Dear Members and Friends of the Alliance,

In preparation for the upcoming NFC Solutions Summit Conference on May 15-16, I have been talking with a lot of industry insiders who have very diverse views about the future of NFC. These conversations ranged from declarations that 2013 is going to be the “year of NFC” to projections that NFC is an old technology that has already missed its opportunity with consumers. Can both points of view be correct?

My feeling is yes, they both can be correct. And I say this by disclosing up front that I do not have any superpowers that can see through solid walls (or board rooms) or get inside the minds of the leaders of smart phone manufacturers, mobile networks, or consumers. My letter in this month’s issue of Smart Card Talk lays out the situation and how I arrived at my conclusion. I’d love to hear your feedback; please feel free to contact me. I always appreciate a good discussion of our industry. Thank you for your support of the Smart Card Alliance.

Sincerely,

Randy Vanderhoof
Executive Director, Smart Card Alliance
Acting Director, EMV Migration Forum

Click Here to Read Letter ...
Dear Members and Friends of the Alliance,

My prediction that 2013 is going to be the “Year of NFC” is based on simple common sense, which is only a good thing if the forces shaping the mobile markets today are common at all. I’m going to dive right in and say that NFC will be the thing mobile analysts and industry experts will be talking about in 2013, and what they’ll say about the “missed opportunity” will likely refer to NFC payments, at least in its purest form of widespread proximity mobile wallet-enabled transactions.

There are a couple of factors that have helped form this opinion. One of them is the belief that the “wow factor” that is expected to drive consumer demand, and likewise, issuer and merchant investment, is overrated for NFC payments. More than two months ago I got my personal phone activated with an NFC wallet in it – but I still haven’t used it. I was excited about getting it; it’s not that I couldn’t use it, but it just doesn’t seem that important to me right now. I went through the personal “wow factor” already with contactless cards and stickers and using my new mobile wallet – which only allows me (today) to link one of my business credit cards to it – is not very motivating. I shop far more frequently with my personal cards. I can also tell you that I have no desire to use my phone to pay with my PayPal account or download a Starbucks loyalty application to buy my mocha latte either.

What does excite me more than using a mobile wallet to buy something in a store is the idea that, in 2013, I may be able to own a laptop that has NFC baked inside that will let me easily pay online rather than needing to fill out those tiresome online check-out forms. The announcement last month that Lenovo was going to include NFC in its ThinkPad laptops in 2013 really can have a big impact. It solidifies NFC as a hardware platform for fast, secure personal transactions and breaks the bindings that restrict NFC to payments schemes controlled by mobile network operators. With my own NFC phone and my own NFC laptop (or Ultrabook notebook or tablet), I can control my own NFC universe. I can create links to launch my favorite web pages or log into my personal banking accounts. I can have fun with it and get more security at the same time. These non-smart-phone devices are not available in large numbers yet, but 2013 might be the year for it.

Another cool breakthrough I read about recently was a company named Adspace Networks that operates advertising displays in 140 malls around the country. They are going to NFC-enable ad displays and allow consumers to touch the display and open a web site, download a audio or video trailer for a movie or a concert, or get a mobile coupon for the nearest store in that mall. We are not talking about payments here, just an interactive marketing experience you can do with any NFC phone. I can see young mall walkers going to every smart display just to experience what it has to offer.

So, in this roundabout way, I have tried to make my point that NFC is going to a “big thing” in 2013. It may also be true that this “old” technology has missed out on its opportunity with consumers like me for at least one main usage – that is NFC payments. We need to move the discussion and the investment in NFC to those things which consumers can’t do today with a mobile phone. I know people will want to point out that QR codes can do most of what I just said was really cool. I would argue that once you put both applications side by side, NFC is going to come out on top in nearly every case – if just for the situations that will fail due to poor network connections or camera issues. I am putting my bet on Lenovo, Dell, Intel, Samsung and other technology giants seeing the potential that goes way beyond payments for NFC.

If you attend the 2013 NFC Solutions Summit on May 15-16th, you will learn more about the changes that are happening across the NFC technology and business services front for increasingly large scale deployments of products and services coming this way. No doubt there will be contrasting opinions about what lies ahead in 2013 and what has already passed the market by. Can they both be right? Yes they can.

I hope to see you next month at the event.

Sincerely,

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

The Future Is Now
Industry Advocacy

Dear Members and Friends of the Smart Card Alliance Latin America & the Caribbean,

This month, I would like to elaborate on SCALA’s role as an industry advocate for smart card technology. The term “advocate” is easily confused by many in Latin America due to the difficulty of finding an accurate translation. While the word “promotion” may seem accurate when translated to Spanish, there are aspects of SCALA’s advocacy that go beyond the promotion of the technology.

Wikipedia defines *advocacy* as “a political process by an individual or group which aims to influence public-policy and resource allocation decisions within political, economic, and social systems and institutions.” In SCALA terms, it is our attempt to influence key decision makers through educational materials, impartial information, use case experiences, and open forums that point out the advantages smart card technology offers.

In the Latin American and the Caribbean markets many technologies compete with smart card technology and provide an alternative for identification, authentication, and verification. In some cases, such as biometrics, the technology can be complimentary to smart cards. When used by itself, biometrics can generate difficulties in identification due to the requirement of needing a large centralized database. The use of smart cards with biometrics can help increase accuracy in identification, allowing for biometric verification on a one-to-one basis.

Identity cards and centralized databases are widely used by federal governments and agencies in Latin America and the Caribbean. The majority of countries in this region have a national ID card that consists of a simple plastic card with a picture, a unique ID number, and a barcode known in Spanish as “cédulas.” Citizens use this plastic card and the barcode to obtain benefits such as public healthcare, social security, voting rights, and other social benefits. But it is also valuable to non-citizens who can try to use it to take advantage of the system fraudulently.

Non-smart-card technologies that are used for identification may be considered less expensive or troublesome on the surface – especially when looking at initial costs and disregarding the risk and cost of fraud, counterfeit cards, and benefits paid for fraudulent claims.

Alternative technologies to smart cards focus on initial costs vs. longer term benefits, and represent a major challenge for governments and the pace of development of the country, state, city or region they govern. One of SCALA’s main goals is to provide the educational tools necessary for organizations to understand smart card technology and the benefits this technology offers that exceed the value-benefit relationship of other technologies.

SCALA reaches out to different government agencies and industries, prepared with white papers, industry experts, and educational materials, to help government executives and private industry leadership learn about the value-added benefits that smart card technology can offer beyond other existing technologies.

This is why SCALA advocates the introduction of smart card technology for government ID over less secure technologies such as laminated cards, barcodes, or magnetic stripes. Our responsibility is to demonstrate the vulnerabilities of other technologies and the additional benefits and opportunities smart card technology can offer -- such as digital verification, multiple applications, offline transactions, encryption, and variable communication methods. It is our technology that serves as a counterfeit-proof secure element for identity verification and that is able to ensure ID authenticity to authorize social benefits or be used as an authentic document to apply for other privileged government IDs such as a driver’s license.

A good example of the type of activities that SCALA delivers to benefit those in charge of public policy is the Government Information Exchange Program. The objectives of these exchanges are to increase the visibility of smart card technology within governments and present government agencies with successful cases of implementation of the technology for different applications that affect public policy. The demonstration of how these use cases relate to their specific situations is another key aspect of the Government Information Exchange Program. This is accomplished through the use of compelling and clear educational material along with presentations from industry experts that cover how smart card technology can relate to public policy – for example supporting a wide variety of applications such as corporate identification, government identification, healthcare, driver’s licenses, resident cards, passports, healthcare cards, and access control.

The next Government Information Exchange Program will be hosted by SCALA, the U.S. Department of Commerce, and the Mexican government. This event – being held May 29, 2013, in Mexico City – is open exclusively to SCALA members and government agencies.

Sincerely,

Edgar Betts
Associate Director, Smart Card Alliance Latin America (SCALA)

[Email and website links]

[Profile picture]

[Event details]
This month Smart Card Talk spoke with David Batchelor, CEO and founder of LifeMed ID, Inc. Mr. Batchelor is responsible for setting the vision and the implementation for LifeMed ID’s global expansion of smart card applications into the healthcare industry. For more than 20 years, he has been a key leader in driving growth and profitability for healthcare providers by influencing market share, increasing administrative efficiencies, reducing costs and unifying patient identity, data and an audited trail of activity across entire healthcare systems and disparate groups. Batchelor has helped drive adoption of smart cards in healthcare by seamlessly integrating patient identity solutions into current provider electronic systems, such as Electronic Medical Records (EMR), Electronic Health Records (EHR) and Admission Discharge and Transfer (ADT), while complying with security and Health Insurance Portability and Accountability ACT (HIPPA) requirements. A Board member of Smart Card Alliance as well as vice chair of the Alliance Healthcare Council, Batchelor participates in the Alliance’s National Strategy for Technology in Cyberspace (NSTIC) Tiger Team and represents the Alliance as a Committee member for the Workgroup for Electronic Data Interchange (WEDI) Health Identification Card Sub-Workgroup research paper on reduction of fraud, overbilling, and Stark Act violations using attributes of an identification card. He is also well known as a national speaker at many conferences throughout the year.

1. Please describe your company’s business profile

LifeMed ID, Inc. is a national leader in providing healthcare systems and infrastructure to support positive patient identity at all points of registration, connectivity and shared data between multiple EMR/EHR/ADT systems to improve healthcare provider patient care, administrative efficiencies and continuity of care. We are also focused on increasing patient satisfaction and safety.

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

LifeMed ID’s SecureReg ID™ solution leverages smart card technology to address specific healthcare industry challenges to authenticate patient identity and to eliminate registration errors, duplicate records, registration bottlenecks and clipboard registration. There is an increased need for a higher level of privacy and security; with smart cards, the right patient care is given to the right patient and documented on the right patient record. Patient safety is improved with the virtual elimination of “overlaid” medical records, which is the root cause of erroneous medical procedures and identity mistakes, leading to over 190,000 preventable deaths in the U.S. each year.

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

The trend in the marketplace is to simplify the healthcare process, increase identity recognition and administrative efficiencies, and utilize a standardized system to manage patient identity. The complexity consumers have is the number of cards in their wallet. For almost every transaction there is a different card -- a health ID card, insurance card, pharmacy card, and payment card. The trend is to consolidate all of the health-related cards securely into one single device. We also see the trends in other industries, such as payments.

Also, we envision that a patient will be able to streamline their engagement with the healthcare provider using one smart card and/or their smart phone. The registration process can be automated. Patients can pay for services by allowing the healthcare provider to verify insurance eligibility or utilize standard payment systems. With embedded patient identity, doctors can access patient health records and provide continuity of care wherever the patient may be located. Most importantly, we are able to simplify the complex process and reduce the number of health-related ID cards while...
increasing patient satisfaction. NFC-enabled smart phones with smart card-based secure elements lend themselves very well to enhanced healthcare services, security and communication.

4. What things must you overcome to leverage those trends?

The barriers to acceptance of the technology include agreement on standards and the enormous effort to proliferate solutions across the different healthcare channels and organizations. The market is often slow in moving towards new technology due to unwillingness to make the necessary changes in the organization or lack of understanding of the benefits. The market is changing and independent providers, clinics and large integrated systems are now adopting smart cards as a uniform patient identity solution used across their internal systems or EHR and Health Information Exchange (HIE) systems.

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

The key factors driving smart card technology growth in the government or commercial healthcare markets in the U.S. are security, privacy, portability of information, efficiency, and patient safety.

- **Security and Privacy** - In addition to HIPAA compliance requirements, it is very important for health IT companies like LifeMed ID to be good stewards of patient information. Smart cards provide an effective medium to protect privacy and deter fraud.

- **Portability of Healthcare Information** - In today’s mobile society, healthcare service providers and patients require information to be rapidly accessible and capable of traversing geographic locations. Smart cards provide secure connectivity to private patient data across disparate systems.

- **Efficiency** - Smart cards will play a more critical role in automating identity, registration and electronic transactions. As the population and the need to have effective patient identity and continuity of care for patients grow, smart cards enable the service providers’ electronic software to automate processes, reducing keystroke requirements and improving data accuracy, care and workflow.

- **Patient Safety** - Patient safety is the heart of healthcare. Medical errors can have negative implications on a service provider resulting in medical errors, increase in healthcare cost and even death. Smart cards as identity tokens continue to be a foundation for patient safety in most developed countries and need to become the standard in the U.S.

6. What type of measureable impact has the Smart Card Alliance and/or its Councils made in your company’s business?

The Smart Card Alliance is a great platform for sharing ideas and information with leaders in the industry. We have gained an understanding of best practices and have forged lasting business partnerships. The Alliance has also been significant in promoting innovations, providing education and facilitating the advancement of vertical solutions ensuring that the relevance of smart card technology continues to remain in the public and private sectors of the country. Our participation in the Alliance continues to be rewarding and has allowed us the opportunity to contribute through leadership and development of resources to expand the usage of smart cards.

**Member point of contact:**

David Batchelor, President and CEO, LifeMed ID, Inc.
www.lifemedid.com
davidb@lifemedid.com
EMV: POS Terminal and Merchant POS System Considerations

The capabilities of the POS terminal play a pivotal role in the success of any payment innovations. Issuers can distribute cards and other payment devices with new functions (such as sophisticated fraud prevention or customer convenience and marketing functions), but the cards are doomed to fail if retailer POS terminals cannot support the innovations. Even the adoption of magnetic stripe technology took years, primarily because of the amount of time it took for appropriate POS terminals to be widely deployed. In the current era of rapid technology innovation, terminal capabilities will have increasing influence over the success of new payment innovations.

The terminal industry itself is going through a revolution that demands greater flexibility and the ability to adapt rapidly to a broad set of possibilities. So, just as retailers need a payments roadmap to plan and develop the POS requirements for their stores, terminal providers need a roadmap for product development to remain relevant and competitive.

In the past, POS terminals in the U.S. were devoted to supporting magnetic stripe technology and, in recent years, contactless magnetic stripe data (MSD) transactions. Going forward, terminals will need to support contactless EMV, contact EMV, and NFC applications. Given all of these requirements, it is important for merchants and acquirers to consider the following parameters for EMV migration:

- Hardware support
- Software support
- EMV and brand type approval
- Transaction messaging support
- Terminal software upgrade capabilities and plans

Hardware Support

To support EMV cards, a terminal needs a contact EMV card interface device (IFD) to read the contact EMV card and a contactless reader that supports the ISO/IEC 14443 standard. Contactless MSD, contactless EMV, and NFC mobile contactless payment all use ISO/IEC 14443 as the communication standard.

However, all terminals with a contactless reader that is ISO/IEC 14443-compliant cannot necessarily accept all types of payments. The terminals must also include software or firmware that supports the contactless applications used by a particular payment brand or NFC device. This is an important consideration when evaluating terminals and requires an understanding of terminal software and certification requirements.

Due to some payment brands’ requirement for supporting offline PIN verification for contact EMV transactions, a popular architecture is to put the contact IFD and the PIN entry device in the same physical unit. Since offline PIN verification is not required for contactless transactions, it is not uncommon (yet not usually desirable from a user experience standpoint) to use a contactless reader that is physically separated from the POS terminal.

Software Support

The EMV specifications defined by EMVCo form the global baseline requirements for contact and contactless EMV transactions. Specifications from payment brands (e.g., American Express, Discover, MasterCard, Visa) are mainly to clarify the options and areas that are out of scope of the EMV specifications. A single EMV kernel can usually be created to fulfill all mandatory requirements from different payment brands. Any customization and out-of-scope requirements can then be implemented outside of the EMV kernel at the POS application level. Examples of customization and out-of-scope requirements are user interface, host communications, and receipt printing.

Contactless implementations are more complicated for terminal manufacturers mainly due to the fact that each payment brand has its own processing logic which can be totally different from other payment brands’ requirements. Because of this, different contactless kernels are usually created to meet different payment...
brand's requirements. Merchants and acquirers should ensure that contactless POS devices contain all contactless kernels available. Again customization and requirements that are out-of-scope for the contactless kernel can be implemented in the POS application level.

Multiple contactless kernels bring up an interoperability challenge: the terminal application does not know which contactless kernel to use until the payment brand of the presented card is known. In order to address this issue, EMVCo created the “Entry Point Specification.” The Entry Point module talks to the contactless card first to select an application in the card for the transaction. Once the application is selected, the contactless kernel that is responsible for transaction processing is known. Each payment brand's kernel operates independently and in isolation from other contactless kernels, so the payment brands do not mandate use of the EMVCo Entry Point. Other “traffic director” modules may be built, but as an impartial and recognized source of specifications and standards, EMVCo seems the obvious source for current and future contactless EMV protocols. EMVCo published version 2.2 of their contactless EMV specifications in June, 2012.

NFC-enabled devices can operate in peer-to-peer mode, read/write mode, or card emulation mode. When operated in card emulation mode, the NFC device acts like a regular contactless chip card. The POS terminal does not require specific logic for NFC mobile contactless payments as long as the NFC payment application on the handset emulates a payment brand's contactless EMV or contactless MSD transaction. To avoid imposing new terminal requirements strictly for NFC, NFC applications are leveraging the contactless infrastructure defined for contactless EMV or contactless MSD.

**POS Configuration**

Not all terminals from a particular terminal brand have the same software support and EMV and brand type approvals. Multiple POS configurations are possible:

- **Standalone terminals**
  
  Standalone terminals are not connected to any other cash register system. A standalone terminal can support EMV as long as the acquirer/processor, gateway or independent sales organization (ISO) supports EMV messaging. The terminal vendors themselves may write the EMV terminal application that supports a particular brand.

Figure 1 illustrates the relationship between application logic and each chip payment type.
• Integrated POS systems
Large retailers often have their own customized cash register software systems with all or portions of the debit and credit card processing logic built in. To support contact EMV, contactless MSD, contactless EMV, or NFC mobile contactless payments, these systems will need additional logic or alterations to leverage the logic in an attached brand-certified terminal.

• Value-added service provider terminals
These terminals are provided with customized software developed as part of an ISO, acquirer, or terminal reseller service offering.

**EMV and Brand Type Approval**

A contact EMV kernel that implements the baseline requirements for contact EMV is required to be certified by EMVCo. There are EMV Level 1 (low level interface) and Level 2 (application level) type approvals. All card brands require EMV Level 1 and Level 2 type approval as a prerequisite for their brand approval. The EMV kernel is usually implemented as payment system independent, such that the terminal vendor can get it certified independently of any future POS application implementation. In general, EMV Level 1 and Level 2 certifications are the responsibility of terminal vendors.

A POS application must get brand approval before it can be used in production to process transactions for the payment brand. Brand approval is usually designed to test the acquirer host system and acceptance system from an end-to-end processing perspective (i.e., from terminal to host and back from host to terminal). Brand approval is the responsibility of the acquirer.

Similarly, the terminal vendor is responsible for getting the contactless Level 1 and Level 2 type approvals for the EMVCo and payment brand requirements that the terminal supports. EMVCo has published the EMV Contactless Specifications for Payment Systems Version 2.2 (June, 2012) which includes the provision for multiple kernels. The specification does not refer to any specific payment brand, but provides the command structure needed to support kernels with different requirements. EMVCo has defined the type approval process for contactless Level 2 kernels which include the Entry Point.

Payment brand end-to-end testing and approval for supporting contactless transactions, which is similar to that of contact EMV transactions, is required for POS applications. This approval is the responsibility of acquirers.

**Transaction Messaging Support**

Figure 2 shows the communication path between the POS terminal and the issuer’s host system. The standard EMV message content for communication between the issuer’s host processing systems and the acquirer is defined by Field 55, the ISO/IEC 8583 standard and payment brand and acquirer-specific message formats. Communication between the terminal and the acquirer is defined by each acquirer/processor and is not standardized.

To support the full EMV messaging specification, which means to support all of the fields carrying EMV data elements, both segments A and B need to be modified. Changing the messaging in segment B requires changes to the terminal application logic and the acquiring host system.

To provide an additional level of security, end-to-end encryption and the Payment Card Industry Data Security Standard (PCI DSS) are two other initiatives that merchants are implementing, which also affect the payment transaction infrastructure and processes. Implementing each initiative in isolation suggests separate development and POS terminal application release efforts. Entities

---

**Figure 2. Communication from Host to Acquirer to Terminal**

---

**Table of Contents**

- Smart Card Talk
- Integrated POS systems
- Large retailers often have their own customized cash register software systems with all or portions of the debit and credit card processing logic built in. To support contact EMV, contactless MSD, contactless EMV, or NFC mobile contactless payments, these systems will need additional logic or alterations to leverage the logic in an attached brand-certified terminal.
- Value-added service provider terminals
- These terminals are provided with customized software developed as part of an ISO, acquirer, or terminal reseller service offering.
- EMV and Brand Type Approval
- A contact EMV kernel that implements the baseline requirements for contact EMV is required to be certified by EMVCo. There are EMV Level 1 (low level interface) and Level 2 (application level) type approvals. All card brands require EMV Level 1 and Level 2 type approval as a prerequisite for their brand approval. The EMV kernel is usually implemented as payment system independent, such that the terminal vendor can get it certified independently of any future POS application implementation. In general, EMV Level 1 and Level 2 certifications are the responsibility of terminal vendors.
- A POS application must get brand approval before it can be used in production to process transactions for the payment brand. Brand approval is usually designed to test the acquirer host system and acceptance system from an end-to-end processing perspective (i.e., from terminal to host and back from host to terminal). Brand approval is the responsibility of the acquirer.
- Similarly, the terminal vendor is responsible for getting the contactless Level 1 and Level 2 type approvals for the EMVCo and payment brand requirements that the terminal supports. EMVCo has published the EMV Contactless Specifications for Payment Systems Version 2.2 (June, 2012) which includes the provision for multiple kernels. The specification does not refer to any specific payment brand, but provides the command structure needed to support kernels with different requirements. EMVCo has defined the type approval process for contactless Level 2 kernels which include the Entry Point.
- Payment brand end-to-end testing and approval for supporting contactless transactions, which is similar to that of contact EMV transactions, is required for POS applications. This approval is the responsibility of acquirers.
- Transaction Messaging Support
- Figure 2 shows the communication path between the POS terminal and the issuer’s host system. The standard EMV message content for communication between the issuer’s host processing systems and the acquirer is defined by Field 55, the ISO/IEC 8583 standard and payment brand and acquirer-specific message formats. Communication between the terminal and the acquirer is defined by each acquirer/processor and is not standardized.
- To support the full EMV messaging specification, which means to support all of the fields carrying EMV data elements, both segments A and B need to be modified. Changing the messaging in segment B requires changes to the terminal application logic and the acquiring host system.
- To provide an additional level of security, end-to-end encryption and the Payment Card Industry Data Security Standard (PCI DSS) are two other initiatives that merchants are implementing, which also affect the payment transaction infrastructure and processes. Implementing each initiative in isolation suggests separate development and POS terminal application release efforts. Entities
that are initiating development in these areas are encouraged to implement the messaging changes that support full EMV messaging, even though the fields may not be used immediately.

**Terminal Upgrade Capabilities and Plans**

Merchants should be sure that their acquirer, terminals and in-house infrastructure support remote terminal management and application upgrade.

The state of contact and contactless chip payment adoption in the U.S. is still in flux. For this reason, increasing numbers of acquirers are offering, and retailers are installing, terminals that include the hardware to support contact EMV or contactless EMV payments but that do not include EMV applications. These terminals are designed to facilitate remote application downloads and updates and have received brand-level type approvals for EMV applications that can be downloaded in the future. If an acquirer plans to buy an upgrade that supports EMV, the acquirer must assure the merchant that the upgrade has been certified by the payment brands for the merchant’s specific terminal model. When evaluating POS terminal deployment options, terminal upgrades provide a potentially cost-effective approach to managing the market’s uncertainties when used in combination with a robust terminal management system. However, when evaluating this approach, it is important to consider the acquirer’s software upgrade costs and deployment strategies.

**Summary**

The terminal roadmap is tightly coupled with merchant support strategies for each acquirer and ISO in the marketplace. Acquirers and ISOs assess the demand for features and functions demanded by their customers and are required to implement the EMV application logic and messaging changes to support EMV. In addition, these organizations are responsible for selling terminals that can meet merchant needs for a number of years ahead. A large part of their investment lies in brand-level EMV application development and certification. Terminals are currently available that have the required approvals, and leading acquirers in the U.S. are installing terminals with the hardware to support contact and contactless EMV transactions. In some cases, these acquirers are activating contact EMV and contactless EMV support; in other cases, they are prepared to download the EMV upgrades as needed.
Access Control

- The Access Control Council collaborated with the Security Industry Association (SIA) to complete the “PACS Primer for PIV” to provide additional guidance for the GSA Evaluation Program Technical Working Group (EPTWG). Members participating in the project included: AMAG Technology, CertiPath, CH2M Hill, Codebench, HP Enterprise Services, Identification Technology Partners, Identive, IDmachines, IQ Devices, NXP Semiconductors, Oberthur Technologies, Quantum Secure Inc., Roehr Consulting, Secure Mission Solutions, Tefco/Software House, U.S. Department of State, XTec, Inc.

- The Council is now working on a project to provide comments to the U.S. Coast Guard on the Transportation Working Identification Credential Reader Requirements Notice of Proposed Rulemaking (NPRM).

- The Council completed the election for the open Steering Committee seat. Lars Suneborn (Oberthur Technologies) was elected to the Steering Committee and elected as the Steering Committee chair.

- Other Council 2013 priorities include: providing input to NIST on FIPS 201-2 related publications; and providing recommendations and guidance on derived credentials.

Healthcare

- The Healthcare Council is collaborating with the Workgroup for Electronic Data Interchange (WEDI) Health ID Card Sub-workgroup to provide input on smart cards and biometrics for a WEDI research paper.

Identity

- Members from the Access Control, Identity, and Mobile & NFC Councils presented in the Smart Card Alliance workshop, “Mobile Devices and Identity and Access Control Applications” at ISC West, on April 9, 2013, in Las Vegas, NV. Workshop presenters included: Brent Bowen (INSIDE Secure); Peter Cattaneo (Intercede); Sal D’Agostino (IDmachines); Frazier Evans (Booz Allen Hamilton); Chris Gardner (SecureKey Technologies); Julian Lovelock (HID Global); James McLaughlin (Gemalto); Lars Suneborn (Oberthur Technologies); Raj Venkat (Ingersoll Rand); Tom Zalewski (CorFire).

- The Identity Council is developing a white paper on smart card technology and NSTIC. The goal of the white paper is to raise awareness of the benefits of smart card technology and show how smart card technology can be used for high assurance credentials in the NSTIC identity ecosystem.

- The Council is leading a cross-council white paper project on supporting the PIV application on mobile devices with the UICC.

Mobile and NFC

- The Mobile and NFC Council held a successful webinar on March 28th, “Secure Elements 101” – the second of four webinars on mobile/NFC security fundamentals. The March 28th webinar had over 410 people registered for the event. Brent Bowen (INSIDE Secure), Sree Swaminathan (First Data), Sanjiv Rawat (Giesecke & Devrient), and Greg Coogan (Morpho) presented in the webinar. The webinar recording is available at: [http://www.smartcardalliance.org/pages/activities-events-mobile-nfc-security-fundamentals](http://www.smartcardalliance.org/pages/activities-events-mobile-nfc-security-fundamentals).
• The third webinar, “NFC Forum Tags and Security Considerations,” will be held on April 18th, with presentations from Tony Rosati (NFC Forum Security Work Group & Blackberry), Joe Tassone (Identive), Mike Zercher (NXP Semiconductors), and Rob Zivney (Identification Technology Partners). Registration for the third webinar is at: https://www1.gotomeeting.com/register/343614305.

• The Mobile and NFC Council is starting a new white paper project on secure credentials on mobile devices.

• A Smart Card Alliance workshop, “NFC Base Camp: The Fundamentals of NFC Mobile Technology and Business Applications,” will be held at the NFC Solutions Summit on May 14, 2013, in Burlingame, CA, and will feature speakers from the Mobile & NFC Council. The workshop will provide attendees with in-depth understanding of NFC mobile technology and the supporting NFC ecosystem that support the rapidly advancing adoption of NFC-enabled applications for payments and non-payments applications.

Payments
- The Payments Council is developing project statements of work for two projects: a white paper on EMV and card-not-present fraud and a white paper on the U.S. payments landscape.

- EMV tutorial videos from the February 4th Smart Card Alliance workshop, “How EMV Changes Payment,” have been posted on the EMV Connection web site. Videos include sessions on EMV fundamentals; considerations for issuers, acquirers/processors and merchants; testing and certification requirements; and EMV migration considerations for transit agencies. Video tutorials include presentations by the following Alliance members: Guy Berg (MasterCard); Greg Boardman (Ingenico); Mike Burden (Consult Hyperion); Randy Burnette (VeriFone); Mike English (Heartland Payment Systems); Allen Friedman (TSYS); and Anna Scurry (First Data).

Transportation
- The Transportation Council is developing project statements of work for three projects: EMV impact on transit; small agency business model for open payments; and transit system reference architecture.

- The Council is currently holding an election for the Council vice chair for parking.

Other Council Information
- Members-only council web pages 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.

- A Council meeting calendar is available on the members-only web site at http://www.smartcardalliance.org/pages/members-council-resources.

- If you are interested in forming or participating in an Alliance council, 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 participating in any of the active councils, please contact Cathy Medich.