D6.4 Blockchain and DLT technologies

Document Due Date:	31.05.2020 (M09)
Document Submission Date:	29.05.2020 (M09)

Work Package 6:
Alternative technologies to identifying people

Document Dissemination Level:	Public

D4FLY - **D**etecting **D**ocument frau**D** and i**D**entity on the fly
This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 833704

Abstract

In the context of alternative technologies to identifying people, this D4FLY deliverable describes the use of digital identity in border identification, and appropriate related blockchain and distributed ledger technologies. Two use cases are defined, that focus on alternative ways to enrol and verify traveller, using digital identity combined with distributed ledger technology, biometric data and smart contracts. In addition, use cases for blockchain technology in the context of document verification are proposed. These use cases are related to immunization passports, travel history ensured by blockchains, and decentralized PKIs. Also, some recommendations and challenges regarding the use of the distributed ledger technologies are identified and described.

Project Information

Project Name	Detecting Document frauD and iDentity on the fly
Project Acronym	D4FLY
Project Coordinator	Veridos GmbH
Project Funded by	European Commission
Under the Programme	Horizon 2020 Secure Societies
Call	H2020-SU-SEC-2018
Topic	SU-BES02-2018-2019-2020 Technologies to enhance border and external security
Funding Instrument	Research and Innovation Action
Grant Agreement No.	833704

Document Information

Document reference	**D6.4**
Document Title	**Blockchain and DL technologies**
Work Package reference	WP06
Delivery due date	31.05.2020 (M09)
Actual submission date	29.05.2020
Dissemination Level	Public
Lead partner:	VTT
Author(s)	Kimmo Halunen, Anni Karinsalo
Reviewer(s)	Mirko Sailio (VTT), Armin Reuter (VD), Dimitris Kyriazanos (Demokritos)

Document Version History

Version	Date created	Beneficiary	Comments
0.1	7.11.2019	VTT	First draft
0.2	15.1.2020	VTT	Version to common workspace
0.3	6.5.2020	VTT	First review
0.4	12.5.2020	VTT	Second review
0.5	22.5.2020	VTT	Final review
1.0	28.05.2020	VD	Final edits

List of Acronyms and Abbreviations

ACRONYM	EXPLANATION
D4FLY	Detecting Document frauD and iDentity on the fly
DLT	Distributed Ledger Technology
EC	European Commission
ETSI	European Telecommunications Standards
EU	European Union
GSMA	GSM Association
ISO	The International Organization for Standardization
ITU	The International Telecommunication Union
NIST	National Institutes for Standards and Technology
OIDF	The OpenID Foundation
PKI	Public Key Infrastructure
W3C	World Wide Web consortium

Table of Contents

1 INTRODUCTION 8

1.1 BACKGROUND: CENTRALIZATION VS DECENTRALIZATION 8

2 BLOCKCHAIN AND DLT 9

2.1 MAIN PROPERTIES 9
2.2 SECURITY CONSIDERATIONS 9

3 DIGITAL IDENTITY 10

3.1 CONCEPTS OF DIGITAL IDENTITY AND DECENTRALIZATION 10
3.1.1 DECENTRALISED IDENTIFIERS 11
3.1.2 CLAIM 11
3.1.3 VERIFIABLE CLAIMS 11
3.1.4 CREDENTIAL 11
3.1.5 VERIFIABLE CREDENTIAL 11
3.1.6 SUBJECT 11
3.1.7 IDENTIFIER 11
3.1.8 ISSUER 11
3.1.9 VERIFIER 12
3.1.10 REQUESTER 12
3.2 SELF-SOVEREIGN TECHNOLOGIES AND PROVIDERS 12
3.2.1 SOVRIN 12
3.2.2 HYPERLEDGER INDY (NODE AND PLENUM) 12
3.2.3 EVERNYM 12
3.3 ASSURANCE AND STANDARDIZATION REGARDING DIGITAL IDENTITY 12
3.3.1 EIDAS 12
3.3.2 NIST 12
3.3.3 ISO/IEC 29115:2013 13
3.3.4 STANDARDIZATION BODIES 13

4 RELEVANT USE CASES IN THE CONTEXT OF D4FLY 14

4.1 EXEMPLARY CASES OF DIGITAL IDENTITY USAGE 14
4.1.1 SISUID 14
4.1.2 ICAO 14
4.1.3 FINDY 14
4.1.4 SINGAPORE NATIONAL DIGITAL IDENTITY (NDI) 14
4.1.5 UK - GOV.UK VERIFY 14
4.1.6 CANADIAN DIACC 15
4.1.7 NETHERLANDS – DIGID 15
4.1.8 DUBAI - SMARTPASS 15
4.1.9 SITA 15
4.1.10 COVID CREDENTIALS INITIATIVE 15
4.2 PROPOSED USE CASES FOR D4FLY 16
4.2.1 DIGITAL IDENTITY AND BIOMETRICS: USE CASE 1 16
4.2.2 DIGITAL IDENTITY AND BIOMETRICS: USE CASE 2 16
4.2.3 USE CASES RELATED TO DOCUMENT VERIFICATION 18

5 DISCUSSION 20

5.1 APPLICABILITY OF TECHNOLOGIES IN D4FLY 20

5.2 DIGITAL IDENTITY AND BIOMETRICS 20
5.3 RECOMMENDATIONS 20
5.4 CHALLENGES 21

6 CONCLUSIONS 22

REFERENCES 23

LIST OF FIGURES 24

1 INTRODUCTION

This document describes the uses of blockchains and Distributed Ledger Technologies (DLTs) for identification in the context of the D4FLY project. The main focus will be on digital identity and its possibilities in the border control context. As a groundwork for this, we present the basic concepts and advances of digital identity, such as self-sovereign identity (SSI) and some applications of digital identity used around the globe.

Related biometrics technology applicability is discussed in such a way, that is useful in the light of applications developed in D4FLY for border use. Potential use cases are described and the technologies that enable those presented in more detail. Also the challenges, limitations and future research topics are discussed. A summary of the findings and a conclusion is given in the end of this document.

1.1 Background: centralization vs decentralization

Nowadays, the more organized aim[1] is that user should be given more control of his own data. General Data Protection Regulation (GDPR) is one consequence of this requirement for privacy, and now there should be more comprehensive systems following this philosophy. A centralized management model of user's identity when accessing and using systems is not always the best option, at least as a single usable option, due to many reasons. One of the reasons is privacy; often decentralized methods enable the user to control better his anonymity and his own data. Another reason to transfer into decentralized systems is security-related: general security can also be improved due to lesser single point of failures and trust added because of the immutable nature of distributed ledger technologies.

On the other hand, some of the properties of decentralized distributed ledger technologies may work against the regulations. For example, the right to be forgotten can be hard to enforce in a DLT system. In addition, the liabilities from regulation are also retained despite decentralization, and thus it is important to pay attention to both what data is stored on DLTs and how this data is protected.

[1] https://id2020.org/

2 BLOCKCHAIN AND DLT

2.1 Main properties

Blockchain applications today are more and more heterogenous, whereas many people earlier considered the term “blockchain” depicting solely virtual currencies. For example, solutions such as Sovrin [2] have proved the strength of distributed ledger solutions in the context of managing a person’s identity online. In the context of digital identity, especially in a decentralized management model and foreseeing the future of it, viable solutions have to offer auditable trust in the underlying technology with the help of open source code and standards. [7] Due to the decentralized and immutable nature of blockchains and decentralized technologies alike, these could be of use as technology for these viable solutions. At the same time, however, these technologies have to maintain privacy and offer data protection.

2.2 Security considerations

When applying distributed ledger technology, there are naturally various implementation variations already inside one technology, not to mention choosing between several technology platforms. Decisions have to be made regarding for instance the used programming language, necessary interfaces and so on. When these are applied in the context of digital identity, the considerations that most affect the end result are first of all with the choice between public vs private blockchain and the choice of used consensus mechanism. Awareness towards the type of data that will be stored on the blockchain is also necessary.

In many cases blockchains and DLTs are categorized by two properties regarding the access to the information on the ledger and the ability to add new information on the ledger. If any actor or organization has access to the information on the ledger, the ledger is called *public*. This means that anyone can see the ledger and the transactions stored in there. A *private* ledger has some restrictions on who can view the information on the ledger. This can be a single organization or a closed consortium of organisations. In a *permissionless* ledger, anyone can make and add transactions to the ledger (depending on the consensus algorithm, of course). A *permissioned* ledger is one, where the ability to add information is restricted by some form of permission system. These can be very lenient or restrictive or something in between depending on the use case and the requirements of the system.

3 DIGITAL IDENTITY

Digital identity is becoming a more and more important concept and technologies to realise it are now emerging at a high speed. Their relevance to border security is immediately obvious and as such they provide a great venue to apply the blockchain and distributed ledger technologies.

This chapter presents the key concepts related to digital identities and some technologies that are used to implement them. For more deeper insights and thorough technical details the reader is instructed to delve into the references provided in this document.

Regarding any digital ID system – identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding/credentialing, authentication, and portability/federation (where applicable) must be digital. [1] Binding or credentialing means that during identity enrollment, user's unique identity data (to be stored) is attached to the authenticating features owned by the user, and which are about the user.

The use of a digital ID system may variate for example amongst:

- Electronic databases, including distributed ledgers, to obtain, confirm, store and/or manage identity evidence
- Digital credentials to authenticate identity for accessing mobile, online, and offline applications
- Biometrics to help identify and authenticate individuals, and
- Digital application program interfaces (APIs), platforms and services that facilitate online identification/verification and authentication of identity. [1]

In this document we will not deeply discuss the more broader issues related to digital identity and authentication. When these are discussed they will be only in the context of D4FLY and mostly related to biometrics.

3.1 Concepts of digital identity and decentralization

In the following, some relevant concepts are shortly described that are focal in the area of digital identity, from the context of decentralization. Some concepts are purely based on decentralization, such as self-sovereign identity. Some concepts, such as credentials, could be also a part of centralized digital identity setting, but explained briefly here from the decentralized model point-of-view whenever possible. Self-sovereign identity

Self-sovereign identity can be considered an extension model or special case of digital identity. Instead having the traditional model of managing and controlling identity data by the third parties, self-sovereign model offers a concept in which an end user can manage and restrict the use of his own data. When giving up the model of having either various user account/password combinations, or single-sign-on systems managed by a single organization, self-sovereignty can be implemented with the use of decentralization, namely storing the data with the help of distributed ledgers. Architecturally this means distributed nodes of the network are sharing the same data and mutually agreeing on how and what data to add to the database (blockchain). If implemented correctly, for the end user self-sovereign model can offer not only easier and more trusted authentication to systems, but also enabling to select whether and what kind of identity proof data (credential) is shown when authenticating into systems.

There are digital identity initiatives around self-sovereign identity management in travel context, such as Known Traveller Digital Identity [5] that adhere to this trend.

3.1.1 Decentralised Identifiers

Decentralised identifiers (DID) are globally unique identifiers, that are not dependent on any centralized verifier. Therefore, one way to realise self-sovereign identity is to utilize decentralised identifiers. In general, as the name implies, any decentralised digital identity model requires that the identity claims are to be stored in a decentral manner. One consequence of this is that the risk regarding single point of failure, existing in traditional identity model relying in central authorities, is removed. Regarding identity management with the help of blockchains, National Institute of Standards and Technology (NIST) defines the term "identifier" as a "blockchain address or other pseudonym that is associated to an entity" [6].

In Sovrin (see 3.2.1), the structure of decentralized identifier architecture is composed of the DID itself (that has no cryptographic properties) and its associated DID document, which contains metadata and cryptographic data of the current identity. The metadata is about how the identity should and could be used in the context of Sovrin.

3.1.2 Claim

A claim is a trait or statement (or a set of statements) that describes the subject, person to be identified.

3.1.3 Verifiable claims

A verifiable claim is a cryptographically trusted, non-reputable digital claim that is made by others about the subject. Verifiable claim can be issued by for example a workplace that announces that the employee has been working at them for a certain period of time, which can be proven by a digital reference. In Sovrin, the verifiable claim is linked to its issuer (more precisely, issuer's DID) by its public key.

3.1.4 Credential

One or several claims together about the subject form a credential. A credential may include also metadata and some identifier.

3.1.5 Verifiable credential

Verifiable credential is just like credential, but it has to include identifier and metadata that allows to prove its validity cryptographically.

3.1.6 Subject

Subject is the person that is identified and who holds the identifier.

3.1.7 Identifier

In a decentralized identity setting, identifier is the blockchain address containing reference to credential.

3.1.8 Issuer

Issuer issues the credential to the requester as he asks for it.

3.1.9 Verifier

Verifier verifies the presentation for the relying party.

3.1.10 Requester

Requester requests a credential from an issuer.

3.2 Self-sovereign technologies and providers

3.2.1 Sovrin

Sovrin [2] is an open source distributed ledger-based, public identity network. In Sovrin, the validator nodes that validate and allow the transaction writing to the blockchain, are called Stewards, and are operated by various trusted organizations. In the context of Sovrin, claims are about the subject and the claim issuer issues the claim originally. Verifiable claims in the context of Sovrin are verifiable by the signature of attestation issuer that has either issued the claim himself or can attest the correctness of it. [3]

3.2.2 Hyperledger Indy (Node and Plenum)

Hyperledger Indy[2] implements a distributed ledger for the purpose of decentralized identity. It is maintained by Linux Foundation and its essential components are, amongst others, Hyperledger Node (the basic self-sovereign identity ecosystem), and Hyperledger Plenum (Byzantine Fault Tolerant Protocol). Indy can be configurated to use Sovrin network, or some other type of network.

3.2.3 Evernym

Evernym is an ecosystem provider for self-sovereign identity management. The ecosystem includes for instance platform, wallet app and authentication tools. It utilizes Hyperledger Indy and Sovrin as part of the ecosystem.

3.3 Assurance and standardization regarding digital identity

3.3.1 eIDAS

eIDAS is applied on an EU level, providing procedures and specifications for digital identity based on EU regulation Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015, and ISO/IEC 29115. Assurance model in the eIDAS specification consist of three distinct levels of different strength (low/substantial/high), relating to evaluated identity framework reliability.

3.3.2 NIST

NIST provides regional procedures and specifications in the United States area regarding digital identity. In NIST model regarding digital identity assurance (Identity Assurance Level,

[2] https://wiki.hyperledger.org/display/indy/Hyperledger+Indy

IAL), authentication assurance (Authentication Assurance Level AAL) and federation assurance (Federation Assurance Level, FAL), there are three levels in each depending on the reliability required from the identity framework under evaluation.

3.3.3 ISO/IEC 29115:2013

ISO/IEC 29115:2013 offers an authentication assurance framework for managing entity authentication in given context. It provides four levels for authentication assurance for the identity framework under evaluation.

3.3.4 Standardization bodies

Main standardization bodies involved in the digital identity development include The International Organization for Standardization (ISO), The International Telecommunication Union (ITU), W3C, The FIDO Alliance, The OpenID Foundation (OIDF), GSMA, European Telecommunications Standards Institute (ETSI).

4 RELEVANT USE CASES IN THE CONTEXT OF D4FLY

This chapter presents on-going or upcoming implementations of digital identity, with some utilizing distributed ledger technology and blockchains in relevant areas for D4FLY, as well as potential new development ideas for the project.

4.1 Exemplary cases of digital identity usage

4.1.1 SisuID

SisuID[3] is a dedicated community-hosted Finnish authentication and digital identity platform for end users and service providers, offering strong authentication for the users and normal and strong authentication levels for service providers. It is used with special mobile application and is based on eIDAS.

4.1.2 ICAO

International Civic Aviation Organization (ICAO) provides specification documentation related to aviation, so called Standards and Recommended Practices (SARPS) and Procedures for Air Navigation (PANS). Regarding digital identity, ICAO provides covering specifications for electronic travel documents, Machine Readable Travel Documents.

4.1.3 Findy

Finnish Indy ledger and network (Findy[4]) is a decentralised identity ledger, that is governed and run locally and aiming at enabling pilot use cases and services that use self-sovereign identifiers in Finland.

4.1.4 Singapore National Digital Identity (NDI)

Singapore National Digital Identity (NDI)[5] is a digital identity system for Singapore residents and businesses to transact securely and digitally with the Government and private sector. The system is constructed of several modules: authentication system Singpass itself, mobile application for Singpass, using fingerprint and facial recognition as well as passcode, MyInfo service for automatic online form filling, and developer and business portal. The system will be used in 2020.

4.1.5 UK - GOV.UK Verify

GOV.UK Verify is a federated digital identity scheme, which uses private sector identity providers to authenticate via GOV.UK Verify Hub. [6] As of May 2020, there are 5 of these

[3] https://sisuid.com

[4] https://www.findy.fi

[5] https://www.smartnation.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/national-digital-identity-ndi

[6] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

"certified companies". GOV.UK Verify Hub is a centrally managed infrastructure managing connections between parties: users, identity providers, and government and related services.

4.1.6 Canadian DIACC

Digital ID and authentication council of Canada (DIACC)[7] is a committee driving several initiatives utilizing digital identity in Canadian government services and alike.

4.1.7 Netherlands – DigiD

Dutch DigiD[8] is an identification and authentication tool to be used within governmental online services. Service providers are given a unique "burgenservicenummer" that is respective of the user's DigiD account. DigiD is used via mobile application with pin code or with a username/password and SMS verification.

4.1.8 Dubai - Smartpass

Dubai is currently utilizing Smartpass[9] digital identity platform developed by Smart Dubai Government Establishment (SDG), Telecommunications Regulatory Authority (TRA) and Abu Dhabi Digital Authority (ADDA). The related application, UAEPASS[10], enables digital identity management, mobile phone based authenticated access to services and digital signature of documents.

4.1.9 SITA

SITA has been accepted as a Sovrin steward and they propose to build a domain specific trust platform for SSI in the air travel domain. This system would be built on top of the Sovrin system and it would provide the legal and technological base for more seamless travel.[11]

4.1.10 Covid Credentials Initiative

One interesting digital identity use case brought about by the COVID-19 pandemic is so-called immunization passports. These would be digital credentials certifying the status of an individual (usually with respect to the COVID-19) and her possible immunization against this disease. At the moment there are some initiatives around this. One example is Covid Credential Initiative[12], where several organisations are trying to solve this problem through digital identity credentials. For more thorough presentations on the subject, please see the video of MyData vs. COVID webinar[13].

---

[7] https://diacc.ca/

[8] https://www.digid.nl/en/

[9] https://www.government.ae/en/information-and-services/g2g-services/smartpass

[10] https://selfcare.uaepass.ae/

[11] https://www.sita.aero/resources/blog/a-turning-point-in-aviations-identity-and-data-management

[12] https://www.covidcreds.com

[13] https://www.loom.com/share/6982824b15da4f21a65996e80ba1cdaf

4.2 Proposed use cases for D4FLY

Blockchain technologies and DLTs are to be utilized from two different point of views in the D4FLY project. The first focus is on alternative technologies to identifying people, therefore this document studies mainly blockchain technologies related to the use of biometrics and digital identity. The other focus in the project related to blockchains, is on document verification and fraud. We describe the potential use cases for both point of views in this report.

4.2.1 Digital identity and biometrics: Use case 1

In Use case 1, digital identity could be incorporated to an existing scenario as an add-on or an alternative solution for identity information. In this existing scenario, the usage of smartphones as an alternative carrier of identity information is investigated. Typically, the smartphone is used as a means of intermediate storage (with some additional functionality) of identity data between an enrollment process and the usage of certain identity related data during an identity verification process e.g. at the border. Blockchain technology could be used to complement or in certain areas substitute the smartphone in these kinds of use cases.

In Use case 1, the user would enrol their additional biometrics through a distributed (self-sovereign) digital identity system instead of the kiosk. This enrolment could be done by the traveller at any point in time before entering information in the kiosk. If there are some requirements (e.g. supervision) on the setting where enrolment needs to be done, these can be enforced by the enrolment system. These biometrics can be anything that the further officials can then verify at the point of verification. The traveller could have these biometrics in a separate cloud storage or distributed through different services as shares (like secret sharing schemes) and then assembled at the kiosk and/or the verification point. The kiosk could verify these biometrics and provide some form of credential to the user. This credential can be displayed as a QR code or some other type of visually readable format. Verification of this credential could be done then also at the border. This approach is illustrated in Figure 1. Alternatively, also the biometrics can be verified as when interacting with the kiosk.

The benefit of this approach would be that the user does not need to share their biometrics with a central database (even if these are encrypted). The kiosk and border checkpoint infrastructure could get the necessary biometrics from the third party store, where the user has decided to keep this information. In addition, this approach can be combined with the Horcrux [8] protocol, which divides the biometrics into distinct shares using Shamir's secret sharing scheme (Figure 1). Thus, the user could have one share with their device and only the other share is requested from the third party store. Each of the shares in themselves do not reveal the biometric. Only the combination will reveal the full biometric and allow matching.

4.2.2 Digital identity and biometrics: Use case 2

Use case 2 describes an alternative way to identify using the scenario, in which there is a coach crossing a border. There are a number of travellers in the coach and a border official needs to check their credentials by entering the coach and checking the tickets, travel documents etc. of the travellers. The aim in this scenario is to study traveller identification with a mobile phone application, using some biometric sample verification and comparing this to pre-enrolled template. The user handles the enrolment and the border guard does the identity checking, both handled with the mobile application.

In the context of distributed ledgers, similar approach to the enrolment as described above in Use case 1 could be used through a digital identity system. In addition, it would be possible to

combine smart contract solutions to the travel document. This could work by combining the journey number with a smart contract ticket (Figure 2). The ticket would get the biometric and other information from the digital identity store specified in the contract. This information could be matched against the data from the read document either at the kiosk or by the border guard in the coach. The smart contract would be specified (and approved) by both the travel agency and the border officials. The border guards could interact with the smart contracts with their mobile devices while entering the coach. This approach is illustrated in Figure 2.

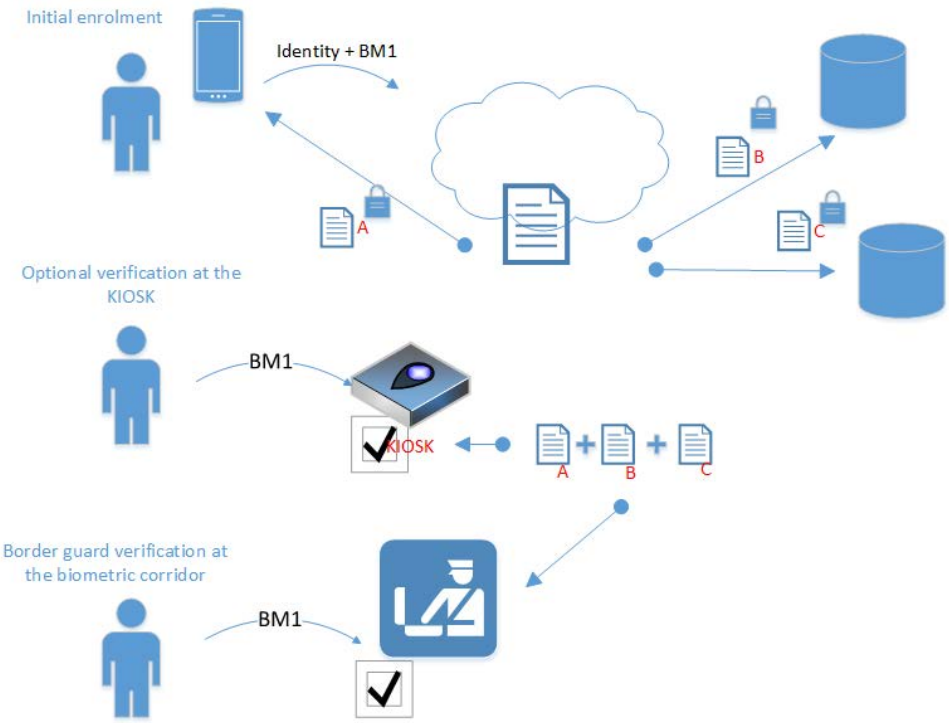

FIGURE 1: ENROLLMENT BY MEANS OF DIGITAL IDENTITY SYSTEM

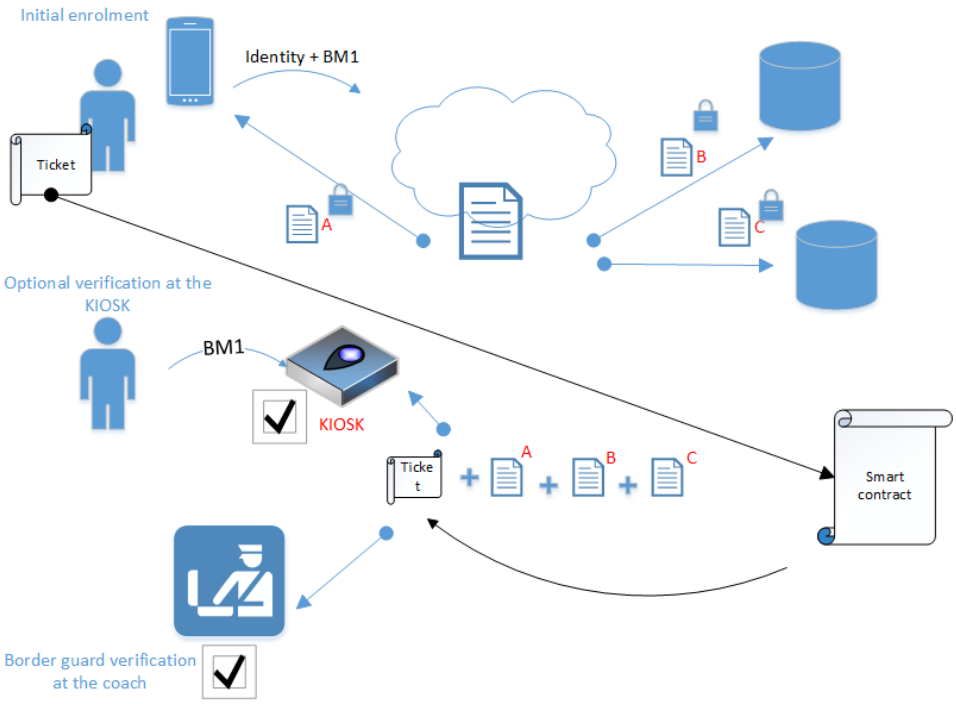

FIGURE 2: ENROLLMENT BY MEANS OF DIGITAL IDENTITY SYSTEM, TICKET STORED TO SMART CONTRACT

4.2.3 Use cases related to document verification

The aim in these use cases is to handle document verification, with the use of DLT technology by preventing digital manipulation with blockchain. The motivation of presenting also the use cases related to document verification with blockchains in this document, is that they share synergy in their technical perspective. Currently two different use cases for blockchains and DLTs have been proposed for document verification. These are 1) faster passport verification through smart contracts and blockchain and 2) document exception verification using blockchain. In practice the first case means that there is a system that can store timestamped and signed records on manual and automatic passport scans into blockchain included in the D4FLY-system. The border officials can access this information and speed their processes through quicker checks of (possibly) irregular passports. The system can also be expanded to include other travel documents (e.g. visas). In the second use case, the aim is to handle exceptional situations, where traveller's travel documents may differ from regular templates and standards due to country of origin's differentiating procedures. Materials may be different or some abnormal document processing may be used. By storing format exceptions into blockchain time can be saved by verifying the authenticity of an irregular travel document. This happens so that during document verification, any deviations can be (manually) checked from the blockchain (ideally, country authorities should have stored these deviations from the standard into blockchain beforehand). In this model, every verifying authority has a local copy of the dataset, thus maintaining the traveller privacy.

Further possible use cases include the topical issue of so called immunization passports. These would be credentials that verify that the holder of the credential is immune to certain disease e.g. COVID-19. This could be tested as a standalone demonstrator. However, there is currently no consensus, if these types of immunization passports are necessary and relevant in the current COVID-19 pandemic. On the other hand, these might be useful also with other immunization requirements.

Fourth use case is trust addition by having a verification history of a given individual and their travel credentials secured on a blockchain. This could provide a track record of verifications that the credential(s) have been subjected to and make the subsequent verifications faster. This might also raise some privacy concerns although it is possible to only store the information in either encrypted or even hashed from to prevent tracking of specific individuals and or credentials.

Overall, there might be a possibility to augment or replace the PKI over which the digital passports etc. are verified with a decentralized blockchain based approach. These types of solutions have already been proposed as decentralized PKI. These could even be combined with smart contracts to facilitate key management. Thus, this action is mainly about the decision whether the end users and their organisations want to retain the centralized model or to move towards a decentralized model.

5 DISCUSSION

5.1 Applicability of technologies in D4FLY

As such, the planned D4FLY technologies do not necessarily "need" decentralized systems to function properly, in other words they are secure and fit for their purpose as they are. In terms of identity verification use cases, decentralized methods suggested in this paper offer either replicated or different (double-reassured) way to verify identity, when it comes to end result. However, as the "under the hood" implementation is different, decentralization in digital identity management decreases the risk of having a single point of failure and enables adding other digital identity functions and services made possible by decentralization.

One possibility is to build "SSI readiness" into the D4FLY system and demonstrate it with some SSI system (e.g. Sovrin) and "mock" credentials as real travel credentials might not be available until very late into the project. This would then make the resulting system ready for application, when SSI becomes more widespread and it is used in for example with SITA systems. It could be possible to partner with third parties such as SITA, Findy or SisuID, who are working on this domain already.

In usage of distributed ledger technologies in D4FLY context, as naturally elsewhere too, one must consider the restrictions for data that is stored in the ledger, due to immutability and especially easy availability of its data.

5.2 Digital identity and biometrics

In the D4FLY project, there are many use cases for biometrics and using different biometric factors as identifying information for border crossing. These biometric factors can also be linked with the digital identities of the users of the D4FLY platform.

When considering SSI systems, biometrics can be used to unlock the claims that the user has in her possession. This can be done through a mobile device or a (web) portal, where the user has access to the necessary keys. In a more extreme scenario, the biometrics could be the keys used to provide the claims about digital identity.

5.3 Recommendations

Based on these early findings of our research we present some recommendations on the use of blockchain and DLT in the context of digital identity and biometrics in D4FLY use cases. First of all, blockchain can provide possibilities in building trust on the current systems e.g. through decentralized PKI. The possibilities and especially acceptability of this type of solution should be studied. The technical capability to realise such a system exists.

In this project, we propose to choose one of the above-mentioned potential use cases to be further studied and demonstrated in a standalone demonstrator later in the project. The decision on which use case should be further studied will be made in collaboration with partners of the consortium. The demonstrated use case can be either related to digital identity or document verification, based on which is deemed the most relevant topic decided by the consortium.

Overall, we see that the use of self-sovereign digital identity and its possible combination with biometrics needs to be studied. Our recommendation is to start by applying SSI in relevant D4FLY scenarios and seeing if biometric information can be added to these in a secure way.

5.4 Challenges

Although blockchain and DLT bring possibilities and enable possible improvements to current systems, there are also challenges related to their use. One challenge is the acceptability of the decentralized solutions over the current centralized and silo-like approach. The trust model is very different in the decentralized model and it might not be possible to realise that without a change in some attitudes towards a more decentralized model.

Many of the DLT and blockchain based technologies are quite young and are changing at a rapid pace. This might be a problem, when attempting to build more lasting and long term solutions. At the very least the organisations implementing these solutions need to be aware of the possible technological change. A better way to prepare for this is to build solutions that allow for easy updates, when the digital identity systems change.

This might also be necessary from a security perspective. The advanced cryptographic systems used in many SSI solutions and in blockchains in general are not necessarily quantum-safe [9]. This means that a quantum computer might break the cryptographic guarantees of such as system. Because these are very long-term endeavours the uncertainty about powerful quantum computers needs to factor in on the decisions how and when to use these digital identities. For the basic use case of signatures, there will be NIST standards available later in the 2020s, but for many other necessary cryptographic features, these will not be available in a short while.

Despite the challenges, it is important to experiment with and adapt to the new digital identities, blockchains and DLTs also in the context of border crossing and biometrics. The challenges are not insurmountable and the benefits of these new technologies can be significant in the right use cases.

6 CONCLUSIONS

We have described the scope and use cases for D4FLY that combine digital identity, blockchains and biometric data for the use of enrolling and verifying traveller's identity, with possibility to add enhancement of storing and combining biometric data shares securely. Another use case focuses on combining smart contract functionality with traveller data. We have also proposed some extensive uses for the current blockchain use cases in the context of document verification. These extensive uses are related to immunization passports, travel history ensured by blockchains, and decentralized PKIs.

The next step is to identify the most suitable potential use case of these technologies for the D4FLY project and build a standalone demonstrator for the partners to evaluate.

In addition, this report includes some general recommendations and challenges regarding the use of these new technologies that have been identified and discussed.

REFERENCES

[1] Draft guidance on digital identity for public consultation. Financial Action Task Force (FATF). http://www.fatf-gafi.org/media/fatf/documents/publicconsultation/Digital%20ID-public-consultation-version.docx

[2] Dmitry Khovratovich, Jason Law. Sovrin - digital identities in a blockchain era. Sovrin foundation. https://sovrin.org/wp-content/uploads/AnonCred-RWC.pdf

[3] Mühle, A., Grüner, A., Gayvoronskaya T. and Meinel, C. A Survey on essential components of a self-sovereign identity. Computer Science Review 30 (2018) 80-86.

[4] Verifiable Claims Working Group https://www.w3.org/2017/vc/WG/

[5] The Known Traveller - Unlocking the potential of digital identity for secure and seamless travel http://www3.weforum.org/docs/WEF_KTDI_Specifications_Guidance_2020.pdf

[6] Loïc Lesavre, Priam Varin, Peter Mell, Michael Davidson, James Shook. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. White paper. 2020.

[7] Self-sovereign Identity – A position paper on blockchain enabled identity and the road ahead, Working Group of the German Blockchain Association. 2018. https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity-_-Blockchain-Bundesverband-2018.pdf

[8] Othman, Asem and Callahan, John.The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity, https://arxiv.org/pdf/1711.07127.pdf (accessed 29.4.2020)

[9] The impact of quantum technologies on the EU's future policies. European commission, jrc science for policy report. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC107386/jrc_report_quantum communications.pdf

LIST OF FIGURES

Figure 1: ENROLLMENT BY MEANS OF DIGITAL IDENTITY SYSTEM 17

Figure 2: ENROLLMENT BY MEANS OF DIGITAL IDENTITY SYSTEM, TICKET STORED TO SMART CONTRACT 18