SECURE TECHNOLOGY ALLIANCE

AUGUST 2018

SECURE TECH TALK

A quarterly newsletter for members and friends of the Alliance

Executive Director Message

Apple announced earlier this month that Apple Pay transactions totaled more than 1 billion in the most recent quarter, mostly from overseas markets. With the continued expansion into new international markets, one analyst predicts that transactions will grow 200% over the next 12 months. My letter in this quarterly issue of Secure Tech Talk addresses the lack of growth in the United States, where Apple Pay was born nearly four years ago and iPhones make up 45% of the smartphone market.

Click to Read Letter ...

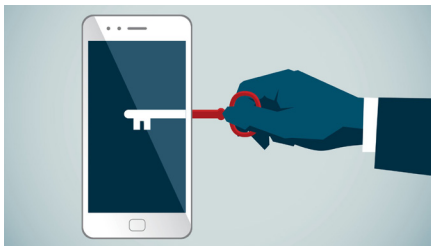
In This Issue:

On the Web:

Identity on a Mobile Device:
Healthcare, Banking and Transportation Use Cases

September 20
2:00 PM - 3:00 PM EDT

REGISTER NOW



Feature Article:
Trusted Execution Environment 101

The Trusted Execution Environment (TEE) is designed to allow mobile and other connected devices to meet their unique requirements for speed and security. The expansion of the Internet, mobile computing, and the proliferation of connected devices have led to increased opportunities for data and identity theft.

This article describes the TEE as a candidate for a mobile security solution that supports a wide range of use cases, such as payment apps, content protection, corporate applications, and loyalty. While various TEE models are emerging, the article focuses on GlobalPlatform-based TEE models for mobile devices, which combine the power of hardware with a software-based solution.

Click to Read More …

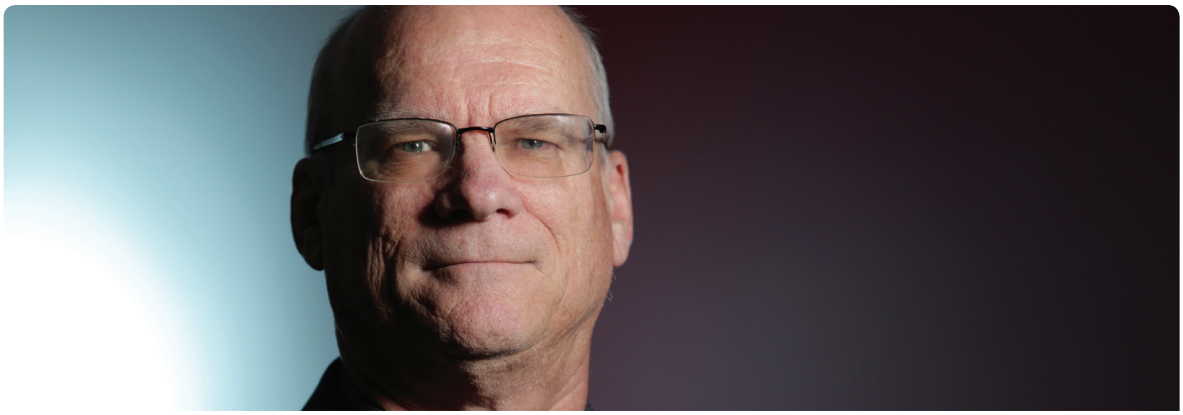
Upcoming Events:

Securing Digital ID
Washington, D.C., Dec. 4-5, 2018

This event is designed for those interested in integrating secure identity technology into their systems. Make your plans to attend and register today.

Payments Summit 2019
Phoenix, AZ, March 11-14, 2019

The Payments Summit covers all things payments over a range of business, technology and FinTech topics. Register today to take advantage of early-bird pricing.



Countdown to Mobile . . . Not Yet, but Maybe Soon?

Dear Members and Friends of the Alliance,

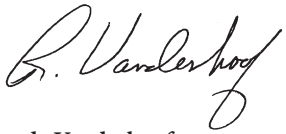
Apple announced earlier this month that Apple Pay transactions totaled more than 1 billion in the most recent quarter, mostly from overseas markets. With the continued expansion into new international markets, one analyst predicts that transactions will grow 200% over the next 12 months. But where's the growth in the United States, where Apple Pay was born nearly four years ago and iPhones make up 45% of the smartphone market?

Maybe it can be explained in terms of the childhood game of hide and seek. Payments industry pundits and mobile wallet technology experts have been making predictions about adoption rates of mobile wallets in the U.S. for much of this decade, yet nobody seems to have figured out the secret to unlock the vast potential of the mobile phone for payments in the physical world. In the game of hide and seek, everyone hides, except the one person who has to "go seek." But before that person can start the game, they close their eyes and count down to zero, before announcing "ready or not, here I come." In the U.S., it seems like the card issuers are the ones counting down and the retailers are off hiding. These banks, who are the primary beneficiaries in this game, are also the ones saying, "ready or not … here I come!"

Big box merchants have reasons to be skeptical about mobile wallets and contactless in general. They are not seeing consumers demanding to pay with their phones. If there were millions of contactless cards in the market, as in faster growing markets like Canada, UK, and Australia, then contactless card acceptance might pull mobile wallet usage along with it, but it is too soon to start counting dual-interface EMV cards in the population. There also are concerns about how many different mobile wallets merchants will have to accept if they turn on mobile acceptance. Lastly is the cost of recertifying their POS systems, and training their customers and staff to handle the variety of phones, watches, rings, and other form factors that come with contactless mobile acceptance.

A lot could change in the next 18 months, when and if dual-interface cards replace many of the EMV chip cards that will reach their expiry dates in 2019 and 2020. Apple, Samsung, and other Android-based device manufacturers are showing no signs of pulling back on their mobile wallet strategies, so eventually it will be the consumers who will be seeking out merchants to accept their preferred method of payment.

Sincerely,



Randy Vanderhoof
Executive Director, Secure Technology Alliance
rvanderhoof@securetechalliance.org

Webinar Program

The Secure Technology Alliance has an active webinar program, with industry councils identifying topics and developing content for the webinars.

Two webinars are currently scheduled in Fall 2018.

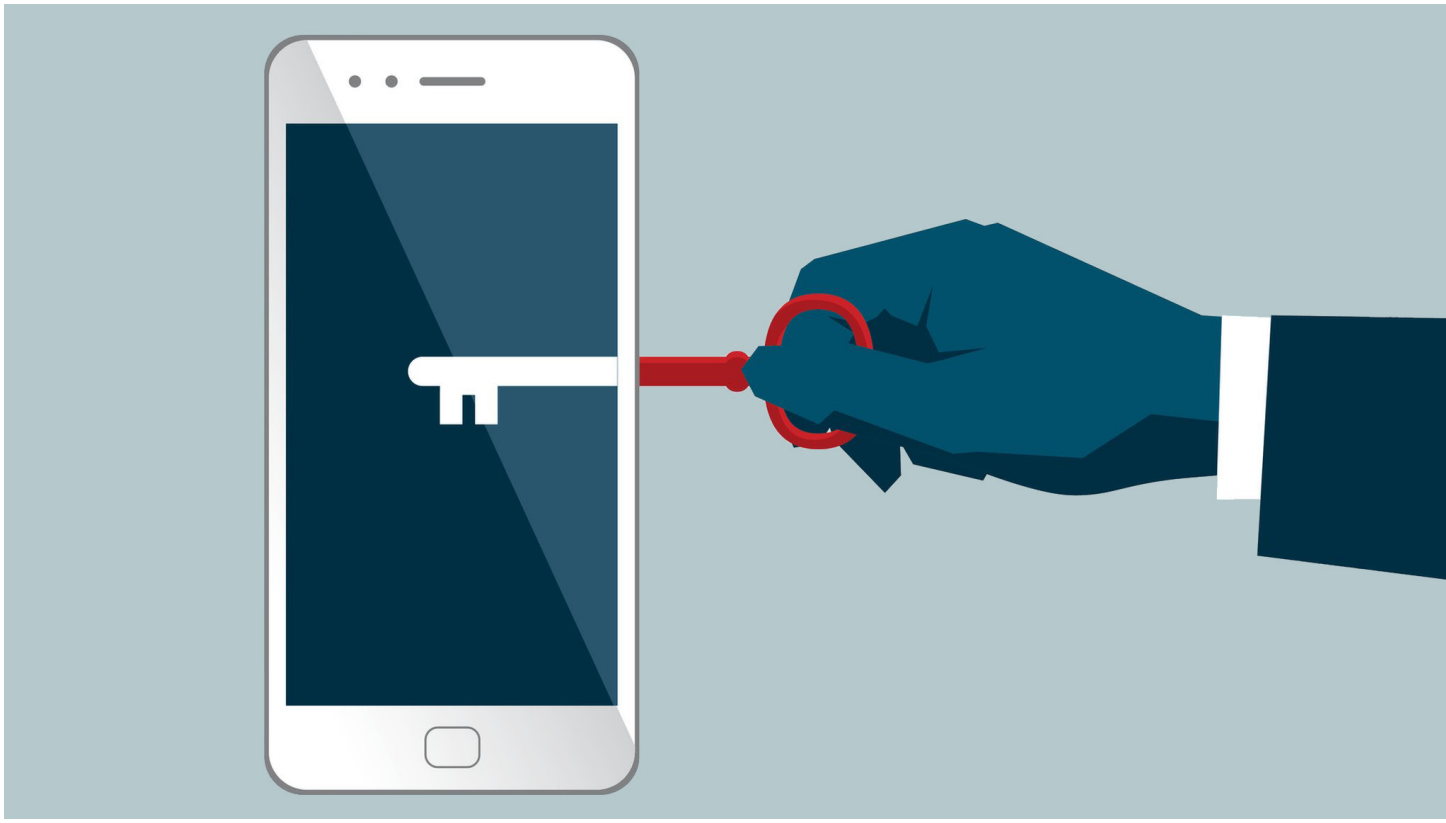
- The Identity Council is hosting a webinar, Identity on a Mobile Device: Healthcare, Banking and Transportation Use Cases, on Thurs., Sept. 20, at 2pm ET/11am PT. The webinar is the third in the Council's series reviewing how mobile identity credentials are used in a variety of use cases. Webinar speakers include: Jeffrey Fountaine, Ingenico Group; Jerry Kane, Southeastern Pennsylvania Transportation Authority (SEPTA); Judy Keator, SecureKey Technologies; Tom Lockwood, NextgenID; Randy Vanderhoof, Secure Technology Alliance

- The IoT Security Council is hosting a webinar, IoT Security: Mitigating Security Risks in Secure Connected Environments, on Thurs., Oct. 11, at 2pm ET/11am PT. This webinar will identify key security risks for IoT implementations and discuss approaches and technologies that are being used to mitigate those risks. Payments, industrial, and automotive use cases will be presented, describing the security approaches that these vertical markets are adopting, and security considerations throughout the IoT device lifecycle will be discussed. Webinar speakers include: Steve Hanna, Infineon Technologies; Josh Jabs, Entrust Datacard; John Neal, NXP Semiconductors; Sri Ramachandran, G+D Mobile Security; Randy Vanderhoof, Secure Technology Alliance

Three webinars were held recently, with recordings available on the Secure Technology Alliance web site by clicking on the following links:

- The Payments Council held two well-attended webinars, Contactless Payments: Issuer Benefits and Considerations and Merchant Benefits and Considerations
- The Identity Council the second webinar in its series, Identity on a Mobile Device: Access Control Use Cases

Registration for upcoming webinars and past webinar recordings are available on the Alliance web site.



Trusted Execution Environment 101

The Trusted Execution Environment (TEE) is designed to allow mobile and other connected devices to meet their unique requirements for speed and security. The expansion of the Internet, mobile computing, and the proliferation of connected devices have led to increased opportunities for data and identity theft. In the mobile ecosystem, the number of mobile applications is growing exponentially, and mobile devices can access services without explicit user intervention, which means the device may be sending sensitive data to an untrusted third-party without proper protection or authorization. In addition, users access Internet resources using untrusted mobile applications and browsers, increasing the probability of propagating malware to their devices. And while the widespread availability of WiFi is convenient for users, it opens the door to unfettered attacks on mobile devices and the unauthorized collection of sensitive data.

Mobile computing is currently so pervasive that besides storage of personal data, personal financial applications and social media activities, corporate applications often coexist on the same device. The device can also serve as an online identity tool and as an additional factor of authentication enabling access to highly sensitive domains and resources. Malicious software can invade a mobile device as a result of user activities that originate from an approved device, but the potential for damage increases significantly with practices such as rooting, jailbreaking, and side loading untrusted applications.

Avoiding or delaying device security updates can also make a device an easy target for vulnerabilities.

Various instances of mobile operating system (OS) and platform security features make managing device application security even more complicated for application providers. Security breaches can result from viruses, malware, and ransomware. Such breaches can result in financial losses and damage to the reputations of individuals and corporations alike; and for corporations, the costs can eventually outweigh the benefits of doing business.

This article describes the Trusted Execution Environment (TEE) as a candidate for a mobile security solution that supports a wide range of use cases, such as payment apps, content protection, corporate applications, and loyalty. While various TEE models are emerging, the article focuses on GlobalPlatform-based TEE models for mobile devices, which combine the power of hardware with a software-based solution.

TEE Evolution

Since the mid-2000s, TEE implementation has evolved from proprietary solutions to a standards-based approach and from mobile devices to a wide variety of Internet-connected devices.

SINCE THE MID-2000S, TEE IMPLEMENTATION HAS EVOLVED FROM PROPRIETARY SOLUTIONS TO A STANDARDS-BASED APPROACH AND FROM MOBILE DEVICES TO A WIDE VARIETY OF INTERNET-CONNECTED DEVICES.

In 2004, Trusted Logic and Texas Instruments pioneered a generic trusted environment. In 2006, ARM developed TrustZone, and the Trusted Logic software became the TrustZone software, licensed by ARM (which then became Trusted Foundations) and commercialized by Trusted Logic.

In 2006, the Open Mobile Terminal Platform (now held within GSMA) published the first set of requirements for a trusted environment, OMTP TR0. In 2008, the requirements were revised to define security requirements for mobile devices. OMTP TR1, also released in 2008, defined a TEE built on top of the TR0 security requirements. In 2010, Giesecke & Devrient (G&D) created their own TEE software, called Mobicore. 2012 was an important year for the TEE community, with ARM, Gemalto and G&D forming Trustonic to boost TEE usage through an open TEE.

Since 2010, GlobalPlatform has been responsible for driving TEE standardization on behalf of the industry. [1] GlobalPlatform has published numerous TEE-related specifications and offers TEE functional and security certification programs to provide assurances to application and software developers and hardware manufacturers that a TEE product will perform in line with the GlobalPlatform specifications and as intended.

The first major business case for use of a TEE surfaced in 2011, for Netflix: protection of high-definition premium content on smartphones and tablets with a secure digital rights management implementation. Content owners (such as the movie studios) required hardware security before allowing a service provider to display high resolution content on an Android mobile device. Only the TEE could satisfy all of the requirements of this business case, particularly the following:

- Extremely high computing power (to download, decrypt, and display streaming content in real time)
- Hardware-independent content decryption and processing
- Hardware-independent content display (through privileged and secure access to the device output)
- Hardware-protected secure storage of sensitive data (e.g., decryption keys and license files)
- Enforced separation of applications (data cannot be copied or intercepted by other applications)
- Standardized APIs (application portability)

The TEE has subsequently been used for consumer, financial, enterprise, media, government, and Internet of Things (IoT) applications.

TEE High-Level Architecture

The fundamental principle of the architecture of a device using a TEE is hardware isolation between the TEE and the mobile device's operating environment.

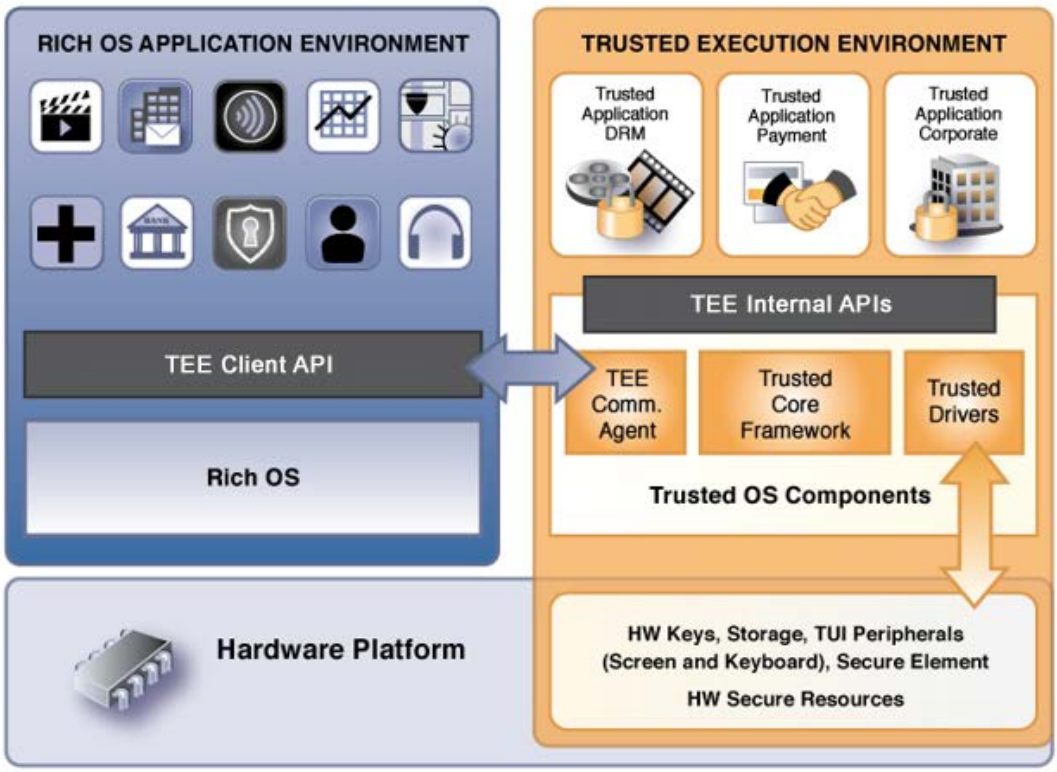


FIGURE 1. ARCHITECTURE OF THE TEE

Source: GlobalPlatform Inc., *The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market,* June 2015.

Figure 1 illustrates a simplified architecture representation of the TEE. As the figure shows, two environments are involved: the rich OS application environment (also called the rich execution environment, or REE) and the TEE. GlobalPlatform specifications require that a TEE be separated from the REE by a hardware-based system. This separation enables cost-effective hardware-based security, since there is no requirement to integrate an extra hardware component into the device to deliver unique, strong security features.

A TEE can run multiple applications, called trusted applications (TAs). Apps in the REE send commands and requests to the TAs through a TEE client API, which connects through a hardware system to a TEE communications agent (see the horizontal arrow in Figure 1). How the hardware connection between the two communications agents is implemented is left up to the TEE provider. The TEE communications agent then forwards these commands and requests to the TAs through the TEE internal APIs.

The trusted OS in the TEE can connect to touchscreens, keyboards, cameras, secured storage, SEs, and other peripherals through trusted drivers (see the vertical arrow in Figure 1). The peripheral services are then available to the TA. Two types of peripherals can be used:

- Peripherals that are accessible only to the TEE (e.g., secure storage and biometric sensors)
- Peripherals that are shared with the rich OS (e.g., screens and keyboards)

When a peripheral is shared, the TEE locks it whenever a TA wants to use it. All communications to and from the shared peripheral are therefore secure and confidential to the TEE.

The GlobalPlatform specifications require the TEE implementation to be separated from the REE by hardware platform protections. A TEE provider can run the TEE implementation on the device's main hardware platform, using the same processor and memory for both the REE and TEE systems (e.g., TrustZone). As an alternative, a TEE provider can use a separate processor and separate resources.

GlobalPlatform also requires that the TEE boot process start before the REE boot process. The boot process loads the security

TEE OFFERS A DEPENDABLE SECURITY PLATFORM. WHEN BUILT USING GLOBALPLATFORM STANDARDS, TEE OFFERS SCALABILITY AND AN EASILY DEPLOYABLE SOLUTION. USING THE TEE IMPOSES NO ADDITIONAL LIMITATIONS ON SPEED, MEMORY, OR COMPUTING POWER.

keys from a root of trust. However, GlobalPlatform does not specify how to initiate the boot process. The example in Figure 1 shows the TEE extending into the hardware platform. A hardware platform boots from a first-level bootloader that is read-only code, and the TEE usually starts its boot process from subsequent bootloader software (a secure boot chain). The TEE may also boot from and run on its own processor in the hardware platform.

TEE Security Principles

A TEE must adhere to certain basic security principles:

- Be part of the device secure boot chain (based on a root of trust) and verify code integrity during each device boot
- Provide hardware-based isolation from the device's rich OS environment to execute sensitive code
- Isolate TAs from each other
- Provide secure data storage, using a hardware-unique key accessible only by the TEE operating system to prevent unauthorized access and modification and any possibility of exploiting the data in other devices
- Provide privileged and secure access to peripherals

Device peripherals (such as fingerprint sensors, displays, touchpads) can be hardware-isolated from the rich OS environment and controlled only by the TEE during specific actions. Access is from inside the TEE, with no visibility or access from the rich OS environment, so that malware running within the rich OS cannot access those peripherals.

Conclusion

Widespread data breaches have made it very important to harden security measures when sensitive data are being processed and stored. This is resulting in an evolution of tokenization and enhanced device security mechanisms in personal computing and connected devices technologies. As in-device payment transactions, mobile identity and authentication, corporate applications and media streaming become more popular, transaction speed and faster time to market are of utmost importance. The wide variety of other connected devices also require security to protect sensitive data.

TEE offers a dependable security platform. When built using GlobalPlatform standards, TEE offers scalability and an easily deployable solution for any device that supports the TEE architecture. Using the TEE imposes no additional limitations on speed, memory, or computing power. The TEE relies on the device's main application processor and the device's native memory space.

Though there are challenges in creating a scalable TEE eco-system, many of these challenges can be overcome by participation in industry standardization efforts from industry players such as chip manufacturers, device manufacturers and TEE solution providers.

References

[1] https://www.globalplatform.org/specificationsdevice.asp

About this Article

This article is an extract from the Secure Technology Alliance Mobile Council white paper, Trusted Execution Environment (TEE) 101: A Primer. The white paper provides an educational resource on the TEE and relevant use cases. Mobile Council members contributing to the white paper included: Cubic Transportation Systems; Discover Financial Services; First Data; GlobalPlatform; Infineon Technologies; JPMorgan Chase; Mastercard; MIPS; Thales e-Security; Trustonic; and Visa.

Updates from the Alliance Industry Councils

Access Control Council

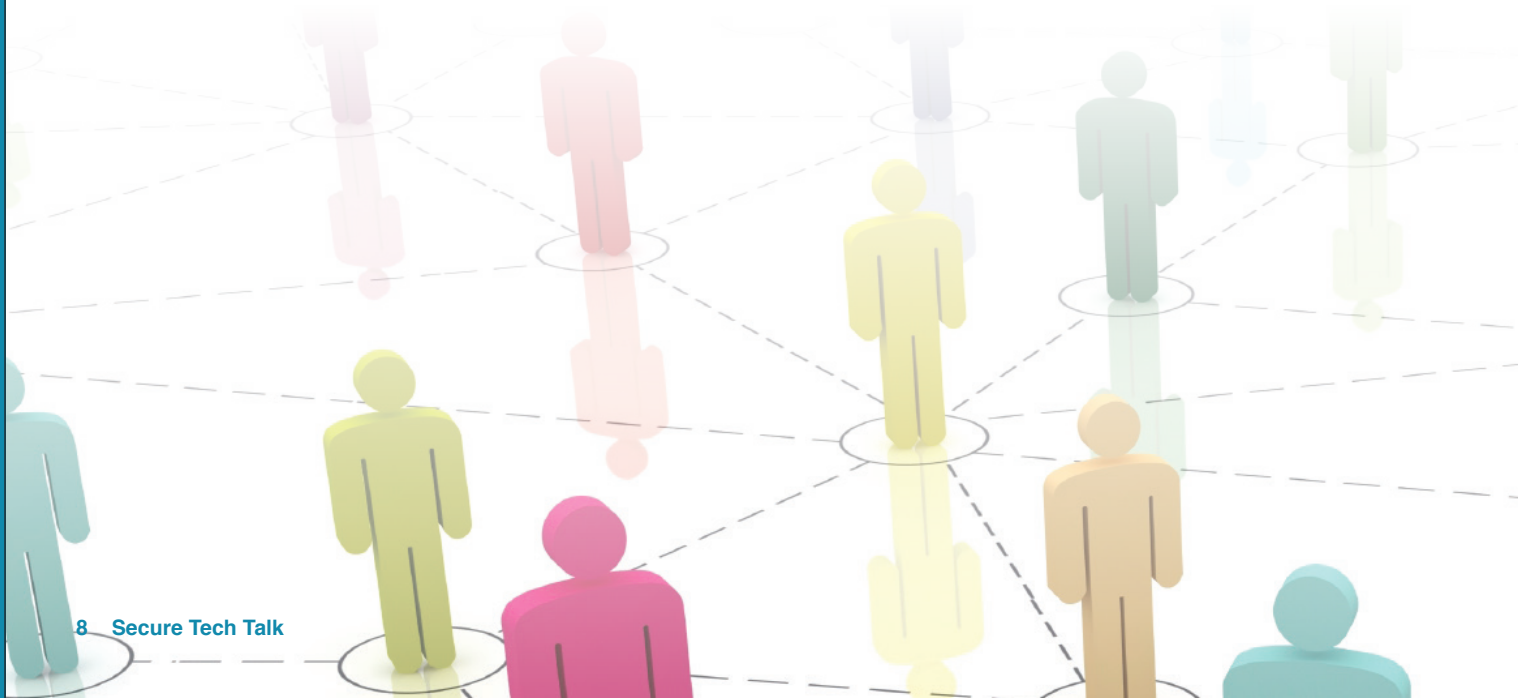
- The Access Control Council published a new white paper, TWIC Card/Reader Challenges with Physical Access Control Systems: A Field Troubleshooting Guide. The project started with the previously-published PIV card/reader troubleshooting guide, which was edited and had new content added to make it specific to TWIC. Members contributing to the white paper included: HID Global; ID Technology Partners; LEIDOS; NextgenID; Parsons
- The Access Control Council and Identity Council held joint in-person meetings on June 5-6 at the Securing Federal Identity Conference in Washington, DC. Representatives from GSA participated on the first day to discuss the planned September "reverse industry day" agenda; NIST participated on the second day for a detailed discussion of the revision to Special Publication 800-116, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)"
- The Council has two active projects, implementing the electronic version of the GSA PACS playbook and contributing to the planned GSA Reverse Industry Day

Identity Council

- The Identity Council held the second webinar in its series, Identity on a Mobile Device: Access Control Use Cases. The webinar provided information for businesses looking to understand and accept mobile identity credentials and featured physical and logical access use cases. Webinar speakers included: Neal Fallon, HID Global; Dr. John Fessler, Exponent; Tom Lockwood, NextgenID, Inc.; and Randy Vanderhoof, Secure Technology Alliance
- The Council has scheduled a third webinar, Identity on a Mobile Device: Healthcare, Banking and Transportation Use Cases, on Thurs., Sept. 20, at 2pm ET/11am PT. Webinar speakers will include: Jeffrey Fountaine, Ingenico Group; Jerry Kane, Southeastern Pennsylvania Transportation Authority (SEPTA); Judy Keator, SecureKey Technologies; Tom Lockwood, NextgenID; Randy Vanderhoof, Secure Technology Alliance. Additional webinars are planned in fourth quarter
- The Council continues work on a white paper on the mobile identity landscape. The white paper will assess the market landscape, document use cases and identify best practices and requirements for industry

Internet of Things Security Council

- The Internet of Things (IoT) Security Council is hosting a webinar, IoT Security: Mitigating Security Risks in Secure Connected Environments, on October 11, at 2pm ET/11am PT. The webinar will identify key security risks for IoT implementations and discuss approaches and technologies that are being used to mitigate those risks
- The Council has launched a moderated, members-only LinkedIn Group, Secure.IoT. The group is intended to facilitate sharing of information related to IoT security and to encourage member discussions. All Alliance members are welcome to join the group at: https://www.linkedin.com/groups/8684363.



Mobile Council

- The Mobile Council published an update to the new white paper, Trusted Execution Environment (TEE) 101: A Primer. The white paper describes the TEE as a candidate for a mobile security solution that supports a wide range of use cases, such as payment apps, content protection, corporate applications, and loyalty.

Payments Council

- The Payments Council held two well-attended webinars, Contactless Payments: Issuer Benefits and Considerations and Merchant Benefits and Considerations. Speakers in the webinars included: Roberto Cardenas, TSYS; TJ Considine, Visa; Jose Correa, NXP Semiconductors; Allen Friedman, Ingenico Group; Oliver Manahan, Infineon Technologies; Cathy Medich, Secure Technology Alliance; Jamie Topolski, Fiserv; Randy Vanderhoof, Secure Technology Alliance
- The Council is working on a new white paper on biometric payment cards. The white paper will provide a high-level description of biometric payment cards to educate issuers on functionality and benefits

Transportation Council

- The Transportation Council currently has two active projects: a webinar on mobile ticketing and Near Field Communications (NFC); part two of the payments convergence white paper, focusing on potential barriers to implementation of multimodal payment strategies and suggesting ways of addressing these challenges

Other Council Information

- Secure Technology 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 Cathy Medich. A list of active Secure Technology Alliance Council projects is also available to promote cross-council participation
- If you are interested in forming or participating in an Alliance council, contact Devon Rohrer

Alliance Members: Participation in all current councils is open to any Secure Technology 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.

from the alliance office

Welcome New Member

- Secure Element Solutions, LLC

New U.S. Payments Forum Resources

The U.S. Payments Forum (a Secure Technology Alliance affiliated organization) published several new industry resources on EMV and mobile payments.

- The U.S. Payments Forum Mobile and Contactless Payments Working Committee published a new resource, Contactless Resources: Implementation Considerations and Clarifications. The document provides clarification on contactless implementation considerations
- The Communications & Education Working Committee published the new white paper, Signature Best Practices, providing guidance on suggested best practices for capturing and storing signatures at physical POS locations
- The Forum Steering Committee published a V1.4 update to the U.S. Debit EMV Technical Proposal to clarify consumer application selection with multi-funding cards

New Certification Recipients

CSCIP/Government

- Graham Gearhart, XTec
- Christopher Matthews, XTec
- Brian O'Rourke, XTec

CSEIP

- Jeremiah Cerra, Lenel
- Stephen Clare, Orion Management
- Fred Conover, Structure Works
- Martin Fletes, Digital Technologies
- Sean Harrison, LS3
- Anthony Iovine, Security 101
- Richard Krehbiel, Kastle Systems Integrated Security Technologies
- Rain Lactaoen, LS3
- Omar Lopez, LS3
- John Murdock, Total Automation Group
- Richard Orr, Secure Install Solutions

Group Exams Available! To make arrangements for a group of employees to take a corporate exam, or for information on "On the Road" training, please contact Lars Suneborn at lsuneborn@securetechalliance.org

Secure Technology Alliance In The News

- "In the Digital World, Health Insurance Cards Remain Analog." Healthcare Analytics News. Executive Director Vanderhoof comments on the feasibility of chip-enabled insurance cards, and how they can provide extra security and identity verification.
- "Federal Policy, Technology Standards for Shaping Secure Identity and Access." Security Today. This article features updates from the Secure Technology Alliance's Securing Federal Identity 2018 conference, and Executive Director Vanderhoof explains the impact of policy updates to securing identity and access in government.
- "Size doesn't matter: Hackers target businesses large and small." NJBiz. In a look at cybercriminal targets, Executive Director Vanderhoof comments on the vulnerability of all businesses, as well as how they can best protect themselves from attack.

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

SECURE TECHNOLOGY ALLIANCE
191 Clarksville Road
Princeton Junction, New Jersey 08550
1.800.556.6828
Fax: 1.609.799.7032
info@securetechalliance.org
www.securetechalliance.org

About Secure Tech Talk

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

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).