**ISO #####-#:####(X)**

ISO TC 307/WG 2

Secretariat: XXXX

**Title** (Blockchain and distributed ledger technologies — Overview of Identity)

WD stage

**Warning for WDs and CDs**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

*To help you, this guide on writing standards was produced by the ISO/TMB and is available at* [*https://www.iso.org/iso/how-to-write-standards.pdf*](https://www.iso.org/iso/how-to-write-standards.pdf)

*A model manuscript of a draft International Standard (known as “The Rice Model”) is available at* [*https://www.iso.org/iso/model\_document-rice\_model.pdf*](https://www.iso.org/iso/model_document-rice_model.pdf)

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO’s member body in the country of the requester.

ISO copyright office

Ch. de Blandonnet 8 • CP 401

CH-1214 Vernier, Geneva, Switzerland

Tel.  + 41 22 749 01 11

Fax  + 41 22 749 09 47

copyright@iso.org

www.iso.org

Contents

*This template allows you to work with default MS Word functions and styles. You can use these if you want to maintain the Table of Contents automatically and apply auto-numbering.*

*To update the Table of Contents please select it and press "F9".*

[Foreword v](#_Toc508979152)

[Introduction vi](#_Toc508979153)

[1 Scope 1](#_Toc508979154)

[2 Normative references 1](#_Toc508979155)

[3 Terms and definitions 1](#_Toc508979156)

[4 Overview of Identity 1](#_Toc508979157)

[4.1 What is Identity? 2](#_Toc508979158)

[4.2 Who do we want to identify? 2](#_Toc508979159)

[4.3 Who wants to identify? 3](#_Toc508979160)

[4.4 Why digital identity? 3](#_Toc508979161)

[4.5 Why DLT? 4](#_Toc508979162)

[4.6 Starting point 4](#_Toc508979163)

[4.7 DLT Identity requirements 4](#_Toc508979164)

[5 Chain verification 5](#_Toc508979165)

[5.1 ID Licenses 6](#_Toc508979166)

[5.2 Self-Sovereign ID Database 6](#_Toc508979167)

[5.3 The role of SSID 6](#_Toc508979168)

[5.4 Smart Contract Framework 6](#_Toc508979169)

[6 Interfaces 7](#_Toc508979170)

[6.1 Accreditation Authority 7](#_Toc508979171)

[6.1.1 Data hash and comparison 7](#_Toc508979172)

[6.1.2 Attestations 7](#_Toc508979173)

[6.1.3 ID redaction 8](#_Toc508979174)

[6.2 Service Provider 9](#_Toc508979175)

[6.2.1 Claims interface 9](#_Toc508979176)

[6.2.2 Blockchain interface 9](#_Toc508979177)

[7 Non-standard ID 10](#_Toc508979178)

[7.1 Legal entity identifiers 10](#_Toc508979179)

[7.2 Objects 10](#_Toc508979180)

[7.3 Processes 10](#_Toc508979181)

[8 Security 10](#_Toc508979182)

[8.1 Storage 10](#_Toc508979183)

[8.2 Distributed database 11](#_Toc508979184)

[8.3 Data transfer 11](#_Toc508979185)

[8.3.1 Zero-knowledge proofs 12](#_Toc508979186)

[8.3.2 Cryptographic hashes 12](#_Toc508979187)

[9 Privacy 12](#_Toc508979188)

[9.1 Data access conditions 12](#_Toc508979189)

[10 Outlook 13](#_Toc508979190)

[11 Interface for Verification of Digital Identity Documents 13](#_Toc508979191)

[11.1 Overview 13](#_Toc508979192)

[11.2 Workflows 13](#_Toc508979193)

[11.2.1 Verification 14](#_Toc508979194)

[11.2.2 Revocation 14](#_Toc508979195)

[11.2.3 Confirmation of Certificate 15](#_Toc508979196)

[11.2.4 SSID Node 15](#_Toc508979197)

[11.2.5 Communications 15](#_Toc508979198)

[11.2.6 Message Polling 16](#_Toc508979199)

[11.2.7 Data Formats 16](#_Toc508979200)

[11.3 Sample Code 17](#_Toc508979201)

[11.3.1 Request Next Pending Transaction from SSID Node 17](#_Toc508979202)

[11.3.2 Document Verification 17](#_Toc508979203)

[11.3.3 Document Revocation 17](#_Toc508979204)

[11.3.4 Certificate Confirmation 17](#_Toc508979205)

[Bibliography 19](#_Toc508979206)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](https://www.iso.org/directives-and-policies.html)).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see [www.iso.org/patents](https://www.iso.org/patents)).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: [www.iso.org/iso/foreword.html](https://www.iso.org/iso/foreword.html).

This document was prepared by Technical Committee *[or Project Committee]* ISO/TC *[or ISO/PC]* ###, *[name of committee]*, Subcommittee SC ##, *[name of subcommittee]*.

This second/third/… edition cancels and replaces the first/second/… edition (ISO #####:####), which has been technically revised.

The main changes compared to the previous edition are as follows:

— xxx xxxxxxx xxx xxxx

A list of all parts in the ISO ##### series can be found on the ISO website

Introduction

Identity management today is fractured and disparate – no one method has been realised with many vested interests slowing evolution towards a unified global system. Digitisation has affected every market and will continue to penetrate down into more sensitive services such as personal finance, credit scoring as well as managing health care records. Current provisioning of these services is held back by the lack of unified digital identity.

There exists a plethora of applications to address related issues – however most still rely on an incorporation of physical documents, and the sending & storage of personal data within company databases [1] and so at their core are still proprietary analogue based systems. A unified digital identity system could act as a catalyst for streamline services and achieve higher assurance delivery and correspondingly a more seamless user experience.

Distributed Ledger Technologies underpin nascent digital ID applications – DLT’s decentralised key management allows true ownership of ID data & provides mathematically assured provenance. These capabilities facilitate audit/compliance by design, providing a more efficient option for many regulated sectors including identity management for the most sensitive use cases of personal data.

Standardisation of DLT for identity management will guide selfish agents towards unified, modular & interoperable global identity system. The benefits of this being apparent, the need for standardisation of DLT is outlined by the portfolio of diverse, separate identity systems and their vastly different architectures.

Blockchain and distributed ledger technologies — Overview of Identity

# Scope

This document provides an overview of identity management as it relates to blockchain and distributed ledger technology (DLT) systems.

# Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 27001, *Information security management standard*

# Terms and definitions

For the purposes of this document, the following terms and definitions apply.

BC – Blockchain

DB – Database

HMPO – Her Majesties Passport Office

LoA – Level of Assurance

PII – Personally Identifiable Information

SP – Service Provider

SSID – Self-Sovereign Identity

ZNP – Zero Knowledge Proofs

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at <http://www.electropedia.org/>

— ISO Online browsing platform: available at <https://www.iso.org/obp>

# Overview of Identity

Currently, in most countries the framework for validation of identity data usually consists of an amalgamation of incumbents and government bodies, providing a network of personal claims and validations – for entities to authenticate themselves to access trusted services.

Identity is foundational to many services today – any transaction with accompanying requirements on either side requires a framework in place to allow each person, process, legal entity or artefact to determine information about the other and thereby create a degree of trust.

Today’s standard analogue identity systems are documents based, siloed & inflexible which creates many limitations. Physical comparison of individuals to documents is time consuming and may not require demonstration of a link between the entity and document, resulting in insufficient degrees of authentication. Identity information is stored in discrete places that are not integrated and reduce data aggregation, which is desirable for businesses to enable cost reduction and simplify the user experience through analytics.

## What is Identity?

The Identity frameworks of today combine data from many different sources with a network of validators – used by companies to ascertain identities of those parties they are interacting with and so better analyse related risks. The current approach, often based around outdated legacy processes, is conducted in the dark – as companies cannot assess the accuracy of validations or trace the process. Overall, their exists a lack of transparency and so a leap of faith is often required.

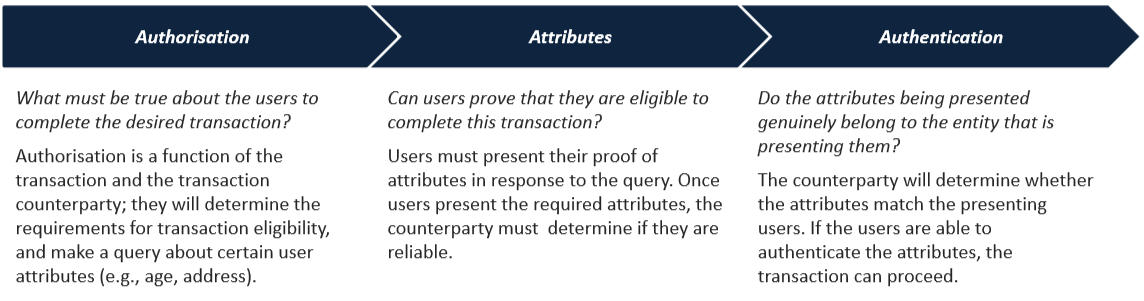
Currently identity validation process depends on the provision and authentication of physical documents and in many cases, this does not require demonstration of strong confirmation of the link between the individual and the document, beyond basic and easily circumventable measures such as assessing a photo or signature likeness. Information is scattered around in discrete places prevent easy aggregation – what is lacking is a standardised set of information about an entity that can be easily adapted to bespoke transaction requirements. Furthermore, siloed approach to data handling presents security risks and compliance difficulties for companies – and often leaves individuals uninformed about how their data is used or profited from.

## Who do we want to identify?

In a broader sense an identity system must accommodate individuals, legal individuals, ‘things’ and processes; so, the framework conceptualises an entity to be an individual, legal entity, a thing or a process. Identity defines the whole set of attributes that describe an entity and determines the types of transactions in which it can participate in. The total set of attributes for these groups are endless but they can be abstracted into three groups: inherent, inherited & assigned.

Inherent attributes are ones that are intrinsic to that entity, such as a person’s eye colour, or the logical structure of a process request. Inherited attributes are ones that an entity will acquire during its lifetime of operation, such as a person’s citizenship or a company’s legal acquisition of another. Assigned attributes are ones attached to an entity, but that are not intrinsic, such as a person’s phone number or a company’s legal jurisdiction.

## Who wants to identify?

An entities attributes allow it to access specific services by proving to the counterparty they have the required characteristics to transact. Regarding individual’s identity related transactions, there’s 3 main aspects to satisfy from a service providers point of view:

World Economic Forum "A blueprint for Digital Identity" [1]

This process can be conducted to different degrees of sophistication regarding the risk/value of each transaction – each service provider will consider the acceptable Level of Assurance (LoA) for individuals and resources being accessed. A high LoA may not always be desirable for each transaction, as the current processes require intensive onboarding and strong authentication – which is cumbersome for the user.

The purpose of a formal identity system is to allow counterparties with no previous relationship to establish trust through a transaction. Within these individual’s attributes are attested to by a trusted third party, who issue credentials that tie their attestation to the specific attributes, with some method of authenticating for the entity who is presenting it. Users use their ‘wallet’ of credentials to transact with new counterparties whom they have no previous relationship with. This can be further translated down to legal individuals, things & processes – who’s owners will traditionally transact on their behalf.

## Why digital identity?

A digital identity system offers many benefits when compared to traditional, physical based systems. These have begun to emerge as a direct response to the developing technical landscape and the high automation, instant access, real time reporting and other general transaction requirements of today’s services.

A digitized identity system has the same basic structure as a physical identity system, however the attribute storage and exchange are entirely digital, removing the dependence on physical documents and processes – greatly increasing efficiency and providing channels for leveraging automation and analytics.

By design, a digital identity offering allows interoperability between separate entities due to the data being standardised & in a digital format. This approach offers greater flexibility, allowing systems to adapt to the nature of the transaction – continuously reviewing requirements and integrating additional information around the process to create a richer view of the user.

Today’s approaches do not accommodate the identification of assets or processes efficiently or transparently. Many sectors have inherent friction around critical processes due to the lack of efficient ID. This may lead to further inaccuracies and fractured systems lacking inter-connectivity often increasing opportunities for human error. However, an effective digital identity framework that can track IoT ‘things’ and the processes they create/interact with will have huge economic and social impact – paving the way for automation to be truly realised in many sectors.

No country or organisation can act as an island of automation in todays digitised wold. One example is, Estonia who are looking beyond their own borders in designing and implementing their state issued ID and government systems – offering bureaucracy-as-a-service to residents of other sovereign states [2].

For ID systems to be relevant and useful now and many years into the future they must be implemented in an internationally minded way whilst retaining the ability for sovereign states to adapt to individual conditions.

## Why DLT?

Current trust frameworks are built around centralised proprietary databases of personal information – through which individuals must authenticate themselves to access systems. These systems require service providers to store and manage PII, leaving them liable for its handling – trust here is placed with the service provider.

Advancements in Distributed Ledger Technology have provided, for the first time, a system by which trust can be moved down to the cryptographic protocol underneath – removing the need for intermediary’s and so providing truly decentralised key management & trust.

Consensus protocols combined with the cryptographic assurance for data provenance means DLT systems produce easily auditable ledgers that can provide regulatory compliance by design – an attractive option for many regulated sectors.

## Starting point

Effective Identity management and ultimately trust in authentication and validation approaches stems from the network effect created by interoperable entities all communicating easily with one another. For an ID system to be relevant today and in future, implementation needs to look beyond physical boarders to accommodate the globalised digital transition inherent in many services today.

Such a system must retain the ability for sovereign states to adapt the solution to fit personalised compliance needs, while being robust enough to communicate on a standard platform with all other solutions globally.

If the framework is to leverage existing infrastructure and communicate with existing solutions it cannot be owned by any single organisation or government body. One solution is to design as a minimal platform, to be further adapted by individual sovereign states and commercial bodies. Such a platform could thereby function to set minimum identity credentials for identity.

Standards are a useful starting point, by which a minimum set of requirements can be captured, and possible use cases published – to align the minimum set of needs common among all sovereign solutions.

## DLT Identity requirements

When considering the historic yet varied and often unsuccessful various attempts to address an identity management solution by different actors the need for standardisation becomes clear [4, 5]. An International standard for DLT identity is intrinsic in order to unite the understanding of users, governments & business and ultimately reach a common framework.

DLT should be viewed as a tool for cutting the paper process during verification of ID documents & a form of decentralised signature sharing to provide truly decentralised attestations.

In this vein, actionable requirements can be determined:

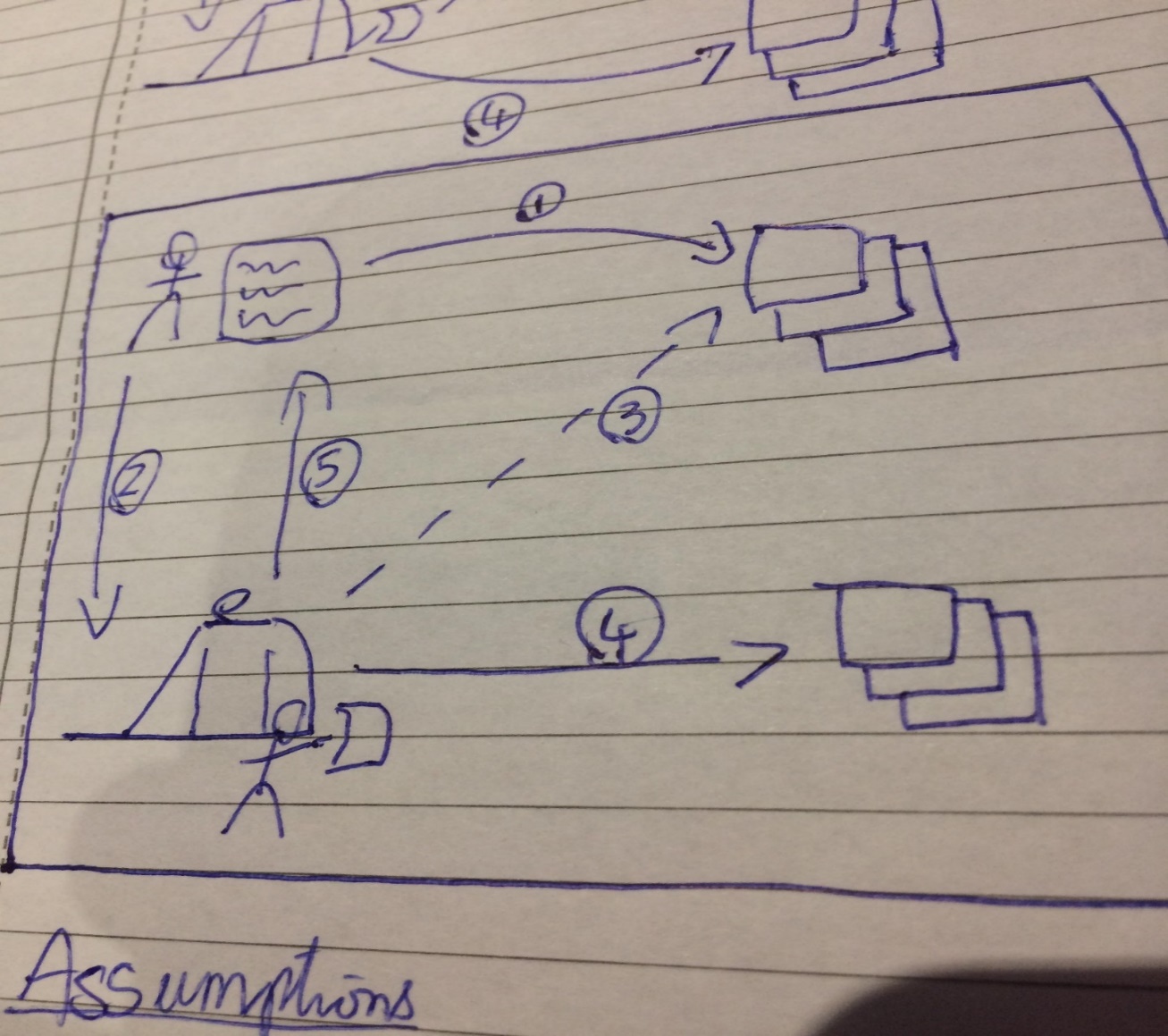
* Blockchain
  + No personal data stored on chain
  + No individual chain to become integral to framework
* Design
  + To be chain agnostic
  + To allow each regulated market to adapt for compliance
  + To work with/alongside existing infrastructure
  + To be secure by design
* Governance
  + Decentralised
  + Internationally-minded
  + Ease of Adoption

# Chain verification

Blockchain verification processes can transform the mechanism by which data is shared and authenticated for an individual. Considering a traditional credential like a passport; using any chain an individual’s PII can be hashed and its location sent to a verifier (Passport Office) – from here the verification body can hash the same PII they already hold, compare, and if the same can cryptographically sign the hash and place it in a new block. The location of this is sent back to the individual for them to use as proof during an identity transaction. This process outlines a method of digitising traditional physical credentials with the same assurance.

Leveraging a blockchain to store a ‘receipt’ of a validated transaction allows entities to have a cryptographically assured, permanent proof to authenticate their request. Blockchains permanence and related assurance of data veracity further allows entities to store associations between identifiers such as a name to a public key. Thus, decentralising previously centralised architectures to achieve common name certificates, used globally within traditional Public Key Infrastructures.

Combined with traditional communication and storage channels, blockchain’s may create a landscape where distributed ID systems can be utilized on a global scale. DLT provides immutable archiving and retrieval of data – causing the paper process of many regulated business sectors to become redundant.

The system abides by data handling regulations such as GDPR, as no PII is ever stored publicly.

## ID Licenses

A Self-Sovereign Identity (SSID) database would contain not only personal data but would also act as a repository of active licenses-for-use regarding the specific ID’s. The digital license-to-use functionality would mirror current contracts agreed into when applying for ID’s such as a new passport (expires in 10 years) or a bank card (typically 4 years).

The ability to revoke a license is required for any identity system to function correctly, and one way this can be achieved is with a smart contract framework.

For example, a passport number is owned by the respective issuer (HMPO), this type of data point is commonly held and could be enforced by the application of English Contract Law. This means that when applying for verification of ‘your own’ passport data, you would be applying for a ‘license to use’ the issuing authority’s passport number.

The constraints agreed to when asking for ID verification would also enable the ‘license-to-use’ license number to be revoked at any time by the issuer (which is generally the case in the ‘real world’).

## Self-Sovereign ID Database

An SSID is not just a repository of data, but also the repository of a list of valid licences. Through the use of smart contracts, the right to use a passport number, for example, could be revoked under a predefined set of conditions. In this example, only the owner of the licence number (i.e. the UK passport office) could revoke a UK Passport.

In summary, a SSID repository must not only include the identity but also meta data including ownership details and details of the issuing body (whether this is a bank/passport office or school, etc).

## The role of SSID

The role of the underlying SSID engine is to:

1. Remain operational within set bounds
2. Execute all contracts as agreed in a timely manner
3. Have access right to any SSID 🡪 to write results of agreed contract to record

This can be facilitated using a network of smart contracts – who’s standardisation is being addressed by TC/307 SG 5. These contracts will have admin access rights to all SSID’s to interact with these licences, agreed to on provision of the ID (much like terms and conditions when opening a bank account). This would provide a secure and transparent identity system – facilitating no backdoors to either party, allowing enhanced data integrity throughout the process.

## Smart Contract Framework

Due to the varying nature of regulation, standards & compliance for each service provider regarding their use case there is a strong case to provide adaptability in the system – so to leave them to make the decision of service provision.

Smart contracts will enable service providers to abide by regulations and will enable businesses to codify unique Terms & Conditions to be met for service. Users will agree to these on sign up. Ultimately, this approach will result in a more transparent system.

# Interfaces

To consolidate the SSID database with today’s physical trust framework, API’s for Service Providers and Accreditation Authorities must be considered and standardised.

These interfaces will provide functionality for Service Providers to better analyse risk, and Accreditors to automate the service they currently provide. It is agreed that the interface should satisfy the minimum possible functionality so to be adaptable to future implementations of identity, where extra functionality is to be developed on top of the core standard.

## Accreditation Authority

The interface for an accreditation authority must be developed in a way as to be secure by design, resistant to gaming and robust. It must satisfy three fundamental principles:

* Hash and compare personal data
* Attest to personal data
* Retract validation

### Data hash and comparison

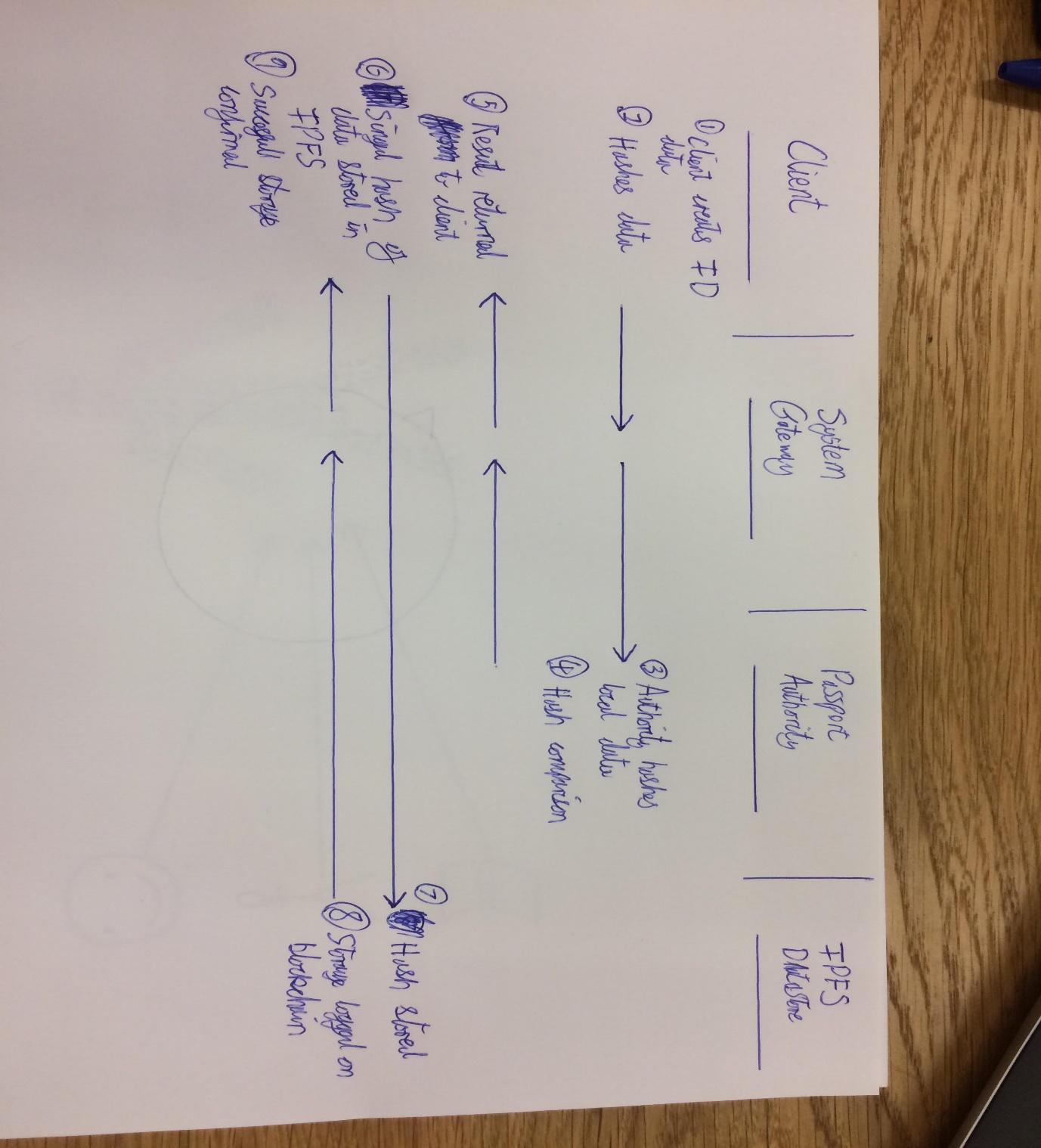
The hashing of personal data is to be achieved through the mutually agreed hash protocol and must satisfy the following:

* Validation request received
* Hash of server-side PII data created
* Comparison of result to hash received
* If successful:
  + See Attestations

Upon request; the hashing and comparison of PII will be automated, and attestation replies sent only on success – following secure by design principles throughout.

### Attestations

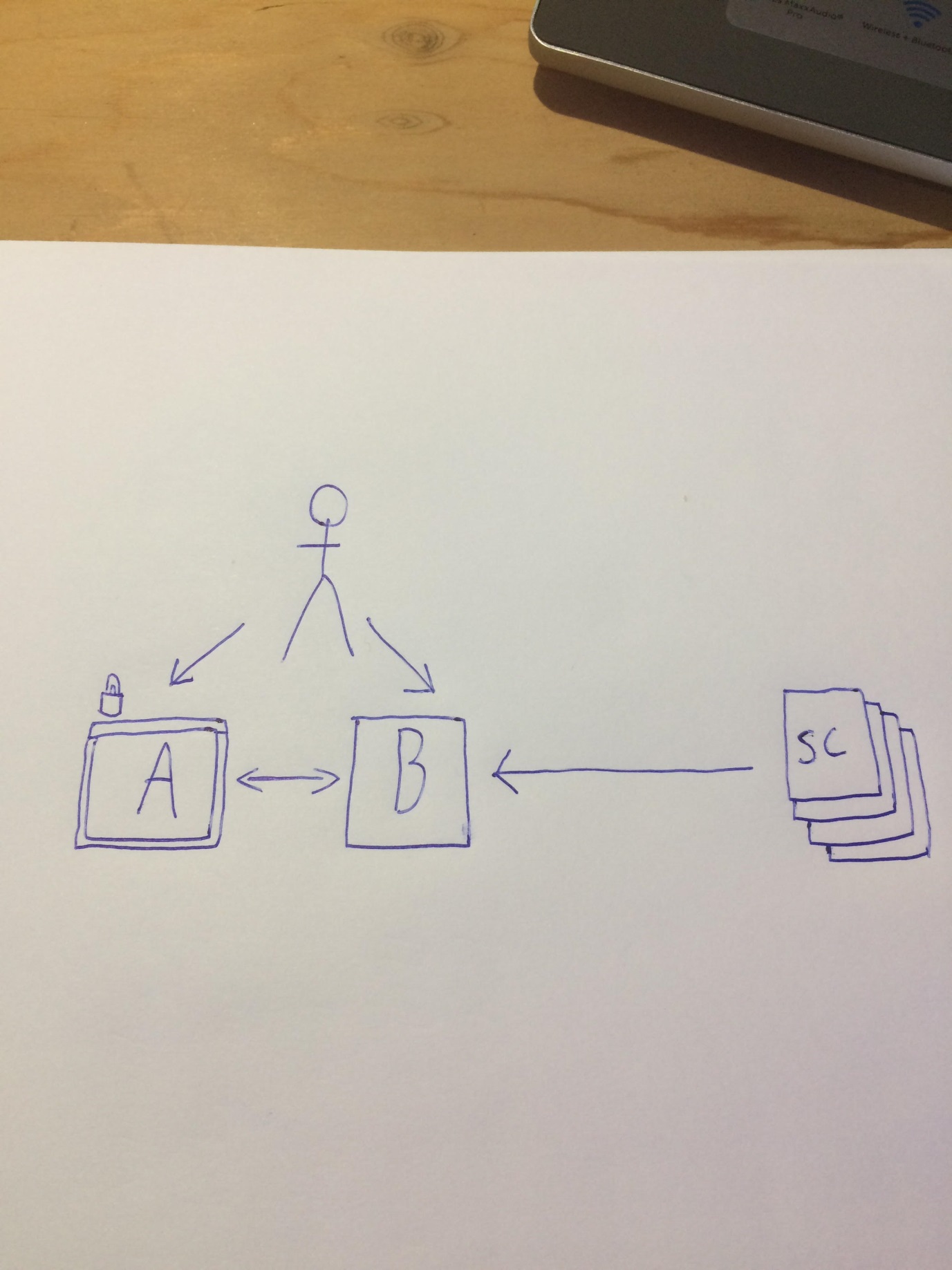
Accreditation authorities can fully digitise the verification process, providing channels to automate the authentication procedure.



The above High-Level event diagram outlines the first stage of the accreditation process, where a user requests a validation on the provided personal data.

### ID redaction

ID redaction can be facilitated through a smart contract framework that is agreed upon during validation request, with each accreditor given the freedom to create/alter the terms of ID provision as suits their industry.

Data within the SSID database is split into two parts, part A containing PII of the entity & any other highly sensitive accommodating attributes. Part B contains license-to-use attestations, such as a cryptographically signed proof of valid passport. This DB section contains no identifying data and thus is not secured, as it is worthless without the accompanying part A. Data in this section added after agreeing to certain T&C’s agreed to upon request, giving smart contracts admin access for ID revocation.

The above HLD outlines the split database and how Smart Contracts interact with the public half, leaving sensitive attribute data in the secure locker.

## Service Provider

Service Providers can, for the first time, truly digitise the Authentication process and outsource the Identity Management stack. An SSID architecture provides cryptographically signed proofs to a service provider who can check their authenticity via the immutable transaction entry in a blockchain, which further provides provenance assurance via traditional public key cryptography.

The Service Provider interface will need to satisfy the aspects that mirror current functionality regarding identity managed services – in some manner where further components can be incorporated in the future:

* Receive ID ‘proofs/claims’
* Confirm attestation certificate

### Claims interface

* User requests service
* SP asks for proofs
* User sends claims
* SP trusts claims
  + If not visit BC address 🡪 attestation ‘receipt’ and further links to authenticate if needed

Upon receiving a request for service, the provider will consider the individual proofs required from the user to prove identity – this will be communicated to the user across a digital interface owned by the provider.

User will select the proofs (with accommodating claims) from their personal Database – the address of said claims is sent with the data to the provider.

SP receives a DB data address, which contains the BC address of the request to data. The SP also receives a key file to decrypt the discrete sector of the DB containing the proof – thereby only viewing the required data points.

If the SP does not trust the user, they can check the validation which is placed on a block. This signature will contain a link to view further information regarding the user & accreditation authority – individual SP’s will decide their own LoA for each transaction.

### Blockchain interface

* SP receives claim
* SP 🡪 block containing signature
  + Contains additional information (WHAT??)

Upon receiving a user’s proof, if the SP does not by default trust the user’s claim, they can further check the validity by viewing the cryptographic signature the accreditor placed on a blockchain.

A cryptographic signature carries better assurance than a traditional signature as the data stored on the chain is signed – thus it is shown to be same data as the original accreditor uploaded. This will contain a link to find more detailed information regarding the specific identity validation.

# Non-standard ID

Identification frameworks need to have the capacity to authenticate not only natural people, but businesses as well – such a framework should accommodate individuals working in a business capacity and provide proof of a semantic relationship between person and legal entity.

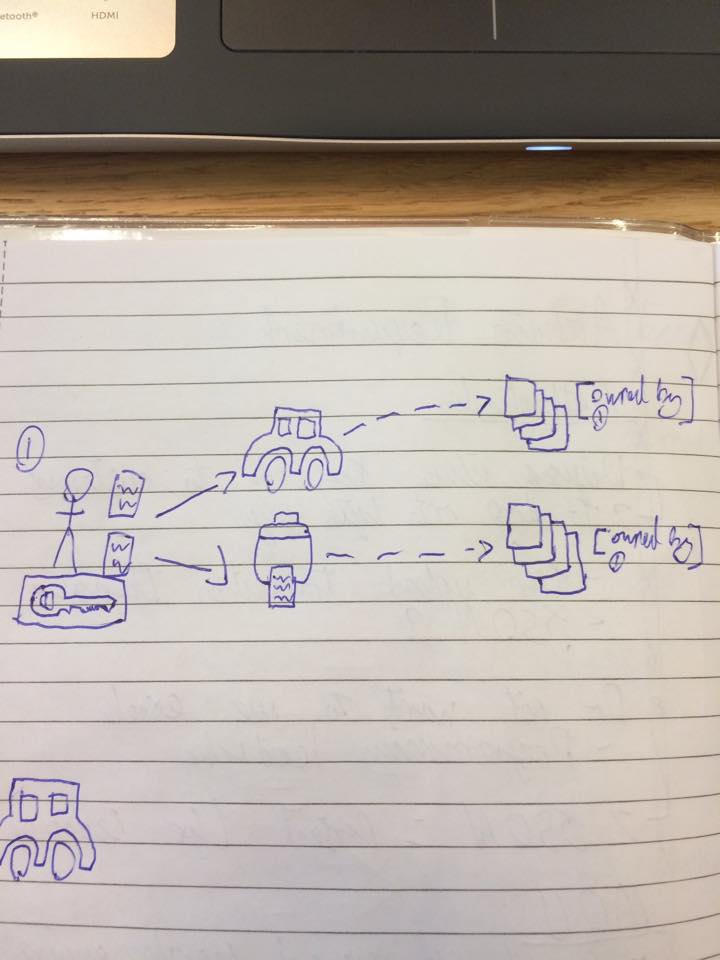
Further to this the proposed framework needs to accommodate identification of Objects (Physical and IoT) and the processes these create.

## Legal entity identifiers

At a very high level we need to be able to represent the identity of legal and natural persons in virtual systems (e.g. IT applications, networks, repositories etc) to support business transactions. At a practical level, this need is expressed in terms of support for identification, authentication and authorization in a secure, efficient and unambiguous way [3].

The LEI report [3] outlines further work needed within the Legal Entity Identification field, to globalise the standard and integrate it within more traditional PKI (X.509) frameworks to achieve strong linkage between natural persons and business processes.

## Objects

The ID framework must have the necessary functionality to address the ownership of objects in the virtual world, and the processes they create and interact with. A means by which an accredited natural person can associate ownership of objects is facilitated by leveraging the immutability of blockchain, by storing relationships between identifiers with assurance.

## Processes

More work needs to be done to examine different approaches for identifying and authenticating processes within digital environments.

# Security

## Storage

Distributing personal data across many databases, controlled by individual identities increases inherent security by design. Traditional cryptography techniques are used to secure & authenticate access to each database ‘locker’ – meaning the security process is moved down to a more granular level, encompassing each individual’s data separately. This greatly improves overall security of the system and makes it systematically impossible for large data breaches (multiple users) to occur as they do today.

Control of the data is now moved from the data handler back down to the individual – mirroring the current physical system where individuals look after their own physical documents.

## Distributed database

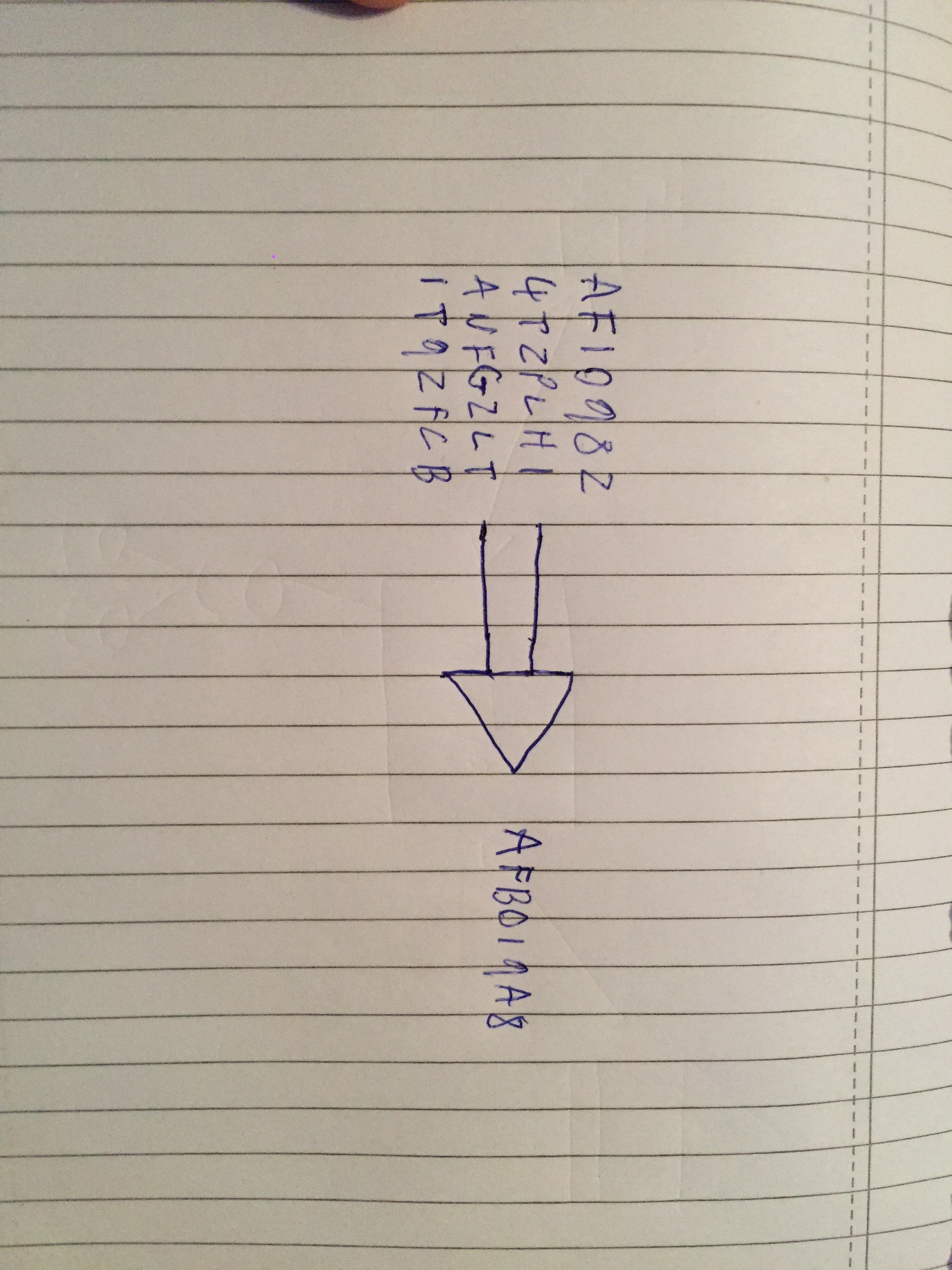
By leveraging distributed storage each individual’s data can be encrypted separately, greatly reducing the work-reward ratio for potential hackers by utilising multiple encryption keys per data set. Storing the data individually creates the opportunity to physically split up the data and utilise multiple different databases, further promoting security by design from increased friction for malicious actors.

## Data transfer

Zero-Knowledge Proofs can be used to share information about data without revealing the actual source – this is valuable in many situations and is backed by the assurance of current military grade encryption techniques.

ZK Proofs provide a protocol by which an individual can prove beyond reasonable doubt that they have knowledge of a data point, without sharing it.

### Zero-knowledge proofs

The above diagram outlines a high-level description of cryptography techniques that can be used to prove ownership of a data point without the need to share the actual data – this can be leveraged throughout an ID framework to ensure that sensitive data is stored only in one place, and that malicious actors cannot easily acquire it.

### Cryptographic hashes

A hash is the output of a cryptographic algorithm that scrambles source data into a machine-readable link of fixed size and is achieved in a way by which no 2 hashes can be the same if given different source input. This is currently leveraged throughout cyber security for sharing or storing sensitive details such as bank account numbers, or user passwords.

Hashes can be leveraged within the data transfer process to protect to integrity of sensitive information, reducing the effect of many targeted cyber-attacks such as man in the middle attacks.

# Privacy

## Data access conditions

Data access conditions will be different for each individual depending on their personal preferences, as will it be for individual businesses within separate markets. By utilising a smart contract framework to agree on criteria for data access, no individual is in control of the conditions and they can be enforced using a smart ledger – removing potential backdoors for either party and improving integrity.

# Outlook

Aims to provide a standardised framework of an identity system that uses blockchain, to provide ID for individuals, legal individuals, things (IoT & objects) and processes. The framework will be immediately useful, globally relevant and be implementable at a minimum of costs. TC307 SG 4 it is to be private by design and include security measures to reduce systematic risks which typically emerge when integrating with existing complex and non-standard systems. To ensure maximum useful adoption, the framework should disrupt the current socio-technical landscape as little as possible. TC307 SG 4 will also draw upon abstract development constructs to be flexible enough to incorporate future conceptualisations of identity. Central to the framework is the necessity that the data should be stored across many databases, each being held by an individual identity – increasing security by design and moving the responsibility of data handling back to the individual.

**The aim**: to provide a comprehensive definition of identity as a point of departure, which satisfies all four identity types (individual, legal, thing & process) to be processed on the blockchain. Additional aims include:

1. Analyse existing identity systems and infrastructure from around the world, minimise change of systems development within those bodies, verification engines etc.
2. Incorporate a flexible design that does not require agreement between governments or verifications bodies their usual role creating and identity data.
3. Responsibility of deciding if data verification meets the requirements of any legal or regulatory domain, or contractual requirements to provide a safe and adequate service must be left in the hands of the service providers themselves who will take due note of the regulatory/legal domains that they operate in and offer services in, and that which the service will be provided in.
4. Consequently, the services provided on the strength of the identity credentials presented, can be appropriately evaluated by the service provider themselves.

Potential future work includes:

* Distributed storage/analytics
* Smart contract framework
* Security risks and vulnerabilities
* Identity for Processes

# Interface for Verification of Digital Identity Documents

## Overview

The Document Verification API provides the issuer of ID Documents with a simple interface for retrieving and verifying electronic document data.

The API can be easily tailored to suit the requirements of the issuer’s existing data systems without the need for expensive code changes.

## Workflows

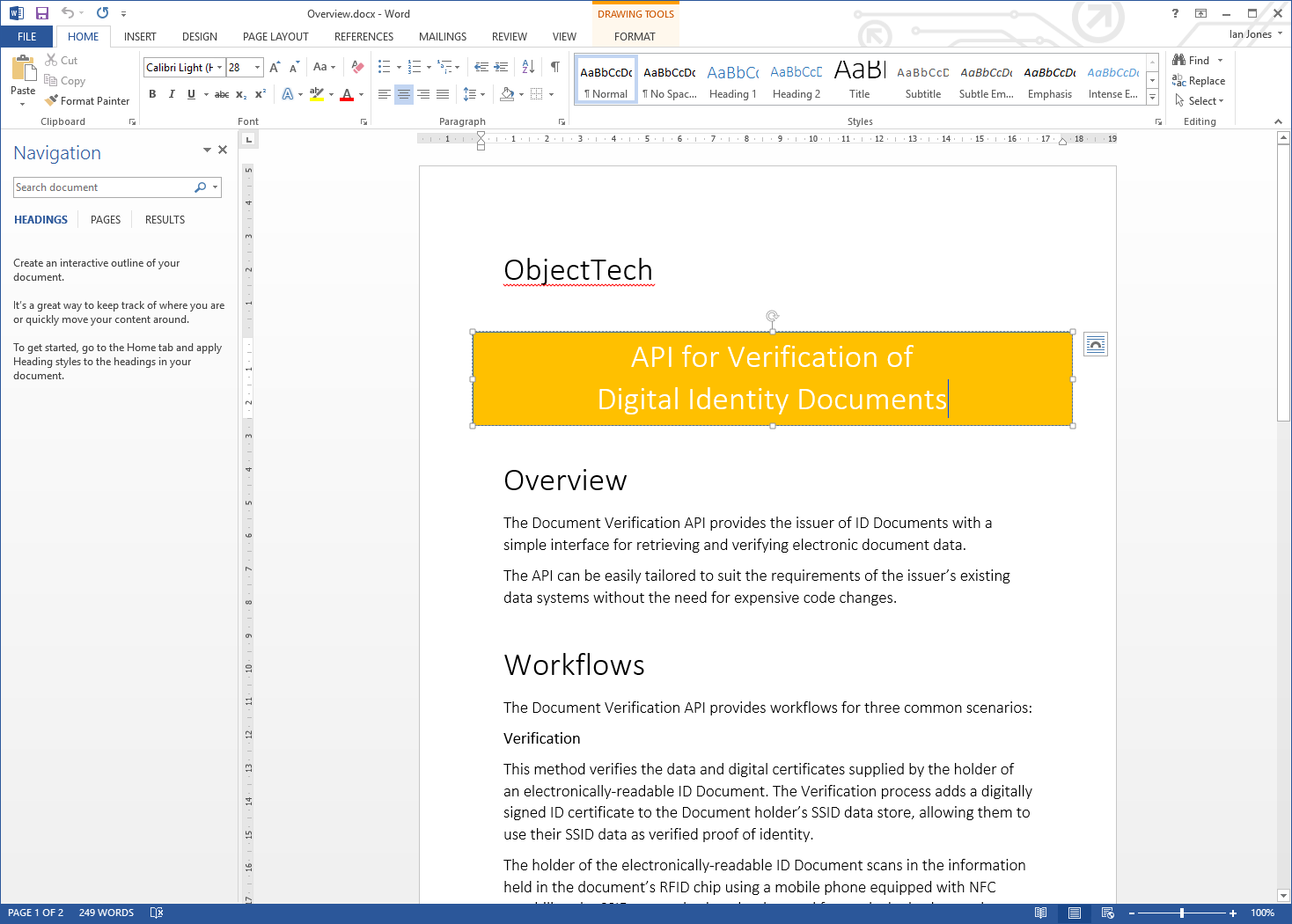
The Document Verification API provides workflows for three common scenarios:

### Verification

This method verifies the data and digital certificates supplied by the holder of an electronically-readable ID Document. The Verification process adds a digitally signed ID certificate to the Document holder’s SSID data store, allowing them to use their SSID data as verified proof of identity.

The holder of the electronically-readable ID Document scans in the information held in the document’s RFID chip using a mobile phone equipped with NFC capability; the SSID system hashes the data and forwards the hashes to the Issuer along with sufficient clear data to allow unambiguous identification of the ID holder.

SSID Request Buffer

Fetch Scanned ID Datata

Hashed ID Data

Clear ID Data

Retrieve Full Dataset

Hash Full Dataset

Compare Hashes

Verification Result

SSID Request Buffer

### Revocation

This method allows the Document Issuer to revoke a digitally signed ID certificate previously lodged in a Document holder’s SSID data store. This would be used when a Document has to be revoked or changed for any reason.

Revocation Command

Generate Acknowledgment

SSID System Actions Command

SSID Request Buffer

SSID Request Buffer

Fetch Acknowledgment

### Confirmation of Certificate

This method transmits the Issuer’s digital certificate to a third party which wishes to cross-check the digital certification on a SSID user’s digital ID document. This would normally be used when an ID Document is presented with an expired digital certificate.

SSID Request Buffer

Fetch Certificate Request

Select Certificate

SSID Request Buffer

### SSID Node

The local SSID Node runs on a Java Virtual Machine. It never initiates transactions with the host system, ensuring Denial Of Service attacks cannot be carried out from the SSID Network. Requests originating within the SSID Network are buffered within the local SSID Node, and are fetched as required by the host system.

### Communications

HTTP is used to communicate with the local SSID Node; all transactions are initiated by the host system polling the local SSID Node for pending transactions using an HTTP POST message; pending transactions are returned as Responses to the polls.

### Message Polling

Polling is entirely under the control of the host system, giving maximum flexibility and security. No commands or transactions are sent from the local SSID Node to the host system.

### Data Formats

Messaging between the local SSID Node and the Issuer’s host system uses XML formats throughout, allowing maximum compatibility with the host system. All messages are processed by XSLT translators within the SSID Node, and changes to the host system’s data formatting requirements can be met simply by editing the XSLT templates.

## Sample Code

### Request Next Pending Transaction from SSID Node

POST localhost:11223/incoming.html

<?xml version="1.0"?>

<TransactionRequest>

<Timestamp>01/02/2018 at 14:38:17 GMT</Timestamp>

</TransactionRequest>

### Document Verification

POST localhost:11223/incoming.html

<?xml version="1.0"?>

<DocumentVerification>

<Timestamp>01/02/2018 at 14:38:17 GMT</Timestamp>

<TransactionID>8948611d6f4a6c654654ee654b</TransactionID>

<VerificationResult>Document Verified</VerificationResult>

</DocumentVerification>

### Document Revocation

POST localhost:11223/incoming.html

<?xml version="1.0"?>

<DocumentRevocation>

<Timestamp>01/02/2018 at 14:38:17 GMT</Timestamp>

<IdDocument>98344-2340938234820394-77</IdDocument>

<RevocationTime>Immediate</RevocationTime>

</DocumentRevocation >

### Certificate Confirmation

POST localhost:11223/incoming.html

<?xml version="1.0"?>

<CertificateConfirmation>

<Timestamp>01/02/2018 at 14:38:17 GMT</Timestamp>

<TransactionID>8948611d6f4a6c654654ee654b</TransactionID>

<Validity>

<Start>20180101</Start>

<End>20201231</End>

</Validity>

<Certificate>3445645d564e56456aaa564c54b454d564c564b45…

</CertificateConfirmation>

Bibliography

[1] World Economic Forum – “A blueprint for digital identity” August 2016 <http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf>

[2] <http://www.wired.co.uk/article/estonia-e-resident> Wired - “Concerned about Brexit? Why not become an e-resident of Estonia”

[3] Global Legal Entity Identifier Foundation (GLIEF) – The true nature of identity in business applications, Stephan Wolf

[4] Pam Dixon – A failure to “do no harm” – India’s Adhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S, 14th June 2017

[5] Shoshana Magnet - When Biometrics Fail: Gender, Race, and the Technology of Identity, Duke University Press 2011