly impacts the nature of the contract between the card issuer and the cardholder.
2. Except in the case of the White Card, a contract links the Card Issuer and the Cardholder. This contract shall comply with legislation intended to protect the consumer for on-line trading
3. Other bilateral contractual relationships may link the Cardholder with Application Providers other than the Card Issuer. These contracts and their acceptance by the cardholder using an electronic signature fall under the on-line trading legislation
4. When the MA card holds an electronic purse, legislation applicable to Bank Operation is relevant, because electronic money handling is assimilated in bank operations. In particular the contracts must refer to the European Commission Recommendation 97/489/CE
5. Contractual relationships must link the Card Issuers with the Application Providers. These contracts are not necessarily concluded on-line.
6. e-Privacy Law is relevant when the card stores Confidential Cardholder Data. These include Personal Identification Data and Medical records
7. Some of the applications intended fall under the scope of.
   Relevant problems include Protection of Digital Multimedia content and Gambling
8. Multi-application Cards are expected to become an effective support for e/m-commerce development.Therefore, the European Legal Framework for e-commerce shall be applicable for transactions conducted between partners operating within EU border.

7.2 Applicable Legislation for Card Operation

Because of the diversity of the applications which can be resident in the card, the following legislation to regulate the card operation may apply:

3.1 Contract Law
3.2 Consummation Code
3.3 Civil Code
3.4 Law of Proof
3.5 Banking Law
3.5 European Directives under application by Member States

The contracts linking the different partners must therefore take these into account

8 CONTRACTUAL RELATIONSHIPS BETWEEN MAS PLAYERS

Specific Issues of the Multi-applicative Card

The operation of the multi-application card potentially *involves several separate contractual relationships between several partners in the multi-application consortium.*

Each application resident in the card is the logical format of a commercial contract and, as such, is liable relative to the legal commercial framework and contract law.

If these contracts are concluded on-line (electronic contracts) they fall under applicable european legislation for on-line trading: The Directive 99/93/CE on Electronic Signature and Electronic Commerce: European Directive 2000/31/CE June 8th, 2000. Both Directives are relevant for the Burden of Proof and the conclusion of the contract issues. Additional discussion of on-line trading applicable legal framework is addressed in $

Contract terms should specify that control over the partnerships rests with the issuer. The Issuer should track and monitor performance of each partnership program, including response and approval rates, utilization rates, purchase volume, delinquencies, charge-offs ets. The bank's planning strategies should factor in the possibility of high attrition rates if such a group or business withdraw its endorsement from the bank.
When launching a MA scheme, there must be clear, detailed and well designed contracts between all the participants (card issuer/application providers, card operators and cardholders, to simplify) spelling out the rights and liabilities of all parties. Each role in the system has its own inherent risks.
In addition, the legal framework is intended to enhance consumer confidence in the multi-applicative card, by empowering the consumers' choice to select applications of their own whilst providing them with effective legal protection.

Finally, the MA card appears to be an appropriate support for Identification, Authentication and Payment for services accessed through the Internet (e-commerce transactions). As such, the operation of the MA card is under the more general framework of the applicable legislation regulating electronic trading.

Role of the Contract

In the Smart Card industry, two types of contracts can be differentiated:

The Cardholder Contract, between the Card Issuer and the Cardholder Delimitating the usage of the card and the respective rights and obligations.

The Card Acceptance Contract between the Card Issuer and the Merchants accepting the Card. The Merchant can be another competitor of the Card Issuer. That is the case with Roaming Contracts between Mobile Telecom Operators.

Both contracts are interdependent, because the rights granted by the Cardholder can only be executed in connection with entities having signed with the Card Issuer a Contract for Card Acceptance.

In the multi-application context, two scenarios can be identified for Card Acceptance Contracts:

1.A contract linking the Card Issuer and a Service Provider, by which, the SP accepts the cards of the Card Issuers, but the SP does not load any proprietary data in the card.

2.A contract linking the Card Issuer and an Application Provider, by which the AP is authorized to download their applications onto the card, on request of the cardholder and with possibly the previous authorization of the Card Issuer. The specific procedural methods for this operation are set out in the contract.Three main methods are identified by Open Platform:

Mandated Data Authentication Pattern (DAP) Verification
DAP Verification
Delegated Management

In the implementation of a recommendation the contracts play a central role. It is expected that the States can put some pressure on the concerned economic agents (MA Card Issuers) in order that the proposed contracts comply with the recommendation principles.

Different criteria can be applied to characterize the nature of the contract:

8.1 The Nature of the Contract Between the Card Issuer and the Cardholder

The Mono-application Card

The card is a document representing the rights of the cardholder as set out in the contract linking the cardholder and the card issuer
These rights can only be exerted on card presentation, along with additional verifications depending on the nature of the card and of the accessed service
These rights can only be accessed through those entities having agreement with the Service Provider

The Multi-application Card

1. The card is the document representing the rights established by a series of contractual relationships agreed between the Cardholder and other entities of the Multi-applicative Scheme. As a minimum, a contractual relationship exists between the Card Issuer and the Service Provider.
2. This primary contractual relationship defines the right of the cardholder to enter into other contractual relationships with other members of the scheme, and eventually with other e-communities.
3. An exception to rules 1 and 2 may apply for the White Multi-applicative card, where the Card Issuer and the Cardholder are the same individual.
4. When the card holds a payment application, the payment function can only be used in those entities having a contractual relationship with the Payment Application Provider.

5. The nature of the contracts is interdependent: The contract between the Cardholder and any Application/Service Provider is dependent on the Contract between the Card Issuer and any of the Application Providers and eventually on the Contracts between the Application/Service Providers themselves.
6. The nature of the multi-application card and the applicable law, depends on the specific application being executed. When several applications are run, the laws relevant to all the active applications are applicable. In case of contradictory terms.

Minimum Content of a Contract for Multi-application Card

1.Information to be provided to the cardholder concerning contractual terms and conditions

Technical Characteristics
Duties and Liabilities of the Cardholder partners
Expenses
Delays for Claim and procedures to be followed

2. Information to be delivered concerning thes operations enabled by the MA cars

Identification of the operation
Total cost per Operation

3. Duties and Responsibilities of the parts:

-Card Issuer
- Implementing a System for keeping track of Card enabled Operations
- Bring the proof of the operations charged to the cardholder

-Service Providers

-Cardholder
- Conditions of usage and storage of the card
- Claiming procedures for theft and/or loss
- Responsibilities up to card notification
- Certification and Registration Authority

4. Notification of card theft or loss. Resolution of differences. Claiming procedures.

8.2 Card Issuer vs Service Provider Contractual Relationships

eEurope/SCC differentiates between two scenarios:

Case 1: The Card Issuer accepts access by the Service Provider to the generic IAS module for the provision of services on request of the cardholder. Case 1 sustains different business models (Fixed Revenue or Revenue-per-transaction requiring capture of the transaction data by the Card Issuer for all the SP operating in this mode and subsequent billing to the SP).

Case 2: The Card Issuer and the Service Provider negotiate the allocation of some memory space to the SP in order to proceed to the donwloading of on-card applications, owned directly by the SP or by a third party under the responsibility of the SP. Case 2 sustains business models enabling direct billing relationships between the Service Providers and the end-user.

One additional obligation for the Card Issuer is the existence of Acceptors of the Card it delivers to the Cardholder:

For Bank Cards, the Card is provided in order to fulfil the obligations (of payment) of the end-user with a third party (a merchant acceptor). The third party must exist. The Card Issuer has previously to sign a contract with the Merchants (for payment) or other Acquirers (Cash Retrieval in their ATM Infrastructure). The Card Issuer has to inform the Cardholder where the card is accepted.

In the case of SIM cards, information is required by the Customer about the coverage of the territory by the mobile network (it is also a marketing feature) directly by the Card Issuer or by another Telecom Operator with a Roaming Contract..This corresponds to the geographical areas where the SIM Card is accepted for mobile phone communications (calls or messages).

In the multi-application card, two situations can be differentiated:

1.The Card Issuers should inform customers which Application Providers, in addition of the List of Acceptors of the Card " as delivered", are enabled to download applications into the Card and the Service they provide. Legally, they correspond to the Card Issuer obligations and shall be contractually specified.

The acceptance of the card must then be subject to the explicit selection of an on-card specific application, which expresses the consent of the Cardholder. The usage of the application may be covered by a contract signed between the Card Issuer and the Application Provider, with no additional contract required between Cardholder and the MA Card Acceptors.

2.For the White Card:

If an IAS standard module is present in the card, the address (@URL), of a Application Provider could be personalized into the card. The AP can then proceed to an initial Card Authentication using IAS Data

If no IAS is present, the White Card can be personalized with the address of a Certification Authority for White Cards. These CA may, in turn, personalize the card with @URL addresses, of AP, accepting their Certificate as a proof enough to accept to grant a Service (Including Application downloading).

8.3 Card Issuer vs Service Providers Liability Issues

The players responsible for the multi-application system security should also bear the costs of security failure. But currently there is little background on how fair rules could be set in order to decide who pays for what when a common responsibility can be engaged. There is probably no substitute for solid legal advice from experienced counsel in drawing up these contracts.

There are specific concerns in some business sectors relative to the contractual clauses of liability linking the card issuer with the application providers. Even if this issue seems to be out of the scope of any standardization activity, some participants have expressed a wish to have TB7 analyse some standard scenarios of shared liability and define some guidelines for contractual settlements.

If the Card Issuer is the only party responsible to the cardholder for losses after card failure:
1.It will closely control the Service Providers authorized to download data in its card. These providers will be only those strongly trusted by the card issuer and probably providing the same type of services within the same sector
2.The card issuer will be in a position to force in a unilateral way, harsh liability clauses on the service providers, which can discourage them from participating in a common scheme.

On the other hand, it is difficult for a Service Provider to accept the whole responsibility if the card fails when executing its application, because this failure may be caused by physical wear of the card as a consequence of its past use. Because the card usage profile is the « average » of the use of the different resident applications (which differ in amount of write access to the card memory) and this is typically different for each user, some kind of data warehousing keeping track of the «whole scheme profile » can make sense in order to solve liability arrangements/pay-back between participants. Yet this Data collection, recording and secure storage involves a lot of specific e-Privacy legal concerns.

A similar problem arises when the security of the card/system is jeopardized because of the use of the common card keys by different applications requiring cryptographic services. Some attempts have been made in the past to model the security policy for a multi-applicative card. This problem is introduced bellow.
On the other hand, accepting this responsibility may lead to the service provider either (1) requiring that the card correspond to a minimum protection profile or (2) demanding to be informed ofthe precise intended use.

A major difficulty is the lack of any previous real legal problems because of the very few operational multi-application systems so far deployed:

1.Even if there is a field open for research in this area, there is a risk that the real future problems will not be addressed

2.Legal/marketing constraints have an impact on the technical requirements for design & operation of MA systems, but usually the technical solutions are available first

The nature of these relationship relys on the selected mode of operation for the system. Different scenarios are possible.

8.4 Contracts Concluded on Internet

In this document we differentiate between:

1. On-line Contract: established and agreed over the Internet, but executed in the physical world. Example Internet purchase and delivery of material goods.
2. Virtual Contract: Set, agreed and executed over Internet. Thais the scenario relevant to Card Application Downloading.

8.4.1 Multi-applicative Card and Internet

It is widely acknowledged that the development of e-commerce over the Internet requires confidence in the security of the transaction by both purchasers and merchants. Basic trust problems include obtaining proof of the commercial order for the merchant to be provided by the purchaser, the Identification and Authentication of the Merchant and the implementation of a Secure on-line Payment Protocol.

The mobile nature of the card means that on-line transactions can be subject to different national Civil and Commercial Legislation depending on where the transaction is concluded.

The multi-application smart card is a powerful device to develop e-commerce because of the intrinsic ability of the multi-application card to support

(1) The diversity of services of any nature offered over the Internet
(2) On-line payment
(3) Secure Authentication of both Merchant and the Cardholder
(4) The generation and storage of a digital proof of the transaction
(5) The generation of an electronic signature to prove acceptance of the terms and conditions
(6) The representation of a Trusted Third Party for the Merchant and/or its Bank,

This means that when the transaction takes place over the Internet, the card must support the rights contracted by the cardholder whilst complying with the Internet applicable laws.

8.4.2 Applicable Law for On-Line Trading

Introduction

Within the European Union, determining the law applicable to contractual obligations between an on-line Service Provider and a Cardholder residing in another member State is governed in principle by the Treaty of Rome. Pursuant to Article 5.2 of the Treaty, the choice by the parties of the law applicable may not result in depriving the consumer of the protection provided by the mandatory terms of the law of the country in which he normally resides from the moment when one of the following two hypotheses is encountered:

1. The conclusion of the contract has been preceded in the cardholder's country by a specially prepared proposal or by some advertising and the consumer in that country has completed the actions necessary for the conclusion of the contract

2. The Service Provider (co-contractor of the cardholder) has received the order in that country

8.5 On-line payment

On-line trading raises naturally the problem of on-line payment even if the provision of an on-line service does not necessarily involve an on-line paymentoperation. However, an e-commerce transaction raises inevitably problems of identification and authentication of the ordering entity (an individual for C to B e-commerce transactions), as well as the obtaining by the merchant of proof that the orderer accepts the agreed terms and conditions for the sale (e-signature)
In addition, when protection of digital content is required, the use of cryptographic technologies for encryption of the transmitted data can be supported by the card (CA technology).
Finally, the possibility for on-line payment which is provided by the card, illustrates why

The European Directive 2000/31/CE

The European Directive 2000/31/CE prescribes that every Internet service provider is ruled by the country where it has its establishment (original States rule).

According to the definition of a communication of the European Commission of 30th July 1998, electronic commerce consists of the development of commercial activities and transactions on electronically and includes several activities like the commercialisation of goods and services on line, including the distribution of digital contents (multimedia, audio, applicative software) and the realisation on line of financial operations,including but not limited to electronic payments.

Regulation is provided by the European Directive 2000/31/CE of the European Parliament and of the Council of 8th June 2000, on certain legal aspects of information about companies' services, in particular electronic commerce, in the Internal Market.

Member States have to assure the juridical efficacy of the contracts, which have been concluded on-line, but they may specify some categories, like

1. Contracts that create or transfer rights in real estate, except for rental rights;
2. Contracts requiring by law the involvement of courts, public authorities or professions exercising public authority; contracts of suretyship granted

and on collateral securities furnished by persons acting for purposes outside their trade,business or profession

3. Contracts governed by family law or by the law of succession.

8.6 Closing of the Contract

A quite widespread means of closing a contract on line is by use of digital signature. An alternative, and frequently used manner overall for the selling of mobile goods between enterprises in the Member States, is closing contracts through exchange of fax letters, or e-mail or through the “point and click" over the icon "OK" of an order-form or by the party’s behaviour (the execution of a payment or the ware’s delivery) or through verbal or phone agreements.

According to the Directive 2000/31/CE the contract’s closing has to happen in the following steps:

1. the supplier sends the offer to the receiver;
2. the receiver sends his acceptance to the supplier (for example, by a "click" on an icon),
3. the supplier receives the acceptance
4. the addressee receives from the supplier electronically the receiver’s notice of acceptance.

It is possible to use a closing behaviour: a buyer sends an electronic order by e-mail and the supplier, without sending his acceptance by e-mail or by any other means, delivers the goods immediately; or the supplier sends an offer by e-mail to an eventual client who does not send his acceptance, but pays the price directly.

Finally, contracts which are closed according to the e-commerce directive and its National Lagislation’s application are also put under the regulation of the civil code (artt. 1469-bis and ff,.) for the protection of the consumer against unlawful clauses, with the general duty of a clear and understandable drawing up of the contract and the prohibition to limit the liability of the supplier.

8.7 Contract Execution

Executing a contract between distant subjects for provision of physical goods involves a legal obligation by the provider to deliver within a period of time (eg 1 month) after the conclusion of the contract.

Should the goods not be available, the supplier has to tell the consumer in writing, still within 30 days, and refund any pre-advanced sum.

Moreover, if no specific clause is accepted by the consumer, the supplier cannot deliver different goods from what has been chosen, even if valued the same or more in terms of price or quality.

Regarding the individual communication to the single consumer, note that that decree n. 185/99 (art.10.1) establishes that the use by a supplier of media like telephone, fax, e-mail requires theprevious written consent of the consumer

8.8 Electronic Signature of on-line Contracts

Authentication is a necessary step to achieve trust, but in many cases it is not sufficient. Authentication enables the decider to verify the identity and/or attributes of the requester. This is enough when the decision and commitment of the decider is immediate (eg to authorize access control to a public transport network).

Most social interactions are based in agreements involving a complex set of commitment and duties spread over a defined period of time (eg. Payback or bank credit). These situations require an additional level of trust between parties guaranteeing that they will each respect the agreement, and providing each with means to have the agreement enforced should one or more of the parties default.

This need has given birth to the concept of contract as a means to formally **represent** the agreement and the signature as a way to formally bind a party to the terms and conditions of the contract.

9 PROTECTIVE CLAUSES FOR THE MA SCHEME PARTNERS

9.1 Protection of the Consumer

The free movement and provisionof Internet Services compatible with the appropriate protection for the end-user to promote trust is a major objective of eEurope. This is reflected in the arrangements planned in the European Legislation relative to the regulation of the Information Society. Two main reasons justify this policy:

Firstly, for business to consumer e-commerce, the increasing importance and influence of the consumers' unions, and therefore the possibility of benefiting from alternative disputes resolutions. These claims address not only specific commercial /payment but also issues relating to the protection of private data.

Secondly, the development of Cross-border on-line services is possible only if the end-consumer trusts the systems.

The European Directives protect the consumer through three major types of provisions:

1. The Obligation of Information and Transparency of Practices by the Service Provider
2. The Clarification of the actual wishes of the end-user when concluding an on-line contract What is the actual commitment expressed by the Cardholder ?
3. The Requirement for the Adoption of appropriate mechanisms for Customer Claims

For the multi-application card, the protection of the customer is specially relevant, at least for three specific reasons:

1. The multiplicity of contracts linking the cardholder to the different MA and to the Card Issuer, due to the diversity of players running MA systems

2. The e-Privacy concerns linked to the capture and exploitation of the data generated by the multiple transactions initiated with the MA card

3. The nature and potential scope of the commitments taken by the cardholder when the transaction is authenticated by an electronic signature (for on-line ordering and e-payment purposes). The non-repudiation of the electronic signature should be counter-balanced by appropriate transaction revocation procedures

9.2 Passive versus Active consumer

The distinction between Passive and Active consumer is relevant in the field of European jurisdiction concerning Internet Regulation. In particular, it is argued that, for e-commerce operation, the role of the Consumer is necessarily active. Therefore, the revocation rights of the purchase should be limited in line with legal rules applied to retail commerce.

9.3 The Protection of the Application Provider: Existing Legal Framework

Legal Nature of the Application Provider

Tha Application Provider (AP) is defined as the legal entity owner of a Card Application. The AP can be identified from the Standard Identifier as specified by ISO/IEC 7816-5 standard, but this method is not mandatory, unless contractually required.

The Application Provider is therefore a software seller, and as such has the generic obligations of consumer information, application delivery, on-card installation and customer satisfaction when using the application. The cardholder has to be guaranteed against non-execution, defective execution or processing error.

The Application Provider grants the contractual right to load its own applications on the Card. Two scenarios are to be differentiated: (1) When the application is already resident in the card when delivered and (2) When the application is downloaded after card delivery on cardholder request (PIP as Post Issuance Personalization).

Whatever the scenario, the application provider is granted this right by the owner of the multi-application card: Card Issuer, Cardholder or an hybrid proprietary scheme (see § However the exercise of this right may result in damage: to the Card Issuer, to the Cardholder himself and to other Application Providers.

Protection of the Rights of a Third Application Provider

Ideally, the individual management of any application (download,deletion, activation/de-activation, upgrade) should have no impact on the security status of all the other applications. For Multi-application Cards, this guarantee should be extended to the other

Application Providers with applications resident in the card at the time of the downloading.

The Card Issuer itself is excluded from this guarantee because the mechanisms and authorization for the application downloading are under its direct responsibility, even if the execution of the procedure can be delegated to a third party (ie the Application Provider itself). In addition, the damage to the Card Issuer may be contractually covered (Example: Damage to the Card Issuer Brand produced by a faulty Application).

However, the Card Issuer remains responsible for the security of the procedure for application downloading notwithstanding any third AP responsibility. This means that if an Application Provider suspects fraud, the Card Issuer must be able to provide the AP with elements demonstrating that there is no correlation between the observed fraud and any previous card or application life cycle management operation performed on the suspected cards.

2. The delivery and installation of the card application is performed by executing an on-line downloading protocol using the card and system resources provided by the Card Issuer. International Specifications and Standards (OP, ISO/IEC 7816-9) support different scenarios for this procedure. In any case, the Card Issuer is liable for any card missfunction during application downloading and installation resulting in economic loss for either the AP or the cardholder.

3. Once successfully installed, subsequent execution of the card application on cardholder's request is supported again by the card and off-card resources, but now the process is at least partially controlled by the proprietary Application Data management of the Application Provider. The Card Issuer and the Application Provider are jointly responsible for any economic loss in case of application failure.

9.4 The Internet Application Provider

We differentiate between Service Providers operating through the Internet with a Web site accessible to everybody and those that can only be accessed through the authentication services provided by the card (URL stored into the card). Juridicially, the difference relies on the personal attitude of the cardholder.

The Nature of the card application provisioning

The personalization of applicative code in the card is to be considered as an Information Society Service (ISS). As such, it is subject to the terms set up in the European Directive on e-commerce

1. It is subject to the Law of the member state where the ISP is registered, irrespective of the countries where WEB Servers are based for the provisioning of card applications

2. Whereas the Cardholder is subject to the State Law of his/her residence

The nature of the Service Offered on the Web is not subject to any specific authorization other than required for the provision of the same service for other channels. However, Services (financial, gambling) may be subject to an explicit authorization when they are regulated (regulation in connection with the type of the service, not to their distribution channel)

The other question is the nature, personalized or not, of the downloaded digital content (application oriented or other). The on-line service (applet download) has the nature of an audiovisual communication.

We can consider thatin this case the broadcasted EMM message which is finally targeted at the requesting individual has the same legal nature as the applet. The EMM enables access to a service which is the access to an enciphered video content. The applet similarly enables access to an on-line service.

ISP Legal Framework

The Problem:

The Internet enables the easy illegal distribution of Digital Content from a Web Server. The lack of a Legal Framework hampers the distribution of content over Internet.

The Internet Service Provider is the entity providing the cardholder with a distant connection to a Web Server (Portal) distributing digital content under IP rights by a Content Provider. This Web Server can then proceed to the provisioning of Digital Content which may actually be illegal, and then produce economic loss to the Content Provider (Application Provider). The ISP is the intermediate entity between the Content Provider and the consumer. The ISP is then merely a Carrier of digital content owned by a third entity. In this scenario, the SP is the entity entitled by the Content Provider to offer digital content through a Web Server owned by the SP. Of course, the CP may act as a SP as well, offering directly their own content.

However an offence may occur when the SP is not entitled to offer the Digital Content of a Third entity. In this case, the ISP is the carrier which enables the illegal transaction by putting consumer and the SP in contact via the WEB, but the consequence is that the CP sustains losses and may claim for compensation. Who is liable to the CP?

Case 1: In principle, the faulty organization is the SP. But while there is no Internet Law it may be almost impossible to go to trial (The SP can be protected by local law in the state of residence, possible insolvency, difficulty in proof of the crime in addition to the problem of identifying the offender, which can be covered by anonymity).
If looking for a person legally responsible, the ISP can then be liable according to the CP, because it is considered a passive abetter of faulty SP (« culpa in causa » principle, the causa is the ISP connection). This liability approach may have a chilling effect on liberty

by urging the ISP to take preventive censorship measures, by installing, eg, a proxy server. Otherwise the ISP endorses the risk (culpa in causa). If the risk converts into a damage, the victim might claim compensation from the ISP. The legal status of the ISP is out of scope of this document.

9.5 Conflict Scenarios for Cardholder vs Application/Service Provider

1. The Application Provider is expected to pay fees to the Card Issuer in order to grant the right of downloading the application. This means that the AP may expect to be paid-back after a critical number of average transactions. Otherwise, the AP loses money, and it can be expected to state contractually that the Cardholder is liable for loss-compensation. Some contracts between an Application Provider and the End-User already include this type of protecting clause stating that the conditions for downloading include a minimum number of transactions. Otherwise, less favourable conditions shall apply for the cardholder.
2. Cancellation of the Transaction.
3. Conditions for Usage of the Application
4. Liability of the Cardholder in case of Application Failure
   Obligation of on-card software delivery as ordered by the Carholder
5. The nature of the transaction: Sale or Rental

Some of these conflictual issues have been adressed by the European Directive on electronic commerce. As mentioned, the recommendations of this document are in line to a maximum extent with the current legislative framework.

10 INITIAL CONCLUSIONS AND PROPOSALS

10.1 Setting a theoretical model for Liability Sharing

a. Based on memory applet apportionment
b. Based on the number of Write Operations.
c. Based on the number of times a particular application is selected.
d. Based on how many cryptographic calculations are required during the application execution.

It is theoretically possible to create a simple mathematical model, to calculate how much the security of the card is « used up » either in terms of physical wear of the common support or of the common cryptographic keys shared by each application provider. This approach can only work if strict fire walling is provided by the card platform: An application is denied access to memory areas other than those reserved for its execution and for its code and data. A more precise protection consists of verifying that every instruction that accesses a memory area is compliant with the definition of the data stored in the area.

10.2 Liability/Security Issues which can be addressed by TB7/WP2

The following is an open list of liability issues that could be addressed by TB7 if we get the necessary expertise

1. Current Legal Situation: New data protection legislation. How not to undermine confidence
2. Fight against fraud: How to motivate System Promoters to improve technical protection measures or to ensure protection cover through insurance.
3. Changes for liability in networked environments
4. Clear procedures for application withdrawing or cancelling
5. Ditto for cancelling the whole card (death)
6. Clear responsibility for managing the customer relationship
7. Service levels for the customer in terms of availability of card readers and response times
8. Clear strategy for card replacement if migration
9. The issuer (issuer specific mechanism) should provide a mechanism to block or unblock an application by means of a hot list distributed to key points in the terminal network
10. Careful allocation and mitigation of risk will be required
11. Authorities should carry out a formal risk assessment including:
    - Commercial failure of the scheme: critical number of users must adopt the card.

Appropriate incentives:

- Liability to compensate the cardholder
- Limits on the cardholder's liability
- Damage to a cardholder through reliance being placed in inaccurate or outdated information being written in the card, must be clearly established
- Damage to a third party through misuse of the card by the cardholder

- ➢ Clear procedures for verifying Information and ensuring Information is kept up to date
- ➢ Provide the cardholder with the ability to correct inaccurate entries (by for example an applet downloaded after authentication)Risk Analysis

APPENDIX 1: Card Technology Evolution and Legal Framework

Card technology innovation is intended to better integrate the smart card with the Internet, through different terminals. One promising technology for the card is the implementation of a real Web Server into the Card itself, for mobile or fixed environments. This Web Card Server has both Client and Server functionalities. From a theoretical point of view and depending on the intended mode of card operation some of the legislation applicable to the Web Server, could be relevant to the card as well. For example, the European Directive on e-commerce states that physically; the problem there is the mobility of the card itself. Depending where physically (which member state) the transaction takes place, the applicable law could change. This is already the case when paying with a bank card. This possible issue is just mentioned in this report.

APPENDIX 2: Possible MA Card Operation Modes

Card Operator	*Risks*	*Liability*	*Legal Impact*
Card Issuer	**1.Damage to brand image because of card failure after load of aggressive code** **2.Responsibility for loss in front of the Cardholder** **3.Responsibility in front of AP in case of AP financial loss** **4. Rely on the Security of the Card Platform.**	**1.Application segregation** **2.Quality of Security Services offered** **3.Data integrity even if an unsecure applet is loaded into the card** **4.The Card Issuer do not leak private data outside the card**	**All the application providers negotiate and agree with the card issuer conditions**
Third entity with aCertification Authority (CA)		**1. Responsible in front of the Card Issuer of the Security of the certified applet** **2. The CA must not necessary get access to the Applet content, proprietary of the AP** **3. Revenue optimization for the Card Issuer: Research for optimum co-existence of synergic**	**The AP must be first certified by the third entity.** **An additional request for download provided by the Card Issuer is in addition required**

		applications **4. Optimization of the Card Memory**	
End User (White Card) Required Certificates		**The Service Provider accepts to download their data in the card after retrieval of the White Card Certificate. The AP trusts the card OS**	

APPENDIX 3: Issues to be considered in a Card Risk Analysis

The purpose of the risk analysis is to focus the decision maker's attention on the financial, technical, and schedule risks associated with multi-applicative cards with PKI functions. When documenting your business case, it is necessary to counter-balance positive financial indicators with real-world factors that could potentially undermine your investment and keep it from reaching its estimated potential. This section will help you better understand the risks associated with both smart card and PKI technologies. Risks are inherent to any investment but can be managed to achieve a favourable return on investment.

An example is, performing an encryption using a public key, or a signature using a private key. Nonetheless, smart cards themselves have inherent drawbacks and risks. These include the high cost of readers, algorithm replacement, lack of standards, loss or theft, and the fact that smart cards are susceptible to many kinds of attacks.

Loss or Theft

Irrespective of the use of the smart card, a primary risk that users face is physical loss or theft of the token. This risk is countered with the inevitable acknowledgement of a missing token and associated revocation procedures to prevent further misrepresentations of the individual's certificate-based trust among associated PKI-enabled applications. A more dangerous risk is theft of keys and discovery of the associated PIN or password used to unlock the keys, without damaging or removing the smart card. This risk poses a far greater threat to the associated trusting PKI-enabled applications and breaches are usually discovered and mitigated only after serious harm occurs, or the certificate is revoked or expires. Regardless of the protections that are built into the system, if the card is not physically protected, laws and security measures will not be effective. This protection is evolving into a combination of user responsibility for physical possession/compliance with associated policies for use and card protection of the keys during generation and/or use.

Attacks on Smart Cards

Smart cards are susceptible to attack by bad people. An attack is defined simply as an attempt to steal or compromise data on the smart card. There are two classes of attackers—those who are parties to the system, and those who are interlopers. Attacks by participants could be a cardholder trying to cheat a terminal owner, a card issuer trying to cheat a cardholder, or similar behaviour. Attacks by outsiders could be mounted via card theft, card misuse, or replacement of terminal software or hardware. Attacks by outsiders are often similar to attacks on protocols involving general-purpose computers; however, they may take advantage of various properties of the system created by the separation **of** roles. Four kinds of attacks can be made on smart cards: logical, physical, trojan horse, and social engineering.

Logical Attacks. One type of attack is logical attack. A logical attack does no physical harm to the smart card, rather, some sensitive information on the card is obtained by examining the bytes being transmitted to or from the card. If successful, this attack creates one of the greatest threats (i.e., potential undetected use increases until substantial damage occurs and is noticed). This attack is difficult to achieve because it involves capturing both the private key and associated PIN to perform private key operations. If the byte level I/O operations are monitored, and processing of PKI functions is not performed on the card, both the keys and PIN are exposed.

Physical Attacks. Physical attacks are carried out, usually using special equipment, by varying temperature, voltage, or clock frequency, etc., to gain access to sensitive information on the card, or by monitoring card parameters (such as power consumption or the timing of certain card processor operations). Most smart card operating systems write sensitive data to the EEPROM area in a proprietary, encrypted manner so that it is difficult to obtain cleartext keys by directly hacking into the EEPROM. Other physical attacks that have proved successful involve an intense physical fluctuation at the precise time and location where the PIN verification takes place. When this happens, sensitive card functions can be performed even though the PIN is unknown to the perpetrator of the attack. A combination of a physical attack with a logical attack will reveal the private key.

Trojan Horse Attacks. A trojan horse attack involves planting malicious code on a user’s workstation without the user's knowledge. When the user submits a valid PIN, the trojan horse presents rogue data to be signed using the private key. The user is never aware that the rogue data has been signed. There are two ways of counter-attacking the trojan horse. The first is to use “single-access device driver” architecture. The operating system allows only one “trusted” application to have access to the smart card (if that one application can be compromised, of course, then even this approach can be circumvented). Not using a multi-application smart card both reduces the number of parties involved and creates a simpler operating environment with less complexity and potential for bugs. Although this reduces the possibility of attack, the benefits to be derived from multifunctionality are, of course, lost. Another way to prevent this type of attack is to require one private key entry per PIN entry; the user must then use the PIN every time the private key is to be used, thereby disallowing the trojan horse access to the key.

Social Engineering Attacks. This kind of attack exploits the vulnerabilities inherent in human beings. For example, a hacker could pose as a network technician and request PIN and passwords in order to hack the system. This attack is not as effective when smart cards are involved because people are less likely (or even able) to share their smart card than a PIN or password.

When a decision to proceed with smart cards is made, it is essential to understand that “eternal vigilance” is not only expensive, but impossible. The risks associated with smart card tokens must be understood and bound and balanced against associated benefits. The benefit of cost savings from increased efficiency or compliance should be weighed against the associated threats resulting from the fact that data will be exposed to remote access by users who hold the appropriate PKI credentials. Incremental steps to cost effectively control and leverage the demand for smart cards should be undertaken. The most appropriate system needs for PKI-enabled security services are unique to each set of specified security requirements of a System Operator.

RISKS LINKED TO PKI OPERATION

PKI has recently become a popular solution for achieving electronic security and digital-based trust, but it does engender risks that vary in accordance with how the PKI is implemented and what user community it serves. Among the key risks are concerns over the maturity of PKI technology as well as key management itself.

Value Definition

Any PKI implementation should commence with an assessment of what data would benefit from increased exposure that PKI-enabled security services could address. The assessment includes evaluating the monetary or other value of the information and the associated savings that can be realized by allowing remote access. The determination of appropriate PKI-enabled security services is derived from the associated System Operator processes and data interchange that could be run cheaper and/or faster, or must comply with Federal mandates (i.e., paperless processes). It is essential to bear in mind that the implemntation of PKI could result in additional exposure of associated data which may not always be desirable.

Lack of Standards

Although in existence for more than 10 years, commercial products implementing PKI technology have had limited use. Because of its limited use, standards have been slow to emerge. Some PKI standards are not mature or remain de facto because vendors must differentiate their products to justify procurement and the additional cost associated with implementing PKI. Fortunately, this situation is improving due to the efforts of vendor-sponsored organizations like the PKI Forum (http://www.pkiforum.org). However, PKI standards that apply to enterprisewide use of PKI are quite stable. Standards that apply to PKI interoperability are still evolving and have been demonstrated to be sufficient for many applications that require interoperability; but they are not yet ubiquitously or consistently implemented, and thus are likely to evolve further.

Certificate Authority Issues

Among the most critical components of a good PKI is a reliable CA. Without proper certification authority, the entire PKI process can be compromised. The CA and associated certification practices/policies are the root of trust by which PKI technology is currently deployed. Credibility, represented through the issuance, revocation, and management of certificates, is supplemented by the goodwill of the issuing System Operator or service (i.e., how firmly the issuer is willing to stand behind the product). A lack of credibility resulting from poor certification authority can break the trust necessary for an effective PKI as the CA component provides the trusted binding between a subscriber's public key and his or her identity through the issuance of a certificate.

Registration Authority Issues

The introduction of human error in the RA process presents a risk to PKI. The RA works in conjunction with the issuance process to securely transmit the X.509 data about the individual and validate the identity of the individual when generating certificates, but is not an authority on the contents of the certificates. A human being is required for identity proofing. Sometimes, due to timing constraints, the verifying person may not always be as vigilant as he or she should be. A recommended solution is to require the maintenance of a log of every person identified, recording their name, identification credentials, and time of verification.

Relying Party/Subscriber Issues

- **Root certification substitution**—The root certificate is a certificate self-signed by a CA, containing the CA's public key. The root certificate is usually placed into a browser's trust list of CAs, that is, a list of CAs whom the user wants to trust. Careful management of this trust list is very important because if a malicious party can surreptitiously place a new root certificate into the list (for a CA that should not be trusted), the user will be relying upon it inappropriately. Thus, centralized management of such a trust list is usually required. In an enterprise PKI, however, only a single root certificate is required—that of the enterprise's "trust anchor" or highest level CA. Managing this approach is much easier because the single root certificate can be placed into the enterprise users' software in such a fashion that malicious alteration of that certificate would be very difficult.

- **Malicious digital signatures**—If a malicious party is able to insert code in a user's computer, he or she can get the user to digitally sign documents or material that the user did not intend to. This can be done without stealing or seizing control of the private key. The malicious code would appear to the user as if he or she is digitally signing something he or she intended to sign. In actuality, the document or material provided to the software that makes the signature occur is actually different from that appearing on the user's screen. However, if a malicious party can insert code in a computer, there is no security approach that will protect the user. Generally, the best way to guard against this type of attack is to protect the user's computer from insertion of malicious code. This however can be difficult to achieve. Furthermore, users should require receipts to be sent for each transaction. Such a protocol makes it very difficult for malicious parties to respond in a timely and effective manner.

- **Name space control**—Certificates contain a public key and the name of the subject to whom the certificate is issued. If that name is ambiguous, such as only a common name, there are opportunities for malicious parties to impersonate the putative holder of the certificate. Additionally, it can be difficult to disambiguate (i.e., distinguish among) the many people who may have the same names as the person cited in the certificate. To minimize the potential for problems, certificates generally should express names using a distinguished naming convention such as that prescribed in the X.500 standard, or that set forth using Internet domain components. An example of the former is "C=US, O=USGovernment, OU=System OperatorX, OU=System OperatorXsubordinateoffice, CN=Joseph.Smith." An example of the latter is "DC=gov, DC=System OperatorX, DCN=subordinateoffice, PN=name.System Operator.gov"

- **Theft of private key and PIN**—If a malevolent party can steal the user's private key (which is usually encrypted) and the PIN or password or other identifier used to decrypt the private key, the user can be impersonated. Doing this, of course, may be very difficult, especially if the private key was generated on and protected on hardware tokens like a smart card. Moreover, such an attack is effective only against the targeted individual—it is not a more generalized attack effective simultaneously against a wide variety of users.

Potential Risk of Implementing PKI

Essentially there are two methods of implementing a PKI; one is to contract for the service and the other is to implement the operation in-house. Both approaches have potential risk, however, these risks are managable. Deciding whether to outsource the service or implement it in-house must be done not only by comparing costs, but most important, by considering the implementing organization's overall security policy and its requirements. That is, should the System Operator retain full control of its PKI, or should the System Operator let someone else execute that aspect of its security? Additionally, an System Operator must decide if this function is critical to its mission. Government mission critical functions can not be outsourced. Other considerations include the degree of control desired by the System Operator, the availability of trained staff to implement and maintain the technology, etc.

Although neither way is inexpensive, many companies, lacking sufficient knowledge of security principles, firewalls, and network topologies, find that contracting the implementation is easier. Specialized network engineering firms with trained resources can help set up the network elements and recommend reputable CA firms to handle the PKI authentication process. In any case, a carefully thought-out PKI implementation can help ensure satisfactory operation of a virtual private network (VPN) that assists the business with its goals.

PKI provided in-house from vendors, such as Entrust Technologies, Baltimore Technologies, and Xcert, give a System Operator greater control. The System Operator can set its own certificate and key management policies and engineer infrastructure to comply with these policies. In addition, in-house PKI products are more feature-rich, and thus more flexible, than outsourced PKI services.

Outsource PKI services from vendors such as VeriSign, Thawte, and GTE also offer advantages. Costs and schedules are more predictable because the System Operator can leverage existing expertise. The System Operator is subject to an outsource PKI service provider's policies but can gain improved interoperability by joining the provider's trust network.

Cost is obviously a concern as well. In-house PKIs cost less per user than outsource PKIs, but overall support costs are higher. Usually, it is expected that a System Operator will have to issue a significant number of certificates before in-house PKI investment begins to pay off.

A third method of implementing PKI involves procuring services that are customized for the user. The user owns the PKI, but services are provided by a contractor that tailors services to the needs of the owner. This is similar to Government Owned Contractor Operated (GOCO) methodology.

LEGAL RISK

The Risk that unexpected interpretation of the law or legal uncertainty will leave the MA system or members with unforeseen financial exposures and possible losses. The logical and physical architecture of a multi-applicative card is to be specified by the Card Issuer in order to minimize the probability of any card failure (operational of security) leading to legal risk exposure.