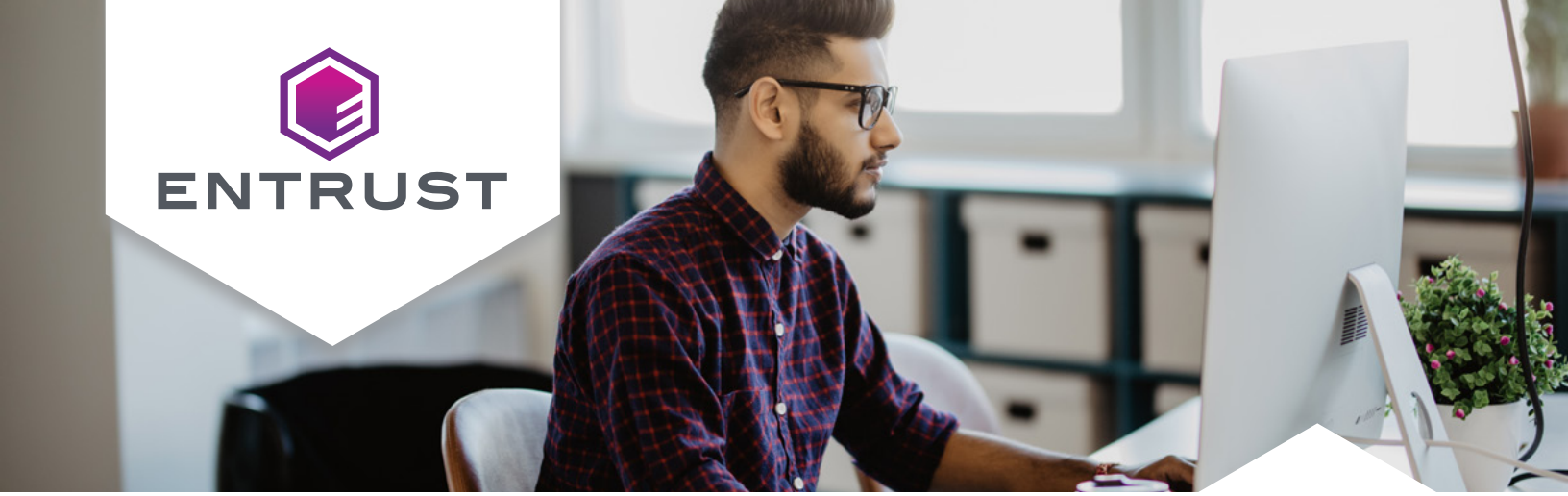

Six Pitfalls of a Poorly Designed PKI

Designing and implementing a well-structured and secure PKI is a complex process, requiring expertise and plenty of patience. If you're building your PKI in-house, be sure to write up a detailed plan before you get started. Fortunately, there are helpful resources such as our PKI Buyer's Guide.

When weighing whether to proceed in-house or to seek an external resource, consider the following six pitfalls of a poorly designed PKI. This does not pretend to be an exhaustive list of what could go wrong, but it highlights some of the major considerations.

If, after assessing your situation and the potential risks, you decide to engage with an external PKI resource, there's no shame in that – after all, your organization's security depends on it!

1

Cost and Reputational Damage

The theft of certification authority (CA) or root private keys enables an attacker to take over your PKI and issue bogus certificates, as was done in the Stuxnet attack. Any such compromise may force revocation and reissuance of some or all of the previously issued certificates. A root compromise, such as a stolen root private key, destroys the trust of your PKI and can easily drive you to re-establish a new root and subsidiary issuing CA infrastructure. This can be very expensive in addition to damaging to your corporate identity.

The integrity of the private keys throughout the infrastructure, from root to issuing CAs, provides the core trust foundation of your PKI and, as such, must be safeguarded. The recognized best practice for securing these critical keys is to use a FIPS 140-2 Level 3 certified hardware security module (HSM), a tamper-resistant device that meets the highest security and assurance standards.

2

Inadequate Separation of Duties

Weak controls over the use of signing keys can enable the CA to be misused, even if the keys themselves are not compromised. A malicious actor might issue certificates that allow a device or user to impersonate a legitimate user and conduct a man-in-the-middle attack or to digitally sign malware that is then propagated because it appears to come from a trusted source.

Proper security controls need to be established when designing your PKI. This includes separating CA roles and setting policies so that the operation fails if an individual attempts to perform more than one CA role. Setting up policies and procedures to ensure proper separation of duties, including establishing contingencies when a team member leaves, is critical to the security and integrity of the PKI and must be part of the initial design. It is preferable to implement a technology that enables a technical solution to the separation of duties policy. For example, presentation of an "M of N" smart card set can enforce a robust separation of duties policy by simply not allowing an individual to issue certificates without the presence of, for example, a security officer.

Six Pitfalls of a Poorly Designed PKI

3

Non-compliance and Failed Audits

Business applications that are subject to government or industry scrutiny may fail an audit if the underlying PKI is found to be inadequate. For example, many industries and regions are subject to specific compliance mandates covering digital signatures. An assessment that reveals weaknesses with the PKI may result in an expansion of the audit's scope, potential failure, and increased future scrutiny. The organization may also experience business disruptions until the audit is completed.

By establishing a PKI with tightly enforced key management, an up-to-date Certificate Policy and Certificate Practices Statement, and technically enforced security policies and procedures, organizations can simplify the task of demonstrating compliance with industry and regional mandates. They can prove that users and devices have been properly authenticated, which can help show that business applications comply with regulations and standards.

4

Insufficient Scalability

A PKI that fails to factor in the growth of the organization and its users will eventually need to be redesigned as the business scales, meaning lost productivity and customer impact. With new applications coming online daily and many users demanding access via multiple devices, PKI scalability must be considered from the outset.
Many organizations will need more than one CA to meet their growing requirements – certificates are used for logon authentication, digital document signing, email, and more. A root CA can act as the "master" with multiple subordinate CAs covering the various use cases. Alternatively, you can plan for scale by establishing multiple root CAs and multiple hierarchies. Regardless of your strategy, the goal is to get it right the first time to ensure your PKI can keep up with the growing needs of your organization.

5

Undetected Threats

Subversion of online certificate validation processes can enable malicious use of revoked certificates. An attacker who can prevent a certificate from reaching the certificate revocation list (CRL) can impersonate a legitimate actor and execute malicious activity while the victim is unaware that he/it is communicating with an illegitimate participant.

Defining certificate authentication policies and procedures is an instrumental part of a PKI's design. Further, proper execution and enforcement will ensure that revoked certificates and users are denied access. While many organizations will use a CRL, your organization might opt for a different approach, such as online certificate status protocol (OCSP) or authentication, authorization, and accounting (AAA).

Such decisions need to be part of the initial design discussions based on the needs of your organization. And remember, any private keys deployed in the certificate revocation process need to be protected equally with the keys that form the basis of the issuing process.

6

Lack of Trust and Non-repudiation

A PKI with inadequate security, especially referencing key management, exposes the organization to loss or disruptions if the organization can't legally verify that a message was sent by a specific user.

A PKI built with security and integrity at its core may provide you with protection in instances when user activity is in dispute. The secure digital signature provides credible evidence of the message's sender as well as the time it was sent, but it is only as defendable as the PKI is strong. By demonstrating that signing keys are adequately protected all the way back to the root key, your organization can defend against challenges to the authenticity of a specific user and their actions.

Six Pitfalls of a Poorly Designed PKI

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com