

# Software Defined Perimeter Glossary



The permanent and official location for *Software Defined Perimeter Working Group* is <https://cloudsecurityalliance.org/software-defined-perimeter/>

© 2018 *Cloud Security Alliance* – All Rights Reserved

You may download, store, display on your computer, view, print, and link to International Standardization Council Policies & Procedures Security at <https://cloudsecurityalliance.org/download/international-standardization-council-policies-procedures>, subject to the following:

- (a) the Report may be used solely for your personal, informational, non-commercial use;
- (b) the Report may not be modified or altered in any way;
- (c) the Report may not be redistributed; and
- (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Report as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to International Standardization Council Policies & Procedures.

# Acknowledgements

## **Lead Authors**

Juanita Koilpillai

## **Contributors**

Jason Garbis

Junaid Islam

Shamun Mahmud

Siva Pochiraju

Alex Shiro

Michael Roza

## **CSA Analysts**

Ryan Bergsma

John Yeoh

**The Software Defined Perimeter (SDP) Working Group** is a Cloud Security Alliance research working group with the goal of developing a solution to stop network attacks against application infrastructure. Formed in 2013, the working group designed elements in a control channel based architecture using standard proven security components. They published a research artifact to determine if there was interest in the concept and called it SDP. The working group research was and will continue to be freely available for use without license fees or restrictions by the CSA.

# Preface

The Software Defined Perimeter (SDP) Glossary is a reference document that brings together SDP related terms and definitions from various professional resources. The terms and supporting information in the SDP glossary cover a broad range of areas, including the components of SDP and common supporting technologies.

Bringing together all the information in this document is meant to minimize misinterpretation about SDP and provide a good understanding in the least amount of time. A balance has also been struck between length of the definitions and understandability with reliance on the reference source as the final arbiter. The result is a common language to communicate, understand, debate, conclude, and present the results of the SDP framework.

## **802.1x**

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. 802.1X has proven to be the strongest method for authentication, affording ease of use in setting access permissions and enhanced security that is not based on pre-shared keys (PSKs), which has the potential to be lost or stolen. VPN access control typically uses 802.1X authentication. SDP architectures define a number of connection types including client-to-gateway, client-to-server, server-to-server, and private cloud-to-public cloud. Each of these connections depends upon strong authentication from layer 2 or 3 up to layer 7; 802.1x being one of these authentication mechanisms.

## **Attribute Based Access Control (ABAC)**

A mechanism for controlling access to resources based on user or process attributes. These attributes may be retrieved from an Identity Management System, from a user's device, or from the overall enterprise security ecosystem (e.g. risk level). SDPs can use attributes to control access to protected resources, as part of an SDP policy.

## **Accepting Host (AH)**

A trusted node within an SDP. The Accepting Host (AH) accepts the communication from the Initiating Host (IH) after the SDP Controller authenticates and authorizes the connection. The SDP Controller instructs the Accepting SDP Hosts to accept communication from the Initiating Host by leveraging policies required for two-way encrypted communications such as mutual TLS.

## **Accepting Host Controller Path**

The AH-Controller Path is the channel used for communication between each Accepting Host (AH) and the Controller.

## **Accepting Host Session**

The AH Session is the period of time that a particular Accepting Host (AH) is connected to a Controller.

## **Accepting Host Session ID**

A 256-bit randomized arbitrary number used once (NONCE), managed by the SDP Controller and used to refer to a particular Accepting Host (AH) Session.

## **Access Policy (SDP Policy)**

For every connection established, SDP must fundamentally determine which users (and/or devices) are permitted to access which resources (e.g. services, gateways), and under which circumstances (e.g. from certain locations). SDPs provide policy decision points and policy enforcement points for connections. A cloud service provider (CSP), who elects to protect its resources behind a SDP, must develop a balanced “registered user access control policy”, as an undue restricted policy is likely to result in the denial of access/service. Expected access control policy's performance attributes should become a part of the Service Level Agreement (SLA).

## **Agent ID (AID)**

The Agent ID (AID) is a 32-bit unique unsigned value that identifies a given Initiating Host (IH) and/or Accepting Host (AH) during Single Packet Authorization.

## **Authentication**

A process or action of verifying the identity of a user or process. Policies governing authentication may require single or multiple factors (see Multi-Factor Authentication below). SDP uses a combination of user authentication as well as device authentication for each connection between the initiating and accepting hosts.

## **Authenticators**

These are factors ( methods of identification) that are presented by users to a system or application to verify that they are who they claim they are. The three classic authenticators are 1. Something you know such as a password, 2. Something you have such as an ID badge or cryptographic key and 3. Something you are such as a fingerprint or other biometric data. The more factors required by the system reduces the risk of intrusion. Requiring more than one factor is referred to as Multi Factor Authentication (MFA). SDP access policies should support authenticators for user authentication.

## **Authorization**

The process of granting or denying access to a network resource. Access mechanisms are typically based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity. SDP uses a combination of user authorization as well as device verification or attestation. SDP policies can define a set of network services (such as geolocation, encryption for communications, etc.) that a given user (or group) is authorized to access, and under what circumstances.

## **Air-gapped Networks**

Air-gapped networks are trusted networks that are isolated from all other untrusted networks. These networks are used to mitigate network-based attacks, unauthorized access, and misuse. SDP is designed to provide an on-demand, dynamically provisioned, network that is the “equivalent of” an air-gapped network.

## **Certificate Authority**

In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. SDP architectures rely on a CA, which the Controllers use as a root of trust, and for generation of the TLS certificate. SDPs can also leverage U2F or UAF for user or device authentication without additional CA requirements, separate from the CA utilized for mutual TLS.

## **Cloud Access Security Broker (CASB)**

A cloud access security broker (CASB) is an on-premises or cloud based software that sits between cloud service users and cloud applications to monitor all activity and enforce security policies. SDPs typically rely on an organization’s existing Identity and Access Management system (and/or external CASB) or an external federated identity service for user authentication and user attributes (such as role or group membership).

## **Client-to-Authenticator (CTAP)**

Client-to-Authenticator Protocol (CTAP), from the FIDO alliance, is a protocol when used with a Web Authentication protocol, collectively enables users to leverage common devices to easily authenticate to online services — in both mobile and desktop environments. SDP can use this as an alternative to UAF and U2F for authenticating users to online services. CTAP enables external devices such as mobile handsets or FIDO Security Keys to work with W3C Web Authentication and serve as authenticators to desktop applications and web services.

## **Controller (SDP Controller)**

An appliance or process that controls secure access to isolated services by ensuring that users are authenticated and authorized, devices are validated, communications are established, and user and management traffic are separated. Initiating Hosts (often user devices) and Accepting Hosts (services and in some instances the SDP Gateway) connect to the SDP Controller.

## **Control Plane**

SDP architectures separate the control of connections called the 'control plane' from the actual connections used to transfer data. The control plane consists of those connections that enable the vetting of users, devices, and ensure access to authorized services only providing extra security for those connections used to transfer data.

## **Data Plane**

SDP architectures separate the control of connections from the actual connections used to transfer data called the 'data plane'. The data plane consists of two-way encrypted connections typically using mutual TLS or another mutual authentication mechanism.

## **Device Attestation**

A process that confirms or authenticates validation and verification of devices and/or associated policy data. SDPs should include a mechanism to prove that the proper device holds the private key and that the software running on the device can be trusted. Device attributes and contents (e.g. files, registry keys) may be used to validate the device.

## **Device Onboarding Process**

Device onboarding for SDP entails the process of including new devices such as mobile phones, servers, and other IoT elements into an SDP.

## **Dynamic Tunnel Mode (DTM)**

Dynamic Tunnel Mode (DTM) is the proposed SDP protocol and encapsulation for the IH to communicate with one or more AHs.

## **Firewall**

A firewall is a network security system that monitors, and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet. SDP architectures can enforce a 'deny-all' firewall policy ensuring that the trusted network enabled by SDP ensures the SDP will not respond to any connections from any clients until they have provided an authentic SPA.



## **Gateway (SDP Gateway)**

An SDP Gateway is an appliance or process that, once a user or device is authorized, allows access to protected processes or services. This gateway can also be used to effectively allow monitoring, logging, and reporting on connections protecting processes or services.

## **GeoLocation**

The identification or estimation of the real-world geographic location of an object, such as a radar source, mobile phone, or Internet-connected computer terminal. Geolocation can be used as a source of information upon which to make access decisions in an SDP. For example, access to resources from users located in certain countries may be blocked. SDPs may also compare user geolocation with connection attempts to detect credential theft.

## **Hypertext Transport Protocol Secure (HTTPS)**

HTTPS (HTTP Secure) is an adaptation of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network and is widely used on the Internet for web applications. In HTTPS, the communication protocol is encrypted by Transport Layer Security (TLS). SDPs require mutual TLS and provides additional user verification not provided by HTTPS.

## **Identity and Access Management**

Management of identities (e.g. user accounts, roles) that enable access to secured infrastructure, platform, and services. Identity systems serve as a source of authentication information as well as attributes for the managed identities. Identities may be associated with users (humans), or devices. SDPs typically rely on an organization's existing Identity and Access Management system (and/or external CASB) for user authentication and user attributes (such as role or group membership).

## **Initiating Host**

An initiating host is a trusted node in an SDP. The Initiating Host (IH) is the host that initiates communication to the Controller and to the AHs. It initiates a two-way encrypted connection to authorized Accepting Hosts.

## **Initiating Host (IH) Session**

The Initiating Host (IH) Session is the period of time that a particular IH is connected to a Controller.

## **Initiating Host (IH) Session ID**

A 256-bit randomized arbitrary number used once (NONCE) managed by the SDP Controller and used to refer to a particular IH Session.

## **Internet Protocol Security (IPSec)**

IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols. SDPs provide two-way secure connections over IPSec for the upper network layers.

## **Keyed-Hash Message Authentication Code (HMAC)**

HMAC is a computed “signature” often sent along with some data. The HMAC is used to verify (authenticate) that the data has not been altered or replaced. It is an integral element of the initial packet that initiates connections into the SDP.

## **Multi-factor Authentication (MFA)**

MFA is a method of identification in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). SDP access policies should support MFA for user authentication. There are several protocols such as UAF and U2F used for multi-factor authentication. SDPs can leverage U2F or UAF for user or device authentication without additional CA requirements, separate from the CA utilized for mutual TLS.

## **Multiprotocol Label Switching (MPLS)**

Multiprotocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks. MPLS directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence its name “multiprotocol”. Layer 3 VPN networks allow multiple customer sites to communicate securely at the IP level over a provider managed MPLS network. SDP architectures define several connection types and each of these connections needs to be secure from layer 2 or 3 up to layer 7; MPLS is one such mechanism.

## **Mux ID**

The 64-bit Mux ID (MID) is used to multiplex connections across a single IH-AH Tunnel in Dynamic Tunnel Mode. The most significant 32 bits form a unique value assigned by the Controller for each remote Service. It is referred to as the Service ID of the MID. The least significant 32 bits form a value maintained by the IH and the AH to differentiate among different TCP connections for a specific remote Service. This is referred to as the Session ID of the MID.

## **Network Access Control (NAC)**

Network access control (NAC), also called network admission control, is a method of bolstering the security of a private or “on-premise” network by restricting the availability of network resources to endpoint devices that comply with a defined security policy. NACs address layer 3 access control and connectivity. SDPs bolster the security of a private or “on-premise” network by securing layer 2 through 7 connectivity.

## **Network Segmentation**

A network segment is a portion of a computer network that is separated from the rest of the network by a device such as a repeater, hub, bridge, switch or router. Each segment can contain one or multiple computers or other hosts. SDPs provide network segmentation policies using gateways (defined above) and in addition the segments behind the gateways will block connections and not respond to any requests from clients until they have provided an authentic SDP.

## **Next Generation Firewall (NGFW)**

A Next-Generation Firewall (NGFW) is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functionalities, such as an application firewall or an intrusion prevention system (IPS). SDPs can sit behind the NGFWs and look for specific SPA packets prior to allowing authorized connections to services behind the firewall; thus, explicitly allowing authorized connections.

## **Privileged Account Management**

A set of additional controls for privileged access accounts e.g. developers and administrators. SDP is often used to control access by users or services with privileged accounts, increasing the security and visibility of access by these accounts by instantly providing information about the users making connections and from what device.

## **Public Key Infrastructure (PKI)**

A public key infrastructure is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage private and public keys used for encryption, decryption, hashing and signing. SDPs may use PKI for generation of TLS certificates and for secure connections. If no PKI infrastructure exists, SDPs can provide TLS certificates for use to secure connections.

## **Role Based Access Control (RBAC)**

RBAC is a policy neutral access control mechanism defined around roles and privileges. The components of RBAC, such as role-permissions, user-role, and role-role relationships make it simple to perform user assignments. SDPs can make use of role information (typically housed in an Identity Management System) to control connections to resources such as servers, devices, processes, and data as part of an SDP policy.

## Security Group

A security group is a named container for security group rules in cloud infrastructures. Examples are Cloud Security Group in Amazon Web Services or Network Security Group in Azure.. Security group rules provide Public Cloud users the ability to specify the types of traffic that are allowed to pass through, to, and from ports (Public/ServiceNet) on a cloud server. Cloud Security Groups can be effectively used with a SDP, by being set to ensure that inbound network access to cloud-based resources is only permitted from an SDP Gateway. By doing so, the SDP policy will act as the access control enforcement point, rather than the cloud security group. The cloud security group can also be used to require that outbound traffic be directed through the SDP Gateway, if supported by the SDP implementation.

## Secure Shell (SSH)

The SSH protocol (also referred to as Secure Shell) is a method for secure remote login from one computer to another. It provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption. It is a secure alternative to the non-protected login protocols (such as telnet, rlogin) and insecure file transfer methods (such as FTP). SDPs require using mutual TLS v1.2 and higher to enable secure connections and better management of keys that are typically not managed effectively with SSH remote logins and file transfers.

## Secure Sockets Layer (SSL)

SSL (Secure Sockets Layer), and TLS (Transport Layer Security), are protocols that provide data encryption and authentication between applications and servers in scenarios where that data is being sent across an insecure network, such as checking your email. The terms SSL and TLS are often used interchangeably or in conjunction with each other (TLS/SSL), but SSL is in fact the predecessor of the TLS — and SSL 3.0 served as the basis for TLS 1.0 which, as a result, is sometimes referred to as SSL 3.1. SSL v3.0 is effectively “dead” as a useful security protocol. Places that still allow its use for web hosting as placing their “secure web sites” at risk. SDPs require using mutual TLS v1.2 and higher to enable secure connections.

## Security Assertion Markup Language (SAML)

SAML, (pronounced sam-el), is an open standard for exchanging authentication and authorization information between parties, in particular, between an identity provider and a service provider. SDPs often support user authentication with identity providers via SAML; it supports the SDP model of connecting to existing enterprise identity management systems.

## **SAML Assertion**

An assertion is a package of information that supplies one or more statements made by a SAML authority. SAML defines three different kinds of assertion statements that can be created by a SAML authority: Authentication, Attribute, and Authorization decisions. SDPs can use a SAML assertion to authenticate and authorize users into the perimeter.

## **Security Token**

A security token (sometimes called an authentication token) is a small hardware device that the owner carries to authorize access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob. Security tokens provide an extra level of assurance through a method known as multi-factor authentication for SDPs.

## **Service ID**

The Service ID, a unique value assigned by the Controller for each remote Service, is the most significant 32 bits of the Mux ID.

## **Session ID**

The Session ID, a value maintained by the IH and the AH to differentiate among different TCP connections for a specific remote Service, is the least significant 32 bits of the Mux ID.

## **Software Defined Perimeter (SDP)**

A secure perimeter that is created based on policies to isolate services from unsecured networks. It's designed to provide an on-demand, dynamically provisioned air-gapped network, by first authenticating users and devices prior to authorizing the user/device combination to securely connect to the isolated services. Unauthorized users and devices are unable to connect to the protected resources. SDPs make extensive use of encryption, including mutual TLS for inter-component communications, and an HMAC within the Single-Packet Authorization packet.

## **Software Defined Network (SDN)**

A Software Defined Network is an approach to computer networking that allows network administrators to manage network services through abstractions of higher-level functionality. SDNs manage the networking infrastructure. This is done by decoupling the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane). SDPs secure all connections to the services running on the networking infrastructure. So, while SDN is the notion of establishing a dynamic networking infrastructure... getting users to connect point to point, fast and efficiently, with as much throughput as possible, SDP is about the ability to secure every connection at all layers of this dynamic network infrastructure.

## **Software Defined WAN (SD WAN)**

SD-WAN is an acronym for software-defined networking in a wide area network (WAN). An SD-WAN simplifies the management and operation of a WAN by decoupling (separating) the networking hardware from its control mechanism. This concept is similar to how software-defined networking implements virtualization technology to improve data center management and operation. While SD-WANs manage the infrastructure for IP networking, SDPs secure connections that use the infrastructure provided by SD-WANs.

## **Software Token**

A software token (a.k.a. soft token) is a type of two-factor authentication security mechanism that may be used to authorize the use of computer services. Software tokens are stored on a general-purpose electronic device such as a desktop computer, laptop, PDA, or mobile phone and can be duplicated. (Contrast hardware tokens, where the credentials are stored on a dedicated hardware device and therefore cannot be duplicated (absent physical invasion of the device).) SDP systems can rely on Software Tokens as a form of MFA, just as they can rely on a hardware token for MFA.

SDPs may use cryptographically secured tokens to transmit information (such as application authorizations) between its components.

## **Single Packet Authorization (SPA)**

A single packet protocol for service protection behind a default-drop packet filter that offers 1) asymmetric ciphers for encryption, 2) authentication with a keyed-hash message authentication code (HMAC) in the encrypt-then-authenticate model, 3) non-replayable packets that cannot be broken by trivial sequence busting attacks. Within SDP, SPA plays a key role by hiding servers (including the SDP Controller and Gateway) until and unless the initiating host sends a valid SPA packet as the initial connection request.

## **Single Packet Authorization OTP**

A Single Packet Authorization based on RFC 4226 (a document describing an algorithm to generate one-time password values, based on Hashed Message Authentication Code (HMAC), but modified to include a counter value which ensures a different password each time. It is used to uniquely identify the IH when initiating communication to both the SDP Controller and the AH.

## **Transmission Control Protocol (TCP)**

A transport layer protocol in the Internet protocol suite provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network. SDP communications between Client, Controller, and Gateway use the TCP protocol.

## **Transmission Control Protocol/Internet Protocol (TCP/IP)**

The design of protocols in the TCP/IP model does not concern itself with strict hierarchical encapsulation and layering. TCP/IP recognizes four broad layers of functionality which are derived from the operating scope of their contained protocols: 1. the scope of the software application; 2. the end-to-end transport connection; 3. the internetworking range; and 4. the scope of the direct links to other nodes on the local network. Despite TCP/IP using a different concept for layering than the OSI model, the TCP/IP layers are often compared with the 7 layer OSI scheme in the following way:

1. The Internet application layer includes the OSI 7) application layer, 6) presentation layer, and most of the 5) session layer.
2. Its end-to-end transport layer includes the graceful close function of the OSI 5) session layer as well as the OSI 4) transport layer.
3. The internetworking layer (Internet layer) is a subset of the OSI 3) network layer.
4. The link layer includes the OSI 2) data link layer and sometimes the 1) physical layers, as well as some protocols of the OSI's 3) network layer.

## **TCP / IP Ports**

In computer networking, a port is an endpoint of communication in an operating system. While the term is also used for physical devices, in software it is a logical construct that identifies a specific process or a type of network service.

A port is always associated with an IP address of a host and the protocol type of the communication. It completes the destination or origination network address of a message. Ports are identified for each protocol and address combination by 16-bit unsigned numbers, commonly known as the port number.

SDP communications between Client, Controller, and Gateway use the TCP / IP ports.

## **Transport Layer Security (TLS)**

A cryptographic protocol, successor to SSL, that provides security for communications over a computer or IP network. SDPs utilize a Mutual TLS (mTLS) connection between pairs of components, in which both components validate the authenticity of the other component while establishing a secure connection.

## **Trust Assessment**

Remote posture checking of an user's device to verify if endpoint protection is operating and if any blacklisted processes are running. Additionally Trust Assessment can also verify if a device is patched and that the hash values of software to detect tampering. Typically Trust Assessment is implemented over the SDP control channel before access to authorized applications is granted.

## **User Datagram Protocol (UDP)**

The User Datagram Protocol offers only a minimal transport service -- non-guaranteed datagram delivery -- and gives applications direct access to the datagram service of the IP layer. UDP is used by applications that do not require the level of service of TCP or that wish to use communications services (e.g., multicast or broadcast delivery) not available from TCP. SPA packets used to initiate connections could use UDP to ensure the SDP will not respond to any connections from any clients until they have provided an authentic SPA.

## **User Threat Management (UTM)**

This is a category of security appliances that combine a number of security features into a single appliance. Generally a UTM appliance includes firewall, gateway anti-virus, and intrusion detection and prevention capabilities.. UTM is designed protect users from blended threats while reducing complexity. The disadvantage of these appliances are that they can represent a single point of failure. To counter this vulnerability UTM's can be combined with SDP's to catch anything that gets through or around the UTM.

## **Universal Authentication Framework (UAF)**

The UAF protocol allows online services to offer password-less and multi-factor security. The user registers their device to the online service by selecting a local authentication mechanism such as swiping a finger, looking at the camera, speaking into the mic, entering a PIN, etc. The UAF protocol allows the service to select which mechanisms are presented to the user. Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms such as fingerprint + PIN.

SDPs can leverage U2F or UAF for user or device authentication without additional CA requirements, separate from the CA utilized for mutual TLS

## **Universal 2nd Factor (U2F)**

The U2F protocol allows online services to augment the security of their existing password infrastructure by adding a strong second factor to user login. The user logs in with a username and password as before. The service can also prompt the user to present a second factor device at any time it chooses. The strong second factor allows the service to simplify its passwords (e.g. 4-digit PIN) without compromising security. During registration and authentication, the user presents the second factor by simply pressing a button on a USB device or tapping over NFC. The user can use their U2F device across all online services that support the protocol leveraging built-in support in web browsers.

SDPs also leverage U2F or UAF for user or device authentication without additional CA requirements, separate from the CA utilized for mutual TLS.



**Virtual Private Network (VPN)**

A technology that securely creates a private network within another network (often an untrusted, public network such as the Internet) by incorporating encrypted connections through that network. A VPN provides confidentiality and integrity for private communications. SDPs provide the benefits of a VPN (message confidentiality and integrity) while overcoming the limitations of traditional VPN products like fine-grained access control.

**Web Authentication (WebAuth)**

The W3C's Web Authentication specification defines a standard web API that can be built into browsers and related web platform infrastructure to enable online services to use FIDO Authentication; UAF and U2F and CTAP being some of the authentication frameworks defined by the FIDO alliance.

# References

[https://en.wikipedia.org/wiki/IEEE\\_802.1X](https://en.wikipedia.org/wiki/IEEE_802.1X)  
[https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP\\_Specification\\_1.0.pdf](https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf)  
[https://en.wikipedia.org/wiki/Cloud\\_access\\_security\\_broker](https://en.wikipedia.org/wiki/Cloud_access_security_broker)  
<https://www.techrepublic.com/blog/tech-decision-maker/avoid-unexpected-problems-by-automating-device-onboarding/>  
<http://www.cipherdyne.org/fwknop/>  
[https://en.wikipedia.org/wiki/Firewall\\_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))  
<http://www.networksorcery.com/enp/topic/ipsecsuite.htm>  
[https://en.wikipedia.org/wiki/Multi-factor\\_authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication)  
[https://en.wikipedia.org/wiki/Multiprotocol\\_Label\\_Switching](https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching)  
[http://www.linfo.org/network\\_segment.html](http://www.linfo.org/network_segment.html)  
<http://searchnetworking.techtarget.com/definition/network-access-control>  
[https://en.wikipedia.org/wiki/Next-Generation\\_Firewall](https://en.wikipedia.org/wiki/Next-Generation_Firewall)  
<https://www.networkworld.com/article/2216499/wireless/what-is-802-1x-.html>  
[https://en.wikipedia.org/wiki/Software\\_Defined\\_Perimeter](https://en.wikipedia.org/wiki/Software_Defined_Perimeter)  
<https://en.wikipedia.org/wiki/SD-WAN>  
<https://www.ssh.com/ssh/protocol/>  
[https://en.wikipedia.org/wiki/Security\\_Assertion\\_Markup\\_Language](https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language)  
<http://saml.xml.org/assertions>  
<http://www.waverleylabs.com/software-defined-network-sdn-or-software-defined-perimeter-sdp-whats-the-difference/>  
<http://searchsecurity.techtarget.com/definition/security-token>  
[https://en.wikipedia.org/wiki/Software\\_token](https://en.wikipedia.org/wiki/Software_token)  
[https://en.wikipedia.org/wiki/Port\\_\(computer\\_networking\)](https://en.wikipedia.org/wiki/Port_(computer_networking))  
<http://www.esg-global.com/blog/software-defined-perimeter-sdp-essentials>  
<https://ijcsits.org/papers/vol2no42012/21vol2no4.pdf>  
<https://luxsci.com/blog/ssl-versus-tls-whats-the-difference.html>  
<https://www.w3.org/Protocols/>  
[https://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol)  
<http://www.networksorcery.com/enp/protocol/udp.htm>  
<https://www.nist.gov/itl/tig/projects/special-publication-800-63>  
[https://en.wikipedia.org/wiki/OSI\\_model#Comparison\\_with\\_TCP/IP\\_model](https://en.wikipedia.org/wiki/OSI_model#Comparison_with_TCP/IP_model)  
<https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf>  
<https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-uaf-overview-v1.2-rd-20171128.pdf>  
<https://www.kaspersky.com/resource-center/definitions/utm>