site-en.html

Emailwerk Signed Email. How it works Signature Paper Engine DE Get in touch

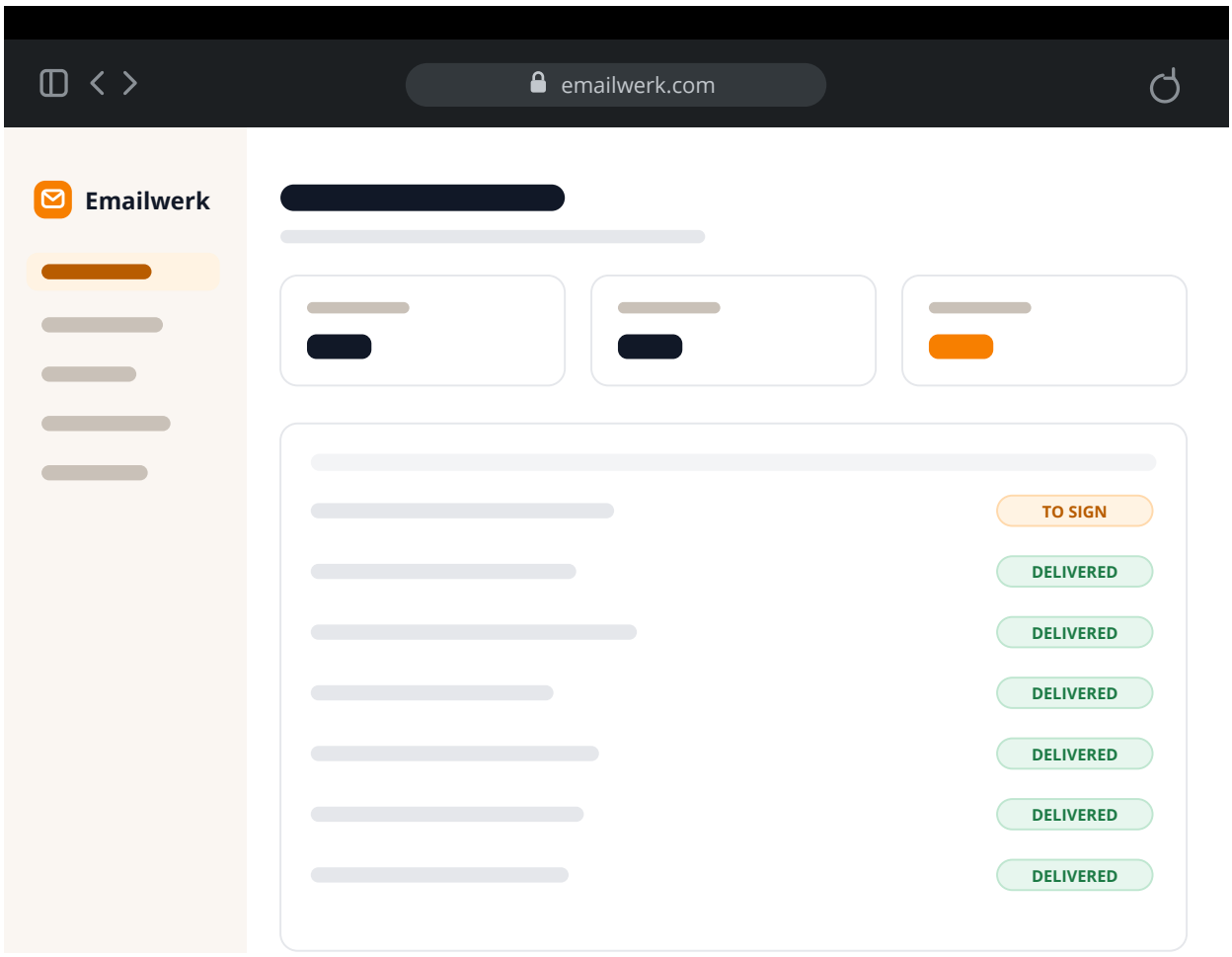
Signed. Sealed.

An email, signed and sealed.

Today's signet ring is a cryptographic key you hold in your hand, a YubiKey for instance. Whatever it signs, the recipient can verify: who the email is from, and that nobody changed a word on the way.

Contact Open the app

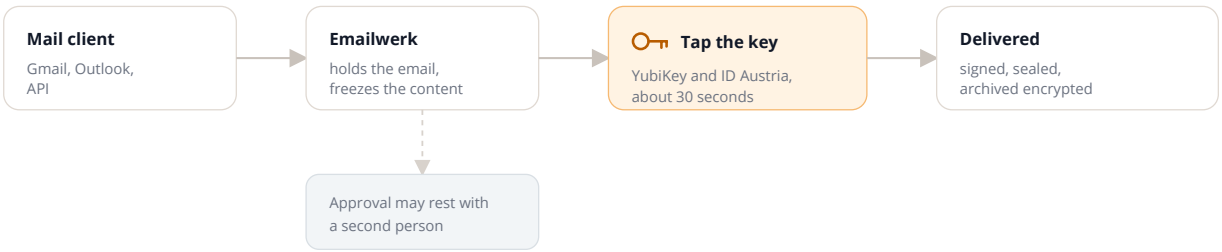
Self-hosted · eIDAS-qualified · Verifiable even on paper



In use at

Write, tap, sent

You write in your usual mail client. Emailwerk holds the email until the key has signed it.



Four layers on one email

Each answers a different question. Together they cover author, content and transport.

1. **PGP on the key — who signed**
2. **Printed codes — readable even on paper**
3. **ID Austria in the PDF — equivalent to a handwritten signature**
4. **A seal over the finished email — any change shows**

Layer 3 is the legally decisive one. The other three bind the content and protect it in transit.

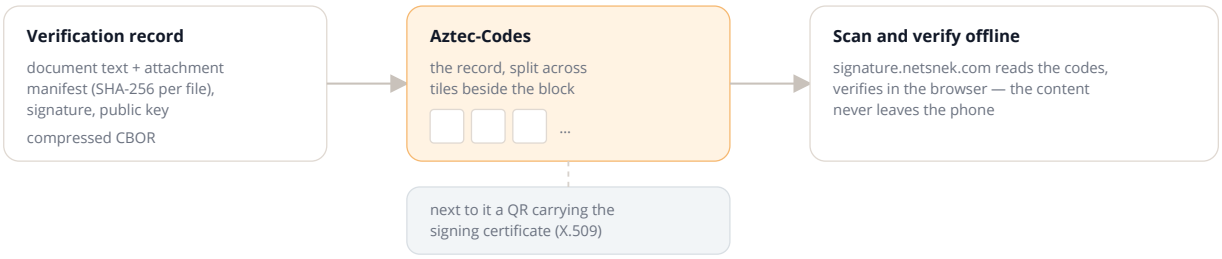
Your own look Letterhead, address field, signature block.
Attachments signed too Each PDF gets its own signature page.
Encrypted archive The server only holds the public key.
Sign in by signing The same ceremony doubles as an OpenID Connect login: register with ID Austria instead of a password (qes-oidc, open source).

The signature block: still verifiable on paper

A conventional PDF signature, ID Austria's included, lives in the file's bytes. On paper it is gone: you can see neither that it was signed nor what was signed. So Emailwerk prints the signed content itself onto the signature page, as codes.

Aztec ISO/IEC 24778 carries the content. Byte-exact, 5 % error correction, no quiet zone — the tiles pack edge to edge in the code grid. **QR ISO/IEC 18004** carries the signing certificate (X.509) as a verify link in the URL fragment — any phone camera opens it, and the fragment never leaves the device. Both codes above were generated with the production library, from a sample record rather than a real letter.
One record, many tiles The record (compressed CBOR, RFC 8949) is cut into parts of at most 500 bytes; each part carries a header with index and total and becomes its own Aztec tile. The verifier scans in any order and reassembles.
Capacity An ordinary letter yields one or two tiles. A real nine-page tax form came to about forty — when the grid overflows, further tiles continue on follow-on pages, so there is no hard limit.
Attachments, sealed one by one Every ticked PDF runs the full chain itself: a signature over text and file hash,

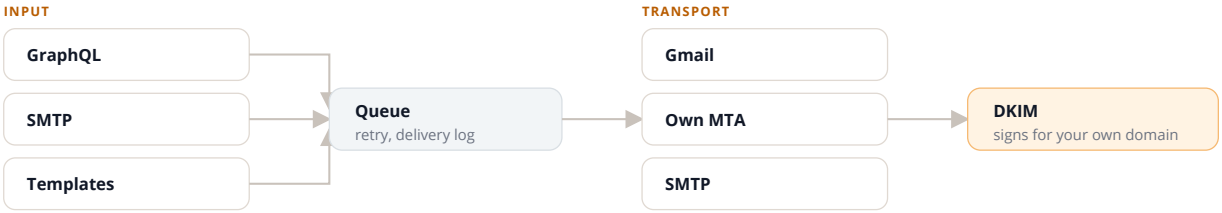
its own record, its own block page, its own qualified signature. The letter carries an attachment manifest with each file's SHA-256 — attachment and letter are chained together, and attachments are signed before the email so the manifest seals their final hashes.



The codes carry what was signed — not merely that. One scan shows the text, compares the hashes and chains the certificate to the A-Trust root. That works on the PDF and on the printout alike, without having to trust the verification server.

A complete mail engine underneath

The unsigned everyday traffic runs on it too: confirmations, codes, notifications.



Self-hosted and multi-tenant. Messages and keys stay on your own infrastructure.

Open Source

Building blocks of the signature chain, open on GitHub.

qes-oidc ID Austria QES login and a minimal OpenID Connect provider: the signing ceremony as authentication.
age-plugin-piv25519 age encryption bound to a YubiKey PIV key — the same key in your hand, used for the archive.

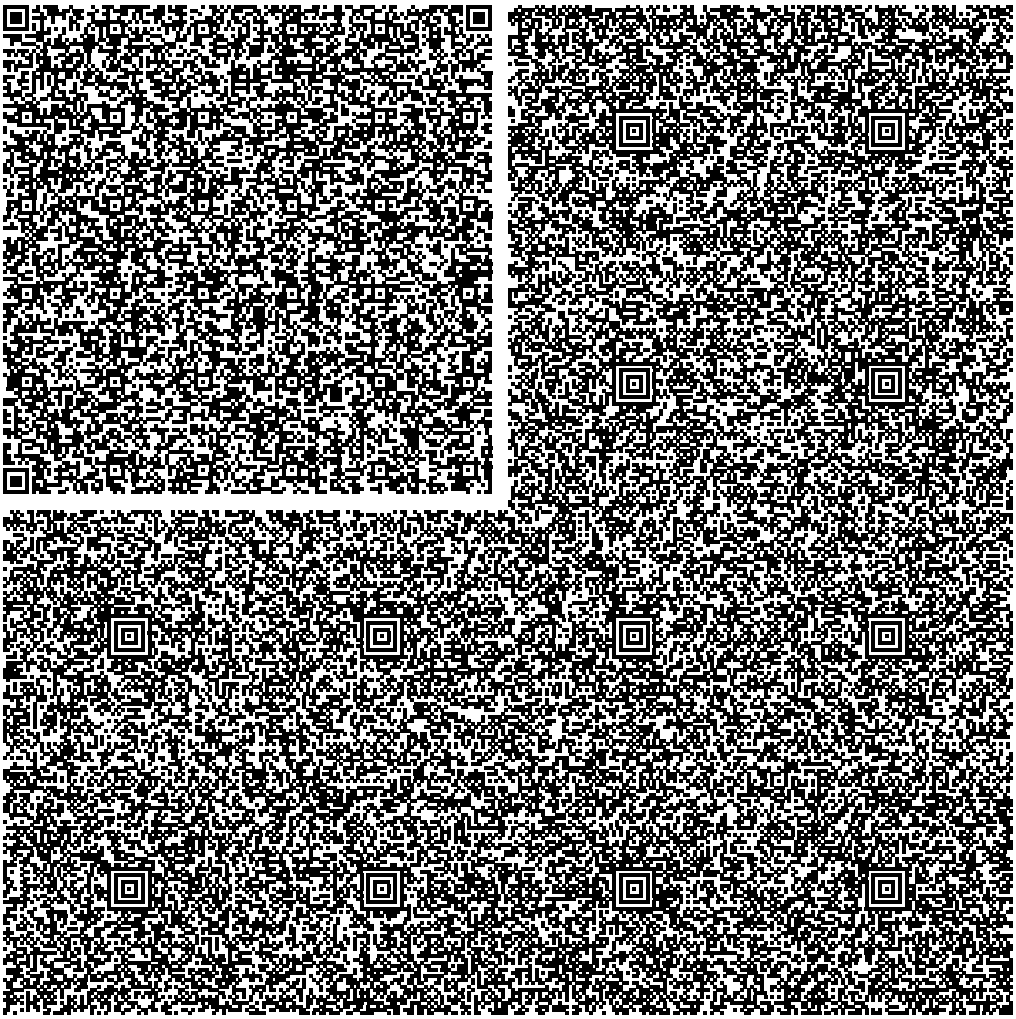
signed PDF signed HTML PGP signature public key

Emailwerk is a project by Netsnek e.U. · Legal notice

Signaturwert	MEUCIFIH7VmUIwTgD4ZX245JayGTneZllX5KeHVhMssBK0CyAiEA8MTXpGQByrgL2kOx9gjSrlUj7gSppq/qNseNd0PYC9Q=

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