NSTIC National Program Office Discussion Draft
STANDARDS CATALOG

Contents

Introduction

This document is a contribution from the NSTIC National Program Office to the Identity Ecosystem Steering Group Standards Coordination Committee. The document contains an illustrative list of some of the applicable standards, guidelines, policies, profiles and frameworks, and basic metadata and analysis about each.

This document is based on limited research and the collection of documents for this catalog does not reflect endorsement by the NSTIC National Program Office and likewise exclusion does not reflect non-endorsement.

SOURCE DOCUMENTS

Source Index

ABADSG, ANSI X9.62-2005, ANSI X9.63-2001, ANSI X9.63-2011, BAE Governance, BAE Overview, BAE SAML 2.0 Profiles, CertiPath CP 3.18, EV Cert 1.1, FBCA CP 2.25, FBCA Cross-certification Methodology 3.0, FICAM Privacy Guidance for Assessors, FICAM TFPAP 1.0.1, ICAM IMI Profile 1.0.1, ICAM OpenID 2.0 Profile 1.0.1, ICAM SAML 2.0 WB SSO Profile 1.0.2, IETF ID OAuth 2.0, IETF ID OAuth 2.0 Threat Model, IETF ID SCIM 1.0, IETF ID SWD, IETF RFC 2026, IETF RFC 2510, IETF RFC 2560, IETF RFC 3647, IETF RFC 4122, IETF RFC 5280, IETF RFC 5849, ISO-IEC Directives Part 2, InCommon Glossary, InCommon IAAF 1.1, InCommon IAP 1.1, Kantara Federal Privacy Criteria, Kantara IAF 1000, Kantara IAF 1100, Kantara IAF 1200, Kantara IAF 1300, Kantara IAF 1400, Kantara IAF 1600, Kantara SAML 2.0 Profile, Kantara UMA, NIST FIPS 140-2, NIST FIPS 186-3, NIST FIPS 201-1, NIST FIPS 201-2, NIST IR 7693, NIST IR 7870, NIST SP 800-130, NIST SP 800-152, NIST SP 800-63-1, NIST SP 800-73-3 Part 1, NIST SP 800-73-3 Part 2, NIST SP 800-73-3 Part 3, NIST SP 800-73-3 Part 4, NIST SP 800-76-2, NIST SP 800-79-1, NIST SP 800-85A-2, NIST SP 800-85B, NSTIC Strategy, OASIS IMI 1.0, OASIS Interop, OASIS SAML Authentication Context 2.0, OASIS SAML Bindings 2.0, OASIS SAML Conformance 2.0, OASIS SAML Glossary 2.0, OASIS SAML Metadata 2.0, OASIS SAML Profiles 2.0, OASIS SAML Protocol 2.0, OASIS TC-Process Sec 2.18, OASIS xNL 2.0, OpenID Attribute 1.0, OpenID Auth 1.1, OpenID Authentication 2.0, OpenID Connect 1.0, OpenID Connect Basic 1.0, OpenID Connect Discovery 1.0, OpenID Connect Dynamic Registration 1.0, OpenID Connect Implicit 1.0, OpenID Connect Messages 1.0, OpenID Connect Session 1.0, OpenID OAuth 2.0 Responses, OpenID Policy 1.0, OpenID SRE 1.0, PACS IG, PIV-I Certificate and CRL Profile, PIV-I for Non-Federal Issuers, RSA PKCS #12, RSA PKCS #5, SAFE-BioPharma CP 2.5, SAML Security and Privacy 2.0, Yadis 1.0,

Source Details

ID: ABADSG
Title: Digital Signature Guidelines
Category: Identity Provider Policy
Date: 8/1/1996
Creator: ABA
URL: http://www.abanet.org/scitech/ec/isc/dsgfree.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: ANSI X9.62-2005
Title: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)
Category: Cryptographic Protocol Specification
Date: 11/03/2005
Creator: ANSI
URL: TBD x9.62-2005 url
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: ANSI X9.63-2001
Title: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography,
Category: Cryptographic Protocol Specification
Date: 11/20/2001
Creator: ANSI
URL: TBD x9.63 2001 url
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: ANSI X9.63-2011
Title: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography,
Category: Cryptographic Protocol Specification
Date: 11/20/2001
Creator: ANSI
URL: http://webstore.ansi.org/RecordDetail.aspx?sku=X9.63-2011#.UFDFDbJlRNQ
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: BAE Governance
Title: Backend Attribute Exchange (BAE) v2.0 Governance
Category: Attribute Provider Policy
Date: 1/23/2012
Creator: ICAM
URL: http://www.idmanagement.gov/documents/BAE_v2_Governance_Document_Final_v1.0.0.pdf
Description: Guidance on how to use Backend Attribute Exchange in a trusted and federated manner within the Federal government. It explains how BAE endpoints perform discovery, the trust model and metadata management. The document scope diagram indicates that it should also cover conformance and interoperability but those topics were not evident.
Privacy: No stipulations.
Security: TBD
Interoperability: TBD

ID:	BAE Overview
Title:	Backend Attribute Exchange (BAE) v2.0 Overview
Category:	Attribute Provider Policy
Date:	1/23/2012
Creator:	ICAM
URL:	http://www.idmanagement.gov/documents/BAE_v2_Overview_Document_Final_v1.0.0.pdf
Description:	High level explanation of Backend Attribute Exchange, including an overview of the document suite, roles and responsibilities, technical and business goals for BAE, design patterns and implementation guidance.
Privacy:	No stipulations.
Security:	TBD
Interoperability:	TBD
Terms:	Attribute Authority, Attribute Subject, Authoritative Source, Backend Attribute Exchange, Backend Attributes, BAE Broker, BAE External Service, BAE Internal Service, BAE Relying Party, BAE Requester, BAE Responder, Batch Processing, Cardholder Unique Identifier, Claimant, E-governance Certification Authorities, E-governance Metadata Authority, E-governance Trust Services, Endpoints, Extensible Markup Language, Federal Agency Smart Credential - Number, Federal Identity, Credentialing And Access Management, Federal Public Key Infrastructure Management Authority, Governance, Hypertext Transfer Protocol, Metadata, Metadata Authority, Card Issuer, Relying Party, Security Assertion Markup Language, Service Provisioning Markup Language, Shared BAE Broker, Simple Object Access Protocol, Locale Identifier

ID:	BAE SAML 2.0 Profiles
Title:	Security Markup Language (SAML) 2.0 Identifier and Protocol Profiles for Backend Attribute Exchange (BAE) v2.0
Category:	Authentication Protocol Interoperability Profile
Date:	1/23/2012
Creator:	ICAM
URL:	http://www.idmanagement.gov/documents/BAE_v2_SAML2_Profile_Final_v1.0.0.pdf
Description:	A SAML 2.0 profile to support direct or brokered attribute exchange over the Backend Attribute Exchange system. It supports names based on FASC-N (from a PIV authentication certificate), UUID (from a PIV-I authentication certificate) or a general X.509 Subject Distinguished Name. It provides a mechanism for looking up sources of metadata information from a repository based on the FASC-N (for government users) and the AKI and organization name for non-government PIV-I users.
Privacy:	The document recommends that BAE servers not store user identities in log files, but it is not required.
Security:	The document is an information security profile. It promotes security by specifying a mechanism for relying parties to obtain user attributes.
Interoperability:	The document promotes interoperability by providing a common profile for BAE messages.

ID:	CertiPath CP 3.18
Title:	CertiPath X.509 Certificate Policy
Category:	Identity Provider Policy
Date:	4/16/2012
Creator:	CertiPath
URL:	https://www.certipath.com/images/stories/data/policy-docs/CertiPath%20CP-v.3.18-clean.pdf
Description:	IETF RFC 3647 certificate policy for CertiPath. The document was digitally signed by the CertiPath Policy Management Authority. It defines certificate policies for the following assurance levels medium-CBP-software, medium-CBP-hardware, high-CBP-hardware, mediumsoftware, medium-hardware, high-hardware, IceCAP-cardAuth, IceCAP-hardware, and IceCAP-contentSigning. The policy domain of the CP applies to the CertiPath Bridge CA (CBCA), the CertiPath Common Policy Root CA (CRCA) and to CAs and end entities under the CRCA.
Privacy:	End entity certificate may contain pseudonyms in order to meet local privacy requirements, if they maintain namespace uniqueness and if the pseudonyms can be traced to the actual person. A link to CertiPath's privacy policy is provided, but when retrieved on 9/3/12 the target page (https://www.certipath.com/component/content/article/58-privacy) has errors and the contact information is not provided.
Security:	The document is an information security policy.
Interoperability:	The purpose of the document is to support interoperation of digital certficates between different enterprise PKIs. The document provides a PKI repository interoperability profile based on LDAP and HTTP and the naming convention defined in the CP, and provides an interoperable smart card profile (which leverages the FIPS 201 profile, with a Globally Unique Identifier used as the CHUID).

ID:	EV Cert 1.1
Title:	Guidelines for the Issuance and Management of Extended Validation Certificates
Category:	Identity Provider Policy
Date:	April 2008
Creator:	The CA/Browser Forum
URL:	http://cabforum.org/EV_Certificate_Guidelines_V11.pdf
Description:	TBD
Privacy:	TBD
Security:	TBD
Interoperability:	TBD

ID:	FBCA CP 2.25
Title:	X.509 Certificate Policy For The Federal Bridge Certification Authority
Category:	Trust Framework Provider Policy
Date:	12/9/2011
Creator:	FBCA
URL:	http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf
Description:	RFC 3647 compliant certificate policy for the Federal Bridge CA. It defines a total of 12 policies, including the following assurance levels for human end users: Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High.
Privacy:	The FPKI management authority is required to conduct a Privacy Impact Assessment. PII shall be protected from unauthorized disclosure, and will only be released to third parties when required by law or court order. No notification is required in the event of such disclosure.
Security:	The document is a information security policy for the FBCA.
Interoperability:	The document supports interoperation of digital certficates between different Federal government PKIs. The document provides a PKI repository interoperability profile based on LDAP and HTTP and the naming convention defined in the CP, and also provides PIV-I as an interoperable smart card profile.
Terms:	Access, Access Control, Accreditation, Activation Data, Affiliated Organization, Applicant, Archive, Attribute Authority, Audit, Audit Data, Authenticate, Authentication, Backup, Binding, Biometric, Certificate, Certification Authority, CA Facility, Certificate, Certificate Management Authority, Certification Authority Software, Certificate Policy, Certification Practice Statement, Certificate-related Information, Certificate Revocation List, Certificate Status Authority, Client (application), Common Criteria, Compromise, Computer Security Objects Registry, Confidentiality, Cross-certificate, Cryptographic Module, Data Integrity, Digital Signature, Dual Use Certificate, Duration, E-commerce, Encrypted Network, Encryption Certificate, End-entity, Entity, Entity CA, FBCA Management Authority, Federal Public Key Infrastructure Policy Authority, Firewall, High Assurance Guard, Information System Security Officer, Inside Threat, Integrity, Intellectual Property, Intermediate CA, Key Escrow, Key Exchange, Key Generation Material, Key Pair, Local Registration, Memorandum Of Agreement, Mission Support Information, Mutual Authentication, Naming Authority, Non-repudiation, Object Identifier, Out-of-band, Outside Threat, Physically Isolated Network, PKI Sponsor, Policy Management Authority, Principal CA, Privacy, Private Key, Public Key, Public Key Infrastructure, Registration Authority, Re-key (a Certificate), Relying Party, Renew (a Certificate), Repository, Responsible Individual, Revoke A Certificate, Risk, Risk Tolerance, Root CA, Server, Signature Certificate, Subordinate CA, Subscriber, Superior CA, System Equipment Configuration, System High, Technical Non-repudiation, Threat, Trust List, Trusted Agent, Trusted Certificate, Trusted Timestamp, Trustworthy System, Two-person Control, Update (a Certificate)

ID:	FBCA Cross-certification Methodology 3.0
Title:	Criteria and Methodology for Cross-certification with the U.S. Federal Bridge Certification Authority
Category:	Identity Provider Policy
Date:	1/25/2012
Creator:	FBCA
URL:	http://www.idmanagement.gov/fpkima/documents/crosscert_method_criteria_v3.0.pdf
Description:	An addendum to the FBCA CP intended to use by personnel involved in cross-certification activities within the Government and between the FBCA and external CAs. Other cross certification activities (e.g. Shared Service Provider CAs, FCPCA, EGCA) are out of scope. The document provides a detailed workflow from the submission of an applicant for cross-certification, through the evaluation steps of policy mapping, review of compliance audit reports, analysis of operations, technical review and testing, and finally through the specific steps involved in performing the cross-certification. Applicants are required to submit a CP in RFC 3647 format for ease of policy mapping.
Privacy:	None.
Security:	The document is an information security policy and procedures document.
Interoperability:	The purpose of the document is to provide a method for achieving trusted interoperability between the U.S. Federal Bridge CA and other CAs operating at compatible levels of assurance.
Terms:	Affiliate PKI, Applicant, Bridge CA, Certification Authority, Certificate Policy, Certificate Policy Working Group, Certificate Revocation List, Certification Practice Statement, Cross-certificate, Cross-certification, Digital Signature, Directory, Federal Bridge Certification Authority, Public Key Certificate, Public Key Infrastructure, Repository

ID:	FICAM Privacy Guidance for Assessors
Title:	Federal Identity, Credentialing, and Access Management Privacy Guidance for Trust Framework Assessors and Auditors
Category:	Security Requirements Specification
Date:	6/29/2011
Creator:	ICAM
URL:	http://www.idmanagement.gov/documents/Guidance_for_Assessors.pdf
Description:	Provides information for trust framework assessors to determine whether Trust Framework Provider participants are complying with FICAM privacy requirements.
Privacy:	The document promotes privacy by ensuring that trust framework assessors understand how to determine whether the FICAM privacy requirements are met.
Security:	The document is guidance for assessors performing accreditations of security related services.
Interoperability:	This document supports interoperation between Federal and non-Federal entities by promoting the Trust Framework Adoption process.

ID:	FICAM TFPAP 1.0.1
Title:	FICAM Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3
Category:	Relying Party Policy
Date:	9/4/2009
Creator:	ICAM
URL:	http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf
Description:	Defines the process the government can determine whether to approve Trust Frameworks for federal purposes. The process covers assessment package submission, value determination, comparability assessment and the adoption decision. For Levels of Assurance 1, 2, and non-PKI 3 (defined NIST SP 800-63), Identity Providers and TFPs demonstrate in each of five categories (registration and issuance, tokens, token and credential management, authentication process, and assertions) the compares to the Level of Assurance for which its credentials might trusted by government applications. For Levels of Assurance 3 and 4, the document relies on the FBCA Cross-certification criteria and methodology (version 2.2 when published, now version 3.0).
Privacy:	TFP member submissions are required to explain the TFPs privacy policy and requirements. Those are evaluated againsst the privacy criteria in Section 3.3. The criteria are (1) opt-in for positive confirmation from users before PII is disclosed, (2) for IdPs to share the minimal set of attributes, (3) for IdPs to share records of user activity, (4) for IdPs to provide users with notice of PII disclosures, for use of PII to be non-compulsory and (5) for PII to be protected after the termination of a service.
Security:	The document is an information security policy.
Interoperability:	The document promotes an interoperable approach to evaluating Trust Frameworks.
Terms:	Adopted Authentication Scheme, Adoption, Approved Encryption Method, Assertion, Assertion Reference, Audit Criteria, Authentication, Authentication Protocol, Bearer Assertion, Biometric, Bona Fides, Certification, Claimant, Comparability, Confidentiality, Cross-certified, Cryptographic, Direct Assertion Model, E-authentication Credential, Entropy, Full Legal Name, Holder-of-key Assertion, Identity, Identity Proofing, Identity Provider, Indirect Assertion Model, Integrity, Issuance, Level Of Assurance, Min-entropy, Multi-factor Authentication, Multi-token Authentication, Network, Nonce, Non-repudiation, Out Of Band, Personal Identifying Information, Proof Of Possession Protocol, Pseudonym, Registration, Registration Authority, Relying Party, Salt, Sensitive Information, Shared Secret, Strong Man In The Middle Resistance, Strongly Bound Credentials, Subscriber, Threat, Token, Token Authenticator, Trust Criteria, Trust Framework, Trust Framework Provider, Verifier, Weak Man In The Middle Resistance, Weakly Bound Credentials

ID:	ICAM IMI Profile 1.0.1
Title:	OASIS Interoperability Guidelines
Category:	Authentication Protocol Interoperability Profile
Date:	11/18/2009
Creator:	ICAM
URL:	http://www.idmanagement.gov/documents/ICAM_IMI_10_Profile.pdf
Description:	TBD
Privacy:	TBD
Security:	TBD
Interoperability:	TBD

ID:	ICAM OpenID 2.0 Profile 1.0.1
Title:	OASIS Interoperability Guidelines
Category:	Authentication Protocol Interoperability Profile
Date:	11/18/2009
Creator:	ICAM
URL:	http://www.idmanagement.gov/documents/ICAM_OpenID20Profile.pdf
Description:	TBD
Privacy:	TBD
Security:	TBD
Interoperability:	TBD

ID:	ICAM SAML 2.0 WB SSO Profile 1.0.2
Title:	Security Assertion Markup Language (SAML) 2.0 Web Browser Single Sign-on (SSO) Profile
Category:	Authentication Protocol Interoperability Profile
Date:	12/16/2011
Creator:	ICAM
URL:	http://www.idmanagement.gov/documents/SAML20_Web_SSO_Profile.pdf
Description:	A SAML 2.0 deployment profile designed to meet Federal government requirements and minimize government risk, promote a consistent user experience and maximize interoperability. It includes three SAML features: single signon, session reset and attribute exchange. It does not require the use of any specific attributes in the authentication exchange, provide a discovery mechanism for attributes, nor discuss the impact of Backend
Privacy:	Implementers are referred to FICAM TFPAP Section 3.3 and advised that many of those privacy principles can be achieved outside the scope of SAML.
Security:	The document is an information security profile. It requires IdPs and RPs to use "approved cryptographic modules per [FIPS140]" but does not clearly specify whether FIPS 140-2 certification is required, nor what security level.
Interoperability:	The document promotes interoperability by providing a common SAML 2.0 profile.
Terms:	Account, Approved, Assert, Authentication Session, Binding, Consolidated Metadata, Digital Encryption, Digital Signature, Discovery, Extensible Markup Language, Holder-of-key Assertion, Identity Provider, Metadata, Persistent, Protected Session, Pseudonymous Identifier, Security Assertion Markup Language, Security Token Service, Signature Verification

ID:	IETF ID OAuth 2.0
Title:	The OAuth 2.0 Authorization Framework
Category:	Authentication Protocol Specification
Date:	7/31/2012
Creator:	IETF
URL:	http://tools.ietf.org/id/draft-ietf-oauth-v2-31.txt
Description:	The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.
Privacy:	TBD
Security:	TBD
Interoperability:	TBD
Terms:	Access Token, Refresh Token, Authorization Code, Authorization Grant, Authorization Server, Authorization Endpoint, Client, Client Identifier, Client Secret, Client Password, Protected Resource, Resource Owner, Resource Server

ID: IETF ID OAuth 2.0 Threat Model
Title: OAuth 2.0 Threat Model and Security Considerations
Category: Security Considerations
Date: 8/14/2012
Creator: OASIS
URL: http://tools.ietf.org/id/draft-ietf-oauth-v2-threatmodel-07.txt
Description: This document gives additional security considerations for OAuth, beyond those in the OAuth specification, based on a comprehensive threat model for the OAuth 2.0 Protocol.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: IETF ID SCIM 1.0
Title: Simple Cloud Identity Management: Protocol 1.0
Category: SDO informational track
Date: 3/15/2012
Creator: IETF
URL: http://tools.ietf.org/id/draft-scim-api-00.txt
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: IETF ID SWD
Title: Simple Web Discovery (SWD)
Category: Attribute Discovery Protocol Specification
Date: 7/6/2012
Creator: IETF
URL: http://tools.ietf.org/id/draft-jones-simple-web-discovery-03.txt
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: IETF RFC 2026
Title: The Internet Standards Process -- Revision 3
Category: Document Development Standard
Date: October 1996
Creator: IETF
URL: http://www.rfc-editor.org/rfc/rfc2026.txt
Description: Describes the standards drafting process for IETF and related organizations.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: IETF RFC 2510
Title: Certificate Management Protocol
Category: Security Protocol Specification
Date: March 1999
Creator: RSA
URL: http://www.ietf.org/rfc/rfc2510.txt
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: IETF RFC 2560
Title: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
Category: Security Protocol Specification
Date: June 1999
Creator: IETF
URL: http://www.ietf.org/rfc/rfc2560.txt
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: IETF RFC 3647
Title: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
Category: Identity Provider Policy
Date: 11/1/2003
Creator: IETF
URL: http://www.ietf.org/rfc/rfc3647.txt
Description: A standard framework for Certificate Policies (CPs) and Certification Practice Statements (CPSs). The document is intended to provide a structure but not the requirements for what the policies should be. A Certificate Policy is defined as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements." The intention is for the CP to provide enough information for a Relying Party to be able to make a determination whether the operations are trustworthy. The Certification Practice Statement is a document detailing the practices employed by the CA in issuing certificates. The CPS is not typically publically available but is used by operators, system adminsitrators, policy management authorities and compliance auditors. IETF RFC 3647 is an update of IETF RFC 2527.
Privacy: The framework specifies where issuers document their privacy policy, what information is considered private within the PKI, responsibilities regarding protection of PII, requirements for consent and/or notification when PII is used or disclosed, and when participants may release PII during legal or administrative proceedings.
Security: The document is an information security standard.
Interoperability: The document supports an interoperable policy framework by providing a common framework for specifying an organization's policies for certificate issuance.
Terms: Activation Data, Authentication, Ca-certificate, Certificate Policy, Certification Path, Certification Practice Statement, CPS Summary (or CPS Abstract), Identification, Issuing Certification Authority (issuing CA), Participant, PKI Disclosure Statement, Policy Qualifier, Registration Authority, Relying Party, Relying Party Agreement, Set Of Provisions, Subject Certification Authority (subject CA), Subscriber, Subscriber Agreement

ID:	IETF RFC 4122
Title:	A Universally Unique Identifier (UUID) URN Namespace
Category:	Naming Standard Specification
Date:	July 2005
Creator:	IETF
URL:	http://www.ietf.org/rfc/rfc4122.txt
Description:	TBD
Privacy:	TBD
Security:	TBD
Interoperability:	TBD

ID:	IETF RFC 5280
Title:	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
Category:	Credential Interoperability Profile
Date:	May 2008
Creator:	IETF
URL:	http://www.ietf.org/rfc/rfc5280.txt
Description:	TBD
Privacy:	TBD
Security:	TBD
Interoperability:	TBD

ID:	IETF RFC 5849
Title:	The OAuth 1.0 Protocol
Category:	Authentication Protocol Specification
Date:	4/1/2010
Creator:	IETF
URL:	http://tools.ietf.org/rfc/rfc5849.txt
Description:	An informational track RFC, OAuth provides a method for clients to access server resources on behalf of a resource owner (such as a different client or an end-user). It also provides a process for end-users to authorize third-party access to their server resources without sharing their credentials (typically, a username and password pair), using user-agent redirections.
Privacy:	TBD
Security:	TBD
Interoperability:	TBD
Terms:	Client, Server, Protected Resource, Resource Owner, Credentials

ID: ISO-IEC Directives Part 2
Title: ISO/IEC Directives, Part 2: Rules for the structure and drafting of International Standards
Category: Document Development Standard
Date: April 2011
Creator: ISO/IEC
URL: http://www.iec.ch/members_experts/refdocs/iec/isoiec-dir2%7Bed6.0%7Den.pdf
Description: Rules for ISO/IEC on how to structure and develop international standards documents, including International Standards, Technical Specification, Publicly Available Specifications, Technical Reports or Guides. A common lexicon of terms is provided in section 3 and later sections address general principles, structure and subdivisions. The section on drafting addresses normative elements such as title page, introduction, scope, references, terms and definitions, and (optionally) requirements. Attention is paid to proper drafting of requirements, if included. A clear distinction shall be made between requirements, statements and recommendations. Definitions of requirements should also include (by definition or reference) test methods for checking conformity to the requirements. The document also addresses proper use of tables figures and mathematical formulae. Further sections address conformity assessment, quality management and presentation. Annex D defines drafting and presentation of terms and definitions.
Privacy: TBD
Security: TBD
Interoperability: TBD
Terms: Standard, International Standard, International Standard, Technical Specification, Technical Report, Guide, Publicly Available Specification, Normative Element, Preliminary Informative Element, Supplementary Informative Element, Mandatory Element, Conditional Element, Requirement, Recommendation, Statement

ID: InCommon Glossary
Title: InCommon Glossary
Category: Trust Framework Provider Specification
Date: 3/18/2006
Creator: InCommon
URL: http://www.incommon.org/glossary.cfm
Description: Definitions of terms for the InCommon trust framework.
Privacy: TBD
Security: TBD
Interoperability: TBD
Terms: Access Management System, Assertion, Attribute, Attribute Assertion, Attribute Authority, Attribute Authority Subject DN, Attribute Authority URL, Attribute Release Policy, Audit, Authentication, Authorization, Billing Contact, Certificate, Certificate Authority, Certificate Policy, Certificate Signing Request, Certification Practice Statement, Digital Signature, Directory, Distinguished Name, Domain Name, Domain Name Service, Eduorg, Eduperson, Electronic Identifier, Electronic Identity, Electronic Identity Credential, Electronic Identity Database, Enterprise Directory, Enterprise Directory Infrastructure, Federated Identity, Federation, Federation Operation Policies And Practices, Handle, Handle Service, Handle Service Subject DN, Handle Service URL, Higher Education Institution, Identity, Identity Credential, Identity Database, Identity Management System, Identity Provider, Incommon CA Root Profile, Incommon Federation, Incommon Technical Advisory Committee, Inqueue, Issuer, LDAP Directory, Liberty Alliance, Lightweight Directory Access Protocol, Lightweight Directory Inter-exchange Format, Metadata, Namespace, Netid, Participant, Participant Agreement, Participant Operating Practices, Privacy Policy, Profile, Public Key Cryptography, Public Key Infrastructure, Relying Party, Resource Provider, Service Provider, Shibboleth, Sponsored Partner, Support Contact, Technical Contact, Uniform Resource Identifier, Uniform Resource Locator, Uniform Resource Name, Validation

ID:	InCommon IAAF 1.1
Title:	InCommon Identity Assurance Assessment Framework
Category:	Trust Framework Provider Specification
Date:	5/9/2011
Creator:	InCommon
URL:	http://www.incommon.org/docs/assurance/IAAF_V1.1.pdf
Description:	The document defines the identity assurance trust model used by InCommon and provides the process for assessing and certifying Identity Provider Operators.
Privacy:	Some discussion of the subject trusting the IDP to protect privacy, and real-time versus pre-approved consent for sharing PII. No requirements though.
Security:	The document is an information security assurance framework.
Interoperability:	The document promotes interoperability by specifying the requirements for a service to operate at the defined identity assurance profiles.
Terms:	Address Of Record, Assertion, Attributes, Attribute Service, Authentication Secret, Credential, Credential Store, Identity, Identity Attributes, Identity Management System, Identity Provider, Idms Database, Idms Operations, Idp Operator, Protected Channel, Registration, Registration Authority, Relying Parties, Service Provider, Subject, Token, User Agent, Verifier

ID:	InCommon IAP 1.1
Title:	Identity Assurance Profiles Bronze and Silver
Category:	Trust Framework Provider Specification
Date:	1/23/2012
Creator:	InCommon
URL:	http://www.incommon.org/docs/assurance/IAP_V1.1.pdf
Description:	Defines requirements for InCommon Silver and Bronze identity assurance certification. These profiles are intended to be compatible with the US federal government ICAMTrust Framework Provider Adoption Process,Levels of Assurance 1 and 2. The requirements are directly applicable to Identity Provider Operators that use Authentication Secret-based Credentials, but equivalent or stronger credentials could be used instead.
Privacy:	No stipulations. For Silver profiles, there are requirements to store PII in the form of registration records (Sec 4.2.2.3).
Security:	The document is a information security profile at OMB-04-04 levels of assurance 1 and 2.
Interoperability:	The document promotes interoperability by specifying the requirements for a service to operate at the defined identity assurance profiles.
Terms:	INCOMMON BRONZE IDENTITY ASSURANCE PROFILE

ID:	Kantara Federal Privacy Criteria
Title:	Identity Assurance Framework: Additional Requirements for Credential Service Providers: US Federal Privacy Criteria
Category:	Trust Framework Provider Specification
Date:	2/15/2012
Creator:	Kantara Initiative
URL:	http://kantarainitiative.org/confluence/download/attachments/45057040/Kantara+Initiative_IAWG_US+FPC+Report_v2.0.pdf
Description:	These additional criteria supplement the Kantara IAF level of assurance requirements found in the Service Assessment Criteria (SAC). The requirements found in the IAF SAC and these additional criteria apply only to CSPs, not to Relying Parties (RPs).
Privacy:	TBD
Security:	TBD
Interoperability:	TBD

ID: Kantara IAF 1000
Title: Identity Assurance Framework: Overview
Category: Trust Framework Provider Specification
Date: 12/31/2009
Creator: Kantara Initiative
URL: http://kantarainitiative.org/confluence/download/attachments/45057040/Kantara+IAF-1000-Overview.pdf
Description: The IAF comprises a set of documents including an Overview publication, the IAF Glossary, a summary Assurance Levels document, and an Assurance Assessment Scheme (AAS), which encompasses the associated assessment and certification program, as well as several subordinate documents, among them the Service Assessment Criteria (SAC), which establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be evaluated. The present document provides an overview of the IAF documents and program.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: Kantara IAF 1100
Title: Identity Assurance Framework: Glossary
Category: Trust Framework Provider Specification
Date: 12/31/2009
Creator: Kantara Initiative
URL: http://kantarainitiative.org/confluence/download/attachments/45057040/Kantara+IAF-1100-Glossary.pdf
Description: Glossary of terms used by Kantara Identity Assurance Framework.
Privacy: No stipulation.
Security: The document defines terms used in a security assurance framework.
Interoperability: No stipulation.
Terms: Accreditation, Annual Conformity Review, Applicant, Approval, Approved Encryption, Approved Service, Assertion, Assessment, Assessor, Assurance Level, Assurance Review Board, Assurance Assessment Scheme, Attack, Attribute, Audit Organization, Accreditation Applicant, Authentication, Authentication Protocol, Authorization, Bit, Certification, Claimant, Certification Body, Certified Service, Credential, Electronic Credentials, Credential Management, Credential Service, Credential Service Provider, Cryptographic Token, Electronic Credentials, Electronic Trust Service, Electronic Trust Service Provider, Federal Information Processing Standards, Federated Identity Management, Federation Operator, Grant Category, Grant (of Rights Ofuse), Grantee, Identification, Identifier, Identity, Identity Assurance Work Group, Identity Assurance Framework, Identity Authentication, Identity Binding, Identity Proofing, Identity Proofing Policy, Identity Proofing Service Provider, Identity Proofing Practice Statement, Information Security Management Systems (ISMS), Issuer, Kantara-approved Assessor, Kantara-accredited Service, Kantara Initiative Board Of Trustees, Kantara Initiative Mark, Kantara Trust Status List, Network, Password, Practice Statement, Public Key, Public Key Infrastructure, Registration, Relying Party, Role, Security, Service Assessment Criteria, Signatory, Specified Service, Subject, Subscriber, Threat, Token

ID: Kantara IAF 1200
Title: Identity Assurance Framework: Assurance Levels
Category: Trust Framework Provider Specification
Date: 12/31/2009
Creator: Kantara Initiative
URL: http://kantarainitiative.org/confluence/download/attachments/45057040/Kantara+IAF-1200-Levels+of+Assurance.pdf
Description: Definition of the levels of assurances used by the Kantara Identity Assurance Framework.
Privacy: No stipulation.
Security: The document defines a set of assurance levels involving increasing levels of security requirements for both functionality and assurance.
Interoperability: No stipulation.

ID: Kantara IAF 1300
Title: Identity Assurance Framework: Assurance Assessment Scheme
Category: Trust Framework Provider Specification
Date: 10/12/2009
Creator: Kantara Initiative
URL: http://kantarainitiative.org/confluence/download/attachments/45057040/Kantara+IAF-1300-Assurance+Assessment+Scheme.pdf
Description: Consists of a set of requirements which assessors must fulfill in order to become 'Kantara-Accredited', a statement of applicable 'credit' granted to assessor applicants with certain prior -qualifications, a description of the application processes from both the Kantara perspective and the applicant's, and guidance on undertaking assessments which will benefit both Kantara- accredited Assessors and Credential Service Providers having their services assessed against the IAF Service Assessment Criteria (SAC)
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: Kantara IAF 1400
Title: Identity Assurance Framework: Service Assessment Criteria
Category: Trust Framework Provider Specification
Date: 12/31/2009
Creator: Kantara Initiative
URL: http://kantarainitiative.org/confluence/download/attachments/45057040/Kantara+IAF-1400-Service+Assessment+Criteria.pdf
Description: Describes the Service Assessment Criteria component of the IAF, including setting out the Assurance Levels.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: Kantara IAF 1600
Title: Identity Assurance Framework: Assessor Qualifications Requirements
Category: Trust Framework Provider Specification
Date: 10/13/2009
Creator: Kantara Initiative
URL: http://kantarainitiative.org/confluence/download/attachments/45057040/Kantara+IAF-1600-Assessor+Qualifications+and+Requirem
Description: Describes the requirements that applicant assessors must fulfill in order to become Kantara-Accredited Assessors.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID:	Kantara SAML 2.0 Profile
Title:	Kantara Initiative eGovernment Implementation Profile of SAML V2.0
Category:	Authentication Protocol Interoperability Profile
Date:	6/11/2010
Creator:	Kantara Initiative
URL:	http://kantarainitiative.org/confluence/download/attachments/42139782/kantara-egov-saml2-profile-2.0.pdf
Description:	Contains an implementation profile for eGovernment use of SAML V2.0, suitable for the purposes of testing conformance of implementations of SAML V2.0. It is not a deployment profile, and does not provide or reflect specific behavior exptected of implementations when used within a particular deployment context.
Privacy:	TBD
Security:	TBD
Interoperability:	TBD

ID:	Kantara UMA
Title:	User-Managed Access (UMA) Core Protocol
Category:	Access Management Protocol Specification
Date:	8/1/2012
Creator:	Kantara Initiative
URL:	http://docs.kantarainitiative.org/uma/draft-uma-core.html
Description:	TBD
Privacy:	TBD
Security:	TBD
Interoperability:	TBD
Terms:	Authorizing User, Authorization Manager, Protected Resource, Host, Claim, Requester, Requesting Party, Resource Set, Scope

ID: NIST FIPS 140-2
Title: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES
Category: Security Requirements Standard
Date: 12/3/2002
Creator: NIST
URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
Description: A set of security requirements specifically pertaining to systems that implement cryptographic mechanisms such as encryption, hashing, digital signatures, random number generation or message authentication. The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; and design assurance. Security Levels 1 through 4 impose increasingly stringent requirements on the requirements, with Level 1 not required to demonstrate any physical security requirements or authenticate users, whereas Level 4 requires tamper response mechanisms, resistance to a range of environmental conditions and identity based authentication of users. This document is the basis of the FIPS 140-2 cryptographic certification scheme administered by NIST and Canada's CSE.
Privacy: No stipulations.
Security: The document is an information security standard. The document specifies security requirements on the functionality and design assurance of cryptographic modules.
Interoperability: The document promotes interoperability by providing a baseline set of requirements for cryptographic modules.
Terms: Approved, Approved Mode Of Operation, Approved Security Function, Authentication Code, Automated Key Transport, Compromise, Confidentiality, Control Information, Critical Security Parameter, Cryptographic Boundary, Cryptographic Key, Cryptographic Key Component, Cryptographic Module, Cryptographic Module Security Policy, Crypto Officer, Data Path, Differential Power Analysis, Digital Signature, Electromagnetic Compatibility, Electromagnetic Interference, Electronic Key Entry, Encrypted Key, Environmental Failure Protection, Environmental Failure Testing, Error Detection Code, Finite State Model, Firmware, Hardware, Hash-based Message Authentication Code, Initialization Vector, Input Data, Integrity, Interface, Key Encrypting Key, Key Establishment, Key Loader, Key Management, Key Transport, Manual Key Transport, Manual Key Entry, Microcode, Operator, Output Data, Password, Personal Identification Number, Physical Protection, Plaintext Key, Port, Private Key, Protection Profile, Public Key, Public Key Certificate, Public Key (asymmetric) Cryptographic Algorithm, Random Number Generator, Removable Cover, Secret Key, Secret Key (symmetric) Cryptographic Algorithm, Seed Key, Simple Power Analysis, Software, Split Knowledge, Status Information, System Software, Tamper Detection, Tamper Evidence, Tamper Response, Target Of Evaluation, TEMPEST, TOE Security Functions, TOE Security Policy, Trusted Path, User, Validation Authorities

ID: NIST FIPS 186-3
Title: Digital Signature Standard
Category: Cryptographic Protocol Specification
Date: June 2009
Creator: NIST
URL: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID:	NIST FIPS 201-1
Title:	Personal Identity Verification (PIV) of Federal Employees and Contractors
Category:	Credential Requirements Specification
Date:	March 2006
Creator:	NIST
URL:	http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
Description:	Specifies the architectural and technical requirements for the Personal Identity Verification (PIV) card system for Federal employees and contractors. The document provides requirements in the area of identity proofing, registration and issuance, as well as credential lifecycle and management requirements. Further NIST documents incorporated by reference are SP 800-73, Interfaces for PIV; SP 800-76, Biometric Data Specification for PIV; SP 800-78, Cryptographic Algorithms and Key Sizes for PIV; SP 800-79, Guidelines for the Accreditation of PIV Card Issuers; SP 800-87, Codes for the Identification of Federal and Federally-Assisted Organizations; SP 800-96, PIV Card to Reader Interoperability Guidelines; SP 800-156, Representation of PIV Chain-of-Trust for Import and Export; and SP 800-157, Guidelines for PIV Derived Credentials.
Privacy:	TBD
Security:	The document is an information security standard.
Interoperability:	TBD

ID:	NIST FIPS 201-2
Title:	Personal Identity Verification (PIV) of Federal Employees and Contractors
Category:	Credential Requirements Specification
Date:	7/9/2012
Creator:	NIST
URL:	http://csrc.nist.gov/publications/drafts/fips201-2/draft_nist-fips-201-2_revised.pdf
Description:	Specifies the architectural and technical requirements for the Personal Identity Verification (PIV) card system for Federal employees and contractors. The document provides requirements in the area of identity proofing, registration and issuance, as well as credential lifecycle and management requirements. Further NIST documents incorporated by reference are SP 800-73, Interfaces for PIV; SP 800-76, Biometric Data Specification for PIV; SP 800-78, Cryptographic Algorithms and Key Sizes for PIV; SP 800-79, Guidelines for the Accreditation of PIV Card Issuers; SP 800-87, Codes for the Identification of Federal and Federally-Assisted Organizations; SP 800-96, PIV Card to Reader Interoperability Guidelines; SP 800-156, Representation of PIV Chain-of-Trust for Import and Export; and SP 800-157, Guidelines for PIV Derived Credentials.
Privacy:	Protection of personal privacy is an explicit objective of the PIV system, directly from HSPD-12. Agencies or departments issuing PIV cards are required to assign a privacy official, conduct Privacy Impact Assessments, identify information collected including its purpose, protection and disclosure policy, restrict access to PII and define consequences for violating the privacy policies. Technology must permit continuous auditing of compliance with privacy policies. The standard permits card issuers to maintain a documentary chain-of-trust for collected identification data, this will contain PII which must be protected and disposed according to agency policy.
Security:	TBD
Interoperability:	The purpose of the standard is to promote interoperability among PIV system components, across departments and agencies and across installations.
Terms:	Access Control, Applicant, Application, Architecture, Asymmetric Keys, Authentication, Biometric, Biometric Information, Capture, Cardholder, Card Management System, Certificate Revocation List, Certification, Certification Authority, Chain-of-trust, Comparison, Component, Conformance Testing, Credential, Cryptographic Key, Authentication Assurance Level, Federal Agency Smart Credential Number, Federal Information Processing Standards, Hash Function, Identification, Identifier, Identity, Identity Proofing, Identity Registration, Identity Verification, Interoperability, Issuer, Match, Model, Off-card, On-card, On-card Comparison, Online Certificate Status Protocol, Path Validation, Personally Identifiable Information, Personal Identification Number, Personal Identity Verification Card, PIV Assurance Level, Private Key, Pseudonyms, Public Key, Public Key Infrastructure, Pki-card Authentication Key, PKI-PIV Authentication Key, Recommendation, Symmetric Key, Validation

ID:	NIST IR 7693
Title:	Specification for Asset Identification 1.1
Category:	Security Requirements Specification
Date:	6/1/2011
Creator:	NIST
URL:	http://csrc.nist.gov/publications/nistir/ir7693/NISTIR-7693.pdf
Description:	Part of the Security Content Automation Protocol (SCAP), Asset Identification is a language for identifying organizational assets, a common initial step in risk management frameworks. The assets are primarily IT components but people and organizations may also be specified. The language supports identification of assets based on intrinsic characteristics, assigned or derived attributes and relationships to other assets. Naming of people and organizations is done with OASIS xNL 2.0. Authentication of the identified assets is out of scope.
Privacy:	There may be PII among the attributes that make up a person's identity. For example the XML Schema for Asset Identification 1.1 allows specification of a person's date of birth.
Security:	No specific security stipulations, relies on the SCAP Trust Model For Security Automation Data (TMSAD) for authentication and confidentiality protections.
Interoperability:	The document promotes an interoperable format for specifying organizational assets.
Terms:	Asset, Asset Identification, Asset Identification Element, Circuit, Computing Device, Data, Database, Extension Identifier, Identifying Information, Matching, Network, Organization, Person, Relationship Identifier, Service, Software, System, Synthetic Identifier

ID:	NIST IR 7870
Title:	NIST Test Personal Identity Verification (PIV) Cards
Category:	Miscellaneous
Date:	July 2012
Creator:	NIST
URL:	http://csrc.nist.gov/publications/nistir/ir7870/nistir-7870.pdf
Description:	The document describes a set of 16 test PIV cards available for purchase as a NIST Special Database. The availability of these cards is intended to facilitate interoperability testing.
Privacy:	No privacy stipulations.
Security:	The document provides test resources for an information security standard.
Interoperability:	The document promotes interoperability by expanding the testing options for implementers of PIV systems.

ID: NIST SP 800-130
Title: A Framework for Designing Cryptographic Key Management Systems
Category: Security Control Implementation Guide
Date: 4/1/2012
Creator: NIST
URL: http://csrc.nist.gov/publications/drafts/800-130/second-draft_sp-800-130_april-2012.pdf
Description: A set of documentation requirements that can be used to express the design of a cryptographic key management system (CKMS). The CKMS is the policies, procedures, components and devices that together provide the functionality of the CKMS. As with IETF RFC 3647, this is not a design or set of functional requirements, but a framework for specifying requirements. The scope of a CKMS includes protection of both cryptographic keys as well as the metadata associated with those keys, such as the digital identity associated with the key. The link between a key and selected metadata elements is called a trusted association, a traditional example of such a trusted association would be an X.509 digital certificate, which links the subject identity with their public key in a trusted fashion.
Privacy: Contains functional requirements related to privacy, requiring the CKMS design to specify the support for the anonymity, unlinkability and unobservability, when it is utilized and how it is technically achieved,
Security: TBD
Interoperability: The purpose of the document is to provide a common means of specifying the design of a CKMS.
Terms: Active State, Algorithm Transition, Application, Archive (key/metadata), Associated Metadata, Association Function, Audit, Authoritative Time Source, Backup (key/metadata), Cryptographic Key Management System, CKMS Component, CKMS Device, CKMS Module, CKMS Profile, Commercial Off-the-shelf, Compromise, Compromised State, Cryptanalyze, Cryptographic Binding (binding), Cryptographic Boundary, Cryptographic Key, Cryptographic Key Management System, Cryptographic Module, Cryptographic Officer, Cryptography, Cryptoperiod, Deactivated State, Designer, Destroyed State, Destroyed Compromised State, Security Domain, Entity, Extensibility, Firewall, Formal Language, Framework, Garbled, Generate Key, Hardening, Hash Value, Identifier, Interoperability, Key Agreement, Key Confirmation, Key Entry, Key Establishment, Key Label, Key Life Cycle State, Key Output, Key Owner, Key Split, Key State Transition, Key Transport, Key Update, Key Wrapping, Least Privilege, Malware, Metadata, Metadata Element, Mode Of Operation, Parameters, Pre-activation State, Privacy, Profile, Qubit, Recover (key/metadata), Registration, Rekey, Renewal, Revoked State, Role, Rootkit, Router, Scalability, Scheme, Sector, Security Domain, Security Policy, Security Strength, Semantics, Standard, Store (key/metadata), Suspended State, Syntax, Trust, Trust Anchor, Trust Anchor Store, Trusted Association, Trusted Channel, Unlinkability, Unobservability, User, Validate

ID: NIST SP 800-152
Title: Requirements and Desirable Features of U.S. Federal Cryptographic Key Management Systems
Category: Security Requirements Profile
Date: 8/8/2012
Creator: NIST
URL: http://csrc.nist.gov/publications/drafts/800-152/draft-sp-800-152.pdf
Description: This document provides policy guidance for designing NIST SP 800-130 conformant Cryptographic Key Management Systems for Federal Government purposes, with the goal of providing requirements to support interoperability and compliance with Federal policy. For all of the requirements categories it provides base requirements, augmented requirements and desirable future goals.
Privacy: Lists anonymity and protection of personal privacy as stretch goals for section 4.4 Accountability. It also refers to personal and function authentication for access to keys and metadata as a desirable goal for a CKMS, this feature would support protection of user attributes by supporting individual accountability.
Security: TBD
Interoperability: The purpose of the document is to provide parameters to SP 800-130 that will permit an interoperable selection for CKMS used by the Government.

ID:	NIST SP 800-63-1
Title:	Electronic Authentication Guideline
Category:	Security Control Implementation Guide
Date:	12/1/2011
Creator:	NIST
URL:	http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
Description:	Technical guidelines for Federal agencies implementing electronic authentication. The document lists technical requirements for the four levels assurance defined in OMB M-04-04 in the areas of identity proofing, registration, tokens, management processes, authentication protocols and assertion mechanisms.
Privacy:	Advises agencies to reference OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 [OMB M-03-22]. Subscribers are assumed to trust relying parties to follow "all relevant privacy policy." PII gathered during registration is required to be protected. The document also defines "private credentials", which are credentials that cannot be disclosed without compromising the token (such as symmetric keys). There is discussion of when Relying Parties may operate anonymously, and discussion of how pseudonymity may be achieved.
Security:	The document is an information security guideline. The requirements in the document are grouped into four assurance levels that provide increasing levels of trust in the authentication process.
Interoperability:	The purpose of the document is to provide sets of requirements for the OMB-04-04 Levels of Assurance. It promotes interoperability by providing a baseline set of requirements for diverse Identity Management systems.
Terms:	Active Attack, Address Of Record, Approved, Applicant, Assertion, Assertion Reference, Assurance, Asymmetric Keys, Attack, Attacker, Attribute, Authentication, Authentication Protocol, Authentication Protocol Run, Authentication Secret, Authenticity, Bearer Assertion, Bit, Biometrics, Certificate Authority, Certificate Revocation List, Challenge-response Protocol, Claimant, Claimed Address, Completely Automated Public Turing Test To Tell Computers And Humans Apart, Cookie, Credential, Credential Service Provider, Cross Site Request Forgery, Cross Site Scripting, Cryptographic Key, Cryptographic Token, Data Integrity, Derived Credential, Digital Signature, Eavesdropping Attack, Electronic Authentication (e-authentication), Entropy, Extensible Markup Language, Federal Bridge Certification Authority, Federal Information Security Management Act, Federal Information Processing Standard, Guessing Entropy, Hash Function, Holder-of-key Assertion, Identity, Identity Proofing, Kerberos, Knowledge Based Authentication, Man-in-the-middle Attack, Message Authentication Code, Min-entropy, Multi-factor, Network, Nonce, Off-line Attack, Online Attack, Online Guessing Attack, Passive Attack, Password, Personal Identification Number, Personal Identity Verification Card, Personally Identifiable Information, Pharming, Phishing, Possession And Control Of A Token, Practice Statement, Private Credentials, Private Key, Protected Session, Pseudonym, Public Credentials, Public Key, Public Key Certificate, Public Key Infrastructure, Registration, Registration Authority, Relying Party, Remote, Replay Attack, Risk Assessment, Salt, Secondary Authenticator, Secure Sockets Layer, Security Assertion Markup Language, SAML Authentication Assertion, Session Hijack Attack, Shared Secret, Social Engineering, Special Publication, Strongly Bound Credentials, Subscriber, Symmetric Key, Token, Token Authenticator, Token Secret, Transport Layer Security, Trust Anchor, Unverified Name, Valid, Verified Name, Verifier, Verifier Impersonation Attack, Weakly Bound Credentials, Zeroize

ID:	NIST SP 800-73-3 Part 1
Title:	Interfaces for Personal Identity Verification - Part 1: End-Point PIV Card Application Namespace, Data Model and Representation
Category:	Credential Requirements Specification
Date:	February 2010
Creator:	NIST
URL:	http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf
Description:	Describes requirements for PIV client-application programming interface, PIV Card application, and PIV Data Models.
Privacy:	TBD
Security:	TBD
Interoperability:	TBD
Terms:	Algorithm Identifier, Application Identifier, Authenticatable Entity, BER-TLV Data Object, Card, Card Application, Client Application, Data Object, Interface Device, Key Reference, MSCUID, Object Identifier, PIV Key Type, Relying Party

ID:	NIST SP 800-73-3 Part 2
Title:	Interfaces for Personal Identity Verification - Part 2: End-Point PIV Card Application Card Command Interface
Category:	Credential Requirements Specification
Date:	February 2010
Creator:	NIST
URL:	http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART2_piv-card-applic-card-common-interface.pdf
Description:	Describes requirements for PIV client application programming interface including information processing and data representation concepts, required commands accessible by the PIV Middleware to communicate with the PIV Card Application, and an informative discussion of the GENERAL AUTHENTICATE command.
Privacy:	TBD
Security:	TBD
Interoperability:	TBD
Terms:	Application Identifier, Algorithm Identifier, Authenticatable Entity, BER-TLV Data Object, Card, Card Application, Client Application, Data Object, Key Reference, Object Identifier, Reference Data, Status Word

ID:	NIST SP 800-73-3 Part 3
Title:	Interfaces for Personal Identity Verification - Part 3: End-Point PIV Client Application Programming Interface
Category:	Credential Requirements Specification
Date:	February 2010
Creator:	NIST
URL:	http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART3_piv-client-applic-programming-interface.pdf
Description:	Describes the required set of entry points accessible by client applications through the PIV Middleware to interact with the PIV Card.
Privacy:	TBD
Security:	TBD
Interoperability:	TBD
Terms:	Application Identifier, Application Session, Algorithm Identifier, BER-TLV Data Object, Card, Card Application, Card Interface Device, Card Reader, Client Application, Data Object, Interface Device, Key Reference, Object Identifier, Reference Data, Status Word

ID:	NIST SP 800-73-3 Part 4
Title:	Interfaces for Personal Identity Verification - Part 4: The PIV Transitional Interfaces and Data Model Specification
Category:	Credential Requirements Specification
Date:	February 2010
Creator:	NIST
URL:	http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART4_piv-transitional-interface-data-model-spec.pdf
Description:	Provides the specification common to both the transitional and end-point interfaces. Also provides an informative discussion of transitional interface specifications that are implemented today by agencies with legacy GSC-IS based card deployments.
Privacy:	TBD
Security:	TBD
Interoperability:	TBD
Terms:	Card, Card Application

ID:	NIST SP 800-76-2
Title:	Biometric Data Specification for Personal Identity Verification
Category:	Credential Requirements Specification
Date:	7/9/2012
Creator:	NIST
URL:	http://csrc.nist.gov/publications/drafts/800-76-2/draft-sp-800-76-2_revised.pdf
Description:	Requirements for biometric data in PIV cards including the aquisition process, sharing with required agencies, data structures for various biometric data, minimum accuracy specifications, and specifications for algorithms used in the generation and matching of PIV Card minutiae.
Privacy:	TBD
Security:	TBD
Interoperability:	TBD

ID:	NIST SP 800-79-1
Title:	Guidelines for the Accreditation of Personal Identity Verification Card Issuers
Category:	Security Assessment Guide
Date:	February 2010
Creator:	NIST
URL:	http://csrc.nist.gov/publications/nistpubs/800-79-1/SP800-79-1.pdf
Description:	Survey of the requirements to be met by a PIV Card Issuer (PCI) and an accreditation methodology for ensuring their conformance with those requirements. Accreditation topics include organizational readiness, security management and data protection, infrastructure elements and processes.
Privacy:	The security management and data protection accreditation topic includes confirmation that privacy requirements from FIPS 201 are satisfied. This document does not add privacy requirements but provides guidelines for assessing conformance to those requirements. Privacy related documents required during the accrediation process include the privacy policy, privacy impact analysis, system of record notice, privacy act statement, rules of conduct and documented processes for requests to review personal information, requests to amend personal information, appeals and complaints.
Security:	Provides a structure for confirming that the PIV Card Issuer meets security obligations and requirements.
Interoperability:	Supports interoperable use of PIV cards by providing a common baseline of security assurance in the issuance process.

ID: NIST SP 800-85A-2
Title: PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-3 compliance)
Category: Security Test Guide
Date: July 2010
Creator: NIST
URL: http://csrc.nist.gov/publications/nistpubs/800-85A-2/sp800-85A-2-final.pdf
Description: Detailed test guidelines for testing the interfaces to card applications and middleware.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: NIST SP 800-85B
Title: PIV Data Model Test Guidelines
Category: Security Test Guide
Date: July 2006
Creator: NIST
URL: http://csrc.nist.gov/publications/nistpubs/800-85B/SP800-85b-072406-final.pdf
Description: Specifices the derived test requirements, detailed test assertions, and conformance tests for testing the dataelements of the PIV systemas per specifications laid out in FIPS 201-1, NIST SP 800-73, NIST SP 800-76, and NIST SP 800-78.
Privacy: TBD
Security: TBD
Interoperability: TBD
Terms: Offline Test, Scenario Test, Operational Test, Interoperability Test, Template Matcher

ID: NSTIC Strategy
Title: NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, Enhancing Online Choice, Efficiency, Security, and Privacy
Category: Miscellaneous
Date: April 2011
Creator: NSTIC NPO
URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
Description: Describes the high-level objectives and benefits of a national identity ecosystem.
Privacy: TBD
Security: TBD
Interoperability: TBD
Terms: Identity Ecosystem Framework, Identity Ecosystem, Individual, Non-person Entity, Attributes, Digital Identity, Identity Provider, Enrolling Agent, Credentials, Identity Medium, Relying Party, Attribute Provider, Participants, Trustmark, Trust Framework, Accreditation Authority, Trustmark Scheme

ID: OASIS IMI 1.0
Title: Identity Metasystem Interoperability Version 1.0
Category: Authentication Protocol Specification
Date: 7/1/2009
Creator: OASIS
URL: http://docs.oasis-open.org/imi/identity/v1.0/os/identity-1.0-spec-os.pdf
Description: Presents a subset of mechanisms from other OASIS work to facilitate and interoperable token issuance and consumption framework using the Information Card Model.
Privacy: TBD
Security: TBD
Interoperability: TBD
Terms: Information Card Model, Information Card, Digital Identity, Claim, Subject, Service Requester, Relying Party, Identity Provider, Security Token Service, Identity Provider Security Token Service, Relying Party Security Token Service, Identity Selector, Trust Identity, Security Token, Signed Security Token, Unsigned Security Token, Proof-of-possession, Integrity, Confidentiality, Digest, Signature

ID: OASIS Interop
Title: OASIS Interoperability Guidelines
Category: Document Development Standard
Date: 1/14/2012
Creator: OASIS
URL: https://www.oasis-open.org/policies-guidelines/interoperability-guidelines
Description: Provides a definition of interoperability and guidelines for when and how to apply techniques for achieving it. It concludes with discussion of ten common mistakes that can inhibit interoperability.
Privacy: No specific privacy relevance.
Security: No specific security relevance.
Interoperability: The document defines interoperability (within the domains of communications protocols and artifacts, at least), discusses the standardization process, lists common mistakes and offers best practices to counter those mistakes.

ID: OASIS SAML Authentication Context 2.0
Title: Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0
Category: Authentication Protocol Specification
Date: 3/15/2005
Creator: OASIS
URL: http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OASIS SAML Bindings 2.0
Title: Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0
Category: Authentication Protocol Specification
Date: 3/15/2005
Creator: OASIS
URL: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OASIS SAML Conformance 2.0
Title: Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0
Category: Authentication Protocol Specification
Date: 3/15/2005
Creator: OASIS
URL: http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf
Description: Provides the technical requirements for SAML V2.0 conformance and specifies the entire set of documents comprising SAML V2.0.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OASIS SAML Glossary 2.0
Title: Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0
Category: Authentication Protocol Specification
Date: 3/15/2005
Creator: OASIS
URL: http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf
Description: Glossary of terms used in SAML 2.0.
Privacy: Defines both transient and persistent pseudonym as mechanisms for privacy-preserving name identifiers.
Security: The document defines terms used in an information security standard.
Interoperability: TBD
Terms: Access, Access Control, Access Control Information, Access Rights, Account, Account Linkage, Active Role, Administrative Domain, Administrator, Affiliation, Assertion, Asserting Party, Attribute Authority, Attribute Assertion, Authentication, Authentication Assertion, Authentication Authority, Authorization, Authorization Decision, Authorization Decision Assertion, Back Channel, Binding, Credentials, End User, Federated Identity, Federate, Front Channel, Identifier, Identity, Identity Defederation, Identity Federation, Identity Provider, Initial SOAP Sender, Login, Logon, Sign-on, Logout, Logoff, Sign-off, Markup Language, Name Qualifier, Namespace, Party, Persistent Pseudonym, Policy Decision Point, Policy Enforcement Point, Principal, Principal Identity, Provider, Proxy, Proxy Server, Pull, Push, Relying Party, Requester, SAML Requester, Resource, Responder, SAML Responder, Role, SAML Authority, Security, Security Architecture, Security Assertion, Security Assertion Markup Language, SAML Artifact, Security Context, Security Domain, Security Policy, Security Policy Expression, Security Service, Service Provider, Session Authority, Session Participant, Site, Subject, System Entity, Entity, Time-out, Transient Pseudonym, Ultimate SOAP Receiver, User, Uniform Resource Identifier, URI Reference, XML Attribute, XML Element, XML Namespace

ID: OASIS SAML Metadata 2.0
Title: Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0
Category: Authentication Protocol Specification
Date: 3/15/2005
Creator: OASIS
URL: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
Description: Describes a set of rules for SAML metadata producers and consumers to follow such that federated relationships can be interoperably provisioned, and controlled at runtime in a secure, understandable, and self-contained fashion.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OASIS SAML Profiles 2.0
Title: Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0
Category: Authentication Protocol Specification
Date: 3/15/2005
Creator: OASIS
URL: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
Description: Defines profiles for the use of SAML assertions and request-response messages in communications protocols and frameworks, as well as profiles for SAML attribute value syntax and naming conventions.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OASIS SAML Protocol 2.0
Title: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
Category: Authentication Protocol Specification
Date: 3/15/2005
Creator: OASIS
URL: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
Description: Definesthe syntax and semantics for XML-encoded assertions about authentication, attributes, and authorization, and for the protocols that convey this information.
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OASIS TC-Process Sec 2.18
Title: OASIS Technical Committee (TC) Process Section 2.18 Work Product Quality
Category: Document Development Standard
Date: 8/1/2012
Creator: OASIS
URL: https://www.oasis-open.org/policies-guidelines/tc-process#specQuality
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OASIS xNL 2.0
Title: Extensible Name Language (xNL) Standard Description Document for W3C DTD/Schema
Category: Naming Standard Specification
Date: 5/31/2002
Creator: OASIS
URL: https://www.oasis-open.org/committees/ciq/Downloads/ciq_all.zip
Description: A standard for specifying person and organization names (as well as a number of related attributes such as former names, aliases, titles, generational identifiers. It does not provide matching rules for determining equivalence between names.
Privacy: Privacy is explicitly out of scope of the specification (q.v. section 4.4).
Security: Security is explicitly out of scope of the specification (q.v. section 4.4).
Interoperability: This standard is intended to provide an interoperable mechanism for representing human and organization names. It is used by SCAP Asset Identification 1.1 (for example) to represent names for those types of entities.

ID: OpenID Attribute 1.0
Title: OpenID Attribute Exchange 1.0
Category: Attribute Discovery Protocol Specification
Date: 12/5/2007 Final
Creator: OpenID
URL: http://openid.net/specs/openid-attribute-exchange-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID Auth 1.1
Title: OpenID Authentication 1.1
Category: Authentication Protocol Specification
Date: 5/1/2006
Creator: OpenID
URL: http://openid.net/specs/openid-authentication-1_1.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID Authentication 2.0
Title: OpenID Authentication 2.0
Category: Authentication Protocol Specification
Date: 12/5/2007
Creator: OpenID
URL: http://openid.net/specs/openid-authentication-2_0.html
Description: The authentication protocol for OpenID version 2.0. It consists of an XRI or Yadis based discovery of any resources required to authenticate the claimed identity.
Privacy: TBD
Security: The document is an information security standard.
Interoperability: TBD
Terms: Identifier, User-agent, Relying Party, Openid Provider, OP Endpoint URL, OP Identifier, User-supplied Identifier, Claimed Identifier

ID: OpenID Connect 1.0
Title: OpenID Connect Standard 1.0
Category: Authentication Protocol Specification
Date: 6/23/2012
Creator: OpenID
URL: http://openid.net/specs/openid-connect-standard-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID Connect Basic 1.0
Title: OpenID Connect Basic Client Profile 1.0
Category: Authentication Protocol Specification
Date: 6/23/2012
Creator: OpenID
URL: http://openid.net/specs/openid-connect-basic-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID Connect Discovery 1.0
Title: OpenID Connect Discovery 1.0
Category: Attribute Discovery Protocol Specification
Date: 5/25/2012
Creator: OpenID
URL: http://openid.net/specs/openid-connect-discovery-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID Connect Dynamic Registration 1.0
Title: OpenID Connect Dynamic Client Registration 1.0
Category: Authentication Protocol Specification
Date: 5/25/2012
Creator: OpenID
URL: http://openid.net/specs/openid-connect-registration-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID Connect Implicit 1.0
Title: OpenID Connect Implicit Client Profile 1.0
Category: Authentication Protocol Specification
Date: 6/23/2012
Creator: OpenID
URL: http://openid.net/specs/openid-connect-implicit-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID Connect Messages 1.0
Title: OpenID Connect Messages 1.0
Category: Authentication Protocol Specification
Date: 6/23/2012
Creator: OpenID
URL: http://openid.net/specs/openid-connect-messages-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID Connect Session 1.0
Title: OpenID Connect Session Management 1.0
Category: Authentication Protocol Specification
Date: 8/2/2012
Creator: OpenID
URL: http://openid.net/specs/openid-connect-session-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID OAuth 2.0 Responses
Title: OAuth 2.0 Multiple Response Type Encoding Practices
Category: Authentication Protocol Specification
Date: 5/25/2012
Creator: OpenID
URL: http://openid.net/specs/oauth-v2-multiple-response-types-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID Policy 1.0
Title: OpenID Provider Authentication Policy Extension 1.0
Category: Authentication Protocol Specification
Date: 12/30/2008 Final
Creator: OpenID
URL: http://openid.net/specs/openid-provider-authentication-policy-extension-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: OpenID SRE 1.0
Title: OpenID Simple Registration Extension 1.0
Category: Authentication Protocol Specification
Date: 6/30/2006
Creator: OpenID
URL: http://openid.net/specs/openid-simple-registration-extension-1_0.html
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: PACS IG
Title: Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems
Category: Security Control Implementation Guide
Date: 12/20/2005
Creator: Government Smart Card Interagency Advisory Board
URL: http://www.idmanagement.gov/iab/documents/PACS.pdf
Description: Guidelines for how to use smart card based systems (such as PIV) with physical access control systems (PACS) in an interoperable and secure manner.
Privacy: Agencies are recommended not to use Social Security Number as the Personnel Identifier field of the FASC-N.
Security: The document is an information security policy.
Interoperability: The document fosters cross-government interoperability of PACS with smart card credentials, by providing a common naming scheme usable to physical access control systems.

ID: PIV-I Certificate and CRL Profile
Title: X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards
Category: Credential Interoperability Profile
Date: 4/23/2010
Creator: Federal PKI Policy Authority
URL: http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf
Description: Specifies a profile for the certificates and CRLs to be used with PIV-I cards.
Privacy: TBD
Security: The document is an information security profile.
Interoperability: TBD

ID: PIV-I for Non-Federal Issuers
Title: Personal Identity Verification Interoperability (PIV-I) For Non-Federal Issuers
Category: Credential Requirements Standard
Date: May 2009
Creator: Federal CIO Council
URL: http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf
Description: Requirements for non-Federal issuers of cards designed to interoperate with the Federal PIV system. Requirements are grouped into the following sections: common terminology for identity cards, technical requirements, an identifier namespace that permits unique identifiers for all users, and the establishment of trusted identities.
Privacy: No stipulations.
Security: The document is an information security policy.
Interoperability: The document promotes interoperability between Federal and non-Federal credentials, issuers and relying parties.

ID: RSA PKCS #12
Title: Personal Information Exchange Syntax Standard
Category: Cryptographic Protocol Specification
Date: April 1997
Creator: RSA
URL: http://www.rsa.com/rsalabs/node.asp?id=2138
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: RSA PKCS #5
Title: Password-Based Cryptography Standard
Category: Cryptographic Protocol Specification
Date: April 1997
Creator: RSA
URL: http://www.rsa.com/rsalabs/node.asp?id=2127
Description: TBD
Privacy: TBD
Security: TBD
Interoperability: TBD

ID: SAFE-BioPharma CP 2.5
Title: SAFE-BioPharma Certificate Policy
Category: Trust Framework Provider Specification
Date: 3/12/2010
Creator: SAFE-BioPharma
URL: http://www.safe-biopharma.org/infocenter/SAFEBioPharmaCertificatePolicy.pdf
Description: RFC 3647 compliant certificate policy for SAFE-BioPharma. It defines policies for basic assurance, medium software and medium hardware.
Privacy: Does not define what information is to be treated as private, that is to be defined in member and issuer agreements and CPSs.
Security: The document is an information security policy for SAFE-BioPharma.
Interoperability: The document supports interoperation of digital certficates between different enterprise PKIs. The document provides a directory interoperability profile based on LDAPv3 over HTTP and the naming convention defined in the CP.
Terms: Assurance Level, Access, Activation Data, Audit, Audit Data, Authentication, Backup, Binding, CA Software, Certificate Status Authority, Client (application), Common Criteria, Compromise, Components, PKI Components, Confidentiality, Cross-certificate, Cryptographic Module, Duration, E-commerce, Encryption Certificate, End Entity, Firewall, Immediately, Integrity, Intellectual Property, Key Escrow, Local Registration Authority (LRA), Non-repudiation, Out-of-band, Principal CA, Privacy, Re-key (a Certificate), Renew (a Certificate), Revoke (a Certificate), Risk, Server, Signature Certificate, Subordinate CA, Superior CA, Threat, Trust Anchor, Update (a Certificate)

ID:	SAML Security and Privacy 2.0
Title:	Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0
Category:	Authentication Procotol Specification
Date:	3/15/2005
Creator:	OASIS
URL:	http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf
Description:	Provides security and privacy considerations for users of SAML 2.0, including some specific implementation requirements (such as mandatory cryptographic algorithms to be supported) but more extensive discussion of threats and countermeasures to be considered when profiling SAML 2.0.
Privacy:	There is discussion of achieving privacy through confidentiality of the transaction and a discussion of pseudonymity. Privacy protections implemented for PII at rest seems to be out of scope.
Security:	The threat analysis within explains design choices within SAML or informs the developers of SAML profiles. The document requires SHA-1 with no mention of more robust hash algorithms (SHA-256 etc did not exist in 2005), requires Triple DES and suggests but does not mandate AES.
Interoperability:	The document specifies TLS cipher suites that are required to be supported.

ID:	Yadis 1.0
Title:	Yadis Specification 1.0
Category:	Attribute Discovery Protocol Specification
Date:	3/18/2006
Creator:	INFOGRID
URL:	http://infogrid.org/trac/export/1639/docs/yadis/yadis-v1.0.pdf
Description:	The Yadis specification includes an identification scheme for people and non-person entities, a syntax for describing service resources available based on that identifier and a discovery protocol for obtaining the resource description document. Given a Yadis ID, it is possible to discover what services that ID can be used to log into. It is designed to work with OpenID and LID.
Privacy:	The services discovered and accessed via Yadis should implement appropriate privacy protections. The resources associated with and ID may provide general information about the user's online activities and thus may be considered private information.
Security:	TBD
Interoperability:	The document promotes an interoperable method for naming entities and for discovering services based on those names.
Terms:	Yadis User, Yadis ID, Yadis URL, Yadis Resource, Yadis Service, Yadis Document, Yadis Resource Descriptor, Resource Descriptor URL, Agent, Yadis User Agent, Relying Party, Relying Party Agent