Nationwide Deployment of Identity Management Solutions

Gordon Hannah
BearingPoint, Inc.

Abstract

Nations around the world have begun to deploy large-scale smart card solutions including National ID card, ePassport, and port security programs to name a few. Programs like these offer a variety of advantages. The ePassport program offers interoperability between countries that could drastically reduce immigration fraud and increase confidence between states. Social services and electronic purses can be integrated and attached to a National ID card. In addition, Nationalized health care, census, voter registration, licensing, and other functions can be integrated into a smart card, which is securely bound to an individual’s identity.

Utilizing smart cards and biometrics as part of an overall identity management system is becoming the security standard the U.S. government is moving toward due to the Homeland Security Presidential Directive (HSPD) 12 mandate.

The Transportation Worker Identification Credential (TWIC) is one of the largest credentialing initiatives currently on-going in the U.S. This paper reviews the successes and lessons learned for the implementation of a large-scale credentialing initiative.

Keywords: smart card, biometrics, HSPD-12, Transportation Worker Identification Credential, TWIC

Nationwide Deployment of Identity Management Solutions

In the United States, all U.S. Government agencies are expected to have a credentialing initiative underway by the end of 2006. One of the largest smart card initiatives is already underway; the U.S. Government began a nationwide deployment of its Transportation Worker Identification Credential (TWIC) program, aimed at securely credentialing an unknown population of transportation workers estimated to be around one million people. The TWIC program aims to increase security and enhance commerce throughout an extensive transportation system.

BearingPoint has been an active player in developing solutions Government-wide and has a wide-range of expertise and experience in nationwide smart card programs.

BearingPoint was contracted by the Transportation Security Administration (TSA) to support the development and implementation of a prototype system for the TWIC program. Under this initiative, BearingPoint was tasked with developing and implementing a solution that will improve security mechanisms, enhance commerce, and protect personal privacy information. The goal is to develop a uniform, nationwide credential for transportation workers that will minimize the requirement for redundant credentials and background checks. The Prototype phase was the third phase in developing a program to improve security at seaports, airports, rail,
pipeline, trucking, and mass transit facilities by creating a nationwide credential that will prevent unauthorized persons from gaining access to secure areas. The TWIC Phase III program provided a smart card as the universal identity card to transportation workers in three regions across the United States.

For the TWIC Prototype, the BearingPoint team built a technical solution that is scalable, secure, and open COTS-based. Capable of supporting a user population more than one billion, the solution was easily implemented through web-based, user-friendly interfaces that lowered administration costs and increased the availability of the system (by using the Internet) across the United States. The components are interoperable and non-proprietary, giving TSA flexibility and choice while ensuring that the solution did not lock the Government into a single product design.

The integrated system provided a comprehensive solution for enrolling and issuing the TWIC to a widely dispersed population of workers across the three regions. The credential was issued only after each worker was sponsored (by a transportation facility, the company for whom they work, etc.) and his or her identity authenticated using biometrics, background checks, and provision of secure documents. The TWIC aided in identifying and verifying the identity of a transportation worker to prevent unauthorized individuals from accessing secure areas through vetting and background checks. BearingPoint developed a comprehensive solution that allowed for the establishment of TWIC sponsors; for Transportation Workers to use a website to pre-enroll for their credential and setup an appointment for data capture; for information to be securely transmitted to a card production facility; and for the TWIC to be activated and disseminated to the correct Transportation Worker. Once the transportation worker had an active TWIC, logical and physical access to sites can be granted using a variety of biometric technologies (e.g., facial, iris scan, hand geometry and fingerprint). The system made use of an end-to-end security infrastructure for establishing a chain of trust for the various processes within the system.

Prototype operations were conducted in three regions of the country: East Coast (Camden, NJ, Islip, NY, Philadelphia, PA, and Wilmington, DE); West Coast (the ports of Los Angeles and Long Beach, CA); and Florida (the 12 major port facilities in the state of Florida). Participation was voluntary and included truckers, longshoremen, and container terminal and airport personnel.

The solution consisted of seven major processes as follow:

- **Sponsor Registration:** Organizations seeking to sponsor an individual for a TWIC were required to become registered sponsors. To become a registered sponsor, organizations had to provide background information to TSA via the TWIC website. The system design was based on the principles of Service Oriented Architecture (SOA). Custom workflows for Sponsor Registration and adjudication were designed for this process.
• **Transportation Worker Pre-enrollment:** The sponsoring organization was responsible for disbursing login credentials and instructions to the transportation worker. The transportation worker then input personal information using the TWIC website.

• **Enrollment Center:** Once at the Enrollment Center, all the information entered during pre-enrollment can be verified and any missing information added. The transportation worker provided documentation to authenticate their identity and a photograph and fingerprints were captured to finalize the enrollment record.

• **Background Check:** Once the enrollment information was packaged, it was parsed and sent through to a number of background checks for approval to issue a credential.

• **Card Production:** The transportation workers enrollment record is sent to the card production facility. The card production facility employee initiates the card personalization, printing, and chip encoding processes.

• **Card Issuance:** Once the cards were received at the Enrollment Center, the transportation worker was automatically notified that his/her card is ready for pick-up and activation at the Enrollment Center. The TWICs were securely stored in safes until the transportation worker picked up the card with a picture identity card. A biometric reference match was conducted to activate the card.

• **Privilege Granting:** Using a variety of biometric technologies, transportation workers could be given physical and logical access to sites for which they are authorized access.

Nationwide rollout of any smartcard program can provide lessons learned from the TWIC program in a variety of areas including:

- Biometric Interoperability – Standards-based biometric templates implementations can be interoperable with no impact on performance.
- Adjudication – Every threat assessment or background check conducted requires in-person adjudication for a small percentage of the total conducted.
- Communication and Stakeholder Buy-in – Though challenging with multiple stakeholders, communication to facilitate buy-in ensures success.
- Physical Access Control Systems – Local facilities often have specific needs and many prefer that access control be managed locally.
- Interoperability and Standardization – Standardization of a credential saves time and money.
- Standard Operating Procedures – Standard Operating Procedures provide the foundation for a standardized credentialing system.
- Privacy – Throughout development, all privacy issues must be addressed. Transparency of data usage is paramount.
- Legacy Conversion – It is important to integrate legacy systems / records in order to issue cards to legacy cardholders with defined expiration dates without forcing the applicants to completely re-enroll.

People and well-defined documented processes support identity management and verification systems. People take on a number of roles including registration/enrollment, performance of background check, adjudication, and the personalization and issuance of credentials. Well-
defined processes address capturing quality biometrics, providing an appeal process for the
denial of a credential, identifying fraudulent documentation, and the ability to quickly revoke
access privileges to individuals identified as a threat. Without well-trained individuals and
strong business processes, “bad actors” will quickly find and successfully target the system’s
weakest link.

The TWIC program has implications that influence the overall development of identity
management systems in the U.S. On August 27, 2004, HSPD-12 was signed directing that a
“government-wide standard for secure and reliable forms of identification issued by the Federal
Government to its employees and contractors” be implemented by all Federal agencies. From
this mandate, more specific instructions have been developed such as the Federal Information
Processing Standard (FIPS) 201 and related special publications to provide further guidance on
how this mandate can be met. FIPS 201 was developed using the TWIC program as a model and
therefore the TWIC program is already aligned closely to the HSPD-12 mandate.

Conclusion

The TWIC Prototype established that commercial off-the-shelf (COTS) technology can be
leveraged/integrated to create cost effective multi-factor authentication applications that can be
deployed throughout very large organizations. Additionally, the TWIC solution has increased
the security mechanisms governing access to the national transportation system. The program
improves security be establishing a common credential with a universally recognized appearance
and standardized security features. The TWIC will positively and securely link an individual to
his or her credential via a reference biometric and to the background information on the claimed
identity of that individual. More importantly, the TWIC program has served as a model upon
which other U.S and international government security initiatives are based.