Public Key Infrastructure (PKI)

Return to Glossary

A **Public Key Infrastructure (PKI)** supports the distribution, revocation and verification of public keys used for public key encryption, and enables linking of identities with public key certificates. A PKI enables users and systems to securely exchange data over the internet and verify the legitimacy of certificate-holding entities, such as webservers, other authenticated servers and individuals. The PKI enables users to authenticate digital certificate holders, as well as to mediate the process of certificate revocation, using cryptographic algorithms to secure the process.

PKI certificates include a public key used for encryption and cryptographic authentication of data sent to or from the entity that was issued the certificate. Other information included in a PKI certificate includes identifying information about the certificate holder, about the PKI that issued the certificate, and other data including the certificate's creation date and validity period.

Source: https://searchsecurity.techtarget.com/definition/PKI

From:
https://www.omgwiki.org/dido/ - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:p:pki&rev=1605548426

Last update: **2020/11/16 12:40**