European Commission | ebsi

What to do when *good* credentials go *bad?*

Unlocking the Challenge of Verifiable Credentials Revocation – A new study by EBSI

Alen Horvat – Lead architect at EBSI
European Commission, Directorate-General for Informatics

Blockchain is one of the technologies that will pave the way to Europe's Digital Decade

ebsi
European Blockchain

European
Blockchain
Services
Infrastructure

Accreditation management

Verification of Authentic documents

Anti-counterfeiting

IP Rights Management

European Commission

Verification matters

European Commission

Verification
is the antidote for fake

European Commission

When someone claims something, we want to verify it

Claim

I studied economics

That's my boss.

True or **False**?

When someone claims something, you want to verify it

Not all proofs have the same value

Claim

I studied economics

You can Google me

I can send you the **PDF**

I can show you the paper document

You can contact my university

Trust

high

low

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

Diploma

PDF

Time

minutes

hours

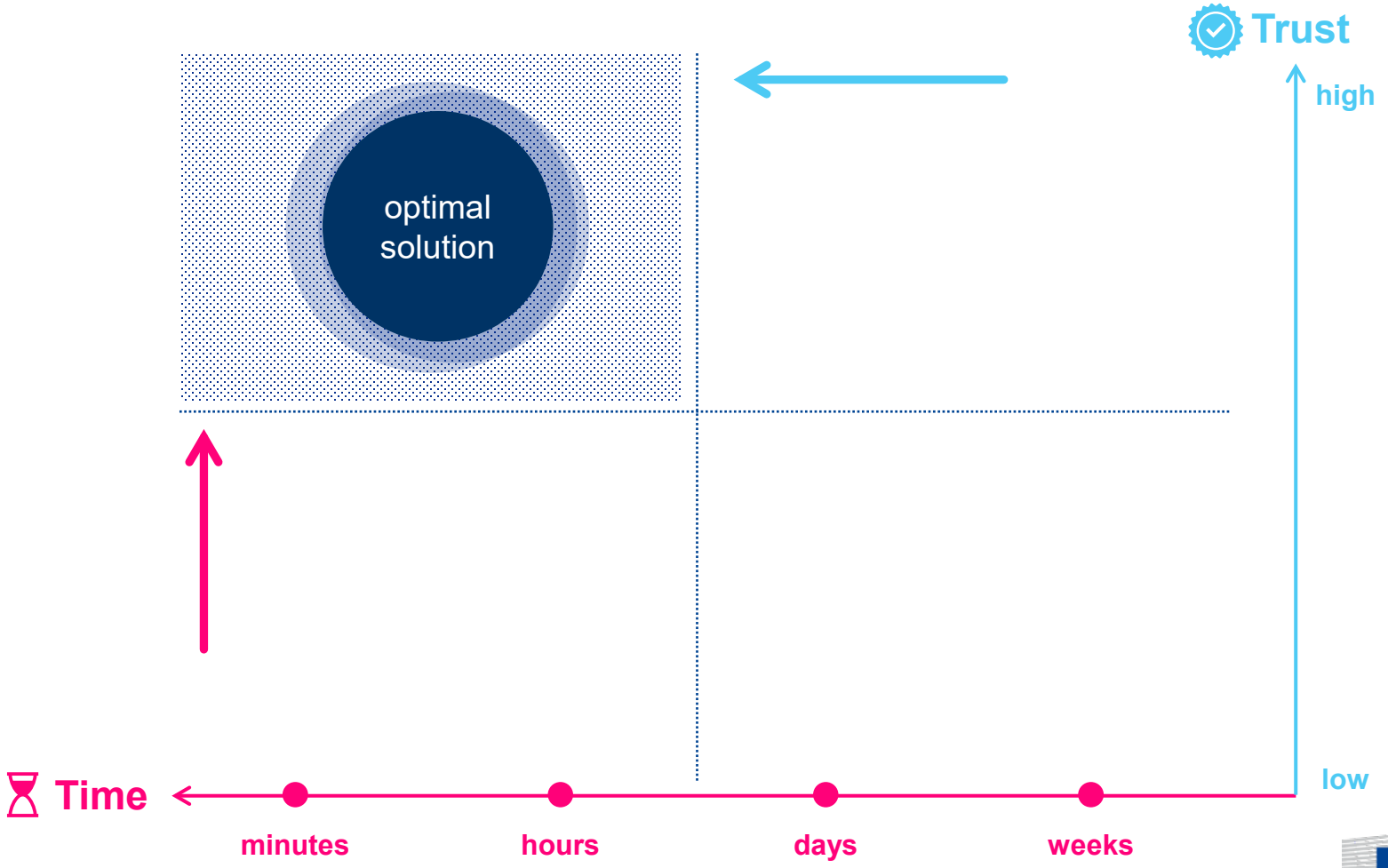
days

weeks

European Commission

When someone claims something, we want to Verify it

Not all proofs have the same value

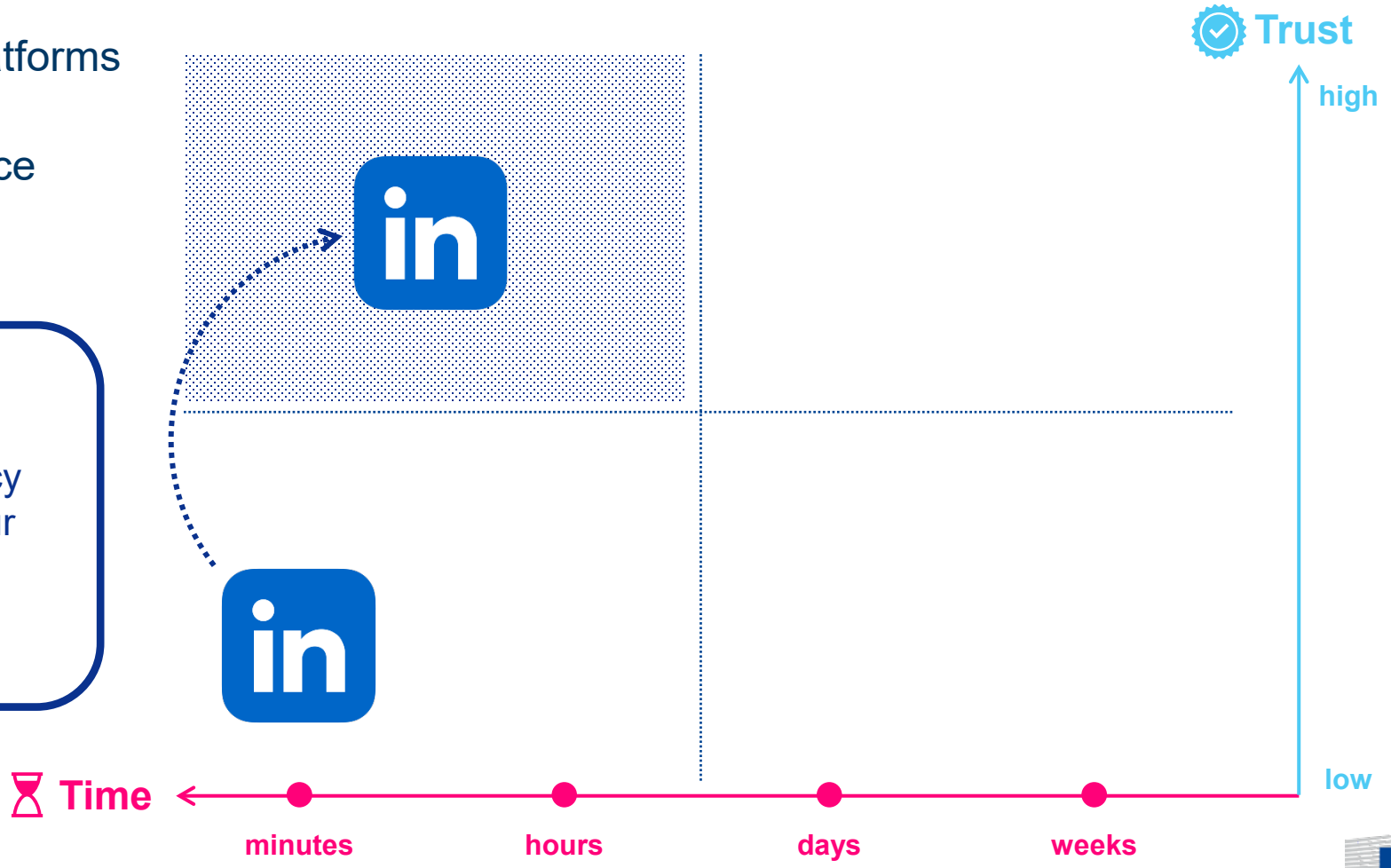


European Commission

Technology can help cut verification time

For example, platforms could provide a verification service

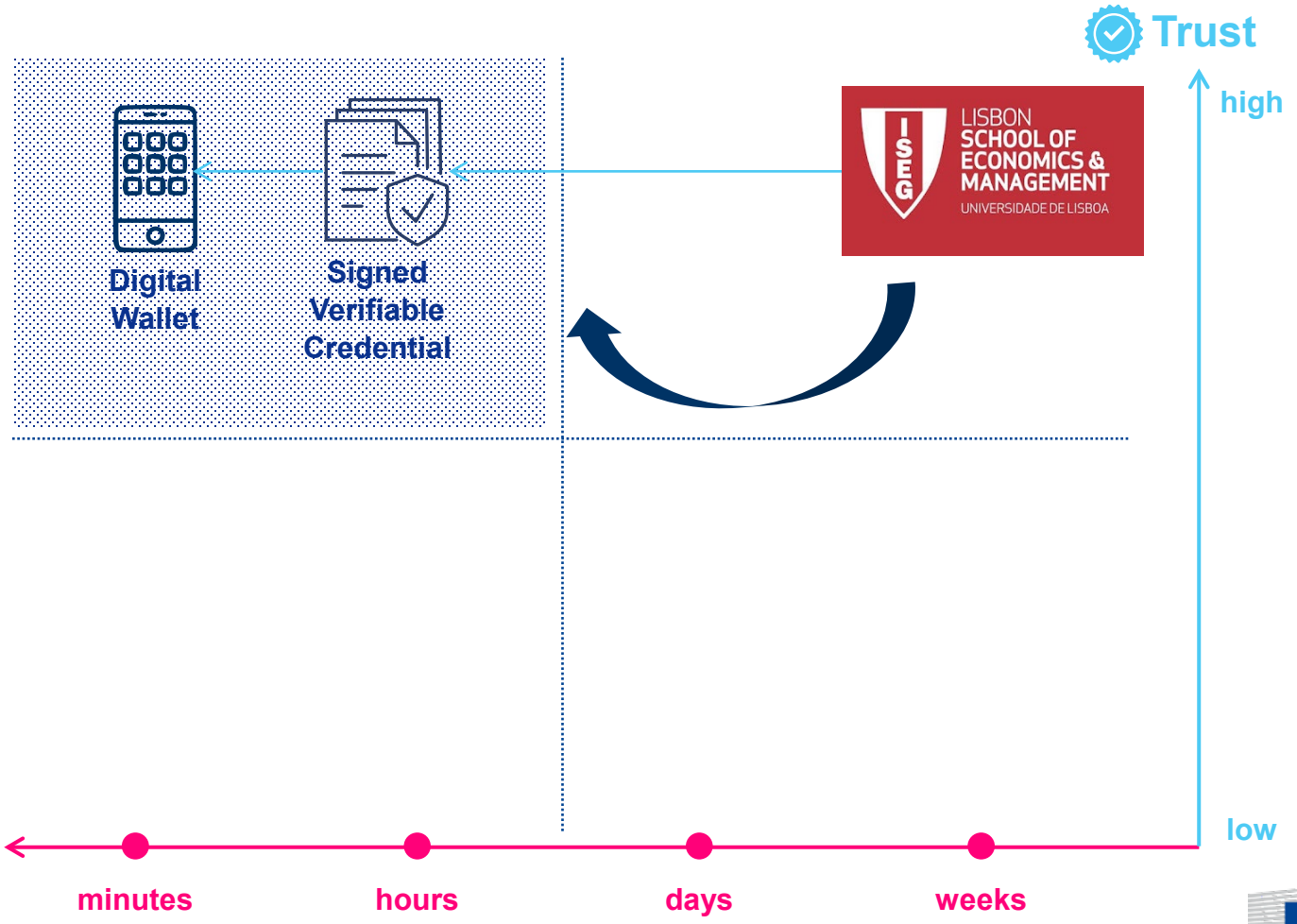
However this would create a dependency on platforms and our data would be controlled by them



European Commission

Today, we can do this without giving our data to a platform

We can use Web3 technologies such as Digital Wallets, Verifiable Credentials and Blockchain to achieve the same



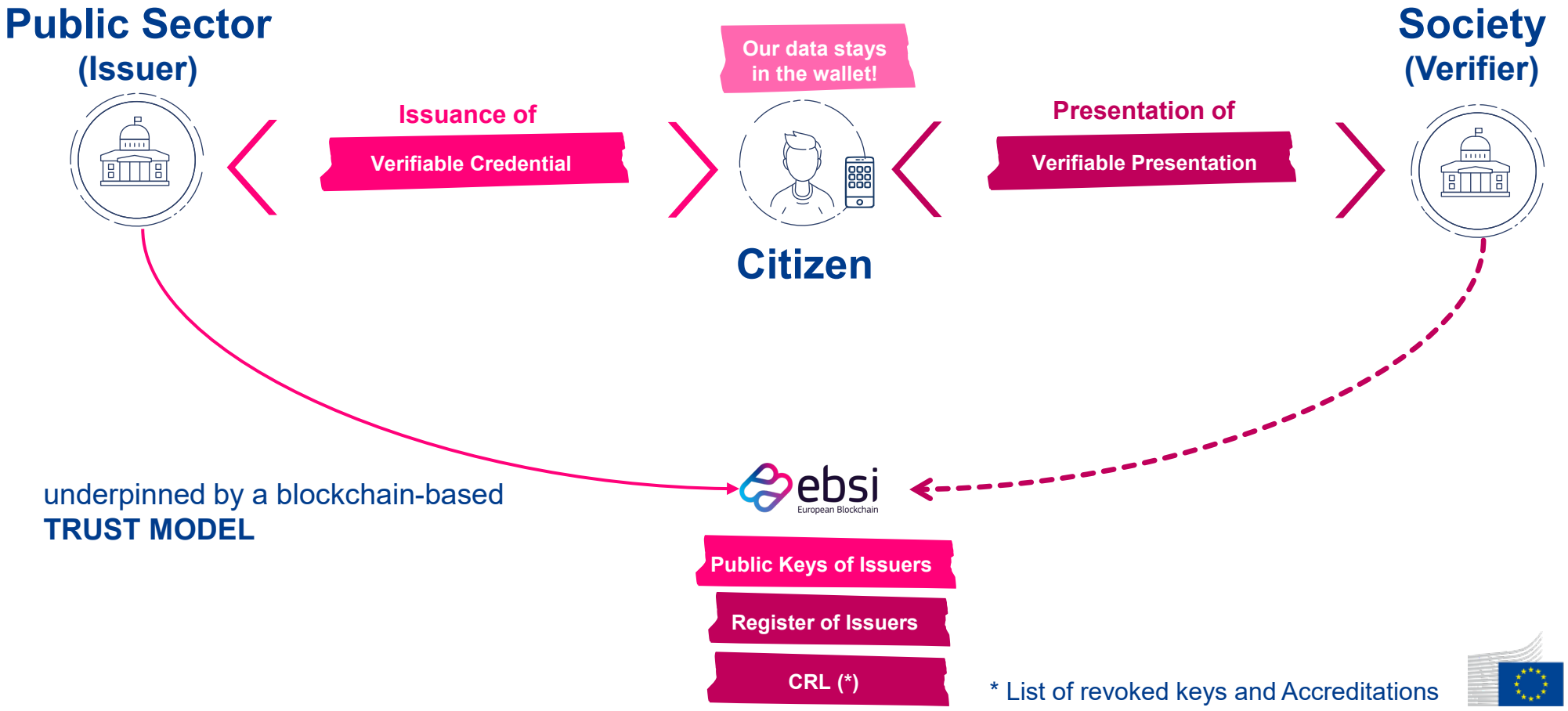
ebsi
European Blockchain

Trusted list of Issuers used to distribute public keys and accreditation info

European Commission

Blockchain is used as a trusted list of Issuers

Verifiable Credentials enable a **G2C information sharing model**



* List of revoked keys and Accreditations

European Commission

When someone claims something, we want to verify it

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

Claim

I studied economics

What if they'd like to take it back ?

European Commission

Revocation in Web3 is hard

01

Contacting the issuer defeats the purpose

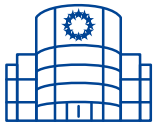
Storing credentials on digital wallets **breaks the connection between Issuer and Verifier by design.** If you contact the issuer to check the status of the credential, not only can the issuer track you (« phone home »), but crucially, **it defeats the point.**

02

Putting revocation information in a “third place” creates new problem

Verifiers could in theory contact a “third place” for revocation information. But this begs new questions: who manages the revocation information? What is publicly available? Who can access it?

Our revocation criteria



Adheres to the GDPR.

Prevents holder traceability.

Respects the privacy of holders.

Does not store or process personal data on the EBSI blockchain.

Prevents issuers or 3rd parties linking revocation checks with the holders.

What types of credentials are we trying to revoke?

In EBSI, there are different types of “claims” (or “attestations”) that need to be revoked, be it for natural persons or legal entities

LEGAL ENTITIES

Verifiable Authorisation

- give **Legal Entity** access to the infrastructure
- give **Legal Entity** authorisation to start a trust chain

Verifiable Accreditation

Legal entity accreditation, describing **rules & boundaries for legitimate VC issuance**

PERSONS

Verifiable Attestation

Statements or claims about holders – Natural Persons

Questions to ask as *Business Owner*?

When your use case requires revocation of credentials

01

What is the level of privacy preservation that is needed?

Assess whether user tracking is permissible with the use case. For example, legal entities like public organisations may not require privacy-preserving approaches. However, natural persons, such as individuals or private entities, must have their privacy protected in compliance with privacy regulations.

02

Should I restrict the access of a credential to a specified time window?

Determine if it's necessary to restrict the access of a credential to a specified time window. This may be important in cases where there is a high level of assurance (LoA), which means there is a high level of certainty of a service provider that a claim from an individual is authentic, such as with medical records. A limited time window can help protect sensitive information and minimise potential misuse of outdated or revoked credentials.

03

Is there a necessity of tracking the validity of the signature?

Evaluate whether monitoring the validity of signatures within the use case is essential. In some instances, tracking signature validity might be critical for maintaining the integrity and authenticity of credentials. Ensuring the validity of signatures can help prevent fraud and unauthorised access to sensitive information.

Questions to ask yourself as an *architect?*

When designing a revocation solution

01

What is the revocation method?

- Holder privacy
- Time-visibility
- Ease of implementation

02

What is important about the data format?

- Interoperability
- Domain-specificity

03

What is the Retrieval method & hosting?

- Traceability
- Availability

EBSI defined three revocation method families

In a privacy-by-design service, different approaches are possible in EBSI when the Issuer is managing the Verifiable Credential status

Binary valid/invalid status

It is a simple yes/no format without additional metadata. Privacy by design principles.

Properties
- herd privacy
- small in size

Limitations
- No additional metadata (date, reason) is provided, which could be needed for certain domains
- State changes can be tracked

Status with VA metadata

It contains VC status with additional metadata, such as reason, date, and other.

Properties
- herd privacy
- per-VC metadata

Limitations
- State changes can be tracked

Status with VA metadata and limited visibility

It contains VC status with additional metadata, such as reason, date, and other.

Properties
- herd privacy
- per-VC metadata
- State changes cannot be tracked

Limitations
- None identified so far

Retrieval methods

Five retrieval methods are possible

VC Status Strategy	Description	Legal Entity	Natural Person	Information revealed
Short VC lifetime*	Issuer issues VCs with a short lifetime, e.g., hours, days. Two strategies are possible: a) Re-issuance of the original VC with new duration b) Issuance of an additional one-time status VC	✓	✓	The Issuer learns what VC is presented and when by a holder. It doesn't learn about the Verifier.
VC Status managed in a Trusted Registry	When a reliable history of the VC status is required, the information can be stored in the corresponding Trusted Registry. Applicable only to Legal Entities.	✓	X	No information is revealed to the Issuer.
VC Status managed by the Issuer - direct retrieval*	The Trusted Issuer hosts VC status information, and verifiers retrieve the VC directly from the Trusted Issuer.	✓	✓	The Issuer learns which Verifier and when one of the VCs is received in the revocation or suspension list.
VC Status managed by the Issuer - retrieval via the Holder	The Trusted Issuer hosts VC status information; however, Holder fetches and presents the revocation/suspension information.	✓	✓	The Issuer learns what VC is presented and when by a holder. It doesn't learn about the Verifier.
VC Status managed by the Issuer - retrieval via EBSI	The Trusted Issuer hosts VC status information; however, the verifiers retrieve the information via EBSI node. This way, issuers never learn who asked for the VC status information.	✓	✓	No information is revealed to the Issuer.

Today's landscape

What are the criteria we use for the analysis?

Criteria

Privacy

- The status record must not serve as globally unique identifier or correlator of the natural person
- Access to the status record alone must not reveal any information about the natural person
- Access to the status record must not allow the issuer or anyone else to track the natural person's use of the VC

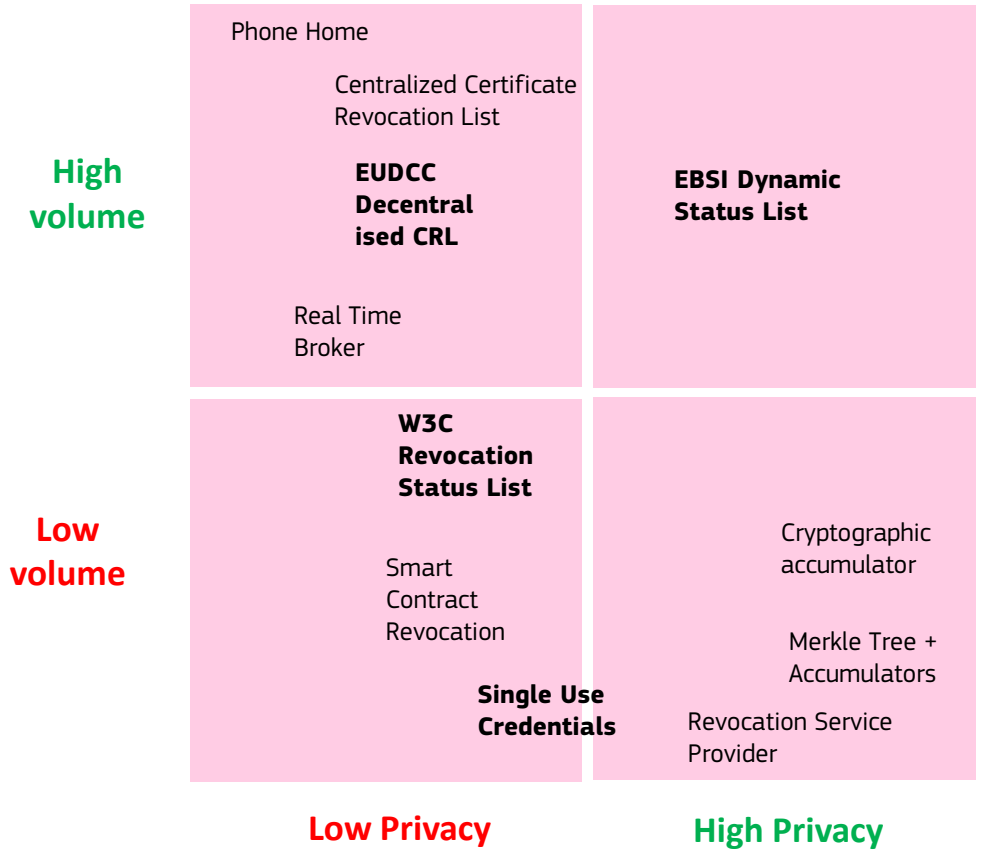
Erasure & Control

- The natural person must be able to view and request erasure of their own status
- The issuer must be able to modify or delete the status record (and thereby revoke the credential)
- In some jurisdictions, a third party (such as a court of law) must also be able to modify or delete a status record

Scalability

- The solution must be proven to scale to hundreds of millions of status records
- Holder and Verifier can be both online

Today's landscape



Revocation/Suspension formats marked with bold are supported/acknowledge today

How have you approached revocation in your projects?
Come find me at the networking drink.

There’s more !

Check out the entire paper and our revocation specs on EBSI’s website: *ebsi.eu*.

Whitepaper (pdf)

Revocation specs