





Supported by





STAFF ACCESS MASTERCLASS \mathbf{O} Decentralised Identity Overview

Andy Tobin Avast





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









verity							DALEJ 🔺	
Stareouto 😅 Tanon(Tor	a 🔝 connections				NAGE TEMPLATES		٠	
Proof Requests		Q. Search	PROF MONTOFINI			COMPLETION OF TALL		
ALL PENDING	EXPRED	Auto Loan Application			🔕 Kristina Staffi			
Request Name 0	Date 0	Connection 0	Loan Information					
Mortgage Application	DE MAR 2019	👼 Meng Cho	Lose Webe		Loan Term		- 16	
Type of Transaction	06 MAR 2019	2 Teachart	\$ 16,500		60 months		Leaf Financial Lear	
Auto Loan Application	08 MAR 2019	Se Kolena Station	Personal Information				Leaf Financial Leans	
Mortgage Application	07 MAR 2019	Online Sanders	First Name			ot Name	Auto Loan Application	
Personal Debt Verification	07 MAR 2019	Dariel Wingte	Kristina Address Number	0	T O S	kafford	First Name Kolstina	0
Mortgage Application	07 MAR 2019	😽 Olver C. Mileton	2236	÷	Slews Street		Made to the	c
Proof of Employment	07 MAR 2019	1 Interation	City		State	Zp	Lat Name Stafford	0
Mortgage Application	06 MAR 2019	Ralph Sanchez	Gig Harbor	*	NIA	98335	Current Address 2236 Siews Street	
Mortgage Application	05 MAR 2019	Cliver C. Millerton	Contact Information				Gig Harbor, WA 98325	
Proof of Employment	05 MAR 2019	1 unit fair	Primary Phone Number 253-509-0930	0	Secondary Phone Nur 253-884-2309	der .	253-509-0930 Primes final Address	
Mortgage Application	05 MAR 2019	Sandersp Prevenues	DESTRATION	0	253-004-2347		kristak@gmail.com	C
							laws See	

O Master Guidance Certif With a Very Long Name 7 attributes

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

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.

Verity

Connect.Me





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

08:33 ...| 🌫 📭 TestFlight Credential Details

Issued by

NHS UAT Primary Testing Environment 1



NHS COVID-19 **Employment Credential**

C19EOAfCPayBand

Not Available

C19EOAreaOfWork

Domestic Services

C19EOCredentialSerialNumber df96c54b-0b2a-484a-ac77fe4739a73dda

C19EODBSBarredAdult

Not Applicable

C19EODBSBarredChildren

Not Applicable

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

Used as the NHS Digital Staff Passport app.

Verity

Connect.Me



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?"





Creden

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

Credentials establish trust.







credentials?

But paper (and plastic) doesn't work online

Why don't we have digital versions of our paper and plastic





either



It's not just about identity

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

They don't work online





Imagine if we all had digital versions of these.

standard.

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

"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.



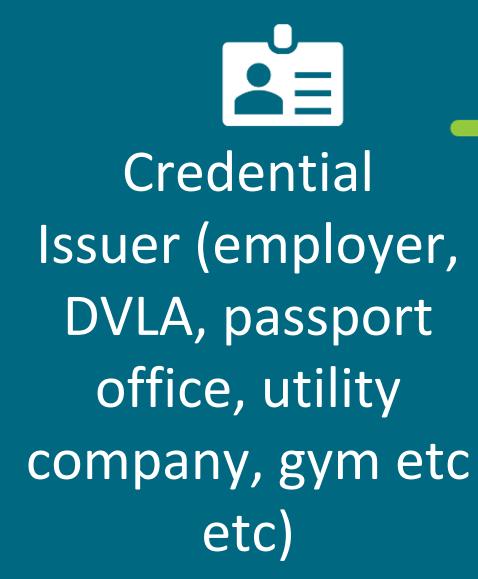
Like this:

Holder



digital proof Verifier (eg hospital, bank, retailer etc etc)

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



Holder

digital

credential

digital proof

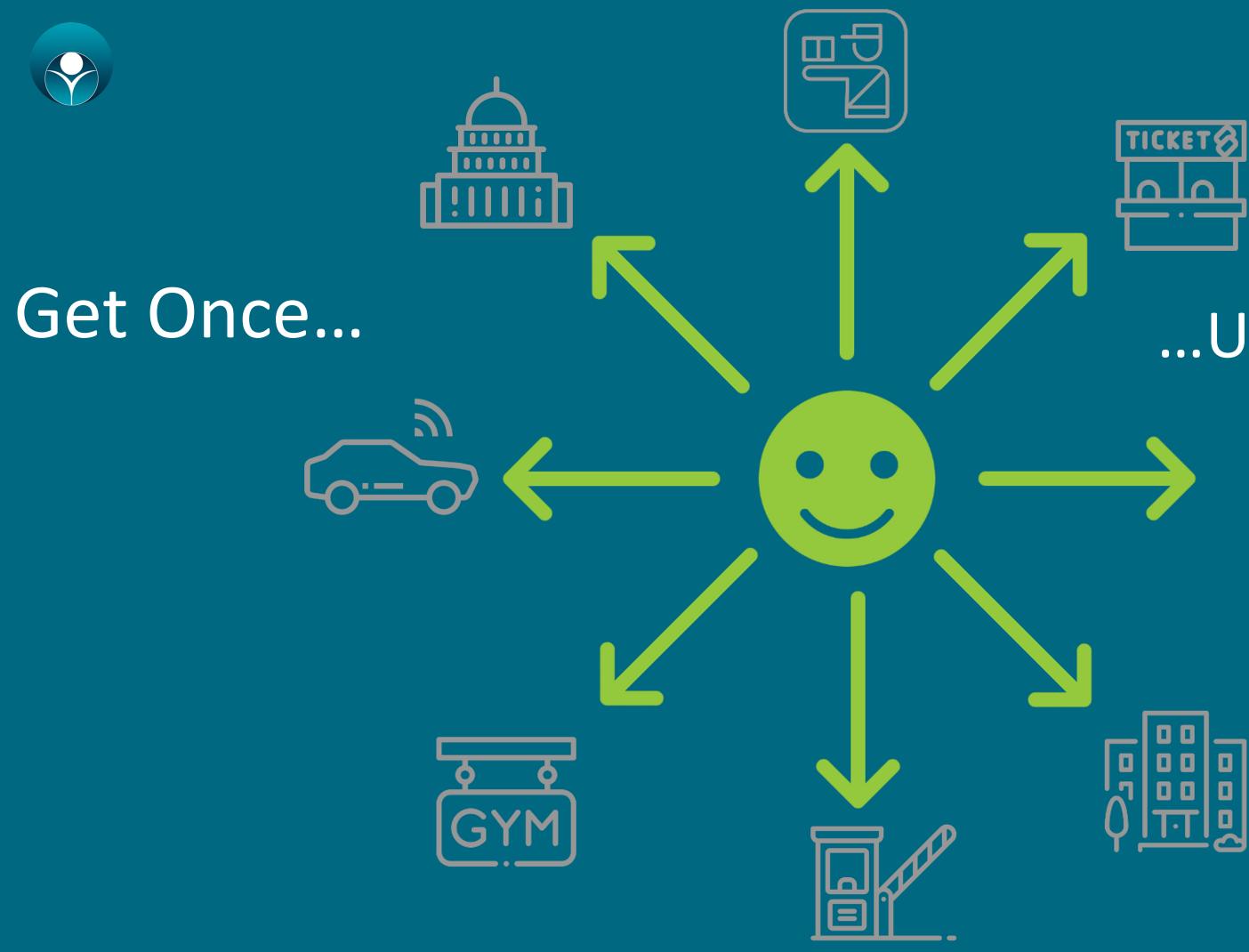
Verifier (eg hospital, bank, retailer etc etc)



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.

Werifier (eg hospital, bank, retailer etc etc)





... Use Many Times





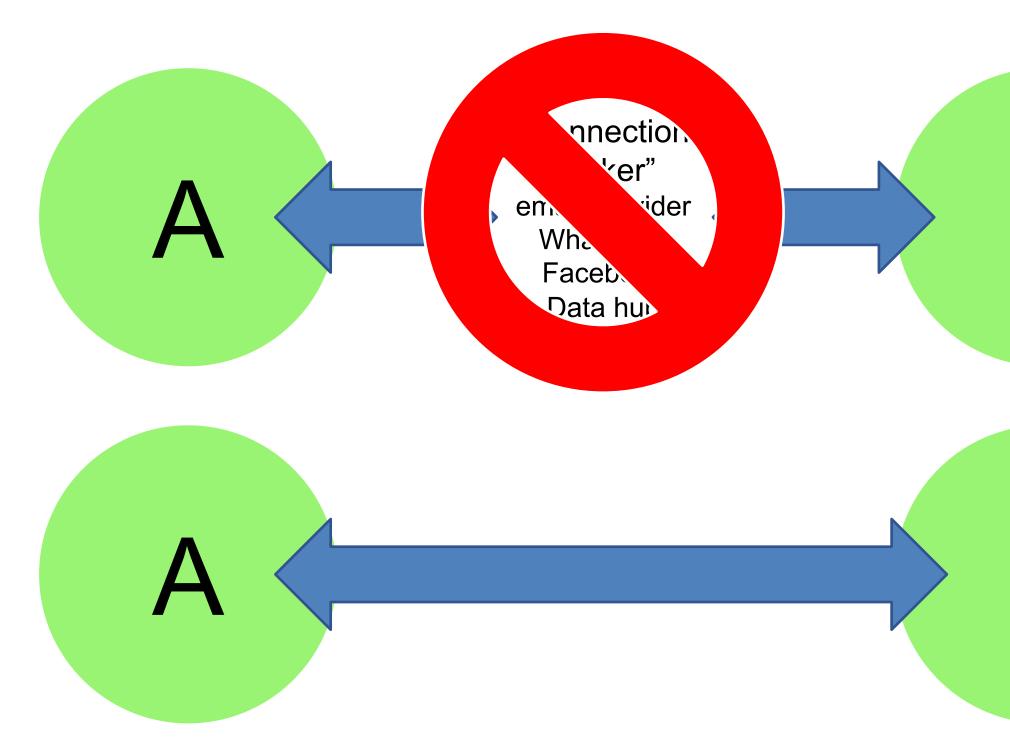
Slightly Techie Bit

How Does This Work?

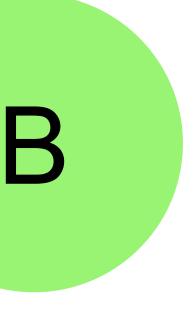
3 Foundational Components



Foundational Component #1 Secure Connections



Secure connections enable trusted communications.



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.



Foundational Component #2 Digital Data "Watermarking"



Watermarked data can be verified as authentic by anyone.

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

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



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:

- Tamperproof.
- Chronologically ordered.

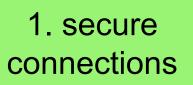
ledgers.

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

Run by many organizations, not one that could shut it down.

These are the characteristics of distributed

The 3 Pillars of Decentralised Identity



private data exchange

2. digital data watermarking

Decentralised Identity

verifiable connections

verifiable data

3. trusted, tamper-proof public key directory



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.

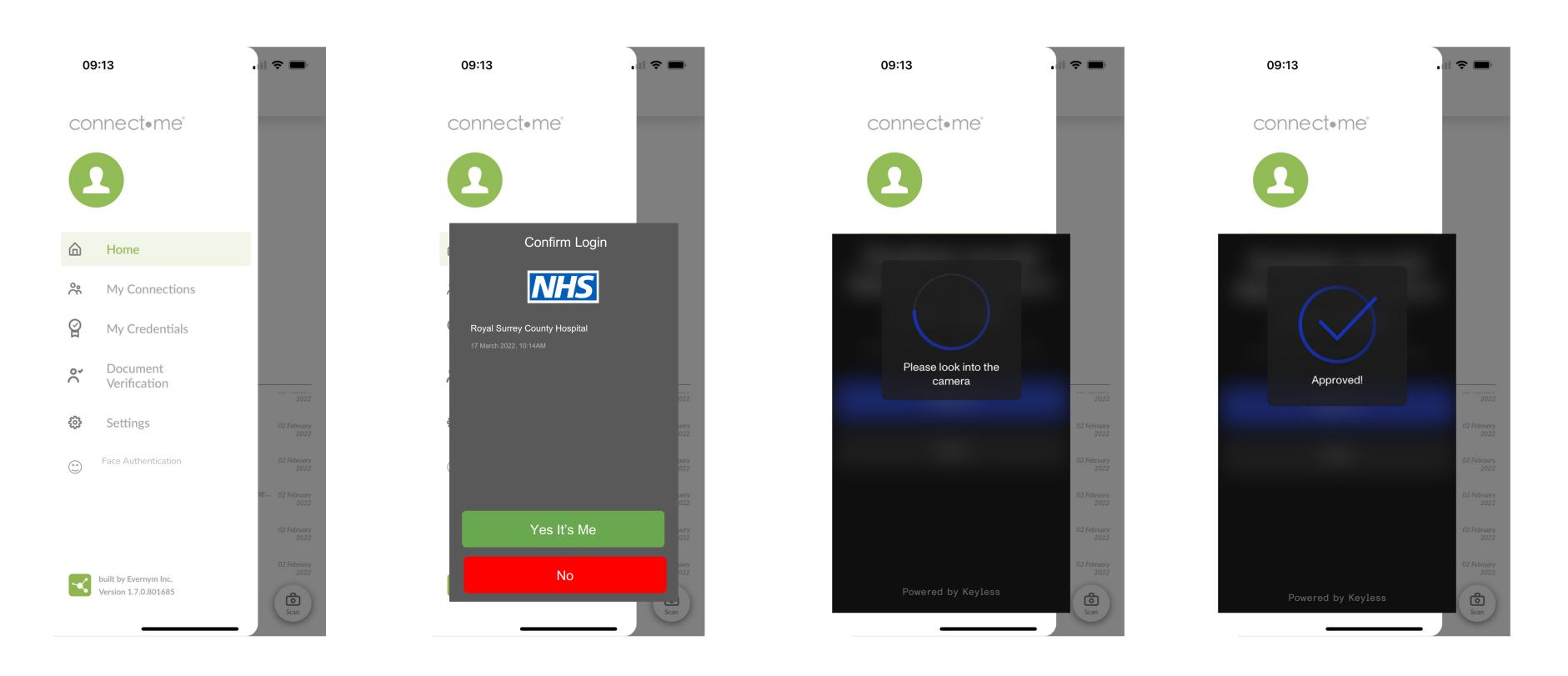
DIDAuth: Proof of possession of a unique private key embedded in a decentralised identifier (DID).

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.



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.



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:

- cases.

- ideas.

• Write applications that issue and verify credentials that have been defined by the NHS for the staff and volunteer use

 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





- 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 •







Supported by





STAFF ACCESS MASTERCLASS \mathbf{O} Decentralised Identity Overview

Andy Tobin Avast