site-de.html

Emailwerk Signierte E-Mail. Ablauf Signatur Papier Technik EN Jetzt anfragen

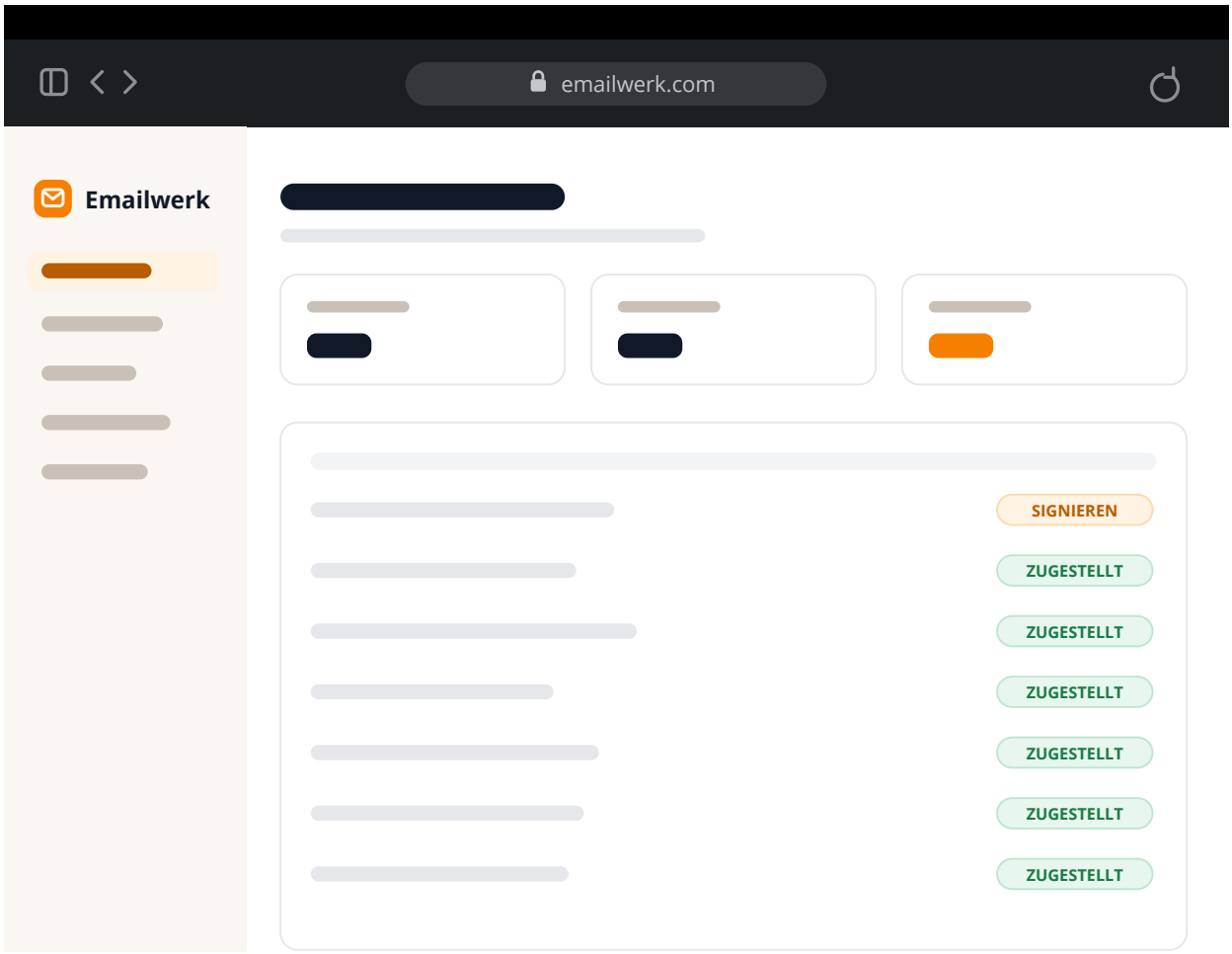
Signiert. Versiegelt.

Eine E-Mail, unterschrieben und versiegelt.

Der Siegelring von heute ist ein kryptografischer Schlüssel in der Hand, etwa ein YubiKey. Was damit unterschrieben ist, kann der Empfänger nachrechnen: von wem die E-Mail kommt, und dass unterwegs niemand ein Wort geändert hat.

Kontakt Zur Verwaltung

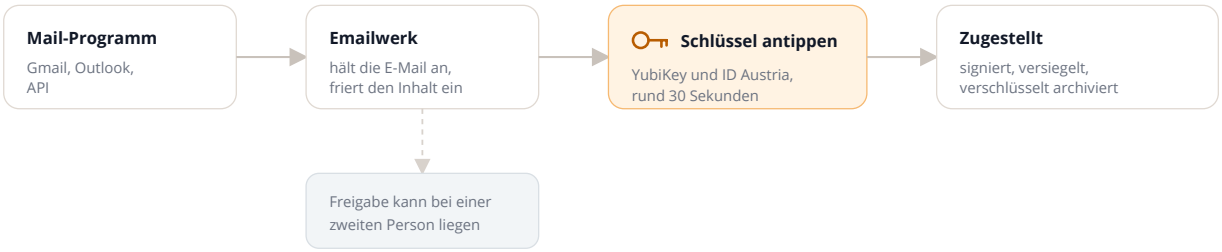
Selbst gehostet · eIDAS-qualifiziert · Prüfbar auch auf Papier



Im Einsatz bei

Schreiben, antippen, versendet

Geschrieben wird im gewohnten Programm. Emailwerk hält die E-Mail an, bis der Schlüssel sie unterschrieben hat.



Vier Schichten auf einer E-Mail

Jede beantwortet eine andere Frage. Zusammen decken sie Urheber, Inhalt und Transportweg ab.

1. **PGP auf dem Schlüssel — wer hat unterschrieben**
2. **Prüfcodes im Dokument — lesbar auch auf Papier**
3. **ID Austria im PDF — der handschriftlichen Unterschrift gleichgestellt**
4. **Siegel über die fertige E-Mail — jede Änderung fliegt auf**

Schicht 3 ist die rechtlich entscheidende. Die anderen drei binden den Inhalt und schützen ihn unterwegs.

Eigenes Erscheinungsbild Briefkopf, Adressfeld, Signaturblock.
Anhänge einzeln signiert Jedes PDF mit eigener Signaturseite.
Verschlüsseltes Archiv Der Server kennt nur den öffentlichen Schlüssel.
Anmelden per Signatur Dieselbe Zeremonie ist ein OpenID-Connect-Login: Registrierung mit ID Austria statt Passwort (qes-oidc, Open Source).

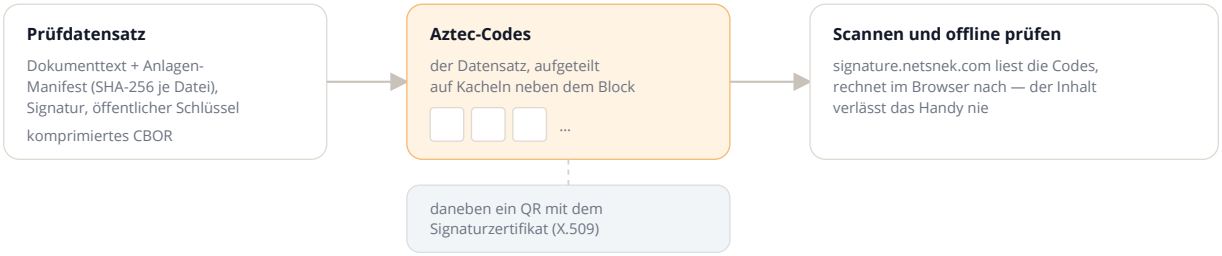
Der Signaturblock: auch ausgedruckt noch prüfbar

Eine herkömmliche PDF-Signatur, auch die von ID Austria, lebt in den Bytes der Datei. Auf Papier ist sie weg: man sieht weder, dass unterschrieben wurde, noch was. Emailwerk druckt darum den unterschriebenen Inhalt selbst als Codes auf die Signaturseite.

Aztec ISO/IEC 24778 trägt den Inhalt. Byte-genau, 5 % Fehlerkorrektur, ohne Ruhezone — die Kacheln packen randlos ins Prüfcode-Raster. **QR ISO/IEC 18004** trägt das Signaturzertifikat (X.509) als Prüflink im URL-Fragment — jede Handykamera öffnet ihn, das Fragment verlässt das Gerät nie. Beide Codes oben sind mit der Produktionsbibliothek erzeugt, mit einem Beispiel-Datensatz statt eines echten Schreibens.
Ein Datensatz, viele Kacheln Der Prüfdatensatz (komprimiertes CBOR, RFC 8949) wird in Teile zu höchstens 500 Byte geschnitten; jeder Teil trägt eine Kopfzeile mit Index und Gesamtzahl und wird eine eigene Aztec-Kachel. Der Prüfer scannt in beliebiger Reihenfolge und setzt zusammen.

Kapazität Ein gewöhnliches Schreiben ergibt ein bis zwei Kacheln. Ein echtes neunseitiges Steuerformular ergab rund vierzig — läuft das Raster über, wandern weitere Kacheln auf Fortsetzungsseiten. Eine harte Grenze gibt es dadurch nicht.

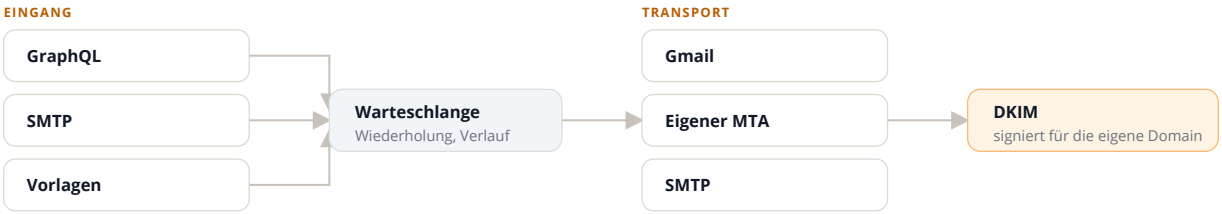
Anhänge, einzeln versiegelt Jedes angehakte PDF durchläuft die volle Kette selbst: Signatur über Text und Datei-Prüfsumme, eigener Datensatz, eigene Blockseite, eigene qualifizierte Signatur. Das Schreiben trägt ein Anlagenverzeichnis mit dem SHA-256 jeder Datei — Anhang und Brief sind aneinander gekettet, und die Anhänge werden vor der E-Mail signiert, damit ihr Verzeichnis die fertigen Prüfsummen versiegelt.



Die Codes tragen, was unterschrieben wurde — nicht nur, dass. Ein Scan zeigt den Text, vergleicht die Prüfsummen und verkettet das Zertifikat bis zur A-Trust-Wurzel. Das funktioniert auf dem PDF wie auf dem Ausdruck, ohne dem Prüfserver vertrauen zu müssen.

Darunter ein vollständiger Mail-Motor

Auch der Alltag ohne Signatur läuft darüber: Bestätigungen, Codes, Benachrichtigungen.



Selbst gehostet und mandantenfähig. Nachrichten und Schlüssel bleiben auf der eigenen Infrastruktur.

Open Source

Bausteine der Signaturkette, offen auf GitHub.

qes-oidc ID-Austria-QES-Login und ein minimaler OpenID-Connect-Provider: die Signatur-Zeremonie als Anmeldung.
age-plugin-piv25519 age-Verschlüsselung an einen YubiKey-PIV-Schlüssel gebunden — derselbe Schlüssel in der Hand, fürs Archiv.

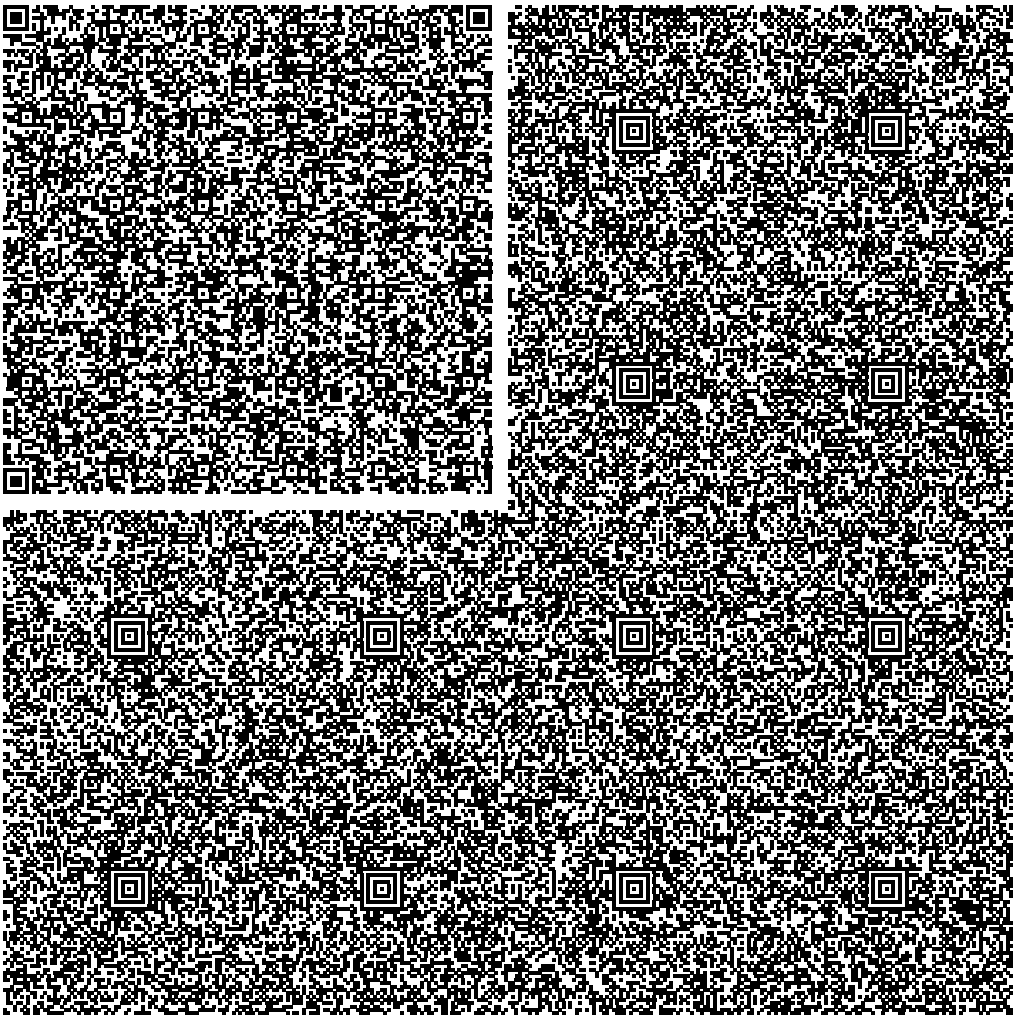
signiertes PDF signiertes HTML PGP-Signatur öffentlicher Schlüssel

Emailwerk ist ein Projekt von Netsnek e.U. · Impressum

Signaturwert	MEUCIQCIcihT3hEwxEMi73lk7DVOyyuUQXYOp/7G18Y65CDHKwIgK9FqkRPSYOj/A0KuaFufUZ8Zg/QCmM5Tgmzow4RdGzU=

Signiert von	signature.netsnek.com
Unterzeichner	Florian Herbert Kleber
Zertifikat	CN=Florian Herbert Kleber, SN=558326663028, C=AT
Datum/Zeit-UTC	2026-08-10T03:34:54Z
Serien-Nr.	0x2D0BE19D
Methode	ETSI.CAdES.detached / netsnek-code:v1

Prüfcodes
QR (Zertifikat) + Aztec (Inhalt) scannen & prüfen



Der signierte Inhalt (Dokumenttext samt Anlagen-Manifest mit Dateiname und SHA-256 jeder Anlage) ist EIN qualifiziert signierter Prüfdatensatz (zlib-komprimiertes CBOR nach RFC 1950 und RFC 8949): die signierten Bytes, die Signatur (ECDSA P-256 über die CMS-signedAttrs nach RFC 5652, ETSI CAdES) und der öffentliche Schlüssel. Er ist auf die Aztec-Codes aufgeteilt; der netsnek-Prüfer liest und fügt sie zusammen. Der Zertifikat-QR trägt das X.509-Signaturzertifikat (RFC 5280) im URL-Fragment für die Handy-Kamera. Damit ist die Prüfung offline und ohne Vertrauen in signature.netsnek.com möglich: Teile zusammensetzen und dekodieren, SHA-256 der signierten Bytes mit dem messageDigest der signedAttrs vergleichen, die Signatur mit dem Schlüssel verifizieren, den SHA-256 jeder beigelegten Datei gegen das signierte Manifest prüfen und das Zertifikat bis zur A-Trust-Wurzel verketten. Das URL-Fragment wird nie an einen Server übertragen.

Prüfinformation	Code scannen und offline prüfen unter: https://signature.netsnek.com/. Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.

Prüfcodes (Fortsetzung) scannen & prüfen