Zero knowledge is not zero trust – but what is it?

Dan Bogdanov, Ülo Jaaksoo

A cryptography professor once told me…

“Teaching zero knowledge usually results in zero knowledge for the students…

… unless you draw lots of pictures.”

This is how we prove things “on paper”

Metro-General Hospital
479 W 58th Street, New York, NY 10019

12/02/2021

CERTIFICATION OF HEALTH RECORDS

I, Claire Temple, Night Nurse at the Metro-General Hospital in New York, certify the attached health records compiled for a Mr **Matthew Michael "Matt" Murdock** born 01/14/1985 in New York, NY, over the period 1985-2021 are complete and correct. They are presented in the ANNEX affixed to this document.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed my Official Seal on the date written.

- Validation guidelines
- Official letterhead?
- Contents reasonable?
- Written signature?
- Official seal?

- Looks like the real thing!

Some graphics from https://marvelcinematicuniverse.fandom.com/wiki/Metro-General_Hospital

All the data goes along with the certificate

ANNEX to CERTIFICATION OF HEALTH RECORDS

Subject: Matthew Michael "Matt" Murdock
Born: 01/14/21 in New York, NY
Healthcare provider: Metro-General Hospital, New York, NY 10019

Certified diagnoses:

ICD-11 code	ICD-11 name	Date of diagnosis
9D90.3	Severe vision impairment	05/06/2012
EA90.50	Scalp psoriasis	03/22/2019

Certified by:

Date: 12/02/2021

- The data is a part of the certificate.
- Even if all of this is not needed!
- E.g., the skin condition is not disqualifying, but the hospital may not know and may not need to.

This is how we prove things digitally (today)

Signature

Attribute	Value
Signer's Certificate	BOGDANOV,DAN,PNOEE-38302284213
Signer's Certificate issuer	EID-SK 2016
Signature method	http://www.w3.org/2001/04/xmldsig-more
Container format	application/vnd.etsi.asic-e+zip
Signature format	BES/time-stamp
Signed file count	1
Signature Timestamp	17.11.2021 10:42:55 +02:00
Signature Timestamp (UTC)	17.11.2021 08:42:55 +00:00
TS Certificate	SK TIMESTAMPING AUTHORITY 2021
TS Certificate issuer	EE Certification Centre Root CA
Hash value of signature	30 31 30 0D 06 09 60 86 48 01 65 03 04 02
OCSP Certificate	EID-SK 2016 AIA OCSP RESPONDER 2021
OCSP Certificate issuer	EID-SK 2016
OCSP time	17.11.2021 10:42:55 +02:00
OCSP time (UTC)	17.11.2021 08:42:55 +00:00
Signing time (UTC)	17.11.2021 08:42:55 +00:00
Claimed signing time (UTC)	17.11.2021 08:42:44 +00:00

- We take the same document, but sign it using digital signatures.
- Validation guidelines
- Official letterhead?
- Contents reasonable?
- Digital signature present?
- Trust chain valid

- Humans need tools to validate.

CYBERNETICA

Future of digital signatures and proofs

	Paper	Digital	Next step
Proof media	Paper with data (often sent digitally!)	Digital document with data	**Digital document with proof on data contents**
Data validation	Receiver validates based on data annex	Receiver validates based on data annex	**User validates, proves result and correctness**
Transparency of validation process	No built-in transparency into validation process	No built-in transparency into validation process	**User will know the result in advance**
Authenticity tools	Letterhead, seals, handwritten signatures	Digital signatures using Trust Providers	Digital signatures using Trust Providers
Human validation	Widely performed, may require forensics	Tool-assisted, trusted tools needed	Tool-assisted, trusted tools needed
Sources of fraud	Visual forgeries (analog/digital)	Unauthorised access to signing tools	Unauthorised access to signing tools

Let’s move to the future!

https://cyber.ee/
info@cyber.ee
cybernetica
CyberneticaAS
cybernetica_ee
Cybernetica

Dan Bogdanov

© 2026 Cybernetica AS. All rights reserved.

CYBERNETICA