

# FlyBuy Duo

## A new SIM-Centric solution for NFC Mobile Payment



Award-Winning Product For  
The Best Mobile Application

**SESAMES**  
2 0 0 7

Lorenzo Stranges - [l.stranges@oberthurcs.com](mailto:l.stranges@oberthurcs.com)  
Aymeric Harmand - [a.harmand@oberthurcs.com](mailto:a.harmand@oberthurcs.com)  
Jean-Marc Meslin - [jm.meslin@oberthurcs.com](mailto:jm.meslin@oberthurcs.com)



## Table of Contents

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>2.</b>	<b>A SIM CENTRIC SOLUTION.....</b>	<b>2</b>
	2.1 SIM-Centric Vs. Non SIM-Centric Architectures.....	2
	2.2 SIM Centric Key Advantages.....	2
	2.3 FlyBuy.....	3
<b>3.</b>	<b>FLYBUY DUO.....</b>	<b>4</b>
	3.1 Why this new product?.....	4
	3.2 FlyBuy Duo architecture.....	4
	3.3 Mobile banking-specific challenges.....	5
	3.3.1 Security.....	5
	3.3.2 Time to market.....	6
	3.3.3 OTA management.....	6
	3.3.4 Costs.....	6
<b>4.</b>	<b>LIFE CYCLE CHALLENGES AND FLYBUY DUO ANSWERS.....</b>	<b>7</b>
	4.1 Manufacturing.....	7
	4.2 Personalization.....	7
	4.3 Activation of the banking application.....	7
	4.4 Use phase.....	8
	4.4.1 Counter reset.....	9
	4.4.2 Battery off mode.....	9
	4.4.3 Interactivity.....	9
	4.5 End of life.....	10
<b>5.</b>	<b>CONCLUSION.....</b>	<b>11</b>

## 1. Introduction

NFC mobile payment is one of the most talked about subjects in the field of payment innovations and mobile related services today. With the launch of more than 10 major pilots and volume deployments in different regions around the world, the demand for NFC technology is increasing at an explosive rate. Before mobile payment can reach 'critical mass' – the point where large-scale NFC deployments can begin to occur, NFC still needs to overcome both major technical challenges and gain industry-wide agreement on a range of issues.



There is still no clear industry consensus on the preferred architecture that NFC technology should adopt. Discussions are still ongoing concerning the use of a SIM-centric approach, non-SIM-Centric or a Multi Secured Element approach.

As discussed in the next chapter, SIM-Centric solutions are proving to better suit NFC requirements. However, at least one problem remains unsolved: how to meet both the banks' security requirements as well as mobile operators' need for flexibility and short Time To Market?

The same question was formulated in a different way in the last Smart Card Alliance Contactless Payments Council white paper (September 2007):

*"The SIM-Centric architecture [...] provides mobility for the consumer financial credentials, which is a strong consumer advantage. The certification cycles of the SIM card and the banking secure elements are very different and may become a hurdle to the adoption of this architecture. The issue will be related to the cost of banking certification and the compromise to SIM flexibility that the carrier will have to manage. Some large trials or soft launches using this architecture are being run in Europe or about to be launched in Asia".*

With a leading position in the US contactless payment market and having participated in major NFC pilots and launches in both Asia and in Europe, Oberthur Technologies has a strong experience in the contactless payment arena. The authors of this white paper propose to share Oberthur Technologies' vision on the mobile payment ecosystem, and to provide answers on the future of NFC and mobile payment technology.

This white paper also introduces Oberthur Technologies' FlyBuy Duo product, which provides banks with a dedicated and secure payment component: a certifiable chip to host NFC payment applications that is positioned beside the traditional (U)SIM chip. The FlyBuy Duo solution allows secured and convenient deployment of NFC payment projects and provides a viable compromise that could help leverage the future mass development of mobile payment.

The SIM card remains the Secured Element for mobile payment, but, instead of using the SIM component to host the payment application, a dedicated component, also located in the SIM plug-in, is used to run the contactless payment application. This provides huge flexibility to the whole system. The details and the advantages of this solution are described in this paper.

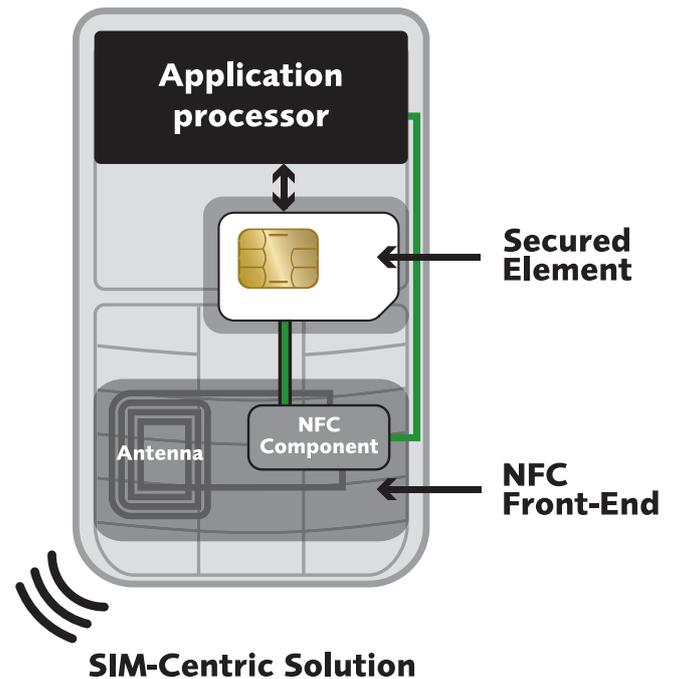
## 2. A SIM Centric Solution

### 2.1 SIM-Centric vs. Non SIM-Centric Architectures

A NFC phone must consist of the two following elements:

- A NFC front-end—consisting of a NFC Component and an antenna – which manages the communications between the handset and external devices or systems that follow the ISO 14443 standard.
- A Secured Element (SE) in which host applications (such as the payment application) are stored.

The antenna and the NFC chip are integrated within the phone. There are basically two different technical architectures which determine the location of the contactless applications: they can be either stored in the SIM that acts as the Secured Element of the NFC front-end (SIM-Centric solution) or they can be stored in a second Secured Element located elsewhere in the phone (non SIM-Centric solution).



### 2.2 SIM Centric Key Advantages

For many reasons (detailed below), the SIM-Centric solution is on the verge of becoming the NFC standard. The GSM Association, in a recent white paper on NFC stated that the SIM should be considered the Secured Element of a NFC System.

This solution has an important advantage: it allows a win-win agreement between MNOs and banks who both want to add value to their commercial offer with new, attractive and innovative services to increase their ARPU. Because the SIM – the only part in a mobile handset that is controlled by MNOs – is used as SE, mobile operators that subsidize phones will remain at the focal point of NFC. The SIM-Centric architecture is the only solution that meets banks' requirements for security, portability and multi-applicative features.

Technically, there are many reasons that push for the adoption of the SIM as a SE of the contactless solution.

Quoting from last GSMA NFC white paper:

*"Mobile NFC applications need to be performed in a secure environment (SE). The UICC provides both logical security (i.e. command encryption) and physical security (i.e. tamper proof and copy protection). Furthermore, the UICC has been identified by MNOs as the recommended SE for NFC because of the following unique advantages that it offers to the market place:*

- *Universal: The UICC has the widest available deployment of any SE, with more than 2 billion users worldwide – hence it is cost effective to use the existing UICC as an SE rather than to develop, implement and deploy a new alternative.*
- *Portable: The UICC is portable – hence Customers can easily transfer their applications and rights from one NFC enabled mobile device to another.*
- *Dynamic Remote Management: MNOs already operate secure remote UICC management systems and processes (Over the Air). These can easily be leveraged to manage the whole life cycle of mobile NFC services. Furthermore, services loaded onto the UICC can be immediately blocked, activated or suspended.*
- *Standardised: UICC Security is based on global, well-established standards (such as ETSI-SCP, 3GPP, Global Platform) covering application storage, OTA communication, privacy and the entire life cycle management.*
- *Long Lifecycle: The UICC has a longer lifecycle than a mobile device - hence it is more suitable to house the NFC applications on it rather than on the mobile device. This permits the Customer to easily transfer and use their mobile NFC services over time.*
- *Business synergies: UICC manufacturers that already supply contactless cards to service providers will benefit from their expertise and their operational excellence.*
- *Customer care service: In addition to providing high quality customer care for mobile telephony and data services, the MNO can also provide high quality mobile NFC customer care services to the customer – for instance the MNO can be the single point of contact to a customer for managing their mobile NFC services if their mobile device is lost, stolen or damaged.*
- *Consistent approach: By deploying mobile NFC applications in the UICC, the MNO can leverage existing capabilities to provide OTA management of services to customers. Battery independent: The UICC mobile solution also allows NFC services to work even when the battery is off".*

## 2.3 FlyBuy

Since 2006, Oberthur Technologies has supported the SIM-Centric industry vision and has developed its SIM-Centric product: FlyBuy.

We are currently testing this solution in different regions worldwide both in the payment and in the transport domains. In parallel to these studies, we are working on developing a more secured evolution that will meet current standard demanded for contactless payment demanded by banks.

### 3. FlyBuy Duo

Today, the whole industry agrees that a SIM-Centric architecture is the best solution to meet the various challenges put forward by NFC. As the Smart Card Alliance stated in their last white paper (Proximity Mobile Payment, September 2007), there is still one critical factor that has yet to be addressed: Certification cycles for a SIM card are very different from those used in a payment Secured Element. The long certification processes enforced by banks internationally have to be balanced with mobile operators' need for flexibility.

Beside the development of its FlyBuy SIM-Centric architecture, Oberthur Technologies has developed another SIM-centric solution that complies with the SWP standard: FlyBuy Duo. Designed to meet both an MNO's requirement for short time to market with a bank's security requirements, FlyBuy Duo's innovative architecture can offer a solution to different certification cycles.

#### 3.1 Why this new product?

Operators and banks have expressed their strong interest in NFC mobile payment.

In this domain, we can draw a parallel with contactless payment. Today's contactless cards are certified to banking standards (for example: EAL4+). This certification process is quite long (around 12 months), relatively expensive and inflexible, as the certification must be resat after every change in the OS. The major question mark remains which certification levels will be required by banks to ensure the security of NFC mobile payment.

Most probably, mobile payment will inherit contactless payment constraints. In this case, we can expect that bank certification processes will require high investments and that SIM time to market will increase. This point is quite crucial for Mobile Operators as a one-year certification process is not compatible with their market: it would imply that MNOs must wait up to one year to update SIMs and to launch new applications which does not fit with their market constraints.

The SIM industry has a challenge: to answer both banks' certification constraints and MNOs' quick time to market. That's why Oberthur Technologies has developed FlyBuy Duo, a solution that meets mobile operators and banks lifecycle requirements.

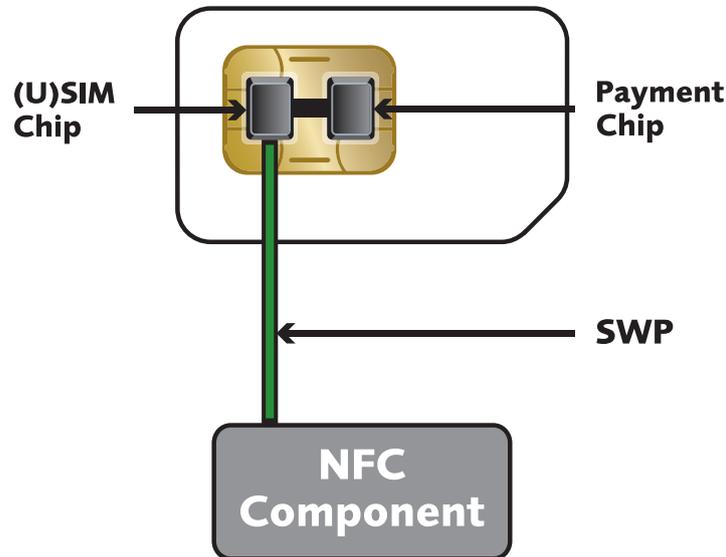
#### 3.2 FlyBuy Duo architecture

The FlyBuy Duo is a SIM-centric solution.

The Secured Element is composed of two distinct chips embedded in the SIM plug-in:

- A (U)SIM chip hosts both non-NFC and NFC applications, except payment: these can include communications, transport, access control, e-ticketing or fidelity applications.
- A payment chip, certified to a banking standard, is dedicated to NFC payment applications

As shown on the figure below, the (U)SIM chip is linked to both the NFC front-end via an SWP connection and to the payment chip. The (U)SIM chip acts as a router between the payment chip and the NFC front-end. The payment chip has no direct link with the NFC front-end.



This solution's innovative architecture enables compatibility with all SWP-compliant handsets. It means that in SWP phones currently on the market, you just have to replace your SIM card with FlyBuy Duo to be able to use NFC services.

### 3.3 Mobile banking-specific challenges

FlyBuy Duo's SIM-centric solution provides the same major advantages over a non SIM-Centric solution: interoperability, portability and standard dynamic remote management capability.

The unique architecture of FlyBuy Duo also allows it to answer mobile payment specific constraints.

#### 3.3.1 Security

Security requirements in the banking world are much more stringent than in the telecommunications domain. The Duo architecture perfectly meets the diverse requirements of these two stakeholder groups: its two chips allow it to have two different security levels in one SIM plug-in.

The (U)SIM element can have the necessary security level to host non-payment applications. There is no need to pass the banks' long and expensive testing processes.

The payment component embedded in the SIM is or can be a chip used in the banking world and therefore 'automatically' complies with financial institutions security requirements. This chip is fully dedicated to payment and can easily be certified, as no other NFC applications will be hosted during the card's lifecycle.

As we have already stated, 'classic' SIM-Centric products can also reach the required security level, but this would require considerable hardware and software developments, and this work will certainly not be accomplished for all of the diverse components used in today's telecom world.

### 3.3.2 Time to market

On this point too, the banking and telecommunications worlds diverge. For banks, time to market is a minimum of 18 months, while for MNOs, new SIM cards can be on the market just one month after their order. Mobile operators simply cannot afford to wait nearly two years before launching a new service.

With the dual component approach, the certification of the SIM component to the banking standard will not be required. The payment component can be associated to any SIM controller allowing the operators to target any market segment with the dedicated product.

Keeping the two worlds (GSM and banking) separated gives greater flexibility to both parties. Above all, mobile operators will be able to modify the OS in the SIM and to launch new services (by Over-The-Air downloading of new applets) without going through another long and tedious certification process.

### 3.3.3 OTA management

Over-The-Air management (OTA) enables SIM content to be managed remotely. It is a very standard practice for Mobile Operators. One of the key factors of NFC Mobile Payment is to succeed in preserving their capability of managing applications OTA. For banks, who do not use OTA management today, it could provide new opportunities.

The challenge for the industry is to know if it will still be possible to manage applications OTA when the chip is certified. That's why Oberthur Technologies has designed a two-chip product.

In the (U)SIM chip, every action (downloading, personalizing, locking and unlocking) is possible and will not break the certification of the payment chip.

In the payment component, OTA management will be done through the (U)SIM chip: personalizing as well as locking and unlocking applications in the payment chip is possible while retaining the chip's certification. Downloading new applications in the payment chip however, while technically possible, would probably imply new certification processes.

### 3.3.4 Costs

The additional cost to add a payment-dedicated component is covered by the fact that certification should not impact on the SIM component. When multiplying the certification costs by the number of different mobile products available in the market today, the calculation is done.

For the secure component, it will be imperative to use already existing – and certified – components. This will considerably lower the cost of the whole solution.

## 4. Life cycle challenges and FlyBuy Duo answers

The life cycle of FlyBuy Duo can be divided in the following phases:

- Manufacturing,
- Personalization,
- Activation on the banking,
- Use phase,
- End of life.

### 4.1 Manufacturing

When manufacturing FlyBuy Duo, the choice can be made on demand between a set of components dedicated to communication. This will allow mobile operators to tailor the product to the needs of their subscriber in terms of functions and memory capacity.

Adding a second component (the payment dedicated component) in the SIM plug-in is now a mature technology for Oberthur Technologies. The industrial process was developed and tested with GIGAntIC SIM cards (a SIM coupling a SIM component and – up to 1 gigabyte of flash memory in the same plug-in).

### 4.2 Personalization

The personalization phase is strongly linked to the distribution phase. It is likely that cards enabling NFC payment will be distributed using the model used today by mobile operators.

In the mobile world, SIM cards are personalized anonymously. It is only when the subscriber signs a contract (in a mobile operator's agency for example) that the card is associated to this particular individual in the databases of the mobile operator. The banking world uses a totally inversed model, where every single card is personalized for a dedicated cardholder in the factory prior to issuing.

As the recipient of a particular card and its bank are not known during this personalization phase, it is impossible to enter any bank cardholder data. Personalization must be similar to the one done for 'classic' SIM cards, except that applications in the payment component could be pre-loaded (but not personalized).

The personalization of the payment chip will only occur during the activation of the banking applications.

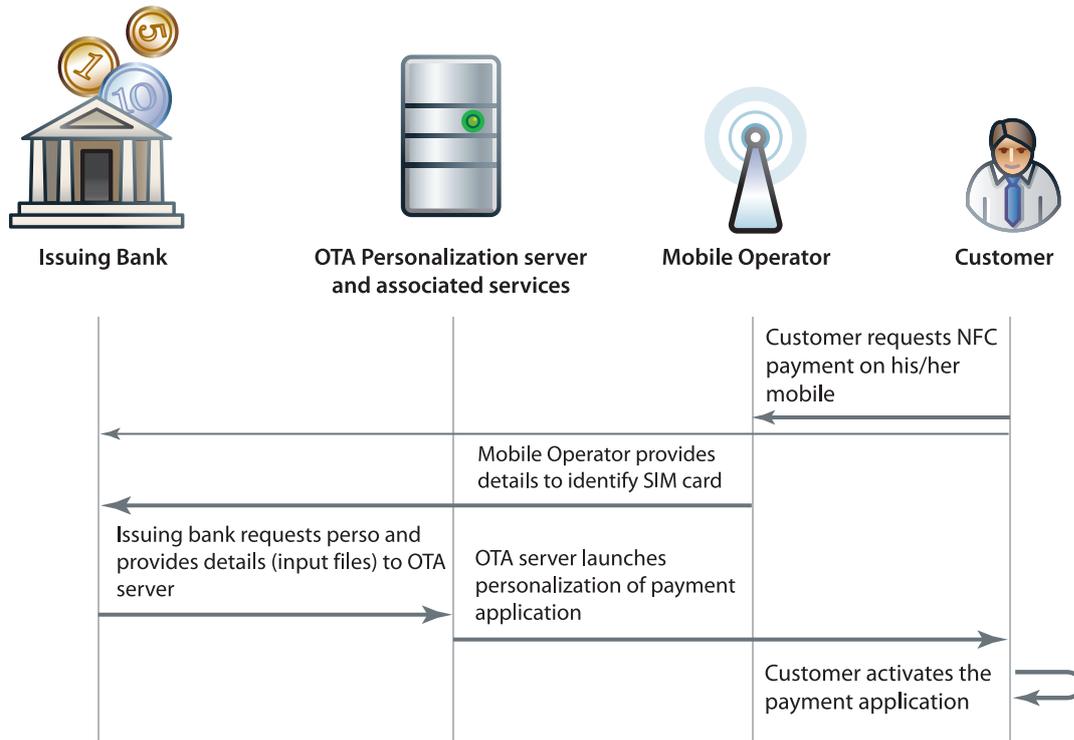
### 4.3 Activation of the banking application

The activation of the payment application can be done using the following data:

- References of the SIM card (MSISDN or mobile phone number assigned to a subscriber, ICCID for Integrated Circuit Card ID),
- Cardholder data (name, etc),
- Bank specific data for personalization (dates, risk management data, etc).

Only after the subscriber has made the request for a payment application in his SIM card that all the data can be known by the bank - which will then provide the associated service. As the card is in the hand of this particular customer (and no longer in a personalization center) the Over The Air channel remains the only way to personalize the payment applications.

The following figure provides a high level overview of the OTA personalization process.



*Overview of NFC payment application's personalization*

Using this sequence, the SIM component will detect the personalization commands as payment commands and will route the personalization scripts to the payment component. For the OTA server, the fact that there is one component or two (with the first one re-routing the information to the second component) in the SIM does not change anything.

## 4.4 Use phase

During this phase, mobile operators and banks have to manage their applications Over-The-Air through the OTA server. For mobile operators, this management will be exactly the same as the one they use today on 'classic' SIM cards.

The following sections highlight some key elements of NFC mobile payment usage.

#### 4.4.1 Counter reset

When activated, the payment application will allow payments following the contactless payment rules which are actually defined for contactless cards. Following those rules, the cardholder must authenticate using a PIN validation, when required by the risk management procedure defined by the bank. As authentication requires a card insertion into a payment terminal, this is something which obviously cannot be envisaged for NFC mobile payment. Today two options are foreseen:

1. The authentication mechanism could be done by connecting the cardholder to the issuing bank server using an OTA infrastructure.
2. The authentication could be done at the point of sale using the payment terminal.

For FlyBuy Duo, both solutions can be implemented.

#### 4.4.2 Battery off mode

Battery off mode allows a person to use their telephone's NFC contactless applications even when the battery is off.

When the battery is off, it is not possible to authenticate the user. Therefore, payments should not be allowed when the phone is switched off. Nevertheless, other contactless applications need to run even when the battery is off: for example, a person using their phone for transport should still be able to catch their train, bus or metro, even when they have run out of battery.

FlyBuy Duo provides a total solution to these problems. With two chips, one dedicated to payment and another that hosts all other applications, it is possible to 'switch off' the payment chip when the phone is off while leaving the other one active for contactless applications (such as transport, fidelity or loyalty).

#### 4.4.3 Interactivity

One of the real advantages of mobile payment over 'classic' contactless payment is the interactivity of the handset and its user interface.

For FlyBuy Duo, an application hosted by the (U)SIM element provides the user interface with needed data for both payment and non-payment applications.

Banks can display messages on the phone's screen using all its display possibilities: text message, logo (of the bank) or an animated image. The user will also be able to use their phone to consult their most recent bank statement via the data stored in the SIM card.

## 4.5 End of life

The end of life of the FlyBuy Duo can occur when needed, for example:

- At the expiry date of the payment application
- If the handset is either lost or stolen
- If the issuer or the customer wants to stop the contract

Using Over The Air services, the issuing bank will have the ability to disable the payment function or to access all script processing capabilities provided by EMV.

## 5. Conclusion

SIM-Centric solutions provide distinct business and technical advantages, and offer the only possible architectures that have a chance to succeed in the NFC ecosystem. However, before being able to be certified to host payment applications, the actual 'standard' SIM must evolve in order to meet the requirements from the banking side. These security improvements are currently being developed and could open the way to NFC's future mass deployment.

Beside the SIM-Centric solution, the FlyBuy Duo provides a new way forward. This new SIM consists of two chips: the payment one is accessible by the outside world only through the SIM component (i.e. the payment chip is SIM-enabled, the Secured Element is controlled by the SIM), to meet the requirements of both mobile operators and banks:

- From the MNOs point of view, the new SIM has the same contact allocations as standard SIMs (C6 for SWP, C4 and C8 for USB...) and acts exactly the same throughout its lifecycle. Even the short time to market constraint of MNOs is met. MNO customers just have to replace their former SIM with a FlyBuy Duo SIM in their NFC handset.
- For banks' requirements, the payment component will be certified in-line with today's contactless payment standard. Banks will be able to instantiate, personalize, lock and unlock banking applications in the payment chip Over-The-Air while keeping within the guidelines of the chip's certification.

As a conclusion, FlyBuy Duo is a completely standard SIM from the outside and from the interface point of view. From the inside, its innovative new architecture will allow enhanced security and flexibility. FlyBuy Duo definitely complies with the needs of both banks and operators and its hybrid architecture could be the meeting point where they will finally make an agreement.

The NFC mobile payment market is still at an early stage of development and it may take a few years before having a mass deployment. Nevertheless Oberthur Technologies believes that a solution such as FlyBuy Duo offers a real enabler to speed up acceptance by all parties. It brings all the necessary elements to deploy and manage NFC mobile payment applications as well as all other NFC applications in a secured and controlled environment.

Beside mobile payment, FlyBuy Duo's architecture can potentially suit all other applications and domains that require high security and certification levels (ID, driving licenses) and therefore can be of interest for governmental organizations.

Some of the details regarding the architecture and the process linked to OTA are today still confidential but could be provided under NDA.



[www.oberthurcs.com](http://www.oberthurcs.com)