Smart Card Alliance

Smart Card Talk

A quarterly newsletter for members and friends of the Smart Card Alliance

September 2014

The Mobile Industry: A Complicated Relationship

On cable television, there are a number of reality television programs with the word "war" in their titles. "Storage Wars," "Parking Wars," "Design Wars" and "Cupcake Wars" all tap into specific viewer interests. Mobile devices – namely their capabilities, features and owner expectations – elicit strong emotions in people, from consumers to industry professionals. Now that Apple has jumped into the payments space, I write more about the co-dependent relationships among mobile device manufacturers, network providers, merchants and payment networks – the "Mobile Wallet Wars" – in my letter in this quarter's Smart Card Talk newsletter. We also have an update on Alliance Councils, a Member Profile on Xerox, new CSEIP recipients, and more. Thank you for your interest and support of the Smart Card Alliance.

Sincerely,
Randy Vanderhoof
Executive Director, Smart Card Alliance

Click to Read Letter ...

Feature Article:
Host Card Emulation (HCE) 101

Host card emulation (HCE) has set the NFC industry abuzz with discussion of its potential and impact on the NFC applications. This month's article provides a primer on HCE and outlines how it differs from secure element-enabled NFC card emulation.

Click to Read More …

Member Profile:
Xerox

This quarter Smart Card Talk spoke with Michael Nash, Senior Vice President, Area of Focus: Public Transportation (Fare Systems), for Xerox. Mike leads global new business development initiatives for the company's public transit sector.

Click to Read More …

In This Issue:

② Executive Director Letter >>
③ Latin America Letter >>
④ Member Profile >>
⑥ Feature Article >>
⑩ Council Reports >>

On the Web:

Alliance in the News >>
Members in the News >>

Smart Card Alliance Events

2014 Government Conference-Smart Strategies for Secure Identity
October 29-30, 2014
Walter E. Washington Convention Center, Washington, DC

Smart Card Alliance Member Meeting
December 7-9, 2014
Rosen Shingle Creek, Orlando, FL

Smart Card Alliance 8th Annual Conference 2015 Payments Summit
February 3-5, 2015
Grand America Hotel, Salt Lake City, Utah

Industry Events

GlobalPlatform Presents: The Trusted Execution Environment (TEE): Next Generation Mobile Security for Today and Tomorrow
September 30, 2014
Santa Clara, CA
http://www.teeseminar.org/

Money 20/20
November 2-5, 2014
Aria, Las Vegas
http://www.money2020.com/register
Discount code for Smart Card Alliance members: SMARTC20

Cartes
November 4-6, 2014
Paris Nord Villepinte Exhibition Centre
http://www.cartes.com/

All Upcoming Smart Card Alliance Conference Events

The Mobile Industry: A Complicated Relationship

Dear Members and Friends of the Alliance,

Three major developments in the mobile wallet and mobile payments markets last week have sparked renewed speculation around the complicated and co-dependent relationships among the mobile device manufacturers, mobile network operators, merchants, and the payments networks. First I'll cover the news surrounding the iPhone 6 and its NFC capabilities, and then I'll address the re-awakening of Merchant Customer Exchange (MCX) and the recent update revealed by MCX CEO Dekkers Davidson. I'll close with some thoughts on Isis' rebranding of its mobile wallet as Softcard, and how perhaps all of these things are loosely tied together.

By now everyone is aware that Apple has finally jumped into the NFC mobile payments market using a secure element. This is a burst of energy for the fledgling mobile payments industry, since the iPhone commands a 41% market share in the U.S. and loyal iPhone customers are ready to upgrade after the iPhone 5 and 5s disappointments. What was more intriguing was learning how they will use an individualized payment account token stored on the phone that can be linked to Apple's 800 million iTunes accounts on file and how they have established an agreement with American Express, MasterCard and Visa, and several large issuing financial institutions -- that collectively represent a large percentage of those card relationships -- to extend card-present rates for ApplePay transactions.

Apple did not break new ground with its use of NFC to transact payments on a mobile phone. Nor are they the first to use a token stored on the phone linked to a payment source in the cloud. What they have done is raise the bar on payment security by adding a layer of user authentication to the transaction by incorporating the iTouch biometrics reader into the transaction and bundled this with dynamic data that can include location and time-based elements with a tokenized account number. Those three elements together are far superior to any current card or mobile transaction. The payments brands and issuers are reportedly rewarding Apple's security efforts by lowering the risk-based interchange fees and rebating some of that lower fee to Apple. Merchants should be pleased that they don't have to do anything more than enable the contactless features on their new EMV-capable terminals to interface with iPhone 6 customers and the payment data in their system will be safe from criminals.

Apple has taken care of the security and has brought its massive customer base to the mobile marketplace. They have also engaged the payments networks and issuers in a positive way. The success of the ApplePay wallet now lies in its ability to get merchants engaged. The chicken-and-egg analogy hasn't changed much in the last five years of mobile adoption. EMV cards have been largely contact only and although the re-terminalization process is underway at retail locations across the country, it is still unclear if and when a large number of merchants will enable the contactless features on those devices when they activate EMV. Also, the big merchants are already heavily invested in making MCX successful and are going to be conflicted as they try to get consumers to favor the MCX-branded CurrentC mobile payment solution. So far, Apple is offering a payments-only mobile application, with none of the mobile offers and redemption components that have been of more interest to merchants than another payments option.

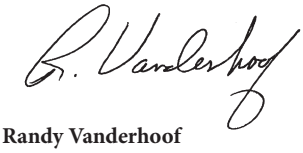
I'm left wondering if there is another move coming that will enable iPhone users to take advantage of the iBeacon Bluetooth low energy devices that can push messages to iPhones and interface with retailer systems to host a variety of merchant to consumer interactions instead of relying on payments alone to be the value proposition. Or perhaps a next move will have something to do with NFC tags or social media involving iTunes, photos, or gaming apps. We should know more soon.

The unexpected timing of the MCX revelations – after nearly a year of silence and just ahead of the Apple release and reported agreement with the payment brands – makes me think that they are concerned that something big is about to happen. It appears to be a defensive move to keep the attention of the media while buying more time for a likely mid-2015 launch, because pilots were rumored to be underway in early 2014. I suspect they are struggling with the complexities of building a new alternative network while addressing the competing interests of security, scalability, and interoperability – and offering the service at a lower cost. The brand name of CurrentC is a peculiar choice since it sounds like more of a cash replacement than a payment card alternative.

Finally, the announced rebranding of the Isis mobile wallet to Softcard makes a statement that the AT&T, Verizon and T-Mobile joint venture still has some legs as they maneuver complicated waters. They're up against issuer indifference based on hopes for a lower-cost HCE option on the horizon, nonexistent dual-interface or contactless EMV issuance by major financial institutions, and slow pace of merchant activation of NFC at the point of sale. The name Softcard indicates that they are opening themselves to the possibility that payments may be delivered with a token on the device or in the cloud, rather than only as a hardware-based stored token. Depending on Apple's next move, we will learn whether Softcard will have to compete with another wallet within the same mobile operator customer base or if Softcard will be compatible with the iWallet innovation and the NFC interface available for either choice for payment.

Both MCX and Softcard, not to mention Google Wallet, are going to have to step up their game or risk being overrun by an Apple tsunami. These and many other questions will be asked and answered over the next few months and the 2014 Money 20/20 event in November in Las Vegas may be a true "Clash of the Titans" event for these mobile wallet wars.

Sincerely,



Randy Vanderhoof
Executive Director, Smart Card Alliance
rvanderhoof@smartcardalliance.org

Florida State University Partners with SCALA To Develop Training Programs in Latin America

Dear Members and Friends of the Smart Card Alliance Latino America – SCALA:

Florida State University (FSU) – Panama and the Smart Card Alliance Latin America (SCALA) have signed a five year agreement for the development of an industry Integrated Circuit Card (ICC) Center of Excellence for the expansion of smart card based educational programs for Latin America and the Caribbean. The Center will help develop industry executives on related smart card technology, through education, certification, and hands-on-training. It will also be a place for experts and professionals from the financial, government, identity, security, transportation, healthcare, telecommunications, M2M, and other sectors to learn about the latest advancements in technology.

FSU – Panama is the first University in the region that will place its best and brightest students in the Center of Excellence. The students will work with industry leaders to develop their knowledge and awareness of smart card technology and explore opportunities for smart card technology in the region. They will have the opportunity to develop white papers, use cases, market trends, research, reports, studies, and other resources that will be published for leading industry companies.

The partnership will help SCALA increase the number of available educational resources and training materials in the marketplace. The deliverables developed in the Center of Excellence will raise the awareness of the benefits that smart card technology can offer. Lastly, it will allow students to experience firsthand the technological applications and help to introduce related subjects into the classrooms.

In the initial stages of this partnership, all training programs will be based on our existing platforms and certification programs including: ***Smart Card Fundamentals; Leadership Education, Advancement Program (LEAP); and Certified Smart Card Industry Professional (CSCIP)***. As more specialized training programs are required by the market to cover technological advances and other vertical markets, so will additional certification programs be created by SCALA.

Some news article references on establishing this partnership can be found in **Mobile Commerce Insider**, **SecureID News** and **Security Document World**.

SCALA has a video available of the signing of the agreement, which documents this landmark partnership between industry and academia. The video features Fernando Mendez, Chairman of the Board of SCALA / VP of Emerging Payments at Visa Inc.; Dr. Carlos Langoni, Rector of FSU – Panama; Edgar Betts, Director of SCALA; Rolando Armuelles, VP of Business Development at The City of Knowledge; and Enrique Tellez, Senior Commercial Specialist at the U.S. Embassy of Panama.

To watch the signing video visit: http://www.sca-la.org/scala-and-fsu-panama-create-comprehensive-center-of-excellence/

In the past years, Latin America and the Caribbean markets have seen significant growth in the use of smart card technology, pioneering the implementation of EMV payment cards, transit fare cards, SIM cards – mobile, e-passports, secure government identification, and other vertical industry application. The region, which includes over 20 countries, is a market that has been driving complex applications, security, interoperability, and convergence.

This has driven member organizations to develop more cooperative structures for their executives, who had focused on different vertical markets and in different parts of the region, to work together to develop solutions for their clients, blurring the lines of market segments and single application cards.

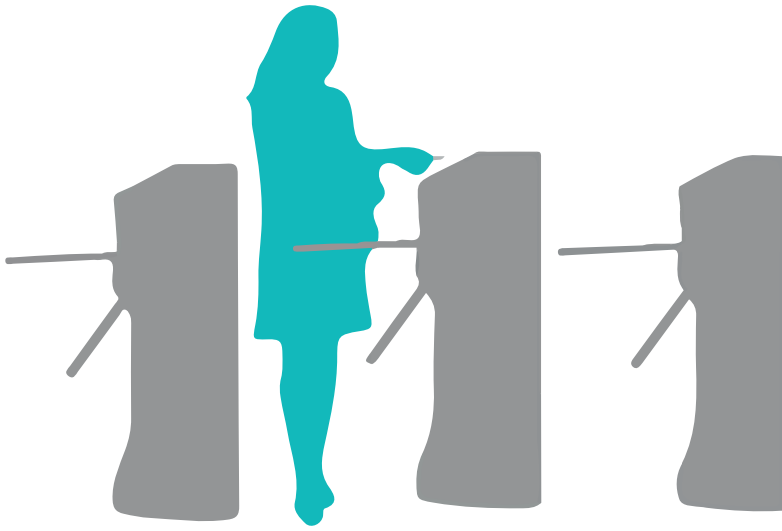
New professionals who have developed an enhanced ability to identify synergies between different vertical markets and create convergence will find that they have a head start in their careers in smart card related industries. The Center will provide them with some of the necessary tools to understand market and technological complexities to develop successful implementations in the region.

As a result, the Center of Excellence and SCALA will be aligned with their mission to promote innovation, interoperability, education, convergence, and widespread application of smart card related technologies in Latin America and the Caribbean.

If you would like further information, please contact us at scala@smartcardalliance.org or visit: www.sca-la.org

Sincerely,

Edgar Betts
Director
Smart Card Alliance Latin America (SCALA)
ebetts@smartcardalliance.org
www.sca-la.org



Michael Nash

This quarter Smart Card Talk spoke with Michael Nash, Senior Vice President, Area of Focus: Public Transportation (Fare Systems), for Xerox. Mike leads global new business development initiatives for the company's public transit sector. With significant knowledge of the transportation and financial services industries, Mike brings a unique combination of payment network and transit fare collection experience which he used to develop a viable open payment fare system approach. Prior to Xerox, Mike worked at ERG Transit Systems, where he held executive level positions responsible for all operations and maintenance activities across the organization including operations for some of the world's most well-known fare systems such as Hong Kong, Singapore, San Francisco and Washington D.C. Mike's tenure in electronic payments includes global leadership roles at American Express, and while at Visa, he initiated payment programs which were precursors to today's prepaid market.

1. What are your main business profile and offerings?

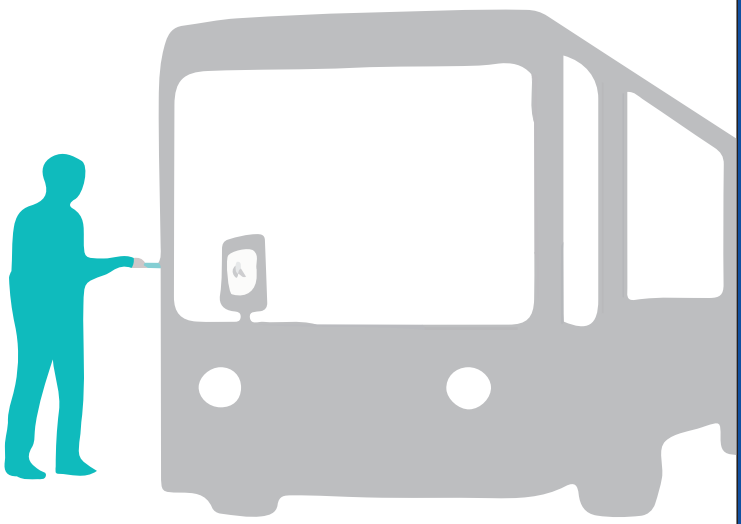
Xerox offers business process outsourcing and IT outsourcing services, including data processing, healthcare solutions, HR benefits management, finance support, transportation solutions, and customer relationship management services for commercial and government organizations worldwide. The company also provides extensive leading-edge document technology, services, software and genuine Xerox supplies for graphic communication and office printing environments of any size. We serve clients in more than 160 countries, and are the world's leading enterprise for business process and document management services.

2. What role does smart card technology play in supporting your business?

Smart cards are a key component of all current transit fare payment contracts. We took an early lead in supporting smart-card-based systems by implementing the first open payment smart card fare system in North America in Gatineau, Quebec and followed years later with the first multi-agency open payment fare system, the NY/NJ Transit Trial. We are continuing with solutions using open standards and open payments systems approaches. We also support traditional fare collection systems around the world that use card-based technologies that are dependent on smart cards.

We use our expertise to support ISO standards committees in developing new standards for smart card technology. Smart cards provide the security and speed needed to support modern fare collection and play a vital role whether the technology is in a card, other device or a mobile phone.

> **“Educating about the technology, financial system infrastructure and its use, its costs and benefits, and consumer adoption is critical since objective information can help demystify the transition.”**



3. What trends do you see developing in the market that you hope to capitalize on?

The movement to open payment standards is a major factor in the market today. The use of contactless bankcards, ID cards and other compliant devices to identify riders as eligible to enter the transit system is fast growing as it is a much more efficient form of fare payment than older approaches. This trend will continue as the impact has changed the IT environment from closed, proprietary fare collection systems to a modern, open architecture solution that can evolve with time to accommodate innovation. The use of NFC phones, Bluetooth Low Energy, and QR code tickets can be easily accommodated in this typology making it more popular and enduring.

4. What obstacles to growth do you see that must be overcome to capitalize on these opportunities?

There remain a number of myths and misunderstandings about contactless cards and the complexity of change from closed proprietary systems to open architecture IT solutions that can support developing intelligent transportation solutions. Educating about the technology, financial system infrastructure and its use, its costs and benefits, and consumer adoption is critical since objective information can help demystify the transition. Change is complex and misinformed people can add unnecessarily to the problem.

5. What do you see are the key factors driving smart card technology in government and commercial markets in the U.S.?

Smart cards provide security and privacy for transactions and improved collection of data. Smart cards can provide solutions that empower consumers to protect their data and privacy from unwanted intrusion. As in fare collection and the transition to EMV chip card processing where fast, efficient payments that are also secure are important, other industries can benefit from this technology.

6. How do you see your involvement in the Alliance and the industry councils helping your company?

The Smart Card Alliance and the Transportation Council have been instrumental in providing white papers and other forms of education that are developed by industry experts. This objective source can be invaluable.

7. What are some of the challenges you see confronting the smart card technology industry?

Challenges stem from meeting the growing needs of multiple industry verticals, as they are converted to smart-card-based systems from less secure technology.

Member point of contact:

Michael Nash
SVP, Emerging Markets
650-812-4997
Michael.Nash@xerox.com

Host Card Emulation (HCE) 101

Near Field Communication (NFC) is a short-range wireless (RF) communication technology for smartphones and similar devices that enables data transfer between the devices. NFC operates at 13.56 MHZ, complies with the ISO/IEC14443 and ISO/IEC18092 standards, and MIFARE and FeliCa specifications,and operates in ranges of less than 10 cm. [1]

NFC, in conjunction with a mobile wallet or a use-case-specific application (app), is used for a variety of applications, such as payment, ticketing, access, RFID tags, loyalty, and coupons, as well as in consumer electronics. Currently, NFC-based applications that use the card emulation mode (i.e., where the reading terminal effectively sees the mobile phone mimicking a traditional contactless smart card and no change to the reading infrastructure is required) require the card application (e.g., payments, ticketing, access control) and its credentials (e.g., account information, ticket, access identifier and tokens) to be stored inside a hardware-based secure element (SE) on the mobile device.

Host card emulation (HCE) enables NFC devices to perform contactless transactions in card emulation mode when the payment, other credentials and related card applicationsare stored somewhere other than the SE: e.g., in the cloud, in a trusted execution environment on the mobile device, or in a virtual, software-based infrastructure on the mobile device. Google's adoption of HCE in the Android operating system (OS) v4.4 (KitKat) has created a new market opportunity for solution providers and issuers to implement and deploy NFC solutions, removing both dependencies on the secure element and trusted service manager (TSM) infrastructure and the need to set commercial agreements with secure element issuers.

Current NFC Support

The availability of NFC-enabled mobile devices continues to grow, with NFC included in over 345 million devices shipping in 2013. [2] According to NFC World [3], over 50 manufacturers support NFC in over 200 phone models and tablets. Although Apple mobile devices do not currently support NFC, NFC capability can be added to iPhones through commercially available cases and accessories.

Numerous NFC-enabled payment, marketing, ticketing, and other applications have been implemented globally.[4] In the United States, the most prominent NFC mobile payment services are offered by Isis and Google.

Isis [5], the mobile carrier joint venture that includes AT&T, Verizon, and T-Mobile, offers the Isis Wallet, which supports mobile payments, loyalty programs, and offers. A total of 68 mobile phones support NFC and the Isis Wallet [6]; consumers with an iPhone must use an Isis Ready case.[7]Consumers set up an American Express Serve account or add participating American Express, Chase, or Wells Fargo cards to the Isis

Wallet. The Isis Wallet can then be used to pay at any merchant accepting contactless payment. Isis stores the payment applications and account information in the SE that is built into the mobile phone's hardware.

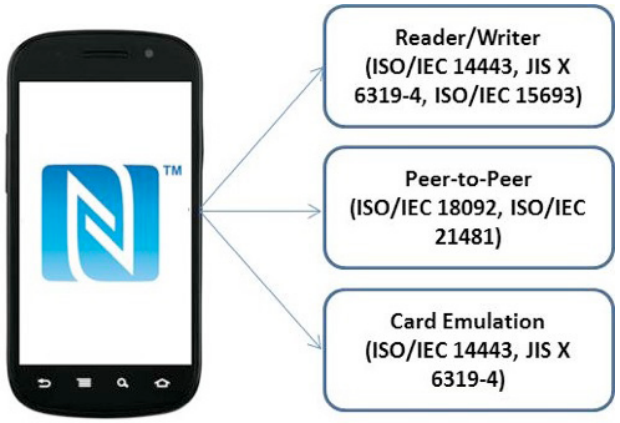
Google,in partnership with Sprint, introduced the Google Wallet in 2011. Google Wallet supports payment, loyalty, money transfer, offers, and online order tracking. In the latest version of the Google Wallet, the payment functionality requires an NFC-enabled device running Android 4.4 (KitKat) or higher on any carrier network. [8] The initial Google Wallet implementation relied on an SE in the mobile phone's hardware; Google has since changed directions, using HCE with payment credentials stored in the cloud. When the consumer taps the phone, HCE enables Google Wallet to pass transaction information to the point-of-sale (POS) terminal to complete the transaction. [9]

NFC Operating Modes

The NFC Forum technical specifications define three NFC operating modes: reader/writer, peer-to-peer, and card emulation.

Reader/writer mode enables NFC devices to read and write information to NFC tags (e.g., in posters or advertisements). In this mode, NFC devices can read NFC Forum-mandated tag types, which are compliant with the NFC-A, NFC-B, and NFC-F specifications.

Figure 1. NFC Operating Modes



Peer-to-peer mode enables NFC devices to exchange data and share files. Peer-to-peer mode complies with ISO/IEC 18092 and may use the NFC Forum's Logical Link Control Protocol specifications to enable bidirectional data transfer.

Card emulation mode enables NFC devices to function as contactless smart cards complying with the ISO/IEC 14443 standard and FeliCa specification. Consumers can conduct transactions such as purchasing, ticketing, and accessing transit with a tap of the device. NFC-enabled devices complete contactless transactions using the current contactless acceptance infrastructures.

Figure 1 summarizes the three NFC operating modes and their related standards.

Card Emulation Mode

In card emulation mode, a mobile device can emulate any contactless smart card (such as those used for contactless payments, transit fare payment and building or hotel room access) when tapped on a contactless reader or POS terminal.

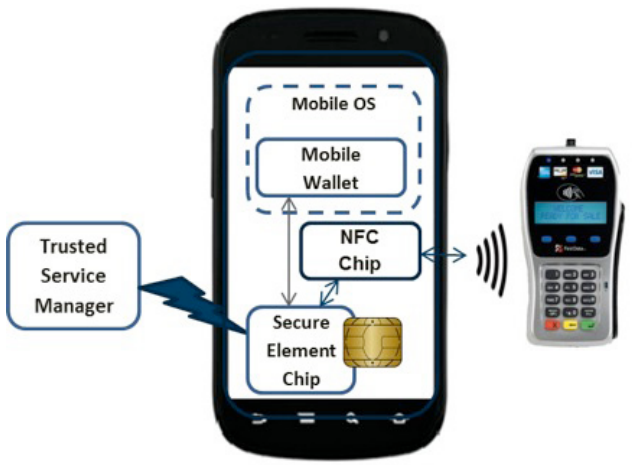
Until recently, the virtualized contactless card application and associated credentials were always stored in an SE, defined by GlobalPlatform as: "a tamper-resistant platform (typically a one-chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g., key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities."

HCE opens up the possibility of storing the virtual contactless card application as a service running on the mobile device operating system. This option is supported today by Google's Android OS (v4.4 "KitKat" onwards) and by the Blackberry OS.

SE-Enabled Card Emulation

With SE-enabled card emulation, the NFC controller routes the communication from the contactless reader or POS terminal to a tamper-resistant dedicated hardware component called the SE. The SE safely stores the card emulation application and associated credentials.

Figure 2. SE-Based NFC Card Emulation



All NFC-enabled mobile devices implement the capability to allow SEs to:

1. Communicate with the NFC controller, and through it, with contactless readers to perform transactions.
2. Communicate with user-interfacing mobile applications running on the mobile device operating system, such as mobile wallets.
3. Communicate over-the-air with the credential provisioning infrastructure, called the TSM.

Figure 2 illustrates the mobile device architecture for SE-based NFC card emulation.

The secure element can reside in an embedded secure smart card chip on the handset, on the Subscriber Identity Module (SIM) or Universal Integrated Circuit Card (UICC), or on a secure digital (SD) card that can be inserted into the mobile phone. SIMs and UICCs are issued by the mobile network operators (MNOs) and embedded SEs are issued by mobile device manufacturers. SEs on microSD cards can be issued by any application provider.

When credentials are stored in the SE, they are provisioned by an entity known as a TSM. Provisioning theNFC SE application and relatedcredentials requires cooperation and integration among multiple entities, which may include issuers, wallet providers, MNOs, payment processors, TSMs, and other members of the ecosystem.

Credentials stored in anSE are stored in security domains that adhere to GlobalPlatform specifications. Each service provider or issuer is assigned a specific domain, and each domain is protected by cryptographic keys that are known only to the participants, protecting them from any unauthorized access. During a payment transaction, the mobile wallet application authenticates itself to the SE, typically through a PIN or password, key, or digital signature, to enable transmission of the credentials to a contactless POS terminal or other acceptance device.

Host Card Emulation

HCE introduces an option for the NFC controller to now additionally route communication from the contactless reader or POS terminal to an HCE service on the mobile device's host CPU. With HCE, an 'APDU Service' running on the host can interface with a contactless reader via NFC. This HCE service can be part of a mobile application with a user interface, such as a mobile wallet for payment. The credentials used by this HCE service can be stored in the application itself, or they could be stored in other secure locations such as a trusted execution environment (TEE) or an SE.

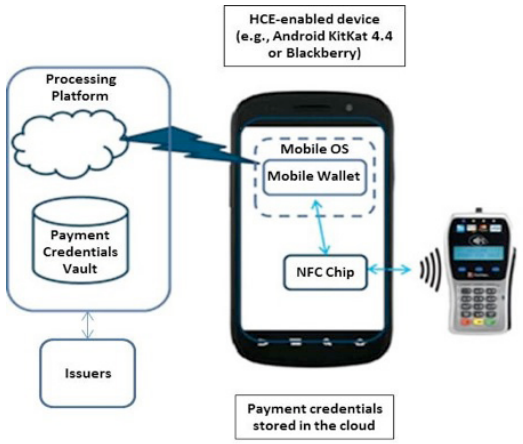
Alternatively, the HCE service could connect in real-time or at given intervals with a back-end server in the cloud to retrieve credentials to exchange with the contactless terminal. Real-time retrieval of credentials from the cloud at the moment of tapping on a reader is a possible but unlikely option, as network latency may result in a poor user experience.

Figure 3 illustrates this process for a payment app.

HCE and Security Considerations

When an app uses HCE, communications with the contactless terminal are no longer routed tothe SE but through the NFC controller to the mobile device's host CPU on which the app is running. This change introduces certain risks.

Figure 3. Obtaining Credentials from the Cloud Using HCE



Communication between the NFC controller and the HCE-enabled app can be spied on by malware applications. Malware applications can attack the operating system, a risk which is exacerbated when the handset is compromised by exploiting, rooting or jailbreaking. The malware itself may also be able to exploit, root or jailbreak the device, or spoof the user into initiating such actions. In addition, denial of service attacks can take place if routing is changed by a malware application. More generally, cloud storage and backup servers can be attacked, as can credentials stored in applications that are used to gain access to cloud storage and backup servers.

HCE implementations need to consider the security requirements for the applications and take risk mitigation approaches to bolster the security of HCE implementations. Approaches could include: white box cryptography; tamper proofed software; biometric factors; device identity; use of a trusted execution environment; encryption; tokenization; and/or use of the secure element.

Conclusions

Of the three modes NFC offers for mobile devices, card emulation has been the most popular, and also the most controversial, mode, due to the need to access the secure element that is owned and controlled by another party. HCE significantly changes card emulation implementation requirements and introduces entirely new business plan considerations for service providers and issuers wishing to use their credentials for NFC use cases.

Along with the greater flexibility HCE offers for service providers and issuers, comes advantages and trade-offs to the traditional SE model and accompanying (required) ecosystem. Some advantages include more direct control and fewer dependencies on other ecosystem players. Some disadvantages include a less secure implementation and, possibly, a degraded end user experience in some cases. The list of advantages and trade-offs will change as more HCE-based solutions are deployed, tested and used in commercial practice.

In summary, NFC continues to gain strong industry support from an increasing number of suppliers, manufacturers and handset models; however, HCE currently is only commercially supported on Android and Blackberry, and specifications still need to mature and be harmonized across OS vendors. While HCE is not the 'silver bullet' many would like to have, it has far-reaching implications for the industry in general. Further, HCE introduces an attractive option and welcome solution for those service providers and issuers whose business models do not require, or cannot thrive within, a traditional secure element-based implementation.

References and Notes

[1] Additional information on NFC can be found on the NFC Forum Web site, http://www.nfc-forum.org.
[2] ABI: Smartphones accounted for 80% of the NFC devices shipped in 2013, *NFCWorld+*, Jan. 8, 2014.
[3] NFC phones: The definitive list, *NFCWorld+*, May 11, 2014.
[4] Additional information can be found at http://www.nfcworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/.
[5] A Message from Michael Abbott: Embarking on a New Brand, July, 7, 2014.
[6] Isis Reports 600K New mWallet Downloads In The Last Month, May 14, 2014, PYMNTS.com.
[7] Isis, http://www.paywithisis.com.
[8] Google, https://support.google.com/wallet/answer/1347934?hl=en.
[9] Google Wallet FAQ, http://www.google.com/wallet/faq.html#tab=faq-security.

About this Article

This article is an extract from the white paper, "Host Card Emulation (HCE) 101," published by the Smart Card Alliance Mobile and NFC Council in August 2014. The white paper was developed to provide an educational resource on HCE, describing what it is, how it's used, how it compares with the secure element-based card emulation approach, what key considerations are for payment applications, and what security aspects should be considered for HCE-enabled applications.Member organizations involved in the development and review of this white paper included: ABnote Group; Advanced Card Systems Ltd.; BetterBuyDesign; Capgemini USA Inc.; CH2M Hill; Clear2Pay; CorFire; Cubic Transportation Systems; Discover Financial Services; Eid Passport Inc.; First Data Corporation; Fiserv, Inc.; Gemalto; Giesecke & Devrient; HID Global; HP Enterprise Services; Identiv; Ingenico; Initiative for Open Authentication (OATH); INSIDE Secure; Intercede; IQ Devices; Isis; MasterCard; Morpho; NXP Semiconductors; Oberthur Technologies; OTI America; Thales e-Security; Underwriters Laboratories (UL); Valid USA; VeriFone.

Updates from the Alliance Industry Councils

Access Control Council

- The Access Control Council submitted comments to NIST on the second draft SP 800-73-4 in June and comments to GSA on the FIPS 201 Evaluation Program Functional Requirements & Test Cases (FRTC) version 0.1.3 in July.
- The Council is working on a project to develop a guide specification for architects, engineers, consultants, integrators, manufacturers and end users that would allow them to easily incorporate smart card-based PACS cards and readers into the A&E specification for non-government PACS.

Health and Human Services Council

- The Health and Human Services Council is working on a new white paper on patient identity.

Identity Council

- The Identity Council is collaborating with the Access Control Council on defining the statement of work for a white paper on the benefits of using a single smart card for physical and logical access.

Mobile and NFC Council

- The Mobile & NFC Council published the white paper, "Host Card Emulation (HCE) 101." The white paper was developed to provide an educational resource on HCE, describing what it is, how it's used, how it compares with the secure element-based card emulation approach, what key considerations are for payment applications, and what security aspects should be considered for HCE-enabled applications. Sree Swaminathan, First Data Corporation, led the project. Member organizations involved in the development of the white paper included: ABnote Group; Advanced Card Systems Ltd.; BetterBuyDesign; Capgemini USA Inc.; CH2M Hill; Clear2Pay; CorFire; Cubic Transportation Systems; Discover Financial Services; Eid Passport Inc.; First Data Corporation; Fiserv, Inc.; Gemalto; Giesecke & Devrient; HID Global; HP Enterprise Services; Identiv; Ingenico; Initiative for Open Authentication (OATH); INSIDE Secure; Intercede; IQ Devices; Isis; MasterCard; Morpho; NXP Semiconductors; Oberthur Technologies; OTI America; Thales e-Security; Underwriters Laboratories (UL); Valid USA; VeriFone. The white paper is available at: http://www.smartcardalliance.org/publications-host-card-emulation-101/.
- The Council is now discussing member input on project priorities for the second half of 2014.

Payments Council

- The Payments Council has three active projects: a white paper on EMV and data breaches; a white paper on the "true cost" of data breaches; and a white paper on EMV, tokenization and encryption. Project teams are now drafting and discussing content.

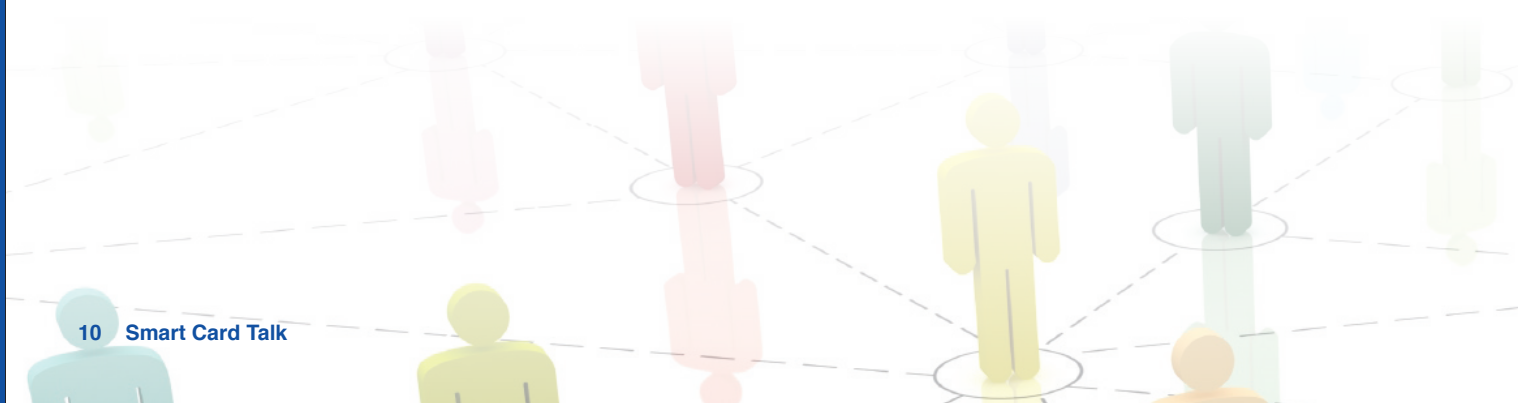
Transportation Council

- The Transportation Council has several active projects: EMV impact on parking white paper; EMV and transit white paper; transit/payment brand project on challenges with open payments.

Other Council Information

- All Smart Card Alliance Industry Councils will be holding elections for their 2015-2016 Steering Committees this fall. If you're not already active in the Councils, this would be a great time to get involved and play a leadership role in the Alliance industry activities. If you're interested in participating in a Council or nominating yourself or another individual for a Council Steering Committee, contact Cathy Medich.
- Members-only council web pages were updated and are available at http://www.smartcardalliance.org/councils. These are password-protected pages that contain council working and background documents and contact lists. Each Council area has a separate password since Councils may have different membership policies. If you are a Smart Card Alliance member and would like access to a council site, please contact Cathy Medich.

Alliance Members: Participation in all current councils is open to any Smart Card Alliance member who wishes to contribute to the council projects. If you are interested in forming or participating in an Alliance council, contact Cathy Medich.



Welcome New Members

- Capgemini USA Inc., Leadership Council (formerly General Member)
- ESQ, Latin America Associate
- TS1 Solutions, Inc., General

Congratulations New CSEIP Recipients

- Steve Bowen, Eid Passport Inc
- Malcolm Caesar, Global Networks Inc.
- Tachung Chang, Integrated Security Technologies, Inc.
- Jesse Devitte, XTec, Incorporated
- Colin Doniger, DHS OSCO
- Jason Goodloe, XTec, Incorporated
- David Helbock, XTec, Incorporated
- Jorge A. Lozano, Condortech Services, Inc.
- Michael Margolis, Integrated Security Technologies, Inc.
- John Placious, Integrated Security Technologies, Inc.
- Blake Smith, Gallagher Group Limited
- Lars Suneborn, Smart Card Alliance
- Shawn Zartman, Integrated Security Technologies, Inc.

For more news, visit our website at www.smartcardalliance.org.
Members can also access white papers, educational resources and other content.

Smart Card Alliance

191 Clarksville Road
Princeton Junction, New Jersey 08550
1.800.556.6828
Fax: 1.609.799.7032
info@smartcardalliance.org
www.smartcardalliance.org

About Smart Card Talk

Smart Card Talk is the monthly e-newsletter published by the Smart Card Alliance to report on industry news, information and events and to provide highlights of Alliance activities and membership.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.