White Paper

PKI: Simplify Certificate Provisioning with EST

What You Will Learn

The concept of a public key infrastructure (PKI) has existed for a long time. The PKI authenticates the identity of users and devices by means of signed public key pairs in the form of digital certificates.

Recently, the Internet Engineering Task Force (IETF) introduced the Enrollment over Secure Transport (EST) protocol to provision these certificates. In this white paper we discuss the advantages of EST. We also compare it with other certificate provisioning standards, namely:

- Simple Certificate Enrollment Protocol (SCEP)
- Certificate Management Protocol (CMP)
- Certificate Management over Cryptographic Message Syntax (CMC)

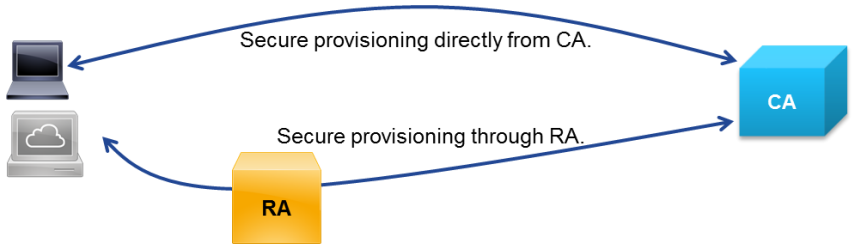
Contents

Introduction

Certificates have been used to authenticate devices and individuals for a long time. They are used to prove the identity of a device in the 802.1AR standard of the Institute of Electrical and Electronics Engineers (IEEE). They are also widely used in Transport Layer Security, VPNs, and many other areas that require authentication. The certificates are usually generated by a trusted entity or certificate authority (CA), and they can be validated using a PKI root of trust and a certificate chain.

Ubiquitous as certificates are, the PKI also needs a mechanism that can securely provide a certificate to an entity. A registration authority (RA) often serves as an intermediary. It can authenticate the client before getting a certificate from the CA (Figure 1).

Figure 1. Common High-Level PKI Architecture



EST

The most recently defined protocol that provides certificate provisioning is Enrollment over Secure Transport, IETF's RFC 7030. EST profiles certificate enrollment for clients using Certificate Management over Cryptographic Message Syntax (CMC) over a secure transport. According to the IETF, EST "describes a simple, yet functional, certificate management protocol targeting Public Key Infrastructure (PKI) clients that need to acquire client certificates and associated Certification Authority (CA) certificates. It also supports client-generated public/private key pairs as well as key pairs generated by the CA."

EST was a standardization effort that went through several iterations through the IETF. Multiple vendors and independent parties in the standards community participated in the effort. EST uses Public-Key Cryptography Standards (PKCS) 10 and Cryptographic Message Syntax (CMS) for certificate requests and certificate definitions, respectively. Cisco itself has open-sourced libEST, an EST library that offers client and server functionality, to promote adoption and interoperability across vendors.

SCEP

EST is the successor to the Simple Certificate Enrollment Protocol (SCEP), initially sponsored by Cisco. Because of its simplicity, SCEP has been the de facto protocol in certificate provisioning for many years. But it has never moved beyond an IETF draft. Recently it was taken up by IETF again (replacing a previous SCEP draft), but a lack of area director support makes standardization unlikely. SCEP has some important drawbacks, which we will describe later.

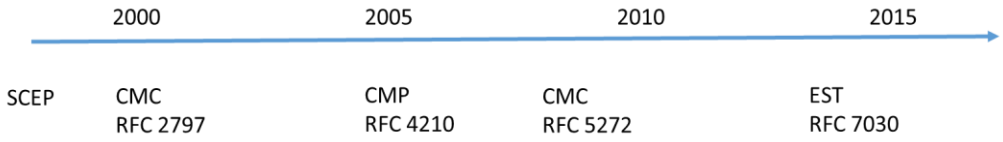
CMC and CMP

In 2000, before EST, the IETF defined "Certificate Management over CMS" (CMC) in RFC 2797. Eight years later, the "Certificate Management protocol using the Cryptographic Message Syntax" (also CMC) in RFC 5272 made RFC 2797 obsolete. CMC is architecturally very similar to SCEP, although it has more options and provides more algorithm agility. RFC 5272 defines a message format, message control, and data structures that provide a wide range of certificate management operations that go beyond the certificate provisioning of SCEP and EST. It uses the Certificate Request Message Format (CRMF) or PKCS 10 for certificate requests. Later, RFC 6402 updated some CMC messages and controls as well as the transport mechanisms (HTTP, file, email, TCP) defined in RFC 5273.

Between RFC 2797 and RFC 5272, IETF came up with a competing protocol in 2005: the Internet X.509 Public Key Infrastructure Certificate Management Protocol, or CMP. (CMP is defined in RFC 4210, which obsoletes RFC 2510). CMP also goes beyond certificate enrollment and defines its own message format. It was updated by RFC 6712, which describes HTTP as the CMP transport mechanism.

In summary, there are two protocols for certificate provisioning and enrollment: EST and SCEP. There are two protocols for certificate management: CMC and CMP. Certificate management covers certificate enrollment, revocation, status, batch requests, and more. **Error! Reference source not found.** shows the creation of these standards over time.

Figure 2. Certificate Management and Certificate Enrollment Standards over Time



In the next section we will present why we believe EST is the best option for certificate provisioning, and we will compare it with SCEP. We also will point out differences between EST and CMC and CMP.

Comparisons

EST Versus SCEP

The EST and SCEP protocols address certificate provisioning. Unlike CMC and CMP, they do not aim to solve all certificate management issues. Their main goal is to provide certificates to endpoints from a CA or through an RA (Figure 1). EST is a much newer protocol that overcomes some of SCEP's limitations. We recommend the use of EST over SCEP where possible for the following reasons:

- EST uses TLS for the secure transport of messages and certificates without the need for further enveloping the messages. SCEP runs over HTTP with pkiMessage messages that are secured in pkcsPKIEnvelope envelopes.
- In EST the certificate signing request (CSR) can be tied to a requestor that is already trusted and authenticated with TLS. In SCEP, the CSR is authenticated using a shared secret between the client and the CA, which introduces security concerns, explained below.

- EST provides cryptographic agility. It supports elliptic curve cryptography (ECC) and secure cryptographic algorithms to come. ECC is used in government mandates around the world. It is computationally more efficient, which benefits resource-constrained devices. SCEP doesn't support ECC because the PKCS 7 methods that it uses to protect data depend on RSA encryption. As stated in the recently submitted SCEP draft: "The message types, being based on CMS and PKCS #10, fully support algorithm agility but the requester has to use a key type that is supported by the server. Specifically, they must employ a PKC algorithm capable of both encryption and signing. RSA is the only widely-used algorithm that has these properties." Updating the algorithms to CMS and getting sufficient alignment with CMC to take advantage of the new work in this area would require as much effort as just moving to EST and wouldn't track with any of the standards work.
- Automated certificate re-enrollment or renewal is important. EST was built to support automatic re-enrollment. Even though the recently submitted SCEP draft includes renewal messages, that was not the case in the previous submission, nor were such messages commonly deployed in SCEP implementations.
- EST can support server-side key generation with an enrollment request. SCEP supports only the private key being generated at the client. Server-side key generation can be important in resource PKI (RPKI) environments or constrained devices that do not have enough power and entropy source to generate a random private key.
- EST was a joint standards effort that included vendors and the standards community. It received wide community scrutiny in its development phase in IETF. There is an open-source implementation of EST for vendors and private parties to adopt and experiment with. SCEP was developed in the 1990s, and even though it is widely used, it failed the vetting process in IETF that EST went through.
- EST offers CA rollover functionality for refreshing the trust anchors by using three certificates in a transition period. The transition period provides a path where all PKI entities can be rolled to the new CA root of trust incrementally without affecting communications between entities. SCEP requires a "flag day" for CA certificate updates. Operators cannot be sure if things will work until the flag day, because there is no transition period. Additionally, CA certificate updates are done using GetNextCACert messages. No request data is associated with this message, so the update is triggered by the CA, making CA rollover less flexible and less automated.
- EST does not provide a mechanism to retrieve a certificate's revocation status. SCEP defines a certificate revocation list (CRL) retrieval message so that endpoints can receive the revocation status of a specific certificate. CRL distribution points (CDPs) can also be retrieved from the certificates themselves. But even though CRL retrieval might be useful in some cases, certificate revocation goes beyond certificate provisioning or retrieving CRLs. Other options for revocation are the Online Certificate Status Protocol (OCSP) and OCSP stapling. CRLs were recently deprecated by Firefox in favor of OCSP. Moreover, if a CA doesn't use OCSP, it needs to break the CRL into multiple individual files. The SCEP method of requesting the CRL doesn't include this information, and thus a SCEP server either needs significant detailed information of the PKI CRL structures or needs the CA to use a non-scalable flat file for the single CRL. That is an important limitation.

In terms of **security risk** specifically, it is worth pointing out the following:

- In EST the certificate signing request (CSR) can be tied to a requestor that is already trusted and authenticated with TLS. The certificate is provided only to the entity requesting it, which owns the private key or username and password (proof of possession, or PoP). In other words, when PoP is enforced, clients cannot get a certificate for anyone but themselves. In SCEP the CSR is authenticated using a shared secret

between the client and the CA. The lack of a username complicates the distribution of the shared key, so in most real-world deployments the shared secret is not a onetime secret for each client. That introduces a vulnerability. Someone with access to the shared secret can generate certificates for entities other than himself. That could never happen in EST when PoP is used.

- TLS's proven security and continuous improvement helps ensure that EST transactions will be secure in terms of cryptographic protection. SCEP's tight integration with RSA to protect data introduces security concerns as technology advances (in processing speed or quantum computing, for example).

EST Versus CMC and CMP

EST does not address the same problems as CMC and CMP. EST addresses certificate provisioning, but CMC and CMP address certificate management, which includes enrollment, revocation, status, batch requests, and more. EST is a profile of CMC over a secure transport that focuses on key enrollment and renewal (leaving all other options to the full CMC messages). EST also follows the CMP paradigm for CA certificate rollover. CMC succeeded the CMP definition. It can be a little puzzling that the IETF defined two standards having the same goal in such a short timeframe. Their lack of mainstream acceptance is partly due to how complicated they are to implement.

EST differs in other ways from CMC and CMP:

- EST is more lightweight and its messages are simple. CMC is complicated because of the multiple wrappings of CMS messages, and the various Abstract Syntax Notation One (ASN.1) structures that define how the control data will be processed. Similarly, CMP uses enveloped message data.
- EST defines a secure transport mechanism and doesn't leave it open to interpretation or other standards.
- EST defines a server-size key-generation option with the enrollment request. By running over TLS, it makes the transfer of the private key simpler to send without extra encryption. CMC does not address the issue. There was a draft about CMC server-side key generation, but it was never ratified. CMP has server-side key generation as out of scope. Server-side key generation can be important in RPKI or constrained devices that do not have enough power and entropy source to generate a random private key.
- CMC does not address the renewal of CA certificates. EST combines the CMP-defined renewal of CA certificates into the CMC specification. The model is proven in the industry and now supported by the enrollment protocol.

Adoption

The protocols we presented in this document are used in various settings. It is important that readers have an idea about where the protocols have been adopted in the industry.

SCEP, being in existence for more than 15 years, is in many vendors' products. Almost all CAs support it, and it has been included in many standards. However, SCEP's limitations (presented above) make it unsuitable for modern environments.

On the other hand, the 3rd Generation Partnership Project (3GPP) standards body mandates CMP as part of its TS 33.310 standard. The actual use of CMP in TS 33.310 is limited to the provisioning functionality like the one described

in EST (although such a profile wasn't actually defined in IETF for CMP). CMP was also included in the National Institute of Standards and Technology's (NIST) Special Publication 800-57. Moreover, some CA vendors and PKI products support CMP. Some support CMC as well.

As for EST, even though it is much younger than SCEP, CMP, and CMC, it is used in IETF ANIMA WG's bootstrapping drafts. EST is also required in Hotspot 2.0, also known as HS2, defined by the Wi-Fi Alliance. Additionally, the International Electrotechnical Commission (IEC) created IEC 62351, which addresses security in power systems, and EST is the certificate provisioning protocol of choice. Finally, CA vendors are currently adding support for EST. Cisco's IOS and IOS-XE product already support EST.

Conclusion

The issue of certificate provisioning and PKI is ubiquitous. Even though other protocols are under consideration, we believe that EST is the best candidate solution for certificate provisioning because of its simplicity, the openness of its development, the open-source code available, and the advantages it offers over its counterparts.

The readers should note that the open-source libEST library is portable and easy to use. As time goes by, more clients and public certificate authorities will adopt EST. The open-source code will make it easier to quickly bring EST into more and more products, so vendors can use this common protocol in a modern and efficient manner.

References

EST RFC 7030: http://tools.ietf.org/html/rfc7030

libEST: https://github.com/cisco/libest

SCEP: https://tools.ietf.org/id/draft-gutmann-scep

Cryptographic Message Syntax (CMS): https://tools.ietf.org/html/rfc5652

Certificate Management over CMS (CMC): https://tools.ietf.org/html/rfc5272

Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF): https://tools.ietf.org/html/rfc4211

CMC Transport Protocols: https://tools.ietf.org/html/rfc5273

PKCS 10: https://tools.ietf.org/html/rfc2986

Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP): https://tools.ietf.org/html/rfc4210

PKCS 7: https://tools.ietf.org/html/rfc2315

Acknowledgments

Panos Kampanakis (panosk[at]cisco[dot]com)
Technical Marketing Engineer

Max Pritikin (pritikin[at]cisco[dot]com)
Principal Engineer

Thanks to Pete Beal and Peter Panburana for their valuable feedback.