



Solve infrastructure security headaches

Using enrollment over secure transport (EST) to validate network devices and their identity

Securely deploying and managing network infrastructure should be an easy process, yet many organizations still struggle with cumbersome, potentially risky processes.



Executive summary

One of the unique challenges that network admins have is validating network devices and their underlying identity, then managing and integrating device identity into an internal Identity Store, such as a Public Key Infrastructure, or PKI. A PKI, whether public or private, allows for the use of certificates to cryptographically represent the specific identity of a device. Best practice is that each device has a unique certificate.

HPE Aruba Networking has for over 15+ years leveraged certificates to represent the identity of a device, and subsequently used certificate identity to represent different service and applications within our hardware. However, some organizations want to leverage their own internal PKI to issue a certificate and thus an identity. Historically this process was admin-heavy and prone to human error. Leveraging Enrollment over Secure Transport (EST) removes the headache and the possibility of human error.

Using EST, organizations using an internal PKI can upscale their infrastructure security by leveraging industry standards. This approach helps organizations avoid the shortcomings associated with other approaches, including approaches that generate certificates but use the same one on every device — a security disaster waiting to happen.

In this paper, you'll learn more about EST, its benefits, and how you can implement EST using HPE Aruba Networking Central.

What is EST?

Enrollment over Secure Transport (EST) is a protocol that has been developed to solve the process of automating [X.509 certificate](#) issuance for public key infrastructure (PKI) clients, like web servers, endpoint devices such as network equipment and user identities (i.e., network access points, gateways, etc.), and for any other place PKI certificates are used. EST can also automate distribution of the associated certificates from a trusted Certificate Authority (CA).

The EST protocol is defined in [RFC 7030](#) and standardizes an authenticated request and response exchange process with the CA via the EST server, making the process of deploying certificates on systems and devices more secure, faster, and easier for IT teams, compared to manually installing the required information.

EST is recognized for its ease-of-use and security features, including the use of HTTPS for secure transport and transport layer security (TLS) for client and server security. Unlike other widely used certificate management protocols like Simple Certificate Enrollment Protocol (SCEP), EST offers flexibility to support multiple crypto suites, such as Rivest-Shamir-Adleman (RSA), elliptic curve cryptography (ECC), and elliptic curve digital signature algorithm (ECDSA). In addition, SCEP has architectural security vulnerabilities that EST does not. For instance, SCEP works by providing a URL and key to devices, so anyone who gains access to that URL and key can enroll for a certificate. This attack allows the issuance of certificates that represent a user or device of the attacker's choice, which can be potentially used for privileged escalation.

Device validity: ensuring you get what you purchase

Today there is more focus than ever on having and deploying secured infrastructure, especially with the most recent supply-chain challenges. Secure deployments mean being able to confidently answer the questions:

- Do you know that you are truly deploying a device from vendor X?
- Do you know that this is the exact device you purchased, or the vendor manufactured, unmodified?

We at HPE Aruba Networking, from our very early days, consider security to be a critical part of our core offerings — it's why we lead with security-first, AI-powered networking.

Table of contents

- 2 Executive summary**
- 2 What is EST?**
- 2 Device validity: ensuring you get what you purchase**
- 3 How to secure the cert identity: why we use a TPM**
- 3 When are IDevID certs not a good fit?**
- 3 Provision certs and alternate identities to a device**
 - 4 Manual enrollment process
 - 5 Automatic enrollment process
- 5 How does EST work?**
- 7 Why use EST?**
- 8 HPE Aruba Networking-specific behavior**
- 8 Advantages of EST for HPE Aruba Networking devices**
 - 8 Process flow advantages
 - 9 Enrollment resilience advantages
- 10 Conclusion**





Consistent with this approach, we provide a digital identity for HPE Aruba Networking devices in the form of an X.509 certificate that is generated for a device in its manufacturing stage, creating a device-unique certificate that is stored and cryptographically secured within a Trusted Platform Module (TPM) for perpetuity of the device. This certificate is called an IDevID, or Initial Device Identifier. You can also think of it as a sort of device “birth certificate.”

These IDevID certificates are created securely under the HPE/Aruba PKI, and they can be used to provide cryptographic identity to a host for platform operations such as Cloud communications, RadSec, Wi-Fi Uplink, AP1X, or for peer-to-peer applications like IPsec or MACsec.

How to secure the cert identity: why we use a TPM

The cert (and private key) are secured in a TPM. A TPM is a microchip designed to provide security-related functions, primarily involving encryption keys. The TPM is installed on the motherboard of a computer or networking appliance and communicates with the rest of the system by using a hardware bus.

Devices that incorporate a TPM can create and encrypt cryptographic keys, so that the keys can only be decrypted by that specific TPM, making the TPM a very important component in the process. This process, often called “binding” a key, helps protect the key from disclosure. Each TPM has a primary binding key, called the storage root key, which is stored within the TPM itself. The private portion of a storage root key, or the endorsement key, that is created in a TPM is never exposed to any other component, software, process, or user, so the TPM is critical in the generation and security of the IDevID and thus the identity of the device.

When are IDevID certs not a good fit?

An IDevID certificate can prove that an AP is a genuine HPE Aruba Networking AP, not that it is a particular HPE Aruba Networking AP. Therefore, some organizations do not want to, or cannot, use the IDevID certificate to represent the identity of the device. Instead, they prefer to use their own PKI for end-entity certificate functions. For organizations with a large estate of networking equipment, this process would be administratively difficult, if not impossible, unless there was a way to automate the process of PKI installation. EST allows customers to tightly integrate HPE Aruba Networking equipment into their own PKI and provides a standards-based approach to certificate provisioning.

Note: The HPE Aruba Networking certificate that is provisioned as part of “birthing” a device in manufacturing can never be removed. The use of EST is to allow for the provisioning of **an additional digital identity** to be used in place of the IDevID for platform functions like RadSec, Wi-Fi uplink, or 802.1X for AP uplink, exposed as AP1x in the UI or IPsec tunnels, or wherever the certificate is involved.

The HPE Aruba Networking certificate that is provisioned as part of “birthing” a device in manufacturing can never be removed.

Provision certs and alternate identities to a device

For organizations that want to manage the certificate lifecycle and issue their own certificate identity, there are several methods of certificate enrollment. These methods facilitate obtaining digital certificates from CAs for securing communications and verifying the identity of entities. They can be categorized as **Manual** or **Automatic** enrollment, each catering to different use cases and environments.





Manual enrollment process

Manual enrollment is the traditional method where the entity generates a Certificate Signing Request (CSR) using software or tools provided by the server or device where the certificate will be installed. The entity then manually submits the CSR to the CA for validation and issuance.

This method is commonly used for obtaining single certificates such as TLS certificates for web servers. This manual process is unlikely to be adopted for critical infrastructure as the need would likely require creation, distribution, and management of hundreds if not thousands of device certificates.

Typical manual enrollment process steps

1. Build a trust establishment environment

Obtain the CA's certificates and establish a trust-anchor/trust-store database to build a trusted Public Key Infrastructure (PKI), which needs to be set up and managed.

2. Certificate Signing Request (CSR)

To initiate the certificate enrollment process, the end entity or user manually generates a Certificate Signing Request (CSR/pkcs#10). From this key-pair generation, ideally, the private key should be generated directly within the TPM (where a TPM exists), or at minimum stored and secured in a cryptographically encrypted place by the TPM.

Keep in mind, this process would be very difficult as access to the TPM requires API level calls, since TPM access is generally never exposed to a UI. The CSR includes the public key and information about the entity that needs to be included in the certificate, such as the domain name for TLS certificates or, more appropriately, the serial-number and/or MAC address for the device certificates. The generating entity signs the CSR using the associated private key. At this stage it's fair to assume that if a manual process was used to generate the key-pair, the private key is not intrinsically secure.

Note: PKI does **not** rely on a TPM or HSM to store keys or certificates. Doing so is completely optional but ensures that critically sensitive PKI elements of data can be stored in a tamper-proof secure enclave that cannot be breached.

3. Submitting the CSR to the CA

The CSR is submitted to the CA during the enrollment process. This would likely be via an API-driven interface (depending on the CA) or a manual upload/sign/download process, which is not very scalable. The CA verifies the identity of the entity and the information in the CSR. The CA may use various methods to verify the entity's identity: email verification, domain validation, and/or proof-of-possession (PoP) of the private key.

4. Certificate issuance

Once the CA has completed the verification process and is satisfied that the entity is legitimate, the CA issues a digital certificate. The certificate contains, among other things, the entity's public key, identity information, validity period, and the CA's digital signature.

5. Certificate delivery/installation

This certificate will require a manual download from the CA and uploading into the end-entity from where the



original CSR/pkcs#10 was generated. This should be where the private key is secured and public/private keypair were generated.

6. Certificate use

Once installed, the certificate is ready for secure communication protocols. Clients, users, or other entities interacting with the certificate holder can verify the certificate's authenticity through the CA's digital signature, ensuring a secure, authenticated, and trustworthy connection. These certificates can now be used to represent the appliance's identity for services such as RadSec, Wi-Fi uplink, or AP1X.

7. Certificate renewal

Certificates have a limited validity period; historically the validity was limited to one to two years but validity periods of less than one year are now common. Deployments are beginning to use shorter life cycles — 60-90 days or less — as security and identity of the infrastructure is accepted as critical. Before expiration, the entity must renew the certificate through a similar enrollment process to continue operations and allow usage of the device without disruption, as without a valid certificate operations and functions will cease. If the renewal is a manual process, then an organization is likely setting itself up for failure.

As can be seen, the complexity of a manual process is wide ranging, potentially very hands-on, potentially prone to error, and most importantly demands human intervention for creation and renewal. An automated process would likely remove human error and ultimately provide a simple and seamless solution.

Automatic enrollment process

Automatic enrollment streamlines the certificate issuance process by automating various steps and is particularly beneficial in large-scale environments with multiple devices or users. There are several automatic enrollment methods:

- ADCS
- ACME
- MDM
- SCEP
- EST

The next section examines the role EST plays in simplifying the end-entity certificate life cycle and ensuring that human error does not play any part in halting operations within your networking infrastructure.

How does EST work?

The EST enrollment service standardizes the interoperability and secure information exchange between a client and a CA required for provisioning RSA or ECC certificates. EST uses HTTPS as a transport protocol and leverages TLS ciphers to establish a secure TLS channel from an EST client to the EST server, which is used to send EST operations. EST is commonly applied to the enrollment of numerous certificate use cases, including web servers, networking infrastructure (e.g., switches, APs, gateways, etc.), DevOps, endpoint devices, IoT devices, user identities, email services, and any other place PKI certificates are used.

In a PKI architecture, the EST service is located between a client and the CA and performs several functions traditionally assigned to the Registration Authority (RA) role. The EST server's job is to provide validation of whether EST clients should receive the certificate they have requested, passing the request on to the CA, and returning the resulting certificate to the client, all within the process of the enrollment API. The client communicates with an EST server, which listens for requests on a well-known URL path. Clients just need to know the IP address/FQDN of the server to make requests.

The EST enrollment process is developed to be easy, e.g., API driven, for the establishment of automatic certificate issuance and renewal from a trusted CA.





The general client/server interaction proceeds as:

1. Configure URI

As EST operates over HTTPS, devices such as HPE Aruba Networking switches, APs, or gateways that need to make use of EST services will need to configure the URI used to access the EST server. EST mandates mutual authentication between the EST client and EST server. The EST server identifies itself with a certificate, just as a standard HTTPS website does. Preferably the EST client (AP/gateway/switch) identifies itself with a certificate during the initial TLS handshake. In the HPE Aruba Networking process the client, i.e., the networking device, will use the TPM IDevID certificate for its identity. However, there exists a workflow where a non-TPM device, such as a Virtual Gateway, does not have any of its certificates to present during initial enrollment attempt. In that case, EST server can authenticate the EST clients using the Username/Password or ChallengePassword once the initial TLS session is established. EST Client will mandatorily verify the EST server certificate. If using HPE Aruba ClearPass Policy Manager (CPPM) as your EST server, a simple shared-secret or basic HTTP authentication is also supported.

2. Distribute CA certificates

EST supports the concept of an “implicit trust anchor database.” This is essentially a list of CAs trusted by the EST server. Distribution of the CA certificates (and maybe a trust-chain), uses the API `/cacerts`. This allows EST clients to retrieve the current list of CA certificates needed for the PKI. The EST client goes through the same process that a browser goes through to determine trust, i.e., by matching the configured URI with the CN in the server certificate. This function does not require client authentication.

3. Verify trust

The client verifies the chain of trust from the server, including any intermediate certificates that lie between the root and the EST CA, and stores the root certificate.

4. Retrieve attributes

Retrieve CSR attributes that the CA requires clients to include in their enrollment and re-enrollment requests. As an example, this can include which elliptic curve to use, the length of an RSA key, or which hash algorithm to use. This step uses the API `/csrattrs`

5. Generate enrollment certificate

The client generates a key-pair and a CSR and the PKCS#10 certificate request and can include the attributes received in the previous step, signs the request with the private key and sends the request to the EST server. This step uses the API `/simpleenroll`

6. Request and receive certificate

The EST server subsequently requests and receives the certificate issued from the CA and then returns the signed certificate to the client in PKCS#7 format for storage on the client device. **Note:** The process to request the CA to sign the PKCS#10 is dependent on the CA capabilities. If using CPPM, the process is seamless as the EST server and CA are tightly coupled. Other deployments may have to utilize APIs or some other method in communicating with the CA. A third-party EST server could use our published REST APIs to integrate with the CPPM Onboard CA for cert signing and issuance.

7. Renew

Sometime after the initial cert provisioning there will be a need to Renew or rekey an existing certificate to replace one that is expiring or revoked (re-enrollment). This is one of, if not the, most important features within the EST framework. This process uses the API `/simplereenroll`

The above steps should be the MVP for leveraging EST to tightly integrate secure networking infrastructure to ensure devices are able to authenticate and leverage certificates for identity validity. EST processes can be used to issue certificates for services such as RadSec, Wi-Fi uplink authentication, etc.



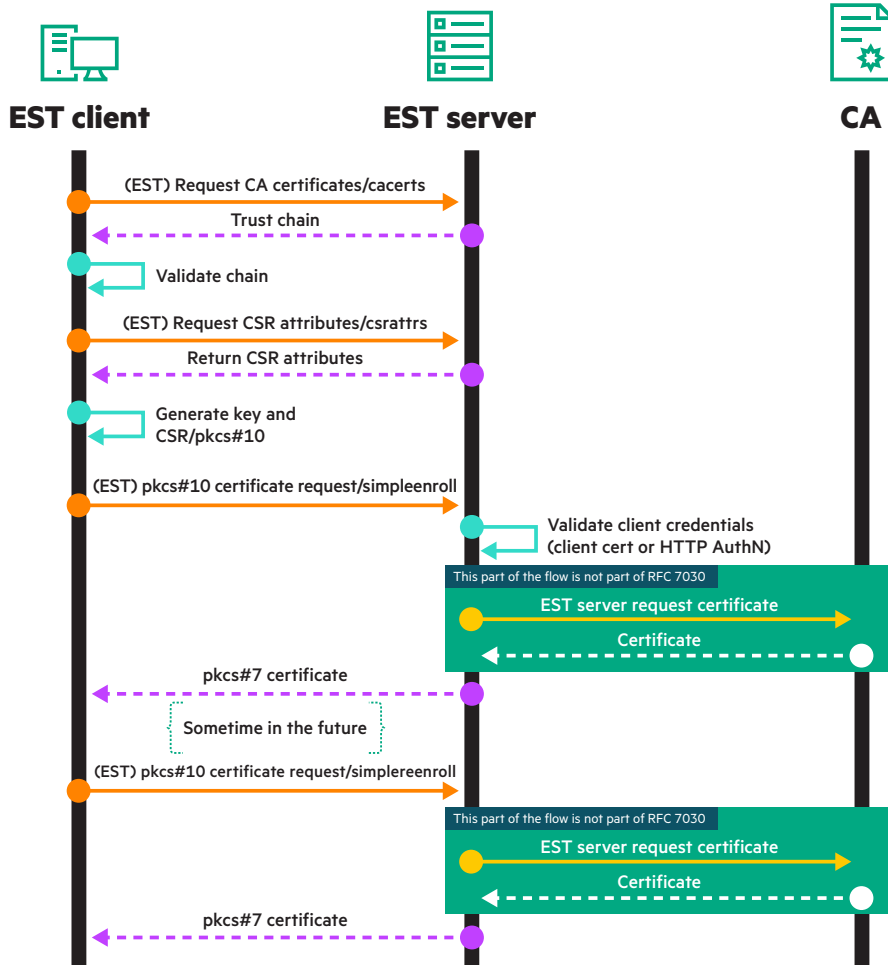


Figure 1. Pictorial view of the model EST process

In addition, an EST client can renew or rekey its existing client certificate by submitting a re-enrollment request to an EST server. This feature validates almost entirely the use of EST for certificate provisioning and renewal. Additional optional requests can be transported via EST to support other certificate operations, such as passing CSR attributes, that may be desired by the CA and server-side key pair generation back to the EST client. HPE Aruba Networking supports the following EST features via API across products to ensure EST services ensure a customer can securely deploy HPE Aruba Networking infrastructure securely with ease.

Why use EST?

While there is no stronger, easier-to-use authentication and encryption solution than the digital identity provided by PKI, there are many potential pitfalls inherent in managing PKI certificates manually as described earlier. Organizations need a certificate management automation standard to ensure certificates are correctly configured and deployed without human intervention, which generally leads to the prevalence of human error when something is being attempted at scale — mistyping, misspelling, monotony, etc.

Busy IT teams can ill-afford to manually deploy and manage certificates as doing so is time-consuming and highly error-prone due to the human element. Whether an organization deploys a single TLS certificate for a web server or manages millions of certificates across all networked endpoints, mobile devices, and user identities in an organization, the provisioning process from issuance to configuration and then deployment can take a significant amount of time. Furthermore, manually managing certificates also puts enterprises at significant risk of certificates being forgotten until after expiration, resulting in sudden and unwanted outage of critical business systems and potential exposure to attacks.





Manual certificate management that leads to missed certificate expiration can put enterprises at risk of sudden and unwanted outage of critical business systems and potential exposure to attacks.

The level of automation enabled by EST not only helps reduce risk but allows IT administrators to gain back precious time in their busy days. Also, other certificate enrollment approaches, e.g., SCEP, support only RSA as a digital signature mechanism and are known to have multiple security vulnerabilities. Globally some government services moved to ECDSA to achieve higher security with smaller keys. Protocols like SCEP prevent the use of ECDSA, as do legacy TPM 1.2 chips in older hardware.

It's critical today that any service that connects over the public internet is securely encrypted. The EST certificate enrollment feature will provide the ability to have new certificates installed on HPE Aruba Networking devices to use them for secure communications and secure services.

HPE Aruba Networking-specific behavior

The HPE Aruba Networking implementation and use of EST includes switches, gateways and controllers, and access points that run the EST client services. An EST server logically sits between a CA and a client requesting services such as certificate enrollment. Currently, no CAs support EST directly. In a solution that is completely powered by HPE Aruba Networking, ClearPass Policy Manager (CPPM) will typically act as the EST server as well as the root/subordinate/issuing CA depending on how you build your PKI. In this role, CPPM can issue certificates from an internal CA, or the requests can be relayed to a separate supported back-end CA, such as Microsoft Active Directory Certificate Services. For other customers who perhaps already have a CA environment deployed and running, an EST service plus orchestration between the EST client and the CA to utilize that existing PKI may be deployed.

While outside the scope of this discussion, a customer could also deploy a Registration Authority (RA) between the EST server and issuing CA. This could be used to validate the To-Be-Signed CSR and as well as used to ensure CSRs are customer policy-compliant.

Advantages of EST for HPE Aruba Networking devices

Process flow advantages

1. Several EST profiles can be configured. The EST profile configurations and EST activation commands are processed and handled by the Certificate handling service. While today some differences of EST capabilities exist across HPE Aruba Networking edge platforms, the core components listed here exist through all platforms.





2. As soon as EST is enabled, a device will process the EST activation and proceed to complete EST enrollment.
3. EST certificate enrollment or re-enrollment status can be seen in CLI using commands:
 - **AOS:** `show est status` or `show est cert`
 - **CX:** `show crypto pki ta-profile`, `show crypto pki est-profile <est_server>`, `show crypto pki certificate`
4. Once an endpoint has completed the certificate provisioning, an admin can assign the EST provisioned certificate to the application or process as required.
5. If tunnels were established using factory-cert based tunnels, then the **IPSec tunnel** using the **factory-cert** between **the device** and a Gateway will be torn down and a new tunnel will be established using the new EST certificate once provisioned.
6. Going forward, certs provisioned under EST, will automatically re-enroll without the requirement for an admin to touch anything, removing the human element that typically results in a maintenance miss and ultimately a service failure.

We continue to expand and develop our EST capabilities across our edge platforms with innovations such as multi-profile support to allow admins to assign different levels of security construct, enabling segmentation of users at different security levels, or enhancing how RadSec tunnels need to be secured, perhaps via different route CA/PKI.

HPE Aruba Networking supports a range of security ciphers, to match the current requirements for non-PQC RSA/ECC certificates, with support coming for PQC as recently specified by NIST.

HPE Aruba Networking algorithm support

- RSA (4096 key-length) with SHA256 signature
- RSA (4096 key-length) with SHA384 signature
- RSA (2048 key-length) with SHA256 signature
- RSA (2048 key-length) with SHA384 signature
- ECDSA (p256)
- ECDSA (p384)

Enrollment resilience advantages

Re-enrollment is almost the single most important reason organizations use EST. These benefits help ensure resilience to avoid disruption.

Retry mechanism

- Controller will do a continuous enrollment retry for every 5 minutes until it succeeds.
- AP will perform 3 retries every 5 minutes in case of enrollment failure if it is unsuccessful. If after the above retries EST has still failed, the AP will clear the EST parameters and trigger an AP reboot. AP will fall back to use factory certs.
- CX switch will perform by default 3 retries (configurable up to 32) every 30 seconds by default (configurable up to 600 seconds) after the initial request fails.

Certificate re-enrollment

- EST client should re-enroll a new certificate before expiry of its existing enrolled certificate, i.e., re-enrollment message is sent to the EST server when 75% of the certificate expiry time elapsed. This is relevant for AP and gateway; for switches, this is a configurable item. This 75% lapse of the certificate expiry is also applicable to both AP and controller.





- As part of the certificate enrollment, CertMgr will generate public and private key pairs. Public key will be part of the certificate, private key will be stored in an encrypted directory. It will be used only during the subsequent IKE/IPSec SA establishment. Re-enrolled certificates will not disturb existing IKE/IPSec SAs.
- The private key corresponding to this enrolled cert will be encrypted by the software-generated AES symmetric keys. These software-generated AES symmetric keys will be in turn encrypted by the device cert's public key. By doing this, CertMgr ensures that private keys are protected by the device's TPM.

Conclusion

Secure network infrastructure is a key component of many cybersecurity and compliance mandates. Several methods for validating network devices and their identity exist, but using enrollment over secure transport (EST) offers several advantages for organizations, especially those with large network estates. HPE Aruba Networking features enable organizations to experience the benefits of EST without the headaches.

Make the right purchase decision.
Contact our presales specialists.



Chat now (sales)



Call now

Visit [HPE.com](https://www.hpe.com)



Get updates


**Hewlett Packard
Enterprise**

© Copyright 2024 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Active Directory and Microsoft are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All third-party marks are property of their respective owners.

TWP_Infrastructure-Security-Headaches_A4_RB_110124 a00143307ENW