Smart Card Alliance

Smart Card Talk

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

February 2017

Change is in the Air

Change is a part of everyday life. While we all sometimes wish we could go back to the "good old days," there will be a point in the future when this very moment will be considered one of those times. My letter in this issue deals with changes and how to adapt, accept and succeed. I also touch upon an upcoming announcement regarding changes for the Smart Card Alliance itself, all designed to ensure we continue to serve the needs of our members. The newsletter also features updates on Alliance Councils, a profile of Leadership Council member FIS, a feature article on embedded hardware security for IoT apps, new members, and CSCIP and CSEIP recipients.

Sincerely,
Randy Vanderhoof
Executive Director, Smart Card Alliance

Click to Read Letter ...

Feature Article:
Embedded Hardware Security for IoT Applications

With over 6 billion connected Internet of Things (IoT) endpoints in 2016, it is no longer possible to consider IoT as a novelty. Uses range from connected homes to smart cities to international industrial applications, This quarter's article focuses on embedded hardware security, where end devices include hardware features and functions to ensure that the appropriate security requirements are implemented and maintained.

Click to Read More …

Member Profile:
FIS

In this first issue of 2017, Smart Card Talk spoke with Bob Woodbury, senior vice president of FIS, an international provider of financial software, world-class services and global business solutions, and general manager of NYCE Payments Network, LLC and PayNet Payments Network, LLC, both FIS companies.

Click to Read More …

In This Issue:

On the Web:

Upcoming Events:

2017 Payments Summit / ICMA Expo 2017
March 28 – 30, 2017
Renaissance Orlando at Sea World, Orlando, Fla
http://www.scapayments.com

Securing Federal Identity 2017
June 6, 2017
Hamilton Crowne Plaza, Washington, D.C.
http://www.securingfederalid.com

Change is in the Air

Dear Members and Friends of the Alliance,

Change is a part of everyday life. As much as we wish sometimes for things to stay the same, or even go back to "the good old days," in reality that will never happen. The best thing to do is recognize that change is taking place around you, prepare for change, and be part of the change for the better. That mindset is what separates successful businesses like Apple, Amazon, and Netflix, from the once great companies they replaced, like Blackberry, Borders, and Blockbuster Video.

The smart card industry has had its share of change, too. For decades, a smart card was the only portable computer in your pocket that could store your private information, execute complex applications, and communicate with many other devices and computer systems wirelessly or through a connection. Now, mobile phones do all of those things and much more.

When the smart card form factor was too big to fit with some applications, like securing a mobile communications network, smart cards changed to SIM cards which could be detached from the card body and inserted inside a smart phone or an automotive computer. When cards were too small to carry the printed images and personal information necessary to protect borders, they became card inlays manufactured in e-passport booklets that enabled the same identity credentials to be electronically authenticated.

The smart card industry's ability to respond to change has kept smart card technology as the gold standard for access security and payments despite the markets searching but never finding disruptive technology to replace cards. When smart phones became the preferred platform for payments security and identity management for startups around the world, many predicted that mobile solutions would leapfrog the use of smart cards and handle identity and payments better, faster, and cheaper.

Yet ten years after the iPhone arrived, and three years after Apple Pay was launched, we have seen – in that same timeframe – the U.S. market issue more than 700 million chip cards, while mobile payments percentages are still in the single digits. The federal government has spent the last four years trying to move beyond smart card-enabled PIV cards and establish derived credentials that can be ported onto smart phones to secure email and sign and decrypt documents on mobile devices. Yet there are still no successful implementations of a mobile PIV. Advances like FIDO get closer by enabling authentication using a trusted device, but they still don't have a way to bind a trusted identity to the trusted device. Only a smart card has proven, over and over, that it enables secure identities and transactions better than any other option.

So with all this discussion on change, the Smart Card Alliance will have some very exciting news to announce in the next couple of weeks. For the past year, the Board of Directors has been evaluating the organization's charter, looking at its current mission, and identifying areas that will allow the Alliance to serve its current market needs and capture more emerging market opportunities and priorities. We have gathered valuable input from our members, ensuring that the Alliance is serving the business needs of its members at all times, now and in the future.

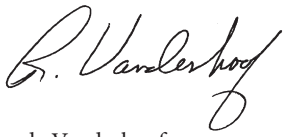
The Smart Card Alliance focus has always been on providing best practices and educational resources that establish requirements for secure payments, identification, access and mobile applications and systems. Those principles have proven to be invaluable to the billions of users of smart card technology. With an increasingly interconnected and mobile world requiring hardware and software solutions that support the implementation of secure solutions, the Alliance is expanding its scope and mission.

To that end, look for an announcement shortly that will be sure to strengthen what the Alliance has always done best – providing timely education, training, conferences, events, news and information; promoting networking; and facilitating industry discussion through industry-focused councils – all within an open and collegial environment for members to collaborate, form consensus, inform, and prepare markets for a more secure future.

Join us as we explore the future of payments at the Smart Card Alliance 2017 Payments Summit Conference, March 27-30, in Orlando FL. Members can register using their complimentary member passes and additional attendees and non-members can take advantage of the early registration discounts in effect until March 4th.

Thank you for your support of our organization.

Sincerely,



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

Helping to Drive the Winds of Change

Dear Alliance Members and Friends,

The winds of change have arrived! Some have found themselves in a world that has changed, losing trust, confidence, and stability. Many have responded to recent changes with sheer panic and fear. For me, this new scenario has filled me with great hope for the future and the transformation of the changes that we have long sought to create in our society.

To say that many people did not see change coming is an understatement. Living in a society based on long held traditions, we've come to expect things to be constant. Humans are creature of habits, and because those habits are so engrained in us, when we are confronted by change, it strikes us as radical.

Technology by its very nature transforms habits, conditions, and the way that things have been done in the past. Not embracing these changes can be catastrophic both for organizations and societies that resist these opportunities to change, improve and/or try to shut out the sun of innovation. This mindset can cause many hardships to organizations, their employees, citizens of a country and vast numbers of populations around the world.

Many societies today still live as our ancestors did many years ago. Some live this way because they live in a remote part of the world without access to information, knowledge, and modern technology. Others live in these conditions because of their countries' political climate, a fear of loss of power by the dominant class, or the need to maintain the relevance of ancient jobs.

To help shape these changes, a social movement is required to transform our societies, and to drive the skill sets and knowledge necessary for professionals to maintain their relevance. Therefore, SCALA has embarked in an ambitious mission to guide the best and brightest minds towards our Digital Center of Excellence – CED (which is pronounced "SED").

The Digital Center of Excellence – CED is a joint effort by the National Bureau of Science, Technology and Innovation of Panama – SENACYT, The City of Knowledge Foundation – FCDS, and the Smart Card Alliance Latin America – SCALA, to help expand the knowledge, awareness, and opportunities for the development and training for the digital transformation in the region.

CED is a word in Spanish meaning thirst, which is a key element and driver for the transformation of any society. The professionals who join our program have this thirst for knowledge, information, self-development, training, and a shared valued towards helping shape our society for the better through technology.

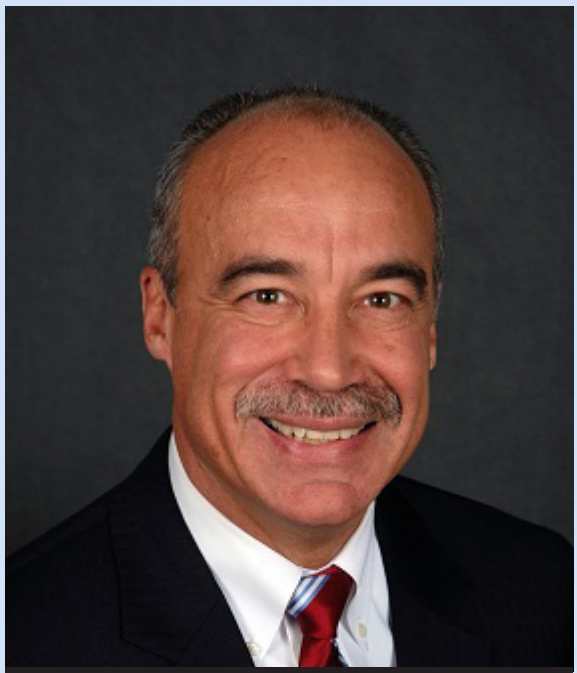
The students from the CED have gone through a rigorous process of selection, competing with the best and brightest students from the two top public universities, University of Panama (UP) and The Technological University of Panama (UTP). These students have worked hard to understand important concepts that are crucial to developing a digital transformation, have received training materials on important concepts related to market verticals, and have begun to create impartial resources on industry best practices.

Edgar Betts, at right, with students from University of Panama and the Technological University of Panama during a programming challenge using smart labels

We invite you and your organizations to get involved with our Digital Center of Excellence – CED, and with SCALA working groups to help drive the winds of change.

Best Regards,

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



Bob Woodbury

In this first issue of 2017, Smart Card Talk spoke with Bob Woodbury, senior vice president of FIS, an international provider of financial software, world-class services and global business solutions, and general manager of NYCE Payments Network, LLC and PayNet Payments Network, LLC, both FIS companies. Bob manages the growth of nationwide and international access of NYCE to thousands of financial institutions throughout the U.S. and the international financial community. Bob, who has been with FIS since 2001, has a Bachelor of Science degree in Chemical Engineering and a Master of Business Administration degree, both from Rutgers University.

1. What are your main business profile and offerings?

FIS is the world's largest global provider dedicated to financial technology solutions. FIS empowers the financial world with software, services, consulting, and outsourcing solutions focused on retail and institutional banking, payments, asset and wealth management, risk and compliance, trade enablement, transaction processing and record-keeping. The company's more than 55,000 worldwide employees are passionate about moving our clients' business forward.

Headquartered in Jacksonville, Florida, FIS serves more than 20,000 clients in over 130 countries, and our technology powers billions of transactions annually that move over $9 trillion around the globe. FIS is a Fortune 500 company and is a member of Standard & Poor's 500 Index.

FIS is driven by commitment to thought leadership, operational excellence and innovation that champions our clients' business and keeps them competitive in today's dynamic and challenging industry environment. We help our clients transform disruption into opportunity, giving them the tools needed to thrive not just today, but in tomorrow's financial world.

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

FIS measures our success through the success of our clients. Smart cards are a key technology enabler for financial institutions, and FIS is a leader in smart card production, having launched over 8,500 EMV card programs for more than 3,200U.S. financial institutions to date. As a merchant acquirer in the U.S. industry, FIS has over 20,000 merchants enabled to accept smart cards for payments and has enabled thousands of ATMs for financial institutions and ATM providers.

Finally, as an owner of a U.S. debit network (NYCE Payments Network), and a technology provider to multiple other U.S debit networks, smart card technology provides additional security to

> **The Alliance and the industry councils have succeeded in bringing the interests and opinions of all stakeholders in the industry into a common forum.**

millions of transactions a month. Our collective group of customers benefit from fraud and risk reductions in their payments, enhancing the overall integrity of our payment options.

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

Specifically related to smart cards and related systemic advances, FIS sees an increasing interest in dual interface cards and technologies that secure other "card" transactions in the industry, including card-not-present (CNP) transactions and mobile transactions. FIS is a front runner in supporting other third party implementations, as well as developing our own solutions, to address these CNP and mobile-enhanced payment advancements.

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

FIS is focused on removing any obstacles that preclude adoption. However, the biggest factors are the multiple technology options being put forth in the industry which create confusion for stakeholders and hinder adoption. As the largest financial technology provider globally, we have a wide diversity of clients and are well prepared to support all schematics, priding ourselves on our thought leadership for our stakeholders.

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

Both markets can benefit from smart card technology in a similar fashion to the existing smart card technology markets, such as making governmental benefit card programs more secure. In addition, since smart card technology allows for additional authentication frameworks to be created, the use cases for these markets are unlimited.

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

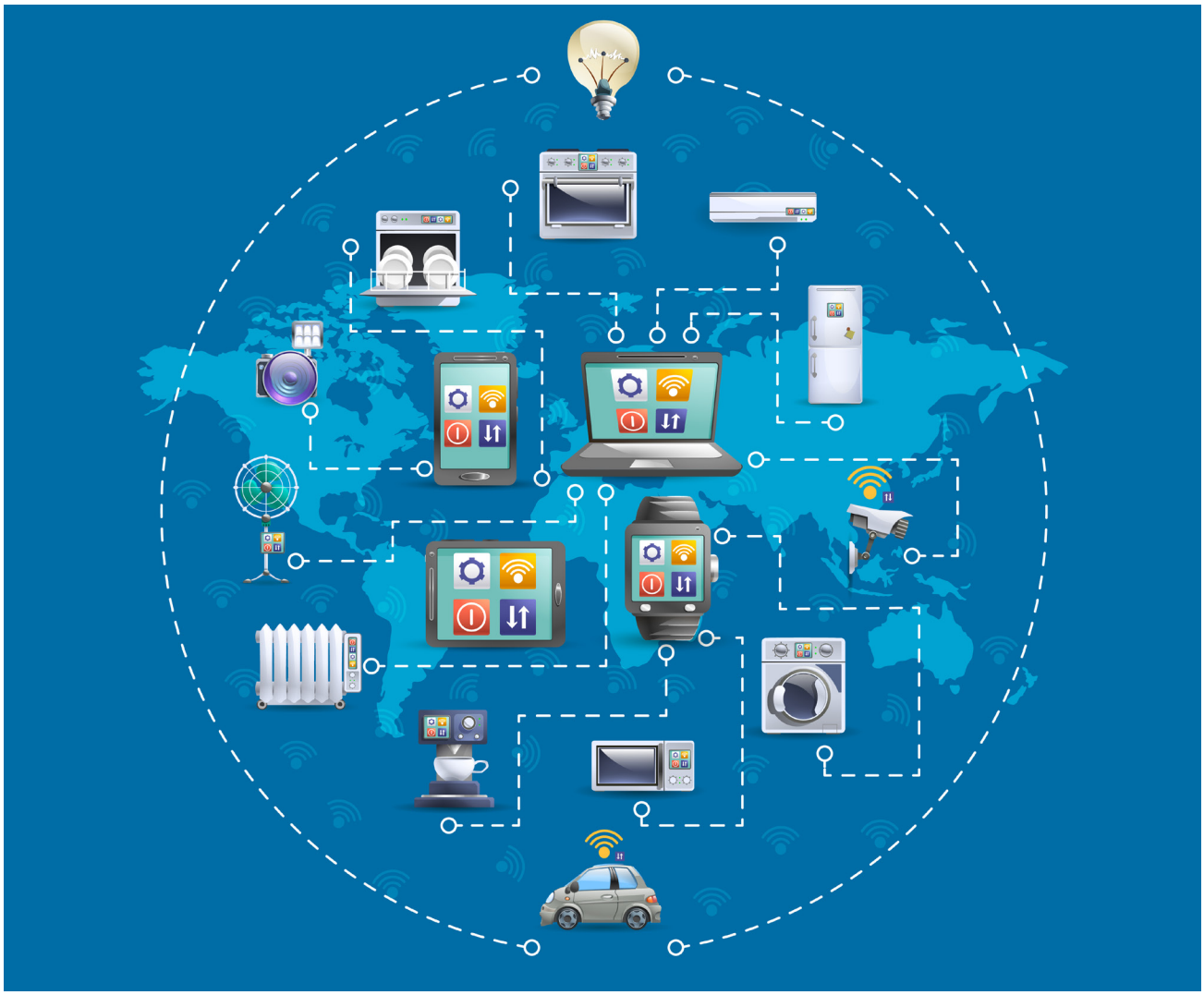
The Alliance and the industry councils have succeeded in bringing the interests and opinions of all stakeholders in the industry into a common forum. Our company values the ability to interact with this diverse group on the variety of topics being addressed. Additionally, the Alliance provides FIS a forum to promote the interests of our clients and assure they are represented in the shaping of the direction of the industry.

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

CNP fraud continues to be most prevalent type of fraud that coexists with smart card rollout. To reduce exposure to CNP fraud, merchants, acquirers and financial institutions must work together to create a layered approach to secure all transaction data of the payment ecosystem.

With a continued focus on security, the Alliance is expected to drive scalable solutions that focus on the continued digitization of payments, the rapid expansion of connected devices with applications in the cloud, and the Internet of Things that is expected to reach more than 20 billion devices by 2020.

Visit http://www.fisglobal.com/ for more information.



Embedded Hardware Security for IoT Applications

From connected homes to cities to international industrial applications, it is no longer possible to consider the Internet of Things (IoT) as a novelty. The world of IoT crossed the 6 billion connected endpoints mark in 2016, according to Gartner's market research.[1] Every day over five million new things are being connected. It has been projected that by 2020, the world will have over 20 billion connected devices – that's around three smart objects for every single person on the planet.[2]

Healthcare, smart city, consumer electronics, industrial, payments and numerous other verticals are developing services that rely on an IoT infrastructure. Security is a core inherent requirement to deliver safe and reliable IoT services spanning from the cloud to connected devices. Industry security practices, however, differ significantly, leading to a lack of common ground to deploy these services with ease, consistency, and ubiquity.

High Profile Hacking

High-profile cases from hacking of IoT devices have already been reported. In July 2015, Fiat Chrysler announced a voluntary recall of 1.4 million vehicles to fix security issues after two security researchers hacked into a Jeep. They were able to interfere with the vehicle's entertainment system, engine, and brakes while the Jeep was being driven on the highway, miles away from the hackers. While this received media attention due to a direct and potential deadly impact to consumers, there have been other incidents that have not received as much mainstream press. In 2014, Germany's Federal Office for Information Security (BSI) issued a report that a steel plant had suffered "massive" damage due to the digital manipulation and disruption of control systems to such a degree that a blast furnace could not be properly shut down.[3] The attackers gained access to the steel mill through the plant's business network using a spear-phishing attack.

IoT security encompasses many different aspects of security such as secure boot, device authentication, encryption, secure

communication, authorized transactions and lifecycle management. Multiple software- and/or hardware-based approaches may be employed in the industry to implement security in each of these areas to meet the requirements of the specific market. This piece focuses on embedded hardware security, where end devices include hardware features and functions to ensure that the appropriate security requirements are implemented and maintained.

Security for IoT Devices

IoT devices are potential entry points to wider IoT ecosystems. For example, the term "thingsbots" has already been coined to point to the risk that these devices may become part of wider botnets, where many different devices– all connected to each other, all network-enabled– can send data, making it harder to detect spam attacks or detect and respond to denial-of-service attacks.[4] Through different IoT devices, including both new connected devices and more traditional network equipment, unauthorized access to wider networks, databases, and systems can be obtained, therefore increasing an attack vector. Hence, it is critical to not only ensure confidentiality, integrity and availability, but also to take into account proper access control mechanisms–specifically identification, authentication and authorization procedures.

The current trend indicates that there is an increased need and market opportunity for embedded hardware and/or software security in IoT ecosystems. Which mechanisms to implement will depend on the security requirements of the specific IoT application.

Security principles can be applied in the IoT ecosystem at the device level (among other levels) through the use of embedded hardware which can ensure proper authentication and access control mechanisms. Embedded hardware may be a "secure element"[5], or another IoT device hardware element with security functionality (such as incorporating the Trusted Execution Environment (TEE) in the microprocessor). The secure element may be a Universal Integrated Circuit Card (UICC) form factor or an embedded secure chip.

Hardware-based secure elements can provide the high level of security required by many IoT applications. Embedded hardware security can provide:

- Robust, tamper-resistant storage of cryptographic keys
- Integrated cryptographic functions
- A proven, standardized means for securing communications between the device, the security-focused hardware element, and external entities such as mobile network servers and other systems interfacing to the IoT ecosystem
- Protection against both virtual and physical attacks (such as power analysis or tampering), with appropriate up-to-date shielding techniques
- Portability among devices, for example as when implemented as a UICC
- Support for authorized and authenticated device lifecycle management (e.g., downloading, activating, changing and deleting the subscriptions)

Embedded hardware security can deliver significant benefits for IoT environments that have critical security requirements – those that require the highest level of confidentiality, integrity and availability and that need to ensure authenticated and authorized access.

Security in IoT Device Life Cycle Management

Because IoT ecosystems involve a multitude of IoT devices, have users bringing their own devices, and have the potential to be extremely complex, the process of securely onboarding, configuring, updating, and operating devices must be taken into account across device categories and industries. This becomes ever more important as network-connected objects and individuals become sensitive targets for hackers seeking vulnerable IoT equipment to exploit, such as devices worn by individuals, and field-deployed meters, sensors and actuators.

To identify how to apply security principles within IoT ecosystems, it is useful to analyze the problem through the connected device's lifecycle: product development, manufacturing, provisioning, operation, change of ownership, removal from service.

Starting at the product development stage, embedded security should be included in the product design. This will ensure that the device can progress through the prototyping, testing and certification phases with the highest level of confidentiality, integrity and availability. Designing with embedded security from the beginning will ensure that the IoT device can benefit from embedded security through its usable life.

During product development, a decision must be made whether to apply embedded hardware security principles to IoT devices in an embedded or removable form factor. A removable secure element is beneficial when it is expected that the stored credentials will travel from device to device (e.g., a mobile phone) while an embedded secure element may be desired in tamper-resistant devices (e.g., insurance telematics module in vehicles) – the latter example providing more total device integrity than the former.

During manufacturing, a device ID in the form of a credential can be stored in a secure element. This device ID can be used to uniquely identify the IoT device and ensure its proof of origin, and take into account the confidentiality and integrity principles. In the case of an IoT device that will connect to a mobile network, an initial mobile network operator subscription can also be provisioned to the secure element.

After manufacturing, a device must then be provisioned and registered to a network regardless of the integrated wireless technology; provisioning may be done by the manufacturer or other ecosystem participants. For this to happen, the integrity of the device must be trusted. A root of trust and device ID from a tamper-proof secure element can be used to ensure this integrity. This integrity can be verified during the authentication process.

Throughout the device's operational lifecycle authentication and encryption can be used to deliver:

- Authenticity – certainty that the sensor or device that sent the message is real and known
- Integrity – certainty that the message is unmodified
- Confidentiality – certainty that the communication has not been intercepted and read by others

A secure element can enable a secure communication channel between the IoT deviceand the backend to provide encryption (e.g., through a virtual private network (VPN)). A secure element could also be used to store device or user authentication credentials.

IoT devices will be deployed for a multitude of use cases and may change ownership multiple times through their service life. Lifecycle management should ensure that integrity and proof of origin of the device are verified before the device is being placed in service on another network. During the operational phase, lifecycle items such as software updates and lost/stolen devices must also be addressed.

In addition, privacy is a concern where the previous user's credentials must be securely removed and the new owner's provisioned.

At the end of an IoT device's life it should be de-provisioned to the point where it is removed from service and cannot be placed back on the network.

Lifecycle management of IoT devices is important for all IoT ecosystems and should be considered during the design of the ecosystem and applications to prevent potential security vulnerabilities over time. The features provided by embedded hardware security can also be leveraged to protect the normal functioning of ecosystems with critical security requirements.

Conclusions

Too often, security is an afterthought in emerging markets experiencing rapid growth and lacking strong standards and regulations. With the rapid growth in IoT deployment, and with no security standards in place, the IoT market falls into that category. There is already evidence of weak security implementations in numerous IoT implementations that have led to IoT systems being hacked – some by security researchers who are highlighting issues and others by criminals who are leveraging the vulnerabilities for their own goals.

Each IoT ecosystem needs to assess its security requirements and its potential for impacting the security of other systems and determine the appropriate level of security that should be implemented. For those systems that impact life safety or the functioning of critical infrastructure, the Smart Card Alliance advocates the addition of embedded security in IoT devices.

Embedded hardware security, among other embedded security techniques, can protect the "identity" of each device, to prevent unauthorized tampering with how these devices are designed to work, and to protect the privacy and security of the vast amount of data the devices generate. A principle behind the security of smart chips is that the chips not only control how the devices perform under normal conditions, but also control how the devices react when they are attacked or tampered with in any way, including self-destruction. Applying embedded security techniques, including hardware-based – as already proven and implemented for other security use cases – can deliver security mechanisms for the billions of connected IoT devices.

Notes

[1] Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, Gartner press release, Nov. 10, 2015

[2] Derived from statistics provided at http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

[3] A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever, Wired, Jan. 8, 2016

[4] Thingbots: The Future of Botnets in the Internet of Things, SecurityIntelligence, February 20, 2016

[5] Global Platform defines a secure element 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.

About this Article

This article is an extract from the Smart Card Alliance IoT Security Council white paper, Embedded Hardware Security for IoT Applications. The white paper provides an educational resource on the value of embedded hardware security in end devices used in IoT applications. Members involved in the development of this white paper included: Accenture; Allegion; CH2M; Discover Financial Services; Exponent, Inc.; First Data; Gemalto; Giesecke & Devrient; Hewlett Packard Enterprise; Intercede Limited; IQ Devices; Metropolitan Transportation Commission (MTC); NextGen ID, Inc.; NXP Semiconductors; Safran Identity & Security; SigNet Technologies, Inc.; TSYS; Underwriters Laboratories (UL); Verifone

Changes Ahead for Smart Card Alliance

The Smart Card Alliance has some very exciting news to announce in the next couple of weeks. For the past year, the Board of Directors has been evaluating the organization's charter, looking at its current mission, and identifying areas that will allow the Alliance to capture current and emerging market opportunities and priorities. Input from members has been invaluable, ensuring that the Alliance is serving the business needs of its members at all times.

The Smart Card Alliance has always been focused on providing best practices and educational resources on establishing requirements for secure payments, identification, access and mobile applications and systems. With an increasingly interconnected and mobile world requiring hardware and software solutions that support the implementation of secure solutions beyond smart cards, the Alliance is expanding its scope and mission.

To that end, look for an announcement shortly that will be sure to strengthen what the Alliance has always done best – providing timely education and training, conferences and events, councils and networking and news and information – all within an open and collegial environment for members to collaborate, form consensus, inform, and prepare markets for a more secure future.

Register for the Feb. 22nd Smart Card Alliance webinar to learn more about the expanded Alliance mission and 2017 plans.

Updates from the Alliance Industry Councils

Access Control Council

- The Access Control Council elected its 2017/2018 officers and Steering Committee. Officers are: Adam Shane, LEIDOS – chair; Dave Helbock, XTec, Inc. – vice chair. The newly elected Steering Committee includes: the officers; Sal D'Agostino, IDmachines; Tony Damalas, SigNet Technologies; Daryl Hendricks, GSA; Martin Janiak, Veridt; Ryan Kaltenbaugh, Lenel; Mike Kelley, Parsons; Stafford Mahfouz, Tyco Software House; Steve Rogers, IQ Devices; Mark Steffler, Quantum Secure; Bill Windsor, DHS; Mike Zercher, NXP Semiconductors
- The Council is currently working on one project, the development of a PACS deployment playbook for the GSA CIO

Health and Human Services Council

- The Health and Human Services Council elected its 2017/2018 officers and Steering Committee. Officers are: Morgan Richard, XTec, Inc. – chair; Jeff Fountaine, Ingenico – vice chair; Stefan Barbu, NXP Semiconductors – secretary. The newly elected Steering Committee includes: the officers; John Ekers, ABCorp; Nicole Williams, Gemalto
- The Council has two active projects: the Client Advisory Board and a webinar based on the concepts in the Healthcare 2.0: A New Paradigm for a Secure and Streamlined Healthcare Industry infographic published in 2016

Identity Council

- The Identity Council is revising and expanding its charter to stimulate project activities and attract new members. An updated charter has been reviewed by Council members

Internet of Things Security Council

- The Internet of Things (IoT) Security Council published the new white paper, Embedded Hardware Security for IoT Applications. The white paper provides an overview of the security threats to the IoT ecosystem and describes the value of embedded hardware security in end devices used in IoT applications. Members contributing to the white paper included: Accenture; Allegion; CH2M; Discover Financial Services; Exponent, Inc.; First Data; Giesecke & Devrient; Hewlett Packard Enterprise; Intercede Limited; IQ Devices; Metropolitan Transportation Commission (MTC); NextGen ID, Inc.; NXP Semiconductors; Safran Identity & Security; Underwriters Laboratories (UL); and Verifone
- The Council also collaborated with Transportation Council to hold the two-day Smart Cities Transportation Workshop on Feb. 1-2, at the Utah Transit Authority in Salt Lake City, UT. The workshop explored the security challenges associated with Smart City IoT initiatives and integration of multimodal mobility transportation related payments.

Mobile Council

- The Mobile Council elected its 2017/2018 officers and Steering Committee. Officers are: Sadiq Mohammed, Mastercard, and Sree Swaminathan, First Data – co-chairs; Damon Kachur, Giesecke & Devrient – vice chair. The newly elected Steering Committee includes: the officers; Maarten Bron, UL; David deKozan, Cubic; Imran Hajimusa, Verifone; Peter Ho, Wells Fargo; Umesh Kulkarni, FIS Open Test Solutions; Simon Laker, Consult Hyperion; Don Malloy, OATH; Sadiq Mohammed, Mastercard; Chandra Srivastava, Visa; Brian Stein, CH2M; Sree Swaminathan, First Data; David Worthington, Rambus Bell ID
- The Council is currently working on three white papers on: mobile identity authentication; mobile profiles and provisioning; Trusted Execution Environment (TEE) 101

Payments Council

- The Payments Council elected its 2017/2018 officers and Steering Committee. Officers are: Jack Jania, Gemalto, and Oliver Manahan, Infineon Technologies – co-chairs; Nick PIsarev, Giesecke & Devrient – vice chair; Jamie Topolski, Fiserv - secretary. The newly elected Steering Committee includes: the officers; Philip Andreae, Oberthur Technologies; Troy Bernard, CPI Card Group; Jose Correa, NXP Semiconductors; Brady Cullimore, American Express; Terry Dooley, SHAZAM; Allen Friedman, Ingenico; Melanie Gluck, Mastercard; Imran Hajimusa, Verifone; Simon Hurry, Visa; Josh Martiesian, NY Metropolitan Transportation Authority; Peter Quadagno, Thales; Sherif Samy, UL; Ellie Smith, Discover Financial Services; Brian Stein, CH2M; Terri Strickland, Wells Fargo; Sree Swaminathan, First Data
- The Council published two new resources in January. The Merchant and Issuer Guides to Contactless Payments in the U.S. include two infographics summarizing the benefits of contactless payments for merchants and issuers. The Contactless Payments Security Q&A answers common questions about the security of contactless payments. Members contributing to the development of these resources included: American Express; CH2M; CPI Card Group; Discover Financial Services; Fiserv; Gemalto; Giesecke & Devrient; Infineon Technologies; Ingenico Group; Initiative for Open Authentication (OATH); Metropolitan Transportation Authority; NXP Semiconductors; Oberthur Technologies; SHAZAM; TSYS; Underwriters Laboratories (UL); Verifone; Visa Inc.; Wells Fargo; and Xerox
- The Council is currently working on two projects – EMVCo Payment Account Reference (PAR) use cases white paper and blockchain and smart card technology white paper – with the goal to complete both by the Payments Summit

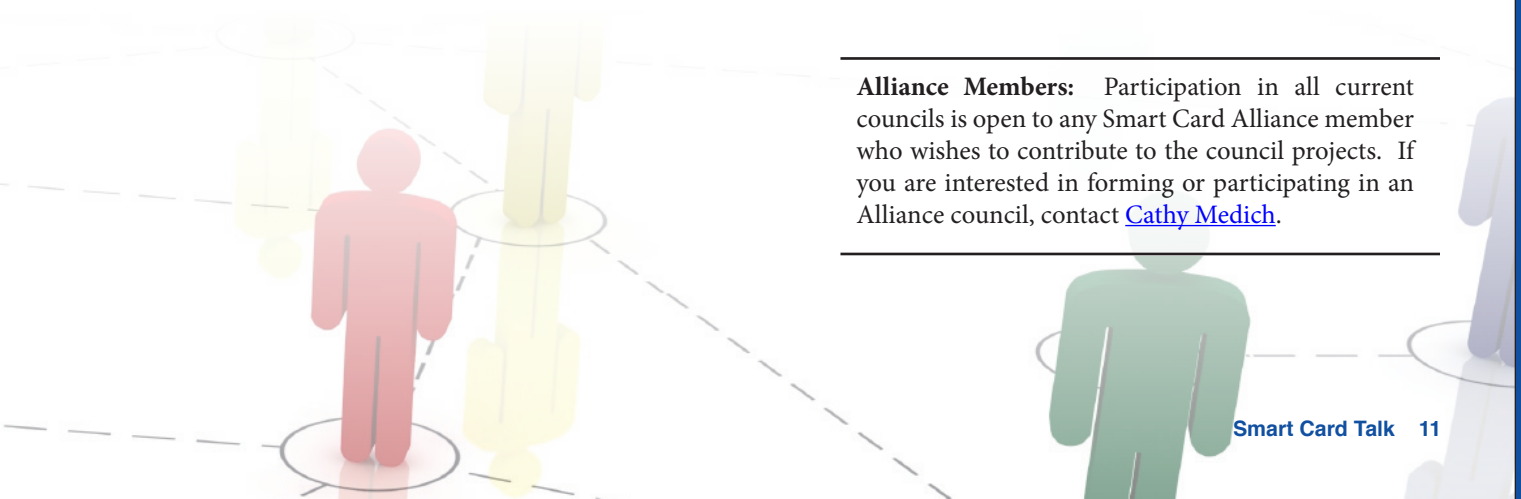
Transportation Council

- The Transportation Council elected its 2017/2018 officers and Steering Committee. Officers are: Jerry Kane, SEPTA – chair; Katina Morch-Pierre, DART – vice chair, transit; Carol Kuester, MTC – vice chair, tolling; Michael Hughes, Moneris – vice chair, parking. The newly elected Steering Committee includes: Ed Baldzicki, Xerox; Francois Baylot, Thales; Randy Cochran, NXP Semiconductors; Michael Dinning, U.S. Department of Transportation/Volpe Center (emeritus chair); Jennifer Dogin, Mastercard; Greg Garback, WMATA (emeritus chair); Jamie Geleynse, G&D; Kathy Imperatore, PATCO; Simon Laker, Consult Hyperion; Rhonda Marx, American Express; John McGee, LTK Engineering Services; Eric Reese, Scheidt & Bachmann; Craig Roberts, InComm (emeritus chair); Eric Schindewolf, Visa
- The Council collaborated with IoT Security Council to hold the two-day Smart Cities Transportation Workshop on Feb. 1-2, at the Utah Transit Authority in Salt Lake City, UT, and approved a pre-release of the white paper, "Multimodal Payments Convergence – Part One: Emerging Models and Use Cases," for workshop. Feedback on the pre-release version will be added to the white paper, with the goal to publish the final version prior to the Payments Summit.
- The Council currently has two active projects: an update to white paper, Reference Enterprise Architecture for Transit Open Payment System, and a new webinar on mobile ticketing and Near Field Communications (NFC)

Other Council Information

- Smart Card Alliance members are now able to request guest participation in U.S. Payments Forum projects. The list of active Forum projects is available on the Alliance member web site. If you would like to participate in one of the Forum projects, please contact Mike Strock. A list of active Smart Card Alliance Council projects is also available to promote cross-council participation
- 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 forming or participating in an Alliance council, contact Cathy Medich.



Welcome New Members

- Cardtek USA
- Chenega Management
- China UnionPay USA
- The Johns Hopkins University Applied Physics Lab
- Waltz, Inc.

New Certification Recipients

CSCIP

- Steven Mehler, WMATA
- Dennis Nguyen, WMATA
- Iniyan Sampath, Capgemini

CSCIP/Government

- Richard Hizon, Tyco

CSEIP Recipients

- Wendy Brown, Protiviti
- Ryan Clapman, Protiviti
- Brian Frieze, FDA
- Troy Hall, Johnson Controls
- Patrick Lackey, Systems Applications & Solutions
- Marquis Laude, Integrated Security Solutions, Inc.
- Dan Morrisey, United Security & Communications, Inc.
- James Morton, NARA
- Kenneth Myers, Protiviti
- Jason Sargent, Protiviti
- Chad Stadig, Siemens Industry
- Duwan Tate, National Science Foundation

Smart Card Alliance In The News

"IoT needs embedded security following record-breaking DDoS attacks," IoT Agenda. Executive Director Randy Vanderhoof shares his perspective on the state of security in the Internet of Things following a record-breaking string of distributed denial of service attacks using IoT devices.

"Smart Card Alliance Educates Merchants and Issuers on Contactless Payments," Bank News. Bank News reports on the Smart Card Alliance's latest educational materials for merchants and issuers on contactless payments, and shares insights from Executive Director Vanderhoof on the state of the market.

For more information, 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.