INTEROPen

Avast

Supported by

NHS X

NHS Digital

STAFF ACCESS MASTERCLASS

Decentralised Identity Overview

Andy Tobin

Avast

Avast

evernym

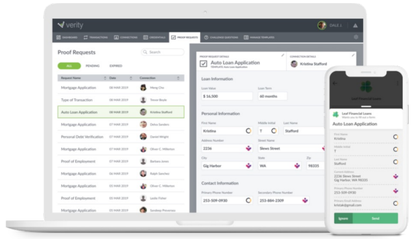
Working with the NHS on decentralised identity for the last 5 years

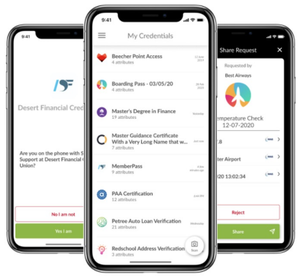
sovrin
identity for all

HYPERLEDGER
INDY

HYPERLEDGER
ARIES

HYPERLEDGER
URSA





Verity

The enterprise decentralised identity platform. For issuing and verifying credentials, for authentication, for secure messaging.

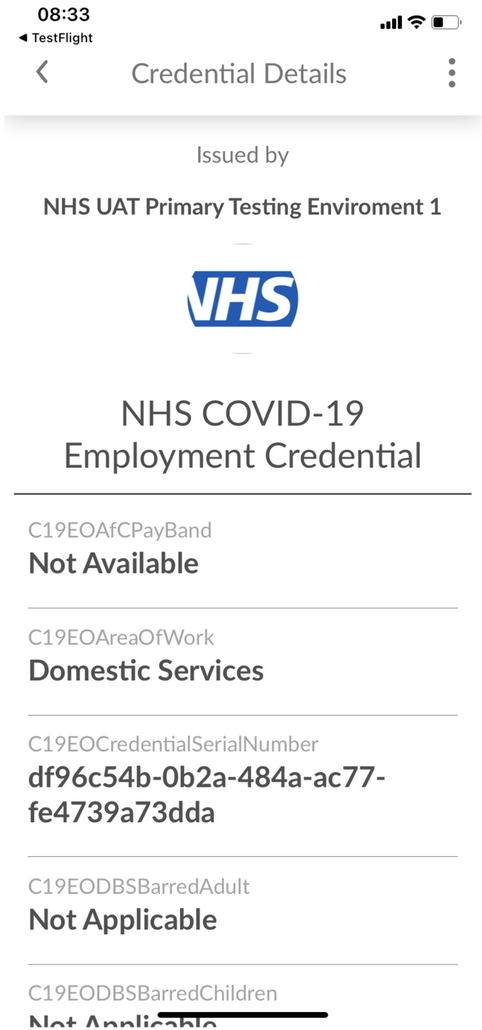
Connect.Me

Smartphone app and mobile SDK for getting, storing and using digital credentials.

Expertise & Guidance

How your business will change, business models, ecosystem building, deployment and operational requirements.

Working with the NHS on decentralised identity for the last 5 years



Verity

Supplied via Sitekit and embedded in each hospital's Staff Passport portal.

Connect.Me

Used as the NHS Digital Staff Passport app.

What Is “Decentralised Identity”

The ability for people to have, manage and control their own digital credentials, just like we do with our physical credentials.

With privacy and security superpowers.

Without needing a huge all-seeing centralised database.

Note 1: Also known as “Self-Sovereign Identity”

Note 2: Also works for organisations and things as well as people.

We call these
“credentials”

They answer the question:
“Says who?”

Credentials establish trust.

There is already a global standard for credentials – it's called paper.

But paper (and plastic) doesn’t work online

Why don’t we have digital versions of our paper and plastic credentials?

It’s not just about **identity**

These are also credentials. They convey a certification, entitlement or achievement.

They don’t work online either

Imagine if we all had digital versions of these.

Credentials that are globally interoperable, verifiable anywhere, and based on open standard.

“Digital Verifiable Credentials”

Imagine if…

Anyone can issue any digital credential about anything, to anyone.

Anyone can verify the authenticity and integrity of any digital credential.

Every interaction is private, secure and encrypted.

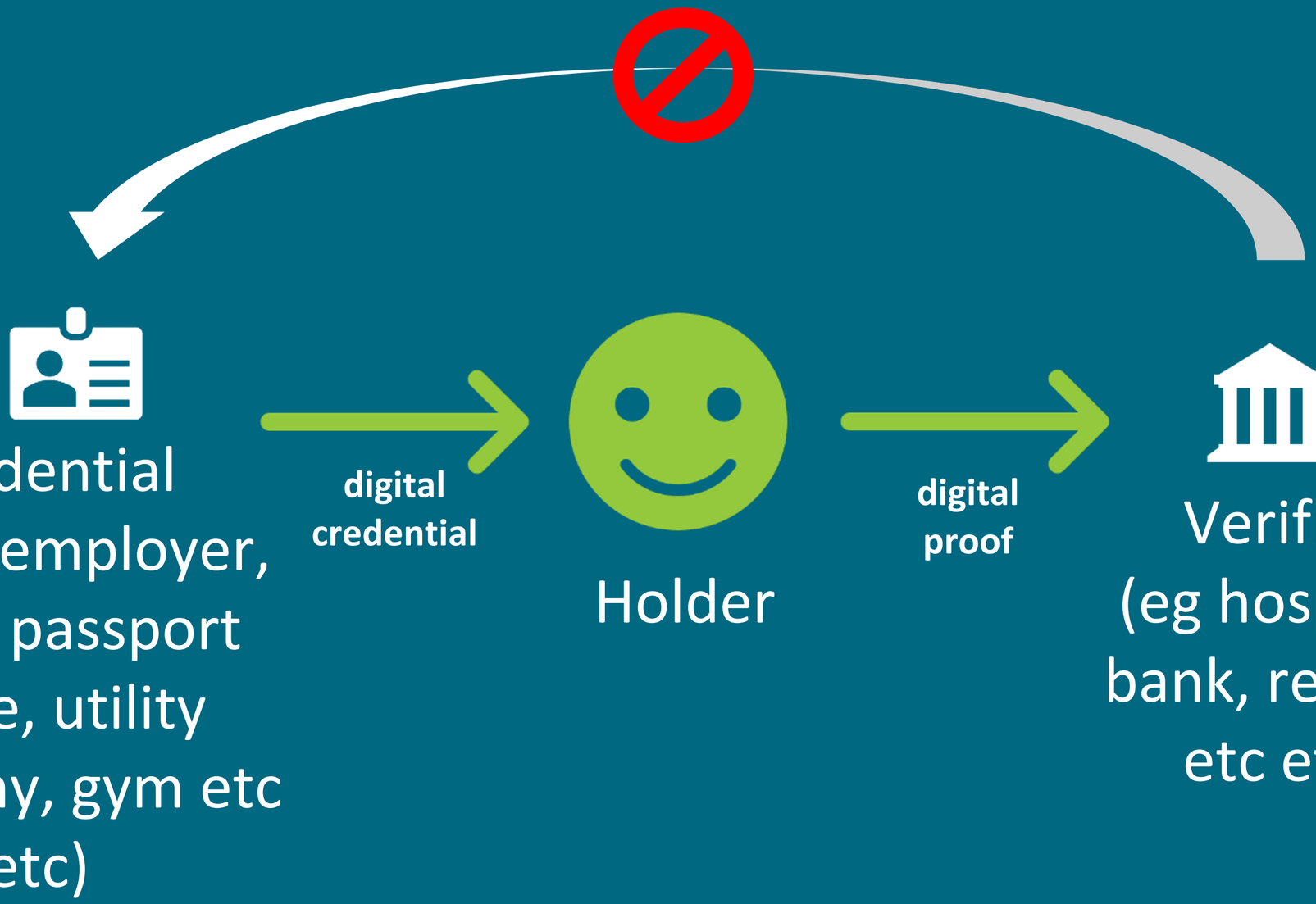
Without needing a huge privacy-busting central database.

And you can get rid of usernames & passwords (and pagers) too.

Like this:


Credential Issuer (employer, DVLA, passport office, utility company, gym etc etc)
digital credential
Holder
digital proof
Verifier (eg hospital, bank, retailer etc etc)

The verifier does not need to contact the issuer to verify a proof

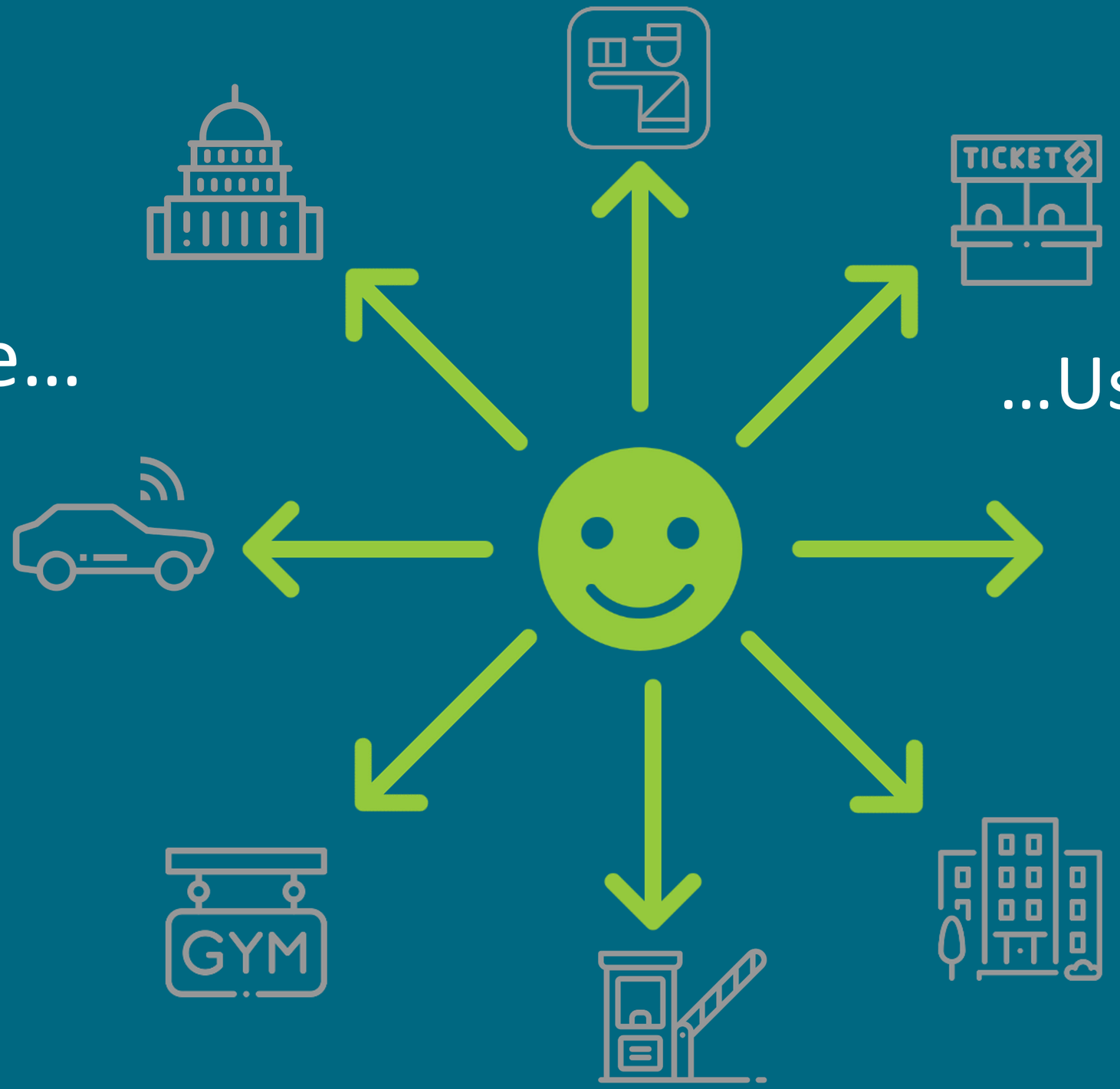


The verifier can check 4 things

1. Who issued the credential?
2. The credential belongs to the holder.
3. The credential hasn’t been changed/edited.
4. The credential hasn’t been revoked by the issuer.

Verifier
(eg hospital, bank, retailer etc etc)

Get Once…



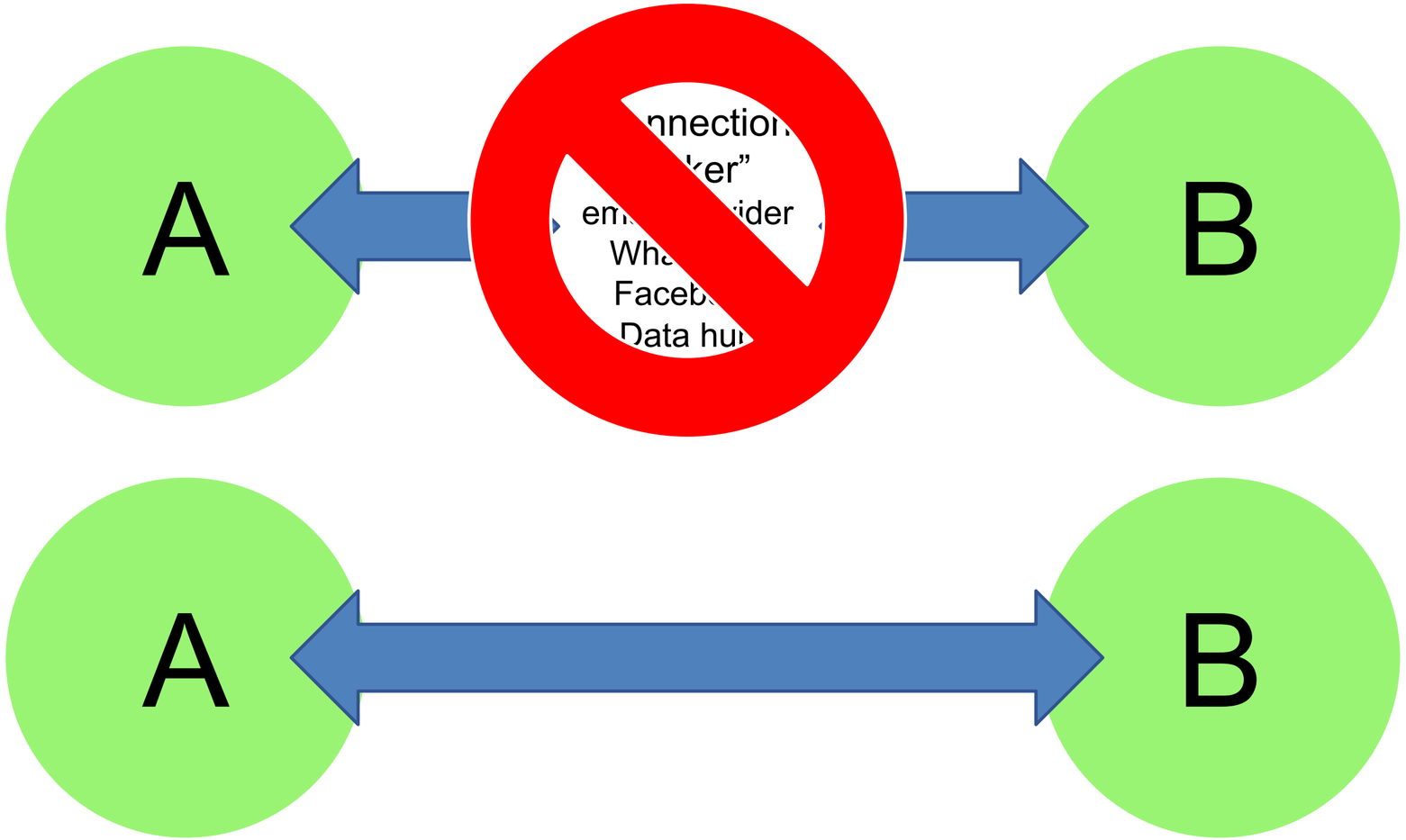
…Use Many Times

Slightly Techie Bit

How Does This Work?

3 Foundational Components

Foundational Component #1
Secure Connections



The old way. Connection brokers are used to establish and maintain digital connections between parties.

The new way. Two parties can independently form secure, unique and persistent connections without needing a broker to do it for them.

Secure connections enable trusted communications.

Foundational Component #2
Digital Data “Watermarking”

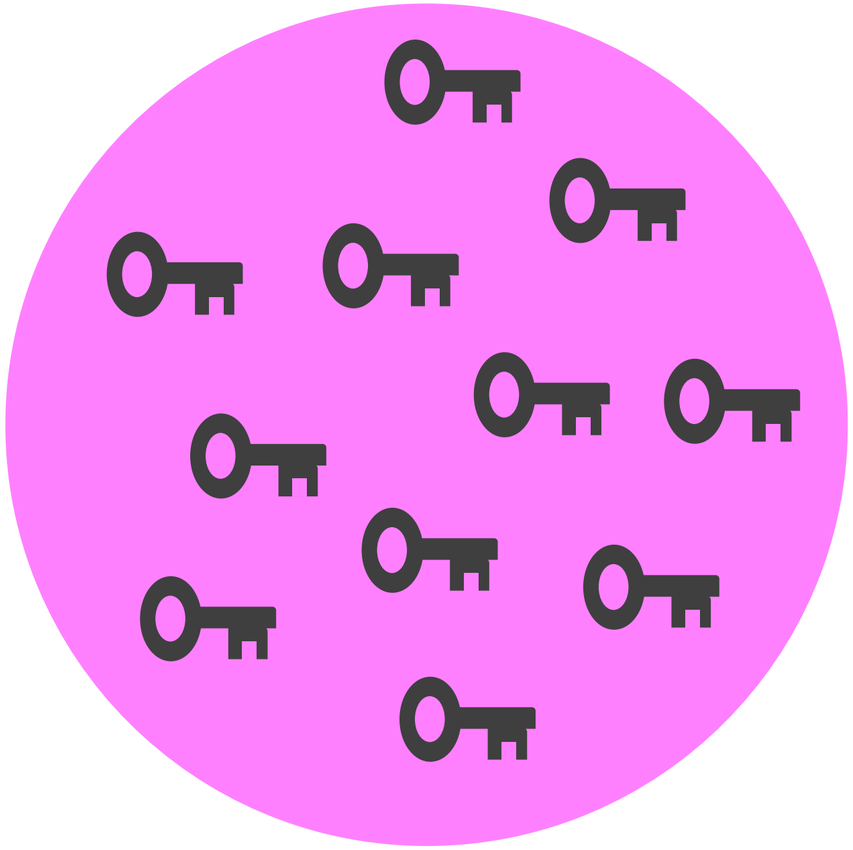
New digital data watermarking techniques enable any data to be given cryptographic superpowers.

These digitally verifiable credentials enable anyone to verify the authenticity of that data by checking:

- **Who issued the data**
- **Was it only issued to the presenter**
- **Has it been tampered with**
- **Has it been revoked**

Watermarked data can be verified as authentic by anyone.

Foundational Component #3
Trusted Public Key Directory



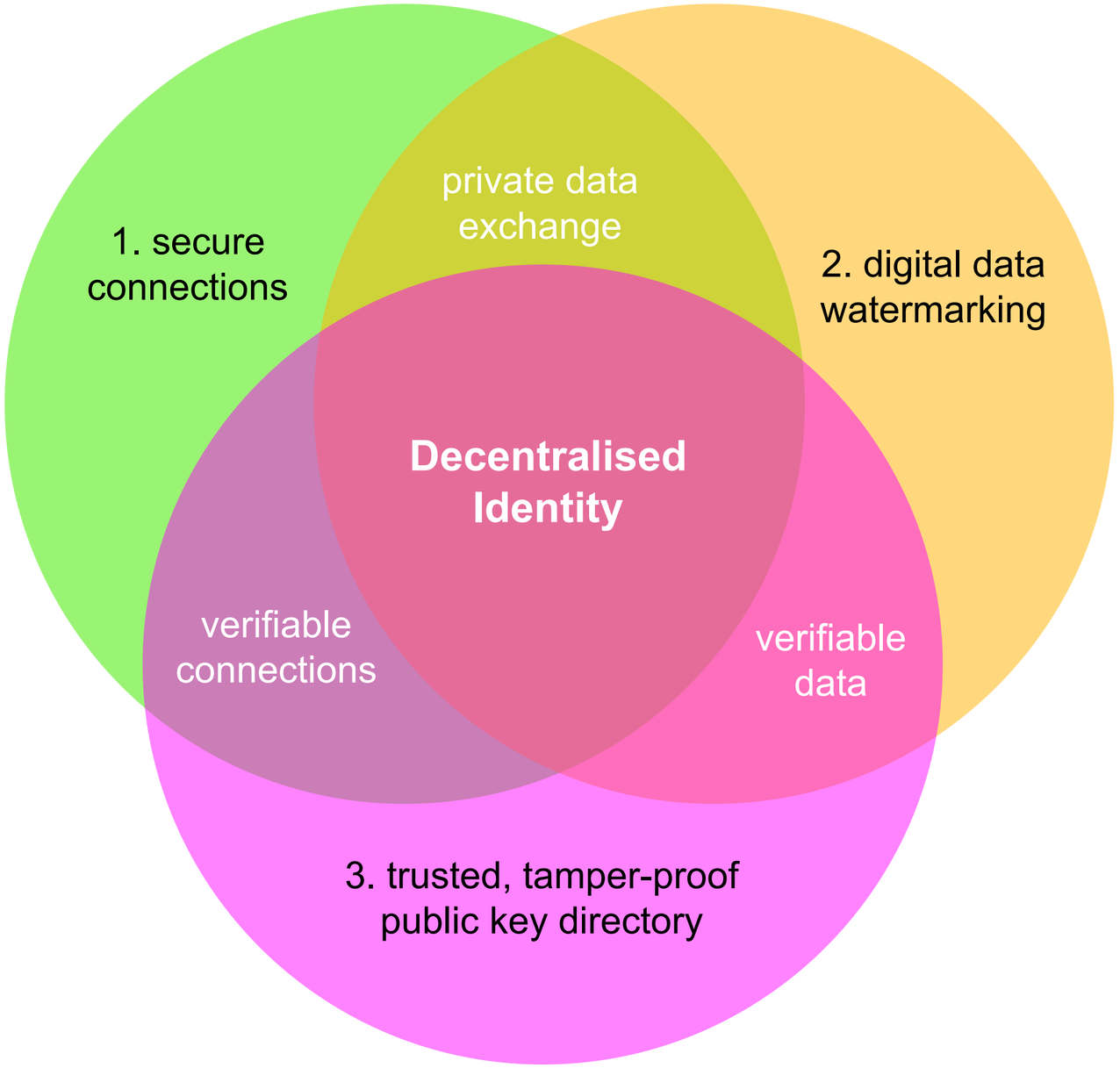
Digital credentials are verified using public key cryptography. The public keys of credential issuers need to be stored somewhere that has specific characteristics:

- **Run by many organizations, not one that could shut it down.**
- **Tamperproof.**
- **Chronologically ordered.**

These are the characteristics of distributed ledgers.

The public key directory gives everyone the tools to verify data.

The 3 Pillars of Decentralised Identity



Cool New Authentication Mechanisms

Already embedded within the tech used by the current Digital Statt Passport are some new authentication mechanisms. All use multi-factor authentication i.e. phone + biometric to open app + keys/credentials in the app.

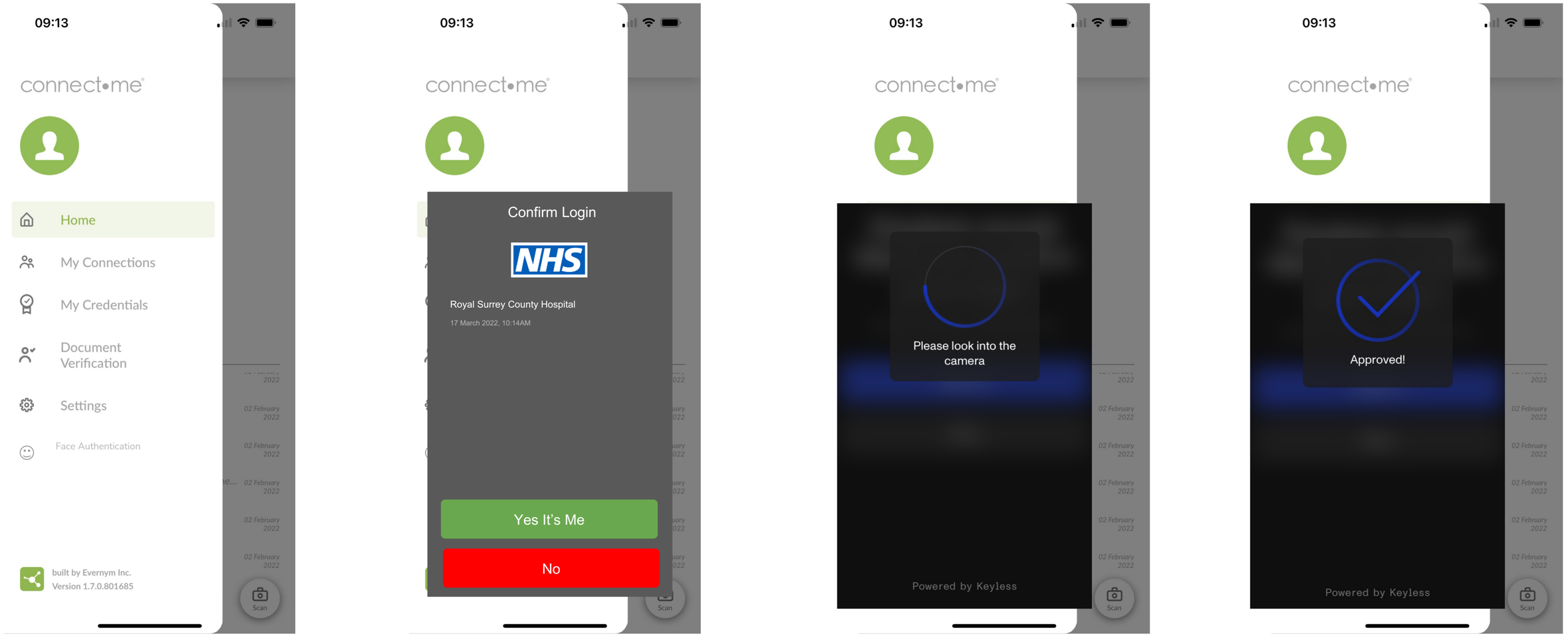
DIDAuth: Proof of possession of a unique private key embedded in a decentralised identifier (DID).

Committed Answer: DIDAuth + configurable on-screen challenge (eg “are you trying to log in to ERS?”

CredAuth: Challenge/Response + proof of ownership of a credential.

Decentralised Permissions: CredAuth + access rights held as attributes within a credential.

Integration of High Assurance Biometrics



Example: Integration of Keyless real-time biometrics verification into authentication flow.

What Does This Mean for You and Me?

Simplicity AND Privacy AND Security:

No more usernames or passwords.

No more registration forms.

No more spam or phishing.

Secure private communications by default.

No more intermediaries watching what I do.

What Does This Mean for Organisations?

Lower friction AND higher security

Instant user data verification

Fast onboarding with great user experience

Simplifying regulatory compliance

Reducing “toxic” data lakes

A secure, private relationship with each user

Interoperability across silos

You'll be able to use Verity and Connect.Me to:

- Write applications that issue and verify credentials that have been defined by the NHS for the staff and volunteer use cases.
- Send authentication challenges to users to replace traditional login mechanisms.
- Send messages to users and receive back authenticated responses.
- And…create your own credential types, use cases, augment the NHS use cases with your own and come up with new ideas.

Developer Resources

- **evernym.com/nhs-hackathon/ for docs, SDK, APIs, sample code, repos.**
- **Connect.Me in the appstores and https://try.connect.me demo site.**
- **Verity technical masterclass and demo coding video**

INTEROPen

Avast

Supported by

NHS X

NHS Digital

STAFF ACCESS MASTERCLASS

Decentralised Identity Overview

Andy Tobin

Avast