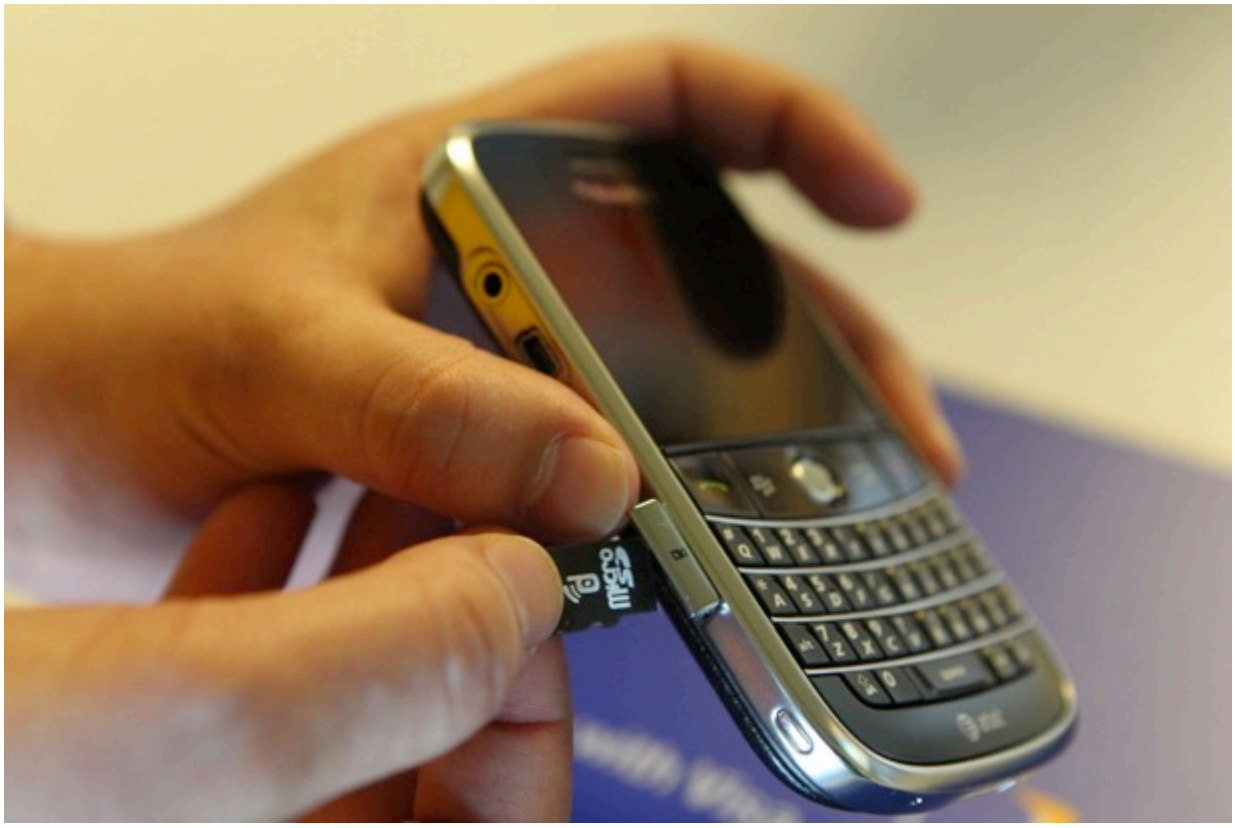
DeviceFidelity

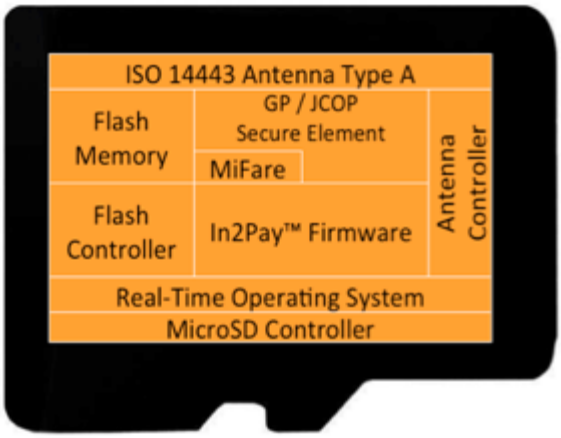
Mobile Contactless Technology Backgrounder



June 2011

DeviceFidelity's patent-pending In2Pay®^{TM} technology is based on a microSD solution that will transform many smartphones with a memory card slot into an interactive contactless transaction device. Financial institutions, handset manufacturers or mobile network operators can issue the microSD as a credit, debit, prepaid or a multiple account digital wallet. The solution allows these issuers to quickly enable large segments of either a pre-existing installed base or even add new customers with mobile contactless capability. The product has earned global recognition, as the world's leading plug and play solution that enables user preferred mobile phones to be used for simple wave and go payments at hundreds of thousands of merchants worldwide.

1. In2Pay®^{TM} microSD architecture



- Integrated antenna
- EMVCo./GP 2.1.1 SmartMX secure element
- 1GB user memory
- Support for Mifare 1K
- SD 1.0/2.0 compatibility
- Issued as a credit, debit, pre-paid or multiple account digital wallet

The In2Pay® microSD includes an integrated antenna that is optimized for good RF performance across multiple readers and mobile phone models. The read range is typically in the 1cm to 2.5cm range. The microSD controller is SD 1.0/2.0 compliant and is designed to work with almost all memory slot enabled smartphones. The real-time operating system and In2Pay® firmware manages the SD interface and also determines whether data coming from the SD interface is meant for the secure element or the flash memory. The secure element embedded within the In2Pay® microSD has been approved by EMVCo and is also Global Platform 2.1.1 compliant. The secure element supports all relevant crypto algorithms with highest security and performance (DES, AES, ECC GF(p), RSA) with optimized chip crypto HW accelerators.

2. In2Pay® microSD basic features

The In2Pay® microSD provides user storage for pictures, video and music. The Smart Chip sometimes known as the Secure Element runs a secure Java Card OS and is capable of hosting secure applets for payments, access, transit and multi-account digital wallets.

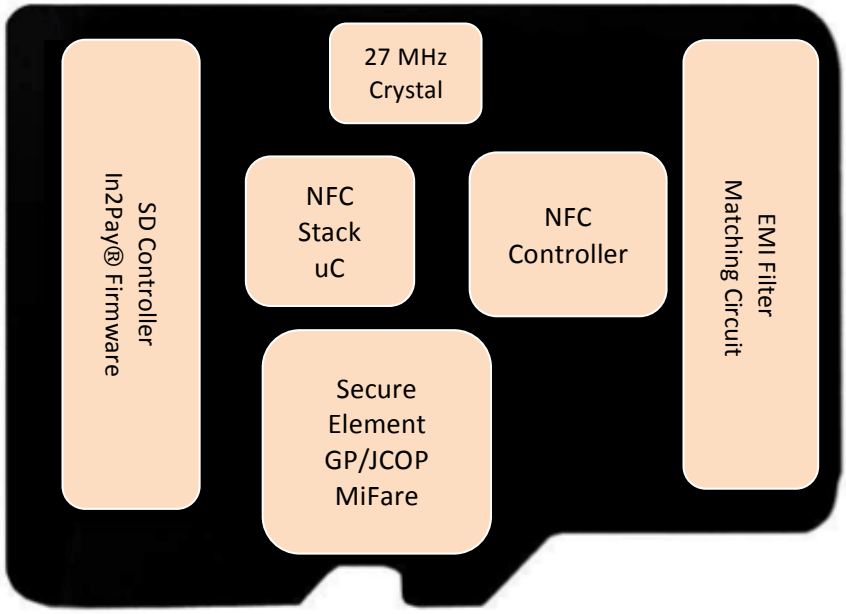
Feature	Benefit
• ISO 14443 Type A proximity interface	• Enables communication with EMV and MIFARE contactless readers deployed globally
• Internal ISO 7816 interface to embedded secure element	• Leverages industry standard interface for smartcards
• SD interface support for SD 1.0/2.0 and SPI	• Most common SD interface for mobile phones
• 2.7 – 3.6V operation	• Compatible with most phone SD interfaces
• “Pay Enable” Antenna	• Stops illicit reading of card.
• Optional password control	• Increased security
• Card Activation	• Increases security
• Support for SD Association optional pins 9 and 10	• Provides support for external antenna if supported by handset
• 1GB user memory	• Storage for 250 3.5 minute MP3 songs or 650 5 MP photos or 4 hours of video @ 384 kbps
• JavaCard JCOP v2.2	• Ensures application interoperability for card issuers as well as application providers

3. Differences between In2Pay® v2.0 and v2.6

Feature	V2.0	V2.6
User Memory	128MByte	1GByte
Two-tap use case support	No	Yes
Mobile device capable of displaying information sent to microSD from POS reader	No	Yes
Support for PIN enabled high value payment	No	Yes
POS field entry/exit detection	No	Yes

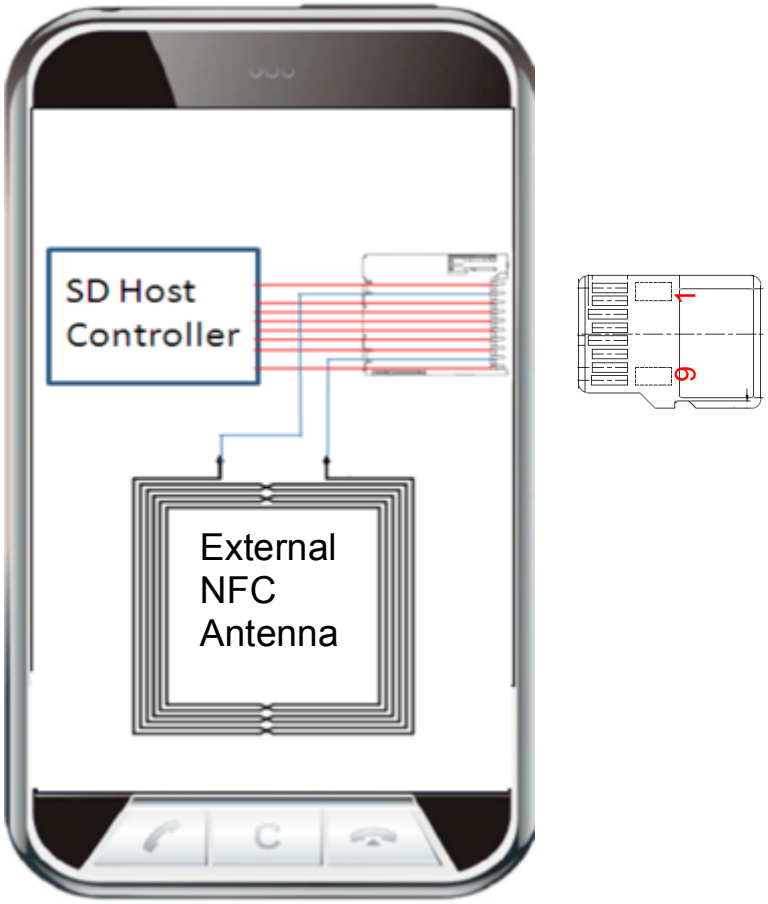
4. Support for full NFC with In2Pay® v3.0

Unlike the In2Pay® v2.x microSD products that only provide support for card emulation, the In2Pay® v3.0 microSD supports all three NFC modes (card emulation, reader/writer and peer-to-peer modes). The In2Pay® v3.0 microSD includes a dedicated NFC controller (NXP PN544), integrated 27MHz oscillator, Secure Element, NFC stack processor and EMI filter/matching circuit for connection to an external antenna.



The SD interface provides the link between the phone and the NFC functionality supported by In2Pay® v3.0. Because the In2Pay® v3.0 fully integrates the NFC protocol stack within the microSD, the software overhead to support NFC with In2Pay® v3.0 is minimal. The functionality supported by the NFC stack is fully accessible via DeviceFidelity's In2Pay® API.

By using In2Pay® v3.0, a handset manufacturer can quickly enable NFC on a handset with minimal changes to hardware or software. If the 8-pin SD connector is simply replaced by a 10-pin connector, the additional 2 pins on the connector can be connected to an external antenna either within the handset or embedded within the handset back cover. DeviceFidelity can provide antenna design guidelines to the handset manufacturer to ensure that the handset antenna matches In2Pay® v3.0.



One possible physical implementation is shown here where the NFC antenna is within the battery cover. The RF connectors on the back cover connect to the 2 RF connectors within the phone body. The phone body RF connectors are wired to pin 9 / 10 on the SD connector.

5. In2Pay® API

The In2Pay® API is available for all popular smartphone operating systems including Android, iPhone iOSx, Blackberry and other J2MEbased operating systems.

The API allows mobile developers to integrate support for In2Pay® into their digital-wallets; TSM OTA proxies and other value add applications with the powerful In2Pay® microSD feature set.

The API enables a mobile wallet resident on a handset to open a session with the microSD, provide power to the handset memory slot, enable payment, open a secure channel with the secure element within the In2Pay® microSD and exchange APDU command/responses with the secure element. Additionally, the rich In2Pay® API feature set provides support for baud rate negotiation that optimizes communication throughput to the secure element. API support for macros can decrease handset polling and simplifies the functionality of a mobile wallet. The API also supports reader field entry/exit events that the handset can utilize in some 2-tap use cases. Finally, the API provides support for writing to and reading from the 1K MIFARE memory within the In2Pay® microSD which enables a mobile wallet to mange MIFARE applications within the In2Pay® based mobile environment.

Please contact DeviceFidelity for more information on API development and commercial license terms.

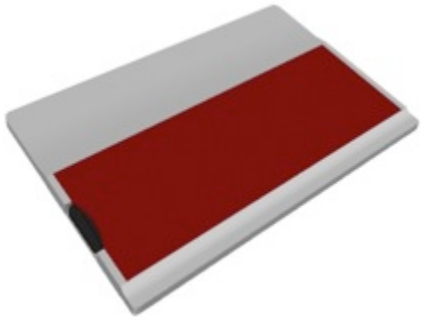
6. Operating System Requirements

In order for a Mobile Phone Operating System to be compatible with In2Pay® v2.x or In2Pay® v3.0, the Operating System has to provide direct access to the microSD file system. This generally means the phone is required to support JSR 75 or similar file connection API. To ensure correct communication between the In2Pay® API and the Secure Element within the In2Pay® microSD, it is necessary to ensure the OS does not cache the microSD contents in any way.

7. Pre-personalization/Personalization

In2Pay® microSD pre-personalization is performed by DeviceFidelity resellers[1]. All resellers are Visa approved smartcard manufacturers. The manufacturer will typically pre-load the applet (if necessary) onto the microSD secure element, complete pre-instantiation, setup communication protocols and complete Global Platform key set diversification by loading the KMC issuer key.

DeviceFidelity provides support for pre-personalization with a specially designed, patent pending Personalization Package ("PP"). Because the PP has the same external dimensions as a standard CR80/ID1 plastic card, smartcard manufacturers are able to pre-personalize the In2Pay® microSD with no impact to their existing in-line manufacturing infrastructure.

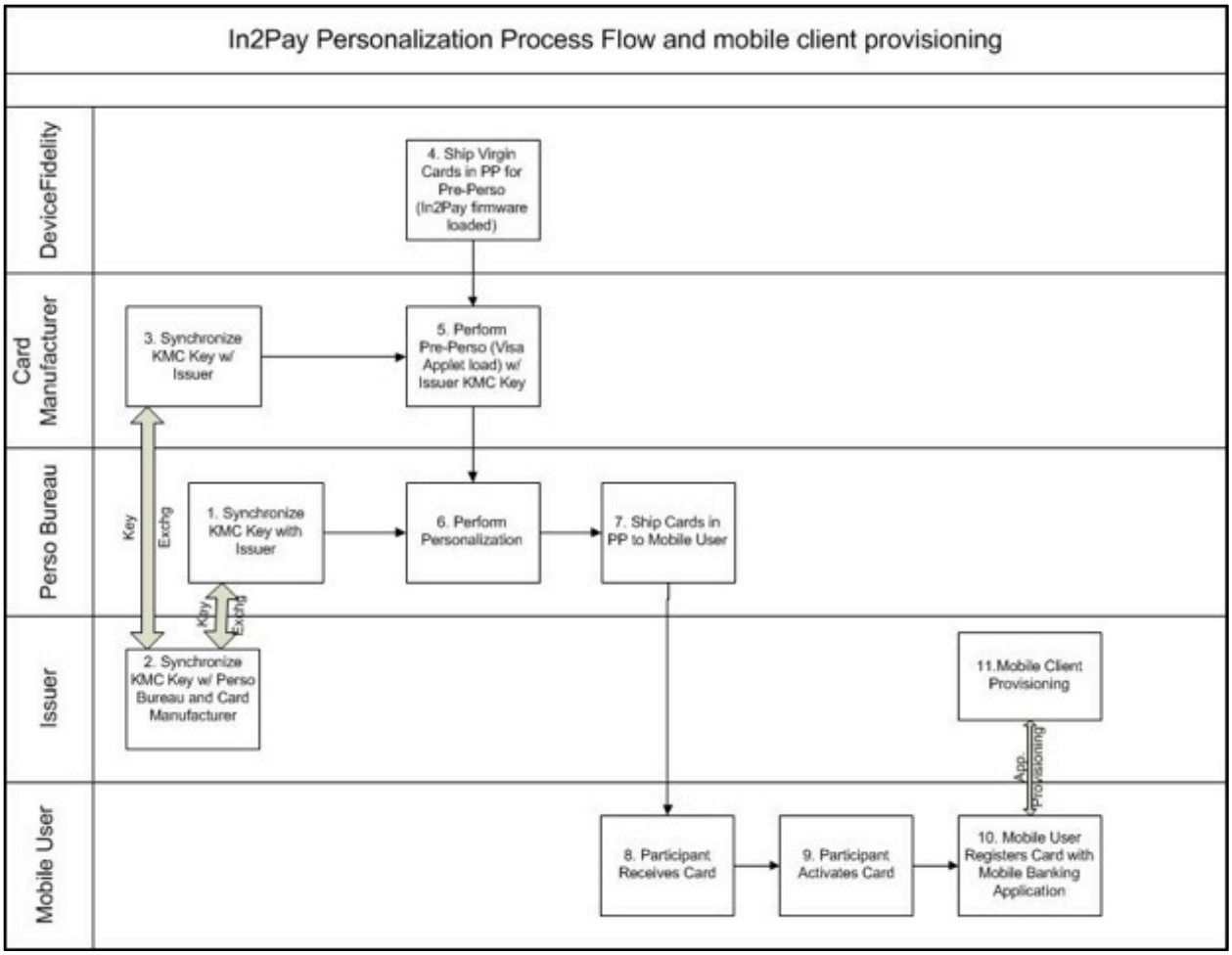


In2Pay® Personalization Package

- External dimensions same as ID1 card 85.60 × 53.98 mm (3.370 × 2.125 in)
- Raised ridge of 1.4mm thickness along length accommodates the microSD card
- Fits standard feeder/hopper of personalization machine
- Supports high throughput volume personalization equipment

In2Pay® microSD personalization can be performed either at a personalization bureau using standard in-line manufacturing equipment or alternatively can be done Over-The-Air (OTA) via a Trusted Service Manager (TSM) after the microSD has been inserted into the mobile device.

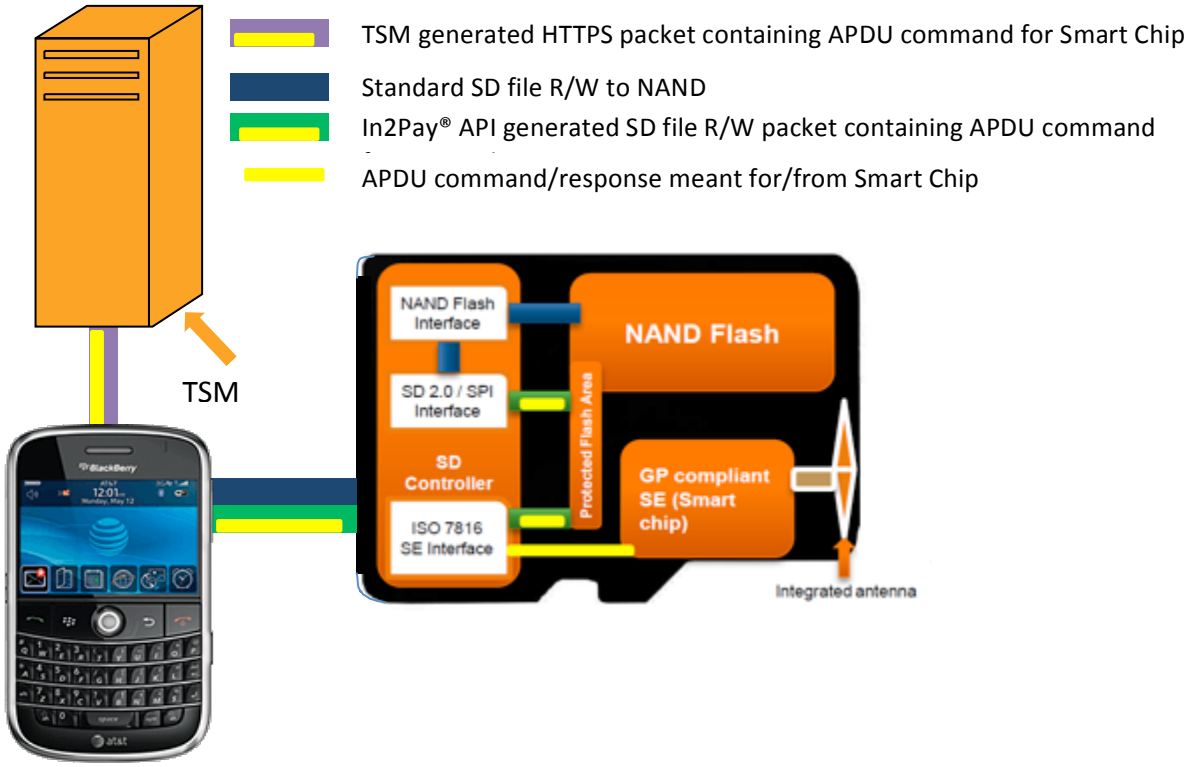
[1] Please contact DeviceFidelity for a list of approved resellers


In2Pay Personalization Process Flow and mobile client provisioning
DeviceFidelity
Card Manufacturer
Perso Bureau
Issuer
Mobile User
4. Ship Virgin Cards in PP for Pre-Perso (In2Pay firmware loaded)
3. Synchronize KMC Key w/ Issuer
5. Perform Pre-Perso (Visa Applet load) w/ Issuer KMC Key
Key Exchg
1. Synchronize KMC Key with Issuer
6. Perform Personalization
7. Ship Cards in PP to Mobile User
Key Exchg
2. Synchronize KMC Key w/ Perso Bureau and Card Manufacturer
11.Mobile Client Provisioning
App Provisioning
8. Participant Receives Card
9. Participant Activates Card
10. Mobile User Registers Card with Mobile Banking Application

8. MIFARE support

The Secure Element within the In2Pay® microSD provides support for Mifare Classic 1K. DeviceFidelity provides an applet adapter that enables the Mifare memory to be written too and read from via the SD interface and the DeviceFidelity In2Pay® API

9. Trusted Service Manager Architecture



DeviceFidelity has partnered with a number of TSM companies to ensure that contactless applications can be securely distributed from a TSM server across a mobile network to the Secure Element within the In2Pay® microSD. The TSM guarantees end-to-end security from the TSM server to the Smart Chip and can provide full application life cycle management of the In2Pay® microSD including:

- Creation of new Security Domain
- Contactless application download
- Personalization of the application

- Activation/De-activation of services

10. In2Pay® microSD embedded antenna and RF performance

An embedded loop antenna within the In2Pay® microSD is used for contactless communication between the In2Pay® microSD and the contactless reader. The RF energy transmitted by the contactless reader and received by the In2Pay® microSD provides power to the microSD and transmits data from the reader to the microSD through modulation of a 13.56MHz carrier signal.

Through extensive lab testing, DeviceFidelity has shown that the In2Pay® microSD RF performance is highly dependent on the location of the memory slot location on the phone. For phones that have the memory slot under the battery, like the early Blackberry Curve 83XX models, it is not possible to complete a proximity RF transaction. Most mobile phone OEMs however are now locating the memory slot where the microSD can be hot swappable. These slot locations are typically more RF friendly for the In2Pay® microSD.

RF contactless transactions are also not possible if the memory slot is behind a metallic back cover. Additionally the microSD has also been observed to perform poorly in phones where the slot is close to a battery or metal within the phone. The presence of metal tends to de-tune the microSD antenna resonance circuit. The HTC HD2 and Blackberry Storm are two examples of phones with metallic back covers that are incompatible with the In2Pay® microSD.

Increasingly handset OEMs are launching new phones that offer excellent characteristics for great RF contactless performance from the In2Pay® microSD. A list of some of the phones compatible for the In2Pay® microSD can be found in section 13 (Compatible Mobile Devices).

11. In2Pay® Range Extender

The In2Pay® Range Extender sometimes referred to as a “Booster” is a patent pending passive antenna which is applied to the inside surface of the mobile battery back cover. The Range Extender concentes the magnetic field flux from the point of sale reader in the area of the embedded antenna within the microSD. The Range Extender enables the In2Pay® microSD to perform in some phones that otherwise would not work at all. In other phones, the RF read range can be improved significantly.

The Range Extender is not physically connected to the microSD and can simply be applied to the mobile back cover with minimal instruction such as the following examples for the Blackberry Bold 9700 and Bold 9650/30.

12. Mobile Phone “sweet spot”

The location of the microSD slot in the mobile device determines the “sweet spot” for optimum RF proximity communication between the mobile device and the contactless reader. Range Extenders are placed on the back cover just above the microSD slot of the phone. The example below shows a range extender on a Blackberry Bold 9000 cover. The ‘X’ indicates the optimum location on the back cover for a transaction.

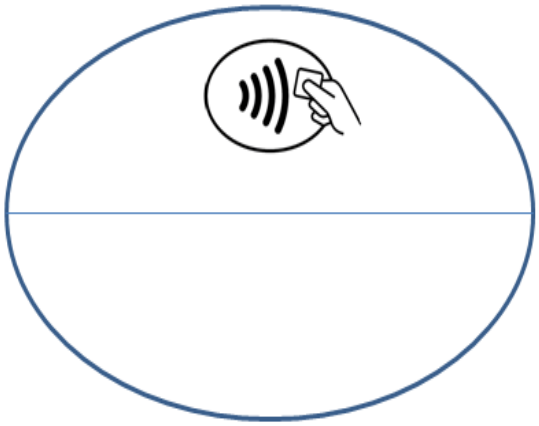
Range Extender stuck on inside back cover of BB9000 (left)

“X” indicates optimum location on back cover for transaction (right)

The Blackberry 9700 has a uSD slot near the top middle of the phone and underneath the battery cover, as shown by the ‘X’ mark. This ‘X’ will be the location to center over the reader when making a transaction.

13. Target location on contactless reader

Most contactless readers have a contactless symbol representing the likely optimum location of the operating field.



Contactless Payment Symbol

For example the Contactless Symbol on the VivoTech 4000 reader shown below is in the top middle of the reader.

For optimum performance, the mobile should be presented to the reader so that the microSD is closest to the contactless symbol.

The microSD device contains the same secure smart card chip that is used in millions of chip and PIN smart cards issued in EMV-compliant countries worldwide. The chip has received EMVCo. hardware approval and has also been certified by Visa.

One simple yet powerful In2Pay® microSD feature is the optional passcode which has to be keyed in before the card can be used to make a transaction. In addition, transactions conducted by the microSD with the contactless terminals are compliant with industry standard payment schemes such as the VISA payWave that generates a dynamic variable verification code for every transaction, helping prevent fraud.

Finally, the In2Pay® microSD can integrate seamlessly with wallet applications on the phone, enabling additional security features such as passcodes and Over the Air account lock if the card is reported stolen.

14. Compatible Mobile Devices

DeviceFidelity can support a large number of mobile phones with memory card slots and is adding to the number of supported phones on a monthly basis.


HTC Thunderbolt


Samsung Charge 4G


LG G2X 4G


Samsung Infuse


Motorola Atrix


Samsung Indulge

There are several requirements that have to be met in order for the In2Pay® microSD to be compatible with a mobile device.

- Phone has to be RF compatible, either with or without Range Extender.
- DeviceFidelity API has to be able to provide power to the microSD slot.

15. Devices Approved for Commercial Use by Visa

Device	Approved Applet	VTF #	Approved Date
iPhone 4	VSDC	MPDEFI0050A	4Q10
iPhone 3GS	VSDC	MPDEFI0045A	4Q10
Blackberry 9650	VSDC	MPDEFI0047A	4Q10
Samsung Vibrant	VSDC	MPDEFI0048A	4Q10
Blackberry 9630	VSDC	MPDEFI0051A	4Q10
Samsung Fascinate	VSDC	MPDEFI0052A	4Q10
Samsung Epic 4G	VSDC	MPDEFI0053A	4Q10
Samsung Mesmerize	VSDC	MPDEFI0063A	4Q10
Samsung Showcase	VSDC	MPDEFI0064A	4Q10
Samsung GT-I9000	VSDC	MPDEFI0066A	4Q10

Additional devices will be added to this list on a frequent basis. Please contact DeviceFidelity for the latest list of approved devices and applets.

16. In2Pay® microSD impact on SAR measurements

In order to understand the impact, if any, on specific absorption rate (SAR) measurements it is important to understand the In2Pay® microSD product does not contain a radio transmitter designed to emit RF energy. The In2Pay® microSD is not a source of RF energy and thus does not create any RF energy for the body to absorb.

To be sure the In2Pay® product has no impact on specific absorption rate (SAR) measurements, DeviceFidelity has worked with a partner and an independent third party lab to measure the impact the addition of the microSD may have to existing SAR measurements performed by phone manufacturers.

These tests were done in June 2010 on the Blackberry Bold 9700 + Range Extender and LG Expo. The testing showed that the addition of In2Pay® had no effect on the SAR compliance rating of the phone. The data in the following table summarizes the test results collected at the lab:

	With microSD	**Without microSD**
Blackberry 9700		
SAR 1g	1.593 W/kg	1.519 W/kg
SAR 10g	1.117 W/kg	1.076 W/kg
LG Expo		
SAR 1g	0.755 W/kg	0.744 W/kg
SAR 10g	0.544 W/kg	0.545 W/kg

All mobile phones must meet RF exposure guidelines the limit of which is 2 W/kg. SAR information for models tested against the international guidelines (ICNIRP) is available as follows: http://www.mmfai.org/public/sar.cfm?lang=eng

17. In2Pay® Case for iPhone

The In2Pay® Case for iPhone is based on the In2Pay® microSD architecture, expanded to support Apple's iPhone products. The cases include embedded hardware which communicates with the iPhone3GS or iPhone 4 via the iPhone 30-pin Universal Dock connector. The smart chip containing the secure element is embedded in the In2Pay® microSD and can work interchangeably with either an iPhone or a non-iPhone device. When used with an iPhone, the In2Pay® microSD is inserted into a microSD socket embedded in the case plastic. The iPhone client application providing the user interface (UI) is downloaded from Apple's App Store and runs entirely on the iPhone.

The In2Pay® Case for iPhone is an approved Apple accessory and can only be connected to an authentic iPhone. Conversely, the iPhone will check to ensure the case is authentic and an approved Apple accessory.

The Apple Universal Connector (AUC) is the main communication channel between the iPhone and the In2Pay® Case system. It allows the iPhone to send commands and receive responses and data back from the In2Pay® Case. Another key function of the AUC is to provide a charging and syncing port to the iPhone when the Case is connected to the phone.

The In2Pay® Case can be permanently connected to the phone even though the Case blocks the user from directly accessing the AUC. A microUSB socket

embedded within the bottom of the case is provided instead for charging and syncing.

The In2Pay® microSD connects to an external antenna embedded within the iPhone Case via pins 9 and 10 on the microSD . The microSD determines whether the external antenna is enabled or not. Also, the Case antenna is only activated when the following three conditions are met:

- The Case is connected and authenticated with an iPhone
- The In2Pay® microSD is properly activated by the card issuer
- The iPhone user initiates a payment (with or without pass code) via a client application running on the iPhone

The In2Pay® API for iOS can be used by iPhone developers to integrate support for the In2Pay® Case for iPhone in their wallet and OTA applications. Usually at a minimum, a developer will want to ensure that their iPhone application will:

- Enable payment (activate antenna and apply power to the accessory).
- Provide pass code setup to enable disable payment
- Possibly include mobile banking links and user preference setups.

More advanced developers use the API to integrate wallet functionality within their applications where iPhone app can be used to determine the default card in the wallet or even be used to select which particular card is used for a given transaction. Many developers have already used the API to provide support for OTA management of the In2Pay® microSD secure element.

18. Mobile User - Basic Use Cases

In2Pay® MicroSD user signup process

1. Bank promotes In2Pay® MicroSD as a standalone account or a companion account
2. Bank validates user phone model
3. Bank issues personalization and shipment order
4. Personalization Bureau ships In2Pay® MicroSD to mobile user

In2Pay® MicroSD issuance to user (scenario 1)

1. Bank Mails In2Pay® MicroSD
2. User extracts In2Pay® (from PP) and activation instructions
3. User calls bank to activate - optional

In2Pay® MicroSD issuance to user (scenario 2)

1. Bank Mails In2Pay® MicroSD
2. User extracts In2Pay® (from PP) and activation instructions
3. User inserts In2Pay® MicroSD
4. User accepts installation
5. In2Pay® application self launches and automatically calls bank or puts link ‘press here to call’ for activation upon first use – optional
6. Phone is ready to make payment

In2Pay® enabled phone used at merchant

1. User identifies a contactless reader at point of sale
2. User presses PAY on In2Pay® enabled mobile phone and taps phone on reader
3. Transaction completes

In2Pay® MicroSD moved between mobile phones

1. User decides to change phones.
2. User removes In2Pay® MicroSD from one phone and inserts into second phone
3. The In2Pay® Browser UI delivers the same In2Pay® functionality on the second phone as the first.
4. The second phone can be used to make payment at a contactless enabled point of sale

In2Pay® MicroSD used in phone with SD slot

1. User chooses to use In2Pay® in a phone with an SD slot
2. User inserts In2Pay® MicroSD into a microSD to SD adapter
3. User inserts SD adapter into phone.
4. Phone is ready to make payment

Low Value Payment

1. Merchant enters low value transaction amount into POS terminal
    a. Mobile user enables payment on handset (turns In2Pay® microSD antenna "on")
2. Mobile user touches the POS terminal by phone
3. Phone shows "payment complete" and transaction details
4. POS terminal shows payment complete

High value payment initiated by POS terminal

1. Merchant enters high value transaction amount into POS terminal
2. Mobile user enables payment (turns In2Pay® microSD "on")
    a. Mobile user touches the POS terminal with phone
3. POS terminal display shows "see phones for instructions"
4. Phone shows payment amount and "enter your Visa passcode"
5. After passcode entered phone is presented to reader again
6. Phone shows "payment complete" and payment details
7. POS terminal shows payment complete