

Digital Certificate

02.05.2024 01:50:18

FAQ-Artikel-Ausdruck

Kategorie:	RRZE: Glossary	Bewertungen:	0
Status:	öffentlich (Alle)	Ergebnis:	0.00 %
Sprache:	en	Letzte Aktualisierung:	15:19:31 - 25.06.2010

Schlüsselwörter

Identity, Security

Symptom (öffentlich)

Problem (öffentlich)

Lösung (öffentlich)

An electronic "document" based on the International Telecommunications Union (ITU) X.509 (1988) standard consisting of a public/private key pair; their usage is governed by a Policy and a Practice Statement. They can be used for verification, encryption and digital signing. A digital certificate can also serve as an electronic notary seal (stamp). A certificate contains a digital signature, verified by another certificate - this creates a chain of certificates that ends with the 'root' certificate (which is self-signed); the owner of the root certificate is called the Root CA.

A Trust Policy can specify appropriate uses for a certificate: "should I trust this certificate for this action?". For example an S/MIME policy specifies that in order to be trusted to verify a digitally signed email, a certificate must contain an email address that matches the address of the sender of the email. This should also be part of an Assurance Framework.

The structure of a digital certificate is: Certificate

- ... a. Version
- ... b. Serial Number
- ... c. Algorithm ID
- ... d. Issuer
- ... e. Validity
 - ... i. Not Before
 - ... ii. Not After
- ... f. Subject
- ... g. Subject Public Key Info
 - ... i. Public Key Algorithm
 - ... ii. Subject Public Key
- ... h. Issuer Unique Identifier (Optional)
- ... i. Subject Unique Identifier (Optional)
- ... j. Extensions (Optional)

Certificate Signature Algorithm
Certificate Signature.

Source: "<http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html>"