BOSCH
Invented for life

Physical Security Solutions for US Federal Government Applications

Dirk Stegemann, Bosch Security Systems, Inc.
Darnell Washington, SecureXperts, Inc.

1. Introduction

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, President Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The president directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework – based on existing standards – of guidelines for reducing cyber risks to critical infrastructure.

The U.S. federal government has also identified the need for improving the physical security of its facilities and integration with logical networks. In particular, several security incidents have led federal agencies to the conclusion that their current video surveillance systems are no longer capable of adequately protecting their facilities because they lack support for facial recognition and video analytics, are insufficiently protected against cyber attacks, and are not aligned with the federal enterprise IT architecture.

Today's increasing level of cyber sophistication, successful exploitation of rogue malicious cyber attacks and the inability to protect Internet Protocol (IP)-connected devices used for physical/logical systems from interception by unauthorized sources, has compelled the U.S. federal government (especially the Department of Homeland Security and the Department of Defense) to introduce stronger methods of authentication and encryption for IP-connected devices.

While advancements in security technologies include video analytics, license plate recognition, sensor and alert integration, behavioral analytics, and more, common information security deficiencies prohibit widespread adoption through federal government, enterprise commercial, retail, health care, and other regulated markets that require higher levels of assurance for access control and security.

Bosch has recently partnered with Florida-based IT security consulting firm SecureXperts, Incorporated (SXI) – www.securexperts.com – in the development of next-generation security products that overcome common security deficiencies and vulnerable security gaps that are prevalent in other network-connected products. Bosch and SecureXperts are currently developing a roadmap of integrated solutions for video surveillance, intrusion detection and access control that span the whole system lifecycle including installation, operation support and maintenance.

This document analyzes the technical requirements for next-generation physical security systems for U.S. federal government applications and outlines an integrated physical security solution for video surveillance, intrusion detection and physical access control targeted with these requirements.

Section 2: U.S. Federal Government Security Strategy
Section 3: Customer Requirements on Physical Security Systems
Section 4: Use Cases for Physical Security Systems
Section 5: Envisioned Technical Concepts
Section 6: Conclusions

The joint project will define, leverage, and improve the current U.S. Federal Enterprise Architecture (FEA) as well as component architecture models for physical and logical IT integration mandates. It will use the process of exchanging and binding person entities and non-person entities with Federated Certificate Authorities. This solution will meet the high availability, fault tolerance, and business continuity/disaster recovery metrics that are mandated for protection of key government and economic assets under Homeland Security Presidential Directive 7 (HSPD-7) and is consistent with the recently published NIST Cybersecurity Framework.

2. U.S. Federal Government Security Strategy

2.1 Overview
The U.S. federal government postulates that security depends on the addressing of both physical and cybersecurity threats with state of the art measures and in a coordinated manner across all federal departments and agencies. We briefly outline several initiatives that have been launched to implement this strategy, from which customer requirements on physical security systems may be derived.

2.2 Physical Protection of Federal Agencies' Facilities

The Government Accountability Office (GAO) has identified a particular need for improving the physical security of the facilities owned by the federal government. This shall be addressed by a common framework for physical security which includes:

- a risk management approach to facility protection
- leveraging advanced technology, such as smart cards
- improving information sharing and coordination
- implementing performance measurement and testing
- using standard performance metrics to evaluate the effectiveness of physical protection in order to make physical and logical security converge into a holistic security capability.

2.3 NIST Cybersecurity Framework
To help organizations charged with providing the nation's financial, energy, health care and other critical systems better protect their information and physical assets from cyber attack, NIST released a Framework for Improving Critical Infrastructure Cybersecurity. The Framework provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs. http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

The framework allows federal and enterprise commercial organizations to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure owned by government and enterprise commercial organizations.

The framework enables federal and enterprise commercial organizations to determine their current level of cybersecurity, set goals for cybersecurity that are in sync with their business environment, and establish a plan for improving or maintaining their cybersecurity. It also offers a methodology to protect privacy and civil liberties to help organizations incorporate protections into a comprehensive cybersecurity program.

2.4 Federal Identity, Credential and Access Management (FICAM)
Since both physical security and information security solutions depend on reliable identity verification (authentication) and authorization of person entities (PEs) as well as non-person entities (NPEs), the U.S. federal government has launched an identity, credential and access management (ICAM) initiative to support its cybersecurity activities with means to enable trust across organizational, operational, physical and network boundaries. Respectively, all federal IT systems are required under mandates to comply with the ICAM architecture proposed by this initiative.

This Federal ICAM initiative (FICAM) relies on two major components, the Federal Public Key Infrastructure (FPKI) and the Personal Identity Verification (PIV) framework.

2.4.1 Federal Public Key Infrastructure (FPKI)
The FPKI enables a trust framework for interoperable, high-assurance person entity and non-person entity authentication. Particularly, it supplies means that maintain X.509 digital certificates for person entities as well as non-person entities. http://www.idmanagement.gov/identity-credential-access-management

2.4.2 Personal Identity Verification (PIV)
As mandated in HSPD-12, a common identification standard for federal employees and contractors has been established in Personal Identity Verification (PIV) of federal employees and contractors. This is used for verifying the identity of individuals, i.e., person entities, who seek physical access to federally controlled government facilities as well as logical and electronic access to government information systems using a standard known as FIPS 201.

The FIPS 201 standard requires a personal smart card credential, called the PIV card; PIV cards typically contain a PIN and a unique ID, and at least a photo of the cardholder printed on the card, an asymmetric key pair of computer generated cryptographic codes X.509 certificate managed by the FPKI, and an electronic representation of fingerprints of the cardholder.

Since the intent of the PIV card is to be used across all federal agencies for a wide range of applications, certain stringent identity proofing, cardholder obligations, and compliance with privacy requirements on personal information in identifiable form (PII) are required to be satisfied.

2.5 Federal Cloud Computing Strategy

Federal agencies are requested to move IT services into the federal cloud in order to reduce inefficiencies and realize cost saving potentials. Therefore, newly purchased or licensed IT systems shall rely on cloud computing technology wherever appropriate.

3. Customer Requirements on Physical Security Systems

Based on official U.S. federal government communication as well as additional analyses provided by SecureXperts, Bosch and SecureXperts will develop the integration platform using the following customer requirements for next-generation physical security systems.

a) Rely on cloud-hosted architecture based on the federal cloud, where applicable
b) Implement federally-auditable and certifiable system architecture based on the Risk Management plan provided under the NIST Cybersecurity Framework.
c) Ensure cross-vendor interoperability
d) Support an open systems framework for capabilities exchange with disparate systems, including secure unified communications networks for public safety
e) Comply with FICAM, especially PIV and FPKI
f) Identify and authenticate Person Entities (PEs) based on PIV cards and NPEs by a suitable analogous mechanism in order to prevent impersonation attacks
g) Authorize access of PEs and NPEs to logical and physical resources in the system and physical resources protected by the system
h) Assure confidentiality of sensitive data, especially personal information in identifiable form
i) Assure system integrity, especially by assuring entity and message integrity

4. Use Cases for Physical Security Systems

The following use cases of next-generation physical security systems were identified:

a) Law enforcement officers access video surveillance data from the surroundings of a crime scene to identify suspects
b) Public safety authorities use video surveillance data for alarm verification
c) Video analytics / face recognition (potentially hosted in a cloud backend) is used to match people in video surveillance data against suspect watch lists
d) Traffic monitoring cameras are used as data sources for dynamic evacuation traffic routing (e.g., in case of hurricane warnings)
e) A federal agent configures users and their access rights to a physical security system in a federated directory (e.g., an Active Directory) rather than in the control panel of the respective system
f) Physical access control rights are managed along the same lines as logical access control rights in a federated directory (e.g., an Active Directory)

5. Envisioned Technical Concepts

This section defines the preliminary technical concepts of the proposed solution in terms of its network architecture and its security measures.

5.1 Network Architecture

The proposed integrated physical security solution consists of the physical security subsystems

a) IP video camera (CCTV)
b) video surveillance system (VSS)
c) physical intrusion detection system (IDS)
d) physical access control system (PACS)

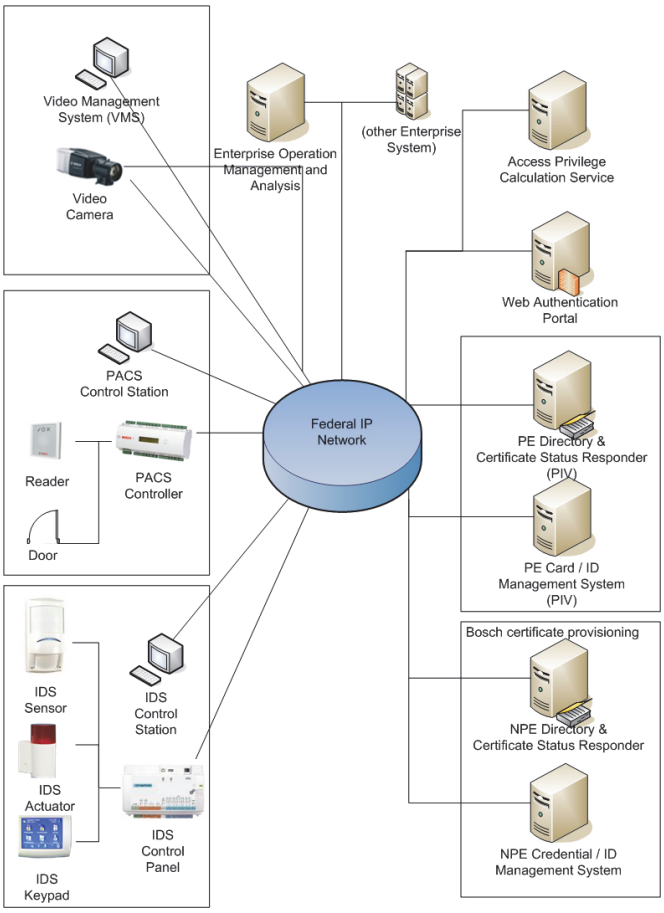
While these subsystems may rely on proprietary field buses for internal communication, at least one subsystem component is connected to the common IP network of all federal agencies (the so-called federal network) in order to allow for interaction across subsystems and with cloud-based services and remote management clients. Middleware components such a public key infrastructure (PKI) is also accessible over the federal network.

The IP camera consists of a web-enabled server that has the ability to connect via secure communications – Secure Sockets Layer (SSL)/Transport Layer Security (TLS) – between the workstation and the camera. The workstation will be application aware of the PIV card, which must be inserted and validated by the FPKI Bridge prior to establishing communication with the camera.

The VSS consists of video cameras and a video management system (VMS) that is used to manage the cameras, view live video, receive camera events, etc. Both video cameras and the VMS are connected to the federal network.

The IDS contains sensors, e.g. motion detectors, and actuators, e.g. a siren, a keypad that is used to arm and disarm the system and a control panel as basic components. The communication between sensors, actuators, the keypad, and the control panel is proprietary, while the control panel is connected to the federal network. Event and alarm handling and potentially also management and configuration are done at a control station, which is also attached to the federal network.

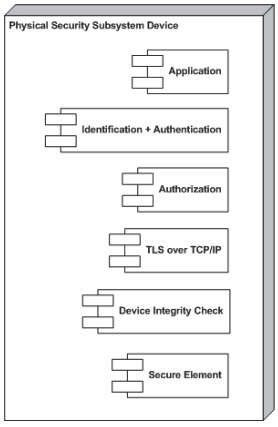
The PACS consists of a PACS controller that communicates to credential readers and door controllers over proprietary communication protocols, and a control station for configuration and monitoring. The PACS controller and the control station are connected to the federal network.

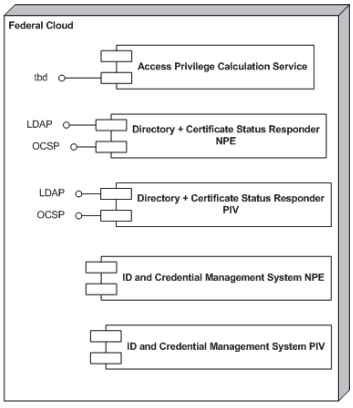


5.2 Security Measures

5.2.1 Entity Identification and Authentication

Person entities (PEs) are identified and authenticated based on their PIV card as the credentials. Non-person entities (NPEs) are identified and authenticated analogously based on a secure element, e.g., a smart card or an SD card that contains, similarly to PIV cards, asymmetric key pairs and corresponding X.509 certificates.





5.2.2 Authorization

Access of both PEs and NPEs to physical or logical resources in the system or resources protected by the system is authorized by an Access Privilege Calculation Service accessible via Lightweight Directory Access Protocol.

5.2.3 Confidentiality

Confidential data travelling in the federal network is protected by a TLS encrypted channel. Confidential data travelling on other communication networks in the system is protected by appropriate means, e.g., message encryption or physical protection of the communication channel.
Confidential data within system devices and components is protected by appropriate device-specific means.

5.2.4 System Integrity

PE integrity is assured by background checks prior to credential issuance and renewal. NPE integrity is assured by periodic firmware verification based on a secure element and by TLS for messages on the federal network and appropriate measures for messages on other communication channels.

6. Conclusions

The use of federally-trusted electronic digital certificates, including network authentication, key encryption and digital hashing functions, to verify and validate that communications have not been altered during transmission and storage provides significant benefit to government, law enforcement, and the private sector for protecting critical assets. Bosch and SecureXperts are defining the next-generation security requirements for successful entry into federal information and critical infrastructure protection sectors.

In addition to the aforementioned security controls, other benefits such as time stamping of physical security devices synchronized with authoritative network time protocols will provide strong forensic data collection capabilities that is effective in legal and evidentiary proceedings, and provides proven chain of custody which cannot be refuted.

The partnership between Bosch and SecureXperts will leverage wide scale adoption across other platforms, including Physical Security Information Management (PSIM), and provide better protection for the infrastructure on which these systems are highly dependent.

Technical Contacts:

Dan Reese
Director, Vertical Market Applications
Bosch Security Systems, Inc.
(717) 735-6308
Dan.reese@us.bosch.com

Darnell Washington
President/CEO
SecureXperts, Inc.
(404) 693-5100
dwashington@securexperts.com