Identity Processes on Concordium Blockchain

Identity Process on Concordium Blockchain

This document outlines the approach to the Identity Process on Concordium blockchain which is geared towards providing secure blockchain infrastructure which maintains accountability while preserving user privacy

Key Participants

Participants in Concordium's identity solution.

- **Users:** These can be individuals or businesses who are interacting on the Concordium blockchain. Users are unable to do so without undergoing an Identification Process
- **Identity Providers (IDPs):** 3rd party organisations which provide off-chain identity verification. Currently Notabene, Digital Trust Solutions and Global Finreg (for businesses) are available to provide identity verification. There is the potential to add additional IDPs in the future.
- **Privacy Guardians (PGs):** Authorized entities which participate in Concordium's Identity Disclosure process if required. PGs are typically legal firms which are adept at handling Identity Disclosure requests in compliance with the process and court orders from the Authorities.
- **The Authority:** The party that initiates both legal scenarios by obtaining court order(s). The court order must originate in the governing jurisdiction in which the PG is based, a second court order from the jurisdiction of the IDP is also required if the IDP is in a different jurisdiction than the PG. The Authority is the only entity that has the full power to learn all information that can link the person, Account Holder, accounts, and transfers.

Key Concepts

- **Account**: An account is used to send and receive funds on the Concordium chain.The account is associated with the user's identity, however this association is encrypted and can only be disclosed through the Identity Disclosure Process
- **Identity Credential**: An identity credential contains attributes on a user's identity. It is used to open accounts on-chain. These credentials are issued by identity providers during user onboarding and are derived from an identity document (e.g. a passport). The IDP keeps an identity record within their database. Identity Credentials are also stored within the wallet application. Concordium does not have any access to the user information within the

identity credential. Individual attributes from the user's Identity Credential can be shared by the user from their wallet with minimal data exposure using zero knowledge proofs.

- **Identity Disclosure Process:** Unique to Concordium, in cases where an Authority suspects suspicious behaviour and wants to open an investigation, a process can be followed with multiple stake holders (Authorities, IDPs and Privacy Guardians) to disclose the identity of the user of a given account or the finding of all accounts of a given user.
- **Base Layer ID:** This is the identity system described above where users open accounts with identity credentials.
- **A Wallet:** is a secure application that allows users to manage their accounts, hold and transfer tokens on the network, and store identity credentials issued by Identity Providers. It also enables users to generate zero-knowledge proofs to share verified identity information without revealing personal data.
- **Seed (Phrase):** Secret randomness that is created on wallet initialization. All cryptographic material needed for identity credential and account credential is derived from this seed. This allows users to recover their Concordium accounts from the seed phrase.
- **Public Holder Identifier:** An encrypted mapping between the users identity credentials and their account. This identifier requires a court order and multiple Privacy Guardians to be decrypted.
- **Account Holder Identity Records:** A collection of records related to the account owner, including their identity information and an encrypted key that links to any other accounts opened with the same identity document.This data is stored in the IDP's database.

Principles of Privacy

Concordium's identity system has been designed to be privacy first, and applies the following principles:

- Users personal identifiable information (PII) such as name, birthdate etc, are never available on chain, either encrypted or unencrypted.
- PII is only stored locally within the user's wallet and within the database of the identity provider to be used if required as part of the Identity Disclosure process. For avoidance of doubt, Concordium does not have access to any of this user information.
- No single party can link a user's Identity to the accounts they have on Concordium. This can only be done through the Identity Disclosure Process
    - IDPs cannot identify a user's account (or on chain wallet address). They cannot connect an identity to on chain activity or an address.
    - A single Privacy Guardian cannot decrypt a user's Public Holder Identifier, this means they cannot access the mapping between a user's

identity and their on-chain presence. In addition they do not have access to the Identity Record data which is stored within the IDP's systems.
    - It is only possible to connect a user's PII identity to an account by following the identity disclosure process.
- With Concordium, users can choose to reveal zero knowledge proof verifications of individual attributes of their identity, without revealing the underlying data (e.g. proving they are over 18 without revealing their birth date)

Initial Setup

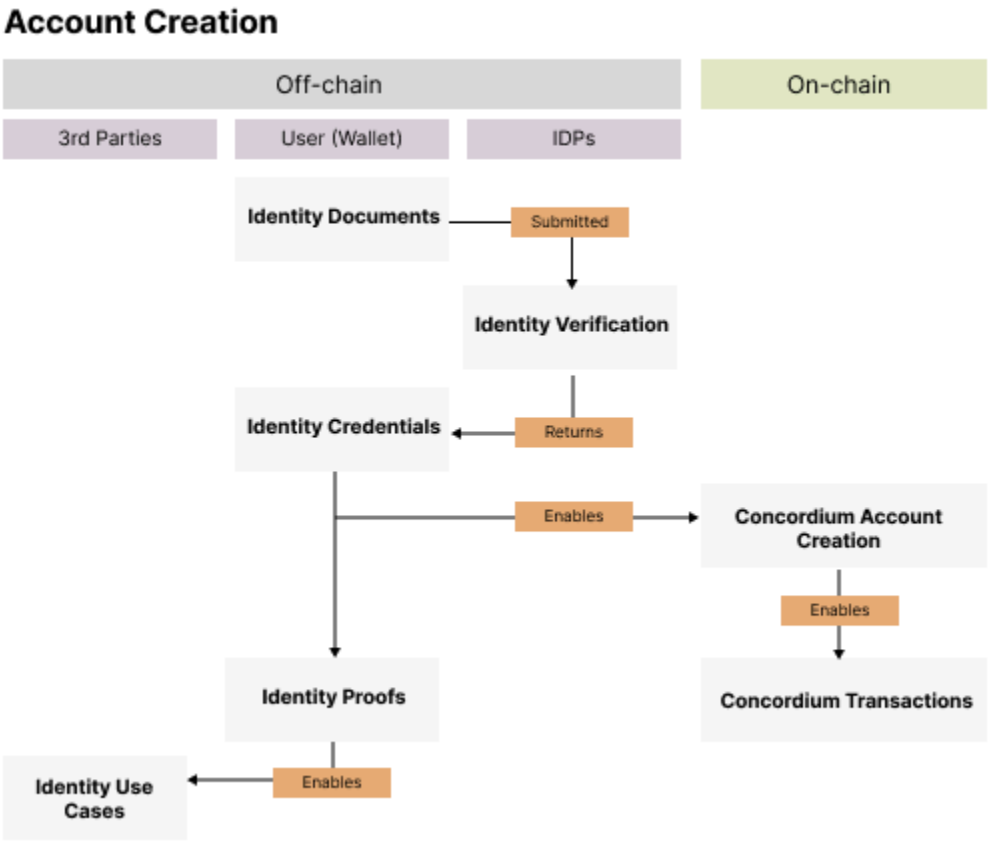
Users must complete an identity verification process to create an Identity Object which allows them to create an account and become a participant on the Concordium network. This guards against unknown actors operating on the network. Wallets in the Concordium ecosystem hold both identities (stored as identity credentials), and accounts (which contain cryptographic addresses). Every account must be linked to an Identity credential. This means on wallet and account setup, a user must complete the identity verification process with an IDP. Users can have multiple accounts under a single Identity Credential, and they can store multiple Identity Credentials within a wallet application.

Account Creation

1. A user downloads their chosen wallet application; mobile, browser and desktop are available. A stand alone identity app will be available in the future, which will allow users optionally to manage their Identity Credential without using a crypto wallet.
2. Within the wallet, the user initiates a request for the creation of an Identity Credential by selecting their IDP of choice.
3. The user is prompted by the IDP to scan an identity document (e.g. a passport) and to undergo an ID Verification process. Businesses can also identify through a similar process, but the requirements vary and will need additional corporate documentation.
4. The IDP follows their standard identity verification process and verifies the validity of the identity document and complete any other checks.
5. For new users the IDP creates an Identity Credential which is stored in two places, in the user's wallet application and within the IDP's systems ("the identity record") for reference as required for the IDP's participation in the Identity Disclosure Process. It's important to note that the IDP does not store associated wallet addresses alongside the Identity Credentials. IDPs are not able to unilaterally map identities to addresses.
6. Once the Identity Credentials have been verified and stored (within the user's wallet and the IDP's system), the user can create an associated account, this

contains a public and private key, to send and receive tokens. Multiple accounts can be created underneath an Identity Credential.

7. For returning users, the IDP recreates an Identity Credential. A user can then use their existing accounts or create a new one.
8. Users can add multiple Identity Credentials within the same wallet application. However to create a new identity, as opposed to a new account, a user will need to complete an additional identity verification process with their chosen IDP.



Verifiable Credentials with Web3ID

As an additional supplementary feature to the base identity provided on wallet creation, verified credentials can be issued to a user to power enhanced use cases.

Web3ID is based on the W3C standards for verifiable credentials. This makes them portable and interoperable. Verifiable credentials can be used for KYC, compliance and regulation, for example to identify accredited investor status. Identity data, both

BaseID and Web3ID verifiable credentials, can be used for off chain uses such as zero knowledge age verification.

Identity Disclosure Process

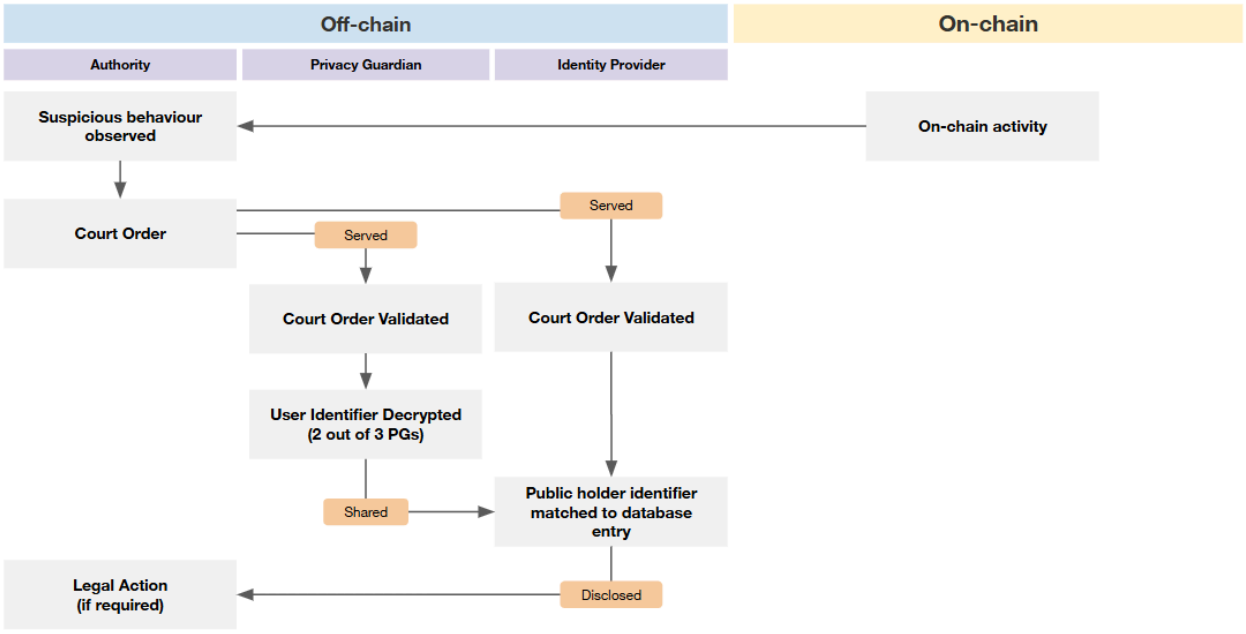
There are two legal scenarios in the context of Identity Disclosure on the Concordium blockchain, i.e., **investigation of on-chain activity**, initialized with an account number, and **investigation of a person of interest**, initialized with off-chain identifying data of a person.

To maintain the integrity of the process, all communication should occur to and from the Authority "in the middle". There is no direct communication required between Identity Provider and Privacy Guardians, nor amongst the set of Privacy Guardians.

Legal scenario 1: Investigation of on-chain activity

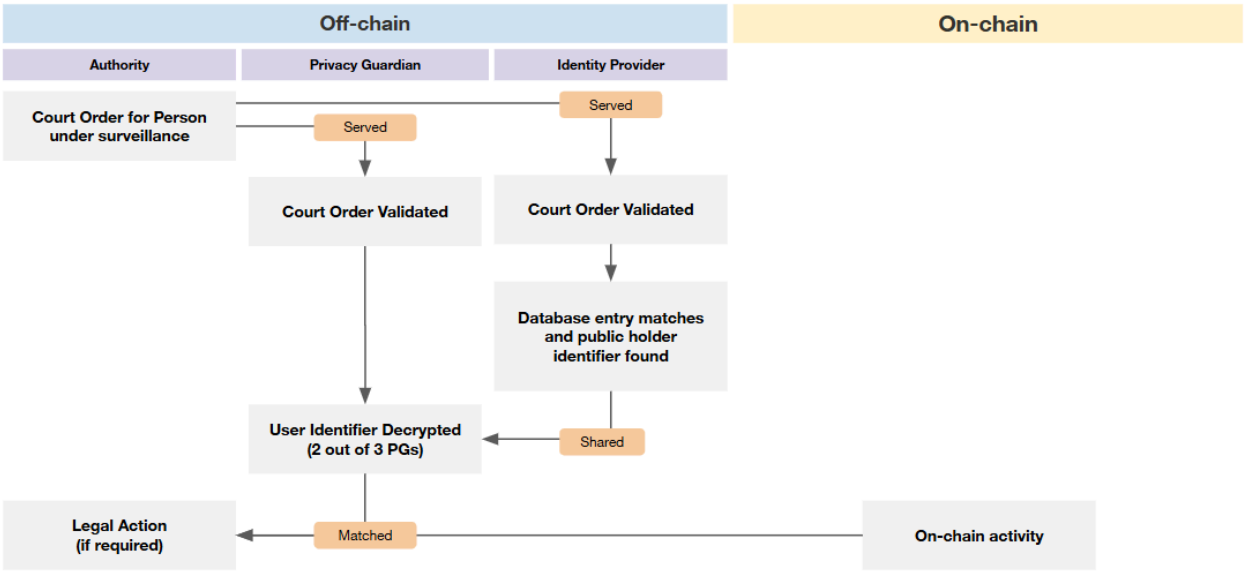
1. The Authority that is conducting the investigation must obtain a court order from the legal jurisdiction of the Privacy Guardian (PG).
2. The Authority initiates the identity disclosure process by presenting an official court order to the PGs from their respective jurisdictions, along with the encrypted *public holder identifier* (obtained from blockchain data) corresponding to the account being investigated.
3. Each PG uses its private decryption key to decrypt its share of the *public holder identifier* and transmits the resulting string back to the Authority.
4. Upon receiving the necessary threshold of valid responses (currently 2 out of 3 threshold), the Authority combines the decrypted shares to reconstruct the public holder identifier.
5. The Authority issues a formal request and submits the reconstructed public holder identifier to the relevant Identity Provider (IDP). If the IDP is in a different jurisdiction than the PG, an additional court order needs to be obtained by the Authority from the home country of the IDP.
6. The Identity Provider searches its internal database for a match to the public holder identifier provided by the Authority. Upon having located the database entry corresponding to the public holder identifier, the IDP sends the account holder identity record to the Authority. At this point, the disclosure process has successfully revealed a verified identity for an account or wallet address.

Once the identity has been revealed, it is possible to find additional accounts that are linked to it. This can be done via a full person to accounts disclosure scenario (detailed below) or via encrypted mapping information stored in the IDP. Both are dependent on a court order.



Legal scenario 2: Investigation of person of interest

1. A court order is required to start the disclosure process by the Authority in the jurisdiction(s) of the IDPs. The Authority sends the identifying data of a real-life person together with the official request to all IDPs on Concordium.
2. The IDPs check their system for account holders that match the identity data they received from the Authority.
3. If the IDP(s) can identify one or several database entries matching the user, then the IDP(s) sends all the corresponding account holder identity records to the Authority. Each record contains an encrypted key, which allows the identity to be linked to the accounts opened with this identity.
4. These encrypted keys are then sent to the PGs along with a court order from their jurisdiction by the Authority. The PGs decrypt their share of each key and return the resulting strings to the Authority.
5. Once the Authority has collected the required threshold of shares (currently 2 out of 3 threshold) for a key from the PGs, it reconstructs the full key.
6. Using the reconstructed keys, the Authority retrieves the list of all accounts associated with each account holder identity record across all IDPs.
7. The Authority takes appropriate action based on the retrieved account and transaction information.


Off-chain
On-chain
Authority
Privacy Guardian
Identity Provider
Court Order for Person under surveillance
Served
Served
Court Order Validated
Court Order Validated
Database entry matches and public holder identifier found
User Identifier Decrypted (2 out of 3 PGs)
Shared
Legal Action (if required)
Matched
On-chain activity

Document version control

Date	Version	Author	Action	Updates
01/05/2025	0.1	Rachel Black	Created	
22/05/2025	1	Rachel Black		"Identity Disclosure Authority" to "Privacy Guardians”
27/05/2025	1.01	Rachel Black	Final review	Alignment with Operational guide.