certME

Mobile eID

powered by blockchain

Current Release

Authors (alphabetical order)	Augustin Jianu
Owner	certME
Version Number	1.0
Document Release Date	January 2021
Classification	Public

Document History

Version	Author	Date	Description
1.0	*Product Owner*	*2021-03-01*	*First publication*

Abstract

The digital age has enabled new types of collaborative business models – commonly referred to as "the sharing economy". These business models create added value by providing organizations and individuals with the technological means to pool resources and processes while maintaining security of operations, transparency of processes and privacy of data. Collaborative business models allow companies to deduplicate efforts and lower overhead, consequently stimulating an increase in competition through quality of products and services.

certME provides a technological and organizational framework, made possible by the use of DLT (decentralized ledger technology), that allows companies to share KYC (know your customer) processes by using mutually recognized electronic identification means.

By using DLT and advanced cryptography, certME enables partner organizations to request issuance of electronic identification means and use them without storing or disclosing person identification data of the user, making the certME electronic identification scheme self-sovereign and GDPR compliant by design.

Company

About

certME is an electronic identification service provided by certSIGN, a well-established Romanian company with vast experience in IT security.

CertSIGN delivers the certME electronic identity as a service by operating an electronic identification scheme that leverages mobile and blockchain technology. This service is built on top of a sharing economy business model that allows organizations to eliminate redundancies, streamline processes and lower overhead.

certSIGN is a qualified trust services provider, a software house developing information security applications and a physical and electronic archiving provider. Over time certSIGN has developed its own solution portfolio and has provided specialized services in the IT Security field. certSAFE, shellSAFE, trust4Mobile are just a few of the products developed by certSIGN's research and development team, that initially were prototypes and now are used by their users at a large scale.

Mission

Our mission is to deliver an electronic identification service tailored to the needs of the global digital society.

Vision

We believe that electronic identity is the centerpiece of the global digital society and that people should have complete control of their person identification data.

Purpose and Scope

Purpose

This white paper aims to inform readers regarding the overall concept of digital identity and regarding the certME eID service – its underlying principles and technology – within the existing regulatory context at EU level.

Scope

This white paper is a high-level presentation comprising existing eID approaches and details of the certME eID service provided by the certSIGN company, covering principles, policies, workflows, business model and technologies in a way that is accessible and easy to understand by the general public.

Approaches to eID

Context

Using electronic identity to provide online services helps companies increase their market share, tap new markets and deliver better services at lower costs. Local and central governments also benefit from the use of electronic identity by providing citizens with 24/7 e-government services.

To deliver services online, some organizations such as government bodies or financial institutions are required by either regulation or risk mitigating policies to perform costly identity proofing procedures (sometimes referred to as KYC – Know Your Customer) before digital onboarding of users.

Current commercial approach

Financial institutions are currently running digital onboarding processes that require a face-to-face verification of identity and multiple documents. This is costly for both the organization and the users. Organizations need to ensure enough staffing of offices. Conversely, users need to repeat these processes for each service provider that they engage with.

The commercial approach to electronic identification typically entails issuing some type identification means, based on one or two factors of authentication (such as username-password and OTP token/SMS OTP), which can only be used between the issuer and its customers.

One problem faced by this approach is that digital onboarding processes are lengthy and resource intensive for both the service providers and their customers. When changes occur in the identification data of a customer, identity proofing processes need to be repeated either partially or in some cases completely. This is even more arduous for customers that need to undergo these processes for all their service providers.

Because this approach requires all service providers to store the identification data of their customers in relation to the electronic identification means issued, organizations face further costs with data protection and cybersecurity, which are usually proportional to the number of customers. From the user's perspective, the privacy risk to their personal data grows proportionally to the number of service providers of which they are customers. Furthermore, customers have no effective control over who has access to their data. In addition, security and compliance auditors face numerous challenges when assessing such electronic identification schemes, as logs and audit trails can be lost, damaged or doctored.

Centralized national eID

National eID cards or passports and other national electronic identification schemes can successfully be used for identification and authentication of users, but have serious drawbacks that require costly workarounds.

One such drawback is the limited storage capacity of the eID card chip. eID cards can only be used to store basic identity or health information, which makes them useful for identification, but incapable of more complex functionality. To circumvent this problem, service providers which use eID cards to authenticate their customers are forced to store more complex personal data on their servers. This gives rise to privacy and security risks and limits the control that people have over their data. In order to manage their data and the access to it, users need to interact with multiple dashboards – one for each of service provider that stores their data. In addition, users can almost never transfer or copy their personal data between repositories of two different organizations. Even if it were possible to seamlessly transfer the personal data, the level of assurance of said data would not be transferred from one organization to another.

Because eID cards offer very low granularity of access to personal data stored therein, privacy risks are high when using an eID card in relation to service providers that are not fully trusted. For example, when a service provider’s authentication mechanism only requires a verified birthdate for age confirmation, users are forced to also reveal all other personal identification attributes, including name, address of residency etc.

Self-sovereign ID

In a self-sovereign electronic identification scheme data is stored, owned and controlled by the user.

A self-sovereign electronic identification scheme provides high granularity of access to person identification data. The proposal of self-sovereign identity schemes is that a simple request needs to receive a simple confirmation without having to reveal more information than is required. Users can choose to disclose only the specific attributes required for a specific service. For instance, a self-sovereign ID allows users to only share their name when attending an event that is invitation based, without sharing their home address.

The consequences of using self-sovereign identity schemes are far reaching as they can provide a basis for further economic and digital innovation.

Current EU directives and regulations such as PSD2, GDPR, eIDAS and MiFID2 support self-sovereign ID, confirming a positive outlook for self-sovereign ID schemes.

Service

Description

certME is an on-demand digital service delivered by the certSIGN company to its customers via an information technology system comprising hardware, software, users and usage procedures. The software component of the certME system comprises a mobile app (available on Android), several web apps, micro-services and APIs that interact with one another via smart-contracts on the Ethereum public blockchain. The certME mobile app allows users to register and authenticate to online service providers which are integrated with certME through the use of APIs.

certME electronic identification means can be issued at a substantial level of assurance following an in-person face-to-face verification of the subject or just a couple of clicks if the subject is already enrolled by a trusted partner organization (i.e., a certME validator).

Because all authentications of user data are handled by the smart-contracts, blockchain transactions create irrevocable audit trails that ensure transparency of the digital ecosystem to all parties involved.

Electronic identification means can be used to generate qualified digital signatures if they are issued based on national eIDs or in person identity proofing and verification. Because certME is blockchain based and allows crypto-wallet features, having qualified signatures associated with crypto assets (e.g., real-estate tokens) can give the token holders legal ownership or usage rights of the asset represented by the token.

Partner network

For in person verification, the certME service relies on a network of partner organizations – called validators – which provide identity proofing and verification as a service to certSIGN. The partnership relies on bilateral contractual agreements between certME and each validator. Contractual agreements abide by the same principles, model and structure, and include unalterable mandatory clauses that are common to all agreements.

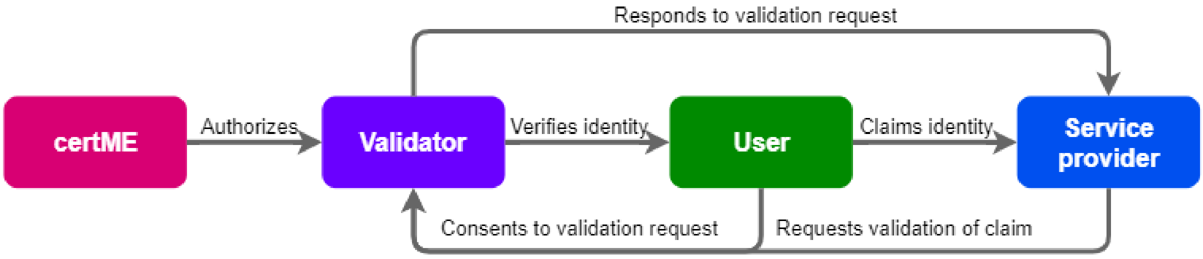
After performing identity proofing and verification of a user, validators request the issuance of electronic identity means which is automatically handled by the certME smart-contracts. The role of validators also includes responding to credential validation requests made by service providers via the smart-contracts when certME eID holders first authenticate or registers to their service. Subsequent authentications don't require confirmation from validators.

Operational model

Within the certME ecosystem actors can have the following non-exclusive user roles:

- ***Scheme manager*** – As legal representative of the eID scheme, the certSIGN company holds the *scheme manager* role. By granting or revoking specific permissions on the certME smart-contracts, the *scheme manager* authorizes/deauthorizes *validators* to request issuance of electronic identification means and authorizes/deauthorizes *service providers* to issue *user* credential validity checks. The *scheme manager* can also suspend, revoke, or unsuspend any identification means in case of lost or compromised mobile devices. The scheme manager is also responsible for operating the authentication mechanism.
- ***Validator*** – A certME *partner organization* authorized to (i) perform identity proofing, (ii) verify users' person identification data, (iii) request issuance, suspension, revocation and unsuspension of electronic identification means and (iv) confirm credential validity checks registered by *service providers* on the smart-contracts. A *validator* can only respond to credential validity checks that are authorized by *users* and that concern users verified by said validator.
- ***Service provider*** – Is a certME client organization authorized to issue authentication requests and credential validity checks on behalf of *users*. A *validator* can also act as a *service provider* and interact with *users* enrolled by other *validators*.

- ***User*** – Is a natural person that has undergone an identity proofing and verification process performed by a *validator* and has been issued a certME electronic identification means that can be used to register/authenticate to a *service provider*. Every authentication request issued by a *service provider* on behalf of a *user*, must be authorized by the *user*.


Responds to validation request
certME
Authorizes
Validator
Verifies identity
User
Claims identity
Service provider
Consents to validation request
Requests validation of claim

Validators

Current certME partner validators are:

- CERTSIGN S.A.

Data policy

certME does not store person identification data of certME eID users in order to deliver the service. Only non-personal data, such as encrypted verification proofs, is stored by certME in order to enable users to register to service providers. Personal data, that the service providers may require to perform or deliver services, can only be sent by the users from their mobile devices following their approval and consent, which is expressed as a digital signature accompanying the data.

certME stores data access logs for compliance and billing purposes. Such data is limited to: timestamp, status, provided service (register/login), scope and unique token of the transaction.

Person identification data is collected by authorized personnel of validators during the identity proofing and verification of certME users, in accordance with the contractual agreement signed with certME and applicable regulation – eIDAS, GDPR and national legislation. The data collected is used to generate proofs of verification, after which it is sent via a secure channel to the certME app of the user and is released from memory without being stored. This ensures that the data is known and controlled only by the person whom it identifies. The proofs of verification are encrypted and stored on the blockchain for security and transparency purposes.

During the identity proofing and verification of certME users, for eIDAS compliance purposes, the authorized personnel of validators generate printed verification reports which are physically signed by users and are subsequently archived. Verification reports are completely analog (i.e., printed paper) and contain all the personal information verified, collected and transferred to the user's mobile device, as well as information regarding the operator and validator that performed the verification, timestamp etc.

Termination policy

In case of service termination, certSIGN will give certME eID users at least 6 months' notice via mobile app notifications and messages. We plan on ensuring continuity of service in accordance with Regulation 910/2014 through our Termination Plan.

Technology

Electronic identification means

The electronic identification means issued to a person under the certME service consist of:

1) The **certME mobile app and private key** – The app is installed and operated by the persons being issued the identification means on a mobile device under their control. The usage of the certME mobile app is protected by using strong encryption keys generated as non-exportable in the device's secure element or secure enclave and accessible exclusively through strong biometric authentication (such as fingerprint or facial recognition with depth perception). An elliptic curve public-private key pair is generated by the person using the certME mobile app, in accordance with the Ethereum blockchain specifications. The public key is hashed to obtain an address which identifies the user on the blockchain. The private key is used to sign transactions which represent the user's consent and authorization of validation requests added by service providers or other types of interactions.
2) A **transaction on the Ethereum blockchain** – Upon completing an identity proofing and verification process, a certME validator signs and issued a transaction to the Ethereum blockchain, containing the user's blockchain address and a list of encrypted proofs of identity verification. This transaction, together with the private key found in the mobile app, constitute the electronic means of identification.

Mobile app

The certME mobile app is a software application available on theAndroid operating systems. The app is available for download on both Google Play and Apple Appstore and can only be downloaded and ran on smartphones and tablets which support secure element or secure enclave and strong biometric authentication interfaces, such as fingerprint or facial recognition with depth perception. The certME mobile app does not run on jailbroken or rooted devices nor on devices which are not secured with screen lock. The certME mobile app can only be run and accessed with biometric authentication and the private key stored in the secure element/enclave is inextricably tied to the biometrics which were used to create it. If users disable the screen lock or the biometric authentication, or root their device, the private key found in the secure element, together with the entire mobile application local database are permanently deleted to protect the user's personal information.

Electronic ID

The certME mobile app allows the user to create an electronic identifier in the form of a secp256k1 elliptic curve public-private key pair (based on the Ethereum blockchain specifications). The private key is generated by the user on their device and is always under their exclusive control. The public blockchain address is obtained by applying the Keccak-256 hash function on the public key. The app allows the user to store up to 253 static attributes. All attributes are encrypted within the mobile app's local database. The secure element or secure enclave is used to create and store two non-exportable keys - inextricably linked to the user's biometrics - with which the Ethereum private key and the local app database are encrypted. The mobile app doesn't run on devices that don't support secure element or secure enclave. Whenever a blockchain transaction needs to be signed by the user, a biometric authentication is required which allows the key stored in the secure element/enclave to decrypt the Ethereum private key. In other words, the Ethereum private is decrypted on-demand following a biometric authentication of the user, and is zeroed out of memory after the transaction is signed.

eID issuance

The certME eID issuance is performed by a smart-contract following an in person face-to-face verification of the user by an authorized Validator. The user's certME mobile app uses a QR-code based system to securely authenticate and exchange data with the certME validator app. The process is further detailed below in the Identity verification section of the Validator app chapter.

Registration

The user can register a new account with a service provider by typing their alias in a textbox provided by the service provider's web or mobile app interface. After entering the alias, the user receives a notification on their mobile device to approve or reject the registration request, including the attributes required. Approving the registration request triggers the mobile app to automatically sends the user's attributes to the service provider via a secure channel created using ECDH over TLS. The user's approval is also registered on the blockchain, signaling to the validator service that the user consents to having their attributes validated by the validator in relation to the specific request issued by the service provider. The service provider uses the data received from the user to generate a validation check and registers it on the smart-contract. The registration is complete when the smart-contract contains a proof from the validator that confirms the authenticity and level of assurance of data provided by the user.

Authentication

The user can authenticate to a service provider - with which they have previously registered - using their certME mobile app by scanning a QR code shown by the service provider on a web interface or by tapping a button shown by the service provider in a mobile app. The user's action triggers a secure transmission of a signed challenge code via REST API over TLS.

User consent and GDPR compliance

All transactions whereby the user's data is sent and received, can only be done by the user using the data stored on their certME mobile app. Blockchain transactions, including those used for authentication/authorization or user consent, are not accepted by the smart contract if they are not signed by the user with their private-key. Any validation of the level of assurance of user data requested by a service provider to the smart-contract must be consented to and signed by the user with their private-key via the certME mobile app. The smart-contract that brokers the credential check between users, service providers and validators does not allow validators to submit proofs of data authenticity and level of assurance, if the user signature and consent are missing.

Suspension

Users that have access to their mobile devices and want to suspend their certME eID can do this by tapping a button and authenticating, which automatically generates a blockchain transaction that is accepted by the smart contract to suspend the eID who's address corresponds with the transaction signatory.

Validator app

certME partners use a software application henceforth called the certME validator app comprising a web application compatible with all major browsers and micro services (accessible via REST API) that facilitate interaction with the Ethereum blockchain and the user's mobile app.

Identity verification

To ensure a substantial level of assurance for electronic means of identification issued under certME, issuance is performed following a face-to-face in person verification. Consequently, the validator app is designed to enforce face-to-face verification of users. This is done by a two-way handshake using QR codes. First, the user scans a QR code (with their certME mobile app) generated by the certME validator app. This scan allows the user to securely receive on their mobile device the attributes collected and verified by the validator's operator. Second, the certME validator app scans a QR code generated by the user's certME mobile app in response to the initial QR. This allows the validator app to securely receive the user's blockchain address and mobile device id, which is necessary to send push notifications to the mobile app (such as validation requests by service providers).

Processing user data

The validator app includes a web form which is used by authorized personnel of the validator to collect the user's person identification data during the identity proofing and verification process. The validator app does not store data attributes provided by users. Instead, the validator app creates proofs for each individual data attribute and encrypts them before passing them to the micro-service to be stored on the Ethereum blockchain. The proofs cannot be used to reverse engineer, infer or otherwise determine the person identification data, and encryption is only necessary for the business model of the certME service. A user is considered enrolled when a specific transaction including the user's blockchain address can be independently confirmed to exist on the Ethereum blockchain and has been accepted by the certME smart-contracts.

Responding to validation checks

A certME validator app micro service constantly monitors the Ethereum blockchain for new validation checks submitted by service providers. If a validation check is related to a user enrolled by the micro-service owner (validator), the micro-service automatically responds to the validation check by submitting to the Ethereum blockchain the necessary proof which the service provider can use to determine the authenticity and level of assurance of data received from a certME mobile app user.

Suspension

The certME validator app includes a web form which is used by authorized personnel of the validator to search for a user's blockchain address based on the user's first name, last name, birth date and unique identifier (as per the eIDAS MDS requirements). This is made possible by storing on the blockchain a proof of the MDS attributes in relation with the user's blockchain address. The MDS proof cannot be used to reverse engineer, infer or otherwise determine the MDS attributes which were used to create it.

The certME validator app also includes a web form which is used by authorized personnel of the validator to suspend a certME eID based on the user's blockchain address. Users can request the suspension of their eID in-person to either certSIGN or their initial validator. Suspension is oerformed following an identity verification with the same level of assurance which was used to issue the eID.

Revocation

The certME validator app includes a web form which is used by authorized personnel of the validator to revoke a suspended certME eID based on the user's blockchain address following an identity proofing and verification process.

Reactivation

The certME validator app includes a web form which is used by authorized personnel of the validator to reactivate a suspended certME eID based on the user's blockchain address following an identity proofing and verification process.

Authenticator service

Service providers using the certME electronic identity scheme need to run a certME micro service (henceforth called the certME authenticator app) in order to register and authenticate certME users to their systems.

User interaction

To receive any data attributes (i.e., credentials) related to a certME eID from users, the certME authenticator app is accessible to the certME mobile app users via REST API. To register (i.e., initial authentication) to the service provider, users send their credentials to the certME authenticator REST API using their mobile app. Communications are protected by two layers of authentication and encryption (ECDH over TLS). Subsequent authentications only require sending a signed challenge by the user via TLS.

Blockchain interaction

The certME authenticator app facilitates communications with the Ethereum blockchain for the service provider. The certME authenticator app is integrated with the service provider’s software infrastructure via a REST API. Upon receiving data from a certME mobile app, the microservice generates a request for authentication (i.e. credential validation check) and submits it to the smart-contract on the Ethereum blockchain. The certME authenticator app constantly monitors the smart-contract for completed validation checks. Validation proofs are extracted from the smart-contract and used to determine the authenticity and level of assurance of the identity data received from certME mobile app.

Although not enabled by default, the certME authenticator app can support automatic payments for authentication to validators via the native crypto-currency of the Ethereum blockchain.

Smart-contracts

System security is assured by a smart-contracts on the Ethereum blockchain, which is secured by Proof-of-Work. The smart contracts manage authorization/deauthorization of validators, service providers and users. User authentication is also managed by a smart contract that brokers interaction between validators, service providers and users. The smart-contracts ensure that only authorized parties can interact and that the users consent to every transaction concerning their data.

Conclusions

By using DLT and advanced cryptography certME enables organizations to share the results of their KYC processes without storing or disclosing person identification data of the user within a self-sovereign eID scheme which is GDPR compliant by design.

This enables a new type of collaborative business model in which added value is created by enabling companies to pool resources and processes while maintaining security of operations, traceability of processes and privacy of data.

Abbreviations

Term	**Definition**
API	Application Programming Interface
DLT	Decentralized Ledger Technology
ECDH	Elliptic-Curve Diffie–Hellman
eID	Electronic Identity
eIDAS	electronic IDentification, Authentication and trust Services
EU	European Union
GDPR	General Data Protection Regulation
ID	Identity
IT	Information Technology
KYC	Know Your Customer
MDS	Minimum Data Set
OTP	One Time Password
PSD2	Payment Services Directive 2
QR code	Quick Response code
REST	Representational state transfer
SMS	Short Message Service
TLS	Transport Layer Security

Glossary

Term	Definition
Blockchain	Blockchain is a shared, immutable ledger that facilitates the process of recording transactions.
Jailbreak	Jailbreaking refers to privilege escalation on an Apple device to remove software restrictions imposed by Apple.
Keccak-256	Hash function used by Ethereum.
MiFID	II is a legislative framework instituted by the European Union (EU) to regulate financial markets in the bloc and improve protections for investors.
Root / rooting	Rooting is the process of allowing users of smartphones, tablets and other devices running the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems.
secp256k1	secp256k1 refers to the parameters of the elliptic curve used in Ethereum public-key cryptography
Self-soverign ID	Self-sovereign identity (SSI) is a term used to describe the digital movement that recognizes an individual should own and control their identity without the intervening administrative authorities.
Smart contract	A smart contract is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.