01

Key action points to cover by SEEBLOCKS & BLOCKSTAND projects

Based on European Commission policy objectives for Distributed Ledgers Technologies – Rolling plan for ICT Standardization

Key action points to cover by SEEBLOCKS & BLOCKSTAND projects

Based on European Commission policy objectives for Distributed Ledgers Technologies – Rolling plan for ICT Standardization

01

DLT as trust anchor infrastructure

Define standards and interfaces to facilitate the role of EBSI as a trust anchor management infrastructure, to support several data formats and proofs (i.e. those included in the ARF)

02

DLT-based profile aligned with eIDAS

Contribution to the standardization of EBSI profile signatures, data formats, interfaces and associated processes in order to guarantee its alignment with eIDAS1&2 requirements.

03

DLT as a trust service

Set the technical framework and cybersecurity standards to facilitate the recognition of DLTs as a trust service in line with eIDAS1&2 requirements.

04

Smart Contracts as trusted technology

In line with the Data Act proposal and eIDAS1&2 , technical work to support the standardization of smart contract business processes, security and related topics from a European perspective

02

DLT as trust anchor management infrastructure

DLT as trust anchor management infrastructure

Objectives and description of this action point

Objectives

Define standards and interfaces to facilitate the rol of EBSI as a trust anchor management infrastructure to support several data formats and proofs. EUDIw ARF specifications should be taken as a reference.

Description

Independently of those digital credentials issued under the EBSI profile (modelled as Verifiable Credentials with proofs based on EBSI-DLT), EBSI as a decentralized network based on a permissioned ledger, can be considered as a trusted infrastructure to support other data format and electronic signatures included in the eUDIw ARF. The ISO23220 / 18013-5 or the OpenID Federation can be taken as an example.

A proposal of task

Starting from current EBSI interfaces and Trust Data Model, define interfaces, data structures, flows and any other technical artifacts or mechanism to onboard Trust Anchors in EBSI based on alternative technology stacks / business requirements

02

A DLT-based proof profile aligned with eIDAS

A DLT-based proof profile aligned with eIDAS

Objectives and description of this action point

Objectives

Standardization of the DLT-based proof EBSI profile, including signatures, data formats and associated processes for its alignment with eIDAS1 regulation and eIDAS2 proposal requirements and European standards (i.e. JADES).

Description

The current ETSI standards for advanced/qualified signatures and seals are not technically neutral because they require using X.509v3 certificates, preventing the adoption of a DPKI approach based in DLT.

For the time being, Q-seals or Q-signatures can only be based on Q-certificates, which standards are only defined for x.509v3.

This action point should extent current standards to provide more inclusive Q-seals/Q-signatures to support seals/signatures based on DLT.

The EBSI profile should be taken as reference and starting point. It is based on the W3C Verifiable Credential data model, W3C Decentralized Identifiers data model, JSON signatures and proofs based on DLT.

A DLT-based proof profile aligned with eIDAS

A proposal of tasks to be delivered in this action point

01

Design of a DPKI-Cert to be promoted as a new type of Q certificate for eSignature/eSeal.

The design should be aligned with the W3C VC Data Model and w3c DID Document data model to enable the verification of the VC using a did:method.

The RFC 5280 and ETSI TS 319 412 could be considered as a reference.

02

Design of creation and validation processes for the DPKI-Cert

Design of creation and validation processes for the DPKI-Cert, as an analogy to ETSI 319 102-1, and based on DLT-proofs.

The validation process should include the design of a VC-status service, aligned with the current EBSI VC-status framework.

03

Common interfaces to validate eSeals / eSignatures based on DLT proofs

Standardization of interfaces to enable the validation of eSeals/eSignatures based on JWS and JADES included in VCs and based on DLT-proofs.

A DLT-based proof profile aligned with eIDAS

A proposal of tasks to be delivered in this action point

04

Standardization of e-Seal / e-Sign creation services based on DLT-proofs

Design of a qualified automated eSeal/eSignature creation service, based in DPKI for VC issuers.

The standard should take as reference protection profiles described in CEN EN 419 221-x, CEN EN 419 241-x

05

Standardization of validation processes for eSeals/eSignatures based on DLT-proofs

Design of a qualified eSeal/eSignatures validation process, based in DLT-proofs, with equivalent functionality with EN 319 102-1/TS 119 102-1.

06

Standardization of JADES Signatures to support DLT-proofs

Change requests to ETSI JAdES and CB-AdES technical specifications. This will include how these signatures can be validated using DLTs.

A DLT-based proof profile aligned with eIDAS

A proposal of tasks to be delivered in this action point

07

Standardization of e-Seal / e-Sign creation services based on DLT-proofs

Evolution of the EBSI Trust Model to support the new D-PKI Cert aligned with the eIDAS Regulation, offering equivalent functionality to Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 and ETSI TS 119 612 v2.1.1.

This task will take into account the trust model and the taxonomy defined in the EBSI Trust Model, including Trusted Issuers, Accreditation data model and Trusted Accreditation Organizations.

08

Standardization of a reference architecture model DLT based to onboard trust frameworks

Design of a reference architecture model to support trust framework for attestations, based on DLT.

This will also include the interfaces to expose DLT services against stakeholders of a decentralized identity system, and related processes.

DLT as a trust service

DLT as a trust service

Objectives and description of this action point

Objectives

Set the technical framework and cybersecurity standards to facilitate the recognition of DLTs as a trust service in line with eIDAS1&2 requirements.

Description

As it was announced, the Council presidency and European Parliament representatives reached a provisional political agreement on the core elements of a new framework for a European digital identity (eID). To respond to the dynamics of the markets and to technological developments, the revised regulation expands the current list of trust services with new qualified trust services, including the provision of electronic ledgers.

This action point should cover standardization work to contribute to the common framework to establish trust in electronic ledgers, starting from the EBSI initiative.

A proposal of task

A common framework to contribute to the definition of electronic ledgers as trust services, including the develop technical specifications and cybersecurity standards for DLT in line with the requirements of qualified electronic ledgers.

Contribution to the EBSI initiative, in coordination with relevant projects like EBSI-NE to explore the alignment of EBSI with the requirements of electronic ledgers as a trust service.