

## Open Call 3

### Transatlantic SSI Interop

### Deliverable 3: Experiment Results and Final Report

Authors	Markus Sabadello, <a href="mailto:markus@danubetech.com">markus@danubetech.com</a> , Danube Tech
Due Date	16 <sup>th</sup> December 2021
Submission Date	16 <sup>th</sup> December 2021
Keywords	Decentralized Identifiers, DIDs, Verifiable Credentials, VCs, SVIP, EBSI, ESSIF, Permanent Resident Card, Digital Diploma

## Deliverable 3: Part I

### Analysis, results, and wider impact

#### 1 Abstract

In this experiment, we demonstrated interoperability of experimental decentralized identity infrastructures in the US and EU. On the US side, our partner Digital Bazaar has set up infrastructure for issuing digital Permanent Resident Cards, as envisioned by the US Department of Homeland Security's (DHS) Silicon Valley Innovation Program (SVIP). In the EU, we issued digital diplomas using the pre-production European Blockchain Service Infrastructure (EBSI). In the experiment, we successfully showed how the US- and EU-issued digital identity credentials can be exchanged between the two sides.

#### 2 Project Vision

The concept behind this experiment was to demonstrate interoperability in the area of the emerging Self-Sovereign Identity (SSI) concept, building on top of infrastructures that are being developed in the US and the EU. SSI is clearly emerging as a next-generation paradigm for digital identity that enables independence, privacy, security, and human dignity for individuals, as well as new opportunities for digital identity of organizations and things. This approach is based on inherently decentralized architectures that eliminate dependencies on centralized authorities.

---

At the moment, many SSI projects and initiatives are being built across the world, but each project in each country and each industry is essentially being designed and deployed in an isolated manner, not paying much attention to how to interact with other related efforts. This stands in strong contrast to both the ideology of SSI and its foundational technical building blocks such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), which have been designed for interoperability across both technical and political boundaries. Just like on the Internet itself, everyone should be able to communicate with everyone else independently of their location, service provider, and software, so should the various global SSI projects connect seamlessly into a single network fabric, instead of working on isolated structures that only fit limited use cases for a limited audience.

In this project, we conducted an experiment that connects SSI infrastructures in the US and the EU, and we demonstrated that decentralized digital identity based on open standards can be globally interoperable and connected. To achieve this, we built upon existing infrastructures and use case narratives that have been developed in the US and the EU.

### 3 Details on participants

Danube Tech (EU):

- Markus Sabadello (CEO, background in standards development and EBSI/ESSIF infrastructure, <https://www.linkedin.com/in/markus-sabadello-353a0821/>) – project coordinator, planning of narratives and technical infrastructure on the EU side.
- Bernhard Fuchs (Full Stack Engineer, background in DIDs and DID resolution, <https://www.linkedin.com/in/bernhard-fuchs-66aa0414b/>) – setting up frontend demo web sites on the EU side.
- Azeem Ahamed (Software Engineer, background in DIDs/VCs and EBSI/ESSIF infrastructure, <https://www.linkedin.com/in/ahamed-azeem-b5171594/>) – developing backend components for creating DIDs and issuing/verifying VCs on the EU side.

Digital Bazaar (US):

- Many Sporny (CEO, background in standards development, <https://www.linkedin.com/in/manusporny/>) – project coordination, planning of narratives and technical infrastructure on the US side.
- Adam Lake (Business Development Lead, <https://www.linkedin.com/in/adam-lake-7a20931b/>) – project coordination and dissemination activities.
- Ganesh Annan (Product Manager, background in DIDs/VCs and US DHS SVIP infrastructure, <https://www.linkedin.com/in/ganeshannan/>) – developing

frontend and backend components for creating DIDs and issuing/verifying VCs on the US side.

## 4 Results

In this experiment, we demonstrated interoperability of experimental decentralized identity infrastructures in the US and EU. On the US side, our partner Digital Bazaar has set up infrastructure for issuing digital Permanent Resident Cards, as envisioned by the US Department of Homeland Security’s (DHS) Silicon Valley Innovation Program (SVIP). In the EU, we issued digital diplomas using the pre-production European Blockchain Service Infrastructure (EBSI). In the experiment, we successfully showed how the US- and EU-issued digital identity credentials can be exchanged between the two sides.

In the US DHS SVIP program, a key narrative is about a French citizen named "Louis Pasteur", who wants to immigrate to the US. He obtains and uses a digital US permanent resident card (PRC) as well as various other credentials (e.g., vaccination, employment, age, citizenship, etc.)


In the EU's EBSI/ESSIF ecosystem, one narrative involves "Eva", a young Belgian student. She wants to study and work in different EU member states and obtains a digital diploma credential from a European university.


Both use cases are also described in more detail in the W3C DID Use Cases document (see ["Digital Permanent Resident Card"](#) and ["Public authority identity credentials"](#)).

In this experiment, we developed and demonstrated a combined story that involves narrative and technological elements from both sides. Digital Bazaar implemented the US side of the experiment, while Danube Tech implemented the EU side, and we reused components that we have already developed during the US DHS SVIP program as well as the EU EBSI/ESSIF Early Adopter program.



We demonstrated the following two combined narratives:

### **Narrative 1: Eva studies in the EU, then wants to work in the US:**

<p><i>Eva is a student at the Graz University of Technology (Austria), which is a "Trusted Issuer" within the EBSI/ESSIF ecosystem.</i></p> <p><i>After graduating, Eva visits the university website to obtain an EU digital diploma VC.</i></p> <p><i>The university website issues the EU digital diploma VC.</i></p>	
--	---

<p><i>Eva now wants to work in the US and apply for an H1B visa.</i></p> <p><i>During the application process, she presents the EU digital diploma VC to a USCIS website in order to prove her qualification.</i></p> <p><i>The USCIS website verifies the EU digital diploma VC and performs some additional steps.</i></p> <p><i>After successful application, the USCIS website issues a visa to Eva.</i></p>	
--	---

**Narrative 2: Louis Pasteur is a permanent resident in the US, then wants to go back to the EU for PhD studies:**

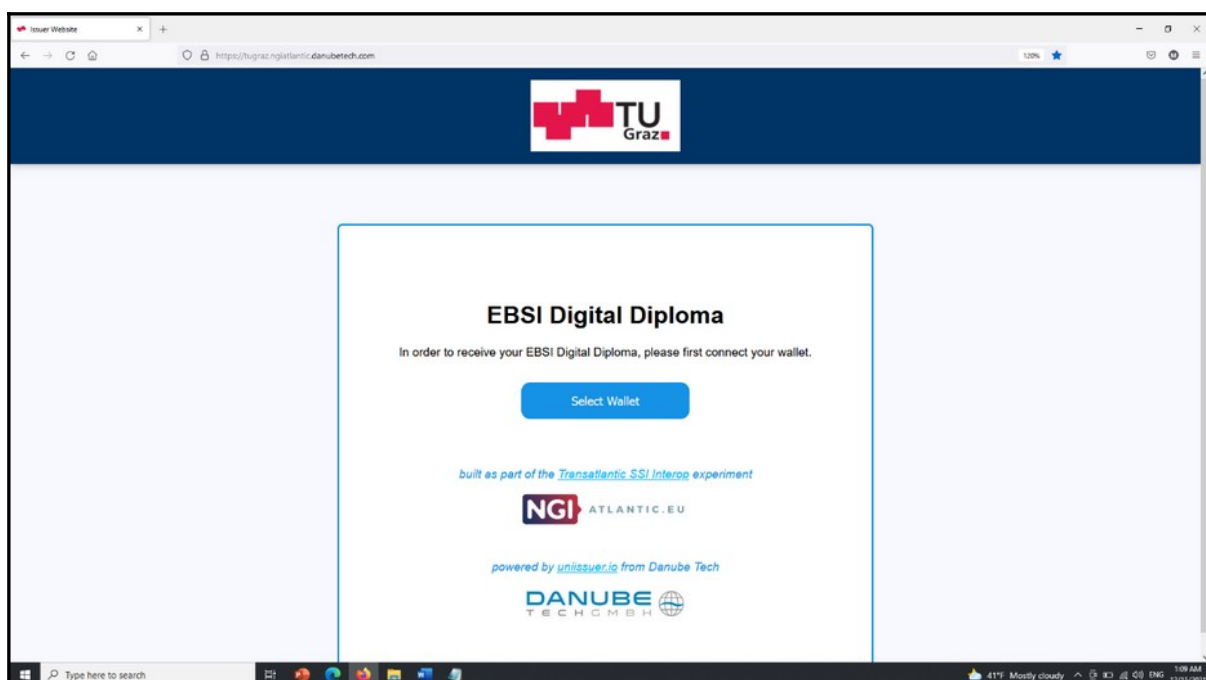
<p><i>Louis Pasteur goes through the process of obtaining a US permanent resident card VC from USCIS. He may also obtain other VC (e.g., vaccination VC, employment VC, etc.)</i></p>	
<p><i>After working for a few years in the US, Louis wants to return to Europe to pursue a PhD study program at the Vienna University of Business and Economics (Austria).</i></p> <p><i>During the application process, he presents the US permanent resident card VC as proof of his identity to the university website.</i></p> <p><i>The university website verifies the US permanent resident card VC and performs some additional steps.</i></p> <p><i>After successful application, Louis can begin the PhD study program.</i></p>	

In order to concretely demonstrate these narratives, we set up the required technical infrastructure for the experiment and have achieved the following results:

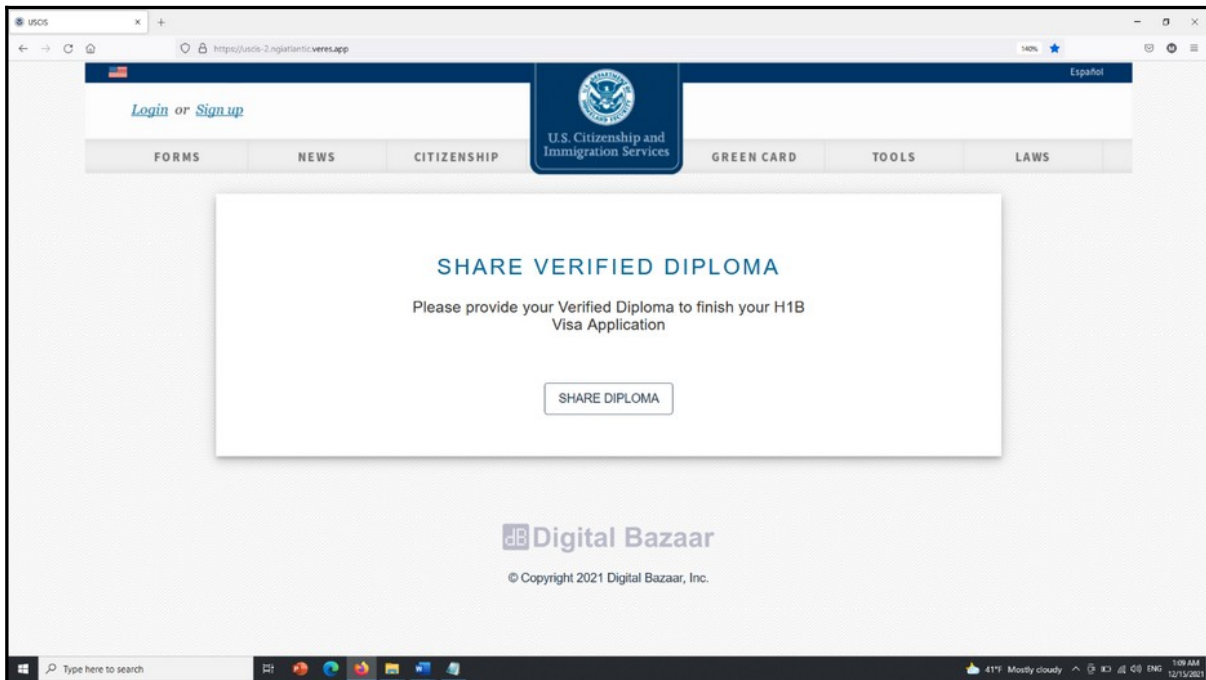
- Digital Bazaar has deployed an instance of their “Veres Wallet” that we used for the experiment:
  - <https://wallet.ngiatlantic.veres.app/>
- Danube Tech has updated the Decentralized Identifiers (DIDs) that will be used on the EU side of the experiment.
  - The DIDs did:ebsi:FqiyP831qX5xUD66CCAKMDs225QNb9Sp3UHvbJ9tSDn6 and did:ebsi:51rzpDXXCtKExG47boFBahAgd2dtfAZbQxMHM17mYKoq have been changed to did:ebsi:zuoS6VfnmNLduF2dynhsjBU and did:ebsi:z23EQVGI5so9sBwytv6nMXMo, due to updates to the underlying EBSI APIs.

- <https://github.com/danubetech/ebsi4austria-examples#dids>
- Digital Bazaar has confirmed that they are able to resolve DIDs from the EU side, using the EBSI infrastructure (also see “Discussion and Analysis on Results” below).
- Digital Bazaar has added support for the EBSI digital diploma JSON-LD context to their wallet:
  - <https://github.com/danubetech/ebsi4austria-examples#contexts>
- After discussions with Digital Bazaar, Danube Tech has updated the type of verification methods used in the DID documents on the EU side of the experiment. While previously we were using EcdsaSecp256k1VerificationKey2019, we are now using JsonWebKey2020 (see “Discussion and Analysis on Results” below).
- Danube Tech has deployed demo websites for the EU side of the experiment, based on the ones that have already been used in the EBSI4Austria project:
  - <https://tugraz.ngiatlantic.danubetech.com/> for the VC issuer in Narrative 1.
  - <https://wuwien.ngiatlantic.danubetech.com/> for the VC verifier in Narrative 2.
- Digital Bazaar has deployed demo websites for the US side of the experiment, based on the ones that have already been used in the DHS SVIP project:
  - <https://uscis.ngiatlantic.veres.app/> for the VC issuer in Narrative 2.
  - <https://uscis-2.ngiatlantic.veres.app/> for the VC verifier in Narrative 1.
- Danube Tech and Digital Bazaar have collaborated on concrete example data to be used as the actual content of issued VCs (e.g. name, date of birth, etc. of a student for the digital diploma VC).
  - On the EU side of the experiment, this example data is based on example VCs we have been using previously in the EBSI4Austria project:
    - <https://github.com/danubetech/ebsi4austria-examples#verifiable-credentials>

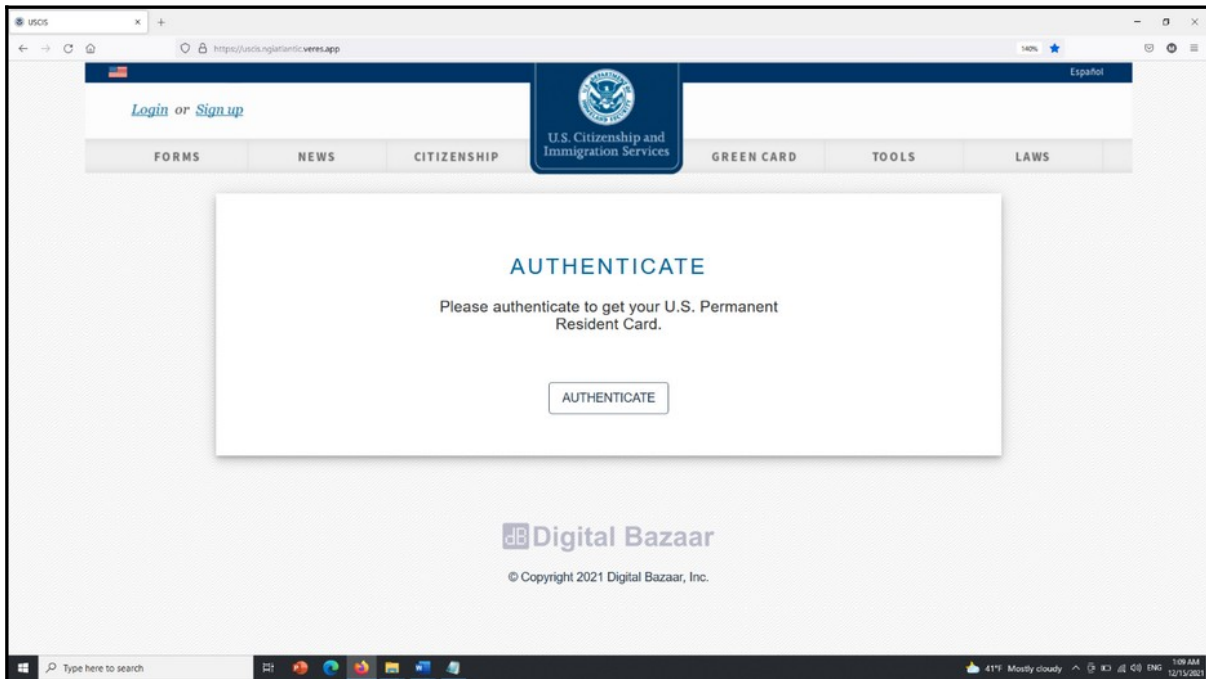
Screenshot of the VC issuer in Narrative 1 (issuing an EU digital diploma VC):



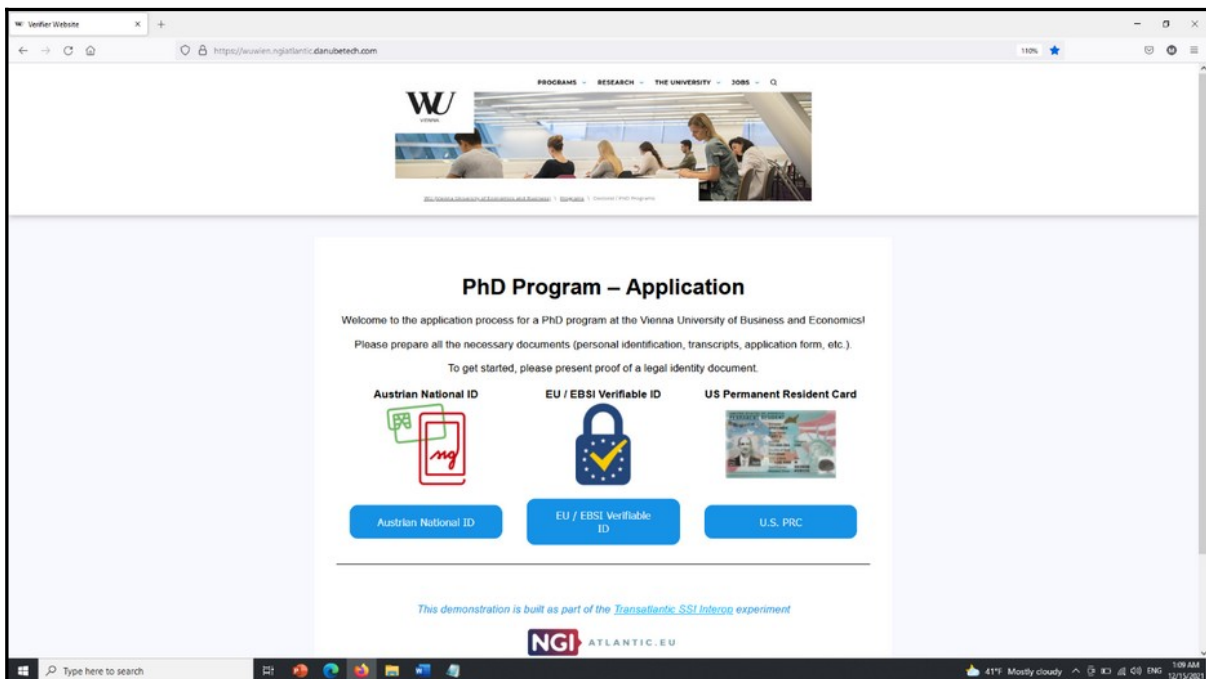
Screenshot of the VC verifier in Narrative 1 (verifying an EU digital diploma VC):



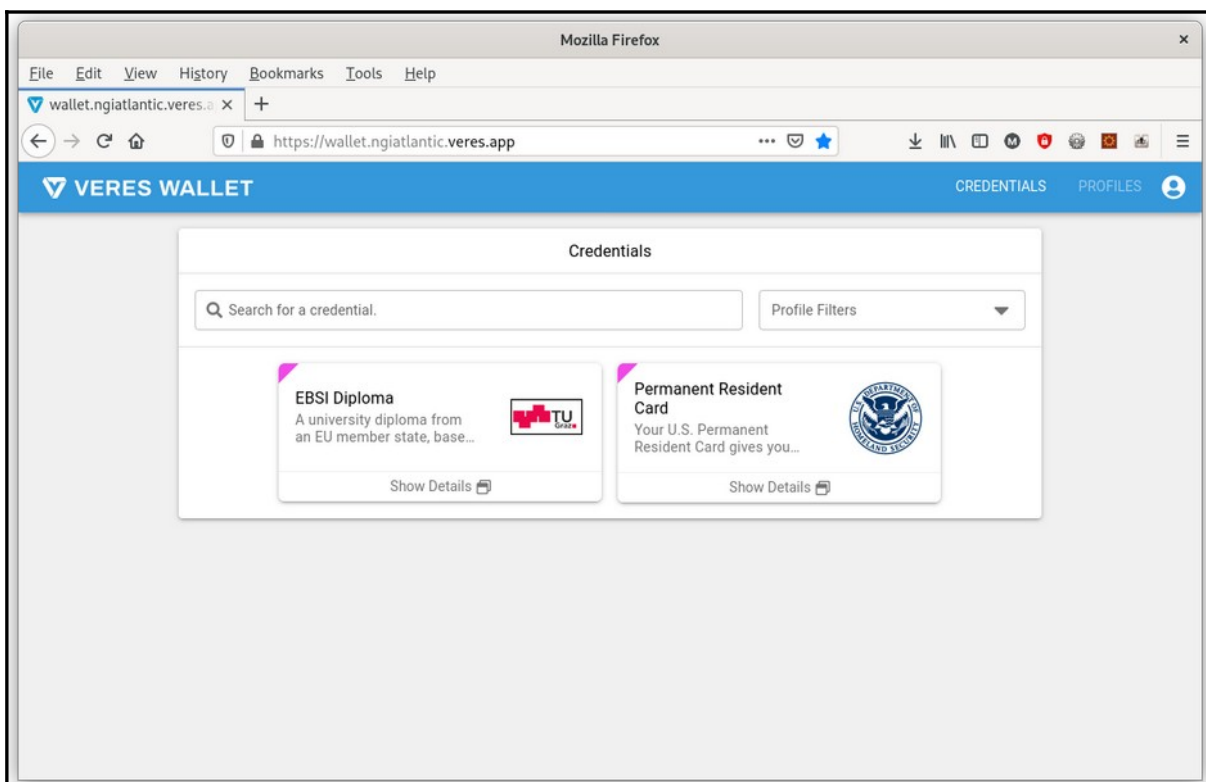
Screenshot of the VC issuer in Narrative 2 (issuing a US permanent resident card VC):



Screenshot of the VC verifier in Narrative 2 (verifying a US permanent resident card VC):



Screenshot of the Veres Wallet containing both an EU- and US-issued VC (EBSI Diploma, and Permanent Resident Card):



## 4.1 Discussion and Analysis on Results

Our analysis generally confirms our original expectations when we began the project: Interoperability between different SSI infrastructures is theoretically easy, since they are all based on shared standards, such as DIDs and VCs. However, in practice there is still a lot of coordination and planning work that needs to be done in order to be able to actually connect the different infrastructures. Both sides have to “understand” each other’s DIDs. Both sides have to agree on a number of technical aspects such as types of VCs, types of cryptographic keys and signatures, schemas, JSON-LD contexts, etc. In all these areas there tend to be nuanced difference that have to be taken into account, even though the underlying technical standards are the same.

### 4.1.1 Interoperability of DID verification methods

One particularly interesting insight so far has been the use of JsonWebKey2020. This is one out of several possible formats of so-called “verification methods”, which are essentially used to express cryptographic public key information in a DID document. At Danube Tech, we haven’t used this format very much and have instead been using other formats such as EcdsaSecp256k1VerificationKey2019 or Ed25519VerificationKey2018. The difference is that those latter formats each only support a specific type of cryptographic key, whereas JsonWebKey2020 is more universal and can be used for many different key types. This property is known as “cryptographic agility”, which is sometimes considered to be positive, and sometimes negative. In our situation, this agility has turned out to be very useful, since it enables both the EU and US side to work with different types of cryptographic keys, while only having to support a single format of a “verification method” in DID documents.

### 4.1.2 Interoperability of DID resolution

Another interesting discussion happened around DID Resolution, i.e., the process of obtaining a DID document for a given DID, which is necessary in order to be able to verify VCs. In our experiment, Digital Bazaar on the US side has to resolve EBSI DIDs. We discussed three different ways of doing this:

1. Digital Bazaar could connect to EBSI APIs directly in order to resolve EBSI DIDs, or
2. Digital Bazaar could use an existing instance of the [DIF Universal Resolver](#) to resolve EBSI DIDs, or
3. Digital Bazaar could deploy their own instance of the [DIF Universal Resolver](#) to resolve EBSI DIDs.

We discussed that option 3 is probably the most desirable from a perspective of global interoperability, since all involved parties would be able to support many different DID methods. However, for now we chose to proceed with option 1, for two reasons: First, it was the easiest approach that we could achieve in the allocated time. Second, it was also



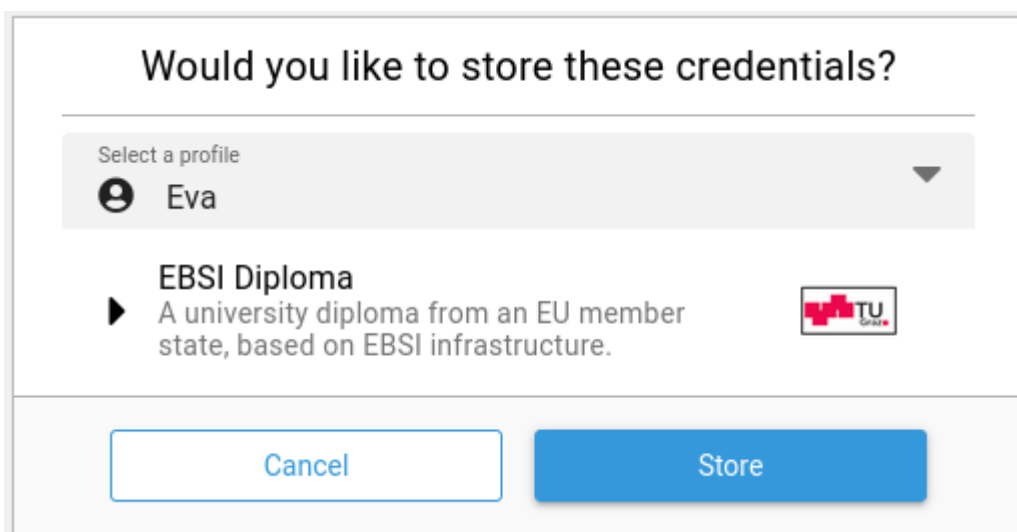
attractive for us since it meant that there was no common software used for the US and EU side of the experiment. In other words, both Danube Tech and Digital Bazaar developed and deployed all their software components independently, including the DID Resolution part, and still achieved interoperability on all layers. In the future, Digital Bazaar may still decide to change this to option 2 or 3 and use the DIF universal Resolver. Danube Tech on the EU side is already using option 3, i.e., is hosting its own instance of the DIF Universal Resolver in order to be able to resolve DIDs from both the US and EU side.

#### 4.1.3 Interoperability of VCs

On the level of VCs, we also learned several important lessons. For examples, VCs issued by Danube Tech in the EBSI4Austria project didn't include credential identifiers ("id" properties), which is not required by the W3C specification. However, while this worked fine within the EBSI4Austria project alone, credentials without identifiers caused certain complications in Digital Bazaar's wallet implementation, since management and deletion of VCs inside a wallet requires a mechanism to identify individual VCs. Therefore, we added "id" properties to all VCs in the experiment.

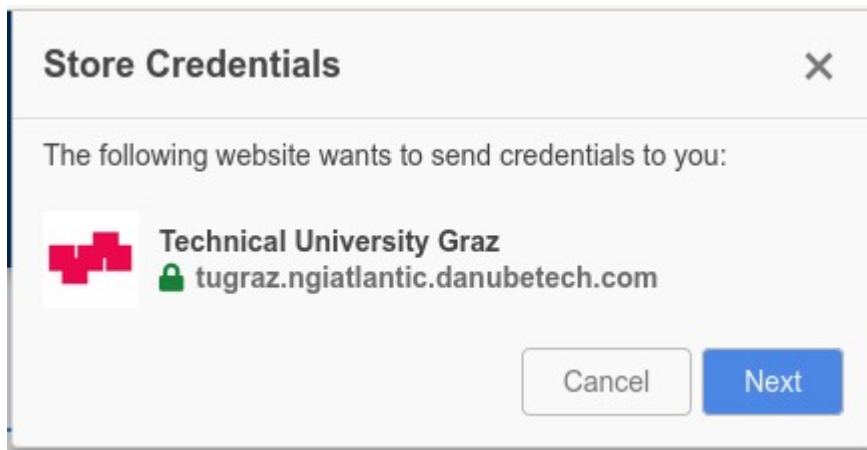
An additional optional feature of VCs are "name" and "description" properties. This hasn't been required in our EBSI4Austria project previously, however, the presence of these properties makes it easier for a wallet like Digital Bazaar's to better render VCs in the wallet UI, so that an end-user can see a human-readable name (e.g., "EBSI Diploma") and description (e.g., "A university diploma from an EU member state, based on EBSI infrastructure").

See here for a rendering of the VC in Digital Bazaar's wallet:



Another technical addition that improved user experience was the deployment of "favicon.ico" and "manifest.json" files, which enabled the wallet to render additional human-readable information about a VC issuer.

See here for a rendering of a VC issuer in Digital Bazaar's wallet:



#### 4.1.4 Additional Analysis

One challenge in general has been that the EBSI technical specifications as well as the exposed EBSI APIs are still changing. This sometimes leaves uncertainties, or even breaks existing parts of our experiment. Technical details such as the format of DIDs, contents of DID documents, types of cryptographic proofs, JSON-LD contexts, wallet protocols, and other aspects have not been finalized yet in EBSI. In some cases, in order to not endanger our experiment, we are forced to make certain choices that deviate from recent developments at EBSI. For example, while EBSI currently envisions the use of JWT Proofs for VCs, in our experiment we continue to use Linked Data Proofs instead of JWT Proofs, which is what earlier versions of EBSI technical specifications suggested, and is also more consistent with what is currently being used in the US side of the experiment.

## 5 Present and Foreseen TRL

For storing and presenting Verifiable Credentials, we used Digital Bazaar's [Veres Wallet](#). For issuing and verifying Verifiable Credentials on the EU side, we used Danube Tech's [Universal Issuer](#) and [Universal Verifier](#) software (TRL 7). On the US side, we used Digital Bazaar's [Veres Issuer](#) and [Veres Verifier](#) software (TRL 9).

We also used [open-source libraries](#) funded by the [NGI ESSIF-LAB](#) program, as well as the [Universal Resolver](#) funded by the [NGI Zero PET](#) program.

## 6 Exploitation, Dissemination and Communication Status

We have presented our Transatlantic SSI Interop project at the Internet Identity Workshop #33 on 14<sup>th</sup> October 2021. In this “unconference”-style event, attendance was unfortunately a bit lower than expected, however, those who participated in our session were genuinely interested and asked good questions.

In addition, we also presented our project at an internal meeting of the U.S. Department of Homeland Security's (DHS) Silicon Valley Innovation Program (SVIP) on 7<sup>th</sup> October 2021. Participants of the meeting included companies that are part of SVIP, as well as representatives of DHS. Feedback from the participants was that demonstrations like this could help to promote SSI, at a time when there is a certain amount of scepticism coming from the W3C standardization groups.

We have presented our project in one of the bi-weekly ESSIF-Lab IOC2 calls, where we are participating along with a number of other European start-ups who are working on SSI infrastructure.

We have also been in contact with members of the EU Commission regarding a possible extension of the project to also include Canadian entities and therefore demonstrate interoperability across three instead of two ecosystems.

We participated at an in-person workshop "Technology and Standardization" organized by the German IDunioin project. It took place in Berlin on 9<sup>th</sup> November 2021. Markus Sabadello gave a presentation on the topic of "Global Interoperability of SSI" where he also shared information about EBSI4Austria as well as our NGIatlantic.eu project.

We published a Medium post, created a Github repository, and recorded a video with information about the project and its results:

<https://medium.com/@markus.sabadello/transatlantic-ssi-interop-52bac6be8dfe>

<https://github.com/danubetech/transatlantic-ssi-interop/>

<https://youtu.be/1t9m-U-3lMk>

## 7 Impacts

**Impact 1: Enhanced EU – US cooperation in Next Generation Internet, including policy cooperation.**

We have communicated our work to representatives both of the US Commission and of the US Department of Homeland Security. We believe that our concrete initiative will help to inspire cooperation, including on the policy level.

On 15<sup>th</sup> September 2021, a panel on the topic of "Choice and Global Interoperability" took place between representatives of the EU, US, and Canada, to discuss deeper collaboration on the topic of decentralized digital identity:  
<https://www.dhs.gov/science-and-technology/svip-demo-week>

**Impact 2: Reinforced collaboration and increased synergies between the Next Generation Internet and the Tomorrow's Internet programmes.**

We are not familiar with the Tomorrow's Internet programmes, but believe that the technologies used in this experiment (DIDs and VCs) will be fundamental building blocks for many future digital infrastructures and applications.

**Impact 3: Developing interoperable solutions and joint demonstrators, contributions to standards.**

We succeeded in developing and deploying our experiment, which demonstrates concrete interoperability based on W3C standards. The fact that the experiment was developed jointly by different companies on different continents is unique and useful for the wider SSI community. We have produced concrete test data structures for the experiment, including DIDs and VCs. Also, both the US partner Digital Bazaar and the EU partner Danube Tech are heavily involved in standardization processes at W3C and other organizations such as DIF.

**Impact 4: An EU - US ecosystem of top researchers, hi-tech start-ups / SMEs and Internet-related communities collaborating on the evolution of the Internet**

This experiment has helped us deepen our pre-existing collaboration with our US partner Digital Bazaar, and also allowed us to further involve other start-ups and SMEs, through existing communities such as ESSIF-Lab and the Silicon Valley Innovation Program.

One particularly exciting development was that a key member from the Digital Bazaar team (Ganesh Annan) visited us in Vienna at the end of November, which gave us the opportunity to work closely with him for several days. This allowed us to proceed with our experiment with increased productivity, and will also generally be advantageous for the collaboration of our two companies, and the SSI community in general.

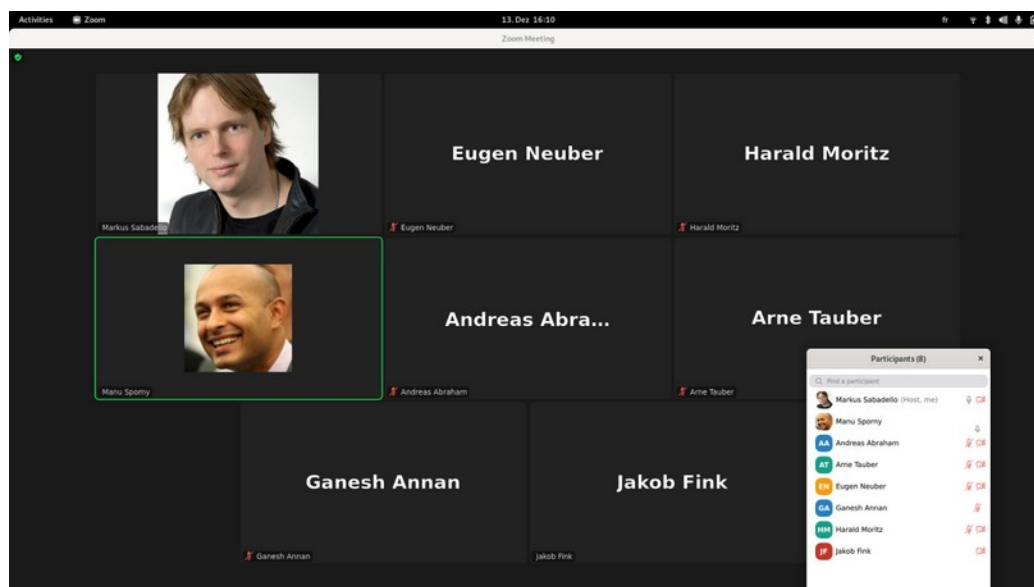
Photo of Markus Sabadello and Ganesh Annan in Vienna:



During this week, we had several joint conference calls, including one with representatives of our EBSI4Austria partners, the Graz University of Technology and Vienna University of Business and Economics, to discuss topics around digital wallets and technical specifications such as CHAPI, OpenID Connect, WebKMS, and Encrypted Data Vaults. We also discussed ongoing SSI community topics such as JSON-LD contexts, different cryptographic proof formats, and different approaches to distributed ledgers. Another very important topic was the creation of test suites for VCs, especially for the digital diploma use case.

After that in-person visit, we had an additional follow-up call on 13<sup>th</sup> December 2021 in which we further discussed technical topics as well as future opportunities for more extended international collaboration.

Zoom meeting between Digital Bazaar, Danube Tech, and other members of the EBSI4Austria project:



## 8 Conclusion and Future Work

The conclusion is that interoperability is always easy in theory if common standards exist, but there is simply no way of achieving interoperability in practice without concrete experiments like this one. We discovered lots of small issues that we would have never found if we hadn't done concrete testing.

Both the US and EU partners in this project have been involved in a number of initiatives that improve interoperability, including official W3C test suites as well as so-called “plugfests” that demonstrate how different vendors can work together seamlessly using multiple implementations of the same standards and interfaces.

This experiment has been extremely useful insofar as it showed interoperability not only between different vendors and across different use cases, but also between different continents and jurisdictions. We are convinced that this will become much more important in the next year, when SSI will continue to grow and attract more interest. Global interoperability will have to become a “default assumption” rather than an afterthought in every SSI initiative, and we hope that this experiment will serve as a blueprint for future similar activities. Danube Tech and Digital Bazaar are committed to continuing work in this direction, together with our friends and partners in the wider SSI community.

## 9 References

Planning Document:

[https://docs.google.com/document/d/1n\\_Ge-8Z0-zO3a\\_p\\_A1i8Nm\\_WT9L3jCpOtFmhTsYvFoA/](https://docs.google.com/document/d/1n_Ge-8Z0-zO3a_p_A1i8Nm_WT9L3jCpOtFmhTsYvFoA/)

Presentation on EBSI/ESSIF:

[https://www.eesc.europa.eu/sites/default/files/files/1\\_panel\\_-\\_daniel\\_du\\_seuil.pdf](https://www.eesc.europa.eu/sites/default/files/files/1_panel_-_daniel_du_seuil.pdf)

Silicon Valley Innovation Program:

<https://www.dhs.gov/science-and-technology/blockchain-portfolio>

## 10 Glossary

5G	Fifth Generation (mobile/cellular networks)
NGI	Next Generation Internet
R&D	Research and Development
SDN	Software Defined Networks
TRUST-IT	TRUST-IT (Project Partner)
VNF	Virtual Network Function
WIT	Waterford Institute of Technology (Coordinating Partner)
DID	Decentralized Identifier
VC	Verifiable Credential
DHS	Department of Homeland Security
SVIP	Silicon Valley Innovation Program
EBSI	European Blockchain Service Infrastructure
ESSIF	European Self-Sovereign Identity Framework

## **Deliverable 3: Part II**

### **Financial and cost information**

This part is to be treated as a consortium confidential deliverable, and access is restricted to consortium partners and EU commission operatives.