# EST
# Enrollment over Secure Transport

SPEAKERS:

- Freeman Huang
- Justin Noonan

aruba
a Hewlett Packard Enterprise company

# Agenda

1. Overview
2. Use Cases
3. Details/Caveats
4. Configuration and Best Practices
5. Troubleshooting
6. Demo
7. Resources

aruba
a Hewlett Packard
Enterprise company

# Overview

# Overview

- EST stands for Enrollment over Secure Transport. It defines the protocol that devices use to request trusted certificate authority (CA) certificates and to enroll/re-enroll device certificates from CA services via secure channels - HTTP over TLS.  Based on RFC 7030 (2013).

- With the support of a secure protocol like EST, devices can be configured to request the trusted CA certificates and to request enrollment/re-enrollment of device certificates automatically, without the need of human intervention, while maintaining the security and integrity of the whole enrollment process.

- An EST client is implemented as a part of the PKI infrastructure in the AOS-CX operating system. It expands the infrastructure's capability of obtaining CA certificates and device certificates from a manual to automatic fashion.

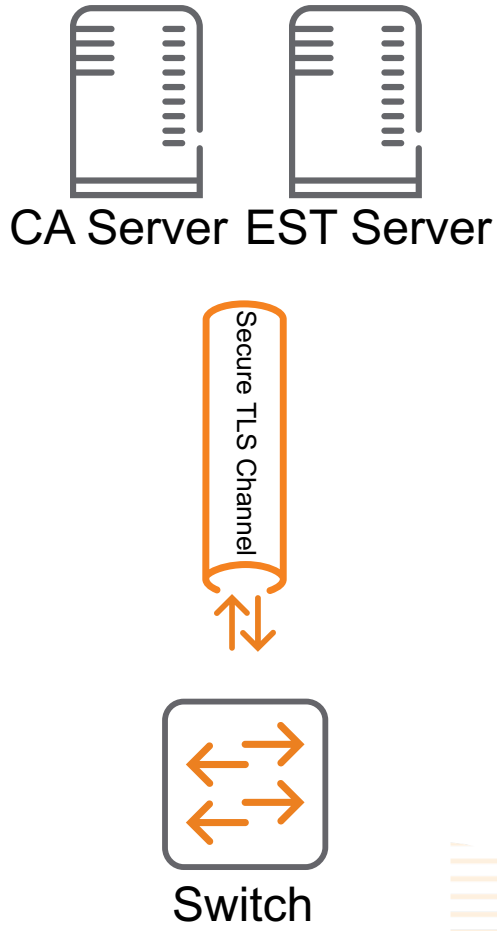
- EST client on AOS-CX uses HTTP over TLS. It relies on the availability of the TCP network, DNS service, and EST services reachable from the host CX switch.

aruba
a Hewlett Packard
Enterprise company

# Use Cases

# Use Case

- Previous to EST, Simple Certificate Enrollment Protocol (SCEP) was used
  - EST is easier to implement than SCEP
  - EST supports more security algorithms
- Leverages HTTPS as transport and TLS for many of its security attributes
- Devices can enroll and re-enroll certificates automatically instead of manual enrollment.
  - Example: Device gets the CA certificate automatically from EST server, to use a secured service such as RADSec, rather than a manual install of certificate to the device.
- Common supported service certificates in AOS-CX
  - Syslog
  - HTTPs
  - Captive Portal
  - RADSec
  - Hardware Switch Controller (HSC)



aruba
a Hewlett Packard
Enterprise company

# Details

# EST Details

- The EST client in the AOS-CX operating system requires CLI configuration to create EST profiles, each including an EST server URL, and the name of the VRF in which HTTP connection to the EST server can be established.
- At the time a user provides an URL for an EST profile, the EST client will try to contact the EST server and download the trusted CA certificate set. The trusted CA certificate set will also be downloaded right before a certificate enrollment or re-enrollment is made, in order to accommodate possible update to the CA certificates.
- The existing certificate enrollment user interface is expended to allow a parameter of EST profile name. When such parameter is provided, PKI (Certificate Manager) will call the EST client to perform the certificate enrollment.
- The current EST client implementation on AOS-CX supports up to:
  - 16 EST profiles
  - 63 trusted CA certificates downloaded from EST servers
  - 18 device certificates enrolled via EST services
- EST profile configuration is supported from both CLI console and REST API “PKI_EST_Profile”.
- CA certificate request and device certificate enrollment are supported from both CLI console and REST custom API “CertificateManager/certificate”.

aruba
a Hewlett Packard
Enterprise company

# Configuration

# Prerequisite for Certificate Enrollment via EST

- Establish the PKI infrastructure for the enterprise, with the CA chain and service ready to issue certificate. Issue a service certificate for the EST server. Optionally, issue a client certificate for the EST client.

- Install the root CA certificate in a TA profile on the Aruba CX switch that will validate the EST server certificate:

```
crypto pki ta-profile <ta-name>
ta-certificate [import [terminal|<REMOTE_URL>|<STORAGE_URL>]]
                    [vrf <VRF>]
```

- Optionally, preconfigure an EST client certificate on the Aruba CX switch.

- Optionally, set TLS to verify certificate purpose:

```
tls check-key-usage
```

- Establish the EST server reachable from the Aruba CX switch. Connect the CA service(s) to the EST server. If there is client certificate for the EST client, install the root CA certificate on the server that will validate the client certificate.

# EST Profile Configuration

In the global configuration context, create an EST profile and enter its context:

```
crypto pki est-profile <est-name>
```

In an EST profile context, configure the EST profile parameters:

```
url <URL>
vrf <VRF>
username <USER> password [ciphertext <PASSWORD> | plaintext <PASSWORD>]
retry-interval <SECONDS>
retry-count <COUNT>
arbitrary-label <LABEL>
arbitrary-label-enrollment <LABEL>
arbitrary-label-reenrollment <LABEL>
reenrollment-lead-time <DAYS>
```

# EST Profile Parameters

`url <URL>`

URL of the EST service. When this is set, the device will try to contact the EST service and download the trusted CA certificate set.

Example: `url https://example.com/.well-known/est`

`vrf <VRF>`

VRF in which the EST service is reachable. Default VRF is '`mgmt`' if supported, if not, default VRF is 'default'.

`username <USER> password [ciphertext <PASSWORD>|plaintext <PASSWORD>]`

The credential for the EST server to authenticate the client when requesting for CA certificates and for device certificate enrollment. Alternative is to set a device certificate for the EST client to present to any EST servers:

`crypto pki application est-client certificate <cert-name>`

# EST Profile Parameters (cont.)

`retry-interval <SECONDS>`

If certificate enrollment or re-enrollment fails, how much time to wait before retry

`retry-count <COUNT>`

If certificate enrollment or re-enrollment fails, how many time to retry

`arbitrary-label <LABEL>`

An optional label to concatenate to the EST URL when requesting EST service. This allows one EST server to support multiple CA's.

`arbitrary-label-enrollment <LABEL>`

An optional label to concatenate to the EST URL when requesting EST enrollment service. This allows the EST server to support multiple version of enrollment service.

`arbitrary-label-reenrollment <LABEL>`

An optional label to concatenate to the EST URL when requesting EST re-enrollment service. This allows the EST server to support multiple version of re-enrollment service.

`reenrollment-lead-time <DAYS>`

How many days before a certificate expiration time to start the re-enrollment request.

# Certificate Enrollment

In the global configuration context, create a certificate and enter its context:

```
crypto pki certificate <cert-name>
```

In a certificate configuration context, configure the certificate parameters:

```
key-type {rsa [key-size <size>] | ecdsa [curve-size <size>]}
subject [common-name <common-name>]
        [country <country>]
        [locality <locality>]
        [org <organization>]
        [org-unit <org-unit>]
        [state <state>]
```

In a certificate configuration context, enroll the certificate via an EST service:

```
enroll est-profile <est-name>
```

# Certificate Re-Enrollment

Re-enrollment is automatic for an EST-enrolled certificate:

- The re-enrollment request will be sent to the same EST server as that for the original enrollment;
- The EST client will present the enrolled certificate being renewed to the EST server for authentication. If the certificate has expired, or authentication fails for any reason, the EST client will fall back to use the username/password in the EST profile and perform a new enrollment;
- Users can configure reenrollment-lead-time with an EST profile to dictate how early the re-enrollment should happen for an EST-enrolled certificate.

# Checking EST Profile and Certificate Configuration

Show the list of EST profiles or the detail of an EST profile:

```
show crypto pki est-profile [<est-name>]
```

Each CA certificate downloaded from an EST server will be stored in a TA profile, with a TA profile name <est-name>-est-taNN, where NN is a two-digit sequence number. To show the list of TA profiles (including both user-configured and EST-downloaded), or the detail of an TA profile:

```
show crypto pki ta-profile [<ta-name>]
```

Show the list of certificates (including those manually enrolled and EST-enrolled), or the detail of a certificate:

```
show crypto pki certificate [<cert-name>]
```

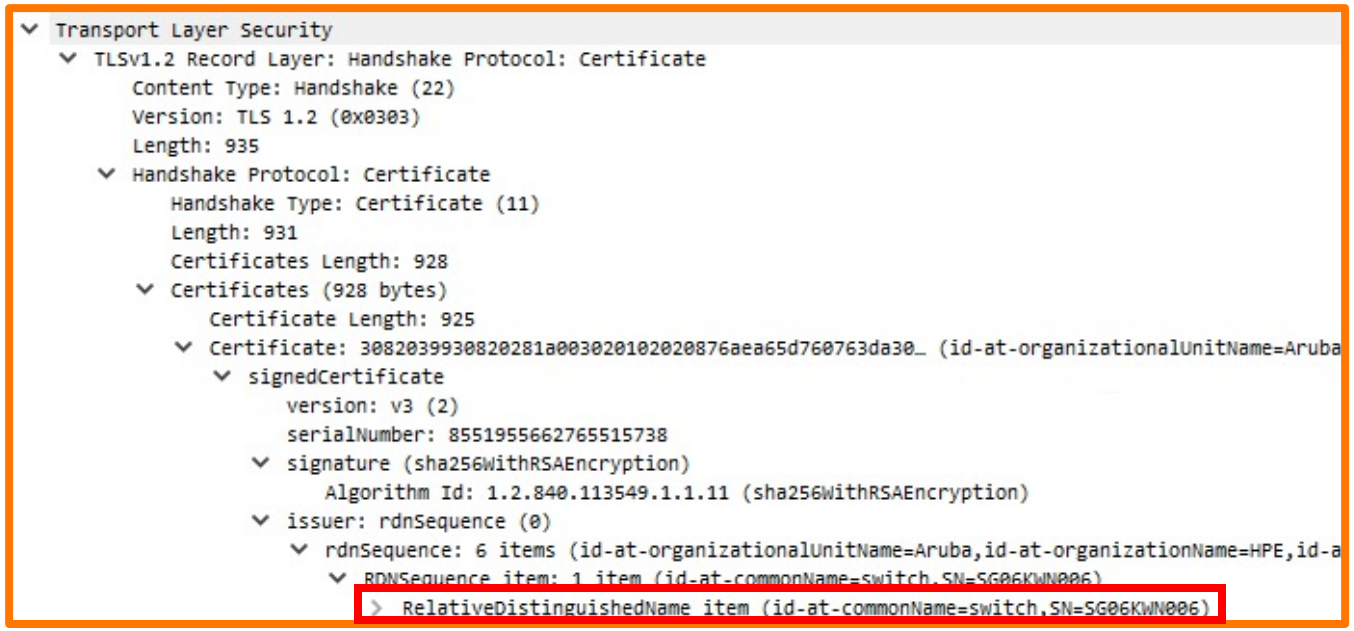
Show the certificate associated with EST client for authentication:

```
show crypto pki application
```

# Certificate Enrollment

Certificates exchanged between EST server and Client

| | | | | | |
|---|---|---|---|---|---|
| 193 | 4.403691 | 10.5.8.32 | 10.5.8.12 | TLSv1.2 | 571 Client Hello |
| 194 | 4.403826 | 10.5.8.12 | 10.5.8.32 | TCP | 60 2083 → 37667 [ACK] Seq=1 Ack=518 Win=30720 Len=0 |
| 195 | 4.418506 | 10.5.8.12 | 10.5.8.32 | TLSv1.2 | 1514 Server Hello |
| 196 | 4.418506 | 10.5.8.12 | 10.5.8.32 | TLSv1.2 | 1380 Certificate, Server Key Exchange, Certificate Request, Serve |
| 197 | 4.418572 | 10.5.8.32 | 10.5.8.12 | TCP | 60 37667 → 2083 [ACK] Seq=518 Ack=1461 Win=32128 Len=0 |
| 198 | 4.418572 | 10.5.8.32 | 10.5.8.12 | TCP | 60 37667 → 2083 [ACK] Seq=518 Ack=2787 Win=35072 Len=0 |
| 199 | 4.430930 | 10.5.8.32 | 10.5.8.12 | TLSv1.2 | 1389 Certificate, Client Key Exchange, Certificate Verify, Change |




Certificate shows switch S/N as subject name

aruba
a Hewlett Packard
Enterprise company

# Best Practices

# Feature Best Practices

- Establish time service to both the Aruba CX switch (the EST client) and the EST server, to ensure the date and time on both systems are in sync.
- EST server Includes not only the root CA certificate, but also the intermediate issuer CA certificates, in the trusted CA certificate set that will be sent to the client upon request.
- For all the CA certificates, make sure their “Basic Constraints” field has CA set to true, and (optionally) pathlen set to appropriate value. Make sure their “Key Usage” field set with keyCertSign.

In your openSSL config for CA certificates:

```
basicConstraints = CA:true,pathlen:2
keyUsage = keyCertSign
```

Example CA certificate:

```
... ...
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:TRUE,pathlen:2
    X509v3 Key Usage:
        Certificate Sign
... ...
```

# Feature Best Practices (cont.)

- For all leaf certificates, recommend to set their “Extended Key Usage” field with appropriate purpose (optional but required by NDcPP):
  - For server certificate, set with serverAuth, or “TLS Web Server Authentication” in display; also in “Key Usage” field has at least one of digitalSignature, keyEncipherment, and keyAgreement.
  - For client certificate, set with clientAuth, or “TLS Web Client Authentication” in display; also in “Key Usage” field has at least one of digitalSignature and keyAgreement.

In your openSSL config for server certificates:

```
basicConstraints = CA:false
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
```

Example server certificate:

```
... ...
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FLASE
    X509v3 Key Usage:
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication
... ...
```

In your openSSL config for client certificates:

```
basicConstraints = CA:false
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth
```

Example client certificate:

```
... ...
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FLASE
    X509v3 Key Usage:
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Client Authentication
... ...
```

# Troubleshooting

aruba
a Hewlett Packard
Enterprise company

# Feature Troubleshooting

- EST client implementation on AOS-CX has very good debug logging messages. Make sure you enable it at the debug level so that you get the most details:

```
debug pki all [severity debug]
debug destination {buffer|console|syslog} [severity debug]
```

- Some common issues:
  - Cannot connect to EST server
    - Cannot resolve the server domain name – DNS service not reachable
    - Connection rejected – TCP port correct?
  - CA certs request fails
    - Server URL correct? Include “/.well-known/est”?
    - Server certificate invalid - root CA certificate for server installed on switch? SAN/CN matches host name? cert purpose set appropriately?
    - All intermediate CA certificates and server certificate have required fields?
  - Enrollment fails
    - Username/password in EST profile correct? Or Certificate for EST client set correctly?
    - Certificate not yet valid – client and server clock sync’d?

# Demo

aruba
a Hewlett Packard
Enterprise company

# Resources

# Feature References

- RFC 5280: https://tools.ietf.org/html/rfc5280
- RFC 7030: https://tools.ietf.org/html/rfc7030

aruba
a Hewlett Packard
Enterprise company

# Thank You