|  |  |  |
| --- | --- | --- |
| Short Title | Name/Link | Security Control Area |
| OAuth 2.0 | **The OAuth 2.0 Authorization Framework**, IETF\* RFC 6749.  <http://tools.ietf.org/html/rfc6749> | Authorization:  Enables a third-party application to obtain limited access to an HTTP service. |
| TLS | The Transport Layer Security (TLS) Protocol, \*IETF RFC 5246<http://tools.ietf.org/html/rfc5246> | Provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. |
| HTTPS | **Secure Hypertext Transfer Protocol**  ("HTTP over TLS"), \*IETF RFC 5246  <http://tools.ietf.org/html/rfc2818> | Provides communications security over the Internet. Uses TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL (the  predecessor to TLS), distinguishing secured traffic from insecure traffic by the use of a different server port. |
| SHS | **Secure Hash Standards**  The current version of the SHS standard is the document [NIST FIPS 180-4](http://csrc.nist.gov/publications/PubsFIPS.html), which specifies seven: [Secure Hash Algorithms](http://en.wikipedia.org/wiki/Secure_Hash_Algorithm): [SHA-1](http://en.wikipedia.org/wiki/SHA-1), [SHA-224](http://en.wikipedia.org/wiki/SHA-224), [SHA-256](http://en.wikipedia.org/wiki/SHA-256), [SHA-384](http://en.wikipedia.org/wiki/SHA-384), [SHA-512](http://en.wikipedia.org/wiki/SHA-512), [SHA-512/224](http://en.wikipedia.org/wiki/SHA-512/224) and [SHA-512/256](http://en.wikipedia.org/wiki/SHA-512/256). | Integrity Assurance:  a set of [cryptographically](http://en.wikipedia.org/wiki/Cryptography) secure [hash](http://en.wikipedia.org/wiki/Hash_function) [algorithms](http://en.wikipedia.org/wiki/Algorithm) specified by the [National Institute of Standards and Technology](http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) (NIST). |
| AES or Triple-DES | **Advanced Encryption Standard**, Federal Information Processing Standards Publication 197, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>  **Triple Data Encryption Algorithm (“Triple DES”)** | Symmetric Encryption and Message Authentication:  AES replaces/update to DES  Triple-DES applies the DES cipher algorithm three times to each data block. |
| PKCS | A group of [**public-key cryptography**](http://en.wikipedia.org/wiki/Public-key_cryptography)**standards** by RSA, Inc.  Some have begun move into the "[standards-track](http://en.wikipedia.org/wiki/Standards-track)" processes of relevant [standards organizations](http://en.wikipedia.org/wiki/Standards_organization) such as the [IETF](http://en.wikipedia.org/wiki/IETF) and the [PKIX](http://en.wikipedia.org/wiki/PKIX) working-group.  <http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm> | Asymmetric encryption:  Standards #1-#15 for public key encryption |
| DSS | **Digital Signature Standards** managed by the  Organization for the Advancement of Structured Information Standards (OASIS), a global consortium that works on the development, convergence, and adoption of e-business and [web service](http://en.wikipedia.org/wiki/Web_service) standards.  <https://www.oasis-open.org/committees/download.php/22725/oasis-dss-overview.pdf> | Digital Signature |
|  |  | **\*** - A Normative Internet Standard as developed by the Internet Engineering Task Force of the [Internet Society](http://www.internetsociety.org) – a NFP international organization dedicated to |