WallID

YOUR ID IN YOUR ETHEREUM WALLET

White Paper

Your ID in your Ethereum Wallet

Table of

Contents

1
Introduction

Businesses and organizations have been trying to tackle the most prominent issues regarding identity management and systems for the last couple of years.

Whereas physical assets have a value which is dependent mainly on their owner's (first-party) skills to use it, digital assets (such as a stored value or any piece of information) depend not only on its owner (proprietorship, first-party) but also on its counterparty (second-party) recognition of the same value. However, unlike the above described, identity assets also require the existence of a third-party, one that issues and certifies a certain identity on one hand, and is trusted to do so by the second element of the transaction on the other hand.

Due to this complexity, there are very few identity standards globally accepted and used, and they are often issued by public or state institutions that define identity certification standards and protocols and issue or validate identity attributes for citizens.

These identity certificates are usually verifiable by the presence of an ID document like the citizenship card and its validation often requires the physical presence of both the citizen and the card.

During the last decade, most industries shifted to online platforms and businesses became more global than ever. Even when all archaic procedures were being adapted to this new reality, identity validation processes, known as "Know Your Customer" (KYC) stayed almost unaltered:

+ Customers are required to submit all requested attributes everytime they go through a KYC process.

+ A copy of the physical citizenship card is sent through unsafe and easy to corrupt channels.

+ A human eye verification is required from KYC services in order to check if sent attributes match the citizenship card attributes, and belong to the person applying to it.

+ Process completion takes up to several days in cases where demand is high.

+ Customer identity data is all distributed and stored on centralized servers.

1
Introduction

There have been some new projects surging in the blockchain space in order to address some of the problems stated above, such as Civic, Uport, Persona, SelfKey, TRC and many more. All of them solve some serious issues, like identity protection, identity sovereignty and identity data immutability.

However, a new issue was brought to light by these solutions - the need to build from the ground all the trust networks that verify that the data uploaded to the blockchain is in fact from the citizen who uploaded it. In other words, the challenge is to find a way to bring the already existing chain of trust produced by offline identity documents and standards.

Some projects tackle that problem by bringing validators trusted by their community into the protocols, or by relying in a centralized but public network of validators.

WalliD is a new Ethereum-based protocol that allows citizens to encrypt and store their certified identity documents and attributes from the real world on the blockchain, access and instantly exchange them with KYC services they trust.

The main innovation in this protocol is the ability to verify if the uploaded attributes are under a globally trusted digital certificates such as the x.509 [1], making sure that every identity uploaded and verified by the system is a valid European identity and certified by its Certifying Authority (CA).

Image 1 WalliD protocol storing ID documents in the Blockchain and Exchanging with KYC service.

2

Market context

Identity issues in the online world

Identity trust is a well solved problem in the physical world. Every jurisdiction has its own Identity Issuer organization who's responsible for certifying every citizen's identity attributes and issuing a respective proof-of-identity. Usually it is represented by physical objects like citizenship cards and passports and everybody, from citizens within those jurisdictions to organizations recognize these certificates as valid.

These issuing organizations are responsible for the creation or adoption of identity certificates like x.509 and for the application of its rules in order to generate specific codes to link its owner to his ID certificate.

Some jurisdictions are moving forward to come together and create common certificates. European Union Countries are some of the first unifying their identity certificates under the x.509 standard. It makes it possible for various countries to recognize other nationality identity attributes.

In the digital world, however, identity trust is far from being a solved problem. User IDs do not necessarily need to match real identities from the physical world. While authentication solutions are well developed, through mobile apps from Google and Facebook like the 2 Factor Authenticator, procedures that require the confirmation that a user is indeed a citizen with a specific set of attributes, still require highly inefficient, costly and insecure human dependent KYC processes for their compliance practices.

Compliance requirements are a growing trend and a mandatory practice for more and more businesses and industries. Due to that, expenses with KYC and due diligence processes have been rising.

On average, financial institutions with an average annual return of 10 Billion USD, has an annual cost of 150M USD with KYC processes and the average annual cost for the same practices on other financial firms is around 60 million USD [2].

Regulation differences within jurisdictions affect KYC processes since the required information is often variable. The same on-boarding process inside an organization must be customized depending on the location where the operation is taking place.

Currently, on-boarding costs for businesses with KYC Processes range from 15$ to 20$ and demand a renovation of due diligence validations periodically. On top of that, in some cases, already on-boarded customers are required to go through the same or similar KYC processes in order to have access to different services or products.

This required customization results in the fact that compliance tasks are still undertaken by man power with individual processing of information, long checks and balances and carry high risks.

For customers this inefficiency represents a long waiting for identity verification in every financial, state, insurance and notary service, amongst many others. It also represents a high exposure to identity theft and fraud risk due to the abundance of transactions and centralized server storage.

At the present day KYC and due diligence practices involve the validation of identity physical objects such as citizenship cards or encrypted identity codes from trusted Public Key Infrastructures (PKI) [3] in order to verify its provenance.

This practices rely on the validation of widely accepted certificate standards, such as national identity certificates issued by governmental Certifying Authorities and

ID issuers. This ensures the data collected authenticity was previously validated by a globally trusted third party and is compliant with eventual local or global regulations and that little to no customers on those jurisdictions are excluded from potential applications.

x.509 certificates and PKI are trusted and used within the European Union Jurisdiction as the strongest proof-of-identity standard and it is used by various governmental CA and KYC services.

Despite these advancements, there are still no solutions that do not require the physical presence of the citizen and his or her ID document through potentially targetable and hackable channels.

During the last three years, dozens of blockchain projects emerged in an attempt to solve most of the issues regarding identity management. Their main focus has been to use the blockchain as a tool to let users keep control of their identities and their transactions. Namely, the CIVIC project [4] whose intention is similar to WalliD. The main difference is that CIVIC builds a web of trust for validators within their own protocol while WalliD only stores already validated identities, from globally trusted PKI and CA in its smart contract, cutting the problem of identity trust to 0%. CIVC's approach is dependent on the community growth and how trustworthy their internal validators are perceived by the other members. On the other hand, the uPort project [5] also deals with the decentralization of identity management, but their approach is to create a separate, independent identity system with their own security and not bound to real documents. Again, the main problem is about the trust and actual effectiveness of having an identity system that is dependent from new traction and trust. The Persona project [6] is a solution for identity management which is also aligned with the latest data protection regulations. Its scope is to empower the individual and grant them the control over their personal data as well as the means to secure access to their private details. The idea again is to allow users to insert identification attributes in the blockchain environment, and then to validate them by the user itself, so once again it is the users who are in charge of inserting the data that will state their identity and they will themselves validate if that data is correct. However, this will not prevent a user from faking stating to be another person and that is one major drawback of these systems. Other similar projects do the same such as SelfKey [7], heKey [8], REMME [9] which implements authentication systems based on blockchain-based data existing electronic ID systems like Eestki, [10] Guardtime [11] and Bitnation [12]. from Estonia which are becoming leading environments for building European enterprise security solutions,.

Despite all success from some of these projects, the issue of connecting the already trusted offline identities with the blockchain and ultimately with online services still remains. All of the existing blockchain protocols start at the point of identity creation or accept fragile and easy to corrupt identity validation sources such as social networks as proof of real life identities.

Furthermore, most of them require the presence of trusted validators in their network. These are organizations that must be trusted by all members of that community as liable to confirm real life identities from everybody.

This scenario generates a huge entropy, separating communities around their trusted validators and requiring these blockchain protocol promoters to spend most of their resources attracting these organizations and building communities. More recently, two new protocols have been testing and developing an approach that uses Digital Certificates in a blockchain context:

EthEstonia [13] is an Ethereum wallet contract that is controlled by the Estonia issued Identity card and tied to the citizen number. EthEstonia uses reverse engineering on the Estonian e-identity under the x.509 as a signature mechanism to trigger the users' wallet transaction.

Eddits [14] is also a pilot Ethereum protocol based in Luxembourg and developed by the tech house In

Tech [15] and combines the Ethereum ID standards ERC-725 [16] and ERC-735 [17] with the X509 certificate used in Luxembourgish ID. The protocol aims to provide a globally trusted and governmental issued asset into authentication and signature Online procedures, by linking a trustlessdigital certificate validator with that ID owner's wallet address.

WalliD's vision is that digital certificates must be brought to the Blockchain as its proof-ofidentity (POI) in order to allow online services to match a users' identity with his or her real life identity when necessary and agreed by both parts. In that sense, WalliD developed an open protocol for all digitally certified identities and an ecosystem for more than authentication and signature operations – It allows users to store multiple IDs in their wallets, and exchange them with different KYC services with different requirements.

While WalliD's smart contract stores encrypted certified attributes, importing apps, read and extract those attributes from ID documents like the citizen card and Customizable KYC services can be built on top of the protocol to request and allow users to exchange their data accordingly to their business partners needs.

WalliD's protocol is currently available for the Portuguese Citizen Card ID and is backed and supported by the Portuguese National Mint House – the Citizen Card Issuer. The protocol is currently being expanded in order to accept other Identity types and jurisdictions and other official identity issuers are joining the protocol.

The team's and investors vision is that WalliD will become the global standard platform for all digitally certified identities to be safely associated with their users' digital wallets and the decentralized
and safe channel for that data to be shared with online KYC services.

3

WalliD's Proof-of-Identity (POI)

The Digital Certificates

In the context of the WalliD protocol a verifiable identity must be provided by a cryptographically strong connection to a real world identity.

In cryptography, a public key certificate, also known as a digital certificate is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can establish a trust relationship with him/her.

The real world usage of digital certificates in particular those of the X.509 variety is widespread namely in Identity Documents or National eID cards issued by several member states of the European Union: Germany, Austria, Belgium, Spain, Portugal, Estonia, Sweden, Finland, Lithuania and Czech Republic. Those eID cards are usually the official citizenship document in the context of people's real world interactions with their country's State but also as eID mechanism to conduct secure online authentication and document signing through the use of the certificates and private keys present in those smart cards.

The legal basis and security requirements of those credentials are regulated in Europe by the standards specified in the eIDAS regulation established by the European Union on 23 July 2014.

WalliD protocol specifies that a secure proof-of-Identity (POI) should be based on a digital signature that can be verified by a global certificate issued by a credible entity such as the X.509 certificate. It doesn't restrict in any way which should be the accepted identity (certificate) issuers for the users of WallID based KYC services.
At the moment of the ICO WalliD's team has developed a prototype implementation of a KYC service that will only accept WalliD identities associated with a Portuguese Citizen Card. The team's vision is that there will be other trustworthy public or private-sector entities that issue X.509 certificates (or other digital certificates) accepted as additional ID types in the WallID ecosystem.

Developers and other members from the blockchain community are also invited to expand the number and types of IDs by creating and implementing their own compatible apps as Certificate Providers for attribute extracted.

4

Blockchain potential for ID management

Blockchain technology and protocols have established themselves as sustainable solutions for providing privacy and security through encryption of information and immutability, transparency and irreversibility through public ledger storage.

The first blockchain protocol (Bitcoin) was created in order to provide a secure and transparent way to exchange a value represented by a token between two accessible but pseudonomily stored wallets.
Blockchains are distributed ledgers that contain and connect blocks of information of a predefined size, and register transactions that respect a predefined set of rules, or protocol.

The Bitcoin protocol defines rules for the amount of tokens in circulation, and how to award recently created (mined) tokens to the right miner. It's blockchain consists of a library of all transactions between wallets with those tokens.

Privacy is achieved by having no connection between a wallet owner identity attributes and its wallet identification (address). Security, immutability and irreversibility is granted by the encryption of data and by the the distributed shape of a blockchain - by having every block connected to another by an hash, it makes it impossible to change or delete any piece of information without the blockchain knowing of it. Transparency is achieved by the fact that all transactions are registered and easily accessible by anyone.

Self-sovereignty is, in itself, the final frontier and the biggest paradigm shift made available by the blockchain technology. By using asymmetric encryption protocols where public keys dependent actions are only triggered by their unique private key match, it requires full responsibility from users to protect and manage their keys but provides total control over their data since no one has access to the combination code within the user's private key.

When it comes to ID management, blockchain provides the potential infrastructural answer to existing problems in the today's online world. The current need to send copies of ID documents through centralized and insecure channels makes anybody's data an easy target to tamper or to corrupt. Thefact that every service has its own KYC process requires users to send multiple times the same documentation, not only increasing the risk stated above but also increasing the user's risk of not being able to keep track and control his or her own identity attributes.

WalliD's core value proposition is to solve this problem. Currently, there is no way to connect real life identity certificates such as Citizen Cards to any blockchain wallet. WalliD protocol and compatible apps provide the tools for any person or organization to extract his or her ID certified attributes from these documents and store them in their wallets. By doing this, the users' private keys encrypt their own data while they keep full control over it and are the only ones with access to their raw and real data. At the same time, it makes their life easier when it comes to share this data with KYC processes or other Identity requesting organizations. By sharing their ID public address, stored on the blockchain, all insecure and centralized channels are avoided and users can track their transaction history recorded in the blockchain.

And the fact that all data is encrypted and decrypted only with their private keys means users maintain total sovereignty over tit since there is no app or service in the WalliD protocol that accesses or retains their real information. All the encryption and storage is made from hashes, and the power to decide whether to decrypt and share real ID attributes with centralized service providers is left to their owner.

5

WalliD Step-by-Step

5.1
Extracting data

WalliD's protocol was designed for two different but related user needs:

1 Having a certified ID stored in his or her Ethereum Wallet;

2 Being able to instantly share this ID with any trusted online service.

At the centre of the protocol and ensuring all surrounding components work in order to keep both value propositions entangled is WalliD's smart contract and the webapp myetherid.io [18]. that accesses it. This website provides the links to all the protocol compatible apps with the features to validate and extract the ID attributes from a certified ID document. It is also the link between the user, his or her Ethereum wallet and WalliD's smart contract, through Metamask [19] plug-in that ensures safety for private keys handling and ID storage.

Around MyEtheriD are the extracting apps like ImportiD reading and validating POI from certified documents and generating a text block (ID data) with the user's attributes and readable by MyEtheriD in order to store them on WalliD's smart contract. Also around MyEtheriD are the POI providers like StoreiD, receiving the POI (digital certificate) alongside the user's Wallet address upon request from the Extracting app and authorization from MyEtheriD. This protocol design ensures the ID attributes are stored in a public smart contract even though they are encrypted and accessed only by their owner private keys.

ID certificates are stored in a different ledger (POI provider) and can only be accessed by KYC services requesting proof-of-identities upon its owner authorization. The following picture describes the three WalliD components in their context and relation illustrating the protocol design in order to provide both main value propositions. Chapter 5.1 and 5.2 describe the technology and flows behind the process of extracting ID attributes from an ID document and storing in its user Ethereum Wallet while chapter 5.3 explores the technology and flows responsible for the transactions between KYC services, users and POI providers:

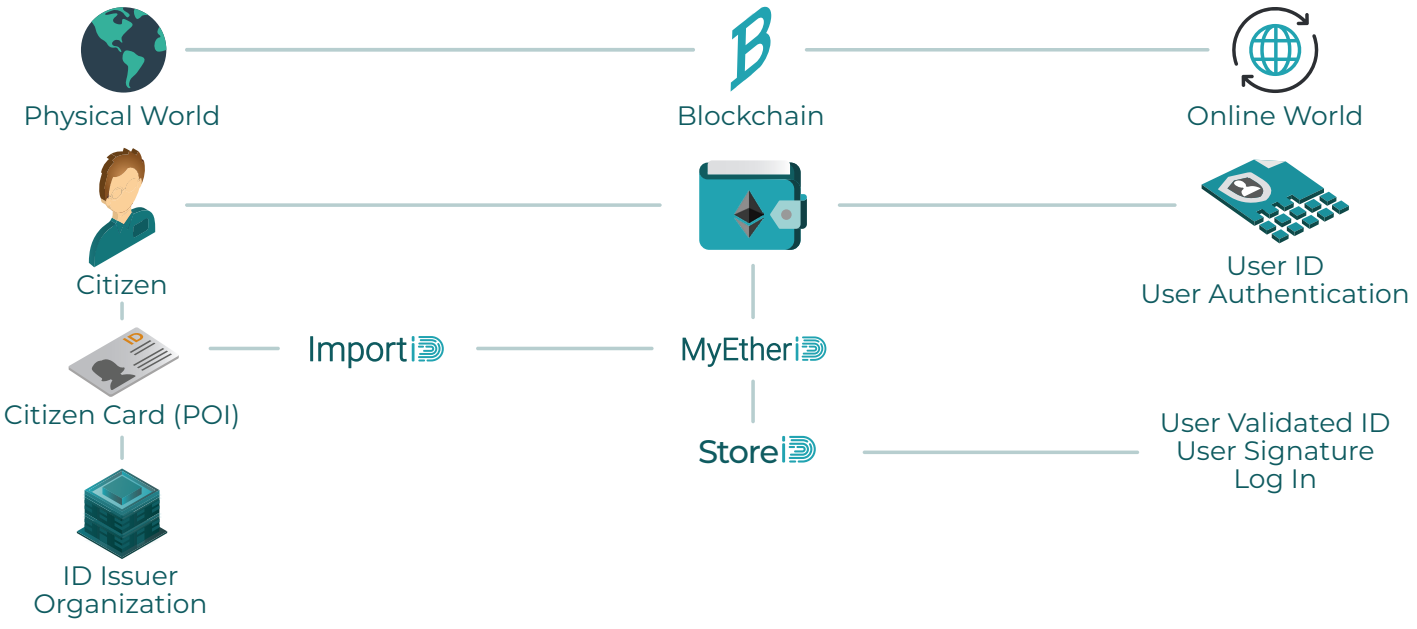

Image 1 WalliD's apps in the context of the protocol.

5.2
Storing identities in the Ethereum wallet

After creating the JSON ID data file the ID attributes must be encrypted and stored in WalliD's smart contract and the digital certificate sent and stored in the POI provider determined in the previous step . All this is done inside MyetheriD.io

MyEtheriD.io is a free, client-side browser app designed to read and write in the Ethereum blockchain. MyEtheriD.io is a Javascript app with no backend associated and able to track or save any users' interaction with the web page. It is connected to Metamask, letting users encrypt and decrypt their data with their own Ethereum private keys operating within the web3 plug in. This means that once again, no server or service associated to MyEtheriD, WalliD or any other person without the users' private keys will have access to their raw data and no way to decrypt the data stored in their ID smart contract.

Using the storing features of MyEtheriD.io to encrypt the ID data the user will generate his or her ID inside WalliD's smart contract and store it in his or her Ethereum Wallet with the following encrypted data in it:

1 Citizen Card EF.SOD file as specified by the ICAO standard for Machine Readable Travel Documents 9303 - Part 10. This file is technically a PKCS#7 digital signature issued by the Portuguese State over a group of data hashes, namely citizen ID Data and citizen address data.

2 Wallet signature - confirmation of the association between user's wallet and ID.

3 ID attributes - user's identity data imported from the Citizen Card,

4 ID document expiration date - turning the smart contract invalid at that moment.

Once this data is generated and stored inside WalliD's smart contract it can be accessed anytime by anyone with the user's wallet address but can only be decrypted with its user private keys.

All transactions inside WalliD's smart contract can be checked at any time by anyone with the smart contract address and Myetherid.io provides the features for users to simply check which identities they have stored in their wallets and what transactions they have performed with them.

At the same time this process occurs, MyEtheriD also separates the Certificate information from the ID data and verifies if the POI provider that shall store it is registered in WalliD's protocol, before sending it there alongside the users' Wallet address.

The certificate does not contain any information that, when accessed separately can identify its owner and it's only valuable when matched with its owner ID attributes, becoming able to assess their validity. They are the most important piece of information for KYC services in order be sure of their customers' identity.

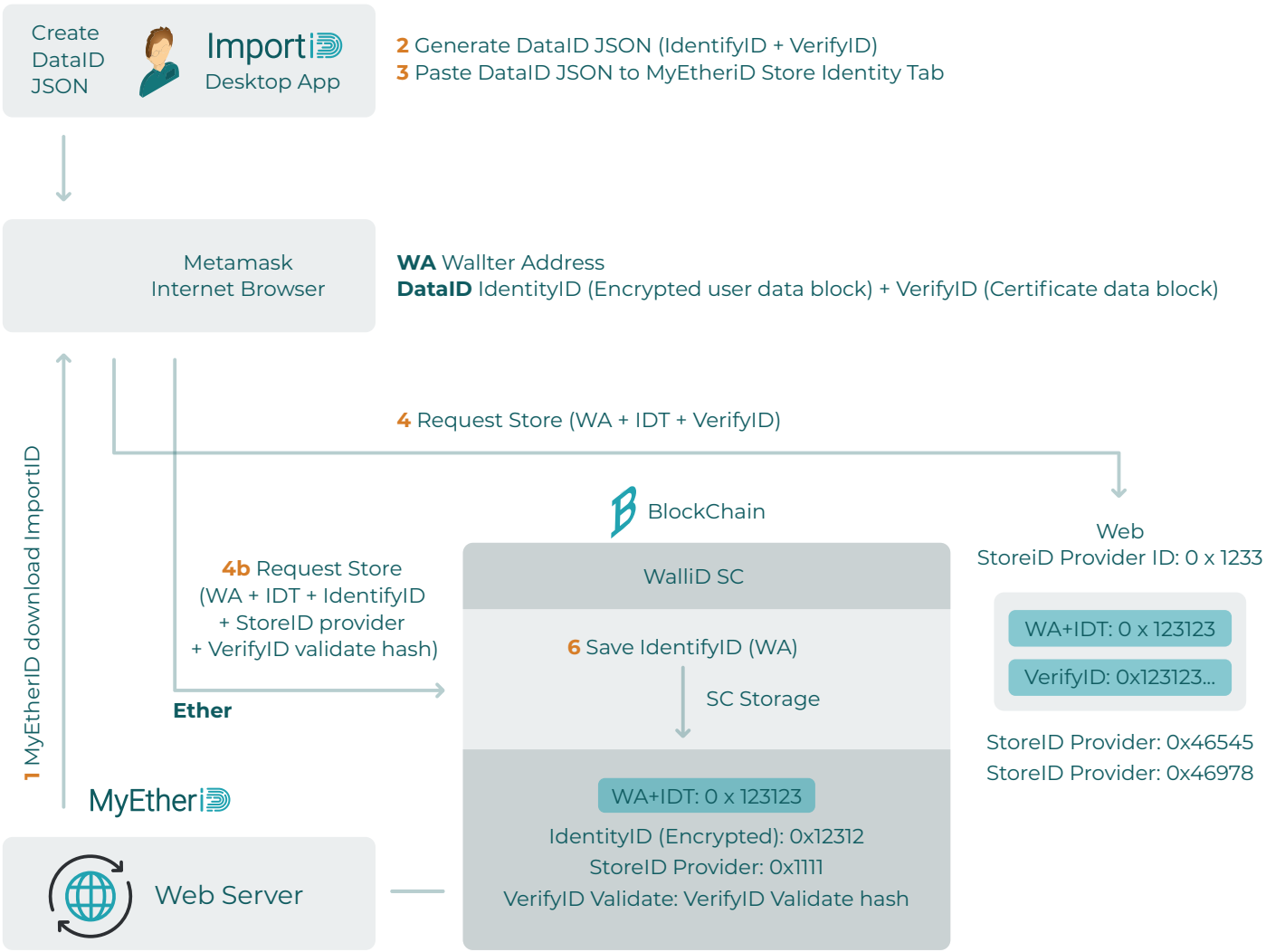

Image 3 Extracting and storing ID attributes and POI on WalliD's protocol

1 User opens Web Browser and navigates to MyEtheriD.io or a POI Provider web site to download an importing application like ImportiD and installs it.

2 User opens ImportID application and follow the instructions to generate and copy DataID data. The application has a tutorial and a how to use guide.

3 User goes back to his or her browser, accesses MyEtherID.io and pastes the DataID data into "Store Identity" tab.

4 User presses "Connect with Metamask" to store DataID. This should open Metamask popup. If the user doesn't have MetaMask plug in installed, instructions will be presented to install and create one account. Confirm the operation details with Metamask and wait while it saves the IdentifyID data in the WalliD Smart Contract and the VerifyID data in the StoreiD Provider. After the operation is finished at the tab "View Identities" the user can see his or her Identity data already saved in the blockchain at the "View Identities" tab.

5.3
Proving identity instantly on a KYC service

Being able to instantly share this ID with any trusted online service is the main value proposition for common citizens using WalliD.

The whole protocol is designed to allow everyone with a certified identity to immediately and safely share their ID attributes alongside a proof of those attributes validity - the digital certificate. The presence of both these blocks of information is indispensable to verify a certain Identity since the attributes alone do not guarantee the origin and validity of the information in them. Only the digital certificate alongside them can ensure that validity.

This way, KYC services compatible with WalliD request their customers' Ethereum wallet address and locally provide the same Metamask connecting features of MyEtheriD.io, allowing users to locally decrypt their attributes from WalliD's smart contract directly on their trusted KYC services.

At this stage the KYC service will need to access that user digital certificate that is stored on the POI provider he or she chose. The service will then send a request to the provider, containing the user's wallet address and the amount of WAL tokens determined by the POI provider for every transaction. All this steps happen simultaneously and after they come to a conclusion, the KYC service will have all the information it needs about the user in order to verify his or her real life identity.

At the present date, WalliD's team has developed a pilot KYC service compatible with WalliD's protocol. This service flows are described in the next image and are ready to be integrated with online services requiring the Portuguese ID attributes contained in the Portuguese Digital Card. The pilot has been successfully tested and integrated with all the other components around the protocol and will soon be integrated in real online KYC services:

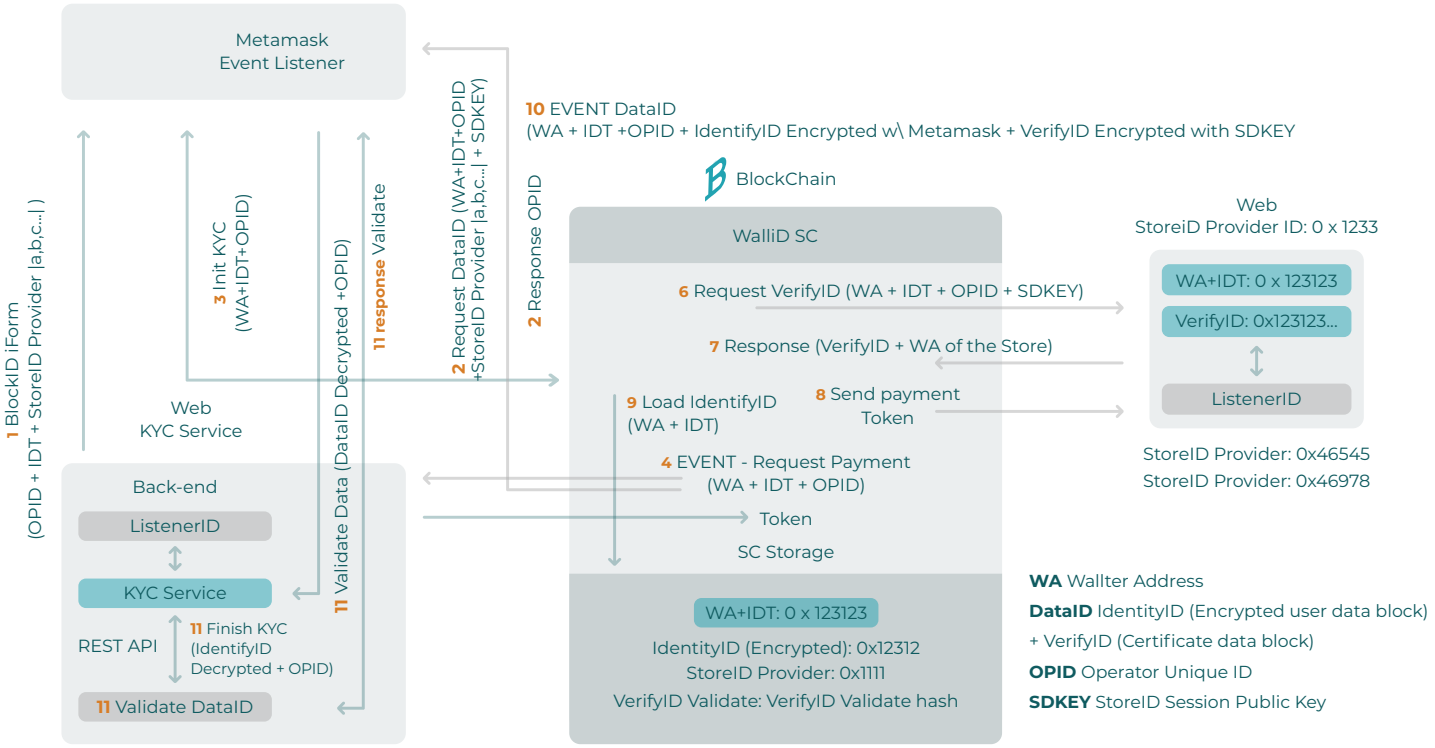

Image 4 Being able to instantly share this ID with any trusted online service

1 User opens Web Browser and logs in Metamask. He or she then navigates to the service provider web page. Each Identify operation (KYC) has a unique ID for every operation ID (OPID) generated by the service provider backend. In the service provider web page, the user is asked to load his or her identity from WalliD. At this moment, the user can select one from the list of the supported “POI Provider’s” (StoreiD providers) and one from the list of the supported “Identity type’s”. He or she then “Connects with Metamask”. If the user had imported his identity to one StoreiD Provider or one identity not accepted by this service provider, the user has to store his identity again in another StoreiD Provider.

2 The Metamask popup open to the user validate the operation. If user accept the request with Metamask, the Metamask request DataID data from WalliD Smart Contract and call the service provider backend to initiate his KYC process.

3 The service provider backend initiates the KYC process.

4 WalliD Smart Contract emits the event - Request Payment about this identify operation.

5 The service provider backend receives the event - Request Payment and verifies with OPID if the identify operation was created by it to process the payment for WalliD Smart Contract.

6 WalliD Smart Contract receives the payment and requests the VerifyID data to the specific StoreiD provider.

7 StoreId Provider responds with VerifyID data to WalliD’s Smart Contract.

8 WalliD Smart Contract pays the StoreiD Provider.

9 WalliD Smart Contract loads IdentifyID data from storage.

10 WalliD Smart Contract emits the event - DataID data with both encrypted IdentifyID data and VerifyID data.

11 The service provider web page receives the event and asks user to decrypt data using Metamask. After data decryption, the service provider web page sends the data to KYC process at the service provider backend to validate the IdentifyID data with VerifyID data. KYC process is finished.

6

Protocol Technical overview

WalliD is an Ethereum protocol and operates under a smart contract (SC) logic. Ethereum was the first blockchain infrastructure to come up with the concept and the possibility to add smart contracts on top of a public ledger. It kept the same basic functions and features as the Bitcoin protocol but added a most significate breakthrough - the possibility to define specific set of rules that, when complied with, would trigger a predefined and precoded set of events, affecting all the intervenients related to it. These automatic sets of rules are called Smart Contracts and can be integrated in the Ethereum Blockchain in order to store and record the transactions happening inside that specific environment.

This technological breakthrough made Blockchains dynamic and opened the possibility for developers to increase the number of features and services a Blockchain could provide, while keeping the privacy, immutability, transparency and decentralization promoted by it.

WalliD protocol provides the possibility for ID services and developers to integrate their customized solutions to import and extract ID attributes for certified documents, encrypt and store those documents in the blockchain and keep the digital ID certificates stored in another ledger. The WallID smart contract is executed in the Ethereum blockchain and developed in Solidity language. The source code is publically available at WalliD's githUb project page [21].

In this section the two main workflows supported by the smart contract (SC) are described:

1 StoreID flow - Responsible for the encryption and storage of the ID attributes on the SC and the Certificates on the POI Provider ledger

2 Verification/KYC flow - Responsible for managing the requests from KYC services to the SC and POI Provider ledger in order to access users' certificate data and ID attributes.

6.1.
StoreID in the WallID Smart Contract

This first flow is supported by a single function storeID that receives as input:

1 Encrypted IdentityID data block with the user's personal information

2 ID Type (the ID type of the original document backing this identity)

3 Name, URL and Wallet Address of the storeID provider which will be used to verify the corresponding identity.

StoreID will store those three elements associated with the calling user's Wallet Address.
This transaction will be performed by the end user's web3-enabled browser, preferably using Metamask extension in order to ensure safe handling of private keys.

6.2.
Identity verification/KYC in the WalliD Smart Contract

The Identity verification process starts when a Service Provider supporting WalliD generates a request in the user browser for the requestDataID function which receives as input:

1 Supported ID Type(s)

2 Accepted StoreID providers

3 Operation ID (randomly generated by the Service Provider)

4 StoreID Session Key: Public key generated by the user browser which will be used by a StoreID Provider to encrypt the VerifyID data block.

The requestDataID will emit an event of type requestPayment if it exists a StoreID entry with at least one of the accepted StoreID providers.

The Service Provider is listening to requestPayment events and generates a request to the function sendPayment with parameters: User Wallet Address, ID Type and Operation ID.

Associated with this request there should be a ERC-20 [22] transfer call to the Wall ID token contract (WAL token) so that Wall ID can perform the escrow function in the Service Provider / StoreID Provider transaction.

The StoreID Provider which holds the VerifyID block for the user must then reply to the requestVerify event using function sendVerifyID(OpID, WA, Encrypted VerifyID).

The SC will then verify if the origin of the sendVerifyID is a valid one for the user WA and then return the data to the user browser through responseWallID event with the Encrypted IdentityID and Encrypted VerifyID data blocks.

If no valid StoreID provider replies in a period of 30 seconds no information will be returned to the user and Service Provider can request the refund of the token held in escrow.

6.3.
KYC Service - identity verification

In this section, the technical process of identity validation that a Service Provider must implement is described. This process is needed to ensure that a given IdentityID data block is consistent within itself and was issued by a trusted entity. Specific validations that should be performed if the ID Type is a Portuguese Citizen Card (CC) will also be described.

Wallet Address Signature

StoreID provider will supply a signature that was computed over the Ethereum Wallet Address of the user in 20-byte binary format. This signature is performed using the RSA-SHA256 algorithm using PKCS#1.5 padding.

In the future evolutions of the protocol there will be a way to specify different signature algorithms for different ID and Certificate Types.

The public key to verify the signature is supplied in the X.509 certificate also supplied by the StoreID provider.

The Service Provider should verify that this signature is correct using the mentioned certificate public key.

X.509 certificate validation: X509 certificate ensures that a minimum set of identification attributes are correct and belong to a person validated by the trusted issuing entity.

For instance, in the case of CC the certificate contains the Full Name, Civil ID Number and Date of Birth of the person.

By performing a certificate path validation using the Citizen Card PKI certificates publicly available [23]the Service Provider will have cryptographic proof that the wallet address signature was produced by a Portuguese Citizen with a given Full Name, Civil ID Number and Date of Birth.

SOD File validation

For the full set of IdentityID attributes of the Portuguese Citizen Card the StoreID provider will also store an additional cryptographic proof which is the SOD file (Document Security Object). This Data structure is specified in the ICAO Machine Readable Travel Document Specification (ICAO Document 9303 Part 10).

It is specified as a PKCS#7 signature generated by a Certificate Authority included in the Citizen Card PKI.

It is computed over 2 blocks of identity data: Identity Attributes and Current Address attributes.

SOD File validation can be split into 2 steps:

1 Validation of the PKCS#7 signature and the respective certificate using Citizen Card PKI certificates

2 If step 1 succeeds compare the 2 Data Group hashes contained in SOD file against the computed SHA-256 hashes of the Identity Attributes and Current Address Attributes.

If the SOD signature verification is successful, the Service Provider should also make sure that the 3 Attributes present in the X.509 Certificate match those present in the IdentityID data block. If this is true we can be sure that the IdentityID data match the identity of the person that performed the Wallet Address signature mentioned previously.

7

References

1 https://www.sslauthority.com/x509-what-you-should-know/

2 http://www.businesstimes.com.sg/banking-finance/know-your-customer-compliance-costs-continue-togrow-at-financial-firms-surveys.

3 https://www.comodo.com/resources/small-business/pki.php?af=7639

4 https://www.civic.com/

5 https://www.uport.me/#about

6 https://persona.im/

7 https://selfkey.org/

8 https://www.thekey.vip/#/homePage

9 https://remme.io/

10 https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

11 https://guardtime.com/

12 https://tse.bitnation.co/

13 https://github.com/LogvinovLeon/estid-sig

14 https://eddits.io/wp-content/uploads/2018/03/EDDITS-Whitepaper.pdf

15 http://www.intech.lu/en

16 https://github.com/ethereum/EIPs/issues/725

17 https://github.com/ethereum/EIPs/issues/735

18 https://myetherid.io/index.html#/

19 https://metamask.io/

20 https://wallid.io/

21 https://github.com/walliDprotocol

22 https://github.com/ethereum/eips/issues/20

23 https:// pki.cartaodecidadao.pt/