# Table of Contents

1. **ABOUT THIS DOCUMENT** .................................................................................................. 1  
   1.1. The ‘Basic’ Transition Process .................................................................................... 1  

2. **KEY TRENDS** ................................................................................................................... 2  
   2.1. Advances in Technology ............................................................................................. 2  
   2.2. Increased Shipment of Microprocessor-based Smart Cards ......................................... 2  
   2.3. What’s Driving the ‘Need’ for Multi-application Smart Cards? ..................................... 3  
      2.3.1. Reduced Costs ............................................................................................................ 3  
      2.3.2. Synergistic Applications ................................................................................................. 3  

3. **BUSINESS ISSUES AND REQUIREMENTS** .............................................................................. 4  
   3.1. Making the Business Case for Multi-application Smart Cards ..................................... 4  
   3.2. Business Requirements ............................................................................................. 4  
   3.3. Characteristics of an ‘Open’ Multi-application Smart Card ........................................... 5  
   3.4. Choosing the Right Open Multi-application Smart Card .............................................. 5  
   3.5. Open Architecture ..................................................................................................... 6  
   3.6. Smart Card Personalization Requirements ..................................................................... 7  
   3.7. A Few of the Skills (Competencies) Needed ................................................................. 7  

4. **SYSTEMS NEEDED FOR MULTI-APPLICATION SMART CARD ISSUANCE AND POST ISSUANCE PERSONALIZATION** ........................................................................................................... 8  
   4.1. Key Generation and Key Management ........................................................................ 8  
   4.2. P3 (Personalization Preparation Process for Chip) ....................................................... 9  
   4.3. Smart Card Personalization Manager (SCPM) ............................................................. 9  
   4.4. Smart Card Management System (SCMS) ................................................................. 10  
   4.5. Personalization Systems .......................................................................................... 11  

5. **TRANSITION OPTIONS AND ALTERNATIVES** .................................................................. 11  
   5.1. Phase 1: Initial Issuance, No Capture of Issuance Data ........................................... 11  
   5.2. Phase 2: Capture/Store/Query on the Stored Data .................................................. 12  
   5.3. Phase 3: Update Cards over the Internet (Post Issuance Personalization) .................. 13  
   5.4. Phase 4: Full Smart Card Management System ....................................................... 14  
   5.5. Investments Needed for Phases 1 through 4 ............................................................. 15  

6. **APPENDIX A: ABOUT DATACARD** .................................................................................... A1  

7. **APPENDIX B: DIFFERENT MULTI-APPLICATION PLATFORM CARDS** .................................................. A3  
   7.1. MULTOS Card ......................................................................................................... A3  
   7.2. Java Card ................................................................................................................. A3  
   7.3. Windows for Smart Cards (WfSC) ............................................................................. A4  
   7.4. “Open Platform” Card .............................................................................................. A5  

8. **APPENDIX C: ACRONYMS USED THROUGHOUT THIS DOCUMENT** ................................................. A6
1. About this Document

This white paper describes the transition to a multi-application smart card issuance program. For those involved in planning such a program, the issues seem daunting…

- Can we do it ourselves or do we need partners?
- What are the business and technical risks?
- What types of cards should we use? How do we acquire these cards?
- What hardware and software is needed for both issuance and post issuance personalization?
- Where do we acquire the applications to put on the cards?
- How do we go about personalizing and issuing the cards?
- How will we manage the cards and applications on the cards after the cards are issued?
- Should we take this on in-house, or should we outsource?
- Where do we start?

This white paper has been developed to help answer many of these questions.

1.1. The ‘Basic’ Transition Process

The following illustration shows the basic process and some of the basic elements needed to implement a full multi-application smart card program, including the ability to update multi-application smart cards with new applications and new capabilities after the cards have been issued and are in cardholders’ hands. Of course, a full program does not need to be implemented all at once – it can, in fact, be implemented in steps.

This paper will help explain some of the options and the corresponding decisions that will need to be made during this transition, and how an issuer might implement this transition in separate steps/ phases. The types of investments that will be needed in both hardware and software will also be summarized.

SCMS = Smart Card Management System
This basic process will be described in more detail in section 5. Section 2 describes key trends that are influencing the smart card industry. Sections 3 and 4 describe important business issues and hardware and software systems that will be needed for this transition.

2. Key Trends

2.1. Advances in Technology

Over the past few years advances in chip technology and chip software technology has been phenomenal. ‘Standard’ are ultra fast chips with 32-to-64K ROM and EEPROM. Advanced co-processors are available that can perform many different types of encryption/decryption. Chips can also run portable operating systems, much like Windows, that support high-level application programming languages (Java, C++, Visual C/Basic) with corresponding software development kits. In fact, smart cards have progressed so much in the past 5 years they are now really small versions of our desktop computers, with the biggest difference being that they operate within the confines of a credit card size form factor.

These advancements have had a dramatic effect on the smart card industry and the applications that run on smart cards. With the increased capabilities that smart cards now offer, at a vastly reduced price, smart cards have become a powerful marketing tool that can help sell and promote new products and services for businesses at a very economical price.

But these new capabilities have also driven the need for change – the need for new software to load and personalize these advanced smart cards, the need for software to manage the life cycle of smart cards after their issuance, and the need for software to keep the development and issuance environments safe and secure.

2.2. Increased Shipment of Microprocessor-based Smart Cards

A key indicator of multi-application smart card growth and acceptance is the number of cards shipped each year by smart card manufacturers to smart card issuers.

As shown in the table below, 1.46 billion memory cards were shipped to issuers in 2000. An additional 550 million microprocessor cards (cards that run operating systems) were shipped in this same period.

<table>
<thead>
<tr>
<th>Smart Cards Shipped (in Millions)</th>
<th>2000</th>
<th>2003</th>
<th>3 Year Growth</th>
<th>3 Year CAGR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>16.2</td>
<td>200.7</td>
<td>114.5</td>
<td>74.9</td>
</tr>
<tr>
<td>Retail &amp; Loyalty</td>
<td>71.8</td>
<td>4.7</td>
<td>126.4</td>
<td>94.6</td>
</tr>
<tr>
<td>Phone - Prepaid</td>
<td>1,224.8</td>
<td>2.0</td>
<td>1,226.8</td>
<td>952.6</td>
</tr>
<tr>
<td>Phone - GSM</td>
<td>0.0</td>
<td>191.1</td>
<td>191.1</td>
<td>150.1</td>
</tr>
<tr>
<td>Transit</td>
<td>36.3</td>
<td>8.6</td>
<td>44.9</td>
<td>31.3</td>
</tr>
<tr>
<td>Healthcare &amp; Social Security</td>
<td>40.5</td>
<td>25.4</td>
<td>75.9</td>
<td>50.5</td>
</tr>
<tr>
<td>Multimedia, Pay TV</td>
<td>5.0</td>
<td>69.3</td>
<td>74.3</td>
<td>50.0</td>
</tr>
<tr>
<td>W &amp; Access</td>
<td>5.3</td>
<td>46.0</td>
<td>51.3</td>
<td>33.3</td>
</tr>
<tr>
<td>Leisure</td>
<td>52.6</td>
<td>2.1</td>
<td>54.7</td>
<td>35.0</td>
</tr>
<tr>
<td>Subtotals</td>
<td>1,459</td>
<td>596</td>
<td>2,008</td>
<td>1,517</td>
</tr>
</tbody>
</table>

The key statistic is the trend that is not so evident in the table. The statistic that says memory smart card shipments are expected to grow by less than 17% per annum over the next 3 years.
On the other hand, microprocessor smart card shipments are expected to grow by nearly twice this amount (~30% per annum) over the same period.

At this rate, it won't take long for microprocessor cards to catch up to and pass memory cards in the marketplace. This acceptance of multi-application smart cards will drive issuers to look for answers on how to transition to multi-application smart cards from their current mag stripe programs or single application smart card program. This white paper has been developed to guide a new issuer through a few of the issues they will be faced with as they consider this transition.

### 2.3. What's Driving the ‘Need’ for Multi-application Smart Cards?

So what is driving this increased acceptance and use of microprocessor-based smart cards in the card market? One reason has already been discussed - advanced capabilities and reduced costs. Another important driver is the increase in “synergistic” applications on a single card - companies who are finding better ways to package and include complementary applications on a single card.

#### 2.3.1. Reduced Costs

The cost of microprocessor cards has dropped considerably over the past few years. 8K microprocessor cards with no co-processor can now (as of May 2001) be purchased for less than $3.00 US per card. For this amount you can get a card with a multi-application operating system (typically the card manufacturer’s proprietary Java operating system), and one application such as VSDC (Visa Smart Debit/Credit) or M/Chip Select (MasterCard’s Debit/Credit application).

This is not the price of a fully personalized card, however. After paying $3.00 the card must still be brought into a card operation center and personalized –encode the mag stripe on the card, emboss characters on the card, print graphics/images on the card, and possibly affixing the card to a printed form and deliver it to a cardholder. These personalization tasks can add an additional $1.00 to $3.00 toward the cost of a fully personalized and delivered card.

#### 2.3.2. Synergistic Applications

Beyond economics and reduced card costs, what else is driving this transition to microprocessor-based smart cards?

In the financial world it is oftentimes the use of synergistic applications on a card. For example, a credit/debit application might be the “anchor” application on the card (the intended revenue-producing application), whereas a loyalty application might be added to the card to drive the use of credit/debit.

In non-financial markets a card which has multiple capabilities might be the driving force. For example there might be a business case for having a single card with multiple applications to drive higher card use, such as having one card that can perform all of the following functions:

- physical access
- logical access
- an electronic purse (for purchases)
- a loyalty application

It is believed by many that simply reducing the number of cards that we currently carry in our wallets and purses might be the incentive that we need to start using a multi-application smart card.
3. Business Issues and Requirements

3.1. Making the Business Case for Multi-application Smart Cards

Many issuers who are considering rolling out a smart card program are wondering how they can "make the business case" for smart cards and card management.

Build a business case for smart cards is not a trivial effort, but when all costs and benefits are calculated, smart cards have proven time and time again they can offer significant economic value to an issuer’s bottom line compared to the issuance of a similar mag stripe card.

The economics of a chip-based card program will be the sum of the revenues gained from the new program minus the cost/expenses of the program. Cost avoidance must also be factored into the equation. Increased marketing capabilities and cardholder retention will also be important considerations. A few additional business drivers for making the business case are shown in the illustration below.

Now appears to be the time for issuers to move to smart cards, to reduce losses and operational costs, and to enjoy new revenues and gain new and loyal customers because of the highly customized applications that can be offered.

3.2. Business Requirements

The ultimate success of any smart card program will come down to the value proposition offered to the cardholder. Winning issuers are likely to be those who provide the most customized services on their cards in the most cost-effective manner.

Some of the more important business requirements an issuer will probably have:

- The cards used and the issuance processes implemented must support the dynamic loading of applications, meaning the ability to add applications to the cards after the cards are in the field.
- The cards must allow for total issuer control, i.e., the issuer must have 100% control over the applications loaded and used on the cards.
• Applications developed for the cards must be portable across different vendors’ cards. You must be able to write applications once and then run those application on other ‘open’ multi-application smart cards provided by other vendors.

• The cards must support applications from different application providers on the same card.

• The type of cards used and the issuance processes implemented must support the concept of ‘markets of one’. Another way of saying this - each card must be 100% customizable anytime anywhere.

• The cards must provide 100% backward compatibility with existing terminals and systems.

### 3.3. Characteristics of an ‘Open’ Multi-application Smart Card

To strengthen an issuer’s business case for multi-application smart card issuance they must issue multi-application smart cards which support industry standards for both hardware and software. True ‘open’ multi-application smart cards will have the following characteristics:

• They will run a non-proprietary operating system widely implemented and supported.

• No single vendor will specify the standards for the operating system and the card’s use.

• The cards will support a high-level application programming language (e.g., Java, C++) so issuers can supply and support their own applications as well as applications from many other vendors.

• Applications can be written and will operate on different vendor’s multi-application smart cards with the same API (Application Programming Interface).

### 3.4. Choosing the Right Open Multi-application Smart Card

So how does an issuer choose the correct open multi-application smart card technology (also known as a ‘platform’ card) and chip technology to use in their smart card issuance program?

Unfortunately there are many different and contradictory definitions and terms used when people try to describe an open platform card. A true open platform card is one which:

• Supports a wide variety of suppliers in both chips used and card software and applications implemented

• Supports standard tools for application development and maintenance/support

• Is portable across a range of chip platforms

• Supports selectable* levels of security

• Facilitates partnership and co-developments with companies in the same and in other industries

• Allows an issuer to experiment in finding and developing new value propositions

• Ensures that all IC chip software and hardware (personalization equipment) investments are well protected and will not become obsolete as card technology advances

*This will be discussed in more detail in a later section of this document

Java is an operating system that satisfies all these requirements. Java can operate on a smart card’s IC chip, at the same time can support the terminal/POS network where the cards will be used, and can also be used to support the application server(s) in the back office. As shown in the illustration below, Java can span all environments of a full smart card program.
Java gives application developers an open and portable smart card platform instead of the proprietary operating systems controlled by many card manufacturers today. Java has moved smart card programming into the realm of mainstream personal computer where there are hundreds of thousands of programmers available with this skill set.

3.5. Open Architecture

“Open Platform”, as defined by GlobalPlatform, is a comprehensive system architecture that enables the fast and easy development of globally interoperable smart card systems. It is comprised of three elements - card, terminal and systems -- each of which may include specifications, software and/or chip card technology. Together these components define a secure, flexible, easy to use smart card environment. To reference these specifications you can visit the GlobalPlatform web site at [www.GlobalPlatform.org](http://www.GlobalPlatform.org).

There are many different cards today which people call an open platform card or an open multi-application smart card. One source of confusion is that GlobalPlatform has a card specification which they call “Open Platform” (capital “O”, capital “P”). But the term “open platform” (no caps) is also used throughout the smart card industry to mean most anyone’s multi-application smart card upon which you can add and delete applications. Of course the typical caveat for most of these ‘open’ multi-application smart cards is that you must abide by the card manufacturers rules, and their rules only, for loading and deleting applications on these cards. But in fact, the rules for adding and deleting applications on these cards have not been defined and specified by any specific industry group, so the ‘openness’ being referred to is really the card manufacturers rules for openness – their rules.

So basically what this means is that when someone says “open platform” you don’t always know what they are talking about until you interrogate further.

Appendix B summarizes the major multi-application smart cards (platform cards) which people typically call open platform, and sometime Open Platform, and maybe even Open platform, and this appendix lists their key differences.
3.6. Smart Card Personalization Requirements

An issuer who is considering getting into smart cards should also be critical of the technology and the processes used to load and personalize the smart cards they wish to issue. The processes and the technology should:

- Provide a common approach to application loading and personalization
- Support ‘common’ personalization across different types of open platform cards and chip types
- Be able to centrally store and manage smart card applications and the objects required for the loading and personalization of smart cards (e.g., keys, certificates, risk parameters)
- Deal consistently with multi-application smart cards which conform to industry standard interfaces and specifications

The personalization solution chosen should be able to operate in all types of issuance environments:

- Within a central issuance environment
- Within a wide area/distributed environment
- Within a hybrid network – one which has elements of both central and distributed issuance
- Over insecure networks (e.g., over the internet) as well as over secure networks
- The personalization solution should standardize on common processes and automation whenever possible

To compete effectively in the world of multi-application smart cards, issuers will need to be able to make operational and marketing decisions quickly so customers ultimately will benefit. As with any smart card program, there will be the need to develop and implement new smart card applications. Having the right competencies and the right tools and processes for issuing cards quickly will be the key to gaining marketing advantages.

3.7. A Few of the Skills (Competencies) Needed

A few of the competencies that will be needed either in-house, or available from a solutions/integration partner, during the rollout of a multi-application smart card program include:

- Application development expertise (knowledge of Java, C++, Microsoft tools) for both chip developments and back-end application developments
- Detailed knowledge of the scheme(s) being implemented and issued – e.g., MasterCard or Visa Credit/Debit, Transit, Healthcare, Telecomm, E-Access/ID, E-purse, Loyalty, or whatever other applications are to be included on the cards
- The ability to integrate standard platforms and software systems with legacy applications and servers and systems
- Tools and toolkits to aid in the custom development of new applications and services
- Network expertise – the ability to manage a new smart card issuance network (wide area and local area networks, secure firewalls, new smart card systems, etc)
- Project management expertise, with experience in smart card implementation planning, deployment, and support
4. **Systems Needed for Multi-Application Smart Card Issuance and Post Issuance Personalization**

The following illustration shows the major types of hardware and software systems that will be needed to implement a full multi-application smart card issuance program. Datacard products are described throughout this section, but non-Datacard systems can, in fact, be implemented if they perform a similar capability.

---

4.1. **Key Generation and Key Management**

Key generation and key management is by far the most difficult task a new smart card issuer will need to be concerned with when transitioning to a multi-application smart card program. Card operations centers typically do not need to be literate on the concepts of key management and key generation for most types of cards – but they will need to be literate on key management and key generation operational aspects for smart card issuance.

As an example, an Issuer’s Master Keys will need to be generated. The Issuer’s asymmetric key pair for EMV (Europay MasterCard Visa) compliance and all associated digital certificates will also need to be generated and stored in preparation for issuance. These are tasks that are done infrequently, but will need to be done nevertheless. The concepts and tasks for key generation and key management must be learned before personalization can occur.

A few of the other types of keys that must be generated and managed:

- Key Exchange Keys (KEKs) needed to share data between data generation (P3) and the personalization systems
• Manufacturers Transport Keys (for cards), used to lock cards before transport
• Public and Private Keys for Asymmetric and Symmetric Security Schemes

Key generation and key management is performed inside three systems in the illustration above – within the P3 system, within the Smart Card Management System (SCMS), and within the Smart Card Personalization Manager (SCPM). All of these systems are described below.

4.2. **P3 (Personalization Preparation Process for Chip)**

Data for smart cards is a complex series of data elements - both cryptographic and clear text - that must be generated, assembled and formatted in such a way as to be understood by a smart card chip and its associated applications. Both initial card issuance and post issuance personalization will require a “P3 data generation capability.”

Datacard’s P3, short for Personalization Preparation Process, provides secure key management and chip data generation for many different financial smart card schemes:

1. VisaCash DES
2. VisaCash RSA (Public Key)
3. Visa Smart Debit Credit (VSDC)
4. M/Chip Lite
5. M/Chip Select (Multos)
6. UK ICC Specification (UKIS)
7. Europay Pay Now Pay Later

Other applications not included in this list will need some way of creating chip data. This may be P3, or a system like P3.

As part of key management P3 provides secure key generation, both symmetric and asymmetric, through an attached Host Security Module (a cryptographic processor ‘black box’). P3 also provides certification generation for card and application certificates and can provide Issuer public keys in self signed formats compatible with most Certificate Authorities.

P3 also generates EMV tags for both static risk control as well as the EMV cardholder specific (dynamic) tags. For the authentication application P3 generates all the appropriate data necessary for the personalization of the application.

Datacard’s smart card MAP (Multi-application Architecture for Personalization) makes it possible to generate IC chip data using P3 without having prior knowledge of the applications or the target cards being used.

4.3. **Smart Card Personalization Manager (SCPM)**

A system such as Datacard’s SCPM will also be needed and must be capable of communicating with the read/write heads in the personalization systems where the cards will be programmed. This type of system must be capable of storing and retrieving a myriad of smart card software objects during the personalization process, such as:

• Keys, for example a Key Exchange Key (KEK), used to securely transfer data between the P3 system and the personalization system. Or a Master Transport Key for the target cards, shared between the card supplier and the personalization system.
• Open Platform objects such as CAP files or Card Creation Scripts
• MULTOS objects such as MSM Controls, ALCs, ADCs and some forms of ALUs,
• Common platform objects such as Card Profiles, Personalization Application Profiles

Datacard’s SCPM facilitates the loading and personalization of applications on a smart card and handles all of the cryptographic processes appropriate to the applications on Open Platform and MULTOS cards without having prior knowledge of the applications and without human intervention.

In the past, personalization of an application on a smart card required intimate knowledge of the application and the target card, followed by custom software development to create the personalization application program. Datacard’s smart card MAP architecture provides a generic personalization process that can personalize any application on any Open Platform card or MULTOS card without unique knowledge of the application, and without custom software development.

4.4. **Smart Card Management System (SCMS)**

A SCMS is a software system that manages data associated with cards (type, manufacturer, memory, and basically any other card or personalization attribute), applications which are on the cards, and also has the ability to execute Post Issuance Personalization (PIP) over a secure or non-secure network connection against those cards.

An open and standards-based SCMS will adhere to the GlobalPlatform Open Platform card specification for loading and deleting applications on an OP card, or the MULTOS card specification for loading and deleting applications on a MULTOS card. A well-designed SCMS will significantly streamline the personalization process by managing individual product configurations together with card and application profiles.

PIP is the process of loading, deleting, updating and personalizing applications on a multi-application smart card after the card has been issued. While in many respects PIP is similar to initial issuance, there are several important differences:

• PIP is almost always a “low-volume” operation - typically performed one card at a time. However with the appropriate SCMS, such as Datacard’s Affina, millions of single card cardholders can be online with Affina at the same time while updating their cards with new applications.

• The card to be PIP’d (Post Issuance Personalized) will not always be in a controlled network environment and is likely be in the hands of a person sitting at an internet-based computer.

• The flow of communication between the PC where the card is located, and the ‘host’ computer where the download will occur, can easily be disrupted or disconnected. The end user might also perform a wrong or invalid or malicious act.

The Internet will be the medium where the majority of PIP will occur. Since the Internet is a public infrastructure one of the main focuses of PIP is on security related issues such as card and cardholder verification, data integrity, and data encryption.

The use of the Internet for PIP is only suitable under the following conditions:

• Bandwidth and reliability can be established with a secure application loader on the host side.

• The application loader is under the control of the issuer or application provider from a key management point of view.
4.5. **Personalization Systems**

Personalization systems can be any hardware system, including Internet connected devices such as Internet PCs, that are used to load, delete, and personalize applications on a smart card.

5. **Transition Options and Alternatives**

There are four basic steps, or phases, an issuer will need to follow to implement a full multi-application smart card issuance program with post issuance personalization capabilities. This section describes these four phases as well as the types of investments that will be needed for each phase.

An issuer will not need to implement all four phases at once, but it will be important to have an understanding of all four phases before implementation planning starts.

The illustration on page 1 of this document will be used again to describe these four phases. Each phase will show a portion of the full illustration and will grow as more capabilities described within the phases are added. Phase 4 will again show a full illustration as a full multi-application smart card issuance program is implemented.

5.1. **Phase 1: Initial Issuance, No Capture of Issuance Data**

In Phase 1 an issuer will issue multi-application smart cards but will go no further. If they choose not to implement beyond Phase 1 all issued cards will be treated as “static” cards – meaning the cards will not be managed by a card management system. Implementing only Phase 1 an issuer is simply saying they will re-issue new multi-application smart cards in the future when dynamic card issuance and post issuance personalization is needed.

As shown in the illustration, P3 is used to generate the chip data for the financial applications on the cards, and SCPM is used to manage the loading and personalization of this chip data on the cards in the personalization system(s). Issuance data is not captured and stored in a card management database unless Phase 2 is implemented.

Implementing only Phase 1, if a cardholder calls and asks for a replacement card, the issuer will simply put in a request for a replacement card and the same card with the same applications will
be re-issued. The same issuance process will be followed for re-issuance and no SCMS will be used.

5.2. Phase 2: Capture/Store/Query on the Stored Data

Phase 2 builds on Phase 1. In Phase 2 an issuer captures issuance data and stores this data in the SCMS database (Datacard’s SCMS called Affina™ is shown in the illustration below). Implementing the Affina Card Manifest Upload module, and the Affina Card Query module, will allow issuance data to be input, stored, managed, and queried on demand.

The captured and stored SCMS data can be used for a wide variety of uses, such as seeing what cards were issued, when they were issued, and what applications were issued on the cards. But of course this is only the “tip of the iceberg” with respect to how this issuance data might be used. An issuer’s marketing organization might want to query this stored data in many other ways to determine what other marketing programs should be undertaken.

Implementing Phase 2, an issuer believes there is a high probability they will want to Post Issuance Personalize the cards they are issuing today (i.e., they will want to update the issued cards with new applications in the future), so they want to capture the issuance data and store it in the SCMS today.

But although they foresee the need to Post Issuance Personalize the cards, they do not yet have the need to implement the delivery mechanism that will allow the cards to be updated in the field - this capability can be added if Phase 3 is implemented.

This phase includes limited integration with any of the issuer’s back-office systems, but will allow various individuals within the organization, or within the cardholder base, to query the stored data to get information about the cards issued and the applications on these cards. A web-based front-end can be the mechanism that will allow customer service and cardholders to access the data stored in the SCMS.

This action defers implementing a ‘full’ SCMS until a business decision is made to do so, but at the same time implementing phase 2 positions the issuer for PIP because issuance data has, in fact, been captured.
5.3. Phase 3: Update Cards over the Internet (Post Issuance Personalization)

Phase 3 adds a Secure Delivery System (SDS) to the SCMS that will allow cardholders to update their cards with new applications, or updates to current applications, via a web-based interface over a secure or non-secure delivery (communication) channel.

The responsibility of the SDS is to manage the delivery of applications and other card ‘data’ over a supported web delivery channel such as the Internet. Other delivery channels, such as over-the-air communication with smart cards on mobile phones, can be implemented if desired.

Supported post-issuance devices such as home PCs will need to support on-line, real-time application loading and deletion interfaces offered by the card’s scheme. The SDS will manage this communication by setting up secure sessions with the target cards used in these devices.

Simply put, in this scenario, when a request is received for a replacement card, or for a new application on an existing card, the SCMS will be interrogated to assess the state of the card as well as applications on the card. The SCMS will also be interrogated to assess the state of the cardholder. The rules may include checking on whether the cardholder should be allowed a new/replacement card and which applications can be given to him/her. The SCMS interrogation will also undoubtedly check on card specifics such as operating system compatibility, cryptographic requirements, available memory, and other relevant application and card specifics such as pre-requisites, co-requisites, release levels, and so on. After all checks are completed, the requested chip data can be generated by P3 (or a P3-like process) and sent to the SDS for delivery to the card.

To complete the process, as soon as the card is updated, issuance data sent to the card will also be sent to and stored within the SCMS to ensure the SCMS is always current.
5.4. Phase 4: Full Smart Card Management System

In Phase 4 an issuer will implement a full dynamic multi-application smart card issuance program and will need to integrate their SCMS with back office systems and their current terminal network (e.g., POS devices, Kiosks) where smart cards and other relevant application systems are used and need to get tied in to the SCMS.

With the integration of back office systems with the SCMS, such as Datacard’s Affina SCMS, the issuer can now be made to manage and control card production, card updates and card renewal. Upon request the SCMS can now generate chip data and card requests and then send those requests to either a bureau for batch production, or to the Secure Delivery System for internet-based delivery.
5.5. Investments Needed for Phases 1 through 4

Before a decision is made to go forth with a multi-application smart card issuance program, the question of cost and required investments needs to be addressed. For example, what investments will be needed to implement each of the phases described in this white paper? The table below answers this question.

To reiterate, the four phases described in this white paper are:

**Phase 1:**
- Issue multi-application smart cards but **do not** capture any issuance data (results) unless Phase 2 is also implemented.

**Phase 2:**
- Capture and store issuance data and provide the ability to query on this stored data through a web server front-end or through some other means.

**Phase 3:**
- Implement the ability to update issued cards over a selected delivery channel (e.g., internet).

**Phase 4:**
- Implement a full smart card management system, integrate with back-office systems.

Of course there are other possible ways to implement these four phases, but the four phases defined within this white paper should give the reader a good idea as to the key investments needed to implement issuance and post issuance personalization.

<table>
<thead>
<tr>
<th></th>
<th>P3 Data Generation</th>
<th>SCPM</th>
<th>Personalization System(s)</th>
<th>Affina Main Engine and Database</th>
<th>Affina Card Manifest Upload Module</th>
<th>Affina Card Query Module</th>
<th>Affina Secure Delivery System</th>
<th>Delivery Channel Support (e.g., Internet)</th>
<th>Integrated with Back Office Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PHASE 1: Initial Issuance, No Capture</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create IC Chip Data for Initial Issuance</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue Cards (Load and/or Personalize)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PHASE 2: Capture/Store/Query</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capture/Store Data in Affina</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform Queries on Affina Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PHASE 3: Internet Updates and Downloads</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Cards via Internet/Web Interface</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PHASE 4: Full Card Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Issuance and Post Issuance Personalization, Manage and Control Card Production</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Affina = Datacard’s Smart Card Management System

Summary:
As shown in the table, in order to issue multi-application smart cards (Phase 1) an issuer will need to invest in P3 if the card will have one of the financial schemes listed in section 4.2 (or they will need to create this chip data some other way). They will also need to invest in SCPM or a like product to manage the loading and personalization of the card in the personalization systems, and they will need to invest in personalization systems which they intend to use. They will also need to invest in the cryptographic processors needed by P3 and the personalization systems. You can see the needed cryptographic resources in the illustration in section 4.0.

To prepare for PIP by capturing and storing issuance data, and then providing the ability to query on this data, there will be an additional investment needed in the Affina Main Engine, the Affina Card Manifest Upload module, and the Affina Card Query module (Phase 2).
To add Post Issuance Personalization capabilities to the SCMS (Phase 3) there will be a need to make an additional investment in a Affina Secure Delivery System and any delivery channel(s) which the issuer elects to implement and support – such as the internet, network kiosks, mobile phones, or other.

Phase 4 investments entails the integration of the implemented SCMS and all previous phases, with all back office systems and the terminal network which need integration with the SCMS to keep it ‘current.’ Phase 4 also involves integrating the SCMS with other card-related issuance processes (e.g., all other 9000 data stream ‘build’ processes) so the SCMS can be made to manage and control card production, card updates and card renewal.
6. APPENDIX A: About Datacard

Datacard provides customers in more than 200 countries with the systems, software and the consultative expertise they need to launch and maintain profitable card programs. Financial institutions, corporations, government agencies, telecommunications companies, transit providers, service bureaus, schools, hospitals and other organizations use Datacard solutions to personalize, issue and manage a variety of financial and identification cards.

The company helped transform the world for consumers and card issuers more than 30 years ago by enabling secure, high-volume issuance of magnetic stripe-based financial cards. Today, more than 90 percent of the world’s financial cards — and a majority of plastic cards used for other applications — are personalized with Datacard® brand systems and software.

Datacard also redefined the identity solutions market 10 years ago, when it introduced the first digital identification systems. Today, Datacard identification systems outsell all other brands. But more important, the company has advanced critical identity technologies — such as smart cards, biometrics and digital imaging — and developed a powerful portfolio of identity solutions. This portfolio includes the world’s premier family of identity software and the largest family of plastic card printers. Corporations use Datacard identity solutions to create enterprise wide identity programs. Colleges, universities and K-12 schools rely on them for highly secure student ID programs. Government agencies around the world insist on Datacard identity solutions for a variety of applications, including national ID, healthcare, driver’s license and passport programs.

After 30 years of plastic card leadership, Datacard stands on the brink of an even greater global transformation. In collaboration with the world’s leading financial institutions, consumer marketers and other leading smart card technology companies, Datacard has created the infrastructure required to personalize, issue and manage multi-application smart cards.

Multi-application smart cards are plastic cards with embedded microchips, which have the ability to store applications and process data. Datacard smart card specialists have a long history in the design of secure, multi-application smart card operating systems. This includes development of a new, high security operating system based on Java Card™ and active participation in the definition of worldwide technical standards through industry associations such as GlobalPlatform and the Smart Card Alliance.

Many of the world’s leading financial institutions and consumer marketers plan to issue multi-application smart cards to consumers, who will use them to make purchases, conduct online transactions, place phone calls, access healthcare services, board airplanes, enter secure facilities and more. Datacard’s multi-application smart card infrastructure will be used to personalize, distribute and manage a vast majority of these cards.

Datacard’s business is to help define and then implement open standards and interfaces needed to issue cards and manage the data needed within a comprehensive smart card issuance program. The standards and interfaces that Datacard has helped develop and now support includes the following.

- Datacard has implemented the Open Platform card specification within the Datacard Java Card product (product name Aptura™).
- Datacard has implemented standardized personalization processes for both the Open Platform multi-application smart card and the MULTOS multi-application smart card, for both central and distributed/instant issuance.
- Datacard has implemented the GlobalPlatform-developed Card Creation and Script Builder (CCSB) specification within the Datacard Smart Card Personalization Manager.
• Datacard has helped define and is now implementing the specifications for Card Management Systems and the interface between Card Management Systems and card issuance/personalization bureau. The goal is to help issuers manage applications, keys and cardholder information for each customer card produced, during both initial issuance as well as post-issuance updates to those same cards after they are in the field.

• Datacard is currently implementing the requirements for systems and processes that will enable authorized entities (e.g., Certificate Authorities) to validate and authenticate the loading of keys on cards that support an asymmetric smart card security scheme.

• Datacard is currently helping identify the synergies that will facilitate cross-industry dynamic loading of smart cards and applications.

A few of Datacard’s accomplishments:

• The first to provide high-volume smart card issuance solutions (as of April 2001 when this White Paper went to press Datacard Group has shipped over 700 high volume central issuance smart card personalization systems to worldwide customers)

• Pioneered generic application loading and personalization solutions for open platform smart cards (e.g., Multos and Java Card)

• Selected by GlobalPlatform as the supplier and Operator of a full Smart Card Management System for a GlobalPlatform reference implementation system.

• Designed and implemented the Mondex electronic purse

• Invented, designed and developed the MULTOS multi-application smart card operating system

• First to obtain certification of commercial products under the European ITSEC Level E6 test criteria (IT Security Evaluation Criteria - Level E6 is the highest level possible)

• Created and developed an open-standard multi-application operating system for smart cards base on the Java operating system (e.g., product name Aptura™)

• Partners with all major scheme providers and payment associations to ensure compatibility between software developments and applications and Datacard card issuance systems

Datacard Corporation, doing business as Datacard Group, is a privately held company owned by the Quandt Family of Bad Homburg, Germany. Datacard is headquartered in Minnetonka, Minnesota, with a sales and service network of direct sales organizations, dealers, distributors, and value added resellers in over 120 countries. In addition, worldwide operations include new software development centers in the U.S., the U.K., India and Japan. The company employs more than 1,600 people worldwide and generates annual revenues of more than $300 million (www.datacard.com).
7. APPENDIX B: Different Multi-Application Platform Cards

7.1. MULTOS Card

Stands for MULTI-application Operating System. Developed in mid-90s by the NatWest Development Team (now a part of Datacard) as a secure platform for the Mondex electronic purse. A consortium called MAOSCO currently controls MULTOS specifications.

MULTOS is the only non-military product in the world to achieve ITSEC Level 6 (E6) certification, the highest certification possible.

MULTOS includes everything you need for a multi-application smart card – the operating system, the virtual machine (abstract layer) which sits on top of the operating system, and a card security manager that determines what can and can’t be loaded onto the card.

A MULTOS smart card requires a co-processor for RSA, therefore necessitating relatively expensive IC chips. MAOSCO has been discussing plans to support the Open Platform API described below.

Pros: High security. Most mature multi-application card on the market. MULTOS code written in MEL has fastest execution speed of all multi-application smart cards to-date.

Cons: Expensive. Digital certificates can only be obtained from a MULTOS CA in the UK.

7.2. Java Card

The first major release of Java Card was in 1997. The current release, at the time of issuing this paper, is Java Card 2.1.1. The specifications for Java Card come in three parts:
- The Java Run-time Environment
- The Java Card Virtual Machine
- The Java Card API

The Java Card Forum develops and recommends specifications to Sun Microsystems, the owner of Java Card VM and Java Card API specifications.
Java Card isn’t an operating system but a series of specifications which defines how a Java VM can run on any vendors’ underlying operating system. In most cases Java implementations are migrating toward support of the Open Platform standards and API described below.

**Pros**: Java applications are developed in Java using standard tools which developers may already have.

**Cons**: Pure Java Card does not provide issuer control and is not secure enough for financial cards.

### 7.3. Windows for Smart Cards (WfSC)

Announced in 1998, and developed and supported by Microsoft, WfSC includes an operating system, a WfSC Virtual Machine, and an API. The current version of WfSC, at the time this paper was issued, is WfSC V1.1. Versions of WfSC are also available that will support the Open Platform API – described below under Open Platform Card.

**Pros**: Possibly the least expensive card since the operating system supports configuration options for what the issuer might want on the card, and what the issuer might want to leave off the card.

This operating system is backed by Microsoft. Even though the specifications to-date are incomplete and haven’t been fully tested, it is widely believed that someday Microsoft will get it right.

WfSC supports many common and popular tools for development and support.

**Cons**: WfSC does not provide issuer control and is not secure enough for financial cards. Microsoft controls all WfSC technology. Also, WfSC does not fully conform to the industry standard for communicating with smart cards at the application level, ISO 7816-4.

WfSC today only support Microsoft VB compiler.
7.4. "Open Platform" Card

“Open Platform” builds on the card platforms mentioned above and the major difference is the addition of an Open Platform Application Programming Interface (API) implemented on top of these other card platforms. This API adds a standard application programming interface and a standard security manager to these different cards.

Visa initially developed Visa Open Platform (VOP) specifications to “fill in the gaps” in the Java Card Forum’s Java Card specifications. In late 1999 Visa handed over the VOP specifications to GlobalPlatform, a consortium of card manufacturers, issuers and operators to further manage the development of these specifications and to ensure a broad adoption of the specifications.

GlobalPlatform is adding the following to the specifications:
- Definitions and standards for “issuer control”
- Device specifications to facilitate ease of acceptance by smart card terminals and POSs
- Definitions and standards for personalization and post-issuance personalization over secure and unsecured networks

Pros: The Open Platform API and card/security manager allows for the secure loading and deletion of applications on an OP card. OP provides secure communication channel between an issuer and card. The OP API is not limited to Java – can be any underlying operating system.

Cons: Not yet field tested with WfSC (Microsoft) or MULTOS (MAOSCO). Portability is unproven.
## APPENDIX C: Acronyms Used Throughout This Document

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADC</td>
<td>Application Delete Certificate</td>
</tr>
<tr>
<td>Affina™</td>
<td>Datacard’s Smart Card Management System (SCPM) product</td>
</tr>
<tr>
<td>ALC</td>
<td>Application Load Certificate</td>
</tr>
<tr>
<td>ALU</td>
<td>Application Load Unit</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>Aptura™</td>
<td>Datacard’s Java portable operating system product (Datacard’s Java Card)</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CAP</td>
<td>A CAP file contains compiled Java code typically loaded onto a smart card</td>
</tr>
<tr>
<td>CEPS</td>
<td>Common Electronic Purse Specification</td>
</tr>
<tr>
<td>CLCM</td>
<td>Card Life Cycle Management</td>
</tr>
<tr>
<td>CMS</td>
<td>Card Management System</td>
</tr>
<tr>
<td>CMU</td>
<td>Card Manifest Upload (a component of Affina)</td>
</tr>
<tr>
<td>EMV</td>
<td>Europay, MasterCard, Visa</td>
</tr>
<tr>
<td>HSM</td>
<td>Host Security Module</td>
</tr>
<tr>
<td>GlobalPlatform</td>
<td>GlobalPlatform was formed in 1999 by organizations interested in issuing multiple application smart cards to their customers. GlobalPlatform’s efforts to advance common specifications are accelerated by the transfer of the Open Platform card specifications and terminal framework developed by Visa International to GlobalPlatform. GlobalPlatform has been chartered to manage, promote and evolve the Open Platform specifications to ensure that card issuers are provided with a wide choice of card technologies with common back-end systems for application loading and management.</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit</td>
</tr>
<tr>
<td>ICC</td>
<td>Integrated Circuit Card</td>
</tr>
<tr>
<td>IC chip</td>
<td>Integrated Circuit chip</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITSEC</td>
<td>IT Security Evaluation Criteria</td>
</tr>
<tr>
<td>Java™</td>
<td>An interpretative programming language</td>
</tr>
<tr>
<td>Java Card</td>
<td>A registered trademark of Sun Microsystems. Java specifications are available from Java Card Form at <a href="http://www.javacardforum.org">www.javacardforum.org</a></td>
</tr>
<tr>
<td>KEK</td>
<td>Key Exchange Key</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MAP</td>
<td>Datacard’s smart card MAP (Multi-application Architecture for Personalization) makes it possible to generate IC chip data and personalize cards without having prior knowledge of the smart card application or the target card.</td>
</tr>
<tr>
<td>MEL</td>
<td>MULTOS Executable Language</td>
</tr>
<tr>
<td>MSM</td>
<td>MULTOS Security Manager</td>
</tr>
<tr>
<td>OP</td>
<td>Open Platform - OP specifications are available from GlobalPlatform at <a href="http://www.GlobalPlatform.org">www.GlobalPlatform.org</a>. OP is typically used to designate an Open Platform card.</td>
</tr>
<tr>
<td>OP API</td>
<td>Open Platform Application Programming Interface</td>
</tr>
<tr>
<td>OP card</td>
<td>A card which conforms to the GlobalPlatform Open Platform card specification.</td>
</tr>
<tr>
<td>O/S</td>
<td>Operating System</td>
</tr>
<tr>
<td>P3</td>
<td>Datacard’s Personalization Preparation Process product</td>
</tr>
<tr>
<td>PAN</td>
<td>Primary Account Number</td>
</tr>
<tr>
<td>PIN</td>
<td>Primary Identification Number</td>
</tr>
<tr>
<td>PIP</td>
<td>Post Issuance Personalization</td>
</tr>
<tr>
<td>SCMS</td>
<td>Smart Card Management System</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SCPM</td>
<td>Datacard’s Smart Card Personalization Manager product</td>
</tr>
<tr>
<td>SDS</td>
<td>Secure Delivery System (a component of Affina)</td>
</tr>
<tr>
<td>TLV</td>
<td>Tag, Length, Value</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine – an abstract layer typically resident on top of an operating system</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WfSC</td>
<td>Windows® for Smart Cards. WfSC specifications are available from Microsoft at <a href="http://www.microsoft.com">www.microsoft.com</a></td>
</tr>
</tbody>
</table>