



Shifting Focus to Changing Requirements for Federal Identity and Security

Our organization's focus shifts to government identity and security with the 16th annual Securing Federal Identity 2017 event being held June 6 in Washington, DC. Our involvement in hosting this important conference spans four elections, three different administrations, and two political parties. Despite the dysfunctional nature of Washington politics, the federal government has been steadfast in its quest to make identity management and access security function across the entire executive branch. My letter this quarter goes into more detail

about the event, including some interesting sessions and speakers you won't want to miss. The newsletter also features updates on Alliance Councils, a profile of Leadership Council member Giesecke & Devrient America, Inc., a feature article on blockchain technology, new collaboration site URL for Alliance councils, new members, and recent CSCIP and CSEIP recipients.

[Click to Read Letter ...](#)



Feature Article: Blockchain and Secure Element Technology

Blockchain technology, the potentially revolutionary technology that implements bitcoin transactions, is suitable for use in a wide variety of applications. This quarter's article provides an overview of blockchain technology and discusses the role of the secure element and of smart card technology in securing transactions.

[Click to Read More ...](#)



Member Profile: G+D Mobile Security

Secure Tech Talk spoke with Brian Russell, Senior Vice President, Financial Institutions, for G+D Mobile Security's U.S. Division. He also oversees U.S. manufacturing operations and R&D, customer service, marketing communications and offer management, and quality across all market segments of the Mobile Security Division. Brian, who is currently chairman of the Secure Technology Alliance Board of Directors, has a bachelor's degree from Colby University and an MBA from the Wharton School at the University of Pennsylvania.

[Click to Read More ...](#)

In This Issue:

- ② Executive Director Letter >>
- ③ Latin America Letter >>
- ④ Member Profile >>
- ⑦ Feature Article >>
- ⑩ Council Reports >>

On the Web:

[Alliance in the News >>](#)

[Members in the News >>](#)

Upcoming Events:



Securing Federal Identity 2017

June 6, 2017

Hamilton Crowne Plaza, Washington, D.C.

<http://www.securinfederalid.com>

New Council Members-Only Site

With the rebranding of the Alliance (from Smart Card Alliance to Secure Technology Alliance), we have updated our members-only collaboration site domain name and all council email addresses. The members-only site is used to manage council projects and communications.

Going forward, the site URL is <http://www.alliance-forumgroups.org>. Council email addresses are [email list name]@alliance-forumgroups.org. If you have any questions or issues, please contact Mike Strock, mstrock@securetechalliance.org.

Shifting Focus to Changing Requirements for Federal Identity and Security



Dear Members and Friends of the Alliance,

In June, our organization's focus shifts to government identity and security with the 16th annual Securing Federal Identity 2017 event on June 6th. Our involvement in hosting this important conference spans four elections, three different administrations, and two political parties. The Executive Office of the President (EOP) within the Office of Management and Budget (OMB) and the Government Services Administration (GSA) have remained steadfast in moving forward with former President Bush's 2004 HSPD-12 policy directive to mandate that the federal government define standards for the use of secure, tamper resistant, interoperable identity credentials with biometrics to protect federal facilities and networks, even when a physical ID card is no longer needed.

Despite the dysfunction of Washington politics, one thing that has remained consistent since 2004 -- the federal government's unwavering quest to make identity management and access security function across the entire executive branch. The Secure Technology Alliance has been unwavering as well. Every step along the way has been scrutinized, debated, and commented on by our industry members who supply the security technology, credentialing services, access control systems, and implementation teams that have made Personal Identity Verification (PIV) cards the international gold standard for government-issued ID.

AS THE ALLIANCE HAS
EXPANDED ITS MISSION TO
ADDRESS SECURITY SOLUTIONS
THAT GO BEYOND SMART
CARDS, SO HAS THE FEDERAL
GOVERNMENT

As the Alliance has expanded its mission to address security solutions that go beyond smart cards, so has the federal government. At Securing Federal Identity 2017, NIST will highlight the last few years of researching mobile identity solutions and approaches to monitor networks and authenticate users with when no PIV card is present. The Department of Homeland Security (DHS) Identity and Privacy Research and Development office will discuss three mobile authentication and entitlement research programs they are sponsoring. The Department of Defense will share their vision of identity and authentication beyond the Common Access Card (CAC), and the Department of Homeland Security Federal Network Resilience office will explain how DHS is using advanced metrics to measure cybersecurity effectiveness.

It's no question that 16 years is a long time to be in this game of managing secure identities, using secure identity credentials and other digital forms of identity to make the federal government secure from unauthorized employees, and having access to fast, flexible mobile authentication solutions to protect federal facilities and their networks. If you have been away from the federal security scene for a few years, don't miss Securing Federal identity 2017 on June 6th. You might be surprised how far HSPD-12 has come.

Thank you for your support.

Sincerely,

A handwritten signature in black ink that reads "R. Vanderhoof".

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

Passionate Believers



Dear Alliance Members and Friends of SCALA,

Any time someone has asked me how much sales I can generate for their company as a way to evaluate joining SCALA, I explain that this is not the purpose of our organization. While we do provide opportunities to connect with potential customers, the purpose of these interactions is to educate, provide impartial information, best practices, and industry recommendations, and expand the understanding of the benefits and uses of smart cards and other innovative digital technologies.

It is a completely different method of worth, and one that establishes our members as industry experts on technology and value-added services/solutions. Sales generation and business come from establishing a record of excellence, competence, and expertise.

If I were asked for the biggest challenge we face as an industry, I'd respond that we always need more leaders who are passionate, committed, devoted, and believers in the organization and mission. We are always looking to engage individuals who care about the subject matter and are willing to dedicate time, resources, knowledge, and expertise to our industry causes and to develop and promote best practices, industry reports and case studies on how innovative digital technologies have transformed our markets and societies for the better.

When looking at our members and leadership, I'm satisfied with what I see – a diverse group of professionals who are passionate about the topics that we cover and who feel a sense of belonging and ownership in the industry and our organization. They care deeply on how smart cards and other related digital technologies are viewed and how they will impact their market segments, customers, and organizations. They are constantly volunteering to contribute and to ensure that the information we provide is up to date, includes best practices, is vendor neutral and impartial, is providing a positive experience about the technologies we are promoting.

Working in this environment is exciting and gratifying. At every level – individuals, company representatives, organizations, end users and specific market segments – we are rewarded by their belief in the technologies. They want to learn more. They come to us for that information and subject matter expertise and become more engaged overall.

Our organization has a strong belief in sharing information and resources. We make sure to include topics, experts, and cutting-edge discussions in all our events and activities, giving the opportunity for further understanding and interactions with leadership.

We are devoted to our causes, believing that our actions can generate great impact in our society, market segments, and our membership; but we can only be as strong and as good as the sum of our parts. This is an area where you can become very valuable by sharing your knowledge and time.

Biometrics, identity, and payments methods have become critically important technologies in the digital age. They have the potential to revolutionize payments and identity both in security and the client experience. If your organization would like to play a critical role on the definition, adoption, and application of these technologies in the marketplace, we invite you to contribute and join us.

I also encourage each of you to check out our upcoming event, Digital Tour-Americas, June 28-29, 2017, in Quito, Ecuador.

Sincerely,



Edgar Betts

Director, Smart Card Alliance Latin America (SCALA)

ebetts@smartcardalliance.org

www.sca-la.org



**G+D
Mobile Security**



Brian Russell

In this first issue of the newly named quarterly newsletter, Secure Tech Quarterly spoke with Brian Russell, who currently serves as Senior Vice President, Financial Institutions, for G+D Mobile Security's U.S. Division. Brian is based in the technology corridor of Northern Virginia and is responsible for the sales and marketing of all G+D's products and solutions to financial institutions. He also oversees U.S. manufacturing operations and R&D, customer service, marketing communications and offer management, and quality across all market segments of the Mobile Security Division. Brian, who is currently chairman of the Secure Technology Alliance Board of Directors, has a bachelor's degree from Colby University and an MBA from the Wharton School at the University of Pennsylvania.

What are your main business profile and offerings?

G+D Mobile Security works behind the scenes to secure today's connected society and envision the needs of tomorrow. We design, build and operate innovative solutions that secure mobile life.

As a worldwide leader in mobile security solutions, we have unparalleled experience in the emerging mobile payment market and offer the full range of payment options from card to cloud. Integrating market-leading EMV solutions into mobile offerings, G+D can authenticate and dynamically deliver payment credentials to mobile devices and cards through central or distributed issuance platforms.

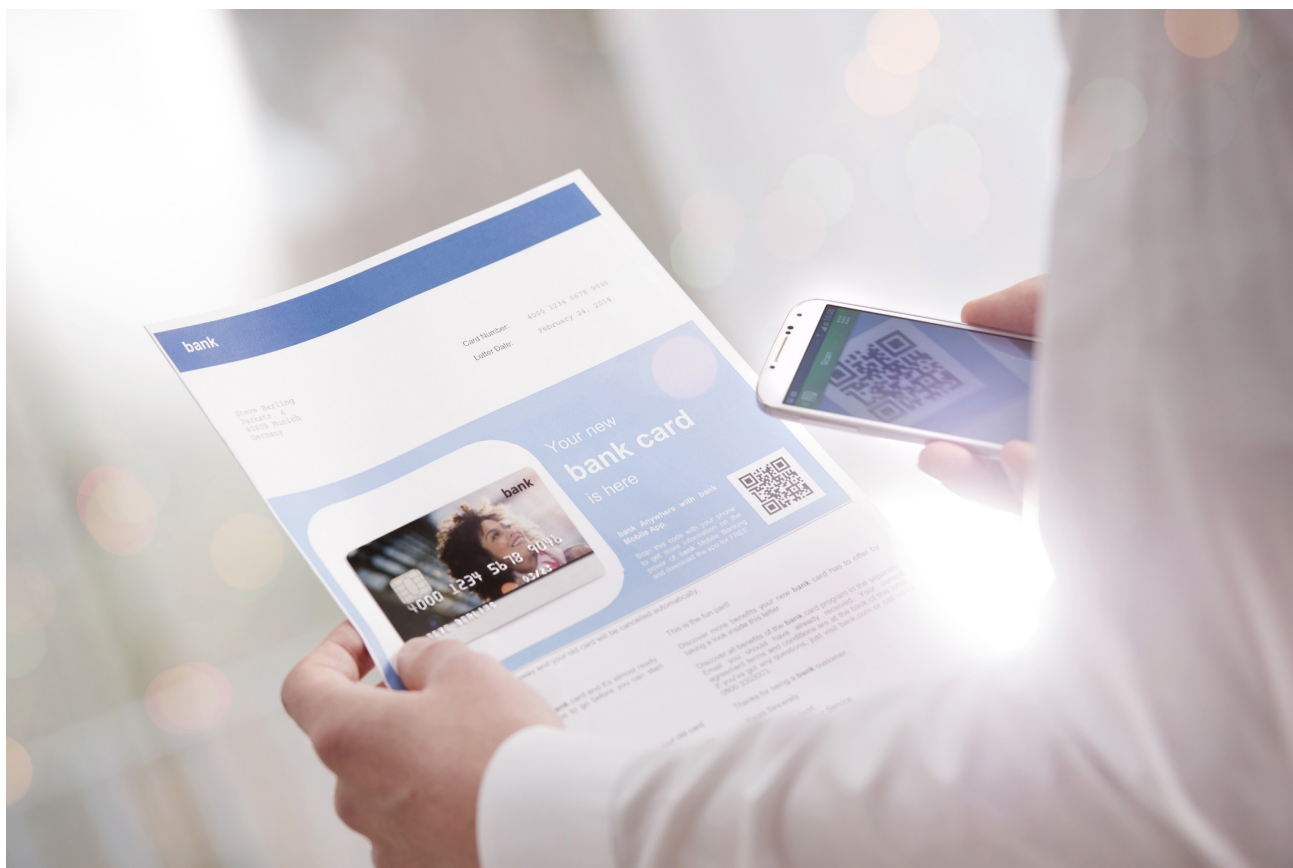
We deliver best-in-class secure elements and remote credential lifecycle management plus over-the-air (OTA), host card emulation (HCE), digital wallets, tokenization and trusted service manager (TSM) services. In the emerging Internet of Things (IoT) and smart wearables market, G+D partners with both established enterprise players and innovative start-ups to incorporate the highest level of security in IoT communications and transactions.

G+D has been trusted by mobile network operators, technology companies, financial institutions and world governments to secure their physical currencies and digital assets for over 160 years. With world headquarters based in Munich, G+D has subsidiaries around the world, employing over 10,000 people and generating \$2 billion in annual revenues.

What role does smart card and secure embedded chip technology play in supporting G+D's business?

For G+D, it's all about identity management. Over the past 40 plus years, G+D has evolved smart card technologies, driven standards to ensure interoperability, and educated our customers. We have built strong, mutually-beneficial relationships with financial institutions, mobile network operators, transit authorities, governments and corporations to secure and manage the identities of their customers. With convergence occurring across these industries and new form factors gaining traction in the IoT-centric marketplace, G+D leads the industry in securing credentials via hardware and software solutions.

G+D continually develops new products and services to meet market demands and innovations to eliminate obstacles to smart card adoption. We actively participate in dozens of standards bodies and industry organizations, like the Alliance, to further interoperability. We work with customers, potential customers and industry associates to help them prepare for and take advantage of advancing security solutions offered by G+D and supported by the STA.



What trends do you see developing in the market that G+D hopes to capitalize on?

The market trend we all need to embrace is the need for mobile, remote, secure access as required to keep the IoT functioning. While our innovation in the card sector will not diminish as the EMV implementation nears completion, we will continue to invest in our software-based solutions complemented by hardware-backed security alongside our traditional products.

G+D is at the forefront of managing identities over-the-air. Our Telecommunication Industries division delivered the first subscription management platform in 2012, and we continue to lead IoT and machine-to-machine (M2M) developments. In the emerging IoT and smart wearables market, G+D partners with both established enterprise players and innovative start-ups to incorporate the highest level of security in IoT communications and transactions.

All payment-enabled smart devices need to offer consumers the same level of security as the physical card, and we're excited to work with our fellow Secure Technology Alliance members to extend the protections enabled by EMV and tokenization to the IoT ecosystem. Whether your phone, your refrigerator or your car can directly make a payment, the credentials and transactions must be secured at all points.

What obstacles to growth do you see that must be overcome to leverage these opportunities?

Over the years, consumer knowledge has greatly increased – and with EMV cards in consumers' hands, we've made a giant leap forward. While there have been delays and resistance to the EMV card, customers and industry alike are in agreement that security is paramount. But with the market shifts driven by the IoT, even some who work in the smart card industry are cautious about the security assurances or lack thereof in cloud-based, software-driven technologies. To overcome these obstacles, we need to provide education, not only to the consumer, but also to the issuer/service provider to ensure they are aware of the latest, most effective security mechanisms, such as tokenization, to protect consumers' private information and reduce fraud.

What are the key factors driving smart card and secure embedded chip technology in government and commercial markets in the U.S.?

The commercial markets are interested in expanding the applications and form factors of the security technology that Alliance members provide. Smart cards are not just for payment anymore. The secure identity management we offer is desired in industries



“**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.**”

beyond payment. Health care cards are a prime example where smart card expertise can be applied to a market where it is of critical importance that access and credentials be kept secure. Health care applications are also a relevant use case where the use of other form factors enhances function. For a patient in a hospital, having all your data accessible via a wearable versus a card that would have to be “in hand” would improve the speed and accuracy of patient information transfer among health care providers.

The government use of smart cards remains focused on the Personal Identity Verification (PIV) card. At a recent Alliance event, we heard many agency inquiries about upgrading card functionality and expanding mobile access options. However, the varied security standards and requirements create a real challenge for us to define what a next-gen government access technology would look like. The Alliance would benefit greatly from taking an increasingly active role in encouraging and guiding the government to define consistent standards that could be applied across platforms and deployed on behalf of the U.S. anywhere in the world.

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

The Alliance provides an invaluable opportunity for G+D to get visibility of the “big picture” of the industries represented within the Alliance. This wider perspective offsets the temptation to focus on our individual role in the smart card and credential management markets. Alliance resources help us better meet and anticipate market needs and share our technologies to a wider audience. The councils are instrumental to the industry in promoting our mutual efforts through published recommendations and education outreach. There is a synergy within the structure that ensures all members benefit.

What are some of the challenges you see confronting our industry?

We are at a pivotal point in the smart “card” industry where the security and connectivity we provide are being adopted by technologies outside the physical card. It is fitting to define our mutual objective as securely managing identities via the many diverse and emerging platforms –starting with the smart cards, phones and wearables already in place today. Alliance members are experts. We need to be sure we don’t lose our vision of the future “secure credentials” market where software- and hardware-based security will be prevalent and complementary. Our focus needs to be broad to ensure we’re leading the market as credentials are increasingly managed in the cloud as well as in the card and other secure element form factors.

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.

Any final thoughts?

We are excited about the next phase for the Secure Technology Alliance – evolving with the industry to focus on next-gen security where software and cloud applications support the hardware we’ve all designed and improved over the years. As we expand our focus, we also would benefit from looking to expand our membership and investigate start-ups and their approach to credential authentication and transaction security. Mobile and cloud payment security are topics that are top-of-mind throughout the market. We would benefit as an organization to reach out and consider the different tactics currently under development. ▲



Blockchain and Secure Element Technology

Blockchain technology, the potentially revolutionary technology that implements bitcoin transactions, is suitable for use in a wide variety of applications. Both startups and established players are deploying or piloting blockchain applications; over \$1 billion has been invested in blockchain and bitcoin startups since 2009, with 60 percent of that funding occurring since the beginning of 2015. [1]

A blockchain is a distributed database that maintains a dynamic list of records, secured against tampering and revision. [2] Blockchains can be used as distributed ledgers that allow financial (and other) transactions to be recorded and verified cryptographically without the requirement for a central clearinghouse or authority.

This article provides an overview of blockchain technology and discusses the role of

the secure element and of smart card technology in securing transactions.

Blockchain Overview

A blockchain is a shared, trusted public ledger that everyone can inspect, but which no single user controls. Participants collectively keep the ledger up to date; it can be amended only according to strict rules and by general agreement. The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority.

In any blockchain-based service, two families of actors can be identified. On one hand, the “users” are the ones using the service by producing transactions, for instance exchanging money with one another. [3] They use standard cryptographic techniques to prove that they are legitimate

to instantiate a specific transaction. For example, in Bitcoin, if a transaction stored in the ledger states that Bob has given 3 bitcoins to Alice, someone willing to spend these 3 bitcoins must prove she is Alice. Actually, “Bob” and “Alice” are replaced by public keys, so proving a user is Alice is done by providing a signature with the corresponding private key. When a user has produced a transaction, the transaction is sent to the second actor of the blockchain: the blockchain network.

The network is (usually) a peer-to-peer network formed of nodes that receive the transactions. The nodes are in charge of checking the validity of the transactions; this means that each node checks the signature of the transactions it receives with respect to the version of the history it is aware of. Remember there is no central authority, hence no trusted copy of the ledger. Once



a node has checked enough transactions, it makes a “block.” A block is a batch of validated transactions that must comply with different requirements: it includes a reference to the last block the node knows (typically, a hash of this block), a timestamp, and the “proof.” (Figure 1) The proof is the piece of data required by the consensus algorithm. This algorithm allows nodes to agree on the right version of the ledger even though there is no reference version.

The consensus algorithm is the core aspect of the blockchain. Several techniques exist. The Bitcoin blockchain, for example, uses a proof-of-work based consensus: in order to produce a valid block, a node has to solve a computationally difficult task. More specifically, it has to find a *nonce*—a random number—such that the hash of the block has a correct number of leading zeros, defined by the algorithm. The nonce is the proof to be included in the block. Once a node has managed to produce such a block, it broadcasts it to the other nodes of the network. The other nodes then perform the following checks: check the validity of every transaction embedded in the block with respect to its local version of the history, check that the referenced previous block exists and is valid, check the timestamp is greater than the one of the previous block,

and check that the proof is correct. If the block is judged valid, then nodes append it to their version of the ledger, and start working on the next block.

Obviously, as there is no unique, central copy of the blockchain, several versions of it exist in the network at the same time. These different versions are called “forks.” (Figure 2) The rule for each node is to work on the longest valid chain it is aware of. By doing so, some forks are abandoned and only one of them eventually “wins.” Indeed, if a majority of CPU power behaves according to the rule, the chain that will grow the fastest is an “honest” chain. Imagine an attacker willing to “rewrite the history,” for example removing the transaction where the attacker gave money to buy a car, after the car is delivered. This attacker would have to go against all the honest nodes and still produce a longer chain. As changing a block changes its hash and hence breaks the chain, this attacker must invest huge computing power – in the case of a proof-of-work – especially when several blocks have been appended to the one he wants to change. When enough blocks have been appended, an attacker must surpass the power of all other nodes, and this is considered to be impossible. This is why in Bitcoin, one has to wait approximately

one hour for a transaction to be sufficiently “confirmed:” this is the time needed for computing six blocks forward. [4]

Smart Card Technology and Blockchain Applications

Many use cases and applications are now being developed that use blockchain technology, with the most prominent application for cryptocurrencies (e.g., Bitcoin). Established companies and new market entrants are also using blockchain technology to implement applications for interbank funds transfer, asset registries, anticounterfeiting and Internet of Things. Some of the important value propositions for blockchain-based applications vs. traditional implementations include:

- Faster, more real-time transactions
- Lower cost
- Ability to do real-time auditing
- Secure, non-repudiable transactions
- Ability to support autonomous actions
- Ability to support pseudonymous transactions

All implementations of blockchain-based applications have the common security requirements of generating, storing and managing the user’s cryptographic keys and would benefit from convenient user access and use of their keys.

The smart card chip or embedded secure element contains a secure microprocessor, RAM, nonvolatile memory, and (typically) a crypto-coprocessor. The memory and processors are protected physically, using a variety of software and hardware security technologies. Implementing blockchain applications using smart card and secure element technology brings the following benefits:

- Generates and protects user cryptographic keys. Smart card and secure element technology is purpose-built to perform key pair generation and other cryptographic operations quickly, with low power consumption. Because a hardware-based secure element is used, key pair generation is performed securely and is efficiently protected, even from advanced attacks. Smart card and secure element technology protects private keys in hardware with tamper-resistant

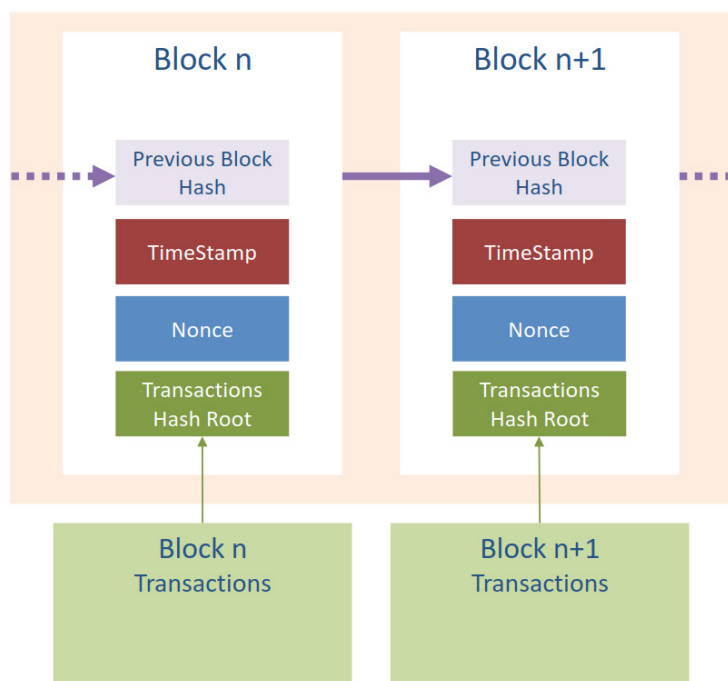


Figure 1. Creation of a Block

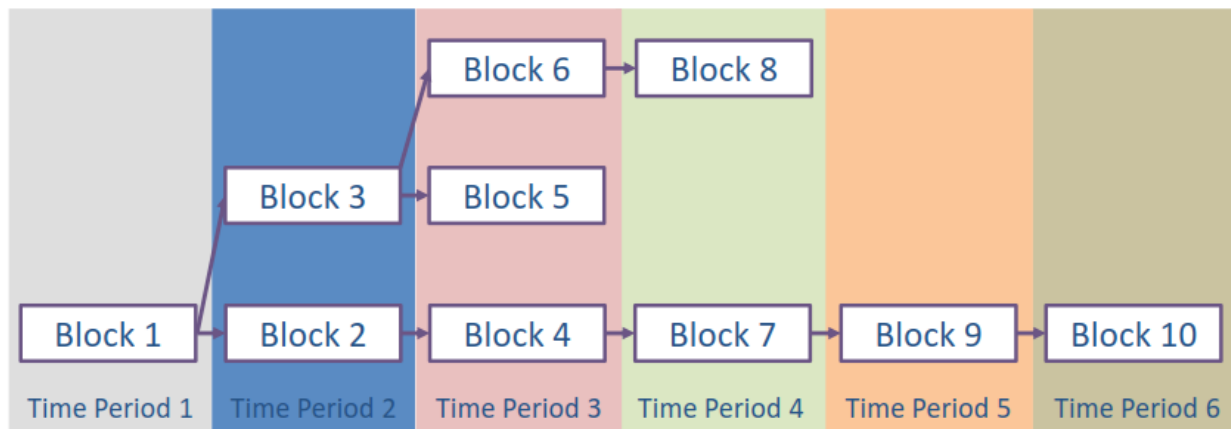


Figure 2. Blockchain Forks

hardware security and interaction restricted to a limited set of commands and responses.

- Provides straightforward user access to cryptographic keys. Smart card and secure element technology enables multiple form factors (e.g., card, USB devices, mobile device secure element, microSD, embedded secure element chip, wearables). This provides convenient, portable, user-controlled access to the keys used for blockchain transactions.
- Provides blockchain application implementers with a standards-based security platform and established standardized security evaluation and certification programs (e.g., Common Criteria).


The white paper, [Blockchain and Smart Card Technology](#), includes examples of smart card and secure element technology used in blockchain applications for vault and Near Field Communication (NFC) front-end use cases. Use cases for funds transfer, asset tracking, asset registry and the Internet of Things (IoT) would also benefit from using smart card and secure element technology for convenient key generation, access and management.

Conclusions

Blockchain technology is widely viewed as revolutionary due to the ingenious way it solves for a transparent, distributed consensus network that is resistant to manipulation or takeover by a central authority.

Blockchain has been dubbed by industry analysts as the fastest development software market in history. New blockchain applications are still emerging, and use beyond digital currencies is still being defined.

Blockchain's crucial innovation is a decentralized ledger, secured with cryptography, that ensures integrity, immutability, and no single point of vulnerability in the network. However, one remaining area of vulnerability is the private keys associated with ownership. If those private keys are lost or stolen, any associated coins or assets are lost forever. Many people have inadvertently erased their private bitcoin keys, and the associated bitcoins have essentially disappeared. In other cases, thieves have hacked into centralized exchanges, stolen private keys, and irretrievably transferred the assets.

Secure element and smart card technology can play a critical role in securing blockchain transactions in certain use cases, including cryptocurrencies and vaults, funds transfer, asset tracking, and the Internet of Things. Since blockchain applications may include the ability to execute contracts and make transactions, they must be secure: secret keys are used and need to be secured. Secure element technology, available in different form factors, can be used to generate, secure and manage these secret keys. 

Notes

[1] CB Insights webinar, "The State of Blockchain," <https://www.cbinsights.com/research-blockchain-transcript>.

[2] Wikipedia, [https://en.wikipedia.org/wiki/Block_chain_\(database\)](https://en.wikipedia.org/wiki/Block_chain_(database)).

[3] It is important to note that a blockchain application may support anonymous or pseudonymous users (as with Bitcoin) or the application may have a separate process for establishing a user's identity prior to producing a blockchain transaction. A "user" may be a person or non-person entity. Discussion of establishing user identity is not covered in this white paper.

[4] <https://en.bitcoin.it/wiki/Confirmation>

About this Article

This article is an extract from the Secure Technology Alliance Payments Council white paper, [Blockchain and Smart Card Technology](#), published in March 2017. The white paper provides a primer on blockchain technology, discusses use cases that are currently commercially available or being piloted, and reviews the role secure element/smart card technology plays in the different use cases. Payments Council members contributing to the white paper include: Capgemini; CH2M; CPI Card Group; First Data; FIS; Fiserv; Gemalto; Infineon Technologies; Ingenico Group; Kona I; NextGen ID Inc; NXP Semiconductors; Oberthur Technologies; PayGility Advisors; SHAZAM; Underwriters Laboratories (UL).

Updates from the Alliance Industry Councils

Access Control Council

- The [Access Control Council](#) submitted comments to GSA on the “Physical Access Control Systems (PACS) Functional Requirements and Test Cases (FRTC),” version 1.3.3, and to NIST on the [Draft SP 800-63 Digital Identity Guidelines](#) (in collaboration with the Identity Council).
- 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](#) has three active projects: Council charter update to align with the revised focus and mission of the Secure Technology Alliance; the Client Advisory Board; 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](#) has an updated charter to stimulate project activities and attract new members. The Council is now discussing possible projects for 2017.
- The Council collaborated with the Access Control Council to submit comments to NIST on the [Draft SP 800-63 Digital Identity Guidelines](#).

Internet of Things Security Council

- The [Internet of Things \(IoT\) Security Council](#) is developing material to recruit IoT industry stakeholders to participate in Council activities.

Mobile Council

- The [Mobile Council](#) published the new white paper, [Mobile Identity Authentication](#); the white paper provides an educational resource on mobile identity authentication techniques and use cases. Members contributing to development of the white paper included: Capgemini; CH2M; CPI Card Group; Discover Financial Services; First Data; FIS; HID Global; ID Technology Partners; Intercede; IQ Devices; JPMorgan Chase; Oberthur Technologies; Paygility Advisors; SHAZAM; TSYS; Vantiv; Verifone; and Wells Fargo.
- The Council is currently completing on two white papers – mobile profiles and provisioning; Trusted Execution Environment (TEE) 101 – and discussing possible new projects for 2017.

Payments Council

- The [Payments Council](#) published the new white paper, [Blockchain and Smart Card Technology](#); the white paper provides a primer on blockchain technology, discusses use cases that are currently commercially available or being piloted, and discusses the role secure element/smart card technology plays in the different use cases. Members contributing to the development of the white paper included: Capgemini; CH2M; CPI Card Group; First Data; FIS;



Fiserv; Gemalto; Infineon Technologies; Ingenico Group; Kona I; NextGen ID Inc; NXP Semiconductors; Oberthur Technologies; PayGility Advisors; SHAZAM; Underwriters Laboratories (UL).

- The Council is currently completing one project – EMVCo Payment Account Reference (PAR) use cases white paper – and discussing possible new projects for 2017.

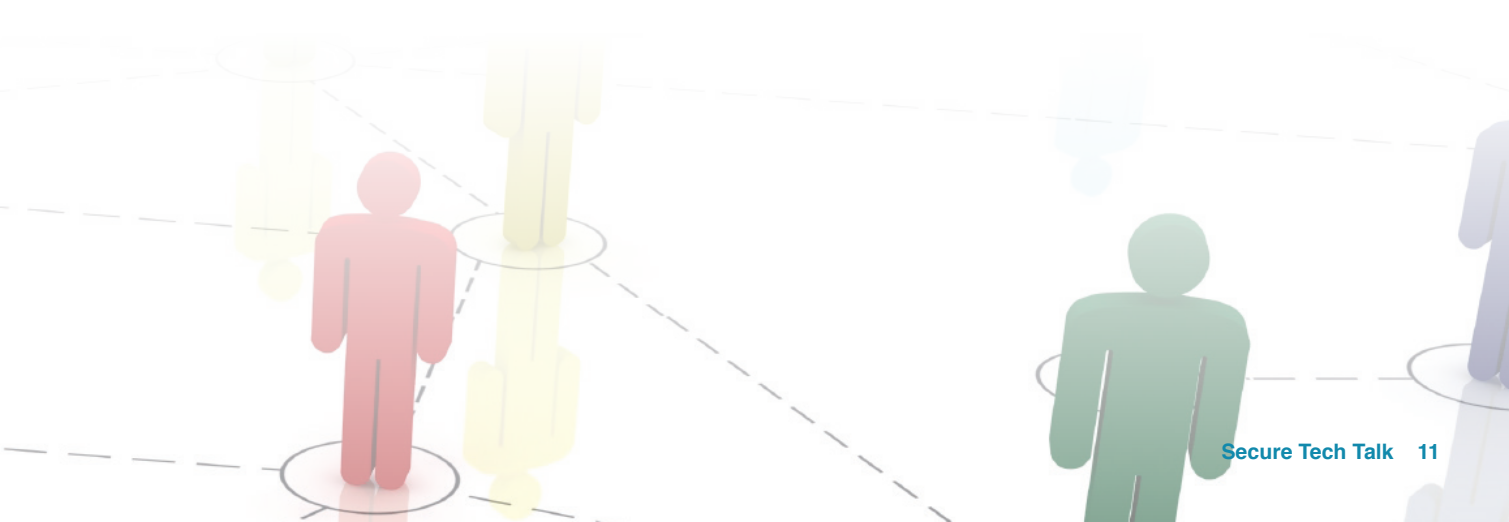
Transportation Council

- The [Transportation Council](#) published the new white paper, [Multimodal Payments Convergence – Part One: Emerging Models and Use Cases](#), developed in collaboration with the Association for Commuter Transportation. The white paper explores the rapidly evolving convergence of multimodal payment, describes emerging types of payments convergence, and provides current examples of convergence. Members contributing to the development of the white paper included: American Express; CH2M; Dallas Area Rapid Transit (DART); Gemalto; Giesecke & Devrient; InComm; INIT Innovations in Transportation; LTK Engineering Services; NXP Semiconductors; Mastercard; Metropolitan Transportation Commission (MTC); Oberthur Technologies; Southeastern Pennsylvania Transportation Authority (SEPTA); Thales Group; U.S. Department of Transportation (DOT)/Volpe Center; Vantiv; Waltz, Inc.
- The Council currently has two active projects – a new webinar on mobile ticketing and Near Field Communications (NFC) and a panel on EMV and Parking at the International Parking Institute's conference – and is discussing other 2017 activities. The Council is also defining the statement of work for the second part 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

- The Mobile, Payments and Transportation Councils held well-attended in-person meetings at the 2017 Payments Summit. During these meetings, Council members discussed past-year accomplishments, reviewed current project status and brainstormed possible new projects for 2017.
- The Council collaboration site has a new URL – [alliance-forumgroups.org](#) – and updated branding. All Councils use the site for document sharing, email lists and project management. If you are an Alliance member and would like to be added to any of the Council mailing lists, please contact [Mike Strock](#).
- 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 [Mike Strock](#). 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 [Cathy Medich](#).

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](#).



New Certification Recipients

CSCIP

- Jim Combs, Beeler Impression Produces*
- Joe Franco, Capture Technologies*
- Ross Kierstead, IDEXPERTS*
- Nate Williamschen, Entrust Datacard*
- David Yen, Visa*

CSCIP/Government

- Kevin Campbell, XTec
- Michael Casey, CertiPath
- Dan Currie, Department of National Defense
- Sok Bonn Dong, XTec
- Francisco Yuan, National Defense Canada

CSCIP/Payments

- Apurv Tripathi, American Express
- Nikita Jain, American Express
- Dipesh Paul, American Express-India Private Limited
- Anirban Roy, American Express
- Rohit Sinha, American Express

CSEIP Recipients

- Scott Chillemi, Identiv*
- John Coker, Identiv*
- Josh Ebert, Identiv*
- Stacey Kanter, Identiv *
- Bryan Semprie, Identiv*
- Sam Tuthill, Identiv*
- Ralph Boone, Kratos Public Safety & Security
- Patrick Lackey, Systems Applications & Solutions
- Marquis Laude, Integrated Security Solutions
- Dan Morrissey, United Security & Communications
- James Pinckney, BAE Systems
- Nicola Pisani, M.C. Dean, Inc.
- Osenaga Osagie, Chenega Management
- Timothy Smith, Chenega Management
- Duwan Tate, National Science Foundation
- Jefferson Tross, Versar

**Denotes corporate exam. For more information, contact Lars Suneborn*



Welcome New Members

- Advanced Card Systems
- Cardtek USA
- Chicago Transit Authority
- EFT Experts
- VenTek International

Secure Technology Alliance In The News

[“Secure Technology Alliance expands mission of former Smart Card Alliance,”](#) Secure ID News. Reporting on the new name and mission of the Secure Technology Alliance, Secure ID News says the Alliance is exchanging its somewhat limiting focus on smart cards for a broader view of chip-based secure technologies.

[“Waves of Change for Payments,”](#) Paybefore. This article by Executive Director Randy Vanderhoof summarizes the highlights of the 2017 Payments Summit, and discusses the overarching theme that ran through many of the sessions: how to adapt to the wave of change in payments.

[“Blockchain without smart card technology is like a house without a roof,”](#) Jaxenter. In this article, Executive Director Vanderhoof talks about the Secure Technology Alliance’s blockchain-focused white paper, organizations’ need for blockchain, smart card technology and blockchain’s potential in IoT.

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



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).