decode

Progress report on standardisation activities and technical sustainability plans

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 732546

Project no. 732546

DECODE

DEcentralised Citizens Owned Data Ecosystem

D6.3 Progress report on standardisation activities and technical sustainability plans

Version Number: V1.0

Lead beneficiary: Waag

Due Date: 30/06/2019

Author(s): Stefano Bocconi (Waag)

Editors and reviewers: Samuel Mulube (TH), Yiannis Psaras (UCL), Jim Barrit (TW), Francesca Bria, Andrea D'Intino (DYNE.ORG)

Dissemination level:		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Approved by: Francesca Bria (Chief Technology and Digital Innovation Officer, Barcelona City Hall)
Date: 30/06/2019

This report is currently awaiting approval from the EC and cannot be not considered to be a final version.

Table of Contents

Abbreviations

ABC	Attribute Based Credentials
BLE	Bluetooth Low Energy
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
IoT	Internet of Things
IRMA	I Reveal My Attributes (App for ABC by RU)
ISO	International Organisation for Standardisation
ITU	UN specialized agency for information and communication technologies
PET	Privacy Enhancing Technologies
NFC	Near Field Communication
W3C	The World Wide Web Consortium

1 Introduction

This deliverable describes the activities carried out in the scope of task T6.4 "Open Standardization". The task's motivation is to "*make sure that the project's technical achievements become embedded in the activities of relevant standardisation bodies in the international community, and have a high probability of being relevant and used after the project itself has finished*".

T6.4 "*aims to **identify the potential standardisation opportunity** related to the DECODE technical results and to **promote the contribution** in the different standardisation groups and alliances*".

As also suggested in the work plan described in the DoA, the activities have been directed at:

- identifying all relevant standards, initiatives and interest groups in this emergent field of blockchains and decentralized and privacy-enhancing technologies for identity and data management
- determining what possible contribution, the particular standardisation effort could provide to DECODE, and/or conversely what possible contribution DECODE could provide to the particular standardisation effort
- engaging when relevant, with the international community and standard organisations.

These activities have led to a comprehensive list of potentially relevant standards and initiatives for DECODE. Based on this overview, Waag and consortium partners have taken part in a number of standardisation efforts, which has also resulted in dissemination of the project internationally, and in the sharing of insights coming from DECODE pilots that could be beneficial to emerging standardization efforts, leading to good impact. Following up on these experiences, we formulate some recommendations for future interactions between DECODE and the selected standardisation efforts/initiatives.

All of the above is documented in this deliverable, which is structured as follows: firstly we detail the approach we followed. We then describe standardisation organisations and their activities that are relevant to DECODE. Following our chosen approach, we look at what contribution DECODE could provide to standards, and what contributions standards could provide to DECODE. Based on this analysis, we formulate recommendations for further standardisation actions.

2 Approach

In this chapter we discuss in more detail the chosen approach for Task 6.4.

The first necessary step was to collect and examine a list of relevant standardisation efforts. In doing so we did not only look at ongoing activities, but also to recently completed ones, since those could also have a positive role for DECODE, as explained in the following.

In fact, two possible benefits are envisioned from engaging with standards: the first is to **influence the development of a standard** in the direction DECODE is going, thereby disseminating the project and greatly increasing the reach of its tools, which can be part of an ecosystem stimulated by the presence of a standard.

The second one is to have (some of) DECODE's tools **implement a standard**, with the same above-mentioned effect of greatly increasing their reach into the ecosystem around the standard. For this latter reason it was important also to have a look at completed standards, where DECODE could not have an influence anymore, but the possible benefits were still achievable.

Even when participating in an ongoing standardisation effort, both of the above-mentioned approaches need to be followed, as a standard is the result of trade-offs between the interested parties, and no single party can dictate all the conditions.

Since this task has taken place while the project was still developing its components, the activities have been mostly directed at two levels:

- Insert DECODE's "spirit" in the agenda of some standardisation efforts, by including DECODE principles and use cases in their output
- Look more closely at some mature DECODE components, namely Zenroom, Coconut and IRMA, for specific and implementable standards.

In the following chapter we present the standardisation bodies we selected and their relevant activities.

3 Standardisation Bodies

In this chapter we describe the standardisation bodies we considered and their working groups, focusing on the ones we have participated in, and describing how DECODE has been disseminated or put on the agenda of those working groups.

3.1 International bodies

The main international standardisation bodies are the three global sister organizations ISO, ITU, IEC. These organisation develop International Standards for the world and their members are mainly national standardisation bodies. Next to them, the W3C has a specific focus on Web standards.

3.1.1 ISO

The International Organisation for Standardisation (ISO)[1] is, as the name says, an international, independent, non-governmental organisation that defines standards in several domains. Membership is restricted and its members (currently 164) are representative of national standardisation organisations (e.g. for the Netherlands this is the Netherlands Standardization Institute (NEN)[2]).

Inside ISO, standards are developed by Technical Committees (TCs), which are composed of[3]:

- Study Groups (SGs) investigate the need and feasibility of additional standardization and/or guidance in a technical area.
- Working Groups (WGs) are established to expedite development of one or more approved work items, and will exist as long as they have responsibility for approved work items.

3.1.1.1 TC 307

The most relevant ISO activity for DECODE is TC 307 - Blockchain and distributed ledger technologies[4], created in 2016 and whose scope is “Standardisation of blockchain technologies and distributed ledger technologies.”

[1] https://www.iso.org

[2] https://www.nen.nl/progressive.htm

[3] From the explanation provided in https://en.wikipedia.org/wiki/ISO/IEC_JTC_1

[4] https://www.iso.org/committee/6266604.html

TC 307 has several relevant subgroups such as "*Use cases*", "*Interoperability of blockchain and distributed ledger technology systems*" and "*Smart contracts and their applications*".

The TC is currently developing 11 standards:

1. Terminology
2. Privacy and personally identifiable information protection considerations
3. Security risks, threats and vulnerabilities
4. Overview of identity management using blockchain and distributed ledger technologies
5. Reference architecture
6. Taxonomy and Ontology
7. Legally binding smart contracts
8. Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
9. Security management of digital asset custodians
10. Discovery issues related to interoperability
11. Guidelines for governance

Many of the items on this list are very relevant to DECODE, and being part of the discussion would be very relevant for the project. This is hindered by the fact that membership is not open and mostly reserved to official national standard bodies, making access to the discussion table not straightforward. Nonetheless there are efforts in DECODE to join this TC, as described in chapter 4 DECODE for Standards.

3.1.2 ITU-T

ITU[5] is the United Nations specialized agency for information and communication technologies, and has currently membership of 193 countries and over 800 private-sector entities and academic institutions.

ITU has a Telecommunication Standardization Sector (ITU-T), which is organised in experts Study Groups (SGs) that develop international standards, known as ITU-T Recommendations, and Focus Groups (FGs) that are more flexible and short-lived than Study Groups. SGs can be joined with an endorsement from one's own member state (country) or if one's own company is a member of ITU-T, while FGs are open to everybody.

3.1.2.1 SG17: Security

A relevant issue for DECODE is discussed in the scope of SG17: Security[6] with Question

[5] https://www.itu.int/

[6] https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

Q10/17 "**Identity management architecture and mechanisms**"[7], which focuses on Identity management (IdM), i.e. "*the management of the life cycle and use (creation, maintenance, utilization, provisioning, and revocation) of credentials, identifiers, attributes, authentication, attestation, and patterns by which entities (e.g., service providers, end-user, social networks, organizations, network devices, applications and services) are known with some level of trust. (...) IdM discusses trusted information exchange between authorized entities that is based on validation and assertion of identities across distributed systems. IdM enables the protection of information and ensures that only authorized information is disseminated. IdM is a key component to the proper operations of telecommunication/ICT networks, (e.g., Internet of Things (IoT), cloud and mobile computing, services, and products) because it supports establishing and maintaining trusted communications*".
This Question is dedicated to the vision setting and the coordination and organization of the entire range of Identity management activities within ITU-T.

Distributed Ledger Technology is also discussed in the scope of the Security SG with Question 14/17 "**Security aspects for Distributed Ledger Technologies**"[8]. The issue focuses on the "*need for identifying the roles and responsibilities of telecom users, operators and service providers with regard to security aspects in the DLT environment*".

In the scope of the standardisation effort, we presented the DECODE project to the co-rapporteur of Q14/17 and asked whether it was possible to join the above mentioned Study Group in some form, but that was only possible for ITU-T members.

3.1.2.2 Application of Distributed Ledger Technology FG

What was possible was to join the Focus Group on DLT, **Application of Distributed Ledger Technology**[9]. This FG focuses on identifying and analysing DLT-based applications and services. Its goal is to draw up best practices and guidance which support the implementation of those applications and services on a global scale, with particular attention to reaching the 17 Sustainable Development Goals[10]. Another planned outcome of the FG is to propose a way forward for related standardization work in ITU-T Study Groups.

Considering the preliminary stage of the discussion in this FG with respect to standardisation and the need to concentrate resources on promising efforts, this option was not explored further.

[7] https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/q10.aspx
[8] https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/q14.aspx
[9] https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
[10] https://sustainabledevelopment.un.org/?menu=1300

3.1.3 IEC

The International Electrotechnical Commission (IEC)[11] is the world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies. The IEC's members are National Committees, and they appoint experts and delegates coming from industry, government bodies, associations and academia to participate in the technical and conformity assessment work of the IEC.

IEC also cooperates with ISO or ITU to ensure that International Standards fit together and complement each other. Joint committees ensure that International Standards combine all relevant knowledge of experts working in related areas.

3.1.3.1 Internet of Things and related technologies

IEC does not focus on ICT but more on hardware related technologies. Potentially relevant to DECODE is IEC's activity regarding IoT, for example in the ISO/IEC JTC 1/SC 41 "**Internet of things and related technologies**", a Joint Technical Committee with ISO, there is a Study Group on Integration of IoT and Blockchain (AHG 18[12]).

Again, due to the closed nature of the participation to these kind of groups, we have decided to focus on trying to participate in the most relevant of them, i.e. ISO TC 307, while at the same time participating in more accessible standardisation efforts, as described in the following.

3.1.4 W3C

The World Wide Web Consortium (W3C)[13] is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C's mission is, in their words, to lead the Web to its full potential.

Membership in W3C is open to all types of organizations (including commercial, educational and governmental entities) and individuals. Standardisation efforts are carried out within:

1. Working Groups (WGs), whose participation is only open to W3C members, and which can produce standards (recommendations in W3C parlance)
2. Community Groups (CGs), open to everybody, which cannot produce standards but can do preparatory work to start a WG and therefore a standardisation effort.

W3C has several activities that are relevant for DECODE:

[11] https://www.iec.ch/

[12] https://www.iec.ch/dyn/www/f?p=103:14:1746970232059::::FSP_ORG_ID,FSP_LANG_ID:22368,25

[13] https://www.w3.org/

3.1.4.1 Web Authentication WG[14]

The Web Authentication WG (end date: 15/09/2019) aims to define a client-side (i.e. in the browsers) API providing strong authentication functionality to Web Applications, obviating the limitations of password-based logins (weak security, vulnerable to phishing attacks, not usable).

This group has recently (4/03/2019) released a Recommendation entitled "Web Authentication: An API for accessing Public Key Credentials - Level 1"[15], which is also referred to as **WebAuthn** API. WebAuthn is one of the building blocks of the **FIDO Alliance**[16] specification (currently FIDO2), an industry-driven effort to reduce the world's reliance on passwords.

The authentication flow enabled by FIDO2 bears a lot of resemblance with the Attribute Based Credential in the DECODE Gebiedonline scenario, and it is therefore presented here in more detail (from the above-mentioned Recommendation).

Relying Parties (such as websites requiring to login) employ the Web Authentication API during two phases. The first is Registration, where a public key credential is created on an authenticator (explained in the following), and scoped to a Relying Party with the present user's account (the account might already exist or might be created at this time). The second is Authentication, where the Relying Party is presented with an Authentication Assertion proving the presence and consent of the user who registered the public key credentials.

Authenticators protect public key credentials, and interact with user agents (e.g. browsers) to implement the Web Authentication API. Authenticators can be implemented on the user device (e.g. fingerprint readers) or on an external device such as a mobile or a USB token key. External authenticators support passwordless, second-factor or multi-factor authentication requests from FIDO2-enabled browsers and operating systems, by using a standard called Client-to-Authenticator Protocol (CTAP[17] currently version 2) over USB, NFC, or BLE.

In order to support FIDO2, Relying Parties need to run a FIDO2-compliant server capable of performing the WebAuthn Relying Party Operations as described in the above-mentioned Recommendation.

[14] https://www.w3.org/Webauthn/

[15] https://www.w3.org/TR/2019/REC-webauthn-1-20190304/

[16] https://fidoalliance.org/

[17] https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html

The Gebiedonline login based on the IRMA[18] app follows a very similar workflow, where the Relying Party Gebiedonline has an IRMA compliant server that generates the session with the request information, which the authenticator (the IRMA app) can retrieve and present to the user for authorisation to disclose the requested information.

It is therefore a possibility that the WebAuthn API could be extended to include Attribute disclosure (and not only authentication), and that IRMA or Zenroom/Coconut could fit the workflow as authenticator implementing the FIDO2 protocol.

3.1.4.2 Decentralized Identifiers WG[19]

The recently started Decentralized Identifiers WG (DID, end date: 15/04/2021) has been proposed to enable identifiers that (from their charter):

1. are controlled by individuals, organizations, and machines, not leased from an authority (e.g. DNS Registrars).
2. are cryptographically verifiable and can authenticate their owners (e.g. DID-based website login).
3. are dereferenceable. i.e. they can be dereferenced to a document that provides information on how to start a secure and privacy preserving communication with the owner (e.g. a set of public keys and a set of service endpoints).

The WG claims that these innovations with respect to traditional IDs are made possible by the advent of Blockchains and Distributed Ledger Technologies.

Practically, DIDs are registered in a blockchain or other decentralized network, and are URNs of the form[20]:

<namespace>:*<DID method>*:*<DID method specific string>*

The DID method specify how to create, resolve and manage the DID documents (mentioned in the third bullet point), whose purpose is "*to describe the public keys, authentication protocols, and service endpoints necessary to bootstrap cryptographically-verifiable interactions with the identified entity*".

DID methods provide Create, Read, Update and Delete operations for DIDs on a particular distributed architecture. DID methods are currently provided using e.g. Sovrin[21], Ethereum (uPort[22]) and IPFS[23] (for an example of method specification see e.g.

[18] https://privacybydesign.foundation/irma/

[19] https://w3c-ccg.github.io/did-wg-charter/

[20] https://w3c-ccg.github.io/did-primer/

[21] https://sovrin.org/

how uPort defines its methods[24]).

The WG will focus on the following points:

1. Define the DID URI scheme.
2. Recommend a data model and syntax(es) for the expression of Decentralized Identifier Documents, including one or more core vocabularies.

Thus, the focus is on syntax more than on tools or protocols. Nethertheless, it can be interesting for DECODE to see whether Zenroom/Coconut could play a role in supporting the implementation of DIDs. This DECODE component supports several cryptographic functionalities already, and it could be worth investigating what would be required to support the form and dereferencability of DIDs. At the same time, Zenroom's developers could possibly become part of the discussion on DIDs as for example invited experts.

The role of Zenroom/Coconut could be even more significant considering that DIDs are only the base layer of decentralized identity infrastructure. The next higher layer is verifiable credentials, that are already supported by Zenroom/Coconut and IRMA. Verifiable credentials are developed in the scope of the following WG.

3.1.4.3 Verifiable Claims WG[25]

The Verifiable Claims WG (end date: 30/09/2019) aims at creating a standard that makes it easy for users to assert their verifiable qualifications to a service provider (e.g. my loyalty card number is X, I have an account at Bank Y, I am over the age of 21, I am a citizen of the USA, I have a degree in Mathematics, etc.). Such standard would allow expressing, exchanging, and verifying claims on the Web more easily and securely, across different industry sectors, and independently from a particular claim provider.

The vision of this WG bears many analogies with the Attribute Based Credentials mechanism in DECODE and the tools based on it (IRMA, Zenroom/Coconut).

The focus on the WG though is very specific[26]: "*The Working Group will:*

1. *Recommend a data model and syntax(es) for the expression of verifiable claims, including one or more core vocabularies.*
2. *Create a note specifying one or more of*
    a. *how these data models should be used with existing attribute exchange*

[22] https://www.uport.me/
[23] https://ipfs.io/
[24] https://github.com/uport-project/ethr-did-resolver/blob/develop/doc/did-method-spec.md
[25] https://www.w3.org/2017/vc/WG/
[26] https://www.w3.org/2017/vc/WG/charter.html

protocols;

b. *a suggestion that existing protocols be modified;*

c. *a suggestion that a new protocol is required.*

3. *Focus their efforts on the identified use cases with a particular focus on the education sector.*"

The main point of the WG is therefore the data model[27] and syntax(es) for the expression of verifiable claims, with a particular focus on the education sector.

Explicitly out of scope are implementing protocols, a reference architecture or APIs, which means that at this stage the WG will be less interested in concrete tools such as the ones produced in DECODE. Considering though that the above mentioned topics will likely be developed in future working groups, there is an interest to follow the work of this group and its "offspring" in the future.
At the same time, it is also worth considering whether the data model developed in this WG an be useful to DECODE.

3.1.4.4 Data Privacy Vocabularies and Controls CG[28]

The mission of the W3C Data Privacy Vocabularies and Controls CG (DPVCG) is to develop a taxonomy of privacy terms, which include in particular terms from the new European General Data Protection Regulation (GDPR). The aim is to provide a machine-readable vocabulary to annotate and categorize instances of legally compliant personal data processing according to the GDPR.

The taxonomy currently discussed in the group contains terms (classes and properties) related to the following concepts (corresponding to GDPR concepts):

- Personal Data Categories
- Purposes
- Processing Categories
- Technical and Organisational Measures
- Legal Basis
- Consent
- Recipients, Data Controllers, Data Subjects

We joined this CG and contributed to the discussion, in particular providing three of the group's use cases[29] (taken from the DECODE project). The use cases were meant to help gather requirements and relevant existing vocabularies for the proposed vocabulary.

[27] https://github.com/w3c/vc-data-model

[28] https://www.w3.org/community/dpvcg/

[29] https://www.w3.org/community/dpvcg/wiki/Use-Cases,_Requirements,_Vocabularies

The vocabulary that is being developed will form a proposal as this group cannot produce a standard. This vocabulary can allow privacy policies to be described in a machine-readable way, thereby creating the conditions for automatic agents to support the user in privacy decisions and general privacy awareness. On the other hand it is rather complex to implement, and the effort should be weighed against the expected benefits.

3.2 European bodies

In Europe there are three bodies officially recognized by the EU as a European Standards Organization:

- the European Committee for Standardization (CEN)
- the European Committee for Electrotechnical Standardization (CENELEC)
- the European Telecommunications Standards Institute (ETSI)

ETSI[30] focuses on telecommunications, broadcasting and other electronic communications networks and services, with international (not only EU) members from private companies, research entities, academia, government and public organizations.

ETSI current standardisation efforts seem to be less relevant for DECODE, therefore we describe only the other two bodies.

3.2.1 CEN/CENELEC

CEN and CENELEC collaborate very closely under a common governance, and their members are mainly the National Standardization Bodies of 34 European countries.

3.2.1.1 Blockchain and Distributed Ledger Technologies (DLT) Focus Group

CEN/CENELEC jointly created in 2017 a Focus Group on "*Blockchain and Distributed Ledger Technologies (DLT)*"[31].

The primary objective of the Focus Group is to identify specific European needs and requirements for the implementation of Blockchain and DLT in Europe, and to map these needs against the work items of ISO/TC 307 "*Blockchain and distributed ledger technologies*" (discussed previously in this document), such as the reference architecture, security and privacy, identity, governance, and smart contracts.

The Focus Group advises the European Commission on European technical requirements relating to Blockchain and DLT, but it does not develop standards. Standardisation is left to international efforts, which are more appropriate in this case (via ISO/TC 307). With that respect, the Focus Group also encourages a broader European participation in ISO/TC 307 and other international bodies.

[30] https://www.etsi.org

[31] https://www.cencenelec.eu/standards/Sectors/ICT/BlockchainLedgerTechnologies/Pages/

Membership of the Focus Group is limited to candidates that are nominated by one of CEN or CENELEC members. However, the Focus Group had a specific subgroup which dealt with drafting a white paper entitled "*Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies*", with an open participation. It was therefore possible to join the subgroup on behalf of DECODE and contribute to the white paper.

The effort was initiated by the European Commission, which contacted CEN and CENELEC to consider the possibility to draft a white paper with recommendations on European Blockchain standardization, which would highlight some European specificities, regarding legislative and policy context, or specific use cases.

This White Paper[32] (approved by the CEN and CENELEC Technical Boards in October 2018) provides 26 recommendations, addresses topics such as sustainable development, digital identity, privacy and data protection, and highlights specific European use cases. The paper emphasises the need to improve the current multi-stakeholder governance processes for the development of standards, and to foster interoperability with wider engagement to avoid vendor lock-ins.

DECODE's use cases are specifically mentioned in chapter "*4.3 Business cases coming from research projects*", which aims to collect the output of national and European level research projects on Blockchain and DLTs, because such outputs may be of high value for standardization bodies.

Another relevant chapter for DECODE is 4.5 "Digital Identity and Signature Management", as it discusses the relation of identity management systems based on distributed ID such as the already mentioned DIDs (see Decentralized Identifiers WG), and the EU regulation eIDAS[33] (electronic IDentification, Authentication and trust Services).

The commitment of DECODE in generating output for public good has also been reflected in Recommendation R4-4: "*EU research projects relevant for standardization should be encouraged to release their results in an open way (open-source license or in any case patent free) to facilitate adoption and uptake into standardization*".

Beyond the above-mentioned contributions, participation to this White Paper has led to disseminate the projects among the contributors of the paper. This in turn has led to further contacts in the scope of ISO TC 307, as described in the following.

[32] ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/ICT/Blockchain%20+%20DLT/FG-BDLT-White%20paper-Version1.2.pdf

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

3.3 Other organisations

3.3.1 IEEE-SA

IEEE is "*the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity*"[34]. The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA)[35] is an organization within IEEE that develops global standards in a broad range of industries.

IEEE-SA is currently running a project about a "*Standard for the Framework of Blockchain Use in Internet of Things (IoT)*"[36] (P2418.1). Its scope is to provide "*a common framework for blockchain usage, implementation, and interaction in Internet of Things (IoT) applications. The framework addresses scalability, security and privacy challenges with regard to blockchain in IoT. Blockchain tokens, smart contracts, transaction, asset, credentialed network, permissioned IoT blockchain, and permission-less IoT blockchain are included in the framework*".

Although the work seems relevant to some of DECODE's activities, participation requires a subscription and an attempted informal contact with the group's chair has not been followed up. IEEE also runs a Slack channel about Blockchain but it has currently a very low traffic. IEEE's focus is mostly in business cases such as supply chains and pharmaceutical applications. For all these reasons no further contact has been attempted.

3.3.2 IETF

The Internet Engineering Task Force (IETF) is "*the premier Internet standards body, developing open standards through open processes. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The technical work of the IETF is done in Working Groups, which are organized by topic into several Areas*"[37].

IETF has a research part for longer term research issues which is called the Internet Research Task Force (IRTF). IRTF "*promotes research of importance to the evolution of the Internet by creating focused, long-term Research Groups working on topics related to Internet protocols, applications, architecture and technology*".

[34] https://www.ieee.org/about/vision-mission.html
[35] https://standards.ieee.org/
[36] https://standards.ieee.org/project/2418_1.html
[37] https://ietf.org/about/

The IRTF has started a Decentralized Internet Infrastructure Research Group (DINRG) to "*investigate open research issues in decentralizing infrastructure services such as trust management, identity management, name resolution, resource/asset ownership management, and resource discovery. The focus of DINRG is on infrastructure services that can benefit from decentralization or that are difficult to realize in local, potentially connectivity-constrained networks*"[38].

This research group focuses on the problem of decentralized infrastructure, since they think it is receiving less attention with respect to the intensive research and development taking place around decentralized applications.

3.3.3 EU Blockchain Observatory and Forum[39]

The European Union Blockchain Observatory and Forum "*aims to accelerate blockchain innovation and the development of the blockchain ecosystem within the EU*". Their mission is to "*promote blockchain in Europe by mapping existing blockchain initiatives, analysing and reporting on important blockchain themes, promoting blockchain education and knowledge sharing and holding events to promote debate and discussion*".

In the scope of the mapping of blockchain activities, we have submitted DECODE to their initiative map[40].

The Observatory runs an online forum[41] open to participation, with the following groups:

1. Blockchain innovation in Europe
2. Community
3. Energy and environment sectors
4. GDPR, data policy and compliance
5. Government services and digital identity
6. Healthcare sector
7. Policy and regulatory framework priorities
8. Scalability, interoperability and sustainability
9. Supply chain and traceability
10. Tokens and ICOs

Currently we are members of 1, 2, 4, 5, 7, and 8, in particular following the discussions about the GDPR.

[38] https://datatracker.ietf.org/rg/dinrg/about/
[39] https://www.eublockchainforum.eu/
[40] https://www.eublockchainforum.eu/initiative-map
[41] https://eublockchain.mobilize.io/network-groups

The Observatory also compiles thematic reports that are available online[42].

3.4 Projects

Among the possibly many relevant projects, we selected the following one since it regards smart contracts, a subject that is relevant to DECODE and not yet present in the previously described standardisation efforts.

3.4.1 Accord project

The Accord Project[43] is an open source, non-profit, initiative working to transform contract management and contract automation by digitizing contracts. They aim to provide a formal language, a data model and an engine to support the creation and the execution of legally enforceable smart contracts.

The main output of the project are 3 components:

- a format for legal contract and clause templates (Cicero)
- a data modeling language (Concerto)
- a domain specific language to express the executable logic of legal templates (Ergo)

Their tools are open-source and are available on Github[44]. Although DECODE has already defined a DSL for smart contracts, it could be worth investigating support for Accord contracts, also considering that the project has relevant partners such as Hyperledger[45] and Sovrin[46].

[42] https://www.eublockchainforum.eu/reports
[43] http://www.accordproject.org/
[44] https://github.com/accordproject
[45] https://www.hyperledger.org/
[46] https://sovrin.org/

4 DECODE for Standards

In this chapter we discuss how DECODE can take part and influence current and future standards developments, building on the overview and the undertaken actions described in the previous chapter.

ISO TC 307

An important opportunity for the project is to participate in **ISO TC 307** (see 3.1.1.1 TC 307), in general and specifically based on the experiences coming from using Zenroom/Coconut and IRMA. A participant to the CEN/CENELEC white paper suggested that, given the importance of the project's goal to give people ownership of their personal data, DECODE could for example join TC 307 Study Group 2 on use cases.

Other relevant groups where Zenroom could be introduced are the WG 2 "*Security, privacy and identity*" Working group and the WG 3 "*Smart contracts and their applications*" Working group.

This participation would need to go though NEN, the Dutch ISO national member, given the fact that Waag and more importantly Zenroom developer Dyne are based in the Netherlands.

Dutch Blockchain Coalition

Via the same link we came in contact with a member of the **Dutch Blockchain Coalition**[47], a joint venture between industry, government and knowledge institutions in the Netherlands.

Among their topics of interest there is Self-Sovereign Identity (SSI)[48], which they consider a necessary element to resolve several important issues on Blockchain. They are already aware of IRMA, but they are looking for more decentralised solutions.

Considering that this coalition is permanently open for experts and stakeholders who want to make a contribution, Zenroom/Coconut could be introduced there to foster a wider reach of the tool.

WebAuthn

The Web Authentication API (see 3.1.4.1 Web Authentication WG) is a well-supported standard for password-less authentication. Besides implementing it (discussed in the next chapter), it is possible that a similar functionality will be developed in the context of Attribute disclosure (see also Verifiable claims in the following).

[47] https://dutchblockchaincoalition.org/

[48] https://dutchblockchaincoalition.org/usecases/self-sovereign-identity-ssi

It is therefore a possibility that the WebAuthn API could be extended to include Attribute disclosure (and not only authentication), and that IRMA and/or Zenroom/Coconut could have a role in the workflow as authenticators implementing the FIDO2 protocol. Even though this is a logic development for this standard, it is difficult to assess how feasible it is.

Decentralised Identifiers

Even though at this stage W3C Decentralised Identifiers (**DID**s, see 3.1.4.2 Decentralized Identifiers WG) standardisation is focused on the data model and syntax, W3C always welcomes implementations (which are also required for a proposal to get the official status of a recommendation), and it seems to be already quite an ecosystem of technologies that aim to support DIDs, as shown in the list of DID method specifications currently in development[49]. It would be worth for Zenroom/Coconut and IRMA to consider implementing the standard (as discussed in the next chapter) and/or become part of the discussion on DIDs as invited experts.

Verifiable Claims

The same holds for a very related standardisation effort also from W3C, **Verifiable Claims** (see 3.1.4.3 Verifiable Claims WG), which is even more similar to DECODE's use cases. Even though the discussion is currently more on data models, there is and will be the need of tools that implement the draft before it can ever become a recommendation. So either at this stage or in the future (in subsequent WGs that will further develop the standard) we see a role for Zenroom/Coconut and IRMA, again possibly as invited experts in the Working Group.

Blockchain and Distributed Ledger Technologies

The Blockchain and Distributed Ledger Technologies (DLT) Focus Group (see 3.2.1.1 Blockchain and Distributed Ledger Technologies (DLT) Focus Group) has produced a white paper with recommendations for the EU commission regarding Blockchain and DLT standardisation.

Since the Focus Group plans to continue to release further editions of the White Paper, it might be relevant for DECODE to participate in these editions, for example by contributing the lessons learnt in the use cases. This can be done by joining the Focus Group's sub-group in charge of the White Paper (see the group's page for how to join the sub-group[50]).

[49] https://w3c-ccg.github.io/did-method-registry/#the-registry

[50] https://www.cencenelec.eu/standards/Sectors/ICT/BlockchainLedgerTechnologies/Pages/default.aspx

EU Blockchain Observatory and Forum

The EU Blockchain Observatory and Forum (see 3.3.2 EU Blockchain Observatory and Forum) can be used for dissemination of project results.

5 Standards for DECODE

In this chapter, analogously to what has been done in the previous one, we discuss how DECODE can profit by closely watching and possibly implementing existing and under-development standards.

Some standards have already been mentioned in the previous chapter, since taking part in a standard implies shaping the direction of the development but also adapting to it, as mentioned in chapter 2 Approach.

ISO TC 307

Participating in **ISO TC 307** (see 3.1.1.1 TC 307) might require following and implementing its results. Since the TC is currently developing 11 standards, this is a decision that should be examined per standard. Participating in the discussion will hopefully inform sufficiently these decisions.

WebAuthn

W3C **WebAuthn** API (see 3.1.4.1 Web Authentication WG) are already implemented in most major browsers, and it could be worth investigating the possibility and cost to implement them in Zenroom. This would open a vast ecosystem of use cases that would greatly increase the adoption of the tool. Especially considering the possibility that WebAuthn API could be extended to include Attribute disclosure (and not only authentication), as discussed in the previous chapter.

Decentralised Identifiers

A possible contribution from DECODE's Zenroom to the **DID**s WG (see 3.1.4.2 Decentralized Identifiers WG) has already been discussed in the previous chapter.

There is enough interest in this standard by looking at the DID method specifications currently in development, with uPort as one of the parties involved, and technologies such as Ethereum, IPFS and Sovrin. Given Zenroom (and possibly IRMA) support already several cryptographic functionality, it could be worth investigating what would be required to implement the DID standard. The first step could be to support the dereferencability of DIDs and the syntax for DID documents.

Verifiable Claims

In the same line, but even more fruitful can be to implement the standard produced by the **Verifiable Claims** WG (see 3.1.4.3 Verifiable Claims WG), currently focussed on a data model for the expression of verifiable claims. DECODE can bring to the table quite some experience in this domain, and implementing the data model might be advantageous to support more use cases and also to join a wider ecosystem for Zenroom and possibly IRMA. Regardless of this, joining this group as invited experts would be very useful, as discussed in the previous chapter.

DPVCG

The Data Privacy Vocabularies and Controls CG (see 3.1.4.4 Data Privacy Vocabularies and Controls CG) is developing a proposal for a semantically well-defined vocabulary to express privacy concepts, mostly based on the GDPR[51].

Having followed and participated in the effort, we can say that the vocabulary is well integrated with other existing vocabularies and it has a good legal basis due to the contribution of lawyers in the group. On the other hand, it is also quite complex for light-weight applications, being a faithful translation of many concepts contained in the GDPR.

Therefore, adoption should be considered but possibly only for some use cases. Another strategy could be to wait for the proposal to reach the recommendation status (official standard), and/or a wider adoption in tools, advantages which would make implementation more worthwhile.

Accord

The Accord project (see 3.4.1 Accord project) has tools to allow the definition of natural language contract and clause templates that can be executed by a computer.

Although DECODE/Zenroom has already defined a human-readable DSL for smart contracts, it could be worth investigating whether this functionality could be "delegated" in the future to the tools produced by Accord. Possible advantages are richer expressivity of the contracts, with the risk to increase the computational load required to process the contracts.

In any case the project looks promising due to the involvement of a large consortium, with interesting partners such as Hyperledger[52] and Sovrin[53].

[51] https://gdpr-info.eu/
[52] https://www.hyperledger.org/
[53] https://sovrin.org/

6 Recommendations

In this chapter we summarize the possibilities discussed in the previous two ones, trying also to give some assessment as what the importance and priority of each action could be.

ISO TC 307

What: There is a chance to participate as a member in the work of ISO TC 307

Disadvantages:

- ISO standardisation processes can be lengthy and time consuming
- ISO standards are not open, contrary to the spirit of DECODE
- The influence of a standard in a rapidly changing technological landscape is hard to predict

Advantages:

- Even in the scope of European standardisation efforts on Blockchain and related issues (CEN/CENELEC), there are continuous references to the work of TC 307. This WG seems to be very central to the standardisation around Blockchain related issues.
- Participation might be limited to some Work Groups or Study Groups, such as the SG on use cases, possibly limiting the effort while still achieving impact.
- Participation leads to get in contact with a vast network of potentially interesting partners.

Advice:

We think that participating in the TC is worth trying, for the possible impact of the project regarding directions for standardisation, as well as for the possible contacts that participation will foster.

Update

Dyne.org has submitted an application to join ISO TC 307 through NEN. Dyne.org's admission in the NEN commission "NC 380307 Blockchain and DLT" and ISO TC 307 "Blockchain and distributed ledger technologies" is underway and is expected to be formalized before the end of the DECODE project.

Dutch Blockchain Coalition

What: we have contacts with members, reaching out to them is possible.

Advice:

Promote Zenroom/Coconut to the group, as from previous contact they seem to be open to solutions and have an interest in advancing the field of Blockchain/DLT for societal benefit.

WebAuthn

What: Extend Zenroom/IRMA to support the role of authenticator in the standard

Advantages:

- Place DECODE components in a large ecosystem supported by all the major browsers, thereby considerably increasing reach.

Disadvantages:

- It does not really use the more innovative results of the project, since WebAuthn is mainly of a replacement for passwords, but it can be the first step to add more functionality.

Advice: If the focus of the standardisation effort is more on the innovative side of the project (e.g. ABC), there are more appropriate groups to interact with. If a strategy based on entering a large ecosystem with basic functionality and once becoming well-known, present added features is deemed useful, this might be an option.

Decentralised Identifiers

What: Participate in the WG and implement the data model.

Disadvantages:

- Closed membership, might be difficult to be invited without becoming a member.

Advantages:

- Very relevant to the project and with considerable impact, being identity one of the foundations for the Web (and not only).
- W3C makes standards that matter (mostly).

Advice: Try to enter the group or at least consider being involved in some way, such as trying to implement their proposal, being listed as one of the supporting tools, giving feedback.

Update

Dyne.org has recently applied for stewardship at the Sovrin foundation. Sovrin has already been mentioned in this deliverable in the context of DIDs, and it is a US based 501 (c)(4) nonprofit organization whose goal is to "creating a global public utility for self-sovereign identity“. Among the stewards are companies such as IBM, Cisco and Deutsche Telekom.

Sovrin’s interests in Dyne.org are Zenroom as well as participation in DECODE, which they seem to be well aware of. Dyne.org’s objective is to increase awareness about DECODE among technology corporation worldwide and more concretely to push Zenroom, Zencode and the UCL’s “Coconut” authentication flow as global standards in the cryptographic authentication space.

The timeframe for admission is 2-4 months.

Verifiable Claims

What: Participate in the WG and implement the data model (analogously and very related to Decentralised Identifiers, even more related to DECODE's core functionality).

Advice: Same considerations as before, with the remark that ABC and Verifiable Claims can largely benefit from each other. Probably these two last efforts should be combined or at least considered for a long-term strategy.

Blockchain and Distributed Ledger Technologies

What: Participate to announced follow-ups to the white paper.

Advantages:

- Contact already established, should be easy to be involved
- Good contact of this groups with other standardisation efforts, most notably ISO TC 307
- The Blockchain and Distributed Ledger Technologies (DLT) Focus Group advises the EU commission on the matter.
- Possibly limited effort

Disadvantages:

- Previous White paper was very high level, unclear the impact of such advice on policy

Advice: If a follow-up of the paper will be announced, participation could be considered which could take place even with a limited effort.

DPVCG

Advice: the privacy vocabulary being produced by the Data Privacy Vocabularies and Controls CG is very semantically rich and therefore not light-weight. Moreover, it is not a standard but the preliminary work possibly leading to one. Assess the need in DECODE for a rich vocabulary and in positive case have a look at it, but only if it serves DECODE's purposes, since it is too early to have an ecosystem of tools around that proposal.

Accord

Advice: Have a look to the tools provided by the project and a quick assessment if they are compatible with DECODE tools (are they usable in DECODE's component architecture?). In case they are, consider those tools as a possible future expansion to the smart contract functionality in DECODE.

EU Blockchain Observatory and Forum

Advice: Use the forum for dissemination of project results.

7 Conclusions

This deliverable describes the activities of Task T6.4 "Open Standardization". In trying to position DECODE in relevant standard bodies, we chose the following complementary approaches:

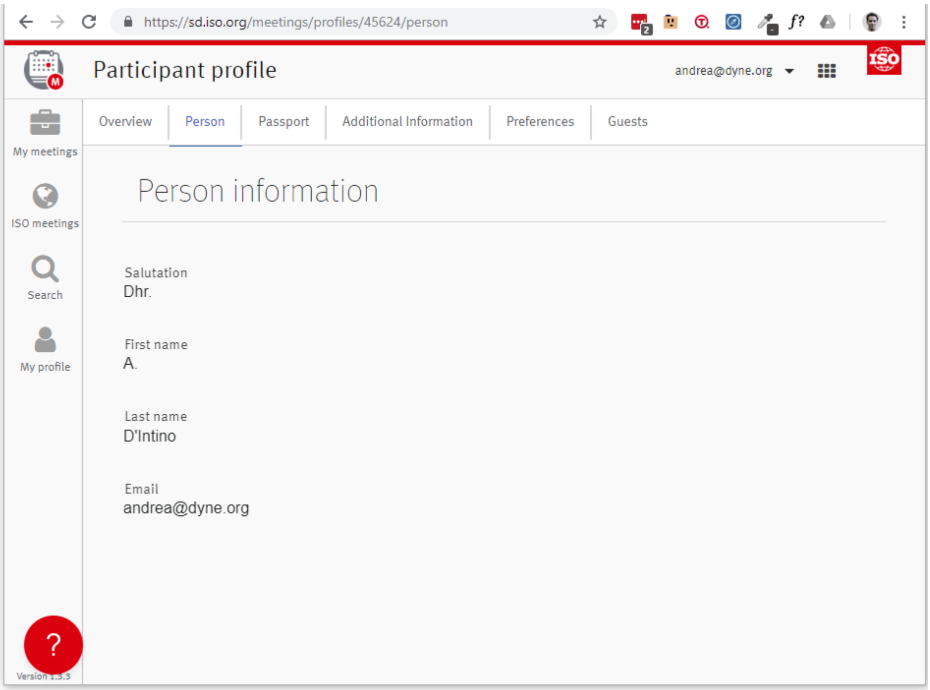
1. When participation was open, promote the project and its principles in relevant standards bodies, for example by having DECODE use cases figure in the list of relevant use cases for particular standardisation efforts.

2. Consider which DECODE functionality/components have standardisation potential and decide what standardisation efforts would be the most appropriate.

3. Determine what standards could be implemented by DECODE components in order to extend the reach of the project by opening other ecosystems.

In order to implement these approaches, we have researched the main standardisation bodies and their ongoing working groups to see whether there were potential matches with the scope and principles of DECODE. This has resulted in an overview of standardisation bodies, the activities that are relevant to DECODE, and the direct engagement of DECODE participants in the relevant standardization working groups. Participation in key standardisation efforts has led to disseminate DECODE and set its use cases on the agenda at European (CEN/CENELEC White paper, EU Blockchain Observatory and Forum) and international level (W3C CG).

Further, through the work of Dyne, the project has applied for membership to ISO TC 307, which is a crucial body for Blockchain standardisation activities. As of June 2019, the membership has been approved (see screenshot below) and Dyne has multiple personnel working in the ISO TC 307, in the WG1, WG2, WG3, WG5, JWG4, and the "use cases" working group.



Person information

Salutation
Dhr.

First name
A.

Last name
D'Intino

Email
andrea@dyne.org

Figure 1: Dyne's profile as a membership of the ISO TC 307

Dyne has also applied for stewardship at the Sovrin foundation, which is related to different standardisation efforts such as DIDs, as described in this document.

Now that some tools are mature enough, there are concrete possibilities to contribute to some standards, most notably W3C's Decentralised Identifiers and Verifiable Claims, as well as consider to implement some standards to extend the reach of DECODE's tools.

This document concludes with recommendations for how to proceed in the standardisation effort, along the lines of the proposed approach.

8 Appendix

8.1 Standardisation Events where DECODE was present

ETSI Security and Trust in ICT event[54], Sophia Antipolis, France, 14-15 June 2018

Poster and participation to Session 4: DLT and standardization

The panel debated about DLT (security/privacy) standardization progress, gaps, overlaps and areas of collaboration.

Program:

- ISO TC 307, Sophie Coutor, French Ministry of Interior and TC 307 participant
- CEN/CLC focus group, Ashok Ganesh
- IEEE, Claire Vishik co-chair IEEE Blockchain WG
- ITU-T SG17 DLT security, Kyeong Hee Oh, TCA Services

Participants contacted before the event (except for ISO) asking whether some form of collaboration with DECODE was possible.

During the event contact with Benoit Abeloos from ISO and Ms Kyeong Hee Oh from ITU-T.

Blockchain and Distributed Ledger Technologies (DLT) Focus Group

Contributions to the White paper, feedback on the document, participation to White paper teleconferences.

W3C Data Privacy Vocabularies and Controls Community Group

Participation to several teleconferences, contribution to use cases, studies on existing vocabularies, feedback on proposal documents.

EU Blockchain Observatory and Forum

Member, Contributed DECODE to the initiative mapping.

Dutch Blockchain Coalition

Meeting at the Dutch Blockchain Coalition office in Delft.

[54] https://www.etsi.org/events/1263-distributed-ledger-technologies

8.2 Other relevant W3C activities

8.2.1 Current

Privacy Interest Group

The Privacy Interest Group (PING) monitors ongoing privacy issues that affect the Web, investigates potential areas for new privacy work, and provides guidelines and advice for addressing privacy in standards development, including privacy considerations in specifications.

8.2.2 Past / Not active

Blockchains and the Web - A W3C Workshop on Distributed Ledgers on the Web - Report

Data Privacy Controls and Vocabularies - A W3C Workshop on Privacy and Linked Data

Blockchain Community Group

The mission of the Blockchain Community Group is to generate message format standards of Blockchain based on ISO20022 and to generate guidelines for usage of storage including torrent, public blockchain, private blockchain, side chain and CDN. This group will study and evaluate new technologies related to blockchain, and use cases such as interbank communications. W3C Blockchain CG Use Cases

This GC was collaborating or planning to collaborate with ISO. Strong work on standardisation related to distributed ledgers and other key components should also happen, since the ambition is to present a reference architecture.

Blockchain Digital Assets Community Group

The group's mission is to discuss and eventually create and propose Web Specifications for creating and using Digital Assets on a Blockchain. The groups primary activities will be to start discussions with regards to use cases of digital assets on blockchains and identify the issues that we have now. Eventually, the group will publish technical thought papers on Digital Assets on Blockchains and eventually produce deliverables like sample codes, use cases, proof of concepts, etc. in order for this community group to become a W3C Working Group to propose technical specifications related to creating and using Digital Assets on Blockchains. The ideal members that should join this group are those who has skills in Web standards and have interests in Blockchain technologies especially in the creation and using of digital assets on Blockchains.

Web Cryptography Working Group

The mission of the Web Cryptography Working Group, part of the Security Activity, was to define a high-level API providing common cryptographic functionality to Web Applications. It resulted in the following Recommendation: "Web Cryptography API", with a new version being drafted here.

Smart Contracts Community Group

Open protocol to define the structure, terminology, and network messages required of smart contracts.