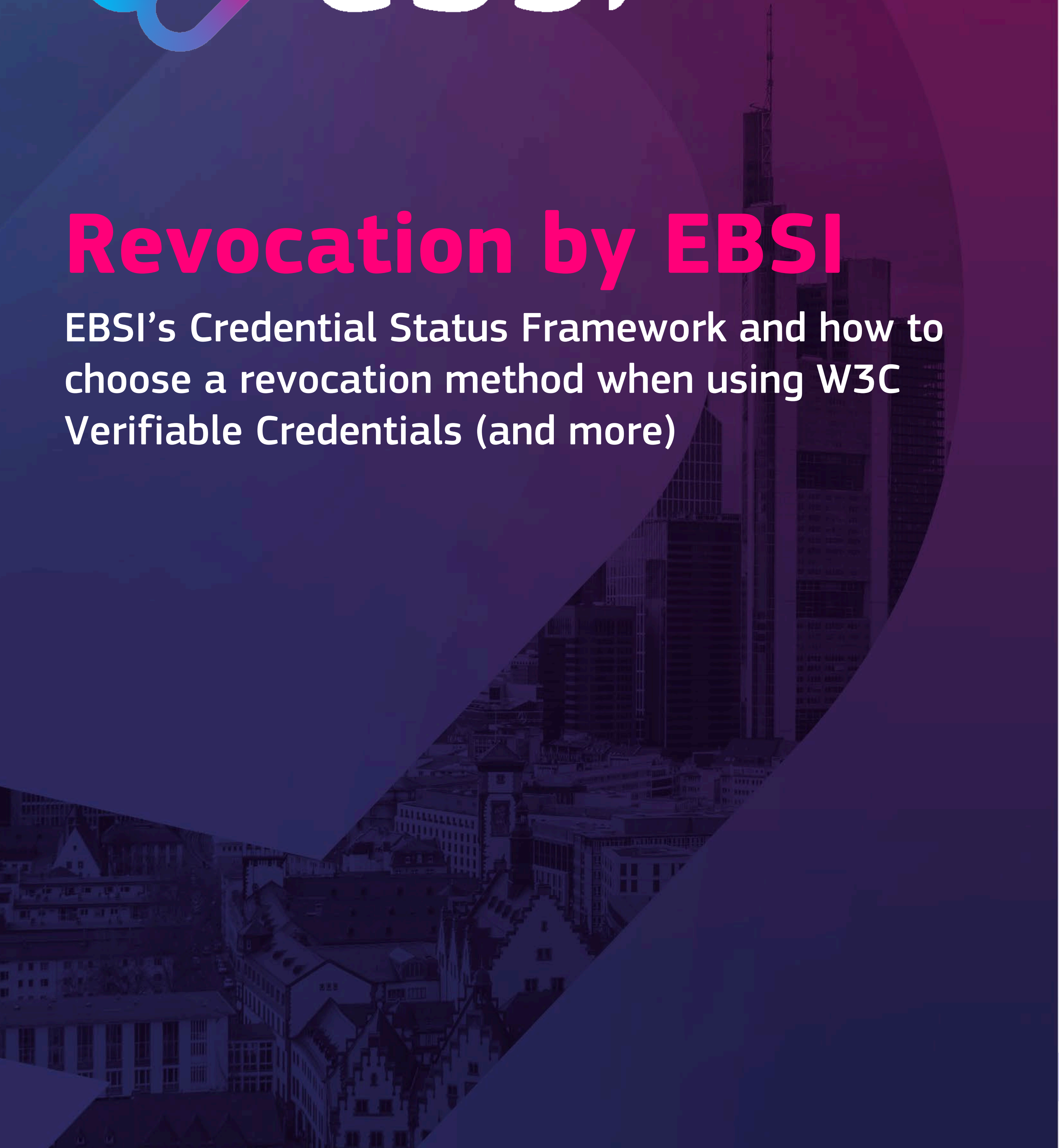
ebsi

Revocation by EBSI

EBSI's Credential Status Framework and how to choose a revocation method when using W3C Verifiable Credentials (and more)



Document History

Table 1: Document Approver(s):

Name	Role
Joao Rodrigues Frade	European Commission – Head of Sector DG DIGIT B3.002

Table 2: Document Reviewer(s):

Name	Role
Alen Horvat	Lead Architect for Verifiable Credentials – EBSI – European Commission (DG DIGIT)

Table 3: Summary of Changes

Version	Date	Created by	Short Description of Changes
V1.0	06/10/2023	European Commission - EBSI	First version

Executive Summary

EBSI's Verifiable Credential Status Framework

EBSI recognises the need for a versatile revocation framework that caters to diverse business scenarios while adhering to privacy compliance regulations. Example business scenarios include revoking credentials issued to legal entities and natural persons, managing access rights, and handling work contracts.

This white paper introduces EBSI's Verifiable Credential Status Framework, which enables the management and expression of a Verifiable Credential's (VC) status, which can be valid, suspended or revoked. The Issuer of the VC is responsible for storing and keeping this status information up to date. The proposed framework offers various strategies configured for different types of VCs, allowing use cases to select the approach that best meets their specific business requirements.

The revocation of VCs issued to legal entities, including Verifiable Authorisations, Verifiable Accreditations, and Verifiable Attestations, is not subject to the General Data Protection Regulation (GDPR). As such, the status of Legal Entity VCs can be managed either in the Trusted Issuers Registry on EBSI's ledger or externally. Two strategies are proposed for Verifiable Accreditation management: storing the status information in the EBSI Trusted Issuers Registry or hosting the information by the Issuer and obtaining it via the registry. Data structures for Verifiable Accreditation management include W3C Status List, Certificate Revocation List (CRL), and others.

For VCs issued to natural persons, the status information for Verifiable Attestations must be managed per the GDPR. Furthermore, Natural Person VC status information must be hosted and managed by the Issuer of the Verifiable Attestation, and no personal information is stored on EBSI. The modular design of the VC status framework enables use cases to meet their business, privacy, and security requirements by choosing from different strategies for either short-lived or long-lived VCs. Short-lived VCs involve the holder obtaining a fresh VC each time it is needed. In contrast, long-lived VCs may involve obtaining status information directly from the Trusted Issuer, through the EBSI network, or from the Issuer or a third party as a separate status VC.

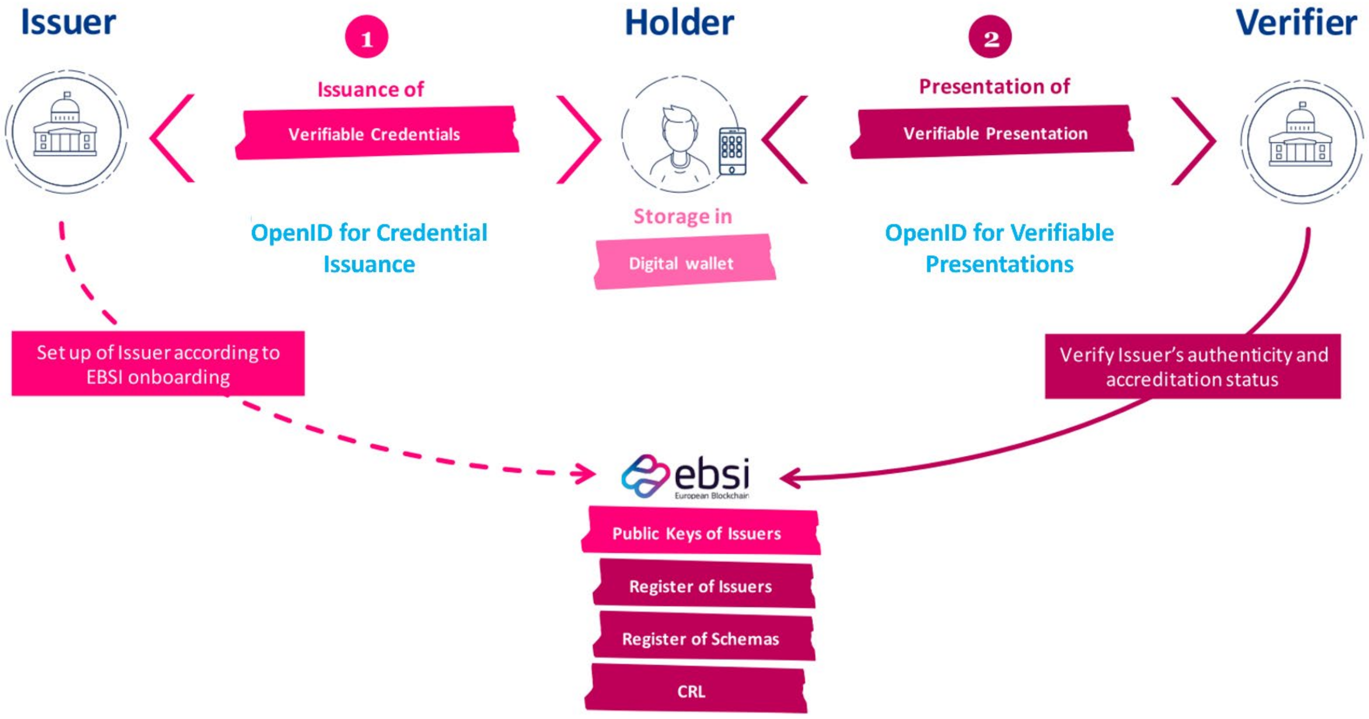
Each strategy has advantages and limitations regarding privacy, connectivity, and up-to-date information. Overall, EBSI aims to provide a modular and adaptable framework that caters to the ever-changing needs of citizens, businesses, and public organisations, striking a balance between privacy, security, and functionality.

Table of Contents

Introduction

Revocation in Verifiable Credentials: Why it Matters

Verifiable Credentials (VCs) are at the core of the European Blockchain Services Infrastructure (EBSI), which offers a secure, tamper-proof, and decentralised system for issuing, storing, and verifying credentials. EBSI's Verifiable Credentials framework provides public sector entities with a self-sovereign information sharing framework that enables the Holders of credentials to have complete control over how, when, and to whom their personal information is shared and verified, facilitated by an EBSI conformant wallet. By leveraging blockchain ledger technology, EBSI ensures that anyone can verify the authenticity of credentials in a trustworthy, easy and reliable manner using EBSI's decentralised trusted registry. The Diploma Use Case demonstrates the core value of VCs, as it streamlines the process of applying to new jobs and educational programmes, increasing cross-border mobility for students and workers throughout Europe. This is one of many examples of how EBSI's sovereign network simplifies the lives of EU citizens by supporting easy verification and offering trusted access to decentralised services.



Pictured: EBSI's trust framework for citizen-to-business (C2B) and citizen-to-government (C2G) information exchanges

As the Diploma Use Case highlights, VCs have the potential to revolutionise the mobility of European citizens and empower individuals with control of their personal information. However, what would happen if a student was found guilty of fraud or any other form of academic misconduct resulting in the revocation of their degree? How can a recruiter or university administrator verify whether the presented diploma is still valid? Verifiers, such as public administrations and businesses, must be able to verify the status and validity of VCs to maintain trust between the Issuer, holder, and verifying organisation. The absence of such a framework could increase the risk of fraudulent activity, eroding the trust and credibility of the entire VC ecosystem. This is where revocation and suspension come into play.

Revocation and suspension measures exist to ensure that the credential holder continues to meet specific criteria, such as possessing certain skills or completing an academic programme. By revoking or suspending a credential, issuers retain control over the credentials they issue, and the holder is held accountable for their actions—or lack thereof in the case of a holder's failure to renew a credential before its expiration.

The revocation and suspension framework must include the following parameters for VCs:

- The **validity** of a VC is determined by three elements: the VC's inherent properties, such as a **validity date** (the date at and after which the VC becomes valid), the authenticity of the public keys used to sign or seal the VC along with their supporting attestations, and the **status** of the VC itself.
- The **status** of a VC indicates its current state, which can be **valid** (active and acceptable for authentication), **revoked** (withdrawn or cancelled permanently), or **suspended** (temporarily disabled but may be reinstated later).
- A VC can also be cancelled after its **expiration** if an expiry date has been assigned. This is often the case for VCs with a short lifetime.

Revocation and suspension follow the same implementation process, with the only difference being that suspension is temporary and reversible, whereas revocation is permanent and non-reversible. In this document, the term "revocation" will be used interchangeably to refer to both revocation and suspension.

Navigating Constraints: Ledgers, Immutability, and Privacy

When implementing revocation procedures, it is also important to be mindful of the challenges that arise when using an immutable or non-changeable, distributed ledger to store credential information. The EBSI ledger is a decentralised database of information that contains a continuously growing list of records, called blocks, which are synchronised within a network of nodes across Europe. When a trusted issuing organisation issues a VC, information about the Issuer and data that connects the Issuer to the issued credential are stored on the immutable ledger. Since this data cannot be easily altered or deleted, the VC itself will remain valid until it expires. If mistake was found, access has been compromised, or issuer had to revoke the credential for other reasons, without a revocation mechanism in place, the holder could continue to use a VC for authentication purposes. As a result, both Legal Entities and Natural Persons face several issues when verifying, changing and proving the validity of VCs issued, held, or presented to other entities.

Challenges for Legal Entities

Availability

Availability is a crucial aspect of revocation, as legal entities need access to timely and accurate information about the status of VCs. Issues can arise when students attempt to access their academic records or diplomas from institutions in another EU country. For instance, if a French student studies in Italy and later applies for a job in the Netherlands, the prospective employer might need to verify the student's Italian diploma or transcripts. The technical burden falls on the Italian university to create and maintain APIs available to verifying organisations and ensure that connectivity is available around the clock.

Operational Burden

Another key challenge Legal Entities face is the operational burden of verifying VCs' revocation status. In the classical trust model for issuers, the verifying organisation must create and maintain applications capable of sending requests to the APIs hosted by the issuing organisation. As the number of credential issuing organisations grows and digital identity requirements become more complex, this can become increasingly time-consuming and costly. Moreover, the need for cross-border interoperability adds another layer of complexity, as Legal Entities may need to manage and verify credentials issued by different authorities in different jurisdictions.

Reliability

Reliability is another critical concern in the context of revocation, as verifiers need to be able to access historical information about the validity of a Legal Entity's credentials in a dependable manner. Similar to the example above with the French student, the Dutch company may need to confirm that the Italian diploma credential and e-sealing keys were valid when the student received them.

Challenges for Natural Persons

The "Phone Home" Problem

Imagine you are a recent graduate applying for a new job at a company. As part of the application process, you must present your university diploma to prove your academic qualifications. To verify the authenticity of your diploma, the prospective employer contacts your university's central administration office to check if your diploma is valid and hasn't been revoked. While this process may seem straightforward, there is no guarantee that someone will always be available to provide this information. It could also prove difficult for the university to identify who is requesting the information and whether the Verifier in question has received the graduate's consent to access the information.

It is also important to consider the privacy of the graduate. When the central administration office receives the request to verify your diploma, they can easily infer that you are applying for a job at a particular company. If they wanted to, they could even monitor your career progress and job applications by tracking these verification requests each time an employer "phones" the university to confirm your diploma's validity.

The Tracking Beacon Problem

Another verification method involves assigning a unique identifier, such as a five-digit number. For instance, a university issues a diploma VC with the identifier "12345" printed on it. This identifier is then used to verify that your diploma is authentic and has not been tampered with. However, if your diploma gets revoked, let's say for academic misconduct, the number code is added to a publicly available list of revoked diplomas.

The problem with this is that the number code on your diploma becomes a tracking beacon. Every time you use your diploma to apply for a job or enrol in a course, the Verifier will see the same number code. This means that anyone can check the status of the diploma at any time and follow any status changes, allowing colluding organisations to build a detailed picture of your online activity. They can see what jobs you have applied for, the courses you have taken, and so on, without your knowledge or consent.

The Tracking Changes Problem

Imagine you share your Student ID with a restaurant to get student meal discount. Once you leave the restaurant the owner should no longer be able to check the validity of your student ID. The problem with most revocation approaches is that once the identifier that resolves the revocation/suspension information is known to the verifier, it can be used to monitor and track the state changes. This way the restaurant can, at any time, check the validity of the Student ID, even after you have left.

EBSI's Use Cases — Requirements for Revocation

The "phone home" and tracking beacon problems raise privacy concerns, as verifiers can potentially access personal information, which can then be used to monitor and track the holder's actions. While this does not impact public entities whose information is publicly available on EBSI's ledger, compliance with privacy regulations like the General Data Protection Regulation (GDPR) necessitates a revocation approach that preserves privacy and prevents user trackability of students, employees, and other natural persons relevant to EBSI's various use case scenarios.

To achieve these goals, EBSI's use cases define the following essential **business requirements** for the revocation framework:

- Ensure compliance with GDPR;
- Eliminate the traceability of holders;
- Protect holder privacy;
- Refrain from storing or processing personal data on the EBSI blockchain;
- Prevent issuers or third parties from linking revocation checks to holders.

Moreover, EBSI's revocation framework must also accommodate the following three types of services:

1. Revocation services associated with Issuers of VCs;
2. Revocation services associated with Holders of VCs;
3. Revocation services associated with VCs themselves.

By ensuring privacy and regulatory compliance, EBSI aims to foster a revocation framework that protects the rights and interests of all participants in the credential ecosystem while also ensuring that the framework supports various revocation service types. Implementing a revocation framework that meets the above requirements will enhance trust and security and contribute to developing a more transparent and accountable digital landscape for students, employees, and other types of natural persons.

Identifying Use-Case Specific Requirements

Owners of individual use cases should carefully analyse various revocation strategies to determine their appropriateness for their specific use case, considering the trade-offs involved. To identify use-case specific requirements, consider the following three criteria:

1. **Level of privacy preservation 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.
2. **Use case 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.
3. **Necessity of tracking signature validity:** 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.

The complexity of revocation for verifiable credentials means there is no one-size-fits-all solution applicable to all use cases. However, by examining these criteria, use case owners can make more informed decisions about the revocation strategies that best meet their requirements, balancing the need for security, privacy, and functionality.

The Current Revocation Landscape

Revocation Landscape

EBSI conducted a study on existing revocation methods to gather insight into how well each solution addresses the problems of tracking and traceability while also meeting EBSI's revocation objectives. The case study identified eleven mechanisms in the current landscape and tested each revocation mechanism against three umbrella criteria: privacy, erasure and control, and scalability.

Privacy

To address the "Phone Home" and Tracking Beacon problems, revocation status records shared with third parties must not be unique identifiers for individuals. Such identifiers could lead to the correlation of user activities by commercial entities or hostile actors. Thus, it is crucial that use cases select a revocation mechanism that safeguards personal information when dealing with status records that belong to Natural Persons.

Erasure & Control

Under the GDPR, individuals must be able to view and request the erasure of their status records. However, revocation information may be exempt from these regulations. To maintain compliance, the Issuer should control the credential status, allowing them to modify or delete it. This control criteria also demonstrates how credential holders can manage the sharing of their status information, balancing GDPR compliance and revocation requirements.

Scalability

While there are sophisticated and highly technical mechanisms that satisfy the above privacy, erasure and control capabilities, they are often not yet proven at scale. In addition to striking a balance between privacy and scalability, the price of the solution must also be considered to ensure the chosen revocation mechanism is economically feasible.

The findings of EBSIs comprehensive study of the current revocation landscape (summarised in Table 1 below) underscores the importance of finding a delicate balance among these criteria while acknowledging the absence of a one-size-fits-all solution. To build a robust and secure infrastructure, use cases must carefully weigh the strengths and weaknesses of each revocation method, taking into account their specific use cases and requirements. By prioritising user privacy, enabling GDPR compliance through erasure and control, and ensuring technical and economic scalability, use cases can foster trust and accountability in an increasingly digital world, safeguarding the interests of both natural persons and businesses.

Table 1: Summary of Existing Revocation Approaches

		Privacy			Erasure & Control			Scalability	
	Case Study	The status record must not serve as a 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.	The natural person must be able to view and request erasure of their own status record.	The Issuer must be able to modify or delete the status record (and hereby revoke the credential).	In some jurisdictions, a third party (such as a court of law) must also be able to modify or delete the status record.[1]	The solution must be proven to scale to hundreds of millions of status records.	Holder and Verifier can both be offline.
Central credential serial number registry	NHS		✓		✓	✓	✓	✓	✓
Phone Home					✓	✓	✓	✓	
Revocation Status List			✓	✓	✓	✓	✓	✓	✓
Decentralised Certificate Revocation List	EU Digital Covid Certificate		✓	✓	✓	✓	✓	✓	✓
Smart contract based revocation	AGID Italy		✓	✓	✓	✓	✓		
Single use credentials		✓	✓		✓		✓		
Real-time Broker	Verified.Me Canada				✓	✓	✓	✓	
Zero Knowledge Broker (aka Revocation Service Provider)		✓	✓	✓	✓	✓	✓	*	
Cryptographic Accumulator (Indy AnonCreds)	German LISSI Wallet	✓	✓	✓	✓	✓	✓		
Merkle Trees and Accumulator (Indy Merkle Trees)		✓	✓	✓	✓	✓	✓		
Dynamic Status List	EBSI	✓	✓	✓	✓	✓	✓	✓	✓

[1] The ability for a natural person to view and request erasure is largely implementation specific e.g. a wallet app may retrieve the user's revocation status for each of their credentials and display it for the user. The wallet functionality may also provide the ability for the holder to request erasure of their status record.

A Modular Approach: Revocation Solutions for Diverse Use Cases

EBSI recognises the need for a versatile and adaptable revocation framework that caters to various business scenarios while adhering to privacy compliance requirements and criteria. This framework must also accommodate diverse business scenarios involving revocation services of Issuers and Holders of VCs and revocation services connected to the VCs themselves.

Example business scenarios to consider include:

1. **Revoking credentials issued to Legal Entities or Natural Persons:** A university issues verifiable diplomas to its students (natural persons) and accreditations to its academic departments (legal entities). Suppose a student's diploma needs to be revoked due to discovered academic misconduct or an academic department undergoing organisational changes that alter its jurisdiction. In that case, EBSI's revocation framework should enable the university to revoke the respective credentials.
2. **Access rights management:** An employee is granted access to a company's confidential documents through a VC. When the employee is promoted or changes roles within the company, EBSI's framework should allow access rights adjustment, either granting additional permissions or revoking previous ones based on the employee's new position.
3. **Work contracts based on credentials:** A software engineer has a verifiable credential that confirms their computer science degree. When a tech company hires them, it issues a verifiable work contract credential based on the engineer's diploma. EBSI's framework should support issuing and managing such work contract credentials, making it easier for the company and the employee to handle employment documentation, including revoking a permanent work contract when the employee leaves the company.

EBSI's revocation framework aims to meet privacy compliance objectives while providing the flexibility to address various business scenarios. By expanding its application to a wide range of business scenarios, EBSI demonstrates its commitment to creating a robust and adaptable framework that caters to the dynamic needs of citizens, businesses, and public organisations, striking a balance between privacy, security, and functionality.

EBSI's Revocation Methods

Expressing Status as a Verifiable Credential

When the Issuer issues a new VC, they also share the VC's **status information.** The status information —stating whether a VC is valid, suspended, or revoked—is shared with the VC when it is issued to a Holder or presented to a verifying organisation. This status information is connected to another type of VC called a **Credential Status VC**. Think of this as a digital "report card" that tells you whether the VC in question is valid. The Issuer of the VC is responsible for storing and keeping this report card up to date. EBSI's decentralised network plays the role of a proxy between the person or organisation checking the status of a VC (the Verifier) and the Issuer responsible for hosting the Credential Status VC. Contact points of the issuing organisation possessing the VC status information are publicly available through EBSI's Trusted Issuers Registry.

Revocation of VCs Issued to Legal Entities (Non-GDPR)

A legal entity is an organisation with a distinct legal existence, separate from its individual members or owners. In the EBSI VC ecosystem, legal entities typically include government agencies and educational institutions responsible for administering credentials to VCs. Before they have the right to issue VCs, they must request authorisation from EBSI or receive accreditation from a Trusted Accreditation Organisation (TAO). Both processes require the issuance of VCs to legal entities.

VCs issued to legal entities can belong to three types:

1. **Verifiable Authorisation:** A VC issued to a legal entity during the onboarding process that provides access to EBSI's infrastructure and initiates the trust chain.
2. **Verifiable Accreditation:** A VC that asserts which types of VCs a Trusted Issuer can issue and under which policies.
3. **Verifiable Attestation:** A VC that asserts statements or claims about the legal entity possessing the VC.

A legal entity's VC may need to change its status from valid to either revoked, suspended, or expired. Such changes can occur due to organisational restructuring in which a government agency undergoes a merger or split, resulting in the need to update their VCs.

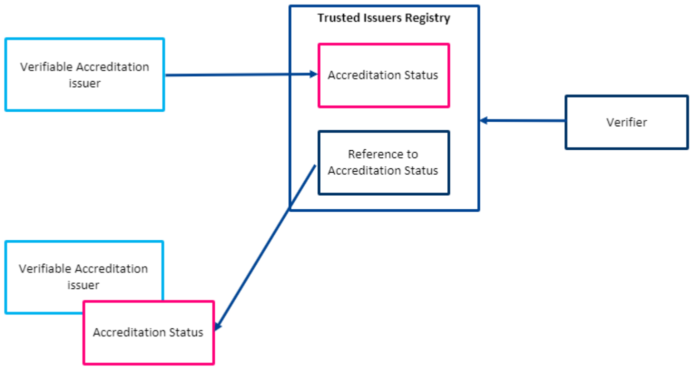
Example scenarios may include:

- **Organisational restructuring:** A government agency may undergo a merger or split, requiring it to update its VCs. For instance, if two educational institutions merge into one, the new entity may require updated Verifiable Authorisations or Accreditations to reflect the change in its structure and scope of credential issuing services.
- **Policy updates:** Changes in regulations or industry standards may require the alteration of existing VCs. For example, if new amendments are added to the GDPR, a legal entity responsible for managing personal data may need to update its Verifiable Attestation to comply with the new requirements.
- **Termination of a legal entity's operations:** When a legal entity ceases its operations, its VCs may expire or require revocation. Suppose a professional certification body goes out of business. Its Verifiable Accreditations may need to be revoked to prevent it from issuing new certifications and ensure the VC ecosystem remains accurate and up to date.

In each of these situations, it is important to maintain the integrity of the EBSI VC ecosystem and trust chain by supporting the management of legal entity VC status information. Since legal entities are often public organisations, their information can be made publicly available, and their VCs are not subject to the GDPR. Consequently, the status of a legal entity's VC can be managed in the Trusted Issuers Registry on EBSI's ledger.

Verifiable Accreditation Management Strategies

Accreditation status information is essential for verifying that a legal entity meets the necessary criteria to issue verifiable credentials. Depending on use case specific requirements, EBSI proposes two strategies enabling Verifiable Accreditation Issuers to store and manage accreditation status information of the credentials they issue.


Trusted Issuers Registry
Verifiable Accreditation issuer
Accreditation Status
Verifier
Reference to Accreditation Status
Verifiable Accreditation issuer
Accreditation Status

Strategy A
The Verifiable Accreditation status information is **stored in the EBSI Trusted Issuers Registry**

Strategy B
The Verifiable Accreditation status information is **hosted by the Issuer and obtained via the EBSI Trusted Issuers Registry**

Strategy A: The Verifiable Accreditation status information is stored in the EBSI Trusted Issuers Registry

The EBSI Trusted Issuers Registry uses distributed ledger technology that allows for the secure storage and management of accreditation status information. The verifying organisation retrieves the accreditation status information directly from the Trusted Issuers Registry, which serves as a proxy between the Issuer and Verifier. This strategy also eliminates the burden of storing the accreditation status information from the Issuer.

Strategy B: The Verifiable Accreditation status information is hosted by the Issuer and obtained via the EBSI Trusted Issuers Registry

In this strategy, the Issuer of the Verifiable Accreditation is responsible for hosting the accreditation status information and making this information available through the EBSI Trusted Issuers Registry. This approach offers the advantage of allowing issuers to maintain control over the accreditation status information while also providing the benefits of the EBSI Trusted Issuers Registry regarding security and tamper-proofing. This approach is useful for issuers who have already established their own systems for managing accreditation status information and wish to integrate with the EBSI Trusted Issuers Registry.

Data Structures for Verifiable Accreditation Management

Two data structures or formats can be used to manage the status information of Verifiable Accreditations: W3C Status List and Certificate Revocation List (CRL).

W3C Status List

A Status List can efficiently store information about the status of a Verifiable Accreditation using a simple "Yes" or "No" format. For example, the Ministry of Education could use a W3C Status List to track a university's accreditation status. If the university is granted accreditation and continues to meet the criteria necessary to issue diplomas, its name will be on the list with a "yes" next to it. On the other hand, if a university is found to be no longer qualified to issue diplomas, its name will appear on the list with a "no". The W3C Status List provides a simple and efficient way for the Ministry of Education to manage the accreditation status of universities.

Certificate Revocation List

The CRL provides more detailed information than a simple "yes" or "no" status. Like the Status List example above, the Ministry of Education could use a CRL to keep track of the status of university accreditations. The key difference with a Status List is that if a university's accreditation status has been revoked, the revocation date, reason for revocation, and other related information may also be provided in the CRL.

Revocation of VCs Issued to Natural Persons (GDPR)

Natural persons, such as students, workers, or citizens, receive **Verifiable Attestations** issued by authorised and accredited legal entities. This type of VC asserts statements or claims about the holder, such as possession of a diploma or training certificate. To receive and use VCs, natural persons can register with an EBSI approved wallet provider to request, store, and present their VCs.

A natural person's VC may need to have its status changed from valid to either revoked, suspended, or expired due to changes in personal circumstances or inaccuracies found in the original VC.

Example scenarios may include:

- **Academic misconduct:** A student may be found guilty of cheating on an examination or plagiarism. In such cases, the educational institution may need to revoke the student's VC for the course or degree in question, as it no longer accurately reflects the student's qualifications.
- **Erroneous issuance:** A VC may have been issued incorrectly, containing incorrect information about the natural person's qualifications or achievements. For instance, a university may have mistakenly awarded a degree with honours when the student did not meet the required criteria.
- **Changes in personal circumstances:** A natural person may have a change in their circumstances that requires updating or revoking their VC. For example, a student may need to withdraw from a course due to personal reasons or health issues, resulting in the revocation of their enrolment VC.

Regarding revocation, the status information for Verifiable Attestations belonging to natural persons must be managed per the GDPR. This means that the status information cannot be stored directly on EBSI's ledger. Instead, appropriate measures must be taken to ensure the privacy and security of personal data while still allowing for the efficient management and updating of VC status information.

Verifiable Attestation Management Strategies

The status information of Verifiable Attestations for natural persons can be managed using different strategies based on whether they are short-lived or long-lived VCs. This section outlines these strategies and differentiates them based on their advantages and limitations.

Short-lived VCs

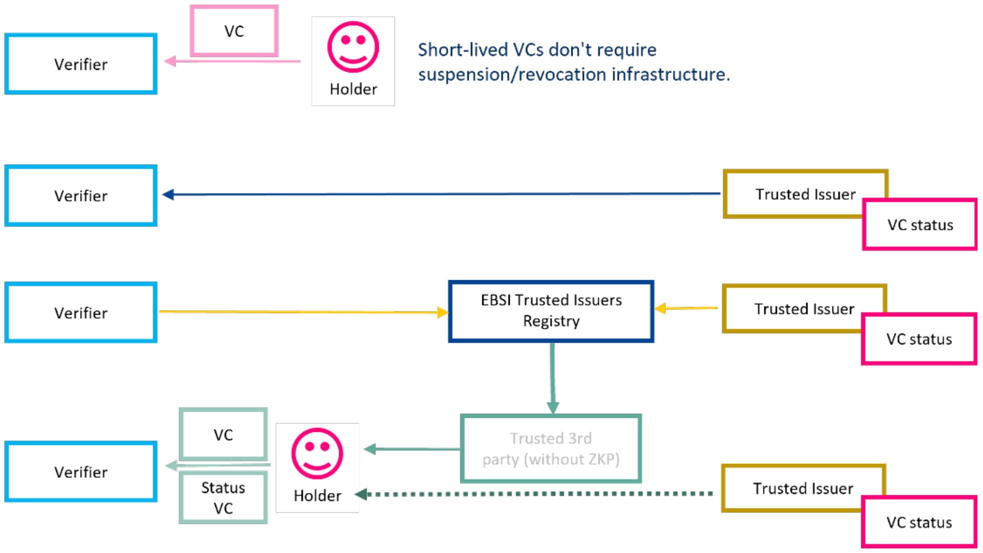
Strategy A: Holder obtains a fresh VC

Long-lived VCs

Strategy B: VC status is obtained directly from the Trusted Issuer.

Strategy C: VC status is obtained from the Trusted Issuer via EBSI

Strategy D: Holder obtains a **status VC** from the Issuer or a third party


Verifier
VC
Holder
Short-lived VCs don't require suspension/revocation infrastructure.
Verifier
Trusted Issuer
VC status
Verifier
EBSI Trusted Issuers Registry
Trusted Issuer
VC status
Verifier
VC
Status VC
Holder
Trusted 3rd party (without ZKP)
Trusted Issuer
VC status

Short-lived VCs

Strategy A: Holder obtains a fresh VC

When using short-lived VCs, the holder obtains a fresh VC each time it is needed. As a result, a short-lived VC does not require additional revocation infrastructure.

Advantages

- Leverages existing VC issuance infrastructure
- Simplifies verification by only requiring an expiration date check
- Ensures up-to-date information
- Prevents tracking of holder status changes by the Verifier

Limitations:

- The Issuer becomes aware of the holder's activities, raising privacy concerns
- Both the Issuer and holder must be online
- The Issuer must support timely VC issuance

Long-lived VCs

Strategy B: Obtaining VC status directly from the Trusted Issuer

In this approach, the status information is retrieved directly from the Trusted Issuer.

Advantages

- Works even if the holder's wallet is offline or has poor connectivity
- Provides up-to-date status information
- Depending on the format, it can limit the duration for which the information is visible to the Verifier.

Limitations:

- The Issuer learns which Verifier received a VC, raising privacy concerns
- Depending on the format, the holder may not be able to limit the duration for which a verifier can check the information

Strategy C: Obtaining VC status from the Trusted Issuer via EBSI

In this approach, the status information is retrieved from the Trusted Issuer through the EBSI network.

Advantages:

- Applicable to both VCs belonging to Legal Entities and Natural Persons
- The Issuer only learns that a VC from the revocation/suspension list has been shared without the knowledge of who shared the information or with whom the information has been shared
- Works even if the holder's wallet is offline (the Verifier must be online)
- Depending on the format, it can limit the duration for which the information is visible to the Verifier.
- Information is shared from the Issuer to the EBSI network to the Verifier, reducing additional traffic for the wallet.
-

Limitations:

- Depending on the format, the holder may not be able to limit the duration during which a verifier can check the information

Strategy D: Holder obtains a status VC from the Issuer or a third party

In this strategy, the holder obtains a separate VC containing status information from either the Issuer or a third party.

Data Structures for Verifiable Attestation Management

Verifiable attestation status information can be stored in one of three formats: W3C Status List, CRL, or as a Status VC. As W3C Status List and CRL-based formats match those used in managing Verifiable Accreditations belonging to legal entities, this section will focus on the **Status VC**. Additionally, within the CRL family of profiles, EBSI introduces a new mechanism, the **Dynamic Status List**, which enables the capability to constrain the time that the status information is visible. The mechanism is applicable to different data formats.

Status VC

A Status VC is a short-lived VC issued to the holder of a credential by either the Issuer or a trusted third party. When the holder shares their credential with a verifier, they share the Status VC along with the original VC. This approach is equivalent to requesting a fresh VC.

Conclusion

The EBSI white paper presents a modular approach to revocation ideal for diverse business scenarios. The revocation framework proposed by EBSI addresses privacy concerns and accommodates revocation services for various stakeholders, including issuers and holders of VCs and the VCs themselves.

EBSI's revocation strategies involve expressing the status of VCs through Credential Status VCs maintained by the issuers. The framework outlines different approaches for managing the revocation of VCs issued to legal entities (non-GDPR) and natural persons (GDPR). For legal entities, the status of VCs can be managed through the Trusted Issuers Registry, using strategies such as storing status information in the registry or hosting it by the Issuer. For natural persons, the status information must comply with the GDPR, and strategies include using short-lived and long-lived VCS and obtaining status information directly from the Trusted Issuer or through the EBSI network.

The white paper highlights the advantages and limitations of each strategy, emphasising EBSI's commitment to creating an adaptable framework that balances privacy, security, and functionality for citizens, businesses, and public organisations throughout Europe.

EBSI
EU-EBSI@ ec.europa.eu

Website:
ebsi.eu

Social handles:
LinkedIn – European Blockchain Services Infrastructure (EBSI)
Twitter – @EU_EBSI

Disclaimer:

This paper was published by the European Commission as a result of a study commissioned to support the work of the European Blockchain Services Infrastructure (EBSI) projectt. The conclusions of presented in this whitepaper do not represent an official recommendation of the European Commission. These conclusions are for informative purposes only.

The European Commission is not liable for any legal, technical, security, or other problems arising from a third party applying this paper’s conclusions in their operations.