decode

Initial definition of Smart Rules and Taxonomy

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

D3.5 Initial definition of Smart Rules and Taxonomy

Version Number: V1.0

Lead beneficiary: Dyne.org

Due Date: April 2018

Author(s): Denis Roio, Marco Sachy (Dyne.org)

Editors and reviewers: Marco Ciurcina (NEXA), Guy Samuel (TW) , Shehar Bano (UCL)

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: 30/04/2018

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

Initial definition of Smart Rules and Taxonomy

Denis Roio, Marco Sachy Dyne.org

Monday, 30th of April 2018

To facilitate transparency, multiple implementations, wide adoption and standardisation, DECODE develops a smart rule language and execution engine. All read and write operations affecting entitlements and accessing data can be expressed in this language, which we will design to become a robust open standard for authorisation around personal data. Such a language will aim to be data centric and functional, to naturally avoid complex constructions and define sets of transformations that can be then easily represented with visual metaphors. For each pilot, an exemplary set of attributes, entitlements and Smart Rules will be presented the second part of this document. In particular, we firstly present an initial set of data subject attributes and controller entitlements governing access to them common to all pilots. Secondly, we introduce seminal Smart Rules governing the consensual relationships between data subjects and data controllers for each pilot from registration to service engagement to opt out.

Table of Contents

List of tables

1 Introduction

This deliverable principally consists of a working implementation (ALPHA stage) made available in source-code format and binary format compiled for several target architectures, demonstrating the extreme portability of this language interpreter.

This document accompanies the deliverable with a brief overview of characteristics and implementation choices deriving from DECODE's deliverable D3.3 "DECODE language design patterns" which is a living document currently indicated as the Whitepaper for the Zenroom implementation.

Following the publication of this deliverable, both documents will be merged into the Zenroom whitepaper, a living document nurtured by all findings published along this research path.

In fact, a language is needed to define, implement and enforce clear and transparent smart rules for data access, governance and identity management. The following sections of this document are briefly illustrating the design choices made so far in developing a minimal language to express key privacy and integrity logic policies for data items, binding cryptographic primitives and human language into a domain-specific language (DSL).

The result for the pilots will be the identification of personal attributes of data subjects as they are relevant for pilots roll out as emerging from pilot inceptions presented in D1.1. Stakeholders relationships in all pilots among data subjects and data controllers interactions are the object of investigation.

After the description of preliminary pilot requirements in terms of data subject attributes, the entities verifying them and data controller entitlements, we run a comparative analysis among the four pilots to make emerge common attributes and entitlements. The latter will inform Smart Rules cryptographically managing data subjects privacy needs and data controllers access control levels of clearance.

The definition of attribute and entitlements in DECODE are as follows:

- An attribute is in the form: ATTRIBUTE = (SUBJECT PREDICATE OBJECT) Where the SUBJECT is the entity to which the attribute relates (in DECODE terms the account), the PREDICATE describes the relationship between the SUBJECT and the OBJECT and the OBJECT is the value of the attribute. Attributes present also PROVENANCE and SCOPE.

- An Entitlement is an agreement of disclosure controlled by the data owner. A data entitlement concerns the sharing of data. In DECODE, an entitlement is defined in a policy and implemented with the application of cryptography. Entitlements are

composed by description, purpose, condition and, possibly, expiry date (Cf. D1.4 - First DECODE Architecture).

We identify attributes and entitlements for each pilot, showing that the scope of an attribute gives purpose to corresponding entitlement policies. Bridging scope and purpose is the basis for the cryptographic operations apt to authenticate personal attributes by data subjects who sign attributes with the public key of a data controller while allowing entitled entities, i.e. data controllers, to verify them with their private keys.

To leverage minimization, we suggest scenarios whereby 'can-access' access control levels are necessary only at onboarding verification, while in most other cases it is sufficient to show the attribute and the associate cryptographic signature without retrieving the actual data from the data base.

In what follows, as a working definition Smart Rules to exercise entitlements on attributes through Zenroom operations, we propose:

A Smart Rule is a set of cryptographic instructions processing privacy requirements among entitlements and attributes to manage consensual relations and data protection conduct of data subjects/owner and data controllers/consumers in a GDPR compliant environment.. The smart rule concept will allow each participant to define in detail his/her sovereignty on his/her personal data.

As we will present below, Smart Rules are a way to bridge attributes (semantic enunciates) and entitlements (access level claims) declared in natural language with Zenroom cryptographic schemes translating them in functional language and execute them. Hence, a Smart Rule can be thought of as a performative translation of natural declarative language into cryptographic functional language apt to express key DECODE policies as use cases in the developed language.

2 High level and low level

This research is best understood by envisioning the dualistic path taken in the effort of making two extremely loose and far apart ends meet: the technical language of cryptography and the human language of rule expression. There is certainly no shortage of literature on the topic and it is well beyond the scope of this document to debate its values.

What this document delivers is a practical attempt which is still a work in progress at the time of writing, to make the loose ends meet by virtue of a foundational DSL implementation that on one side facilitates the expression of cryptographic schemes and on the other side, still in progress, matches the emerging semantic with the studies made on DECODE pilots and their needs to clearly express credentials and entitlements.

The following implementation has therefore to be seen as the common ground on which we are grafting our understanding of the pilot needs on the cryptographic schemes implemented in DECODE.

2.1 Implementation

The implementation is named "Zenroom" and is available at the following web address https://zenroom.dyne.org and the release of this deliverable coincides with the release of version 0.5 of this software, following the progression that was started by deliverable D3.3 and that lead to this deliverable across the iterations reported in its ChangeLog.

The technical documentation of Zenroom is partially already covered in its online API documentation and should be seen complementary to this document, made available on https://zenroom.dyne.org/api

2.1.1 Features

Zenroom can be primarily defined as a "virtual machine". It is self-contained and can be compiled as a completely static binary, without any dependency and ties to the host operating system.

Zenroom does not require any access to the network nor to the file system, it simply processes data as input to return data as output and in doing so it adopts its own experimental memory management without even relying on the memory allocation calls provided by the OS. Its development will continue in the direction of making this

component as minimal and independent as possible in covering its role, which is that of interpreting language describing a set of rules that operate cryptographic transformations on rather complex data structures.

The namespace of reference for cryptographic primitives in Zenroom, likely to be adopted also in other DECODE component implementations, is the one provided by the Apache Milagro library, which seems to be well successful in establishing itself as an efficient (Budroni and Pintore, 2017) and de-facto standard implementation library with no further dependencies, undergoing adoption for privacy aware services (Rios et al., 2017) and Internet of Things products (Scott and McCusker, 2016).

Zenroom is extremely portable, being written following the C99 standard (Ritchie et al., 1988) whenever possible. As of today we managed to port its binaries to all major desktop platforms (Windows, Apple and GNU/Linux) plus major mobile platforms (Android and iOS) and to Java platforms via JNI. Last not least Zenroom successfully compiles and run as "Javascript code" via LLVM/Emscripten, de-facto placing this software as an active player for the upcoming wave of innovations bound to the adoption of the "WebAssembly" enabling technology in web browsers (Haas et al., 2017).

As indicated already in D3.3 Zenroom adopts the Lua engine (Ierusalimschy et al., 1996) in a slightly modified form of version 5.3 as its direct-syntax parser.

Zenroom facilitates a declarative approach by implementing efficient schema validation, a crucial feature to secure the development of taxonomies to a solid data-centric paradigm (Murata et al., 2005). It also allows writing code in lazy functional programming style based on recursion operators associated with data type definitions on data (Meijer et al., 1991).

At last, it aims at establishing as first-class citizens (Kosar and Livny, 2004) both simple cryptographic primitives and complex concepts as key rings belonging to people and entities.

3 Pilot Specific Taxonomy of attributes and entitlements

This section presents an analysis that is foundation to future development directions for Zenroom to express nouns and predicates emerging from the analysis of entitlements across pilots. The challenge ahead will be that of connecting this taxonomy with well understandable scripts that can cover most of the configurations described.

We proceed presenting an exemplary set of Smart Rules and related attributes for the application of DECODE's language development to pilots. The rationale for the selection of privacy by design strategies for this pilot descends from the need to apply the principles of minimization, separation, abstraction, hide, information, control, enforcement and demonstration as outlined in deliverable D1.2 (Privacy Design Strategies for the DECODE Architecture).

By endorsing an inductive methodology with a heuristic approach to Smart Rules design, the goal is to define a general taxonomy of Smart Rules composed to serve the relationships among attributes and entitlements under the framework of Attribute Based Credentials as defined in deliverable D1.4 (First Version of DECODE Architecture).

As state in the Technical Annex, the flexibility of the DECODE architecture rests on a set of smart rules expressed in a formal language, that allow people to define conditions for the access and use of data, and legal/contractual obligations and other constraints. Through the smart rules, one may provide or revoke authorisation for access to personal data; their association with its identity; or change the legal status and the conditions of use and exploitation of the data (Technical Annex, Part B, p. 10).

In the following, we will therefore identify what in our opinion are the attribute or attributes relevant to define data subject credentials for each pilot. Secondly, we will arrange preliminary entitlements connected to such attributes and to be exercised by data controllers following the consent of data subjects. Finally, we will propose a set of associate Smart Rules emerging from Zenroom operationalization of attributes and entitlements in the interrelation between data subjects and controllers both common and specific to each pilot.

3.1 iDigital Decidim

In this first case, the problem to be solved is to provide safe identification for users while endorse a deontology aligned with GDPR requirements about sharing user personal data to extract valuable information about city concerns that might be later be used

to propose data-driven policies in the city. (Cf. D1.1 - Scenarios and Requirements Definition Report). Accordingly, the solution or service to be provided is a set of rules for data sharing/ data "donation" by participants/owners under the rules issued by the issuer, i.e. the promoters of the Decidim platform. This dynamic can be audited by a relying party, for instance the Municipal Information technology Institute at Barcelona City Council.

The rules, attributes and entitlements summarised below are meant to show in an intelligible form how personal data can be used for the public good, shaping the form of the "data commons". The service is open source and can be adopted by other municipalities or companies who want to study the data for both data-driven public policymaking and private business, within a GDPR compliant environment.

In such an environment the stakeholders are all users of Decidim, research institutions interested in urban matters such as Eurecat and UB, data journalists, data service related industries and developers (Data Beers BCN, BCN Analytics Hub) and app developers and hackers who want to use Metadecidim data and DECODE platform to develop new services. Also citizens who wish to learn / use data analysis techniques and share them (Cf. D1.1 - Scenarios and Requirements Definition Report).

Key enabling factors: - Transparency in data storage and user entitlements: enable users to control where their data is stored, choose what identifying information is shared and the granularity of access levels for that information - Auditable petition signing process: As a provider for enabling citizens to make collaborative decisions, there should be a way to audit and verify transactions in the system in a reliable manner

Hypothesis statement:

As a user I want to sign a petition in a secure, transparent and auditable process, and control the granularity of access to personal information I share with my petition.

Result:

- Minimal app for users to decide data sharing rights and who accessed their data.
- Minimal visualisation of Decidim data and knowledge extraction to show to users that donated their data.

Below a preliminary set of requirements for Decidim as derived from the current Privacy Policy and Terms of Use as published by Barcelona City Council on decidim.barcelona:

- audit storage —> the user can audit the storage of her data within the file "Citizens Participation" located in the Decidim servers on the premises of Barcelona City Hall updated to run a DECODE node.
- data subject credentials for registration —> national ID number, date of birth, post code to be accessed by Decidim according to Attribute Based Credentials

framework. Moreover the data subject must create a password and accept of GDPR compliant privacy policy and terms of use

- granularity of access levels for that information
- Audit transactions, i.e. petition vote
- verify transactions, i.e. petition vote
- submit a proposal
- modify proposal
- inform data subjects of any change in privacy policy
- allow data subjects to amend their personal data sharing policy
- allow data subject to cancel their subscription
- allow registration for an individual only if attribute "age" : decode account; age of subscriber; > 16 years
- allow registration to legal entities such as groups, collectives, city organisations with the following credentials —> name of organisation, responsible person, telephone number of the organisation, email of the organisation, password, acceptance of GDPR compliant privacy policy and terms of use
- act upon illegal use of the platform (copyright, trademark infringements; publishing personal data belonging to other data subjects; sending spam or viruses; setting up pyramid schemes, ponzi schemes; commercial ads; non conformity with public decency; create multiple users to steer voting)
- banning a participant
- wavering Decidim from the responsibility to address disputes among participants.
- participants Intellectual Property Right: all users generate contents will be published under Creative Commons license (CC-BY-SA).
- Only the user name, a pseudonym, is public information accessible to third parties.

From these requirements, we will now isolate what we consider the necessary attributes for participants to disclose.

Relevant attributes for DECIDIM as derived from their website are summarised in the table below:

ATTRIBUTE 1 DECIDIM	Date of birth	Verification: DECIDIM	Scope: age Verification
ATTRIBUTE 2 DECIDIM	National ID number	Verification: DECIDIM	Scope: public Identification
ATTRIBUTE 3 DECIDIM	Post Code	Verification: DECIDIM	Scope: Localization

Table 1 DECIDIM Attributes

Relevant entitlements derived from the privacy and data protection requirements emerging from the scopes of data owners attributes (Barcelona residents) to be exercised by data consumers (Barcelona City Council/DECIDIM) within DECIDIM. Each row is an entitlement policy implemented with cryptography:

ENTITLEMENT DECIDIM	DESCRIPTION	PURPOSE	CONDITION	EXPIRY DATE
Date of Birth	('being over the age of 16')	Identification by Barcelona City Hall	Can be used to run verify the age of DECIDIM participants	N/A / user opt out
Post Code	('being resident in Barcelona')	Localization by Barcelona City Hall	Can be used to run verify the localization of DECIDIM participants	N/A / user opt out
National ID	('having a national ID number issued by Barcelona City Council')	Certification by Barcelona City Hall	Can be used to verify the public identity of DECIDIM participants	N/A / user opt out

Table 2 DECIDIM Entitlements

In this case, data subjects entitle Barcelona City Council to verify their public identity. However, we suggest that DECIDIM data controllers do not have to necessarily access data subjects actual data as access to attributes signatures should suffice to manage petitions lifecycle and participants signing them.

3.2 IoT Pilot involving CitizenSense

This pilot focuses on data produced by citizens in the context of crowdsourced scientific research through leveraging data subjects' data donations. The latter come from different sensors and devices, especially smartphones that can put at risk both the implementation of the research and the safety of data subjects producing and donating data.

In the case of this pilot the sensor is made by an Arduino chip and a minimal web interface that communicates with the Smart Citizen platform.

In particular, Barcelona second pilot, CitizenSense is a pilot designed to solve the problem of suitable and safe participation to the initiatives promoted under the umbrella of "Oficina de Ciencia ciutadana" (City Science Fabric). The goal is to offer a GDPR compliant smart city service connecting the Open Data Barcelona portal to the Open Data infrastructure through DECODE to build and manage "data commons" datasets.

These datasets are currently gathered on ODI (Open Data Infrastructure), Sentilo, IRIS (Incidències, Reclamacions i Suggeriments), ASIA (Aplicatiu de Sistemes Integrats d'Atenció), CityOS (City Operating System) from Barcelona City Council infrastructure; and two public sources, i.e. Smart Citizen and Inside Airbnb (CF. D5.3 - Data analysis methods and first results from pilots).

The pilot would be a proof of concept for how a decentralised storage and access rights ledger, with dynamic permissions (in the sense that citizens can revoke access, could be used to support distributed sensing projects. This includes the data sharing part, but also the decentralised (or at least hashed) data storage solutions of highly non scalable IoT sensing data streams (Cf. D1.1 - Scenarios and Requirements Definition Report).

Key enabling factors:

- DECODE Hubs to store the data access permissions, that should be connected to the infrastructure where the actual IoT data is stored.
- DECODE Node running on DECODE OS that would mediate access of a specific CitizenScience project to the DECODE Hubs.

Hypothesis statements:

- As a user I want to be in control of my data"
- As an IoT platform provider I want to give users a transparent , traceable, secure, collaborative platform. (CF. D1.1 - Scenarios and Requirements Definition Report).

Below a preliminary set of requirements (SR) for CitizenSense:

- audit storage —> the user can audit the storage of her data, also by mining the dataset s/he co-produced in complete anon- or pseudonymity.
- citizen revokes access to the data produced and donated by data subjects.
- find data from citizens
- access data from citizens
- manage data from citizens
- save data from citizens
- register data donor with the possibility to recall them for new research
- register research projects and put them in touch with data donors willing to take part to the research
- banning a participant
- verify integrity of data
- data access traceability
- Data transparency
- Data reusability
- expiration date

From these requirements, we will now isolate what we consider the necessary attributes for participants to disclose.

For CITYSENSE, there is only one attribute that is in our opinion necessary to operationalise this pilot in a GDPR compliant context:

ATTRIBUTE 1 CITIZENSENSE	Home Address	Verification: Making Sense IoT platform provider	Scope: Localization

Table 3 CITIZENSENSE Attribute

For CITIZENSENSE, those who donate their data collected by Making Sense, entitle the latter with 'can-discover' access level to verify the provenance of sensor data.

Relevant entitlements derived from the privacy and data protection requirements emerging from the scopes of data owners attributes (Citizens taking part to Making Sense and residing in Plaça del Sol) to be exercised by data consumers (Making Sense platform) within CITIZENSENSE:

ENTITLEMENT CITIZENSENSE	DESCRIPTION	PURPOSE	CONDITION	EXPIRY DATE
Home Address	('being resident in Plaça del Sol')	Localization by MakingSense	can be used to verify provenance of sensor data	N/A / user opt out

Table 4 CITIZENSENSE Entitlement

3.3 Holiday Rental Registry / FairBnb

The pilot aims at combining the FairBnb community and Short Term Rental Register in Amsterdam. The goal is to show that DECODE can support the implementation of a city wide register. In order to achieve this goal, a web application that enables Amsterdam residents to register rental periods with the municipality will be developed.

Below a preliminary set of requirements for Holiday Rental Registry / FairBnb:

- audit storage —> the user can audit the storage of her data, also by mining the dataset s/he co-produced in complete a non- or pseudonymity.
- revoke access to data produced and shared by data subjects.
- landlord submit data once
- enabling FairBnb to interact with data collected by the city
- citizen authenticates as an Amsterdam citizen against Municipal Personal Records Database
- citizen registers address for rental on Short Term Rental Register in Amsterdam (Check address validity against public records)
- landlord registers rental periods on Short Term Rental Register in Amsterdam
- give landlord information on the balance within the 60 days annual rental limit
- give municipality information on the balance within the 60 days annual rental limit
- FairBnb issues a certificate to the municipality to record that two peers reached consensus for a rental transaction
- banning a landlord from business if s/he goes beyond the 60 days limit
- register guest
- register local business to take part to distribute hospitality platform FairBnb
- register citizen who is not a landlord

From these requirements, we will now isolate what we consider the necessary attributes for participants to disclose.

For instance, FAIRBNB attributes, for the data subject 'landlord', are as follows:

ATTRIBUTE LANDLORD 1 FAIRBNB	Home Address	Verification: Amsterdam City Hall	Scope: Localization
ATTRIBUTE LANDLORD 2 FAIRBNB	Home Deed	Verification: Amsterdam City Hall	Scope: Certification
ATTRIBUTE LANDLORD 3 FAIRBNB	Date of Birth	Verification: Amsterdam City Hall	Scope: Age Verification
ATTRIBUTE LANDLORD 4 FAIRBNB	National ID Number	Verification: Amsterdam City Hall	Scope: public identification
ATTRIBUTE LANDLORD 5 FAIRBNB	National Tax Code	Verification: Amsterdam City Hall	Scope: Public Identification
ATTRIBUTE LANDLORD 6 FAIRBNB	Number of rental days	Verification: Amsterdam City Hall	Scope: tracking landlord rental periods

Table 5 FAIRBNB Attribute

Relevant entitlements derived from the privacy and data protection requirements emerging from the scopes of data owners attributes (in this case, the class 'landlord') to be exercised by data consumers (Amsterdam City Hall and FairBnB community) within FAIRBNB:

ENTITLEMENTS Amsterdam City Hall	DESCRIPTION	PURPOSE	CONDITION	EXPIRY DATE
Home Address	('being resident in Amsterdam')	Localization by Amsterdam City Hall	Can be used to verify landlord residence	N/A
Home Deed	('owning a home in Ansterdam')	Private premise certification by Amsterdam City Hall	Can be used to verify private ownership for short term rental	N/A
Date of Birth	('being over the age of 18')	Identification by Amsterdam City Hall	Can be used to verify landlord age	N/A
National ID Number	('having a national ID number issued by Amsterdam City Council')	Certification by Amsterdam City Hall	Can be used to verify landlord public identity	N/A
National Tax Code	('having a national ID number issued by Amsterdam Tax Authorities)	Identification by Amsterdam City Hall/Local Tax Authorities	Can be used to verify landlord fiscal compliance	N/A

Table 6 FAIRBNB Entitlements

In this case, the data controller/consumer, i.e. Amsterdam City Hall, has the right to access landlords attributes for verification. However, FairBnb participants can only access the signature of the attribute, not the attribute itself. This configuration can be amended by the FairBnb community.

3.4 Gebiedonline

Gebiedonline (Neighborhood Online) is an Amsterdam based online neighbourhood platform that is cooperatively run and owned. Every decision is made within the community. The platform aims to enable people, groups and organisations to view events taking place in the area, share news, exchange and borrow products and services, and to meet people in a GDPR compliant environment.

Below a preliminary set of requirements for Gebiedonline:

- Audit storage —> the user can audit the storage of her data, also by mining the dataset s/he co-produced in complete a non- or pseudonymity.
- revoke access to data produced and shared by data subjects.
- collective decision making
- citizen registration
- group registration
- organization registration
- create event
- publish event
- view event
- share news
- contact peers
- offer product
- borrow product
- offer service
- borrow service
- banning subscriber
- manage data sharing rights

From these requirements, we will now isolate what we consider the necessary attributes for participants to disclose.

GEONLINE attributes for data subjects are as follows:

ATTRIBUTE 1 GEONLINE	Date of birth	Verification: GO platform	Scope: identification by GO
ATTRIBUTE 2 GEONLINE	Post Code	Verification: GO platform	Scope: identification by GO

Table 7 GEBIEDONLINE Attribute

Relevant entitlements derived from the privacy and data protection requirements of data owners (Gebiedonline participants) to be exercised by data consumers (Gebiedonline organisers) within the Gebiedonline pilot.

ENTITLEMENTS GEONLINE	DESCRIPTION	PURPOSE	CONDITION
Date of Birth	('being over the age of 18')	Identification by GONLINE platform	Can be used to verify participant age
Post Code	('being resident in 103AK')	Localization by GONLINE platform	Can be used to verify participant localisation

Table 8 GEBIEDONLINE Entitlements

In this last case, GONLINE participats entitle GEONLINE platform management to access their attributes on age and location at on boarding and to other participants for when they are relevant for social networking interactions.

In the following section, we present a comparative analysis between pilots attributes and entitlements in order to isolate those common to various pilots as an initial basis for the composition of Smart Rules to be processed by Zenroom.

3.5 Comparative analysis among pilots' attributes and entitlements

In order to find commonalities among pilots, in the next table, we show the results of a comparative analysis among the attributes concerning different data subjects from different pilots:

ATTRIBUTE/ENTITLEMENT	DECIDIM	CITYSENSE	FAIRBNB	GEONLINE
Date of Birth	X		X	X
Post Code	X		X	X
Home Address		X	X	
National ID	X			

Table 9 Comparison analysis among pilots

As the table shows, there are attributes and corresponding common among various pilots pointing to the possibility to generalise Smart Rules among pilots. Also in this case there are overlapping entitlement policies which can be generalised in rules that can apply to more than one pilot and are related to the same attributes.

According to the working definition of Smart Rules presented above, we now have the elements needed to propose Smart Rules for the data subjects and data controllers participating in the four DECODE pilots.

4 Conclusion

In this document, we identified a preliminary set of attributes for each type of data subject registering on the relevant service. We then stated for each pilot the corresponding entitlements components, i.e. description, purpose and condition in a declarative language. The Smart Rule will be the syntax-directed translation of the relationship between attributes and entitlements in the functional language of executed by Zenroom virtual machine

From here onwards the research of this task in DECODE will proceed to complete the implementation of Zenroom and then compile Smart Rules for all the functions that can be solved by this implementation. It is evident that not all functions can be satisfied by a single language interpreter, but the operations done in DECODE should be expressed as much as possible using this language whenever they are dealing with private data and cryptographic operations, while leaving out the relationship that do not require cryptographic validation.

5 Bibliography

Budroni, A. & Pintore, F. (2017) *Efficient hash maps to g2 on bls curves*.

Haas, A. et al. (2017) 'Bringing the web up to speed with webassembly', in *Proceedings of the 38th acm sigplan conference on programming language design and implementation*. 2017 ACM. pp. 185–200.

Ierusalimschy, R. et al. (1996) Lua-an extensible extension language. *Softw., Pract. Exper*. 26 (6), 635–652.

Kosar, T. & Livny, M. (2004) 'Stork: Making data placement a first class citizen in the grid', in *Distributed computing systems, 2004. proceedings. 24th international conference on. 2004 IEEE*. pp. 342–349.

Meijer, E. et al. (1991) 'Functional programming with bananas, lenses, envelopes and barbed wire', in *Conference on functional programming languages and computer architecture*. 1991 Springer. pp. 124–144.

Murata, M. et al. (2005) Taxonomy of xml schema languages using formal language theory. *ACM Transactions on Internet Technology* (TOIT). 5 (4), 660–704.

Rios, R. et al. (2017) 'Query privacy in sensing-as-a-service platforms', in *IFIP international conference on ict systems security and privacy protection*. 2017 Springer. pp. 141–154.

Ritchie, D. M. et al. (1988) *The c programming language*. Prentice Hall Englewood Cliffs.

Scott, M. & McCusker, K. (2016) SOK it to the iot.