Kryptografische Schlüssel, Verschlüsselung und Zertifikate

Einführung

Kryptografische Verfahren schützen Informationen, Kommunikationsverbindungen und IT-Systeme vor unbefugtem Zugriff und Manipulation.

Dabei kommen unterschiedliche Arten von Schlüsseln, Zertifikaten und kryptografischen Verfahren zum Einsatz. Obwohl sie häufig ähnliche Begriffe verwenden, unterscheiden sie sich erheblich in ihrer Funktionsweise und ihrem Einsatzzweck.

Diese Dokumentation erläutert die technischen Grundlagen, die wichtigsten Verfahren und deren praktische Anwendung unter Linux.

Neben der Erstellung und Verwendung von Schlüsseln werden auch deren sichere Aufbewahrung, Sicherung, Erneuerung und gegebenenfalls Widerruf behandelt.

Schutzziele

Kryptografische Verfahren dienen insbesondere folgenden Schutzzielen:

Schutzziel	Bedeutung
Vertraulichkeit	Informationen können nur von berechtigten Personen oder Systemen gelesen werden.
Integrität	Veränderungen an Daten können erkannt werden.
Authentizität	Die Herkunft von Daten oder die Identität eines Kommunikationspartners kann überprüft werden.
Verbindlichkeit	Eine Handlung kann unter bestimmten Voraussetzungen einer Identität zugeordnet werden.

Nicht jedes kryptografische Verfahren erfüllt alle diese Schutzziele.

Eine Verschlüsselung schützt beispielsweise die Vertraulichkeit, während eine digitale Signatur vor allem der Überprüfung von Integrität und Authentizität dient.

Grundlegende Schlüsselarten

Symmetrische Schlüssel

Bei der symmetrischen Verschlüsselung wird derselbe geheime Schlüssel zum Ver- und Entschlüsseln verwendet.

Symmetrische Verfahren werden insbesondere zur Verschlüsselung größerer Datenmengen eingesetzt.

Typische Anwendungen:

- VeraCrypt
- LUKS / dm-crypt
- BorgBackup
- Verschlüsselte Datenübertragung innerhalb einer TLS- oder SSH-Verbindung

Asymmetrische Schlüsselpaare

Asymmetrische Kryptografie verwendet zwei mathematisch zusammengehörende Schlüssel:

- **Privater Schlüssel (Private Key):** Muss geheim gehalten werden.
- **Öffentlicher Schlüssel (Public Key):** Darf weitergegeben werden.

Je nach Verfahren dienen diese Schlüssel zur Verschlüsselung, Authentifizierung, digitalen Signatur oder Vereinbarung gemeinsamer Sitzungsschlüssel.

Typische Anwendungen:

- OpenPGP
- OpenSSH
- WireGuard
- TLS-Zertifikate
- FIDO2 und Passkeys

Passwörter und Passphrasen

Ein Passwort oder eine Passphrase ist nicht zwangsläufig mit dem eigentlichen kryptografischen Schlüssel identisch.

Passphrasen können beispielsweise verwendet werden, um private Schlüssel oder Verschlüsselungsschlüssel geschützt zu speichern.

Die Sicherheit hängt dabei unter anderem von der Stärke der Passphrase und dem eingesetzten Schlüsselableitungsverfahren ab.

Weitere Informationen: Kryptografische Grundlagen

Wichtige Begriffe

Begriff	Bedeutung
Schlüssel	Kryptografischer Wert, der für eine bestimmte Operation benötigt wird.
Schlüsselpaar	Zusammengehörender öffentlicher und privater Schlüssel.
Hashwert	Ergebnis einer kryptografischen Hashfunktion; dient unter anderem der Integritätsprüfung.

Begriff	Bedeutung
Fingerprint	Kompakte Kennzeichnung eines Schlüssels oder Zertifikats anhand eines Hashwerts.
Digitale Signatur	Kryptografischer Nachweis, mit dem Integrität und Herkunft von Daten überprüft werden können.
Zertifikat	Digitales Dokument, das einen öffentlichen Schlüssel mit einer Identität verbindet und üblicherweise signiert ist.
Zertifizierungsstelle (CA)	Vertrauenswürdige Instanz, die Zertifikate ausstellt und signiert.
Widerruf	Kennzeichnung eines Schlüssels oder Zertifikats als nicht mehr vertrauenswürdig beziehungsweise gültig.
Schlüsselrotation	Geplanter Austausch kryptografischer Schlüssel.

Ausführliche Erläuterungen: Hashwerte, Fingerprints und digitale Signaturen

Verfahren und Anwendungen

Datei- und Datenträgerverschlüsselung

Verfahren	Anwendung	Dokumentation
GnuPG / OpenPGP	Verschlüsselung und Signatur von Dateien und E-Mails	GnuPG und OpenPGP
VeraCrypt	Verschlüsselte Container, Partitionen und Laufwerke	VeraCrypt
LUKS2 / dm-crypt	Verschlüsselung von Linux-Datenträgern	LUKS2 / dm-crypt

Netzwerkverbindungen und Authentifizierung

Verfahren	Anwendung	Dokumentation
OpenSSH	SSH-Anmeldung, SFTP, SCP und sichere Fernadministration	OpenSSH
WireGuard	Verschlüsselte VPN-Verbindungen	WireGuard
TLS	Verschlüsselte Netzwerkverbindungen, insbesondere HTTPS	TLS und Let's Encrypt
FIDO2 / Passkeys	Kryptografische Benutzeranmeldung und Hardware-Sicherheitsschlüssel	FIDO2 und Passkeys

Datensicherung

Verfahren	Anwendung	Dokumentation
BorgBackup	Verschlüsselte und deduplizierte Datensicherungen	BorgBackup

Bei BorgBackup ist zwischen der Verschlüsselung der Backup-Daten und der Authentifizierung gegenüber einem entfernten Backup-Server zu unterscheiden.

Beide Aufgaben können unterschiedliche Schlüssel verwenden.

E-Mail-Sicherheit

Verfahren	Anwendung	Dokumentation
OpenPGP	Ende-zu-Ende-Verschlüsselung und digitale Signatur von E-Mails	GnuPG und OpenPGP
S/MIME	Zertifikatsbasierte E-Mail-Verschlüsselung und Signatur	E-Mail-Sicherheit

Verfahren	Anwendung	Dokumentation
DKIM	Kryptografische Signatur ausgehender E-Mails durch die sendende Domain	E-Mail-Sicherheit

Schlüsselverwaltung

Die Sicherheit kryptografischer Verfahren hängt nicht allein von den eingesetzten Algorithmen ab.

Ebenso wichtig sind die sichere Erstellung, Aufbewahrung, Verwendung und Verwaltung der Schlüssel.

Zu den wesentlichen Aufgaben gehören:

- Verwendung geeigneter Schlüsselalgorithmen und Schlüssellängen
- Trennung von Schlüsseln nach Geräten und Einsatzzwecken
- Schutz privater und symmetrischer Schlüssel
- Sicherung unersetzlicher Schlüssel und Wiederherstellungsinformationen
- Regelmäßige Überprüfung von Berechtigungen und Zugriffsrechten
- Austausch kompromittierter oder nicht mehr benötigter Schlüssel
- Dokumentation der Schlüsselbestände

Weitere Informationen:

- Grundsätze der Schlüsselverwaltung
- Aufbau und Pflege eines Schlüsselkatasters

Hinweise zur Sicherheit

Private Schlüssel, Passphrasen und Wiederherstellungsdaten dürfen nicht ungeschützt veröffentlicht werden.

Öffentliche Schlüssel und Fingerprints sind grundsätzlich nicht geheim. Ihre Zuordnung zu einer Person oder einem System muss jedoch über einen vertrauenswürdigen Weg überprüft werden.

Der Verlust eines Zugangsschlüssels kann häufig durch die Erstellung eines neuen Schlüsselpaares behoben werden.

Der Verlust eines unersetzlichen Entschlüsselungsschlüssels kann dagegen dazu führen, dass verschlüsselte Daten dauerhaft nicht mehr zugänglich sind.

Deshalb müssen Sicherungs- und Wiederherstellungsverfahren bereits bei der Einrichtung berücksichtigt werden.

Aufbau der Dokumentation

Die einzelnen Fachartikel enthalten, soweit für das jeweilige Verfahren sinnvoll:

1. Zweck und typische Anwendungsfälle
2. Technische Funktionsweise

3. Schlüsselarten, Formate und Speicherorte
4. Erstellung und Konfiguration
5. Praktische Anwendung unter Linux
6. Prüfung von Schlüsseln, Zertifikaten und Verbindungen
7. Sicherung und Wiederherstellung
8. Schlüsselwechsel und Widerruf
9. Sicherheitsaspekte und typische Fehlerquellen

Die verwendeten Beispiele sind allgemein gehalten. Als Beispieldomain kann `wiki.bluegnu.de` verwendet werden.

Die Dokumentation enthält keine privaten Schlüssel, Zugangsdaten oder persönlichen Schlüsselbestände.

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

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

Last update: **2026/11/15 17:02**