conclusion as of 08/03/2023 @13:30

11 Conclusion and future work

The goal of this paper was to propose a UDT architecture and identify its security risks. To do so, the UDT architecture was split into 6 layers themselves divided into two zones. One controlled by the city actors the other controlled by the UDT federation. From this divide, requirements covering the layers under the authority of the federation were derived from literature reviews and associated with each layers. This approach allowed to clearly identify at which architectural level each requirements could be covered. The main points that came out from the identified requirements were:

- The need for a governance framework due to the multi actor component of UDT
- The need for heterogeneous data integration
- The need to define the trust model gauging the relationship between city actors and the federated UDT platform
- The need for security and data quality standards
- The need for real time data streams

From there a general micro service architecture framework was derived covering some of the technical requirements. That architecture was then evaluated against the STRIDE threat model which permitted the identification of 3 high threats namely:

- Message broker single point of failure
- Access control management
- Access control bypass

3 threats of high risk

proposed solutions

Mitigation addressing each of these high threats were proposed making use of client certificate authentication, user-managed access control (UMA) and message integrity guarantees via the use of digital signatures. Taking into account these mitigation point a POC proposal was then presented with technical implementation details.

Not all requirements identified were covered. Requirements centered around governance, security and quality standards were omitted. Further research is required with concrete use cases and data to determine the type of non architectural standards to foster the creation and adoption of UDT. This led to certain assumptions in our architecture proposal mainly centered around the type of trust the city actors would have over the UDT federation. federation has ALL the power

In the creation of the PKI infrastructure the assumption taken was that the UDT federation would want each city actor to independently manage their identities. The use of Certificate Transparency system ensuring a transparent view over the list of valid identities accepted on the platform and their origin.

where i come in ?

For the UMA proposal, the assumption taken was that city actors would trust a central access control system managed by the federation. However if that level of trust changes, other implementations such as smart contract access control methods would need to be considered. As they allow for transparency and non-repudiation over the access rights that an entity may have over a resource.

To conclude, this paper sets the base for a high level UDT architecture and requirements. A base that should be extended with further research centered around, its current technical implementation feasibility, around the type of trust model that it should abide by, around its ability to actuate back in real time onto the physical world and around concrete use cases to determine its capacity to become a production ready UDT solution architecture.