NGI ESSIF-LAB

SUBGRANTEE SSI Infrastructure

and business-oriented projects

Projects descriptions

02/03/2021

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

Index

Introduction

What is the Next Generation Internet (NGI)?

NGI (ngi.eu) is a European Commission funded programme to evolve the Internet, Internet technologies and uses in a more human centric way.

The European Self-Sovereign Identity Lab (essif-lab.eu) is part of the NGI programme and is an ecosystem of parties that work together to make existing (and new) Self-Sovereign Identity (SSI) technology into a scalable and interoperable infrastructure that businesses can use very easily for conducting (business) transactions with other businesses and individuals alike.

Who is eSSIF-Lab seeking to engage in this ecosystem?

The eSSIF-Lab project seeks to fund European SME and Innovators that want to contribute to the eSSIF-Lab vision by:

- making open-source technological components available that may be considered part of an SSI infrastructure (comparable with the roads/highways of various kinds). Such an infrastructure must remain business-agnostic, be interoperable with technologies of others (also outside eSSIF-Lab, specifically W3C, Aries, DIF and ToIP), and scalable. Typically, infrastructural components facilitate business applications to make use of SSI technologies. (Infrastructure-oriented Open Call - ongoing)

- making open-source technological components available that are not necessarily part of the infrastructure, but extend it to provide value for businesses that want to connect to such infrastructure (comparable with driveways, that connect parking lots or garages to a road). Examples include components that implement e.g., eIDAS signing, credential revocation mechanisms, or credential catalogues. In this call, funding must also be used to demonstrate the business value of the contribution. (First Business-oriented Open Call – already closed).

- making a technological project that actually uses the components that are produced in the aforementioned calls and demonstrates that a business can be made with that. Such projects typically validate the infrastructural components and its extensions. (Second Business-oriented Open Call – forthcoming in late spring 2021).

Who is already part of our ecosystem?

NGI eSSIF-Lab launched both its first Business-oriented Open Call and its Infrastructure-oriented Open Call in March 2020.

First Business-oriented Open Call closed on 7 May 2020 with 54 applications from SMEs providing SSI-related business solutions. 19 participants joined initially the 8-month acceleration programme and 5 best from those are expected to reach its end.

Infrastructure-oriented Open Call, which is still ongoing until 30th June 2020, has received so far 69 applications from innovators willing to join the ecosystem and contribute to eSSIF-Lab Framework with SSI open-source components. 14 of those innovators are already benefiting from eSSIF-Lab Infrastructure Development Instrument.

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

In the second business-oriented open call, subgrantees can build on open source components of the infrastructure-oriented projects. They can also make use of TNO's SSI Gateway. This gateway was developed outside the context of eSSIF-Lab and is made available to the eSSIF-Lab ecosystem.

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

SUBGRANTEE BUSINESS-ORIENTED PROJECTS

Verifiable Credentials: User-friendly Magement Interface for Verifier Policies

An interface to allow resource owners to specify in controlled natural language their policies for granting access to users who possess verifiable credentials

This interface will develop for eSSIF is a policy management tool that will allow resource owners e.g. web sites, hotels, etc. to easily specify 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.

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 Data Sharing Hub with Consent Flow

This hub brings SSI benefits to the wider economy by enabling a privacy preserving full data life cycle including consent.

The concept of the Dynamic Data Sharing Hub (DDSH) eSSIF-lab project was born from Human Colossus Foundation experience in the pharmaceutical sector where the exchange of large 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 down innovation, increasing costs and liabilities for all stakeholders as more complex compliance and data protection regulations are administered by governing authorities.

The DDSH 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 consent has been authorised by the data subject and all flagged PII data has been encrypted (or removed), data can then be shared across multiple stakeholders through a Data Sharing Hub (DSH).

The DDSH project provides the necessary components for an SSI-based data sharing flow that can be used within the eSSIF-Lab architecture as well as the realisation of a specific instance addressed to, but not limited to, the health care 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.

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

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

NGI ESSIF-LAB

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

NGI ESSIF-LAB

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

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


NGI
ESSIF-LAB