Standard Link	Standard Description/Purpose
FIDO U2F 1.1	The Fast Identity Online (FIDO) U2F protocol enables relying parties to offer a strong cryptographic 2nd factor option for end user security. The relying party's dependence on passwords is reduced. The password can even be simplified to a 4-digit PIN. End users carry a single U2F device which works with any relying party supporting the protocol. The user gets the convenience of a single 'keychain' device and convenient security. This document is an overview of the U2F protocol and is a recommended first-read before reading detailed protocol documents.
FIDO UAF 1.1	The FIDO UAF strong authentication framework enables online services and websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-user computing devices for strong user authentication and to reduce the problems associated with creating and remembering many online credentials.
IDEF Core Documents	The Identity Ecosystem Framework (IDEF) v.1 was approved by the IDESG Plenary on October 15, 2015. The IDEF v.1 represents three core documents that describe the Identity Ecosystem and the requirements, best practices, and approved standards needed to be considered in compliance with it.
IETF Kerberos v5	The Internet Engineering Task Force (IETF) Kerberos v5 document provides an overview and specification of Version 5 of the Kerberos protocol, and it obsoletes RFC 1510 to clarify aspects of the protocol and its intended use that require more detailed or clearer explanation than was provided in RFC 1510. The document is intended to provide a detailed description of the protocol, suitable for implementation, together with descriptions of the appropriate use of protocol messages and fields within those messages.
IETF OAuth 2.0	The IETF OAuth 2.0 authorization framework document 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.
IETF X.509 PKI Attribute Certificate Profile for Authorization	The IETF X.509 PKI Attribute Certificate Profile for Authorization document defines a profile for the use of X.509 Attribute Certificates in Internet Protocols. Attribute certificates may be used in a wide range of applications and environments covering a broad spectrum of interoperability goals and a broader spectrum of operational and assurance requirements. The goal of this document is to establish a common baseline for generic applications requiring broad interoperability as well as limited special purpose requirements. The profile places emphasis on attribute certificate support for Internet electronic mail, IPSec, and WWW security applications.
IETF X.509 PKI Certificate Management Messages over CMS	The IETF X.509 PKI Certificate Management Messages over CMS document defines a Certificate Management protocol using CMS (CMC). This protocol addresses two immediate needs within the Internet PKI community: 1. The need for an interface to public key certification products and services, and 2. The need for a certificate enrollment protocol for Digital Signature Algorithm (DSA)-signed certificates with Diffie-Hellman public keys.
IETF X.509 PKI Certificate Policy and Certification Practices Framework	The IETF X.509 PKI Certificate Policy and Certification Practices Framework document presents a framework to assist the writers of certificate policies or certification practice statements for certification authorities and public key infrastructures. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy definition or a certification practice statement.
IETF X.509 PKI Certificate Request Message Format	The IETF X.509 PKI Certificate Request Message Format document describes the Certificate Request Message Format (CRMF). This syntax is used to convey a request for a certificate to a Certification Authority (CA) (possibly via a Registration Authority (RA)) for the purposes of X.509 certificate production. The request will typically include a public key and associated registration information.
IETF X.509 PKI Online Certificate Status Protocol - OCSP	The IETF X.509 PKI Online Certificate Status Protocol document defines a protocol useful in determining the current status of a digital certificate without requiring CRLs. Additional mechanisms addressing PKI operational requirements are specified in separate documents.
IETF X.509 PKI Proxy Certificate Profile	The IETF X.509 PKI Proxy Certificate Profile document describes a certificate profile for Proxy Certificates, based on X.509 Public Key Infrastructure (PKI) certificates as defined in RFC 3280, for use in the Internet. The term Proxy Certificate is used to describe a certificate that is derived from, and signed by, a normal X.509 Public Key End Entity Certificate or by another Proxy Certificate for the purpose of providing restricted proxying and delegation within a PKI based authentication system.
IETF X.509 PKI Qualified Certificates Profile	The IETF X.509 PKI Qualified Certificates Profile document describes a certificate profile for Qualified Certificates, based on RFC 2459, for use in the Internet. The term Qualified Certificate is used to describe a certificate with a certain qualified status within applicable governing law. Further, Qualified Certificates are issued exclusively to physical persons.
IETF X.509 PKI Time-Stamp Protocol (TSP)	The IETF X.509 PKI Time-Stamp Protocol (TSP) document describes the format of a request sent to a Time Stamping Authority (TSA) and of the response that is returned. It also establishes several security-relevant requirements for TSA operation, with regards to processing requests to generate responses.
OASIS WS-SecureConversation v1.3	The OASIS WS-SecureConversation specification defines extensions that build on WS-Security to provide a framework for requesting and issuing security tokens, and to broker trust relationships.
OASIS WS-Security Kerberos Token Profile Version 1.1.1	The OASIS WS-Security Kerberos Token Profile v1.1.1 specification describes how to use Kerberos tickets with the Web Services Security: SOAP Message Security 1.1.
OASIS WS-Security REL Token Profile Version 1.1.1	The OASIS WS-Security Rights Expression Language (REL) Token Profile Version 1.1.1 specification describes how to use ISO/IEC 21000-5 Rights Expressions with the Web Services Security (WSS) specification.
OASIS WS-Security SAML Token Profile Version 1.1.1	The OASIS WS-Security SAML Token Profile v1.1.1 specification describes how to use Security Assertion Markup Language (SAML) V1.1 and V2.0 assertions with the Web Services Security SOAP Message Security Version 1.1.1 specification.
OASIS WS-Security: SOAP Message Security Version 1.1.1	The OASIS WS-Security:SOAP Message Security v1.1.1 specification describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies. The document includes security, privacy, and interoperability concerns and challenges that must be considered when implementing solutions utilizing SOAP.
OASIS WS-Security Username Token Profile Version 1.1.1	The OASIS WS-Security Username Token Profile v1.1.1 specification describes how to use the Username Token with the Web Services Security (WSS) specification.
OASIS WS-Security X.509 Certificate Token Profile Version 1.1.1	The OASIS WS-Security X.509 Certificate Token Profile v1.1.1 specification describes how to use X.509 Certificates with the Web Services Security: SOAP Message Security [WS-Security] specification.
OASIS WS-SecurityPolicy v1.3	The OASIS WS-SecurityPolicy v1.3 specification indicates the policy assertions for use with WS-Policy which apply to WSS: SOAP Message Security, WS-Trust and WS-SecureConversation.

Standard Link	Standard Description/Purpose
OASIS WS-Trust 1.4	The OASIS WS-Trust v1.4 specification defines extensions that build on WS-Security to provide a framework for requesting and issuing security tokens, and to broker trust relationships.
OASIS PKCS 11 TC	The OASIS PKCS #11 publication provides a standard for cryptographic tokens controlling authentication information (personal identity, cryptographic keys, certificates, digital signatures, biometric data).
OASIS SAML 1.1	The OASIS Security Assertion Markup Language (SAML) specification defines the syntax and semantics for XML-encoded SAML assertions, protocol requests, and protocol responses.
OASIS SAML 2.0	The OASIS SAML 2.0 specification provides an extension of SAML 1.1. which defines the syntax and processing semantics of assertions made about a subject by a system entity.
OASIS WS-Security: SOAP Message Security Version 1.1	The OASIS WS-Security:SOAP Message Security v1.1 specification proposes a standard set of SOAP extensions that can be used when building secure Web services to implement message content integrity and confidentiality. This specification refers to this set of extensions and modules as the “Web Services Security: SOAP Message Security” or “WSS: SOAP Message Security”.
OASIS WS-Federation 1.2	The OASIS WS-Federation 1.2 specification defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. This includes mechanisms for brokering of identity, attribute, authentication and authorization assertions between realms, and privacy of federated claims.
OpenID Foundation OpenID Connect 1.0	The OpenID Foundations OpenID Connect 1.0 protocol is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable manner.
W3C WS-Policy	The World Wide Web Consortium (W3C) Web Services Policy Framework (WS-Policy) provides a general purpose model and corresponding syntax to describe the policies of a Web Service. WS-Policy defines a base set of constructs that can be used and extended by other Web services specifications to describe a broad range of service requirements and capabilities.

Standard Link	Standard Description/Purpose
Data Management Body of Knowledge (DMBOK)	The Data Management Association (DAMA) DMBOK 2nd Edition provides an industry accepted knowledge guide about data management, including definitions, process models and context diagrams.
IETF Domain Name System (DNS) Protocol	The goal of domain names is to provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations.
IETF Hypertext Transfer Protocol and Hypertext Transfer Protocol Secured (HTTP 1.1)	HTTP is a stateless application-level protocol for distributed, collaborative, hypertext information systems.
IETF JavaScript Open Notation (JSON) Format	JavaScript Object Notation (JSON) is a lightweight, text-based, language-independent data interchange format. JSON defines a small set of formatting rules for the portable representation of structured data.
IETF Representational State Transfer (REST) Format	For the purposes of HTTP, a "representation" is information that is intended to reflect a past, current, or desired state of a given resource, in a format that can be readily communicated via the protocol, and that consists of a set of representation metadata and a potentially unbounded stream of representation data.
IETF Secure Shell (SSH) Protocol	The Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network.
IETF Secure Sockets Layer (SSL) Protocol	This standard specifies version 3.0 of the Secure Sockets Layer (SSL 3.0) protocol, a security protocol that provides communications privacy over the Internet.
IETF Transport Layer Security (TLS)	HTTP was originally used in the clear on the Internet. Increased use of HTTP for sensitive applications has required security measures. SSL, and its successor TLS were designed to provide channel-oriented security.
IETF Uniform Resource Identifier (URI) Format	A Uniform Resource Identifier (URI) is a compact sequence of characters that identifies an abstract or physical resource. This specification defines the generic URI syntax and a process for resolving URI references that might be in relative form, along with guidelines and security considerations for the use of URIs on the Internet.
IETF XML Configuration Access Protocol (XCAP)	These specifications define the XML and XML Configuration Access Protocol (XCAP). XCAP allows a client to read, write, and modify application configuration data stored in XML format on a server.
OpenAPI (Swagger) RESTful API Documentation Specifications	The files describing the RESTful API in accordance with the Swagger specification are represented as JSON objects and conform to the JSON standards.
Open Data Protocol (OData)	The Open Data Protocol (OData) enables the creation of HTTP-based data services, which allow resources identified using Uniform Resource Identifiers (URIs) and defined in an abstract data model, to be published and edited by Web clients using simple HTTP messages.
REST API Modeling Language (RAML) Schema Modeling Specifications	RAML is a language for the definition of HTTP-based APIs that embody most or all of the principles of Representational State Transfer (REST). The RAML specification represents an application of the YAML Specification. The RAML specification provides mechanisms for defining practically-RESTful APIs, creating client/server source code, and comprehensively documenting the APIs for users.
W3C Extensible Markup Language (XML)	Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. XML is an application profile or restricted form of SGML, the Standard Generalized Markup Language [ISO 8879]. By construction, XML documents are conforming SGML documents.
W3C Simple Object Access Protocol (SOAP)	SOAP Version 1.2 is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. "Part 1: Messaging Framework" defines, using XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols.
W3C Resource Description Format (RDF)	The Resource Description Framework (RDF) is a framework for representing information in the Web. RDF Concepts and Abstract Syntax defines an abstract syntax on which RDF is based, and which serves to link its concrete syntax to its formal semantics.
W3C Wab Application Definition Language (WADL)	Describes the Web Application Description Language (WADL). An increasing number of Web-based enterprises (Google, Yahoo, Amazon, Flickr, others) are developing HTTP-based applications that provide programatic access to their internal data. Typically these applications are described using textual documentation that is sometimes supplemented with more formal specifications such as XML schema for XML-based data formats. WADL is designed to provide a machine process-able description of such HTTP-based Web applications.
W3C WebService Definition Language (WSDL) Specifications	A WSDL document defines services as collections of network endpoints, or ports. In WSDL, the abstract definition of endpoints and messages is separated from their concrete network deployment or data format bindings. This allows the reuse of abstract definitions: messages, which are abstract descriptions of the data being exchanged, and port types which are abstract collections of operations.