Key and Certificate Management Reference Architecture

Peter Treacy

Pace University

Introduction to Cybersecurity FALL 2024 72308

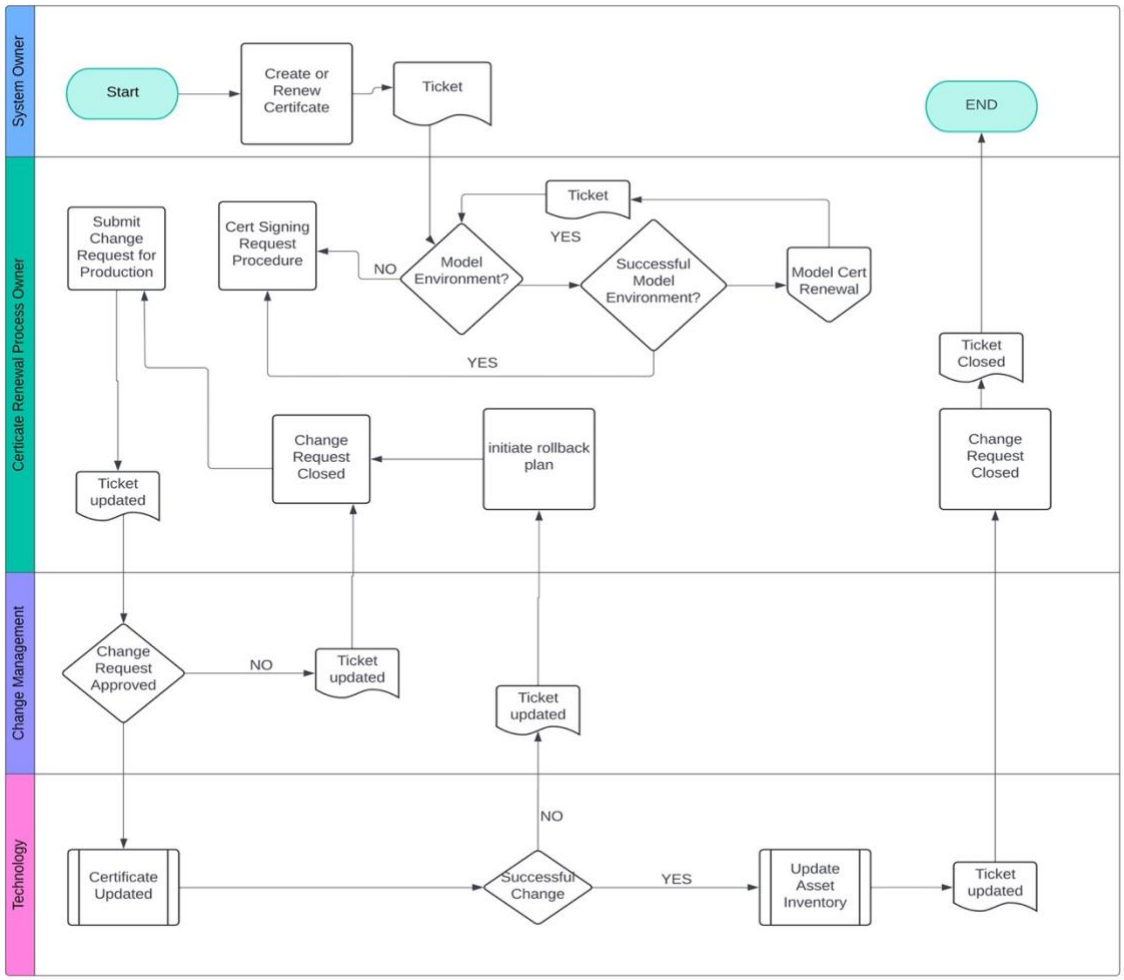
Todd Hammond

November 2nd 2024

Key and Certificate Management Process

Trust is everything when it comes to the Internet. TLS certificates play one of the most critical roles in keeping electronic communication between a client and server operating securely. This is the core fundamental concept of our modern-day Internet. Monitoring, processing, and executing every process in a certificate lifecycle is crucial for TLS protocol and internet security. The internet would be a digital Wild West without TLS certificates and our modern world can easily, safely, and securely transmit data to unknown endpoints. Let's see how they function:

Visual 1.1

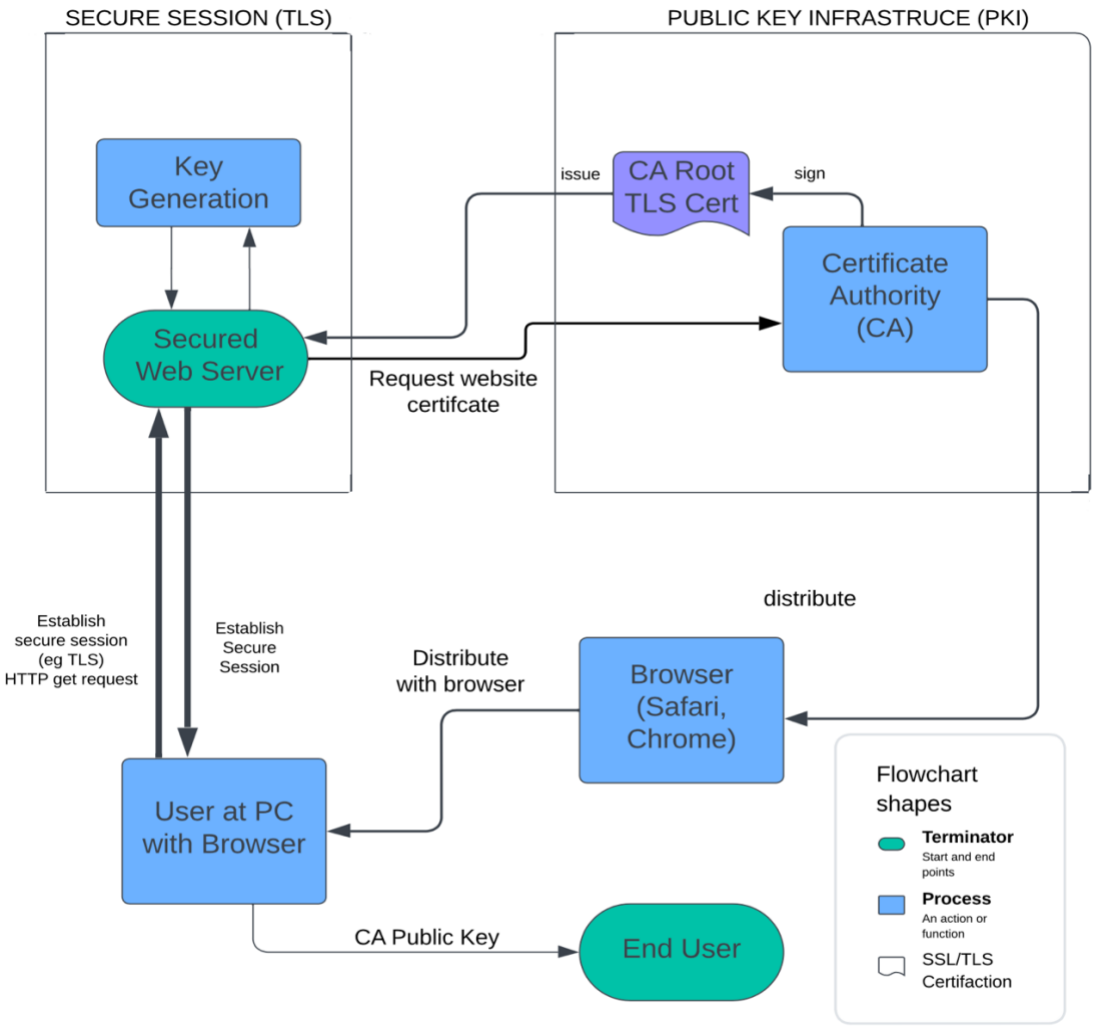


Visual 1.1 shows the complete lifecycle of a certificate renewal process. The process begins when an organization or individual realizes they need a certificate. The Certificate Signing Request (CSR) creates a ticket submitted to the Certificate Authority (CA) for validation. If there is already a certificate, a subprocess begins, which updates and approves the certificate that is already in place. Once the CSR is received, the Certificate Authority applies identity checks and domain checks. These certificates must be renewed before expiring, which is usually 12-36 months. If they are not updated periodically, the system will default to insecure, and web browsers will give warnings or display other problematic messages to clients looking to visit their web server, per the SSL/TLS protocol.

Certificate issuance improves transparency by providing key revocation and reducing reliance on trusted parties. The CT system has four components: CA, certificate log, certificate monitor, and certificate auditor. Verified information, such as the domain user's identity, expiration date, and certificate logs, is important. Monitoring systems and documenting the new certificate's expiration date and details are also important. Ideally, certificate logs will maintain a record of all SSL Certificates issued. (DigiCert, 2024)

To use a certificate, for secure e-mail, a sender would acquire the certificate of the intended recipient and validate it by checking the digital signature using the public component of the CA which issued the certificate. If successful, the user can be assured that the public key contained in the certificate belongs to the intended recipient and it is safe to encrypt a symmetric key with this public key. The message data can be encrypted with the symmetric key and the encrypted symmetric key can be placed in the secure e-mail header. (Yu and Ryan, 2017)

Visual 2.1



Visual 2.1 shows how cryptographic keys and certificates are generated, distributed, and securely stored. There are a lot of functions happening underneath the hood, and they're all equally important for this process to flow seamlessly.

TLS is the communication protocol that securely allows the certificate secure sessions to happen. The client/server applications communicate with this protocol to prevent eavesdropping or packet manipulation.

Diving into Key Generation

The Key Generation is fundamental to building trust between the server/client, it is located on the top left of Visual 2.1. NIST defines a cryptographic key as a "parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the correct key can reproduce or reverse the operation, while an entity without knowledge of the key cannot." (Barker et al.) Sensitive and high-value information can be vulnerable to attacks during transmission so cryptography relies upon these algorithms. The Federal Information Processing Standards (FIPS) and NIST SP (Special Publications) specify and approve which ones are acceptable.

Two types of keys can be generated: Symmetric and Asymmetric. Symmetric Keys are first generated with a Random Bit Generator (RBK). These ensure the strength needed for an unbreakable key, usually 128 or 256 bits (e.g. AES). The same key is used for both encryption and decryption, making it fast. That's where asymmetric differs; this method uses an RBK but both a public and a private key are created. The public key is freely shared, while the private one is kept secret. This is the process used for certificates and signatures. Diffie Helman is most commonly the key exchange algorithm for these two untrusted endpoints.

PKI**,** on the top right of Visual 2.1, is the system that signs and validates certificates. Its purpose is to enable secure communication from two unknown parties. They usually expire and have a set duration time, so this process must happen periodically.

A x.509 certificate management or CMS (Certificate Management System) can be used to monitor and execute the process for much-needed uninterrupted network operations. This process can monitor the entire certificate process in real-time and automate renewals and oversight. Designing a strategy is critical for a major business to gain control over its

infrastructure and prevent downtime. A faulty or misconfigured certificate could cost the enterprise a lot of revenue if its operation has network downtime. This includes all applications, servers, and devices involved.

Certificate revocation acts as a safeguard if an SSL/TLS certificate is compromised. When signs of trouble are detected, digital certificates should be revoked to prevent unauthorized users from impersonating entities or otherwise allowing bad actors to exploit compromised certificates. At the individual level, this ensures that each certificate is capable of carrying out its primary function: establishing secure connections and ultimately, greater peace of mind. Revocation capabilities are also important on a larger scale, as they play into broader risk management efforts and can help improve trust among web servers, browsers, and other parties. (France, 2023)

Each CA periodically issues a CRL or certificate revocation list to complement the revocations. The CRL uses serial numbers to identify revoked certificates. Firewalls support CRLs in Distinguished Encoding Rules (DER) and Privacy Enhanced Mail (PEM) formats.

As stated in Article 17 of the GDPR, non-compliance can result in hefty fines for any operational businesses that do not follow appropriate rules and regulations with regard to storing and managing a customer's data. PCI and DSS requirements that are not met can also cause a loss of customers, potential business growth, and a public perception of reputational damage. Security and trust throughout the TLS/Internet process is critical in ensuring businesses can operate safely and continuously to a vast audience, both domestically and abroad. It is a cornerstone of our modern economy and ensuring this process stays updated and well-run is one of the most important continuing milestones we’re faced with today.

References

Barker, Elaine, et al. *Recommendation for Cryptographic Key Generation*. 4 June 2020, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf, https://doi.org/10.6028/nist.sp.800-133r2.

France, Nick. "Certificate Revocation: What Happens When an SSL Is Revoked." *Sectigo® Official*, Sectigo, 2023, www.sectigo.com/resource-library/certificate-revocation-crl.

Yu, Jiangshan, and Mark Ryan. "Evaluating Web PKIs." *Elsevier EBooks*, 1 Jan. 2017, pp. 105–126, www.sciencedirect.com/topics/computer-science/certificate-issuance, https://doi.org/10.1016/b978-0-12-805467-3.00007-7. Accessed 27 Oct. 2024.

"How Does Certificate Transparency Work? | DigiCert FAQ." *Digicert.com*, 26 July 2024, www.digicert.com/faq/certificate-transparency/how-does-certificate-transparency-work. Accessed 1 Nov. 2024.