Concordium ID

Concordium's innovative identity layer is designed to provide a solution to the adoption of blockchain technologies across regulatory regimes. The goal of the identity layer is to provide privacy for its users, while at the same time achieving accountability in the sense that in the presence of a reasonable suspicion, law-enforcement agencies will be able to identify a given user based on their real-world identity and access their transaction history in a way similar to what is guaranteed today by traditional financial institutions.

This document provides an overview of the design of Concordium's identity layer in terms of protocols and entities involved. The ID layer has been proven secure in [DGKOS21].

There are three types of entities in the identity layer.

Users

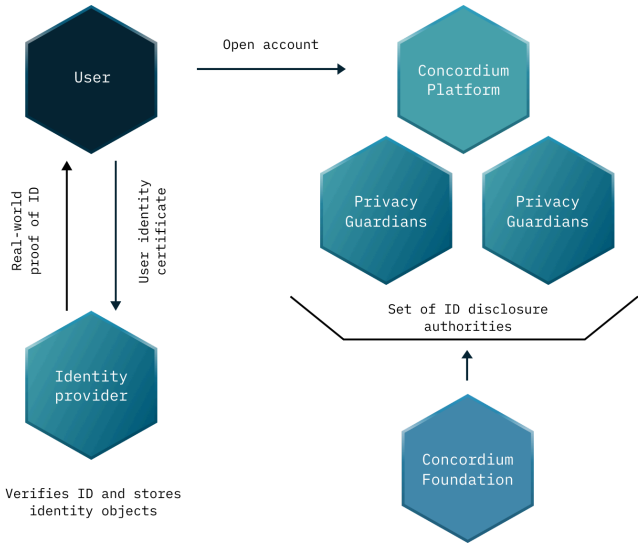
Users are interested in creating accounts and performing transactions on the Concordium blockchain. A user—be it an individual, a business, or a physical device—cannot hold an account on Concordium without registering with an identity provider.

Identity Providers

The first step towards creating an account on Concordium is to obtain a **verified Concordium identity** from an **identity provider**. An identity provider is an organization, approved by Concordium, that performs off-chain identification of users.

As part of the identification, an identity provider collects and verifies several user **attributes**, such as name or passport number. Once this information is verified, the identity provider issues an **identity object** which contains information about the user structured in an ID schema. Information supporting an ID verification, used prior to issuance of the identity object, is held alone by the ID providers in their own off-chain records.

A number of ID schemas have been defined to manage various kinds of users. Personal IDs include name, date of birth, and ID card number. Business IDs include company registration number, official address, and so on.



Privacy Guardians & identity disclosure process

Privacy guardians exist to counter one of the most troublesome issues of blockchains today: the fact that bad actors believe they can act with impunity and no fear of prosecution. The very presence of bad actors in the same system dissuades corporate and professional users due to the immense reputational risk by association.

Privacy guardians are the interface between authorities and users of the Concordium blockchain. They will receive court orders in their jurisdiction, which will demand the privacy guardian to provide all information that enables deanonymizing a certain user. This process will vary depending on the country and is the output of a legal process. The privacy guardian will provide the decrypted user identifier which also contains details of the identity provider who issued the Concordium identity to the authority. By way of a second court order, served to the identity provider, the identity of the user can be revealed. It is the requesting authority who is required to serve the two court orders.

Privacy guardians are typically legal firms which are adept at handling identity disclosure requests in compliance with the process and court orders from the authorities. The privacy guardians currently working with Concordium are law firms from Switzerland, the location of the Foundation. They have been approved to perform the identity disclosure process by the Foundation. As law firms, they are able to work correctly with the authorities. The cost of the identity disclosure process is covered by the Foundation.

Details needed for creating a verified Concordium ID

Person

To establish an account as a person, you will need to supply the identity provider with a government-issued ID, such as a passport or a driver's license with a photograph as part of the document.

Businesses

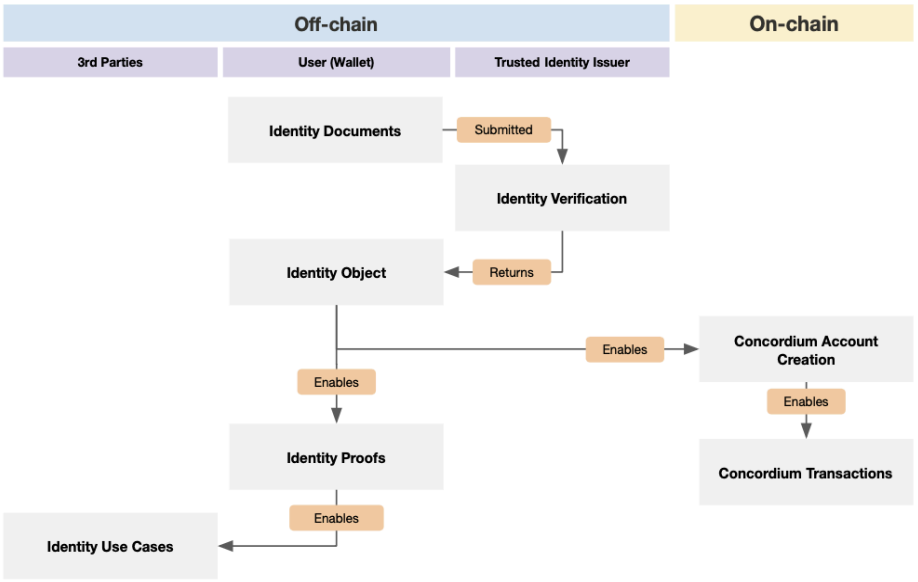
Business verification is typically a more comprehensive exercise, as there are more parameters to take into account. These include business or LEI numbers, registered and/or business addresses, names of directors, and details of signing rights.

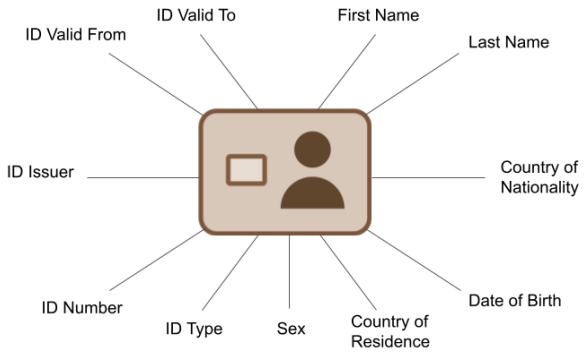
Detailed identity processes

Details of the identity processes for creating an account on the Concordium blockchain and for identity disclosure can be found here.

Proving Statements About Identity Attributes

The new generation of Concordium wallets allows users to store and manage their attributes that have been issued by identity providers. A user by being in control of their wallet can decide in a self-sovereign manner how and when to provide their attribute information to applications. When an application needs to verify some statements of attributes, the user can generate a zero-knowledge proof that attests to the truth of the requested statement. This allows users to convince the application that they meet verification requirements without their personal data, apart from the statement, ever being collected. For example, one can prove that "I am older than 18 and I am a resident within the EU".





Schema of example attributes for a person

Technology

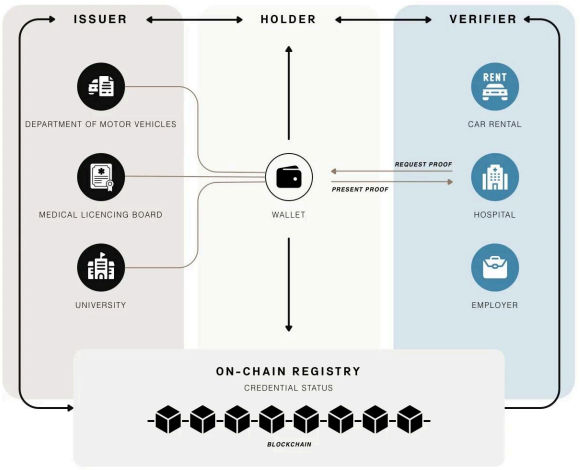
Concordium uses two types of non-interactive zero-knowledge proofs:

- Classic **Sigma protocols** are used to prove (in)equality of an attribute with a public value.
- **Bulletproofs** are used to prove
  - Set (non-)membership of attributes in a public set
  - Range proofs, e.g., attribute <= public value

The **Fiat-Shamir** transformation is used to make the protocols non-interactive. In the future, Concordium will use SNARKs to prove more general properties of the attributes efficiently.

Verifiable Credentials and Web3 ID

In 2023 Concordium introduced **Web3 ID**. The web3 ID infrastructure allows any company or individual—under some requirements—to become an **Issuer** and attest to claims about users (**Holders**) in the form of verifiable credentials. Holders can use the credential to prove, in zero-knowledge, arbitrary statements about their attested claims to other parties (**Verifiers**). Apart from off-chain attestation, the status information of the issued credentials (e.g., expiration date, revocation status, etc.) is also stored on the Concordium blockchain. To verify a claim, the verifier checks the validity of the proof provided by the holder and the on-chain status of the credential. The trust level of proven statements depends on the trust level of the issuer. Anyone with an account on the Concordium platform can become a holder and an issuer.



References

[DGKOS21] Damgård I., Ganesh C., Khoshakhlagh H., Orlandi C., Siniscalchi L. (2021) Balancing Privacy and Accountability in Blockchain Identity Management. Topics in Cryptology – CT-RSA 2021. Lecture Notes in Computer Science, vol 12704. Springer, Cham. https://doi.org/10.1007/978-3-030-75539-3_23