Anleitung zur sicheren Kommunikation mit externen Partnern für S/MIME Verschlüsselung

enercity betreibt ein eigenes Signatur- und Verschlüsselungsgateway, um vertrauliche Kommunikation per E-Mail mit externen Partnern zu gewährleisten. Unterstützt werden dabei folgende Standards und Algorithmen.

Standard

- S/MIME nach RFC 2633 (S/MIME Version 3 Message Specification)
- OpenPGP nach RFC 2440 (OpenPGP Message Format) und RFC 3156 (MIME Security with OpenPGP)

Kryptographische Algorithmen

- Asymmetrische Verschlüsselung: RSA, DSA, El Gamal, Diffie-Hellmann
- Symmetrische Verschlüsselung: RC4, 3DES, Blowfish, Twofish, Cast5, AES, AES192, AES256
- Hash: MD5, MDC2, SHA, SHA-1, RipeMD160

Generelle Regelung zum Vertrauensstatus

- Generell werden nur vertrauenswürdige Zertifikate von enercity anerkannt.
- Die Zertifikate müssen für die Signatur und/oder Verschlüsselung von E-Mails ausgestellt worden sein.
- Es wird ein selektives Vertrauen nach entsprechenden Erfordernissen eingerichtet.
- Das heißt, die IT-Administration reagiert auf entsprechende Erfordernisse und pflegt die Vertrauensverhältnisse nach erfolgreicher Verifikation ein.
- Organisationen, die eigene Public Key-Infrastrukturen betreiben, wird nach Überprüfung der jeweiligen Policys vertraut.

Es wird kein Zertifikat anerkannt, das von Einzelpersonen, E-Mail-Clients oder anderen Tools erstellt wurde. Des Weiteren wird keinem Testzertifikat von Trustcentern vertraut.

Informationen zu Zertifikaten und Schlüsseln

enercity verwendet primär S/MIME Class 2 Zertifikate der Deutschen Telekom, Zertifizierungsstelle TeleSec Shared-Business-CA

Voraussetzungen seitens des Kommunikationspartners

- Der Partner muss der Deutschen Telekom Zertifizierungsstelle (Trustcenter) vertrauen.
- Um die Verifikation der Zertifikate zu ermöglichen, muss der Zugriff auf die bereitgestellten CRLs gewährleistet sein (http oder ldap Download der CRL-Listen).