Signing Doesn't Always Claim Authorship

Daniel Hardman

2026-02-07

Abstract

Introduces some nuance about the assumption common in decentralized identity circles, that a digital signature is a claim of authoriship. This is sometimes the intended meaning, but numerous use cases provide counter examples.

People often treat a signature as if it were a claim of authorishop. That is sometimes true. But it is not what signatures *are* in general — and it is not what digital signatures are in particular.

A signature is a mechanism. Its meaning depends on context.

UNCITRAL makes this explicit in its *Guide to Enactment for the Model Law on Electronic Signatures*. It notes that handwritten signatures traditionally identify a person, show personal involvement in signing, and associate that person with a document. But it also says a signature can perform *many* functions depending on the document — including intent to be bound by a contract, intent to endorse authorship, intent to associate oneself with content written by someone else, or even to attest that a person was at a place at a time.[1]

That is a crisp statement of the nuance. Authorship is only one possible interpretation.

Common-sense examples outside cryptography

Petitions. When you sign a petition, you did not write it. Your signature expresses a stance: "I support this" (or at least "I support enough of this to lend my name").

Autographs. A sports figure signs a baseball or a photograph. That signature does not mean "I authored this object". It means "this object is now associated with me". Even the dictionary sense of *autograph* captures this: "the signature of a famous person".[2]

Notaries. A notary signs and stamps documents all day long, but the notary is not claiming authorship of those documents. Instead, the notary is certifying specific facts about the signing event.

For example, Utah's notary handbook defines an acknowledgment as a notarial act where the notary certifies that an identified signer "has admitted, in the presence of the notary, to voluntarily signing a document for the document's stated purpose".[3] Utah law uses essentially the same definition.[4] A signature witnessing similarly certifies that a voluntary signature was made in the notary's presence.[3] In other words: the notary's signature is about *identity and procedure*, not authorship.

If we can remember these ordinary cases, we will make fewer mistakes in digital identity.

What a digital signature proves (and what it does not)

In technical standards, a digital signature is usually defined narrowly: it provides integrity and origin authentication for signed data.[5] That is powerful, but it is not a complete theory of intent.

A digital signature can show that *someone controlling a private key* processed some bytes. It does not, by itself, tell you whether they meant:

- "I wrote this".
- "I witnessed this".
- "I approve this".
- "I authorise this".
- "I am acting as an agent".

Those meanings have to come from protocol, policy, ceremony, or surrounding evidence.

That is why modern ecosystems often *encode* purpose explicitly. The W3C Verifiable Credentials work includes a `proofPurpose` field (for example, `assertionMethod`) precisely to avoid guessing what a signature "means".[6, 7]

And the EU Digital Identity Wallet Architecture and Reference Framework is unambiguous that signing is not just about documents you authored: the Wallet "will allow the User to create qualified electronic signatures or seals over any data".[8] It even includes a blueprint titled "Remote QES — Creating a signature for authentication / authorisation".[9] If a signature can be for authentication or authorisation, then "authorship" cannot be the default inference.

The practical lesson

A signature is evidence that a signing mechanism ran.

If you need to know what was meant, do not assume. A governance framework or specification may answer. Otherwise, Ask where semantics come from:

- What role was the signer in?
- What ceremony or policy governs the act?
- What does the protocol say the signature is for?
- What facts (like notarial acknowledgments) are being certified?

References

[1] UNCITRAL. *Model Law on Electronic Signatures (2001) with Guide to Enactment*. See "Functions of signatures" (paras. 29–31). https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

[2] Britannica Dictionary. "Autograph". https://www.britannica.com/dictionary/autograph

[3] Utah Lieutenant Governor's Office. *Utah Notary Public Study Guide and Handbook* (2017). Definitions of acknowledgment / jurat / signature witnessing. https://notary.utah.gov/wp-content/uploads/2017/07/UtahNotaryPublicStudyGuideandHandbook5steps-7-5-2017.pdf

[4] Utah Legislature. Utah Code § 46-1-2 ("Acknowledgment"). https://le.utah.gov/xcode/Title46/Chapter1/46-1-S2.html

[5] NIST CSRC Glossary. "Digital Signature". https://csrc.nist.gov/glossary/term/digital_signature

[6] W3C. *Verifiable Credentials Data Model v2.0*. (See `proofPurpose` usage.) https://www.w3.org/TR/vc-data-model-2.0/

[7] W3C. *Verifiable Credential Data Integrity 1.1* (Editor's Draft). (See "proof purpose".) https://w3c.github.io/vc-data-integrity/

[8] European Digital Identity Wallet. *Architecture and Reference Framework v2.7.3*. Section 3.9 (QESRC Providers). https://eudi.dev/2.7.3/architecture-and-reference-framework-main/

[9] European Digital Identity Wallet. *Architecture and Reference Framework v2.7.3*. Annex index entry: "Blueprint Remote QES — Creating a signature for authentication / authorisation". https://eudi.dev/2.7.3/architecture-and-reference-framework-main/