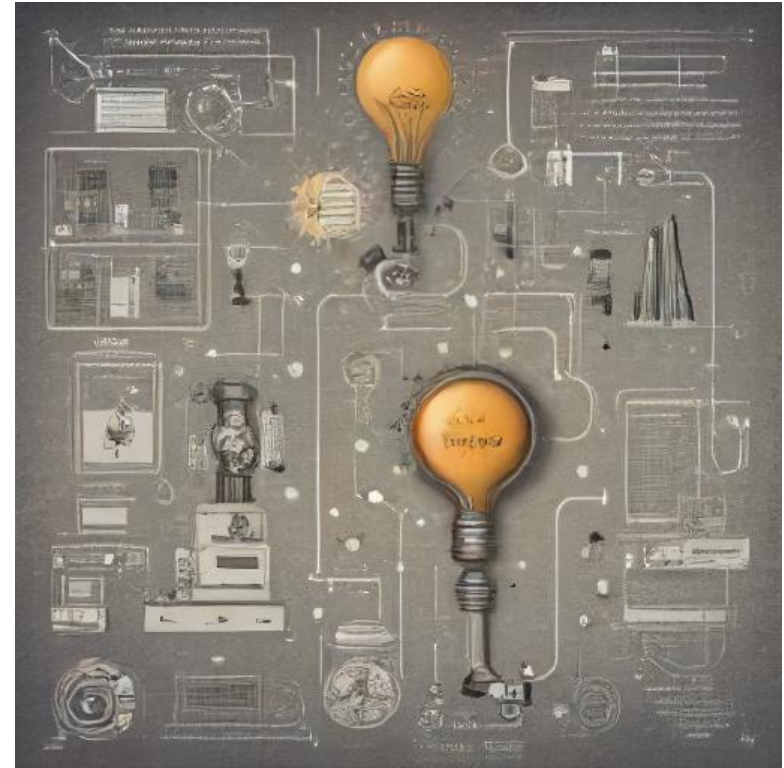


Digitale Signaturen – Der Schlüssel zum Vertrauen in der digitalen Welt



Um was geht es heute?

- › Einführung in digitale Signaturen
- › EU Rahmenbedingungen
- › Signaturen in Österreich
- › Validierung / Langzeitsignaturen
- › Potential für Geopackage Standard



Warum digitale Signaturen

- › Sicherheit im digitalen Raum
 - › Dokumente nachhaltig und prüfbar unterschreiben
- › Authentizität: Wer hat unterschrieben?
- › Integrität: Wurde etwas verändert?
- › Nicht-Abstreitbarkeit: Ich habe nicht unterschrieben!
- › Rechtliche Verbindlichkeit

Digitale vs. Elektronische Signatur

- › Elektronische Signatur = allgemeiner Begriff
- › Digitale Signatur = technische Umsetzung (Kryptographie)
 - › Unterschiedliche Verfahren (RSA vs. ECDSA)
 - › Schlüsselpaar (privater / öffentlicher Schlüssel)
 - › Basieren prinzipiell alle auf mathematisch schwer lösbaren Problemen (Gefahr durch Quantencomputer)
- › Grundlage für Vertrauen im E-Government & Wirtschaft

Elemente einer digitalen Signatur

- › Neben kryptografischen Teil...
- › Zertifikat
 - › Bindet den öffentlichen Schlüssel an eine bestimmte Person oder Organisation
 - › Ausgestellt von einer Zertifizierungsstelle (CA) oder einem qualifizierten Vertrauensdiensteanbieter (QTSP)
- › Signaturerstellungseinheit
 - › Die Umgebung, in der der private Schlüssel geschützt ist
 - Smartcard, USB-Token, Hardware Security Module (HSM)
 - Mobile Lösung (z. B. ID Austria am Handy, EU Wallet).
- › Signaturformat
 - › Definiert, wie die Signatur und die Prüf-Infos in das Dokument eingebettet werden

Signaturformate allgemein

- › Jedes Datenformat hat seine Eigenheiten
 - › daher angepasste Signaturformate
- › PKCS#7 / CMS (technische Basis)
- › XML-Signaturen
- › PDF-Signaturen (basieren auf CMS)
- › JSON-Signaturen (JWS)
- › (Open)PGP (seltener)

Die eIDAS-Verordnung

- › Seit 2016 in Kraft – hat Signaturrechtlinie von 1999 ersetzt
- › Novelle Frühjahr 2024 (eIDAS 2)
- › Regelt Arten elektronischer Signaturen
 - › Einfache – Fortgeschrittene – Qualifizierte Signaturen/Siegel
- › Qualifizierte Signatur-/Siegelerstellungseinheiten
- › Vertrauensdienste
 - › Ausstellung von Zertifikaten für elektronische Signaturen/Siegel
 - › Management von Remote QSCD (qual. signature creation device)
- › Aufsicht

Fortgeschritte vs. Qualifizierte Signaturen

- › Einfache Signatur
 - › sehr schwach, kann auch nur ein Name unter einer E-Mail sein
- › Fortgeschrittene Signatur (AdES)
 - › kryptographisch abgesichert, integritäts- und identitätsprüfbar
- › Qualifizierte Signatur (QES)
 - › eine AdES mit zusätzlichem qualifizierten Zertifikat und erstellt mit einer qualifizierten Signaturerstellungseinheit (QSCD) → gleiche Rechtswirkung wie handschriftlich.

AdES-Formate nach eIDAS

- › XAdES – XML Advanced Electronic Signatures
- › CAdES – CMS Advanced Electronic Signatures
- › PAdES – PDF Advanced Electronic Signatures
- › JAdES – JSON Advanced Electronic Signatures
- › ASiC – Associated Signature Containers

Signaturen im öst. E-Government

- › Benutzersignatur durch ID Austria
- › Amtssignaturen serverseitig (fortg. Siegel)
- › Größenordnung mehrere Mio. pro Monat
- › Hauptsächlich PDF Signaturen, vereinzelt XML
- › Open-Source Module für Erstellung
 - › PDF-AS(-web), PDF-Over, MOA-SP/SS

ID Austria

- › Neben eID auch Signatur
- › In Verwaltung & Privatwirtschaft nutzbar
- › Merkmale
 - › Qualifizierte Signatur
 - › Sichere Signaturerstellungseinheit (QSCD)
 - › Proprietäre Signaturschnittstelle (Security-Layer)
 - › Formate: XAdES, CAdES (implizit PAdES)

EU Digital Identity Wallet

- › Geplante „digitale Briefftasche“
 - › Zusammenführung ID Austria und eAusweise
- › Einheitlicher Zugang in Europa
- › Auch für Signaturen vorgesehen
 - › Einheitliche Schnittstelle für Erstellung von Signaturen
- › Verpflichtend ab Ende 2026

Warum Validierung wichtig ist

- › Prüfen: ist Signatur gültig?
 - › Dokument unverändert?
 - › Zertifikat noch vertrauenswürdig?
 - › Status: widerrufen oder nicht?
 - › Zum Zeitpunkt der Signatur gültig?
- › Prüfmöglichkeiten
 - › Commodity Software: Adobe Reader (sofern qualifiziertes Zertifikat)
 - › Nationale Prüfservices wie das der RTR (kann eIDAS Formate)
 - › Proprietäre Implementierungen

ETSI-Standards für Langzeitsignatur

- › Formate mit Zeitstempeln & Widerrufs-Infos:
- › -T (mit Zeitstempel)
 - › Zusätzlicher qualifizierter Zeitstempel, beweist wann signiert wurde
- › -LT (mit Validierungsinfos)
 - › Enthält zusätzlich alle Validierungsinformationen (OCSP/CRL), die nötig sind, um die Signatur auch nach Ablauf des Zertifikats prüfen zu können.
- › -LTA (Langzeitarchivierung)
 - › Enthält neben -LT auch periodische Nachzeitstempel (Renewal)

GeoPackage Standard

- › Kernstandard definiert keine Signaturen
- › Signaturen könnten über eine eigene Extension eingebettet werden
- › Beispiel: Tabelle 'gpkg_signatures' für Signaturdaten
- › Oder Referenz zu externer ASiC-Signaturdatei
- › Nutzung bestehender eIDAS-Formate
 - › CMS/CAdES in weitere Tabelle/Spalte
 - › ASiC Container (ZIP Struktur mit .gpkg + CAdES)

GeoPackage Standard

- › Extensions = flexibler Erweiterungsmechanismus
- › Standardkonforme Software ignoriert Unbekanntes
- › Ermöglicht Signaturen ohne Änderung des Kernstandards
- › Potenzial für OGC/ETSI-Standardisierung von Geosignaturen

Trends

- › Mehr mobile Signaturen
 - › Mobile by default
- › Integration in EU Wallet
 - › Verpflichtend in ganz Europa
- › Automatisierte Validierung

Herausforderungen

- › Benutzerfreundlichkeit
 - › Insbesondere auf mobilen Geräten
- › Interoperabilität
 - › Standardisierung (!)
- › Langzeitarchivierung

Fazit

- › Digitale Signaturen = Schlüsseltechnologie
- › EU schafft einheitlichen Rahmen
- › Einsatzgebiete wachsen – auch bei Geodaten

Fragen?

a-sit.at/
technology.a-sit.at