Information Sciences 321 (2015) 150–161

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A novel consumer-centric card management architecture and potential security issues

Raja Naeem Akram [a,*], Konstantinos Markantonakis [a], Damien Sauveron [b]

[a] Information Security Group, Smart Card Centre, Royal Holloway, University of London, Egham, United Kingdom
[b] XLIM (UMR CNRS 7252/Université de Limoges) Département Mathématiques Informatique, Limoges, France

ARTICLE INFO

Article history:
Received 11 May 2014
Received in revised form 19 December 2014
Accepted 28 December 2014
Available online 12 January 2015

Keywords:
Smart card
GlobalPlatform
Java Card
Multos
User centric smart cards
Card management architecture

ABSTRACT

Multi-application smart card technology has gained momentum due to the Near Field Communication (NFC) and smart phone revolution. Enabling multiple applications from different application providers on a single smart card is not a new concept. Multi-application smart cards have been around since the late 1990s; however, uptake was severely limited. NFC has recently reinvigorated the multi-application initiative and this time around a number of innovative deployment models are proposed. Such models include Trusted Service Manager (TSM), User Centric Smart Card Ownership Model (UCOM) and GlobalPlatform Consumer-Centric Model (GP-CCM). In this paper, we discuss two of the most widely accepted and deployed smart card management architectures in the smart card industry: GlobalPlatform and Multos. We explain how these architectures do not fully comply with the UCOM and GP-CCM. We then describe our novel flexible consumer-centric card management architecture designed specifically for the UCOM and GP-CCM frameworks, along with ways of integrating the TSM model into the proposed card management architecture. Finally, we discuss four new security issues inherent to any architecture in this context along with the countermeasures for our proposed architecture.

1. Introduction

Existing multi-application smart card platforms (e.g. Java [39], Multos [35]) support the installation of applications remotely (post-issuance). Standardisation efforts that enable an application to be managed remotely – for example, GlobalPlatform [21] have been effective in the Issuer Centric Smart Card Ownership Model (ICOM) field [4]. The advent of NFC technology and the growing convergence of different services on mobile phones have prompted GlobalPlatform and the GSMA[1] to propose a new application management architecture (e.g. TSM) [24,26,20,30]. Similarly, Multos has a strong card and application management architecture that is heavily issuer-centric and it can be argued that it can easily be adapted to the Trusted Service Manager (TSM) architecture. The GlobalPlatform and Multos cards along with their associated application management architectures provide two contrasting views of the smart card industry. We limit our analysis of traditional card management architectures to these two examples. The Java Card does not have any associated management architecture and in most commercial deployments it is coupled with the GlobalPlatform management architecture. In the ICOM, the issued smart

* Corresponding author.
E-mail address: r.n.akram@rhul.ac.uk (R.N. Akram).

[1] The GSM Association (GSMA) is an association that represents the interests of mobile operators worldwide, along with developing and prompting the Global System for Mobile Communication (GSM) specification.

http://dx.doi.org/10.1016/j.ins.2014.12.049
0020-0255/© 2015 Elsevier Inc. All rights reserved.

cards are under the complete control of the card issuer. By contrast, in the User Centric Smart Card Ownership Model (UCOM) [4] the consumers (end-users) get ''freedom of choice'' which allows them to install or delete any application as they desire from their smart cards. The UCOM supported smart cards can hold multiple heterogeneous applications from various organisations. The only limitation on the number of applications a UCOM supported smart can have is based on its store capacity. The GlobalPlatform Consumer-Centric Model (GP-CCM) [27] provides consumers the ability to choose the applications they want. Although the finer details for the GP-CCM are still to be articulated, we consider that the overarching aim of both UCOM and GP-CCM are similar. In this paper, the expression Consumer-Centric Model is used for conciseness to indicate both UCOM and GP-CCM. As the card management architecture in the Consumer-Centric Model has to consider the contrasting needs of both the administrative authority (i.e. TSM) [7] and the consumers (end-users), it has to remain flexible. It must determine the ownership requirements of each of these entities and then articulate how a Consumer-Centric Model framework will manage them. In addition, the management architecture proposed in this paper deals with application issuance (lease), application domain provision on the smart card, installation, deletion, and application/domain management. Furthermore, this paper an architecture for the proposed application download/installation protocols [8,7,9]. As the Consumer-Centric card management architecture brings forward conflicting views smart card management architectures, it also highlights new security issues. These issues relate to the card and its rightful owner. They include simulator problems, user ownership issues, parasite application problems, and platform insider attacker problems.

1.1. Contributions

The salient contributions of this paper are to:

1. Describe and compare traditional application management architectures (Multos and GlobalPlatform) and justify why they might not be considered as adequate for the Consumer-Centric Model.
2. Specify a flexible card management architecture for the Consumer-Centric Model.
3. Provide a flexible card management architecture for the integrated TSM and Consumer-Centric Models.
4. Discuss the security issues and related countermeasures for the proposed architecture.

1.2. Structure of the paper

The GlobalPlatform card management architecture is discussed in Section 2, followed by the Multos card management architecture in Section 3. The proposed architecture of the Consumer-Centric card management is described in Section 4, along with different types of relationships between a user and a Service Provider[2] (SP). In Section 5, we discuss the issues that are inherent to any architecture in this context along with providing related countermeasures for our proposed architecture.

2. GlobalPlatform card management architecture

In this section we discuss the GlobalPlatform card management architecture along with the mechanics by which it supports TSM-based card management.

2.1. Architecture overview

The GlobalPlatform card security requirement specification [21] specifies eight entities (excluding the smart card and the cardholder) that perform various tasks in the overall card management architecture. The overall architecture is depicted in Fig. 1, which is a simplistic representation of the architecture described in [21]. The shaded entities in Fig. 1 have different titles and roles, but together they form the card issuer. The term ''card issuer'' as defined by GlobalPlatform in [21] is restrictive, so that issuers only have the responsibility to acquire the smart cards, set a security policy, and issue cards to individual cardholders. The card administrator is responsible for managing the cards once they are issued to individual customers. If application provider would like to issue its applications, these must first be verified by the verification authority. The verification authority performs an off-card application code verification to ascertain whether the given code conforms to the security policy set by the card issuer. Once the verification is performed, the application provider requests the controlling authority to give permission to load the application. The controlling authority checks the verification authority's verification and issues the permission to load the application. If the application is going to be loaded at the pre-issuance stage then the domain keys and data will be sent to the card issuer [22] through the card enabler. Otherwise, the domain keys and data will be sent to the application loader. In Fig. 1, we opt for the pre-issuance model. Finally, the application provider will send its application, keys and application personalisation data to the application loader, which will load them onto the smart cards of individual customers. The keys in aforementioned message, used to secure the application download to a smart card, are security domain keys. In Fig. 1 the security domain keys that are used by the application provider to manage its domain

[2] A Service Provider (SP) is an entity which is also referred as Application Provider (AP) that develops smart card applications in order to facilitate its customers to securely access their services. The terms SP and AP are used interchangeably hereafter.