Open Smart Card Infrastructure for Europe

v2

Volume 5: **Multi-applications**

Part 2: **Current and Future Business Models for Multi-Application Systems**

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

eESC TB7 Contacts:

Chairman: Lorenzo Gaston gaston@montrouge.tt.slb.com

Secretariat : MTA brains@mta.fr

Version	Date	Contributor(s)	Main Alteration vs. previous revision
WDv1.0	23 Oct 01	L Gaston, TB7 Chairman	Creation of the document
WDc1.1	6 Dec 01	L Gaston, TB7 Chairman	Complements on Business Models
WDc2.0	30 May 02	E.Graindor, M. Barjansky L. Gaston	Comments on previous Draft. Initial Models for MA Cards. Kick-Off meeting outcome
WDc2.1	14 Nov 02	M. Barjansky	Comments on Business Model Classification
v1.0	March 2003	L Gaston, TB7 Chairman	English Review

TABLE OF CONTENTS

1 <u>INTRODUCTION</u>

The « universal » multi-applicative card, providing different services, appears to be a promising technology for the years to come. The problem arises because if you are a financial institution, a mobile telecom or public transport operator you want this « universal card » to remain in your own control domain. The need to share a common support system means that the collaborating attitude of the card partners from different industry sectors will be a key factor for the development of the multi-applicative card market.

In order to provide a consistent frame to our analysis, WG3 makes these two basic assumptions for the multi-application card:

1. It is supposed that multi-application means a "joint venture" in a unique card holding different applications like payment means, transport, telecom and other applications which have been recorded as part of the contract.

2. *Ideally* such a card is built up respecting the customer's choice: each one will "own" and "create" his own card by selecting the applications he wants and needs.

The business case for the MA card relies on a consistent cost/benefit analysis. In addition, the business case must capture the essential elements of the business strategy. Tools must include project management concepts, financial analysis techniques , risk analysis and packaging and review of the business case. The final objective is identification of a business model: how partners will participate in the common investment effort and how value will be obtained for all the parties involved.

2   <u>MARKET EVOLUTION CONSIDERATIONS</u>

The smart-card market is expected to experience a significant shift from the current mono-applicative segments towards « horizontal » approaches (global payment systems, e/m-com, network and multimedia access control, local administration services or national transportation multi-modal schemes). Such a smart card might provide services to cardholders that will represent additional revenues for the card issuer.

<u>**TB7**</u> is intended to consider technology and business in a unified approach. Even if the technology were available for MA systems and cards, the market appears not to be mature enough for the general deployment of these systems. We find the fundamental issue about who drives whom (market needs pushing the technology or vice versa) is at the core of TB7 work. In the history of the card industry, we find several examples of failed deployment for reasons which remain unclear. Spain has probably the world's most dense electronic payment infrastructure in terms of terminals and number of cards deployed. However , the generated business is small compared to the investment efforts. The health card in France represents another example of disappointing experience. Bearing the cost of the deployment of a new system requires a clear perception of the business benefit of the investment effort.

The benefits of using a multi-applicative card must be evident and real to the cardholders. That is an obvious necessary condition to obtain a critical mass of customers justifying a positive business case. Moreover, users may be unwilling to hold a card if they fear that sensitive information (bank account number, health record) resident in the card may be publicly known and used against their own interests. A European Directive on privacy has been published and obviously the capture and exploitation of multi-applicative card transaction-related data must comply strictly with it. Yet the application data of service provider A must not be accessible to other partners unless explicitly stated. That is one of the reasons why the MA card must strictly guarantee the separation between applications. The card and the system have to comply with a security model as explained below.

As seen previously, even if their refusal depends on their national culture, most citizens resist inappropriate exploitation of a technology which could keep track of their private lives. That is likely if one of the applications resident in the card allows the personal identification of the user.

Other than for pure business reasons (two competitors must not have applications on the same card) the evaluation of what applications can coexist on the same physical support is the key question. The potential for coexistence means that the use of one of the applications increases the probability of subsequent use of the others (i.e. Movement increases the probability of Expending) Even if there are more or less generally identified « business synergies » between applications, there is no clear understanding (standard "usage cases"); of how the card facilitates everyday life for its bearer. After that additional analysis about basic security, interoperability card and application life cycles should be conducted.

In addition, TB7 intends to look at ways of making compatible the centralized management of the system under the strict control of the card issuer but with some input from the cardholder.

Willingness to adopt this approach depends on the industry issuing the card. Cultural/Security reasons make some industries very reluctant to share card resources.

WP3 represents an opportunity for testing old and new business models and theories, using new paradigms for product, service, delivering, support and pricing.

The rationale for WP3 action can be summarized as follows:

1. The cost of multi-application card issuance is regarded as a major inhibitor. It is not simply the average cost of the card but also the infrastructure costs to exploit the card which make it difficult to build the business case. Common infrastructures may reduce the costs to each party and increase the number of merchants where the card is accepted.

2. It is assumed that cards will need to play multiple roles so that partners can contribute to payback the costs of card issuance initially borne by the card issuer. An example is the card issuer passing on costs to service providers by taking fees for every transaction performed.

3. It is assumed that additional applications would enhance the business case for the card issuer by increasing the total number of transactions initiated by the card compared with the mono-applicative card. Yet the multi-application card requires the issuer to assume roles and responsibilities they do not have in their current business environment.

But:

4. When adding a new application, the intended application has to be perceived as not only incompatible with the other applications but also as having the potential to generate additional transactions for the other resident applications.

5. This does not, of course, imply that a single card will serve every purpose but multi-application means that some investors will take the initiative to issue and distribute cards for others. Somehow, the final purpose of the card will depend on the partners accepted to come into the scheme under the business conditions fixed by the issuer.

6. The challenge is therefore the identification of card content aggregators (« pillars »), dynamic application combinations (« clusters ») for new business cases around Consumer/Citizen Services (Smart Card Charter approach)

7. A specific type of application is the « single-use token ». The token allows for just one execution, once it has been executed it is deleted: e.g. Ticketing, which in some ways may be treated like the debit in an e-purse. We must be sure that a single operation can take place only once.

The application provider requests the stamp from the card issuer: Authorization is required to load a token in the card on cardholder request. The card OS only accepts tokens signed by the card issuer. The application provider then pays the Card Issuer for the « rent » of a part of the

silicon resources of its chip. The terms and conditions for the rental of memory and eventual use of security resources (cryptographic keys share of files) are to be bilaterally agreed between the Card Issuers and the Application Providers. In addition to the rental model for the card, the multi-ownership model has been mentioned. This model raises a number of legal issues which are to be analyzed by TB7/WG2.

3 THE NEW BUSINESS MODELS DRIVEN BY MA SYSTEMS: How to give a lift to Multi-application Technology.

The objectives of TB7 are (1) to collaborate on the creation of a more favourable business environment and (2) to prepare the ground for future development and deployment of MA systems driven by all the business sectors.

The identification of innovative business models is expected to

> ➢ Encourage the card industry to take advantage of identified opportunities

> ➢ Encourage the card industry to search for new opportunities

> ➢ Develop the necessary trust and confidence between partners of future multi-application schemes

> ➢ Stress schemes that take into account the future reactions of the Public

WP3 may focus on

(1) Investigate Innovative Business cases for MA system

- ❑ The Business Case for the White Card, pre-personalized with a Certificate

- ❑ The Business Case for a partial White Card

- ❑ Differentiation Strategies in the offer of MA services

- ❑ Card Management System Business case

- ❑ Data Warehouse Business Case

(2) Investigate Return on investment (ROI) methodologies specific to MA systems:

- ❑ Total Cost of Ownership

- ❑ Framework for capturing the elements of cost

- ❑ Assumptions for very short-term returns

- ❑ Longer term revenues from transactions and application *licensing*

(3) Risk Evaluation methodologies for MA schemes:

- ❑ For different scenarios: New scheme, Migration of an existing scheme, Integration

of a CMS, Integration of a Data Warehouse

❑ For different stakeholders: Card Issuer, New Service Providers

(4) Revenue breakdown analysis (card sales, licensing of service providers, token and applet certification) for the card issuer and the other partners of the MA scheme.

(5) New transaction revenue models and new sources of revenue. Cost share models for MA schemes

3.1 PROPOSED DIVISION OF MULTI-APPLICATION CARDS

GENERAL

Different configurations of multi-application cards may be taken into consideration, each of them leading to a specific business case.

Four main configurations seem to cover all the possible MULTI-APPLICATION cases:

Case 1: Multi-application card issued by a specific Card Issuer other than a Bank which also acts as main Application Provider. In Case 1 cards the Issuer allows the loading of some other applications owned by different Service Providers, under mutually agreed business terms and conditions. A specific scenario is when one of the loaded applications is a payment one, owned by a Bank but other than an e-purse. These applications may be either
(1) already pre-personalized in the card and then activated on cardholder request
(2) Downloadable in the card on cardholder request after card delivery. In this case, the Card Issuer provides the required Infrastructure (Card Management System) to allow the post-issuance application downloading process.

This case covers for example the case of a SIM card with an integrated payment (i.e. EMV compliant) application.

Case 2: The same multi-application card with an E-purse added. In this case, a prior agreement is required between the Card Issuer and a Financial Organization representative of Banks collecting the pre-paid e-money held in the purse. The security problem there is the firewalling between the e-purse and the other applications not necessarily requiring the same level of protection. The cost for implementation of the security policy in the card required for e-purse integration should be supported by Service Providers. It is therefore expected that the « per byte cost » for memory rental is higher than in Case 1, when that card « Case 1 » does not integrate payment functionalities.

An example of a Case 2 card is a Public Transport Card with an integrated independent e-purse.

Case 3: Multi-application card issued by the banking industry and containing other applications selected by the banks and, therefore, imposed on the final customer. The

ability to have multiple applications on the smart card optimising the use of the available memory, has been identified by banks as the one of the key components for enhancing the business case to roll out a chip program in the context of EMV migration. In this case multi-application downloading infrastructure must coexist with existing Open Payment Systems Infrastructure according to the four-partner model (Cardholder, Acceptor, Issuer and Acquirer). Technical solutions for Case 3 practical implementations are addressed by TB7/WG4 and WG5.

An example of Case 3 is a Debit/Credit Card with a Loyalty program

Case 4:Multi-application card issued by an independent body and containing different applications answering to the final customer needs and desires The « independent » Card Issuer may be the same card manufacturer and the card distributed in shops for example. A certification authority specific for White Cards (a new role White Card CA) could then electronically certify the identity of the cardholder for billing purposes. Service Providers could then account for an installed base of White Cards for hosting their applications without having to negotiate with an existing MA scheme. They might then accept the risks linked to the lack of responsibility for card tampering.

TB7/WG4 objective is to provide the generic technical architecture able to support any of the four cases identified above. Regardless of the specific case, the following roles can be identified in the architecture as a Value Chain component:

•the certification bodies, which control or validate applications in compliance with a specific security policy on behalf of the card issuer

• the smart card issuer, which provisions and distributes the card

• the service providers, in agreement with the Card Issuer, load their own applications into the card

• the final customers (or card holders)

Of course and considering the four "generic" business cases, some of those roles may be concentrated into one player. This will be developed now.
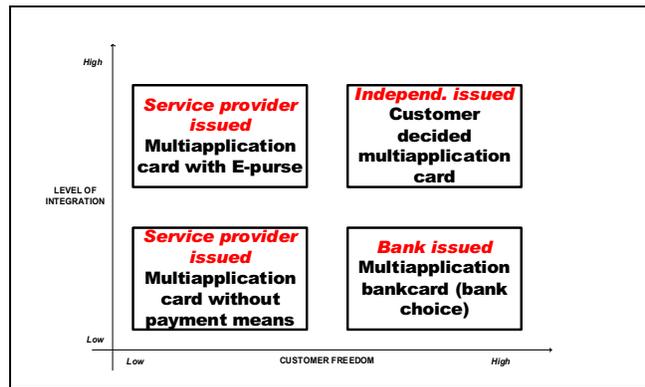
Case 1: Multi-application Card Issued by a Non-financial Institution

A specific service provider issues a card with other facilities than its own business, according to a strategy of cross benefit between different activities that produce added-value for each other *(e.g. a transport operator may increase its own activity from social or cultural events and on the other hand those events gain advantage from the transport activity to enlarge their markets)*.

Furthermore, each partner takes benefit from the share of the investment and operating costs of the smart card scheme.
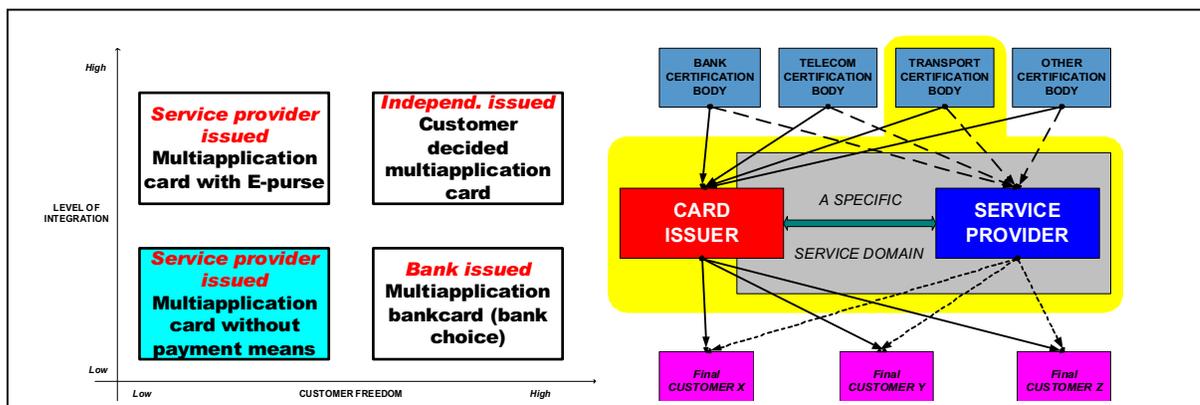
For this first business case, card issuer and service provider are the same body, which of course acts as certification body for itself

Case 2: Multi-application Card Issued by a Non-financial Institution completed with an e-purse

This case is very similar to the first one, but an E-purse facility appears relevant
to develop accessibility to at least the services of the main provider, but eventually also for the services of the other service providers. The banking industry finds here some interest through the increase in e-payments, as these may be the source of complementary revenues.
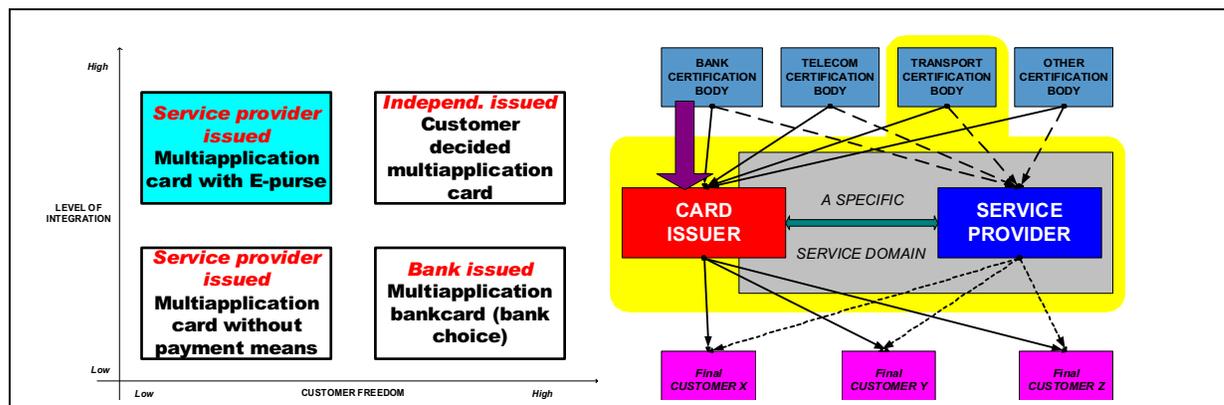
For this second business case, card issuer and service provider are the same body, but receive from the bank certification body a « right of use » for an E-purse scheme or more (e.g. debit).

Case 3: Bank Issued Multi-applicative Card

For this third case, the understanding of the bank industry regarding the relation-
ship between multi-application and the increase in e-payments is greater and, consequently, the banks accept, or, even more, express a willingness to host other service providers on their own bank issued cards. The main service providers and/or the banks may offer the critical mass of customers that justify this kind of « joint venture » in which the share of costs may be relevant.
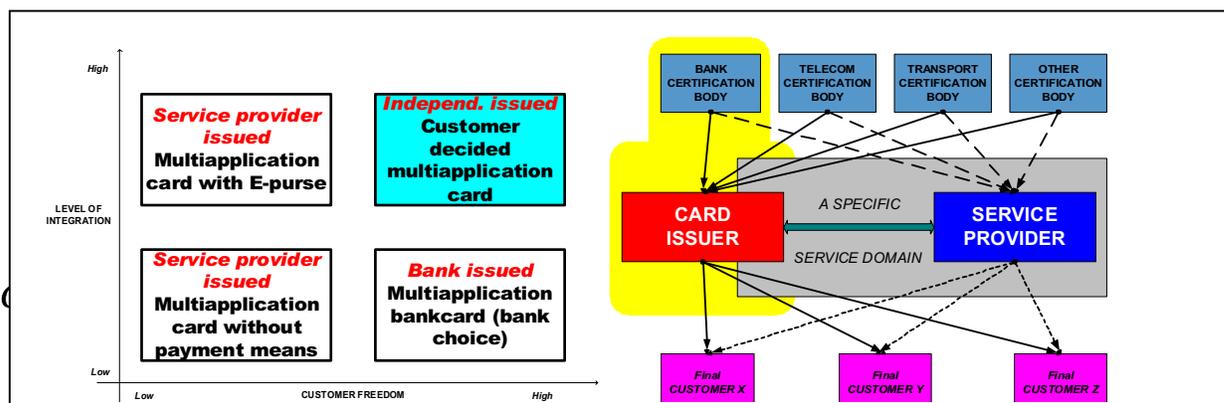
For this third business case, the card issuer is the bank industry. Even if this one does not manage the other applications, it wants to keep full control of the selection of the hosted applications as those must be relevant for the increase in e-payments, which is the objective of the bank.

Case 4: White Card

This fourth and last case supposes of course that changes of attitude must occur in the bank industry and also within the services providers, leading to a new culture and different security thinking, so that the smart card schemes may be fully out-sourced.
This supposes too that smart card issuing proves to require less investment and operating costs when subcontracted than when "home managed".
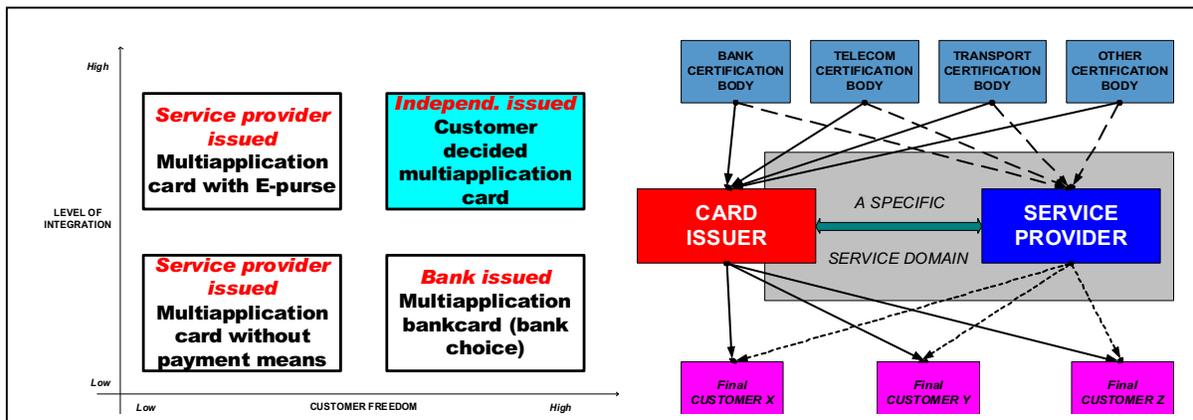
For this fourth business case, all the components of the generic model work independently, without any kind of concentration.

3.2   PUTTING THE FOUR CASES IN A DYNAMIC PERSPECTIVE

The four cases that are described above appear to be four possible outcomes in an area where the number of possibilities is vastly richer.

The situation today is that most of the cards are single application cards launched by operators exclusively on their card. That position can evolve along two axes:

The integration axis: several applications are on the same card. The notion of integration can also lead to different applications working together. It seems that it is through this process that new services can be provided to the users. This definition of Integration implies that somebody has finally masterminded the co "working " of different application from different application providers.

Freedom of choice for the user: the user can select the applications he wants to have on

his card.

The key condition for success for the multi applicative card, appears to be progressing along those two axes towards the "white card".

Integration

White card

0   Freedom of choice
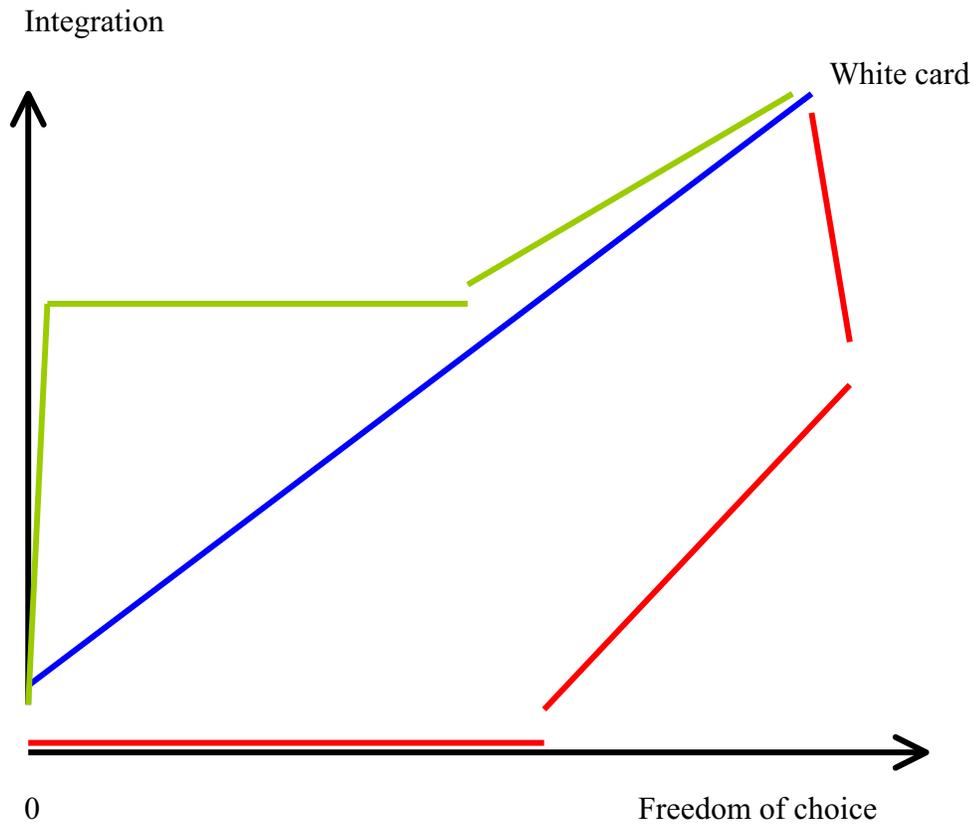
In this zone there are several ways (a lot of them in fact) to go from the mono application single provider card to the white card, which for the group stands as a kind of ideal. Continuous progress on both axes at the same time probably will not be the way to get there. There are a number of reasons for thinking that progress will be made first on one axis then on the other, and so on: regulations, business cases, technicalities, habits, training of users, etc.,

It is for that reason important for the card industry to allow both those uneven developments at the same time and so push for the white card.

4   TB7/WP3:APPROACH FOR BUSINESS CASE FOR CMS

4.1   Scope

Despite projected growth, the actual deployment of Card based Multi-application Systems appears to be disappointing, probably because of the lack of sustainable Business Models

(BM). We refer to the BM as « the intermediate item » between technology development and economic value creation. In our context the BM is a description of how a multi-application scheme made up of a partnership of competing, and even not competing, companies intends to generate revenue in the card market.

TB7 is set to explore an innovative business case liable to stimulate the launching of new sustainable Multi-application Systems and Cards. These are more than small adjustments to the existing BM; they represent a new way of looking at the business.

The main objectives of this Working Group include to understand:

(1) How to spread the Infrastructure Costs

(2) How to create « natural » partnerships

(3) How the integration of applications leverage individual applications

in order to help companies to capture value from card technology they have created.

This capture of value is made either through incorporating the technology in their current business or launching new ventures that exploit the technology in new business areas.

The CMS integration in a System means the ability of the card to access a distant Server and download an application after (1) Selection, (2) Acceptance of the sale conditions and possibly (3) Payment with the card itself. Ideally the card should be able to access this server from any terminal accepting cards, fixed or mobile, private or public, generalizing thus the multi-channel distribution concept

CMS integration in Multi-application Systems is expected to grow as broadband networks are deployed for digital content distribution.

One essential commercial difference between narrowband and broadband is that, for the most part, the demand for narrowband service is derived from the network itself, that is, the connectivity that it provides to other users of the same network or of closely related local networks, plus the "intelligence" built into the network. The demand increases just by facilitating the interconnection of private networks, enabling access to a larger number of users and facilitating the mobility of any user (ie Roaming, International Payment System (VISA) with National Payment Systems, Réseau Cartes Bancaires in France)

The demand for broadband by contrast, derives largely from the access it provides to the Internet and to the rich media and bandwith-dependent applications to be supplied by service providers who have no commercial interest in the networks itself. For this reason some broadband network operators believe that it is important to invest in the content and applications side of the business as well, rather than merely to focus on the transmission of basic telecommunications services as they currently do. Even if network operators have no traditional expertise in these areas, the multi-applicative Java Card appears as a very suitable device to sustain the provision of these new applications.

In a broadband-mobile world, the interconnection is no longer simply "horizontal" between networks but also "vertical" between the access network (facilitated by the card), the Internet and the Application Service Providers. The issue of "Conditional Access" appears to be central, with its specific issues of the interoperability of Set Top Boxes (MHP, Java TV),

cross-owner regulations and so on.

The technological synergies that allow the common delivery of different services (Telephony, Internet Access, Digital TV, Mobile Health , Mobile Payment) to end users appears to be irreversible, even if the roadmaps in this migration trend are different. So there is an urgent need for the development and certification of new cards ready to support this convergence. The card technology needs then to be designed in a way that is independent of the specific terminal to which the card is most often connected.

Even if the approach of TB7 is pragmatic, new theoretical models may be considered. This is necessary because business models for card systems tend to become more complex, since they have to take into account network-specific issues. As online revenues become a significant part of the overall revenue, concerns are growing about (1) Internet fraud and/or (2) Cost of connection for the faster data transmission rates required. Because Internet revenues are still a very low proportion of total card revenues, Internet business models are still much more concerned with growth. However, security may soon become a key differentiator.

2. The Business Case for the Card Management System: Generic considerations

The business model spells out how a company makes money by specifying where it is positioned in the value chain. The functions of the BM can be summarized as follows:

1. Articulates the Value Proposition, that is the value created for users by the offering based on the technology. In the MA context, there may be several levels of users. A CMS can be integrated in the offer of an industrial (first-level user) to a Card Issuer leading a MA scheme (second-level user), who makes the CMS available for Service Providers (third-level user) in order to allow on-line application downloading for the cardholder (end-user).

2. Identifies a market segment, those users to whom the technology is useful and for a specific purpose. (Keep in mind that TB7 is cross_sectoral and addresses all the major market segments)

3. Defines the structure of the Value Chain

4. Estimates the cost structure and profit potential of producing the offering, given the value proposition and value chain structure selected

5. Describes the position of the firm within the value network linking suppliers and customers, identifying the market structure: complementary partners and competitors

6. Formulates the competitive strategy

This document is intended to provide input on points 1 to 4. The competitive strategy and identification of business environment are obviously a private issue for each company. The cost structure is also an internal issue, but some guidance can also be provided.

In any case, any Business Model is driven by the final user demand. There is currently a

feeling of « service-crisis » in the card industry, which hampers the development of the MA market. The BM for multi-application has so far been « card-issuer » centred with little, if any, involvement from the Service Providers (Which act as Acceptors of the MA card for the provision of Services). This is simply because of the extension of the Card Issuer=Service Providers basic equation for monoapplication systems. The evolution of the roles played by each partner in the MA Card means that the Multi-application Card Issuer shall have to strongly consider basic SP concerns when designing the System. This includes soliciting SP participation in business rules agreements, managing the technical aspects of the system, developing an understanding of all aspects of the merchant day-to-day operation, and other activities which may even lead to enabling a direct business relationship (Direct Billing) between an Application Provider and the Cardholder.

4.2   The Aggregation of Services Offer: Marketing Issues

The essential problem is to understand the impact of « aggregation ». As an example, the first business models for e-commerce were based on the fact that the Internet has a very low cost of entry, leading to a short product life. This means that early services have to be replaced by new content aggregators.

These contents may come from different Service Providers, which must be

> *1.Certified* (Security Concerns for the MA card). Different schemes can be considered:

- To rely on a Certificate Tree similar to X.509 PKI architecture, with CA for services and other higher level CA.

- To rely on a third independent authority, within the MA scheme with this specific role (which could be in addition linked to a role of CA for card verifiable certificates).

- To be directly performed by the System Issuer. This could be the case for a Public Administration Authority.

- To be directly endorsed by a Domain Service Operator (NICSS architecture) for its own domain of responsibility.

The final object of the certification is to leverage the role played by the application providers. A basic security condition is that a new loaded application must not jeopardize the security that the card provides to the resident applications.

The certification of an application is an acknowledgement of its ability to be loaded into a card supporting a security policy defined by its card issuer. Once its applet has been certified by a CA, the Application Provider (AP) is expected not to have to undergo a second expensive certification procedure by another CA. The AP is then in a position to offer its product to different MA schemes at no extra-cost and therefore decide to distribute the application through the MA system providing the better business conditions. The theoretical analyses so far performed agree on the fact (External Network Effect of services provided through a Network Communciation System) that the System can only be economically efficient (To simplify it, generating a profit for all the parties involved in the provision of a service with a level of quality to a final user at the lowest cost) when the competition can choose between the different partners (Card Issuer vs Application Providers) and the Abuse of Dominant Position is made difficult.

2.Advertised and their contents made available through enlarged distribution channels. These services have to be provided through different types of terminals, fixed or mobile, in public or in private places in a transparent way. TB7/WP4 is in charge of studying possible ways to get around this issue. The STIP architecture seems a good solution with the additional advantage of requiring low hardware resources to adapt existing terminals.

An additional requirement is that these applicative contents must be provided online through a suitable file format which:

- Minimizes the required bandwidth (Cost and Transmission time concerns)

- Allows the inherent heterogeneous nature of the downloaded information to be managed in an interoperable way by the local browser (embedded in the terminal)

- Requires minimum local hardware resources

To summarize, the problem could be stated like this:

(1) What is the impact on the common business model when aggregating applications which are already offered in a mono-applicative card offer?

    … and conversely

(2) What are the applications which are not profitable alone, and can profit if integrated on the same card? And with what other applications? In other words, Is service-aggregation liable to make profitable any service supported by a card application?

A first conclusion is that these evaluations can only be performed after detailed cost estimations.

This problem is not only raised for the business case. Security concerns (the fire-walling to be provided between data application on the same support) and legal (common share of responsibility). From the business cases we look for synergy and not for effective isolation: e.g. how to add App2 by SP2 to the existing App1 in Card1 so that revenue generated by App1 is increased? In principle, this revenue can obviously be increased by just the fees from renting part of the card memory resources to the Service Provider 2 (SP2).

But the problem here is to understand how App2 can leverage App1. As for any marketing analysis we must remain realistic in the final outcome actually achievable.

Anyway before going ahead we can probably accept the following:

A MA solution (and generally speaking any new product) may only be successful if **1.It is profitable for the Industry** (*for any industry player participating in the production of the Multi-application System)*

    2. It is not very expensive for the final consumer. « Final Consumer» is taken here as the Value Added Chain, made up of Service Providers of different levels and ending up with the cardholder, who's the starting point for the revenue generation chain

    3. It is endorsed by the System Issuer because it fits his business case requirements. The System Issuer is playing the role of an intermediary between customers (demand) and industry

(product) and in charge of specifying a System potentially attracting final consumers.

In addition, sharing the same physical support, involves other marketing considerations:

1. Consideration of competing Service Providers having their applications resident in the same card
2. Flexibility in terms of security/interoperability to be provided to the applications
3. Common agreement on liability share
4. No veto from other participants
5. Need for the application security certification for loading in the card

4.3   The Aggregation of Services Offer: The Technical Approach

4.3.1   Interoperability Issues

In this context, a First technical approach relies on the specification of a modular Multi-applicative Architecture *to maximize the number of possible business models even if the Architecture is proprietary and not interoperable.*

Secondly, from the Card Issuer Point of View, the Multi-application Systems and the Card must be able to be upgraded in a transparent way with no impact on the service provided to the cardholder other than the improvement of the product. Finally, when calling for tenders, the Card Issuer is always interested by Architectures choices which are interchangeable and transparent from the point of view of the system management. This highlights the need for interoperability at system level (currently only the card/terminal interface is interoperable to some extent, rather within a particular card industry like GSM).

In addition, but contrary to a widely held belief, this interoperability is even more important for emerging markets. Before rolling out a new big system, it is always interesting to implement a pilot by operating two competing and *interoperable* solutions before taking the final decision.

This means that the System Issuer must base its specification on an international agreed standard which guarantees the interoperability (that is not always the case). On the other hand, industry must be able to adapt its product to the same standard with a minimum of upgrade.

The roles of the stakeholders of the MA system are to be defined, their relationship clearly established in order to obtain "interoperability at the business level". These roles have already been defined in a number of public specifications (OP, MAOSCO, NICSS). This means that the scheme allows commercial relationships to be established between any pair of stakeholders.

As a "rule of thumb", the proposed Architecture , must provide a clear Interface between "any pair" of stakeholders who wish to cooperate within the scheme. The architecture can be mapped into a graph, where the nodes represent a role, responsible for a series of functions.

These nodes exchange messages and data in a standard way (protocol) to obtain some predefined result which is independent of who are actually playing the roles associated with the nodes.

4.3.2 The limits to the System Architecture approach

In a similar way that the business approach is limited by the technical solutions available, the technical solutions to consider are constrained by cost of ownership considerations. Roughly:

1. *New services cannot add to fixed costs*, because, apart from generating new revenues one of their roles is to contribute to lowering the average cost by service (or application) provided by the System. This means that their deployment is possible since the new service provider is certified (the infrastructure is ready and the MA cards can be personalized after delivery).

2. This involves the integration of the Card Management System in the MA system from the beginning. But CMS deployment, operation and maintenance is not free. The d*ecision to integrate a CMS can only be taken if the range of services is soon to be enlarged*. Otherwise it is "wait and see" (current situation!)

3. Another fundamental decision for the Technical Architecture is the *channel for the payment of fees* and the subsequent management of the payment infrastructure. This is a formidable problem well known and recognized in the financial world and to transit agencies as a killer of positive business models. The MA card is an attractive solution to manage payment systems, because the system in principle allows the sharing of high fixed costs (TB7/WP5)

4. *Aggregation of services= Aggregation of responsibilities* and increased risks for system/card failure because of increased use. A technical solution must be provided to deal with this issue (TB7/WP2).

The application of Data Warehousing solves this problem. But DW is expensive, and raises privacy concerns. In addition it is tempting to sell the data collected from card transactions simply because the DW must contribute to the common effort to generate net revenue. Electronic payments yield significant information about customers and transactions in terms of preferences and buying patterns, which both merchants and card-issuing entities would like to mine.

4.3.3 Integration of Business and Technical Requirements for the Aggregation of Services Offer: The Card Management System

The approach can be achieved by:

1. The ability to change the services supported by the card once it is in the field: these new features must be implemented without re-issuing the card.

This capability to load dynamically after issuance leads to
(1) Greater profit for the issuer

(2) Stronger alliance opportunities

(3) Greater customer retention

(4) Offer Differentiation

2. The independence between Service Providers, Card Issuers and eventual intermediate operators (Domain of Services Operators).

4.4   The Market For Dynamic Loading

The following drivers can be identified for this market:

1. Consumers for more individualized or personalized services

2. New partnerships are being formed to improve brand image

3. New strategies are being followed to increase customer activity and retention.

But the offered product can only have a chance if it integrates the end-user requirements whilst preserving the Card Issuer/Service Provider interests. Both must be clearly understood.

At this time, a subset of initial requirements can be listed:

1. The smart card must allow the simple addition of new services in order to support new product lines, new partnerships, or the changing needs of the consumer.

2. The card must also allow the removal of redundant services that are taking up space on the card and are no longer needed under strict card issuer control.

3. It may also need to support the addition of temporary services, such as a ticketing application (Voucher) , that the consumer may only need for a short period of time.

4. To allow a card to be reconfigured after issuance, the card needs to have a secure mechanism that allows the card to determine that the reconfiguration request has been approved by the card issuer. With multiple-application cards this is commonly in the form of an application delete request, or an application load request message. These requests use cryptographic techniques so that the card can verify that the request is genuine and also the credentials of the requestor **(request authentication)**.

5. A complete system, therefore, requires the card issuer (or an authorized third party) to have a host system that provides a database of cards and a description of the functionality/applications that are currently loaded onto the cards. This host system is referred to as Card Management System (CMS). Management rules for the CMS must comply with the European Directive on Privacy Rights.

Rationale

1.Managing software on the card is a cheaper solution for resolving technical issues than re-issuing the card, and as long as easy-to-use multiple terminals are available is simpler for the consumer too (STIP approach).

2.A smart card that can be reconfigured after issuance extends the commercial life of the card

and makes the business case much more attractive to card issuers:

(1) It allows for new services to be introduced to an issuer's customer base, increasing the importance of the issuer to the customer.

(2) It also enables the issuer to allow access to their customer base on negotiated terms to close alliance partners.

(3) It offer issuers an opportunity to increase both their profits and their presence in the end-user's mind (personalized relationship).

(4) It maintains the issuer's competitiveness with new services introduced at a later date by other issuers.

(5) Nevertheless, issuers that are quick to implement new services still have the advantage of establishing their market share at an early stage and, because the issuance of smart cards creates an opportunity to substantially shift customer loyalty/numbers between issuers, dynamic loading generally means that early issuers gain competitive advantage.

4.4.1 The Past

Dynamic reconfiguration of cards has been in use in the GSM SIM market for a number of years. Network operators have termed this Over The Air (OTA) management and it has been used to manage the small file systems in SIM cards.

The host system also needs to maintain a library of applications and be able to generate delete or load requests, when necessary, as a card is presented.

There are a number of leading providers of host systems, including companies such as ACI, Cards Etc, Hitachi, Softcard, Oberthur and Platform7/Datacard. Issues that these providers have had to overcome include:

- The variety of communication media such as GSM, internet, Digital-TV and dial-up communications at the Point Of Sale (POS).

- The close relationship between communication of application management and the various scheme transactions – does the card management system hand-over transactions to the legacy network or expect the legacy network to hand-over card management activities?

- The fact that some card schemes require the issuer to provide their own cryptographic services to control the card base. This is seen by some issuers as desirable, but adds complexity to card issuance.

4.4.2 Standardization Issues for CMS

1. It is healthy for the multi-application business that there are differences in the methodologies of application load and management mechanisms. This diversity in the offer brings innovation and quality.

2. This diversity does not complicate the issuer's task of managing their card base. The idea is that the same Card Management System be able to address Java and MULTOS cards. From the card issuer point of view, a business case is supported by a modular architecture made up of interoperable subsystems allowing competitive play between interchangeable solutions.

3. From this point of view it is highly desirable that MAOSCO and Global Platform cooperate order to define mechanisms for interoperability. The need for interoperability - for devices that coexist and that can collaborate where appropriate - is fundamental to mass adoption. The goal for Global Platform and MAOSCO is to remove the barriers to successful interoperability whilst maintaining the pace of innovation and diversity in the services and products that the emergent smart card industry needs.

4. The technical architecture TB7 is looking after is based on a

backbone/platform or common virtual layer linking Terminals and Back-Office subsystems (Application Servers, Payment Gateways, IMDES, Card Management System) in a transparent way. This means that irrespective of their specific technology, the Card Management System must present the same interface to the common Platform. TB7 strongly encourages this effort to have compatible, fully interchangeable solutions. The technical issues concerning similarities and differences, the benchmark of both approaches and ways for convergence will be analyzed by WP4.

5   INDUSTRIAL ECONOMY METHODOLOGY BASED APPROACH

In order to guide the work some standard analytical procedures from industrial economy methodology (structure of the supply, structure of demand, identification of market entry barriers) can provide some insight. Keep in mind that the fundamental purpose remains to get a better understanding of the multi-application market, in order to work out rational strategies for its promotion

5.1   Structure of supply in MA market

Analysis of distribution channels and service networks. Distribution systems prevailing on the market and their importance. Estimation of the extent to which MA service distribution is performed by the Card Issuer and/or third parties, who may or may not be members of the MA scheme.

5.2   Structure of demand in MA market

Analyze the structure of the demand in terms of:

(1) The phases of the markets, take-off, expansion, maturity and decline, try to forecast the growth rate of demand)

(2) The importance of customer preferences, in terms of brand loyalty, product differentiation and the provision of full range of MA products and services

(3) The degree of concentration or dispersion of MA card issuers

(4) The importance of exclusive distribution contracts and other types of long-term contracts

(5) Evaluation of the extent to which public authorities, government agencies, state enterprises are important participants as a source of demand for MA cards and systems

(6) Identification of the largest independent customers in each affected market (banking, transport, telecommunication, public administration)

5.3   Analysis of Multi-application Market Entry Barriers

Significant incomers into the MA card market
Analysis of the various factors influencing entry in the MA market

(1) The total cost of entry (R&D, establishing infrastructure for service distribution, communication, promotion, advertising costs)

(2) Any legal or regulatory barriers to entry, such as government authorization (in the case of cards providing cryptographic services, for example, regulation on communication cyphering. European Directives on individuals' privacy or electronic signature regulations, and impact on the MA market).

(3) Restrictions created by the existence of patents, know-how and other IPR in these markets and any restrictions created by licensing such rights. In the MA market consider:Card manufacturing, Protocols and Cryptographic Algorithms, Programming languages, Database management software, Licensing for Platform Implementation)

(4) The extent to which each of the major players are licensees or licensors of patents, know-how and other rights relevant to the MA market

(5) The course of technological development for these markets over an appropriate past period of time (product/service development, production processes, new protocols/algorithms, web server technology, new development languages)

(6) The cycle of innovation for products and service of the MA market

ANNEX: INITIAL ANALYSIS OF DOMAINS OF CARD APPLICATIONS

To start the discussion, the following (disputable!) major groups of Card applications are suggested. This division is purely functional.

(1) Proof of Identity: On/Off line. Biometric/PIN authentication. With electronic signature capability. Personalized with a Certificate.

(2) Payment: Debit/Credit, Prepaid (EP, Phone card). In some way the payment is an inter-sectorial application.

(3) Proof of ownership rights for access to services

> On-line: Mobile, Pay per View

> Physical Access to facilities: Public Transport, Reserved Areas

(4) Portable Database:Requiring strong/selective external authentication for secure channel set up for subsequent read/write operation with data probably requiring encyphering. E.g.: Health Card. These data typically are to be linked to large databases for back-up purposes..

(5) Applications in which electronic signatures play some role. This case is particularly critical, because reliability of the design rely on right integration of PKI into applications. At the card level ISO standardization is in progress to specify a sub-directory « e-sign oriented » based on PKCS#15. Such architecture allows for sharing of e-sign services for card applications requiring them.

Multi-application is an opportunity to integrate PKI features in existing cards. The issue is how the PKI will be added to the application. Creating a new version that intrinsically supports PKI provides the best integration, but the cost can be high to update existing software.

Caution: PKCS#15 supports a file structure ISO 7816 compliant. Current architecture for Multi-application platform is «application-oriented » rather than « file-oriented », and some problems remain to match directly a Java or Multos architecture with a PKCS#15 directory. In any case, the ISO/IEC 7816 standard provides for the necessary mechanisms, which unfortunately remain largely misused by developers.

(6) Logic behind issuance of MA cards. Investment based on increased revenue opportunities, typically as Value added services capable of being delivered via network. What card? What Infrastructure? Who will pay for the Infrastructure?.

(7) Business models and their relationships with contractual terms

- ❑ Funding and fee arrangements

- ❑ Contract Duration

- ❑ Incentives

- ❑ Contract Expiry / Termination Costs: Consideration of how to ensure continuity of

service on termination or expiry of the contract or /and to engage in an alternative contract if required.

(8) Impact of multi-application project on stakeholders

- ❑ Impact on Issuers
- ❑ Impact on acquirers
- ❑ Impact on system integrators
- ❑ Impact on payment scheme networks and brands
- ❑ Impact on vendors

« ONE-TO-ONE MARKETING »

The individual is identified and individual-specific services are provided. This approach applies both to what services are provided and how these services are presented and can subsequently be selected by the cardholder (user interface issue).

In addition, probably more and more applications will rely on digital signature for authentication purposes. A service provider might, for example, agree to accept a privately issued digital signature card and the corresponding certificate as sufficient proof of identity for its own purposes.

Rather than adding a new application, a simple attribute certificate granting access to the services and signed by the service provider might be linked to the identity certificate of the card.

Such an option could be used for the implementation of « white cards »

ANNEX: INTRODUCING GLOBAL PLATFORM & MAOSCO

GlobalPlatform is an international, cross-industry forum, founded in September 1999 to focus on the development, management and promotion of specifications for multiple application smart cards, smart card applications, and enabling devices. With support from its global member organizations, which totalled 50 in March 2001, GlobalPlatform promotes a standard framework facilitating the implementation of smart card programs in any industry around the world. GlobalPlatform allows flexibility in the choice of technologies and vendors through an emphasis on open standards for cards, terminals and support infrastructure.

The Open Platform card and terminal specifications developed by Visa are the first open standards adopted by GlobalPlatform and will provide a solid foundation from which the organization will define the future of multiple application smart cards.

MAOSCO is a consortium of thirteen of the world's most innovative smart card companies and was formed in 1997 to drive the adoption and manage the on-going development of MULTOS, the most highly secure open multi-application standard platform for smart cards. MULTOS consists of an operating system designed specifically for smart cards, an application development language, specific silicon chip families, and the supporting key management infrastructure. MULTOS is licensed on an open, non-discriminatory, royalty-free basis and is a standard for multi-application smartcards across all industry sectors. Third party software developers can develop MULTOS applications or custom design Value Added Services for the card issuer using both low level and high level languages and publicly available API's.

A number of companies, such as Keycorp, Infineon and Telstra are members of both GlobalPlatform and MAOSCO. Many smart card issuers will issue both MULTOS and Open Platform based products, a clear example of the growing need for smart card management systems (SCMS) to be able to easily identify which platform they are dealing with on any one card. MAOSCO and Global Platform have, therefore, co-operated to identify mechanisms that will allow an SCMS to easily identify the capabilities of the platform with which it is dealing. This will ease the development of the SCMSs, and remove any current trial and error identification mechanisms, making these critical systems easier to develop and easier to use.

TECHNICALITIES OF THE SOLUTION

The common framework developed by GlobalPlatform and MAOSCO defines a Card Management Identification mechanism that enables smart card systems to identify the on-card technology, whether it is MULTOS, Open Platform or any other standard. It allows a card management system, or any other system, to handle various smart card platform technologies, using common commands to automatically determine the card platform type, after which appropriate platform and management processes can be performed as required.

This Card Management Identification mechanism makes use of two ISO 7816-4 commands that can be issued to the smart card at any time. These commands give access to information in the card which ISO 7816-6 calls 'card data'. This data can provide a range of information, for example:

- The type of platform and its version, indicating to the card management system what management functions the card supports and how they can be invoked.

- The card identification scheme ensuring that the chip identifier can be made globally unique, so that the card management system can unambiguously identify the smart card.

Specifically, the two ISO 7816-4 commands are:

- A special form of the 'SELECT' (or 'SELECT FILE') command, providing unambiguous treatment of the second command.

- The 'GET DATA' command for retrieving the 'card data' information from the card.

'Card data' includes a template containing the following data elements:

- The Card Management Identification data object, containing an ISO object identifier, identifying the card platform organisation, the platform type, and its version.

- Optionally, the Card Identification Scheme data object, containing an ISO object identifier, identifying the card identification organisation, the identification scheme, and the unique smart card identifier.

- The ISO object identifier of the 'Tag Allocation Authority'. This is the organisation that assigns tag values to the various data elements of the template.

The template is ASN.1 BER encoded and uses a 'compatible tag allocation scheme', according to ISO 7816-6. With its tagging approach, this template can be easily extended to cover other platform configuration information that may be defined in the future. Using a tag allocation scheme approach, and object identifiers, allows the card management information to be universal, while the future addition of data elements and their associated tags remains possible.

By leveraging the widely used ISO 7816-4 commands and a minimum set of data, this framework causes minimal overheads in memory, input/output and processing to any existing and future smart card platform. It does not compromise privacy requirements, because it primarily provides platform technology and management information. It simply identifies the smart card, but not the individual.

Targeted for card and application management activities, this framework is generic and can be extended to smart card platforms other than Open Platform and Multos. It allows continuing platform differentiation and competition and has no impact on the applications themselves and

their interaction with users: cardholders, merchants, or acquiring systems and devices. It is backward compatible with existing MULTOS and Open Platform cards and can be implemented today. The solution is integrated into release 5 of Multos specifications and release 2.1 of Open Platform card specifications.

PRACTICALITIES FOR GLOBALPLATFORM

Because the solution is compatible with existing Open Platform technology, backward compatibility with existing Open Platform cards can be ensured. A small application is added, pre-issuance at the personalisation stage, or even post-issuance in the field, to handle the Card Management Identification template. The card management system should be able to select such application and retrieve the relevant information. If an existing Open Platform card does not contain the Card Management Identification template, the card management system should be able to fall back to existing trial-and–error mechanisms – in other words try to select Card Manager and retrieve the (more limited) management information. With the issuance of Open Platform cards compliant to release 2.1 of the Open Platform Card specification, such a situation will no longer occur and smart cards will respond appropriately to card management system queries.