

PAYMENT SOLUTIONS FOR TRANSPORTATION
EMBEDDED CHIP TECHNOLOGY

SECURE HARDWARE AND SOFTWARE SOLUTIONS
EMV AND CONTACTLESS PAYMENT CARDS

Annual Review 2017



NFC AND MOBILE PAYMENTS
HEALTHCARE DATA SECURITY
ACCESS CONTROL

INTERNET OF THINGS

IDENTITY AND SECURITY



SECURE
TECHNOLOGY
ALLIANCE



G+D
Mobile Security

mobile secyourity

It's all about
managing
identities.

EXECUTIVE DIRECTOR'S LETTER: A MESSAGE FROM RANDY VANDERHOOF

Delivering Value to a Diverse Market

Thank you for taking the time to read the 2017 Annual Review. This publication captures the best aspects of the membership experience for 2017 that hundreds of individual members and their organizations helped to provide. This year was especially significant, as the organization expanded its mission beyond smart cards and was re-branded as the Secure Technology Alliance. The new name and scope allows the Alliance to include embedded chip technology, hardware and software, and the future of digital security in all forms.

The vast number of deliverables and member-driven activities recorded in the publication illustrates the diversity of the markets we serve and the commitment of all the industry professionals who contribute their knowledge and leadership toward expanding the market for smart card and related secure chip technologies.

CHANGE COMES WITH NEW OPPORTUNITIES

The decision to expand the mission and rebrand the organization was driven by the changes in the secure chip industry, mostly from mobile technology and the growth of Internet-connected devices. This does not mean the market for smart cards has disappeared. In fact, over the last few years, the U.S. saw the largest mass issuance of EMV chip cards in the world outside of China. The mobile and IoT markets need further education and thought leadership on how to apply smart card technology security principles to make mobile and Internet of Things (IoT) devices secure. That's precisely where our strength lies, and what generates the highest value for our members. In my 15 years as Executive Director, the markets for smart cards and secure chip technology have grown from tens of millions to over one billion units shipped. This growth is expected to continue in the IoT market, which is expected to exceed 23 billion devices in 2020. It will be a challenge to secure all those devices, but the industry is ready.

The Secure Technology Alliance relies on its two affiliated organizations to further advance secure technology. The U.S. Payments Forum continues to be the leading industry body to address issues related to the adoption of EMV technology and the complex issues of mobile wallet adoption, the acceptance of contactless payments, and the business drivers and acceptance challenges of implementing card-not-present fraud tools among issuers and merchants. The Forum is where industry leaders resolve real obstacles affecting the adoption of advanced payments technologies to reduce fraud and enable secure digital transactions online and in physical stores. SCALA, the Latin American chapter, is advancing the use of digital technologies for national ID programs, consumer payments, and transportation.

A BRIGHT FUTURE AHEAD

Our members have been the core security technology innovators in payments, identity, and mobile for many years. The Alliance has a solid foundation of individuals with the knowledge, experience, and vision for security to lead those organizations building the smart commerce, smart home electronics, smart healthcare, and smart cities of the future.

The Secure Technology Alliance maintains its industry leadership through collaborative industry councils, training and certification programs, conferences, workshops and webinars. The Alliance performs outreach to other standards bodies and industry groups, and communicates to the outside world via the Internet, media relations, and speaking engagements across the Americas and around the world.

We will continue our support for the smart card technology in use today and prepare for the new digital security technologies for the future. Our organization will grow stronger, bring increased value to our members, and accelerate the adoption of secure chip technology and related hardware and software.

I wish you all continued success and I thank you for your support of our expanded mission and new name.

THE DECISION TO EXPAND THE MISSION AND REBRAND THE ORGANIZATION WAS DRIVEN BY THE CHANGES IN THE SECURE CHIP INDUSTRY, MOSTLY FROM MOBILE TECHNOLOGY AND THE GROWTH OF INTERNET-CONNECTED DEVICES THAT RELY ON EMBEDDED SECURITY CHIPS.



Randy Vanderhoof
Executive Director,
Secure Technology
Alliance



The Secure Technology Alliance Annual Review is produced by the Secure Technology Alliance, 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.

PUBLISHER

Randy Vanderhoof
rvanderhoof@securetechalliance.org

MANAGING EDITOR

Debra Marshall
dmarshall@securetechalliance.org

EXECUTIVE EDITOR

Cathy Medich
cmedich@securetechalliance.org

ADVERTISING EDITOR

Shelbey Votapek
svotapek@securetechalliance.org

CONTRIBUTORS

Edgar Betts, Solmoraine Guzmán C., Jack Jania, Gerald Kane, Heather Klein, Nicole Lauzon, Oliver Manahan, Debra Marshall, Cathy Medich, Sadiq Mohammed, Morgan Richard, Brian Russell, Adam Shane, Sridher Swaminathan, Randy Vanderhoof, Shelbey Votapek

ART DESIGN AND PRODUCTION

AVISIAN

COVER DESIGN

Edward Maichin

MAIN OFFICE

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550
800.556.6828
www.securetechalliance.org

Membership inquiries or comments?
Please email info@securetechalliance.org

Copyright © 2017 Secure Technology Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Secure Technology Alliance. The Secure Technology Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Secure Technology Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this publication.



36 – ACCESS CONTROL COUNCIL



40 – HEALTH AND HUMAN SERVICES COUNCIL



42 – IDENTITY COUNCIL



44 – IOT SECURITY COUNCIL



48 – MOBILE COUNCIL



52 – PAYMENTS COUNCIL



56 – TRANSPORTATION COUNCIL

ANNUAL REVIEW CONTENTS



SECURE
TECHNOLOGY
ALLIANCE

- 3 **Executive Director's Letter**
[A Message from Randy Vanderhoof: Delivering Value to a Diverse Market](#)
- 6 **Year in Review:**
[A Message from Brian Russell, Outgoing Board Chair, Secure Technology Alliance, 2015-2017 A Year of Transition](#)
- 7 **Year in Review:**
[A Message from Jack Jania, Incoming Board Chair, Secure Technology Alliance, 2017-2019 Security: As Important As It's Ever Been](#)

8 ABOUT THE ALLIANCE

- 8 [Alliance Management](#)
- 9 [Board of Directors](#)
- 10 [Membership Benefits](#)
- 12 [2017 Member Survey Report on Member Satisfaction and Value of Alliance Activities](#)
- 14 [Membership List](#)
- 15 [Leadership Council](#)
- 16 [Member Profiles](#)
- 18 [Member Recognition Program](#)
- 20 [Training and Certification Programs](#)
- 22 [CSEIP and CSCIP Recipients](#)
- 23 [2017 Professional Certification Trainers](#)
- 24 [2017 Conferences and Events](#)
- 26 [2017 Conference Sponsors](#)
- 27 [2018 Conferences and Events](#)
- 28 [2017 Event Photos](#)
- 30 [Executive Director Letter Highlights](#)
- 32 [Web Site Highlights](#)

34 INDUSTRY COUNCILS

- 35 **Year in Review: Industry Councils Letter**
[A Look at Our Councils in 2017 Nimble Councils Deliver Visibility and Generate Sales](#)

36 ACCESS CONTROL COUNCIL

- 37 **Year in Review: Access Control Council Chair**
[Technology as a Protector](#)
- 38 [Industry Commentary: OMB Circular A-130 – Managing Information as a Strategic Resource](#)

40 HEALTH AND HUMAN SERVICES COUNCIL

- 41 **Year in Review: Health and Human Services Council Chair**
[A Year of Focus](#)

42 IDENTITY COUNCIL

- 43 **Year in Review: Identity Council**
[A Look at the Identity Council](#)

44 IOT SECURITY COUNCIL

- 45 **Year in Review: IoT Security Council**
[A Look at the Internet of Things Security Council](#)
- 46 [Embedded Hardware Security for IoT Applications](#)
- 47 [IoT Payments Market Landscape](#)

48 MOBILE COUNCIL

- 49 **Year in Review: Mobile Council co-Chairs**
[Innovations Make for an Exciting Time in Mobile](#)
- 50 [Mobile Identity Authentication](#)

52 PAYMENTS COUNCIL

- 53 **Year in Review: Payments Council co-Chairs**
[Innovation in the Payments Industry](#)
- 54 [Implementation Considerations for Contactless Payment-Enabled Wearables](#)
- 55 [Blockchain and Smart Card Technology](#)

ADVERTISERS

- 2 G+D Mobile Security
- 25 Discover Financial Services
- 59 Fiserv
- 33 Infineon Technologies
- 75 IDEMIA

56 TRANSPORTATION COUNCIL

- 57 **Year in Review: Transportation Council Chair**
[Open Payments, Payments Convergence and Smart Cities Take Spotlight](#)
- 58 [Multimodal Payments Convergence – Part One: Emerging Models and Use Cases](#)

60 U.S. PAYMENTS FORUM

- 60 [New Membership Levels Offered Participation in Forum and Alliance Activities](#)
Looking ahead, Forum plans to prioritize mobile and contactless payment guidance for issuers and merchants
- 60 [U.S. Payments Forum Officers and Steering Committee](#)
- 61 **Director's Letter: A message from Randy Vanderhoof**
[U.S. Payments Forum – Looking Beyond EMV](#)
- 62 [U.S. Payments Forum Resources](#)
- 63 [U.S. Payments Forum Working Committees](#)
- 64 [U.S. Payments Forum Membership Mix](#)
- 65 [U.S. Payments Forum Members](#)

66 LATIN AMERICA CHAPTER

68 SECURE TECHNOLOGY ALLIANCE MEMBER DIRECTORY

YEAR IN REVIEW: A MESSAGE FROM OUTGOING BOARD CHAIR BRIAN RUSSELL SECURE TECHNOLOGY ALLIANCE CHAIR, 2015-2017

A Year of Transition

While we formally started the year as the Smart Card Alliance, we engaged the full Alliance membership to assist in the transition to our newly branded Secure Technology Alliance. Similar rebranding efforts had occurred for the U.S. Payments Forum and at several of our member organizations, including my own organization transitioning from Giesecke & Devrient to G+D Mobile Security. Oberthur transitioned to OT-Morpho and now IDEMIA, and Xerox transitioned to Conduent. Change is always an interesting challenge, letting go of the old and embracing the new – along with all the uncertainty and excitement that accompanies it.

CHANGES AROUND

From an industry standpoint, we have also seen a lot of transition this year. The Real ID Act extensions are concluding, which means a lot of changes pending for the identification sector. We are seeing a stronger emergence of digital identities and the management thereof, which rises out of the severe impact of the data breaches. We are finishing the transition of magnetic stripe cards to EMV and finding ways to mitigate fraud in card-not-present transactions. For transit, next generation ticketing is emerging, taking us from the card to mobile and even to ticketless transactions. The plug-in SIM is being replaced by an embedded secure element and an electronic SIM, allowing for the emergence of new devices like wearables and connected cars.

EMBRACING THE NEW

As we become more mobile, our identities are linked to everything. We are no longer a home phone number, a mobile number, and three bank accounts. Our digital identities are everywhere. They are ubiquitous and linked to each other in ways that we don't even realize, let alone know how to manage. The Internet of Things (IoT) permeates all of our communications, payments and transactions, and it's up to us – an alliance of experts – to work together as it relates to those communications. Things like buying/paying and authentication are key. In order to ensure that someone hacking your coffee maker can't empty your bank account, we have to find unobtrusive methods of securing the connected everything. Security has to come first and not added as an afterthought – built in from the start.

I am proud to have been part of the Alliance's extensive efforts in responding to the market changes and driving new innovations to add real value to this new IoT landscape.

I look forward to continuing the transition with you in 2018. As this concludes my two-year term as chairman of the Alliance board, I wish my friend and colleague Jack Jania of Gemalto, who was recently elected to serve as chairman, the best of luck, with the knowledge that he will be working with very dedicated, hard-working, and passionate individuals in the Alliance.

IN ORDER TO ENSURE THAT
SOMEONE HACKING YOUR
COFFEE MAKER CAN'T EMPTY
YOUR BANK ACCOUNT, WE
HAVE TO FIND UNOBTUSIVE
METHODS OF SECURING THE
CONNECTED EVERYTHING.
SECURITY HAS TO COME FIRST
AND NOT BE ADDED AS AN
AFTERTHOUGHT – BUILT IN
FROM THE START.



Brian Russell

Former Senior Vice President,
Financial Institutions
Giesecke & Devrient Mobile
Security Americas Inc.

YEAR IN REVIEW: A MESSAGE FROM INCOMING BOARD CHAIR JACK JANIA SECURE TECHNOLOGY ALLIANCE CHAIR, 2017-2019

Security: As Important As It's Ever Been

I'd like to thank the Alliance for electing me as chairman of the board, as well as send my gratitude to Brian Russell. His two-year tenure as chairman has set up both me and the Alliance for success in the future.

Picking up where Brian left off, it has indeed been a year of transition, and I expect that trend to continue. We've all heard the statistic: the Internet of Things is said to reach more than 20 billion connected devices by 2020, according to Gartner's market research, from smart appliances and connected cars to M2M modules and computers with endless connectivity through embedded SIM cards. The Alliance's focus has been, and will continue to be, educating on the security challenges associated with this growth so that the technology industry can not only capitalize on that growth but also protect their customers and end users.

NEW CONCEPTS EVOLVING

While our key areas of concentration remain the same, new solutions and concepts are evolving every day, and I expect to see more and more overlap across the varying councils. Identity can stand on its own but it's also woven into every other type of technology.

Payment is another expanding identity opportunity. Key features are being woven into new use cases such as mobile payment, transportation and online shopping. By securing those transactions and decreasing card-not-present fraud, we can protect both financial institutions and consumers.

ROAD TO SECURITY

The media has been abuzz with the news that 143 million Americans' personal information was exposed in a data breach at Equifax. Everyone from consumers to key technology players are reeling, but the lesson is clear: the fight for a more secure digital world is nowhere near its end. The efforts of the Secure Technology Alliance are just as, if not more, valuable to the industry today and moving forward, as we expect these type of breaches to continue. As technology gets smarter, so do hackers.

But by continuing to serve as a leading educator on secure technology solutions, we have the opportunity to pioneer that movement forward with new resources and membership growth.

Again, I'd like to thank the executive board for their support in this new position. I look forward to a new year, and I am honored to serve alongside each of you.

WITH SO MANY EXTRA DEVICES AND METHODS OF CONNECTING, BEING ABLE TO **SECURELY PROVE YOU ARE WHO YOU SAY YOU ARE** IS INVALUABLE IN SITUATIONS LIKE OPENING A NEW BANK ACCOUNT FROM A REMOTE LOCATION ON A MOBILE DEVICE.



Jack Jania

Senior Vice President of
Strategic Partnerships
Gemalto

ALLIANCE MANAGEMENT

RANDY VANDERHOOF

Executive Director

rvanderhoof@securetechalliance.org

Randy Vanderhoof is the Executive Director of the Secure Technology Alliance, formerly known as the Smart Card 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. In addition to his leadership role with the Secure Technology Alliance, in August 2012 Randy became the Director of the U.S. Payments Forum (formerly called the EMV Migration Forum), an independent, cross-industry organization established to support the alignment of global payment networks, regional payment networks, issuers, processors, merchants, and industry suppliers.

Randy is a frequent speaker at high-level industry events, including Money 20/20, has appeared on major network news broadcasts, and is featured in industry publications for his extensive background in secure payment solutions. Randy is also a contributor to blogs and often authors columns on topics including Internet of Things, security, mobile payments, and access and identity.

Randy has led the Alliance since 2001. Prior to that, he spent a majority of his professional career in management positions with a number of global organizations involving smart card identity and payments technology.

Randy is a graduate of Saint Joseph's University in Philadelphia, PA, with a B.S. in Management Marketing. He received his M.B.A. from Rider University in Lawrenceville, NJ.

EDGAR BETTS

Associate Director, SCALA

ebetts@sca-la.org

Edgar Betts came to the Alliance in March 2005 to help develop and complete the Market Development Cooperator Program (MDCP) grant for Latin America issued by the International Trade Administration to the Alliance. He is now responsible for the Latin American and Caribbean chapter of the Alliance. Prior to joining the organization, Edgar was the Executive Director and Co-Founder of the Smart Card Division for Integra Group Corporation, responsible for the promotion, distribution, and implementation of smart card and RFID solutions for the Central American and Caribbean markets. He also worked under the Director of Electronic Business Technologies at the U.S. General Service Administration (GSA). Edgar has a B.A./B.S. in Economics and International Affairs from Florida State University.

BRYAN ICHIKAWA

Consultant, Event Marketing and Sales

bichikawa@securetechalliance.org

Bryan Ichikawa serves as a consultant to the Secure Technology Alliance, and is responsible for marketing and sales for the organization's events and conferences. Bryan has more than 30 years of security technology, systems integration, and program management experience. He previously worked for Deloitte, Unisys, and Thomson Media. He holds a B.A. from Lynchburg College.

KRISTIN KREBS

Coordinator, Conference Services

kkrebs@securetechalliance.org

Kristin Krebs is responsible for supporting event and conference logistics for the Secure Technology Alliance and U.S. Payments Forum. She is a graduate of Katherine Gibbs College.

NICOLE LAUZON

Membership

nlauzon@securetechalliance.org

Nicole Lauzon is responsible for membership management and database support for both the Secure Technology Alliance and U.S. Payments Forum. A 2005 graduate of Douglass College at Rutgers University, she joined the Alliance in 2009.

DEBRA MARSHALL

Director, Communications

dmarshall@securetechalliance.org

Debra Marshall is Communications Director for both the Secure Technology Alliance and the U.S. Payments Forum. Her responsibilities include developing and editing monthly and quarterly newsletters for the two organizations, maintaining website content, creating original copy, and supervising logo and branding development. She handles daily and weekly news digests for members, and coordinates all written announcements, updates and news alerts. Debbie graduated cum laude with a B.A. in Communications from Seton Hall University.

CATHY MEDICH

Director, Strategic Programs

cmedich@securetechalliance.org

Cathy Medich is Director of Strategic Programs the Secure Technology Alliance, and Associate Director for the U.S. Payments Forum. In these roles, she manages marketing and industry initiatives, directs industry council and working committee activities, and manages strategic projects. Working with member teams, Cathy leads the development of educational resources covering priority topics for the industry. Cathy has over 20 years of experience in marketing and strategic planning for technology businesses, including consulting engagements or positions with Hewlett-Packard, VeriSign, Verifone and CommerceNet. Cathy has B.S. and M.S. degrees in Electrical Engineering and Computer Sci-

ence from M.I.T. and an M.B.A. from the Wharton Graduate School.

JACLYN SAUVÉ

Manager, Conference Services

jsauve@securetechalliance.org

Jaclyn Sauvé is the Manager of Conference Services for the Secure Technology Alliance and U.S. Payments Forum, leading the logistic support team responsible for all conference operations. Jaci also supports each conference program committee as a speaker liaison and the sales and marketing staff by managing all exhibitor and sponsor communications. Jaci holds a degree in Communications/Media with a concentration in video production from Western Connecticut State University.

MIKE STROCK

Project Coordinator, Industry Councils

mstrock@securetechalliance.org

Mike Strock serves as the Project Coordinator for Industry Councils for the Secure

Technology Alliance. He joined the organization in late 2014 after supporting projects and Working Committee efforts for the U.S. Payments Forum since June 2013, a role he continues. Prior to his experience with the Alliance and Forum, Mike supported EMVCo and GlobalPlatform. Mike holds a Master of Science in Business Administration from Texas A&M and a B.A. in both Public Relations and Spanish from Weber State University.

LARS SUNEORN

Director, Training Programs

lsuneorn@securetechalliance.org

Lars Suneorn is responsible for directing all of the Alliance training programs for members and industry professionals. He works to promote the industry credentials to organizations, leads training classes, and arranges corporate training courses. Before joining the Secure Technology Alliance in 2014, Lars worked for more than 30 years in the security industry, where his numerous achievements included developing the concept and implementation plan

for nationwide E-PACS network for several Federal agencies. Lars holds an Electronic Engineering degree from Aso Technical, in Stockholm, Sweden.

SHELBEY VOTAPEK

Consultant, Communications

svotapek@securetechalliance.org

Shelbey Votapek joined the Secure Technology Alliance in 2013. She currently manages all electronic communications for the Alliance and U.S. Payments Forum. Shelbey oversees the maintenance of the web sites and assists on various projects for both the Alliance and Forum, including newsletter distribution, member awards and recognition, and Annual Review advertising. Prior to becoming a consultant with the Alliance, Shelbey worked for Verizon Wireless, Realogy Corporation and Comcast. She has a Master of Business Administration from Centenary College and a Bachelor Degree in International Business and Marketing from Fairfield University.

BOARD OF DIRECTORS

2016-2017 EXECUTIVE COMMITTEE

Chair: Brian Russell, G+D Mobile Security

Vice Chair: Jack Jania, Gemalto

Treasurer: Brian Stein, CH2M

Assistant Treasurer: Morgan Richard, XTec, Inc.

Secretary: Thomas Lockwood, NextgenID, Inc.

Technology Vice Chair: Kelly Urban, First Data Corporation

2017-2019 EXECUTIVE COMMITTEE

Chair: Jack Jania, Gemalto

Vice Chair: Oliver Manahan, Infineon Technologies

Treasurer: Brian Stein, CH2M

Assistant Treasurer: Morgan Richard, XTec, Inc.

Secretary: Tom Lockwood, NextgenID, Inc.

Assistant Secretary: Kelly Urban, First Data

Technology Vice Chair: Allen Friedman, Ingenico

2016-2017 DIRECTORS

Tim Baldridge, U.S. Department of Defense/
Defense Manpower Data Center

Jane Cloninger, Accenture (beginning July 2017)

Willy Dommen, Accenture (through July 2017)

Allen Friedman, Ingenico

Melanie Gluck, Mastercard

Wendy Humphrey, Conduent

Simon Hurry, Visa Inc.

Thomas Lockwood, NextgenID, Inc.

Oliver Manahan, Infineon Technologies

Elinor Smith, Discover Financial Services

Garfield Smith, IDEMIA

2017-2018 DIRECTORS

Tim Baldridge, U.S. Department of Defense/
Defense Manpower Data Center

Allen Friedman, Ingenico

Melanie Gluck, Mastercard

Wes Haworth, Verifone

Simon Hurry, Visa Inc.

Oliver Manahan, Infineon Technologies

Eric Megret-Dorne, G+D Mobile Security

Elinor Smith, Discover Financial Services

Garfield Smith, IDEMIA

MEMBERSHIP BENEFITS

Your membership dollars support these Alliance activities and more:

- Council initiatives
- Conferences and events
- Daily industry news bulletins
- Industry commentary
- Media outreach
- Monthly and quarterly newsletters
- Website content

These efforts all help to contribute to the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software.

There is something for everyone in the Alliance. Members and their organizations enjoy:

- ✓ **Networking** – Establishing valuable contacts to help your organization improve and grow, using meetings and events to maximize business opportunities
- ✓ **Lower research or implementation costs** – Sharing work with peers from other organizations to reduce the time and cost needed to evaluate new business models, think through and plan complex implementation details, develop best practices and resolve industry issues
- ✓ **Advance knowledge** – Gaining market advantage by getting information and acting on it before many “outsiders” know it is happening
- ✓ **Growing the pie** – Working collectively with other organizations and end users to help to grow the size of the market for secure technologies

The Secure Technology Alliance is a unique organization where individuals from U.S. and multi-national companies, government agencies, industry associations, and industry suppliers meet to exchange ideas, discuss common issues and work together to further the adoption of secure technologies. Members represent a mix of users implementing secure applications and leading industry suppliers of the full range of products and services supporting the implementation of systems for secure payments, identification, access, and mobile communications.



“The Metropolitan Transportation Authority has benefited greatly from the information sharing and collaborative nature of Secure Technology Alliance’s activities. We may be at an inflection point for the convergence of transit merchants into the broader retail payments industry, and the cooperative dialogue that occurs within the Alliance is a critical component towards understanding the issues important to successful cross-industry coordination. The Alliance provides a robust forum for any person or organization seeking to explore possible areas for convergence or exploration of innovative next-generation payment technologies.”

Joshua C. Martiesian
*Payments Business Development,
Metropolitan Transportation Authority*





"I appreciate receiving member communications as they are generally informative and valuable."

Walter Hamilton
ID Technology Partners



- ✓ Alliance meetings and conferences
- ✓ Company visibility
- ✓ Information, research and education
- ✓ Support for standards and industry interoperability
- ✓ Outreach to government and commercial organizations
- ✓ Innovative ways of approaching common business goals
- ✓ Training and professional development



2017 MEMBER SURVEY

REPORT ON MEMBER SATISFACTION AND VALUE OF ALLIANCE ACTIVITIES

Each year the Secure Technology Alliance conducts an annual member survey to understand what members value and how satisfied members are with our programs and deliverables. For the 2017 survey, we received 129 responses from 54 member organizations. Also new this year – questions regarding the re-branding and expansion of the organization, from the former Smart Card Alliance to the Secure Technology Alliance.

SURVEY HIGHLIGHTS

Overall satisfaction increased slightly from 2016 - 84.3 rating in 2017 vs. 83.9 rating in 2016

- 86% of respondents are still clearly satisfied
- Value and satisfaction with Alliance activities were similar to or slightly better than 2016
- Members showed strong support for the expanded mission and re-branding

VALUE OF ALLIANCE OFFERINGS

Members continue to value, and be satisfied with, Alliance events, communications, publications and council activities.

- Events: complimentary and discounted registration to Alliance events; networking opportunities; speaking opportunities at Alliance events
- Communications: Secure Technology Alliance public website; members-only website; email announcements about Alliance events; EMV Connection website, GoChipCard website
- Publications: Annual Review yearly publication; Council white papers and reports; industry council participation



ALLIANCE REBRANDING

In last year's survey, members were asked whether they would support rebranding the organization and changing its focus to embrace technology beyond smart cards. Members were favorable then, and we are delighted that this year's survey revealed that 86% of respondents rated the expanded mission as either valuable/very valuable/highest value regarding their continued interest in the Alliance.

TOP FIVE RATED MEMBER BENEFITS

1. Knowledge from industry contacts in the Alliance
2. Networking
3. Market intelligence
4. Thought leadership opportunities
5. Participation in council projects and activities

SATISFACTION RATINGS

On a scale of 1 to 5:

- 4.15 – Published resources
- 4.13 – Communications programs and activities
- 4.11 – Conference and events
- 4.06 – Council activities
- 3.69 – Training and certification programs

86%

of respondents agreed that expanding the mission of the Alliance was very valuable

63%

of respondents participated in one or more councils

Active members and council members typically had higher than average **satisfaction**



WHAT'S IMPORTANT TO YOU

We use the Annual Survey to get input on the most important topics for Alliance activities in the coming year. We have an open-ended question to learn what members feel are the most important industry issues. Multiple write-in responses included:

- Cybersecurity
- IoT ecosystem security
- Payment in IoT
- Software and cloud based security
- IoT and smart cities
- Security issues in mobile
- CNP fraud/ecommerce
- Security and authentication
- Promoting the secure element in mobile
- Digital transformation

ALLIANCE PARTICIPATION AND ENGAGEMENT

Each year, we also get feedback from the survey that there are a significant number of members who are unaware of Alliance programs or who would like to get more engaged.

- Make sure you're getting our monthly member bulletins and Daily News Digest. Contact Debra Marshall, dmarshall@securetechalliance.org to receive the communications
- Create a login to the [Alliance members-only site](#) for special content
- Follow us on Twitter or join one of our LinkedIn Groups
- Join one of our [industry councils](#)
- Attend one of our conferences, webinars, workshops or training programs for education and networking opportunities

We value all members' opinions on how the Alliance is meeting your needs and what you would like to see us do differently. We'd love to hear more from you!

We thank everyone who responded to the 2017 member survey!

"The Secure Technology Alliance has been instrumental in bringing together key players from industry and government for addressing important issues this whole community has been confronted with. It facilitated a continuous dialogue with lawmakers and other external stakeholders, contributing greatly to the adoption of major smart card-based ID programs"

Stefan Barbu, NXP Semiconductors

"The Secure Technology Alliance is a great forum to both exchange ideas and advance smart card innovations and applications. The Alliance is also an authoritative source when it comes to promoting the benefits of RFID or contactless technologies, and plays an important role in educating the consumer about the value of these technologies"

John Vasilj, Accenture

"The councils are a great benefit – both for personal education, and to help promote ideas in the industry"

Oliver Manahan, Infineon Technologies

"Great events. They help steer the industry's direction toward more secure technologies"

Sridher Swaminathan, First Data

"The Secure Technology Alliance is one of the few independent organizations driving change within the emerging smart card and NFC markets in the USA. They provide a great forum in which to obtain agreement around the conflicting concerns of the various stakeholders"

Nick Norman, Consult Hyperion

MEMBERSHIP LIST

- A LA CARD Marketing and Consulting Services Limited
- ABCorp NA Inc.
- Accenture
- ACI Worldwide
- ACT Canada
- Advanced Card Systems, Ltd.
- Allegion
- AMAG Technology, Inc.
- American Express
- Argotechno
- Benefit Resource, Inc.
- Burden Consulting, Ltd.
- Cardtek USA
- CertiPath Inc.
- CH2M
- Chase Card Services
- Chenega Management, LLC
- Chicago Transit Authority
- China UnionPay USA
- Clear2Pay
- Consult Hyperion
- CPI Card Group
- Cubic Transportation Systems, Inc.
- Dallas Area Rapid Transit (DART)
- Datawatch Systems, Inc.
- Defense Manpower Data Center
- Department of Homeland Security
- Department of the Interior
- Discover Financial Services
- E4 Security Consulting, LLC
- EFT Experts
- Entrust Datacard
- Exponent, Inc.
- FEITIAN Technologies Co., Ltd.
- FIME
- First Data Corp.
- FIS
- Fiserv
- G+D Mobile Security
- Gallagher Group Limited
- Gemalto
- General Services Administration
- Genfare
- Glenbrook Partners, LLC
- Global Enterprise Technologies Corp.
- Hewlett-Packard Enterprise Services, LLC
- HID Global
- Hillsborough Transit Authority
- ICMA
- IDEMIA
- Identification Technology Partners, Inc.
- Identiv
- InComm
- Infineon Technologies
- Ingenico, North America
- Init Innovations in Transportation
- Initiative for Open Authentication
- Integrated Security Technologies, Inc.
- Interac Association/Acxsys Corporation
- Intercede Limited
- Invoke Technologies
- IPS Group, Inc.
- IQ Devices
- Jack Henry Processing Solutions
- JCB International Credit Card Co., Ltd
- KICTeam, Inc.
- KONA I co. Ltd.
- Leidos, Inc.
- Lenel
- Linxens Holding SAS
- LTK Engineering Services
- Malaysian Electronic Payment System SDN BHD (MEPS)
- Massachusetts Bay Transportation Authority
- Mastercard Worldwide
- Metropolitan Transportation Authority
- Metropolitan Transportation Center
- Moneris
- Monitor Dynamics
- Morpho (SAFRAN) – now IDEMIA
- Multos International PTE LTD.
- National Institute of Standards and Technology
- NBS Technologies, Inc.
- NextgenID, Inc.
- NXP Semiconductors
- Nxt-ID, Inc.
- Oberthur Technologies – now IDEMIA
- Parsons Corporation
- Port Authority of NY/NJ
- Port Authority Transit Corporation
- Q-Card Company
- Quadagno & Associates, Inc.
- Raak Technologies
- Rambus
- RF IDEas
- SAIC - Science Applications International Corporation
- San Francisco Bay Area Rapid Transit District (BART)
- San Mateo County Transit District
- Scheidt & Bachmann USA
- SecureKey Technologies
- Servired, Sociedad Espanola de Medios de Pago, S.A.
- SHAZAM
- Signet Technologies, Inc.
- Southeastern Pennsylvania Transportation Authority (SEPTA)
- Stanley Black & Decker
- STMicroelectronics
- SureID, Inc.
- Systems Engineering, Inc.
- Thales
- The Johns Hopkins University Applied Physics Lab
- The Utah Transit Authority
- TransLink
- Tri County Metropolitan Transportation District of Oregon
- Tyco Integrated Security
- Tyco Software House
- U.S. Department of State
- Ultra Electronics Card Systems
- Underwriters Laboratories (UL)
- US Department of Transportation/ Volpe Center
- US Government Printing Office
- Valid USA
- VenTek International
- Veridt, Inc.
- VeriFone
- Visa Inc.
- Vix Technology
- Waltz, Inc.
- Wells Fargo
- XTec, Inc.

As of September 30, 2017

LEADERSHIP COUNCIL

accenture



ch2m



CONDUENT



DISCOVER
GLOBAL NETWORK

First Data

FIS

gemalto
security to be free

G+D
Mobile Security

IDEMIA
augmented identity

infineon

ingenico
GROUP



leidos



SAIC

VALID

vantiv

VISA



Learn how to upgrade your membership online:
www.securetechalliance.org/membership-information



MEMBER PROFILES

In our Secure Tech Talk quarterly industry newsletter, we turn the spotlight on a Leadership Council member company. This popular feature focuses on both the company's membership point of contact and their company, offering an opportunity for members to learn more about the business profiles of their professional colleagues. Access the complete interviews by visiting the [Secure Technology Alliance website](#).

FEBRUARY 2017 MEMBER PROFILE



FIS

FIS is the world's largest global provider dedicated to financial technology solutions. FIS empowers the financial world with software, services, consulting, and outsourcing solutions focused on retail and institutional banking, payments, asset and wealth management, risk and compliance, trade enablement, transaction processing and record-keeping.

Secure Tech Talk spoke about the company's services and solutions with Bob Woodbury, senior vice president of FIS and general manager of NYCE Payments Network, LLC and PayNet Payments Network, LLC, both FIS companies. Bob manages the growth of nationwide and international access of NYCE to thousands of financial institutions throughout the U.S. and the international financial community.



Bob Woodbury

"Smart cards are a key technology enabler for financial institutions, and we're a leader in smart card production, having launched over 8,500 EMV card programs for more than 3,200 U.S. financial institutions to date," Bob said. "As a merchant acquirer in the U.S. industry, FIS has over 20,000 merchants enabled to accept smart cards for payments and has enabled thousands of ATMs for financial institutions and ATM providers. And as an owner of a U.S. debit network (NYCE Payments Network), and a technology provider to multiple other U.S. debit networks, smart card technology provides additional security to millions of transactions a month."

"FIS helps our clients transform disruption into opportunity, giving them the tools needed to thrive not just today, but in tomorrow's financial world," said Bob. "Our collective group of customers benefit from fraud and risk reductions in their payments, enhancing the overall integrity of our payment options."

MAY 2017 MEMBER PROFILE



G+D MOBILE SECURITY

As a worldwide leader in mobile security solutions, G+D Mobile Security has unparalleled experience in the emerging mobile payment market and offers a 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.

Secure Tech Talk spoke with Brian Russell, Senior Vice President, Financial Institutions and Transit, for G+D's U.S. Mobile Security Division. Brian, who recently completed a two year term as the chairman of the Alliance Board of Directors, is responsible for the sales and marketing of all G+D's products to financial institutions and transit market segments.

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

"We're fortunate that mobile network operators, technology companies, financial institutions and world governments rely on us to secure their physical currencies and digital assets. Right now, we're 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 being trusted to securely manage credentials via the many diverse and emerging platforms – starting with the smart cards, phones and wearables already in place today."



Brian Russell

AUGUST 2017 MEMBER PROFILE



FIRST DATA CORPORATION

First Data Corporation is a global leader in commerce-enabling technology and solutions, serving approximately six million business locations and 4,000 financial institutions in 118 countries. From start-ups to the world's largest corporations, they help conduct commerce by securing and processing more than 2,500 transactions per second.

Secure Tech Talk spoke with Kelly Urban, Director, Digital Commerce Solutions at First Data Corporation, who helps lead the Integrated Token Solutions product team, specializing in the enablement of mobile payments. Kelly has been with First Data since 1984 in a variety of roles.

"Smart card technology spans the entire breadth of First Data," said Kelly. "Our Clover line offers industry-compliant POS devices supporting both contactless and contact chip cards.

We also personalize chip-enabled plastics and process plastic card-based and mobile device-based chip-initiated financial transactions."

"One factor driving smart card technology is its ability to support a portable, secure, standardized environment. Multifunction cards used for identification, authorization, and payments require a robust, well-developed platform. Payment products with integrated rewards/incentives are also growing. Whether embedded in plastic or in a mobile device, smart card technology is an ideal solution for all these things. It's arguably the best portable cryptographic engine anywhere."

"At the same time, cloud-based services will continue to encroach on traditional chip-based services, setting up a period of equilibrium between the two technologies. Each will hold a solid position in the market, but until that time, I think the technology pendulum will swing between the two, favoring one over the other for a time."



Kelly Urban

MEMBER RECOGNITION PROGRAM

ALLIANCE RECOGNIZES OUTSTANDING MEMBER COMPANIES



The Secure Technology Alliance Company of Excellence (COE) was created to recognize an elite mix of member companies who, each year, reach the highest level of active participation in the Alliance by having made outstanding contributions in the form of providing valuable time, talent and resources across a wide mix of Alliance activities.

Member involvement is not measured by how large an organization is, but by the actions of that organization and the commitment of its employees when it comes to engaging in industry activities and helping to fulfill the mission of the Secure Technology Alliance.

In 2017, 12 member companies received the COE designation. We are proud of the 10 returning recipients, and thrilled to welcome Cubic, and Entrust Datacard, the newest two member organizations.

Inclusion in this exclusive level is directly related to the following criteria members demonstrated in 2016-2017:

- Industry Council recognition for Honor Roll participants or Top Contributor to one or more of our Industry Councils
- Council officer position elected by peers
- Number of employees with LEAP/CSCIP/CSEIP training and certification
- Corporate CSCIP training and certification participation
- Alliance conference and event sponsorship of \$5,000 or greater in the last year
- Supporting membership in multiple chapters (SCALA) or affiliated organizations (U.S. Payments Forum)

Congratulations to the companies for their continued involvement in Alliance activities.

CONGRATULATIONS TO THE 2017 RECIPIENTS

This year we are delighted to announce the 12 member companies who comprise the 2017 class of Center of Excellence (COE) organizations. These COE recipients will be recognized in a number of ways throughout 2018.

- American Express
- Cubic Transportation Systems, Inc. (NEW in 2017)
- Discover Financial Services
- Entrust Datacard (NEW in 2017)
- G+D Mobile Security
- Gemalto
- IDEMIA
- Infineon Technologies
- NXP Semiconductors
- Underwriters Laboratories
- Visa Inc.
- XTEC, Inc.

These elite member companies have reached the highest level of active participation in the Alliance in 2017



SECURE TECHNOLOGY ALLIANCE CENTER OF EXCELLENCE (COE) PROFILE EXCERPTS

JANUARY 2017 PROFILE XTec, Inc.



XTec, Inc., a Center of Excellence recipient for the third year in a row, provides identity, credential and access management security solutions that are compliant with Federal mandates and standards. The company is also distinguished by having the most Certified Smart Card Industry Professionals in Government (CSCIP/G) employees. XTec's keystone solution, AuthentX, offers the only end-to-end, high assurance identity management infrastructure available for government and commercial enterprises. The company has invested significantly in cloud infrastructure, with three high security data centers in the U.S., and automated load balancing. This assures that their hosted customers' uptime validation is over 99.9999%.

MARCH 2017 PROFILE VALID



A 2016 Center of Excellence recipient, Valid is a Brazilian company with a global presence and production in Argentina, Spain and the U.S. Established in 1957, it is the world's fourth largest producer of financial cards, while continuing to develop new technologies and services. Valid has vast experience serving financial institutions and mobile operators with products and services associated with smart card technology. With a proven track record supplying EMV technology and SIM cards in the Americas for many years, they have expanded in recent years to create a presence in other regions of the world like Europe, Africa, Middle East, and Asia.

APRIL 2017 PROFILE ACS



A 2016 Center of Excellence recipient, Advanced Card Systems (ACS) develops and provides smart card operating systems (COS), smart card readers, and related services to facilitate the implementation of smart card-based systems for various applications and industries. It offers end-to-end solutions, such as micropayment systems and automatic fare collection (AFC) systems. The company is Asia Pacific's top supplier, and one of the world's top three suppliers of PC-linked smart card readers. Always current, ACS leverages trends by diversifying its devices to accommodate a mix of older and the latest technologies, offering all-in-one devices able to support dual interface, contactless, contact, and older technologies such as magnetic stripe.

JUNE 2017 PROFILE Intercede



A 2016 Center of Excellence recipient, Intercede is a cyber-security company specializing in digital identity, derived credentials, and trusted application management. Intercede has been delivering trusted solutions to high profile customers for over 20 years. The company's products, services and solutions create a foundation of digital trust between connected people, devices, apps and service providers, combining expertise with innovation to provide world-class cyber-security. They also offer mobile credential solutions, including a derived PIV solution for the U.S. federal market that is fully compliant with FIPS 201-2. Intercede has worked with U.S. federal agencies, large aerospace and defense corporations, and major players in financial services and telecommunications.

TRAINING AND CERTIFICATION PROGRAMS

The Secure Technology Alliance is strongly committed to offering industry education programs, training opportunities and resources so that individuals and organizations can get in-depth education on smart card technology, applications and implementation best practices. Through its active membership composed of leading technologists and practitioners in payments, identity, government and other sectors, the Alliance currently provides a large number of educational resources examining important industry issues or implementation considerations, summarizing best practices and informing stakeholders on latest developments in secure technologies.



National Center for Advanced Payments and Identity Security

A SECURE TECHNOLOGY ALLIANCE INITIATIVE

NATIONAL CENTER FOR ADVANCED PAYMENTS AND IDENTITY SECURITY

For the past two years, the National Center for Advanced Payments and Identity Security has served as the location for our robust training and exam certifications. Located in Crystal City, VA, just outside of Washington, D.C., this facility is the venue for live, interactive and dynamic educational activities hosted by the Alliance, including workshops, educational courses, briefings, symposiums, and training and certification

XTec, Inc. is one of the member organizations who have fully taken advantage of the Corporate Training Program. More than 30 XTec employees have their CSCIP/G certification.

testing for the Certified Smart Card Industry Professional program (CSCIP) and Certified System Engineer ICAM PACS (CSEIP) training and certification program.

support of the mission to better protect consumers' privacy, and advance the security of payments and identity through education programs on best industry practices and advances in security technology. The activities of the Secure Technology Alliance Educational Institute, which conducts educational workshops at Alliance events, is also part of the Center.

The Center was established through a grant from Heartland Payment Systems in sup-

CORPORATE TRAINING PROGRAM

Both LEAP and the CSCIP professional development and smart card training program and exam are available as a corporate training program for organizations with a large number of professionals who would benefit from organized, comprehensive training course and exam. In these programs, training and exam are delivered at the corporate location at a reduced group rate cost. Corporations who enroll ten or more individuals qualify for the group rate and two or more companies can combine their individual training into one class to reach the minimum participants.



LEAP

The [Leadership, Education, and Advancement Program \(LEAP\)](#) is an online, members-only organization for smart card professionals. Its purpose is two-fold:

- To advance education and professional development
- To manage and confer, based on a standardized body-of-knowledge exam, the [Certified Smart Card Industry Professional](#) (CSCIP) designation

LEAP provides members with resources and materials including white papers, FAQs, position papers and archives of webinars, workshops and conference proceedings in the access control, payments, identity, healthcare, mobile and transportation markets, all of which are updated regularly. LEAP membership also offers opportunities for individuals to further their careers and showcase their professionalism within the industry.

LEAP is especially valuable for new entrants to the market or professionals working for small organizations without access to full Secure Technology Alliance membership benefits.



CSCIP

The Secure Technology Alliance offers three CSCIP credentials: CSCIP, CSCIP/Government and CSCIP/Payments. CSCIP is an internationally recognized credential for smart card industry professionals. The CSCIP program prepares professionals to gain advanced levels of smart card technology and applications knowledge, and then move on to complete training and pass a multi-part exam.

Regardless of the specific credential, CSCIP certifications require demonstrated proficiency in a broad body of industry knowledge, including:

- Smart card technology fundamentals
- Security
- Application and data management
- Identity and access control usage models
- Mobile and Near Field Communication (NFC) usage models
- Payments usage models

The Alliance's CSCIP Smart Card Technology and Applications Training Course Modules serve as the primary review materials for the CSCIP certification exam. Training and exam preparation classes led by seasoned smart card industry experts further solidify the technical and broad smart card business applications training experience. The Alliance maintains and updates its training materials to reflect industry changes.



CSEIP

The [Certified System Engineer ICAM PACS \(CSEIP\) training and certification program](#) has been extremely popular in the two years since it was established. This GSA-approved training program provides the training and certification required for E-PACS engineers employed by commercial organizations that are looking to bid on GSA procurement agreements for access control systems.

To ensure that procurements of approved E-PACS for GSA managed facilities are installed properly, GSA requires that all billable work performed on such systems be done using certified system engineers.

The classroom training curriculum includes learning objectives that provide system engineers with the knowledge to properly implement E-PACS, and hands-on training demonstrates the engineer's abilities to set up, test and configure access control features within the security system.

CSEIP RECERTIFICATION

In 2017, the Alliance began its recertification program for the first group of CSEIP certificants, as the designation is valid for two years.

Recertification extends the value of the CSEIP certification by demonstrating that the certificant is current with any new requirements or changes in the technology of E-PACS systems.

Recertification provides confirmation to industry colleagues, business partners and potential customers that the certificant:

- Maintains competency and has the necessary working understanding of Federal E-PACS system requirements, system design, engineering and life cycle disciplines covered under the CSEIP certification
- Is proven to possess continued eligibility to participate in contracts serving Federal E-PACS projects



The CSCIP certification has become the benchmark for executives in increasingly competitive markets where proven expertise is critical. Through corporate and individual training programs, the Alliance offers professionals training and tools to earn the certification and differentiate themselves from their peers. At the same time, corporate participation in these programs demonstrates an employer's commitment to developing and maintaining highly skilled workers.

CSEIP AND CSCIP RECIPIENTS

2017 CSEIP RECIPIENTS



- Todd Adams, Allegion
- Dennis Anfield, Allegion
- Brent Arnold, XTec, Inc.
- Neil Bolin, CertiPath Inc.
- Ralph Boone, Kratos Public Safety & Security
- Wendy Brown, Protiviti
- James Burke, SynchroCyber Corporation
- Michael Casey, CertiPath Inc.
- Richard Childree, Department of Homeland Security/FEMA
- Scott Chillemi, Identiv
- Ryan Clapman, Protiviti
- John Coker, Identiv
- Josh Ebert, Identiv
- David Fogle, Star Asset Security, LLC
- Deon Ford, Prism International, LLC
- Brian Frieze, Food & Drug Administration
- Patrick Grandpre, Allegion
- Troy Hall, Johnson Controls
- Michael Hamilton, KBRwyle
- David Harjo, Bureau of ATF
- Sean Hernandez, Identiv
- Derek Hileman, Allegion
- Frederick Holt, Allegion
- Philip Hosack, LVW Electronics
- Eric Johnson, Volta Systems Group, LLC
- Norman Kadnar, NIH Contractor
- Stacey Kanter, Identiv
- Jacob Knoll, Global Enterprise Technologies Corp.
- Larry Kolb, Allegion
- Robert Krecker, Booz Allen Hamilton
- Patrick Lackey, Systems Applications & Solutions
- Marquis Laude, Integrated Security Solutions, Inc.
- Larry Lillard, RFI Enterprise Inc.
- Nnamdi Martyn, U.S. Environmental Protection Agency
- Michael McKinnon, The Coleman Group Inc.
- Terry Meier, Allegion
- Stephen Mergens, XTec, Inc.
- Dan Morrissey, United Security & Communications, Inc.
- James Morton, NARA
- Kenneth Myers, Protiviti
- Osenaga Osagie, Chenega Management, LLC
- James Pinckney, BAE Systems
- Nicola Pisani, M.C. Dean, Inc.
- Bruce Riddle, Environmental Protection Agency
- Rodney Rourk, Department of the Navy, Space and Naval Warfare Systems Center Atlantic
- Jaime Santiago, Bureau of ATF
- Jason Sargent, Protiviti
- Donald Sawyer, U.S. Navy CNSS-14
- Bryan Semprie, Identiv
- David Smith, Signet Technologies, Inc.
- Timothy Smith, Chenega Management, LLC
- Chad Stadig, Siemens Industry, Inc.
- Douglas Talbott, Allegion
- Duwan Tate, U.S. Marshals Service
- Ron Taylor, Allegion
- Scott Tingley, Allegion
- Jefferson Tross, Versar Inc.
- Sam Tuthill, Identiv
- Brandon Welling, ASI
- Paul Wojdyski, Controlled Key Systems, Inc.
- Brian Young, Integrated Security Solutions, Inc.

As of September 30, 2017

"As somewhat of a novice to the physical security arena I was looking for the right place to get further educated in this area. I found that needed knowledge in your CSEIP training class. I have recommended the class to all my co-workers and senior management. The depth of information and the learning atmosphere you provided was some of the best training I have received in my career."

Bruce Riddle, Environmental Protection Agency



2017 CSCIP RECIPIENTS

- Jim Combs, Beeler Impression Products
- Joe Franco, Capture Technologies
- Ross Kierstead, IDEXPERTS
- Maziya Mavvaj
- Steven Mehler, Washington Metropolitan Area Transit Authority (WMATA)
- Dennis Nguyen, Washington Metropolitan Area Transit Authority (WMATA)
- Nate Williamschen, Entrust Datacard



2017 CSCIP/G RECIPIENTS

- Megan Bledsoe, XTec, Inc.
- Kevin Campbell, XTec, Inc.
- Michael Casey, CertiPath
- Dan Currie, Department of National Defence
- Sok Bonn Duong, XTec, Inc.
- Diana Farris, XTec, Inc.
- Richard Hizon, TYCO
- Nikita Jain, American Express
- Nic Pavel, Interac
- Morgan Richard, XTec, Inc.
- Lawrence Sutton, CH2M
- Apurv Tripathi, American Express
- Michelle Wilson, U.S. Department of State
- Francisco Yuan, National Defense Canada



2017 CSCIP/P RECIPIENTS

- Ximena Azcuy, Discover Financial Services
- Srinivasa Chigurupati, Capital One Bank
- Leigh Garner, Discover Financial Services
- Tracey Harrington, Discover Financial Services
- Kenny Lage, Discover Financial Services
- Krishna Mohan, Discover Financial Services
- Dipesh Paul, American Express - India Private Limited
- Lokesh Rachuri, Capgemini
- Anirban Roy, American Express
- Iniyan Seerangapattan Sampath, Discover Financial Services
- Rohit Sinha, American Express
- Vijay Kumar Soni, Discover Financial Services
- Itzamna Vilchis, Discover Financial Services
- Daniel Willis, Discover Financial Services
- John Xie, Foothill Transit
- David Yen, Visa Inc.
- Ahmad Husaini Ahamad Zakeri, Malaysian Electronic Payment System Sdn Bhd

As of September 30, 2017

CERTIFICATION TRAINERS

BRETT CHEMALY, CSCIP Trainer

Brett Chemaly works for Discover Financial Services as Senior Manager: Strategic Alliances - Global Commerce, where he manages debit implementations in the U.S. market and Discover's technical components of their Global Alliances business. Prior to joining Discover, he was employed within Mastercard's Emerging Payments team based in Toronto, Canada, where he was responsible for managing and consulting on Mastercard's chip programs on both sides of the border. Brett is a native of South Africa, holding a Bachelor of Commerce Degree from Rhodes University.

BRYAN ICHIKAWA, CSCIP and CSEIP Trainer

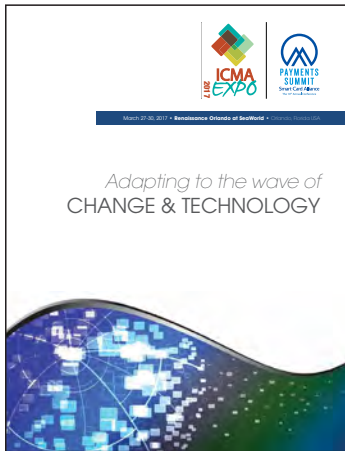
Bryan Ichikawa serves as a consultant to the Secure Technology Alliance, and is responsible for marketing and sales for the organization's events and conferences. He is also a trainer for the organization's certification programs. Bryan has more than 30 years of security technology, systems integration, and program management experience. He previously worked for Deloitte, Unisys, and Thomson Media. He holds a B.A. from Lynchburg College.

LARS SUNEBO, CSCIP and CSEIP Trainer

Lars Sunebo is responsible for directing all of the Alliance training programs for members and industry professionals. He works to promote the industry credentials to organizations, leads training classes, and arranges corporate training courses. Before joining the Secure Technology Alliance in 2014, Lars worked for more than 30 years in the security industry, where his numerous achievements included developing the concept and implementation plan for nationwide E-PACS network for several Federal agencies. Lars holds an Electronic Engineering degree from Aso Technical, in Stockholm, Sweden.

For a list of all CSCIP recipients go to: www.securetechalliance.org/activities-leap-cscip-registry

2017 CONFERENCES AND EVENTS



SMART CARD ALLIANCE PAYMENTS SUMMIT

Renaissance Orlando at Sea World • Orlando, FL • March 27-30, 2017

With so much change and innovation impacting the payments industry, the Payments Summit is the key event payments stakeholders look forward to every year because it brings together like-minded individuals looking for new ways to overcome challenges impacting emerging and developing payments technologies. Invisible transactions, frictionless consumer experience, brand awareness, product development and innovation were all listed as keys to success in payments. Presenters and panelists in tracks discussed:

- Card-not-present (CNP) fraud
- Contactless and mobile payments
- EMV chip technology and emerging transit payments innovations

The event, co-located for the second year with the International Card Manufacturers Association's 27th annual EXPO, will continue in 2018. Also noteworthy – just weeks before the conference, the Smart Card Alliance officially announced the re-branding of the organization as the Secure Technology Alliance.



SECURING FEDERAL IDENTITY 2017

Hamilton Crowne Plaza • Washington, DC • June 6, 2017

For the last 15 years, this government-focused event has brought together thought leaders and executives with security, government and technology backgrounds, providing opportunities for cross-industry discussion of the most important topics impacting government identity and authentication. Interest was high concerning the most important developments and innovations in federal identity credentialing and access security. The agenda did not disappoint. Keynotes, roundtables and panels covered:

- Federal secure identity policy and technology guideline updates
- Federal identity programs and standards, including discussions on the future of FICAM, PIV, PIV-I and the Common Access Card (CAC)
- Further use of two-factor authentication in federal agencies
- Mobile identity and authentication approaches

Based on the quality and caliber of presentations, attendees left with renewed energy to accelerate identity and security in government.




IOT PAYMENTS 2017 CONFERENCE

Hyatt Regency Hotel • Austin, TX • October 10-11, 2017

Industry executives from the IoT and payments communities met before enthusiastic attendees to discuss solutions that meet the “big three” criteria for IoT payments success: security, mobility and usability. Speakers focused on secure chip technology for IoT devices to provide the foundation for security for transactions, such as authentication, data security and life cycle management. Some universal agreements emerged, including:

- IoT implementation is moving ahead but security is generally poor
- Secure payments and authentication are difficult and expensive to implement
- Time to market drives a lot of IoT applications, so the security option chosen is often the one easiest to deploy

This conference provided a solid opportunity to hear wide-ranging IoT challenges and opportunities, and for attendees and speakers to share anecdotal and factual experiences from the IoT world.

A smiling woman with dark hair, wearing a striped apron over a patterned shirt, holds a blue Discover card. She is in a cafe setting with a chalkboard menu in the background. A large orange circle frames the right side of the image.

You want
to attract
customers

We can open more doors

Together, we'll expand your checkout to a world of diverse payment methods.

Learn more about Discover® acceptance and the free resources we have to offer.

- Open your clients to millions of global cardholders
- Attract loyal customers¹
- Enhance your payment offerings

Together We Work

Find out more at DiscoverNetwork.com

DISCOVER[®]
GLOBAL NETWORK

¹ 68% of Discover Cardmembers have not returned to a merchant in the last month if their Discover Card was rejected
C+R Research Study of 2,000 Discover Cardholders commissioned by DFS Services LLC and completed in December, 2016.

THANK YOU TO OUR 2017 CONFERENCE SPONSORS

accenture



CONDUENT

cpi card group®
Solutions For Your Success

ARD Testing International
AN ISO 17025 TEST LABORATORY

CUBIC™

DISCOVER®
GLOBAL NETWORK

DXC.technology

ePay™
RESOURCES

FEITIAN



FIME®
One Action. A billion transactions.

FIS

GD G+D
Mobile Security

gemalto
security to be free

ICC
SOLUTIONS

IDENTIV

infineon

MATICA
TECHNOLOGIES

NXP

oberthur
TECHNOLOGIES
THE M COMPANY

Perfect Plastic

QCard™
The Lab Authority

SAFRAN

SAMSUNG
pay

SCHEIDT&BACHMANN **SB**

ST
life.augmented



verisoft

VISA

SAVE THE DATE FOR THESE 2018 EVENTS

A vibrant graphic for the Payments Summit 2018. The title "PAYMENTS SUMMIT" is in large blue letters, with "2018" below it. Below the title, the phrase "THE FUTURE OF PAYMENTS" is written in a large, light blue font. The background is a collage of colorful geometric shapes (triangles, squares) in shades of blue, yellow, and green, each containing a white icon representing various payment and technology concepts like mobile phones, Wi-Fi, cloud computing, and security. Arrows point in various directions, suggesting movement and progress. At the bottom left, the website "www.STAPayments.com" and the dates "March 26-29 | Orlando, Florida" are listed. At the bottom right, it says "In partnership with:" followed by logos for the Secure Technology Alliance, US Payments Forum, and ICMA Expo.

**PAYMENTS
SUMMIT**
2018

THE FUTURE OF PAYMENTS

www.STAPayments.com
March 26-29 | Orlando, Florida

In partnership with:

SECURE TECHNOLOGY ALLIANCE US PAYMENTS FORUM ICMA EXPO

A graphic for the Securing Federal Identity 2018 event. The left side features a photograph of the Lincoln Memorial in Washington, D.C., with its iconic columns and steps. The right side has a solid orange background with the title "SECURING FEDERAL IDENTITY 2018" in large white letters. Below the title, the Secure Technology Alliance logo is shown next to the text "GOVERNMENT EVENT". The dates "JUNE 5-6, 2018" and the location "HAMILTON CROWNE PLAZA WASHINGTON, D.C." are listed. At the bottom, the website "www.SecuringFederalID.com" is provided.

**SECURING
FEDERAL
IDENTITY 2018**

SECURE TECHNOLOGY ALLIANCE GOVERNMENT EVENT

JUNE 5-6, 2018
HAMILTON CROWNE PLAZA
WASHINGTON, D.C.

www.SecuringFederalID.com

2017 EVENT PHOTOS

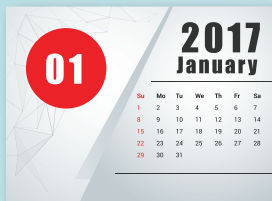
The conferences and events produced by the Secure Technology Alliance are specifically tailored to cover every vertical market. These meetings also allow our collective industry knowledge and technology expertise to extend beyond the edges of the organization. Our conferences are always infused with fresh new insights from industry leaders. Industry councils also meet in person at these events, allowing for valuable one-on-one interaction and group collaboration.





EXECUTIVE DIRECTOR LETTER HIGHLIGHTS

One of the most popular sections of the Secure Technology Alliance newsletters is the letter from Executive Director Randy Vanderhoof. Check out his thoughts during a very busy year for the Alliance and the industry. To read the complete letters, visit the [Secure Technology Alliance website](#).



HOW DID I DO?

In January 2016, I made a few predictions: EMV payments would be the norm; mobile wallets would take off, and merchants would become serious about card-not-present fraud mitigation.

While I was fairly accurate, what I did not see coming was an information bubble that rendered people unable to communicate and understand other people's views. Perhaps part of that was a result of a tremendous partisan divide in the U.S. that spilled out of D.C. politics and made its way into every other aspect of some people's lives. I took the opportunity to reassure members that our organization, and the U.S. Payments Forum, were two groups where effective communication and broad understanding were not only welcome, but necessary so we could understand, and implement, complex security solutions.



PAYMENTS SUMMIT LOOMS LARGE

For decades, a smart card was the only portable computer in your pocket that could store your private information, execute applications, and communicate with other devices and computer systems.

Now, mobile phones do all that and more. When the smart card form factor was too big to fit with some applications, smart cards changed to SIM cards which could be detached and inserted inside a smart phone or an automotive computer. When cards were too small to carry printed images and the personal information necessary to protect borders, they became card inlays manufactured in e-passport booklets that enabled the same identity credentials to be electronically authenticated. Join us as we explore the future of payments at the 2017 Payments Summit Conference next month in Orlando.



WELCOMING THE FUTURE OF SECURE TECHNOLOGY

Over the past 17 years, the Smart Card Alliance became a leader by presiding over a multi-industry association that worked to stimulate the understanding, adoption, use and widespread application of smart card technology for payments, mobile, identity and access security, transportation, and healthcare. Over time, technology evolved for smart cards and

other forms of embedded chip technology. This month, March 2017, we officially announced a new name – the Secure Technology Alliance – to go along with an expanded charter to include a broader range of security and privacy-enhancing technologies. We are proud of our past and excited about our expanded focus, which has already taken shape by our members' enthusiastic support for our broader engagement in technology being used in things such as wearables and Internet-connected devices.



FROM ONE ALLIANCE TO ANOTHER

Through media coverage, member newsletters email and word of mouth, news of the name change from the Smart Card Alliance to

the Secure Technology Alliance has been filtering out. It's not easy changing 17 years of identity and history overnight, but it helps when that change is welcomed by many as being done for the right reasons. The core of the previous organization remains under the expanded mission of the new Alliance. The demands to support issuance and usage of smart cards for payments and identity, while paving the way for faster adoption of embedded chip technology and other related hardware and software security solutions, puts the Secure Technology Alliance on a sustainable path for the organization and provides exciting new growth opportunities for members.



SHIFTING FOCUS TO FEDERAL IDENTITY AND SECURITY

In June, we shift focus to government identity and security with the 15th annual Securing Federal

Identity event in D.C. We've hosted this conference through four elections, three 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 that mandated that the federal government define standards for the use of secure, tamper-resistant, interoperable identity credentials with biometrics to protect federal facilities and networks. Despite the dysfunction of Washington politics, what's remained consistent since 2004 is the government's quest to make identity management and access security function across the entire executive branch. Our determination hasn't diminished either.



DIGITAL PAYMENTS IN FOCUS

For most of the mainstream payments and mobile commerce world, digital payments adoption centers around mobile wallets and

NFC for making purchases at retailers, or merchant apps on mobile devices using QR codes. These two camps represent the bulk of payments transactions involving alternatives to EMV chip cards. The increasing availability and frequency of use of digital forms of money and payments mean that people of all ages, particularly millennials, are relying more on mobile devices for their daily usage habits. With new advances by Apple Pay and Samsung Pay to include everything from membership cards, gift cards, and merchant loyalty cards with personal online payment credentials, digital forms of payment are coming into focus quickly. And eliminating the physical wallet is starting to seem very likely.



NO TIME FOR WAITING ON IOT SECURITY

Many articles have pointed out security shortcomings of Internet-connected devices and networks. Our IoT information portal

– www.iotsecurityconnection.com – was created to raise awareness of these security concerns, but there's little interest from organizations to investigate the issue. Perhaps no one wants to admit the security problem is already too embedded in the devices in the market or the cost to address the problem and proactively fix it is too unpleasant. So nobody owns the solution and the problem continues. Security experts agree that a few simple changes to the design of video cameras, home health monitors, industrial sensors, and connected consumer devices would prevent attacks from hacking systems. While this approach would address present threats, security needs the development of technology that will prevent attacks in the future.



EMV IS THE CURE FOR HEALTHCARE

It's time for healthcare to embrace EMV for payments. As consumers adjust to using chip readers elsewhere, they're still swiping cards at

doctors' offices. If more offices had EMV chip readers rather than the cheap, insecure magnetic stripe readers, it would lead banks to

issue health savings account (HSA) cards with secure EMV chips. An EMV chip-enabled healthcare system opens the door for insurance companies to issue cards with the same EMV chip technology to authenticate patients receiving treatment. It's been more than 5 years since banking and retail made the transition to EMV after fraud levels reached "critical condition." Healthcare is already very ill. If it doesn't receive a shot of EMV medicine soon, healthcare payments may be on life support before we know it.



IS CONTACTLESS AROUND THE CORNER?

The next wave of EMV chip cards is approaching, and whether by coincidence or not, it appears that the time has arrived for dual-interface

cards. With the cards having both contact and contactless capability, consumers will likely appreciate the option of a simple tap to pay. And while the actual transaction speed is not dramatically different, it will feel like time is shaved off, because consumers can tap to pay at any point and put their card away, rather than waiting until the final item is scanned and then inserting their card. The economics for investment for issuers in dual-interface cards are never going to be better than they are right now. Let's hope this change occurs, and is welcomed by everyone involved.



SUBSTANCE WANTED

Coming off the heels of our successful IoT Payments 2017 Conference held in Austin, my view of the impending market readiness for adding payments to all types of

consumer-managed devices, such as watches, fitness bands, rings, home appliances and other "Internet of Payment Things," has evolved into guarded realism. That's based on knowing that for the merchant terminal to blink green requires much more activity and actions. The consumer needs to want to use it for payments, issuers need to make their accounts available for each device on the market, and merchants need to contactless-enable their point of sale. The payment technology and electronics surrounding IoT payments is real, but the substance that makes them really work for payments – the compelling use case – isn't there yet.

WEB PRESENCE

The Secure Technology Alliance hosts two main web sites that members can visit. Industry news, white papers and publications, event information and proceedings, educational resources, links to webinars, member press releases and Alliance newsletters can all be found on www.securetechalliance.org. The Alliance also provides a wealth of resources on EMV on www.emvconnection.com.

WEB SITE HIGHLIGHTS



MOST POPULAR: WEB RESOURCES

- Secure Technology Alliance information and members
- Secure Technology Alliance white papers and publications
- Secure Technology Alliance events and event proceedings
- Smart card technology and applications information

MOST DOWNLOADED: PUBLICATIONS AND WHITE PAPERS

- [Blockchain and Smart Card Technology](#)
- [Mobile Identity Authentication](#)
- [Embedded Hardware Security for IoT Applications](#)
- [Smart Card Technology in Healthcare: Frequently Asked Questions](#)
- [EMV and NFC: Complementary Technologies that Deliver Secure Payments and Value-Added Functionality](#)
- [Multimodal Payments Convergence – Part One: Emerging Models and Use Cases](#)
- [Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers](#)
- [Contactless Payments in the U.S.: Guides for Merchants and Issuers](#)
- [Host Card Emulation 101](#)
- [A Healthcare CFO's Guide to Smart Card Technology and Applications](#)



BY THE NUMBERS

Statistics for www.securetechalliance.org:

- Average site visits per month: 13,301
- Number of page views per visit: 1.83
- Over 73% new visitors

NEW IN 2017: PUBLICATIONS, REBRANDED WEB SITE

- [Secure Technology Alliance](#) web site. New, rebranded site for Alliance organization and resources
- [Secure Technology Alliance Publications](#): Twelve new white papers, position papers or infographics on contactless EMV payments, payment tokenization, mobile identity authentication, IoT security and payments, and multimodal payments convergence in transit

EMV CONNECTION WEB SITE

www.emv-connection.com

- Over 59,000 visits from over 45,000 unique visitors
- EMV educational resources for issuers, merchants, acquirers/processors, ATM owners/operators and consumers
- New resources from the U.S. Payments Forum: [Card-Not-Present \(CNP\) Fraud around the World](#); [EMV Receipt Best Practices](#); [Mobile and Contactless Payments Glossary](#); [Optimizing Transaction Speed at the POS](#); [Petroleum Industry: EMV FAQ](#); [Technical Solution for Transit Contactless Open Payments Use Case 1: Pay As You Go/Card](#); [Understanding the U.S. EMV Fraud Liability Shifts](#)
- New [U.S. Payments Forum](#) public and members-only web sites



SOCIALLY ACTIVE

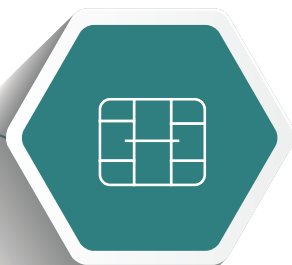
Join us on LinkedIn and follow us on Twitter.

LinkedIn Groups

- [Government Smart ID](#) – 2,285 members
- [Smart.Payments](#) – 1,702 members
- [Healthcare Identity Management](#) – 191 members
- [LEAP](#) – 642 members

Twitter

- 600+ tweets
- 4,268 followers



- › State-of-the-art personalization and transaction performance
- › New wearable form factors for best customer experience
- › Card integration support
- › Contactless certification support
- › Terminal/reader infrastructure support



Contactless excellence. Built on excellent infrastructure.

Trust in Infineon's secure approach, from design and manufacture to certification and system optimization

Infineon is a leading provider of security solutions for payment applications.

www.infineon.com/contactless-competence



INDUSTRY COUNCILS

Through seven industry councils, the Secure Technology Alliance proactively addresses topics of concern in the different vertical markets for secure technologies. Alliance members lead Council activities and contribute to a wide variety of projects, including white papers, webinars, workshops, web resources, position papers and industry commentary. The results of the councils' work help to drive implementations of both hardware and software security solutions in the U.S. and provide authoritative educational material for both the U.S. and international secure technology markets.



ACCESS CONTROL

The Access Control Council focus in 2016/2017 was on supporting government implementations of PIV-enabled physical access control systems, with submission of comments on GSA, NIST and OMB documents and development of detailed educational material. Over 40 member organizations participate in the Council.



HEALTH AND HUMAN SERVICES

The Health and Human Services Council revised its charter this year: to promote the adoption of secure technologies for healthcare and human services organizations, in accordance with industry standards. The Council also was successful at securing speaking engagements at key healthcare industry events. More than 25 member organizations participate in the Council.



IDENTITY

The Identity Council's updated charter is to raise awareness and provide thought leadership and education on real-world issues of implementing and operating identity and identity authentication and authorization systems. A new Identity Council mobile identity landscape white paper project is engaging strong cross-council participation. More than 35 member organizations participate in the Council.



IOT SECURITY

The IoT Security Council focused its activities in 2017 on establishing foundational educational resources and engaging in cross-council projects and discussions. Council activities included planning and participating in Alliance IoT events and providing resources on IoT security threats and embedded hardware security. Over 50 member organizations are participating in the new Council.



MOBILE

The Mobile Council focused on projects that explored technical approaches for implementing application and data security in mobile devices and tethered wearables. Council activities included a webinar on EMV tokenization and development of two white papers on mobile identity authentication and the Trusted Execution Environment (TEE). The Council is made up of more than 50 member organizations.



PAYMENTS

The Payments Council had a very active year, providing educational resources for issuers, merchants and other industry stakeholders on contactless payments and other emerging technologies. Council activities included hosting webinars and publishing guides and a security Q&A on contactless payments, as well as exploring blockchain technology and payment-enabled wearables. Over 50 member organizations participate in the Council.



TRANSPORTATION

The Transportation Council continues to address topics of interest to transit agencies, publishing a multimodal payments convergence white paper and hosting a smart cities workshop in collaboration with the IoT Security Council. The Council is also collaborating with the U.S. Payments Forum on a transit contactless EMV technical solution framework. More than 55 member organizations participate in the Council.

YEAR IN REVIEW: INDUSTRY COUNCILS LETTER

A Look at Our Councils in 2017

Nimble Councils Deliver Visibility and Generate Sales

Councils have proven to be remarkably adaptable and nimble – anticipating new market directions and working on topics that promote secure technologies and help members establish market visibility and generate sales. What continues to be true is that the Alliance's membership composition – including both technology implementers and solutions providers – provides the ideal mix for our projects to deliver practical guidance.

2017 was another productive year for Alliance industry councils, producing white papers, industry commentaries, webinars, workshops and other educational resources. We also continued to have strong member engagement, with over 74 percent of all member organizations participating in the councils.

MISSION ALIGNMENT

One of the priorities for the Alliance this year was turning the organization to activities that delivered on our expanded mission. While the councils have historically tackled issues “beyond the card,” the Access Control, Health and Human Services, Identity, and Payments Councils recognized that their stated charters needed to align with the Alliance's expanded mission. The new council charters provide the foundation for the councils to tackle implementation of a broader range of secure technologies and to look at overall ecosystem requirements for security.

A few themes emerged among the councils this year. One was the ever-increasing importance of mobile devices to all of our vertical markets.

The Identity Council launched a cross-council project to document mobile identity use cases – where the mobile device is used to provide secure access to an individual's identity credential. New mobile technologies were also explored by the Mobile Council, with the Trusted Execution Environment 101 white paper, and by the Transportation Council, with projects looking at the impact of mobile on transit ticketing and multimodal payments convergence.

A second theme was new payment form factors. The Payments Council published a white paper on key implementation considerations for payment-enabling wearables. And the IoT Security Council looked at the landscape for IoT payments and started the discussion on how IoT devices can be deployed with the foundation of trust needed for a secure payments infrastructure.

A third theme was collaboration. We see increasing collaboration among councils as mobile devices and mobile technologies solve multiple vertical market challenges. Our councils are also collaborating with the U.S. Payments Forum working committees. Our Payments Council contactless challenges and solutions white paper will provide the basis for a Forum project on implementation guidance. And Transportation Council members are collaborating with the Forum to define the technical framework for accepting EMV contactless payments at transit points of entry.

FULL PLATE

As usual, we're going into the next year with another full plate of projects – with topics including new technologies, new types of devices with embedded security technology, and new approaches to mitigate fraud.

We've heard from many members that council participation is valuable both for their organizations and for the individuals contributing to council projects. Contributing members are featured in our industry outreach, which highlights member organizations' thought leadership and industry stature, and acknowledges the expertise and commitment of the individuals who participate in the many projects.

The Secure Technology Alliance thanks all of our members for their strong commitment to the industry. Through collaborative projects, the Alliance provides critical and practical resources that enable organizations to implement secure technologies in their payments, identity and access security applications.

WE SEE INCREASING
COLLABORATION AMONG
COUNCILS AS MOBILE DEVICES
AND MOBILE TECHNOLOGIES
SOLVE MULTIPLE VERTICAL
MARKET CHALLENGES.



Cathy Medich
Director, Strategic Programs
Secure Technology Alliance



ACCESS CONTROL COUNCIL

MISSION: Accelerate the widespread acceptance, use, and application of secure technologies, in various physical and digital form factors, for physical and logical access control, as applicable to both persons and non-person entities

OFFICERS

- Chair: Adam Shane, Leidos
- Vice Chair: Dave Helbock, XTec, Inc.

STEERING COMMITTEE

- Tony Damalas, SigNet Technologies
- Dave Helbock, XTec, Inc.
- Daryl Hendricks, GSA
- Martin Janiak, Veridt
- Ryan Kaltenbaugh, Lenel
- Mike Kelley, Parsons
- Stafford Mahfouz, Tyco Software House
- Steve Rogers, IQ Devices
- Adam Shane, Leidos
- Mark Steffler, Quantum Secure
- Bill Windsor, Dept. of Homeland Security
- Mike Zercher, NXP Semiconductors

TOP CONTRIBUTORS

- Daryl Hendricks, GSA
- Mike Kelley, Parsons/Secure Mission Solutions
- Steve Rogers, IQ Devices

HONOR ROLL

- Tim Baldridge, Defense Manpower Data Center
- Mark Dale, XTec, Inc.
- Tony Damalas, SigNet Technologies
- David Helbock, XTec, Inc.
- Daryl Hendricks, GSA
- Mike Kelley, Parsons/Secure Mission Solutions
- Lolie Kull, Hewlett-Packard Enterprise Services LLC
- Steve Rogers, IQ Devices

- Adam Shane, Leidos
- Mark Steffler, Quantum Secure
- Rob Zivney, Identification Technology Partners

ACTIVITIES

- [Position paper](#) on OMB Circular A-130 on "Management of Federal Information Resource" (Sept. 2016)
- Council Steering Committee and officer elections (Dec. 2016, Jan. 2017)
- Submission of industry comments on GSA FIPS Evaluation Program "PACS Functional Test Requirements and Test Cases (FRTC)," version 1.1.3 (Feb. 2017)
- Submission of industry comments on NIST Draft SP 800-63 "Digital Identity Guidelines," in collaboration with the Identity Council (Mar. 2017)
- Physical access use cases for the Mobile Council ["Mobile Identity Authentication"](#) white paper (Mar. 2017)
- In-person meeting at the Secure Technology Alliance National Center for Advanced Payments and Identity Security (June 2017)
- PIV-enabled physical access control system (PACS) deployment playbook for the GSA CIO (July 2017)
- Council charter update (Sept. 2017)
- ["How to Plan, Procure and Deploy a PIV-Enabled Physical Access Control System"](#) webinar series (in process)
- Relationships with International Biometrics + Identity Association (IBIA) and Security Industry Association (SIA)

ACCESS CONTROL COUNCIL MEMBER ORGANIZATIONS

ABCorp • Accenture • Allegion • AMAG Technology • Brivo • Cardtek US • CertiPath LLC • CH2M • Cubic Transportation Systems, Inc. • Datawatch Systems • Defense Manpower Data Center (DMDC) • Entrust Datacard • Exponent, Inc. • G+D Mobile Security • Gallagher Group Limited • Gemalto • General Services Administration (GSA) • Hewlett-Packard Enterprise Services LLC • HID Global • IDEMIA • Identification Technology Partners, Inc. • Identiv • Initiative for Open Authentication (OATH) • IQ Devices • Leidos, Inc. • Lenel • NXP Semiconductors • Parsons/Secure Mission Solutions • Quantum Secure • SAIC – Science Applications International Corporation • SecureKey Technologies • SigNet Technologies, Inc. • Stanley Security Solutions • STMicroelectronics • SureID, Inc. • Tyco Software House • U.S. Department of Homeland Security • U.S. Department of State • U.S. Department of Transportation/Volpe Center • Ultra Electronics Card Systems • Veridt, Inc. • Visa Inc. • Wells Fargo • XTec, Inc.

YEAR IN REVIEW: ACCESS CONTROL COUNCIL CHAIR

Technology as a Protector

Businesses and private persons strive to protect those things that are important to them, including physical assets, information, and people. There are several threats to each of these categories, but technology exists to assist in protecting these things. The Secure Technology Alliance Access Control Council focuses on accelerating the widespread acceptance, use, and application of secure technologies in various form factors for physical and logical access control as it pertains to both persons and non-person entities (NPE).

The group brings together, in an open forum, leading users and technologists from both the public and private sectors. The Council works on activities that are important to the access control community and helps expand adoption of secure technologies in this important market.

ACTIVE PARTICIPATION

Access Control Council members participate in a variety of activities in support of our mission:

- Developing white papers and briefings on best practices for use of secure technologies to access buildings, networks, devices and information systems
- Providing industry resources to assist public and private sector organizations including international, federal, state and local governments, and private enterprises in leveraging standards – such as NIST's Federal Information Processing Standard (FIPS) Publication 201 Personal Identity Verification (PIV), PIV interoperable (PIV-I), and Commercial Identity Verification (CIV) credentials – for physical and logical access management and developing policies governing their use
- Providing industry resources to assist organizations in using standards-based biometrics and other forms of authentication for determining access control authorization
- Participating in the development of standards and specifications for using secure technology in physical and logical access control systems
- Collaborating with other industry organizations to influence standards and develop best practices
- Providing subject matter experts for various speaking engagements

Several trends impact the focus of our work; among them are:

- The accelerating adoption of biometrics of all types to include behavioral modes as well as physical traits
- Mergers and acquisitions such as Canon/Axis/Milestone, Oberthur/Morpho, and HID/Codebench/Mercury, all contributing to changing landscapes, innovation, and integrated solutions
- Highly public cyber attacks on U.S. and foreign government agencies and corporations of all sizes, particularly alarming when those trusted to protect our personal and confidential information are responsible for its release
- Increasing reliance on mobile phones to do a variety of things other than making phone calls

Thank you for your support over the past year! The Access Control Council welcomes all interested parties to learn more about our activities and to participate in our current projects such as webinars and documenting best practices.

WE GENERALLY WANT TO BE ABLE TO DO EVERYTHING ON OUR MOBILE PHONE – IN ADDITION TO MAKING CALLS, TEXT MESSAGING, WE ANSWER EMAIL, WATCH VIDEO, STAY INFORMED THROUGH NEWS FEEDS AND SOCIAL MEDIA, CONTROL OUR ENVIRONMENT THROUGH HOME AUTOMATION, ACCESS ACCOUNTS, AND CONDUCT BUSINESS. MOBILE CREDENTIALS NEED TO ADOPT SECURE TECHNOLOGIES AND NOT RELY ON USERNAME AND PASSWORD.



Adam Shane
Principal Solution
Architect
Leidos



Industry Commentary: OMB Circular A-130 – Managing Information as a Strategic Resource

Circular A-130, “Managing Information as a Strategic Resource,” published by the Office of Management and Budget (OMB), sets policy and establishes guidance for management of Federal information resources. As OMB is within the Executive Office of the President, OMB A-130 is authoritative and clarifies policies for both Federal agencies and service providers.

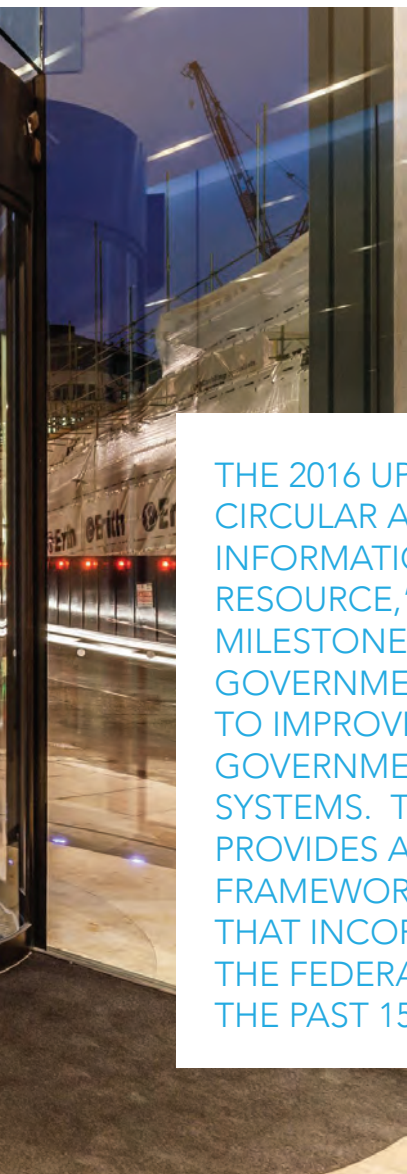
The previous version was published in 2000 on the heels of the dot-com collapse, yet before the creation of the Department of Homeland Security (DHS). Much has changed. The world and government have become heavily dependent on information technology (IT) and the security of the IT ecosystem. After the Office of Personnel Management (OPM) data breach and subsequent

“cybersecurity sprint,” OMB released a new revision of Circular A-130 in July of 2016. The 2016 revision addresses new statutory requirements (e.g., FISMA 2014) and the enhanced technological capabilities that are now available.

MAJOR CHANGES

The 85-page July 27, 2016 revision can be considered a major rewrite with significant changes throughout the document. The following aspects of the revision are particularly significant to entities involved with logical and physical access control, smart card technology, identity management, and associated security systems:

- Federal Information is now seen as a strategic resource, with a focus on IT, security, data governance, and privacy



THE 2016 UPDATE TO THE OMB CIRCULAR A-130, "MANAGING INFORMATION AS A STRATEGIC RESOURCE," IS AN IMPORTANT MILESTONE FOR THE FEDERAL GOVERNMENT IN ITS INITIATIVES TO IMPROVE THE SECURITY OF GOVERNMENT INFORMATION SYSTEMS. THE DOCUMENT PROVIDES AN OVERARCHING FRAMEWORK OF GUIDANCE THAT INCORPORATES MANY OF THE FEDERAL INITIATIVES OF THE PAST 15 YEARS.

Accordingly, the guidance establishes general policy for IT planning and budgeting through governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. The guidance includes:

- » Moving from periodic checklist compliance to ongoing monitoring assessment and evaluation and providing guidance to embrace new technology and solutions
- » Conducting proactive risk management with repeated testing of agency solutions
- » Assigning responsibility and accountability to everyone (government and citizens) for assuring privacy (especially personally identifiable information (PII)) and the security of information
- The guidance establishes the chief information officer (CIO) as the accountable party and mandates a Senior Agency Official for Privacy (SAOP)

- The guidance reinforces aspects of Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standard (FIPS) 201, and associated documents and encapsulates the principles into one authoritative policy document
- The guidance more explicitly brings the existence of a physical access control system (PACS) under the jurisdiction of the CIO and IT departments, who now clearly have the budgeting, planning, funding, and decision-making authority

The 2016 update to the OMB Circular A-130, "Managing Information as a Strategic Resource," is an important milestone for the Federal government in its initiatives to improve the security of government information systems. The document provides an overarching framework of guidance that incorporates many of the Federal initiatives of the past 15 years.

KEY AREAS IMPACTED

For Federal agencies implementing and industry suppliers providing logical and physical access control, smart card technology, identity management, and associated security systems, the Secure Technology Alliance identified several key areas that the guidance impacts, including:

- Providing a continued strong focus on the need for implementing updated Federal information systems that address information security and privacy
- Reinforcing the requirements of HSPD-12 and FIPS 201 and the use of the PIV credential for Federal employees and contractors
- Defining PACS as an information system that is under the jurisdiction of the CIO and IT departments
- Assigning responsibility to specific agency staff for modernization of IT resources
- Requiring agencies to prioritize funding for modernization of IT resources

The Secure Technology Alliance believes that OMB Circular A-130 will help Federal agencies implement identity and information security systems more efficiently and effectively.

ABOUT THIS POSITION PAPER

The Secure Technology Alliance [Access Control Council](#) developed this position paper to highlight the impact of the OMB Circular A-130 2016 update on the access control industry and on government agencies procuring and implementing access control systems. The position paper focuses on highlighting relevant changes in the 2016 update to A-130, discussing the impact of these changes on the Federal government and commercial industry, and outlining issues to be considered in complying with A-130 for selected topic areas. Access Control Council members involved in the development of this position paper included: Defense Manpower Data Center (DMDC); General Services Administration (GSA); ID Technology Partners; IQ Devices; Parsons/Secure Missions Solutions; SigNet Technologies, Inc.; XTec, Inc.



HEALTH AND HUMAN SERVICES COUNCIL

MISSION: Promote the adoption of secure technologies in healthcare and human services organizations

OFFICERS

- Chair: Morgan Richard, XTec, Inc.
- Vice Chair: Jeff Fountaine, Ingenico
- Secretary: Stefan Barbu, NXP Semiconductors

STEERING COMMITTEE

- Stefan Barbu, NXP Semiconductors
- Jeff Fountaine, Ingenico
- Morgan Richard, XTec, Inc.
- Nicole Williams, Gemalto

TOP CONTRIBUTORS

- Stefan Barbu, NXP Semiconductors
- John Ekers, ABCorp
- Jeff Fountaine, Verifone

HONOR ROLL

- Stefan Barbu, NXP Semiconductors
- John Ekers, ABCorp
- Jeff Fountaine, Verifone
- Morgan Richard, XTec, Inc.

ACTIVITIES

- Council Steering Committee and officer elections (Dec. 2016, Jan. 2017)
- Client Advisory Board: development of recruiting material (Dec. 2016)
- Healthcare infographic webinar project (in process)
- Relationships with Healthcare Information Management Systems Society (HIMSS), National Association of Healthcare Access Management (NAHAM), Secure ID Coalition, and Workgroup for Electronic Data Interchange (WEDI)

HEALTH AND HUMAN SERVICES COUNCIL MEMBER ORGANIZATIONS

ABCorp • Advanced Card Systems Ltd. • Clear2Pay • Conduent • Entrust Datacard • First Data • Fiserv • G+D Mobile Security • Gemalto • Hewlett-Packard Enterprise Services LLC • IDEMIA • Ingenico • Initiative for Open Authentication (OATH) • Lenel • Mastercard • NXP Semiconductors • PPG Industries, Inc. • Rambus • SAIC – Science Applications International Corporation • SecureKey Technologies • STMicroelectronics • SureID, Inc. • Thales • Tyco Software House • U.S. Department of State • Verifone • XTec, Inc.

YEAR IN REVIEW: HEALTH AND HUMAN SERVICES COUNCIL CHAIR

A Year of Focus

The Health and Human Services (HHS) Council, like the Secure Technology Alliance, has gone through a year of development, refocus and change. The Council focused on strong authentication beyond the roll of smart cards in the public and private healthcare market. This year, key discussions and projects focused on updating the Council mission statement to include the increased focus on mobility and the Internet of Things (IoT), developing material for Council marketing and outreach to other organizations, discussing the role of the new government administration on healthcare reform, and developing a presentation to augment and describe in detail the Healthcare 2.0 infographic. These projects continued to highlight the theme that a higher level of assurance is needed in all aspects of the healthcare market.

CURRENT STATE OF HEALTHCARE IDENTITY MANAGEMENT

The current healthcare environment continues to remain complex, fragmented and highly regulated. A number of converging factors highlight the need to rethink the current models of operations for public and private organizations, and there is no “silver bullet” to solve all of the current challenges. Key areas in need of attention continue to be: patient identity; patient healthcare record management; medical identity theft; medical fraud; patient privacy; and the security and portability of identity and healthcare records. Additionally, healthcare organizations are moving toward mobile solutions allowing an easier access to care. Strong authentication is not the only solution for solving all identity management challenges; however, it is the cornerstone for any solid solution to be implemented. Mobile solutions built on the core technology provided by smart cards are offering greater opportunity and flexibility; however stringent identity management standards are still vital to protecting an individuals’ personal health information (PHI).

COUNCIL HIGHLIGHTS

The HHS Council is a small and very effective council. Our members have diverse backgrounds and represent organizations from payers to providers to government contractors. This year we focused on aligning our mission and outreach material to support the expanded mission of the Secure Technology Alliance. This included discussing how the HHS Council can make an impact in the market, partnering with other organizations like the Health Information Management and Systems Society (HIMSS), attracting new members, and developing new strategic contacts. The Council also finalized our one-page marketing document that highlights the “new” Council ideals and mission and developed an initial draft of the presentation that details the Healthcare 2.0 infographic. The goal of this presentation is to aid Council representatives in presenting and describing the Healthcare 2.0 infographic, the ideal identity management solution for healthcare, in detail. The resulting presentation can be used for conference presentations, webinars and future marketing.

FUTURE PROJECTS

Future projects for the Council include contributing a use case to the Secure Technology Alliance Identity Council’s mobility use case white paper, finalizing the presentation that describes the Healthcare 2.0 infographic, and focusing on projects that highlight mobility and the Internet of Things (IoT) – including potentially the security of wearable devices – in healthcare. New ideas, recommendations for guest speakers on our conference calls, and topic discussions are always welcome. We look forward to another successful year and welcome new participation. Thank you to all of the current HHS Council members for your ideas, dedication, participation and efforts.

IT IS EVIDENT THAT ONE OF THE KEY TASKS IN CREATING HEALTHCARE POLICY IS TO SOLVE THE PROBLEMS OF PROPERLY IDENTIFYING PATIENTS AND HEALTHCARE PROVIDERS, MATCHING HEALTHCARE RECORDS, AND IDENTIFYING THOSE THAT HAVE AUTHORIZED ACCESS TO PROTECTED HEALTH INFORMATION.



Morgan Richard
Manager, U.S. Health Care
XTec, Inc.



IDENTITY COUNCIL

MISSION: Raise awareness and provide thought leadership and education on real-world issues of implementing and operating identity and identity authentication and authorization systems

OFFICERS

- Vice Chair: Neville Pattinson, Gemalto

STEERING COMMITTEE

- Stefan Barbu, NXP Semiconductors
- Ahmed Mohammed, IDEMIA
- Neville Pattinson, Gemalto
- Steve Rogers, IQ Devices
- Rob Zivney, Identification Technology Partners

TOP CONTRIBUTORS

- Peter Cattaneo, Identiv
- Salvatore D'Agostino, IDmachines
- Tom Lockwood, NextgenID, Inc.
- Neville Pattinson, Gemalto

HONOR ROLL

- Peter Cattaneo, Identiv
- Salvatore D'Agostino, IDmachines
- Tom Lockwood, NextgenID, Inc.
- Neville Pattinson, Gemalto
- Steve Rogers, IQ Devices

ACTIVITIES

- Submission of industry comments on NIST Draft SP 800-63 "Digital Identity Guidelines," in collaboration with the Access Control Council (Mar. 2017)
- Council charter update (Mar. 2017)
- Mobile identity credentials landscape white paper (in process)
- Relationships with American Association of Airport Executives (AAAE), American Association of Motor Vehicle Administrators (AAMVA), and International Biometrics + Identity Association (IBIA)

IDENTITY COUNCIL MEMBER ORGANIZATIONS

Burden Consulting, Ltd. • CH2M • Consult Hyperion • Defense Manpower Data Center (DMDC) • Discover Financial Services • Entrust Datacard • Exponent, Inc. • Fiserv • G+D Mobile Security • Gemalto • General Services Administration (GSA) • Hewlett-Packard Enterprise Services LLC • HID Global • Identification Technology Partners, Inc. • IDEMIA • Identiv • Infineon Technologies • Initiative for Open Authentication (OATH) • Intercede Limited • IQ Devices • Kona I Co., Ltd. • Lenel • Metropolitan Transportation Commission (MTC) • Multos International • NextgenID, Inc. • NXP Semiconductors • Quantum Secure • SAIC – Science Applications International Corporation • SecureKey Technologies • SigNet Technologies, Inc. • Southeastern Pennsylvania Transportation Authority (SEPTA) • SureID, Inc. • Tyco Software House • Ultra Electronics Card Systems • U.S. Department of Homeland Security • U.S. Department of State • Visa Inc. • Wells Fargo • XTec, Inc.

YEAR IN REVIEW: IDENTITY COUNCIL

A Look at the Identity Council

The Identity Council expanded its charter in 2017 to focus on broader identity authentication solutions leveraging embedded chip technology and privacy- and security-enhancing software. The Council works on projects to influence standards and best practices, serves as an educational resource, and provides a voice in public policy influencing adoption, implementation, and use. The Identity Council remains the focal point for the Alliance's identity-related efforts, and collaborates with other councils to provide guidance on relevant projects. Key areas of focus for the Identity Council are: identity trust frameworks; digital identity; strong authentication; authorization; and biometrics.

UPDATED PRIORITIES

As part of expanding its charter, the Council also reviewed its activities and developed an updated set of priorities. Going forward, the Council plans to:

- Develop identity-related educational resources for the public and private sectors to inform buyers and requirement setters and promote market adoption and expansion
- Promote a person-centric view of identity management supporting both central identity management and the interoperability of systems to reduce silos or closed identity environments
- Promote identity trust frameworks and best practices as potential solutions in the absence of a single government or commercial issuer
- Enhance and support awareness across the identity community to gain synergy of efforts, reduce redundancy and reduce overlap of member resources
- Develop industry positions on key identity issues and offering perspectives on solutions
- Maintain an active, public voice on identity topics, promoting the positive aspects of identity technology solutions, and responding to misinformation about identity technology
- Advocate the use of biometric technology as an important component of many identity systems

Having already published a comprehensive set of foundational resources on how to design security and privacy into identity management systems, the Council shifted its efforts in 2017 to look specifically at mobile.

RESOURCE CREATION

The Council identified a key problem in implementing mobile identity credentials: the industry is faced with inconsistent solutions, methodologies, and practices, impacting quality and consistency of products, services and user experience. The Council is developing a new white paper to provide an educational resource that discusses the current mobile identity landscape. Members from multiple councils are collaborating on this project to document current mobile identity credential use cases, including how the use case is being implemented and what challenges are being faced. Use cases include: mobile driver's licenses; PIV derived credentials, airline/airport identity credentials; physical and logical access credentials; and multi-modal ticketing for transportation.

The Council actively supports other Alliance industry councils with its expertise in identity and identity management, and welcomes new participants the Alliance tackles the challenges of implementing identity systems in the increasingly connected world.

THE COUNCIL IDENTIFIED A KEY PROBLEM IN IMPLEMENTING MOBILE IDENTITY CREDENTIALS: THE INDUSTRY IS FACED WITH INCONSISTENT SOLUTIONS, METHODOLOGIES, AND PRACTICES, IMPACTING QUALITY AND CONSISTENCY OF PRODUCTS, SERVICES AND USER EXPERIENCE.



IOT SECURITY COUNCIL

MISSION: Develop and promote best practices and provide educational resources on implementing secure IoT architectures using “embedded security and privacy”

LEADERSHIP COMMITTEE

- Willy Dommen, Accenture
- Gonda Lamberink, UL
- Sami Nassar, NXP Semiconductors
- Christopher Williams, Exponent

TOP CONTRIBUTORS

- Imran Hajimusa, Verifone
- Gonda Lamberink, UL
- Nicholas Vondrak, IDEMIA

HONOR ROLL

- Stefan Barbu, NXP Semiconductors
- Maarten Bron, UL
- Ilker Caner, Cardtek US
- Hank Chavers, GlobalPlatform
- Touhid Choudhury, Kona I co. Ltd.
- Stu Cox, G+D Mobile Security

- Willy Dommen, Accenture
- Chris Edwards, Intercede Limited
- Tara Gay, American Express
- Imran Hajimusa, Verifone
- Jack Jania, Gemalto
- Gonda Lamberink, UL
- Tom Lockwood, NextgenID, Inc.
- Mina Malak, G+D Mobile Security
- Sami Nassar, NXP Semiconductors
- John Neal, NXP Semiconductors
- Nick Norman, Consult Hyperion
- Jerome Schang, NXP Semiconductors
- Srinath Sitaraman, UL
- Fatih Teksoy, Cardtek US
- Nicholas Vondrak, IDEMIA
- Christopher Williams, Exponent

ACTIVITIES

- IoTSecurityConnection.com content hub (Aug. 2016)
- Security of Things conference program planning (Aug./Sept. 2016)
- In-person meeting at the Security of Things conference (Oct. 2016)
- “[Embedded Hardware Security for IoT Applications](#)” white paper (Dec. 2016)
- Smart Cities and Transportation Workshop at Utah Transit Authority (UTA) in Salt Lake City, UT, in collaboration with the Transportation Council (Feb. 2017)
- IoT Payments 2017 program planning (July/Aug. 2017)
- IoT and Payments: Current Market Landscape white paper (Dec. 2017)

IOT SECURITY COUNCIL MEMBER ORGANIZATIONS

Accenture • Allegion • American Express • Burden Consulting, Ltd. • Cardtek US • CH2M • Chase Card Services • Conduent • Consult Hyperion • CPI Card Group • Datawatch Systems • Defense Manpower Data Center (DMDC) • Discover Financial Services • Entrust Datacard • Exponent, Inc. • First Data • FIS • Fiserv • G+D Mobile Security • Gemalto • Hewlett-Packard Enterprise Services LLC • HID Global • IDEMIA • Identification Technology Partners, Inc. • Infineon Technologies • Ingenico, North America • Initiative for Open Authentication (OATH) • Interac Association/Acsys Corporation • Intercede Limited • IQ Devices • LTK Engineering Services • Mastercard • Metropolitan Transportation Authority (MTA) • Metropolitan Transportation Commission (MTC) • NextgenID, Inc. • NXP Semiconductors • Quantum Secure • Rambus • SAIC – Science Applications International Corporation • San Francisco Bay Area Rapid Transit District (BART) • Scheidt & Bachmann USA • SHAZAM • SigNet Technologies, Inc. • Southeastern Pennsylvania Transportation Authority (SEPTA) • STMicroelectronics • SureID, Inc. • TSYS • Tyco Software House • U.S. Department of Transportation/Volpe Center • Underwriters Laboratories (UL) • Valid USA • Verifone • Visa Inc. • Wells Fargo • XTEC, Inc.

YEAR IN REVIEW: IOT SECURITY COUNCIL

A Look at the Internet of Things Security Council

Analysts are forecasting over 20 billion IoT devices by 2020 for a wide variety of applications in many industries, including industrial, energy, automotive, smart city, healthcare, freight/logistics, and home automation. The pervasiveness of connected devices and the impact that they will have on society demands proactive discussion of potential security vulnerabilities and architectures/technologies that have been designed to mitigate the vulnerabilities. Security vulnerabilities have already been found in initial IoT implementations; it is critical for the growth of the market that security and privacy be designed into the IoT ecosystem.

FOCUS ON IOT MARKETS

The Secure Technology Alliance IoT Security Council was formed last year to develop and promote best practices and provide educational resources on implementing secure IoT architectures using “embedded security and privacy.” The Council focuses on IoT markets where security, safety and privacy are key requirements and leverages the industry expertise and knowledge gained from implementing embedded security technology for payment, identity, healthcare, transport and telecommunications systems to provide practical guidance for secure IoT implementations.

The Council established the following priorities for its activities:

- 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-focused organization to discuss best practices and implementation of IoT architectures using embedded security and privacy
- Provide a single organization where all industry stakeholders can network, 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

THE SECURE TECHNOLOGY ALLIANCE IOT SECURITY COUNCIL WAS FORMED LAST YEAR TO DEVELOP AND PROMOTE BEST PRACTICES AND PROVIDE EDUCATIONAL RESOURCES ON IMPLEMENTING SECURE IOT ARCHITECTURES USING EMBEDDED SECURITY AND PRIVACY.

RESOURCES PRODUCED

During 2017, the IoT Security Council published two resources. First was the development of a foundational white paper on “Embedded Hardware Security for IoT Applications.” While acknowledging that each IoT ecosystem needs to assess its security requirements and determine the appropriate level of security that should be implemented, the white paper shows how embedded hardware security is critical for IoT environments that require the highest level of confidentiality, integrity and availability and that need to ensure authenticated and authorized access.

A second project on “IoT payments” was launched in collaboration with the Payments Council. The resulting white paper reviews the environments and use cases for IoT and payments, discusses security implications, and outlines key implementation considerations for implementing payment. While IoT payments are still emerging, the potential for growth demands early attention on how security is implemented, so that security is designed into products and transactions, and not added as an afterthought.

Council members also presented multiple sessions in the Secure Technology Alliance IoT Payments 2017 event and discussed plans for follow-on projects on IoT device authentication and secure life cycle management – functions that embedded hardware security technologies are well suited to address.

The Council is currently developing plans for 2018 and welcomes new member participation!

Embedded Hardware Security for IoT Applications

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

Healthcare, smart city, consumer electronics, industrial, payments and numerous other verticals are developing services that rely on an IoT infrastructure. Security is a core inherent requirement to deliver safe and reliable IoT services spanning from the cloud to connected devices.

EMBEDDED HARDWARE SECURITY FOR IOT DEVICES

IoT devices are potential entry points to wider IoT ecosystems. Through different IoT devices, including both new connected devices and more traditional network equipment, unauthorized access to wider networks, databases, and systems can be obtained, therefore increasing an attack vector. Hence, it is critical to not only ensure confidentiality, integrity and availability, but also to take into account proper access control mechanisms – specifically identification, authentication and authorization procedures.

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

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

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

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

SECURITY BY DESIGN

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

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

Embedded hardware security, among other embedded security techniques, can protect the “identity” of each device, to prevent unauthorized tampering with how these devices are designed to work, and to protect the privacy and security of the vast amount of data the devices generate.

A principle behind the security of smart chips is that the chips not only control how the devices perform under normal conditions, but also control how the devices react when they are attacked or tampered with in any way, including self-destruction. Applying embedded security techniques, including hardware-based – as already proven and implemented for other security use cases – can deliver security mechanisms for the billions of connected IoT devices.

ABOUT THIS WHITE PAPER

This white paper was developed by the Smart Card Alliance [IoT Security Council](#) to provide an educational resource on the value of embedded hardware security in end devices used in IoT applications. Members involved in the development of this white paper included: Accenture; Allegion; CH2M; Discover Financial Services; Exponent, Inc.; First Data; Gemalto; Giesecke & Devrient; Hewlett Packard Enterprise; Intercede Limited; IQ Devices; Metropolitan Transportation Commission (MTC); NextgenID, Inc.; NXP Semiconductors; Safran Identity & Security; SigNet Technologies, Inc.; TSYS; Underwriters Laboratories (UL); Verifone.

IoT Payments Market Landscape

The Internet of Things (IoT) is growing rapidly—8.4 billion connected “things” are in use today. Gartner forecasts the number of things will increase to 20 billion in 2020, and starting in 2017, Statista projects that the IoT market will be worth more than \$1 billion annually. “Things” range from thermostats to automobiles, are used by individuals and businesses, and enable use cases that only a few years ago seemed like fiction. Cars talk to each other, and your refrigerator can order groceries.

and technology companies can now create innovative capabilities that deliver increasingly frictionless, relevant, and secure payment experiences.

Figure 1 illustrates the five key components of IoT payment: device, connectivity, credentials, experience and security. IoT devices range from small wearable devices and shopping carts to home appliances and cars. Depending on the environment, the IoT device will use a connectivity channel to trigger the payment transaction. Pay-

INFANCY STAGE

IoT payments are currently still in their infancies. A majority of IoT devices do not have the ability to engage in commerce, much less imbed the ability to conduct secure payments. The future of IoT payments depends not only on the creation of use cases that solve a customer problem or improve the consumer experience, but also on the IoT economic ecosystem’s ability to create and sustain consumer trust in the ability to perform commercial transactions using an IoT device.

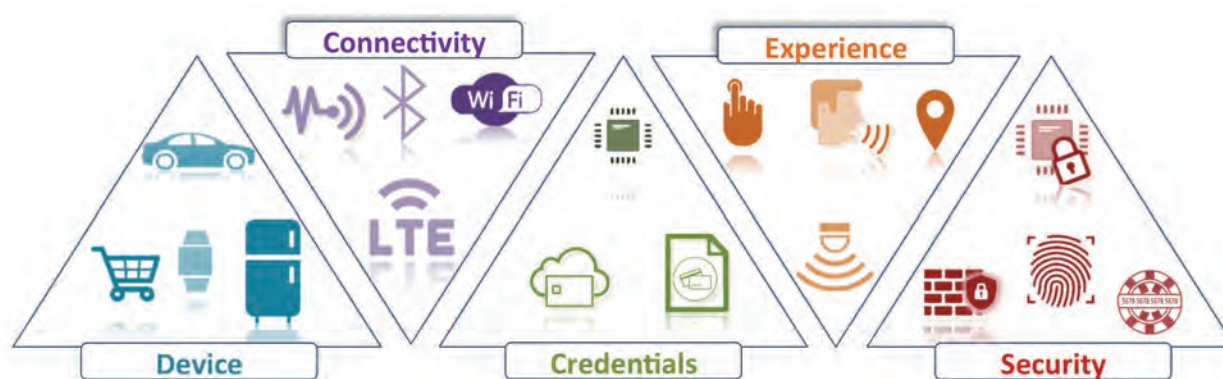


FIGURE 1. KEY ASPECTS OF IOT PAYMENTS IMPLEMENTATIONS

As more devices become connected, new digital experiences can be developed for both consumers and businesses alike. One of the experiences that can be enabled is extending payments directly into these IoT devices, either as ways to pay or ways to accept payment. The movement towards the IoT demonstrates the continued evolution of digital payments, with the addition of this new category of devices building on browser and mobile experiences.

PAYMENT TOUCH POINTS

Consumers can pay using a range of newly connected devices, including connected cars, household appliances, and most recently, fitness wearables. In parallel, the IoT is also expanding the point of sale to include a number of new touch points, including parking meters, fitting room mirrors, and vending machines. As a result, financial institutions, payment providers,

merchant credentials can be stored remotely, in the cloud, or locally, in a secure element, depending on the form factor and payment use case. The consumer experience can vary; it ranges from pushing a button or using voice commands to a frictionless experience based on location or sensors. Data is secured using a variety of techniques to authenticate the consumer and device and transmit the payment credentials securely.

Several categories of IoT commerce use cases that have emerged thus far are: connected cars, smart home appliances, wearables, virtual or augmented reality devices, industrial devices, and retail. In addition, global payment networks are playing a central role in fostering IoT payments, including helping build the industry framework to ensure interoperability and payment acceptance across IoT devices.

ABOUT THIS WHITE PAPER

This white paper was developed by the Secure Technology Alliance IoT Security Council to provide a resource for the industry that describes the current landscape for IoT payments and outlines key considerations for implementing payments with IoT devices. Members involved in the development of this white paper included: American Express; Cardtek; Consult Hyperion; CPI Card Group; Discover Financial Services; Entrust Datacard; G+D Mobile Security; Gemalto; GlobalPlatform; IDEMIA; Ingenico; Initiative for Open Authentication (OATH); IQ Devices; Mastercard; Metropolitan Transportation Commission (MTC); NextgenID; NXP Semiconductors; Rambus; Underwriters Laboratories (UL); Visa Inc.



MOBILE COUNCIL

MISSION: Raise awareness and accelerate the adoption of secure payments, loyalty, marketing, promotion/coupons/offers, peer-to-peer, identity, and access control applications using mobile and tethered wearable devices

OFFICERS

- Co-Chairs: Sadiq Mohammed, Mastercard; Sridher Swaminathan, First Data
- Vice Chair: Damon Kachur, G+D Mobile Security

STEERING COMMITTEE

- Maarten Bron, UL
- David deKozan, Cubic Transportation Systems
- Imran Hajimusa, Verifone
- Peter Ho, Wells Fargo
- Damon Kachur, G+D Mobile Security
- Simon Laker, Consult Hyperion
- Umesh Kulkarni, FIS Open Test Solutions
- Don Malloy, OATH
- Sadiq Mohammed, Mastercard
- Brian Stein, CH2M
- Chandra Srivastava, Visa Inc.
- Sridher Swaminathan, First Data
- David Worthington, Rambus

TOP CONTRIBUTORS

- Hank Chavers, GlobalPlatform
- Christine Lopez, Vantiv
- Lokesh Rachuri, Capgemini
- Tony Sabetti, JPMorgan Chase

HONOR ROLL

- Deborah Baxley, PayGility Advisors
- Hank Chavers, GlobalPlatform
- David deKozan, Cubic Transportation Systems
- Jose Diaz, Thales e-Security
- Chris Edwards, Intercede Limited
- Sarah Hartman, TSYS
- Peter Ho, Wells Fargo
- Damon Kachur, G+D Mobile Security
- Christine Lopez, Vantiv
- Oleg Makhotin, IDEMIA
- Jean-Louis Meyer, Entrust Datacard
- Sadiq Mohammed, Mastercard
- Manish Nathwani, SHAZAM

- Joseph Pearson, HID Global
- Lokesh Rachuri, Capgemini
- Steve Rogers, IQ Devices
- Tony Sabetti, JPMorgan Chase
- John Sheets, Visa Inc.
- Sridher Swaminathan, First Data

ACTIVITIES

- “[EMV Tokenization](#)” webinar (Nov. 2016)
- [Council Steering Committee and officer elections](#) (Dec. 2016, Jan. 2017)
- “[Mobile Identity Authentication](#)” white paper (Mar. 2017)
- In-person meeting at Payments Summit (Mar. 2017)
- Trusted Execution Environment (TEE) 101 white paper (in process)
- Relationship with GlobalPlatform

MOBILE COUNCIL MEMBER ORGANIZATIONS

ABCorp • Accenture • Allegion • American Express • Burden Consulting, Ltd. • Cardtek US • CH2M • Chase Card Services • Conduent • Consult Hyperion • CPI Card Group • Cubic Transportation Systems, Inc. • Datawatch Systems • Discover Financial Services • Entrust Datacard • Exponent, Inc. • FIME • First Data • FIS • Fiserv • G+D Mobile Security • Gemalto • Hewlett-Packard Enterprise Services LLC • HID Global • IDEMIA • Identification Technology Partners, Inc. • InComm • Infineon Technologies • Ingenico, North America • Initiative for Open Authentication (OATH) • Interac Association/Acsys Corporation • Intercede Limited • IQ Devices • Kona I Co., Ltd. • Lenel • Mastercard • NBS Technologies • NXP Semiconductors • Quantum Secure • Rambus • SecureKey Technologies • SHAZAM • STMicroelectronics • SureID, Inc. • Thales • TSYS • U.S. Department of Homeland Security • Underwriter Laboratories (UL) • Valid USA • Verifone • Visa Inc. • Vix Technology • Wells Fargo • XTEC, Inc.

YEAR IN REVIEW: MOBILE COUNCIL CO-CHAIRS

Innovations Make for an Exciting Time in Mobile

In 2017, the mobile industry continued its trend of bringing new innovations and user experiences to consumer mobile devices. The latest smartphones from Apple, Google and Samsung show significant improvements in hardware with increased processing power and battery life, improved biometric sensors, sophisticated cameras and the ability for wireless charging. Further, Google's \$1.1 billion investment in acquiring HTC's mobile team that built the Pixel smartphone shows an emphasis on hardware, and that the hardware/software synergy that has propelled Apple and Samsung is an important competitive aspect.

From a software perspective, device software is becoming increasingly sophisticated, with image/pattern recognition algorithms to drive biometric sensors for authentication, built-in personal assistants and other artificial intelligence (AI) features. In addition, improved hardware is allowing for the development of CPU intensive applications like virtual reality (VR) and augmented reality (AR) applications.

VOICE-ACTIVATED ASSISTANTS

When it comes to personal assistants, however, mobile devices appear to be in competition with a new segment of hardware –voice activated speakers. Starting with Amazon Echo, both Google and Apple have their own versions of home speakers that are capable of conversing with you and getting simple tasks done. Nevertheless, like many wearables and other accessories, they all may eventually tie back or integrate with the mobile device, creating new opportunities for mobile applications. For example, you can ask the Google Home device for directions and it will send directions to your mobile device.

With numerous innovations in the mobile space, it is an exciting time for the Mobile Council to drive activities that help us understand and educate fellow industry members about these innovations. Some of these discussions are happening as part of other council projects, and we are glad to see Mobile Council members participate in these various initiatives. Given that mobile plays an integral role in many different verticals, we anticipate that cross-council collaboration will continue to be the preferred approach.

On the payments front, we are starting to see mobile devices stretch beyond contactless or NFC payments to payments using QR codes. EMVCo has also published specifications for QR-code-based payments. Walmart has been experimenting with its "Scan and Go" payments, and Amazon has been testing Amazon Go, a checkout free shopping experience. With Amazon's acquisition of Whole Foods, the retail experience is about to see quite a few innovations and the competition is fierce. This is good news for mobile, as mobile apps will play a huge role in the development of these new retail experiences. Banks not wanting to be left behind are also aggressively pursuing various mobile-based capabilities. For example, person-to-person (P2P) payments have been rolled out with the launch of Zelle, and chatbot applications are being experimented with to address simple customer service needs.

Smartphone penetration is growing at a rapid pace and is expected to surpass six billion devices by the year 2020. With that kind of penetration, we anticipate that new mobile applications will push the use of mobile phones into areas never imagined before. We sincerely thank all Mobile Council members for their efforts this year and encourage everyone to actively participate in this journey.

GIVEN THAT MOBILE PLAYS AN INTEGRAL ROLE IN MANY DIFFERENT VERTICALS, WE ANTICIPATE THAT **CROSS-COUNCIL COLLABORATION** WILL CONTINUE TO BE THE PREFERRED APPROACH.



Sadiq Mohammed
Vice President, EMV
and Digital Devices
Mastercard



Sridher Swaminathan
Director, Product Man-
agement | Emerging
Payment Solutions
First Data



Mobile Identity Authentication

Consumers expect to be able to use their mobile phones to interact with remote systems and experience the same level of functionality and security as when they use a personal computer, laptop, or tablet. While the size of the mobile phone's screen has expanded, the interface displayed on the screen is still relatively restricted. For example, a recent study has shown that the transaction abandonment rate for eCommerce shoppers using mobile phones outpaces the rate for shoppers using personal computers, laptops, and tablets. Users noted that it was too complex to load user ID and credit card information into the system during checkout while using their mobile phone. This limitation means that systems wishing to grant secured access to mobile users need to find elegant ways to authenticate users quickly, without compromising system security.

Mobile ID authentication is a response to this dilemma. Mobile ID authentication can identify a mobile phone user, reliably and securely, through a greatly simplified user experience, reducing friction for the user without compromising security.

MOBILE ID AUTHENTICATION CAN IDENTIFY A MOBILE PHONE USER, RELIABLY AND SECURELY, THROUGH A GREATLY SIMPLIFIED USER EXPERIENCE, REDUCING FRICTION FOR THE USER WITHOUT COMPROMISING SECURITY.

MULTIPLE TECHNOLOGIES USED

Mobile ID authentication relies on a number of technologies that leverage both hardware and software techniques to reliably identify a user and that user's mobile device for security purposes. Mobile ID authentication supports legally binding authentication and transaction signing for online banking, payment, corporate services, and other secure consumer services (e.g., streaming online content). A user is issued digital credentials that are stored securely on the mobile device (for example, in a hardware secure element (SE)). The user must then be authenticated

locally to the mobile device by entering a passcode or PIN or by using device-level biometrics to be able to use the stored credentials.

Users can prove device ownership and present their secure credentials in several ways:

- **In app** - The credential is pulled from the secure storage location and transferred to a mobile app for sign in
- **In browser** - The credential is pulled from the secure storage location and transferred to a mobile-enabled secured website using a browser

AUTHENTICATION TECHS

Mobile ID authentication relies on a number of technologies that leverage both hardware and software techniques to reliably identify a user and that user's mobile device for security purposes. Users can prove device ownership and present their secure credentials in several ways:



In app

The credential is pulled from the secure storage location and transferred to a mobile app for sign in



In browser

The credential is pulled from the secure storage location and transferred to a mobile-enabled secured website using a browser



Using NFC

The credentials are pulled from the secure storage location and transferred to an NFC reader using card emulation



Using an out-of-band sign on

The credentials are used as a primary or secondary factor for strong authentication

- **Using NFC** - The credentials are pulled from the secure storage location and transferred to an NFC reader using card emulation
- **Using an out-of-band sign on** - The credentials are used as a primary or secondary factor for strong authentication



The white paper provides an overview of mobile ID authentication technology and market trends. It discusses various authentication techniques and the approaches to securing sensitive user credentials on a mobile device. The white paper highlights several technology and solution options which are in use today, and looks at efforts underway to solidify some of the emerging standards (e.g., 3D Secure and the FIDO protocols). A variety of example use cases are summarized, including implementation considerations and challenges and, where appropriate, real-world implementations. Uses highlighted include access control, payments, government-to-consumer services, and corporate applications. Mobile devices include smartphones, tablets, and smart watches.

ABOUT THE WHITE PAPER

The Secure Technology Alliance Mobile Council developed this white paper to provide an educational resource on mobile identity authentication techniques and use cases. Participants involved in the development of this white paper included: Capgemini; CH2M; CPI Card Group; Discover Financial Services; Entrust Datacard; First Data; FIS; Giesecke & Devrient; GlobalPlatform; HID Global; ID Technology Partners; Intercede; IQ Devices; JPMorgan Chase; Oberthur Technologies; PayGility Advisors; SHAZAM; TSYS; Vantiv; Verifone; Wells Fargo.



PAYMENTS COUNCIL

MISSION: Focus on securing payments and payment applications in the U.S. through industry dialogue, commentary on standards and specifications, technical guidance and educational programs

OFFICERS

- Co-chairs: Jack Jania, Gemalto; Oliver Manahan, Infineon Technologies
- Vice Chair: Nick Pisarev, G+D Mobile Security
- Secretary: Jamie Topolski, Fiserv

STEERING COMMITTEE

- Laurie Dornberger, CPI Card Group
- Jose Correa, NXP Semiconductors
- Brady Cullimore, American Express
- Terry Dooley, SHAZAM
- Allen Friedman, Ingenico
- Melanie Gluck, Mastercard
- Imran Hajimusa, Verifone
- Simon Hurry, Visa Inc.
- Jack Jania, Gemalto
- Oliver Manahan, Infineon Technologies
- Josh Martiesian, MTA
- Nick Pisarev, G+D Mobile Security
- Peter Quadagno, Thales
- Sherif Samy, UL
- Ellie Smith, Discover Financial Services
- Brian Stein, CH2M
- Terri Strickland, Wells Fargo
- Sridher Swaminathan, First Data
- Jamie Topoloski, Fiserv

TOP CONTRIBUTORS

- Jose Correa, NXP Semiconductors
- Nick Pisarev, G+D Mobile Security
- Jamie Topolski, Fiserv

HONOR ROLL

- Andreas Aabye, Visa Inc.
- Clinton Allen, American Express
- Philip Andreae, IDEMIA
- Suresh Bachu, Discover Financial Services
- Deborah Baxley, PayGility Advisors
- David Bibby, Discover Financial Services
- Stefania Boiocchi, Infineon Technologies
- Jay Bozicevich, Wells Fargo
- Maarten Bron, UL
- Roberto Cardenas, TSYS
- Hank Chavers, GlobalPlatform
- Jose Correa, NXP Semiconductors
- Brady Cullimore, American Express
- Cindy Custers, American Express
- Simon Dix, Mastercard
- Emmanuelle Dottax, IDEMIA
- Allen Friedman, Ingenico
- Melanie Gluck, Mastercard
- Amanda Guillen, Discover Financial Services
- Murat Guzel, Cardtek US
- Imran Hajimusa, Verifone
- Sarah Hartman, TSYS
- Peg Heuer, Wells Fargo

- Simon Hurry, Visa Inc.
- Jack Jania, Gemalto
- Umesh Kulkarni, FIS Global
- Christine Lopez, Vantiv
- Don Malloy, OATH
- Oliver Manahan, Infineon Technologies
- Chris Marconi, Conduent
- Josh Martiesian, MTA
- Sadiq Mohammed, Mastercard
- Manish Nathwani, SHAZAM
- Nick Pisarev, G+D Mobile Security
- Peter Quadagno, Quadagno & Associates
- Michele Quinn, First Data
- Lokesh Rachuri, Capgemini
- Ellie Smith, Discover Financial Services
- Brian Stein, CH2M
- Terri Strickland, Wells Fargo
- Sridher Swaminathan, First Data
- Jamie Topolski, Fiserv
- Erdal Yazmaci, Cardtek US

ACTIVITIES

- Contactless EMV payments benefits webinars for [merchants](#) (Oct. 2016) and [issuers](#) (Nov. 2016)
- “[Contactless EMV Payments in the U.S. Guides for Merchants and Issuers](#)” infographics (Dec. 2016)
- “[Contactless EMV Payments Security Q&A](#)” (Dec. 2016)
- Council Steering Committee and officer elections (Dec. 2016, Jan. 2017)
- Council charter update (Feb. 2017)
- “[Blockchain and Smart Card Technology](#)” white paper (Mar. 2017)
- In-person meeting at Payments Summit (Mar. 2017)
- “[Implementation Considerations for Contactless Payment-Enabled Wearables](#)” white paper (Oct. 2017)
- EMVCo Payment Account Reference (PAR) use cases white paper (in process)
- Challenges of contactless payments implementation white paper (in process)
- Approaches to secure the CNP environment white paper (in process)
- Relationships with GlobalPlatform and U.S. Payments Forum

PAYMENTS COUNCIL MEMBER ORGANIZATIONS

ABC Corp • Accenture • ACI Worldwide • American Express • Burden Consulting, Ltd. • Cardtek US • CH2M • Chase Card Services • Conduent • Consult Hyperion • CPI Card Group • Cubic Transportation Systems, Inc. • Discover Financial Services • Entrust Datacard • Exponent, Inc. • First Data Corporation • FIS • Fiserv • G+D Mobile Security • Gemalto • IDEMIA • InComm • Infineon Technologies • Ingenico, North America • Initiative for Open Authentication (OATH) • Interac Association/Axsys Corporation • IQ Devices • Jack Henry Processing Solutions • JCB International Credit Card Co., Ltd. • Kona I Co., Ltd. • Lenel • Mastercard • Metropolitan Transportation Authority (MTA) • Multos International • NXP Semiconductors • Quadagno & Associates • Rambus • SecureKey Technologies • SHAZAM • STMicroelectronics • Thales • Tri County Metropolitan Transportation District of Oregon • TSYS • Underwriter Laboratories (UL) • Valid USA • Verifone • Visa Inc. • Vix Technology • Wells Fargo • XTec, Inc.

YEAR IN REVIEW: PAYMENTS COUNCIL CO-CHAIRS

Innovation in the Payments Industry

Innovation is the name of the game across all technology sectors, payments included. With the Internet of Things said to reach 34 billion connected devices by 2020, it's time for the payments industry to capitalize on that growth and utilize new solutions to keep them with the times. Contactless and wearables are just two of those opportunities in addition to tokenization, blockchain and many more.

This year, the Payments Council has focused on educating the industry on these innovative opportunities and encouraging them to look into the future.

RESOURCES FOR ALL

With contactless on the mind, several initiatives of the Payments Council served as continued education resources for all industry players. A series of infographic guides were produced to help both merchants and issuers understand the unique value and benefits contactless payments provide, and separate webinars allowed us to focus on the distinct opportunities for each player.

The Alliance also held an "EMV Tokenization" webinar in the Fall of 2016 to explore an additional important industry topic. The webinar provided an overview of EMV tokenization, reviewed the requirements for token service providers, discussed the tokenization methods used in digital wallets like Apple Pay, Samsung Pay and Android Pay, as well as in-app purchases, and addressed tokenization implementation and security considerations.

Now through next year, we'll be stretching our focus into other innovative payment solutions in addition to contactless, such as securing the CNP environment and implementing payments with wearables. Through documenting best practices, we hope to advance the industry by encouraging major players to stay dynamic and provide new options for their customers.

MOVING TOWARD INNOVATION

In the years to come, innovation is going to be the challenge to address the remaining challenges within the payments world. But by continuing to serve as a leading educator and resource, we have the opportunity to pioneer that movement forward toward contactless, wearables, tokenization and IoT solutions. We also collaborate with other Secure Technology Alliance councils where payments may intersect, such as transit or mobile.

This year, we were honored to have 43 contributors on the honor roll, and we thank each and every one of you for your hard work and contributions. We look forward to a new year, and we are honored to serve as your Co-Chairs of the Payments Council.

WHILE THE PAYMENTS COUNCIL HAS LONG SUCCEEDED IN IDENTIFYING AND EDUCATING ON HIGH LEVEL TRENDS WITHIN THE PAYMENTS INDUSTRY, THE U.S. PAYMENTS FORUM HAS BEEN STRONGEST IN DIVING DEEPER INTO THE SPECIFICS OF WHAT THESE TRENDS FORESHADOW AND HOW THEY WILL IMPACT THE FUTURE. BY UTILIZING EACH GROUP'S STRENGTHS, WE'VE BEEN ABLE TO CREATE A GREATER SYNERGY ACROSS THE INDUSTRY WITHOUT DUPLICATING WORK OR PROVIDING COMPETING MESSAGES.



Jack Jania
Senior Vice President
of Strategic Partnerships
Gemalto



Oliver Manahan
Director, Business Development
Infineon Technologies



Implementation Considerations for Contactless Payment-Enabled Wearables

Wearables, as a general category, cover wide variety of device types – from smartwatches to rings to wristbands to clothing – using different communications and security technologies. The total wearables market is expected to have significant growth, with a recent Gartner report estimating that 310.4 million wearable devices will be sold in 2017, growing to over 504 million by 2021.

This market growth for connected devices presents opportunities for device manufacturers, service providers and the payments industry. Payment-enabling wearables can make payment easier and more convenient for consumers. BI Intelligence estimates that 62 percent of wearable device shipments will include payments functionality by 2020.

Wearables are being developed with many form factors and technologies, with the payment enablement processes varying significantly depending on the device and technology selected. To provide concrete guidance for implementers, the white paper, *Implementation Considerations for Contactless Payment-Enabled Wearables*, published in October 2017, focuses on a subset of wearables and payment processes that encompass the most common implementations today – i.e., contactless transactions using technology that complies with ISO/IEC 14443 and security based on hardware secure elements.

WEARABLES HARDWARE TECHNOLOGIES AND PROVISIONING

Passive wearables include a chip/secure element that has an operating system and payment app (one or more), is connected to an antenna, and has an ISO/IEC 14443 interface. Passive wearables are powered through the contactless interface. A passive *enabled* wearable needs to be personalized at a personalization bureau and may require custom equipment to handle different form factors. A passive *disabled* wearable needs to be personalized at the distribution channel using instant issuance personalization equipment.

Active connected wearables are powered devices that requires a battery. The device connects to a mobile device and has a means to connect to a trusted service manager (TSM) for provisioning. The

wearable device includes a secure element and Near Field Communication (NFC) functionality and is integrated with digital-wallet-enabled solutions (e.g., Apple Pay).

IMPLEMENTATION CONSIDERATIONS

When implementing payment-enabled wearables, the following topics should be considered:

- How will the consumer be motivated to use the wearable for payment? Will there be sufficient acceptance points?
- What is the use case for the wearable? Who is the target customer and when, how and where is the wearable going to be used?
- Who are the stakeholders that will be involved in manufacturing, provisioning, distributing and managing the wearable device?
- What is the certification, testing and approval process? How does this process fit with the overall timeline required for the wearable project?
- How will the payment-enabled wearable lifecycle be managed?

Payment-enabled wearables offer new opportunities for wearable device manufacturers, service providers and the payments industry to offer consumers exciting new payment form factors. From improved convenience for consumers to increased loyalty and “brand stickiness” sought by device manufacturers and service providers, wearables deliver benefits to all stakeholders in the ecosystem.

ABOUT THIS WHITE PAPER

The Secure Technology Alliance Payments Council published this white paper to provide an educational resource on the wearables landscape and to discuss key considerations for implementing payments in wearables.

Participants involved in the development of this white paper included: American Express; Cardtek US; Discover Financial Services; G+D Mobile Security; Gemalto; GlobalPlatform; Infineon Technologies; IQ Devices; Mastercard; Metropolitan Transportation Administration (MTA); Multos International; NXP Semiconductors; OT-Morpho.

Blockchain and Smart Card Technology

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. As a result, FinTech startups, financial institutions, and technology companies have invested in blockchain at an unprecedented rate—more than \$1 billion since 2009—and this investment is still accelerating dramatically. Blockchain has been dubbed by industry analysts the fastest development software market in history.

New blockchain applications are still emerging, and use beyond digital currencies is still being defined. Blockchain implementation for financial services applications is expected to be a significant area of growth. Financial institutions are expected to spend more than \$1 billion in 2017 on blockchain applications and increasing numbers of large banks around the world are experimenting with blockchains and bitcoins. Financial services expected to use blockchain are real-time settlement; money transfer; and smart contracts.

BLOCKCHAIN DEFINED

A blockchain is a distributed database that maintains a dynamic list of records, secured against tampering and revision. 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.

The white paper, *Blockchain and Smart Card Technology*, published in March 2017, provides a primer on blockchain technology, including the role of smart card and secure element technology in blockchain applications, and discusses:

- Use cases for several blockchain technology applications (cryptocurrencies, vaults, interbank funds transfer, asset registry, anticounterfeiting and IoT), including considerations, challenges and real-world pilots or commercial implementations
- Challenges that need to be addressed for blockchain implementations, including permissioned vs. permissionless blockchains, scalability, standards, reputation and consumer perception, security and legal and regulatory considerations

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.

APPLICATION BENEFITS

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 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)

Blockchain use cases for vaults, funds transfer, asset tracking, asset registry and the Internet of Things (IoT) would benefit from using smart card and secure element technology for convenient key generation, access and management.

It's anticipated that a diverse set of applications will be implemented using blockchain – everything from cryptocurrencies to funds transfers, asset registries and autonomous Internet of Things (IoT) device payment. With all of these implementations, proper management of cryptographic keys is critical; if those private keys are lost or stolen, any assets associated with the blockchain are lost forever. Secure element and smart card technology can play a critical role in securing blockchain transactions to generate, secure and manage these secret keys.

ABOUT THIS WHITE PAPER

The Secure Technology Alliance Payments Council developed this white paper to provide a primer on blockchain technology, discuss use cases that are currently commercially available or being piloted, and discuss the role secure element/smart card technology plays in the different use cases.

Participants involved in the development of this white paper included: Capgemini; CH2M; Consult Hyperion; CPI Card Group; Discover Financial Services; First Data; FIS; Fiserv; Gemalto; Infineon Technologies; Ingenico; Kona I; NextgenID Inc.; NXP Semiconductors; Oberthur Technologies; PayGility Advisors; Quadagno & Associates; Rambus; SHAZAM; Underwriters Laboratories (UL); Verifone; Visa Inc.



TRANSPORTATION COUNCIL

MISSION: Promote the adoption of interoperable contactless smart card and other secure device payment systems for transit and other transportation services and accelerate the deployment of standards-based smart card and secure device payment programs within the transportation industry

OFFICERS

- Chair: Gerald Kane, SEPTA
- Vice Chair - Transit: Katina Morch-Pierre, DART
- Vice Chair - Parking: Michael Hughes, Vantiv
- Vice Chair - Tolling: Carol Kuester, MTC and Bay Area Toll Authority (BATA)

STEERING COMMITTEE

- Ed Baldzicki, Conduent
- Francois Baylot, Thales
- Randy Cochran, NXP Semiconductors
- Michael Dinning, U.S. Department of Transportation/Volpe Center
- Jennifer Dogin, Mastercard
- Greg Garback, WMATA
- Jamie Geleynse, G+D Mobile Security
- Simon Laker, Consult Hyperion
- Kathy Imperatore, PATCO
- Rhonda Marx, American Express
- John McGee, LTK Engineering Services
- Eric Reese, Scheidt & Bachmann
- Craig Roberts, InComm
- Eric Schindewolf, Visa Inc.

TOP CONTRIBUTORS

- Mike Dinning, U.S. Dept. of Transportation/Volpe Center
- Carol Kuester, MTC and BATA
- Tina Morch-Pierre, DART
- David Weir, MTC

HONOR ROLL

- Stephen Abbanat, MTC
- Robert Anyumba, UL
- Charl Botes, Mastercard
- Marc Clevén, Visa Inc.
- Randy Cochran, NXP Semiconductors
- Mike Dinning, U.S. Dept. of Transportation/Volpe Center
- Jennifer Dogin, Mastercard
- Willy Dommen, Accenture
- Steven Grant, Aberdeen Management Group
- Michael Hughes, Vantiv
- Jerry Kane, SEPTA
- Carol Kuester, MTC and BATA
- Simon Laker, Consult Hyperion
- Tina Morch-Pierre, DART
- Peter Quadagno, Quadagno & Associates

- Craig Roberts, InComm
- Kirstyn Smith, UL
- Tyler Standage, Visa Inc.
- Brian Stein, CH2M
- David Weir, MTC

ACTIVITIES

- Council Steering Committee and officer elections (Dec. 2016)
- Smart Cities and Transportation Workshop in Salt Lake City, in collaboration with the IoT Security Council (Feb. 2017)
- [“Multimodal Payments Convergence -- Part One: Emerging Models and Use Cases”](#) white paper, in collaboration with the Association for Commuter Transportation (Mar. 2017)
- In-person meeting at Payments Summit (Mar. 2017)
- “EMV and Parking” panel at International Parking Institute (IPI) conference (May 2017)
- Multimodal payment convergence white paper – part 2, in collaboration with the Association for Commuter Transportation (in process)
- Guest collaboration with the U.S. Payments Forum Transit Contactless Open Payments Working Committee on development of a framework for a contactless EMV technical solution for transit (in process)
- Mobile ticketing and Near Field Communication (NFC) webinar (in process)
- Relationships with IPI and U.S. Payments Forum

TRANSPORTATION COUNCIL MEMBER ORGANIZATIONS

ABCorp • Accenture • ACI Worldwide • American Express • Benefit Resource Inc. • Cardtek US • CH2M • Chase Card Services • Conduent • Consult Hyperion • CPI Card Group • Cubic Transportation Systems, Inc. • Dallas Area Rapid Transit (DART) • Defense Manpower Data Center (DMDC) • Discover Financial Services • FIME • First Data • G+D Mobile Security • Gemalto • IDEMIA • InComm • Infineon Technologies • INIT Innovations in Transportation • Intelligent Parking Concepts LLC • Interac Association/Acxsys Corporation • Invoke Technologies • KICTeam • KONA I Co., Ltd. • Lenel • LTK Engineering Services • Mastercard • Metropolitan Transportation Authority (MTA) • Metropolitan Transportation Commission (MTC) • NXP Semiconductors • Port Authority of NY/NJ • Port Authority Transit Corporation (PATCO) • Quadagno & Associates • Rambus • San Francisco Bay Area Rapid Transit District (BART) • Scheidt & Bachmann • Smartrac N.V. • Southeastern Pennsylvania Transportation Authority (SEPTA) • STMicroelectronics • Thales • Tri County Metropolitan District of Oregon • U.S. Department of Homeland Security • U.S. Department of Transportation/Volpe Center • Underwriters Laboratories (UL) • Utah Transit Authority • Vantiv • Verifone • Visa Inc. • Vix Technology • Waltz, Inc. • Wells Fargo • XTec, Inc.

YEAR IN REVIEW: TRANSPORTATION COUNCIL CHAIR

Open Payments, Payments Convergence and Smart Cities Take Spotlight

This past year, the Transportation Council project initiatives focused on topics ranging from the convergence of payments, integration of mobile technologies, open payments and coordination with federal and state smart cities initiatives. I'll cover more details on these initiatives later in this letter, but let me first turn to a noteworthy [global payment survey](#) released in late 2016. This study focused attention on a long-standing challenge in the passenger transportation sector – the high level of cash transactions, specifically in public transportation. The survey findings are especially noteworthy in view of the considerable investment public transport operators have made in electronic fare systems that provide options to cash fare payments.

CASH IS STILL KING

Conducted by ACI Worldwide, Inc., the survey included 2,006 riders from the nine largest metropolitan transportation systems in the U.S. Surprisingly, the survey findings indicated the most popular payment method for mass transit is cash! When asked which payment method they preferred, a total of 51 percent preferred cash at a physical location, followed by credit/debit (31%) and mobile app (12%). Although the survey sample was small, the findings underscore the challenge agencies face in reducing cash transactions, which represent the highest collection cost in revenue operations.

The first Council project covering cash and other payment choices was a publication called “Multimodal Payments Convergence – Part One: Emerging Models and Use Cases.” Published in March, the white paper was the result of collaboration between Council members and the Association for Commuter Transportation. The first of a two-part series, the paper reviews evolving payments industry technology and payment media designed to increase travel and purchase convenience for travelers in cities and across regions. Through open design architectures that accept multiple forms of payment, riders may travel over different modes seamlessly and pay through a linked account. In addition, convergence involves a portal in which a mobile application allows both trip planning and payment; these converged solutions are coming to fruition in many parts of the U.S. and abroad. A second white paper being developed now, “Multimodal Payments Convergence—Part Two: Challenges and Opportunities for Implementation,” will focus on alternative visions for payment systems, identify potential barriers to implementation of multimodal payment strategies, and suggest ways of addressing these challenges.

OPEN PAYMENTS

Council members are actively involved in advancing open payments for U.S. transit systems and joined the U.S. Payments Forum's Transit Contactless Open Payments Working Committee. The Committee's first deliverable, “Technical Solution for Transit Contactless Open Payment Use Case1; Pay As You Go/Card,” was published in September this year. This paper both identifies requirements and provides guidance for technological solutions that could be used to implement contactless open payments. Transit seeks to deploy a retail payment experience in which a customer may use his or her own form factor at the transit entry point. The paper explores the technological approaches needed in the payments ecosystem for using contactless EMV chip cards for open payments in transit.

Over the past year, the Council has also worked on a project that looks at the feasibility of integrating separate but closely related technologies: mobile payments with NFC and mobile payments using QR and bar code technology. The project team has prepared content and material for a future webinar that compares the two technologies across key features, and then presents examples how their integration can assist transit agencies to create or enhance a mobile fare collection strategy.

Another initiative undertaken by the Council was a workshop in February that included transportation payments and the smart cities initiative. The session focused on the security of the Internet of Things (IoT) and IoT device security, and payments systems in smart cities, including a discussion on multimodal payments convergence and the accompanying issues and possible solutions.

Thanks to the Transportation Council co-chairs and members for their work and participation in the projects over the past year. Going forward, let's continue to identify the key issues and challenges facing transportation, payments and security and work toward developing appropriate solutions.



Gerald Kane
Senior Project Planner
New Payment Technologies
SEPTA

Multimodal Payments Convergence – Part One: Emerging Models and Use Cases



Transportation providers have adopted a variety of payment technologies, such as contactless smart cards, electronic tolling, and mobile payments for transit, parking, and shared use transportation, that make travel more convenient and efficient. In some regions, integrated payment systems let multiple transit agencies accept the same contactless smart card or mobile ticketing application. Toll agencies, such as members of the E-ZPass Interagency Group, have adopted common toll tag technologies and share payment data to allow the same toll tag to be used in multiple states.

Recently, several transit agencies have started to implement open, account-based payment systems that enable travelers to use many types of payment media or identification credentials to access transit services. Mobile ticketing and contactless payment using mobile devices have been implemented at many transit and parking agencies.

EXPANDED OPTIONS

In most urban areas, the mobility options from which travelers can choose are expanding. Services such as bike share, car share, and ride-hailing have grown rapidly. Travelers can get real-time information on available transportation options and make selections based on the current situation.

Integration of payment services for any type of transportation, or multimodal payments convergence, is a natural extension of these capabilities. The white paper, *Multimodal Payments Convergence – Part One: Emerging Models and Use Cases*, published in March

2017, describes four types of convergence that have been implemented; other types could emerge in the future.

The Secure Technology Alliance Transportation Council recognized the trend toward multimodal mobility at the 2014 Payments

Summit and initiated activities to explore the potential for multimodal payments convergence. In January 2015, the Transportation Council hosted a workshop on payments convergence that was attended by representatives from transit agencies and from tolling, parking, and intelligent transportation system and shared-use mobility associations. The workshop participants recommended continuing discussions about potential opportunities for multimodal payments convergence.

FOCUS ON PAYMENTS

Payments convergence was a featured topic at several transportation industry conferences during 2015 and 2016, generating substantial interest.

The shared use mobility industry (car share, bike share, ride-hailing) is particularly interested in payments convergence, and the Association for Commuter Transportation (ACT), whose members include many shared-use mobility providers, asked to be involved in the Secure Technology Alliance efforts.

The Secure Technology Alliance Transportation Council and the ACT collaborated to develop this white paper. Other industry groups, such as the Shared Use Mobility Center, also contributed. The white paper describes:

TECHNICAL ISSUES MUST BE ADDRESSED TO SUPPORT INTEGRATION OF MOBILE APPS FOR DIFFERENT TYPES OF SERVICES, SUCH AS CAR SHARE AND BIKE SHARE. PROCESSES MUST BE DEVELOPED FOR HANDLING PAYMENTS AND ACCOUNTS INVOLVING MULTIPLE TRANSPORTATION PROVIDERS.

- Emerging models of payments convergence, including use of a common payment technology, linked or integrated mobile apps, common or linked payment accounts and incentives or co-marketing
- Profiles of current regional examples of convergence, including initiatives in Chicago, Dallas, London, Los Angeles, Portland, Raleigh, Sacramento, Saint Petersburg, San Francisco Bay Area, Toronto and Washington, DC
- Roles and responsibilities of industry stakeholders involved in multimodal payment initiatives

While much progress has been made in payment integration, many challenges must be addressed to advance multimodal payments convergence. Technical issues must be addressed to support integration of mobile apps for different types of services, such as car share and bike share. Processes must be developed for handling payments and accounts involving multiple transportation providers. Institutional and governance issues must be addressed to determine how payment data will be shared among transportation providers, how new technology should be acquired and introduced, and how transportation incentives will be coordinated. While all transportation providers want to improve customer convenience, the business case and risks must be evaluated for specific payments convergence strategies on a case-by-case basis. The

principles of equity and accessibility cannot be overlooked in the drive toward technological innovation.

These issues and their potential solutions will be discussed in Part Two of this white paper, *Multimodal Payments Convergence: Challenges and Opportunities for Implementation*, which is a current Transportation Council project.

ABOUT THE WHITE PAPER

This white paper was developed by the Secure Technology Alliance Transportation Council, in collaboration with the Association for Commuter Transportation, to explore the rapidly evolving convergence of multimodal payments.

Secure Technology Alliance members involved in the development of the white paper included: Accenture; American Express; CH2M; Dallas Area Rapid Transit (DART); Discover Financial Services; Gemalto; Giesecke & Devrient; Incomm; INIT Innovations in Transportation; Kona I; LTK Engineering Services; NXP Semiconductors; Mastercard; Metropolitan Transportation Commission (MTC); Oberthur Technologies; Port Authority Transit Corporation; Southeastern Pennsylvania Transportation Authority (SEPTA); Thales Group; U.S. Department of Transportation/Volpe Center; Vantiv; Waltz, Inc.

payments @ the speed of life®

Think it. Do it.
Money movement – safely,
securely – at the point of thought.

fiserv.com/EMV

fiserv.



New Membership Levels Offered Participation in Forum and Alliance Activities

LOOKING AHEAD, FORUM PLANS TO PRIORITIZE MOBILE AND CONTACTLESS PAYMENT GUIDANCE FOR ISSUERS AND MERCHANTS

The U.S. Payments Forum (the "Forum") is a cross-industry body focused on supporting the introduction and implementation of new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the U.S. The Forum is the only non-profit organization whose membership includes the whole payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry.

Forum membership includes global payments networks, financial institutions, merchants, processors, acquirers, domestic debit networks, industry associations and industry suppliers.

The Forum resulted from the expansion of the charter and activities of the EMV Migration Forum, which was formed by the Secure Technology Alliance (formerly the Smart Card Alliance) in 2012 to support the industry cooperation and alignment of the move from magnetic stripe technology to more secure EMV contact and contactless technology. The transition of the organization to the U.S. Payment Forum took place in August 2016.

FORUM AND ALLIANCE

Last year, the Forum and the Secure Technology Alliance added new membership levels that offered the most advantages for companies who wanted equal standing and benefits in both organizations. The Prin-

cipal Plus and Leadership Council PLUS membership proved to be a popular level for those companies desiring full participation on both the Forum and the Alliance.

2016-2017 U.S. Payments Forum Officers and Steering Committee

OFFICERS

- Kristy Cook, Target (Chair)
- Jesse Lee, Wells Fargo (Vice Chair)
- Karen Czack, American Express (Secretary)
- Sarah Hartman, TSYS (Treasurer)

STEERING COMMITTEE

- Steve Cole, Vantiv
- Kristy Cook, Target
- Karen Czack, American Express
- John Drechny, Walmart
- Allen Freidman, Ingenico
- Melanie Gluck, Mastercard
- Barry Hanen, Walgreens
- Scott Haney, Woodforest National Bank
- Kathy Hanna, Kroger
- Art Harper, PSCU
- Sarah Hartman, TSYS
- Linda Horwath, JCB
- Simon Hurry, Visa Inc.
- Jesse Lee, Wells Fargo
- Oliver Manahan, Infineon Technologies
- Manish Nathwani, SHAZAM
- Jesse Pamperin, McDonald's
- Nick Pisarev, G+D Mobile Security
- Tom Pouliot, China Unionpay USA
- JC Raynon, PayPal
- Ellie Smith, Discover Financial Services
- Jamie Topolski, Fiserv
- Bob Woodbury, FIS/NYCE

DIRECTOR'S LETTER: A MESSAGE FROM RANDY VANDERHOOF

U.S. Payments Forum – Looking Beyond EMV

The U.S. Payments Forum celebrated its fifth anniversary at its Chicago meeting this past September. The organization was founded in August 2012 as the EMV Migration Forum and, even after five years, there was still plenty of discussion of the issues that remain with the complex U.S. migration to EMV. More importantly, members have expanded the discussions to strategize about the relevant topics payment industry leaders are focused on today, namely the rising volume of fraud in the fast growing online ecommerce channel, the new faster EMV solutions, mobile and contactless payments, and the transit requirements for implementing open loop payments.

TRANSFORMATION, EMV-STYLE

It is impossible to look ahead to new ecommerce fraud management solutions and consumer payments technologies on the horizon without considering where the U.S. payments marketplace would be without the transformation that took place over the last few years. That transformation was largely driven by EMV chip technology. Now that there are nearly 800 million EMV cards issued, more than 50 percent of transactions are made with a chip card at a chip-enabled retailer, and counterfeit fraud is declining, the EMV discussions in the Forum have shifted to understanding how to make chip transactions faster and more efficient, and resolving issues that lead to lingering pockets of EMV delays for retail petroleum merchants, the hospital-ity industry, and restaurants.

Today, many retailers are more focused on protecting online ecommerce channels and understanding how contactless and tokenization are making their way into consumer payments. To support these initiatives, the Forum is placing added emphasis on coming 3-D Secure 2.0 online security standards, has established two new member work groups – the Mobile and Contactless Payments Working Committee and the Transit Contactless Open Payments Working Committee, and has formed a new mobile special interest group (SIG).

Many card issuers are coming close to their first chip card reissuance cycle and should be aware of the new considerations and changes in the environment since their first issuance cycle. Key reissuance considerations include product choices (cards and services), product lifecycle management, dual-interface cards, certification, instant issuance impact and Faster EMV. The U.S. Payments Forum will be working through these considerations at upcoming meetings in 2018 and helping to inform card issuers who attend these in-person meetings.

COMMITMENT, COOPERATION EQUAL SUCCESS

The remarkable progress we've seen across the U.S. payments ecosystem to date is a direct result of the commitment and cooperation that has been present in the U. S. Payments Forum from the entire payments industry. It is appropriate that the Forum continue to facilitate the sharing of critical information among payments industry leaders, and host educational workshops and discussion groups on the implementation of other payments innovations. These innovations are going to leverage the new upgraded networks, payment devices, and point-of-sale systems in physical stores and also look at helping merchants and issuers solve the challenges of online ecommerce and omni-channel consumer shopping.

The U.S. Payments Forum continues to welcome new members who are the next generation of payments innovators, security specialists, and providers of mobile payments, tokenization, and card-not-present fraud and encryption solutions. Through the diverse mix of payments industry stakeholders who led the U.S. through its EMV transformation, Forum members are at the forefront of keeping the U.S. the most advanced payments market in the world.

It's been an exciting year. Thank you for being part of it.

THE REMARKABLE PROGRESS WE'VE SEEN ACROSS THE U.S. PAYMENTS ECOSYSTEM TO DATE IS A DIRECT RESULT OF THE COMMITMENT AND COOPERATION THAT HAS BEEN PRESENT IN THE U. S. PAYMENTS FORUM FROM THE ENTIRE PAYMENTS INDUSTRY.



Randy Vanderhoof
Director,
U.S. Payments Forum

U.S. PAYMENTS FORUM RESOURCES

The U.S. Payments Forum had an active year, developing business and technical resources to assist with EMV migration and emerging payments technology implementation, and continuing outreach and education initiatives for issuers, merchants and ATM owners and operators. All published resources are available on the U.S. Payments Forum and EMV Connection web sites.

BUSINESS AND TECHNICAL RESOURCES

- [“Card-Not-Present \(CNP\) Fraud around the World”](#) white paper, reviewing the status of CNP fraud in countries that have migrated or are in the process of migrating to EMV
- [“Data Quality for Security: Circumvention Attacks”](#) white paper, discussing various attacks intended to circumvent the use of chip technology and mitigation approaches (Forum members only)
- [“EMV Receipt Best Practices”](#) white paper, reviewing recommendations and requirements for data elements found on receipts for chip-on-chip transactions
- [“EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community”](#) white paper update, adding information on contactless testing and certification
- [“Implementing EMV in the U.S.: How the U.S. Common Debit AIDs Facilitate Debit Transaction Routing and Ensure Durbin Compliance”](#) video recording update, discussing cardholder verification method choices
- [“Managing Card-Based Tip and Gratuity Payments for EMV Chip”](#) update, adding additional scenarios
- [“Mobile and Contactless Payments Glossary,”](#) defining mobile and contactless payments terms to encourage cross-industry standardization of terminology
- [“Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud”](#) white paper update, adding 3D-Secure comparison and CNP definition appendices
- [“Optimizing Transaction Speed at the POS”](#) update, adding Q&A appendix
- [“Petroleum Industry: EMV FAQ,”](#) answering frequently asked questions about EMV chip implementation for petroleum retailers
- [“Technical Solution for Transit Contactless Open Payments Use Case 1: Pay As You Go/Card”](#) white paper, providing technical solution guidance for implementing transit contactless open payments use cases with contactless EMV cards
- [“Testing & Certification Terminology”](#) glossary, providing a resource to assist merchants in completing the acquirer testing and certification forms used for EMV certification
- [“The 101 on Transit Contactless Open Payments”](#) presentation, providing an educational resource on what are “transit open payments” and how EMV contactless open loop payments may work in the U.S. and Canadian transit environment (Forum members only)
- [“Troubleshooting Data Quality Issues”](#) white paper, providing a guide for troubleshooting common data quality issues that have been seen by the networks, acquirers, merchants and issuers (Forum members only)
- [“Understanding the U.S. EMV Fraud Liability Shifts”](#) white paper update, providing information on payment network liability shifts for retail point of sale, automated fuel dispenser and ATM transactions

EDUCATIONAL WEBINARS AND WORKSHOPS

- [“Accepting EMV Chip Payments at the Fuel Pump”](#) Webinar, providing an overview of EMV chip technology and key considerations for petroleum merchants migrating to EMV
- “EMV Contactless Testing and Certification for VARs/ISVs” workshops, providing educational sessions on payment network processes for testing and certifying EMV contactless payment implementations
- [“Implementing EMV at the ATM”](#) workshop at ATMIA annual conference, providing guidance on EMV migration for ATM owners and operators

STATE OF THE MARKET

In October 2017, the Forum produced its quarterly market snapshot, which can be found on the U.S. Payments Forum website. Among the highlights and news:

- 96 percent of the top 200 merchants now accept chip payments
- ATM enablement is growing rapidly, with the ATM Industry Association (ATMIA) estimating that 80 percent of ATMs will be chip-enabled by the end of 2017
- Small and medium-sized businesses (SMBs) have seen an impressive jump in enablement, with reports that between 70 and 80 percent of SMBs are now chip-enabled
- Chargeback limit policies from American Express and Visa Inc. expire in April 2018; these policies gave merchants who need extra time to become chip-enabled financial relief from chargebacks under \$25

U.S. PAYMENTS FORUM WORKING COMMITTEES

The U.S. Payments Forum has had seven working committees and three special interest groups active in 2017 focused on different topics relevant to EMV migration and emerging payments technologies. The working committee topics and activities are chosen by Forum members based on critical issues discussed in the Forum meetings. Forum members can join any working committee and lead or participate in committee projects. Projects are defined by the committee members to focus on the critical issues or challenges that impact implementation of EMV and other emerging payments technologies in the U.S. Working committees meet at U.S. Payments Forum in-person meetings and in regular teleconferences.



ATM WORKING COMMITTEE

The ATM Working Committee goal is to explore the challenges of EMV migration for the U.S. ATM industry, work to identify possible solutions to challenges, and facilitate the sharing of best practices with the various industry constituents, with the goal result being more positive EMV migration experience for consumers. The Working Committee provides input, solutions, and expertise that are specific to the needs of the ATM channel to other Forum working committees.

- Working Committee co-chairs: Marcelo Castro, Diebold; Craig Demetres, Chase; Brenda Pino, BMO Harris Bank N.A.



CARD-NOT-PRESENT FRAUD WORKING COMMITTEE

The Card-Not-Present Fraud Working Committee goal is to create a comprehensive best practices strategy to mitigate card-not-present fraud in the new EMV chip card environment, using a balanced approach considering all key stakeholders – issuers, consumers, merchants, acquirers, networks and third parties. Working Committee projects included reviewing and assembling lessons learned from other country migrations, benchmarking potential tools used to address fraud, monitoring fraud levels, collaborating with other organizations to understand fraud costs, and providing best practices for online fraud management.

- Working Committee co-chairs: Ben Dominguez, Visa Inc.; Malcolm Nunes, Fiserv



COMMUNICATION AND EDUCATION WORKING COMMITTEE

The Communication and Education Working Committee goal is to deliver communications best practices and educational resources for key payments industry stakeholders that promote an efficient, timely and effective implementation of EMV-enabled cards and payment credentials, devices and terminals and emerging payments technologies in the United States.

- Working Committee co-chairs: Lori Breitzke, E&S Consulting; Mansour Karimzadeh, SCIL EMV Academy; Cynthia Knowles, FIS



MOBILE AND CONTACTLESS PAYMENTS WORKING COMMITTEE

The Mobile and Contactless Payments Working Committee goal is for all interested parties to work collaboratively to explore the opportunities and challenges associated with implementation of mobile and contactless payments in the U.S. market, identify possible solutions to challenges, and facilitate the sharing of best practices with all industry stakeholders.

- Working Committee co-chairs: Deborah Baxley, PayGility Advisors; Bradford Loewy, Dover Fueling Solutions; Nick Pisarev, G+D Mobile Security



PETROLEUM WORKING COMMITTEE

The Petroleum Working Committee is for all interested parties to work collaboratively to identify, review and resolve challenges associated with implementation of EMV within the U.S. petroleum and convenience market. The Petroleum Working Committee includes payment networks, petroleum and convenience merchants, petroleum-specific acquirers, petroleum and convenience POS vendors and fuel dispenser manufacturers, and other organizations servicing the petroleum and convenience category.

- Working Committee co-chairs: Kara Gunderson, CITGO Petroleum Corporation; Tomas Levy, Gilbarco; Terry Mahoney, W. Capra Consulting Group

A LOOK INTO THE FUTURE

Looking forward, the U.S. Payments Forum is prioritizing mobile and contactless payment implementation guidance for issuers and merchants. The Forum also plans to focus attention on implementation of new specifications including 3D Secure 2.0 and other solutions for secure online payments.



TESTING AND CERTIFICATION WORKING COMMITTEE

The Testing and Certification Working Committee goal is to discuss the challenges with EMV certification and define approaches for achieving certification to meet the payment brand milestones for fraud liability shift. Areas for focus include: education on the testing and certification that is required for different industry stakeholders; evaluation of current processes to define approaches for streamlining testing and certification.

- Working Committee chair: Cindy Kohler, Visa Inc.



TRANSIT CONTACTLESS OPEN PAYMENTS WORKING COMMITTEE

The Transit Contactless Open Payments Working Committee was formed in March 2017. The Working Committee goal is for interested stakeholders to work collaboratively to identify possible solutions that address the challenges associated with the implementation of contactless acceptance devices at customer points of entry (POE) within the unique retail environment of the U.S. public transit market. This includes acceptance of all open loop

payment devices (e.g., cards, mobile, wearables) and all payment methods (e.g., credit, debit, prepaid, gift).

- Working Committee co-chairs: Jennifer Dogin, Mastercard; Joshua Martiesian, Metropolitan Transportation Authority; Nick Pisarev, G+D Mobile Security

SPECIAL INTEREST GROUPS

The U.S. Payments Forum has three special interest groups (SIGs), one for merchants, one for issuers and one focused on mobile topics.

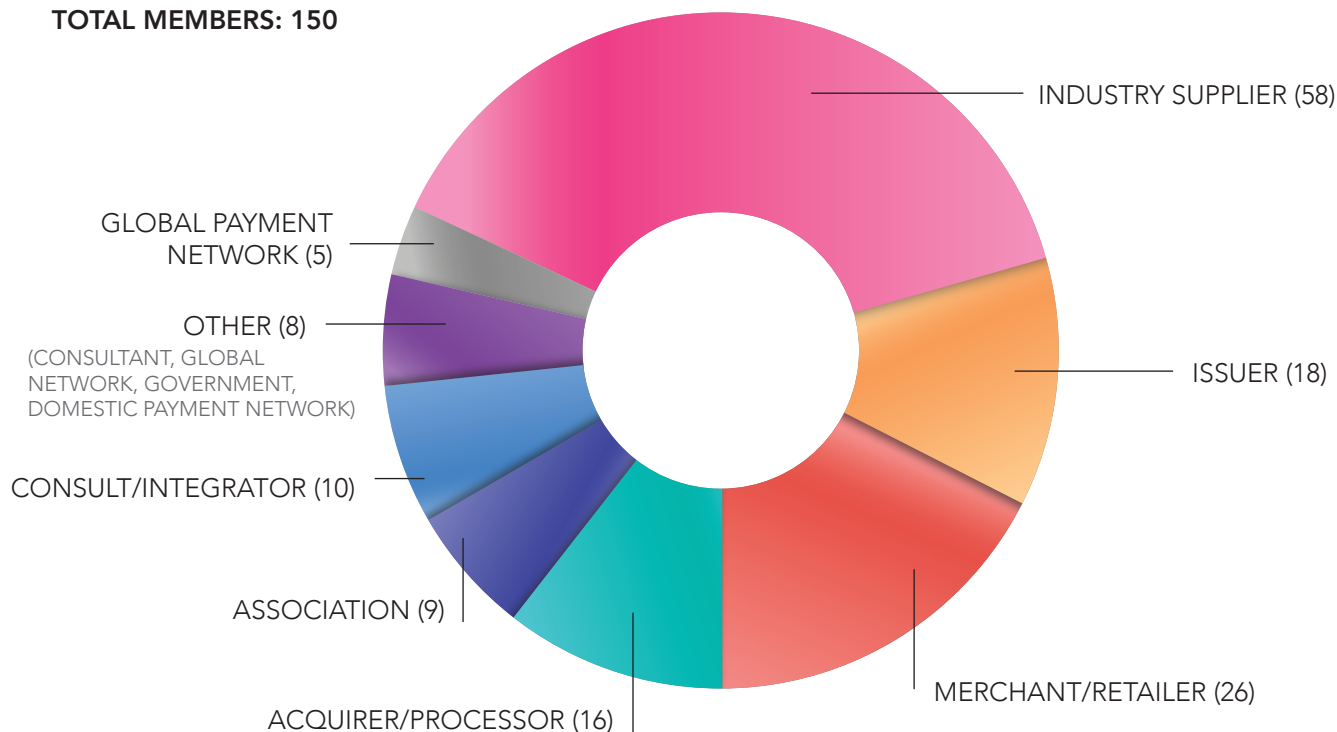
- SIG leads: Kristy Cook, Target (merchant); Jesse Lee, Wells Fargo (issuer); Deborah Baxley, PayGility Advisors (mobile)

SPECIAL TOPIC GROUPS

At each U.S. Payments Forum meeting, “birds-of-a-feather” sessions are held to discuss topics of interest to specific groups. 2017 meetings have included sessions focused on transaction data quality, contactless payments challenges, Faster EMV, and EMV implementation for hospitality merchants and unattended locations.

U.S. PAYMENTS FORUM MEMBERSHIP MIX

TOTAL MEMBERS: 150



U.S. PAYMENTS FORUM MEMBERS

- ABCorp NA Inc.
- ACI Worldwide
- Acquirer Systems
- Ahold Delhaize
- ALDI
- Alliance Data
- American Express
- Apple, Inc.
- Argotectno
- Arroweye Solutions, Inc.
- ATM Industry Association
- ATMequipment.com
- B2 Payment Solutions Inc.
- Bank of America
- Bank of the West
- Barnes International Limited
- Best Buy Co. Inc.
- BMO Harris Bank N.A.
- BP Products NA
- Capital One
- CardConnect
- Cardtek USA
- CETECOM INC.
- Chevron
- China UnionPay USA
- CHS Inc.
- CITGO Petroleum Corporation
- City National Bank
- Clear2Pay
- CMS Payments Intelligence
- COMPRION GmbH
- Conduent
- Conexus, Inc.
- Connie Driscoll Associates
- CPI Card Group
- Credit Union 24 Network
- CreditCall Corporation
- Cryptomathic Inc.
- Cubic Transportation Systems, Inc.
- Debit Network Alliance
- Deltec Consulting, Inc.
- Diebold Incorporated
- Discover Financial Services
- Dover Fueling Solutions
- E&S Consulting LLC
- EchoSat Communications Group
- Elan Financial Services
- Elavon, Inc.
- Electronic Trade Solutions Ltd
- Electronic Transaction Association
- Entrust Datacard
- ePayResources
- Equinox Payments
- Euro Tech Sales LLC
- ExxonMobil
- Federal Reserve Bank of Atlanta - Retail Payments Risk Forum
- Federal Reserve Bank of Boston
- Federal Reserve Bank of Minneapolis
- Fifth Third Bank
- FIME
- First American Payment Systems
- First Data
- First National Bank of Omaha
- FIS
- Fiserv
- G+D Mobile Security
- Gemalto
- Gilbarco
- Heartland Payment Systems
- ICC Solutions Limited
- ID TECH, INC.
- IDEMIA
- Infineon Technologies
- Ingenico Inc.
- Intelligent Parking Concepts LLC
- Interac Association
- Jack Henry Processing Solutions
- JCB International Credit Card Company
- JPMorgan Chase
- KONA I co. Ltd.
- Linxens Holding SAS
- Lou Seitchik
- Lowe's
- Magellan Consulting Inc.
- Magicard
- MasterCard Worldwide
- McDonald's
- Merchant e-Solutions
- Merchant Link, LLC
- Metropolitan Transportation Authority
- Morpho N.A. Inc. – now IDEMIA
- Multos International Pte. LTD
- NXP Semiconductors
- On-Line Strategies Services, LLC
- Paragon Application Systems
- PAX Technology Inc.
- PayGility Advisors
- PayPal, Inc.
- PCI Security Standards Council, LLC
- Perfect Plastic Printing
- Phillips 66 Company
- PNC Bank
- Poynt Co.
- PSCU
- Publix Super Markets Inc.
- Q-Card Company/Brush Industries
- Rambus
- Reef Karson Consulting, LLC
- Safeway Inc.
- Savage Consulting Group
- SCIL EMV Academy, Inc.
- Sears Holdings Corporation
- SHAZAM
- Shubert Ticketing
- SPS
- Sterling Payment Technologies
- STMicroelectronics
- SunTrust
- SWIFT
- Target Corporation
- TD Bank NA
- Tesoro Refining and Marketing Company, LLC
- Thales E-Security Inc.
- The Home Depot
- The Kroger Co.
- The Members Group
- The National ATM Council, Inc.
- Toppan Printing Company, Ltd.
- Toshiba Global Commerce Solutions, Inc.
- Toshiba Infrastructure Systems & Solutions Corporation
- Trader Joe's Company
- Tritan Systems of Delaware, LLC
- TSYS
- UBIVELOX Inc.
- UBS Bank USA
- Underwriters Laboratories (UL)
- Utimaco Inc.
- Valid USA
- Vantiv
- VeriFone, Inc.
- Visa Inc.
- W. Capra Consulting Group
- Wakefern Food Corp
- Walgreen Co.
- Walmart
- Wells Fargo
- WEX Inc.
- WISEKEY
- Woodforest National Bank
- WorldPay US

As of September 30, 2017



LATIN AMERICA CHAPTER

MISSION: Stimulate the use, understanding, interoperability, convergence, evolution, and widespread use of innovative applications of emerging digital technologies, including smart cards, devices with integrated circuits and related components in the region.

SCALA Overview

SCALA is the Latin American and Caribbean chapter of the Secure Technology Alliance. Its projects include the development of industry best practices, technical documents, and specifications, educational programs, market research, advocacy, a Digital Center of Excellence, open forums and relationships with industries impacted by related technologies. SCALA keeps its members and partners connected to industry leaders in all its sectors. SCALA is proud to be a leader on promoting the impact and value of smart cards and related technologies in Latin America and the Caribbean.

Events and Industry Participation

SCALA held this year's edition of the Digital Tour Americas-2017 in Quito, Ecuador. The event brought together more than 120 participants from Ecuador's payment and financial sectors, who heard topics including the future of payments, solutions in a digital era, mobile payments, biometrics in payments, and security. One of the highlights of the event was the presence and use of wearables, allowing participants access to the conferences, as well as testing the device making payments. The event's agenda included different topics such as: the future in payments, solutions in the digital era, mobile payments, biometrics in payments, biometrics security, among others.

SCALA also participated in a number of industry events, including

- Clarciev
- Cumbre Gerencial ALAS
- eID Conference Americas
- II Information Security and Fraud Prevention Summit
- II International Financial Summit



The Digital Center of Excellence

The Digital Center of Excellence (CED)

The Digital Center of Excellence (CED) is a training center for the development of industry professionals and market leaders on emerging digital technologies. In 2017, the CED welcomed 10 university students, each of whom received training in new tools relating to emerging technologies and education/information on the impact in a digital society. The students had the opportunity to experience both theoretical and practical training to reduce the risk of the implementations of digital secure technologies through education, best practices, and the expansion of innovation. The students came from Florida State University, InterAmerican University, Universidad del Istmo, University of Panama, Technological University, and Juntos Podemos.

Areas of Leadership:

Access Control, Biometrics in Mobile, Biometric Payments, Contactless Payments, Derived Identity, Digital Currency, Financial Inclusion, Frictionless Payments, Identity of Devices, Identity Payments, Mobile ID, Open Payments, Public Key Infrastructure – Blockchain, PKI, Tokenization, 3D Secure 2.0, Reciprocal Recognition of Identity, E-Gov, E-Passport, Healthcare, Multi-application, and Related Applications

SCALA Councils

PAYMENTS COUNCIL

The SCALA Payments Council focuses on facilitating the adoption and convergence of chip-enabled payments systems and related applications in Latin America and the Caribbean. The Council brings together industry stakeholders, payment leaders, and suppliers. The Council works to reduce the barriers to adopt emerging digital technologies in projects related to EMV, open payments, contactless payments, mobile payments, e-commerce and other payments projects. The Council's goal is to promote the value of chip-enabled payments and related components to the market to improve the security and quality of service.

Council Projects

The Council works on projects to provide educational resources for innovation in and convergence of smart-card-related implementation for financial inclusion, transportation, and payments. The Payments Council has played a key role in the development of the Open Payment Initiative in Transportation in the region. The focus of this project is the evolution of payments in transportation as the transportation industry moves toward a system that accepts dual-interface EMV-compliant cards such as prepaid, debit and credit cards, as well as using these initiatives to promote financial inclusion of marginalized populations.

IDENTITY COUNCIL

SCALA's Identity Council focuses on promoting adequate policies and best practices concerning the implementation secure interoperable identity credentials and related applications within the Latin American and Caribbean regions. The Council addresses the challenges of secure identity by developing guidelines for organizations, so that they can realize the benefits that secure identity delivers. The Council's members share their experiences in a non-partisan manner with industry leaders, organizations, government agencies, countries' authorities, and international bodies, in order to find solutions to the problems faced and to seek the development of collaboration

among the sectors and countries impacted by identity.

Council Projects Specification

The Council has helped to develop an open specification to facilitate the reciprocal recognition of national identity documents, moving toward a system that allows different countries to electronically validate the identity credential information of another. The specification also considers the interoperability of multiple applications in a single credential, allowing validation of the authenticity of the credential and traceability of the validation to guarantee the compliance of basic human rights.

The Council works on projects to raise awareness of the issues that organizations and the public face in implementing and using identity systems.

BIOMETRIC PAYMENTS COUNCIL

The Biometric Payments Council focuses on promoting adequate policies and best practices concerning the implementation of biometrics in the payment ecosystem, and authentication mechanisms to access financial services and/or conduct transactions. The Council addresses the use of this innovative technology by examining the variety of infrastructure models, deployment options, modalities, human dynamics, and regulatory considerations that can generate significant challenges in establishing interoperability, common methodologies, and compatibility across industries and use cases.

The Council helps define the overall scope of use of biometrics authentication systems for payments and develops frameworks of collaboration among the different interested parties. This technology may also create additional opportunities for vendors, technology providers, and end users to cross-authenticate users utilizing different biometric authentication systems securely to access products or services.



SCALA MEMBERS

- ABnote
- APOLOLAB
- Arjo Systems
- Banco Central de Costa Rica
- Banrisul S.A.
- Discover Financial Services
- Entrust Datacard
- Gemalto Mexico SA DE CV
- Giesecke y Devrient de Mexico
- Global Enterprise Technologies Corp (GET Group)
- HID Global
- IDEMIA
- Instituto Nacional De Tecnologia Da Informacao - ITI
- Inter American Development Bank
- Linxens Holding SAS
- MasterCard Worldwide
- PPG TESLINÁ® Substrate Products
- Redeban Multicolor S.A.
- Registro Publico de Panama
- Servired, S.A.
- Ultra Electronics Card Systems
- Visa Inc.

As of September 30, 2017

To learn more about SCALA, visit www.sca-la.org.

SECURE TECHNOLOGY ALLIANCE MEMBER DIRECTORY

A LA CARD Marketing and Consulting
Services Limited
112 Crawford Rose Drive
Aurora, ON L4G 4R9 Canada
www.alacard.com

ABnote North America
225 Rivermoor Street
Boston, MA 02132
www.abnote.com

LEADERSHIP COUNCIL



Accenture
161 North Clark
Chicago, IL 60601
312-693-0161
www.accenture.com

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations.

ACI Worldwide
6060 Coventry Drive
Elkhorn, NE 68022
www.aciworldwide.com

ACT Canada
85 Mullen Drive
Ajax, ON L1T 2B3 Canada
www.actcda.com

Advanced Card Systems, Ltd.
Units 2010-2013, 20th floor
Chavalier Commercial Centre
8 Wang Hoi Road
Kowloon Bay, Hong Kong
www.asc.com.hk

Allegion
11819 N. Pennsylvania Street
Carmel, IN 46032
www.allegion.com

AMAG Technology, Inc.
20701 Manhattan Place
Torrance, CA 90501
www.amag.com

LEADERSHIP COUNCIL



American Express
200 Vesey Street
New York City, NY 10285
212-640-9982
www.americanexpress.com

American Express is a global services company, providing customers with access to products, insights and experiences that enrich lives and build business success. Learn more at americanexpress.com.

Argotechno
201 S. Biscayne Blvd., Suite 1200
Miami, FL 33131
www.argotechno.com

Benefit Resource, Inc.
245 Kenneth Drive
Rochester, NY 14623
www.benefitresource.com

Burden Consulting, Ltd.
3000 Cathedral Hill
Guildford
United Kingdom GU2 7YB

Cardtek USA
17901 Von Karman, Suite 600
Irvine, CA 92614
www.cardtek.com

CertiPath Inc.
11921 Freedom Drive, Suite 710
Reston, VA 20190
www.certipath.com

LEADERSHIP COUNCIL



CH2M
CH2M World Headquarters
9191 South Jamaica Street
Englewood, CO 80112
888-CH2M-HILL (888-242-6445)
www.ch2mhill.com/transit

CH2M is an industry leader in assisting transit and rail clients with the design, procurement, and implementation of electronic fare payment systems. CH2M's electronic payments group has performed a wide variety of fare system assignments for large, medium, and small transit and rail operators. Our staff has developed innovative fare solutions for transit and rail operators that optimize their objectives and meet passenger needs. Our professionals are experts in the analysis and development of fare systems, including project management, fare policy, pricing, structure and fare system design, testing, installation, and procurement management.

Chase Card Services
301 North Walnut Street
Floor 15
Wilmington, DE 19801
www.chase.com

Chenega Management, LLC
14295 Park Meadow Drive
Suite 400
Chantilly, VA 20151
www.chenegaiss.com

Chicago Transit Authority
567 West Lake Street
Chicago, IL 60661
www.transitchicago.com

LEADERSHIP COUNCIL



NEW IN
'17

China UnionPay USA
3 Second Street
Plaza Ten, Suite 208
Jersey City, NJ 07311
www.unionpayintl.com

LEADERSHIP COUNCIL



Leading the Way in Access Control

Datawatch Systems, Inc.

4401 East West Highway, Suite 500
Bethesda, MD 20814
301-654-3282
www.datawatchsystems.com

Datawatch is a complete managed security solutions provider for commercial office buildings, securing and monitoring assets and resources in more than 2,500 buildings domestically and globally.

LEADERSHIP COUNCIL & SPONSOR



Discover Financial Services

2500 Lake Cook Road
Riverwoods, IL 60015
224-405-0900
www.discovernetwork.com

Discover® issues the Discover card, offers student loans, personal loans, home equity loans and direct banking products and operates the Discover Global Network.

Clear2Pay
4110 N. Scottsdale Road, Suite 310
Scottsdale, AZ 85251
www.clear2pay.com

Defense Manpower Data Center
4800 Mark Center Drive, Suite 04E25-01
Alexandria, VA 22350
www.dmdc.osd.mil

E4 Security Consulting LLC
8902 Octavia Avenue
Morton Grove, IL 60053
www.e4securityconsulting.com

Conduent
3333 Coyote Hill Road
Palo Alto, CA 94304
www.conduent.com

Department of Homeland Security
245 Murray Lane SW
Mailstop 0123
Washington, DC 20528
www.dhs.gov

EFT Experts
8 Kimberly Court
Richmond Hill, ON L4E 4C6
Canada
www.eftexperts.com

Consult Hyperion
535 Madison Avenue
New York, NY 10022
www.chyp.com

Department of the Interior
12201 Sunrise Valley Drive
Room: 2P105B
Reston, VA 20192
www.doi.gov

Entrust Datacard
1187 Park Place
Shakopee, MN 55379
www.entrustdatacard.com

CPI Card Group
10368 West Centennial Road
Littleton, CO 80127
www.cpicardgroup.com

Exponent, Inc.
149 Commonwealth Drive
Menlo Park, CA 94025
www.exponent.com

Cubic Transportation Systems
5650 Kearny Mesa Road
San Diego, CA 92111
www.cubic.com/cts

FEITIAN Technologies Co., Ltd.
F/17 Tower B Huizhi Mansion
No. 9 Xueqing Road
Haidian, Beijing 100085
China
www.ftsafes.com

Dallas Area Rapid Transit (DART)
P.O. Box 660163
Dallas, TX 75266
www.dart.org

FIME
1080, Cote Du Beaver Hall
Suite 1400
Montreal QC H2Z 1S8 Canada
www.fime.com

LEADERSHIP COUNCIL

First Data®

First Data
5565 Glenridge Connector NE, Suite 2000
Atlanta, GA 30342
404-890-2000
www.firstdata.com

First Data is a global leader in commerce-enabling technology and solutions, serving approximately six million business locations and 4,000 financial institutions in more than 100 countries.

LEADERSHIP COUNCIL



FIS
11601 Roosevelt Blvd,
St. Petersburg, FL 33716
800-822-6758
www.fisglobal.com

FIS is the world's largest provider of financial institution core processing, card issuance, network, and transaction payment processing services to financial institutions, merchants and businesses worldwide.

SPONSOR



Fiserv, Inc.
1880 Park View Drive
Shoreview, MN 55126
800-872-7882 | 262-879-5322
getsolutions@fiserv.com
www.fiserv.com

Fiserv enables clients to achieve best-in-class results by driving quality and innovation in payments, processing services, risk and compliance, customer and channel management, and business insights and optimization.

LEADERSHIP COUNCIL & SPONSOR



G+D Mobile Security
45925 Horseshoe Drive
Dulles, VA 20166
703-480-2000
mobilesecurity-us@gi-de.com
www.gi-de.com

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

Gallagher Group Unlimited
5005 NW 41st
Riverside, MO 64150
855-846-1395
www.gallagher.com

LEADERSHIP COUNCIL



Gemalto
9442 N Capital of Texas Highway
Arboretum Plaza II, Suite 100
Austin, TX 78759
888-343-5773
www.gemalto.com

Gemalto is the world leader in digital security: protecting, verifying and managing digital identities and interactions. We enable our clients to offer personal mobile services, payment security, authenticated Cloud access, identity and privacy protection, eGovernment documents, biometrics, machine-to-machine applications and many other services.

General Services Administration
1800 F Street, NW
Washington, D.C. 20405
www.gsa.gov

Genfare
800 Arthur Avenue
Elk Grove Village, IL 60007
www.genfare.com

Glenbrook Partners
384 Provident Avenue
Winnetka, IL 60093
www.glenbrook.com

Global Enterprise Technologies Corp.
230 Third Avenue, 6th Floor
Waltham, MA 02451
www.getgroup.com

Hewlett-Packard Enterprise Services, LLC
11241 Suncrest Court
Baton Rouge, LA 70818
hp.com/gov/transformation

HID Global
15370 Barranca Parkway
Irvine, CA 92618
www.hidglobal.com

Hillsborough Transit Authority
1201 E. 7th Avenue
Tampa, FL 33605
www.gohart.org

ICMA
P.O. Box 727
Princeton Junction, NJ 08550
www.icma.com

LEADERSHIP COUNCIL & SPONSOR



IDEMIA
296 Concord Road, Suite 300
Billerica, MA 01821 USA
www.idemia.com

IDEMIA: the global leader in trusted identities for an increasingly digital world. We empower citizens and consumers to interact, pay, connect, travel and vote in a connected environment. By standing for Augmented Identity, we ensure privacy and guarantee secure, authenticated transactions for international Financial, Telecom, Identity, Security and IoT sectors.

Identification Technology Partners, Inc.
12208 Pueblo Road
Gaithersburg, MD 20878
www.idtp.com

Identiv
1900 Carnegie Avenue
Santa Ana, CA 92705
www.identiv.com

InComm
250 Williams Street, Suite M-100
Atlanta, GA 30303
www.incomm.com

LEADERSHIP COUNCIL & SPONSOR



Infineon Technologies
640 North McCarthy Boulevard
Milpitas, CA 95035
866-951-9519
www.infineon.com

Infineon provides security components for passports, identity cards and contactless payment cards. It is the leading supplier of chips for credit cards, access cards and trusted computing solutions worldwide.

LEADERSHIP COUNCIL



Ingenico, North America
3025 Windward Plaza, Suite 600
Alpharetta, GA 30005
678-456-1211
www.ingenico.us

Ingenico Group is the global leader in seamless payment, providing smart, trusted and secure solutions to empower commerce across all channels, online, in-store, unattended and mobile.

Init Innovations in Transportation
1420 Kristina Way, Suite 101
Chesapeake, VA 23320
www.initusa.com

Initiative for Open Authentication
398 S. San Vicente Ln.
Anaheim Hills, CA 92807
www.openauthentication.org

Integrated Security Technologies, Inc.
520 Herndon Parkway, Suite C
Herndon, VA 20170
www.istonline.com

Interac Association/Acxsys Corporation
Royal Bank Plaza, North Tower
200 Bay Street, Suite 2400, P.O. Box 45
Toronto, ON M5J 2J1 Canada
www.interac.ca

Intercede Limited
11951 Freedom Drive, 13th Floor
Reston, VA 20190
www.intercede.com

Invoke Technologies
13366 Caminito Mar Villa, Suite 100
Del Mar, CA 92014
www.invoketechnologies.com

IPS Group, Inc.
5601 Oberlin Drive
San Diego, 92121
www.ipsgroupinc.com

IQ Devices
Number 32
Carmel Valley, CA 93924
www.iqdevices.com

Jack Henry Processing Solutions
1100 Olive Way, Suite 320
Seattle, WA 98101
www.weknowpayments.com

LEADERSHIP COUNCIL



JCB International Credit Card Co., Ltd.
800 W. 6th Street, Suite 200
Los Angeles, CA 90017
262-269-6081
www.jcbusa.com

JCB is a major global payment brand aiming to provide the highest quality service worldwide as a travel and entertainment card.

KICTeam, Inc.
1130 Minot Avenue
PO Box 1120
Auburn, ME 04211
<http://kicteam.com/en/Index>

KONA I, Inc.
3003 North First Street, Suite 330
San Jose, CA 95134
408-519-5799
www.konai.com

LEADERSHIP COUNCIL



Leidos, Inc.
11951 Freedom Drive
Reston, VA 20190
571-526-6000
www.leidos.com

Leidos is a FORTUNE 500® company that solves problems in national security, energy and the environment, critical infrastructure, and health. For more information, visit leidos.com.

Lenel Systems International
1212 Pittsford-Victor Road
Pittsford, NY 14534
www.lenel.com

Linxens Holdings SAS
6 Greenland Walk
Amersterdam Building 2-8
279227 Singapore
www.linxens.com

LTK Engineering Services
100 West Butler Avenue
Ambler, PA 19002
www.ltk.com

Malaysian Electronic Payment System
SDN BHD (MEPS)
MEPS@Horizon, Tower 5 Avenue 3,
Bangsar South 8 Jalan Kerinchi
Kuala Lumpur 59200 Malaysia
www.meps.com.my

Massachusetts Bay Transportation
Authority
10 Park Plaza, Rm 4730
Boston, MA 02116
www.mbtta.com

LEADERSHIP COUNCIL



Mastercard Worldwide
2000 Purchase Street
Purchase, NY 10577
914-249-2000
www.mastercard.com

Mastercard is a global payments and technology company, operating the world's fastest payments processing network and making everyday activities more secure and efficient for everyone.

Metropolitan Transportation Authority
2 Broadway, Room D27.83
New York, NY 10004
www.mta.info/nyct

Metropolitan Transportation Center
375 Beale Street, Suite 800
San Francisco, CA 94105
www.mtc.ca.gov

Moneris
150 N. Martingale Road, Suite 900
Schaumburg, IL 60173
www.moneris.com

Monitor Dynamics
6800 Alamo Downs Parkway
San Antonio, TX 78238
www.monitordynamics.com

Multos International PTE LTD
Level 14, The Zenith
Tower B, 821 Pacific Hwy
Chatswood NSW2067
Australia
www.multosinternational.com

National Institute of Standards and
Technology
100 Bureau Drive
Gaithersburg, MD 20899
www.nist.gov

NBS Technologies
703 Evans Avenue, Suite 400
Toronto, ON M9C 5E9 Canada
www.nbstech.com

NextgenID, Inc.
288 Christian Street
Oxford, CT 06478
www.nextgenid.com

NXP Semiconductors
411 East Plumeria Drive
San Jose, CA 95134
www.nxp.com

Nxt-ID, Inc.
288 Christian St
Oxford, CT 06478
www.nxt-id.com

Parsons Corporation
286 Locktown Road
Flemington, NJ 08822
www.parsons.com

Port Authority of NY/NJ
1 PATH Plaza, 10th floor
Jersey City, NJ 07306
www.panynj.gov

Port Authority Transit Corporation
P.O. Box 4262
Lindenwold, NJ 08021
www.ridepatco.org

Q-Card Company
301 Reagan Street
Sunbury, PA 17801
www.q-card.com

Quadagno & Associates, Inc.
1626 Herron Lane
West Chester, PA 19380
www.quadagno.com

Raak Technologies
602 East 42nd Street
Austin, TX 78751
www.raaktechnologies.com

Rambus
Stationsplein 45 A6.002
Rotterdam, AK 0313 Netherlands
www.bellid.com

LEADERSHIP COUNCIL



SAIC - Science Applications International Corporation

12901 Science Drive
Orlando, FL 32026
(407) 243-3774
www.saic.com

Science Applications International Corporation (SAIC) is a leading technology integrator that provides full lifecycle services and solutions in the technical, engineering, and enterprise IT markets.

San Francisco Bay Area
Rapid Transit District (BART)
300 Lakeside Drive
Oakland, CA 94612
www.bart.gov

San Mateo County Transit District
1250 San Carlos Avenue
San Carlos, CA 94070
www.smctd.com

Scheidt & Bachmann USA
31 North Avenue
Burlington, MA 01803
www.scheidt-bachmann.de/en/

SecureKey Technologies
555 Twin Dolphin Drive, Suite 620
Redwood City, CA 94065
www.securekey.com

Servired
C/ Gustavo Fernández Balbuena, 15
Madrid 28002 Spain
www.servired.es

SHAZAM
6700 Pioneer Pkwy
Johnston, IA 50131
www.shazam.net

Signet Technologies, Inc.
12300 Kiln Court, Suite E
Beltsville, MD 20705
www.signetinc.com

Southeastern Pennsylvania
Transportation Authority (SEPTA)
1234 Market Street, 13th floor
Philadelphia, PA 19107
www.SEPTA.org

Stanley Black & Decker
805 15th Street NW, Suite 710
Washington, DC 20005
www.sbdgov.com

STMicroelectronics
1375 East Woodfield Road, Suite 400
Schaumburg, IL 60173
www.st.com

SureID, Inc.
5800 NW Pinefarm Place
MS 315-B
Hillsboro, OR 97124
www.sureid.com

Systems Engineering, Inc.
21351 Gentry Drive, Suite 100
Dulles, VA 20166
www.seisystems.com

Thales
900 South Pine Island Road, Suite 710
Plantation, FL 33324
www.thales-esecurity.com

The Johns Hopkins University Applied
Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
www.jhuapl.edu

The Utah Transit Authority
669 West 200 South
Salt Lake City, UT 84101
www.rideuta.com

Translink
400-287 Nelson's Court
New Westminster, BC V3L OE7 Canada
www.translink.ca

Tri County Metropolitan
Transportation District of Oregon
1800 SW 1st Avenue, Suite 300
Portland, OR 97201
www.trimet.org

Tyco Integrated Security
4700 Exchange Court
Boca Raton, FL 33431
www.tyco.com

Tyco Software House
6 Technology Park Drive
Westford, MA 01886
www.tyco.com

U.S. Department of State
DS/ST/FSE
SA-18 Room #242
Washington, D.C. 20522
www.state.gov

U.S. Department of Transportation/
Volpe Center
55 Broadway
REVT-50
Cambridge, MA 02142
www.volpe.dot.gov

U.S. Government Printing Office
732 North Capitol St NW
Mail Stop: SID
Washington, DC 20401
www.gpo.gov

Ultra Electronics Card Systems
6724 185th Avenue NE, Suite A
Redmond, WA 98052
www.ultraid.com

Underwriters Laboratories (UL)
3900 Northwoods Drive, Suite 350
St. Paul, MN 55112
www.ul-ts.com

LEADERSHIP COUNCIL



Valid USA
1011 Warrenville Road, Suite 450
Lisle, IL 60532
630-852-8200
www.validusa.com

Valid USA provides secure solutions
for data, payment, identity, mobile, and
targeted brand messaging.

VenTek International
1260 Holm Road
Suite A
Petaluma, CA 94954
www.ventek-Intl.com

Veridt, Inc.
7182 US Highway 14
Suite 401
Middleton, WI 53562
www.veridt.com

VeriFone, Inc.
1400 West Stanford Ranch Road, Suite
200
Rocklin, CA 95765
www.verifone.com

LEADERSHIP COUNCIL



Visa Inc.
P.O. Box 8999
San Francisco, CA 94128 - 8999
650-432-3200
www.visa.com

Visa Inc. is a global payments
technology company that connects
consumers, businesses, financial
institutions and governments around
the world to fast, secure and reliable
digital currency.

Vix Technology
710 Second Avenue, Suite 950
Seattle, WA 98104
www.vixtechnology.com

Waltz, Inc.
95 Wall Street #706
New York, NY 10005
www.waltzapp.com

Wells Fargo
350 SW Jefferson St
MAC P2819-010
Portland, OR 97201
www.wellsfargo.com

LEADERSHIP COUNCIL



XTec, Inc.
11180 Sunrise Valley Drive, Suite 310
Reston, Virginia 20191
703-547-3524
www.xtec.com

XTec offers enterprise solutions
for identity, credential and access
management programs on a wide scale
for over 95 federal agencies providing
hosted smart card, mobility and access
control solutions through the AuthentX
Cloud.

Oberthur Technologies, #1 Provider of EMV in the U.S., and Safran Morpho, #1 Provider of Automated Biometric Solutions, have joined forces and are NOW



**The
global
leader**

**in trusted identities
for an increasingly
digital world**

Well positioned
in our markets

Trusted by
1,800 financial Institutions

#1 in **US driver's license issuance**

Trusted by **500+ mobile operators**

#1 in **police biometric systems**

Trusted by major industrial OEM's

#1 in **civil identity solutions**

www.idemia.com





Secure Technology Alliance

191 Clarksville Road
Princeton Junction, New Jersey 08550
www.securetechalliance.org

