THE MODERN FIGHT FOR FREEDOM

PRACTICAL ASPECTS OF TAKING BACK CONTROL OF YOUR DIGITAL IDENTITY

ASSURED WEBINAR 11/07/2023

WHAT IS

DIGITAL IDENTITY

DEVELOPMENT OF IDENTITY

SELF-SOVEREIGN IDENTITY

I hold **my** claims.
I am in **control**

CENTRALIZED IDENTITY

IANA, ICANN, Phone Company, CA's

USER-CENTRIC IDENTITY

Consent & Interoperability

FIDO, OPENID

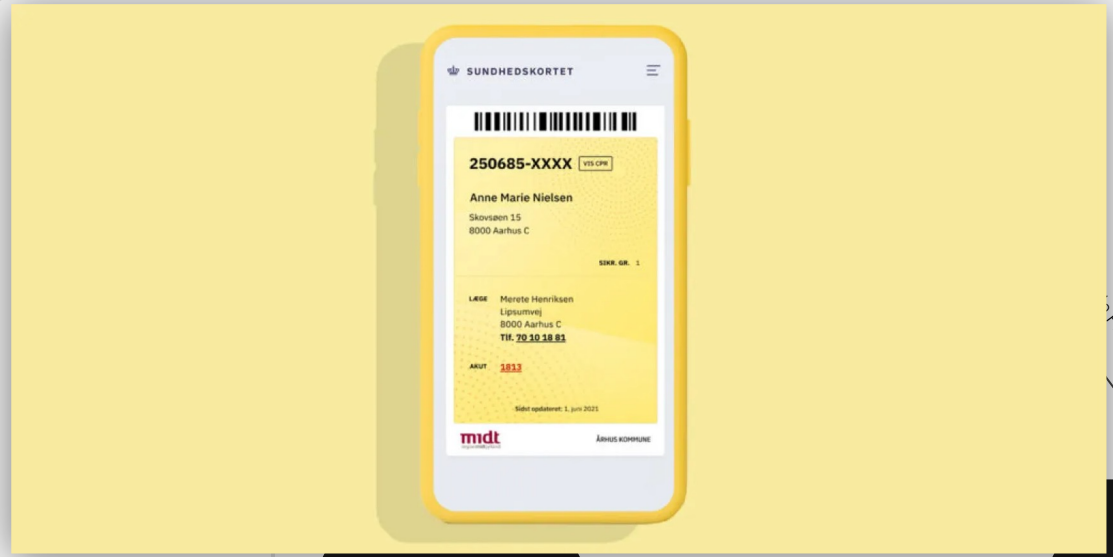
FEDERATED IDENTITY

Same Identity - multiple places.

TRIANGLE OF TRUST

Verifiable Credential (VC)
Contains claims and attributes

Verifiable Presentation (VP)
Contains a subset of claims, including proofs, from the VC



Presentation

ISSUER

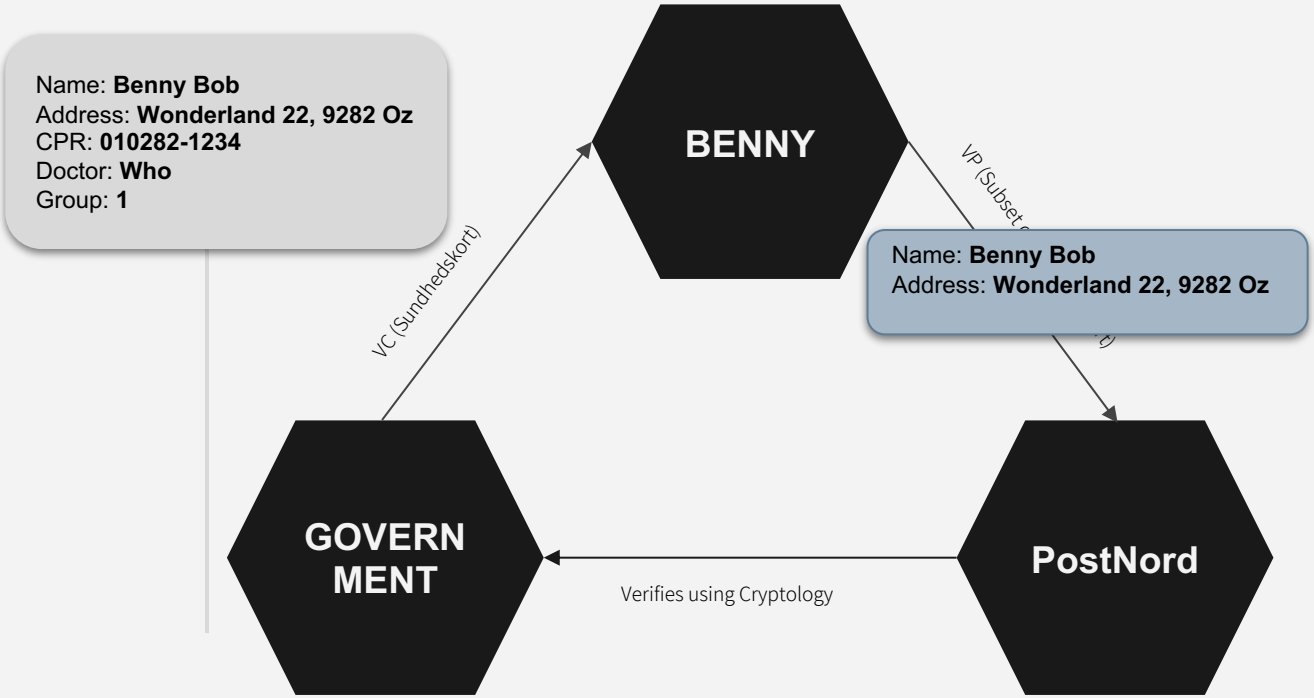
VERIFIER

Verifies using Cryptology

TRIANGLE OF TRUST

Verifiable Credential (VC)
Contains claims and attributes

Verifiable Presentation (VP)
Contains a subset of claims, including proofs, from the VC



THE CHALLENGES OF SELF-SOVEREIGNTY

1. How can we *guarantee* that the credential was not moved?
2. How do we make sure the wallet-platform isn't compromised?
3. ...And how do we do this, while giving the user control over their own privacy?

USER RESPONSIBILITY

Trust and responsibility moved f
centralized, **high-value, high-security** organizations to **low-value, low-security** users.

MALICIOUSNESS

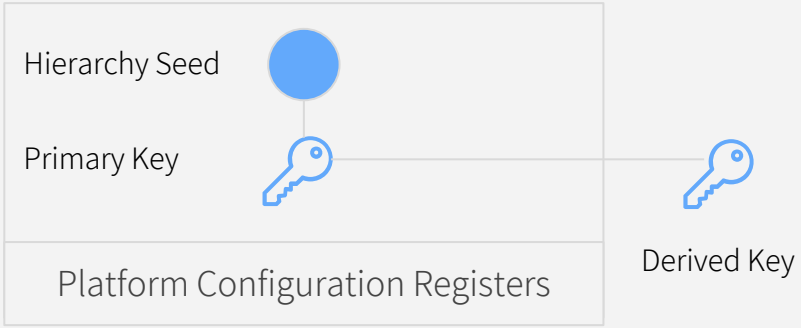
, might share credentials and act in malice.

Triangle of Trust

THE TPM

TPM Fundamentals

- Cryptographic Processor
- Small Internal Storage
- Policy Engine: Conditional Cryptography
- Keys are encrypted - can *only* be read by this particular TPM



Keys

Can be linked to *policies*, that can make the key usable under certain conditions, or limit the abilities of the key. Can *not* be moved to another platform*.

PCRs

Contains a digital fingerprint of the residing platform. Firmware, bootloader, etc. Can even hold fingerprints of applications.

*Keys can, if needed, be created to be copyable, but it's not common.

The ASSURED approach

By adding a **unique TPM key** to every issued **credential**, the issuer can get guarantees that the credential is safe. How?

By signing all **presentations** with this key. But it requires some properties.

KEY PROPERTIES

- May only be used in a Trusted State (PCRs)
- May only be used by authorization of the wallet
- Can only be used on particular TPM (hence: platform)
- Can provide *unlinkable* signatures (DAA)
- Policy (Trusted State) can be updated by the issuer, and only the Issuer.

All **presentations** must be signed by this key. If verified, the verifier knows

- The presentation comes from a trusted platform according to the issuer - if the verifier trusts the issuer, it now trusts that the presentation isn't a product of malicious software
- The presentation is made through an authorized wallet
- The credential has not been moved … Or has it?

DAA KEY

It's not possible for the verifier to determine *which* key gave the signature, only that it was valid and issued by that Issuer. What if a *similar* holder provided a signature, but he had a different security level?

SOLUTION

- Make the key part of the credential
  - Only a platform that can load that particular key, can get the claims.
  - This is possible through DAA-A

Conclusion

IT IS DIFFICULT

It is very difficult to protect privacy while at the same time guarantee security.

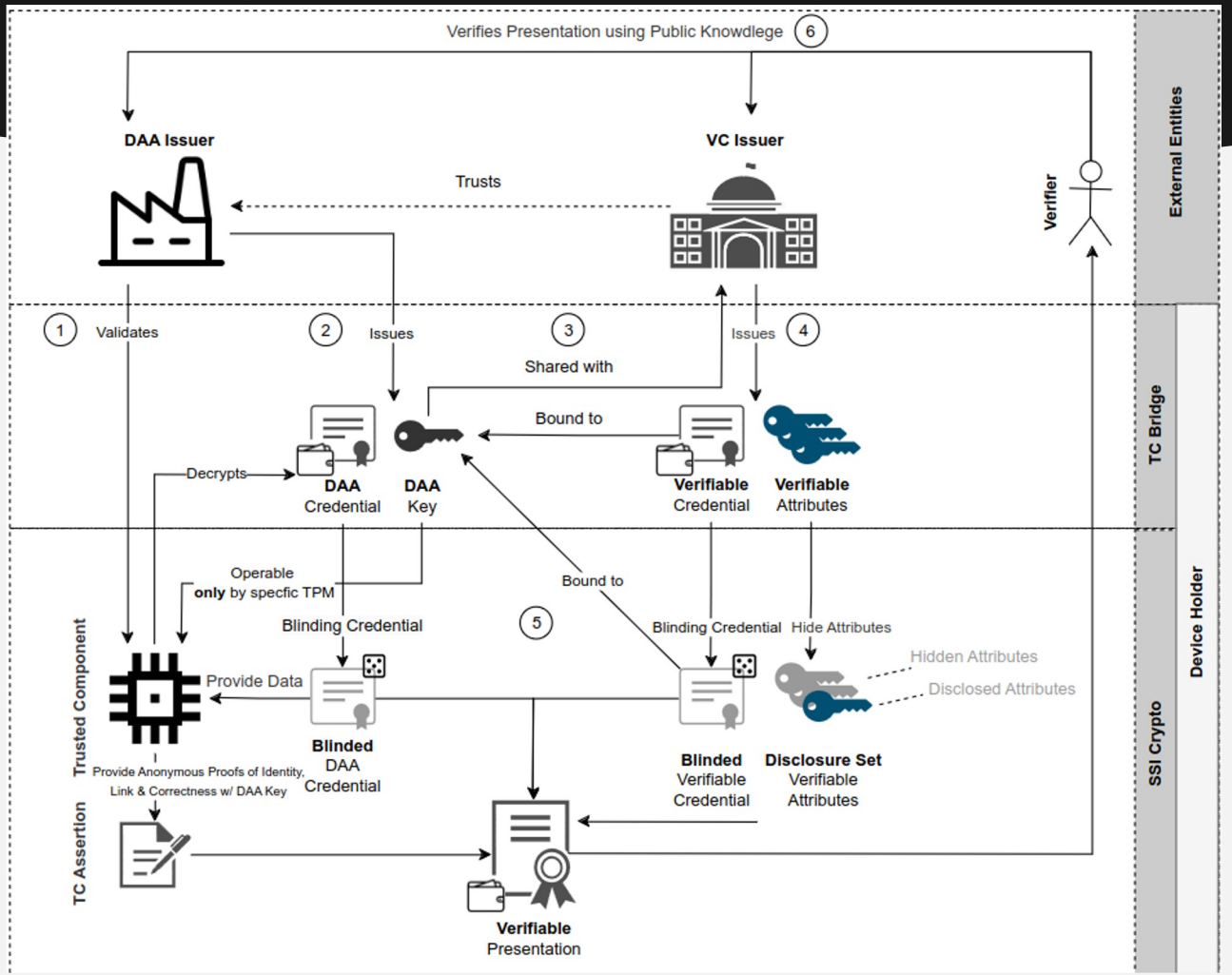
IT IS WORTH IT

Ensuring **we** hold our identities reduces the amount of data out there, enhances the privacy of the holder.

THERE IS A LOT TO BE DONE

We're not finished, there is a lot to be done, and a lot of parties that need to work together. But it can be done, and it must be done.

This is the modern fight for freedom, and it's worth the fight.


Verifies Presentation using Public Knowdlege
6
DAA Issuer
VC Issuer
Trusts
Verifier
External Entities
1
Validates
2
Issues
3
Shared with
Issues
4
Bound to
Decrypts
DAA
Credential
DAA
Key
Verifiable
Credential
Verifiable
Attributes
TC Bridge
Operable
only by specfic TPM
Bound to
Blinding Credential
5
Blinding Credential
Hide Attributes
Hidden Attributes
Disclosed Attributes
Trusted Component
Provide Data
Blinded
DAA
Credential
Blinded
Verifiable
Credential
Disclosure Set
Verifiable
Attributes
Provide Anonymous Proofs of Identity,
Link & Correctness w/ DAA Key
TC Assertion
Verifiable
Presentation
SSI Crypto
Device Holder

THANKS

Does anyone have any questions?