UN/CEFACT
39th Forum

Verifiable Credentials
for
Cross-border trade

Steve Capell
steve.capell@gmail.com

A new data exchange framework

Issue a digitally verifiable trade document

Present the digitally verifiable trade document

Manual verification

-OR-

Automated verification

Issuing authority **existing** business system

Trader

verifying authority **existing** business system
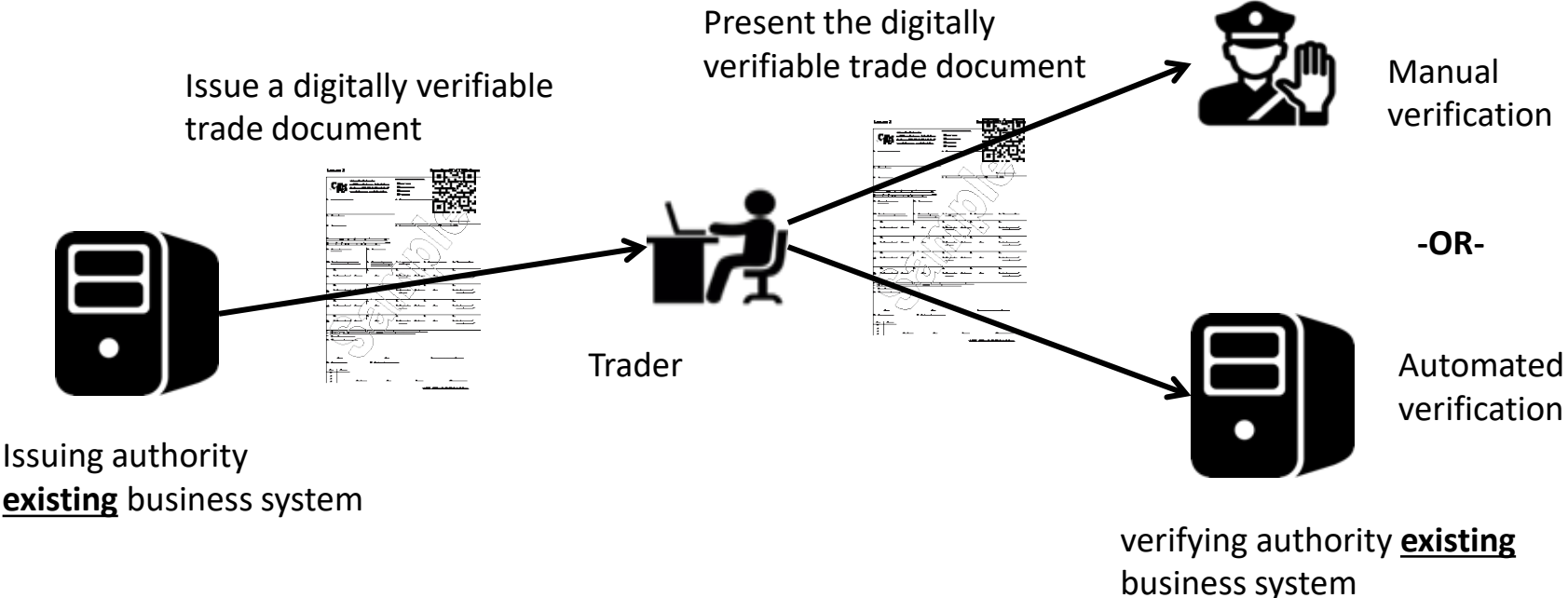
Using some new technology standards

From the world's leading web standards body:

W3C® WORLD WIDE WEB consortium

Two key technology standards

Verifiable Credentials
https://www.w3.org/TR/vc-data-model/

Decentralised Identifiers
https://www.w3.org/TR/did-core/

And from the world's leading digital trade standards body:

UNECE UN/CEFACT
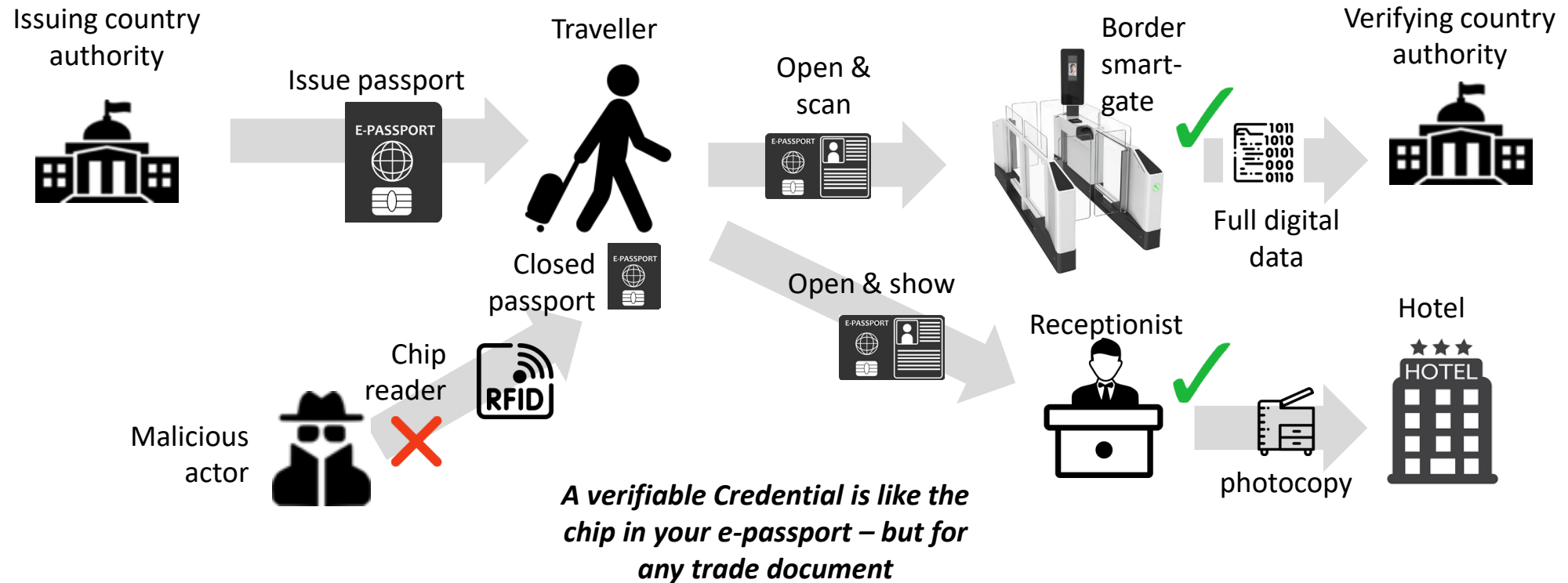
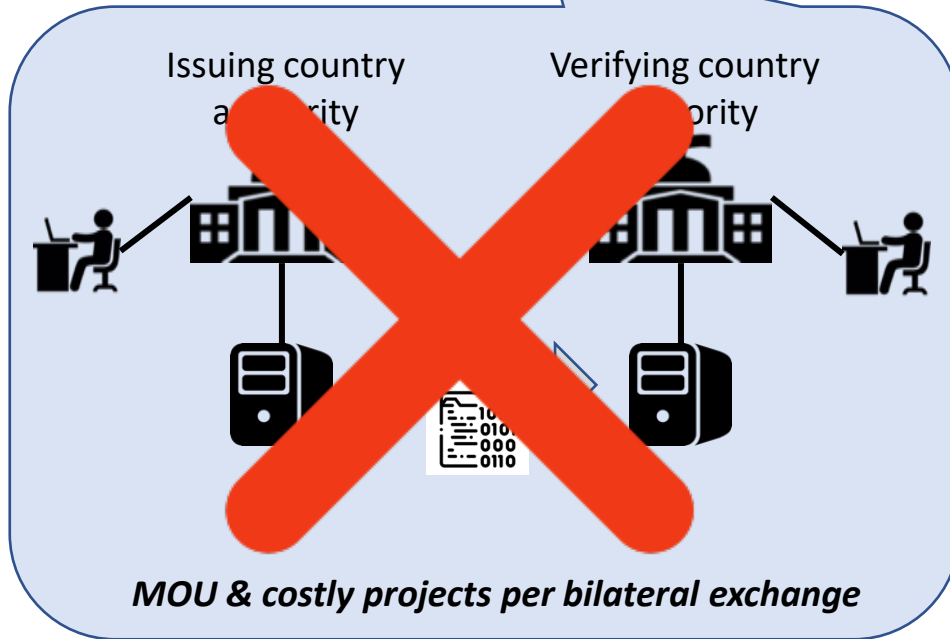A white paper that explains why they are important and how to use them

VCs for cross border trade
https://unece.org/sites/default/files/2022-09/WhitePaper_VerifiableCredentials-CBT.pdf

Which are best understood with an analogy

Issuing country authority

Issue passport

Traveller

Open & scan

Border smart-gate

Verifying country authority

Full digital data

Closed passport

Open & show

Receptionist

Hotel

Malicious actor

Chip reader

RFID

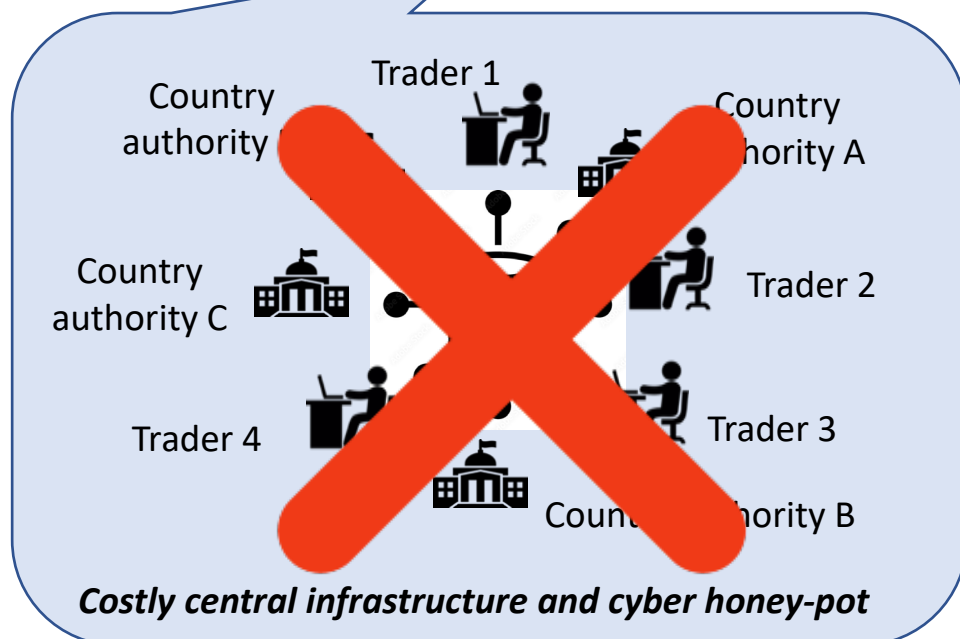*A verifiable Credential is like the chip in your e-passport – but for any trade document*

photocopy

They are cheaper and simpler than alternatives

The EDI pattern

Issuing country authority
Verifying country authority

MOU & costly projects per bilateral exchange

The Hub pattern

Country authority
Trader 1
Country authority A
Country authority C
Trader 2
Trader 4
Trader 3
Country authority B

Costly central infrastructure and cyber honey-pot

VCs can be verified simply by scanning a QR

Signed and encrypted,
placed in public store

Any Verifier
Service

Retrieve, decrypt,
and verify the VC

Redirect to hosted
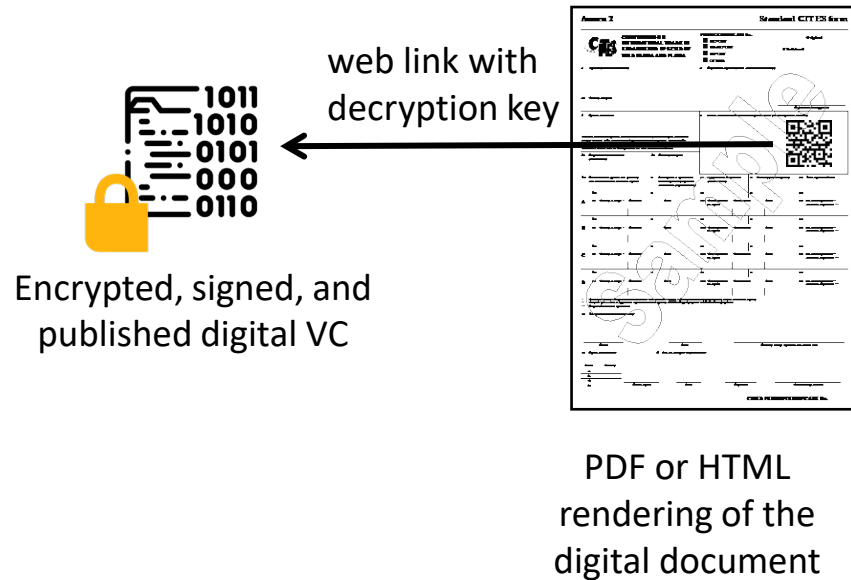verifier service

Issue permit
as VC

Verification

✓ No Tampering

✓ Not revoked

✓ Authorised
Issuer

Scan QR

Issuing country
authority

Issue document
as PDF with QR

Trade document

Importing
authority
verifies
document
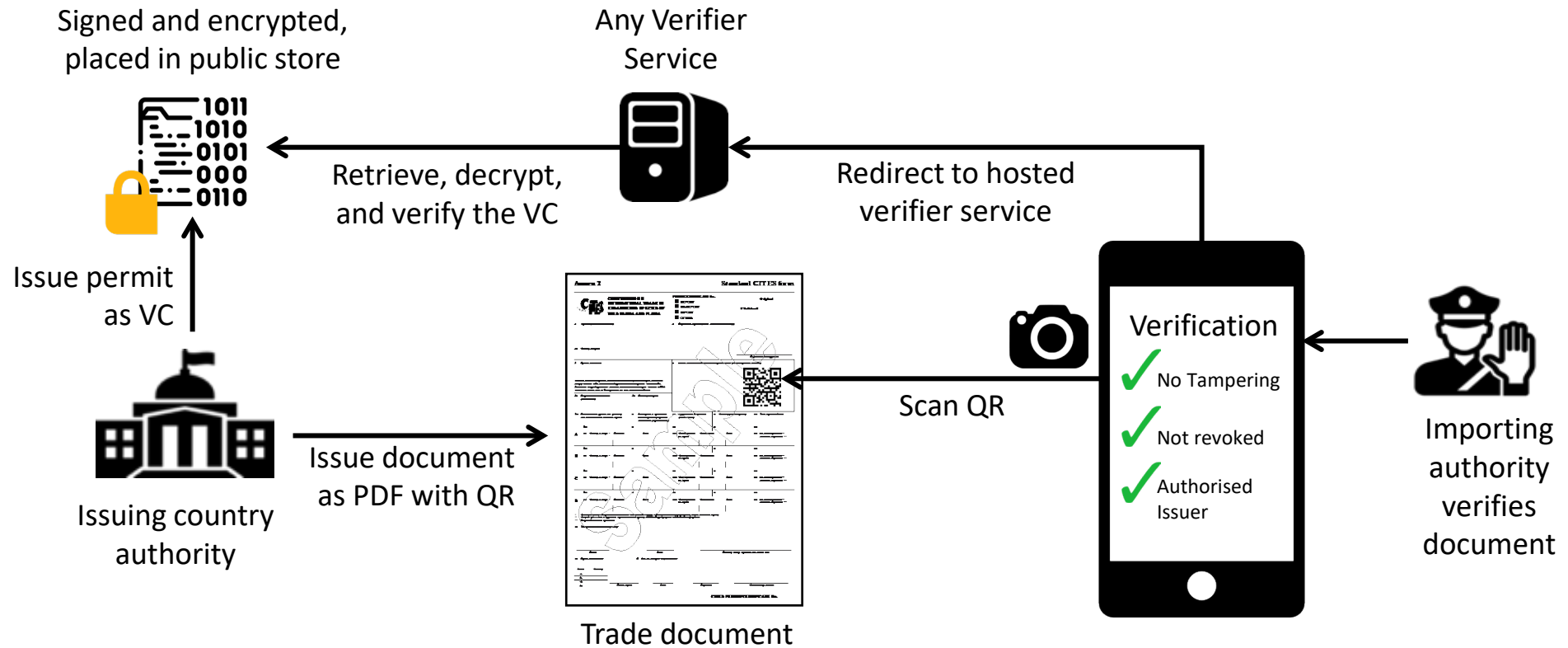
But advanced verifiers can still get all the data.

Signed and encrypted,
placed in public store

Retrieve, decrypt, verify the VC
and ingest full digital data

Authority business system
with VC capability

Issue permit
as VC

Issuing country
authority

Issue document
as PDF with QR

CITES permit

Permit
submitted to

QR
processed
by

verifying country
authority

Uses

Importing
authority
verifies
document
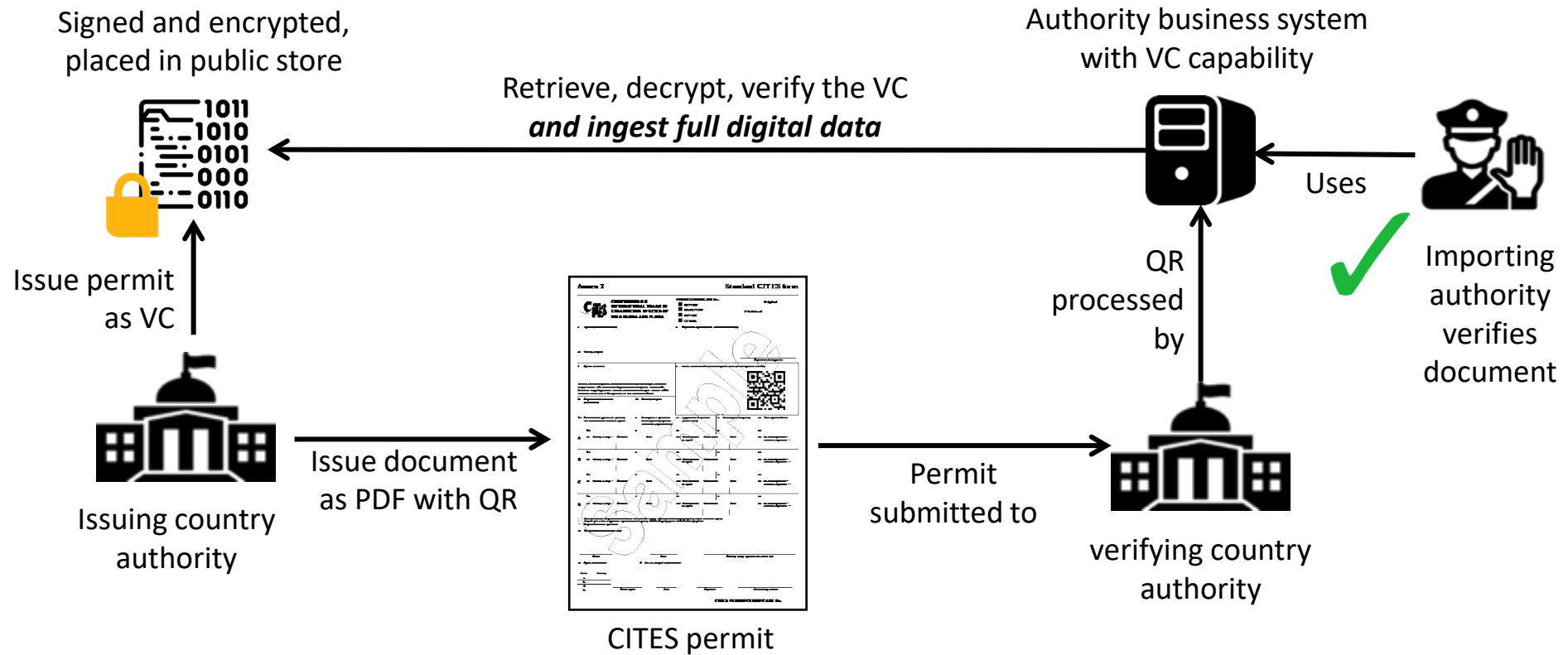
Wait, the same document is both paper and digital?

web link with decryption key

Encrypted, signed, and published digital VC

PDF or HTML rendering of the digital document

Yes! – and this is the key to scalability. You can go 100% digital without any dependency on verifier digital maturity

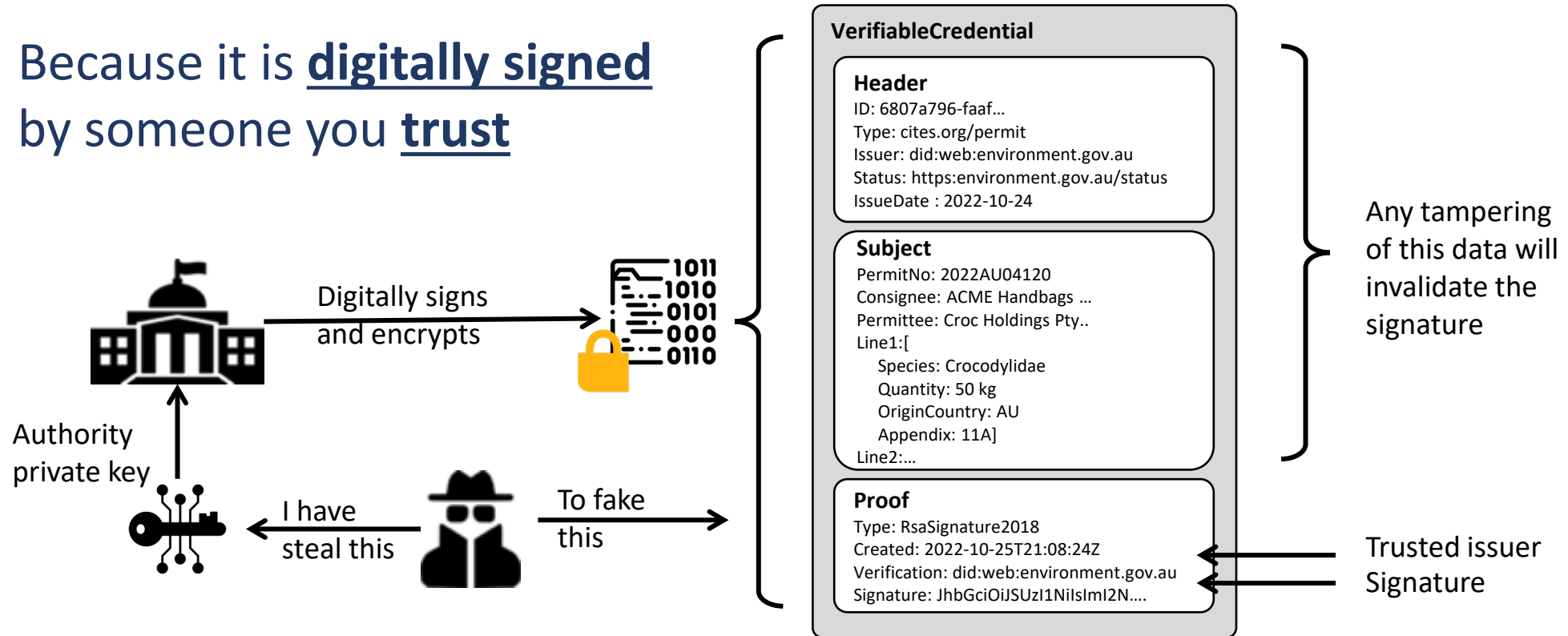# Published & public? But what about privacy?

An un-guessable ID: 6807a796-faaf-4194-9eaa-f2078621d643

A strong encryption key: r4u7x!A%D*G-JaNdRgUkXp2s5v8y/B?E

De-identified and encrypted with a unique key for each VC

Contains

Used to find & decrypt

Uses

Owns

Shares

In the very unlikely event that the link is discovered, the VC still cannot be decrypted

Only the holder of the permit has the keys – and can choose who to show them to

And how can I be sure that the VC is genuine?

Because it is **digitally signed** by someone you **trust**

Digitally signs and encrypts

Authority private key

I have steal this

To fake this

VerifiableCredential

Header
ID: 6807a796-faaf...
Type: cites.org/permit
Issuer: did:web:environment.gov.au
Status: https:environment.gov.au/status
IssueDate : 2022-10-24

Subject
PermitNo: 2022AU04120
Consignee: ACME Handbags ...
Permittee: Croc Holdings Pty..
Line1:[
    Species: Crocodylidae
    Quantity: 50 kg
    OriginCountry: AU
    Appendix: 11A]
Line2:...

Proof
Type: RsaSignature2018
Created: 2022-10-25T21:08:24Z
Verification: did:web:environment.gov.au
Signature: JhbGciOiJSUzI1NiIsImI2N....

Any tampering of this data will invalidate the signature

Trusted issuer
Signature

OK, what is it going to cost me to <u>issue</u> these?

Very little..

Use free software from UN or any compatible commercial VC toolkit
https://github.com/uncefact/project-vckit

VC software plus standard document schema

VC issuing / verifying software

Your **existing** document management system

New VC capability that you need to plug-in to your system

Your documentsas VCs
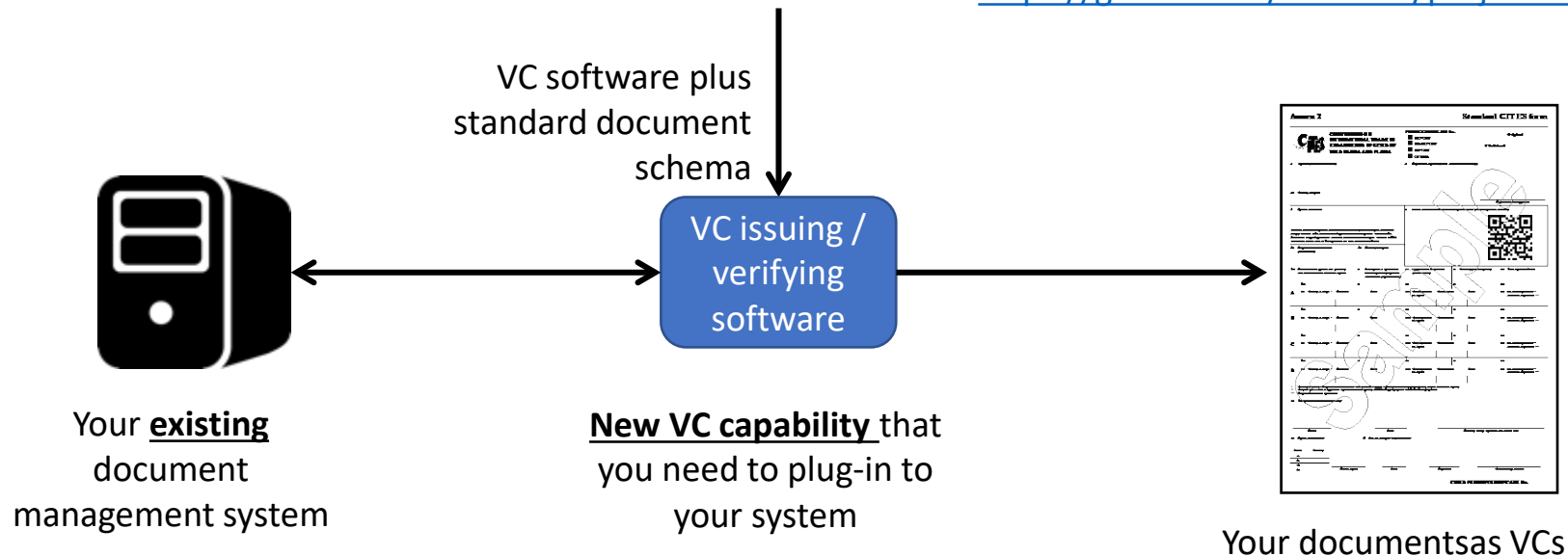
Wont I need some blockchain stuff?

Some VC solutions do use some blockchain – but it adds very little value.

Bitcoin

...hereum

Some oth...
cryto/blockchain
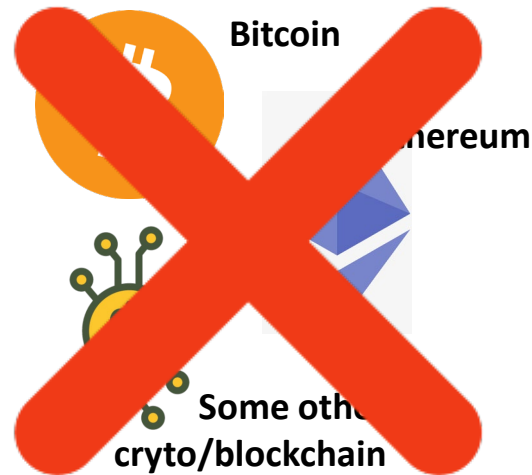
NOT NEEDED !

Lets see it working – scan this QR code

A Certificate of Origin as a VC

- Note the human readable version
- But click on the "JSON" tab to see the machine data

Note : We use a certificate of Origin as the sample – but could equally be any trade document

An advanced topic to close – trust graphs
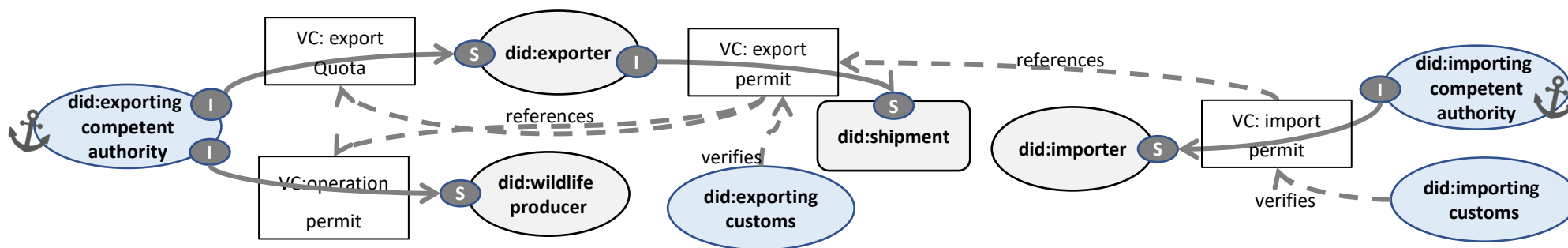
VCs can be linked together to form chains of trust. For example an importer permit linked to an export permit that is linked to a quota license and to an authorised wildlife producer. We call the linked set of credentials a **trust graph**. Valuable trust graphs are traceable to a **trust anchor**.

Some nodes can be hubs – VCs glue them together
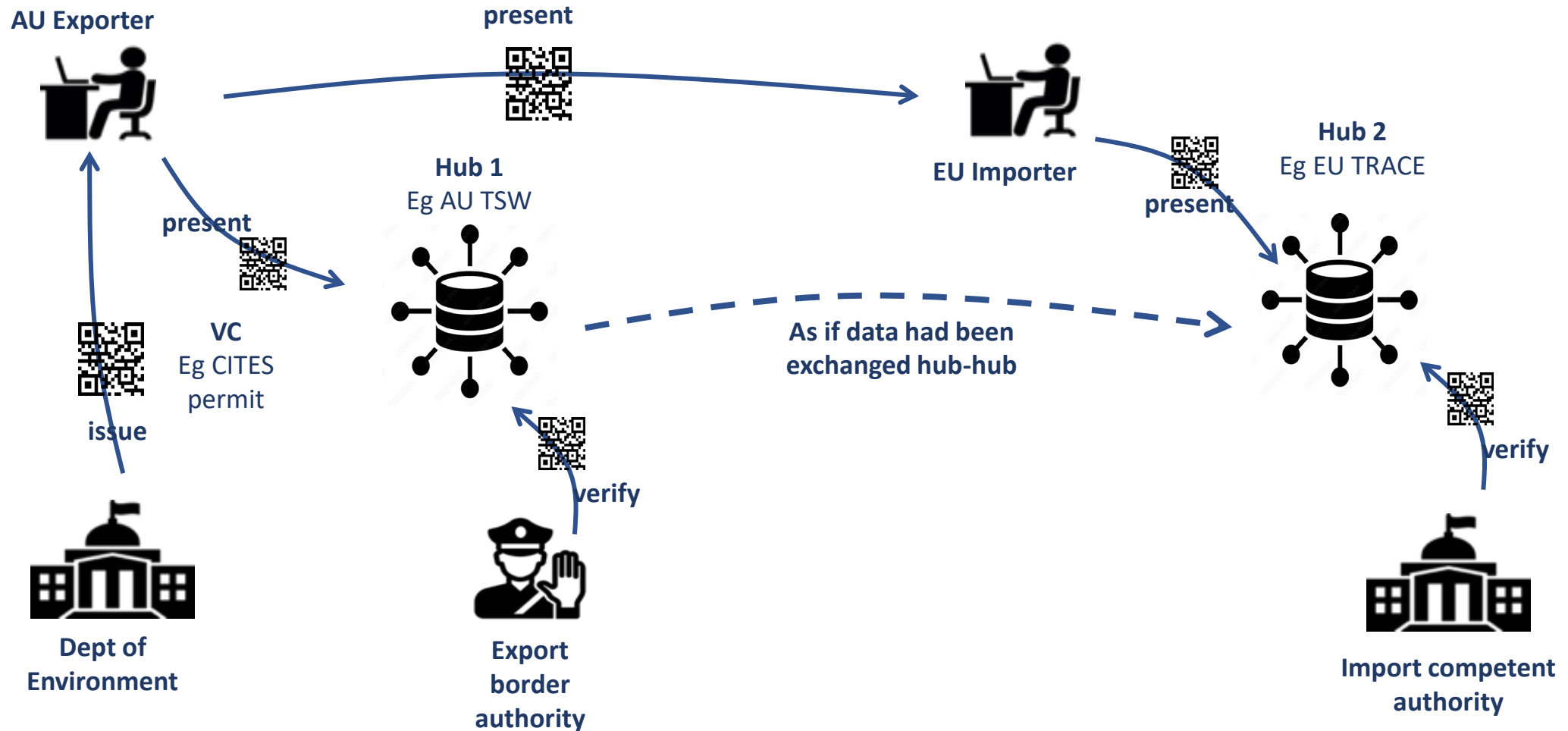
In summary – it's the best way forward

Verifiable Credentials for global electronic trade

✔ Scalability – Go 100% digital without dependencies

✔ Cost – No central infrastructure and free software

✔ Privacy – No honeypot cyber-threat

✔ Integrity – cryptographically verifiable trust

Thanks

Please feel free to contact me at Steve.capell@gmail.com

Now let's do a walk-through of the white-paper.

https://unece.org/sites/default/files/2022-09/WhitePaper_VerifiableCredentials-CBT.pdf