Kryptografische Schlüssel und Zertifikate

Einführung

Diese Dokumentation erläutert kryptografische Schlüsselarten, ihre Einsatzgebiete und die praktische Verwendung unter Linux. Sie unterscheidet **Software**, **Protokolle** und **kryptografische Verfahren**.

Schutzziele

Ziel	Beschreibung
Vertraulichkeit	Nur berechtigte Stellen können Inhalte lesen.
Integrität	Unbemerkte Änderungen werden erkannt.
Authentizität	Ein Schlüssel oder Kommunikationspartner kann überprüft werden.
Authentifizierung	Ein System überprüft die Berechtigung einer Gegenstelle.

Grundlagen

- Symmetrische und asymmetrische Kryptografie, Schlüssel und Passphrasen
- Hashwerte, Fingerprints und digitale Signaturen

Datei- und Datenträgerverschlüsselung

- GnuPG / OpenPGP – Dateien und E-Mails
- VeraCrypt – Container und Laufwerke
- LUKS2 / dm-crypt – Linux-Datenträger

Verbindungen und Authentifizierung

- OpenSSH – SSH, SFTP und Schlüsselpaare
- WireGuard – VPN-Schlüssel
- TLS, Zertifikate und Let’s Encrypt
- FIDO2, Passkeys und Hardware-Sicherheitsschlüssel

Datensicherung und E-Mail

- BorgBackup – Repository-Verschlüsselung und SSH
- E-Mail-Sicherheit – OpenPGP, S/MIME und DKIM

Verwaltung

- Schlüsselverwaltung und Lebenszyklus
- Schlüsselkataster – Aufbau und Pflege

Begriffe im Überblick

Begriff	Kurzbeschreibung
Symmetrischer Schlüssel	Geheimer Schlüssel zur Ver- und Entschlüsselung
Öffentliches/privates Schlüsselpaar	Zusammengehörende Schlüssel für Signatur, Verschlüsselung oder Schlüsselvereinbarung
Fingerprint	Aus einem Schlüssel oder Zertifikat abgeleitete Kennzeichnung
Digitale Signatur	Prüfbarkeit von Integrität und Zugehörigkeit zu einem Signaturschlüssel
Zertifikat	Signierte Zuordnung eines öffentlichen Schlüssels zu einer Identität
Passphrase	Geheimnis, das beispielsweise gespeicherte Schlüssel schützt

Sicherheitshinweis

Private Schlüssel, symmetrische Schlüssel, Passphrasen und Wiederherstellungsdaten dürfen nicht in öffentlich zugänglichen Wikiseiten gespeichert werden. Öffentliche Schlüssel und Fingerprints sind zwar nicht geheim, ihre Zuordnung zu einer Identität muss aber verifiziert werden.

Die konkreten Einstellungen einzelner Server oder Geräte sind nicht Bestandteil dieser allgemeinen Dokumentation.

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:index

Last update: **2026/11/15 20:12**