E-Authentication

Certificate Credential Assessment Profile

Business Owner: Federation Management
Creation Date:
Last Updated: 3/16/05
Version: EA-PL-0014-2.0-F
Audience: Public

Release Notes

PMO Approved

Executive Summary

This document is the Credential Assessment Profile for certificate-based credentials (i.e., public key certificates). It is part of the Credential Assessment Portfolio, as described in the Credential Assessment Framework (CAF). The reader is assumed to be familiar with the CAF. This document contains the specific criteria used to assess certificate-based Credential Services (CSs) for use in the E-Authentication Initiative.

The Federal government governs certificate-based CSs through the Federal Public Key Infrastructure Policy Authority (FPKI PA). The policy mapping determination of the FPKI PA is the basis of this profile. This document specifies the E-Authentication Assurance Levels that correspond to the FPKI PA policy levels.

Document History

See Appendix C for a detailed listing.

Editors

Chris Louden	Judy Spencer	Bill Burr
Kevin Hawkins	David Temoshok	John Cornell
Richard G. Wilsher	Steve Timchak	Stephen Sill
Dave Silver	Von Harrison	

Table of Contents

1 INTRODUCTION

This document is part of the Credential Assessment Framework (CAF) portfolio governing the assessment of credentials for use in the E-Authentication Initiative. Please refer to the CAF for an overview. Additional information about the E-Authentication Initiative is available at http://www.cio.gov/eauthentication/.

This profile specifies the criteria for certificate-based Credential Services (CSs) that authenticate public key certificates. It is based upon guidance specified in National Institute of Standards and Technology (NIST) Special Publication 800-63, version 1.0.1, which is available at http://csrc.nist.gov/publications/nistpubs/.

The E-Authentication Initiative defers governance of public key certificates to the Federal Public Key Infrastructure Policy Authority (FPKI PA). The criteria in this document are based on the findings of the FPKI PA. Approval for cross-certification by the FPKI PA means all current E-Authentication requirements have been met by the candidate certificate-based CS, for a particular E-Authentication Assurance Level. Therefore, no additional criteria are required in this CAP, at this time.

A certificate-based CS that has not had their policies mapped by the FPKI PA cannot be assessed according to this profile. More information on the FPKI PA is available at http://www.cio.gov/fpkipa/.

The overall authentication Assurance Level is determined by the lowest assurance level achieved.

2 SCOPE

The scope of the E-Authentication Initiative is remote electronic authentication of human users to Federal agency IT systems over a network. It does not address the authentication of a person who is physically present.

In addition, certificate-based authentication is limited to certificates based on asymmetric key cryptography, where the CA is cross-certified with the FPKI Architecture, or meets x509 PKI certificate policy, or federal common policy.

This profile contains requirements that must be met by any certificate-based CS based on a Public Key Infrastructure (PKI). This document contains the full set of criteria for certificate-based CSs.

3 TERMINOLOGY

This document relies on terminology defined in NIST Special Publication 800-63, version 1.0.1 ‘Recommendations for Electronic Authentication’, and the OMB ‘Guidance for E-Authentication’. See Appendix A, Glossary, for a complete listing of terms used in this context.

4 CRITERIA

4.1 Summary

	Level 1	Level 2	Level 3	Level 4
Overall Mapping		□ Level 2 FPKI	□ Level 3 FPKI	□ Level 4 FPKI

4.2 Assurance Level 1

Not Applicable

4.3 Assurance Level 2

4.3.1 Overall Mapping

Tag	Description	Suggested Evidence of Compliance	Assessment Status
Level 2 FPKI	The FPKI PA must have determined the CS maps to Basic, Citizen and Commerce Class, Medium, High or Common Certificate Policy or other policies that meet all Level 2 requirements.	Approved by the FPKI Architecture	

4.4 Assurance Level 3

4.4.1 Overall Mapping

Tag	Description	Suggested Evidence of Compliance	Assessment Status
Level 3 FPKI	The FPKI PA must have determined the CS maps to Medium, High, Common Software, or Common Hardware Certificate Policy.	Approved by the FPKI Architecture	

4.5 Assurance Level 4

4.5.1 Overall Mapping

Tag	Description	Suggested Evidence of Compliance	Assessment Status
Level 4 FPKI	The FPKI PA must have determined the CS maps to High, or Common Hardware Certificate Policy.	Approved by the FPKI Architecture	

5 REFERENCES

[OCSP] “Internet X.509 Public Key Infrastructure Online Certificate Status Profile” (RFC 2560) Feb 2002.

[PKCS #5] “Password-Based Cryptography Standard”, RSA Laboratories, v2.0, March 25, 1999

[QCP] “Policy requirements for certification authorities issuing qualified certificates”, ETSI TS 101 456.

[X.509] "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU Recommendation X.509. (03/00)

[M-04-04] The OMB E-Authentication Guidance

[SP 800-63] NIST Special Publication 800-63 version 1.0.1

Appendix A Glossary

Term	Definition
Address of Record	The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.
Approved	FIPS approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation. Approved cryptographic algorithms must be implemented in a crypto module validated under FIPS 140-2. For more information on validation and a list of validated FIPS 140-2 validated crypto modules see http://csrc.nist.gov/cryptval/.
Assurance Level	Level of trust, as defined by the OMB Guidance for E-Authentication. This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four levels of assurance are: Level 1: Little or no confidence in the asserted identity's validity. Level 2: Some confidence in the asserted identity's validity. Level 3: High confidence in the asserted identity's validity. Level 4: Very high confidence in the asserted identity's validity.
Asymmetric Keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Authentication	The process of establishing confidence in user identities.

Term	Definition
Authentication Protocol	A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority. See [RFC 3280]
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates.
Claimant	A party whose identity is to be verified using an authentication protocol.
Credential	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Note that this document uses "credential" broadly, referring to both electronic credentials and tokens.
Credential Assessment Profile (CAP)	A list of related criteria used to *assess* the Assurance Level of a Credential Service. The E-Authentication Initiative has several CAPs.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential then each one is considered a separate CS.
Credential Service Provider (CSP)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.
Cryptography	The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof. [ANSI X9.31] Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption. [NIST SP 800-2]

Term	Definition
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number.
Cryptographic Strength	A measure of the expected number of operations required to defeat a cryptographic mechanism. For the purposes of this document, this term is defined to mean that breaking or reversing an operation is at least as difficult computationally as finding the key of an 80-bit block cipher by key exhaustion that is it requires at least on the order of 279 operations.
Cryptographic Module	The set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Cryptographic Token	A token where the secret is a cryptographic key.
Digital Signature	An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.
Electronic Credentials	Digital documents used in authentication that bind an identity or an attribute to a subscriber’s token.
Federal Bridge Certification Authority (FBCA)	Allows PKIs to trust digital certificates issued by other entities that have been policy mapped and cross-certified with the FBCA. See http://www.cio.gov/fpkipa/.
Federal Public Key Infrastructure (FPKI)	Employs a BCA to harmonize policies and procedures for CAs. See http://www.cio.gov/fpkipa/.

Term	Definition
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKI Policy Authority sets policy governing operation of the FBCA and approves applicants for cross certification with the FBCA. The FBCA allows discrete Public Key Infrastructures (PKI) to trust digital certificates issued by other entities that have been policy mapped and cross-certified with the FBCA. The FPKI Policy Authority is composed of organizations that wish to interoperate and exchange digital certificates that have been signed by their Certification Authority with the FBCA. Determinations by the FPKI Policy Authority apply to the issuance of cross-certificates to approved participants but does not prescribe how those entities are to rely on digital certificates for transactions; all entities are free to accept or reject any digital certificate issued by any other entity at their sole discretion, using available FPKI Policy Authority determinations to assist in making informed decisions.
Federal Identity and Credentialing Committee (FICC)	The FICC will make policy recommendations and develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture, to include associated services (identity proofing, credential management, etc.), for the Federal Government. Objectives are: • Simplify and Unify Identity Authentication for Federal Employees • Create requirements for Physical Credentials, electronic credentials, and issuance. • Develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture

Term	Definition
FIPS 140-2	Specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The FIPS 140-2 standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.3 d) FIPS 140-2 shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract.
Identity	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
Identity Proofing	The process by which a CSP and an RA validate sufficient information to uniquely identify a person.
Man-in-the-middle attack (MitM)	An attack on the authentication protocol run in which the attacker positions himself in between the claimant and verifier so that he can intercept and alter data traveling between them.
Network	An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party).
On-Line Certificate Status Protocol (OCSP)	An on-line protocol used to determine the status of a public key certificate. See [RFC 2560].
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.

Term	Definition
Possession and control of a token	The ability to activate and use the token in an authentication protocol.
Practice Statement	A formal statement of the practices followed by an authentication entity (e.g., RA, CSP, or verifier); typically the specific steps taken to register and verify identities, issue credentials and authenticate claimants.
Private Key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.
Proof of Possession (PoP) protocol	A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password).
Protocol Run	An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant.
Public Key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See also [RFC 3280].
Registration	The process through which a party applies to become a subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP.
Registration Authority	A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Relying Party	An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.
Secure Sockets Layer (SSL)	Protocol for transmitting private documents via the Internet by using a private key to encrypt data that's transferred over the SSL connection.
Shared Secret	A secret used in authentication that is known to the claimant and the verifier. There are two durations for a shared secret: • Session (temporary) secret – duration of the secret is limited to the duration of the user session. That is, the secret is created, used, and expired during a single user authentication session. • Long-term secret – duration of the secret persists ongoing, and is used from one user authentication session to another user authentication session.

Term	Definition
Subject	The person whose identity is bound in a particular credential.
Subscriber	A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol.
Symmetric Key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.
Transport Layer Security (TLS)	An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 2246] and [RFC 3546]. TLS is similar to the older Secure Socket Layer (SSL) protocol and is effectively SSL version 3.1.
Verified Name	A subscriber name that has been verified by identity proofing.
Verifier	An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status.

Appendix B Acronyms

Acronym	Definition
ANSI	American National Standards Institute
CA	Certification Authority
CAF	Credential Assessment Framework
CAP	Credential Assessment Profile
CRL	Certificate Revocation List
CS	Credential Service
CSP	Credential Service Provider
FBCA	Federal Bridge Certification Authority
FICC	Federal Identity and Credentialing Committee
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
FPKI PA	Federal Public Key Infrastructure Policy Authority
IT	Information technology
NIST	National Institute of Standards And Technology
OCSP	Online Certificate Status Protocol
OMB	Office Of Management And Budget
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
SSL	Secure Socket Layer
TLS	Transport Layer Security

Appendix C Detailed Document History

Status	Release	Date	Comment	Audience
Release	1.0.0	07/10/03	First Release	Limited
Interim	1.3.0	12/19/03	Released for customer review with the proposal that it be accepted for publication as 2.0.0: • Reduction in tag names for token strength criteria. AND minor proofing amendments which have changed neither the semantics nor the intentions of the document. NB - this document supersedes 1.1.0, which was overtaken by release of the Nov. 2003 draft of NIST SP 800-63 and withdrawn before release.	Customer
Draft	1.5.0	1/14/05	• Added Acronyms as Appendix B. • Move definitions listing from section 3 to Appendix A because the listing is so long. • Move Executive Summary off the cover page and onto its own page immediately following the cover page. • Rework presentation to consolidate credential assessment checklist into this document (added “suggested evidence of compliance” and “status” columns).Change “levels” to “Assurance Levels” throughout, for clarity and consistency. • CP #2 – cite latest version of NIST SP 800-63. • CP #3 - Add indication that overall assurance level is determined by lowest level achieved. (§1) • CP #4 - Add clarification to Scope section that scope is limited to asymmetric key cryptography. (§2) • CP #48 – change tag names to include level reference. (§4.1, §4.3.1, §4.4.1, §4.5.1) • CP #48 and CP #68 - Deleted previous categories and replaced with “Overall Mapping” category, per NIST SP 800-63 (§4.1) • CP #49 - Add glossary listing, to reflect NIST 800-63, and terms of interest relating to Level 3 and Level 4 PKI, instead of simply referencing terminology that is listed in the CAF. • CP #57 - Delete “Interim” • CP #58 - Change citations to be “certificate” instead of “PKI” • CP #81 – Add clarification to Introduction section that approval for cross-certification indicates that the CS has met all E-Auth	FSTC Working Group for feedback, via Georgia Marsh

Status	Release	Date	Comment	Audience
			requirements – no additional criteria (i.e., tags) are required at this time. (§1) • CP #81 – change evidence of compliance, to be more precise. (§4.3.1, §4.4.1, §4.5.1) • CP #84 - change “Public Key Infrastructure” to “authentication of public key certificates” (§1) • CP #85 – change “”based primarily on” to “based on” • CP #86 - Added scope of E-Authentication as remote electronic authentication of human users…. (§2) • CP #95 - Add clarification in Introduction section that The E-Authentication Initiative defers governance of public key certificates to the Federal Public Key Infrastructure Policy Authority (FPKI PA). (§1)	
For Approval	1.6.0	1/17/05	• Add References section (§5)	CEWG
For Approval	1.7.0	2/4/05	• No changes	PMO
PMO Approved	2.0.0	3/16/05	Approved by the PMO	Public