

— INNOVATION EVIDENCE PLATFORM

Trusted timestamping at Bernstein

Proof of when your evidence existed - anchored to the Bitcoin blockchain and corroborated across independent timestamping authorities, verifiable by anyone.

Every Bernstein certificate carries independent, court-grade timestamps. This brief explains how they work - the RFC 3161 standard, what eIDAS 'qualified' means, the authorities we use, and how qualified timestamps and Bitcoin anchoring compare and combine.

UPDATED

June 2026

AUDIENCE

Technical & procurement

ANCHORS

Bitcoin · 3 RFC 3161 TSAs

1 · THE BASICS

1 What a trusted timestamp proves

A trusted timestamp is signed proof that a specific piece of data existed at a specific moment - issued by an independent authority, not by you.

DEFINITION

A **Time-Stamping Authority (TSA)** receives only a cryptographic **hash** of your data, binds it to the current time, and returns a digitally signed **timestamp token**. The authority never sees your content - only the hash. The token is later verifiable by anyone, independently of Bernstein.

Bernstein applies client-side, zero-knowledge encryption first, then timestamps the hash. Your content never leaves your control. What the authority signs - and what a court or expert can later re-check - is the hash, the time, and the authority's own signature.

What the token attests

- ◆ **Message imprint** - the exact hash that was timestamped, proving which data the token belongs to.
- ◆ **Generation time** - the UTC moment the authority issued the token.
- ◆ **Serial number** - a unique identifier for the timestamp.
- ◆ **Authority signature & certificate** - the TSA's cryptographic signature and its certificate, so the token verifies on its own.

RFC 3161

OPEN IETF STANDARD

sub-second

TSA CONFIRMATION

Bitcoin

PERMANENT ANCHOR

2 · THE STANDARD

2 RFC 3161 - the time-stamp protocol

Bernstein's timestamps follow **RFC 3161**, the IETF standard for the Time-Stamp Protocol (TSP). It is the same standard used across regulated industries - so the proof is portable and independently checkable with off-the-shelf tools, not locked to a vendor.

1 · Request

Bernstein hashes your (already encrypted) data with SHA-256 and sends the hash - plus a random nonce - to the authority. No content leaves your control.

2 · Token

The authority binds the hash to the current time and returns a signed TimeStampToken carrying the time, the hash, a serial number and its certificate.

3 · Verify

Bernstein checks the signature, the hash, and the nonce, then stores the raw token. Anyone can re-verify it later - no Bernstein cooperation required.

WHAT RFC 3161 DOES - AND DOES NOT - GIVE YOU

RFC 3161 is an open, audited standard, so a court-appointed expert can validate a token directly. It proves **existence at a point in time** and **integrity** - but says nothing about *who* authored the data, and confers no legal status on its own. Whether a token is 'qualified' depends on the issuer, not the protocol. That distinction is the next section.

3 · THE FRAMEWORK

3 eIDAS: what 'qualified' means

In the EU, trust services are governed by **eIDAS** (Regulation EU 910/2014). It defines three different instruments that are easy to confuse - they answer three different questions. A timestamp is not a signature.

e-Signature

Answers WHO. A natural person's identity and intent to sign a document. (Art. 3(10).)

e-Seal

Answers ORIGIN. A legal person or organisation's stamp on data - its provenance and integrity. (Art. 3(11).)

e-Timestamp

Answers WHEN. Proof a datum existed at a point in time and is intact - no identity claim. (Art. 3(34).) This is what Bernstein applies.

Qualified vs baseline - the difference is the burden of proof

Under eIDAS **Article 41**, every timestamp is admissible in court - it cannot be rejected just for being electronic or non-qualified. A **qualified** timestamp additionally carries a legal presumption and is recognised EU-wide.

Qualified electronic timestamp

Issued by a Qualified Trust Service Provider on the EU Trusted List, sealed under Art. 42. Carries the Art. 41(2) **rebuttable presumption** of accurate time and data integrity, EU-wide - the challenger must disprove it.

Baseline RFC 3161 timestamp

Any compliant TSA. Admissible and not denied effect (Art. 41(1)), but assessed on its merits - no automatic presumption. Still a strong, independent third-party time anchor.

WHAT MAKES A TIMESTAMP QUALIFIED - ARTICLE 42

Three conditions: **(a)** it binds date and time to the data so any later change is detectable; **(b)** it uses an accurate time source linked to **UTC**; **(c)** it is sealed with the qualified provider's advanced electronic seal. Meet all three, be listed on the EU Trusted List, and the token is qualified.

4 · THE AUTHORITIES

4 Our timestamping authorities

Every Bernstein certificate carries all of these authorities at once - not one selected by region - so the proof holds wherever it is challenged. All use the same RFC 3161 protocol. One is EU-qualified; the others are baseline RFC 3161 authorities that add independent corroboration - and Bitcoin anchoring (next sections) sits alongside every one of them.

Universign

EU-QUALIFIED

EU · eIDAS

RFC 3161 · Qualified TSA

French Qualified Trust Service Provider, on the EU Trusted List. Issues **qualified** electronic timestamps - the only one of the three carrying the eIDAS Art. 41(2) legal presumption across the EU.

UniTrust

CN-QUALIFIED

China

RFC 3161 · CN TSA

China's trusted-timestamp authority, time-sourced from the National Time Service Center (Chinese Academy of Sciences). Named in the Supreme People's Court Internet-Court rules and widely relied on in Chinese judicial practice.

DigiCert

CORROBORATING

Global

RFC 3161 · baseline

DigiCert's public RFC 3161 authority - a globally trusted, independent time anchor whose root is in every OS and browser. **Not** an eIDAS qualified timestamp: it adds redundancy, not a legal presumption.

Every certificate carries the full set, not a regionally routed subset - so the proof can be independently verified worldwide, under several trust frameworks at once. Bernstein preserves each authority's raw token in full and renews it through long-term validation, so the evidence stays verifiable for its full life.

5 · THE DETAIL

5 Validity, legal recognition & verification

For technical and procurement review, three questions decide whether a timestamp will hold up: how long it lasts, what legal weight it carries, and how an independent party checks it. These are the lens for the comparison below.

How long it lasts

On its own, a TSA timestamp is only as durable as the issuing authority's signing certificate, which expires. Long-term validation re-stamps the token before that happens, and Bitcoin anchoring - with no certificate to expire - keeps the Bernstein certificate verifiable for the life of the evidence.

What legal weight it carries

Every token is admissible. The weight ranges from an EU-wide qualified presumption that shifts the burden to the challenger (Universign), to recognition under Chinese Internet-Court rules (UniTrust), to admissibility on the merits backed by ubiquitous root trust (DigiCert).

How anyone checks it

Each token is a standard RFC 3161 TimeStampToken - re-hash the file, match the imprint, verify the authority's signature up its chain. Off-the-shelf tools, no vendor lock-in, and no cooperation from Bernstein required.

Side by side, for the three authorities:

	Universign · EU	UniTrust · China	DigiCert · Global
Class	Qualified eIDAS TSA	RFC 3161 (CN)	RFC 3161 baseline
Legal recognition	✓ eIDAS Art. 41(2) presumption, EU-wide	PRC e-Signature Law; SPC Internet-Court rules Art. 11(2)	Admissible on its merits; ubiquitous root trust
Time source	UTC · ANSSI-qualified HSM (EAL 4+)	UTC(NTSC) - China's national time service (CAS)	UTC · public TSA
Token validity	Proof indefinite; auto-verify 5 yrs; signing cert 6 yrs / CA 10 yrs	Proof persists; long-term validation recommended	Proof persists; TSA cert rotated ≤15 months
Long-term	Qualified preservation re- stamps before certs/algorithms age	Re-timestamping (LTV) for long horizons	Re-stamping (LTV) for long horizons
Verification	Any RFC 3161 tool, or Universign's web verifier	Public verification centre at v.tsa.cn	Any RFC 3161 tool; chain trusted everywhere

Every token is a standard RFC 3161 TimeStampToken - re-hash the file, match the imprint, verify the authority's signature up its chain. No Bernstein cooperation required.

WHAT EXPIRES - AND WHY A BERNSTEIN CERTIFICATE DOES NOT

A standalone TSA timestamp does not stay automatically verifiable forever. Its automated validation is only as durable as the issuing authority's signing certificate, which expires (Universign's in about 6 years; DigiCert's rotates roughly every 15 months) - once it lapses, the token can no longer be validated automatically up a live trust chain, and a qualified token's legal presumption weakens with it. What does not expire is the **Bernstein certificate**. Two mechanisms keep it verifiable for the life of the evidence: long-term validation re-stamps each token before its certificate or hash algorithm ages, and - decisively - **Bitcoin anchoring** depends on no certificate and no central authority, and stays verifiable for as long as the Bitcoin network persists. The Bernstein certificate therefore holds even as the individual timestamps inside it are renewed.

6 · THE COMPARISON

6 Qualified timestamps vs Bitcoin anchoring

The two methods solve the same problem from opposite ends. A qualified timestamp brings regulatory recognition inside its framework; Bitcoin anchoring brings borderless permanence with no authority to trust and nothing to renew. Bernstein uses both.

WHERE A QUALIFIED TIMESTAMP WINS

- ◆ **Legal presumption.** Under eIDAS Art. 41(2) it is presumed accurate and intact in EU courts - the regulatory bar, met directly.
- ◆ **Instant.** Confirmation is sub-second; no waiting for network finality.
- ◆ **Regulated trust.** The authority is audited and accountable under a recognised framework.

WHERE A QUALIFIED TIMESTAMP IS BOUNDED

- ◆ **Bounded reach.** Recognition follows the framework - one country or a bloc such as the EU. It does not automatically carry worldwide.
- ◆ **Authority dependence.** The proof leans on a single authority remaining trusted and accredited.
- ◆ **Certificate lifecycle.** Signing certificates and revocation must be tracked, and tokens re-stamped, to keep very long-term validity airtight.

	Qualified timestamp (eIDAS / RFC 3161)	Bitcoin blockchain anchoring
Legal recognition	✓ Presumed admissible in the EU (eIDAS)	Accepted on its merits; increasingly recognised by courts
Jurisdictional reach	One country or a bloc (e.g. the EU)	✓ Universal - no borders
Trust model	Relies on an accredited authority	✓ No single authority; public ledger
Expiry / renewal	Signing certificate ages - manage re-stamping (LTV)	✓ Nothing to renew - the proof is the chain
Longevity	Valid long-term with lifecycle management	✓ Immutable once confirmed
Cost to forge	Compromise the authority's keys or accreditation	✓ Redo the block's proof-of-work - economically infeasible
Confirmation speed	✓ Sub-second	~10-60 min to finality
Independent verification	Needs the authority's certificate chain	✓ Anyone can check the public chain
Privacy	Only a hash leaves your control	Only a hash is anchored on-chain

The two are complementary - the qualified timestamp carries regulatory weight inside its framework, while Bitcoin needs no authority and no renewal to stay verifiable anywhere. That is why every Bernstein certificate carries both, with Bitcoin as its backbone.

7 · THE BERNSTEIN APPROACH

7 Anchored several ways, on purpose

Bernstein does not ask you to choose. Every certificate is anchored to **Bitcoin**, to an **EU qualified timestamp**, to a **China TSA**, and to a **global RFC 3161 authority** - so you get regulatory strength where it is required and a borderless, authority-independent record everywhere else.

Bitcoin

Borderless and durable. No authority to trust and no certificate to renew - the proof is the public chain itself, secured by proof-of-work and verifiable for as long as the network persists.

EU qualified · eIDAS

Univsign's qualified timestamp: presumed accurate and intact in EU courts (Art. 41(2)). The regulatory bar, met directly.

China TSA

UniTrust, time-sourced from China's National Time Service Center and named in the Supreme People's Court Internet-Court rules.

Global RFC 3161

DigiCert's ubiquitously trusted authority - an independent, redundant corroboration that verifies anywhere, with no special tooling.

WHY BITCOIN IS THE BACKBONE

A qualified timestamp is strongest inside its framework, but it leans on an authority staying accredited and a certificate staying current. A confirmed Bitcoin anchor has neither dependency: it is verifiable by anyone, in any jurisdiction, with open tools - and stays so even if Bernstein and every authority disappeared. Rewriting a confirmed block would mean redoing its proof-of-work, which is economically infeasible. That is why Bitcoin is the backbone of every certificate, reinforced by the qualified and regional authorities.

INDEPENDENTLY VERIFIABLE

We provide proof, not a legal opinion. The EU timestamp meets eIDAS; blockchain evidence is increasingly accepted in courts worldwide; Bernstein is cited by WIPO and WTO. Every anchor can be checked without us.

8 · ROADMAP

8 Expanding national coverage

The authority list grows as customers need new jurisdictions. Current and near-term coverage:

**EU, China & global** **LIVE**

Universign (EU · eIDAS-qualified), UniTrust (China), and DigiCert (global · baseline RFC 3161) - all in production today, alongside Bitcoin anchoring on every certificate.

**Switzerland - SwissSign** **NEXT**

A qualified Swiss time-stamping authority (SwissSign), for ZertES recognition in Switzerland. Planned, same RFC 3161 integration pattern.

**Further national authorities** **ON REQUEST**

Additional qualified or national authorities can be added per jurisdiction for enterprise and white-label deployments.

Want this brief tailored to your jurisdiction or integrated into a procurement pack? Contact your Bernstein partner - www.bernstein.io.