Certificates:

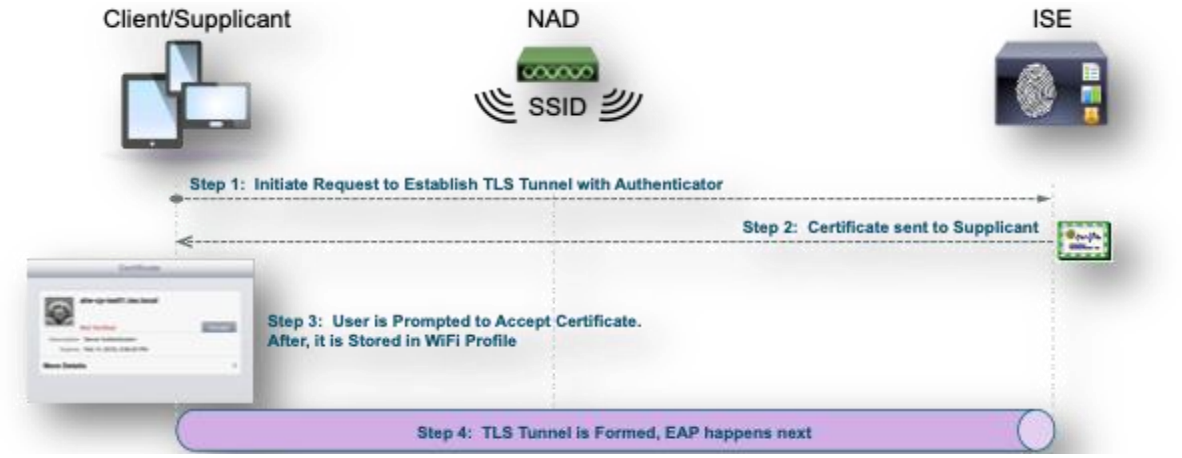
A certificate is a signed document that represents an identity. Certificate, is like a passport, a driver's license, or other personal identification card. That identification card is meant to represent you, and prove you are who you say you are. That certificate also contains the public key of that entity, so anyone with the public certificate will be able to encrypt data that only the certificate owner can decrypt. Certificates are employed often in a network implementing Secure Access. The certificates are used to identify the Identity Services Engine (ISE) to an endpoint as well as to secure the communication between that endpoint and the ISE node. The certificate is used for all HTTPS communication as well as the Extensible Authentication Protocol (EAP) communication.

Admin Certificate:

Admin certificate is used for internode communication and authentication of the Admin portal. Admin certificate is a server certificate used to authenticate or secure communication with ISE It is also used to establish trust relationship and secure communication between ISE Nodes in a Multi-Node deployment. Whenever, you browse to ISE GUI on an endpoint just like other HTTPS server, ISE will present its certificate to the client browser, if the client trusts the certificate, a TLS/SSL tunnel will be formed. The client will then send the required login credentials and further requests/response via the established tunnel. If the client did not trust the certificate a warning will be displayed on the browser which in most cases will give user, the privilege of accepting the risk and proceed to establish communication with the server. But if the client did not trust the certificate and not willing to accept the risk, then the HTTPS connection to ISE will be terminated.

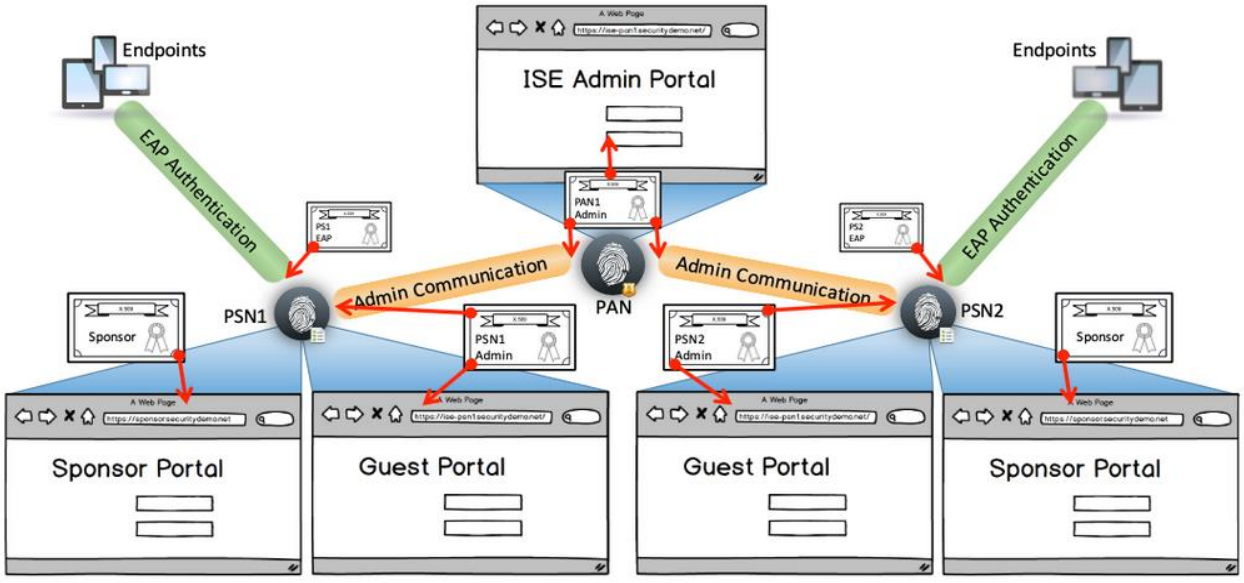
EAP Authentication Certificate:

Certificates are used with nearly every possible EAP method EAP-TLS, PEAP and EAP-FAST. With tunneled EAP methods such as PEAP and FAST, Transport Layer Security (TLS) is used to secure the credential exchange. Much like going to an HTTPS web site, the client establishes the connection to the server, which presents its certificate to the client. If the client trusts the certificate, the TLS tunnel is formed. The client's credentials are not sent to the server until after this tunnel is established, thereby ensuring a secure exchange. In a Secure Access deployment, the client is a supplicant, and the server is an ISE Policy Services node. The client must trust the server, and the keys from within the certificates are used to encrypt and decrypt the communication.



Portal Certificate:

Portal certificate refers to the sever certificate used to secure communication with all Cisco ISE web or end-user portals. Examples of end-user portal are Guest, Central Web Authentication CWA Portal, Sponsor Portal, My devices Portal and so on. As with all ISE portals, each one will need to identify itself and protect the communication to and from the portal with a certificate.

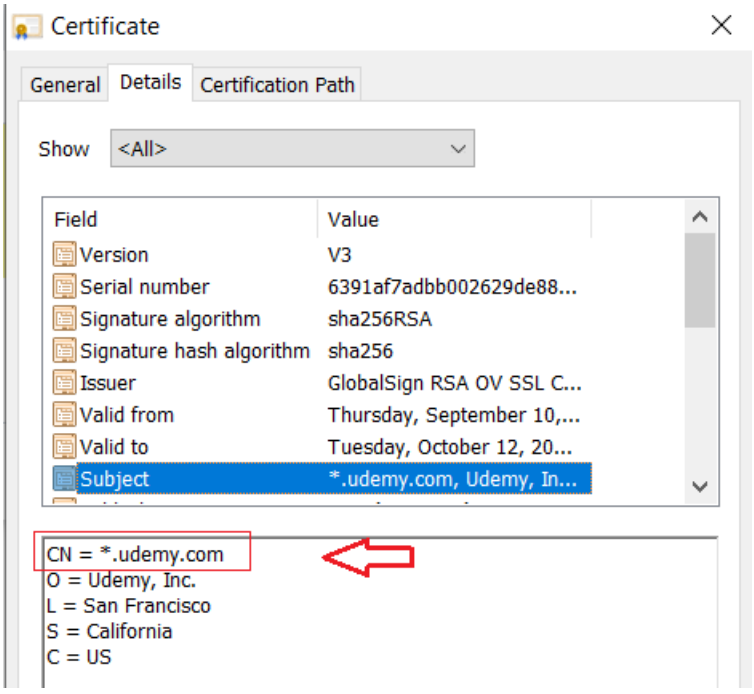


PxGrid Certificate:

When ISE is configured to be a pxGrid controller, it requires a certificate with both server and client extended key usages. PxGrid certificate is a client and server certificate used for establishing secure communication between pxGrid client and server.

Wildcard Certificate:

A wildcard certificate is one that uses a wildcard notation (an asterisk and period before the domain name) and allows the certificate to be shared across multiple hosts in an organization. An example CN value for a wildcard certificate's Subject Name would look like *.test.local. If you configure a Wildcard Certificate to use *.test.local, that same certificate may be used to secure any host whose DNS name ends in ".test.local", such as: aaa.test.local, psn.test.local, mydevices.test.local and sponsor.test.local



RADIUS DTLS:

RADIUS DTLS (RADIUS Datagram Transport Layer Security) certificate is a server certificate used for RADIUS DTLS authentication. RADIUS DTLS is used for encrypting RADIUS traffic between a Network Access Device (NAD) and RADIUS DTLS server Cisco ISE. RADIUS DTLS is a method used to authenticate network access devices with certificates instead of shared secrets (password). Example of Network Access Device are Access Switches, Wireless LAN Controller etc.

System Certificate:

The Certificates associated to the individual ISE Node. These are server certificates that identify a Cisco ISE node to client applications. Every Cisco ISE node has its own system certificates, each of which are stored on the node along with the corresponding private key.

Trusted Certificate:

Certificates Authorities ISE trusts. These are certificate authority (CA) certificates used to establish trust for the public keys received from users and devices. Certificates in the Trusted Certificates Store are managed on the Primary Administration Node (PAN), and are automatically replicated to all other nodes in a Cisco ISE deployment.

OCSP Client Profile:

Checks with the CA for revoked certificates. The Online Certificate Status Protocol (OCSP) is a protocol that is used for checking the status of x.509 digital certificates. This protocol is an alternative to the Certificate Revocation List (CRL) and addresses issues that result in handling CRLs. Cisco ISE has the capability to communicate with OCSP servers over HTTP to validate the status of certificates in authentications.

Certificate Signing Requests:

Template to create a signing request with CA. For a certificate authority (CA) to issue a signed certificate, you must create a certificate signing request (CSR) and submit it to the CA. To obtain signatures from a Certificate Authority (CA), you must export the CSRs & then send certificates to the CA. The CA signs and returns your certificates.

Certificate Authority:

Settings to turn ISE into a CA Server. The Cisco ISE Internal Certificate Authority (ISE CA) issues and manages digital certificates for endpoints from a centralized console to allow employees to use their personal devices on the company's network.