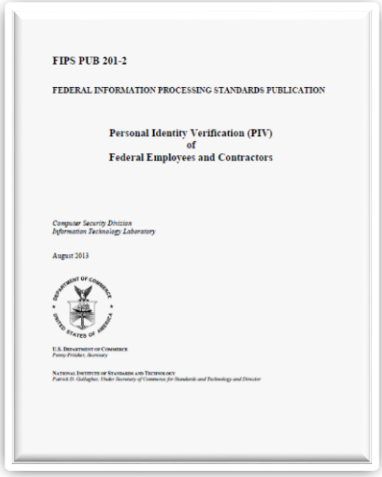
Consullition
Consultancy Coalition

Stop Issuing Secure Credentials to Imposters!

Much has been said about the difficulties in screening persons for possible imposter fraud or security concerns based upon use of current identity documents like birth certificates, driver's licenses or passports. The most often reasons given are the lack of standardization of security features and the layout for these documents. This criticism is focused on the inability of even a trained person to recognize valid documents and the specific parameters for each of these documents. In this paper, the value of machine screening of the identity documents in circulation and the requirement for a standardized metric for adjudication of the identity assurance process. The distinction is between human screening and the power of machine processing. The diversity of the identity documents and the issuer's attempts to exert their own unique identity for their documents is actually a benefit to machine screening. The rich variety of specific layout and production characteristics provide many examination points for evaluation. The processing power, storage capacity, and imaging options, only recently available at a reasonable price point, make real-time examination of all of the unique properties and a subsequent risk analysis of the results a practical identity authentication approach.


FIPS PUB 201-2

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Personal Identity Verification (PIV)
of
Federal Employees and Contractors

Computer Security Division
Information Technology Laboratory

August 2013

U.S. DEPARTMENT OF COMMERCE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Although published in August 2013, the Federal Information Processing Standards (FIPS) 201-2 was released in September 2013. The *Key Issue for this paper is the standard* Recommends Electronic Verification of source documents used to obtain secure credentials. The first concept noted in the standard is: *"...Authentication of an individual's identity is a fundamental component of physical and logical access control processes..."*

This citation sets the stage for the core theme of the standard. additionally, it states: *"...An accurate determination of an individual's identity is needed to make sound access control decisions..."*

FIPS 201 was developed and published as directed by Homeland Security Presidential Directive 12 (HSPD-12). It established the requirements for a common identification standard for identity credentials issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. The strength of this initiative is summarized by this quote:

"...The strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential..."

The first phase of Identity proofing was that a Card issuing organizations must use the identity source documents listed on the United States Immigration document I-9, Employment Eligibility Verification. In this revision, FIPS 201-2 state: **"... It is recommended that departments and agencies perform electronic verification of identity source documents, where possible..."**

This revision of FIPS 201 will assist with the Stopping the Issuance of Secure Credentials to Imposters