Project Title: Blockchain infrastructure will be introduced in the National ID Card.

Motivation

Authentication with a username and password is becoming an inconvenient process for the user. End users typically have little control over their personal privacy, and data breaches affecting millions of users have already happened several times. There will be a system where a user can get all the services in one place. The user does not need to go to many systems to get each service. Users don't need to memorize usernames and passwords for different services. In each system, users are not required to provide all of the information.

Many websites support Facebook and Google single sign-on (SSO) solutions for end users. Unfortunately, this comes at a cost in terms of privacy. Often, the business interests of such centralized service providers like Facebook and Google are not aligned with the users' interests. This may lead to the users' data being used beyond their intention when initially sharing it. Users could still seek the benefits of the SSO customer experience of not having to register at each web site without sacrificing their privacy. The idea of our research aims at a solution to this by decentralizing digital identities.

Proposed Idea

Firstly, users just have to register themselves in our system. Then they have to give some information to get it verified. When they are verified by the government, the government will issue them a government ID.

Secondly, after getting the government ID, they can use other services. If they want their birth registration certificate, they just have to give their government ID number. When they give their ID number, the system will retrieve all the information from the system and a birth certificate will be generated. Using the government ID and birth certificate ID, they can get a national ID card. These three ID numbers will be needed for getting other services. This means these three IDs are the primary DIDs. After that, users can apply for a driving license, open a bank account, trade license, and so on.

The information that the users have to provide to get the government ID:

- User's complete name
- User's father's name
- User's mother's name
- User's date of birth
- User's mobile number (if he is under the age of 16, he can register himself using his parents' mobile number)
- User's father's nid card in pdf format.
- User's mother's nid card in pdf format
- sex (male/female/other)

- present address
- permanent address
- educational qualification
- User’s occupation details: student/job/housewife-if a job, then have to give job details.
- nationality
- Proof of nationality is required in the form of a utility bill/wasa bill in the name of his parents or householders where they live.
- His photo
- Signature

Our Main Concern

Decentralizing the currently highly centralized digital identity ecosystem to deliver more control, privacy, and security for the end users with blockchain has been an agenda of this research.

1. Decentralized Identifiers(DID)

   A decentralized identifier (DID) provides a verifiable and decentralized means for interacting with a DID subject controlling the DID. A DID can be resolved into a DID Document, which can contain cryptographic material, verification methods, and service endpoints. A DID is not meant to provide trusted personal information about the DID subject on its own. Instead, it is intended to give the DID holder more control over their own life and allow them to be more private.DLT is a framework called Hyperledger Indy that makes it easy for people to get decentralized identifiers (DID) for themselves.For example, with Indy, an identity holder like Alice is expected to have a single DID for each connection. The bank and the college can use the same DID to link up any personal information they have about Alice. This is because Alice has one DID when she interacts with her school.

2. Verified Credentials(VC)

   DIDs let users authenticate themselves online in a privacy-preserving and decentralized manner, but in many use cases we need to obtain trusted information about one’s identity to carry out certain transactions. This can be achieved by using Verifiable Credentials (VC), which complement DIDs by providing a means for receiving trusted identity information from end users that is cryptographically verifiable. In general, VC provides us with a digital equivalent of the credentials we use in our daily lives, like a driver’s license, a passport, or a university degree, in a secure, privacy-preserving, and machine-verifiable manner. Selective disclosure means end users can prove their identity without disclosing more information than is required to perform a specific action. VCs can show any information that a physical credential can show, but the use of digital signatures from both the issuer and the identity holder makes them tamper-proof and more trustworthy to the person who is checking them out.

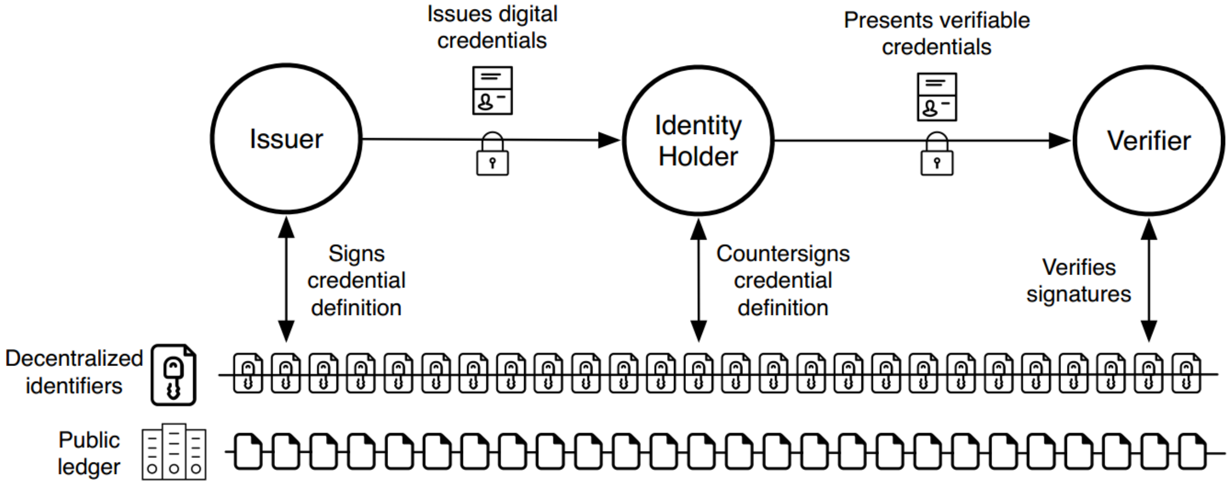
Issues digital credentials
Presents verifiable credentials
Issuer
Identity Holder
Verifier
Signs credential definition
Countersigns credential definition
Verifies signatures
Decentralized identifiers
Public ledger

Fig: The Verifiable Credential (VC) role model includes an issuer, an identity holder, and a verifier. In addition, there is a publicly readable verifiable data registry, which can be a blockchain, a distributed ledger, or any secure decentralized storage. For example, a municipal office (issuer) issues a passport credential to Alice (identity holder), who then presents it to her bank (verifier), when opening a new account.

Current Status of the project and Challenges

Above, I tried to give a conceptual idea of our project and how we are going to design our system. I started working on this project on the basis of this concept. During the analysis, I encountered some troubles, such as how we can authenticate a user with our system or how a user can be verified to use our system.

The challenges are:

- User authentication
- Credential verification
- Credential Store

As our idea is similar to self-sovereign identity, it has to be a decentralized system. For a user, there will be decentralized identifiers; for verification, there will be verified credentials; and, of course, we have to think about credential storing systems. We cannot use any central database like MySQL or NoSQL for user authentication, credential verification, or storing verified credentials there. If we use any third-party central database, then our idea will be compromised.