



Spring 2017

# ACCESS CONTROL COUNCIL

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. 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.

## ACCESS CONTROL COUNCIL ACTIVITIES

The Council works on projects and initiatives to stimulate the use of secure technologies in various form factors for access control. Activities include:

- 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 international, federal, state and local governments, and private enterprises in leveraging NIST's Federal Information Processing Standard (FIPS) Publication 201 Personal Identity Verification (PIV) and PIV interoperable (PIV-I) credentials for access management and developing policies governing their use
- Providing industry resources to assist organizations in using standards-based smart cards, mobile credentials, and credentials in other form factors for access control
- 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

## COUNCIL PARTICIPATION

Get involved, get active. Raise your company's profile in the industry. Participation in the Access Control Council is encouraged and appreciated. Engage with industry leaders to shape the direction for implementing secure solutions in the access control industry.

## COUNCIL RESOURCES

### White Papers

- Commercial Identity Verification (CIV) Credential: Leveraging FIPS 201 and the PIV Card Standards
- A Comparison of PIV, PIV-I and CIV Credentials
- Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance Summary
- FIPS 201 and Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems
- FIPS 201 PIV II Card Use with Physical Access Control Systems: Recommendations to Optimize Transaction Time and User Experience
- Guide Specification for Architects and Engineers for Smart Card-based PACS Cards and Readers for Non-government PACS
- Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Businesses
- PIV Card/Reader Challenges with Physical Access Control Systems: A Field Troubleshooting Guide
- Smart Cards and Biometrics
- Strong Authentication Using Smart Card Technology for Logical Access
- Supporting the PIV Application in Mobile Devices with the UICC

## INDUSTRY COLLABORATION AND COMMENTARY

- Collaboration with the International Biometric Industry Association (IBIA) and Security Industry Association (SIA)
- Submission of industry comments and recommendations to: GSA on FIPS 201 Evaluation Program Functional Requirements and Test Cases; NIST on SP 800-63; OMB on Circular A-130.

**FIND ACCESS CONTROL COUNCIL RESOURCES ONLINE:**

[www.securetechalliance.org/activities-councils-access-control](http://www.securetechalliance.org/activities-councils-access-control)





## MEMBER COMMENTS

"The Secure Technology Alliance Access Control Council has been a very valuable source of current and relevant information regarding technology trends and government and industry initiatives and also serves as a forum to provide input, share views and help influence the future of our industry. It provides a view of things to come which helps tremendously in planning and solutions development."

—Tony Damalas, Vice President, ICAM Division, SigNet Technologies, Inc.

"The Secure Technology Alliance Access Control Council provides an important forum for information exchange, education, and leadership on important matters pertaining to the use of technology for secure access to facilities and information systems. The objective work of this group is highly respected by both government and commercial enterprises and I am proud to be a participant in the Council."

—Walter Hamilton, Sr. Consultant, Identification Technology Partners

"This is a powerful and important council that provides abundant guidance from an segment of access control users, product manufacturers and technologists – both public and private. There is nearly a century of knowledge collectively on real-life experiences on how to better this dynamic and important space. The Access Control Council listens, suggests, collaborates and promotes access control guidance. In the end, this important group provides solid input and application guidance for the better good."

—Ryan Kaltenbaugh, Vice President, Federal Government Solutions, Lenel

"The Access Control Council provides real life implementation guidance for corporations, agencies and end users. It leverages the combined expertise of private and federal members to address industry topics and trends. As a result the resources that are available through the Access Control Council are useful to any stakeholder involved in a smart card implementation."

—Kevin Kozlowski, Vice President, XTEC, Incorporated

"For most of a decade, participation in the Secure Technology Alliance Access Control Council has provided me with a venue to meet and engage leaders and experts involved in the many facets of the smart card industry. Through thoughtful discussions and numerous deliverables I have gained important insights into the key issues tackled by this effective team of dedicated and concerned professionals and illuminated by the collective voice of this vendor neutral group. Alliance membership has been a valuable navigational aid in guiding my business and my career, as well as leading to many long standing friendships."

—Steve Rogers, President, IQ Devices

"The Secure Technology Alliance's Access Control Council provides a unique forum for government and industry to collaborate on mutually beneficial strategies and practices concerning ICAM. Having this forum brings together some of the most experienced and professional people available to accomplish any challenge."

—Jason Rosen, PSP, Sr. HSPD12 SME Manager, Team Business Integra,  
U.S. Department of State Bureau of Diplomatic Security

## ABOUT THE SECURE TECHNOLOGY ALLIANCE

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT). The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

The Secure Technology Alliance industry and technology councils are focused groups within the overall structure of the Alliance. Councils were created to foster increased industry collaboration within a specified industry or market segment and produce tangible results, speeding the adoption of secure solutions and industry growth. Groups collaborate on specific deliverables, including reports, briefings and educational material. The Secure Technology Alliance currently has seven active councils focusing on the payments, health and human services, identity, Internet of Things (IoT) security, access control, mobile, and transportation industries. Council participation is open to any Secure Technology Alliance member who wishes to contribute to the council projects.

### Council Officers

Chair: Adam Shane, Leidos  
Vice Chair: Dave Helbock, XTEC, Inc.

### Council 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

### Council Members

ABCorp  
Accenture  
Allegion  
AMAG Technology  
Brivo  
CardTek  
CertiPath LLC  
CH2M  
Cubic Transportation Systems  
Datawatch Systems  
Defense Manpower Data Center (DMDC)  
Entrust Datacard  
Exponent  
Gallagher North America Inc.  
Gemalto  
General Services Administration  
G+D Mobile Security  
Hewlett Packard Enterprise  
HID Global  
Identification Technology Partners  
Identiv  
Initiative for Open Authentication (OATH)  
IQ Devices  
Leidos  
Lenel Systems International  
NXP Semiconductors  
Oberthur Technologies  
Parsons  
Quantum Secure Inc.  
Safran Group  
SAIC  
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  
Visa Inc.  
Wells Fargo  
XTEC, Incorporated