A Comparison of PIV, PIV-I and CIV Credentials

Homeland Security Presidential Directive 12 (HSPD-12) mandates a standard for a secure and reliable form of identification to be used by all Federal employees and contractors. Signed by President George W. Bush in August 2004, HSPD-12 initiated the development of a set of technical standards and issuance policies (Federal Information Processing Standard 201 [FIPS 201]) that create the Federal infrastructure required to deploy and support an identity credential that can be used and trusted across all Federal agencies for physical and logical access.

The policy, processes and technology in FIPS 201 also reflect specifications defined in a number of other special publications (SPs) specifically written for FIPS 201 and build on other National Institute of Standards and Technology (NIST) standards and SPs that support best practices. Importantly these standards also build on international and national standards from organizations such as the Internet Engineering Task Force (IETF), the International Telecommunications Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE), the International Organization for Standardization (ISO), the Organization for the Advancement of Structured Information Standards (OASIS) and others.

Two additional credentials have been defined – the Personal Identity Verification-Interoperable (PIV-I) and Commercial Identity Verification (CIV) credentials – with the goal of taking advantage of the infrastructure created by the Federal government's PIV program. The policy, process and technology applied to each of these credentials result in a level of assurance and interoperability, and ultimately the extent to which it can be used and trusted in its intended application. As shown in the table below, the policy and process around PIV and PIV-I enable the interoperability and trust of the credential. The CIV credential definition was developed to define a commercial credential that could take advantage of the PIV infrastructure. Identity and credential infrastructure requires an additional investment in order to adhere to and maintain these policies and processes. In return, users and organizations can access identity and credential services in the commercial arena with many of the advantages enabled by the creation of the PIV infrastructure.

	PIV	PIV-I	CIV
Policy			
Breeder documents	Follows FIPS 201	Follows FIPS 201	Follows the issuing organization's policies
Background checks	National Agency Check with Investigation	None required, directly impacts level of suitability for access	Follows the issuing organization's policies
Process			
Application Adjudication Enrollment Issuance Activation	Follows FIPS 201, including separation of roles, strong biometric binding	Follows Federal Bridge cross-certification certificate policies[1] Follows SP 800-63-1 for Federal issuance Based on FIPS 201, including separation of roles, strong biometric binding	Follows the issuing organization's policies For Federal relying parties, follows SP 800-63-1
Technology			
Card data model	Must follow SP 800-73	Must follow SP 800-73	"Follows" SP 800-73 (recommended)
Current primary credential number	FASC-N[2] (requires Federal agency code)	UUID (no Federal agency code required)	UUID (recommended) (no Federal agency code required)
Object identifiers	Federal Bridge	Federal Bridge	Organization Internet Assigned Number Authority (IANA) (if exists)

[1] http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

[2] The FASC-N contains a federal agency code which is managed by NIST. PIV-I and CIV credential numbers (UUIDs) are generated by the issuing organization. See NIST SP 800-87 for additional information.

	PIV	PIV-I	CIV
Types of Federation and Levels of Assurance			
Trustworthiness	Trusted identity, credential and suitability	Trusted basic identity and credential but not suitability	Trusted credential only within the issuing organization.
Trust among organizations	Federal Bridge	Clustered through Federal Bridge	Clustered alone
Origin			
Organization	NIST	Federal CIO Council	Smart Card Alliance Access Control Council[3]
Defining documents	FIPS 201, SP 800-73 and other related NIST publications	Personal Identity Verification Interoperability for Non-Federal Issuers[4] FICAM PIV-I FAQ[5]	The Commercial Identity Verification (CIV) Credential–Leveraging FIPS 201 and the PIV Specifications[6]
Motivation	HSPD-12	Interoperable credential for organizations doing business with the government and for first responders	Commercial credential that could take advantage of the PIV infrastructure
Markets			
Organizations that may issue and/or use the credential	Federal agencies	Federal agencies Federal contractors Commercial organizations doing business with the Federal government State and local governments Critical infrastructure providers First responder organizations Commercial organizations who are part of an industry initiative and require an interoperable, trusted credential	Commercial organizations seeking a credential for use for their employees, subcontractors, non-employee visitors and customers Federal agencies who accept credentials with medium hardware assurance[7]
Resources that the credential may be used for	Credential can be used in a wide range of both employment-related and consumer-based transactions. Examples include physical access, logical access[8], mass transit, and closed loop payments.		

About this Brief

This brief was developed by the Smart Card Alliance Access Control Council to provide an easy-to-use comparison of PIV, PIV-I and CIV credentials. The Access Control Council is focused on accelerating the widespread acceptance, use, and application of smart card technology for physical and logical access control. The group brings together, in an open forum, leading users and technologists from both the public and private sectors and works on activities that are important to the access control community and that will help expand smart card technology adoption in this important market. Additional information can be found on the Smart Card Alliance Web site, http://www.smartcardalliance.org.

[3] The Smart Card Alliance Access Control Council selected the name CIV and documented the specifications that would define a credential that was technically compatible with the PIV specifications.

[4] http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf

[5] http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf

[6] http://www.smartcardalliance.org/resources/pdf/CIV_WP_101611.pdf

[7] Requires that the CIV credential have a medium hardware certificate.

[8] Logical access includes: computer logon, digital signatures, network access, application access, data/communication encryption.