Location Based Application Availability

Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes

Information Security Group Smart card Centre, Royal Holloway, University of London
Egham, Surrey, United Kingdom
{R.N.Akram,K.Markantonakis,Keith.Mayes}@rhul.ac.uk

Abstract. Smart cards are being integrated into a diverse range of industries: ranging from banking, telecom, transport, home/office access control to health and E-passport. Traditionally, cardholders are required to carry a smart card for each application. However, recent developments in the Near Field Communication (NFC) have renewed the interest in multiple applications for different services on a single device. This paper builds onto the NFC initiative and avoids the smart card ownership issues that hinder the adoption of such devices. The proposal integrates the Global Positioning System with the NFC in mobile phones to provide a ubiquitously and flexible service access model.

1 Introduction

The smart card based service model is predominately issuer centric. This model gives the control of cards to its issuing organisation (i.e. banks, Telco, transport operator). The multi-application smart cards gave the technical capability of having multiple applications on a single card; however, the business case for such a scenario has been considered difficult until now. The Near Field Communication (NFC) [1] has enabled a Secure Element (SE) in a mobile phone to communicate with the terminal (e.g. ATM, Access Control, smart card reader etc) as a contactless smart card. A SE is an electronic chip that can securely store and execute programs (e.g. smart cards). Over the course of this paper, the term SE and smart card are used interchangeably. There are many organisations [2-4] that are putting new business models on trial to foster partnerships to accommodate this trend of convergence revitalised by the NFC initiative of different services onto a single chip. However, the traditional ownership issues of the SE are not being addressed. In this paper, a model based on the SE, NFC and Global Positioning System (GPS) [8] is proposed, enabling cell phones to be used ubiquitously to access a range of services. The proposal avoids the ownership issues of the smart card based service model that has decelerated the adoption of multi-application smart card technology.

In section two the Location Based Application Availability (LBAA) is described along with the motivation. The architecture that supports the LBAA proposal is discussed in section three. Different processes of the proposed model are described in section four. In section five, future research directions are listed, and finally in section six, we present the concluding remarks.

R. Meersman, P. Herrero, and T. Dillon (Eds.): OTM 2009 Workshops, LNCS 5872, pp. 128–138, 2009.

2 Location Based Application Availability

In the following section we provide the motivation behind the proposed model, followed by the description of the LBAA proposal.

2.1 Motivation

The multi-application smart card technology has been introduced for more than a decade. However, the adoption of the technology is not being encouraged and it is mainly hindered by the issues of smart card ownership and associated relationship with customers. The issuers of smart cards actively control the relationship with the customer, as in most cases customers have to register with the issuers.

Recent developments like NFC [1] and SE [4, 14, 15] in cell phones has re-energised the multi-application smart card initiative. It can enable a user to have multiple applications from different organisations that are installed on their SE, and use their cell phone to access associated services. Reducing the number of cards a user has to carry to perform mundane tasks.

To support the initiative, there are different proposals for hardware and application lifecycle management. One proposal is to keep the traditional issuer ownership model that has been existing in the smart card based service model for decades. Another proposal is to delegate the ownership to a third party referred to as a Trusted Service Manager [4, 5, 6] that only manages the SE platform lifecycle. In both of these proposals, the ownership has to be delegated to an organisation. Whereas, other companies (lease holders) has to establish a trust relationship with the owner of the SE before they are able to provide services to their customers. The lease holders also have to trust the underline platform where their application is going to be installed. Thus, not only the lease holder has to trust the owner but also the actual platform.

The ownership issue is still not fully resolved in the NFC initiative, puting it off for later resolution. However, it is evident from the multi-application smart card initiative that if these issues are not resolved satisfactorily, the fate of this trend would also be similar. In this paper, we present a theoretical proposal that removes the ownership issues and implicit trust in the underlying platform (SE).

2.2 Location Based Application Availability

The Location Based Application Availability (LBAA) enables a user to utilise a service by connecting to an associated remote application, based on its location information. The LBAA does not require the installation of an application onto a SE, removing the requirement of implicit trust and ownership of the platform. The remote application is hosted on a Remote Application Server (RAS) that is in total control of the application issuer (i.e. banks, transport, etc). The SE will support the LBAA model independently of its owner. The security of the SE is ensured by the manufacturer, making the ownership issues irrelevant in the LBBA model.

The SE only has a secure binding with a RAS that enables the cell phone to connect with it and use the associated services. The cell phone connects through

the internet provided by the mobile operators, as soon as the user enters the associated service zone. The service zone is identified by the aid of the GPS, collaborated with the published service terminals. The GPS is a navigational system that utilises a constellation of satellites in the medium earth orbit. The GPS can lock a position accurate to about 5 to 15 meters horizontal depending upon the atmosphere and geographical factors [8]. Most of the modern cell phones are equipped with the GPS, and it is used by the LBAA framework as a primary reference to the user's position. The list of service terminals and their GPS locations can be advertised by mobile operators, third parties or users.

The customers are only required to carry their cell phones, and applications to access services (i.e. banking, transport, etc) will be made available on demand. The location of a user plays an important role in the model. It decides whether to connect with a RAS, depending upon the services available in close vicinity. For the LBAA, the functionalities provided by the proposed model are as below:

1. A user only presents his/her mobile phone to a terminal and the related application should be available automatically without user's involvement.
2. Applications are not stored on SEs. They are hosted on their issuer's RAS and execute remotely.
3. The SE has credentials to access the remote application and acts as a secure communication bridge between the remote application and the terminal.
4. It provides a secure and flexible interface/mechanism to register with a RAS.
5. The SE connects with the remote application(s) as soon as the user enters into the proximity of the terminal. For example, if a user enters the proximity of an ATM the SE would connect with a remote banking application.
6. The SE should provide adequate security and privacy to the security parameters for each of the remote application, which is registered with it.

The details of the proposed architecture based on the Smart Card Web Server (SCWS)[7], NFC, and GPS are discussed in the next section.

3 Location Based Application Availability Architecture

This section details the architecture of the proposal and its integral components.

3.1 Generic Architecture of Location Based Application Availability

The LBAA framework is based on cell phones and Service Providers (SP) that supports the LBAA to provide services to their customers. The mobile phones have SE(s) that also has the capability of the SCWS. The architecture is illustrated in figure 1 and main components are described in the following sections.

The mobile phone provides an interface that enables a user to enter SP's registration credentials. The SP's registration credentials are issued by the relevant SPs after the user is registered. From the SP's registration credentials the SE will initiate an enrolment process with the Remote Application Enrolment Server (RAES). The RAES enables the SE to establish a secure binding for the

Remote Application Server (RAS). The secure binding will be used in future to establish a connection with the RAS to access the remote application(s).

As a user enters in vicinity of a service terminal, the Event Triggering Software sends an alert to the Behaviour Analyzer. That calculates the probability of the user accessing the service. If the user is predicted to use the service, it would request the SCWS to establish a connection over the internet with the corresponding RAS and then act as a bridge between the terminal and the remote application(s).

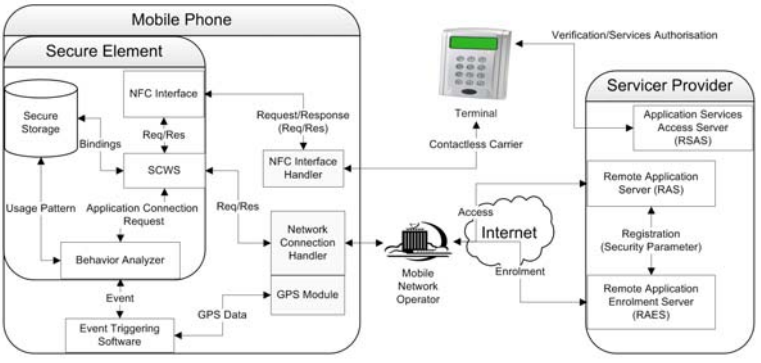

Fig. 1. Location Based Application Availability Architecture

When the user waves the mobile phone on a terminal to access service(s), the terminal challenges the mobile phone to authenticate the user (application). The challenge is sent to the remote applications by the SE. Once the remote application authenticates the user, the terminal will provide the requested service(s).

3.2 Secure Element

A removable smart card based memory card is a suitable option for the SE for its mobility and in most case under user's ownership. The SE provides the operational and security support for the LBAA model and it will ensure that the user would have the total privilege to bind their SE to any RAS they require.

3.3 Smart Card Web Server

The Smart Card Web Server (SCWS) enables a SE to communicate directly over the internet. The LBAA model requires that the SCWS supports the TCP/IP and SSL/TLS protocols. The functions of the SCWS in the LBAA framework are listed as below:

1. Facilitate the establishment of a secure binding between a SE and a RAS.
2. The Secure and unique bindings are store in a secure storage in complete isolation to any other applications/processes or bindings.

3. On the request of either the Behaviour Analyzer or the user, the SCWS establishes and maintains the connection with the RAS.
4. The SCWS act as a communication bridge between the terminal and the remote application, once the connection is being established.

3.4 Behaviour Analyzer

As the user enters in the vicinity of a service terminal, the SE establishes a connection with the corresponding remote application. The establishment of the connection adds up to the time that a user would have to wait before (s)he can access the service(s). Therefore, a possible solution is to anticipate the user's behaviour. For this purpose, an Artificial Intelligent Agent is included in the model, referred to as a Behaviour Analyzer. The Behaviour Analyzer can base its decision on the availability of terminals in the proximity environment, the direction of movement and the behaviour of the user. If the probability is high for a particular service, the Behaviour Analyzer will request the SCWS to establish a connection with the relevant RAS.

3.5 Event Triggering Software

The Event Triggering Software (ETS) checks the GPS measurements and matches with its own or off-site (i.e. mobile operator's) database for service terminals along with supported applications. The ETS maintains a set of services that lists the unique services available in a user's proximity. When the ETS detects any changes in the location of the user, it scans for unique services provided by new terminals in the vicinity. If it finds a unique service, it will trigger an alert to the Behaviour Analyzer. Thus ETS limits the alerts to the Behaviour Analyzer by only alerting for terminals with new services.

3.6 Service Provider

A service provider (e.g. banks, transport, health services) is a company that offers smart card based services. In the LBAA framework, an SP is a company that supports the framework and offers their remote application(s) to their customers. To support the LBAA functionality, SPs are required to implement the following servers.

Remote Application Enrolment Server. A Remote Application Enrolment Server (RAES) enables a SP to enrol their user's SE to access their remote application(s). The RAES should base its enrolment process on a mechanism that does not rely on the active involvement of the telecom operators. In addition, the SPs rely on the trust relationship with their customers but not with the mobile operators or the owner of the SE. To support the LBAA model the RAES should provide the following services;

– User's Account Management This provides the crucial service of managing the details of the user's registered SEs for accessing the remote application(s).

- User's Device Enrolment: : This service allows a user to enrol a new SE to access remote application or remove a SE.
- Remote Application Server Update: Once a binding is generated, the RAES will send the binding to the RAS along with the user's SE details. These bindings, referred to as security parameters are used to access the remote application(s).

Remote Application Server. The Remote Application Server (RAS) stores the personalised applications for each of the enrolled customers. A personalised application holds the customer specific data that may include customer's personal details along with unique cryptographic keys.

The RAS also allow the remote execution of application(s) and communicate the execution results to the requesting terminal via user's SE. To provide this service, the RAS first authenticates the user's SE to hold a valid binding and permission to access the remote application(s) without involving the users.

Application Service Access Server. The Application Service Access Server (ASAS) is an authentication server that authorises the user's requests to access the services provided by the SP. The current architecture of the ASAS as implemented in the banking, transport, etc, does not require to be modified. This enables an SP to implement the LBAA framework without any extensive modification to their existing infrastructure.

4 Location Based Application Availability Framework Processes

This section describes the processes involved in the proposed architecture of the LBAA framework

4.1 Remote Application Enrolment

The Remote Application Enrolment (or Scheme Enrolment) process registers a user's SE with the Remote Application Enrolment Server (RAES) and establishes a secure binding that the SE can use to access the remote application(s).

Before the Scheme Enrolment process can be initiated, the SP registers their customer with the RAES and provides them the registration credentials. The credentials include the RAES web address, user's account ID and password. The description of the credentials is in the SP's discretion. The operations performed in the Remote Application Enrolment process are listed as below:

1. A SCWS initiates the connection with a RAES. The connection is based on two-way SSL/TLS protocol [9]. After the connection is established, the user provides his/her credentials through the cell phone. The credentials are communicated to RAES and they should not be stored by the SCWS.

2. If credentials are verified, the RAES send the platform specification that contains cryptographic requirement for establishing and using the binding to access remote application(s). It also include the validity (lifetime) of the binding. The lifetime can be a number of executions, or time depending upon the discretion of the SP.
3. If SCWS satisfies the platform specification, it initiates the binding process by sending a binding request. The binding request contains a unique device number from the SE that is used to create a unique binding and manufacturer certificate. The certificates are cryptographically generated by the manufacturers and they assure that SE meets the platform specification.
4. The RAES will generate a unique remote application access identifier and a cryptographic binding key (K-Binding). The remote application access identifier is generated by taking the MAC [10] of the SE's unique number along with user credentials, remote application details, and a random number [10]. The identifier acts as a login name to access the RAS and the K-Binding acts as a password.
5. The RAES updates the RAS with the new binding. The RAS uses the binding to authenticate the SCWS when it requests the access of the remote application(s).

4.2 Application Availability Process

The LBAA depends upon the active recognition of terminals and associated services. The owner of the terminal registers their terminal location with either the mobile operator or a third party. When a user enters the vicinity of a terminal, the ETS recognizes it, and decides whether to invoke the Behaviour Analyzer or not.

However, if the user decides that only the GPS is not sufficient, the LBAA framework can use other mechanisms like Bluetooth, Wireless network, etc. The terminals can advertise their geographical location and services maintained through these mediums. This would be a preferable option for small/close company environment (e.g. University, Leisure Centre, etc).

The LBAA framework also allows a user to manual enter a terminal's GPS location information along with supported applications to the ETS. This allows small businesses or an individual to customize the LBAA to their requirements. Regardless of the mechanism through which a terminal advertises its location, the application availability process will be the same.

4.3 Remote Application Connection Establishment

The SCWS in LBAA framework establishes a connection to access a remote application on a RAS. The main requirement is the SCWS establishes a secure and low footprint communication channel. The protocol to establish a secure channel is illustrated in the figure 2.

The SCWS generates a cryptogram that is encrypted by the application's binding key (K-Binding). It contains the SCWS identifier, a random number, user's location information, and application identifier.

The RAS has the same K-Binding and it decrypts and verifies the message. If the message is valid, the RAS would issue a remote application access ticket. The ticket contains a new session key encrypted with the SCWS key along with the RAS Identifier, location information and lifetime of the ticket. The structure of the RAS Identifier is left on the discretion of the SP.

The SCWS retrieves the session key and sends an acknowledgement message.

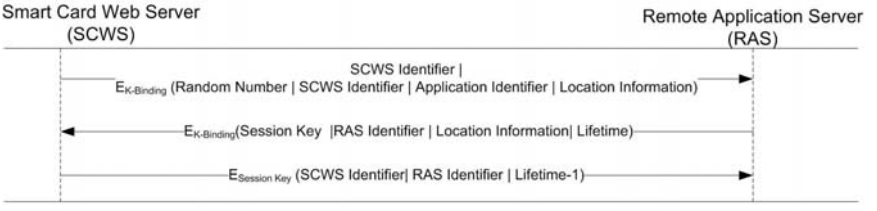

Fig. 2. The Protocol to establish the connection between the SCWS and RAS

The protocol is kept simple and less computational intense to reduce the overhead of establishing the connection. The location information in the protocol is added for the audit purposes. If a user claims that his/her device was not used to access services at a particular location, the SP could verify the remote access logs to confirm it. There is a possibility that in certain situation the services like the GPS and mobile Internet are not available (i.e. blank spots in-terms of coverage or in an underground system). In these cases, the LBAA model should have some alternate methods like requesting the service terminal to provide internet gateway.

4.4 Application Services Access

The application access is initiated when user presents his/her cell phone to request a terminal. The process presented in this section is generic and it does not dive into the details of different application (i.e. banking, transport, and access control). The process can be divided into two distinctive phases. In first phase, the remote application connects with the terminal and verifies the locality of the mobile phone and terminal to avoid replay attacks. Second phase will be application specific, conforming to their specific standards/specifications (i.e. EMV [11], ITSO [12]). In this section we will only discusses the first phase as illustrated by the figure 3.

A terminal sends a signed message by its signature key (SKT) to a SE. The message consists of a Challenge (i.e. Random Number) along with the terminal's GPS location and cryptographic certificate. The cryptographic certificate verifies the authenticity of the signature key. The signature generated on the message is verified by the RAS, and it can match the certificate with blacklisted terminals and revoked certificates from the terminal manufacturers.

A terminal sends signed messages by its signature key (SKT) to a SE (actually to SCWS in the SE). The message consists of a Challenge (i.e. Random Number

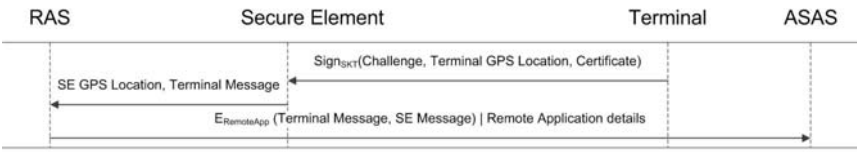

Fig. 3. Application Services Access Process Phase 1

[10]) along with the terminal's GPS location and cryptographic certificate. The cryptographic certificate verifies the authenticity of the signature key and the message verifies the location of the terminal. The certificate is generated by the manufacturer of the terminal and it also verifies the authenticity of the terminal itself. An adversary can emulate a terminal with desirable location information but it would be difficult to get a verifiable certificate to authenticate the genuine terminal. The signature generated on the message is verified by the RAS, and it can match the certificate with blacklisted terminals and revoked certificates from the terminal manufacturers.

The SCWS then generates a message and sends it to the RAS. The message consists of the SE's location and the message sent by the terminal. The RAS verifies the certificate for the terminal and also the signed message. It checks the location information sent by SE and terminal. If the variation is beyond the locality threshold of the SP, the process would be terminated. The locality threshold is the maximum variation in the GPS information of the SE and terminal, acceptable to a SP. The locality threshold is used to avoid the replay attacks over long distances. If the RAS is satisfied with the locality of the SE and Terminal, it encrypts the messages sent by SE and terminal with remote application LBAA key to Application Services Access Services (ASAS) along with remote application details. These details help ASAS to quickly locate the relevant decryption key for the remote application. The ASAS then initiates the application specific dialog with the remote application through the terminal and SE.

5 Future Research Directions

In this section, we will discuss the research topics that require further deliberations

- Remote Application Execution: It is challenging to remote application execution in a resource constraint environment like smart cards. The implementation to support it should be secure, robust, and efficient.
- Behaviour Analyzer: It is essential to the LBAA model for performance reasons; therefore, it should be a light weight implementation. The design should take into account that its purpose is to avoid unnecessary connections requested by the SCWS for remote applications.

- Vicinity Exploration Mechanisms: The main emphasis of this paper is on using the GPS to determine the available services in the vicinity of a user. However, other mechanisms that can provide the service availability in the vicinity in adequate timeframe should be explored.
- Distributed Execution Model: This topic builds on the work remote application execution. As remote application execution will take longer then local execution. One possible solution to this execution lag is to distribute the execution between the SE and RAS. The common component of the application will be executed on the SE. The common components are sections of the application that a SP implements as part of their compliance with corresponding standard/specification. The sensitive part (i.e. cryptographic processing, proprietary algorithms) will execute on the RAS. This solution may reduce the communication and execution load on the RAS.
- Practical Feasibility: We consider that it is necessary to measure the performance of the framework in the real world application. This analysis will assess whether such a model can be commercially feasible or not.

A secure, robust, reliable and flexible solution of these questions will enable the model to be regarded as a practically feasible model.

6 Conclusion

The convergence of different applications on to a single chip is encouraging; however, the centralised control of the chip will still decelerate the adoption of a true open platform based service access model. The proposal does not violates the security and privacy requirement of each of the SPs as the applications are in total control of their SPs and they only provide the credentials to access them for remote execution. The proposal has its limitations and we expect it to be slower on performance than applications executing locally on the SE. However, it provides an alternative way to the present application execution model and research into the topics list above will determine whether it is possible to shorten the performance gap with the locally executing application.

References

1. Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications, NFC Forum, White Paper (November 2006)
2. Co-Branded Multi-Application Contactless Cards for Transit and Financial Payment, Smart Card Alliance, Princeton Junction, NJ 08550. USA, White Paper TC-08001 (March 2008)
3. Pay-Buy-Mobile: Business Opportunity Analysis, GSM Association, White Paper 1.0 (November 2007)
4. Mobile NFC Services, GSM Association, White Paper 1.0 (2007)
5. Mobile NFC Technical Guidelines, GSM Association, White Paper 2.0 (November 2007)

6. Best Practice for Mobile Financial Services: Enrolment Business Model Analysis, Mobey Forum Mobile Financial Services, White Paper 1.0 (2008)
7. Smartcard-Web-Server, Smartcard Web Server Enabler Architecture, Smartcard Web Server Requirements, Open Mobile Alliance (OMA), Version 1.1 (2008)
8. Parkinson, B., Spiker, J.J.: Global Positioning System: Theory and Applications. AIAA 1 (January 1996)
9. Dierks, T., Rescorla, E. (eds.): The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346 (2006), http://tools.ietf.org/html/rfc4346
10. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC, Boca Raton (1996)
11. EMV 4.2: Book 1 - Application Independent ICC to Terminal Interface Requirements, Book 2 - Security and Key Management, Book 3 - Application Specification, Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements, EMVCo 4.2 (May 2008)
12. ITSO Std., http://www.itso.org.uk/
13. Küpper, A.: Location-Based Services: Fundamentals and Operation. Wiley, Chichester (2005)
14. Madlmayr, G., Langer, J., Scharinger, J.: Managing an NFC Ecosystem. In: ICMB 2008: Proceedings of the 2008 7th International Conference on Mobile Business, Washington, DC, USA, pp. 95–101. IEEE Computer Society, Los Alamitos (2008)
15. Dynamic Management of Multi-Application Secure Elements, StoLPaN, White Paper 1.0 (2008)