IT-Sicherheit, 2FA, etc.

Dokumente signieren und verschlüsseln

PGP und Kleopatra

- Signieren und Verschlüsseln mit Kleopatra
- OpenPGP-Schlüssel beglaubigen

X.509 Zertifikate

- Eigene X.509-Zertifikate erstellen und verteilen
- Linux 2FA mit Smartcard X.509 Zertifikaten
- Verbindungssicherheit - Eigene Zertifikate für openVPN

Zeitbasierte Einmalpasswörter (TOTP)

Grundlagen und Quellen

- TOTP Paper
- Wikipedia Artikel zu TOTP

Hardware Token Hersteller

- Token2
- Solokeys
- Yubico
- Reiner-SCT

Online Generatoren

- Self hosted TOTP-Generator
- Self hosted TOTP QR-Code Generator
- TOTP Token Generator
- TOTP Token Generator - GitHub Repo
- TOTP QR-Code Generator
- TOTP QR-Code Generator - GitHub Repo
- Token2 TOTP Toolset

für Mikrocontroller

- Arduino libary for TOTP generation, zusätzlich wird die Bibliothek `Base32-Decode` benötigt
- Mifare RC522 mit einem Arduino Mikrocontroller ansteuern
- RFID und Arduino

Passkey & Passphrase

Unterschiede zw. Passkey und Passphrase

Merkmal	Passkey	Passphrase
Was es ist	Ein kryptografisches Schlüsselpaar (öffentlich und privat).	Eine besonders lange Folge aus mehreren Wörtern (z. B. 15+ Zeichen).
Speicherung	Der private Schlüssel liegt nur auf Ihrem Gerät (Handy, PC).	Sie müssen sie sich merken oder in einem Tresor speichern.
Eingabe	Keine Eingabe; Sie entsperren ihn per Fingerabdruck, Gesichtsscan oder PIN.	Sie tippen die Wortkette manuell ein oder nutzen Auto-Ausfüllen.
Phishing-Schutz	Sehr hoch: Bindet sich fest an die echte Website (Phishing greift nicht).	Geringer: Kann auf einer gefälschten Website von Betrügern eingegeben werden.
Wiederverwendung	Automatisch pro Konto einzigartig (nicht übertragbar/wiederverwendbar).	Kann theoretisch für mehrere Konten genutzt werden (ist aber unsicher).

Quelle: Google Suche mit den Schlagworten „passkey vs passphrase“

Links

- Bundesamt für Sicherheit in der Informationstechnologie - Anmelden ohne Passwort mit Passkey
- Liste mit Diensten die bereits Passkey unterstützen

Passkey

Passphrase

Server Security

SSH

- Shell Kommandos zu ssh
- SSH Key Best Practices for 2025 – Using ed25519, key rotation, and other best practices
- How To Set up SSH Keys on a Linux / Unix System

Bundesamt für Sicherheit i.d. Informationstechnik

- Checklisten, Flyer & Schritt-für-Schritt-Anleitungen
- IT-Grundschutz
- IT-Grundschutz-Kompendium (Edition 2023)
- BSI – Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- BSI TR-02102-4 "Kryptographische Verfahren: Teil 4 – Verwendung von Secure Shell (SSH)" Version: 2025-01

Linux härten

- Linux Systemhärtung: Hintergründe, Maßnahmen und Tool-Tipps
- Debian Sicherheitshandbuch

From:
https://www.von-thuelen.de/ - **Christophs DokuWiki**

Permanent link:
https://www.von-thuelen.de/doku.php/wiki/sicherheit/uebersicht

Last update: **2026/11/15 12:50**