Ephemeral Key

27.07.2024 06:59:22

FAQ-Artikel-Ausdruck

Kategorie:	RRZE: Glossary	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	15:40:48 - 25.06.2010

Schlüsselwörter

Identity, Security, Access

Symptom (öffentlich)

Problem (öffentlich)

Lösung (öffentlich)

A cryptographic key associated with an expiration time. The ability to encrypt data in such a way that ensures it cannot be decrypted after a given date/time. This results in ephemeral data. One party establishes a number of ephemeral public/private key pairs, each of which will be destroyed at a time in the future and makes them publicly available; a second party then selects one of these key pairs having an expiration time appropriate for its needs. The requesting party first encrypts the data using an encryption key of the party which will receive the message, and then encrypts the resulting encrypted data again using the acquired ephemeral encryption key. It is not necessary to encrypt an entire message using an ephemeral encryption key; it may simply be used to encrypt another key contained within the message header.

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