SSI and MyData Operators
A Nordic perspective

Lal Chandran
Co-Founder and CTO

Jan Lindquist
Data Privacy Consultant

iGrant.io®
Your data, your choice.

LINALOTEC
Content

1. MyData Operator and iGrant.io solution
2. Consent lifecycle and Agreements
3. Demonstration: SSI in MyData Operator
IT’S PERSONAL
The human-centric paradigm is aimed at a fair, sustainable, and prosperous digital society, where the sharing of personal data is based on trust as well as balanced and fair relationship between individuals and organisations.
Towards a MyData Operator model

Organisations manage the whole value chain

Integrating data from multiple sources is hard

Non standardized interfaces and agreements
MyData Operator Reference Model

We use the metaphor of a ‘journey of interoperability’ throughout and lay out its initial roadmap with the minimum interoperability criteria for operators. The operators must always strive to work towards and within open ecosystems.
mydata.org/operators

download the paper

Ongoing work: Governance framework
iGrant.io: A MyData Operator creating win-win between organisations and individuals
iGrant.io: Enabling consented data exchange

DATA WALLET & PREFERENCE CENTRE
- Holds credentials and exchange personal data w/ a mobile PDS (Personal data store)
- Personal data dashboard
- Exercise Data Subject Rights (GDPR)

ENTERPRISE DASHBOARD
- Consent Empower individuals
- Compliance with Regulations (GDPR)
- Facilitates Data Subject Rights (GDPR)

DATA EXCHANGE ECOSYSTEM
- Enable data exchange via QR codes
- KYC enabler
- Federates quality data
- Business opportunities/ efficiencies
iGrant.io tech stack: High-level overview

Client:
- User App
- Mobile SDKs
- Privacy Portal
- Dev Portal
- Audit Portal

Governance:
- RESTful APIs
- Identity Mgmt including DID
- Permission and Consent Management
- SSI Tech and Roles
- Metadata (Data Model) repository
- Datasharing and Exchange
- Audit Logger

Distributed Infrastructure (Ledgers)

External:
- External Data Sources
- Certification Bodies
- National ID, eIDAS, Aadhar, BankID
2. Consent lifecycle and Agreements
Reference solution demo: SSI Roles

Issuer (Data Controller) 
- Signs Certificate

Holder (Data Subject) 
- Data and Consents
  - Presents Conditions

Verifier (3\textsuperscript{rd} Party) 
- Verifies data and consent

Wallet

Pairwise Unique DID

Legal Entity 
- Test Center (Data source)

Alice (Individual)

Travel Company (Data using service)

Decentralized Identifiers (DIDs)

Stewards (Data Operator)

Decentralized Registry
Privacy Agreement engagement
Privacy Policy Example

Privacy policy

Protecting your data, privacy and personal information is very important for us at our testing center facilities. It is important for us that our customers feel secure when using the Services. Our test centers provide health related tests for example covid-19 immunity tests. The data we can gather are secured based on best practices set by GA4GH.

Topics

What Information we collect

- How the information is used
- How long the information is kept
- Who do we share your data with
- Newsletter, Promotions and Marketing
- Cookies
- Your rights
- Changes to the privacy policy
- How to contact us

What Information we collect

When you use our services we only collect information provided by you. We attempt to limit the information we collect to only what is necessary to legitimately provide our services. The information is stored within the EU.

1. The following information is collected when you first register at one of our test centers
   - **Name**
   - **Personal identification number**
   - **Phone Number (if provided)**
   - **Email Address (if provided)**
   - **Address (if provided)**

2. Depending on the nature of the test performed we collect health related information from blood samples, physical information and/or other biological output. This information can include but are not limited to:
   - **Disease**
   - **Biomarkers**
   - **Physical conditions**
Form and VC relationship

- **Conditions of use**
  - Ex. Privacy policy (Kantara Consent Notice)

- **Extension**
  - Ex. Proof of consent and verify permission for use (provides governance and helps with 3pp collaboration)

- **Captured information or data**
  - Ex. Completed Forms (covid test results) or intended captured data

- **Verifiable attributes of conditions**
  - Ex. Proof of data condition (covid-19 result)

- **Verifiable attributes relating to data**
Kantara Consent Notice & Personal Data Processing

Kantara schema

PDP schema
What to include in the privacy agreement (VC)?

CONSENT_SCHEMA = {
    did: "did:schema:27312381238123",
    name: 'privacy agreement for test center data collection',
    description: "Created by Test Center",
    version: '1.0',
    # MANDATORY KEYS
    attr_names: {
        consentTimestamp: "20200830 00:00:00T01",
        policyUrl: "www.test-center.com/privacy",
        jurisdiction: "EU",
        piiControllers: [
            properties: {
                piiController: "Test Center Inc",
                Address: "Main street 10, 12312 Stockholm, Sweden",
                email: "privacy@test-center.com",
                piiControllerUrl: "www.test-center.com"
            }
        ],
        Services: [
            properties: {
                purpose: "Our test centers provide health related tests for example covid-19 immunity tests.",
                consentType: "request for testing",
                purposeCategory: "healthcare",
                primaryPurpose: "yes",
                termination: "10 years after last visit",
                thirdPartyDisclosure: "no"
            },
            properties: {
                purpose: "You may opt in to our newsletter with the latest information on our tests and research behind them. The newsletter may include promotions.",
                consentType: "opt in",
                purposeCategory: "communication/social",
                primaryPurpose: "no",
                termination: "10 years after last visit",
                thirdPartyDisclosure: "no"
            }
        ]
    }
}
What to include in the privacy agreement (VC)?

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>How applied to SSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>geographicRestriction</td>
<td>Where is the collected data stored. For regulatory reason data may not leave a given reason.</td>
<td>An audit is possible to perform by a government agency and the attribute brings transparency to how data is stored.</td>
</tr>
<tr>
<td>noShare</td>
<td>Privacy agreement required to state if the data is shared with any 3rd party.</td>
<td>An audit is possible to perform by a government agency and the attribute brings transparency to how data is stored.</td>
</tr>
<tr>
<td>expiration</td>
<td>Initial consent is tied to a service. When the service period expires then restricted conditions of access to the data apply.</td>
<td>The private data that may have been collected are stopped when service expires. The conditions of access are traceable through proof requests.</td>
</tr>
<tr>
<td>limitation</td>
<td>All personal data that is collected shall not be kept longer than is reasonable.</td>
<td>The private data needs to be purged after set limitation. The conditions of access are traceable through proof requests.</td>
</tr>
</tbody>
</table>
Example of VC using pdp

- **Issuer** (data controller)
- **Operator**
- **Holder** (data subject)

- Consent receipt credential

- **Conditions**
  - Expiration = 1 year
  - Limitation = 2 years
  - ValidityTTL = 3 day

- **Subscription to service**
  - Renews in 1 year.

- **Collected data**
  - Will have 2 year storage limitation.

- **Validity TTL allows extended proof duration** so not checks required for 3 days.
3. SSI and the MyData Operator Demonstration
Trusted Digital Agent: Enable organisations to adopt SSI

- Individual
  - Trusted digital agent (TDA)
    - Application with full service e.g. a bank
  - Trusted digital agent (TDA)
    - Application with TDA services in wallet, e.g. Data4Life
  - Trusted digital agent (TDA)
    - Application with TDA services in wallet, e.g. DataForGood
  - Human Centric Services
    - Mobile SDKs
  - Mobile SDKs
  - Mobile SDKs

- MyData Operator Infrastructure
  - Data Sources
  - Data Sources
  - Data Sources
  - Data Sources

- Ecosystem Enablers
  - Trusted Digital Agent: Enable organisations to adopt SSI
Demo set-up of reference solution: SW Components

**Frontend**
- Test Center, Travel Company
  - Enterprise Dashboard
- Legal Entity
  - Schema definitions and audit service ([https://audit.igrant.io](https://audit.igrant.io))

**Backend**
- Backend with Data Operator microservices
- Ledgers and databases

**Individual (Data Subject)**
- Reference App: Data4Life App or any 3PP App
  - Mobile SDKs
    - Privacy Board SDK
    - Data Wallet SDK
  - RestFul APIs
- Data4Life Backend (Or any 3PP backend service)
- Agent backend (Aries)
- Distributed ledger (Indy) ([https://indy.igrant.io/](https://indy.igrant.io/))

Existing Data Operator services with open APIs at: [https://developer.igrant.io/](https://developer.igrant.io/)

Open sourced reference implementation, Data4Life

eSSIF-Lab code, Open sourced
Reference solution demo: SSI Roles

Issuer
(Data Controller)

Holder
(Data Subject)

Verifier
(3rd Party)

Wallet

Issues Certificate

Data and Consents

Presents Conditions

Verifies data and consent

Pairwise Unique DID

Pairwise Unique DID

Decentralized Identifiers (DIDs)

Legal Entity

Test Center (Data source)

Lal
(Individual)

Travel Company
(Data using service)

Stewards
(Data Operator)

Decentralized Registry
Roadmap for SSI integration to MyData Operator services

**SEP 2020**

**Demo Iteration, Basic Flow**
- Get the architecture and basic end-to-end solution framework in place
- Aries playgroup beta version with beta Indy network integrated with MyData Operator services

**OCT 2020**

**Agreement Handing and Consents in SSI**
- A specification openly available based on Aries RFCs (0133 and 0167)
- Demonstrated verifiable consents and agreements
- Aries playground released for developers with interoperable with other Indy networks
- Web socket for agent to client notifications

**NOV 2020**

**Audit functions integrated**
- Aries Mobile Agent - Flutter Open source beta version (iOS and Android)
- Agreement handling and Consents SSI
- Verifiable and auditable consents,
- Attribute level consents during data sharing
- Integrate RFC 0133 to Aries Cloud Agent - Python

**JAN 2021**

**Aries Mobile Agent - Flutter Release 1.0**
- Release AMA-F full version with Interoperability tests with every other agents (iOS and Android)
- Organisation Agent SDK
- Full-fledged iGrant.io MyData Operator platform fully integrated with SSI
Express interest to join the standardisation efforts at:
https://airtable.com/shrnc3DqvoQ0OHHFeO