Open Smart Card Infrastructure for Europe

v2

Volume 5: **Multi-applications**

Part 5: **Integration of Multi-application Systems**

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

Integration of Multi-application Systems

eESC TB7 Contacts:

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

Secretariat : MTA brains@mta.fr

WG5 Chair : M.Mustafa mmustafa@ibigroup.com

Document History

Version	Date	Contributor(s)	Main Alteration vs. previous revision
WDv1.0	23 Oct 01	L Gaston, TB7 Chairman	Creation of the document
WDv1.1	May31th 02	M.Mustafa, WG5 Leader	Revised document based on comments received at WG5 meeting in London, April 11, 02
WDv2.0	Nov15th 02	M. Faher	Appendix: Integration of EMV system and MA infrastructure
v1.0	March 03	L Gaston, TB7 Chairman	English Review

EXECUTIVE SUMMARY

This report summarises key issues for the integration of multi-application smart card systems. The document is being prepared by working group 5 (Integration) of Trailblazer 7 (multi-application systems) of the EU smart card charter. The document addresses the following key objectives:

- To start discussion on how system integration issues can be addressed;
- To identify some fundamental Technical/ Procedural constraints;
- To contribute in providing guidelines to build the business case for multi-application system integration;
- To address along with other working groups of TB7 issues of security needs, business needs, associated risks and benefits
- TO identify scenarios for migration to multi-application systems including:
  - Existing multi-application systems' adaptation to new functionalities
  - Paths for achieving a Multi-Application system from an original single application one;
  - Integration of new providers
  - Evolution from closed to open system
  - Integration of a payment application

TABLE OF CONTENTS

1 Introduction

WP5 is justified because of the central role of the system integrators when deploying a multi-application scheme. The smart card is only a part of a wider system infrastructure that involves user interface devices, networks, transaction processing, card management and other back-end components.

When the need for a smart card scheme has been identified several acquisition options are possible:

- Make direct use of an existing card/scheme;
- Negotiate the renting of memory space in an existing card and integrate it through a CMS;
- Starting with a new card, trying to offset the cost by sharing the space available in the card memory.

WP5 is intended to provide the toolbox necessary for the effective deployment of a multi-application system, by analysing different standard scenarios (see Executive Summary).

Regardless of the fact that only very recently experience has been gained in integration of real MA systems, WP5 wants to analyse the available options for supporting a business model and then setting up realistic procedures to integrate MA systems whilst minimising the total cost of ownership (TCO).

The feeling is that card issuers require a higher level of comfort not only with the business case economics but with the technical case as well.

Keep in mind that a MA system is a complex technology with many available options, and obviously not all options are required for every business process (transport public sector is not currently very demanding of card management systems). The integration procedures must, however, recognise that the deployment of MA infrastructure may require upgrade, expansions or other incremental costs that must be minimised from the beginning.

WP5 assumes that the User Requirements, Legal and Privacy Issues are clearly understood and specified. The Business Models have been produced, the resources are available and decision on the scheme deployment taken.

WP5 covers the major issues to be considered for practical integration of MA systems in order to:

1. Enhance the value of the MA system for the participants by increasing revenue
2. Reduce Infrastructure Costs
3. Shorten Deployment Cycle
4. Minimise Payback period
5. Enable later infrastructure evolution

A fundamental factor affecting the potential of the multi-application systems and arrangements between business sectors is the nature of the financial implications of such efforts from both the revenue and the cost side.

There will be various capital and operating costs associated with implementing any new system or just upgrading it, and the net effect on any participating partner (financial institution if a payment application is included or other) is difficult to estimate because of the lack of publicly available in-field results.

***Important Note**: This document is intended to start discussion on WG5 of TB7. In this document, system integration will be analysed in the context of a particular implementation. Extrapolation to a different context is hazardous. The author is aware that TB7 is inter-sector, and that focusing on specific scenarios is somehow inconsistent.*

2 Definition of terms

This paragraph is justified because in the transit industry sector the terms are somehow different. TB7 members reviewing the document are kindly invited to make any comment they feel relevant.

System Integration refers to the degree to which cardholder-facing, internal and partner-facing systems and applications are integrated with each other. Ideally, tighter system integration is usually correlated with higher financial returns.

Open System In this context, it usually refers to a payment system in which an outside entity's card (bank card) is accepted for use by a transport operator.

In a truly multi-applicative context, it refers to the system where multiple card issuers and multiple service providers can coexist. Such a system needs to be supported by standards.

Closed System The card is issued by a single entity and can be used only for that entity's services. Interoperability is not an issue. The system is proprietary and the specifications are secret. An example could be a Pay-per-view system. An e-purse which can only be used in the context of the service providers under the control of the purse emitter is also closed.

Multipurpose versus Multi-application Card

> ***Multipurpose Card*** refers to a card with a single application, but that can be used to get access for multiple merchants and multiple services. A payment debit bank is a multipurpose but single applicative card.
>
> A SIM card allows access to different mobile networks operated by different entities, but the service offered to the user is the same and cannot be considered multipurpose.
>
> ***Multi-application Card*** refers to the card hosting different applications that can be selected in an independent way. Once the application is selected, it can be run as if the card was mono-applicative with the data access restrictions imposed by the multi-applicative OS. The selected application can then be multipurpose.

3 System Integration Design, Planning, Organisation

Implementing a MA scheme involves many steps , including preparation, planning, organising, designing, developing, deploying, training and supporting the partners and educating final users.

In order to provide some guidelines for practical System Integration, this chapter is divided into two sections:

- *The first section specifies « The Core Principles » intended to provide a baseline for best-practice procedure when integrating a multi-application system.*
- *The second one, is a proposed methodology to apply the Core Principles in a real development context*

3.1 The core Principles for Multi-application System Integration

They are expressed in a deliberately general way to help ensure that they can be useful and durable. They do not represent a blueprint for the design or operation of any individual system, but suggest the key characteristics that all operational Multi-application system should satisfy. It does not provide a single model for every practical application of the core principles.

These principles are intended for use as generic guidelines to encourage the design and operation of safer and more efficient Multi-application Systems, integrating Payment services.

1. ***The system should have a well-founded legal basis under all relevant jurisdictions (WP2)***

   The rules and procedures of a system should be enforceable and their consequences predictable . A system which is not legally robust or in which the legal issues are poorly understood could endanger its participants. Poor understanding can give participants and even final users a false sense of security, leading them, for example, to underestimate their risks and/or to subcontract services they may repudiate in the event of incident.

   The legal environment relevant to Core Multi-application Systems includes the general legal infrastructure in the relevant jurisdictions (such as the law relating to contracts, linking, terms and conditions for payments/settlement/clearing, securities, banking, debtor/creditor relationships and insolvency) as well as specific statutes, case law, contracts (for example, payment system rule, share of responsibilities) or other relevant material.

   The jurisdiction under whose law the system's rules and procedures are to be interpreted should be specified clearly. In most cases, the most important legal environment will be the domestic one, although, in particular where the system involves cross-border elements such as foreign bank participation or the use of multiple currencies, it will also be necessary to consider whether there are many material legal risks stemming from other relevant jurisdictions. *At an European level, TB7 may recommend a European Directive which could harmonise the*

legal framework for multi-application systems deployed within EC borders (domestic one, in the context of eEurope/SCC).

2. ***The system's rules and procedures should enable participants to have a clear understanding of the system's impact on each of the legal and financial risks they incur through participation in it. This involves the performance of a comprehensive Risk Analysis at the very beginning of the Project.***

   Participants, the System Operators, and other involved parties – including final users- should understand clearly the legal/security/financial risks in the system and where they are borne (point 3 next). An important determinant of where the risks are borne will be the rules and procedures of the system. These should clearly define the rights and obligations of all the parties involved and all such parties should be provided with up-to-date explanatory material. In particular, the relationships between the system rules and the other components of the legal environment should be clearly understood and explained. In addition, key rules relating to security/legal/financial risks should be made publicly available

   Obviously the existence of a previous common legal framework should facilitate the practical implementation of point 2.

   The purpose of a risk analysis is to focus the decision maker's attention on the financial, technical, and schedule risks associated with the option under consideration and to counter-balance positive financial indicators with real-world factors that could keep the option from reaching its estimated potential. In our case, because MA systems are an emergent market, these "real-world" factors are difficult to quantify.

   Because any look into the future involves an inherent level of uncertainty, business case analyses for MA systems are subject to risk. Once again, this risk is more evident because of the lack of previous significant experience in large-scale MA systems operation.

   Several reliable methodologies for risk assessment are currently used in the industry. They may be used to Identify the risks associated with the MA smart card investment so that they can be managed and controlled. After that, the use of ***cost risk analysis tools*** is recommended to account for any cost risk associated with your estimates. Some additional considerations are mentioned in the next paragraph.

3. ***The system should have clearly defined procedures for the***

   1) *Management of any identified risk for the different stakeholders and, in particular, for a new incomer.*
   2) *which provide appropriate incentives to manage and contain those risks*

      These risks mainly refer to :

      1. *Risks inherent in remote payment systems*
      2. *System Risk : The likelihood of an accidental or malicious attack on the system resulting in loss for any stakeholder (System Operator, Card Issuer, Service Provider…)*

3. *Fraud Risk : The likelihood that either party deliberately defaults on the transaction*
4. *Risk of System failure due to technical incident (see below)*

The threats are assessed from the perspective of the end-user (cardholder) and of the merchant or recipient of the funds, as well as

1. The rules and procedures for a systemically important system are not only the basis for establishing where security/financial risks are borne within the system, but also for allocating responsibilities for risk management and risk containment (to be addressed by WP2). These risk apportionments have direct contractual implications.
2. A system's rules and procedures should therefore ensure that all parties have both the incentives and the capabilities to manage and contain each of the risks they bear and that limits on credit exposure are particularly relevant in systems involving payment services (example e-purse integrated in a multi-application card issued by a small/medium sized city).
3. There are a variety of ways in which risks can be managed and contained using both analytical, operational procedures and technical design :
   - Analytical procedures include on-going monitoring and analysis of the credit and liquidity risks participants pose to the system.
   - Operational procedures include the implementation of risk management decisions through limits on exposure, by pre-funding or collateralising obligations, through the design and management of transactions queues or through other mechanisms.
   - For many systems, the use of risk management processes that operate in real time will be a key element in satisfying Core Principles 3.
   - These can include redundant design for some key elements of the system in order to improve overall reliability, and collateral arrangements with other MA system schemes to take over in case of incident.
4. As mentioned, recommendations for specific solutions are in principle out of the scope of TB7. However, in the context of integration of a Payment function in the MA system, the quantitative analysis of the incremental cost for tighter levels of security is strongly recommended. Maximum security implies maximum cost.
5. Current card schemes are more concerned with authenticating the card and to protect against the merchant fraud. Cardholders (WP2) may also be expected to prefer schemes which help to authenticate the merchant, specially for e-commerce transactions. This may lead to a decision to integrate PKI services in the System . These services should be supported by the card, which provides the authentication environment and digital signature capabilities able to protect the merchant, the payment system provider and the final user. In turn, PKI may serve as a secure authenticator service opening the door to new services (e-commerce, m-commerce) in an open system.

6. The idea is that System Integration may act as a catalyser (Integration of a Payment Function leading to integration of PKI) allowing the aggregation of new services, leading to multiple alternatives and new business cases. Even if not considered by the System Operator in short, TB7 recommends an initial evaluation of these alternatives (cost/revenue and risks). The decision to support the Multiapplication System by an open card type Java or MULTOS, and to design the system based on a Virtual Network Modular Layer (STIP), which enables low cost and fast integration of new services makes the system far more attractive.

7. It is important for the parties to have the incentive, as well as the capacity to manage and contain any identified major risk for the system security/functionality. All the participants in the MA system have the possibility (to be minimised) of jeopardising the security of the other partners. One way might be the provision of incentives by means of the pricing structure, including possibly contractual penalties. This can have an effect on the promotion of safety and efficiency overall. But keep in mind that Pricing polices determine the cost of transactions to the users of the system (Service Providers, end-users). Inappropriate policies may drive system users to cheaper but less safe systems. Some input on this issue is provided in # 5 and #6.

4. ***The system should provide prompt final settlement on the day preferably during the day and at minimum at the end of the day (NOTE :Obviously this is a negotiable issue, subject to the individual contractual trends and conditions linking the System Integrator with the other system stakeholders).***

   The multi-application system should be designed so that it can achieve final settlement on the day under normal circumstances. A transaction that has been submitted to the system and has passed all the risk controls is accepted by the system for settlement.

   The objective is to minimise the exposure of the system participants to financial risks, for the period during which settlement is deferred (between acceptance of the settlement and final settlement). The principle here is that these credit risks must be monitored and controlled, so that limits must be applied by the system operator on the maximum level of risk that can be created by any participant.

5. ***The system should provide secured and reliable revenue management and clearing functions.***

   The financial settlement requirement (*outlined in requirement 4 above*) highlights the fact that clearinghouse is a particularly important element, because it is responsible in relation with the other partners (under system operator supervision and following clear specific procedures) for managing many of the key support functions of the system including revenue management and settlement (fee collection, apportion revenue, revenue clearinghouse), customer service and perhaps marketing and communication.

6. ***The system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion and daily processing***

Card based Multi-application schemes are an emerging market, involving multiple partners taking financial and technical risks, and sometimes with no clear business cases. In order to motivate commitment from stakeholders, the system must from the beginning be based on clear procedures in order to deal with possible failure scenarios and the way to manage them.

1. The purpose of a system's business continuity arrangements is to seek to ensure that the agreed service levels are met even if one or more components of the MA system fails.
2. The MA system operator and, where relevant, the participants and infrastructure service providers should carry out a formal exercise to plan arrangements to provide continuity of the service in a variety of plausible scenarios. These scenarios could involve :
    - The failure of each of the central components, shared by each partner
    - The participants' components
    - The telecommunication infrastructure
    - The suspicion of hacking
3. Reliability of the Service provided by the MA system, can be improved using classic techniques like use of redundant equipment for those components identified as more liable to fail and/or critical from the system security point of view.
4. The interoperability of MA systems should promote collateral arrangements between different System Operators in order to take over, at least partially, the management of a failed system. The difficulties in this area are political (get undue information from client base of a competitor) rather than technical. Procedures for such agreements in case of disaster could be embodied in Schemes based on the Financial System adapted to the MA system needs.

7. The system should provide a means of making payments which is practical for its users and efficient for the merchants and end-users and the Payment System Provider (Financial institution)

Two major considerations have to be taken into account :

- From the cardholder point of view, flexibility in the choice of the payment means is an important point. Depending on the amount to be paid, several ways can be considered : Debit./Credit Card, billing, e-purse, micropayment. It appears that currently most of the e-commerce transactions abort because of lack of confidence of the cardholder in providing their bank account data over the net. The cardholder specific requirements for e-payment is a paramount issue for which WP2 is expected to provide some insight. On the other hand, ideally the payment activation procedure in terms of ease-of-use should be irrespective of the specific terminal(fixed or mobile, private or public). The most suitable payment means and the corresponding fee should only depend on the absolute value of the transaction. It would be nonsense to kill one type of payment just for lack of friendliness. In the multi-application context, several business cases rely on an efficient

micropayment scheme at a minimum cost for the service provider. TB7 will ask TB5 for recommendations concerning an adapted micropayment scheme.

- From the merchant, point of view, the critical issue is the guarantee of being paid for the service it provides. This means that the card (cornerstone of the security of the system) has to certificate the elements of the transaction that prevents the cardholder from repudiating the payment. Currently, the most advanced way to obtain this is by a digital signature produced by the card. Payment and funds-transfer applications have a natural affinity with traditional e-security functions (authentication, confidentiality, non-repudiation). In the multi-application card context the integration of the payment function is beneficial for the parties involved:

    1. For friendliness reasons for the cardholder
    2. For merchants, because electronic payments yield patterns about consumer preferences. This creates a personal privacy issue (WP2)
    3. For the payment institutions that can charge the merchants. Because the volume of transactions in any particular bank card system is determined by the interactions of cardholders' decisions to use their cards and of the merchants to accept them, we must expect that the merchants may have some control on the interchange fees they pay the banks.
    4. The above problem can be generalised in a multi-application context, where there are cross-relationships between the card issuer and the different service providers, that generate revenue from the use of the card, and that, in return, shall be charged by the card issuer and/or the system operator. The estimation of the interchange fees that optimise the revenue for all the stakeholders of the MA system is an interesting, yet not easy to solve problem. Some guidance is provided in #6.

8. The system should have objective and publicly disclosed criteria for participation, which permit fair and open access, for Service Providers

This means that the System Operator establishes a realistic business structure. The basic elements of this structure include:

- Ensuring that the roles and responsibilities of the participants in the programme in designing, implementing and operating the system are clearly defined. These roles depend obviously on the system architecture. Card Management Systems have for example their own well-defined roles which are not found elsewhere.
- Roughly any MA system has the following roles : Cardholder, Card Issuer, System Operator, System Administrator, System Clearinghouse responsible, Domain of Service Provide, Service Provider, Payment Service Provider. Obviously the same organisation may simultaneously play several roles.
- This business structure is necessary for :

1. Identifying what the system will cost, the expected revenues for each partner, how the system will be financed, and benefits and how risks and benefits will be shared among the participants.
2. Considering the advantages and disadvantages of alternative management and financing options
3. Finally to create a business case for any stakeholder. Any participant in the system must be convinced of the benefit he will derive.

9. The system's management arrangements should be effective, accountable and transparent

Participants need to understand the risks they bear. System Operators should therefore have rules and procedures that :

- Are clear, comprehensive and up-to-date
- Explain the system architecture, the rationale for the design choices, its timetable and risk management procedures
- Explain the system compliance with applicable law, basic roles and responsibilities
- Set out decision and notification procedures for handling abnormal situations and the way to deal with them.

The basic management strategies for a MA system will depend on the nature of the system (open, closed,) and the legal organisation which is operating it (Public, Private or Public/Private partnership).

3.2 A proposed Methodology for Multi-application System Integration

1. Definition of Business Objectives

- Maximise revenues from existing clients
- Minimise the cost of finding and acquiring new clients
- Reduce costs, to share infrastructure cost
- Set up new strategic partnerships
- Leverage of existing services by integration of new applications
- Innovative business model from m-commerce new on-line services

2. Identification of user needs and constraints(WP2)

- Fast secure access to on-line services through different Terminals (fixed or mobile)
- Service Provider authentication (support PKI)
- Privacy
- Flexibility of the payment scheme, depending on the customer needs (billing, micro-payment, debit/credit card)
- Independent of the transaction gateway (fixed or mobile)

- Scaleable level of security depending on the amount of the transaction
- Common easy-to-use User Interface between different access environments,

3. **Identification of Service Provider Requirements (WP2-WP3)**
   - Multiple channel of Distribution with a similar level of friendliness and security
   - The system provides the Proof of the Transaction which prevents the repudiation by the customer
   - Fair interchange fees
   - Low cost of readers and authentication hardware
   - Confidence in the longevity and/or free upgrade of the technical solutions
   - Secure storage of the data application they own
   - Client on-line authentication
   - Profitability assessment from revenue modelling
4. **Identification of Institutional and Legal constraints (Addressed by WP2)**
   - Legal and regulatory requirements to be addressed : Digital Signature, Privacy, e-commerce
   - Whether the system will be managed by a transit System Operator (transport operator) public or private or by a financial private entity
   - The types of entities involved, their roles and their legal and organisational relationship.
5. **Evaluation of Aggregation of Services for new revenue streams (WP3)**
6. **Evaluation of Payment Methodologies (WP4)**
   - Business Models for Payment Service Providers
   - Financial impact of leverage of interchange fees
   - Estimation of best policy for interchange fees price to stimulate demand
   - Security Services to be provided for payment transactions
   - Micropayment low cost schemes
   - Optimisation of payment function fixed and transaction costs
7. **Methodology for Data Collection and Analysis (WP4)**
   - Data Mining alternatives
   - Privacy considerations/issues
   - Conditional Access to transaction Data
   - Centralised versus Decentralised issues
   - Determination of consumer patterns
8. **Migration path from existing technology : Identification of Integration alternatives and data sources**

- Card Technology
- E-purse integration (WP3)
- Card Management System Integration
- Data Capture and Exploitation System Integration
- Back Compatibility with existing infrastructure
- Technological evolution planning

9. Perform Initial Business Case Analysis (WP3)

- Cost Structure
- Revenue Evaluation
- Financial return for each Identified Alternative, cost/benefit or other structured analysis
- Identify Resources
- Risk Assessment for the Business case

10. Compare and Recommend the Business case

11. Develop Decision Choices

12. Consider your possible partners

- Business Drivers
- Expected costs and benefits analysis for each participant
- Capital and operating costs . Who will pay for them ?
- Potential cost savings, new revenues and other non-financial benefits, and distribution amongst the participants

13. Planning, Deployment and Operation

- Planning the System
  - Architecture Planning
  - User Impact
  - Support and Administration of the System
  - Infrastructure Impact
  - IMDES Integration
  - Legal and Policy Considerations
  - Security Policy Models (see #4)
- Deployment Considerations
  - Testbed
  - Vendor negotiations
  - Installation

- Pilot
- Limited Deployment
- Final Roll out

More specific System Administration issues are considered in next section

4 Multiapplication System Administration and Migration Paths

4.1 Generic Considerations

The new incomer theoretically has to be able to leverage the business case for the System Operator acting as a new revenue stream.

But the new applicant to integrate a MA system has to be convinced of the benefit of its participation. The #3.1 guidelines have been set with this objective in mind. In a more concrete way, the incomer needs to be aware that :

1. The card scheme is properly administrated
2. The scheme must be made attractive to users in terms of cost, user friendliness and suitability of all applications which share the card
3. The roles and responsibilities of the system operator and service providers for monitoring and facilitating a smooth flow of payment through the system are clearly defined

4.2 Multiapplication System Management Overview

The problem is the following : Some organisation is responsible for the economic exploitation of a service (which may in principle range from a Public Transport Infrastructure to a Web Portal for e-/m-commerce on-line services). This organisation may be private (a bank) or public (a not privatised transport operator, if any).

This organisation issues a Card to access the service after cardholder authenticator by the card itself (The Service Operator only trusts what the card it has launched says). If the card decides that the cardholder is authentic the Service Provider grants the service after correct execution of the corresponding application resident in the card.

The management of the Volume of Data generated by the issued cards (transaction data, certification, billing, payment, renew of the cards, downloading/upgrade/deleting of applications, hot-line, re-issuance of lost/theft cards, infrastructure monitor and maintenance) is not the core of its business (It's not so amazing. Banks always complain that they loose money with their payment services, it is reasonable that System Operators and/or Card Issuer collecting revenue from specialised services might have a similar sight).

The card issuer organisation may then decide to subcontract or not the day-to-day management of the system. The point that matters here is how the nature of the system impacts their Administration and Management roles. Different approaches are thus possible following the intended degree of « openness ».

Notes:

1. Closed Systems (single or multipurpose) are out of the scope of TB7, which focuses in principle on open multi-application systems: a system supported by a card in which any service provider may download the data application of its own provided that it fulfil a certain number of conditions (for example to be certified

by the Card Issuer or by a trusted authority, or does not to take up more than a certain memory size).

2. Our objective is to create competition between Multi-application Systems to « attract » the best Service Provider applications. This approach is then the exact opposite of the closed mono-application (even multipurpose) system, one card issuer which is also the merchant/service provider. This scheme obviously simplifies everything because the card issuer endorses the whole responsibility, he is free to organise the system's management on his own.
3. However, WP5 is intended to analyse the best procedures to allow these closed systems to expand towards « openness ». The systems' administration of an open system «from the beginning » differs from a closed one. But for business purposes, a former closed system shall have to keep their old management practices to have a chance to survive in its new context. The new business opportunities must never jeopardise the existing profits.

4.2.1 Management and Administration of Open and Closed MA Systems

For simplicity, the exposition that follows concentrates on an eventual co-brand arrangement between a Public/Private Transport Operator and a Financial Institution, although the basic analysis applies more generally.

The e-purse was felt in the past to be the common application linking both industries. E-purse is specially adapted to pay transit fees, characterised by a high volume of low cost transactions not requiring an on-line connection for card debit.

Three different situations are considered

Closed single application (Transportation only system) : The card issued directly by the transport operator is only used to access the transport services of the issuer operator or, at most, of other transport operators with whom a clearing arrangement has been agreed. The only service available with this card is a Transport Service. With this approach, the transport operator retains full control on the system. Often, the card functional requirements for Transport applications (need for speed, contactless interface, less stringent security requirements) are not compatible with other industry requirements, typically those of banks. A problem raised in the past was for example the lack of interoperable standards for the e-purse, which reduced interest in integrating this product in an original product.

The Business model is the simplest: The Operator sells a transport service to the cardholder. If all goes well, the revenues from sales exceed the cost of operation and the operator realises a profit. The card is proof of the right to grant the service. It simplifies Administration of the system, results in - a better knowledge of travellers' preferences and optimises the service. In addition with a contactless card, the access time to transit facilities (rail station) is reduced. With the same number of access gates, the flow of passengers is dramatically increased, avoiding queuing.

Closed Multipurpose (Transport Environment) : The card also allows payment for some goods in « electronic value » to some merchants accepting this payment because they operate in the transport environment (kiosk, Bus/Train Stations). This card is useless outside. In this case, the Card Issuer is able to generate extra-revenue from

side sales to travellers (newstands, snacks). The administration is slightly more complex, but the card issuer keeps a close control on card management. The same business reasoning used for the previous « pure closed » system applies to this scenario. However, this case is a « business enabler » one and helps transport operators to understand their business case if a move towards openness is planned.

Open Multi-application Card : The card issued by the Transport Operator or a financial institution can also be used to pay services/goods outside the transport environment. Eventually this card may have application downloading capabilities. If the card is issued by the bank, the transport operator may participate as a merchant in the scheme. Hybrid strategies are also possible: The operator participates in the bank scheme whilst launching its own cards for internal purposes.

4.2.2 Open and Closed Multiapplication System Benchmarking

	Closed	**Open**
Complexity	1. In principle, less, the system is designed with a number of well defined functions. 2. The flow of transaction information is always the same 3. Same level of Security.	1. Depends on the number of offered services 2. Increasing with time, because the service offered is expected to increase 3. Legal complexity 4. Difficult to merge different interests 5. Security requirements may differ. The infrastructure (lack of PKI support) cannot be adapted to each partner needs
Responsibility **For management**	Card Issuer full responsible. He may decide on different system management options (see bellow), depending on the business case and the flexibility required	1. Shared. Some responsibility schemes are possible : 2. Need for a clear risk and responsibility chart (see #3) 3. Subject to contractual terms and conditions 4. Decentralised approach for administration, clearing and settlement functions (see bellow)
Clearinghouse	Several options possible (for more details refer to #4.3) 1. Directly assumed by Operator 2. Overall management contracted	1. Contracted by a third organisation under the direct control of the Card Issuer, the System Operator and/or a board of representatives of the MA scheme according to the legal nature. It is in principle motivated, its profits rely on the

	3. Joint Venture with another company specialising in Card Management 4. (Similar to co-brand schemes between banks and Stores launching credit cards for internal sales financing only)	volume of transactions processed 2. If a financial institution is participating in the scheme, they can assume this role (infrastructure and trained staff already available). But other partners may be reluctant. 3. Allows the introduction of economies of scale. The stakeholders get out of the « payments and settlement business » and can focus on their core business of providing new Value Added Services 4. Requires to be absolutely trusted by all the other partners of the scheme. It can then handle other system functions (marketing, communication, research of new partners) 5. Settlement period to be negotiated with each partner, depending on their financial needs and the contribution they make to the total turnover
Evolution	Less important : 1. Scheme focus on a very reduced number of services 2. Card cannot be easily upgraded. The cost of adding a new service in the offer higher than for an open scheme	1. The Open system is designed to upgrade software at both card and terminal level so it is easily adaptable. New Service Providers are welcomed to share direct costs specially to support Card Management System. 2. The Evolution of the system (new offer, new distribution channels, new payment schemes) does not require changing the cards
Need for Standard	Interoperability is not a must. But : 1. If the Operator is Public a Tender is required and the terms have to be supported by national standards	1. Critical. But the standards at the Card/ Terminal Interface exist. 2. Overall Multi-application Architectures integrating Card Management Systems already exist and are implemented 3. The problem of Back-Office Interoperability remains, but

	2. For Multioperator Transport a sectorial standard is required, but limited to a geographical area	solutions have been suggested and convergence isunder way (OP, STIP, MULTOS)
Benefit	1. Not to be shared. It can be optimised with loyalty programs supported by the same card 2. If the Operator is Public, profitability is less critical unless partial privatisation is undergo	1. Require net benefit for each stakeholder but the profits are necessary shared. The optimisation of the business case of each partner is unfeasible 2. Highly dependent on the contractual terms and conditions agreed with the Card Issuer 3. Business case possible when insufficient funds to acquire the system and provision the cards

4.2.3 Closed Multipurpose System Management

For simplicity purposes this analysis refer to a Transport Operator, public or private.

	Management Options for MA Systems		
	Direct Control by the Transport Operator (Card Issuer also)	**Delegated Management**	**Partnership with a specialised Company (« Joint Venture »)**
Advantages	1. Transport Operator retains direct responsibility over all functions (but has the ability to contract for specific functions) 2. The Operator keeps the full control of its system management. He may decide to change on his own. 3. Simpler Legal issues	1. Transport Operator able to reduce day-to-day administrative responsibility and focus on its core business 2. Transport Operator avoid needs to hire significant additional staff, but it still has to control his contractor 3. Transport Operator able to take advantage of private sector expertise and existing financial infrastructure if arrangement with a bank 4. Transport Operator keeps (or should !) most of the benefits. The administration and payment functions have a reputation for losing money	1. Transport Operator able to share risks and costs 2. Transport Operator able to take advantage of private sector expertise and existing financial infrastructure 3. Easier evolution Towards an Open system
	1. Transport Operator assumes full risks and costs 2. Transport Operator may need to hire significant additional staff 3. Transport Operator unable to take advantage of private sector expertise and existing financial	1. Transport Operator still assumes full risks and costs whilst sharing benefits 2. Transport Operator may be unwilling to yield day to day control of customer service functions ; contractors may not have the same level of concern or	1. Transport Operator must share benefits 2. Implementation may be difficult and take a long time : Choice of common overview, contractual arrangements 3. Point 2, is specially true if the transport operator is a Public Company and the

	infrastructure	motivation 3. The Contractor remains in a monopolist position, so in a powerful position in relation with the Operator 4. Once the first contractor system is implemented, it is difficult to make the system evolve further. 5. Legal issues if contract stopped	Choice of the partner has to go through Public Tender

4.2.4 Migration Paths towards Open Multi-application Systems

The previous considerations enable us to consider a global vision for the architectural and legal upgrade of a former closed system to obtain the « open label ». It is assumed that the business objectives are fixed

This paragraph will be completed with WP5 contributions.

At least , the following issues shall be discussed :

1. Management and Operational functions required to run the System
2. Legal Issues : Responsibility for Payment System
   - Proprietary payment, no interchange fees
   - Collectively determined by all the stakeholders
3. Financing of the System

5 Financial Implications for the Stakeholders : economic models

5.1 Introduction

In economic theory, the study of the offer of a good or service is the result of a three-phase analysis :

1. Study of the techniques of production of the product through the production function (which can only be roughly assessed)
2. Economic study of the production costs
3. Business structure of the offered product (« Value Added Chain »)
4. Study of the offer in terms of the market structure leading to the pricing strategy

The process of on-line production services is capital intensive. Fixed costs represent most of the operational costs and appear to be independent of the volume of activity.

The same element of the infrastructure can be used as a common resource for the offer of different types of services (Application Server). Telecommunications are the principal element of multiservice, and therefore of the common and joint costs.

The cost elements associated with developing, implementing and operating a MA system will vary to some extent depending basically on :

1. The specific type of System (Open/ Closed)
2. The domain of applications offered: Number and range of services that can be accessed using the card
3. The payment mechanism/s selected
4. The security requirements
5. The existing equipment
6. The extent to which the new equipment will be integrated into the current system and the software upgrade required
7. The possibility of evolution of the retained Architecture
8. The business structure supporting the system

5.2 Cost generation considerations

1. A business case is incomplete without a well-documented section on costs. Most investment decisions rely on the cost analysis as a significant factor in the final decision. Therefore, when integrating a Multi-application System a life cycle cost estimate should be calculated for each alternative. This total cost should be expressed in constant monetary units and used to measure the value of purchased goods and services in terms of the price level in a given base year.
2. Because there are both subtle and large differences among Operators, a single model for determining the cost of integrating a MA system cannot be recommended.:

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

3. Even if the starting conditions are very different between Operators, commonalties in order to estimate the financial impact of the investment remain:
   - A common factor is to decide whether existing operator resources can be leveraged for System Integration and maintenance or whether these will have to be purchased or contracted for. The resource requirements associated with the planning, deployment operation, and on-going maintenance of the infrastructure must be defined.
   - The software upgrades and purchases that will have to be made as a result of this implementation also factor into the overall cost.
   - Policies and procedures necessary to support external users or external organisations must also be defined. The results of these and other analyses can help Operators budget for new MA system infrastructure costs as part of the normal IT upgrade budget.
   - If the PKI is meant to be interoperable, it is essential that a standards-based product and vendor be selected. Without the use of standards, interoperability problems may arise later and would be costly to correct. Liability protection is essential in many cases, especially when interoperability is required with external users or other PKI domains.
   - Training costs for both end users and administrators may be substantial and will be an on-going cost that declines as the MA System knowledge within the user community increases. Once again, the "make it simple" approach for the end user applies. Other administrative costs like helpdesk and end entity registration procedures will be on-going and should be included in the cost.

5.3 Cost categories

This section identifies the cost elements associated with the Integration of a Multi-application System. General cost information is provided here.

The elements to complete this chapter are being consolidated.

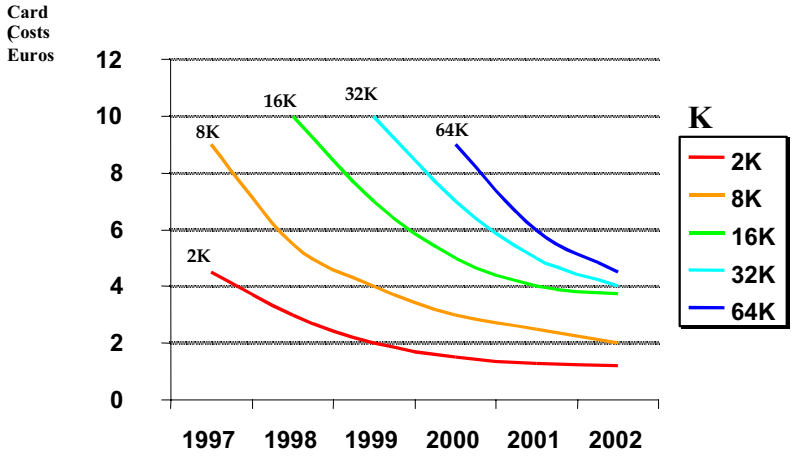
5.3.1 Decreasing cost

As technologies mature, their costs often drop. This is true of smart card technology, where costs are decreasing rapidly (see Figure 4-4). As usage and acceptance of smart cards have increased, the cost of implementation has decreased. With a Card Management System smart cards can be updated without having to reissue the card,

creating tremendous cost savings in card stock for issuing organisations (refer to WP3/WP4 deliverables).

In recent years, the storage capacity of the card has increased from 2 K to 32 K. Sixty-four Kilobyte cards have been produced and are expected to be used widely over the next 12 months. In fact, storage capacity on the card has been doubling every 12 to 18 months over the last three years. Additionally, the cost per card has dropped. When initially fielded, many cards cost more than 10 euros; but by the time they were used widely, the price had dropped to less than 6 euros. It is also worthwhile to point out that the cost of the card is one element of the overall cost of the system.

Figure 4-4: Decreasing Costs of Smart Cards



The addition of a cryptographic coprocessor can increase the cost of today's smart cards by 50 to 100 percent. Costs are likely to drop as coprocessors become more widespread. In spite of the increased cost, the benefits to computer and network security of including the cryptographic coprocessor are considerable. Two typical examples of application are:

1. PKI support if the card can produce electronic signatures and verify electronic certificates. This scenario will arise when the MA system offers e-commerce or m-commerce applications to their subscribers. Some details on PKI integrations are provided bellow.
2. End-to-End secure transactions. The next generation of smart cards (2003-2005) are expected to directly execute crypto-protocols for secure payment over the Internet. The messages supporting the protocol will be directly processed by the card and the Bank Server, the intermediate devices (Card Terminal, Merchant Server, Net nodes) merely acting for secure gateway and relay purposes.

5.4 Incremental Cost Analysis for system integration : integration of PKI services for the subscribers

5.4.1 Introduction

This section presents a notional example of an Operator that is trying to decide on what security services its system is to offer. It estimates the costs and the benefits that can be achieved at each level of security. Four options are presented. This example is based on certain assumptions. They are as follows:

1. Cost of infrastructure in this example includes the cost of setting up PKI, the cost of issuing stations, cost of purchasing kiosks, etc.
2. If an Operator requires a commercial off-the-shelf (COTS) middleware package, an additional licensing fee of approximately 70 euros per desk will be incurred.
3. Overhead and programme management costs are assumed to be the same for all Operators.
4. The cost of readers, cards, and infrastructure is based on very approximate data and just serves as an illustrative example.

5.4.2 Example : considerations for the security that the PKI card offers to the system

1. There is an increasing need to secure the transfer of Information over Open Networks, which by their nature are accessible to attackers. This Security is provided by processing the Information with cryptographic mechanisms. These mechanisms are based on the execution of an algorithm, public or not, using cryptographic keys which are confidential and must therefore be securely protected against unauthorised access.
2. It is assumed that as long as the cryptographic keys are safe, the Information processed using such keys is securely transmitted. As a consequence, storage location devices protecting all the confidential cryptographic information are critical. The smart card is the most suitable storage location and protection device. The existence of the Smart Card makes cryptographic technologies useful to protect sensitive Information.
3. Confidential keys are considered safe, if they remain exclusively under the control of only the person authorised to use them. The smart card must guarantee the protection of the stored information, even if the card is lost.
4. From the above scheme, it appears that the level of Security provided to the Information transmitted over an Open Network depends on the security provided by the smart card to the cryptographic keys used to process this information. This fact justifies the efforts of hackers attempting to break the smart card. A cat and mouse game exists between smart card manufacturers and hackers.
5. The Society of the Information mandates the generalised transmission of sensitive information over unsecured networks. In addition, these Open Networks are increasingly attacked using more sophisticated tools. From #4 statement it appears

that the most efficient way to counterbalance these increased risks is to develop new smart cards integrating innovative tamper-resistance techniques.

6. The very-high degree of security level provided by the card to internally stored data relies on four components : The card body, the chip hardware, the secure card operating system and the cryptographic-based mechanisms necessary to access the card data. Any reliable security policy for the smart card must consider specific defensive mechanisms for each of these four components. A secure cryptographic protocol can then be executed with the elements stored in the card.
7. Smart Cards are evolving to higher-end processors based on 32-bit RISC architectures with increased memory sizes. These platforms support Secure Operating Systems able to manage several applications in an independent way. Some of these applications might take advantage of the Digital Signature function of the card : The mult-iapplication leverages the PKI services.

The above justifies a business model for the System integrator.

1. To expand the offer of Services , specially in the area of e-commerce, shall require the certification of a transaction with a DS produced by the card.
2. Furthermore this DS function is useful to download applets providing new services : Software purchasing is a specific scenario of e-commerce. For e-commerce transactions, the merchant requires strong proof that the order has been mandated by the end-user. Only the DS can provide it with a legal value.
3. The DS produced by the card has to comply with the European Directive requirements for Secure Signature Creation Device, this card has to comply with EAL 4 or EAL 4+ Protection Profile defined by EESSI
4. For the Service Provider business case, portability of the applications they develop is a critical point. The definition of a Java API solves the problem. The card has then to implement a Virtual Machine supporting the API to obtain the application interoperability. The problem with the Java Card is that it is slow, specially when downloading an applet or producing a DS. The card therefore needs more powerful processors (see#7).

Points 1 to 4 require provision of expensive smart cards which need to be paid-back. The business case for the Card Issuer who pays for them requires new revenue streams. These cards have therefore to offer large memory sizes, which can be rent to Service Providers and then to charge them, whilst preserving their profits. If this works, Service Providers will be able to offer new value added services that leverage the revenues again. The price of the square mm of memory card available will increase, reducing the payback period.

6 Business Case Analysis Methodology for System Integration

6.1 Generic Considerations

Benefits and cost savings/avoidance need to be identified for continuing current operations (the status quo alternative) and for each of the viable alternatives. The business case assumes varying levels of benefits for each alternative in addition to varying costs. To the fullest extent possible, an Operator must identify and quantify

benefits that will be derived from alternative investments made in implementing PKI/smart cards. Benefits can be expressed as both quantifiable and nonquantifiable (also referred to as qualitative).

- Quantifiable benefits are those that can be assigned a numeric value, such as euros, physical count of tangible items, or percentage change. Euro valued benefits comprise cost reductions, cost avoidance, and productivity improvements.
- Nonquantifiable benefits include enhanced information security, consistency and compatibility throughout the enterprise, improved quality, enhancement of best practices, adherence to statutory and regulatory requirements, and enhanced modernisation.

Quantifiable benefits are calculated by subtracting the cost of an alternative from the cost of baseline operations. The difference is the "savings" that are often referred to as ROI. Three ways to maximise an alternative's ROI include minimising costs, maximising returns, and accelerating returns. A relatively small improvement in any of the three may have a major impact on the overall rate of return. A sensitivity analysis can be performed to identify the major cost drivers and assumptions and their affect on the alternative's estimated benefits.

Keep in mind that many benefits realised through an investment will be qualitative and will not lead directly to euro savings. Improvements in customer service, regulatory compliance, security, and accountability are certainly recognised as benefits, but they can rarely be included in the euro-valued benefits stream or ROI measures. PKI/smart cards may be difficult to quantify reliably and validly in euro units, so intangible benefits are vital to understanding the total implementation outcome. These qualitative benefits can be numerically scored by assigning a value to fully meeting, partially meeting, or not meeting stated business or functional drivers. The purpose of this section is to identify the potential benefits of implementing PKI as compared with the potential benefits of implementing smart cards both with and without PKI.

6.2 Revenue Models

Financial metrics is the core of the business model.

A fundamental factor affecting the potential for MA system and co-branding arrangements is the financial implications of such efforts from the cost-revenue side. In order to compare alternatives, TB7 recommends the use of standardised methodologies for Return on Investment Assessment.

This document (To be completed) shall provide some guidance.

6.2.1 Cost Recovery Method

This would involve recovery of the total costs (fixed and operating cost) over a defined time-period on a break-even basis. Costs to be recovered could be allocated by estimating the unit cost per transaction and pricing it accordingly. This would require a reasonable forecast of the likely volumes to be achieved in the given time frame. Alternatively, costs could be allocated equally between the participants or

proportionately to the volume or value of the transactions. At-cost pricing may be used by non-profit organisations, typically a co-operative of users, or by System providers as a strategy to consolidate an aggregation of services offer.

APPENDIX: INTEGRATION OF EMV PAYMENT SYSTEM AND MAS

Abbreviations :

PSI Payment System Infrastructure

AMS Application Management System

CMS Card Management System

TMS Terminal Management System

PSE Payment System Environment

ADF Application Definition File

EMV transactions and synergy between a Payment System and a Card

EMV is progressively becoming widespead as several European countries are currently migrating, while others are committed to migrate or analysing the migration to EMV. It is known to provide Banks with advantages, of which the major are :

- Fight against fraud (for Acquirer & Issuer)
- Offer of additional services (e-commerce, e-purse, access rights, transport, loyaly etc.)
- Reduction of the cost of communication (off-line transaction)
- Common and flexible terminal-card interface
- Card interoperability throughout the world
- Ensure customer satisfaction and enhance consumption

EMV is a set of rules and global specifications for cards, terminals and applications jointly developed by the three main issuer associations (VISA, Europay, Mastercard) to facilitate global smart card infrastructure for Debit / Credit. EMV provides a common basis of interoperability with a common functional kernel that does not depend on any specific payment scheme. EMVs define particular Issuer functions enabling the Issuer to set up his own Card Risk Management parameters, and value added services).

The Figure A1 outlines the EMV multi-application card architecture. Each application is sheltered behind a firewall provided by the environment that could be the JCRE on a Java open platform for example. As for this protection principle preventing from data disclosure, there is a sharing mechanism based on client/server scheme with shareable interface object exchanged through the JCRE on a Java platform, allowing data sharing between applications. For example, a loyalty application may share data with a payment application.

While EMV applications are managed through the Payment System infrastructure (PSI) which handles the banking transactions, non-banking applications will be maintained by an AMS (Application Management System) or a CMS (Card Management System) outside the boundaries of the PSI.

For this purpose, the terminals would be equipped with the functionality necessary to recognize the applications available on the card (through a Get Data command sent by the terminal to the card to retrieve data). Before selecting an application, the terminal would allow confirmation on behalf of the cardholder. Once the cardholder makes his choice, the terminal would identify the current application and manage the subsequent transactions, forwarding the messages to the Application Management System since the application is identified as a non banking-application.

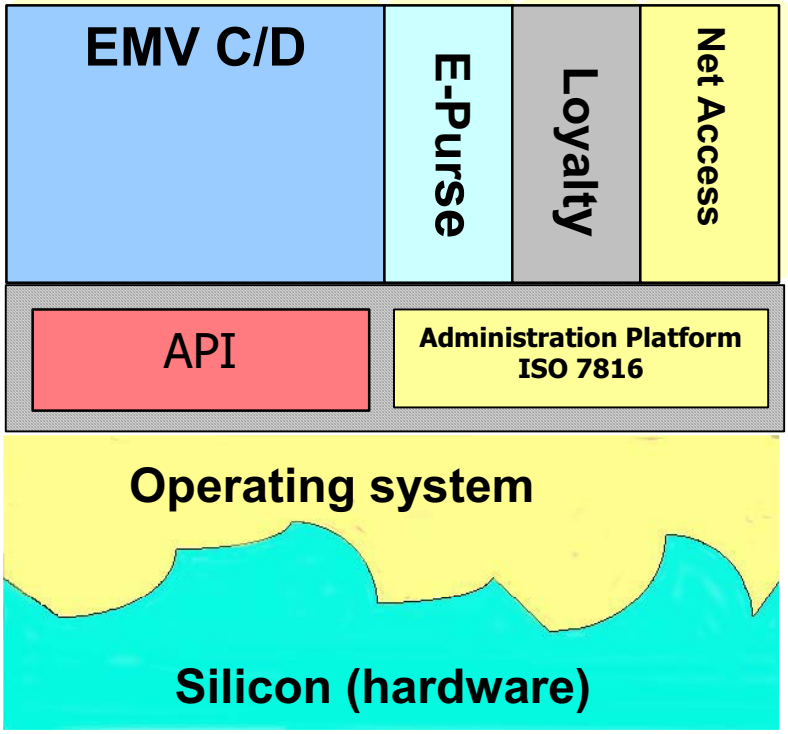


Figure A1: *Multi-application card architecture*

It being known that the PSE (Payment System Environment) is dedicated to payment applications, we consider nevertheless the case of two alternatives, with their possible drawbacks and advantages, to take control of the card during an EMV transaction :

During an issuer script

The first alternative consists of using the Issuer-to-card script processing that takes place during the online processing. Script processing is provided to allow for functions that are outside the scope of EMV specifications but are nevertheless

necessary (called administrative commands). The issuer may provide, along with his Authorization Response — in case of online authorization request process (ARQC) — command script containing a sequence of APDUs to be delivered serially to the card.

But the limitation for such option are as follows :

- The Issuer-to-card script processing occurs only in the context of online authorization, which is not always the case.
- Only status words (SW1, SW2) are returned to the terminal during the Issuer-to-card script process.
- The APDU list provided by the Issuer script is addressed to the application currently activated.

During application selection

The second alternative uses the PSE Directory Record Format : in order to match ATM terminal applications to card applications, the ATM terminal, once it detects a Payment System Environment (PSE) on the card, sends a series of READ RECORD commands to get the data encapsulated in each entry of the PSE Directory. An application entry delivers its Priority Indicator (useful for the ATM terminal to know the sequence in which it has to select the application) and the information indicating whether the application may be selectable on behalf of the cardholder. This scheme is performed at the very beginning of the EMV transaction and provides, seemingly, the most common way to manage a multi-application EMV card.

But the limitation for such option are as follows :

- Terminals should be enabled to provide confirmation on behalf of the cardholder (Application Priority Indicator [tag 87 of ADF] set to b8=‘1’).
- The Payment System Environment is limited to host payment applications only.
- In the case of a non-banking application hosted by the PSE directory, the update of such an application will be difficult for both the issuer and the application provider.
- since non-banking applications are intended for domestic use, not for being used abroad like EMV applications, this will lead to a problem regarding the non-banking applications recognition abroad by foreign terminals.

The main advantage provided by taking control of the EMV transaction rules for the non-banking application is the ability for the Acquirer to route the messages from the card to the AMS and to return commands from the AMS to the card (§ Figure A2) and therefore to charge the Service Provider by keeping track of the non-banking transactions more easily. The Acquirer may maintain a log file of non-banking transactions so that the interchange fees will be extended easily to the scheme of a PSI-AMS interfacing.

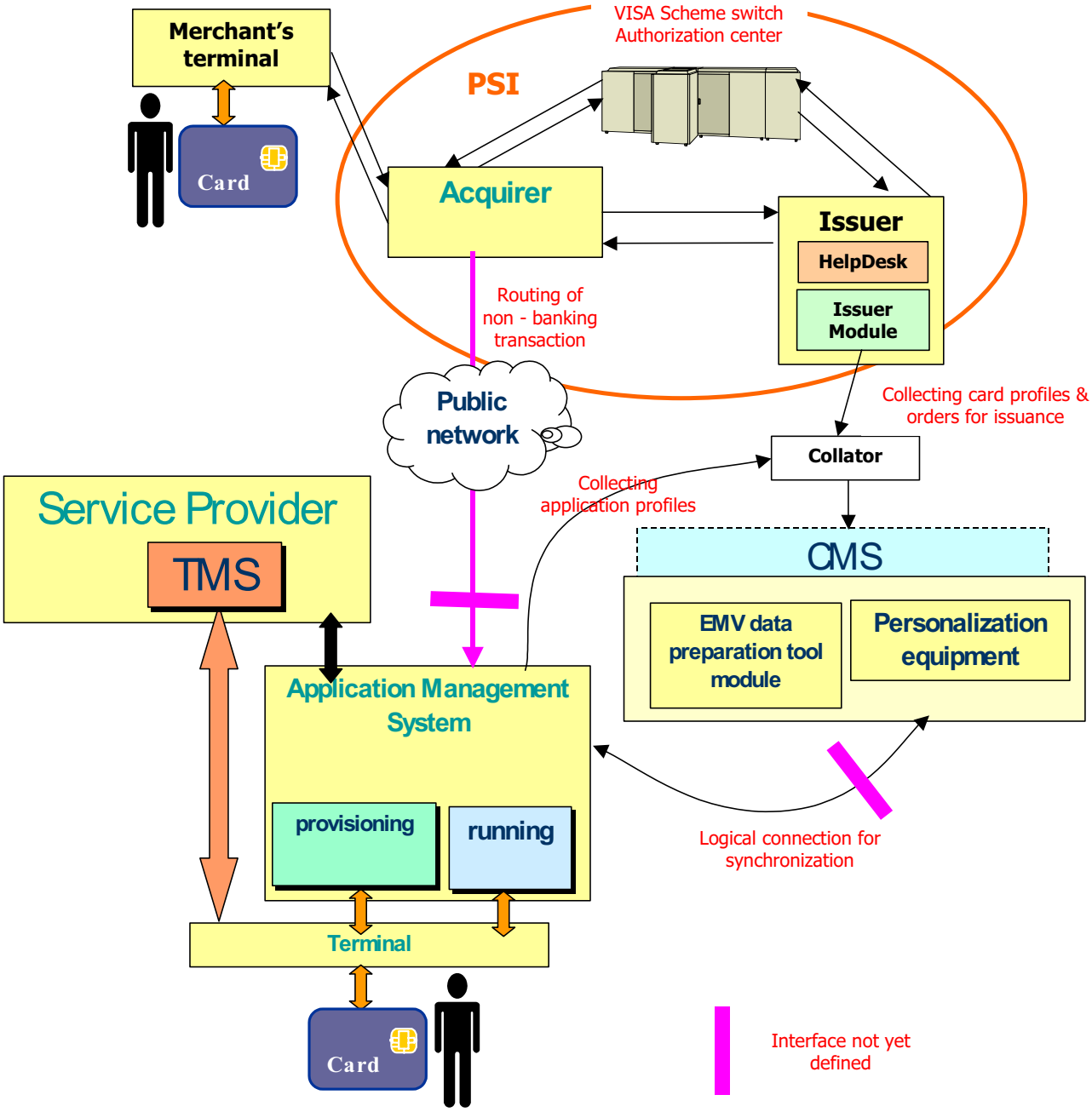


Figure A2: *interfacing CMS & PSI with EMV migration function*

The Figure A2 breaks down into modules the global architecture of a PSI interfaced with a CMS.

The AMS should be distinguished from the CMS since the AMS belongs to the Service Provider and is intended to maintain and keep track of the life cycle of his own applications as well as to update, block, unblock, delete, personalize (in post-issuance) these applications.

The AMS should at least attend to two functions provided for client cards through terminals :

- provisioning functionality which consists of delivering rights to card (transport ticket rights for example)
- running functionality which consists of executing the application on-card (use of the rights on-card)

The TMS (Terminal Management System) is operated at Service Provider's level and is intended for terminal applications maintenance (update, delete). Terminal applications may be configured to request the TMS for update at a predefined moment.

The CMS is under the control of the Issuer (owner of the card). The Issuer is allowed to address some high priority commands to the card (card_block, card_unblock, card_terminate). Those commands impact directly on the life cycle of the card, and are not accessible to the AMS unless a delegated management procedure applies.

The interface provided between the CMS and the AMS is useful for the following reasons :

- allows the issuer to send high priority commands to the cards through the AMS
- allows the CMS to keep track of card transaction (the AMS log file may also be accessible to CMS through a request.
- For billing purpose
- For re-issuance request sent by the AMS to the CMS (in case of card lost or stolen)

The Issuer disposes of a GUI to control the CMS parameters.

The CMS receives Issuer's order for card issuance. On the whole, those orders are conveyed along with the card profile and relevant data. Card profile and Applications profiles that are sent by the AMS are collected (§GlobalPlatform), parsed, controlled for conflict rules and compatibility checking, and forwarded to the personalization equipment. For the purpose of EMV migration, issuer's data related to magstripe cards are handed in to the EMV data preparation tool module (P3-like) to be processed into data convenient for chip cards.