Schlüssel-verwendungs-zwecke

ASN.1 steht für "Abstract Syntax Notation One"

digitalSignature (0) Dieser Schlüsselverwendungszweck gibt an, dass der öffentliche Schlüssel zur Erzeugung digitaler Signaturen verwendet werden kann. Dies wird typischerweise für die Authentifizierung und Integritätsprüfung von Daten verwendet.

nonRepudiation (1) Dieser Zweck stellt sicher, dass der Inhaber des privaten Schlüssels nicht abstreiten kann, dass er eine bestimmte Aktion ausgeführt hat. Es wird oft in Zusammenhang mit digitalen Signaturen verwendet, um die Nichtabstreitbarkeit von Transaktionen zu gewährleisten.

keyEncipherment (2) Dieser Zweck ermöglicht die Verschlüsselung von Schlüsseln, die zur Verschlüsselung von Daten verwendet werden. Es wird häufig bei der SSL/TLS-Verschlüsselung von Kommunikationskanälen eingesetzt.

dataEncipherment (3) Dieser Zweck ermöglicht die direkte Verschlüsselung von Daten mit dem öffentlichen Schlüssel. Es wird oft bei der symmetrischen Verschlüsselung von Daten verwendet.

keyAgreement (4) Dieser Zweck legt fest, dass der öffentliche Schlüssel zur Vereinbarung eines geheimen Schlüssels verwendet werden kann. Es wird typischerweise in Schlüsselaustauschalgorithmen wie Diffie-Hellman verwendet.

keyCertSign (5) Dieser Zweck ermöglicht es dem Schlüssel, andere Zertifikate zu signieren. Es wird normalerweise für Zertifizierungsstellen verwendet, um Zertifikate zu signieren.

cRLSign (6) Dieser Zweck ermöglicht es dem Schlüssel, Zertifikatswiderruflisten (CRLs) zu signieren. Eine CRL listet Zertifikate auf, die nicht mehr gültig sind.

encipherOnly (7) Dieser Zweck gibt an, dass der öffentliche Schlüssel nur zum Verschlüsseln von Daten, nicht aber zum Entschlüsseln, verwendet werden kann.

decipherOnly (8) Dieser Zweck gibt an, dass der öffentliche Schlüssel nur zum Entschlüsseln von Daten, nicht aber zum Verschlüsseln, verwendet werden kann.

Dr.Kleinhirn.eu