NGI ESSIF-LAB

SUBGRANTEE SSI Infrastructure

and business-oriented projects

Projects descriptions

11/08/2022

Grant Agreement No.: 871932
Call: H2020-ICT-2019-2
Topic: ICT-24-2018-2019
Type of action: RIA

Index

Introduction

The NGI eSSIF_Lab initiative has launched four Open Calls since its inception in November 2019.

The first two Open Calls, **the Business-oriented Open Call** and the **Infrastructure-oriented Open Call** were launched at the same time, in March 2020. The Business-oriented Open Call (BOC) was focused on the extension of the eSSIF-Lab basic infrastructure/architecture with business solutions that make it easy for organisations to deploy and/or use SSI; it closed on 7 May 2020 with 54 applications from SMEs providing SSI-related business solutions. Finally, 20 of them were selected to join the Business-oriented Programme.

On the other hand, the Infrastructure-oriented Open Call (IOC), was closed on 29 June 2020 and resulted on 3 programmes. With 36 submitted proposals, from innovators in SSI domain, from 14 countries, 7 of these 36 proposals were selected in the first programme to contribute with open source technical enhancements and SSI Framework extension. The second programme had 7 selected applications, and the third programme had 9 selected SSI-related business solutions.

The **2nd Business-oriented Open Call** was opened on 10 May 2021, and 11 of the most promising projects out of 21 proposals submitted in the open call were selected to join the programme. There were 154 applications started all together, from 27 countries.

An additional Business-oriented Open Call, named "Completing the Framework", aimed at completing and reinforcing the eSSIF-Lab SSI Framework, was directed at SMEs, non-for-profits and research organisations. After a tough competition among overall excellent proposals, eSSIF-LAB selected the 4 most promising proposals out of 42 submitted applications. 161 applications were started altogether, from 22 different countries.

This booklet gives an overview of the 4 Open Calls subgrantee projects started within the infrastructure-oriented and the business-oriented track of eSSIF-Lab.

Selected Completing the Framework Projects

Go Aries! - Enabling CL-Support on Aries Framework Go by Datarella GmbH

The "Go Aries!" project focuses on enabling CL signatures and -credentials within the Aries Framework Go to make it compatible with Aries Cloud Agent Python (ACA-Py) agents and the Indy-SDK. Therefore, the benefits of the Aries Framework Go are accessible to ACA-Py and Indy.

Background and Goals

Hyperledger Aries is the dominant protocol to enable SSI applications. The most popular framework is the ACA-Py which enables cloud-based SSI agents based on Python and is closely entangled with Hyperledger Indy, a purpose-built blockchain as trust anchor. The dominant signature scheme are Camenisch-Lysyanskaya (CL) Signatures to sign and verify DIDs and Anoncreds.

The Aries Framework Go (AfGo) comes more from a ledger-independent approach, which is based on Golang and natively supports JSON-LD credentials and standard support for ec cryptography and BBS+ signatures. Due to its language wrappers, it can be deployed directly on machines which gives it a crucial advantage over the ACA-Py and its corresponding mobile frameworks.

To make machine interaction available to ACA-Py Agents, AfGo agents need to support CL signatures. We want to add support of these signatures to make the Aries Framework Go more complete and allow for new use cases in the ACA-Py ecosystem.

Problem Statement

There are currently two distinct universes within the Hyperledger Aries Framework. The ACA-Py in connection with Hyperledger Indy is already a quite mature agent and trust anchor framework and is the mostly used framework for SSI projects to date. However, it has its limitations as is aimed to be a cloud agent and does not support mobile or other kind of edge agents. Even though the compatible Aries Framework .NET provides a framework for mobile devices it cannot be implemented on standalone devices like car internal computers. This limits the use of the ACA-Py primarily on cloud agent and mobile devices.

The Aries Framework Go comes from a more independent approach and is not tied to a specific ledger. It can be connected to Hyperledger Indy, but comes with a different form of signature schemes which limits today's interoperability between these universes.

In order to have strong interfaces between these frameworks, the Aries Framework Go requires support for CL-signatures.

SICPA's ambition is to build bridges between various technical approaches to facilitate and encourage the adoption of identity systems based on verifiable credentials by citizens, governments, organizations, guaranteeing inclusion for all, avoiding segregation based on technology or providers. Finally, as the holder will have a broad choice of wallets, it will create sound competition and foster innovation.

Solution approach

The project will use the Aries Framework Go as the starting point as this approach ensures high compatibility with existing projects based on the Aries Framework Go and it later allows us to easily provide merge requests. We will rewrite existing components and include CL-Signatures that are required for a well performing Aries Framework Go agent. We will also focus on the new modules Aries Askar, that acts as a new wallet to store key material and credentials, Indy CredX for credential handling, and Indy VDR to store public DIDs. Therefore, our new CL-compatible Go agents would be able to create connections by establishing CL-signed communication channels, anchor public DIDs on Indy, issue, store and verify CL-credentials, and creating and reading revocation registries. Furthermore, this makes the ACA-Py also independent from Hyperledger Indy, as it is possible to connect any ledger as a Verifiable Data Registry. This is a major leap towards completing the SSI framework as it unifies the AfGo with ACA-Py and Indy.

Results

The results will be shown in a demonstrator where an Aries Framework Go agent will create and issue Anoncreds and send it to an Aries Cloud Agent. The repository containing the framework solution itself will be open-sourced.

Country: Germany

Team: Datarella GmbH

Further information: https://datarella.com/

GitLab: https://gitlab.grnet.gr/essif-lab/cfoc/datarella

Infrastructure to facilitate payments for verifiable credentials by Symfoni AS

We aim to provide one essential piece that is missing for uncommitted parties to engage in SSI with enthusiasm: the ability to get paid for sharing valuable insights (verifiable credential) will greatly encourage SSI uptake.

We believe three components are necessary and sufficient.

- Issuers get the means to specify the terms and conditions for sale and verify that a payment has been executed.
- Holders get the means to pay using "programmable money," drawing on a prepay system, or tapping into an escrow account. More commonly, the holder will be able to forward the bill to a verifier.
- Verifiers, typically a service provider seeking business from qualified holders, get the means to deal with the invoice or draw on a partner to facilitate the payment.

To protect privacy, we propose to link payments to the act of issuing (as opposed to presenting or verifying VCs). As a minimum, the logic would need to support most both debit and credit payments, the ability to charge different prices based on urgency and expiry, "invoicing" compliant with account and vat rules, and possibly to deal with refunds and the assistance of third parties to settle a transaction on behalf of all parties involved.

Country: Norway

Team: Symfoni AS

Further information: https://www.symfoni.dev/

GitLab: https://gitlab.grnet.gr/essif-lab/cfoc/symfoni/Symfoni_project_summary

CorpoSign | DID

CorpoSign | DID is an SSI-based authorisation solution for cross-border government and business representatives in logistics developed by Systems Integration Solutions, UAB.

Currently there are no authorization mechanisms in place to link natural persons to organizations in the cross-border logistics ecosystem. Problems arise when the organization and the representative are from different countries, or when the representative refuses to allow the organization to use their personal identity. Furthermore, the lack of such a solution leads in the inability to assure interoperability, security, and fraud prevention. The representative will be able to be authorized via CorpoSign|DID wallet (by issuing him/her verifiable credentials). It will ensure greater governance, security, and interoperability, and will help to accelerate the eCMR development/implementation process.

Country: Lithuania

Team: Systems Integration Solutions, UAB

Further information: https://essif.sis.lt/credentials

GitLab: https://gitlab.grnet.gr/essif-lab/cfoc/sisuab/SISUAB_project_summary

Product Circularity Data Sheets Digital Passport (PCDS-DP) by Compellio

The Product Circularity Data Sheets Digital Passport (PCDS-DP) is a trusted accountability system delivering decentralized verification to businesses and auditors in circular supply chains.
With PCDS-DP, Compellio enhances trust and accountability within the PCDS ecosystem by building blockchain-enabled verifiable data and verifiable credentials that leverage SSI components to ensure trusted authentication, auditability, and data access services in Europe and beyond.

Driven by the Luxembourg Ministry of the Economy and supported by major international industry leaders, the PCDS initiative addresses the difficulty for industry and consumers to access reliable data on the circular properties of a product. For each product, an internationally accepted dataset will describe all relevant information in controlled and auditable statements, helping the consumer and manufacturer to make educated choices, increasing the value of the product and enabling future uses in a circular economy. Since its inception, more than 50 companies from 12 different European countries, including global industry leaders, have joined the initiative.

Country: Luxembourg

Team: Compellio S.A.

Further information: https://compell.io/

GitLab: https://gitlab.grnet.gr/essif-lab/cfoc/comp/Compellio_project_summary

Subgrantee Infrastructure-oriented Projects

Sicpa: Bridge project

BRIDGE for ledger-agnostic interoperable issuance and verification of W3C verifiable credentials

SICPA proposes three technological building blocks that will enhance interoperability and scalability by giving freedom of choice between verifiable credentials exchange protocols, credential types, and DID-methods.

Indeed, companies will be able to select the best technical option for their ecosystem and use-case, knowing that the issued credentials will be broadly compatible with all wallets and therefore saving development and operational costs. Thus, verifiable credentials exchange and verification will be greatly facilitated and scalable.

SICPA's ambition is to build bridges between various technical approaches to facilitate and encourage the adoption of identity systems based on verifiable credentials by citizens, governments, organizations, guaranteeing inclusion for all, avoiding segregation based on technology or providers. Finally, as the holder will have a broad choice of wallets, it will create sound competition and foster innovation.

Country: Spain

Team: SICPA Spain S.L.U.

Further information: https://sicpa.com

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure/sicpa/bridge_project_summary

Jolocom: Capability-Based Authorization System

A capabilities-based authorization system, utilizing DIDs, Verifiable Credentials, Verifiable Presentations, etc.

The proposed SSI component is an implementation of a capabilities-based authorization system, utilizing DIDs, Verifiable Credentials, Verifiable Presentations, DID Comm (or JSON Web Messages), etc.

Jolocom believes that numerous relevant use cases (e.g. delegation, complex authorization logic, automated operations, etc.) can be simplified given a simple and extendible way to define and communicate credentials encoding object capabilities.

The intention is to focus on developing a usable implementation (alongside an open-source reference integration with the Jolocom SmartWallet and Jolocom Library) and avoid defining new standards wherever possible.

Jolocom intends to align the development efforts with emerging standardization efforts, most notably the Authentic Chained Data Container task force active in the Trust Over Ip Foundation.

Country: Germany

Team: Jolocom GmbH.

Further information: https://jolocom.io/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure/jolocom/cbas_project_summary

FRAUNHOFER IAO: ESSIF-TRAIN

TRAIN (TRust mAnagement INfrastructure): Trust Management Infrastructure Component for the ESSIF-Lab Architecture.

eSSIF-TRAIN aims to extend the ESSIF-Framework through a global trust infrastructure that can be used to verify the trustworthiness of involved parties in an electronic transaction. The trust layer enables actors using the ESSIF-Framework to verify the root of trust of certificates used to sign credentials.

In addition, the component allows for the definition, consideration, and verification of Trust Schemes compliance (e.g. eIDAS including LoAs or other Trust Schemes that can also be application/industry-specific) of involved parties. It is not dependent on a hierarchical CA infrastructure.

The component builds on the infrastructure developed in the EU project LIGHTest (2016-2020, G.A. No. 700321). The trust layer is flexible, individual parties can define their own trust policies, manage and publish them. TRAIN is fully in line with the open and decentral SSI approach and complements other approaches.

The trust management architecture that is made possible by TRAIN enables secure, trustable digital interactions. At the same time a classical hierarchical CA-type structure is avoided – so is fraud, chaos and the pure dominance of the economically strongest actors in the system.

Individuals or groups (industry organizations, NGOs, etc.) of validators can define for themselves the trust standards they require. Issuers can publish to what standards they comply. The system is open, but standards for trust are transparent, as the Trust Schemes and Lists can be published.

Country: Germany

Team: Fraunhofer IAO (Project Lead) and University of Stuttgart IA

Further information: https://www.hci.iao.fraunhofer.de/de/identity-management.html

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure/fraunhofer/train_project_summary

Evernym UK: Evernym Open Sourcing Project

Open sourcing Evernym's credential exchange platform.

Evernym has a history of open sourcing their work. Until now, they have kept the top layer of their SSI architecture proprietary. This layer provides a much easier to use SDK and platform for developers to create compelling SSI deployments compared to the lower level Hyperledger Indy/Ursa/Aries stack.

Evernym wants to encourage anyone to develop SSI solutions. For this reason, they will use ESSIF-Lab support to convert their proprietary software into repositories covered by a business source license, which itself will convert to an open-source Apache 2.0 license after 36 months. This will enable anyone to use and develop on their code, with all non-production use permitted as well as production use up to a limit.

We believe this will accelerate SSI adoption, removing technical and commercial barriers to entry, by providing the world with access to the best SSI technology available.

Evernym's products that are the target of this open sourcing initiative cover enterprise and consumer uses:

- Verity: the enterprise SSI SDK and server to operate on-premises or as Saas. This performs all enterprise functions that are needed in an SSI ecosystem including forming DID connections, authentication, credential issuance and verification.
- Mobile SDK: the app SDK to allow anyone to build Android or iOS-based apps with full SSI wallet functionality.
- Connect.Me: the mobile app that provides SSI wallet capability for making DID connections, holding credentials and sending proofs.

Country: United Kingdom

Team: Evernym UK Ltd.

Further information: https://www.evernym.com/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure/evernym/openup_project_summary

Ubicua: Self-Sovereign IDentity Online

Online passwordless authentication based on SSI and FIDO2

Self-Sovereign IDentity Online (SSIDO) is an online passwordless solution for SSI users' authentication through the standard Fast IDentity Online (FIDO2) protocols. SSIDO is aimed at consolidating both two technologies related to the Identity and Access Management (IAM). As a result, emerging SSI-enabled solutions can be seamlessly integrated with the existing FIDO2 applications. The proposed solution provides a high level of identity assurance and serves as a basis of trust in decentralized ecosystems.

The Web Authentication ceremony begins at the Application Layer between a user (Holder) and a Relying Party (Verifier) and implies an authentication assertion about the presence and consent of that previously registered user using the Public Key Infrastructure (PKI). SSIDO extends the traditional PKI-based approach by introducing the Decentralized Public Key Infrastructure (DPKI) built upon the concepts of SSI, such as Distributed Ledger, Wallet, Agent and DID Record (DID and DID Document). To proceed with the Authentication ceremony at the Agent Layer, SSIDO incorporates the following two components:

- SSIDO Authenticator, an edge-side agent (Holder's Agent) designed for both mobile devices and desktop environments.
- SSIDO Validator, a server-side or cloud-side agent (Verifier's Agent).

SSI Authenticator responds to a challenge generated by SSI Validator with the assertion signed by the user's private key. While attesting the received assertion, SSI Validator employs the user's public key retrieved from the DID Document.

The SSIDO solution is compatible with different schemes of verifiable credentials and verifiable presentations, and it can be generalized on Multi-Factor Authentication (MFA).

Country: Spain

Team: UBICUA S.L.

Further information: https://www.ubicua.com/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure/ubicua/ssido_project_summary

Validated ID: SSI eIDAS Bridge

An eIDAS bridge, which is a component that proposes to enhance the legal certainty of any class of verifiable credentials

The eIDAS bridge is a component that proposes to enhance the legal certainty of any class of verifiable credential, by incorporating the issuer's advanced or qualified electronic signature (if the issuer is a natural person) or seal (if the issuer is a legal person).

Basically, it allows Issuers to issue credentials that incorporate the issuer's advanced or qualified electronic signature (if the issuer is a natural person) or seal (if the issuer is a legal person).

Trustworthiness in a Verifiable Credential is linked to the issuer's DID: Verifying the identity of the issuer is paramount, since there is no binding of a DID to a real-world natural or legal person per se.

The main role of the eIDAS Bridge is to assist:

- issuers, in the process of signing/sealing a verifiable credential, and
- verifiers, in the last mile of the verification process, to help identifying the natural or legal person behind an issuer's DID.

Its functions are:

- assist in setting up the Issuer's qualified certificate.
- assist in signing or sealing Verifiable Credentials with the private key of a qualified certificate.
- assist in the verification process of a Verifiable Credential to retrieve the Qualified Certificate and verify it against the EU Trusted Lists.

Country: Spain

Team: Validated ID S.L.

Further information: https://www.validatedid.com/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure/validated-id/seb_project_summary

NYM: Verifiable Credential Authority

A DLT/blockchain independent platform to Issue and Verify certified attributes and claims, under different formats, and for any SSI system

With the introduction of notified eID schemas, thanks to eIDAS regulation, Europe made a big step forward in the identity management interoperability field. Yet these systems rely on centralized standard models and protocols (SAML being the most spread).

The enrichment of identity attribute with other types of attestations and claims, as of today, remains an unfulfilled promise: Federated Identity Model, upon which the whole eID system is based, isn't enough agile to let new player come in and provide certified attributes services.

Italy is one of the main exemplifications: tough systems like SPID and CIE are gradually taking over the eID scenario, Attribute authorities, which should have provided attributes and claims about identities are, as of today, completely absent.

With the advent of SSI, we have an extraordinary opportunity to deploy new technology standards to enrich eID: verifiable credential. Yet, we need to perfectly fit the regulatory trust model while still being compliant to eIDAS schemes.

But still SSI is a very complicated subject, both from the theoretical and technical point of view, mainly because it requires a deep understanding of blockchain and cryptography concepts.

Further on, each SSI project tends to propose its own solution as a closed platform, with no particular attention to interoperability and blockchain-independent solution approach.

Country: Italy

Team: NYM S.r.l.

Further information: https://www.nymlab.it/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure/nym-srl/vca_project_summary

Verifier Universal Interface (VUI)

Verifier Universal Interface (VUI) is an interoperability working group that aims at building a complete set of standard APIs for Verifier components in SSI ecosystems.

As different technology providers build SSI solutions, it becomes critical to ensure interoperability between these solutions. Available standards for SSI still have important gaps, leading us to an ecosystem of full-stack providers whose approach to interoperability is building proprietary plug-ins for each one of the other available solutions. This approach to interoperability is not scalable. The underlying problem is that building standards take time. That is the reason that we launched a practical and focused approach to enable scalable interoperability in the SSI community.

GATACA proposed the SSI community to start with a specific SSI component, namely the Verifier component, and lead the definition of the minimum set of standard APIs necessary to implement or interoperate with such module. That is a role-centric approach to standardization at the API level.

VUI identified a minimum set of 6 APIs to offer an end-to-end credential verification flow.

- DID resolution
- Status resolution
- Data agreements
- Presentation exchange
- Issuer resolution
- Schema resolution

Under the eSSIF Lab program, GATACA led an interoperability group of 12 organizations that contributed to this initiative.

RESULTS

The results of these efforts included specifications built on ReSpec, API swaggers, and an open-source library that organizations can use to easily implement these APIs. These resources can be found in the following links:

- Verifiable Universal Interface Specification: https://identity.foundation/vui/
- Data Agreements: https://identity.foundation/vui/dataAgreements
- Presentation Exchange: https://identity.foundation/vui/presentationExchange
- Issuer Resolution: https://identity.foundation/vui/issuerResolution

API Swaggers

- Presentation Exchange & Data Agreements:
  https://gataca-io.github.io/vui-core/issuerResolution.html
- Issuer resolution: https://gataca-io.github.io/vui-core/

VUI-core library -

- Consists of an open-source library that implements the above-mentioned APIs. While they do not obtain the complete functionality of a verifier, they offer the core implementation of these APIs. https://github.com/gataca-io/vui-core

NEXT STEPS

The VUI initiative has been steadily gaining international traction. It was recently mentioned in a report published by the European Commission (DG Connect) and the Canadian Innovation, Science and Economic Development Canada, (ISED) , as a key global interoperability approach to explore.

Its work was in early 2022 donated to the Decentralized Identity foundation to ensure the contribution of a broader community for the maturity of the Data Agreement, Presentation Exchange, and Issuer Resolution APIs, and the launch of the Schema resolution API

For more information on how to join the group as an implementor or integrator, please reach out to us directly at vui@groups.io or just subscribe to our communication list to keep updated on the latest news by sending an email to vui+subscribe@groups.io.

Country: Spain

Team: https://gataca.io

Further information: Gataca Spain

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_2/gataca

iGrant.io

iGrant.io is an SSI enabled consented data exchange platform with auditable data agreements, helping organisations unlock the value of personal data. In the Automated Data Agreement (ADA) project, we accelerate SSI adoption by connecting Data Agreements to a legally endorsed Data Protection Impact Analysis (DPIA), automating the flow from DPIA to SSI workflow. This ensures that any company adopting SSI for data exchange has a highly auditable solution where any data agreement receipt can be substantiated by a code of conduct to the originating DPIA performed.

The project aims to standardize data agreement schemas and receipts (Consent being one type of data agreement) and a component that standardizes the process and decision tree to populate the verifiable credential and remove the pain point from organisations related to data regulatory compliance. In addition, it addresses the challenges with delegated consents.

The key value propositions offered by the iGrant.io platform are:

- Automated compliance, by reducing the risk of non-compliance to data regulation when it comes to personal data usage, for example by linking Data Agreements to a legally endorsed DPIA process.
- Improved access to high quality personal data by providing transparency and empowering users to control data usage.
- SSI enabled personal data exchange where companies can leverage personal data assets legally for advanced personalisation.
- End-user SDKs (e.g. Data Wallets, User preference center) that can be embedded into existing mobile applications and portals.

As a certified MyData Operator, iGrant.io also drives interoperability via the MyData community as well as Trust-Over-iP.

Country: Sweden

Team: https://igrant.io/

Further information: support@igrant.io

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_2/igrantio

Sphereon

Sphereon as part of its Vindicatio project brings the new DIF Presentation Exchange to DIF/W3C SSI solutions compatible with Aries Present Proof Protocol v2 using a layered approach to achieve both integration and interoperability.

At the lowest layers there are TypeScript (Javascript) libraries for the rules engine component, validations and logic. These libraries are easy to integrate in other projects for both web and mobile. The models and a REST API are also exposed using an OpenApi specification close to the VCC HTTP API as well as Sphereon's own implementation. The models can be generated to a programming language of choice.

The REST Api and state machine can run in Docker and exposes the functionality to other programming languages for a more direct integration. Then there is a stateful bridge that integrates DIDComm v2 and CHAPI (and future OpenID-Connect). The bridge will be similar to Aries Present Proof v2 and integrate with it and in the future support a backend like Verity or similar as well. This means parties can talk using Presentation Exchange compatible datastructures, across different transports and with different products.

Country: Netherlands

Team: https://sphereon.com

Further information: Sphereon B.V.

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_2/sphereon

walt.id

Walt.id offers the Wallet Kit, an open source infrastructure for consumer and enterprise wallets. The Wallet Kit is used by developers, public authorities and enterprises to extend their existing apps with holistic (self-sovereign) identity capabilities. (There is also a progressive web app that can be whitelabelled, if users do not yet have a web or mobile app.)

The Wallet Kit is fully open source (Apache 2) based on open standards (e.g. W3C, DIF, OpenID Foundation, ESSIF) and supports a quickly growing number of digital identity ecosystems (e.g. EBSI, Gaia-X, Velocity Network, IOTA, Ethereum/EVM-chains, ...). You can learn more here.

The Company

Walt.id offers open source identity and NFT infrastructure used by thousands of developers as well as governments, public authorities, DAOs and enterprises across industries.

The Mission

We enable developers to build ownership, identity and trust into the web.

Contact

Get in touch here or via mail: office@walt.id

Country: Austria

Team: https://walt.id/about

Further information: https://walt.id

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_2/letstrust

SSI Java Libraries

Danube Tech has been building SSI technologies and solutions for several years, for example by launching the Universal Resolver open-source project at DIF, or by participating in the eSSIF-Lab Business call, where we worked on a SaaS platform for creating and resolving DIDs. In these various efforts, we have consistently relied on a set of basic open-source components that implement DIDs, Verifiable Credentials, and related building blocks for the SSI ecosystem. These independently implemented components include jsonld-common-java, did-common-java, ld-signatures-java, verifiable-credentials-java, key-formats-java. All of them need more work in several areas, and additional components are currently being planned. In this project, we will improve and complete these libraries, which will result in the availability of a high-quality and generic set of open-source Java components for higher-level SSI applications

Country: Austria

Team: https://danubetech.com

Further information: Danube Tech GmbH

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_2/danubetech

Associazione Blockchain Italia

NGI ESSIF-LAB

WordPreSSI

WordPreSSI is an authentication plugin enabling ESSIF/SSI Verifiable Credentials for logging into WordPress sites.

In order to encourage adoption of SSI among users, we believe that some bridges are needed between the old and the new way of handling identities. In this context the importance of our project lies in its relevant social impact as WordPress currently powers 39% of websites at global level.

Beside scalability, WordPreSSI:

- give back to users the control over their own data, ensuring a privacy-by design decentralized passwordless login system and enabling simpler and more secure Internet transactions: users will login minimizing the sharing of personal data and without relying on centralized parties for storage and management.
- significantly increase security for all WordPress sites. With the current system, all the WordPress sites have repository of usernames and password, which are subject to serious risk of hacking. With our plugin, passwords will no longer be stored on the servers as credentials are passed at the start of user sessions via VC. In addition, we give the option to webmasters to requests, via a claim at login, a key which is held only by the user in its wallet to decrypt server-side user data during the user session only (data-at-rest encryption).
- will give the community of open source developers the opportunity to extend the plugin with other functionalities.

Country: Italy

Team: Associazione Blockchain Italia

Further information: https://associazioneblockchain.it

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_2/blockchain-italia

GIMLY

NGI ESSIF-LAB

SSI-NFC bridge: tap to id, verify and access.

Gimly ID is a self-sovereign identity and data solution that bridges the digital and physical realities of our world. Through the use of NFC technology we enable secure access management to digital systems and physical environments by the tap of a mobile phone or a secure NFC smartcard.

Thereby, we can leverage the high security and privacy preserving benefits of SSI in mobile-first experiences as well as use cases where personal devices are not allowed, not practical, or not available. Example use cases may include access management in hotels and accommodations, private health records, eID cards with eIDAS compliant signatures, eMobility, or enterprise employee authorisations, access management, and transactions.

Within the essif-lab, Gimly has built an open-source SDK to implement SSI smart cards as physical identifiers in SSI solutions. The SSI card is designed blockchain and did-method agnostic to allow for easy integration of SSI smartcards in any SSI solution. The smartcards hold an NFC microchip with an EAL6+ grade secure element for authentication and signing with their embedded DID and can be used for sovereign storage and selective disclosure of verifiable credentials.

Visit gimly.io to learn more about our work on SSI over NFC and request a demo.

Country: Netherlands

Team: https://gimly.io

Further information: Gimly

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_2/gimly

Netis - Authority Delegation & Verifiable Mandates

With this project, we will address the SSI aspect of Authority Delegation (AD) or Verifiable Mandates (VM) – as referred within EBSI/ESSIF. VM are fundamental for the broad adoption of SSI by businesses (e.g. mandate employees) & individuals (e.g. parents representing children). However, there are no detailed governance frameworks and outlined process flows, which cover the VMs, particularly no solutions aligned with ESSIF as well as legacy frameworks like eIDAS. Furthermore, there are no viable tech solutions for it, which would enable simple usage.

Our innovation will be multi-fold and will contribute to 1) the governance of authority delegations (AD), 2) with defined models, schemas, as well as 3) a technical solution. The latter will be a library, which will enable the core functions for ADs (secure and user-friendly management of ADs in the form of VCs) and which will be usable in other IT solutions (e.g. android mobile wallet, java-based enterprise wallets). We will build on the "LetsTrust.org" (SSI Fabric GmbH) library, which already supports the core SSI functionalities & is EBSI/ESSIF compliant. The lib provides OSS SDKs & libraries in Java/Kotlin. Furthermore, we will demonstrate the innovation of SSI cloud-based enterprise & consumer edge agents. For the former we will build on the Blockchain Lab:UM's SSI Enterprise Agent also used within the DE4A (EBSI Early Adopter). It is a deployable java-based solution incorporating HL Aries (Go). For the consumer edge agent we will build on Netis's user wallet.

Country: Slovenia

Team: Netis

Further information: https://netis.si/en/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_3/netis

TRAIN extension into trust registry

SSI-powered interactions need to be trustworthy and safe for all participants in order to achieve widespread adoption. In addition to technical assurance through cryptography, human trust must be achieved through governance. These capabilities must usable offline, transparent to wallet holders, and configurable by enterprises. Trust Registries are one of the critical components of machine-readable governance frameworks. Through this component, holders can avoid coercion by verifying the verifier; verifiers can discern offline which issuers they trust; issuers can communicate to holders which governance framework they are associated with. It will lead to additional safety and confidence for all participants.

In order to address this problem, Trust Registries offer a way for these parties to utilize the benefits of this network, but also provide means for them to build their own trust network on top of the open system. It's the network within a network principle.

Trust Registries solve this problem by using the open SSI infrastructure, while providing a central authority to extend it with its own governance mechanism. This is done by adding technical solutions that leverage decentralized systems, such as identifier PKIs, decentralized storage, blockchains. In the form of open or secured API's, governing authorities can provide a central registrar of trusted participants, publish governance framework and allow entities to use this service to check if other parties are authorized to issue and verify given credentials.

Country: United Kingdom

Team: Trinsic

Further information: https://trinsic.id/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_3/trinsic

Enabling Zero Trust Architectures w/ OAuth2.0

Enabling Zero Trust Architectures using OAuth2.0 and Verifiable Credentials (ZeroTrustVC) implements Authentication and Authorization for HTTP-based resources using JWT-encoded Verifiable Credentials.

ZeroTrustVC provides an HTTP proxy that intercepts the communication between a client application and the protected resource. This HTTP proxy is configured with a set of "rules" used for validating a VC. Client applications initiate a session with a protected resource (through the proxy) by including in the appropriate HTTP header: (i) the received credential, and (ii) a proof of possession. The HTTP proxy validates the VC based on the pre-configured rules and it verifies the proof of possession. If all checks succeed the session is initiated and all subsequent requests are forwarded to the protected resource.

ZeroTrustVC also enables authorization servers to provide an efficient and privacy preserving revocation mechanism. This revocation mechanism includes a compact list of revoked VCs. At any point, any entity can verify the status of a VC.

Country: Greece

Team:

Further information:

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_3/aue-brc

ANIMO - Aries Mobile SDK for React Native

The Aries Mobile SDK is a complete toolkit for cross-platform iOS and Android development using React Native. With this one SDK, developers can build mobile SSI solutions for any use case. The SDK contains reusable issuer, holder and verifier components as well as essential components for mobile development (e.g. deep linking, state management, biometric wallet unlocking). Developers can either start from scratch or integrate a selection of components into their existing mobile app. The Aries Mobile SDK is credential format and DID method agnostic, it uses the latest open standards to break out of the Indy & Aries ecosystem (e.g. W3C VCs, DIF PE, BBS+ Signatures).

The Aries Mobile SDK is 100% open-source, focuses on interoperability and open standards and is accessible for developers of any skill level. It aims to drastically lower the barrier of mobile SSI development.

Country: Netherlands

Team: Animo

Further information: https://animo.id

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_3/animo-solutions

UBITECH - Hardware Roots of Trust

DOOR - Hardware Roots of Trust as an Enabler of Trustworthiness in Digital Transactions

We achieve the above goal by providing a new component on the Holder side that enables the use of hardware-based keys and offers the possibility to bind Verifiable Credentials (VCs) to the wallet of the holder. This process, referred to as Device Binding, creates a differential security model by anchoring a hardware-generated secrete key to the credential. To enable this functionality we leverage Direct Anonymous Attestation (DAA) for ensuring the following properties:

- Proof of Knowledge: Proof that the wallet that produced the VC belongs to the intended holder, thus, ensuring that the presented VC really belongs to the claimed entity;
- Proof of Integrity: Proof that the holder device (where the wallet resides) has not been compromised when producing a VC or a subsequent Verifiable Presentation selectively disclosing some attributes; and,
- Proof of Unforgeability: Proof that a produced Verifiable Presentation is presented by the correct holder to whom the VC was issued;

In this way, we transfer the root of trust of the SSI ecosystem purely on the digital wallet by considering an underlying Trusted Component as part of the wallet, without making any assumptions on the trustworthiness of the other layers.

We achieve the above goal by providing a new component on the Holder side that enables the use of hardware-based keys and offers the possibility to bind Verifiable Credentials (VCs) to the wallet of the holder. In this way, we transfer the root of trust of the SSI ecosystem purely on the digital wallet by considering an underlying Trusted Component as part of the wallet, without making any assumptions on the trustworthiness of the other layers.

Country: Greece, United Kingdome, Germany

Team: Ubitech

Further information: https://ubitech.eu/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_3/gioumpitek

Download the code here: https://github.com/Door-project

Human Colossus Foundation - Decentralised Key Management Infrastructure 4 SSI

A Decentralised Key Management Infrastructure (DKMI) is essential to any SSI implementation. DKMI is the cryptographic infrastructure upon which the necessary authentication keys are exchanged between SSI actors. In 2020, a new type of ultra-secure, ledger-agnostic DKMI made its way through the SSI community: Key Event Receipt Infrastructure (KERI). Currently being standardised at IETF (The Internet Engineering Task Force), KERI is making its first appearance in real-world applications as the first truly and fully decentralised identity system.

With KERI components, developers of SSI solutions will be able to:

- operate between blockchain and non-blockchain networks and ledgers using self-certified identifiers
- delegate self-certified identifiers to other identities regardless of the network or system of their creation
- provide key provenance logs for production-ready Verifiable Credential management
- enable key recovery through pre-rotation events
- use self-certified identifiers at scale with resolution through Distributed Hash Tables
- utilise algorithms without relying on centralised resolvers or networks
- operate any type of Verifiable Credential across networks

Country: Switzerland

Team: Human Colossus Foundation

Further information: https://humancolossus.foundation/

GitLab: https://gitlab.grnet.gr/essif-lab/inf rastructure_3/humancolossus

OnboardSSI

Public and private organisation undergo digital transformation that has been speed up with the effects of COVID-19, creating a shift towards offering the majority of services online. However, this has created also a geometrical increase in identity fraud and account takeover. According to Experian, during COVID-19 lockdown there was a 33% increase in fraud rates. The Federal Trade Commission received 650,570 identity theft complaints in 2019, 46 percent increase from the previous year.

SSI constitutes a well-promising approach for tacking the increase in identity fraud and account takeover. However, existing wallets do not provide the ability for users to easily onboard their existing identity documents such as passport to SSI as there are only proprietary solutions available introducing unbearable costs. Existing user onboarding solutions fall short in four ways:

1 The costs for the organisation to purchase such solution are huge; up to $2 per user onboarding and $0.12 per liveness detection.
2 Not privacy-preserving and no transparency about the data collection/processing on the cloud. There is no open-source solution for organisations to adopt and integrate, forcing organisations to vendor lock-in.
3 The majority of them lack security as they do not offer remote identity verification with High Level of Assurance based on eIDAS regulation.
4 In several cases the onboarding process fails, creating huge frustration to users, leading to an increase of the abandonment rate and the need to maintain an in-house operations team to address these failures.

The concept of SSI was designed with the citizen and privacy in mind. However, existing implementations lack user-friendliness (e.g. showing hash codes to users), creating potential barriers in users' adoption. OnboardSSI focuses on providing a secure and user-friendly wallet solution creating an easier way for citizens to manage their identity. OnboardSSI will leverage AI to remotely verify users' identity, without human validator intervention, and creating verifiable credentials.

Country: United Kingdom

Team: OnboardSSI

Further information: https://www.quadible.co.uk

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_3/quadible

Visma Connect

The current digital infrastructure for mandates is not without problems. In many cases providing a mandate digitally isn't even possible and those systems around mostly still require a wet signature on a PDF which can easily be falsified. The digital systems out there are fragmented and siloed between various service providers with a poor user experience. As a result people share their passwords rather than actually providing mandates resulting in insecure systems. To make matters worse most people use similar passwords for different systems increasing the attack vectors to compromise the identity and as a result also the identity of the person providing a mandate.

By providing mandates using SSI we can provide a solution to the problems mentioned above.

The SSI mandate service is a generic and holistic approach to provide and request mandates. Mandates are SSI credentials signed by the dependent that can be requested by either the dependent or authorized representative. These credentials can be used to prove to a verifier that the authorized representative is authorized to act for specific actions on behalf of the dependent. The mandate credentials are stored in the wallet of the authorized representative as opposed to a central database in current systems. The dependent can revoke this credential at any point in time if he/she no longer wants the authorized representative to act on their behalf by updating a revocation hash on the blockchain. The SSI mandate provides mandates completely peer to peer and isn't limited to individuals only. A SSI wallet can also represent a device or institution, for example a company can use a SSI company wallet to authorize employee's to access the building or use the company credit card up to a certain amount.

Country: Netherlands

Team: Mandate SSI

Further information: https://www.visma.nl/connect/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_3/visma-connect

Bloqzone

One of the things people enjoy the most about the internet, is that it enables them to talk to others remotely almost without limit.
Unfortunately, remotely often means that parties are not sure who they are communicating with. Think of the epidemic of robocalls and prank calls the telecoms industry has been battling for years, or you yourself simply trying to video conference with your bank: the absence of an identity layer can be a huge problem.
Adding SSI to internet communications resulting in seamless identified communications is the solution to this problem. It enables people engaging in any form of internet communication to exchange presentation requests and proofs, and communicate at the same time.

Dedicated to identified communications, Dutch startup and initiator of the SSIComms project Bloqzone (bloqzone.com) has built several solutions to this problem in the past using more standard local identity solutions such as DIGID and IDIN. Unfortunately, these sofar tended to result in a somewhat awkward customer experience since the end user has to switch between multiple applications during one session.
A more thorough approach is therefore needed where not only one application is able to handle both communications sessions and identity sessions, but also where both communications and SSI protocols are interwoven.

The project SSIComms adds SSI to internet communications by adding SSI wallets to the renowned SYLK Suite, an award winning ensemble of communications solutions. In terms of protocols, SSIComms connects the open standard SIP on the internet communications side to the open standard DIDComm messaging on the SSI side. This enables users to respond to presentation requests for credentials entirely voluntarily and according to SSI principles during communications sessions.

Country: Netherlands

Team: Bloqzone

Further information: https://bloqzone.com/

GitLab: https://gitlab.grnet.gr/essif-lab/infrastructure_2/blockchain-italia

SUBGRANTEE BUSINESS-ORIENTED PROJECTS

NGI ESSIF-LAB

Verifiable Credentials: User-friendly Magement Interface for Verifier Policies

This project will develop for eSSIF a policy management tool that will allow resource owners e.g. web sites, hotels, etc. to easily specify, in their own controlled natural language, which VCs they require from users in order for the users to access their resources.

Different policies can be specified for each resource, so for example, each web page at a web site could have a different policy, or different rooms in a hotel could have different policies. The policies are specified by the administrator in controlled natural language (CNL) and the administrator will configure the locale of their web browser to their own language. Example GUIs in several different European languages will be demonstrated. The policies can be specified using either disjunctive normal form or disjunctive normal form so that any conceivable policy can be constructed by the administrator. The CNL will be converted into machine readable JSON and processed by the holder's verifiable credential wallet to select the VCs that match the verifier's policy. The verifier will check that the returned verifiable presentation contains VCs that match its policy.

Country: United Kingdom

Team: Verifiable Credentials Ltd.

Further information: https://verifiablecredentials.info/

GitLab: https://gitlab.grnet.gr/essif-lab/business/policyman/policyman_project_summary

UNIKK.ME: TRUSTED DIGITAL AGENT

Every individual has the fundamental right to control their data rights including their identity. This project enables parties to transform their applications, so they become trusted digital agents (TDAs) catering for safety and protection, convenience and benefits for every individual and organisation.

The project aims to transform any organisation's application(s) using Self-Sovereign Identity (SSI) and other Data Operator services as defined by MyData. The SSI technology provides real-time data exchange capabilities for the individual's Data Wallet provided by the TDA, using data from multiple Data Sources. The SSI brings in decentralized application capabilities within the Data Operator framework. This enables the individual to be a Data Source and exchange consented personal data from their wallet with a Data Using Service. The Data Using Service can verify this data authenticity independently as well. In this project, we design and develop ready-to-use services and toolkits for any organisation to transform their application to a TDA. The toolkit includes, mobile Software Development Kits (SDKs), extending the current hyperledger Indy/Aries software with a consent lifecycle. With the TDA add-on, the organisation can become a trusted entity while continuing to provide advanced user experience. We reuse the data operator service stack as described by MyData to provide the services required for a TDA to offer a fully-fledged, data regulatory compliant, service. The solution also supports human centric services provided, under the governance of the TDA, by a third party.

Our target contribution to eSSIF-Lab is to reduce barriers for developers (and the businesses they serve) via a reference implementation and advocate standards that be developed and adopted by various stakeholders. Thus, the SDKs, the reference implementation and the consent lifecycle design will be key assets for eSSIF-Lab stakeholders and subgrantees, as well as basis for the interoperability work in the SSI ecosystem and beyond.

Country: Denmark

Team: unikk.me (in cooperation with Grant.io)

Further information: https://www.unikk.me/

GitLab: https://gitlab.grnet.gr/essif-lab/business/tda/tda_project_summary

Human Colossus Foundation: Dynamic Search Engine with Consent Flow

This engine brings SSI benefits to the broader economy by enabling a privacy-preserving complete data lifecycle, including consent.

The concept of the Dynamic Search Engine(DSE) eSSIF-lab project was born from the Human Colossus Foundation's experience in the pharmaceutical sector, where the exchange of extensive and sensitive data has driven complexity and costs to unprecedented levels in clinical trials.
With personal patient data involved in the transaction flows, adding privacy continues to slow innovation as governing authorities administer more complex compliance and data protection regulations, increasing costs and liabilities for all stakeholders.

The DSE project, designed with decentralisation, privacy and consent at its core, starts with a Data Capture Hub (DCH) where data is captured in a harmonised state, ready for secondary data sharing.
Once the data subject has given consent and all flagged data has been encrypted (or removed), engaged participants can share data across multiple stakeholders through a Data Sharing Engine(DSE).

The DSEproject provides the necessary components for an SSI-based data sharing flow compliant with the eSSIF-Lab architecture. Although the project focused on the healthcare vertical, the implementation described is fractal and not limited to a specific sector.

Country: Switzerland

Team: The Human Colossus Foundation

Further information: https://humancolossus.foundation/

GitLab: https://gitlab.grnet.gr/essif-lab/business/SSISharing/data-sharing-hub

RESONATE BEYOND STREAMING: COMMUNITY CREDENTIALS

An open-source Discourse plugin that allows community-friendly transparent recognition, award and governance of verifiable credentials as represented by user-friendly 'badges'.

Simple agreements may be formed in a forum discussion and sealed in a 'digital handshake' between verified human vc/badge holders:

- verifiable credentials mapped as 'proven capability' badges
- portable 'badge' credentials, exported and verifiable across communities. For example, as a low-cost mutualised 'commons' for trusted co-operative membership, making it easier for members to join, reducing the cost of KYC, and improving security without relying on centralised identity providers.
- simple 'digital handshake' VC- backed agreements between parties, verified access to protected services, such as licencing agreements, ticketing, gig entry and third-party fulfilment.

Country: Ireland

Team: Resonate Beyond Streaming Ltd.

Further information: https://resonate.is/

GitLab:
https://gitlab.grnet.gr/essif-lab/business/iris-dcc/open_source_community_credentials_project_summary

Off-Blocks: Digital ID and Signatures for Businesses and Organisations

Onboarding businesses and organizations in a self-sovereign world through user-friendly and low-cost control over trusted digital identities, verified credentials and digital signatures

OBDID is a platform for digital agreements and transactions between people and businesses. Re-imagining the way we transact using verifiable credentials improves upon legacy competition in a number of ways, whilst vastly expanding the scope of signatures beyond only documents.

This project initially focusses on applying SSI technology to traditional use cases - requesting and tracking signed agreements, data, and forms whilst complying with current eIDAS guidelines. Either remotely, or in-person; bridging the gap between the physical and digital worlds.

In addition to this business approach, the technological approach seeks to provide standardized SSI components that are usable in every SSI solution. This lays the groundwork for core functionalities such as enabling the resolution of identities, as well as the issuing, exchanging, and verification of credentials.

Country: United Kingdom

Team: Off-Blocks Ltd.

Further information: https://www.off-blocks.com/

GitLab: https://gitlab.grnet.gr/essif-lab/business/obdid/project-summary

NYM

NGI ESSIF-LAB

Nym Technologies: NYM Credentials for Self-Sovereign Identity

A bulletin-board and search system for privacy-enhanced services.

This project aims at creating a public "bulletin board" that lists Nym-enabled SSI services and a search facility to allow users to search through the kinds of services they may want.

Country: Switzerland

Team: NYM Technologies SA

Further information: https://nymtech.net/

GitLab: https://gitlab.grnet.gr/essif-lab/business/nym-cssi/cssi_project_summary

NYM: Gaya

Supports public notaries to remotely incorporate Limited Liability Company, providing all the tools they need to apply digital transformation to their business.

GAYA is the solution that allows public notaries (and other professionals and companies) to digitize the process of making agreements remotely, granting the same features of de visu meetings in terms of recognition, easy signing and event control.

GAYA leverages SSI protocols in order to:

- promote the role of professionals (such as notaries) as issuers of verifiable credentials
- ease the process of Identity Verification and Power of acting on behalf of a company by its users

GAYA solution pillars are:

- identification, via Verifiable Credential validation or KYC process
- collaboration, via an internal dedicated videoconference and document sharing components
- signature, supporting all the eIDAS signature types (electronic signature, advanced electronic signature and qualified electronic signature)
- audit and management, thanks to the notarization and archival of all the relevant events of an agreement signing procedure.

Last but not least, GAYA shall focus on an innovative concept of Agreement in the form of a Ricardian Contract, which shall be a legally binding and valid document.

Country: Italy

Team: NYM S.r.l.

Further information: https://www.nymlab.it/

GitLab: https://gitlab.grnet.gr/essif-lab/business/gaya/gaya_project_summary

Netis: SSI-as-a-Service

An Interoperable Authentication Layer to Connect the SSI Providers and Online Services, simplifying SSI integration and adoption.

Although the field of SSI is gaining wider recognition, several challenges such as lack of standards, clear implementation documentation, security concerns and regulatory uncertainty inhibit its rapid adaptation.

Consequently, the decision-making process for SSI authentication implementation can be time-consuming, and it is challenging to choose a trustworthy solution-provider that also meets all technological requirements.

This will change with SSI-as-a-service, representing a one-stop-shop for developers by bringing a collection of services and libraries for SSI integration in one place.

The solution, based on universality, compliance and interoperability, will therefore greatly simplify the SSI integration processes, and consequently accelerate its use in many services and industries, all leading to SSI mass adoption.

Country: Slovenia

Team: NETIS, raćunalniški inźeniring d.o.o.

Further information: https://netis.si/en/

GitLab: https://gitlab.grnet.gr/essif-lab/business/SSIaaS/SSIaas_project_summary

Jolocom: Universal Backup Service for SSI Agents

A vendor-neutral, plug-and-play component for equipping SSI Agents with a service to generate interoperable backups of end user data.

The UBS component is intended to enable integrating SSI agents with encrypted backup functionality.

More specifically, by integrating the UBS client library, SSI Wallets and Agents will be able to easily create, update, and retrieve encrypted data backups from a remote (either self-hosted, or maintained by a backup provider) backup service.

Access to encrypted backup documents (as well as the endpoints for creating, updating and deleting them) will be protected using a (configurable) authorization strategy.

The UBS client library / service will integrate with existing DID infrastructure to resolve cryptographic material used for encrypting content and authorizing requests.

The UBS component is intended to be an easily deployable, highly configurable, plug and play component, that can suit a wide range of use cases and deployments.

Country: Germany

Team: Jolocom GmbH

Further information: https://jolocom.io

GitLab: https://gitlab.grnet.gr/essif-lab/business/ubs/solution-description-for-ubs

Joinyourbit: SSI4DTM: Self-Sovereign Identity for Digital Transaction Management

A Digital Transaction Management platform to execute any cross-border transactions: NDAs, contracts, bids, etc.

NGI ESSIF-LAB

Self-Sovereign Identity for Digital Transaction Management (SSI4DTM) project aims at implementing an innovative platform to execute any cross-border transactions such as NDAs, contracts, bids, etc. among trusted digital users. It enables users to:

- create and control their own Self-Sovereign Identity (SSI) identities;
- eSign and notarize the whole document-based transactions on blockchain;
- be recognized by other participant within the eSSIF-Lab European ecosystem with which the holder will be or is already in a business relationship.

The project outcome is to identify parties and allow them to access and scale the Digital Single Market (DSM), improve business performances and confidence, while connecting business peers with the eSSIF-Lab open community.

Country: Italy

Team: Joinyourbit SRL

Further information: https://www.joinyourbit.com/en/

GitLab: https://gitlab.grnet.gr/essif-lab/business/ssi4dtm/ssi4dtm_project_summary

Order our product: https://www.joinyourbit.com/pricing/

GATACA: GATACA CONNECT

Trusted Single Sign On for a human-centric Internet

GATACA Connect is an SSI Solution for Verifiers that allows them to request and verify W3C-compliant Verifiable Credentials to authenticate users.

GATACA Connect integrates with other GATACA components, such as its GATACA wallet app, its DID resolver or its Schema and Issuer Registries in order to verify DIDs and Verifiable Credentials.

GATACA Connect -and the entire GATACA platform- was designed following global interoperability principles. For this reason, it implements existing W3C standards and provides an interoperability layer to detach the blockchain infrastructure layer from the SSI solution layer.

The immaturity of the market and the lack of interoperability among different implementations makes it difficult for stakeholders to choose a specific vendor to start promoting real use cases, as they fear vendor lock-in situations or waste of resources on discontinued technologies. For this reason, the goal of this project is to make GATACA Connect vendor-agnostic; that is, for it to work with other wallets and DID resolver providers.

As a result of this project, GATACA has integrated Connect to the Universal Resolver and contributed to its specs by proposing new authentication mechanisms. Furthermore, GATACA has defined open APIs for GATACA Connect to allow other providers to integrate their wallets with Connect in case they wish to, or to build new Verifiers following the same interfaces, allowing GATACA Wallet to interoperate to said verifiers.

Beyond this project, GATACA embarked on the Verifier Universal Interface project, an initiative to standardize those APIs with the collaboration of other stakeholders worldwide.

The ultimate goal behind this work is to allow clearing the existing binding between the Wallets and Verifiers of any technology provider.

Country: Spain

Team: Gataca España SL

Further information: https://gataca.io/

GitLab: https://gitlab.grnet.gr/essif-lab/business/GATC-BIZ/documentation

e-Origin: e-Origin Wallet

Digital wallet of verifiable credentials for products

e-Origin Wallet projects aims to deliver a collaboration platform providing trustable information (verifiable credentials) about Products (and Companies); a platform where all parties collaborate to gradually enrich and/or certify Product's information.

This solution targets the need to transmit verifiable credentials of products through the entire supply chain, from the manufacturer to the consumer, via the logistics and European authorities (e.g. customs).

Country: Belgium

Team: e-Origin SRL

Further information: https://eorigin.eu/

GitLab: https://gitlab.grnet.gr/essif-lab/business/e-origin/e-origin-wallet_project_summary

Domi Labs: SSI-enabled "Contractual Event" Passport

Enabling businesses to integrate SSI into their contractual record management processes

Domi Labs is building an SSI-enabled electronic contracting solution which allows credentialization of legal contracts and contractual events.

This supports the building of verifiable contractual records that can be used as evidence of fulfilment of contractual obligations. It also provides verifiable selective disclosure of contract details or content in order to build trust with third parties outside of the contract, including potential creditors, regulators, business counterparties and more.

This project is building a solution that:

- generates, handles, and verifies contracts that are machine readable and tamper-proof, while still being legally binding across EU member states,
- encapsulates the full lifecycle of a contract between two or more parties,
- provides a mechanism for linking real world events to pre-existing contracts, allowing individuals or legal persons to maintain an SSI-capable "passport" of such events.

Country: Germany

Team: Domi Labs UG

Further information: https://domilabs.io/

GitLab: https://gitlab.grnet.gr/essif-lab/business/scep/SCEP_project_summary

Danube Tech: Universal DID SaaS

Building a hosted service that allows developers to easily work with Decentralized Identifiers (DIDs), without having to set up their own infrastructure

Danube Tech is building the Universal DID Saas, a hosted platform that allows developers to create, update, resolve, and deactivate Decentralized Identifiers (DIDs), as well as to perform several other advanced DID-related operations.

This will build directly on the well-known open-source tools Universal Resolver and Universal Registrar and integrate with other SSI community efforts that also work with DIDs.

Country: Austria

Team: Danube Tech GmbH

Further information: https://danubetech.com/

GitLab:
https://gitlab.grnet.gr/essif-lab/business/universal_did_saas/udidsaas_project_summary

NGI ESSIF-LAB

Commerc.io: CommercioKYC

Easy KYC with Self-Sovereign Identities

Commerc.io wants to create a KYC protocol that will empower both Companies and individuals:

- a Company will onboard customers with high confidence about their true Identity and simplify the internal KYC process and potentially limit privacy data Liabilities
- a Customer will instantly sign-up and sign-in effortlessly to a service, without losing control of their role identity holders, without being forced to request permission of an intermediary or centralised authority and gives control over how their personal data is shared and used.

CommercioKYC is a protocol that enables to instantly Issue a KYC VC (Verifiable Credential) based on data accessed through PSD2 Bank Payment Service Directives.

CommercioKYC will improve customer experience Automating the KYC process by obtaining information straight from end-customers' banks accounts instead of asking them to manually input form fields or send in physical documents and will reduce user drop-out by making it easier and quicker for end-customers to sign up and start using a company service, we increase the chances of them successfully completing the process.

Country: Italy

Team: Commerc.io srl

Further information: https://commerc.io/

GitLab: https://gitlab.grnet.gr/essif-lab/business/comkyc/kyc_project_summary

filancore

NGI ESSIF-LAB

Filancore: Filancore Identity Gateway

Cheaper, faster and more secure next generation identities

This security solution "Identity Gateway" mainly focuses on the ease of use for DIDs and VCs.

The Identity Gateway aims to provide easy to use service for everyone to highly automate and standardize the issuing process of DIDs and VCs including processes for the complete identity lifecycle.

The service will help to build and manage decentralized identities for the internet of things.

With Filancore Identity Gateway organizations we will be able to register, issue, verify and validate a large number of devices.

Country: Germany

Team: Filancore UG

Further information: https://www.filancore.com/

GitLab: https://gitlab.grnet.gr/essif-lab/business/filancore/filancore_project_summary

wellbeing cart

Wellbeing cart: Data As Currency

Making the use of SSI easy and motivating by focusing on the value of the data.

We believe that the adoption of SSI will be thwarted unless the user clearly understands the benefits that the technology provides. An integrated solution and user-friendly UX is required to demonstrate that data has value.

With Data as Currency we will solve how data is valued, how the value is connected to data flows between services, how to present the value and underlying system in a way that can be easily understood, and how to integrate the system into any service that utilises SSI.

Country: Finland

Team: Welbeing cart Oy

Further information: https://www.wellbeingcart.com/

GitLab: https://gitlab.grnet.gr/essif-lab/business/dac/dac_project_summary

MyData Global: MyData Commons

The MyData Commons project seeks to empower people with their personal data through the COVID 19 crisis and beyond.

The idea is to complement the data available from traditional top-down sources with that which can be volunteered by individuals when they have the right tools, including decentralised identity and verified claims.

Country: Finland

Team: MyData Global ry

Further information: https://www.mydata.org

GitLab: https://gitlab.grnet.gr/essif-lab/business/mdcommons/mdc_project_summary

Spherity: KERI

Key Event Rotation Infrastructure – JavaScript Reference Implementation

KERI is both a "spanning layer" and open-source mechanism for interoperability across DID methods, and an upgrade to the SSI stack as a whole.

It is a paper-thin protocol logging CRUD events for DID control, which allows some peer-to-peer use cases to detach from blockchains altogether, and others to rely less on full nodes or real-time access to a chain.

Country: Germany

Team: Spherity GmbH

Further information: https://spherity.com

GitLab: https://gitlab.grnet.gr/essif-lab/business/KERI-JS/kerijs_project_summary

HonorBox-SSI by LearningProof UG

The HonorBox project allows self-publication with a “pay afterwards”/honor-system approach, a business model that has been adopted in much of the world (particularly in Latin America) where e-book piracy is a major issue and impediment to small-scale/independent publishing.

Country: Germany

Team: LearningProof AG

Further information: https://learningproof.xyz

GitLab:

https://gitlab.grnet.gr/essif-lab/business_2/learning-proof/HonorBox_project_summary

Decentralized Open Innovation Platform (DOIP) by Stichting Alkemio

Enabling effective, inclusive and self-sovereign collaboration on multi-stakeholder challenges

The challenges facing society require many parties to collaborate, effectively. Cherrytwist is designed for multi-stakeholder challenges, allowing wider societal involvement (inclusiveness), greater societal impact and ultimately increasing our collective ability to solve hard problems like climate change.

Decentralization is a core guiding principle, reflected in design choices at all levels: core patterns cannot be retrofitted later. Two examples: usage of non-verified credentials for authorization, actor model for interactions between entities (e.g. challenges, users).

Next is the usage of SSI for citizen engagement in The Hague (partner: The Hague). Further we will work to shape and provide feedback on how the patterns of usage and policy guidelines should evolve (partner: Digicampus). On the technical side a Trust Framework will be defined, integrating with CBAS for managing authorizations and finally also exploring how to move towards externally held wallets (partner: Jolocom).

Country: Netherlands

Team: Stichting Alkemio (Foundation)

Further information: https://alkem.io

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/alkemio/DIOP_project_summary

BCdiploma - Blockchain Certified Data

To overcome these challenges, Blockchain Certified Data will develop and integrate an SSI-enabled enterprise wallet and a student wallet, including a verifier, into its TRL9 BCdiploma application, in production.

Integrating SSI technologies into an already decentralized solution like BCdiploma will provide a level of interoperability unique in the market, increasing institutional confidence in the sustainability and viability of the solution. Also, BCdiploma's expertise in the academic environment combined with the eSSIF framework's capabilities in terms of user sovereignty over their data will allow maximum adoption.

BCdiploma has chosen to take up this challenge in collaboration with the walt.id teams: we share a common vision of a future open-source wallet, compliant with the new EU identity standards (ESSIF), easy to integrate and easy to use for all citizens.

Country: France

Team: BCdiploma

Further information: https://www.bcdiploma.com

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/blockchain-certified-data

Genia - Patient-controlled info flow 4 learning health sys

Genia is a personal information exchange that empowers people living with long-term illness, supports co-production of care, and generates valuable health data in patient-controlled information flows.

Clinical trials have been the standard for showing value of treatments. So-called real-world data (RWD) is a new important source for further value demonstration of health technologies, e.g. to assess the effectiveness on individual patient level or follow-up of reimbursement restrictions or pay for performance pricing schemes.

The Sweden Coalition CF mission is to be the leading Swedish example of introduction of personalized precision medicine for optimal health. Extraction of patient level RWD for this mission is possible today, but the main challenge is to create good datasets when data is captured in silos governed by different parties.

Solutions are needed that:

- Overcome hurdles to integration and consolidate data silos
- Collect new patient reported data to enrich existing data,
- Automate data extraction for research and other purposes such as the near real-time improvement of healthcare and follow-up of therapies
- Engage patients and healthcare professionals.

Country: Sweden

Team: Genia

Further information: https://www.genia.se/

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/upstreamdream

Amlet

Amlet enhances customer due diligence for financial institutions by automating KYC processes using the Self-Sovereign Identity framework. Nowadays, onboarding is a long and complex process made of various steps of form-filling and credentials sharing: this process deeply affects customers' experience as they are requested to perform repetitive and time-consuming tasks. The process is not smoother nor simpler for financial institutions, as they are required to check and verify information and data with multiple third-party providers, often using human-based activities and non-scalable processes. As we believe that making the KYC process smoother and more effective is a key step to improve customers' experience, in Amlet we transform data and identity credentials into digital twins, stored into the customers' digital identity wallet. When a customer presents her own wallet, Amlet checks data using a broad range of databases to screen names, info, PEP, sanctions and terrorist lists, and Ultimate Beneficial Owners for business customers.

Thanks to the automation of onboarding and KYC process, the time required to conclude controls on users is reduced to a bunch of seconds, and anti-fraud defences result enhanced.

Country: Italy

Team: Amlet

Further information: https://amlet.eu/en/

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/mopso-srl

Credenco - Digital Certificate of Good Conduct

G3C (Good Conduct Certificate Credential) provides a solution for issuing, verifying, processing and archiving digital Certificates of Good Conducts. We provide a solution for issuing, verifying, processing and archiving digital Certificates of Good Conducts with the following characteristics:

Privacy preserving, control over your own data, GDPR friendly

- This will improve the privacy of the citizens controlling which data they share and with whom
- Organizations do not necessarily have to store the person's data themselves. Registration of the receipt and verification (including the unique reference to the VC) should be sufficient, according to Justis.

Providing automatic, Straight Through Processing (STP/RPA) of data

- This saves organizations significant amounts of work, time and money
- Shorter cycle means the employee/citizen can start quicker

Any tampering with data is immediately evident

- This will prevent attempts of fraud and expose bad actors

Supports intermediate revocation of the CoCG credential

- This will improve safety and security for the goal and purpose for which the CoCG certificate is being issued

Country: Netherlands

Team: Credenco

Further information: https://www.credenco.com/?lang=en

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/credenco

Alkemio - Decentralized Open Innovation Platform

Alkemio puts Challenges central. This starts by having a clear shared understanding of where we are now and where we wish to go i.e. what is the change to be achieved. Around this shared understanding, "Context", build up a "Community" of users, organisations and knowledge that can contribute. The Community can then Collaborate and Coordinate to make progress on the Challenge.

This is a simple yet fundamental change: it is not organisations or users that are central but the change that we wish to achieve.

A Challenge centric platform needs to have trust as a core principle, so that the collaborating parties can interact with each other with confidence in the fairness of the platform. This implies that the wider trust framework has to be clear, and that parties can interact with each other in a self-sovereign way.

Alkemio has been designed to be ready for a decentralized future. Authorization is based on (non-verified) Credentials, all core entities in the platform have Agents that manage the Credentials. Important to note that these Credentials are all platform issued - so non-verified.

Country: Netherlands, Belgium, Ireland

Team: Alkemio

Further information: https://alkem.io/

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/alkemio

Truu - Healthcare Professionals Digital Staff Passport

Truu was founded in 2015 by two NHS doctors who personally experienced the inefficiencies in the healthcare systems regarding pre-employment and identity checks and the effect they have one healthcare worker satisfaction and frustration and patient care. Dr Nijjar and Dr Goodier identified SSI as a structure and methodology that could be applied to this scenario, enabling healthcare workers to own their credentials and complete checks remotely. This means data is more secure, controlled by the individual and minimises administration time and time away from patient care.

Dr Nijjar has contributed to the UK All Party Parliamentary report on Blockchain in Healthcare and has been advising the NHS on the benefits of SSI for these use cases.

Truu's healthcare digital staff passport platform creates trusted digital identities for healthcare workers using verifiable credentials meaning checks can be completed remotely and securely reducing onboarding time from 2 months to 2 minutes. This reduces the administrative burden for healthcare professionals and organisations as well as reducing organisational risk and improving patient safety. Truu's digital staff passport also enables passwordless single sign-on to clinical apps and IT systems reducing delays to patient care and increasing governance. The platform was deployed by the NHS as the COVID-19 Digital Staff Passport to speed up clinician movement between hospitals during the pandemic and piloted by the US Federation of State Medical Boards. The recent project with UK private healthcare addressed systemic failures identified in the UK Government Paterson Inquiry.

Truu is founded on the shared principles of SSI and medical ethics, namely privacy and consent.

Country: United Kingdom

Team: Truu

Further information: https://www.truu.id

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/truu

FairBnB - Common cooperative membership using VC

The Coop Passport provides portable membership between cooperatives. It is based on mutual trust and a 'common' of membership and resource exchanges between three founding co-operatives: FairBnB, Pavilion and Resonate. They have founded a consortium to launch a use case cantered on community-powered independent music micro-touring and tourism - "Stay Fair, Play Fair" - later expanding it to a wider cooperative platform ecosystem.

A co-op industry body and/or designated Co-operatives issues verifiable credentials using a standardised Know Your Co-operator process. Members hold and present these credentials to new co-ops within the network, who them verify them before granting access. Partner co-operatives mutualise the KYC process costs through a separate accounting process.

The Cooperative Password will save KYC costs, reduce sign-up friction, boost membership and enable privacy-respecting cross-membership deals and 'affinity' offers. Co-operatives could reduce risk where membership checks are mutually recognised and trusted.

Country: Italy

Team: FairBnB

Further information: https://fairbnb.coop/

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/fair-bnb

Zenlife eConsent -

There is a global shortage of organ. The need is much higher than the offer, even in countries where citizens and residents are all presumed donors. Even if 80% of the population are willing to donate, 61% have never expressed their consent. In this case, medical staff approaches family to ask for consent and the refusal rate is high.

In addition, collected consents in the existing solutions have compliance issues. Consent extension module of EHR software vendor is too naive. Sometimes the consent is just a flag stored in the database. There is no way to prove the authenticity and the integrity of the consent. Public healthcare institutions are exposed to legal risks.

Institutions still use paper based process. It is impractical and incurs administrative burden. There is 2000 complains per year in Luxembourg on the average and file a court case takes several days.

Zenlife eConsent is a turn key solution and we make it easy of manage the whole life cycle of consents and give them the probative value.

Country: Luxembourg

Team: Zenlife

Further information: https://zenlife.lu/

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/zenlife-sarl-s

Work Performance Intelligence

Because jobs are changing rapidly due to technological developments, skillgaps are emerging. WorkPi helps people measure and decrease their skill gaps by providing an open marketplace for assessments & e-learning courses

WorkPi measures the skills, characteristics and preferences that are important for the jobs of today and tomorrow. With a unique datamodel, skills taxonomy and aggregator tool for assessments, WorkPi is able to give employers and employees exclusive insights into their skills and performance.
Because this data is personal and privacy sensitive, it is important that there are no central intermediaries that control it. To realise this, Self-Sovereign Identity can help.

All WorkPi data will be stored in SSI wallets, thereby enabling users to take control over their own career related data. At the same time, this techniques gives companies across various industries a safe environment to collaborate, and share anonymised data insights about the most important skills for different jobs. Now, companies will be able to make data driven decisions, based on an inter-enterprise algorithm without privacy concerns. Also, employees will be able to control work-related for their entire career.

WorkPi enables employees to take back control over their career, by granting them a unique opportunity to collect work-related data in one place without losing it when changing jobs.

Country: Netherlands

Team: WorkPI

Further information: https://workpi.com

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/workpi

EuBic - European Bank Identity Credentials

Use bank-issued verifiable credentials to prove your identity when requesting and presenting your diploma. yes.com operates a large-scale identity federation of about 1000 financial institutions in Germany. The objective of this project is to extend existing (bank) identity providers with the capability to issue verifiable credentials asserting these bank-verified identities. This will allow graduated students to prove their identity when requesting their diploma (again as verifiable credentials). Subsequently, both credentials can be used in combination to prove the graduation and the identity of the holder, e.g. in the course of a job application. The bank identity credential can certainly be used in other scenarios as well, such as onboarding with insurance websites, car sharing, vacation flat rental services, or age verification for gaming.

The project also aims at underpinning the service with a sustainable business model and suitable security level (e.g., regarding the wallet's key management). As a result, bank customers can enjoy the freedom of self-sovereignty while financial institutions will have an incentive and the security allowing them to contribute their tremendous reach of verified identity data to the European SSI ecosystem.

Country: Czech Republic, France, Austria

Team: EuBic

Further information: https://www.yes.com

GitLab: https://gitlab.grnet.gr/essif-lab/business_2/yes-com-ag

Other SSI Components Available

TNO: SSI Service/Gateway

Issue and obtain credential-data to/from your users, without you needing to worry about the kind of wallets they use, nor about the different protocols and credentials such wallets use.

In order to build an IT application that issues credentials, or uses them, the application must communicate with their users' wallets. So either the application prescribes the wallets their users must use – forcing them to add that wallet to the set of wallets they already have, or it must find a way to support the many different kinds of wallets that are, and will be out there.

The SSI-Service/Gateway (SG) is an open source IT component that does this heavy lifting for you: it allows your application to simply issue, request and obtain credential data, without having to worry about the kind of wallet the user has, nor about the different associated protocols or the kind(s) of credentials that the wallet supports. This allows you to focus on the application you are building rather than on spending resources on hooking up different kinds of wallets.

Already, the wallets of Jolocom, IRMA, and Hyperledger/Indy wallets (e.g. Esatus) are supported. Additional ones (e.g. the IDA wallet) will be added as needed.

Country: Netherlands

Team: TNO

Further information:
https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/data-sharing/ssi/

GitLab: https://gitlab.grnet.gr/essif-lab/tno-ssi-service

Contact: Hidde-Jan Jongsma | hidde-jan.jongsma@tno.nl

Rieks Joosten | rieks.joosten@tno.nl


NGI
ESSIF-LAB