



November 2004

Guest Columnist - Eric Widlitz, HID Corp.



Anyone looking at the many U.S. federal government's security initiatives can see that one thing is clear – in smart cards we trust.

Smart card technology has become a digital Fort Knox in the effort to strengthen ID credentials, network security and even passports. The new Homeland Security Presidential Directive 12, issued August 27, 2004, gives this movement even greater impetus.

But as smart cards move more strongly into physical access control systems, an important question arises: Are the standards ready or not? And, what, if anything, remains to be done?

Government Smart ID Cards Today

The use of smart cards for identity credentials is already quite extensive within the federal government. The most advanced program is the Department of Defense Common Access Card (CAC), with cards issued to over 3.4 million employees, contractors and others.

Building on this success, GSA, State, Treasury, Homeland Security, Veteran's Affairs and NASA all have established programs to issue new smart ID cards. These initiatives have spawned the need for a common identity credential that is used for both physical and logical access control across all branches of the federal government.

Several factors have driven the need for a new form of ID credential. First, organizations have been looking for ways to make the credential significantly harder to counterfeit. In addition, there has been a need to complement or replace the "flash pass" method of ID verification with a machine-based ID authentication. Finally, agencies and departments have wanted to extend the use of the badges into online security application areas.

While the need to tie these credentials to physical access control was obvious from the outset, the U.S. federal government initially was not in a good position to standardize as it began looking into new forms of ID badges. Although federal agencies are pervasive users of physical access control systems, until now they have procured full systems and system components with little or no central guidance. The result has been technical incompatibility between cards and systems that now present a formidable challenge to standardizing an approach for ID credentials.

Government Smart Card Interoperability Specification

The Defense Department's CAC program laid the foundation to rectify this situation, because it provided a real program around which standards efforts can coalesce. Across the federal enterprise, the primary point of integration is the card itself. The CAC and other ID programs have produced the NIST Government Smart Card Interoperability Specification (GSC-IS), currently in version 2.1. This standard incorporated the industry's most widely accepted standard technologies, including contactless smart cards (ISO 14443) and contact smart cards (ISO 7816).

With a common credential comes the opportunity to promote physical access control interoperability across agencies, so the issue of access control standards took center stage. The Physical Access Interagency Interoperability Working Group (PAIIWG) was charged with creating and documenting guidance for such an approach. The resulting guideline, "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems," was published in July 2004, and is the primary specification followed today by HID Corp. and other physical access control systems equipment manufacturers. This guidance reflects current U.S. Government technical requirements and has been approved by the Government Smart Card Interagency Advisory Board (GSC-IAB).

The guideline correctly states that the key to credibility, non-repudiation and reciprocity in a government-wide credential program is defining and accepting a unique number assigned to a single individual. To achieve this the guideline specified the Federal Agency Smart



GSN: Government Security News; November 2004

3

Credential Number (FASC-N) to replace the SEIWG-012 definition, which has been in use for over 10 years. The FASC-N will be the primary identification string used on all government issued credentials.

The FASC-N, a very robust and forward thinking definition (read "lots of bytes"), was created to ensure legacy compatibility with existing systems based on the SEIWG-012 definition.

The specifications also cover what chip technology can be used and provides the command set for use with physical access control. In short, it adequately specifies how to build interoperable readers and the card-reader security level.

The current guidelines, however, do not fully specify readers to access the entire control panel output. The FASC-N is too large for many access control panels to support its full output because a range of assurance profiles – low, medium, and high – are associated with the extensible data model on FASC cards. These assurance profiles provide for increasing the integrity of the transaction between the card and the reader, but put significantly greater demands on readers and access control panels than was traditionally required.

Wisely, the government working groups have left this issue to the industry to resolve, with the goal of extending the standard over time as the best solutions emerge. NIST will be releasing a new specification in February 2005 to comply with HSPD#12. This is an extremely aggressive schedule for developing an entirely new specification and I believe they will look to the GSC and Technical Implementation Document for guidance to create this new specification. A few ambiguities do exist in these specifications today and this new spec will help clear things up and make it easier to achieve a truly interoperable system.

Four months after the release of the specification, each government agency is to have a program or plan in place for compliance. Four months after that, they are required to start implementing the plan. Although there is no government funding for this initiative, each agency is asked to find the funds to comply. This should be a very interesting time.

One thing is certain, new access control readers will require a great deal of flexibility from reader manufacturers to achieve interoperability. This is particularly true in the near term, where the only sensible way to achieve interoperability will be to support several upstream options for communicating out of the reader to the access panels.

Over time, these older products will give way to a new generation of open, flexible access panels. These new systems will consist of open architecture, and will include options for handling the full capabilities of the FASC-N identifier, stronger encryption and advanced network communications capabilities.

The consensus of both industry and government stakeholders is that the standards and guidelines that are in place today are sufficiently detailed to support development and implementation of physical access control readers and cards.

The FASC-N definition provides a long range, extensible foundation. At the same time, the guidelines are flexible in defining how readers and panels communicate. This practical approach positions government organizations to gradually evolve to new access control card and system technology. Going too far would create an unworkable situation in the short term by discouraging organizations from continuing to use existing panels and systems, thereby making it economically infeasible to migrate. Over time, standards will move higher up the system chain as best practices for reader to access panels emerge.

Eric Widlitz is manager for government & technology applications for HID Corporation. He can be reached at ewidlitz@hidcorp.com