decode

Design & implementation interface for smart rules

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

D4.9 Design & implementation interface for smart rules

Version Number: 2.0

Lead beneficiary: TW

Due Date: December 31th, 2018

Author(s): Federico Bonelli (Dyne.org), Taco van Dijk (Waag), Guy Samuel (TW)

Editors and reviewers: Denis Roio (Dyne.org), Oleguer Sagarra (IMI), Marco Ciurcina (NEXA), Paul Ripley (TW)

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: 31/01/2019

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

Table of contents

1 Introduction

When setting up "privacy preferences" in online platforms many are the things usually listed to define the level of access to information about oneself. The complexity of conditions about what information one can decide to disclose in different context is high to the point that is nearly impossible to be aware of what really happens to our data in different contexts and in the hands of different operators. This complexity has grown to a point in which it has become common to even delegate the responsibility of privacy to third-party companies or default settings.

Beyond technical and political implications, this deliverable focuses on the possibility to clearly perceive who is doing what with our data and take clear decisions when it matters. In designing this aspect of DECODE we shouldn't give up and think it is difficult to make someone conscious to protect his or her own identity, opinions, whereabouts and relations. To facilitate the conscious choice about one's own privacy settings emerges as an important part in DECODE's mission and this part of the work focuses on inventing new visual and sensory metaphors and patterns of interaction that can facilitate this sort of awareness.

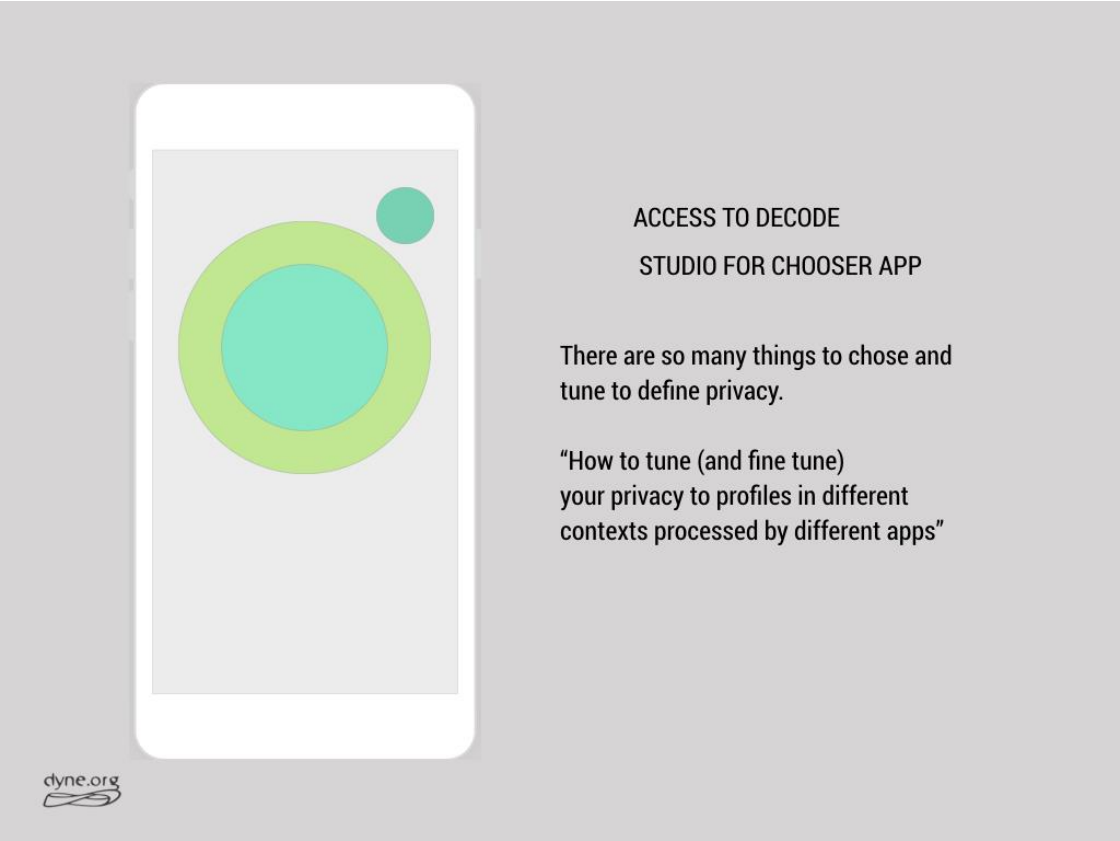


Figure 1

2 The challenge of diversity

While researching this part it must also be taken into account that the notion of privacy changes dramatically between different European heritages and cultures. In the northern countries, for example the way the concept of privacy is expressed often carries a negative fashion: it defines a border and underlines an act of emancipation separating the group from the individual. We find as well in the wikipedia (en) definition of Privacy as:

"the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively."

But if we go to read the definition on the Italian wikipedia page for example we find:

indica - nel lessico giuridico-legale - il diritto alla riservatezza della vita privata di una persona.

Literally "[privacy] indicates, in the juridical jargon - the right to discreetness about the private life of a person". The difference is striking as the "ability (to seclude)" becomes "a right" (to have a private life) and the term "vita privata" substitutes "selective expression".

3 Inspiring projects

Even in a limited capacity, it has been important to take into account these differences during this design process. Designers and developers from Catalunya, Italy or The Netherlands involved in DECODE are often surprised when talking about "privacy by design": it's then easy to realise we think of different operational values end representative metaphors connected to the same lemmas.

The challenge becomes to map a set of ever-changing and self-adjusting habits into a taxonomy of behaviours for a digital device and one's own presence on the net. Are we talking about a footprint here?

What becomes an useful asset for this task is then the study of the interface of Dowse. Dowse is an IoT project by Dyne.org (Kranenburg, 2017) that, among other value propositions, aims at moving the language of networking out of the defence and military jargon of security into a friendly, down to earth idiolect capable of addressing hospitality and politeness through the quest to "dowse for network events" (Dragona, 2016). Quoting the Dowse Whitepaper:

Dowse is not only a functional tool, but a symbolic operation proposing a different linguistic approach to networking. In conceptualizing and documenting Dowse, all references to military traits are removed: there is no use of "defense", "shield", "guardian" or "firewall" words.

Privacy awareness (rather than protection) is envisioned and presented to its users not as a violent process, but as a responsible, natural act — one in search of harmony among those things connecting the inside and outside of a person's private, common, and public aspects of life.

We can agree to inherit this mission in DECODE and adopt a lexicon that suggests the possibility for harmony rather than the treat of anxiety.

Another inspiring approach is provided by a manifesto published in 2016 by "The Plumbing Birds" (collective name) and titled Data Prevention Manifesto: in this lyrical text "awareness" is said to be "a merciful weapon for the wise" while metaphors morph technical choices into other perceptive and narrative forms.

4 Privacy in context

Following up with various brainstorming sessions and taking into account all considerations and inspirations provided, this brief study and implementation will not answer the question of "what is privacy" in DECODE. To the contrary, considering privacy a public cultural construction, we intend to design a usable and intuitive way for DECODE applications to assess one's privacy preferences in a particular context. It is not a definition of privacy conditions that we need, but a procedural structure for their enunciation: our attention shifts from the boundary of privacy to the process by which it can be defined accorded to specific contexts.

This is also functional to the established idea in DECODE that there is not such a thing as "identity": each participant should be able to represent his or herself according to a set of attributes that are disclosed to specific operators in specific conditions. Such attributes can change, as can also change the will and needs to disclose different ones in different conditions.

While the global operational trend is to consider privacy as a context-free set of conditions, DECODE should aim at representing the different context in an intuitive way in order to inform choices that are aware and balanced.

DECODE should be seen as a project that offers grounds for this design to take place and even evolve and mutate into more complex formulations: the interface design process can be facilitated by the adoption of a declarative language as Zenroom and should consist of a series of LEAN iterations to satisfy these goals requiring none or just a few gestures:

- Allow to tune (and fine tune in time) preferences for privacy in decode
- Grant different levels of access to data in different contexts
- Indicate the best way to create, adjust and change privacy profiles in DECODE
- Minimise the information needed to introduce oneself in each context

To move forward we propose a representation of DECODE's technological layer that can hopefully be understood by anyone without any particular technical knowledge. First and foremost we need to set-up a visual metaphor that guides the design process: to trace guidelines above the complex set of practices and crypto technologies, observing their functions and role in the context of interaction design.

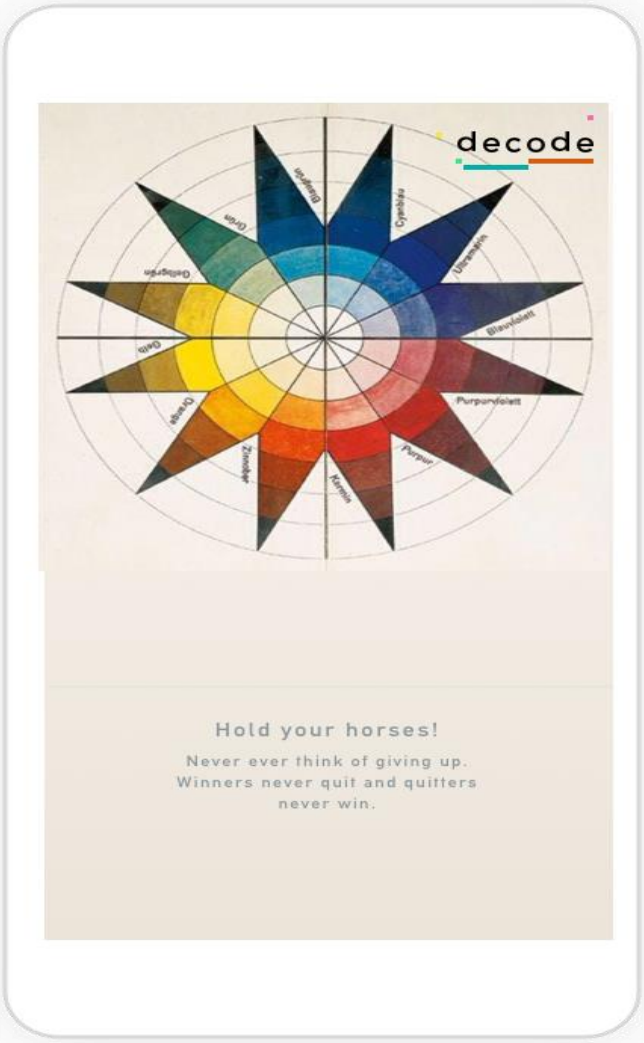

decode
Hold your horses!
Never ever think of giving up.
Winners never quit and quitters
never win.

Figure 2

5 A new look at the Internet

DECODE is a lot of things interconnected. Some concrete, some rather abstract and some technically complex. All those synergies create a complex and intertwined cluster of entities. But this should not be the starting point for our task of human-machine interaction design. We simply want to make a story understood and for that we only need an associative field were all elements can be narrated before than explained. This section proposes a way to square the problem and carve the right field to morph our stories inside it.

Let's start with the minimal, top level and crude version of the narration.

First. Immagine all there is : - applications, simple or complex, whatever device powers them, whatever computation they run upon - a space were these applications live - data transfer (input and output) between applications - metadata: for example timestamps and locations (latitude and longitude, traditionally lambda and phi)

Anything there is can be put into this space. See the figure below:

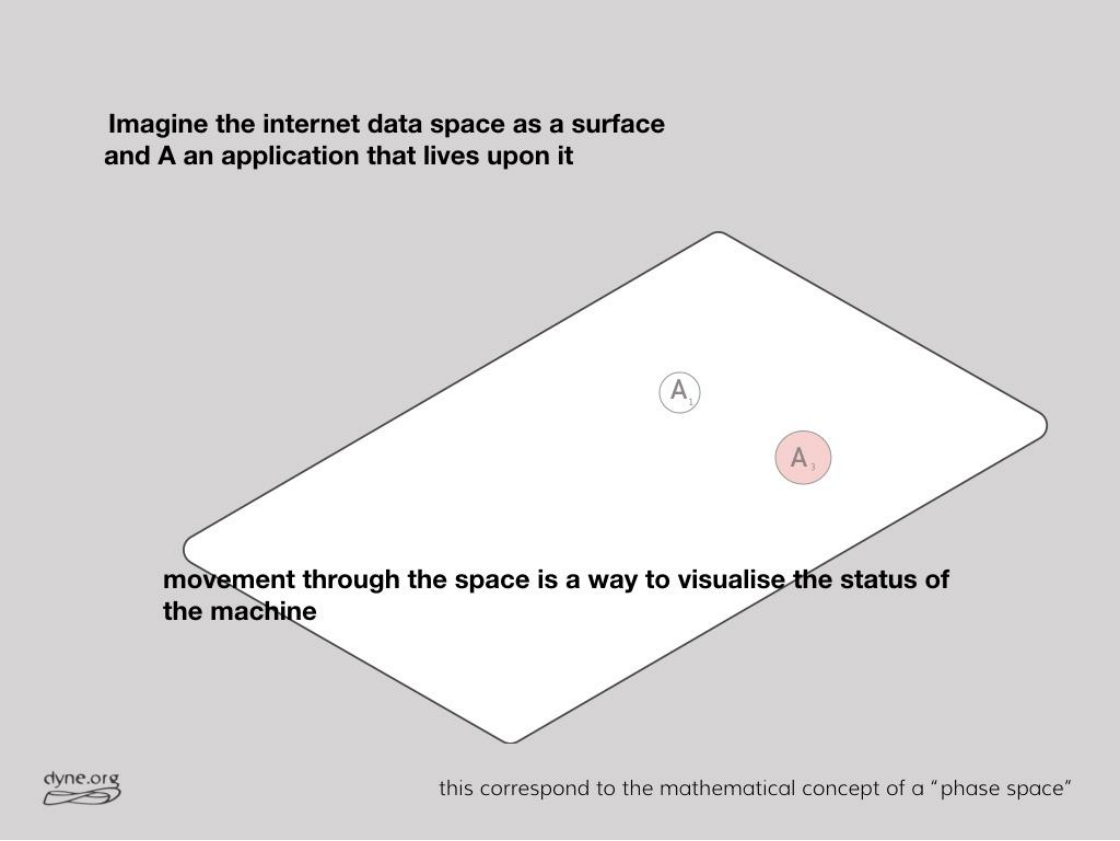


Figure 3

So what DECODE boils down to? a **sublayer** to this space were computation can be trusted, anonymity is granted but **uniqueness can be granted as well**. Is a p2p grid of trusted operations that operate in a different condition than the layer above.

All this is de-facto transparent to DECODE participants, therefore we represent it as a sublayer in our representation. Above is the Internet, below is DECODE: a tracing algorithm is seen as something that is able to recognise, and trace patterns in metadata.

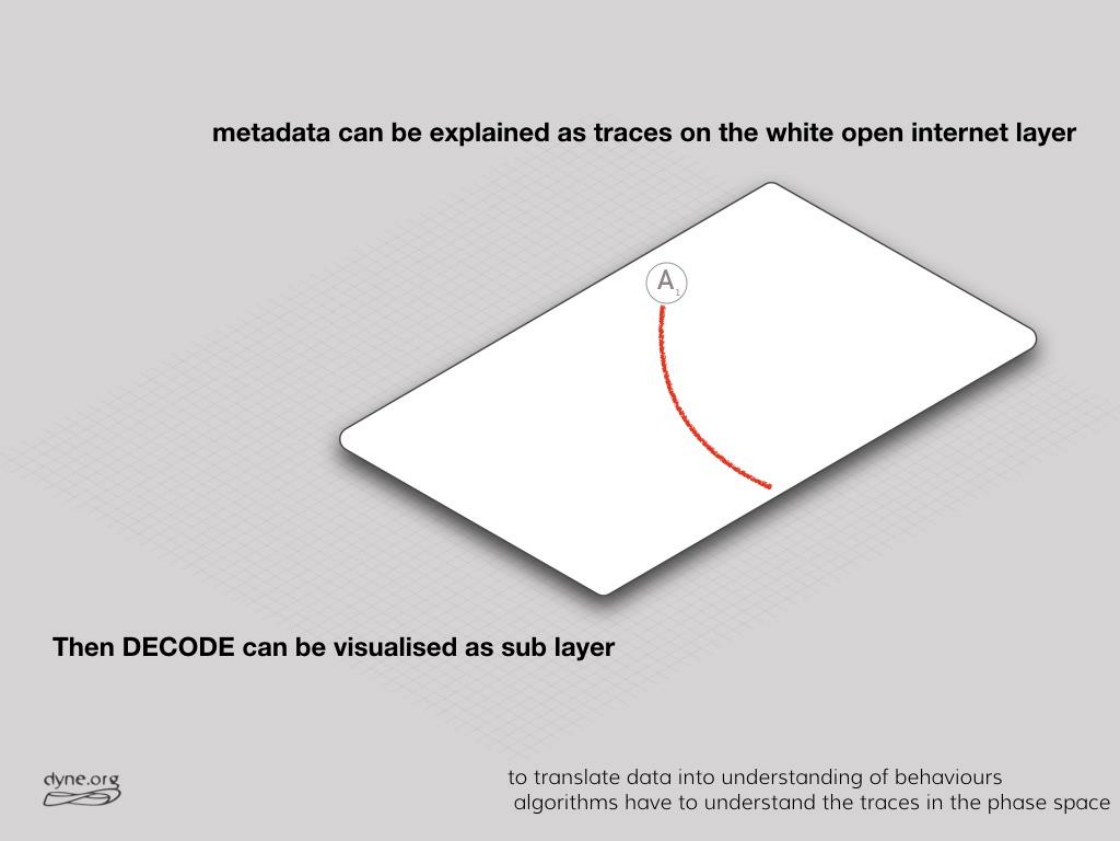


Figure 4

This is all we need to represent DECODE to a participant. Applications entering in and out of the most generic contexts of communication. This is then represented as the act of rooting onto a trusted layer below, to perform transparent computations were the result may, or may not, include transactions of all types. Transactions that can be forgotten or recorded on a distributed ledger.

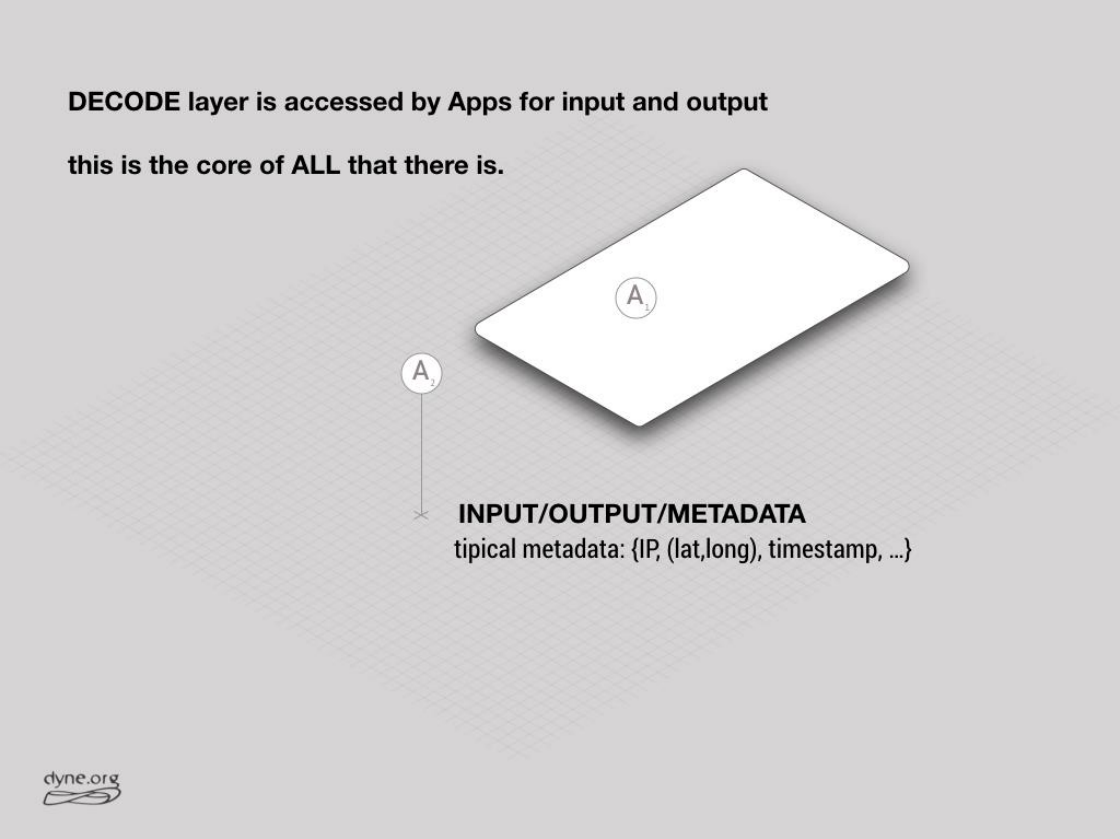

DECODE layer is accessed by Apps for input and output
this is the core of ALL that there is.
A1
A2
INPUT/OUTPUT/METADATA
tipical metadata: {IP, (lat,long), timestamp, ...}
dyne.org

Figure 5

6 Recognising the situation

A situation is a concept mutuated from art. It calls for a triadic logic. By triadic is implied that at least tree entities concur to effect any given situation. In art we call the concept regarding to the artwork, the context it is shown, the author views about the piece and the viewer place in it. For some art theorists this cannot be expressed as a hierarchy, but has to be accounted in a complex dynamical relation. Michael Foucault talks about it in a brief seminal work about Velasquez "Las Meninas" (Foucault, 1966). The situation has also been the playing field of an extremely influential art movement during Europe's XX century: The Situationist International.

Our central idea for the analysis of any human to machine and machine to machine interface is the construction of situations, that is to say, the concrete construction of momentary ambience of life and their transformation into a superior emotional quality. We must develop a systematic intervention based on the complex factors of two components in perpetual interaction: the material environment of life and the behaviors which that environment gives rise to and which radically transforms it. (McDonough, 2004)

It is proven in mathematical theory of complexity that in feedback processes at least a period of three is necessary to see a cascade effect. This does not imply any mathematical rule to allow situation assessment, but is an interesting analogy to keep, just as a analogy for now.

So as a general empirical rule we can assume that 3 is the minimum number of entities to be considered in any design. For example in a theatrical form of spectacle there is the text, the artistic production, comprehensive of cast and crew, and the audience, their behaviour, motivation and stamina, to determine the result of the production.

A situation is generally composed by various concurring factors that are designed to concur and collide in a specific space/time to determine a specific effect. Teather, as cooking for friends for a special occasion's dinner are ways to design effects, with a certain degree of freedom on the desired outcomes.

A situation, as a notion and as a conceptual instrument, pertains both to psychology and to history of ideas. What we propose here is to use it explicitly as a conceptual framework in which to perform various types of analysis.

After such an analogical introduction let's give ourselves an operative and pragmatic type of definition: a situation is an occurrence of intentions, people and objects in any lived space/time. This determines at least three concurrent causal chains to intervene. Lived space/time here points to the "real world assumption" (RWA): no situation can be isolated completely from a more general context. As we see we will use the RWA to our advantage in design.

7 Sketches of the privacy choser app

To select the way we prefere to be known, identified, tracked and eventually forgotten in the digital domain has to be naturally simple to operate.

Here we follow up with a sequence of sketches made to foster the intuition of this design, used to iterate among a sample of participants in Amsterdam.

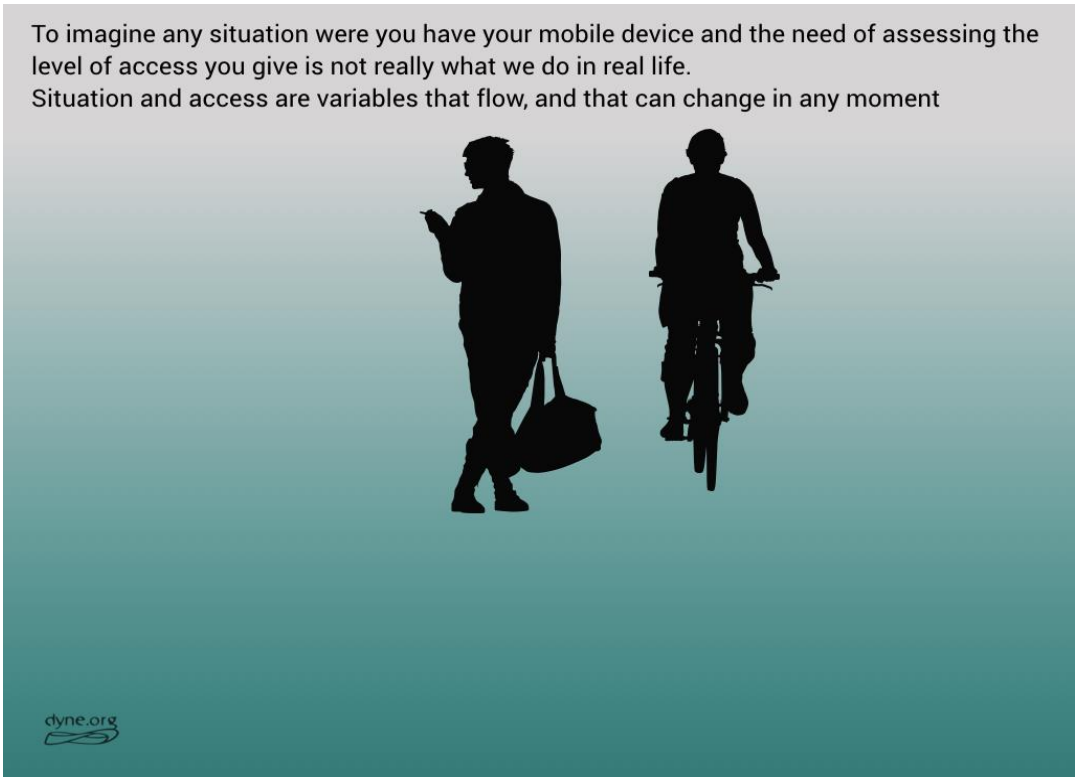


Figure 6

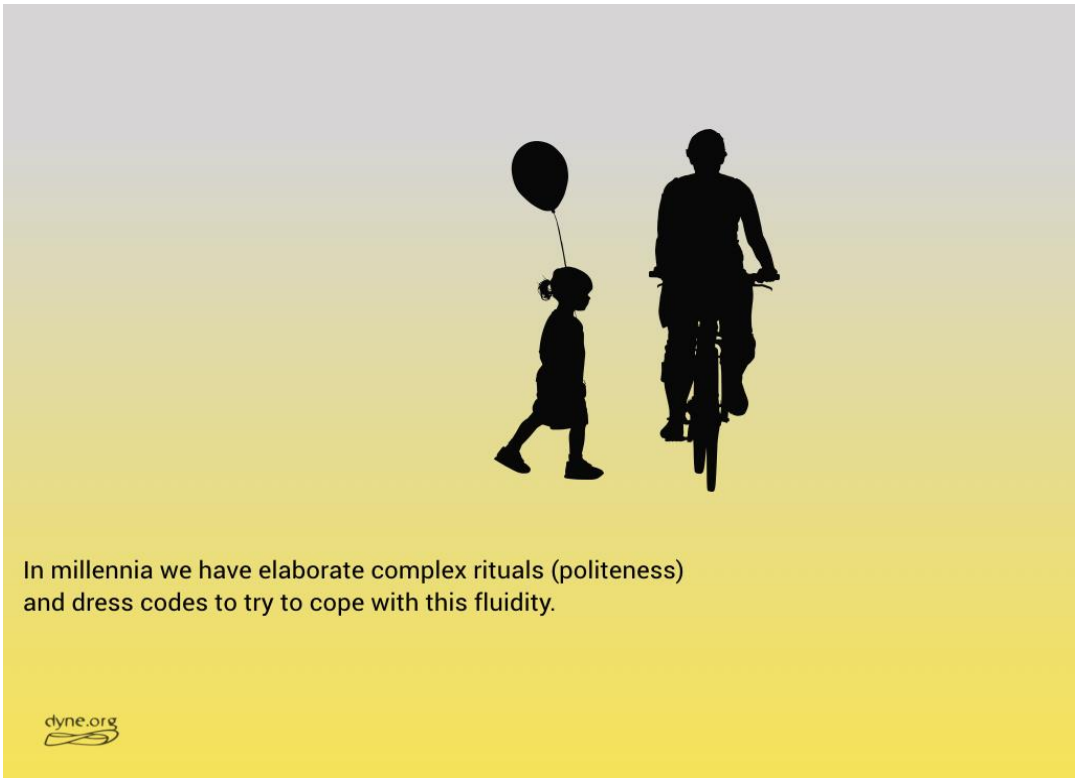


Figure 7

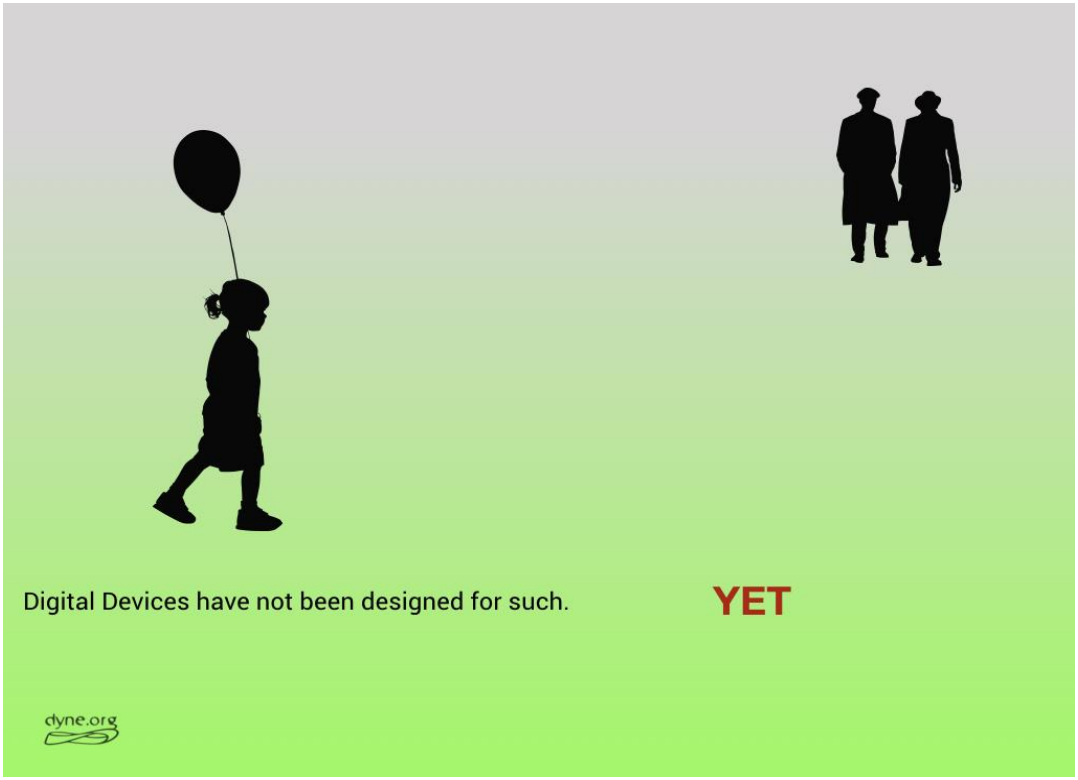


Figure 8

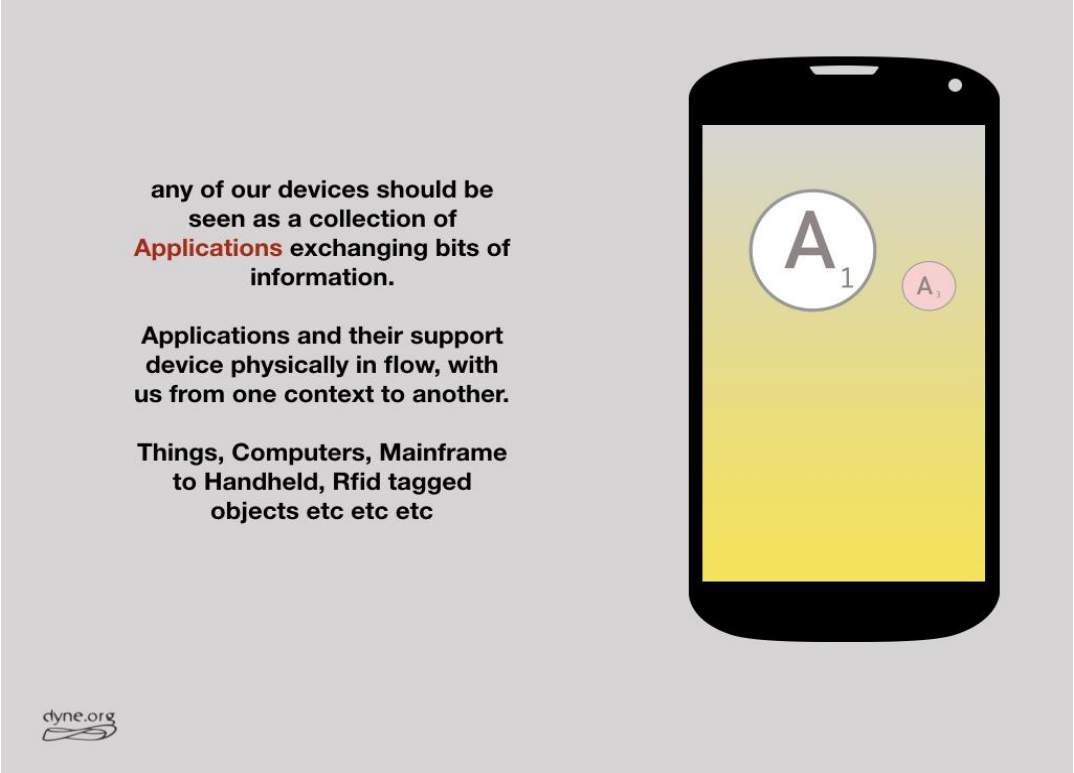


Figure 9

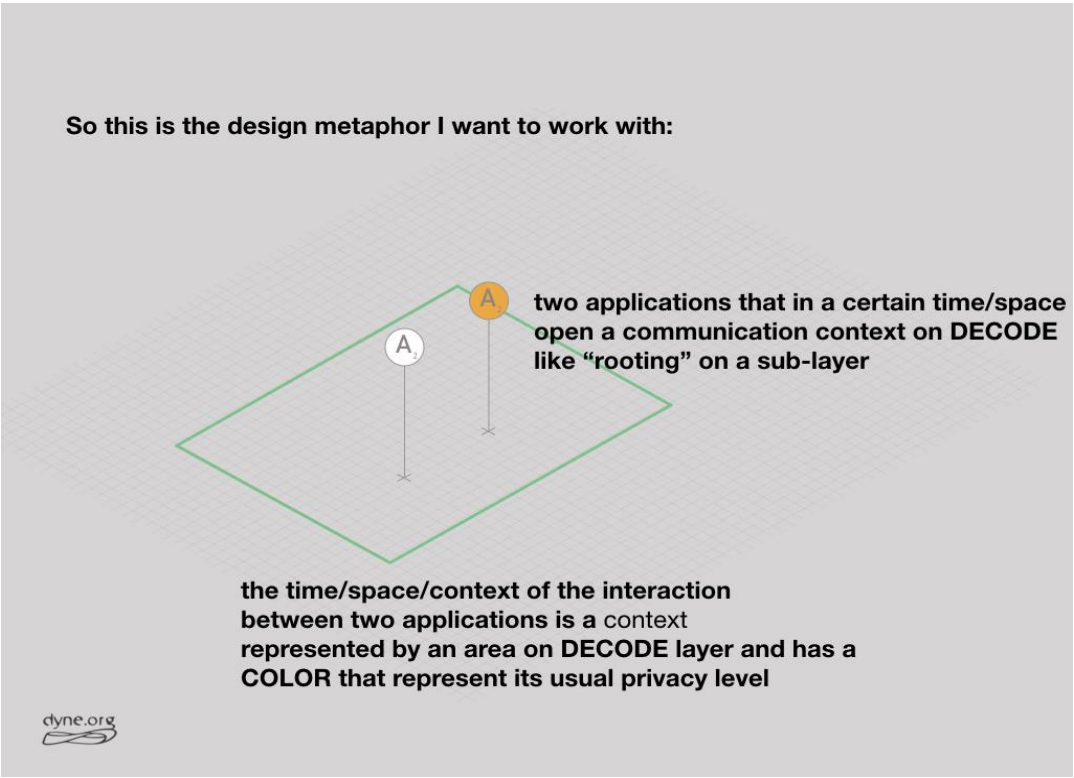


Figure 10

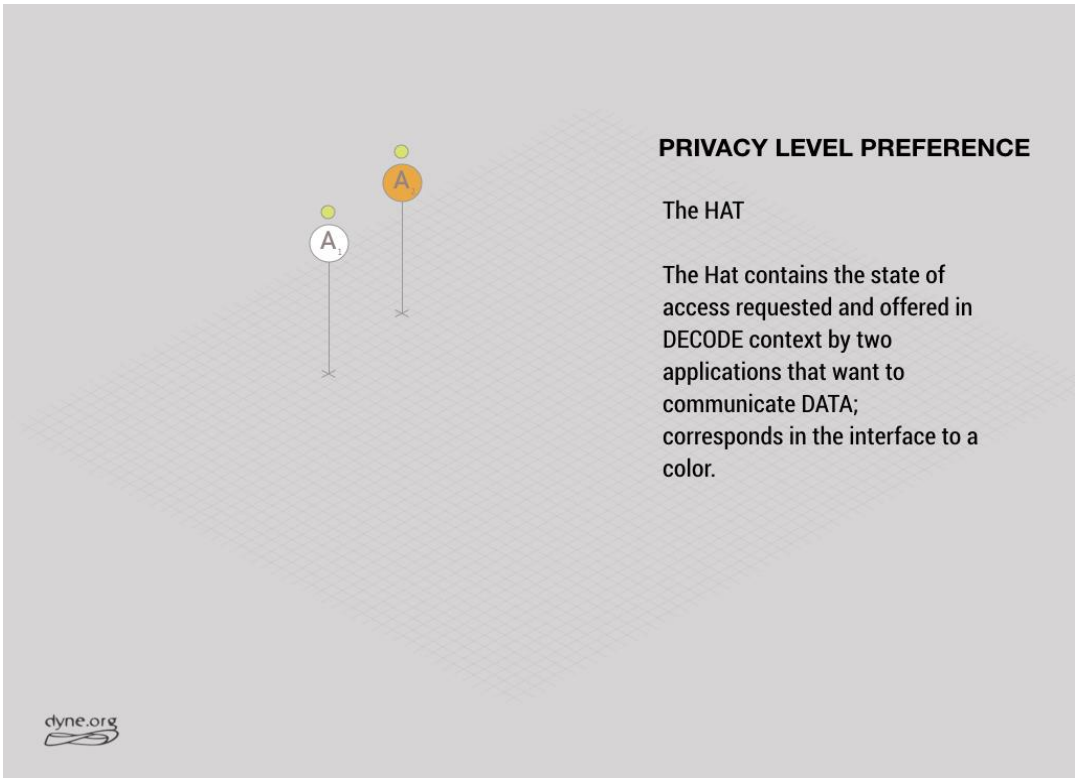

PRIVACY LEVEL PREFERENCE
The HAT
The Hat contains the state of access requested and offered in DECODE context by two applications that want to communicate DATA; corresponds in the interface to a color.
dyne.org

Figure 11

8 Visualisation in the Zen Room

The Zenroom component developed for the DECODE project is a virtual machine (VM) that can parse and execute a simple, restricted language which is evolving together with the project. This VM and its language are an important building block for DECODE as they can be embedded in any client to realise point-to-point encryption schemes. From its whitepaper on zenroom.dyne.org:
Zenroom's restricted execution environment is a sort of sandbox whose parser is based on LUA's syntax-direct translation engine and has coarse-grained control of computations and memory. The Zenroom VM it is designed to "brittle" and exit execution returning a meaningful messages on any error occurred.

Zenroom's documentation and examples are being written to encourage a declarative approach to scripting, treating even complex data structures as first-class citizens.

Due to its integration in the client-side of things the Zenroom also brings the opportunity to implement a visualisation of data procedures and settings - or at least produce the semantic information needed for a visualisation to be rendered.

In our proposed visualisation for DECODE workings from the point of view of the participant we see the Zenroom as the context on DECODE layer were the two apps root.

The point of intervention are then two: 1. the "Abstract Syntax Tree" (AST) of the smart-rule executed by Zenroom 2. the input and output schemas of the data processed by Zenroom

Both points are being researched and the most recent iteration of Zenroom in its upcoming 0.6 release has been taking these opportunities in consideration, adding the feature of AST rendering of a script as well a functioning schema validation of data at the input and output rendering from and to JSON format.

9 Flow analysis

For the analysis of flows of data and decisions related to it we are thinking of possible representations that can easily explain a smart rule and its relation to other rules. This is now only a proposal we explored for a conceptual visualisation tool that stays in the narrative of the visual metaphor used so far. The easier possible way to implement such a visualisation is at the crossing between the use of the "blockly" type of programming paradigm and the flow programming paradigm implemented by "node-red" to represent information flows.

Figure 12

Blockly is a client-side JavaScript library for creating visual block programming languages and editors. It is a project of Google and is open-source under the Apache 2.0 License. It typically runs in a web browser, and visually resembles Scratch. Blockly is also being implemented for Android and iOS; not all web browser based features are available for Android/iOS. Blockly uses visual blocks that link together to make writing code easier, and can generate JavaScript, Python, PHP or Dart code. It can also be customised to generate code in any textual computer language. After some qualitative evaluations of it for the visualisation of smart-rule pilot examples we quickly draw a conclusion: blockly can help someone that is nearly illiterate about a scripting

language to write a script, but does not help to understand what the script does and in fact it can make it more difficult to understand.

Node-RED is a flow-based development tool developed originally by IBM for wiring together hardware devices, APIs and online services as part of the Internet of Things. Node-RED provides a browser-based flow editor, which can be used to create JavaScript functions. Elements of applications can be saved or shared for re-use. The runtime is built on Node.js. The flows created in Node-RED are stored using JSON. Since version 0.14 MQTT nodes can make properly configured TLS connections. In 2016, IBM contributed Node-RED as an open source JS Foundation project.

The evident advantage of node-red's visual approcach is the fact that it uses a flow paradigm for programming actions and integrates IoT protocols like MQTT and technology like email, twitter, telegram, etc. basing it on the universal presence of node.js and javascript in their api's.

The most common elements of a smart-rule language colud be integrated in the node red visual language as modules. This approach can enhance: - integration - re usability of software - transparency - social acceptance and reach of zenroom programs

It is anyhow necessary more exploration in this regard. Our research then moves forward to consider solutions developed ad-hoc for the DECODE pilots, as a sort of minimum viable prototype that adapts itself to the higher complexity, mostly provided by the Amsterdam/GO pilot.

10 Differences are meaningful

The main intuition moving us forward in designing a new visualisation pattern, according to the previous reasoning on the importance of context for privacy, has been that of considering the difference of requested privacy settings in different contexts.

The assumption we make is simple: every new and known context will propose us a rather consistent set of privacy settings that can be shared among similar contexts, grouped and understood as something we are comfortable with in similar situations, that is when the same operators and similar contexts are at play.

This way we envision the need to operate on privacy settings a few times and not for every interaction, establishing what we feel comfortable sharing

Here some visual experiments around this concept:

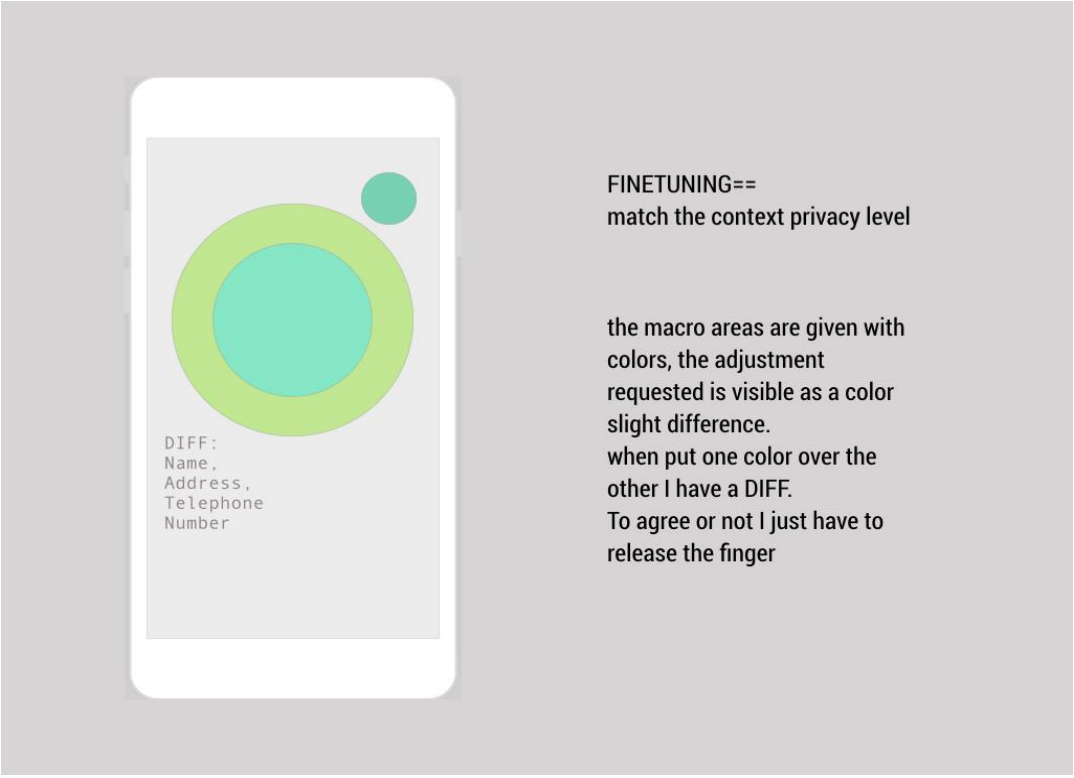


Figure 13

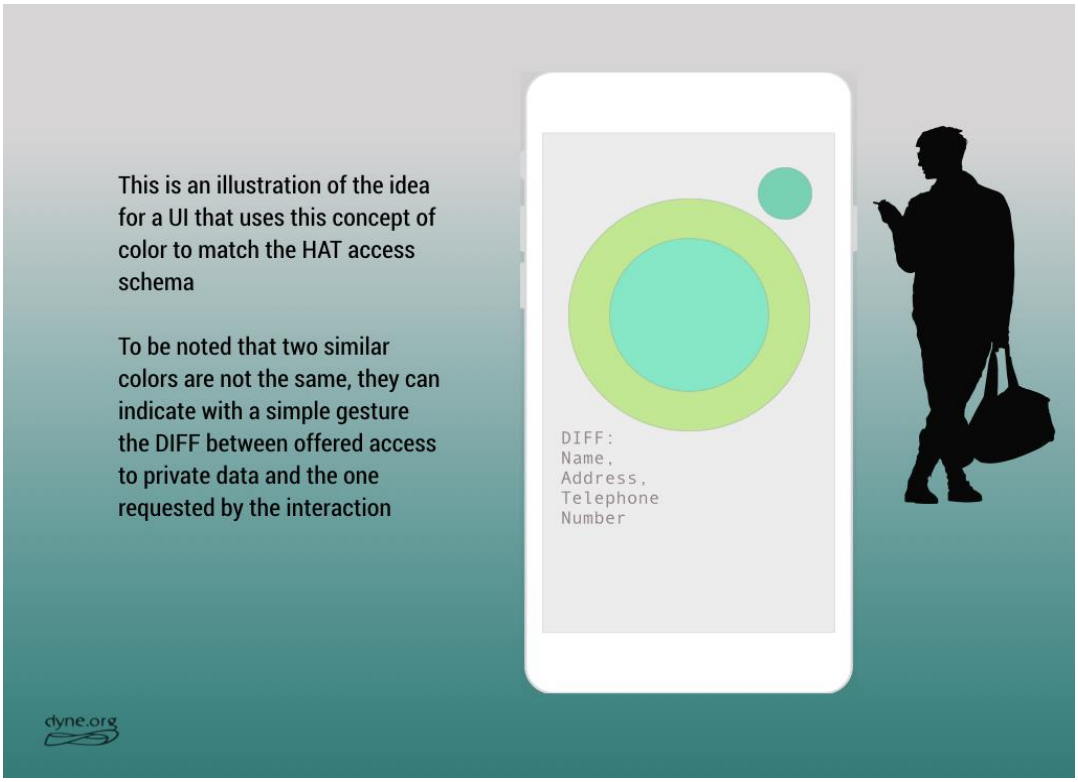


Figure 14

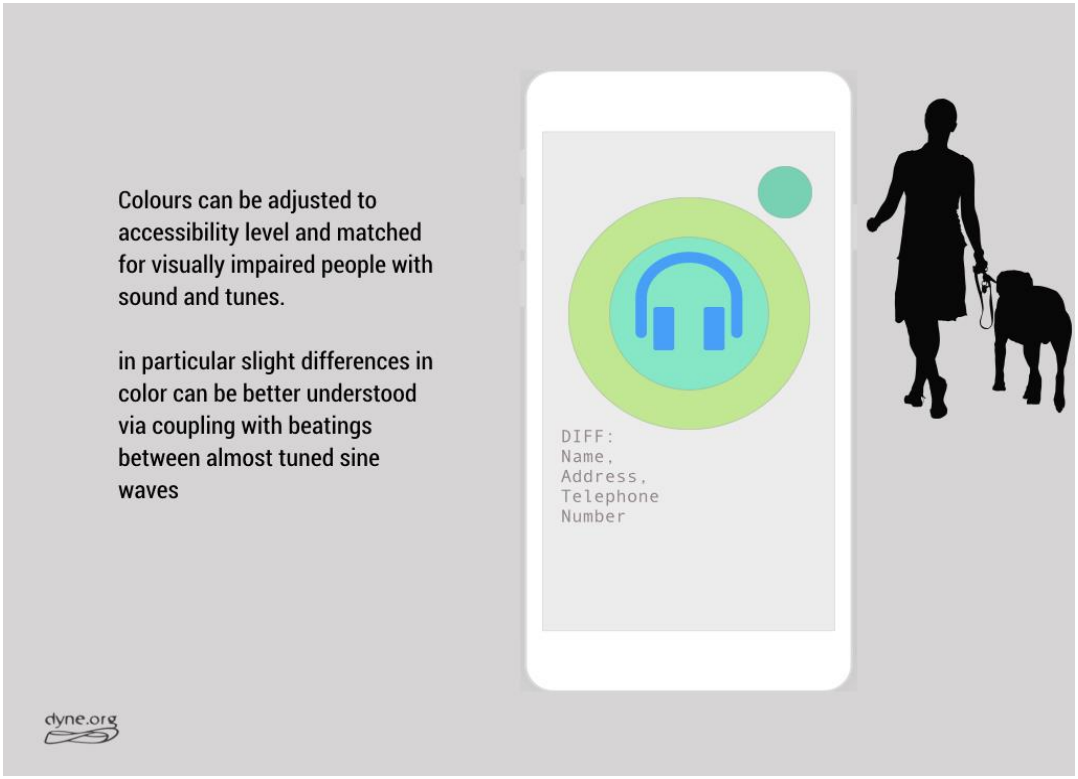


Figure 15

Colors and sounds then play an important role, here an experimentation on the color of the contexts:

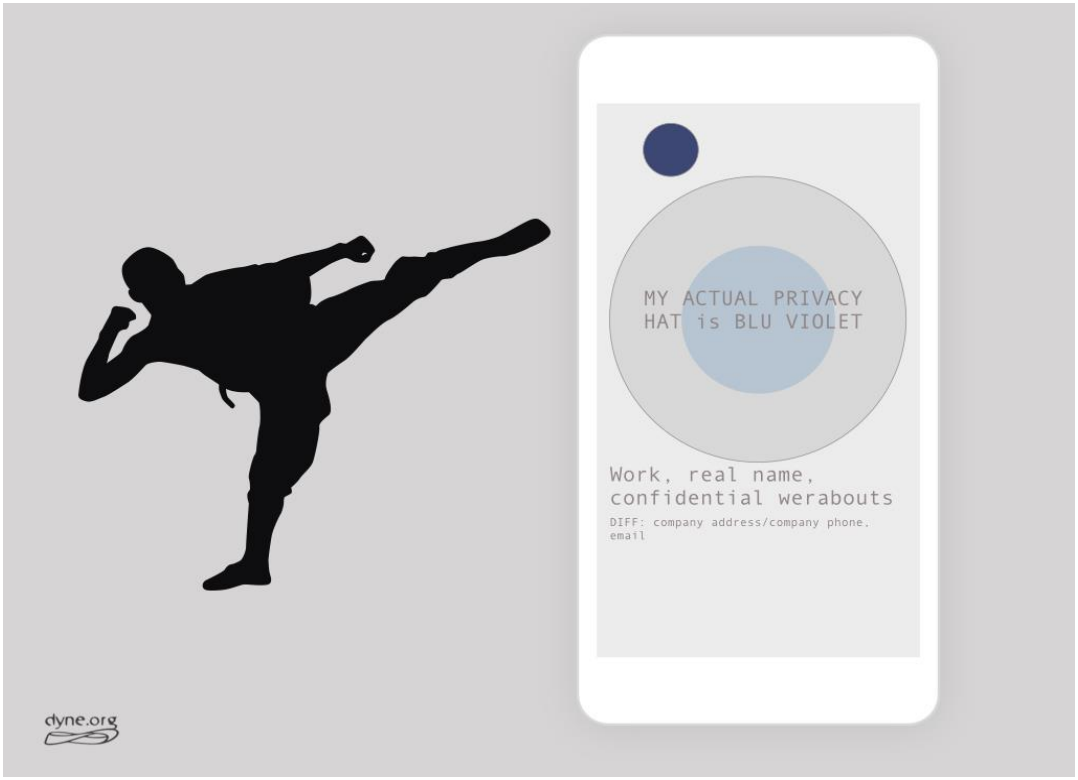


Figure 16

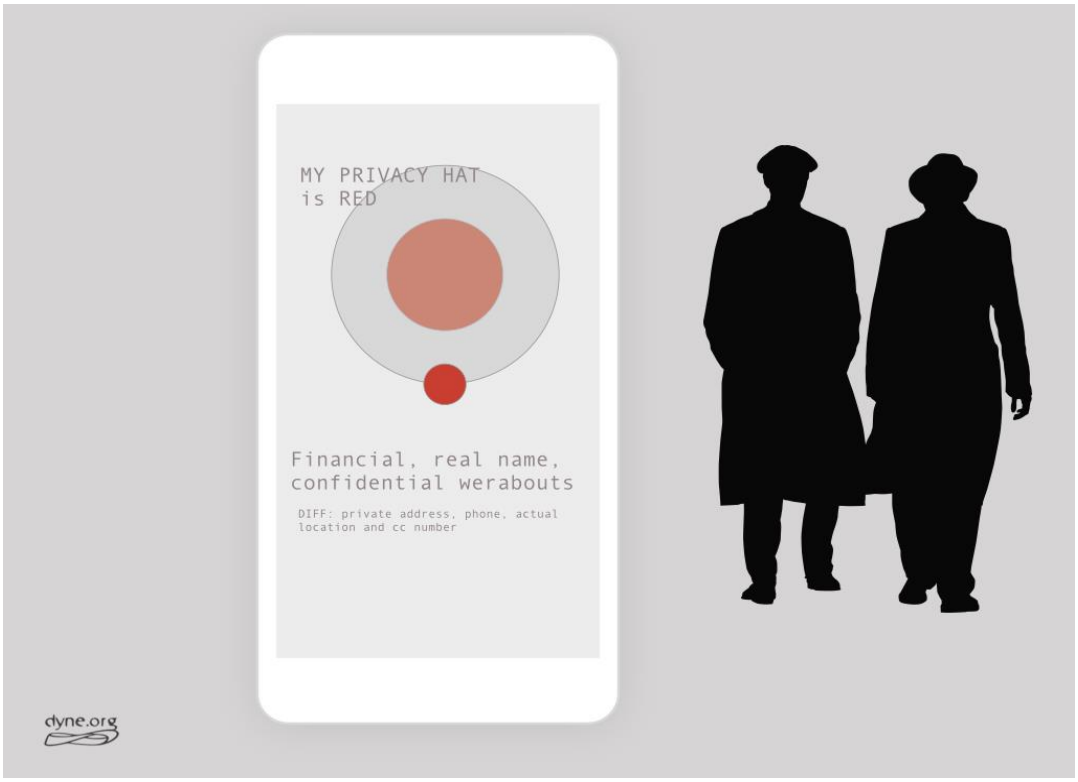


Figure 17

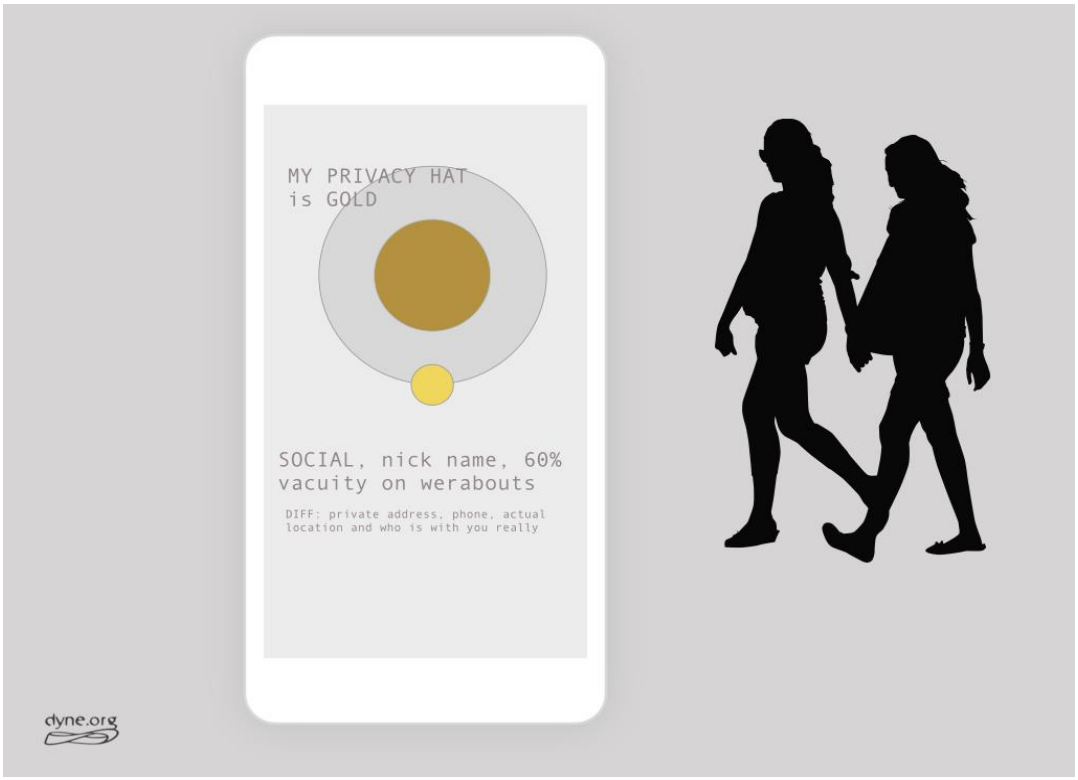


Figure 18

And settings that one may consider default:

CHOOSER CONFIGURATION:
should be a pre populated table of properties with color and tones open to
USER CUSTOMISATION VIA LEARNING AND ADAPTATION

Table 1

property	public/work	public social	friends	family	healt	financial	taxe
name	yes	nick 01	nick 01	nick 02	yes	yes	yes
age	in my 40es	in my late thirties	my day of birth	my date of birth	my date of birth	my date of birth	my c
sex	no	yes	yes	yes	yes	no	no
address	no	no	yes	yes	depends	yes	yes
work address	yes	no	no	yes	yes	no	no
work phone number	yes	no	no	yes	no	yes	no
home number	no	no	yes	no	yes	no	no
car plate	no	no	no	yes	no	no	yes
passport	no	no	no	no	no	yes	no
social security	no	no	no	no	no	yes	yes
position with insurance	no	no	no	no	yes	no	yes
position with bank	no	fake	no	no	no	yes	no
location at present	no	yes+30%	yes	10%	yes	no	no
home location	no	yes + 40%	YES	yes	no	yes	yes
marital status	no	no	yes	yes	no	no	no
favourite color	yes	yes	yes	fake	no	no	no
smoker	no	yes	yes	no	no	yes	no
penal record	yes	no	no	no	no	no	no
hobbies	no	yes	YES	no	no	no	no

Figure 19

11 Implementation and Testing

The development of these interrelated concepts must now be brought to the sphere of user-facing applications, to be applied in specific contexts and use cases. Our next challenge is to describe how the broad visual representations of context and difference, supported by colour and spatial metaphors, can be applied in these applications.

In addition to the concepts discussed above, the following considerations have informed our implementation guidelines:

- For the sake of simplicity, a user must be presented only with the minimum amount of information in order to take action in an informed manner.
- We must specify which principles should be followed by all services, and which elements of the UI can be adapted to a specific application. The goal is to ensure a common framework between services (e.g. the definition of contexts will be universal, as is the UI element indicating consent), while allowing adaptation for specific uses (e.g. some services can present a subset of context or available attributes).
- Usability in various digital media is of prime importance. For maximum versatility, we have proposed UI based on a smartphone form factor.

User Journey

DECODE is envisioned to serve a broad variety of services. Nevertheless, the core process of sharing data is the common thread that ties these services together. While the exact process for each application will depend on the nature of the data and the general context, we propose the following generic steps for the process of setting entitlements by the user:

1. A user wishes to use a DECODE application or service. This application can then request attributes from the user.
2. The application directs the user to the DECODE app, where the following visualisations appear. The interface clarifies what data is being requested, which attributes the has or not, and which granularity of data is applied and shared.
    a. Attributes: the user views a list of requested attributes intersecting with the selected context. If the application requests an attribute that the user is missing, they are able to add it to their local app.

   b. Values: under each attribute description (e.g. Date of Birth), the user will see the actual data that is proposed to be shared (e.g. 14/10/1986 or 1986 or 1980-1989), depending on the context selected.

   c. Available context: applying a context to the attribute request can change both the list of attributes that will be shared and the value of selected attributes.

3. Upon creating a satisfactory match of attributes and context, the user accepts the policy visualized in the app.

4. After submitting their preferences, the user receives positive confirmation that their request has been received and that their desired policy will be applied. This can take the form of:

   a. Submitting a smart contract to the distributed ledger and that it has passed validation.

   b. Submitting a smart contract to the distributed ledger and awaiting confirmation that it has been processed and added to the chain.

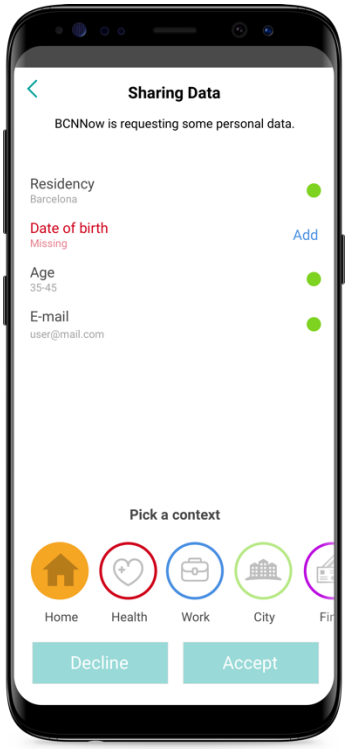
   c. Submitting their preferences to another application-specific store, where the policy will automatically be applied and where the user can audit the results.

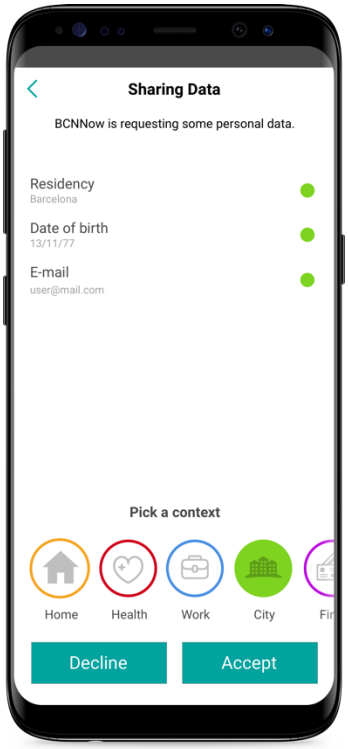
For a concrete example of the role of context, consider the case of using DECODE to sign up for a neighbourhood social group. The nature of this group may require users to verify their residence in the neighbourhood, as well as a minimum age requirement. The user is now empowered to apply different contexts that reflect how they want to define their relationship with this group.

- Is this a close support group of trusted peers? Applying the **Friends** context would share my name, full address and date of birth.

- Is this a group for managing administrative issues between neighbours? If so, I would apply the **Public Social** context and thus share only my neighbourhood and broad age range, but not my full name.

- Is this a forum for managing rent and community payments? I can authorise the **Financial** context in this case, giving the service legal identity data for the processing of payments.





User Interface Description

The format of the list view to visualise and personalise the precise attributes that are being shared has been tested with representative users of the DECODE platform. The main components of the screen are:

1. List of attributes requested by the application or service. Here, the user will see the description of the attribute, the actual value that will be shared, and an option to add missing attributes.

2. Context picker, from which the user will choose which context filter to apply to the data being shared. When applying a different context, the user will immediately see how the data share is updated.

3. Accept and Decline buttons for submitting the user's desired policy. Following mobile UI guidelines, these are placed at the bottom of the screen with the Accept button on the right (in left-to-right language locales), following conventional actions to continue a flow.

User Testing

Following software development best practices, we have run three rounds of iterative testing with users representative of our target audience. Users were selected from the meta-decidim community in Barcelona, with diversity in gender, age range, and technical knowledge. The methodology used during the test was semi-structured exploratory testing, in which users navigated a petition signing process while being asked for feedback on their understanding of the application. The first two testing sessions were conducted on a prototype, while users in the third session used the real Decode application. After each round, the conclusions and issues raised in the tests were analysed and used to inform the next stages of application development.

The general feedback from these sessions, which became more pronounced in later iterations, is that there is great value to simplicity. In each round of testing, users completed the flow with increasing ease. With their input, the design has gradually been simplified in terms of interface elements, texts and colours.

The main challenge raised by the user test was that of clarifying precisely which information would be shared and with whom. This was especially difficult when combining the Decidim website, the mobile app, and a credential issuer. In subsequent iterations, this was address with additional texts and imagery to clarify that the information submitted to the service is anonymised, even though a user may have been required to submit personal data to an external credential issuer.

Future Development & Extension

Application developers are encouraged to adopt both the principles (context and difference) as well as the practical elements (screen design) in order to maintain a consistent visual metaphor across DECODE applications.

Nevertheless, the nature of defining broad global principles may preclude us from finding the ideal implementation for each specific use case. However developers choose to apply these UX principles in their applications, we leave it to their judgement to decide whether these guidelines should be adapted for special circumstances. We understand there may be a trade-off between having consistent UX that users are familiar with in different interactions and the specific needs of a certain application or process dealing with specific personal data.

12 Research perspectives

The presence of context and preferences bound to them and operators may open up the possibility of introducing automated inferences made for instance by artificial intelligence mechanisms (AI) about one's privacy preferences. Self learning algorithms then can be studied and implemented to shape the privacy grid of a user according to different situations. To avoid false positives then it is important that the "self learning" algorithm is bound to some situations only (low sensitivity ones) and that high sensitive data is manipulated only from expert settings.

A Delta is the form used in mathematic and physics to denominate a range of value in which the precise one is located. This concept is connected with both the notion of measure and of requested precision in calculations. A lower precision of data can be an optimal solution for most of the DECODE pilots observed and we assess that this range could be used as a feature in the DECODE client or directly inside the Zenroom. This allows to design the passage of data between applications to be compliant to the needs of privacy by design. Some examples:

- How many people are in a certain area approximated by radius
- How many people live in a certain neighbourhood

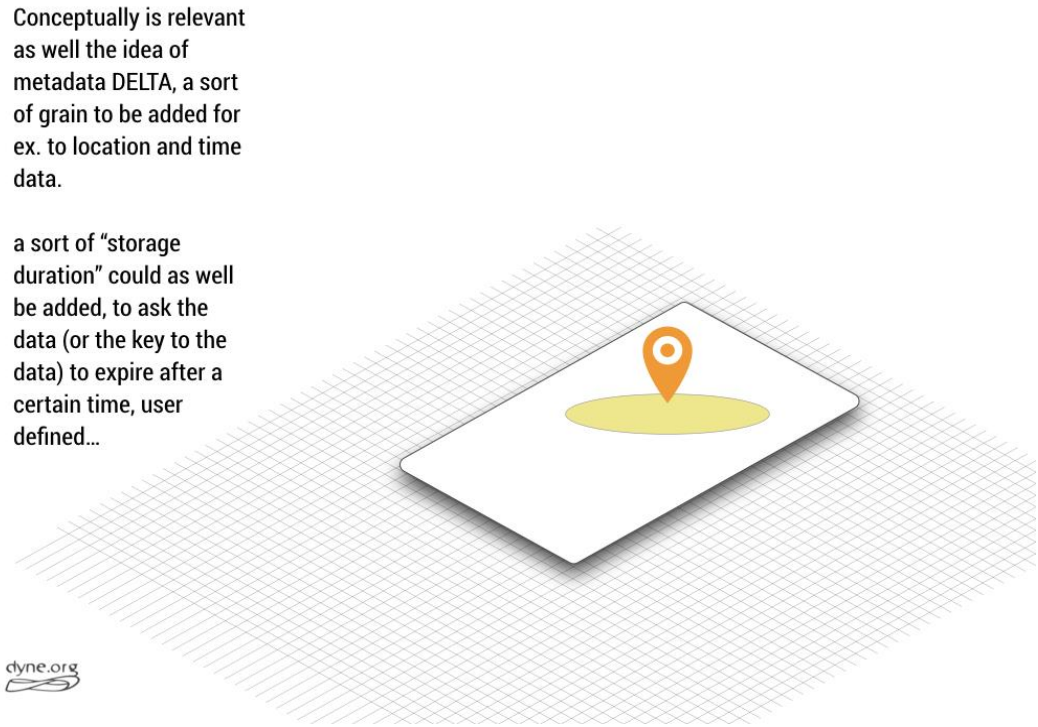


Figure 20

In a similar fashion privacy settings can be evinced in many cases adding a delta on time, or better variating the precision on the time sample. The delta on time has to be announced and quantified: this data is issued with a delay of 5 minutes or precision on this time is +-3 days). This very well applies to the DECODE/IoT pilot needs.

More information on DECODE's pilots is available in D3.5 and research continues in order to match their particular cases with a final implementation included in the DECODE mobile client. For the purpose of completeness we will include here a brief analysis of the private attributes requested by the DECODE/Decidim pilot.

In this case, data subjects (people, participants) will entitle the Barcelona City Council to verify their private attributes (date of birth, place of residence, etc.) and we suggest that Decidim data controllers do not have to necessarily access this data but only the crypto signatures of the attributes: that may suffice to manage petitions lifecycle and participants signing them.

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 1 Decidim pilot entitlements

13 Bibliography

Dragona, D. (2016) *From community networks to off-the-cloud toolkits art and diy networking*.

Foucault, M. (1966) *Les mots et les choses: Une archéologie des sciences humaines: Une archéologie des sciences humaines*. Gallimard.

Kranenburg, R. van (2017) Council: The emergence of an iot think tank. *IEEE Pervasive Computing*. 16 (4), 22–24.

McDonough, T. (2004) *Guy debord and the situationist international: Texts and documents*. MIT Press.