DESfire Emulation Using Java Card

Jorge Prado Casanovas\(^1\) and Gauthier Van Damme\(^2\)

\(^1\) Universidad de Vigo, ESTIT, Campus Lagoas-Marcosende, 36.310, Vigo, Galicia, Spain
Jorge.Prado.Casanovas@gmail.com,
Gauthier.VanDamme@esat.kuleuven.be

1 Introduction

This paper presents a Java Card applet offering the same functionality as a widely used contactless storage card. The goal is to provide a solution for secure and widely deployable data storage for smart phones. The applet provides an independent storage space for different applications with their own keys and configuration and is fully compatible with the MIFARE DESfire Card EV1 technology. It can be installed in every Java Card 2.2.1 compatible Smart Card. Integration with Google Android phones is possible using a secure micro-SD card or other secure platforms that feature a JavaCard chip and a NFC antenna. The DESfire emulator can be accessed both externally through NFC, or internally through the smart phone OS.

In the last few years, the number of different electronic applications using secure elements have grown markedly.\(^1\) It is easy to take a look at things that are used day by day and find that secure storage is needed for a big part of them. Credit cards, access control, public transport, supermarket vouchers... Curiously most of them are found in our wallets. On the other hand, mobile phones have been growing recently in the number of applications where they are used, increasing their value in our pockets. It has been found interesting to move all this stuff to our smart phone with the aim of reducing the number of things carried by the clients. Thus, a secure storage is needed in the smart phone to provide such a service.

Up to now, each card within our wallet had its chip where the secure data was stored. Our credit for public phones, our vouchers for our

\(^1\) Secure elements are modules offering a space for the secure storage of data. This data will be protected against hardware and software attacks and are frequently used for store critical data as cryptographic keys or credit values.
favourite video club or even our identity were kept within each application's cards. Also, there were other ways to store data like barcodes, links to an internet account or simply a piece of cardboard where seals were stamped. Those systems actually use Smart Cards or could be using them. The data in there is secured with keys such that the access to it is restricted to authorized. Depending on the card's configuration, the data in it could not be manipulated even by it’s owner. So it would be possible to use the Smart Card for storing the credit of the user of a particular application such that only the entity that manages the system (for instance an online sales company) could decrease or increase the balance. Smart Cards are also a very useful tool for adding secure elements to devices or systems that don’t have such a property. They are already used for electronic identity systems, payment systems, club membership or storage of vouchers to name just a few.

As an example of their use, imagine the next scene: A simple bus card where the credit of the client is stored. Every time the client takes a bus, he chooses his bus card among the other cards within his wallet, and puts the card in the reader. The reader decreases the credit stored in the card with the price of the travel and the client takes out his card and the payment is done. Obviously if the client can increase his credit by himself the system will collapse. It will work only when the access to this credit (i.e. the data within the card) is restricted to those who own the secret key which allows to modify it. In this example the bus company would be the party that possess this key.

The point is that as the number of systems requiring secure storage are growing, the number of things that have to be carried in our wallet is growing too. The idea of putting all of them together in a mobile phone appears to be the right solution to this, as the number of mobile phone is huge and still growing. Moreover, it seems to be nice to have everything in a device that we carry with us all the time.

Of course, the need of a multi-application card appears where independency between each application within the card is needed meaning each application needs to be able to have its own keys and configuration. Also, they need to be protected against illegal access even from the owner of another application also installed in the card. Actually, there are already Smart Cards providing such a service.

Among the huge range of different Smart Cards from different manufacturers, the MIFARE chips (trademark owned by NXP Semiconductors) are widely used in contactless and proximity cards all over the world and were therefore considered. One of their variants is DESfire Card EV1.
This variant is sold already programmed with a general purpose software for the management and control of the storage system. These cards are working already in several systems (with more than 3.5 billion cards sold). Its operating system is similar to the Java Card’s, it is a multi-application operating system that works with cryptographic algorithms as DES and AES, and is compatible with the ISO/IEC 7816-4 standard.\(^2\)

It has been found interesting to create an applet able to run in every Java Card programmable Smart Cards emulating the MIFARE DESfire Operating System. Compatibility with the systems where DESfire cards have been working will be offered. Also, it offers enough functionalities for most of the applications where it could be used (loyalty programs, closed loop payment, access management...). We thus developed a DESfire emulator for Java Cards that is fully compatible with existing DESfire systems and that bridges the gap for future secure and smart phone based multi-application systems.

2  Integration with Google Android Phones

The original goal of this applet was to be integrated with Google Android mobile phones. The applet provides secure elements and thus the mobile phone generic and secure storage for applications that need it. The applet is installed inside a secure micro-SD card which can be inserted in the mobile. Then, using a specific library provided by Giesecke & Devrient (which also provided the secure micro-SD card that has been used), it is possible to send and receive APDUs to and from the Smart Card, and thus Google Android Applications that use the secure Java Card applet can be built.\(^3\)

The Google Android application can then communicate with an online server asking, for instance, to increase the balance of a specific entity. The balance is stored in a file of the Java Card applet. The APDUs with the commands will be sent by the server and the Google Android application just forward them to the Java Card applet. The keys to manipulate that file are only known by the server and the Google Android application can never get them, thus providing for a secure application a key management system.

\(^2\) The ISO/IEC 7816-4 standard is an international standard related to electronic identification cards, especially smart cards

\(^3\) An APDU is the communication unit used between a smart card reader and a smart card
3 Features

The DESfire Emulator applet offers support for multiple applications in just one Java Card. As for real DESfire Cards, up to 28 applications can be created although theoretically the emulator is not restricted to this number. The management of each application is self-configured so independence between them is provided. Up to 32 different files can be created within the application. Each file can be chosen among the 3 types supported by the operating system. Data Files offer a memory space to store plain unformatted data; Record Files are used for identically structured data and the Value Files for storing a single 32 bit signed integer where limits for this value can be set.

Furthermore, each application can manage 14 keys that can be selected by the user. The applet supports the single DES, 3DES, 3KDES and AES and 8 byte CMAC cryptographic algorithms. Once created, any application’s key can be used to restrict the access to an specific file. Each one of the files has its access permission that allows reading, writing or both after authentication with the key. One key can be used for any of the files.
within the application and for any of its accesses. It’s possible, then, to
give to one entity using the applet (for example, an access control ma-
chine managing the door to a laboratory) one of the keys such that the
entity can read one of the files, write to another (without knowledge of
the previous value) and increase the value of a third one.

An integrated backup mechanism is supported by the operating sys-
tem. Changes are stored in a temporary file until the changes are commit-
ed (a command for that purpose has been implemented). This mechanism is
integrated in all the types of files.

For the data manipulation the operating system offers basic function-
alities for reading from and writing to data files, to add records and to
increase or decrease the value of a Value File.

Moreover, according to ISO/IEC 7816-4 standard, a set of inter-industry
commands is also provided in the applet. Therefore, the scope of the ap-
plet is extended to every system where the standard was integrated.

4 Advantages

Regarding the MIFARE DESfire card, this applet, because it can be in-
stalled in every Java Card programmable Smart Card, extends the carac-
teristics to the ones of the Smart Card where it is installed. Then, some
limitations can be overcome such as the maximum user memory (8 KBytes
is the biggest in MIFARE DESfire card set) or the length of the messages
exchanged (big data transactions are faster since less messages has to be
send to the card). The applet doesn’t have to limit the number of appli-
cation to 28 or the number of files to 32 so it allows more applications to
be running at the same time and also more complex applications. Also,
it’s completely open to the development of new features.

Besides, the integration on devices as diverse as Smart Phones is pos-
sible. Moreover, the communication of these devices with the Smart Cards
has been already implemented so it is possible to have all these perfor-
mane even where MIFARE DESfire Cards where not compatible. Thus,
this DESfire emulator briges the gap between the existing technology
and the future mobile payment technology because it provides what was
needed, a secure and widely deployable data storage for mobile phones.