



SD Association

Activating New Mobile Services and Business Models with smartSD Memory cards

White Paper | November 2014 - enhanced from September 2013

Table of Contents

Definitions	3
Executive Summary	5
Introducing the smart microSD memory card	6
Security Certifications	7
smartSD issuance and acquisition	7
Host implementation and integration	8
Roles of smartSD	9
The smartSD ecosystem	10
Mobilization of services	11
Go to market	12
Evolution of services	12
Benefits Summary	13
For the service providers	13
For the card issuers	13
For end users	14
smartSD Business Cases	15
HCE	15
Payment card	16
Transit pass	16
Dematerialized Loyalty card	16
Express check out for Retailers	16
Parking meter	17
Ticketing / VIP event	17
Machine to machine	17
Hotel room card	17
Campus card	17
Enterprise	18
Government / Secure communication	18
TSM operator & MNO	18
Handset bundle	18
Self-service kiosks	18
Secure services for multimedia in consumer devices	19
Conclusion	20

SD Association

2400 Camino Ramon, Suite 375
San Ramon, CA 94583 USA
Telephone: +1 (925) 275-6615,
Fax: +1 (925) 886-4870
E-mail: help@sdcards.org

Definitions

App	An application running on the mobile handset	OTA	Over the Air
Applet	A Java Card application running on the NFC SE; also called a cardlet	PPSE	Proximity Payment System Environment defined by EMVco that specifies the default payment card.
APDU	Command for Java Card applet (Application Protocol Data Unit)	PVR	Personal Video Recorder.
ASSD	Advance Security SD is SDA transport protocol for APDU	SDA	SD Association manages standard related to SD, miniSD and microSD memory cards
BOM	Bill of Material, i.e. cost of the finished good	SE	Secure Element chip that provides a secure run time environment approved for banking Applet A tamper resistant component used to provide the security, confidentiality, and multiple application environments required to support various business models.
Dematerialized card	Many virtual cards sharing the same physical microSD memory card	SIM	The Subscriber Identification Module used to authenticate a subscriber on the mobile network
EMVCo	Standard body that defined the Contactless Mobile Payment, Application Activation User Interface	smartSD	smartSD is the general term defined by SDA for memory card that embeds a SE
FIPS	Federal Information Processing standard that defines security certification profile	SWP	Single Wire Protocol that allows interfacing with NFC front end as defined by ETSI SCP (TS102 613)
HCE	Host Card Emulation. A function for NFC device to route Applet calls/commands to a mobile App	TAM	Total Available Market
microSD	a memory card format defined by the SD Association	TSM	The Trusted Service Manager provides a secure gateway to remotely administrate the NFC SE
MNO	Mobile Network Operator	UICC	Universal Integrated Circuit Card contains the SIM applets and can store other personal data.
NFC	Near Field Communication, a contactless communication, as defined by ISO18092 standard 18092		
Contactless smart microSD	Self-contained microSD card with SE and contactless interface. The contactless interface (i.e. NFC card emulation) is not defined by SDA		



smartSD Memory Card Application Ecosystem

Executive Summary

Smartphones are everywhere and rarely outside consumers' reach, giving service providers unprecedented reach into their customers' daily lives. Mobile phones have created a new channel to deliver exciting new services to consumers and mobilization of services is becoming a strategic imperative to build and extend your brand. This white paper presents the compelling benefits of smartSD™ memory cards as not only the best, but also the easiest solution to enable Near Field Communications card emulation and deploy mobile security tokens on mobile devices.

Using smartSD memory cards as the Secure Element for mobile payment and identity enables value-added services to be interoperable across millions of devices, thousands of consumer products and hundreds of global brands. New opportunities in mobile commerce, advertising, location based services, access control, rewards programs and transportation emerge.

At a minimum, smartSD memory cards can achieve the same security certification as smartcards and security tokens and, therefore, can be used to bridge existing services with various mobile devices, including mobile phones.

However, smartSD memory cards are more than just another option for contactless communication or smartcard and security features. The removability and cross-compatibility of smartSD enables many business models and provides great flexibility for providers and customers. With access to more than 78 percent of the mobile phones in the world and the market weight of the SD standard, smartSD gives service providers unequal access to consumer devices.

The smartSD memory card also supports a consumer-centric business model envisioned by GlobalPlatform™ that sets in motion a virtuous ecosystem and ultimately creates value for all parties.

smartSD memory cards offer service providers and card issuers a superior approach to deploy services to the total available market using existing business processes and existing hardware. smartSD memory cards help service providers and card issuers reach the largest audience, retain business independence, launch faster and with lower costs, and differentiate their services.

The smartSD memory card also supports a consumer-centric business model envisioned by GlobalPlatform that **sets in motion a virtuous ecosystem** and ultimately creates value for all parties.



Introducing the smart microSD memory card

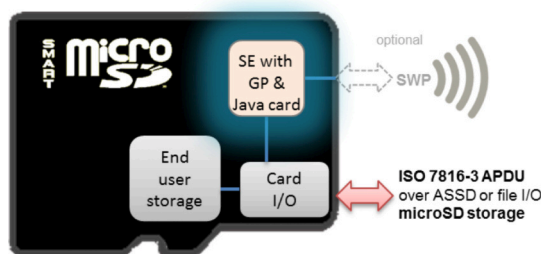
A smart card secure element can be packaged into various form factors including all SD memory card formats such as full-sized SD and microSD memory cards of any storage capacity or speed. The smartSD memory card comes with an embedded Secure Element (SE) that features the exact same level of security as other smart card form factors. smartSD is accessible to the host application and through contactless (when applicable) therefore it is ideal for mobilizing both the world of digital security and the world of contactless cards, bringing innovative new services to mobile devices. The smart SD card is available in two flavors: a smartSD that features Java Card technology and complies with GlobalPlatform™ specifications and a contactless smartSD that additionally features a contactless antenna. Fully compatible with each other, both are compliant with legacy microSD specifications thus maintaining portability and universal storage capabilities.

smartSD covers business needs such as User Identification, Remote Authentication, Non-Repudiation and Confidentiality. It enables new business models for service providers and protects end users.

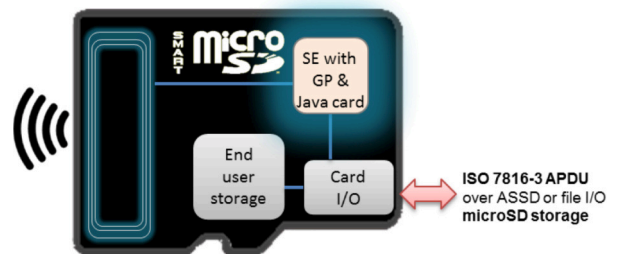
Most importantly, smartSD provides a SE independent from both the OEM and MNO.

smartSD combines the advantages of memory cards with those of security tokens while it benefits from the host capabilities such as display and 24/7 connection.

As such smartSD could be distributed, initialized, and pre-personalized with a service or mailed personalized to the end user like regular banking cards. Services can also be issued in the field, allowing end users to purchase smartSD cards and configure them to fit their unique needs.



smart microSD with optional SWP
smart microSD features a SE that is accessible through ASSD for host applications and may connect to the host NFC frontend via SWP



Contactless smart microSD
Contactless smart microSD is a self-contained solution for SE and contactless smart card emulation for most microSD host devices. SDA doesn't define the contactless interface

Figure 1: Types of smartSD

The smartSD card isn't specific to a particular SE chip, Java Card and GlobalPlatform versions: the card can be customized to meet security requirements and certification of particular use cases. smartSD cards can protect all cipher, authentication and signature keys, validate PIN and biometrics, and run cardlets of different types including transit, payment, ticketing, loyalty, and many more.

Typical target usages are:

- **Security token:** The embedded SE is typically used to protect credentials used for authentication, digital signature, data encryption, etc.
- **Secure Element:** The smartSD is the secure element for the host device NFC
- **NFC card emulation enabler:** Contactless smartSD brings NFC card emulation and SE to the host device independent of the host device being present or NFC capabilities missing.

Security Certifications

Security certifications are typical of target services and as such are not covered by SDA. SDA also doesn't define the contactless interface of smartSD which is driven by NFC standards and ISO14443.

Security certifications are attached to the SE in a microSD package and are therefore dependent on the security level of the selected smartcard chips. User storage has no impact on the certification and a certification is typically valid for multiple storage capacities. Certification is product specific and obtaining certification is a business decision.

There are already multiple certification programs and labs that can certify a smartSD card: Visa®, MasterCard®, American Express®, EMVCo, FIPS 140-2 for government and enterprise applications and more. SmartSD could also be used in transit applications when the chip features MIFARE™ or can be loaded with the adequate transit App such as Calypso™ or Cipurse™.

smartSD issuance and acquisition

The smartSD memory card has a similar life cycle as legacy smartcards, SIM cards, contactless cards and other security tokens. Despite a different physical communication interface, the manufacturing is very similar to the other form factors as many components are shared, including the embedded secure chip that meets the security and functional requirements mandated by the different markets (e.g. banking, identity, transport).

The following table illustrates the similarities and differences for these different form factors:

Silicon	Operating System	Packaging	Init and perso	Distribution	Mobile Host Devices	Service access	Remote Management
<ul style="list-style-type: none"> Security sensor detectors Secure memory management 	<ul style="list-style-type: none"> Secure run time environment ISO7816-3,4 compliance ISO 14443 compliance and ISO 18092 	contactless smart microSD	<ul style="list-style-type: none"> Electrical initialization and personalization Physical personalization 	<ul style="list-style-type: none"> Retail Banks Service provider 	Most microSD host devices	Instant gratification or	TSM & other (optional)
		smart microSD with SWP			Phones with SWP to microSD		TSM & other (optional)
		Security token		<ul style="list-style-type: none"> MNOs Handset bundle Mailing 	N/A	TSM issuance when applicable	PC solution only
		Contactless card			N/A		
SIM card with SWP	<ul style="list-style-type: none"> MNO Handset bundle 	Only NFC phones from partner MNOs	After issuance through TSM	TSM			
Embedded SE		Phone model specific		TSM			

Figure 2: smartSD life cycle

smartSD can be configured and distributed as typical smart card and security tokens.

The configuration of the SE can be done using standard smart card software as PC/SC drivers are typically available for microSD as well. Only the physical interface to the card is different. Initialization and personalization of the SE can be done on anything from desktop solutions using a simple USB reader up to mass personalization solutions with automated machines that can handle many microSD at one time.

Smart microSD can be distributed to the consumer in different ways: retail purchase, from the service provider, kiosk, received by mail, on-site issuance, bundled with the phone, etc. The secure element in the smartSD can be initialized with a specific security configuration or be ready for a service or personalized in the field.

smartSD is also compatible with TSMs that can communicate to the card through mobile apps or services. Typically a compatible service would check in at the TSM and look for specific job(s) to perform.

The GlobalPlatform Consumer Centric Model will ensure that post-issuance of cardlets would be the same as getting a new App on a mobile phone. GlobalPlatform Consumer centric specifications provide the security mechanisms and the user control to ensure such a user experience can be implemented.

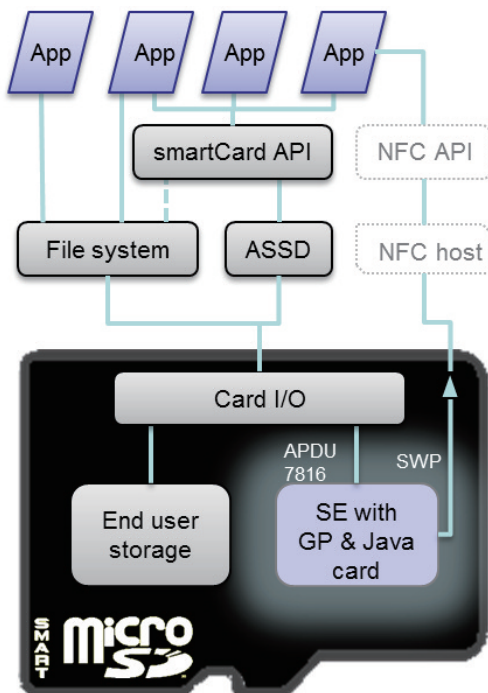
Host implementation and integration

smartSD defines a memory card that embeds a SE. The typical SE features JavaCard and Global Platform and communicates with APDU.

Therefore SDA has defined a transport for APDU: ASSD is a software protocol to send APDUs using a standard microSD interface (no extra or dedicated pin for APDU is needed). ASSD is available on Blackberry and the source code is available for Android SEEK.

Many smartSD cards typically feature the capability to transport APDU using files, which has the advantage of working over a standard file system and can address devices where ASSD hasn't been implemented. These file I/O solutions are however proprietary and not defined by SDA.

SDA has also defined a pin for Single Wire Protocol (SWP) that is used to connect to the host NFC and provide a secure element for NFC card emulation. In some cases, where supported by the SE and the host NFC, this SWP pin could also be used to transport APDU.



The implementation of a smartSD App is quite simple. It only requires standard mobile App development and takes advantage of a few APIs to exchange APDUs.

Most smartSD and contactless smartSD will work without an App however the value-add typically results from the inclusion of an app that takes advantage of the host/phone capabilities.

The smartSD could be implemented as a security token where it protects credentials and could be used to secure email, messaging, digital signatures, transaction approval, identification, VPN access and many more. In that case the smartSD would be implemented into different apps where the card services and security features would be made available to the end user.

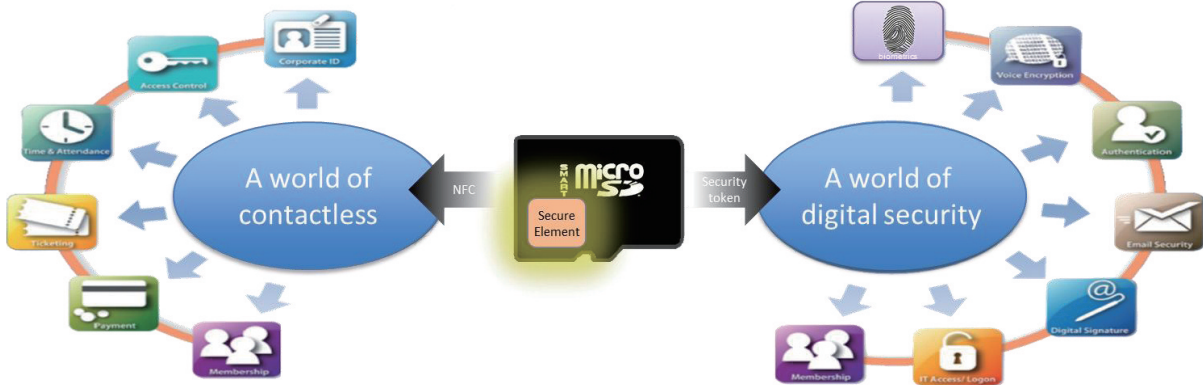
The smartSD can be implemented for NFC card emulation use cases. NFC card emulation covers many applications and multiple target markets. The smartSD would typically run the cardlet required for the service and take advantage of the App to provide additional value to the end user. This could also apply to MIFARE when the smartSD SE features such capabilities. For these implementations the mobile and its App typically adds value on top of what a contactless card could do.

smartSD could also perfectly combine with HCE (host card emulation) and TEE (Trusted Execution Environment) where it would bring the necessary certified security to reduce the operation cost inherent to HCE while keeping all the value propositions of HCE unchanged. The integrated SE in a smartSD card allows for a more secure HCE implementation without a major overhaul of the existing solution.

Overall the smartSD implementation ensures that the service provider can decide on the role of the card, the type of user interface and the business model. Furthermore the card provides complete independence from the phone model and from the mobile operator.

It also makes it very easy for today's card issuer as smartSD can be distributed as current cards and prepared using the same software solutions.

Roles of smartSD



smartSD can be used for both contactless services and for the security of App and services.

Contactless services would rely on contactless smart microSD or on a smartSD implemented within an HCE capable host.

Therefore smartSD could be used to mobilize existing contactless card services and solutions and take advantage of the mobile host display and connection capabilities to enable value-add services. This would be applicable to transit, access control, ticketing, payment, loyalty, and many more applications.

smartSD would run the needed cardlet that would be accessible from the contactless side and from the App that provides a UI and facilitates a connection to a backend.

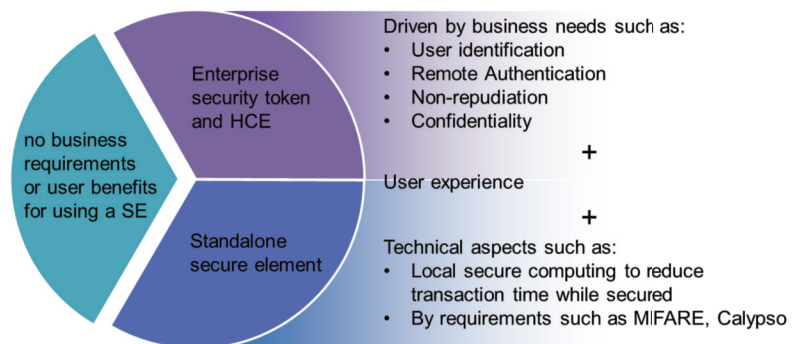
This would also permit the development of new innovative services taking advantage of the contactless interface to communicate with a cardlet in the smartSD that maintains the required security to protect the end user and to enable business models while an App provides a nice user interface.

App and services could take advantage of smartSD security to ensure specific business requirements such as privacy, confidentiality, non-repudiation, user identification/authentication, and more.

For this usage the smartSD provides a known level of security that meets business requirements and ensures tamper resistance.

In this world, smartSD is typically used to protect cipher keys, perform strong authentication and perform user identification using PIN or biometrics. The card ensures that keys cannot be copied and that user information remains protected.

SmartSD is typically integrated into crypto libraries such as PKCS#11 or CSP that are used by an App for secure email, privacy and confidentiality, backend authentication, document authenticity or approval cycles.



The smartSD ecosystem

The smartSD enables an ecosystem that creates value for all parties. It is not like other approaches where a single party is perceived to extract all the value at a disproportionate cost to all other parties.

First, smartSD provides freedom to the end user as it is available to most users independently from their phone model or mobile operator. This means that in addition to extra storage always valued to the end user, changing phone and mobile network operator doesn't come at the expense of losing credentials and benefits of associated services.

It also means the service providers can address most of their customers (including iPhone 4/5 owners through a specific case adaptor¹).

smartSD can be issued by service providers or purchased directly by consumers, as well as distributed by traditional operator controlled smartcard channels.

In particular, smartSD memory cards allow service providers to differentiate and determine a specific business model that does not have to involve a third party.

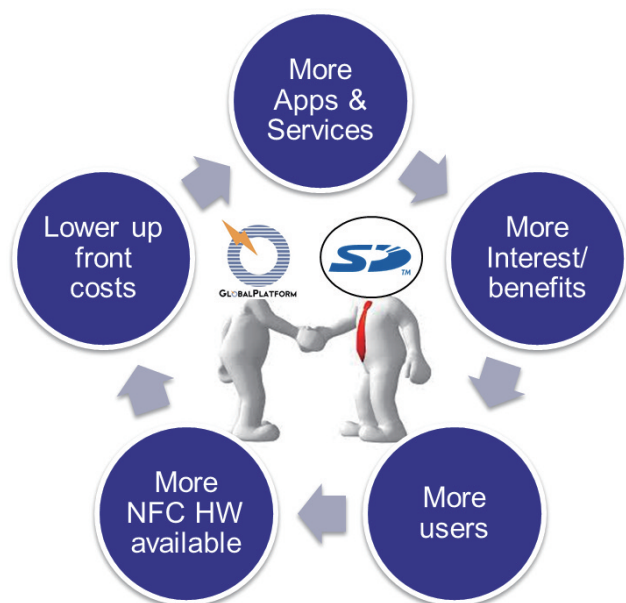
Therefore smartSD presents more benefits for stakeholders than any other mobile security solution. And business independence is key for the service providers as mobile is a necessary strategic move.

This ecosystem becomes virtuous as more parties, users, services and applications, take advantage of smartSD, creating greater value for all.

GlobalPlatform Consumer Centric Model allows consumers, rather than issuers, to control multiple services on a single smartSD as they do with apps on a mobile phone.

Driven by the SD Association and with the support of GlobalPlatform, the smartSD memory card ecosystem will continually evolve to meet new industry needs, even gaining the ability for consumers to add third-party services on their smartSD memory card.

The smartSD is not a transitional technology simply waiting for NFC handsets to become available to the masses or until another SE takes over; rather, smartSD offers the market a compelling value for today and tomorrow.



**A VIRTUOUS
ECOSYSTEM
CREATING VALUES
FOR ALL PARTIES**

Figure 3: A virtuous ecosystem

¹ iPhone 6 TBC

Mobilization of services

With smartphones and super phones becoming widely available and various app stores making it very easy to download new applications to any device, consumers now want all services on a single device which they always carry with them.

Therefore mobilization of a service is not only a must have capability but also a strategic move. It is a real opportunity to create new revenue streams and strengthen customer relationships while differentiating your offering with a better user experience and value added services. Mobilization is typically a real success when taking advantage of the display and the connectivity of the phone. This is when the end user value-add shines on top of what contactless card or security tokens already provide.



As such, mobilization should be carefully considered and more particularly for services that involve security such as smartcard, contactless services and security tokens. The choice of SE or no SE could be critical.

Some service requirements would dictate the need for a specific type of SE. Such mobilization should be thought through carefully and the choice of form factor for the secure element could be critical to keep control of the business model, easily differentiate from competition, and facilitate go-to-market.

There are services using card and security tokens where the continuity of existing operation process is critical. In that case, smartSD is a perfect fit as it can use the same distributed process and channels already in place. smartSD also brings the value of being a hardware token providing strict control on the issuing process.

Other services rely on implementation in the app such as HCE. smartSD is also very relevant for this type of implementation as it brings increased security to reduce the financial risk and minimize operation costs. HCE services such as for payment typically rely on transaction tokens delivered by a server. The

smartSD would typically secure the connection to the server and provide strong identification. It can also increase the security of the received tokens and associated rules. As such the smartSD brings a known level of security into the solution and increase the security on critical parts. As such the HCE App and client-server relationship does not need a constant update to stay ahead of hackers. Therefore for these types of services smartSD is ideal as it doesn't change the value propositions of business independence and differentiation provided by HCE while adding a smart card level of security into the solution.

The development of new features and the release of value added apps that can reach all customers without any MNO or handset model limitation is perhaps the biggest value of smartSD.



The smartSD is the best approach to mobilize security services by:

- Delivering the largest market reach as more than 78 percent of mobile phones and thousands of other devices have a microSD memory card slot
- Working on most users' current phones independent from the mobile subscription and operator
- Offering unsurpassed portability and easy transfer by the consumer to a device of choice
- Allowing familiar issuance processes that fit contactless card and security token operation and business processes
- Providing an open choice of business models
- Simplifying the launch of services, reducing time to market and eliminating the need for third parties and for upfront TSM deployment

Go to market

The smartSD memory card makes mobilization easier for service providers/operators who focus on delivering value propositions.

Once the type of smartSD implementation has been chosen, launching is very easy as it fits existing business processes and does not require any agreement with third parties.

Driving market adoption, however, requires understanding what it takes for consumers to change their habits. This means understanding their perceived value of the services as well as knowing what value would inspire them to buy the service or the smartSD memory card.

Millions of microSD cards are sold every day and a (contactless) smartSD would be an inexpensive add-on to the standard card consumers buy today. Demonstrating and promoting consumer benefits is important to facilitate adoption and potentially transfer the entire cost of the card to the consumer. In short creating awareness at key locations drives adoption of the service

Here are some examples of real life end-user value proposition applicable to various markets:

Type	Tag line	Implementation
Cash back	2% cash back for every purchase	<i>Using interchange rate Annual membership could pay for the card</i>
Cost saving	\$Save - Up to 50% off	<i>Promotion to smartSD holder for purchase at specific target stores</i>
VIP	VIP yourself! Skip the queue	<i>Special line for smartSD contactless check in</i>
Pack lighter	Downsize your wallet Travel lighter	<i>Leverage dematerialized loyalty and payment cards and security tokens for badge and VPN</i>
Safety	Protect your money	<i>PIN protection and consumer control RF</i>
Control	Get back in control of your finance	<i>Takes full advantage of mobile UI and alerts</i>

A smartSD consumer centric approach can provide for multiple services thus making the smartSD cards an even more valuable investment for the end user. Also, smartSD memory cards include all of the current benefits from being the world's leading memory card form factor: extra portable storage for end-user content and data.

Evolution of services

App stores make it easy to inform users about updates and to deliver and install these updates. Updated apps can have additional features and value propositions on the smartSD device. This makes improving the user experience and differentiating the service easy.

Existing cardlets on the SE can be configured or personalized with a simple data connection to the mobile device (Cell, Wi-Fi or tethered), through contactless communication, or using onsite issuance.

Adding new applets on the SE may require the use of a TSM. However, most TSM vendors support smartSD with their TSM supporting data connection. This is typically the same as communicating with other SEs over a data connection, but some TSMs might be set for a specific SE and would require an additional module to handle a second SE such as smartSD

Overall, GlobalPlatform's consumer centric approach specifies all the information and the processes needed to facilitate such updates or service evolution and work seamlessly with smartSD.

Benefits Summary

For the service providers

- Largest reach:** User's current and future mobile devices, any mobile operator and mobile plan, phones with and without NFC
- Business independence:** No dependence on any 3rd party, including MNO's or handset manufacturers.
- Easier launch:** Fits existing business process. No need to involve a 3rd party.
- Lower cost:** Upfront TSM integration optional. Simplify service delivery
- Differentiation:** No constraints to differentiate from competition with your own user experience, set of features and business model.



For the card issuers

- Service Providers:** In some cases the service provider is also the smartSD issuer. In that approach, the smartSD could be sold as part of the service and advertised as consumer centric compliant and thus usable and compatible with multiple services. Such service provider contributes to the ecosystem by making these cards available for other services and can take advantage of cards sold by other service providers.
- Retailers:** Millions of microSD are sold every day and smartSD could be sold in retail alongside or instead of regular SD cards. smartSD could come with a service pre-installed to add upfront value and the GP consumer centric model facilitates the issuance of additional applets post-sale.
- Mobile network operators:** smartSD lowers the upfront cost of NFC as it could be targeted to specific users. SmartSD has a larger reach and could assist in acquiring subscribers from competition.
- TSM operators:** smartSD provides new TSM opportunities, a larger reach and business independence



For end users

- Instant Gratification:** smartSD works with existing phones and can potentially require only a software upgrade to integrate with users existing applications, providing immediate value to the user upon purchase.
- More choice:** smartSD provides a choice of suppliers and more products to choose from.
- Greater freedom:** smartSD provides the freedom to choose phones and mobile plans independently from services.
- Extra storage:** smartSD provides the same benefits of millions of microSD sold every day for extra storage which supports the growing need for music, photos, videos and games.
- Ease of Upgrade:** consumers can upgrade their phone or change their MNO without losing their existing services.
- Application Control:** users can choose the applications can services they want and make changes easily.



smartSD Business Cases

While the consumer could purchase a smartSD memory card directly in any of the following scenarios, these business cases focus on the examples where the smartSD memory card is subsidized or provided at no-cost to the consumer. They demonstrate how the cost of issuing the smart microSD memory card can be recovered even when provided free to the customer.

This focus does not detract from the consumer ability or interest in buying the smartSD memory card directly to access value-added services on their mobile phones. Other business cases can include selling the smartSD to the end user providing an immediate return on invest, but they are not considered in this section.

HCE

HCE allows for software emulation of contactless JavaCard and is typical of contactless use cases. It is unrelated to security tokens for mobile application and online services. It is also specific to JavaCard and may not apply to contactless solutions with proprietary features such as MIFARE and DESFire.

Host Card Emulation would not seem to be a target market for smartSD but once the costs of maintaining HCE services secure such as for contactless payment are considered, smartSD can be seen to add significant value to these implementations.

For example there are HCE solutions that rely on client server architecture and temporary tokens. Such solutions are designed around temporary credentials to ensure strong security is not required to protect them. However these architectures usually involve connecting to a server to get the tokens. The App typically authenticates to the backend or uses some other identification means in order to identify the user and deliver tokens.

In some implementations protection of those credentials could cripple the user experience. For example it won't be convenient for the end user to have to present his/her PIN every time new tokens are required. It also will not be convenient for the end user to enter their credit card information every time new tokens are required.

In some implementations non repudiation is a must-have and proper user identification is required. Once again this could damage the user experience if the user is asked to be identified too often.

Ideally the connection to the backend should be transparent to the end user and if possible done at convenient times, e.g. not at transaction time. However caching information to maintain a good user experience requires adequate security. Caching is not optimal when the number of transactions is unpredictable such as for transportation or fare-collection systems.

The token server is a great target for hackers and for impersonation as tokens are personal.

Tokens are also delivered to the device and only protected in software. This would be another target for hackers who can get free transactions either by changing the expiration rules (when applicable) or by using the renewal mechanism to get more tokens.

In both cases the App is the weakest link because it contains the information to authenticate to the backend and the information to access to local tokens. To stay ahead of hackers, the App must be continuously updated along with the server side. This represents a large cost as the App would have to be continuously tested for all supported phone models. Furthermore the financial risk remains unknown because software hack could be unpredictable. Additional software layers such as TEE might help on the security side but could also increase the cost for a financial risk that remains unknown as TEE does not have security certification at the moment.

This is where smartSD becomes valuable for HCE:

- ensure a great user experience
- provide non-repudiation and protection for identity theft
- provide a hardware root of trust that could be preconfigured for the service
- be pre-personalized to ensure strong authentication to the backend token server, for example by using PKI as suggested by Fido.org

- perform strong user identification (protection of PIN, biometrics match on card, etc), also suggested by Fido.org
- protect the tokens from the end user

More importantly smartSD reduces the risk to a known security level as it has already passed adequate security certification. Therefore smartSD not only helps lower the financial risk but also reduces operation cost as hackers would focus on the card rather than the App.

Using smartSD along with HCE gives the best of both worlds: the flexibility of HCE and great integration in the OS with all the security of a certified smartcard chip, without the trouble of implementing a TSM for evolution of the service or having to sign agreements with all mobile operators and mobile phone makers.

Payment card

The main revenue from a payment card is typically derived from serving as a deposit account. Nevertheless, there are other revenue streams that could cover the costs of issuing a smartSD memory card:

- When interchange fees are applicable, the cost of a smartSD memory card with average use is easily paid back within the first year. Furthermore, interchange fees revenue could be used to build a cash-back value proposition to the consumer that could both drive sales of the card and absorb the entire cost.
- The revenue from a referral program with partners can also easily pay for the card within a few transactions. Program partner merchants would pay for customers to be directed to their stores or services.
- A futuristic business case would capture smartSD memory card benefits in online payment scenarios where it could be used for card-present transactions and for 3D Secure using http(s) as an alternative to potentially costly SMS.

Transit pass

The ease and convenience delivered by smartSD memory cards should compel consumers to purchase the smartSD memory cards. However, some transit services may want to promote mobile phone usage to save on kiosk costs and to keep workforce costs low. In that case, a reloading fee

would pay for the smartSD memory card. The consumer can easily accept a minor fee to take advantage of the convenience and shorter wait times. A regular user would pay for the card within the first year.

Transit operators could also consider the additional revenue opportunity from advertising in the mobile App. As the smartSD memory card is the sole SE option without recurring fees, advertising, so revenue stream could recover the cost of the smartSD before adding to the bottom line. This example provides real value for local shops and transit passengers, plus transit traffic numbers would attract advertisers.

Dematerialized Loyalty card

Dematerialized loyalty cards not only reduce clutter in users' wallets, they mobilize smartcard-based loyalty services by taking advantage of mobile phone communication channels and localization capabilities. The first allows for a direct marketing channel that could be used to increase sales and strengthen the brand and the second makes it easier to locate a nearby store. While increased sales would recover the costs of the smartSD memory card, targeted marketing would also affect customer retention.

For these programs the embedded SE in the smartSD memory card could play a role to locally and securely manage some of the rules so the consumer could redeem benefits even when offline.

Express check out for Retailers

A basic program for a retail shop to issue smart microSD memory cards is sustained by the use of a retailer specific mobile app to leverage shopping lists, target promotions, and reward loyalty; however, the current programs still require payment from the user via credit card or cash transaction. A richer approach would also allow shoppers to use their phone cameras to scan the goods added to their cart (also allowing for instant promotions) to reduce checkout time. This richer approach would deliver an improved shopping experience for the user and require fewer cashiers for the retailer. Plus, this experience could also motivate shoppers to buy the smart microSD memory card to obtain this value-added service.

Parking meter

Contactless communication clearly reduces costs for parking meter service and maintenance. It facilitates money collection, reduces vandalism and dramatically lowers maintenance costs. The mobile app opens a new world of premium services for users. For example, a typical premium service uses the mobile app to secure a parking spot. Additionally, like the transit pass business case, the parking meter app could be used for highly targeted advertising based on the user's parking spot location.

Ticketing / VIP event

This business case is partially supported by reducing time at event checkpoints. Contactless technology presents many advantages over other technologies: it works even when it is dark and does not require a lens to focus, its built-in anti-cloning/ anti-pass back security enables offline validation, and the use of contactless communication reduces the risk of failure as no mechanical parts are involved. Overall, this new method helps reduce operation costs and, more significantly, reduces the number of people needed at the gates to ensure a good user experience.

Users would also gain the option to make purchases from within the mobile app. The app creates new revenue generating premium services such as paying extra for VIP access and paying the issuer a percentage on resold genuine tickets.

Since the smartSD memory card typically does not present a reason for recurring fees, a card can be issued once and used for multiple events by the consumer.

Machine to machine

The smartSD memory card presents the perfect combination to leverage mass secure storage and a secure run time environment. One consideration for this business case is the communication cost savings yielded by using the smartSD memory card to securely store data for later transmission during lower cost, low-traffic times.

Another consideration for the business case is in the cost savings realized on a design that could have lower BOM costs and the option to adapt the storage capacity to need, thus optimizing inventory costs.

Hotel room card

Hotels will definitively benefit from the dematerialized loyalty card business case taking advantage of local advertising from partnering restaurants, bars and other local events. It would provide benefit to both service providers and users.

Additionally, the smartSD memory card with NFC reduces costs as it decreases staffing required for a good user experience at check-in and checkout. The user could take advantage of the hotel booking app to reserve a room and receive the credentials to access such room directly on its smartSD. Taking advantage of the smartSD contactless capabilities, the customer could go direct to his/her room while the booking system can benefit from strong authentication.

The value add for the consumer could justify the consumer purchase of a smartSD memory card, yet the cost savings and the optional revenue opportunities from referring local partners and advertising also provides a hotel operator with ROI on the smartSD memory card.

Campus card

The cost of a campus smartSD memory card could easily be included in the students' tuition fees since it supports many use cases such as physical access control to campus premises, library and other campus assets, remote access to the school network and online courses, and payment of services and fees. It could also serve as a payment card for parents interested in managing their child's spending, allowing them to remotely add funds when needed to provide additional functionality over typical credit/debit card setting.

Some campus usage may generate revenue from this program. For example, payment could leverage an e-purse or pre-paid MasterCard or Visa that would generate interest on the pool of funds, which could help subsidize the cost of the card. This might be complemented as well by customer acquisition fees from partner banks.

Universities can also use smartSD cards in the management of textbooks and related class materials. The smart SD card can securely load and store required materials for a class in a format that can be easily accessed by students on the mobile phones, tablets or laptops. Rental options, where the materials are only available during the class, are easily added to this model.

Enterprise

The smartSD memory card in the enterprise is a perfect example of mobilization of services. The smartSD memory card with NFC can actually address multiple use cases such as physical access control and IT security, including secure email on mobile devices, secure data storage and VPN access. smartSD memory card storage can also be used to easily move files around the enterprise in a controlled manner. As such, in the context of mobilization of the enterprise, the smart microSD memory card with NFC has a clear business case based on cost savings. First, it does not have recurring costs unlike many other SEs. Then, it allows the enterprise to reduce the total cost of ownership by reducing the number of devices per employee and allowing use of the employees' own mobile devices. This move cuts the cost of VPN tokens, sophisticated contactless badges, CDs and USB memory sticks, to name a few. Finally, having an SE entirely controlled by the enterprise adds freedom and facilitates additional services.

Government / Secure communication

Today's mobile devices provide the average consumer more communication abilities than a U.S. president could access 20 years ago. The mobile device is a must-have tool that provides instant access to most information, which could be critical in certain situations. So while the potential of mobile technology should be embraced, it should be very secure so that sensitive information and communication remains protected at all times. The cost of compromised information could have immeasurable consequences. The smart microSD memory card could be used to provide secure voice communication, emails and remote access. It can also secure the data on mobile devices to ensure that sensitive information is always protected. Furthermore smartSD meets BYOD requirements.

TSM operator & MNO

There are various business models and opportunities to be considered by TSM operators and MNOs. Typically, the smart microSD memory card with NFC could be subsidized by charging a fee for loading a new applet on the SE. When charging a one-time fee, a few applets could easily cover the cost of the smart microSD memory card with NFC. Rental fees could also be considered as an alternative, but rental fees could have a more direct impact on the service

provider's business model. Also, additional revenue sources are created from managing the applet store and proposing additional services to the consumer.

When a TSM operator is an MNO, the smart microSD memory card allows the TSM to expand NFC services beyond its customers and to acquire subscribers from other MNOs. Furthermore, the removable smart microSD memory card allows TSMs to target specific users, keeping upfront NFC promotion costs very reasonable compared to other solutions where contactless communication is provided whether the user needs it or uses it.

Handset bundle

The removability of the smartSD memory card is a key asset when adapting a global device to local markets, as it reduces costs through higher production volume. Not only does the smart microSD memory card allow available storage capacity to be adapted to the desired level for the market and price point in regards to the device positioning, but it also facilitates enabling NFC where needed or requested by mobile operators. As such, adding smart microSD memory cards to targeted markets results in overall cost savings and potentially larger sales revenue through better market positioning.

Self-service kiosks

At the self-service kiosk – and photo kiosks in particular since content sizes are growing every day – there is opportunity for improvement and innovation in the way content and payment are handled. With smartphones and other mobile devices emerging as the de-facto content source, secure payment would significantly improve the user experience. Today, issues being reported from the kiosks include growing concerns with respect to user experience, including issues with Bluetooth™ pairing, cable management and accessing removable media. These problems multiply in heavy traffic zones and during peak engagement times such as the holiday season.

The smartSD memory card also offers additional upselling opportunities with the availability of additional storage capabilities. The removable feature offers consumers the option to store content from other sources like a camera or another mobile device. At the service point, the content from these sources can also be used to generate commerce like the printing of high-resolution pictures at a photo kiosk.

The service provider could then communicate coupons and promotional materials based on the user activity. The presence of an SE in the smartSD memory card helps validate these upsell items both while dispensing and consuming them. The idea of a two-way communication between the SE host and the payment point expands the prospects for self-service at the kiosk. The limitations of the current contactless payment tokens are overcome with smart microSD memory cards.

Pairing of NFC and smartSD memory cards provides a secure and flexible way for transferring content and facilitates payment at self-service kiosks. This is an improvement on the current trend of fragmented services available to consumers. Providing the consumer with mobility, flexibility and security, smartSD technology can hasten the adoption of the mobile device as their payment source.

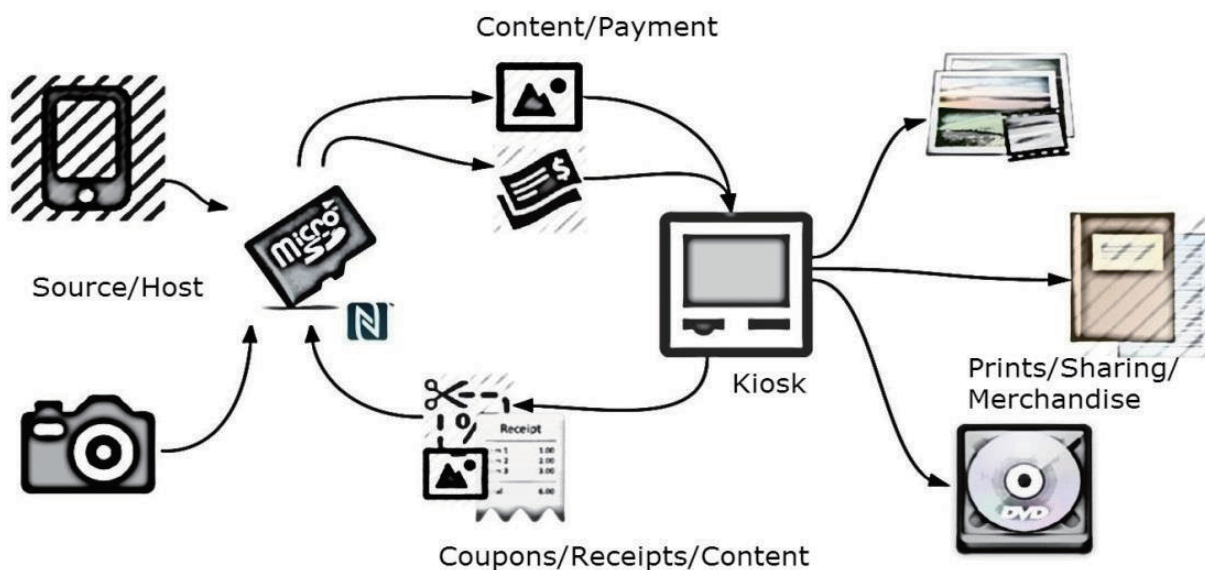
The GlobalPlatform Consumer Centric Model provides the technical framework to connect the token providers and the service providers in delivering a better retail experience for the consumers and the service providers and smartSD is perfectly adapted to take full advantage of this model.

Secure services for multimedia in consumer devices

smartSD memory cards also present a convenient approach to provide secure services such as payment or user authentication for HDTV sets, gaming consoles, ebooks and more.

For example, a smartSD memory card could be used in gaming to buy credits or additional game tools to move forward and faster in a game. It can also be used to authenticate the gamer for online multi-players games or to easily report success on social networks. Overall, the smartSD memory card helps protect identity theft, which is crucial for online gaming where virtual goods are traded.

In the case of HDTV, the smartSD memory card could be used to create a link between payment and a Digital Rights Management feature to grant access to multimedia content. This smart microSD memory card could be included with the television, allowing support of DRM systems from different content providers or with the download of a new DRM system. In that architecture, the DRM licensing cost is only paid when the smartSD memory card is present, allowing for lower upfront cost on the television for customers who are not interested in personal video recording.



Conclusion

The smartSD memory card is the most versatile solution available today to enable secure mobile services and to support contactless card emulation. It fits numerous use cases and brings value to both the service provider and the consumer. smartSD extends the universal, convenient and portable value of SD memory cards to secure applications and contactless communication services. smartSD memory cards present the most benefits to mobilize existing services as it fits with existing business processes and ensures business independence. Plus, a competitive and thriving ecosystem means smartSD memory cards are available for purchase from many SDA members.

All Copyrights and Trademarks referenced in this document are property of their respective owners.