Funded by the European
Commission

EBSI Wallet Conformance Testing

Service Offering Description

Document Status:

Status
Service Offering Description: Version 1.3 (this document)

Wallet Conformance Testing service: 3.0 |

Document Author(s):

Name	Role
Kevin AMBROGI (DIGIT-ext)	**EBSI Technical Office**

Document Approver(s):

Name	Role
Joao RODRIGUES-FRADE (DIGIT)	**EBSI**

Document Reviewer(s):

Name	Role
Joao RODRIGUES-FRADE (DIGIT)

Gregory STEENBEEK (DIGIT-ext) | **Reviewer**

EBSI Stakeholder Management Office |

Summary of Changes:

Version	Date	Created by	Short Description of Changes
V0.1	12/10/2021	Kevin AMBROGI	First draft.
V0.2	13/10/2021	Kevin AMBROGI	Edited section 1.1 figure 2; section 2.1 (last bullet point) and 2.2 (last bullet point) see comments for each bullet point.
V0.3.1	14/10/2021	Gregory STEENBEEK	General comments.
V0.3.2	15/10/2021	Joao RODRIGUES-FRADE	General comments.
V0.4	18/10/2021	Kevin AMBROGI	Implementation of comments from V0.3 from Joao RODRIGUES-FRADE and Greg STEENBEEK.
V0.5	20/10/2021	Kevin AMBROGI	Review of updates with Gregory STEENBEEK, Wesley DEGLISE and Regina DELA EVA.
V0.6	21/10/2021	Gregory STEENBEEK	Review of updates, corrections of typos, design and layout. Addition of a schema in section 4.2. Verification of links and replacement with dynamic links. Addition of comments.
V0.7	22/10/2021	Joao RODRIGUES-FRADE	General comments.
V0.8	26/10/2021	Gregory STEENBEEK	Review of updates, corrections of typos, design and layout.
V0.9	26/10/2021	Joao RODRIGUES-FRADE	Review
V0.9.1	26/10/2021	Gregory STEENBEEK Kevin AMBROGI Regina DELA EVA	Minor modifications.
V1.0	26/10/2021	Joao RODRIGUES-FRADE	Final Review.
V1.1	23/11/2021	Kevin AMBROGI	Added missing URL to 1.4.2 - Users Onboarding.
V1.2	17/12/2021	Kevin AMBROGI	Update to match automated conformance log trace process.
V1.2.1	13/1/2022	Joao RODRIGUES-FRADE Gregory STEENBEEK Kevin AMBROGI	Review. Modification of Terms and Conditions. Implementation of updates, corrections of layout.
V1.2.2	17/1/2022	Joao RODRIGUES-FRADE	Final Review.

V1.2.3	25/1/2022	Gregory STEENBEEK	Modifications of Terms and Conditions.
V1.2.4	11/02/2022	Gregory STEENBEEK	Update of all links for publication in the EBSI documentation and inclusion of updated links from the new EBSI website. Added the information that the logs are kept 2 weeks.
V1.3	04/04/2023	Kevin AMBROGI	Updates related to WCT v3 Document simplification
V1.3.1	18/04/2023	John YATES	Updates from Support Office
V1.3.2	18/04/2023	Matti Taimela	Updates from Architecture
V1.3.3	19/04/2023	Kevin AMBROGI	Final technical review before legal review
V1.3.4	25/04/2023	Kevin AMBROGI	Final review of legal comments and corrections
V1.3.5	26/04/2023	Kevin AMBROGI	Updates to branding guidelines section
V1.3.6	09/06/2023	Kevin AMBROGI	Added URL pointing to EBSI branding guidelines web page to Section 3
V1.3.7	06/12/2023	Kevin AMBROGI	Updated URL pointing to Master Service Arrangement in section 3

Table of Contents

The EBSI Wallet Conformance Testing service is intended for third-party application providers developing digital wallets and applications that want to ensure the interoperability and conformance of their wallet(s) and applications with the specifications defined by the European Blockchain Services Infrastructure (EBSI).

Disclaimer

By having their wallet listed as an EBSI-conformant solution on EBSI's website, the EBSI team confirms that a specific wallet fully abides by the EBSI core services specifications and the technical specifications based on W3C Verifiable Credentials, DIDs and GDPR. This conformance testing does not include a security assessment of the wallet, nor a security certification.

Definitions and acronyms

Here you will find an overview of key terms used in this document:
https://ec.europa.eu/cefdigital/wiki/x/TAfvB

Here you will find an overview of key acronyms used in this document:
https://ec.europa.eu/digital-building-blocks/wikis/x/AwBXHQ

1. INTRODUCTION TO THE EBSI WALLET CONFORMANCE TESTING SERVICE

This document describes the Wallet Conformance Testing service provided by EBSI. It introduces the purpose of the service, its users, its scope, its benefits, the related roles and responsibilities, the data being created, stored or exchanged as well as who creates it and the overall process.

➢ Follow the link below to access the Wallet Conformance Testing service:
https://api-conformance.ebsi.eu/docs/wallet-conformance

1.1. Objective

The goal of the EBSI Wallet Conformance Testing service is to verify that third-party wallets conform to the:

- **EBSI core services specifications:** this will assess if a wallet can correctly interact with the core services endpoints of EBSI. In simplified terms, that wallets' requests are well formed and that the core services return a successful answer. Follow the link below to access the EBSI API documentations in the EBSI Developers Hub
- **EBSI playbook of Verifiable Credentials and their lifecycle:** this section will clarify how a wallet can correctly interact with Issuers of Verifiable Credentials (VC) and Verifiers of Verifiable Presentations (VP). Follow the link below to access the EBSI VC Playbook in the EBSI Developers Hub

1.1.1. EBSI Core Services Specifications

This set of tests will assess if a third-party wallet and applicationsare able to communicate with EBSI via their APIs. For example, a wallet must be able to interact with EBSI's DID Registry API. This register is a generic core service of EBSI enabling wallets to resolve EBSI Decentralised Identifiers (DIDs).
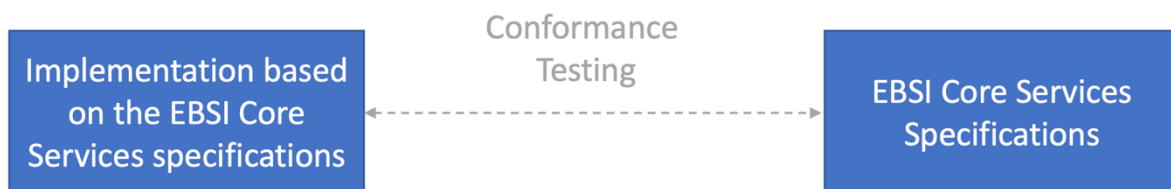

Figure 1 – EBSI Wallet Conformance Testing

The EBSI team provides ready to use guidelines and test endpoints for each core service and supports the users of the conformance testing service during the entire testing process. The overall approach for testing the conformance to EBSI's Core Services Specifications is shown in the figure below:
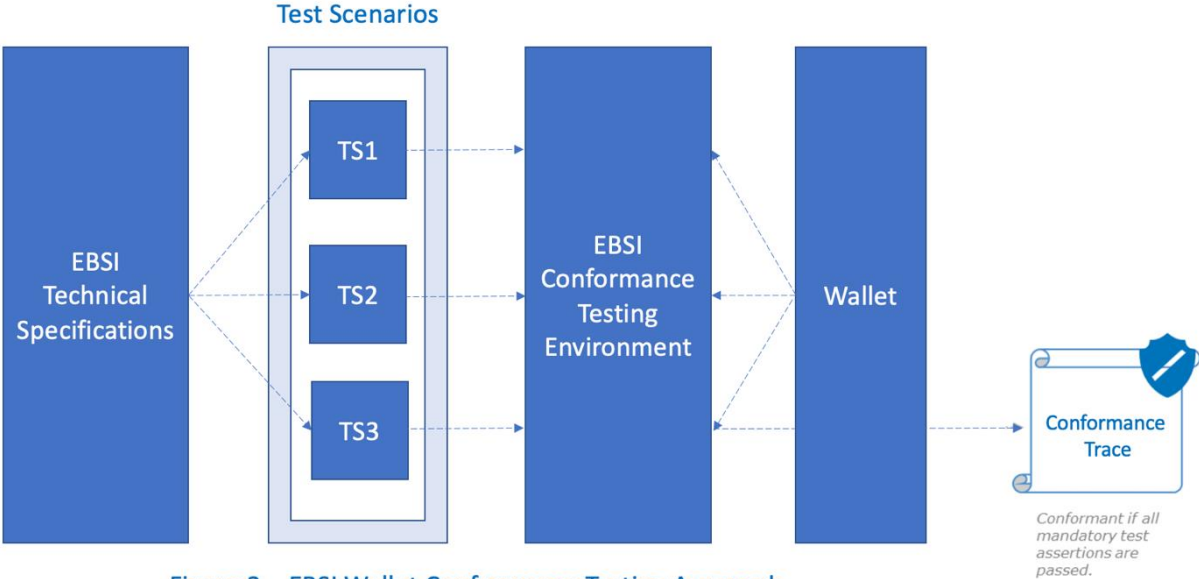

Figure 2 – EBSI Wallet Conformance Testing Approach

These tests will:
- ensure that a given wallet from a third-party developer (wallet app, mobile app, web app, etc.) conforms to the EBSI core services API;
- enable the app developers to self-assess their applications by recording a "conformance testing header" over the core services API;
- enable the app developers to leverage the Conformance Trace and prove the conformance of its app (a specific version with each EBSI APIs (e.g. a specific version of the APIs and test scenario).

→ To perform the wallet conformance testing, the wallet provider needs to initiate the process by following these steps:

Who	Steps

Wallet provider	- defines the conformance testing metadata needed to evaluate if a request is conformant as specified here; *Note: The conformance testing header attests that a given major version* of a wallet conforms to a given major version* of EBSI;*
	 - performs the selected test scenarios as specified below:
	   - Accredit & Authorise
	   - Issue to Holder
	   - Holder Wallet
	   - Verify
	 - contacts the EBSI Support Office to submit the conformance testing header together with the self-assessment spreadsheet and request its anchoring.

* A major version is, as defined per [semantic versioning](#), a version that introduces breaking changes and is consequently not compatible with the previous major version.

1.1.2. EBSI Playbook of Verifiable Credentials (VC) and their Lifecycle

As defined on the [EBSI Verifiable Credentials Playbook](#), EBSI aims to create a generic profile for the full life-cycle of Verifiable Credentials (VC) and Verifiable Presentations (VP) for use cases that involve VCs (not exclusively), building on the [W3C's Verifiable Credentials standards](#), the [GDPR](#) and any other relevant EU Regulations.

The diagram below demonstrates the relations between actors (Trusted Accreditation Organisations [TAO]), Holders, Issuers and Verifiers), use cases, wallet providers, standards, regulations ([W3C Verifiable Credentials](#), [DIDs](#) and [GDPR](#)), and the EBSI VC Playbook.
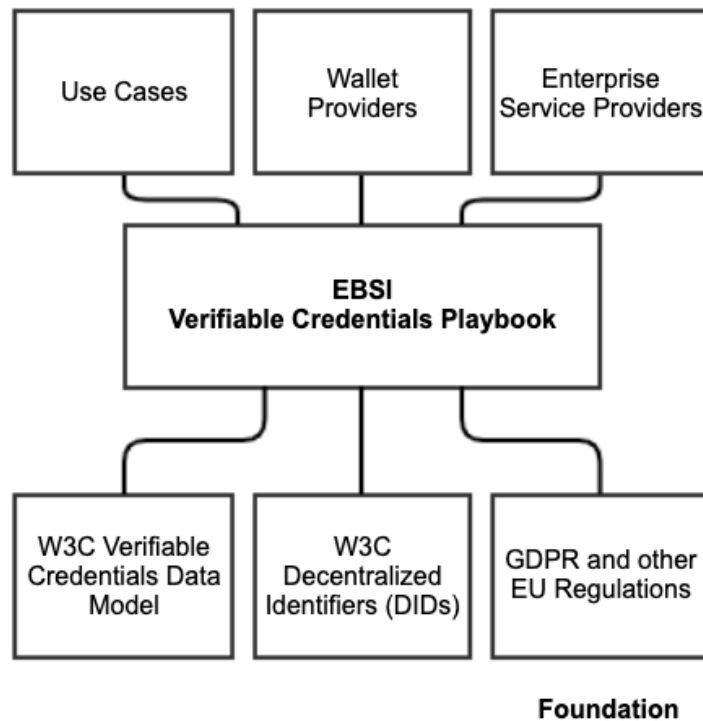
1.2. Users

The EBSI Wallet Conformance Testing service is intended for third party **wallets and applications providers.** The service confirms that a wallet solution (a specific version) conforms to the EBSI specifications (a specific version).

1.2.1. EBSI Core Services Specifications

In the context of the EBSI Wallet Conformance Testing, the only capabilities considered are the ones provided by the wallet provider to the holder, or natural person, who uses the wallet.

Interactions with services, other than EBSI services, or with other actors than the holder, e.g. TAO, Verifier, Issuer, will be mocked by the Wallet Conformance Testing service in order to allow the Wallet Provider to test all interactions with all actors involved in the VC lifecycle.

1.2.2. EBSI Playbook of Verifiable Credentials (VC) and their Lifecycle

For the purpose of the EBSI Wallet Conformance Testing, the interactions between the main actors and EBSI are in scope, as defined in the following test scenarios:

- Accredit and Authorise:
    - Trusted Issuers
    - Trusted Accreditation Organisations
    - Root Trusted Accreditation Organisations

- Issue to Holder:
    - Trusted Issuers

- Holder Wallet:
    - Holder Wallet

- Verify:
    - Verifier

1.3. Benefits

The EBSI Wallet Conformance Testing service has been designed to provide a number of benefits to the users of the service. These are explained below.

1.3.1. EBSI Core Services Specifications

One of the benefits of the Wallet Conformance Testing service are that wallet providers can leverage the EBSI API Developers Hub. It serves as fully testable core service specifications, which allow wallet providers to test, modify, copy and build their API requests at no cost and in real time.

The additional value for wallet providers is that the EBSI API Developers Hub displays conformance-specific endpoints with specific success/error messages, along with detailed guidance to facilitate the completion of the Wallet Conformance Testing processes.

1.3.2. EBSI Playbook of Verifiable Credentials (VC) and their Lifecycle

The table below highlights the benefits for each actors involved in the Wallet Conformance Testing:

Who	Benefits
Wallet provider	- to confirm to and assure its users that the wallet or implementation is conformant with the specifications of the EBSI Core Services; - to benefit from a testing service supported by professional staff of the European Commission; - to benefit from a quick testing cycle with reduced cost; - to be able to test anywhere and at any time; - to provide a testing service that is core-service-based and with ready-to-use test cases with a common and standardised plugin; - to provide an easy way to share and verify the conformity of the wallet by anchoring the conformance testing header on-chain on the EBSI network; - to be able to confirm to and assure its users that the wallet is conformant for a given major version* of the wallet (meaning that the wallet needs to go through the Wallet Conformance Testing process each time a new major version* is released).
End users	- to have an increased number of EBSI-conformant wallets available to choose from depending on their use or personal preference; - to be sure that conformant wallets behave as expected with the EBSI Core Services for any given major versions* of the wallet and of the EBSI Core Services; - To be able to easily verify the conformity of a specific version of the wallet by checking its conformity for a given major version* of the EBSI Core Services (meaning that the wallet needs to go through the Wallet Conformance Testing process each time a new major version* of the EBSI Core Services is released).

* A major version is, as defined per semantic versioning, is a version that introduces breaking changes and is consequently not compatible with the previous major version.

1.4. Scope

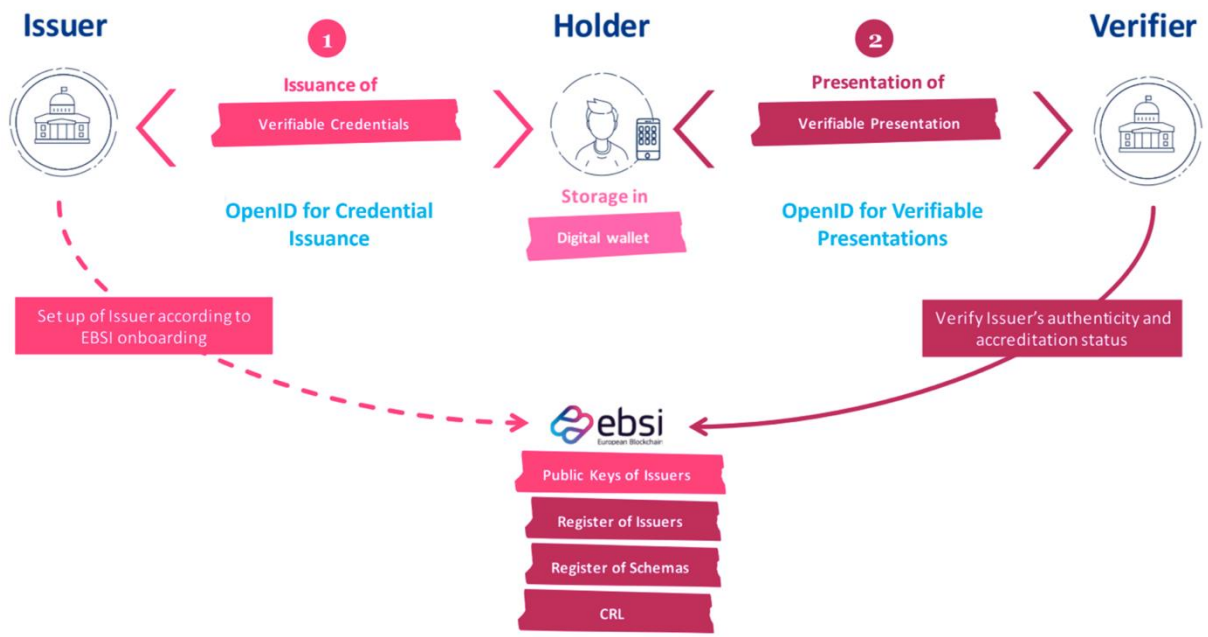### 1.4.1. EBSI Core Services Specifications

The table below presents an overview of the test flows, the expected outcomes and the corresponding services offered by the EBSI Wallet Conformance Testing service:

Table 1: EBSI Wallet Conformance Testing service

Test Flow	Outcome	Guidelines
Accredit and Authorise	• Legal Entities can manage and work with accreditations. • Legal Entities can revoke with different revocation strategies. • Demonstrate working configuration through exposed metadata • DID is registered on EBSI Ledger. • Trust Chain accreditations are registered on EBSI Ledger.	See Providers and Wallets Metadata See Accredit and Authorise Functional Flows
Issue to Holder	• Issuer can issue credentials synchronously and asynchronously • Issuer can handle different authentication models • Issuer can work without accreditations	See Issue to Holder Functional Flows
Holder Wallet	• A Natural Person presented its Verifiable Attestation(s) [VC-Type] to a Legal Entity. • Wallet Holder can request different credentials from known Issuers • Wallet can handle synchronous and asynchronous credential issuance • Wallet can handle different authentication models	See Holder Wallet Functional Flows
Verifier	• Verifier can request Verifiable Presentations • Verifier understands minimum domain exceptions	See Verifier Functional Flows

1.4.2. EBSI Playbook of Verifiable Credentials (VC) and their Lifecycle

The diagram below summarises the scope and actors associated to the testing of the Verifiable Credentials lifecycle, full specifications are available here:

Steps	EBSI Verifiable Credentials Lifecycle	W3C Verifiable Credentials Lifecycle	Guidelines	Actor
Step 1	Registration and onboarding of actors (Trusted Accreditation Organisation, Holder, Issuer, Verifier)	Out of scope of W3C's Lifecycle.	- Onboarding Legal Entities - Learn how Legal Entities on-board on EBSI; - Register Natural Persons - Learn how Natural Persons on-board on EBSI; - Register TAO and TI in Trusted Issuers Registry - Learn how to verify, register, and update Trusted Accreditation Organisation (TAO) information in the Trusted Issuers Registry	- Issuer, TAO, Verifier - Holder - TAO - Issuer

Step 2	Issuing and Storage of Verifiable Credential	Issuance of one or more Verifiable Credentials.	• [Verifiable Credential issuance guidelines](#) - Learn how holders request and issuers issue Verifiable Credentials	• Holder, Issuer, TAO
		Storage of Verifiable Credentials in a credential repository (such as a digital wallet).		
Step 3	Sharing Verifiable Presentation	Composition of Verifiable Credentials into Verifiable Presentations and Verifiable Presentation exchange.	• [Verifiable Presentation exchange in a (un)authenticated session](#) - Learn how a verifier requests and holder presents Verifiable Credential(s) using Verifiable Presentation(s)	• Holder, Verifier
		Verification of the Verifiable Presentation by the Verifier.		
Step 4	Managing schemas	Out of scope of W3C's Lifecycle.	• [Managing schemas in the Trusted Schemas Registry](#) - Learn how to verify, register, and manage schemas in the Trusted Schemas Registry	• Issuer, Verifier

1.5. Data

1.5.1. EBSI Core Services Specifications

In the context of the EBSI Wallet Conformance Testing, the capabilities considered are the ones provided by the wallet provider to the holder, who uses the wallet: please refer to 1.5.2. for full details of who creates, stores and exchanges data. Please note that the Wallet Conformance Testing v3 will test interactions with the following main actors:

- the trusted issuer,
- the trusted accreditation organisation,
- the root trusted accreditation organisation
- and the verifier

Please note that the Holder Wallet flow can be completed using either same or cross-device interactions, please refer to the matrix below.

Flow Name	Supported Device
• Accredit & Authorise	• Same-device
• Issue to Holder	• Same-device
• Holder Wallet	• Same-device • Cross-device
• Verify	• Same-device

Important note: no personal data is allowed to be used at any time during the Wallet Conformance Testing.

1.5.2. EBSI Playbook of Verifiable Credentials (VC) and their Lifecycle

The table below presents which data is created, stored or exchanged; and who creates it:

Test Scenario	Done by / sub-Flow	Data-related Action	Data	Outcome
Accredit & Authorise	• Wallet Provider	• Set up wallet • Create your DID • Input your DID and ClientID	• DID and associated public/private keys • DID • ClientID	• User Wallet has been set up • Wallet DID created but not registered in EBSI • DID and ClientID input
	• Trusted Issuer	• Onboarding • Get Accredited as Trusted Issuer (TI) • Issue & Revoke	• Trusted Accreditation • Revoked Trusted Accreditation	• DID registered on EBSI • Trusted Accreditation registered on EBSI • Trusted Accreditation revoked

• Trusted Accreditation Organisation	• Request Verifiable Accreditation to Accredit • Register Verifiable Accreditation to Accredit into the Trusted Issuer Registry (TIR) • Issue Verifiable Accreditation to Attest for sub-account DID • Revoke Trusted Issuer rights from sub-account DID	• Trusted Accreditation to Accredit • Trusted Accreditation to Attest	• Verifiable Accreditation to Accredit requested • Verifiable Accreditation to Accredit registered into TIR • Trusted Accreditation to Attest issued to sub-account DID • Trusted Issuer rights from sub-account DID revoked
• Root Trusted Accreditation Organisation	• Request Verifiable Authorisation For Trust Chain • Register Verifiable Authorisation For Trust Chain into the Trusted Issuer Registry (TIR)	• Verifiable Authorisation For Trust Chain	• Requested Verifiable Authorisation For Trust Chain • Registered Verifiable Authorisation For Trust Chain
• Wallet Conformance Testing Validation	• Request Wallet Conformance Testing Accredit & Authorise Credential from Conformance Issuer	• Wallet Conformance Testing Accredit & Authorise Credential • Wallet provider Details	• Requested Wallet Conformance Testing Accredit & Authorise Credential • Conformance Badge ready to download

	• Inspect your Conformance Logs	• Input Wallet provider company details for Conformance Badge	• Wallet provider Details • DID • ClientID	• EBSI Helpdesk successfully submitted
	• Contact EBSI Helpdesk with DID and ClientID to request the issuance of the Wallet Conformance Testing report	• Fill in EBSI Helpdesk form		
Issue to Holder	• Trusted Issuer	• Create your DID • Input your DID and ClientID	• DID and associated public/private keys • ClientID	• User Wallet has been set up. • Wallet DID created but not registered in EBSI yet. • DID and ClientID input
	• Initiate Credential Issuance	• Issue In-Time Credential • Issue Deferred Credential • Issue Pre-Authorised Credential	• In-Time Credential • Deferred Credential • Pre-Authorised Credential	• Issued In-Time Credential • Issued Deferred Credential • Issued Pre-Authorised Credential
	• Wallet Conformance Testing Validation	• Request Wallet Conformance Testing Accredit & Authorise Credential from Conformance Issuer	• Wallet Conformance Testing Accredit & Authorise Credential	• Requested Wallet Conformance Testing Accredit & Authorise Credential
	• Inspect your Conformance Logs	• Input Wallet provider company details for Conformance Badge	• Wallet provider Details	• Conformance Badge ready to download
			• Wallet provider Details	• EBSI Helpdesk successfully submitted

	• Contact EBSI Helpdesk with DID and ClientID to request the issuance of the Wallet Conformance Testing report	• Fill in EBSI Helpdesk form	• DID • ClientID	
Holder Wallet	• Holder	• Insert your DID & URL scheme • Initiate Credential Issuance cross-device • Initiate Credential Issuance same-device	• DID • URL Scheme • QR code for In-Time, Deferred and Pre-Authorised Credential	• Issued QR Codes for In-Time, Deferred and Pre-Authorised Credential
	• Wallet Conformance Testing Validation	• Request Wallet Conformance Testing Accredit & Authorise Credential from Conformance Issuer	• Wallet Conformance Testing Accredit & Authorise Credential	• Requested Wallet Conformance Testing Accredit & Authorise Credential
	• Inspect your Conformance Logs		• Wallet provider Details	• Conformance Badge ready to download
	• Contact EBSI Helpdesk with DID and ClientID to request the issuance of the Wallet Conformance Testing report	• Input Wallet provider company details for Conformance Badge • Fill in EBSI Helpdesk form	• Wallet provider Details • DID • ClientID	• EBSI Helpdesk successfully submitted
Verify	• Verifier	• Input Client ID Token • Input Verifiable Presentation Token	• ID Token Request • VP Token Request • Presentation Definition and Submission	• Validated ID Token • Validated VP Token • Validate VCs

- Test ID Token and Verifiable Presentation Token
- Identify expired VC in VP
- Identify revoked VC in VP
- Identify not yet valid VC in VP

- Inspect your logs

- Fill in EBSI Helpdesk form

- Wallet provider Details
- DID
- ClientID

- EBSI Helpdesk successfully submitted

2. HOW TO USE THE SERVICE STEP-BY-STEP

This chapter presents information on how to use the EBSI Wallet Conformance Testing service, including the roles and responsibilities of the different actors involved in it.

2.1. For the wallet provider

The wallet provider commits to integrate its wallet with the EBSI Core Services, and to conform to the EBSI Core Services specifications.

The table below summarises the steps that the wallet provider should follow to complete the Wallet Conformance Testing process.

Who	Steps
Wallet provider	- defines the conformance metadata needed to evaluate if a request is conformant as specified here; *Note: The conformance metadata attest that a given major version* of a wallet conforms to a given major version* of EBSI;* - performs the selected test scenarios as specified here; - contacts the EBSI Support Office to submit the conformance DID and Client ID.
EBSI Support Office	- evaluates the conformance testing metadata . - extracts the specific conformance trace based on the header provided by the wallet provider, - confirms that the tests have been passed, by checking for each test scenario that the relevant tested API and HTTP code match; - alternatively, if clarifications are needed, the EBSI Support Office contacts the Wallet provider with questions or corrective measures until the conformance can be confirmed; - declares the wallet conformant, once all tests have been confirmed as successful; - adds the wallet provider company details and logo together with its EBSI-conformant wallet (incl. version of the wallet) to the public list of EBSI-conformant wallets. Each entry is displayed together with the detailed conformance report and test result(s); - sends a confirmation to the wallet provider detailing the exact date and time of the conformance, its recording on EBSI, and detailed results of the tests performed in a report annexed to the ticket.

* A major version is, as defined per semantic versioning, a version that introduces breaking changes and is consequently not compatible with the previous major version.

2.2. For the EBSI Support Office Team

The EBSI Support Office team liaises with the wallet providers interested in testing the conformance of their wallets with the EBSI infrastructure and standards. It has the following responsibilities in the context of the EBSI Wallet Conformance Testing service:

- to liaise with the wallet providers and handle all inbound conformance testing requests;
- to support the wallet providers with every EBSI Wallet Conformance Testing actions:
  - to review conformance test results;
  - to add the company details and logo of the wallet provider and its EBSI-conformant wallet to the public list of EBSI-conformant wallets, together with the detailed conformance report and test result(s).

3. TERMS AND CONDITIONS

Please consult the EBSI Master Service Arrangement, outlining the general terms to be respected by EBSI stakeholders when using and managing the EBSI Software sample implementation and/or Service, available here on the EBSI website:

The table below describes the terms and conditions specific to the EBSI Wallet Conformance Testing service.

Table 2: EBSI Wallet Conformance Testing service - Terms and conditions

Term / Condition	Description
Obligations of the user	It is the responsibility of the user to abide by the Terms and Conditions of the EBSI Wallet Conformance Testing Service Offering Description and the EBSI Core Services specifications.
	It is the responsibility of the user to ensure that no personal data is used at any time during the Wallet Conformance Testing.
	The wallet needs to go through the conformance testing process each time the wallet provider plans to release a new major version* of their software **OR** each time a new major version* of EBSI is deployed.
	Wallet providers should provide correct company details and logo as specified in the request form sent to the EBSI Support Office.
Branding Guidelines	Only conformant Wallet Providers who are recipients of a signed and valid EBSI Conformance certificate should be allowed to use the EBSI branding guidelines and display the EBSI conformance badge on their website. You may only display the Conformance badge that corresponds to the conformance test you have passed. You may display more than one Conformance badge if you have successfully passed more than one EBSI Conformance test. EBSI Conformance badges and guidelines regarding their use can be found on the EBSI Branding guidelines webpage.
	Please do not alter the EBSI conformance badge in any way, including changing the colour or dimensions. Do not use the EBSI conformant badge as text, for example, as part of a sentence instead of words "EBSI conformance badge".
Delivery of the services	The European Commission will provide the Wallet conformance testing services using reasonable care and skill and in accordance with the technical specifications and

	procedures outlined in this document. The timing of completion of the Wallet conformance testing services and the delivery of the test results by the European Commission is based on best effort. The European Commission is entitled to suspend or terminate the provision of the services in case of failure of the user to comply with its obligations, as described above, or any other conditions preventing the successful delivery of the service. Please note that the **logs created by the wallet provider for the purpose of the wallet conformance testing service will be erased two weeks after creation**. It is advised to request the verification of the results of the tests from the EBSI Support Office as soon as possible.
Warranty disclaimer	The Wallet conformance testing services and the result thereof are provided on the basis of the information, documents and implementations supplied by the wallet provider or its organisation. The test report and the recorded log trace issued by the European Commission are issued on an AS-IS basis and will reflect the facts as recorded at the time of testing. The European Commission is under no obligation to refer to, or report upon, any facts or circumstances which are outside the scope of this service and the procedures outlined in this document.
Limitation of liability	In no event shall the European Commission be liable to the wallet provider or its organisation or anyone claiming through the user, for any kind of damages resulting from reliance on the test result. If the product/implementation passes all mandatory test assertions, the wallet provider will receive a Wallet conformance test report. It should be clear that this test report has no legal value, and is a technical report, outlining the test results based on the version of the test platform and test cases in effect at the time of testing. The conformance test report is restricted to, and only applies to, the specific version of the product that was subject to testing for a specific test run at a specific date. Other products offered by the wallet provider or its organisation or versions of that product which did not undergo testing cannot be considered as conformant.
Disclosure	The wallet provider is entitled to disclose to third parties the fact that the product/implementation passed the

	Wallet conformance test. This should be done only in accordance with the rules outlined below::
	1. There should be a clear indication of the version of the EBSI specifications, the version of the product to which the result of the Wallet conformance test applies, labelled with the specific test run and date; 2. The Wallet conformance test report can only be reproduced and shared in its entirety; 3. The Wallet conformance test report should not be used in such a manner as to bring the European Commission into disrepute and should not make any statement regarding the result of the conformance test that the European Commission may consider misleading or unauthorised. 4. The wallet provider agrees to modify or remove part of or the integrity of the Wallet conformance test report and/or associated communication at the request of the European Commission. 5. The Wallet conformance test report does not include a security assessment of the wallet, nor a security certification. The user of the Wallet conformance testing service agrees to the publication of the test result, including details provided by the wallet provider (wallet provider organisation, website, name of the product, logo) by the European Commission on any material or platform deemed relevant. As the conformant wallets are tested against a specific version of the EBSI specifications, wallet needs to go through the Wallet conformance testing process each time the wallet provider plans to release a new major version* of their software OR each time a new major version* of EBSI is deployed. The European Commission will remove wallets that are conformant with deprecated version of the EBSI specifications from any above-mentioned material or publication. Should the wallet provider disagree with the publication of the test result and aforementioned details, a request can be sent to the EBSI Support Office.

* A major version is, as defined per semantic versioning, a version that introduces breaking changes and is consequently not compatible with the previous major version.

3.1. Limitations of the current service

This conformance testing does not include a security assessment of the wallet, nor a security certification.

4. CONTACT INFORMATION

4.1. How to request the service

As described under section 2.1, the wallet provider should initiate the service by following the detailed steps described on this page.

For the purpose of testing the conformance of its wallet, the wallet provider should connect its wallet with the EBSI Core Services in order to be able to perform the conformance tests and to conform to the EBSI Core Services specifications.

After completing all the steps, the wallet provider should contact the EBSI Support Office to complete the conformance testing process.

4.2. Best practices

The wallet conformance testing is estimated to require up to a week-worth of work of up to two full-time-resources, e.g. two man-weeks, to perform the complete set of tests.

Ideally a small cross-functional team, e.g. two developers or one developer and one tester (or more if available), should be sufficient to perform the tests.

For faster completion time, it is highly recommended that the team is fully focused on the wallet's conformance tests exclusively.

Please note that the **logs created by the wallet provider for the purpose of the wallet conformance testing service will be erased two weeks after creation**. It is advised to request the verification of the results of the tests from the EBSI Support Office as soon as possible.

4.3. Conformance testing flow

The diagram below illustrates the high-level timeline of the Wallet Conformance Testing:
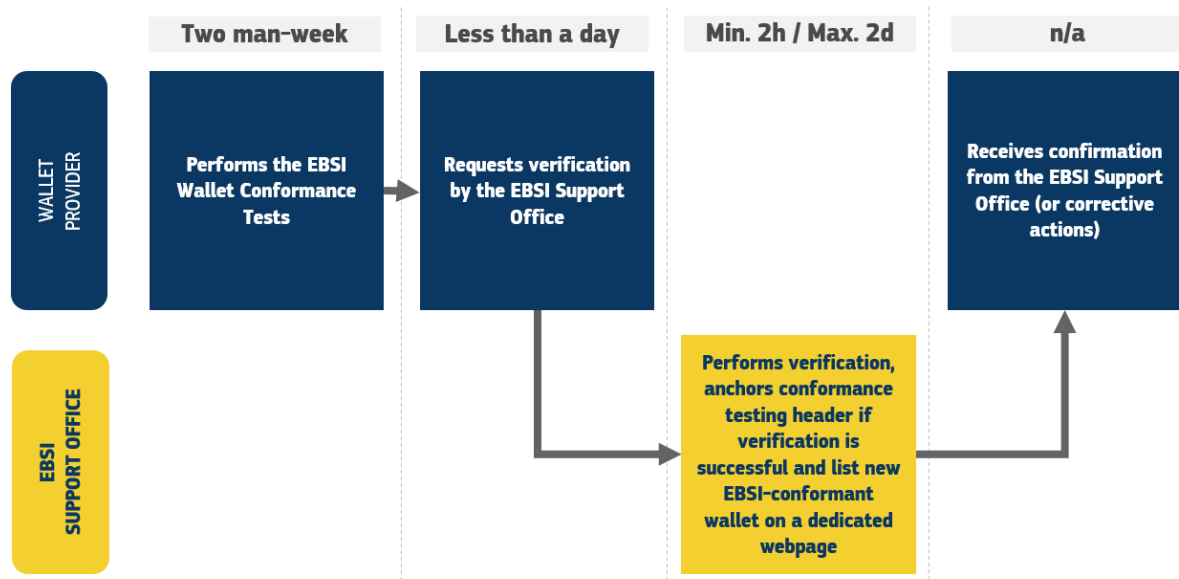
4.4. What will happen if the wallet passes the Conformance Testing process?

After completing all the steps listed in section 2.1 the wallet provider should contact the EBSI Support Office to request the verification of the self-assessment spreadsheet and the Wallet conformance testing header, and the anchoring of the conformance testing header.

After the Wallet conformance testing header together with the self-assessment spreadsheet has been successfully verified, the EBSI Support Office will schedule a meeting with the wallet provider to review the Wallet conformance testing results, confirm which test scenarios were implemented, and confirm the conformance of the wallet.

Then, the conformance log trace will be anchored on-chain by the EBSI Support Office, the wallet provider will receive a confirmation by the EBSI Support Office that the Wallet conformance testing process has been successful. The wallet provider's company details and logo will be added to the list of EBSI-conformant wallets on a dedicated webpage, together with the detailed conformance report and test result(s).

EBSI Wallet Conformance Testing service:

➢ **Visit the WCT service page**

EBSI Support Team

➢ **Visit the Help desk**

Support Service: 8am to 6pm (Normal EC working Days)