Encryption

04.05.2024 22:59:02

FAQ-Artikel-Ausdruck

Kategorie:	RRZE: Glossary	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	15:28:30 - 25.06.2010

Schlüsselwörter

Security

Symptom (öffentlich)

Problem (öffentlich)

Lösung (öffentlich)

The conversion of clear text (readable data) into a form called cipher text that cannot be easily understood by unauthorised people or systems, by using cryptographic keys. These keys need to be kept secure from software hacking and loss - PC motherboards that have a Trusted Platform Module can be used. For example; Microsoft's BitLocker in Vista can use the TPM chip to store disk encryption keys.

Authentication data should also be encrypted from its initial input source to the final authenticator to ensure that it is protected from in-transit attacks - this especially applies to smart-card readers and biometric devices.

Encryption methods are either symmetric or asymmetric. In symmetric algorithms (Private-key cryptography), e.g. DES (USA 1976, 56-bit key, can now be broken in less than 24 hours), TripleDES (168-bits or three 56-bit DES keys) and more recently AES (USA 2001, fixed block size of 128 bits and a key size of 128, 192 or 256 bits, approved by NSA for TOP SECRET), the sender and receiver must have a shared key set up in advance and kept secret from all other parties; the sender uses this key for encryption, and the receiver uses the same key for decryption. In an asymmetric key algorithm, e.g. RSA (USA 1977, MIT 1983, based on factoring large prime numbers, typically 1024 or 2048 bits long) there are two separate keys: a public key is published and enables any sender to perform encryption, while a private key is kept secret by the receiver and enables only him to perform decryption.

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