X-Sieve: CMU Sieve 2.2
From: "Regan, Thomas (LNG-WAS)" <thomas.regan@lexisnexis.com>
To: "'DraftFips201@nist.gov'" <DraftFips201@NIST.GOV>
Cc: "W. Curtis Barker (wbarker@nist.gov)" <wbarker@NIST.GOV>,
"Donna Dotson (donna.dotson@nist.gov)" <donna.dotson@NIST.GOV>,
"Willox Jr, Norman A. (LNG-WAS)" <norman.willox@lexisnexis.com>,
Abby Stewart <astewart@jdstrategies.com>
Subject: Comments on Public Draft FIPS 201
Date: Thu, 23 Dec 2004 13:20:06 -0500
X-Mailer: Internet Mail Service (5.5.2657.72)
X-Scanned-By: MIMEDefang 2.38
X-MailScanner:
X-MailScanner-From: thomas.regan@lexisnexis.com

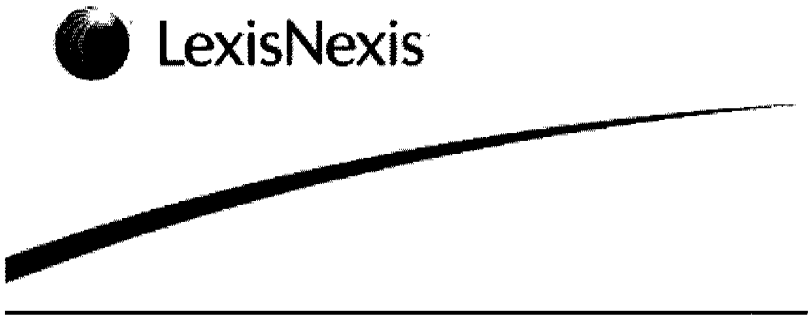
Please find attached additional comments by LexisNexis regarding FIPS 201. For ease of reference, I am also attaching our original comments of October 29.

Thank you for your kind consideration.

Thomas M. Regan, Esq.
Executive Director for Privacy and Regulatory Affairs
LexisNexis
1150 Eighteenth Street, NW
Suite 600
Washington, DC 20036
Office: 202-857-8281
Mobile: 202.441.5922


PIV_Draft_2_12.23.04.tmr.2.doc


NIST.ltr.2.1029041.doc



Norman A. Willox, Jr.
Chief Officer for Privacy, Industry and Regulatory Affairs
LexisNexis
1150 18th Street, N.W.
Washington, DC 20036
202-776-1306
202-857-8233 (fax)
norman.willox@lexisnexis.com

December 23, 2004

Shashi Phoha, Director
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive
Stop 8900
Gaithersburg, MD 20899-8900

Re: FIPS PUB 201: Personal Identity Verification (PIV) for Federal Employees and Contractors- PUBLIC DRAFT ver. 1.0 (FIPS 201)

Dear Director Phoha:

Please accept the following as supplementing our original comments of October 29, 2004 and as responding to discussions which Thomas M. Regan of our office had on December 6, with W. Curtis Barker, Donna Dotson, William Burr and Tim Polk. Specifically, we respectfully request that NIST consider two previously government-promulgated documents as supporting our strong recommendation that Section 2.2 of FIPS 201, Identity Proofing and Registration, be revised to include, at all four levels, use of commercial database solutions to enhance the identity authentication process. These documents are:

- The Customer Identification Program (CIP) regulations jointly issued on May 9, 2003 by the Department of the Treasury, the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Commodity Futures Trading Commission and the Securities and Exchange Commission, 68 Fed. Reg. 25090; and
- The Identity Proofing process of the General Services Administration's Access Certificate for E-Services (ACES) program.

Introduction

Initially, LexisNexis wishes to again express its thanks to the National Institute of Standards and Technology (NIST) for continuing its open dialogue with the public, through the submission and review of comments and in-person meetings, on FIPS 201.

In its capacity as a premier information solutions company, providing identity authentication solutions to both governmental agencies and commercial entities, LexisNexis submitted comments to NIST on the initial PIV Draft Standard on October 29, 2004. These preliminary comments focused primarily on the need for the Draft Standard to bolster its identity proofing and vetting ("enrollment") phase. Following submission of those comments, on December 6, LexisNexis had the fortunate opportunity to meet with NIST personnel responsible for managing the identity proofing requirements in the Draft Standard.

At the December 6 meeting, LexisNexis emphasized the need for NIST to greatly enhance the identity proofing and vetting phase of the PIV Standard by incorporating language into the Standard providing a method for non-documentary, information-based identity authentication. LexisNexis further presented information on the CIP regulations promulgated pursuant to Section 326 of the USA PATRIOT Act, Verification of Identification, 31 USC §5318(l). These regulations provide minimum requirements for financial institutions to implement Customer Identification Programs to authenticate individuals opening an account, thorough the use of documents and/or non-documentary (i.e., information-based) verification methods.

Another government-initiated process for authenticating, or identity proofing, individuals, is the GSA program "ACES," which facilitates secure electronic access to government information and services using public key infrastructure/digital signature technology. (A comprehensive discussion of ACES can be found at the GSA website, www.gsa.gov.)

Both the CIP regulations and the ACES program, and their applicability to Section 2.2 of FIPS 201, will be discussed below.

Section 326 Regulations

Section 326 of the USA PATRIOT Act is found within Title III, entitled "International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001." Section 326 requires the Secretary of Treasury to prescribe regulations setting forth minimum standards for financial institutions and their customers regarding the identity of a

customer in connection with the opening of an account at a financial institution. The minimum requirements mandate that financial institutions create reasonable procedures for: 1) verifying the identity of any person seeking to open an account to the extent reasonable and practicable; 2) maintaining records of information used to verify a person's identity; and 3) checking terrorist watchlists provided by any government agency to determine whether a person seeking to open an account is on a list.

The Department of Treasury, along with other financial regulatory bodies, promulgated regulations implementing Section 326 of the USA PATRIOT Act on May 9, 2003. When promulgated, The Department of Treasury proclaimed the purpose of the regulation as to "[p]revent money laundering, terrorist financing, identity theft and other forms of fraud."[1] This purpose is strikingly similar in importance to the aims of NIST for FIPS 201.

The Section 326 regulations require each financial institution to implement a written Customer Identification Program that includes risk-based procedures to verify the identity of each customer to the extent reasonable and practicable to help the institution form a reasonable belief that it knows the true identity of each customer.[2] The CIP must include "identity verification procedures."[3] As part of the identity verification procedures, the regulations require, among other things, that certain customer information be provided, to include, at a minimum, name, date of birth, address and an identification number (for a US person, this would be the taxpayer number, i.e., a social security number).[4] In addition, the regulation mandates that the customer-supplied information be verified through documentary, non-documentary or, as determined by the circumstances, some combination of both.[5]

With regard to documentary verification of customers, the regulations specify that "[f]or an individual, unexpired government-issued identification evidencing nationality or residence or bearing a photograph or similar safeguard, such as a driver's license or passport" can be used.[6]

For customer verification through non-documentary methods, the CIP states as follows:

> These methods may include contacting a customer; ***independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other***

---

[1] Department of Treasury, Office of Public Affairs, "Treasury and Federal Financial Regulators Issue Final Privacy Act Regulations on Customer Identification," April 30, 2003. (www.treas.gov/press/releases/js335.htm).
[2] 31 CFR § 103.121(b)(1-2) (Department of Treasury Regulation).
[3] Id. at § 103.121(b)(2).
[4] Id. at § 103.121(b)(2)(i).
[5] Id. at § 103.121(b)(2)(ii).
[6] Id. at § 103.121(b)(2)(ii)(A)

source; checking references with other financial institutions; and obtaining a financial statement. (Emphasis added).[7]

By providing a method through which financial institutions can and should use public databases to verify an individual's identity, the Section 326 regulations acknowledge that there are times when conducting a review of source documents, or even conducting a limited background search, is simply not enough to accurately verify an individual's identity. In fact, the American Bankers Association, the largest association of US banks, has specifically endorsed to its members the use of the LEXIS information-based identity authentication solution, as a means for meeting the Section 326 CIP regulatory requirements.

From all accounts, the CIP regulation, which had a compliance date of October 1, 2003, has worked successfully. It is respectfully submitted that it should therefore be a model for the identity proofing provisions of FIPS 201.

ACES Identity Proofing

The program adopted by the Government Services Administration for secure electronic access to government information and services using public key infrastructure/digital signature technology is Access Certificate for E-Services (ACES). Among a variety of benefits, GSA asserts that ACES "provides governmental agencies with the capability to authenticate electronic digital services utilizing secure e-commerce." GSA's confidence in ACES has resulted in its making Delegated Procurement Authority (DPA) for ACES available to interested agencies. The DPA enables agencies to order directly off the ACES contract.

An essential component of ACES is "identity proofing." On this point, GSA includes as identity proofing components the following:

Identity Proofing

- Online Registration
- Verification that identity exists
- Verification the requestor owns identity
- Out of band notification
- **Multiple independent source databases**
- In-person antecedent
- Government or vendor provided

(Emphasis added.)

[7] Id. at § 103.121(b)(2)(ii)(B)(1)

The significance of the use of "multiple independent source databases, is further emphasized by Digital Signature Trust Company (DST), an industry partner with GSA in the ACES program. In its "Public Key Infrastructure White Paper," at p.10, DST describes its identification process, within its three levels of personal authentication, silver, gold and platinum, as containing the following elements:

- Collection of identity information, public key, pass phrase from applicant during registration;
- **Checking of registration information against multiple, mutually exclusive and reliable data sources**
- (For Gold and Platinum level) an "in-person" authentication via a trusted individual (i.e. Notary) will be required.
- Out of band delivery of activation code to a verified data point. "Out of band" refers to communication via an offline mechanism linked to a verified piece of data (e.g., physical address or phone number)
- Two factor authentication at certificate issuance. (First factor: hashed passphrase provided during registration, second factor: activation code distributed to user out of band). Emphasis added.

It is clear form the above that GSA and its industry partner, Digital Signature Trust, place significant reliance on receiving data from multiple sources in order to verify the information supplied from the PKI applicant. The reason is quite simple, and that is that in the absence of a reliable trusted credential, the only basis for independently verifying that a person is who they say they are is through information. There exist commercial entities, (like LEXIS), that not only provide reliable, fast and efficient sources of the type of information needed, specifically names, addresses, telephone numbers, social security numbers, etc., but do so in solution that can assist in resolving apparent discrepancies.

To the extent that NIST agrees that information-based identity authentication is essential for FIPS 201, we also strongly recommend that it be accompanied by privacy principles that not only insist upon compliance with existing law but also upon common notions of fair information practices. LEXIS has consistently been an industry leader in establishing privacy best practices and would suggest its Data Privacy Policy as a guide for FIPS 201 implementation.

Conclusion

Obtaining a PIV card will provide agency employees and contractors admittance into protected government facilities and secure information systems, regardless of the Position Security Level at which he or she is employed. As such, LexisNexis believes that the Registration Authority within each agency who conducts the checks on applicants should be required to access the most effective, accurate, up-to-date data and technology to make the decision to provide a credential, using both documentary ***and*** non-documentary methods. Employing policy-driven information-based identity authentication will provide agencies with that opportunity.

Therefore, LexisNexis recommends that NIST adopt language similar to that in the CIP regulations implementing Section 326 of the USA PATRIOT Act, and in GSA's ACES program, as part of the minimum requirements for FIPS 201 VIP identity proofing.

LexisNexis again thanks NIST for the opportunity to comment further on the PIV Draft Standard and looks forward to a continuing dialogue on this very important subject.

Respectfully yours,

s/ Norman A. Willox, Jr.

Norman A. Willox, Jr.
Chief Officer for Privacy, Industry and
Regulatory Affairs
LexisNexis
1150 18th Street, N.W.
Washington, DC 20036
202-776-1306
202-857-8233 (fax)
norman.willox@lexisnexis.com

October 29, 2004

Shashi Phoha, Director
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive
Stop 8900
Gaithersburg, MD 20899-8900

Re: FIPS PUB 201, Personal Identity Verification Standard-Draft

Dear Director Phoha:

Please consider the following comments that we present concerning the above:

Introduction

As a premier information solutions company, providing identity authentication solutions to both governmental agencies and commercial entities, LexisNexis appreciates the opportunity to provide the National Institute of Standards and Technology (NIST) and Department of Commerce with these comments on FIPS PUB 201, the Federal Personal Identity Verification (PIV) Draft Standard ("PIV Standard").

For 30 years, LexisNexis has provided various information solutions that have aided in authenticating identities, locating people and assets, protecting the critical infrastructure, conducting background screening and supporting a variety of other risk management initiatives. LexisNexis has worked closely with Federal and state government agencies in promoting national security, counter terrorism and law enforcement activities and with major law firms, financial institutions, utilities, insurance companies and Fortune 500 companies in protecting against identity theft, responding to fraudulent transactions, evaluating financial risk and promoting responsible information sharing. In the area of identity management, issues of identity assurance, data modeling and privacy and security safeguards have become company hallmarks. It is with this background that LexisNexis respectfully offers its assistance to NIST in this very important endeavor.

The PIV Standard is being developed by NIST pursuant to Homeland Security Presidential Directive-12 (HSPD-12), issued by President Bush on August 27, 2004. HSPD-12 directed the Secretary of Commerce to promulgate, by February 25, 2005, a government-wide standard for the Federal government's issuance of "secure and reliable forms of identification" to its employees and contractors.[1] In response, NIST released the subject PIV Standard which specifies a framework and technical requirements for a comprehensive Federal Personal Identity Verification (PIV) card. With the release of the draft standard, NIST requested comments by October 30. These comments are being submitted pursuant to that request. LexisNexis welcomes the opportunity to work with NIST as this standard is further refined.

LexisNexis Recommendation

An important component of the draft PIV standard is highlighted in Section 5, entitled "PIV Issuance," which explains how a PIV application is processed (hereinafter "enrollment phase").[2] As explained below, in order to fully comply with HSPD-12 and to help agencies effectively, timely, and cost efficiently implement a PIV card, LexisNexis recommends that NIST incorporate the use of information-based identity authentication into the enrollment phase. Using information-based identity authentication would allow the issuing agencies to verify, validate and authenticate the information provided by PIV card applicants and thereby help to ensure, prior to the issuance of the card, that the applicant is who he or she claims to be.

Information-Based Identity Authentication

Information-based identity authentication determines identity on the basis of identifying information provided by an applicant, through the use of qualified databases and commercially developed scoring models and algorithms. In this way, it supplements the process of verifying the applicant's identity through authenticating the credentials provided by the applicant.

In the past, absent direct contact with employers, references, neighbors and others, an entity attempting to determine the identity of a person, previously unknown to the entity, would have to do so solely through the reliability of the person's credentials, such as a birth certificate, driver's license, social security card, etc. If the applicant matched the entire set of source documents presented at the time of registration, a credential was granted. However, as recently discussed in a published white paper entitled *Identity Fraud: A Critical National and Global Threat*, "[i]t has been widely conceded that driver's licenses and similar credentials are easily counterfeited or obtained fraudulently. [Therefore], in the absence of a universally accepted credential, the only practical solution must be to employ an information-based authentication system."[3] With identity theft plaguing our society and fears of terrorists using false or fictitious identities

---

[1] To view HSPD-12, please visit http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

[2] The "enrollment" or "application" phase is referred to by NIST in the PIV Draft Standard as the "identity proofing" phase.

[3] *Identity Fraud: A Critical National and Global Threat*, Dr. Gary Gordon, Professor Utica College, and Norman Willox, Jr. Chief Officer for Privacy, Industry and Regulatory Affairs, October 2003, page 27. To view, please visit http://www.ecii.edu/identity_fraud.pdf.

recognized as a real threat by the 9/11 Commission, it is essential that our identity management systems incorporate all available technologies in assuring that an applicant is who he or she claims to be.[4]

Information-based identity authentication employs a three-tiered approach to give a credentialing provider as much assurance as possible concerning the authenticity of an applicant's identity. The first tier, or Level One, is "validation."[5] Validation is the lowest level of risk management and serves two purposes: 1) to determine if the identifying information presented by an individual is real and not fabricated, and 2) to determine whether the information conforms to an established format. To check whether the information is real and not fabricated, a table or schedule of records is consulted. "If the identifier provided by the individual, such as an address, phone number, or date of birth satisfies an existing logic or format, then the identifier is considered to be 'real.'"[6]

Ascertaining whether an identifier conforms to an established format involves determining if the data set presented matches the code established for that particular identifier (e.g., the first three digits of a Social Security Number represent the state where the card was granted and, since most people born in the United States obtain a social security number at or shortly after birth, the state indicated by these digits should match the state provided by the applicant as the place of birth.).[7]

Level Two of information-based identity authentication is called "verification." Identity verification analyzes whether the information provided by an applicant belongs together, whereas validation looks at the information in isolation.[8] Determining whether the information belongs together is accomplished by the parallel searching of various databases such as public records, change of address requests, phone numbers, etc. As explained in *Identity Fraud: A Critical National and Global Threat,* "If a person supplies his name, address, phone number, and Social Security Number on an application, a search is constructed to confirm whether all four identifiers appear in the given combination in several databases."[9] If the identifiers in the given combination match the data as it appears in multiple databases, then the information is verified. Crucial to this step is an evaluation of the databases to be used for comparison matching. Those that are refreshed most often with accurate and comprehensive data should be chosen for the verification phase.[10]

Level Three is Authentication. Authentication involves the use of specifically tailored modeling and scoring algorithms that are used to provide assistance in determining the probability that the claimed identity of an individual is authentic. Once an applicant provides the requested information, the authentication engine models and scores that

---

[4] *9/11 Commission Report*, July 22, 2004. To view, please visit http://www.9-11commission.gov/report/911Report.pdf.
[5] *Identity Fraud: A Critical National and Global Threat,* at 32.
[6] Id.
[7] Id.
[8] Id.
[9] Id.
[10] Id.

information. There are three potential scores that can result from the authentication engine and that are used to ultimately make a decision about the authenticity of an individual's claimed identity; an affirmative score, meaning the person's claimed identity has been authenticated based upon the rules set for a particular application; a negative score, representing an unsatisfactory authentication score; and an "exception" score, meaning the process is inconclusive on authentication.[11]

Information-Based Identity Authentication and the PIV Standard

For the reasons that follow, § 5.1 of the PIV Standard appears to partially incorporate an information-based process, but without receiving any of the benefits that are found in information-based identity authentication. These benefits include: speed, with processing capability measured in seconds; reliability, with commercially demonstrated proof of effectiveness; cost, with authentication transaction charges of less than one dollar; and privacy sensitivity, with privacy impact limited to accessing databases comprised of commercially available identifying information only.

The first weakness appears in Position Sensitivity Level (PSL) 1. It is totally devoid of any information-based checks. It relies solely on document authentication, and no attempt is made to verify the information provided by the applicant on Form I-9. Given the inherent unreliability of the referenced documents (drivers license, etc), it is respectfully submitted that the standard fails to provide a meaningful process for identity authentication and, for that reason, information-based identity authentication is necessary to bolster the PSL 1 identity authentication process.

Secondly, for PSL 2 and PSL 3 of § 5.1, the National Agency Check and Inquiries (NACI) process requires written inquiries be sent by the issuing authority to the applicant's current and past employers, schools attended, references and local law enforcement agencies. Although such checks might prove helpful in determining the applicant's trustworthiness and suitability for security clearances (an important process and one which LexisNexis also has particular expertise), it provides limited benefit in authenticating his or her identity. Information-based identity authentication would provide a proven means for verifying that the applicant is who he or she claims to be. Further, to the extent that employer, educational and residential information is deemed necessary as part of the identity authentication process, much of it can be obtained through publicly available databases, without having to resort to making written inquiries, with the attendant time and cost involved.

Thirdly, the credit check requirement of PSL 3 has limited bearing in determining the applicant's identity and what little assistance it provides is contained in the identifying information on the report, all of which is contained in the information-based identity authentication process. Further, since the balance of the credit report provides no additional assistance in determining the identity of the applicant, serious questions arise concerning the privacy impact associated with obtaining such information, let alone the inefficiencies associated with collecting significant amounts of unneeded information.

---

[11] Id.

Finally, the in-person interviews, called for in the Limited Background Investigation (LBI) and the Background Investigation (BI) of PSL 4, if done properly, are undoubtedly the most effective means of acquiring information to authenticate the applicant's identity. However, since the cost of doing a BI or LBI, and the time needed for their performance, are so taxing, they undoubtedly will be reserved for a very small percentage of the applicant pool. Information-based identity authentication can undoubtedly reduce the time and resources needed to perform a PSL 4 identity authentication, by helping to focus limited resources on those areas of an application that appear to warrant scrutiny.

In the final assessment, there undoubtedly must be a fine balance struck with the competing interests of effectiveness, time, cost and privacy impact. It is respectfully submitted that the automated process of information-based identity authentication will provide substantial assistance in properly striking that balance and for that reason it should be incorporated into the enrollment phase of the process.

Conclusion

Because the PIV smart card will serve as the gatekeeper for access to Federal government facilities and information systems, its enrollment process needs to be as robust as possible, but also capable of being applied efficiently and in a privacy sensitive manner. Therefore, LexisNexis recommends that NIST incorporate information-based identity authentication in the PIV enrollment process. Specifically, information-based identity authentication should be used for federal employee and contractor positions in PSL levels 1 2 and 3 because the document review and limited background check required by the draft standard fails to incorporate an information-based system that would properly assess the identifying information submitted by the applicant. It should also be used for PSL 4 applicants to help focus the investigative inquiry into those areas suggested by the information-based identity authentication process.

We greatly appreciate the opportunity to provide these comments to the NIST PIV Draft Standard and are willing to assist NIST in any way in this very important effort. Please feel free to contact me with any comments or questions.

Respectfully submitted,

s/ Norman A. Willox, Jr.