

Glossary

A reference for all the words address – An address is an identifier to which asset records can be transferred

address book - The CAPE address book maps user addresses to encryption public keys. Users publish their encryption public keys in the address book. This is done by submitting users' UserPubKey bundle (which includes both address and encryption public key) and signing the request using the user private key associated with the address.

asset code – A unique identifier generated during asset creation designating an asset type

asset creation – The act of defining a new asset type in CAPE. Creation of a domestic CAPE asset includes minting the asset's initial supply, whereas defining a sponsored asset links the asset type to the specified ERC-20 token

asset creator – A user that defines and creates a new asset type on CAPE. Asset creators select the privacy features associated with an asset type and are responsible for the corresponding viewing keys and freezing keys, if any

asset policy – The privacy options associated with an asset definition

asset record – In CAPE, the transferable units of value are called asset records. Asset records contain the following information

- amount
- asset code
- owner address
-

asset type – An asset created on CAPE along with its defined policies. The asset type is discernible by its unique asset code which is generated during creation. This can be either a CAPE domestic asset or an ERC-20 based asset.

burn – Tokens are burned by sending the token to a public address from which those particular tokens can never be spent. CAPE tokens are burned to maintain the consistency of the system when Ethereum tokens are unwrapped

Configurable Asset Privacy (CAP) – A protocol developed by Espresso Systems that enables creation of digital assets with configurable privacy properties

Configurable Asset Privacy for Ethereum (CAPE) – Implementation of the CAP scheme where transactions are validated and settled within an Ethereum smart contract

domestic CAPE asset – An asset that has been created directly on CAPE.

ERC-20 based asset – An asset on CAPE linked to an ERC-20 token type. Users can wrap their ERC-20 tokens from Ethereum to CAPE to add privacy to their ERC-20 transactions.

freezing key – A user with access to a viewing key and freezing key for a specific asset type can freeze individual asset records of that asset. A freezing key can only be generated prior to asset issuance, and cannot be retroactively attached. Users can see whether an asset type has a freezing key attached before they decide whether to use a specific asset type.

freezing policy – The freezing policy set during the asset issuance stage determines whether a freezing key for an asset type is created

keystore – A keystore file (sometimes called a UTC file) in CAPE is an encrypted version of a user's private key.

merkle tree frontier - Membership proof of the latest added record commitments.

minting - Bringing tokens of a new domestic CAPE asset type into circulation on CAPE

relayer – A relayer processes and protects the privacy of withdrawals of ERC-20 based tokens from CAPE to Ethereum. This obviates the need to link a user's Ethereum address to a CAPE withdrawal by paying fees with the Ethereum address, thereby retaining privacy throughout all types of CAPE transactions.

sponsor – A user who creates a sponsored asset on CAPE

sponsored asset – A method for user to describe an ERC-20 based asset on CAPE. Example: a sponsor creates a sponsored asset for the DAI ERC-20 token called CAPE-DAI. Users can then wrap their ERC-20 DAI tokens on Ethereum and receive CAPE-DAI tokens on CAPE.

transaction – An atomic update to the state of the CAPE smart contract on Ethereum

unwrapping – Burning some amount of tokens from a sponsored asset type on CAPE and receiving an equivalent amount of

some corresponding ERC-20 token on Ethereum.

viewing key – Part of the asset policy for a CAPE asset. A user with access to a viewing key for a specific asset can view the content of viewing memos attached to transactions involving that specific asset. Depending on the parameters of the viewing key the can see some or all of the following: sender, receiver, amount, asset type, credentials. Users can see which part of their transaction may be viewable through the viewing key before they decide whether to use a specific asset type.

viewing memo – An encrypted note that contains information about the sending and receiving party in a transaction, as well as the asset type and amount being transferred, and credential information.

viewing policy – The viewing policy determines which part of a transaction becomes viewable through a viewing key

wrapping – Depositing an ERC-20 token into CAPE and receiving an equivalent amount of tokens from some corresponding sponsored asset chosen by the user.

[Previous Components Interactions](#) [Next FAQ](#) Last updated 2 years ago On this page