Comments from Identity Alliance

for
FIPS 201 – Public Draft of Nov 8, 2004
&
SP 800-73 – Public Draft of Nov 8, 2004

Document Version 0.1

Prepared By:

Identity Alliance
Austin, TX

Prepared For:

National Institute
of
Standards and Technology

December 23, 2004

Table of Contents

Figures

Version #	Date	Document Status	Principle Editor
0.1	December 23, 2004	Draft Sent to NIST	Timothy M. Jurgensen

Overview Comments

NIST is to be commended for its preparation of the public drafts for FIPS 201 and SP 800-73 given the exceedingly short time-frame established by HSPD-12. While there are many not-insignificant problems to be found in the drafts, the general framework provided by both documents follows very much the obvious spirit as well as the letter of HSPD-12.

HSPD-12 is very clear in mandating a standard identification system for all agencies of the federal government, not a simple standard for using a smart card. HSPD-12 makes it clear that this should be an identification system that is to make identity authentication a common experience for all federal employees and contractors at all venues within the federal government (excluding those related to national security systems). This is not an excuse for a "federated" identity system in which each agency is autonomous, but rather is a mandate for a single system that encompasses the entire federal government. Also, it is clear that this identification system is to be grounded in state-of-the-art technology so as to preclude counterfeiting and fraud to the maximum extent possible. Further, this identification system is to guarantee, to the maximum extent possible, the privacy of the individuals represented within this identification system. This essentially requires that an individual's identity be based upon biometric characteristics of the individual, and not upon information merely related to that individual. Without a doubt, biometric based identity is the state-of-the-art for strong authentication of identity. When coupled with strong individual privacy measures *vis-à-vis* attributes to identity, this system can guarantee that such attribute information will not be arbitrarily disseminated without the knowledge and permission of the individual involved.

Perhaps most important, it must be remembered that the token issued to, and carried by the individual is not a credential based identity system. That is, the token does not convey identity; it merely aids in the authentication of identity. What it can convey, as an extension beyond a pure identity system, are credentials that define authorization for activities that are to be allowed for a specific identity when authenticated. Thus, the token may well assert that "John Doe is an employee of the United States Government" but it does not assert that "The bearer of this token is John Doe." Rather, the token may assert that if the token bearer possesses this (or these) biometric characteristics (conveyed through a credential stored on the token) as determined through this standard authentication protocol, then the bearer is authenticated to be John Doe. The token provides a convenient and secure mechanism for conveying information in the form of credentials and it provides a secure mechanism for projecting a secret across an unsecured communication channel. These capabilities are very different from a credential based identity system.

With these organizing observations in mind, we offer the following, more specific comments regarding the two documents in question.

Detailed Comments

1. ***Enrollment and Card Management*** - The purpose of an identification system is to convey trust in the authentication of the identity of an individual. To convey trust, it is necessary to build a "chain of trust" from the seminal activities related to the system until its use in actual authentication operations. This chain of trust must encompass the construction of any tokens used in the system, the personalization of these tokens, and the on-going "use management" of these tokens. For any identification system, the initial enrollment operation and token issuance operations are notorious risk areas. Consequently, both the FIPS 201 standard and the associated SP 800-73 specification MUST cover the enrollment, attribute confirmation (a.k.a. identity vetting or identity proofing) and token issuance operations. If any of these operations are not included within the standard, then there is little hope that an adequate trust environment can be ensured for subsequent authentication operations.

   The current mechanisms specified in the FIPS 201 document are an excellent start in this direction. However, they are too heavily oriented toward establishing or confirming a set of information pertaining to the identity of the applicant and not enough toward streamlining the biometric capture and vetting that is the primary focus of the identity system.

2. ***Biometric Enrollment*** - FIPS 201 should be based on the use of biometric markers through which the identity of individuals is established. Consequently, the initial procedure for enrollment of an individual into a federal-government-wide identification system should be to capture the necessary biometric images and conduct a one-to-many comparison of these images to individuals already "identified" so as to confirm that each individual is enrolled once and only once. The most secure (and thus trustworthy) mechanism for this identification process is to maintain a single biometric registry comprised of all applications for federal government employment or contractor status. Once the necessary biometrics have been captured from the individual and the uniqueness of these biometrics confirmed, the attribution of other characteristics to this identity is a process (or processes) that can occur rather asynchronously over an arbitrary period of time. That is, the establishment of identity and the establishment of an employment status with the federal government are orthogonal operations. As long as identity is established first, then determination of employment status, or any other attributes of identity (name, address, date of birth, medical history, education history, prior employment, etc.) can be validated at some subsequent time.

   It appears to us that HSPD-12 establish two major needs: (a) be able to reliably authenticate the identity of a person over time and distance, and (b) as a secondary goal, convey the fact that the person so authenticated is an employee or contractor of the federal government. Both of these can be accomplished in a rather straightforward fashion with current technology. What is more difficult,

and is not a requirement stated by HSPD-12, is how to answer the question "Should this person be an employee or contractor of the federal government?"

3. ***Backward Compatibility*** – Since the initial development of the GSA Common Access Card Requirements in 1999, it has been clear that interoperability among identification systems deployed by various agencies of the federal government was a significant issue. With the initial round of authorization awards to potential vendors of Common Access Card systems went a mandate for the providers and agencies to develop interoperability standards. This mandate was reiterated by the OMB during 2003. Consequently, the issuance of HSPD-12 should have found a solid interoperability standard in place that could immediately suffice to satisfy the standards requirements. It is arguable whether this has actually been the case. In particular, the variances currently found in both the identity validation data models for electronic authentication systems and the token issuance and operational management functions currently in place, leave much to be desired for a government-wide interoperable identity system.

   In defense of the current CAC deployments, there is significant functionality that allows for the adoption of true interoperability standards without requiring the deployment of new tokens. The use of the Java Card virtual machine platforms and the Global Platform card management platform are noteworthy capabilities on which to build interoperability standards. The inclusion of this technology in SP 800-73 is an excellent start. However, until such time as the full measure of token issuance and token management can be integrated into the FIPS 201 standard and the SP 800-73 specification, a *carte blanche* should not be given to current deployments. Moreover, the architecture and designs of middleware used to connect application systems to tokens must be subject to the same oversight as are cryptographic operations through the FIPS 140-2 certification process. In particular, a thorough review of the design approaches used by middleware for such things as "PIN escrow" operations that are not compatible with secure identity authentication operations is required.

   The true measure of success regarding interoperability of identity tokens is the degree of commonality of authentication protocols used. To date, there is no existing standard for the variety of electronic authentication protocols possible within various government agencies. Without this standard (or set of standards), it is difficult, if not impossible, to determine the sufficiency of existing deployments.

   Finally, while procurement practices are not the specific purview of HSPD-12, the legal grounding of NIST practices would seem to mandate a level playing field for vendors that seek to provide products in the identification system framework. To this end, it is important that the standards defined by FIPS 201 and SP 800-73 should not be based on gratuitous "intellectual property" that preclude the full and open competition among vendors and the expectation that interoperable components can therefore be provided by multiple vendors without requiring

them to be subject to arbitrary licensing practices. Consequently, it is important that any intellectual property claims related to existent or future identification systems be fully and openly stated as early in the standards development process as possible. Certainly, the goal in establishing the standards should be to include technology prejudiced by license requirements in only the most special circumstances.

4. ***Forward Evolution*** – Deployment of an identification system for federal employees and contractors will, by definition, include millions of individual identities and will remain in operation for many years, perhaps indefinitely. It is to be expected that the state-of-the-art for the components of identification systems, or the identification systems themselves, will evolve over this time period. At any point in time, it is further expected that the federal identification system will continue to operate reliably and securely and that it will encompass new technology and/or techniques in a consistent and coherent fashion. Consequently, the system must be able to smoothly evolve in the face of changing technology and/or threat profiles. To do so, mechanisms for such evolution must be incorporated in the standard(s) at the earliest possible opportunity.

   The SP 800-73 document, by encompassing ISO/IEC 7816, the Java Card specification and the Global Platform specification lays the groundwork for this evolutionary framework. However, the evolutionary mechanisms should be more thoroughly stated in this document. Further, the FIPS 201 standard should be expanded to encompass the evolving certification needs of identification systems as well.

5. ***State-of-the-Art Identity Technologies*** – HSPD-12 places the onus on NIST to identify the most applicable technologies to use for secure identity authentication and to establish standards to encompass those technologies. This is not necessarily a mandate to develop technology specific standards, but rather to use state-of-the-art technologies as the "straw man" through which to identify what is acceptable from a security viewpoint versus what is reasonable from a technology viewpoint. To this aim, we can identify the current state-of-the-art in a number of identify related areas.

   To counter the threat of counterfeiting and fraudulent identity, a biometric marker is the best mechanism to authenticate the unique identity of an individual. Taking accuracy and privacy concerns into consideration, the iris scan is the best biometric characteristics to use. Taking equipment costs and cultural acceptance into consideration, the fingerprint may well be the best.

   A biometric "one-to-many" match is the best mechanism for establishing unique identity within an arbitrary population of people. Iris scans offer a false positive rate of about 10^{-6} versus 10^{-4} for a fingerprint. To attain an identification accuracy of 10^{-10}, it will probably be necessary to use multiple biometric compares to reach true "identify" levels, but a single compare should be good enough for a "verify"

level. That is, only the enrollment process needs the extremely high accuracy rate as part of the identification process; subsequent processes are aimed only at verification.

A dedicated, secure authentication platform is the best authentication mechanism; that is a certified (complete) system in a secure location and containing or connected to a single database with all known identities against which an identification (one-to-many) match of new individuals is made.

A public key infrastructure (PKI) is the best means of projecting strongly authenticated identity beyond an authentication platform. Within a PKI, the most cost-effective means of storing a private key is a smart card; cost-effective includes the concept that an individual has their private key for use where they want to use it.

The best cardholder verification mechanism (to allow use of a public key) is biometric with image capture and match done on a secure authentication platform that is authenticated by the card. The second best cardholder verification mechanism (and, actually the best "portable" mechanism) is biometric with image capture done on a certified platform (assumed under control of the cardholder) authenticated by the card and match done on the card. PIN based token bearer authentication can be included in authentication protocols for certain situations, but should not be included in the highest trust requirement areas.

The least secure and yet most commonly used authentication mechanism is human match of a biometric and/or credential (i.e. "Are you the person whose face is on the card? Is this a valid card?) The second question of this protocol is rarely asked because it is very hard to implement.

These mechanisms define what is readily available through identity technology today. The FIPS 201 and SP 800-73 standards should accept no less than the capabilities offered by this technology. In particular, the practices defined in FIPS 201 should encompass these current state-or-the-art mechanisms and should provide processes through which the state-of-the-art can evolve over time.

6. ***Smart Card Architecture*** – A smart card is the best available technology for a personal identity token. Such a token can convey one or a set of biometric characteristics through which the identity of the individual can be authenticated. The smart card also provides a secure information storage and processing capability that can be used to assist in the identity authentication of the cardholder as well as the projection of this identity into a computer system or network. In addition, the smart card provides a secure storage and conveyance mechanism for attribute credentials that establish information or permissions that are connected to the identify of the cardholder. There are three sets of standards that should be recognized by and incorporated into the FIPS 201 and SP 800-83 standards: (a) the ISO/IEC 7816 standard defining the semantics of basic smart card operations,

including file oriented, named data storage and retrieval (b) the Java Card specification for post-issuance programmability of smart cards, and (c) the Global Platform specification for secure card management and operations. As noted previously, many aspects of these standards are included, but the level of specificity should be enhanced.

7. ***Sharing Data Among On-Card Applications*** – The Java Card specification is weak with respect to the secure sharing of data among different code segments (applets) installed on a smart card. A preferable mechanism is to provide to each on-card applet a file storage interface that makes use of security mechanisms such as those found in the ISO/IEC 7816 standards. This is an area of some ambiguity within the current version of the SP 800-73. It would seem to imply that such a file system is mandatory; in fact, it should merely be an option for sharing data among different applets. Further, an applet (on-card) API should be defined to support this data sharing option. This is not currently found in the SP 800-73 specification.

8. ***Authentication Protocols*** – A variety of authentication protocols are used in smart card identity systems today; in fact, there are generally many variants of each variation. The FIPS 201 standard needs to include a detailed set of acceptable authentication protocols, including token bearer interactions. It is through the specification of authentication protocols that the acceptable level of identity authentication for the particular situation can be determined. Consequently, not only should a variety of authentication protocols be defined, but a mechanism should be defined through which an acceptable level of authentication can be negotiated.

   The suitability of a physical connection mechanism between a token and a sentinel platform should be specified through the acceptable authentication protocol(s). Specifically, there are certain protocols that are just not currently feasible through a contactless interface, either because of the lack of necessary I/O opportunities or the lack of adequate processing capacity on the token. The suitability of an authentication protocol should be based on the desired security level and this should not be compromised simply for the sake of convenience. Inadequate security in a specific situation should never be accepted merely for the sake of convenience.