Public Key Infrastructures (PKI)

Secure Communications between People, Applications, and Devices

A Public Key Infrastructure (PKI) is a hierarchy of digital certificates. In digital communications, it allows the participants of a conversation to be uniquely identified and authenticated. This guarantees confidentiality and data integrity when using electronic services.

PKI and the Principle of Asymmetric Encryption

Digital certificates are used to secure communications over computer systems. They provide a form of digital verification that allows trust to be established between the sender and the receiver. PKI is based on the principle of asymmetric encryption. Every participant in an encrypted communication is assigned a key pair, consisting of a private key and a public key. The key-lock principle is then applied to all of their communications. Any file that is encrypted with an individual's public key can only be decrypted with the corresponding private key. A digital certificate contains the public key of a public-private key pair, together with information about who issued the certificate, on behalf of whom, and for how long the certificate will remain valid.

The PKI is the technical infrastructure used to generate and publicly distribute these certificates and encryption information. The PKI manages and hierarchizes the certificates. The so-called "root certificate" is the starting point and basis of trust of the hierarchy, and contains the relevant key pair. Every other certificate of the infrastructure is signed with the private key of the root certificate. These certificate chains can be made as long as necessary, provided that they begin with the root certificate. Any given certificate in the PKI is considered to be genuine and trustworthy if all certificates between it and the root certificate have been successfully verified.

The Benefits of a Public Key Infrastructure at a glance

Compliance with information security and non-repudiation requirements

A PKI helps to implement key information security criteria such as authentication, integrity, and confidentiality. Furthermore, the use of digital signatures ensures that the author of a signed message

cannot deny that he or she wrote the message.

Reduced administrative costs

The public keys of a PKI are managed centrally and must be protected against attacks. A centralized system considerably reduces the complexity and administrative effort associated with managing the various certificates and their keys.

Increased security and trusted automation of business processes

As well as improving security levels, PKIs facilitate the central administration of cryptographic security mechanisms and asymmetric encryption techniques. The use of digital certificates allows communication partners to benefit from high mutual credibility and trustworthiness. Digital signatures also allow business processes to be comprehensively automated by trusted procedures.

Easier to enforce policies and guidelines

A centrally administered PKI supports the company-wide implementation of guidelines and codes of conduct, e.g. for renewing and blocking certificates.

ASCONSIT: Careful Planning is Critical!

Businesses face a wide range of challenges when implementing a PKI. An inadequately planned PKI or

premature installation of specific software solutions can be disastrous. Short-term actions rarely achieve the desired results. This is especially true when it comes to implementing a PKI. The most important aspects are careful planning and system design, built upon the company's existing security concept. The overarching objective of a PKI is to standardize the various security and encryption procedures (e.g. for network logins, email access, or remote access from a home office) used by a company in order to minimize mistakes and reduce the administrative burden, thereby saving on expenses.

Our experts can help you to design a carefully planned and sustainably designed PKI!