[DRAFT] Self-Sovereign Identity—Test Plan

R.M. Chotkan

June 2021

1 Introduction

This serves as a test plan for *Industry-Grade Self-Sovereign Identity*: a fully distributed Self-Sovereign Identity scheme, capable of offline-verification and distributed revocation, built with the academic IPv8 protocol stack. The test plan describes several scenario's capable of evaluating the usability and performance of IG-SSI. The test plan is built for an international trial with a focus on the novel revocation model of IG-SSI.

2 Use Cases

We identity four prime use-cases capable of benchmarking the properties of IG-SSI:

1. **Across-border trust**
   This scenario entails the verification of identity credentials. For instance, a simple identification comprising name and age or a drivers license. This verification spreads further as any digital service requiring registration could utilise such identities.

2. **Qualifications**
   The verification of previous academic and professional ventures can counteract fraud in qualifications. This makes it possible for e.g. a foreign university to easily verify a prior education or an employer to gain trust in any relevant experience of a possible employee.

3. **COVID-19**
   The COVID-19 virus has led to an increase demand of digital variability, with initiatives such as storing negative COVID tests in mobile applications and registering COVID vaccination in digital passports. SSI can be a prime candidate for satisfying these demands, especially due to privacy benefits.

4. **Age of majority**
   Age verification is a process required for many activities. May it be for

entering a venue or purchasing certain goods. However, drawbacks to current age verification, especially digitally, is the disclosure of the actual age, which can be considered personally identifiable information (PII) when combinable with other information. SSI can prove to overcome this by allowing age verification in zero-knowledge.

3 Test Scenarios

Scenario #1: The Airport Trial

In airports, identities must be quickly verified in order to ensure travellers are eligible to cross borders. This scenario satisfies this identification procedure using SSI credentials.

Stakeholders:

- Authorities: Country **A**, Country **B**
- Subject: Traveller **C**

Prerequisites:

- Traveller **C** holds **valid**/**invalid** credential IDENTITY attested by Country **A**.

Steps:

1. Country **B** requests IDENTITY from Traveller **C**. (may be performed verbally).
2. Traveller **C** presents IDENTITY.
3. Country **B** verifies validity of IDENTITY.

Scenario #2: Study Abroad

Diplomas are not recognised world-wide. Even in Europe, the recognition of academic diploma's is not a given, possibly requiring hefty verification processes [1]. SSI can overcome this by having governments actively attest to a diploma, with easy variability. This can make the process of applying to a foreign university instantaneously.

Stakeholders:

- Authorities: Country **A**, University **B**
- Subject: Scholar **C**

Prerequisites:

- Scholar **C** holds **valid**/**invalid** credential DIPLOMA attested by Country **A**.

Steps:

1. University **B** requests DIPLOMA from Scholar **C**. (may be performed verbally).
2. Scholar **C** presents DIPLOMA.
3. Country **B** verifies validity of DIPLOMA and the fulfilment of any prerequisites possibly filled by the diploma.

Scenario #3: The health check

Negative COVID-19 tests and digital vaccination passport haven proposed for entry prerequisites for venues. This introduces issues in terms of verification for venues hosts. Additionally, the storage of medical data itself is heavily regulated. SSI can achieve both verification and storage compliance as the medical data will be stored by only the subject.

Stakeholders:

- Authorities: Health Organisation **A**, Venue Host **B**
- Subject: Guest **C**

Prerequisites:

- Guest **C** holds **valid**/**invalid** credential COVID_NEGATIVE attested by Health Organisation **A**.

Steps:

1. Health Organisation **B** requests COVID_NEGATIVE from Guest **C**. (may be performed verbally).
2. Guest **C** presents COVID_NEGATIVE.
3. Country **B** verifies validity of COVID_NEGATIVE and verifies that the claim is not more than 48 hours old.

Scenario #3: The Age of Majority check

When checking whether one is of age of majority, the actual age must not be revealed.

Stakeholders:

- Authorities: Country **A**, Venue Host **B**
- Subject: Guest **C**

Prerequisites:

- Guest **C** holds valid/**invalid** credential AGE attested by Health Organisation **A**.

Steps:

1. Health Organisation **B** requests AGE from Guest **C**. (may be performed verbally).
2. Guest **C** presents AGE.
3. Country **B** verifies that the value of AGE is 18+ and does not learn the underlying age.

4 Revocation Scenario's

Scenario #1: The Airport Flood Trial

As discussed earlier, identities must be verified at airports. In this instance, a user has his privilege to travel revoked. However, malicious nodes in the network attempt to stop the propagation of the revocation by flooding the network with bogus revocations, acting as authorities. The outcome of this trial must be failure during verification.

Stakeholders:

- Authorities: Country **A**, Country **B**, Venue Host **Z**
- Subject: Traveller **C**

Prerequisites:

- Traveller **C** holds valid credential IDENTITY attested by Country **A**.

Steps:

1. Country **A** revokes IDENTITY for Traveller **C**.
2. Venue Host **Z** floods the network with fake revocations.
3. Country **B** requests IDENTITY from Traveller **C**. (may be performed verbally).
4. Traveller **C** presents IDENTITY.
5. The verification performed by Country **B** for IDENTITY fails.

Scenario #2: Revocation Routing

As nodes may exist across border, revocations must be propagated by any client. In this scenario we investigate the speed of such revocations.
Stakeholders:

- Authorities: Country **A**, Country **B**, Venue Host **Z**
- Subject: $\emptyset$

Prerequisites:

- Country **A** acknowledge Country **B** as an authority.

Steps:

1. Country **A** revokes x credentials.
2. Country **A** gossips revocations.
3. Venue Host **Z** does not propagate any revocations.
4. Country **B** receives all revocations within the theoretical bound.

References

[1] Your Europe. Recognition of academic diplomas, Nov 2020.