



Ten Critical Success Factors for Successful Smart Card Projects

charismathics

Index

1. Introduction	4
2.1. Smart Card Profile	5
2. Smart Card Integration	5
2.2. Smart Card Middleware	6
2.3. Smart Card Readers	8
3. Smart Card Lifecycle Management	10
4. User Enrollment and Card Issuance	12
5. PIN Management	14
6. Smart Card Management Systems	16
7. Card Procurement	18
7.1. Card Manufacturers	18
7.2. Pricing and Delivery Terms	19
8. End User Support	21
9. Conclusion	22

1. Introduction

Many large organizations are planning projects to introduce PKI capable smart cards and USB tokens for end user authentication. Typically such projects plan to use such devices to securely store certificates and keys that enable the user to access web based applications.

This white paper is intended for business and technical personnel involved with the planning and executing large-scale smart card projects. It presents the critical success factors such organizations should consider including like integration, lifecycle management, PIN management, enrollment and issuance, card management systems and procurement. The paper also addresses the significance of the card profile and smart card middleware in relation to these issues.

This white paper is based on the experience **charismathics**® and its partners have had in a large variety of projects, by a large variety of organizations. Examples of projects **charismathics** and its partners have been associated with include:

- Government ID: a Central American country issuing ID cards to first responders and citizens
- Corporate ID: an oil and gas company issuing 120,000 cards to employees, contractors and visitors that replace all passwords.
- Remote Access: a worldwide food company issuing smart cards to its employees for VPN and WLAN security.
- Healthcare: a European country issuing smart cards to identify qualified healthcare professionals
- Education: a US State university issuing student badges to 40,000 students and faculty

2. Smart Card Integration

Most of the smart cards currently used in the world are not used with PC or web based systems. Instead they are used with GSM phones, and payment systems. In order to integrate a smart card with a PC or a web based application it needs a card profile, middleware and a smart card reader. The diagram below shows the smart card components and how they fit into the PC architecture.

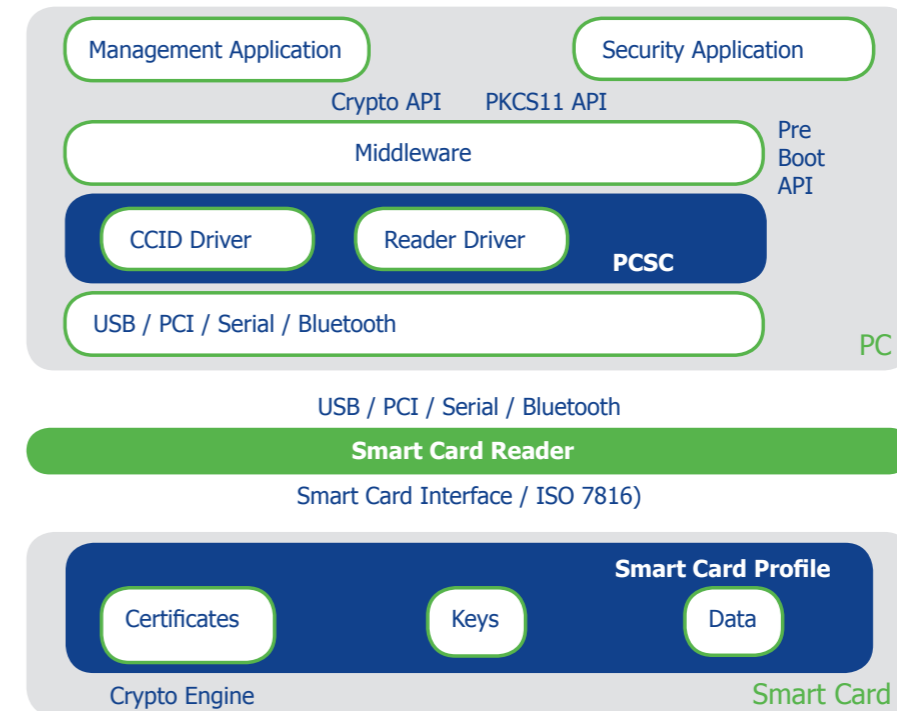


Figure 1: Smart Card Components

2.1. Smart Card Profile

The smart card profile is the means by which the card user data is represented on the card. Typically the profile is defined as a set of files as well as a set of security rules to be enforced by the card, such as card and file access conditions. How the profile is implemented is dependent on the smart card technology involved. Some cards may require the loading of a small application, called an applet, onto the card to enable the profile. Other cards do not. Typically the profile is proprietary – either to the vendor, or the customer. The choice of profile determines the capabilities of the card, as well as the security properties associated with the card. It is therefore a crucial choice.

The industry has worked to define an open standard for a profile standard called PKCS#15. This standard allows a customer to define a profile that is then, in principle, interoperable with smart card applications. However, the specific configuration of the PKCS#15 profile, is still proprietary. In addition, the PKCS#15 specification, as defined,

leads to severely diminished performance. As a result, most vendors have optimized their PKCS#15 implementations to ensure better performance.

Most large smart card vendors (such as Gemalto, Oberthur, G&D, Sagem and HID Global) have their own smart card profiles. By providing their own profile, they can optimize the performance and capabilities of their hardware. However, the proprietary nature of their profile means that the customer is **locked into the vendor's specific hardware**. This means that there is a very high cost to the customer to switch from one vendor to another. Sometimes this leads to customers paying very high prices for outdated smart card products without any alternatives.

Critical Success Factor 1: Select a card profile that meets the project requirements, independent of the hardware vendor. Don't get locked into a single hardware vendor.

charismathics is hardware vendor neutral. Though **charismathics** provides its own highly optimized profiles, these profiles support a wide range of smart cards from different hardware vendors. Customers can choose between hardware vendors, handle procurement directly, and switch at a later stage without incurring additional costs.

Going further, for those customers that have a requirement to fully control their profile, who need to configure the data structures or security rules, or need certification of the profile, **charismathics** can help define and support custom profiles, and in fact, currently supports a wide variety of smart card profiles.

2.2. Smart Card Middleware

The smart card middleware is the software that sits on the end users PC, and interfaces to the smart card on the one hand, and the application on the other. Typically the smart card middleware provides multiple Application Programming Interfaces (APIs), including the Microsoft CryptoAPI CSP, and PKCS11, which is common on non Windows platforms, as well as a low level interface for such applications as pre-boot authentication.

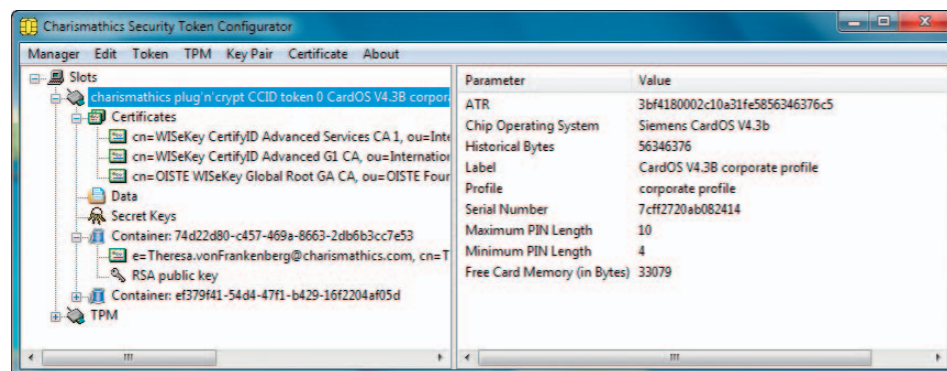


Figure 1: Middleware Utility

In the past most hardware vendors provided their own smart card middleware – often just a simple PKCS11 stack or CSP. However, as PC security technology has developed, the smart card middleware has become more complex.

- Different smart cards implement functions in different ways – even basic cryptographic primitives, such as 3DES, RSA and ECC vary. This means that applications that work with one smart card, may not work with another.
- Middleware needs to support not just standard smart card readers, but also class 2 and 3 secure smart card readers (with integrated PIN pads) as well as biometric readers, “Match on Card” biometric smart cards.
- The PKCS11 and CSP specifications are subject to interpretation. Many applications – including ones from major vendors – are non compliant. Middleware vendors must constantly test applications, and often have to build in “workarounds” to enable support.
- In projects that involve consumers or citizens, the smart card middleware needs to be installed by the end user. The middleware needs utilities and functions that simplify the installation, usage and support of the middleware by the end user, and needs to be dependable and stable on a large variety of systems.
- Many security applications require support for custom or specialized functionality in the middleware. This is true for example with pre-boot, disk encryption and most Single Sign-On applications. Middleware vendors have to implement this support through custom functionality avoiding multiple tokens to be bought.
- More and more platforms are being enabled for use with smart cards. Where before there was just Windows, now there is Mac, Solaris, many different flavors of Linux, and a variety of mobile platforms. Middleware needs to support the platforms required by the customer.
- Many tokens now use smart card commands (APDUs), although they may not use traditional smart card ICs. Such tokens include biometric, special purpose, flash memory and other non-USB devices. Middleware needs to support such tokens in the same PKI projects that include standard smart cards.

The cost and complexity of supporting middleware has become prohibitive for even some of the largest smart card vendors. For example, until very recently, Schlumberger (one of the largest providers of smart cards to the oil and gas industry) did not support any Linux flavors, and even now does not support Mac. As a result customers have become limited in their ability to deploy new applications or platforms and many projects fail simply because of lack of user acceptance.

Critical Success Factor 2: Ensure that the middleware meets your current and future requirements. Standards “compliance” does not ensure interoperability.

Unlike the major smart card vendors, **charismathics**' core business is developing and maintaining smart card middleware. The middleware product has been developed and tested over more than 5 years and implemented with numerous large and small scale projects. **charismathics** supports a wide variety of smart cards, tokens and alternative authentication devices, and has certified numerous security applications and platforms. **charismathics** also supports class 2 and class 3 readers, as well as biometric smart card readers and "Match on Card" smart cards. **charismathics** also supports a variety of alternative devices including biometric tokens, combination smart card/flash tokens and contactless devices.

2.3. Smart Card Readers

Smart card readers are often an afterthought in the smart card project. For consumer and citizen projects, smart card readers can be a significant percentage of the overall project cost. As a result, customers often try to save money by specifying inexpensive readers.

In the past, the quality of smart card readers have been the largest single cause for end user problems – especially with consumer and citizen projects which require user installation of hardware. Several things have changed to improve the situation: smart card reader driver quality has improved. The PCSC specification has been clarified and stabilized. The introduction of the standard Microsoft CCID driver, and CCID compliant drivers have improved. And the introduction of the Microsoft smart card reader certification program promises to ensure compliance.

However at the same time many new smart card reader vendors are introducing new products. Remember that the smart card reader provides the power, communications and clock for the smart card to function. Many of the less expensive products were originally designed for a specific applications (such as payment or loyalty cards, or GSM SIM applications), and are not well tested for PKI smart cards. One common problem is with computers that don't provide enough power over USB. Smart card readers and drivers that don't compensate for this may crash or fail to read or write a card. Or they may simply provide an error message that makes it seem as if the card or software are not functioning correctly. Such problems are extremely hard to trouble shoot and resolve.

With the growing adoption of RSA 2048 bit keys, support for PCSC 2.0 and extended APDU command sets is essential. Performance is also an issue. Smart card readers can be made less expensive by executing commands in the PC driver. This slows things down considerably. Some inexpensive readers don't even provide enough power to the card even when the USB functions correctly. This is especially a problem for cards when they are generating keys (as they do when a certificate is created). Some high performance smart cards draw a lot of power especially when executing cryptographic functions. Other readers don't provide support for alternative platforms such as Mac or

Linux, or even older versions of Windows. As an example – the PCSC compliant smart card reader in certain Dell Latitude notebook computers is well-known for its inconsistent behavior. Specifically high end crypto cards have failed with these readers during generating keys, but the behavior has been inconsistent, with some version testing fine, while others fail making problem reproduction difficult.

Finally, with the vulnerability of the PC platform, many projects are requiring class 2 and class 3 readers. These readers integrate a secure PIN pad that handles the PIN entry within the secure device. This eliminates the PIN capture on the PC, and the associated vulnerability to malicious software intercepting the PIN. For even higher security, some customers are adopting biometric readers that complement or replace a PIN with a fingerprint. Typically the fingerprint is stored on the card, and with some vendors, the biometric is validated on the card itself using "Match on card" technology. These additional security functions requires support in the smart card middleware.



Figure 3: PIN Pad Reader

All card manufacturers provide PCSC compliant drivers. But not all are equal. It is therefore strongly recommended to test the proposed smart card readers with the card to be used, in a real world situation – with real world PCs, and real world applications.

Critical Success Factor 3: Ensure that smart card readers meet the real world usage requirements – not just the nominal "PCSC" rating.

charismathics has extensive experience with all types of smart card readers. For PKI projects it recommends Omnikey and SCM readers. **charismathics** supports PIN pad readers from Omnikey, SCM and others, as well as biometric smart card readers from Precise Biometrics and the Precise "Match on Card" functionality on a variety of smart cards.

charismathics also recognizes that not all projects have control over what reader is used. Through extensive testing it has architected its smart card profile and middleware solution so that it is resilient, and can recover from PCSC failures.

3. Smart Card Lifecycle Management

smart card lifecycle management deals with the different stages that a card passes through during the use of the card, as well as the processes for moving a card from one stage to another. For most PKI cards the smart card lifecycle includes the following stages:

- card issuance
- PIN change
- PIN unblock
- card usage (for each application)
- card revocation

Typically though, more stages are required, and other steps and functions in the smart card lifecycle may include:

- card ordering
- card transport
- card storage
- card initialization
- card type management
- card version management
- card applet management
- card key management
- user/card enrollment (data capture)
- card personalization
- PIN Set
- card activation
- post issuance credential loading
- credential renewal
- card suspension (lost/stolen)
- credential revocation
- card replacement
- card retirement
- card re-use

Other steps in the lifecycle are dependent on the specifics of the project. The overall smart card lifecycle process can be complex or fairly straight forward. A successful smart card lifecycle plan is essential to a successful project. Such a plan should outline the details of what happens in each step (including the information that is captured and processed), who is responsible for the step, and how the step is executed. Often, the lack of a clear card lifecycle plan (and more specifically a clear card issuance process) is a warning sign. Other warning signs include:

- Disagreement over who is responsible for a particular step in the process.
- Lack of clear requirements for data capture and processing
- A card issuance or management process that is very different from existing processes (especially if the smart card replaces or complements an existing document).
- Lack of detail in the (manual) processes required by end users and operators

One advantage of a detailed smart card lifecycle plan is the ability to use it to model the performance and load requirements in each step.

Critical Success Factor 4: Develop a detailed plan for each step in the smart card lifecycle, from ordering to revocation.

charismathics' consultants and consulting partners have extensive experience in analyzing and developing smart card lifecycle plans, and in helping you define the requirements that a particular plan generates for the smart card, software and systems.

4. User Enrollment and Card Issuance

For many large-scale smart card projects the card lifecycle steps that are the most complex are enrollment and issuance. Enrollment involves the steps required to gather and capture the user data needed to produce a card. Issuance involves the steps required to produce a card and get that card in the hands of the end user.

The actual issuance process may vary greatly depending on the security and business requirements of a specific project. In general, however, the enrollment and issuance process can be described as being centralized or decentralized, with the following matrix as a result:

Enrollment	Issuance
Centralized	Centralized
Centralized	Decentralized
Decentralized	Centralized
Decentralized	Decentralized

An example of centralized enrollment is a bank card that is generated using existing user account information, or a citizen card may be created using information from the civil registry. An example of decentralized enrollment is a national ID card that requires the user to go to a government station to present ID, be photographed and provide a signature and/or a fingerprint.

An example of centralized issuance is a driver's license program that mails the card to the address of the user (often the address printed on the card). An example of decentralized issuance is a company ID card that requires the end user to show up at the HR office and sign paperwork.

Whether issuance and enrollment is centralized or decentralized determines much of the work flow requirements as well as the technology and products required.

Centralized issuance processes can often be fully outsourced to specialized card vendors, where the card can be personalized in a secure production facility and sent by mail to the end user. The card can then be activated through an online or phone process. Decentralized issuance processes may still benefit from centralized card production, however cards are then shipped to the issuance location, and customized issuance processes then need to be implemented to get the card into the end users hands.

Decentralized processes work especially well if existing processes are already in place that can be extended or duplicated to handle smart card issuance. For example, school or enterprise may already issue ID cards. By extending the process to include PIN management, the same general resources can be used to issue the smart card.

At the same time, decentralized enrollment and issuance processes are often difficult to implement if entirely new resources need to be developed and implemented.

Critical Success Factor 5: The process of enrolling users and issuing them cards needs to be defined and clarified as soon and in as much detail as possible.

charismathics and its partners have extensive experience with analyzing and defining enrollment and issuance processes, and in helping develop and integrate the card profile and middleware.

5. PIN Management

One crucial aspect of the card lifecycle that is often overlooked by IT managers is PIN management. PIN management entails three functions: setting the PIN, changing the PIN and unblocking the PIN.

The smart card provides strong 2 factor authentication. The card itself is the first factor. The second factor is typically a PIN which needs to be remembered by the end user. Without the PIN, the smart card cannot be used. (Biometrics is generally not used for online smart card applications because of the high cost of the biometric/smart card reader).

Setting the PIN can be done interactively – by the end customer, online as the card is activated or in person during enrollment. It can also be done by sending out a PIN mailer (a process that is common in Europe, but less so in North America).

Changing the PIN can be done by the end user locally, using a utility such as the **charismathics** CSSI® Security Device Configurator. In this scenario a certain number of security rules can be enforced – such as the minimum length of the PIN. Alternatively, some projects call for enforcement of more comprehensive PIN rules, including PIN history and enforcement of types of characters (for example a requirement to use both number, lower case and upper case letters). This often requires an online PIN change system, such as provided by most smart card management systems.

Unlocking the PIN is by far the most complex aspect of card management. Smart cards are enabled for offline PIN authentication. That means that the PIN is presented to the card, and the card then verifies the PIN. The smart card enforces a limited number of tries. If the incorrect PIN is presented too many times, the card is blocked. It then requires a PIN unblock process to reset the PIN for the end user.

The PIN unblock process needs to tie into an “out of band” authentication process. In an enterprise, the “PIN unblock” process often ties into the same system that handles password resets. It might be an automated process that requires the end user to answer questions, or it might require the end user to phone a call center, or even to show up in person. When the user is authenticated, the system can unblock the card by interfacing to the card using the smart card middleware. The security rules and processes for PIN unblock processes vary so much, that no single system provides a complete solution, and typically custom integration of systems is required.

Finally, PIN management requires a great deal of end-user education and support. It is necessary to manage end users expectations to avoid confusion and frustration, and it is also necessary to provide appropriate end user support when things go wrong.

Critical Success Factor 6: An effective and efficient process of PIN management needs to be defined.

charismathics support the PKCS11 PIN management calls – the industry standard process for managing PIN changes and PIN resets on the smart card. Depending on the scenario, the customer may choose to implement a custom solution that interfaces to the card, or use the standard **charismathics** CSSI Security Device Configurator that is part of the smart card middleware package. CSSI also warns the end user once a PIN is entered wrongly, to ensure that they have an opportunity to recover.

6. Smart Card Management Systems

Because the smart card lifecycle can be complex, some vendors strongly advocate for the implementation of a smart card management system (SCM systems) to manage the process. Many general and specialized vendors have such systems.

There are certain situations where SCM systems are strongly advised. However, in many projects SCM systems add additional cost and overhead without adding much value. That is because in many large-scale smart card projects the work flow processes are often quite particular to the project. In addition, the existing technical infrastructure is often predetermined, requiring specialized integration.

One area in which SCM systems are very useful is projects that require extensive certificate management, as well as customized work flows. For example, a bank may use digital certificates to enable the employee to access different sets of assets and applications. Such a bank may have to implement different work flows for different certificates.

A user in Austin, for example, may need a certificate to access the local network infrastructure. Such a certificate has to be authorized by the local manager. The same user, though, may have to get access to the wealth management application in Germany, authorized by a manager there, as well as a trading application in New York, with its own manager.

In such a project, it is necessary to be able to handle a diverse user base, and many different certificate usage profiles, as well as to be able to extend the certificates and processes in the future. Typically SCM systems are well suited for this.

However many large smart card projects have fairly straight forward processes and only a single credential on the card. The complexity of such systems is in implementing the large-scale personalization systems and logistics systems with specialized equipment and processes. Even when a project has more complex processes, this is often because of operational or political complexities and a SCM system may not be a solution. Although SCM systems may have highly flexible workflow engines, the particular workflow of a project may be more cost effectively implemented using custom software.

Smart card management systems can be very expensive. Quite often they require significant customization to handle the specific requirements of a project. In such situations, a dedicated custom system, often in combination with outsourced issuance services, can be a better solution.

Quite often, the complexity lies in the issuance processes and logistics where SCM systems frequently don't have comprehensive solutions. Often it is these physical processes that are overlooked or underestimated by IT oriented managers. In this

area standard Card Management Systems (CMS) are a viable option. These are systems designed for ID badges or plastic card processing, and – though they may have some smart card functionality – are not designed for post issuance management, credential management or full lifecycle management. Typically, CMS systems are well suited for user enrollment and data capture, because they integrate well with cameras, signature and fingerprint capture equipment, areas where SCM systems typically lack in functionality.

Smart card management systems are sometimes selected because the customer has not yet determined the card and credential lifecycle, where there is lack of consensus on the processes, where the customer wants to keep his options open, or expects that addition of credentials or card lifecycle steps post issuance. In such a situation, the choice of a smart card management system is not going to help. Understanding the card lifecycle requirements and selecting an appropriate solution is critical.

Critical Success Factor 7: Smart card management systems are no panacea. Choosing the right card management system – or no system at all – is crucial.

charismathics and its partners have a great deal of experience with many different kinds of smart card management systems including those from Microsoft (ILM), Intercede and partners (MyID), BellID (ANDiS) and others, as well as badge and card management systems from ScreenCheck (BadgeMaker/CivilID), Fargo (Asure ID), DataCard (ID Works) and others. The **charismathics** CSSI middleware is well suited to custom integration and development, providing an excellent platform component for customers that need to implement their own workflow processes.

7. Card Procurement

7.1. Card Manufacturers

PKI smart cards are not generally provided as standard off the shelf products. Instead they need to be custom ordered and custom manufactured. Specifically, during card production, the card needs to be configured so that it is ready to interoperate with the smart card middleware. This entails setting the appropriate configuration for the card, setting security keys, and possibly also setting security policies and loading card applets.

The large smart card manufacturers (Gemalto, Oberthur, Giesecke & Devrient, Sagem and others) generally focus on large production runs for GSM SIM cards and banking cards. These typically are multi million card orders that run for weeks and even months. As a result they are not well suited for smaller runs, especially when this requires a lot of configuration and setup.

Any run less than 10,000 units, and often less than 25,000 units is considered a small run. This should be kept in mind, because typically, even a large smart card project (100K and above) starts with a smaller trial or slower roll out. Often the larger smart card vendor look for the customer to lock into large committed orders to get adequate pricing and delivery terms before the cards or processes have even been tested. Smaller card vendors can be more flexible.

In the past, the large card manufacturers had a unique position in the smart card business, because only they had the specialized equipment and knowhow to create smart card chips, smart card operating systems and modules, and embed them into plastic card bodies.

In the last 5 years however, the industry has changed. Chip manufacturers such NXP and others now offer complete card modules with smart card operating systems. At the same time many card machinery manufacturers have developed highly sophisticated equipment that have enabled other plastic card vendors to provide smart card products. Many plastic card vendors already have experience with security sensitive operations (especially if they produce bank or credit cards). In addition, many such vendors have experience in card personalization and mailing, which is relevant for customers that need to ship directly to end customers. As a result national and international plastic card vendors may be an excellent alternative to the large card manufacturers in providing card manufacturing, printing and issuance solutions.

The large card manufacturers also prefer to sell their own hardware and card operating systems which, though often of excellent quality, means customer get locked into a particular platform, and find it difficult to switch to alternative vendors.

Finally, production expertise varies greatly between manufacturers depending on the type of module and card body that is required. For combination contact/contactless cards for example, where the card body includes an antenna that must be bonded to the smart card chip, certain manufacturers have a great deal more experience than others.

Critical Success Factor 8: The large smart card vendors are not the only alternative: find a reliable smart card vendor in the right geographic location who provides the needed volume and services specific to the program.

Though **charismathics** is not a card manufacturer, it does have excellent relationships with both smart card chip and card manufacturers. Through these relationships **charismathics** can provide pre-certified card modules that can be embedded by local plastic card vendors, or by specialized card manufacturer partners in Europe, Asia or the USA. **charismathics** can also provide independent advice on the pros and cons of specific technologies and services, and on the quality and reliability of products and vendors.

7.2. Pricing and Delivery Terms

Although smart cards are pretty much a “commodity” product at this time, there can be a large fluctuation in pricing and delivery terms between vendors. There are various reasons for this. It may be because card manufacturers are often restricted to using particular production lines for particular cards (such as PKI capable cards) and such production lines may be tied up for long periods with SIM or bank card production. At the same time, there is a high cost to keeping production lines idle, and so manufacturers with gaps in their production planning may often be willing to provide capacity at very low prices.

In addition, large card manufacturers are dependent on chips from the chip vendors, and at any time there may be bottleneck and supply issues in that channel. For example, when a particular chip vendor switched to new manufacturing technique, or new chip design, there may be a large lag in production volume that affects smart card production.

For specialized card bodies (for example ones that include contactless technologies, or high security technologies), card manufacturers may be dependent on third party suppliers that have their own priorities and supply issues.

Finally, manufacturers vary greatly in their production reliability. Typically card manufacturers will require the customer to accept some over or under production. This may be as high as 5% over or under the target volume required. This covers cards lost

due to manufacturing problems (typically production “start-up” loss). When the card body contains additional technologies (like contactless or holograms) this card loss may be expensive, therefore the quoted per unit price needs to be adjusted with the requirement to accept overage production.

As part of the ordering process, it is essential that the customer gets approval of sample cards, and that the customer establishes a good process with the middleware vendor and the card profile vendor to ensure that the sample cards are approved and functional. This process may take anywhere from a week to 6 weeks depending on the responsiveness and technical capabilities of the smart card manufacturer. This will prevent the situation that some customers have found themselves in: with a large inventory of cards that did not meet spec, and were essentially useless for the project they were intended for.

Depending on the manufacturer and the state of the market, delivery times will range from 3 months from order to as long as 9 months.

Critical Success Factor 9: Procurement should be prioritized. Identify what is needed as soon as possible, and start the procurement process.

Through its relationships with chip and card manufacturers, **charismathics** can provide unparalleled insight into the state of the market, and can provide bidding advice as well as quotes on cards and modules.

8. End User Support

In the end the success of a large-scale smart card project depends on the end user. Projects that make for unhappy end users have a large chance of failing. Even in projects where end users can be forced to make use of a smart card for a particular application, lack of end user support can lead to delays and excessive costs. For this reason, effective end user support is crucial.

The end user experience is especially important when the end user is responsible for installing and configuring the smart card reader and middleware. In such a situation, it is strongly advised to pay attention to the packaging, documentation and the quality and effectiveness of the installation package.

For application use, it is crucial that the application user interface integrates the smart card usage steps, and provides useful hints and documentation. For example, a log in screen should include information on inserting the smart card and PIN.

Farther throughout the lifecycle, the integration of the application and management functions is also useful. For example, if a digital certificate needs to be requested or renewed, it is useful that the appropriate functions are prompted during the application use, rather than requiring the end user to read a separate email and start up a separate smart card application.

It is useful to be reminded that different users prefer different support processes. This means that multiple ways of figuring out a problem should be provided. For example, information on changing a PIN could be provided through a quick start doc, a detailed manual, a help screen, online faq as well as by interactive chat and telephone call.

Finally, effective user support starts by minimizing user problems in the first place. This includes choosing reliable hardware and software components that don't crash and provide effective user feedback when problems occur.

Critical Success Factor 10: The success of a project is defined by the end user – ensure that the appropriate end user support processes are in place.

charismathics' CSSI software has been in the market for more than 5 years, and has been used by millions of users in all types of situations. The result is a highly dependable end user application that minimizes problems with the installation and use, and provides information on the state of the card and the problem to enable the end user and program support staff to resolve any problems that occur.

9. Conclusion

Planning and implementing large-scale smart card projects is inherently complex. Identifying and analyzing the particular aspects of a project that are potential pitfalls or bottlenecks as soon as possible is essential. The objective of this white paper has been to identify the critical success factors that most projects must deal with, and provide an initial overview of the issues involved.

No single document can effectively cover all the essential issues, however. **charismathics** and its partners have many years experience in providing the software, hardware and services required to make your project a success. We strongly encourage you to contact us, and help us work with you on the particulars of your project.

CSSI®



The charismathics smart security interface is a PKI middleware supporting all major standard industry interfaces like CSP, PKCS#11, tokenD, mini-driver as well as a wide range of operating systems including Windows, Mac OS, Linux, Solaris and several smart card platforms (i.e. JCOP, CardOS, StarCOS, GemXpresso, CosmoID). CSSI improves your ROI by allowing the user to rely on multiple hardware authentication solutions simultaneously. Together with iEnigma, CSSI supports smart phones in replacement of USB tokens and smart cards.

iEnigma®



The charismathics iEnigma is an application for mobile phones which makes them act as a hardware security device. It runs in dual mode operation, either in replacement of a smart card and its reader to perform two-factor authentication actions like digital signature and encryption on your laptop; or to support stand-alone applications for the smart phone to carry out cryptographic operations. iEnigma also strongly enhances the user convenience by upgrading the mobile environment.

plug'n'crypt®



The charismathics plug'n'crypt is a driverless USB token embedding a smart card chip, a flash memory component and a RFID tag into one unique robust housing. Perfectly integrated with CSSI, it's a commodity for daily use in operations like digital signature, file and email encryption, VPN and PC logon even at pre-boot level, password management. Together with smart security interface, you have your digital credentials always with you and can run applications safely without leaving footprints behind.

charismathics is a global leader in identity management software. Since 2004, charismathics has pioneered the field of Public Key Infrastructure opening the way to a more flexible offering for the customers. Enabling complex IT architectures and PKI software solutions, charismathics puts forward a wide range of products and services for a variety of industries including banking and finance, healthcare, telecommunications, security, government and PC manufacturing. charismathics offers the only true middleware solution worldwide.

charismathics

the middleware company

47 Sendlinger St
Munich, Germany 80331

www.charismathics.com
sales@charismathics.com

phone +49 (89) 3090-6700

charismathics

the middleware company

2033 Gateway Place Suite 500
San Jose, CA 95110, USA

www.charismathics.com
sales@charismathics.com

phone +1 (408) 573 6440