Smart Card Alliance

Smart Card Talk

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

May 2016

A Message From the Executive Director

It's been a few months since I've talked about the government market, and with our 2016 Government Conference coming up in a few weeks, I've turned my attention to the government security marketplace.

I hope you'll join us for Securing Federal Identity 2016, which will be held on June 6th at the Ronald Reagan International Trade Center Building in Washington, DC. This issue of the newsletter also features updates on Alliance Councils, a profile of our newest Internet of Things (IoT) Security Council, new members and CSCIP and CSEIP recipients.

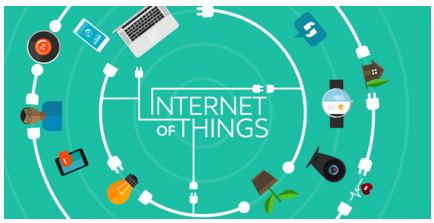
Sincerely,
Randy Vanderhoof
Executive Director, Smart Card Alliance

Click to Read Letter ...

Feature Article:
Smart Card Technology and the FIDO Protocols

Today, the FIDO Alliance is working to provide simpler, stronger authentication to reduce reliance on usernames and passwords, which are susceptible to a wide range of attacks. This month's article provides an overview of the FIDO authentication standards and describes how smart card technology can enhance the security of FIDO protocol implementations.

Click to Read More …



Profile:
Internet of Things Security Council

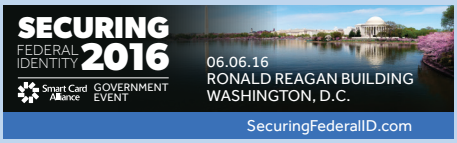
In the spring issue of 2016, Smart Card Talk spoke with Executive Director Randy Vanderhoof about the organization's new Internet of Things (IoT) Security Council, which was formed to develop and promote best practices and provide educational resources on implementing secure IoT architectures by using embedded security and privacy.

Click to Read More …

In This Issue:

On the Web:

Smart Card Alliance Events



Securing Federal Identity 2016
June 6, 2016
Ronald Reagan Building
Washington, D.C.

GLOBALPLATFORM®

GlobalPlatform TEE Conference 2016 Call for Papers – Speakers are invited to participate in the world's only dedicated trusted execution environment (TEE) conference: Next Generation Mobile Security for Today and Tomorrow Conference, which will take place in October 2016 in Santa Clara, CA.

Security of Things Conference
October 19-20, 2016
Hilton Rosemont Chicago O'Hare
Chicago, Illinois

executive director's corner

A Look at the Government Security Marketplace

Dear Members and Friends of the Alliance,

In this month's letter to our Smart Card Alliance organization members, I turn my attention to our government security marketplace. It has been a few months since I've talked about the government market; much attention instead has gone into the complex payments industry migration to EMV chip cards and our efforts in forming the new IoT Security Council. But we have our annual Government Conference coming up in a few weeks, so I think it would be wise to share some insights into the Alliance efforts in education, industry collaboration, and training that is supporting government use of HSPD-12 based PIV credentials.

The 2016 Government Conference event, Securing Federal Identity 2016, will be held on June 6th at the Ronald Reagan International Trade Center Building in Washington, DC. The event has undergone a complete make-over from previous years. What we came to realize is that, more than anything, most people wanted to learn about the new identity management and security programs that are coming, rather than look back on past successes and existing standards and policies for using chip-enabled PIV credentials for physical access for the federal market.

In the past, we held a three-day event at the Washington Convention Center with over 75 speakers and multiple tracks covering every aspect of identity, security, biometrics, and healthcare. It was costly for industry participants to attend and for government workers to devote three days from their schedules to sit through all of the tracks and talk with scores of exhibitors.

The Securing Federal Identity 2016 event is a one-day, highly-focused and high-energy event that will concentrate on how federal agencies are using PIV and PIV-I credentials as strong, two-factor authentication devices to secure federal networks. It will also focus on how federal programs are extending the usage of the PIV credential's identity management and authentication capabilities to mobile devices through the use of derived credentials. The agenda features a select group of mostly federal government speakers, and we will have room for a small group of government security industry exhibitors who will highlight the present capabilities and the future direction of the government's efforts to replace user names and passwords on desktops and mobile devices and use PIV-based authentication to log into Microsoft Windows-based network systems and legacy systems for all federal agencies.

In preparing for this event, I worked closely with our federal and industry contacts. Doing so, I learned of the renewed commitment to further adoption of the PIV card to replace weaker log-in credentials for administrators with access privileges to the most secure systems so that breaches of personal information, like last year's OPM data breach, will not be repeated.

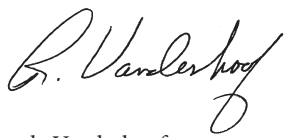
What I heard during the preparation is that infrastructure interoperability remains the "devil in the details" for faster adoption, particularly with mobile credentials. When most of the federal enterprise mobile infrastructure was built on the Blackberry operating system platform, development and testing could be concentrated on a few smart phone models and a common mobile management system approach. However, now there are Apple and Android and Windows devices, and still some Blackberry devices, that need to be supported, with multiple mobile operating system revision levels running on multiple smart phone devices. Developing a testing program to validate all of the use cases to meet the identity management and authentication requirements for encryption services and mobile access to remote networks will be challenging, as demand for such services is increasing.

I learned that the biggest challenge to using PIV credentials for two-factor authentication in government IT networks is that federal CIOs need to evaluate all of the existing IT services that rely on Windows log-in and legacy system access rules before developing a solution that will replace current approaches with the certificate-based PIV smart card credential. Likewise, those IT systems in need of strong two-factor authentication lack uniform means of access, run on different types of PC platforms and mainframe servers, and require the addition of a smart card reader at every access point to leverage the two-factor authentication the PIV credential provides over weaker and more easily compromised user names and passwords.

It is the challenge for technology providers and standards groups to work with their government customers to come up with the solutions that work across this wide array of infrastructure conditions. I am confident that our Smart Card Alliance members will leverage their experience with commercial clients and overseas markets to find the solutions that meet these challenges and adapt to the changing hardware and software needs of our federal enterprise customers. If you are interested in the government identity management and access security markets, you should definitely plan on attending the June 6th Securing Federal Identity 2016 event.

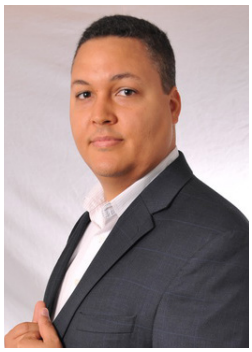
Thank you for your continued support.

Sincerely,



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

Transformation Moves Forward



Dear Members and Friends of the Smart Card Alliance Latin America (SCALA),

Today we find ourselves in the middle of a digital transformation, where it seems that services, processes, companies, and governments are changing their core businesses to serve the needs of a population that demands transparency, efficiency, speed, convenience, and personal attention, all of which can only be provided through a digital medium. The transformation process has not been equitable for all.

It wasn't too long ago that I remember a period when tablets, cell phones, and other digital means of customer service didn't exist. I still recall all of the processes that were completed in person, on paper, signed and handwritten; that created long lines in public institutions such as banks; that resulted in office file cabinets filled to the top and lost paperwork; and that required return trips to resolve a small but vital procedure such as getting a letter notarized or adding extra postage stamps.

We all enjoy, laugh, and smile when we see movies like "Zootopia," that show this reality in a comical way – where there is a public servant called "Flash," a sloth who helps the movie's bunny and fox heroes search for a license plate in the city's DMV. The bunny is in a rush and tries her best to expedite the process; but when they finally finish the search for the plate information, it's too late because it's nighttime.

This reality is also seen in some traditional private and public institutions where many legal and bureaucratic procedures occur. Through these procedures, a hierarchy is in place that establishes the power, influence, authority, and importance of each representative of the organization; they measure the diligence, accuracy and capability of people to fill out forms, spend time in lines, and receive the correct number of seals, stamps, and signatures from other institution representatives, with the justified end proceeding to the next step or finally completing the objective of the procedure without losing patience. The process is extremely important, solemn, and laborious, ensuring that nothing innovative or important occurs in these institutions.

Changing circumstances have caused well-established companies to disappear or, in the best of cases, become skeletons of what they used to be. I'm thinking of Blockbuster, Tower Records, and Borders book stores, among others.

I trust that none of us or our companies want to become obsolete. Innovation is not an easy path. It creates resistance and fear, especially in people who have conducted the same activity in the same way all of their lives, and now see the need to learn a new approach for those tasks, even though the new approach is more efficient.

Companies that have been able to change this paradigm are those who have chosen digital transformation, creating collaborative cultures within their institutions. They are rewarded by the market and their employees, and are viewed as important icons of society, wisdom, knowledge, innovation, riches, efficiency, and collaboration. They offer their customers the tools to accomplish a high level of existence while connecting the world with services and solutions. Some examples are Google, Samsung, Apple, Facebook, WhatsApp, YouTube, Netflix, Skype, Uber and Amazon.

In this context and to promote this digital transformation, we have created The Digital Tour – Americas, organized in collaboration with the Banking Association of Panama (ABP). We also have support from the Latin American and Caribbean Council for Civil Registration, Identity, and Vital Statistics (CLARCIEV), the Latin American Security Association (ALAS), the Panamanian Public Health Society (SPSP), the National Bureau of Science, Technology, and Innovation (SENACYT), the Public Registry of Panama (RPP), and the Panamanian Association of Company Executives (APEDE), among others. These organizations are focused on the implementation of systems that facilitate interaction with their clients/citizens and at the same time remain at the forefront of technology advances.

For the Digital Tour – Americas, we have created an experimental city, which consists of a series of stations in the exhibitor area where participants can interact and experiment with new technologies for payment, digital convergence, and identification using their conference credential. It is a simulation in which attendees can utilize their credentials in different applications, demonstrating the value-added benefits our technology brings to convergence and efficient functionalities in each sector.

The technology being displayed at the event will showcase integration through integrated circuit cards of four vertical markets in the experimental city. The applications include:

- Methods of payment: contactless payments
- Identification: national identity documents
- Healthcare: eHealthcare records
- Access control: perimeter security

It is important to note that the level of interoperability and convergence could only be achieved in this demonstration thanks to our interoperable industry specification, GENUeiD.

I invite you not to miss this opportunity to interact with leaders for these sectors that are being influenced by our emerging digital technologies. The Digital Tour – Americas event provides you with the opportunity to position your institution as an innovative leader promoting convergence in market.

Best wishes.

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

Smart Card Alliance

Randy Vanderhoof

In the spring issue of 2016, Smart Card Talk spoke with Executive Director Randy Vanderhoof about the organization's new Internet of Things (IoT) Security Council, which was formed to develop and promote best practices and provide educational resources on implementing secure IoT architectures by using embedded security and privacy. This new Council is the first in almost four years since the formation of the Mobile and NFC Council in 2012. Continuing its track record of successfully bringing industries together to move technologies forward, the Smart Card Alliance created the Council to provide a single forum and unified voice for all industry stakeholders with a role in digital security to become involved in the broader IoT ecosystem.

> **"We want to encourage broad participation from additional IoT technology firms and device manufacturers to join the new IoT Security Council."**

1. Please describe the "Internet of Things" and how this new Council fits into that definition.

The Internet Society defines Internet of Things (IoT) to mean "the extension of network connectivity and computing capability to objects, devices, sensors and items not ordinarily considered to be computers. These 'smart objects' require minimal human intervention to generate, exchange and consume data; they often feature data collection, analysis and management capabilities." The IoT Security Council will focus on IoT markets where security, safety and privacy are key requirements; privacy and security are paramount in a world where connected devices are expected to reach 21 billion by 2020. The Council will also leverage the expertise and knowledge gained from implementing embedded security technology across other industries to provide practical guidance for secure IoT implementations.

2. What types of projects will the Council work on?

While we recently formed the council and are still working on some of the finer details, we know that we'd like to work on projects to:

- Accelerate market adoption of secure IoT architectures that incorporate embedded security and privacy
- Provide a forum for intra-industry and cross-industry collaboration on secure IoT architectures
- Provide a business forum where stakeholders can network to discuss best practices and implementation of IoT architectures using embedded security and privacy

> **The Internet Society defines Internet of Things (IoT) to mean "the extension of network connectivity and computing capability to objects, devices, sensors and items not ordinarily considered to be computers.**

- Develop resources for the IoT market and communicate details about emerging industry standards, share implementation experiences, and discuss applications and security approaches
- Identify and collaborate with other industry organizations to define and promote standards for secure IoT architectures using technologies that provide embedded security and privacy

3. What type of members do you hope will participate?

IoT security is already well represented by existing smart card security technology organizations in the Smart Card Alliance. We want to encourage broad participation from additional IoT technology firms and device manufacturers to join the new IoT Security Council. This is an ideal venue for organizations seeking an industry forum to promote security awareness, encourage the widespread adoption of security standards, and define best practices that will help protect and maintain privacy of IoT devices and the data they generate.

4. Are there any activities or events upcoming?

We're very excited to announce that one of the Alliance's first IoT activities will be the Security of Things conference scheduled for October 19-20, 2016 at the Hilton Rosemont Chicago O'Hare Hotel in Chicago. We're putting the agenda together now, and it's going to be groundbreaking event focusing on security, authentication and the Internet of Things, in the same way that the Alliance has produced events to address security and privacy in other markets we serve, like payments, government, and mobile. The event will look at the common use cases for IoT – such as healthcare, connected automobiles, smart cities, and consumer electronics – and explore security vulnerabilities and approaches.

5. Where can members go to obtain more information?

We've put together a dedicated web page on the Smart Card Alliance site about the Council, which can be accessed by visiting http://www.smartcardalliance.org/activities-councils-internet-of-things-security/. We also plan to post white papers, briefs, infographics and a variety of other resources as we move deeper into activities. Information about the Security of Things Conference will be announced shortly.

Point of contact:

Cathy Medich,
Director, Strategic Programs
cmedich@smartcardalliance.org

Event Reminder!

Keep an eye out in your email for more information on the Security of Things Conference, which will be held October 19-20. The meeting will be held at the Hilton Rosemont Chicago O'Hare Hotel. You'll be notified as soon as registration is available. We hope you join us for this new conference.

Smart Card Technology and the FIDO Protocols

The de facto standard for online authentication is the use of user names and passwords, implemented through the web form capability that is supported by all web servers and browsers. However, password-only authentication is susceptible to a wide range of attacks. To mitigate some of these attacks, users must use a different password for every web site, which can rapidly become a burden. Historically, in order to improve security, stricter rules must be imposed, adding friction or inconvenience for the user. It is an unfortunate fact that for both enterprise (employee) and public (consumer) authentication convenience has been the goal, while security has been an afterthought.

The Fast IDentity Online (FIDO) Alliance addresses these issues with a simple enrollment protocol and a highly secure authentication protocol. The FIDO specifications promote principles of good design to improve the user experience. The devices used to implement a FIDO solution are manufactured by different vendors; therefore, the user experience and security level achieved vary by device.

FIDO Authentication Protocols

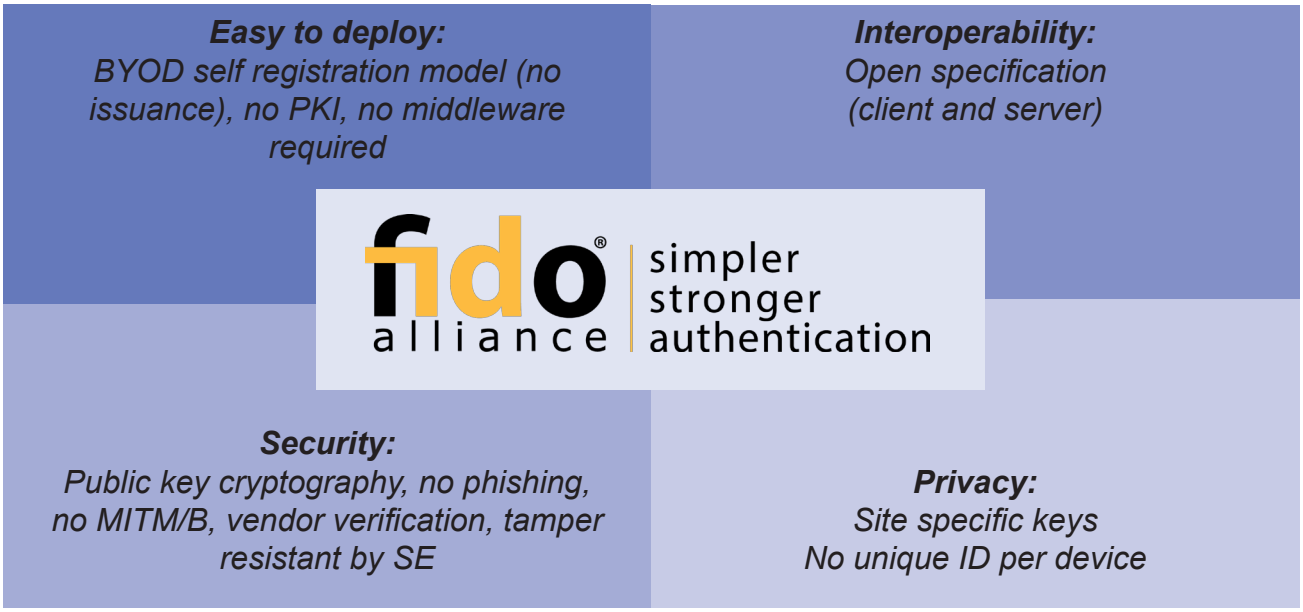
The FIDO authentication protocols are designed to allow robust authentication while providing a superior user experience and protecting user privacy. They incorporate the following principles:

- Strong authentication
- A user experience that combines ease of use with proof of intent: proof of a user's physical presence activates the protocol
- Privacy protection

The protocols rely on strong cryptographic techniques to authenticate a user device to online services. Secrets are stored only on that device and are never exposed to the cloud. This design principle is the cornerstone of the FIDO protocols, Universal Second Factor (U2F) and Universal Authentication Framework (UAF). Both protocols improve security while providing satisfactory usability. U2F strengthens password authentication by adding a requirement for a simple-to-use token, the presence of which constitutes a second authentication factor. UAF can eliminate the password requirement by using biometrics or another authentication factor to authenticate the user to the local device. That same authenticator can be used across multiple online services.

The FIDO specifications also include several requirements that put user friendliness in focus, without jeopardizing user privacy. Unique site-specific credentials authenticate each user to each individual web site, thus preventing tracking a user across on-

Figure 1. FIDO Protocol Principles



line services. The architecture is designed in a way that user's passwords, biometrics or private keys are securely kept in the user's device. Figure 1 illustrates the FIDO protocol principles.

The U2F protocol allows online services to augment the security of their existing password infrastructure by requiring a physical token, called an authenticator. The authenticator provides a strong second user authentication factor to augment user login. In a U2F deployment, the user logs in to an online service as usual, with an established credential. When prompted, the user presents a U2F token and "unlocks" it. At the moment three interface types are specified in FIDO U2F. Universal Serial Bus (USB) was the first, followed by Near Field Communication (NFC) and Bluetooth (Classic and Smart aka Low Energy (BLE)). Unlocking is a test of user physical presence and requires a token-specific gesture, such as pushing a button on a USB device, tapping a U2F device to an NFC-enabled device such as a mobile phone or tablet, or pressing a button on a BLE-enabled token or fob. The user can use the same FIDO U2F device [1] on all online services that support the protocol.

The UAF protocol authenticates a user locally, before the local device used to access the online service authenticates itself to the server. No user password is required.

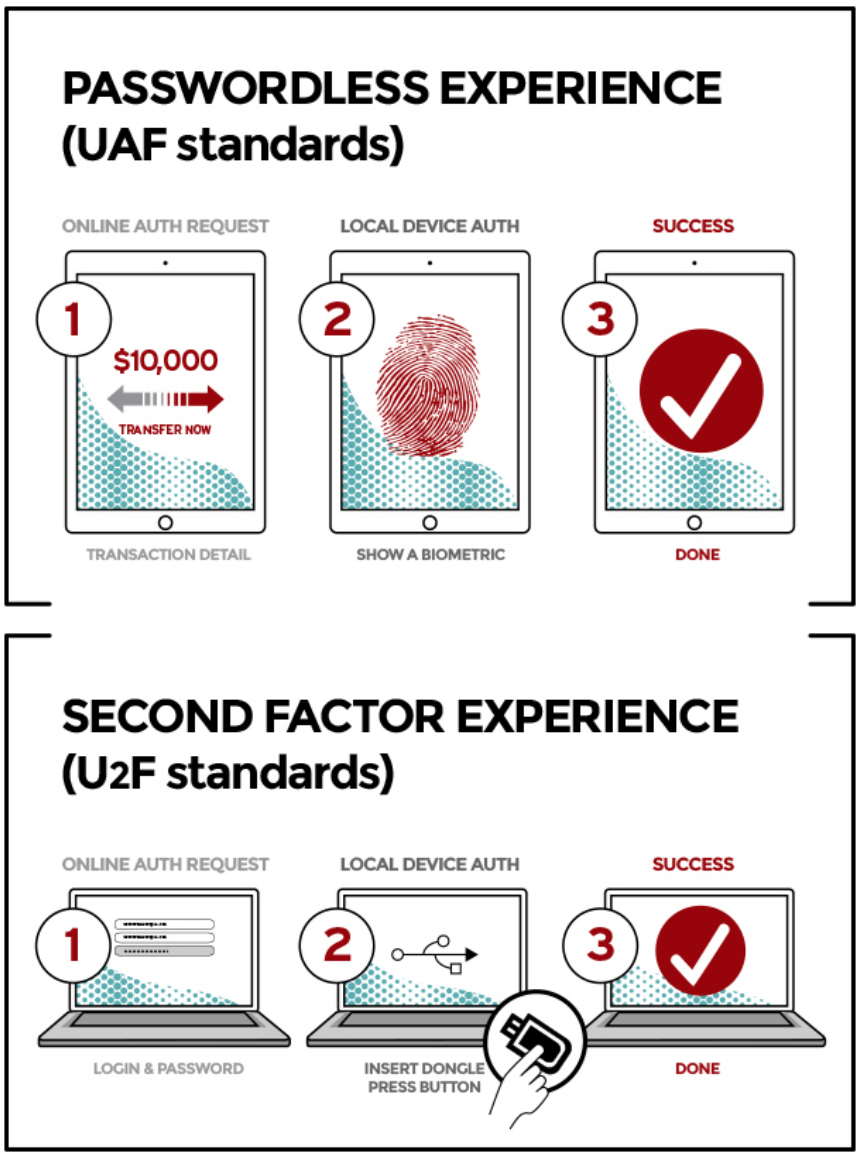
The FIDO authenticator authenticates the user using a PIN, biometric factor (e.g., face, voice, iris, fingerprint recognition), or similar data before proving presence to the online services. The PIN or biometric data should be securely stored, thereby preventing these credentials from leaving the device. FIDO specifications define a common interface for whatever local authentication method the user exercises.

FIDO Protocol Implementation and Security

The FIDO protocols are based on strong cryptography and provide a high security level. However, this is of limited benefit if the actual implementations of these protocols do not provide the corresponding assurance. The following properties should be ensured:

- The cryptographic keys should be securely generated, stored and used. Any recovery or modification by an attacker would potentially allow impersonation of the user.
- The random number generator should be secure, meaning that its outputs are cryptographically strong and unpredictable. The random number generator is used in key generation and signatures and the strength of this security mechanism relies on its quality.

Figure 2. UAF and U2F Experience



- All data used for the local user authentication (e.g., PIN, biometric data) should be securely stored. Any disclosure or modification would allow impersonation of the user or constitute a privacy breach.

The importance of these properties is underlined by the FIDO Alliance in the document, "FIDO Security Reference," [2] which provides an analysis of the security goals and the threats to the FIDO authenticator. As will be discussed in the following sections, smart card technology is the most capable of providing the highest level of security for FIDO implementations.

Smart Card Technology in FIDO

The smart card chip or embedded secure element contains a secure microprocessor, working RAM, nonvolatile memory, and (typically) a crypto-coprocessor. The memory and processors are protected physically, using a variety of software and hardware security technologies. The processor includes either a single external input/output (I/O) interface or, in the case of a dual-interface contact-contactless chip, two separate interfaces, that are controlled by the processor. Vendors creating FIDO authenticators can either include a second processor to manage I/O and control user input and output on the device or provide a single-chip solution that combines both functionalities. When the FIDO authenticator is implemented within an embedded secure element (eSE), it takes advantage of the smart card security features as well providing a secure environment to host other security-critical applications like payment or transport.

Implementing FIDO using smart card technology and hardware-based security brings the following security benefits:

- Generates keys using true random number generators
- Protects keys
- Generates cryptographic signatures
- Provides tamper-resistant hardware security
- Prevents cloning and counterfeiting
- Enables multiple form factors (e.g., card, USB devices, mobile device secure element, microSD, wearables)
- Leverages device manufacturers' security certifications
- Provides the highest level of security available to protect FIDO-related credentials and biometrics

Running the software that implements the FIDO protocols on the processor in a smart card chip or embedded secure element physically isolates the software from the device hosting the browser, allowing the software to execute securely. Both code and data are encrypted. In addition, they are protected by the layers of hardware in the chip and module packaging. An attacker must first obtain the device and then implement a difficult, time-consuming, and expensive attack to have any chance of accessing the device holder's private keys. Even if an attacker succeeds with one device, the same sequence will not be successful on a different device so the attack is not scalable.

Every FIDO authenticator needs to be able to generate key pairs securely and store private keys, and must include a cryptographic engine that includes a random number generator and that can operate on the stored keys. FIDO authenticators generate public key pairs for each web site with which they communicate. Key generation places a high load on computing resources, especially in the case of general purpose CPUs. Smart card technology is purpose-built to perform key pair generation quickly, with low power consumption. Because smart card technology uses a secure element, key pair generation is performed securely and is efficiently protected, even from advanced attacks. Smart card technology protects private keys in hardware with interaction restricted to a limited set of commands and responses.

In addition to the security benefits, smart card technology enables small, light, lower power devices with very fast response times to enable a positive user experience. This provides an ability to do strong authentication over a wide range of use cases without the well-known problems associated with username and password. By making strong cryptography widely available, smart card technology in the FIDO use case creates a better online world for all of its users. It also enables a wide range of manufacturers to implement these solutions and promotes competition and user choice as a result. It can also be combined easily with many existing commercially available devices and other authentication technologies to further enhance user choice and online security.

Conclusions

The FIDO Alliance has tackled a crucial problem in the online world: to promote the use of strong multi-factor authentication as an alternative to usernames and passwords. The collaborative cross-industry effort has succeeded in publishing important specifications for a standardized solution that is now being implemented by multiple stakeholders. This work is foundational for achieving a trusted online environment for both end users and online service providers.

The use of smart card technology in FIDO protocol implementations is integral to achieving the FIDO Alliance goals for broad use of the protocol to provide simple, secure online user authentication. Smart card technology provides tamper-resistant hardware security to store and protect keys and generate cryptographic signatures or hashes. Smart card technology is widely available in a variety of form factors from multiple vendors, providing a cost-effective, easy-to-use device for FIDO U2F implementations and enabling hardware-based security for FIDO UAF implementations using mobile devices. Smart card technology is in use globally, providing security for identity, access and payment applications, and is a foundational technology for providing an easy-to-use and secure user device. While smart card technology is typically used for strongly proofed identity, it can also be used to support anonymity with the FIDO protocol.

Broad implementation and use of the FIDO protocol have the potential to solve one of today's most troubling problems – authenticating users to online services using a cryptographically sound protocol. It also has the potential to drive increased adoption of smart card technology for authentication, providing an easy-to-use, browser-friendly implementation that leverages the security of smart card technology built into the end user's device. Multiple vendors are now offering FIDO-compliant devices that use smart card technology, enabling relying parties to have a high degree of trust in the FIDO token.

The combination of smart card technology and FIDO protocol implementation is a critical piece of the puzzle to make the online world more trusted. The Smart Card Alliance is a strong supporter of the FIDO effort. Many members are active in both the FIDO Alliance and the Smart Card Alliance and increasingly support many of the same users. This white paper describes how smart card technology is integral to the FIDO effort and how the advancement of the FIDO protocols and smart card technology together will bring a wide range of benefits.

References and Notes

[1] A U2F device could be a USB device, a card, or other physical object.

[2] FIDO Security Reference, FIDO Alliance, December 8, 2014

About this Article

This article is an extract from the white paper, "Smart Card Technology and the FIDO Protocols, published by the Smart Card Alliance Identity Council in April 2016. The white paper is part of the Smart Card Alliance and FIDO Alliance liaison partnership, which allows cooperation and collaboration between the two organizations to accelerate informed adoption of the FIDO standards. Additional information on the FIDO protocols can be found on the FIDO Alliance web site.

Smart Card Alliance members involved in the development of this white paper included: CertiPath; CH2M; Deloitte and Touche LLP; Gemalto; IDmachines; Infineon Technologies; Initiative for Open Authentication (OATH);Morpho (Safran); NXP Semiconductors; Oberthur Technologies; SAIC; SureID, Inc.; XTec, Inc.

Updates from the Alliance Industry Councils

Access Control Council

- The Access Control Council will be developing physical access use cases for the Mobile Council white paper on mobile identity authentication.
- The Council conducted a survey of members on possible next projects and will be launching other new projects this quarter.

Health and Human Services Council

- The Health and Human Services Council published the new white paper, Healthcare Identity Authentication and Payments Convergence: A Vision for the Healthcare Industry. The white paper outlines a vision for convergence and provides insight into the opportunities and challenges afforded to the healthcare community as the U.S. migrates to EMV. Members contributing to the white paper included: ABnote; Ingenico; MasterCard; LifeMed ID Inc.; Verifone; Visa Inc.; XTec, Inc.
- The Council published a new infographic, Healthcare 2.0: A New Paradigm for a Secure and Streamlined Healthcare Industry. The infographic depicts the impact of smart card technology on the future of healthcare identity authentication and suggests how current challenges can be solved through interoperability, increased security, and multi-factor authentication. Members contributing to the infographic included: ABnote; LifeMed ID Inc.; XTec, Inc.
- The Council has been successful in securing speaking opportunities at leading healthcare events. The council sponsored the session, "Patient Identity and Digital Matching: A New Approach," on March 1 at the HIMSS 2016 Conference, featuring Tess Coody, CEO, and Roderick Bell, CIO, of Tenet Health. The Council will have its Healthcare 2.0 infographic featured in a poster session at the upcoming National Association of Healthcare Access Management (NAHAM) conference, May 24-27, in New Orleans, LA.

Identity Council

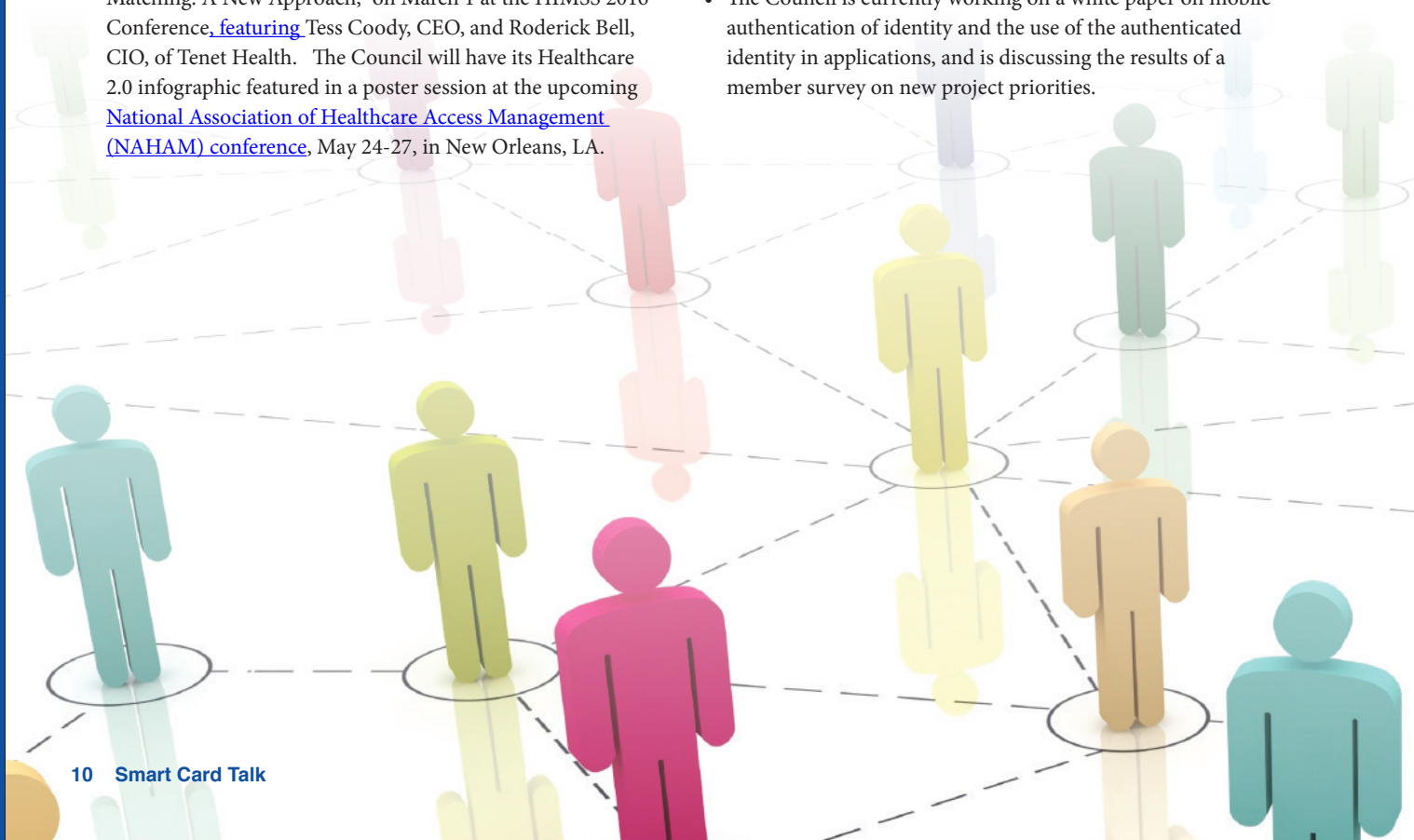
- The Identity Council published the new white paper, Smart Card Technology and the FIDO Protocols. Developed as part of the Smart Card Alliance and FIDO Alliance liaison partnership, the white paper describes the role of smart card technology in implementations of the FIDO protocols and includes examples of use cases currently implementing the FIDO protocols with smart card technology. Members contributing to the white paper included: CH2M; Deloitte & Touche LLP; Gemalto; IDmachines; Identiv; Infineon Technologies; Initiative for Open Authentication (OATH); Morpho (Safran); NXP Semiconductors; Oberthur Technologies; SAIC; SureID, Inc.; XTec, Inc.

Internet of Things Security Council

- The IoT Security Council launched in April, bringing together a broad cross-section of members to develop and promote best practices and provide educational resources on implementing secure IoT architectures using "embedded security and privacy." Council members are currently planning initial projects.

Mobile Council

- The Mobile and NFC Council has a new name, Mobile Council, and updated charter. Council members revised the charter to expand the Council's activities to include all interface technologies and to focus on mobile applications requiring security.
- The Council is currently working on a white paper on mobile authentication of identity and the use of the authenticated identity in applications, and is discussing the results of a member survey on new project priorities.



Payments Council

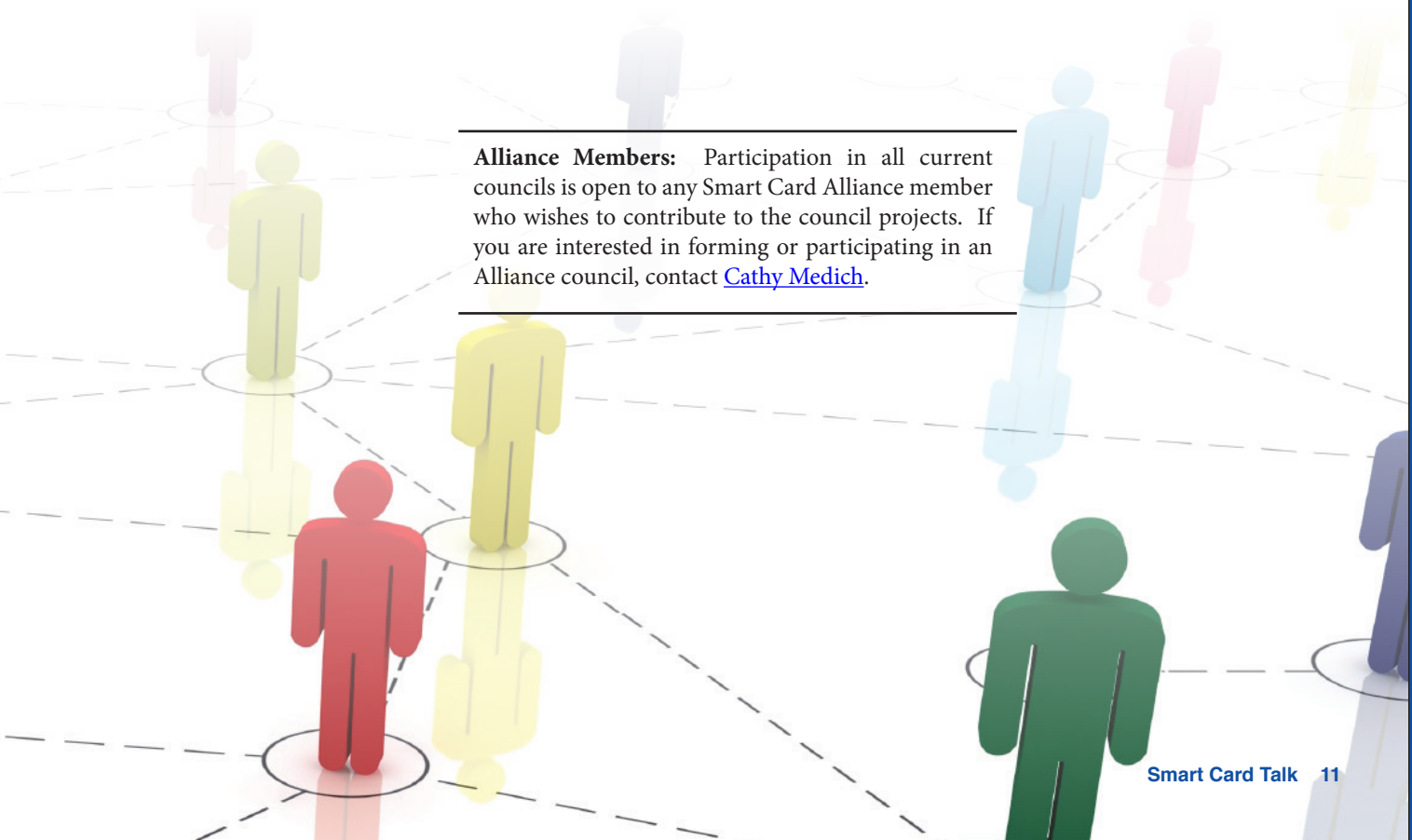
- The Payments Council Steering Committee has elected a new vice chair and secretary to fill open positions. The newly elected vice chair is Nick Pisarev, Giesecke & Deverient, and secretary is Ellie Smith, Discover Financial Services.
- The Council is currently working on three white papers: blockchain and smart card technology; EMVCo Payment Account Reference (PAR) use cases; contactless value propositions for issuers and merchants.

Transportation Council

- The Transportation Council collaborated with the International Parking Institute (IPI) to publish an update to the EMV and Parking white paper. Originally published in June 2015, this update provides current information on the U.S. EMV migration and refreshed scenarios covering the critical aspects of deploying EMV-compliant solutions within the parking infrastructure. Council and IPI members contributing to the white paper included: 20/20 Parking Consultants; Aberdeen Management Group; CH2M; CPI Card Group; Cubic Transportation Systems; Dallas Area Rapid Transit (DART); GO Systems & Solutions; Lumin Advisors; MasterCard; Metropolitan Transportation Authority (MTA); Metropolitan Transportation Commission (MTC); Moneris; Quadagno & Associates; Southeastern Pennsylvania Transportation Authority (SEPTA); Visa Inc.; Walker Parking Consultants.
- The Council also published the white paper, Reference Enterprise Architecture for Transit Open Payment System. This white paper provides a framework for specifying, developing, integrating and managing the lifecycle and evolution of transit open payment systems. Members contributing to the white paper included: American Express; CH2M; Giesecke & Devrient; GO Systems and Solutions; INIT Innovations in Transportation; Metropolitan Transportation Commission (MTC); NXP Semiconductors; OTI America; Southeastern Pennsylvania Transportation Authority (SEPTA); Underwriters Laboratories (UL); U.S. Department of Transportation/Volpe Center; Utah Transit Authority (UTA); Xerox.
- The Council is currently working on a white paper on multimodal payments convergence and is surveying members on priorities for next projects.

Other Council Information

- 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

- BetterBuyDesign
- EPX-Electronic Payment Exchange
- KICTeam, Inc.
- Pinellas Suncoast Transit Authority
- San Mateo County Transit District
- Superintendencia de Banca, Seguros y Administradas de Fondos de Pensiones

New Certification Recipients

CSCIP

- Mario Egoavil, PS2U

CSCIP/Government

- Medge Canseco, Secure Missions Solutions, Inc.
- Gerald Murphy, Deloitte & Touche LLP

CSCIP/Payments

- Jennifer Besenski, LTK Engineering Services
- Greg Brown, JPMorgan Chase
- Keith Flemons, LTK Engineering Services
- Hitesh Shah, CPI Card Group

CSEIP Recipients

- Antonio Araujo, PowerComm
- Gabriel Ciurescu, MC Dean, Inc.
- Perry Galloway, Brivo Systems, LLC
- Sterling Gawthrop, PowerComm
- Dana Kellog, Brivo Systems, LLC
- Joe McCollum, Identiv
- Opy Robbins, Bergelectric
- Freddy Salas, TIC Security
- Jared Schmall, World Telecom & Surveillance, Inc.
- Don Smith, HLCG
- Todd Soderstrom, Security Install Solutions, Inc.
- Nicholas Suarez, General Services Administration
- Rodney Taylor, Office of the Comptroller of the Currency
- Jason Tesori, Bergelectric
- Maniram Tiwari, Tyco Integrated Security
- Ricardo Torres, Siemens Industry, Inc.
- Anthony Tran, Star Asset Security, LLC
- Jon Waters, Signet Technologies, Inc.

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

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.