

An Open Smart Card Infrastructure for South African e-Services

P T Nkomo University of Fort Hare Computers Science Department Box x1314, Alice, 5700 pnkomo@ufh.ac.za	A Terzoli Rhodes University Computer Science Department Box 94, Grahamstown, 6140 a.terzoli@ru.ac.za	H N Muyingi University of Fort Hare Computer Science Department Box 1314, Alice, 5700 hmuyingi@ufh.ac.za
--	--	--

Abstract

The emergence of electronic services in South Africa presents a challenge of online identification and effecting payments. The South African government through the Home Affairs National Identification System (HANIS) project has identified the smart card as an ideal technology to develop a secure digital identification and payment tool that will be used in future to access and pay for electronic services. This has raised the need to develop a secure transaction environment to support smart card based payments over public networks like the internet. This paper proposes the adoption of open smart cards and the related open smart card based infrastructure, all based on open Java technologies that can be deployed to promote electronic services in South Africa. Special focus is given to technologies that ensure interoperability and software portability at card terminal level in order to promote home-based access to electronic services using smart cards. Development of such an open platform will provide a set of reusable building blocks from which future secure smart card based services are deployed.

Key words: e-services, open smart cards, card terminals

1.0 Introduction

Web-enabling of transactions for electronic government and electronic commerce has made the development of a multifunctional digital identification and payment tool urgent. This tool is now necessary because when accessing electronic services (e-service), users can no longer communicate directly with an agency or employee. Communication is between a web application and a device which acts on behalf of the device holder as a client in a distributed architecture. These client devices should provide enough evidence supporting their trustworthiness and integrity to represent and interact with a web application in effigy of their owners or holders [1]. In South Africa, a smart card has been identified by government as an ideal technology to develop such a secure automated identification and payment card [2].

A smart card is a credit card sized plastic card with an embedded single-chip computer [3]. The chip contains a central processing unit, random access memory, and non volatile data storage space. Using smart cards, encryption and decryption of data using public key infrastructure is possible. They offer solutions to the inherent problems of cryptography of how to perform key distribution, securely store keys and determining an entity entrusted with the role to perform encryption and decryption. Smart cards are resistant to attack because they do not depend on potentially

vulnerable external resources [4]. Querying information in the card requires physical possession of the card, good understanding of the smart card hardware and software and possession of additional equipment.

Smart cards are service-providing devices that are portable and programmable. Service in this context refers to resources either directly on the card or on other nodes in a network. Users of smart cards carry them in their pockets and as a result have the data available wherever they go and wherever it is needed if the connection to the relevant network is available. This provides a unique opportunity to create new classes of distributed application that are able to seamlessly integrate the pocket portability of smart card services with the internet [5]. This is essential in enhancing online transactions. Allowing multiple applications to be bundled in a single smart card provides the necessary convenience people need when they access one-stop web portals.

1.1 Challenges to deploying smart cards

Although smart cards as a technology seem to offer an ideal solution to the problem of secure digital identification systems and payment methods, the greatest challenge is how to adapt the technology to solve these problems. Realizing the potential that smart cards have on offer as multi-application card can be achieved if various stakeholders in the card industry endorse the smart card infrastructure developed [6]. As with any social interaction, online interaction is based on attaining mutually acceptable levels of trust between various stakeholders. For example, success of smart cards as a payment tools requires support and underwriting by financial institutions. This is only possible if the smart card infrastructure is secure, modular, flexible and scalable, ensuring interoperability of smart card based services [6]. End users, in this case, cardholders are prepared to use smart cards if they offer access to value-added services. However, as Ort [7] has noted, the application programming interfaces (APIs) that support smart cards and card terminals are typically proprietary and

complex in nature. This makes it difficult to write general-purpose e-service applications that are portable and interoperable.

In order for the smart card infrastructure to be sustainable, the problems of interoperability and portability have to be addressed. The infrastructure should allow for installation of software and loading of data on smart cards using the card terminals on the network [6]. This is because cardholders should be able to download applications of their choice onto their card using card terminals. This demands a secure automated way of delivering software to card terminals on an open network to be accessed by cardholders. A standardized storage data file formats should be adopted and this has to be adapted for use in memory-constrained devices like the smart card. Adopting a shared data file format will offer shared ability to smart cards to execute applications irrespective of the smart card specific technologies.

Closely related to the concept of interoperability is the need to interface card terminals with open networks like the internet. This requires adoption or development of a shared application programming interface (API) implemented by most card terminals. This API should be adapted to run on small card terminals with limited memory resources. It has to support multiple applications and allow downloading and running of applications on a variety of card terminals. Security issues of a card terminal for home-use also require attention because there is currently no secure infrastructure for this type of set-up [8]. PC/SC, which is currently the most used industry standard in the PC-attached smart card technology, does not provide such security [8]

Adoption of smart cards as a security tool in a multicultural society should not be taken for granted. Security tools may raise negative perception as shown by studies conducted by Hsu, Davison and Stares [9]. Cardholder will need to know who has access to their personal information on their cards. As a result, there is a need to come up with mechanisms

that will ensure better control of the card contents by the cardholder. The card should be viewed as a tool to access personalized services with a provision for future dynamic downloading of information onto the card. This is important because services providers will need assurance that their services will be made accessible to a large pool of consumers.

The various challenges associated with deploying smart cards make the adoption of open multifunctional smart cards and development of an open smart card infrastructure ideal. As Tambouris [10] has recognized, online one-stop services will only reach their maximum potential if they are supported by open and extensible platforms. An open smart card is a card that is able to execute application code independent of the operating system running on the card. Applications installed on the card are personalized in such a way that they can be selected and personalized in an independent way with one application not being able to access another application's private information. These cards allow implementation of authentication and identification at the application level rather than as part of the card runtime environment or card operating systems. This is ideal for security since the cards offer each application a firewall mechanism to protect application data.

1.2 Challenges of deploying open smart cards

Although adoption of open smart cards seems an ideal option, their deployment on an open network like the internet presents a number of challenges. Allowing dynamic data downloading onto the smart card using card terminals on an open network opens the smart card based identity card or payment tool to attack. This is because such a network offers an environment to transmit malicious code. In an effort to address security of cards against dynamic downloading of malicious code, conflict of expectation has to be addressed. An application provider will not desire to go through a rigorous security process when downloading an application onto the smart card. On the contrary, the card

issuer is obliged to provide a certification process that the application provider should go through before downloading an application on the smart card.

Another problem of open smart cards is data sharing. Smart cards are low memory systems that will require sharing of data objects in order to be able to handle a larger number of applications. For example, use of smart cards for electronic commerce might require sharing of digital signatures to save memory space and to allow the card issuer to be able to bill the application provider each time their application accesses the digital signature on the identity card. This poses a security challenge. An efficient data-sharing scheme has to be developed to allow application on the card to be able to access the shared data while being denied a way to share that data with application outside the card [11].

1.3 Developing an open smart card infrastructure

The development of an open smart card infrastructure should involve the development of a digital identity and payment tool using open smart card technologies. The smart card terminals should be standardized and a common public key infrastructure to be used on the platform agreed upon.

1.3.1 The identity card

Adoption of the Java Card technology which supports GlobalPlatform [12] is an ideal option for developing an open smart card based identity card. Experiments by the authors of this paper at the University of Fort Hare proved the feasibility of developing an open, cost effective multifunctional smart card to support electronic services [13]. The card developed hosted an identity module and an electronic wallet. Development was based on free and open source software that supports open standards.

The Java Card technology was used because its application programming interface is based on open smart card standards like ISO7816 [14], GlobalPlatform, EuroPay MasterCard Visa (EMV) [15]. Java Card technology is

ideal for open smart card infrastructure because it provides a secure and interoperable execution platform that can store and update multiple applications on a single card. Applets developed with Java Card technology run on any Java Card technology enabled smart card and are independent of the card vendor and underlying hardware.

Implementation of the GlobalPlatform specifications by Java Card technology offers a solution to the problem of secure dynamic downloading of application on the smart cards discussed above. This brings into the open smart card infrastructure the benefits of software or application portability. Figure 1 below shows the implementation of the GlobalPlatform architecture on Java Card technology to ensure security of application.

Card Domain	Security Domain	Smart Card Applications
GlobalPlatform API		Java Card API
Java Card Virtual Machine		
Operating system		
Microprocessor	Memory	

Figure 1: GlobalPlatform architecture on Java Cards

The identity card middleware was developed using the OpenCard framework (OCF). This is an open standard framework providing an architecture and a set of application programming interfaces (API) based on Java that enables application developers and service providers to build and deploy smart card solutions without having to worry about terminals or smart card specific features [16]. Adherence to the framework makes components directly usable by different applications and services.

1.3.2 Standardization of terminals

Once the identity card and the payment tool is developed, smart card terminals should be standardized to ensure

interoperability at the smart card terminal level. The adoption of Small Terminal Interoperable Platform (STIP) and the Global Platform Device (GPD) specifications commonly referred to as the GPD/STIP specifications [17] is an ideal option. These specifications provide an open, adaptable, and interoperable software platform technology for secure transaction devices, including, but not limited to card terminals. It supports a number of point-of-sale devices [17]. GPD/STIP provides a Java API that allows for interoperability of applications among a variety of card terminals and independence from card terminal vendors. The API also offers functionality to secure remote maintenance of multiple applications on the card. This technology has been tailor made for low memory devices with the core technology and the APIs alone consuming less than 100KB of storage memory [18]. The STIP architecture also provides functionality for developing a distributed computing model using smart cards [19].

To ensure file format compatibility at card terminal level, we propose the adoption of the Java Executable File Format (JEFF) file format. JEFF is an ISO certified efficient file format that provides a ready-to-execute format for object-oriented programs designed especially for Java programs [20]. JEFF drastically cuts the requirements for run-time memory and makes the usual class file format twice as small without any compression. JEFF is of great importance for the effective deployment of object-oriented programs on small devices.

1.3.3 Securing card terminals

Security is a major issue on open platforms. The unavailability of a secure communication infrastructure between a PC and a smart card terminal necessitates the development of a functional architecture to ensure security of the communication link. This functional architecture should not only be limited to the PCs but should be extensible to support small personal computing devices like the PDAs and mobile phones. This is because these are gaining much popularity and have a potential to boost

mobile commerce in South Africa. The Embedded Financial Transactional IC Card Reader specifications (Embedded FINREAD) [21] offer the right platform to address this problem. The specifications describe a card terminal used for payment and ecommerce transactions, which guarantees security in an untrusted environment like home-access and the internet. The aim is to ensure interoperability of secure transactions on open networks through offering a common format for downloading applications and a common set of APIs between the card terminal software and the downloaded applications [21]. Its Core API is defined by the Java Virtual Machine specifications. Figure 2 below shows the proposed open smart card terminal architecture.

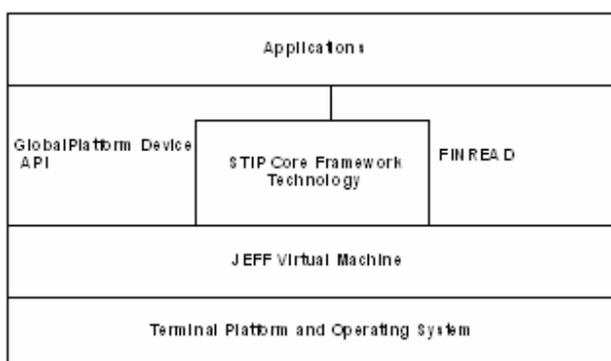


Figure 2: An open platform terminal architecture

1.3.4 Public key infrastructure

There is a need to revisit the use of public key infrastructure (PKI) in smart card for identification and authentication so that a generic PKI module is developed and provided by a nationally recognized and legal supported institution. When developing this security module, an optimal balance between security and the limited memory constraints of smart cards has to be found. There is also a need to identify the type of security information to encode into an on-card application and which one to provide using an off-card application. Smart cards have been used in a fragmented and proprietary manner in South Africa. Once the issue of a common PKI module is addressed, a large smart card community accessing electronic services may emerge.

1.4 Conclusion

This paper has presented various challenges associated with deploying smart cards that makes the adoption of open smart cards necessary. The open smart card infrastructure has been proposed beginning with the development of the identity card that can be used as a payment tool. Specific focus has also been given to interoperability and security issues at card terminal level. Developing such an open infrastructure will provide a platform on which future smart card based services are deployed with easy. It will also promote home-based access to e-services using smart cards.

1.5 References

- [1] Reinhard Riedl, *Facilitating Administrative Services for Mobile Europeans (FASME) with Secure Multi- Application Smartcards*. Available at: <http://www.ifi.unizh.ch/egov/EU2000new.pdf> [Last accessed April 2006]
- [2] The Directorate: The South African Department of Home Affairs, *The Home Affairs National Identification System (HANIS) Project, March 2003*. Available at: <http://home-affairs.pwv.gov.za/projects.asp> [Last accessed January 2006]
- [3] C Cagliostro, *Smart Cards Primer*. Available at: http://www.smartcardalliance.org/industry_info/smart_cards_primer.cfm [Last accessed May 2006]
- [4] Smart Card Alliance, *Security*. Available at: http://www.smartcardalliance.org/industry_info/security.cfm [Last accessed May 2006]
- [5] A T S Chan, F Tse, J Cao, H V Leong, *Distributed Object Programming Environment for Smart Card Application Development*. In of Proceedings of the Third International Symposium on Distributed Objects and Applications, 2001, IEEE Computer Society Washington, DC, USA. Available at: <http://portal.acm.org/citation.cfm?id=874058.875275&coll=GUIDE&dl=GUIDE> [Last accessed May 2006]
- [6] eESC, *Open Smart Card Infrastructure for Europe v2*. Available at: <http://eeurope-smartcards.org/index.php> [Last accessed May 2006]
- [7] E Ort, *Writing a Java Card Applet, June 2001*. Available at: www.developers.sun.com/techttopics/mobility/javacard/articles [Last accessed May 2005]
- [8] K Schmid, H Zeitlhofer, *FINREAD Whitepaper*. Available at:

www.omnikey.com/fileadmin/documents/FINREAD_Whitepaper.pdf [Last accessed May 2006]

[9] C Hsu, R Davison, C Stares, *Cultural Influences on Attitudes Towards Hong Kong's Smart Identity Card*. Available at: <http://www.pacis-net.org/file/2004/S05-004.PDF> [last accessed May 2006]

[10] E Tambouris, *An Integrated Platform for Realizing Online One-Stop Government*. Available at: http://www.egov-project.org/egovsite/tambouris_dexa2001.pdf [Last accessed January 2006]

[11] P Girard, JL Lanet, *Java Card or How to Cope with the New Security Issues Raised by Open Cards?* In Proceedings of Gemplus Developer Conference. Paris, France, 1999. Available at: <http://www.cert.fr/francais/deri/wiels/Pacap/rapports-pres/GDC99.pdf> [Last accessed May 2006]

[12] GlobalPlatform specifications. Available at: www.globalplatform.org. [Last accessed January 2006]

[13] P T Nkomo, *Developing a Multifunctional Smart Card Based Identity Card to Support e-Government In South Africa*. A Master of Science in Computer Science thesis, University of Fort Hare, 2006.

[14] International Standard Organization. Available at: www.iso.org [Last accessed May 2006]

[15] Verifone, *EMV: Global Framework for Smart Card Payments*. Available at: www.verifone.com/pdf/EMV_white_paper.pdf [Last accessed January 2005]

[16] D Gildea and T Dowling, *A Java OpenCard Framework based Medical SmartCard system*. ACM International Conference Proceeding Series, Vol. 42. Available at: <http://portal.acm.org/citation.cfm?id=957289.957320> [Last accessed January 2006]

[17] GlobalPlatform, *GPD/STIP Specifications*. Available at: <http://www.globalplatform.org/showpage.asp?code=gdpstip> [Last accessed may 2006]

[18] GlobalPlatform, *GPD/STIP Specification 2.2 Overview Java Version*. Available at: <http://www.globalplatform.org/showpage.asp?code=gdpstip> [Last accessed may 2006]

[19] European Committee for Standardization, *Embedded Financial Transactional IC Card Reader - Part 4: Technical Architecture And Definition Of Apis*, CEN Workshop Agreement CWA 14722-4 January 2004.

[20] ISO/IEC20970, Information technology, *Programming Languages, their Environments and System Software Interfaces, JEFF File Format*. Available at: <http://webstore.ansi.org/ansidocstore/product.asp?sku=INCITS%2FISO%2FIEC+20970%3A2002> [Last accessed may 2006]

[21] FINREAD consortium, *FINREAD Technical Specifications*. Available at: http://www.finread.com/pages/about/specifications/01_specifications.html [Last accessed May 2006]

About The Author

Peter T Nkomo did his MSc in Computer Science at the University of Fort Hare. He enjoys smart card programming using Java.