What is Citadel?

Citadel is a self-sovereign identity (SSI) protocol that runs integrated into Dusk Network. It can be seen as a framework for SSI solutions, as anyone can use it for their own use case. We call SSI to those systems allowing users to manage their identities, their personal information, in a fully transparent manner: knowing at each time which information about them they are sharing, being able to consent or deny each request for personal information.

How does it work?

We have a user and a service provider SP. The user wants to use a service provided by a SP. To do so, the user needs to request a license, a set of attributes that represent his right to use that service. This license could be seen also as a "certificate" that we need to "show" to be provided with the desired service, but there are many technical differences. There are many approaches to request a license, for instance, issuing a payment in Dusk.

After paying for the service, the SP will provide a license to the user's account, without knowing which account it is. From now on, the user can prove possession of a valid license in ZK.

The cool thing is that it is not necessary for the SP to be the same one that issued the license. The license can be issued by another party the SP trusts, and the user provides a proof that he owns such a license.

Where does it come from? Why is there such a need?

FORT, our previous research on the field, stated a novel way to acquire rights (a.k.a. licenses), and prove their ownership. However, it lacked two main features. First, it relied on non-ZK-based blockchains like Ethereum. This means that, even when the protocol itself is performed in ZK, the storage of such licenses is done as public NFTs on the Blockchain. Citadel overcomes this problem thanks to the usage of Dusk, becoming what we call a full-private-by-design protocol.

Second, FORT allows us to spend licenses, but only the SP we are interacting with is aware of it. This means that, in the case of having a license representing a spendable ticket within a set of SPs, only a single SP will know that. With Citadel, we have "decentralized nullification": the whole network verifies that a license can be spent, without learning anything about the user, the license, or the service that is being used. Furthermore, this same approach also solved another problem: malicious SPs or eavesdroppers could impersonate a user upon receiving their valid license, by reusing the involved ZKP. However, decentralized nullification prevents such an attack.

Which are the main properties of the protocol?

We can summarize them as follows.

Proof of Ownership: a user of a service is able to prove ownership of a license, by means of a ZKP, that allows them to use such a service.

Proof of Validity: our solution introduces the possibility that SPs can revoke the licenses they issued, later on. Users can prove ownership of a valid license that has not been revoked.

Unlinkability: the SP cannot link any activity of their users with other activities done in the network.

Decentralized Nullification: our system solves the problem regarding the possibility of reusing the licenses, where a malicious SP could impersonate the user after receiving a valid one: by means of an on-chain and decentralized nullification, like done in the standard stack of Dusk, the ZKP proving ownership of a valid license cannot be reused.

Attribute Blinding: the user is capable of deciding which information they want to leak to the SP, blinding the value and providing only the desired information.

Other more technical properties: It runs integrated into a L1 ZKP-based Blockchain: Dusk. The whole protocol has been designed around it: full-private-by-design architecture; proof generation delegation; retrieve all information knowing only the secret key; etc.

Which are the novelties?

Users can prove their licenses in ZK, what we called Proof of Ownership. This by itself is not a novelty, but we are providing this feature along with all the other ones. This is the novelty of the protocol. Especially what is explained in the section "Where it comes from?".

Additional uses

This is just one way that Citadel can be used. Citadel offers much more than can be described in a single article, so expect more information and use cases in the future.

Citadel offers access to services without having to share personal data or information. This is practical, efficient, and preserves privacy for users. We're so used to having to share and expose our personal data to gain access to services that it's hard to imagine not needing to do this.

It has benefits for companies and provides relief from GDPR which is currently a heavy burden for companies to bear. By allowing users to access services and membership etc without sharing their identity or data, there is nothing that needs to be "forgotten" to comply with GDPR. This will be a huge relief for companies operating in the EU.

It offers protection from hacks and data leakages. From LastPass to Celsius to the countless hacks and leaks you won't have heard of, companies simply won't have this data so there's nothing to hack. This is good for institutions as it makes them more secure and is good for users who don't have to trust a 3rd party to look after their most important data.

Citadel changes the relationship between users and providers and eliminates the need to swap your identity for access, and the security and management needed to keep that identity private. And it does so in a way that is compliant to regulations, providing a real and necessary solution to the challenges users and companies face, and will continue to face as more and more parts of life go online.