



decode

**Design &
implementation
interface for smart rules**





Project no. 732546

DECODE

DEcentralised Citizens Owned Data Ecosystem

D4.9 Design & implementation interface for smart rules

Version Number: Interim

Lead beneficiary: TW

Due Date: June 30th

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

Editors and reviewers: Denis Roio (Dyne.org), Oleguer Sagarra (IMI), Marco Ciurcina (NEXA), Guy Samuel, 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)	

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

Table of contents

1 Introduction	3
2 The challenge of diversity.....	5
3 Inspiring projects	6
4 Privacy in context	7
5 A new look at the Internet	9
6 Recognising the situation	12
7 Sketches of the privacy choser app.....	13
8 Visualisation in the Zen Room	17
9 Flow analysis	18
10 Differences are meaningful	20
11 Wearing hats	25
12 Research perspectives	26
13 Bibliography	28

1 Introduction

This Deliverable is an intermediary outcome of T1.4 “Graphical interfaces design for DECODE OS and for smart contracts”.

A core theme within DECODE is to put the citizen at the centre of control of how has access to their data and for what purpose. Key to this is that we invert the current world of large corporations possessing the control and push control back to the individual. DECODE allows the individual to create an “entitlement” that codifies the terms and agreement to access and use the individuals data.

The core objective for this work is based on the rational that while sharing potentially privacy sensitive information according to consensual choices, a good user experience is paramount to make sure citizens have trust in the DECODE ecosystem¹. The consequences of users’ actions should be clear at all points, demanding transparency and accountability in order to defend the right to privacy of the individual. An inclusive design, in which the end user is fully informed and empowered is one of the core values of the whole DECODE project.

This Task will determine the functionality to be exposed for user profiles and user needs; what the system needs from the user and what the users need from the system. The design of the interface will enable users to edit and generate their respective contributions and requests data, i.e. provide the input for the entitlements generation.

When setting up “privacy preferences” in online platforms many are the things usually listed to define the level of access to information about individuals. 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 – usually large corporations- 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 start from the difficult to make

1

The nature of this deliverable is technical and its core contribution to the DECODE project consists in a prototype implementation made available here: <https://zenroom.dyne.org/entitlements-ux/> This is still work in progress and it is published as INTERIM: to be completed in the coming months with the contribution of task leader Thoughtworks. The objectives of this work consists on (i) proposing a general visual habitat for the DECODE design; (ii) proposing the simplest possible metaphor for privacy preferences in DECODE; (iii) sketching a usable entitlement application for DECODE

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.

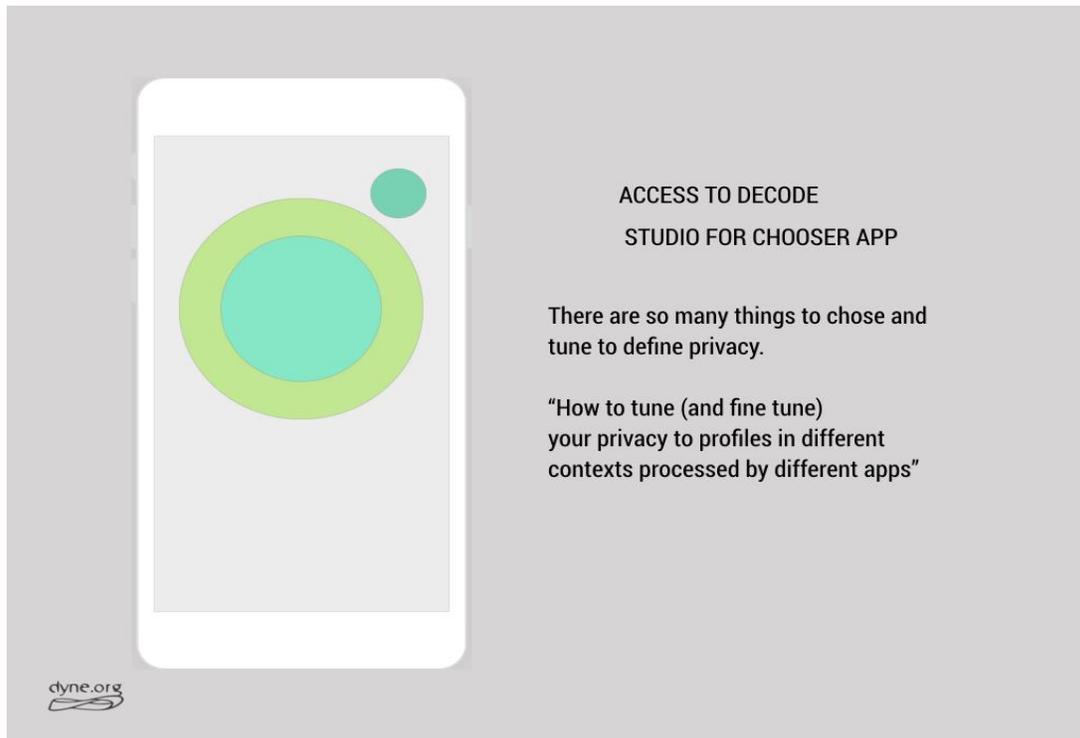


Figure 1

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 and 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.



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 where 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. Imagine all there is : - applications, simple or complex, whatever device powers them, whatever computation they run upon - a space where 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:

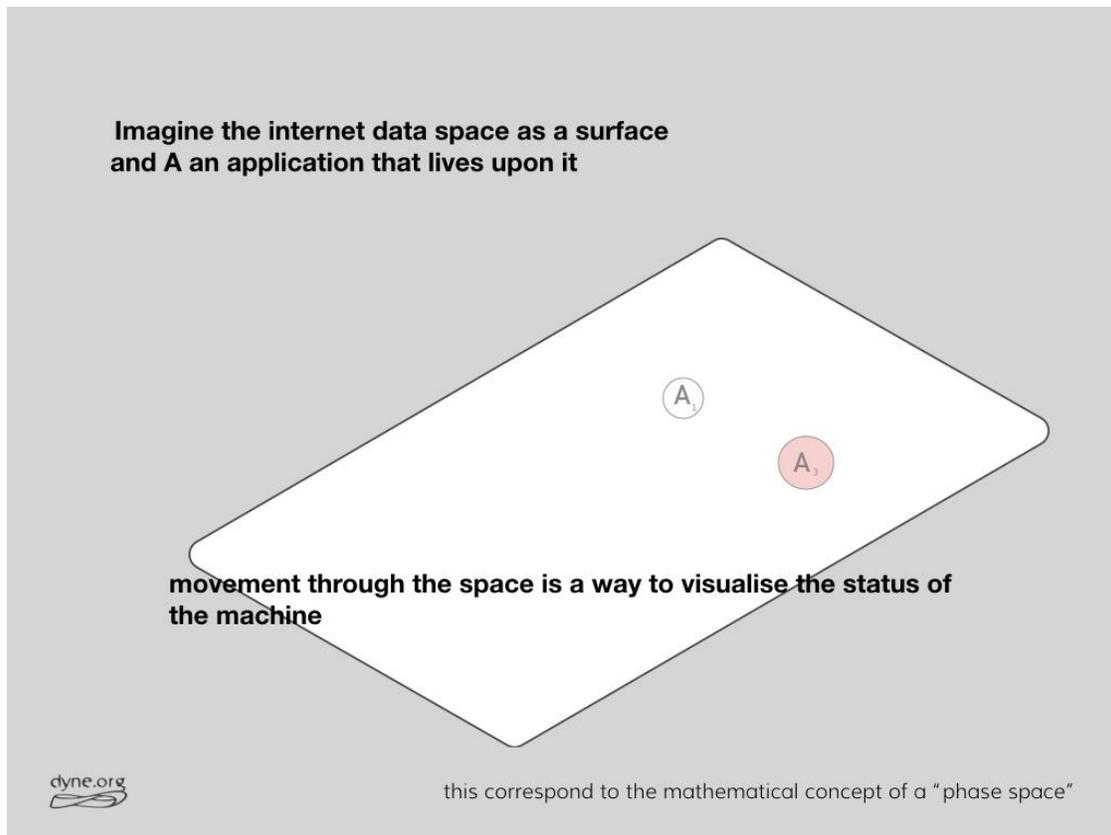


Figure 3

So what DECODE boils down to? a **sublayer** to this space where 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.

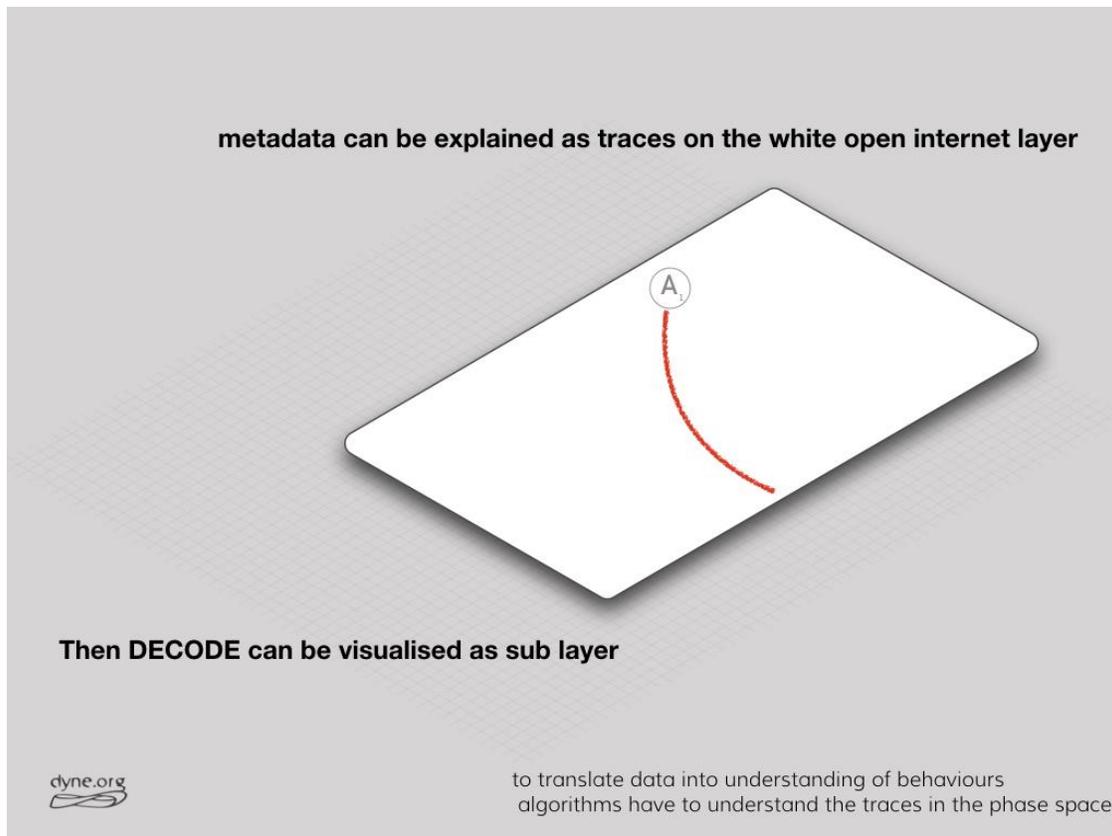


Figure 4

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 where the result may, or may not, include transactions of all types. Transactions that can be forgotten or recorded on a distributed ledger.

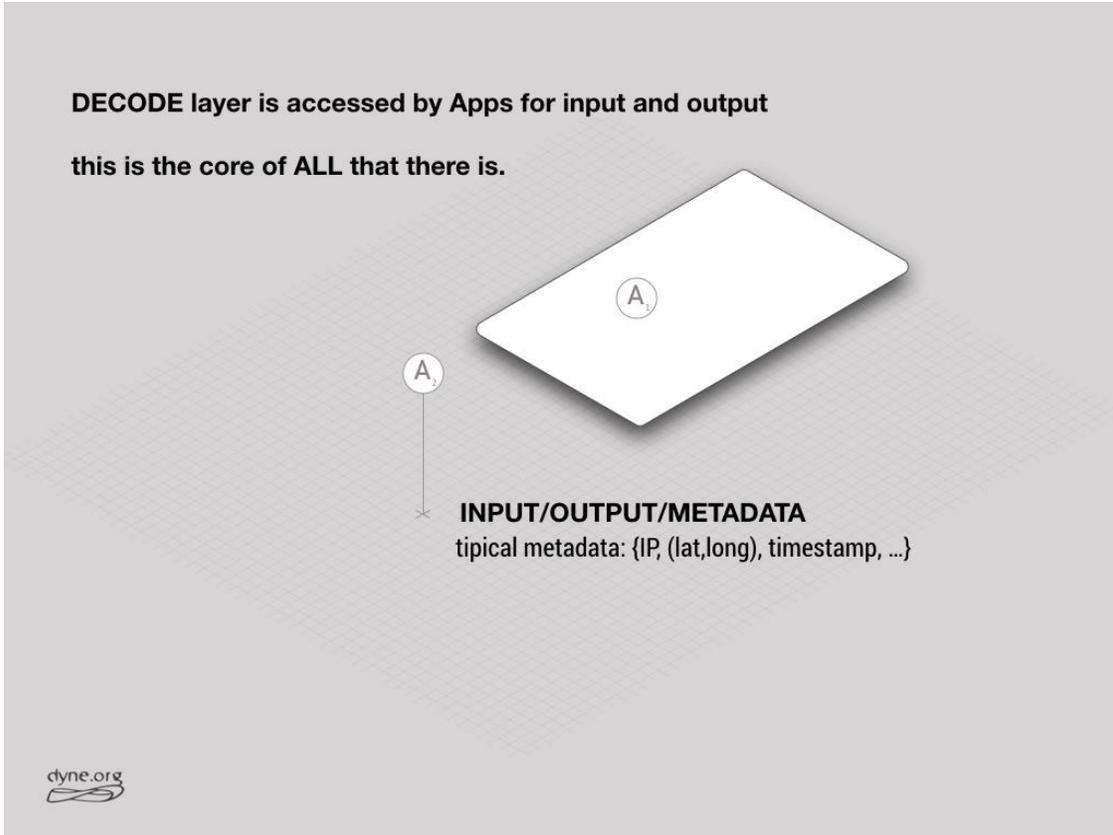


Figure 5

6 Recognising the situation

A situation is a concept mutated from art. It calls for a triadic logic. By triadic is implied that at least three 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. Theater, 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 prefer 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.

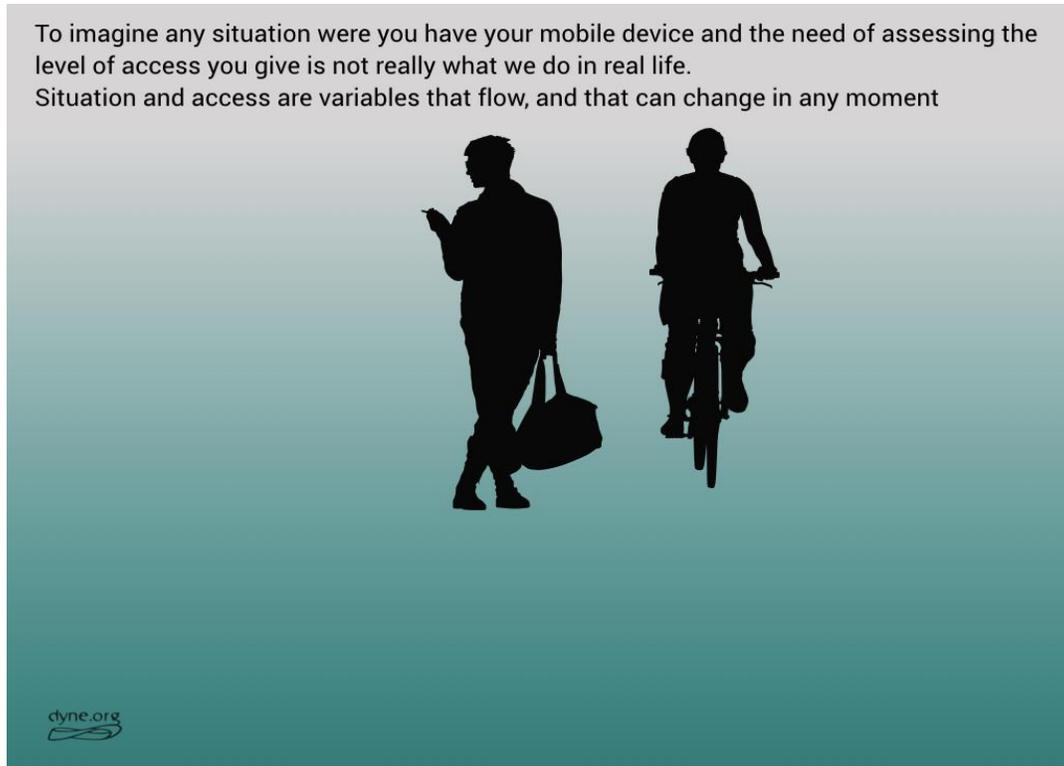


Figure 6

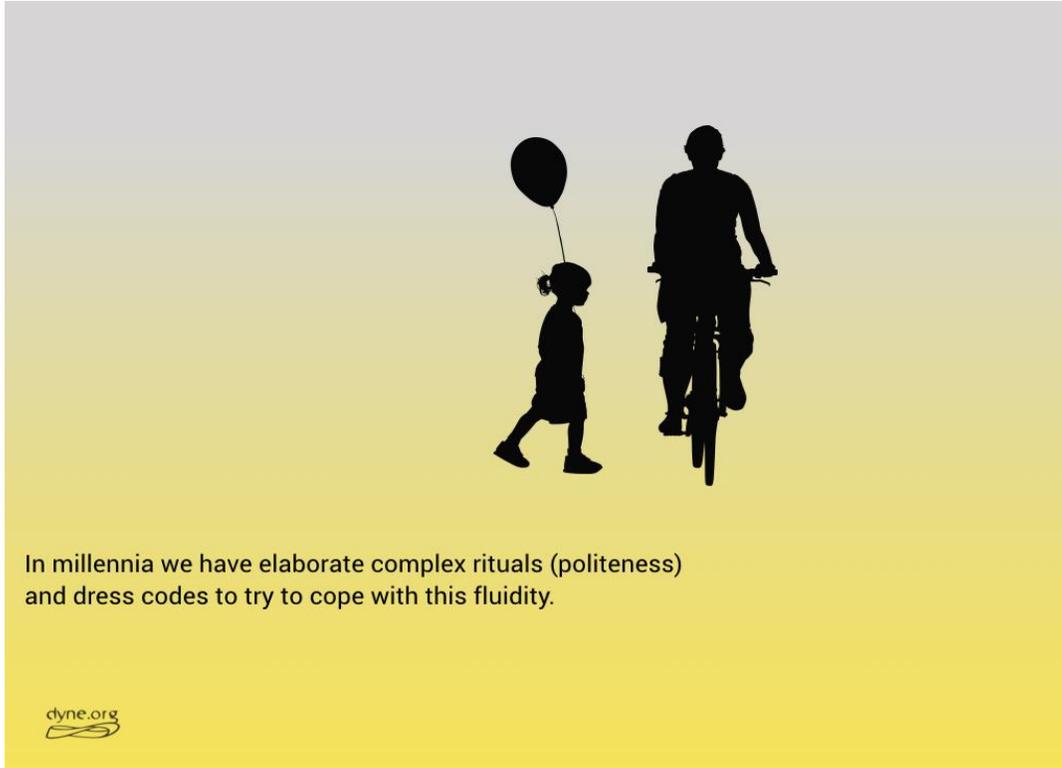


Figure 7

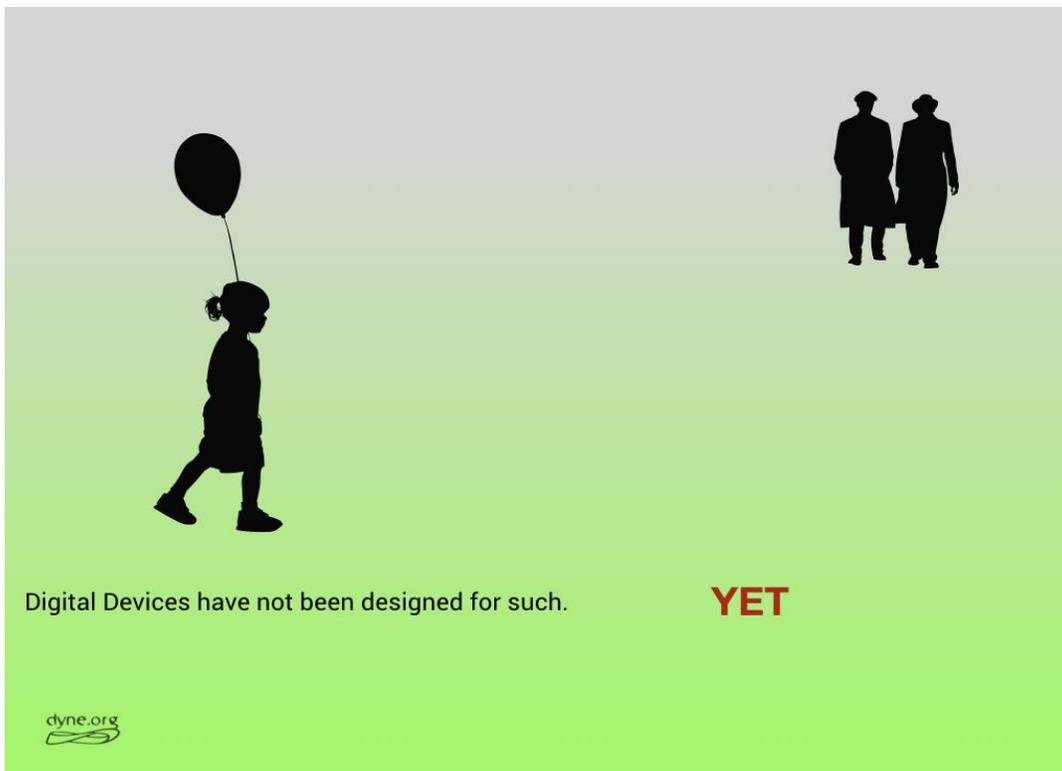


Figure 8

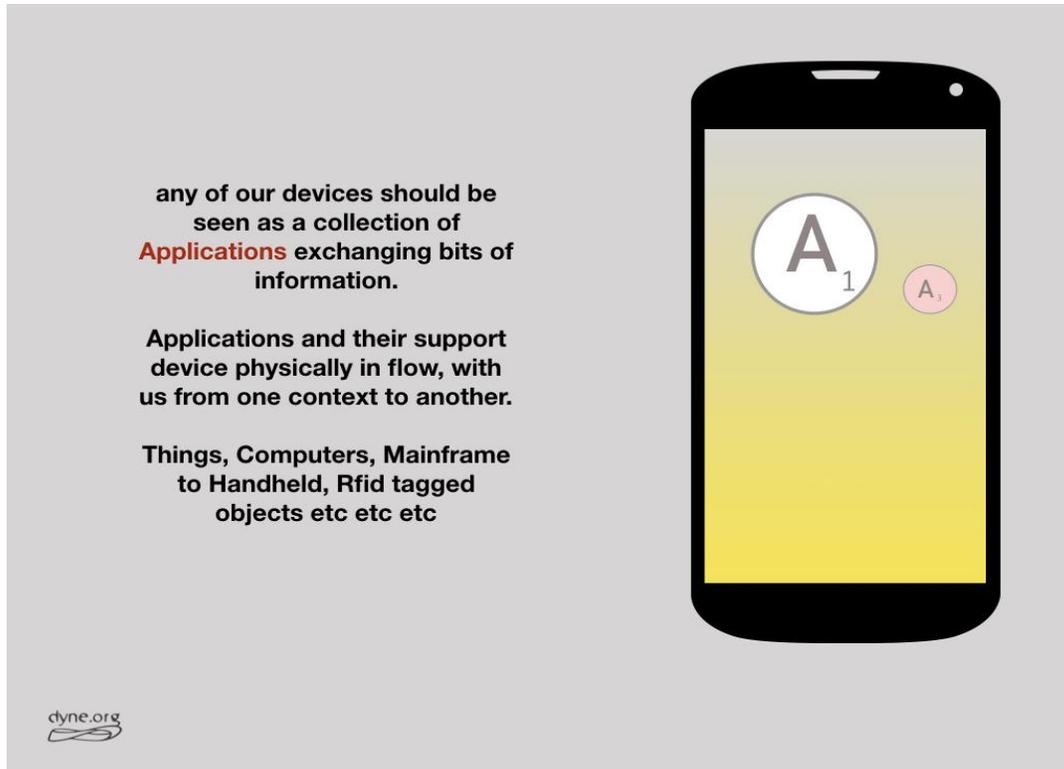


Figure 9

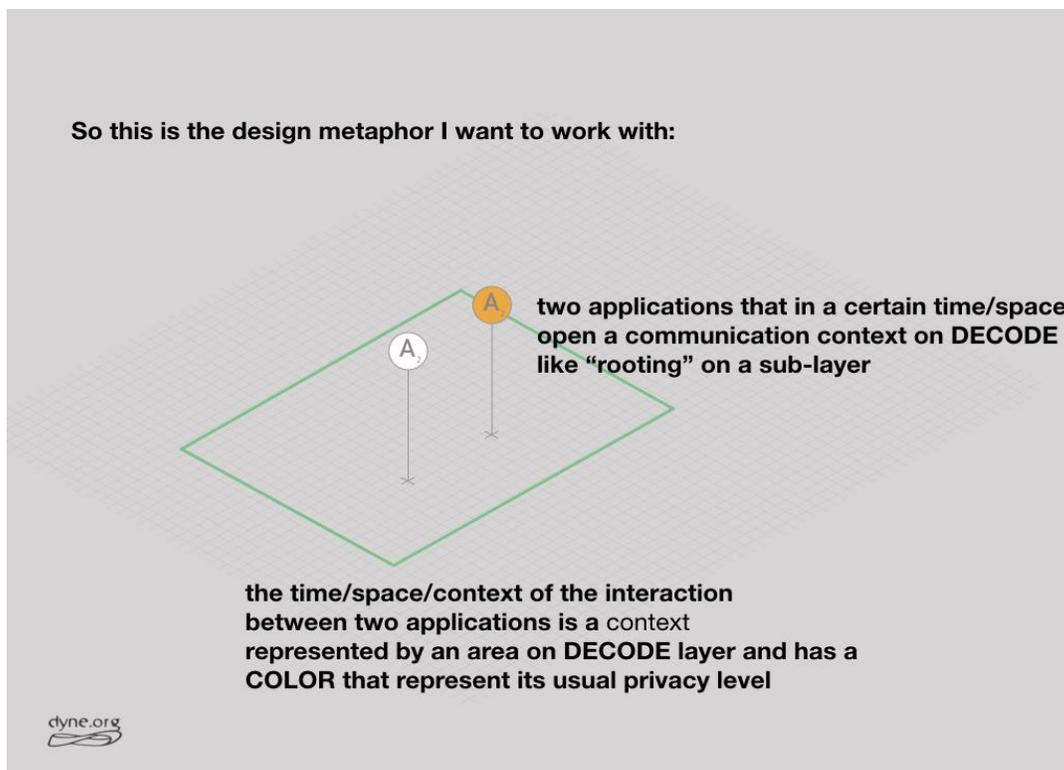


Figure 10

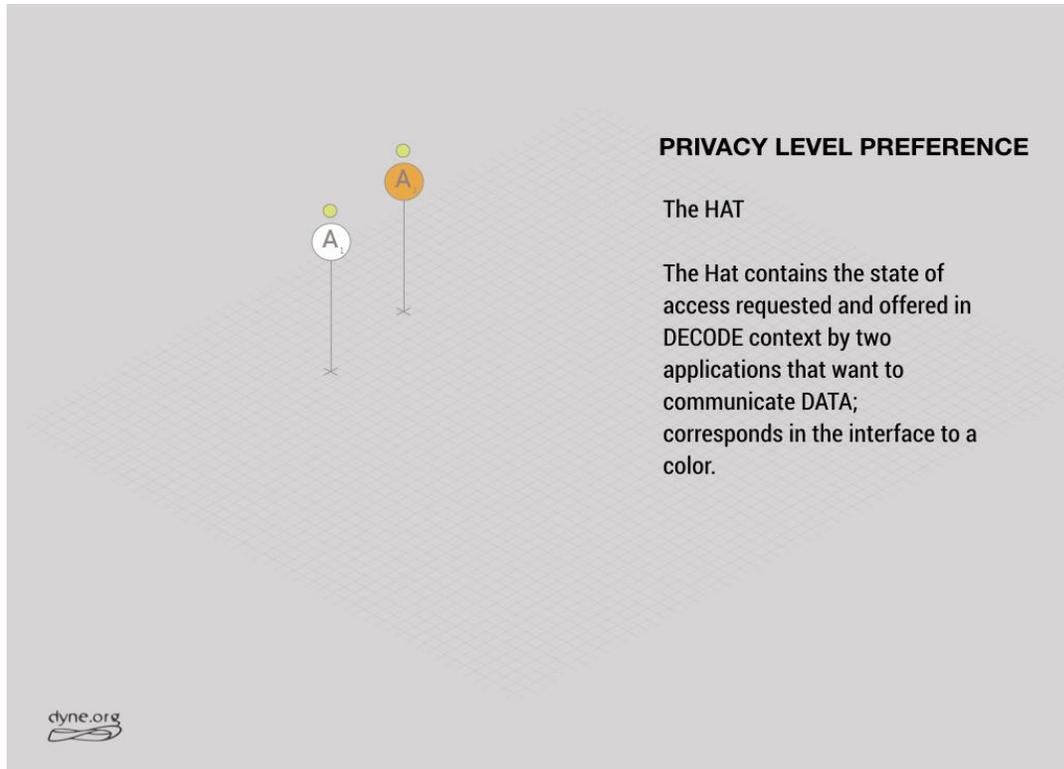


Figure 11

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.

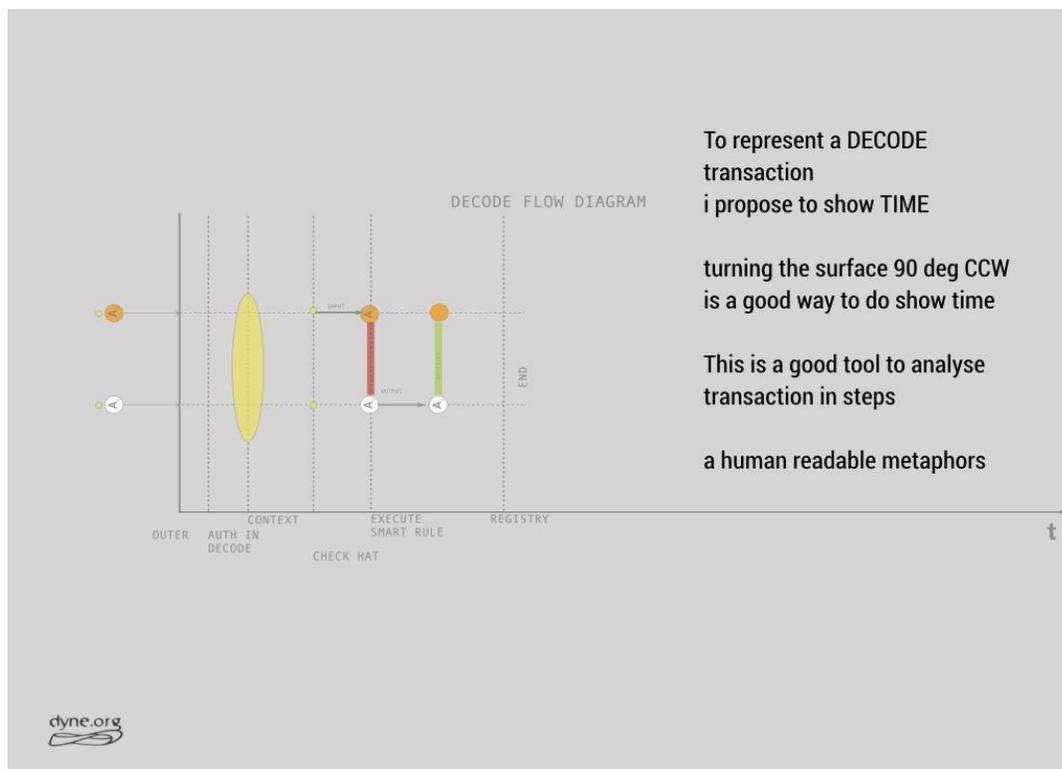


Figure 12

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 approach 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 could 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:

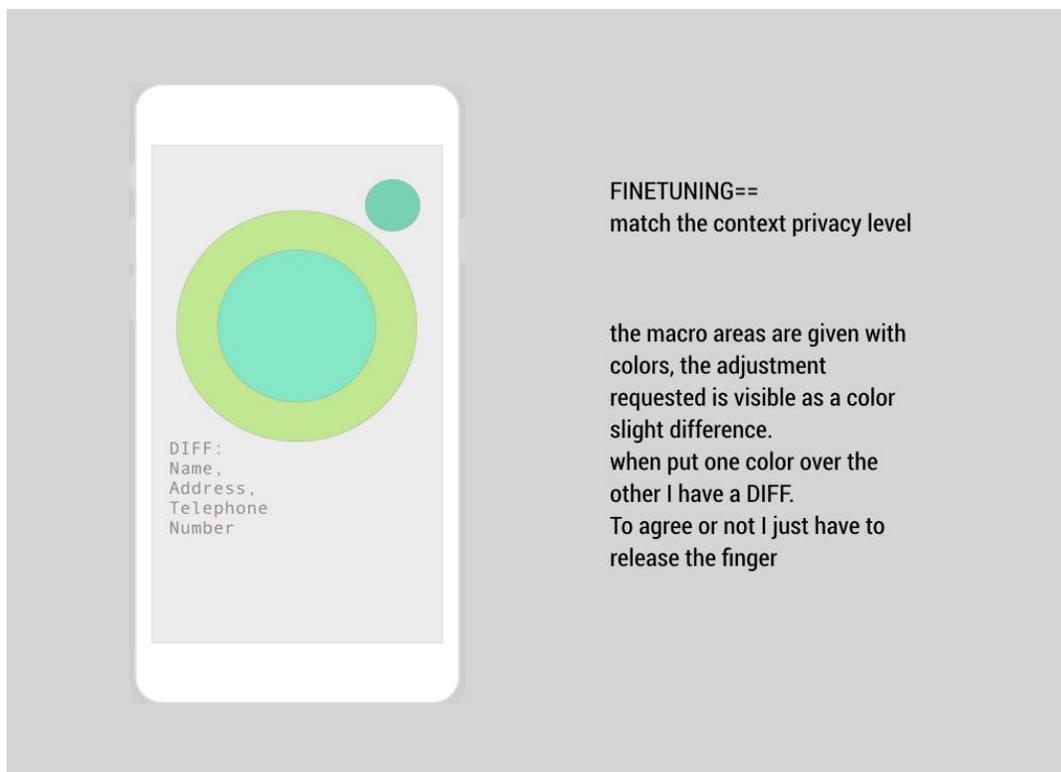


Figure 13

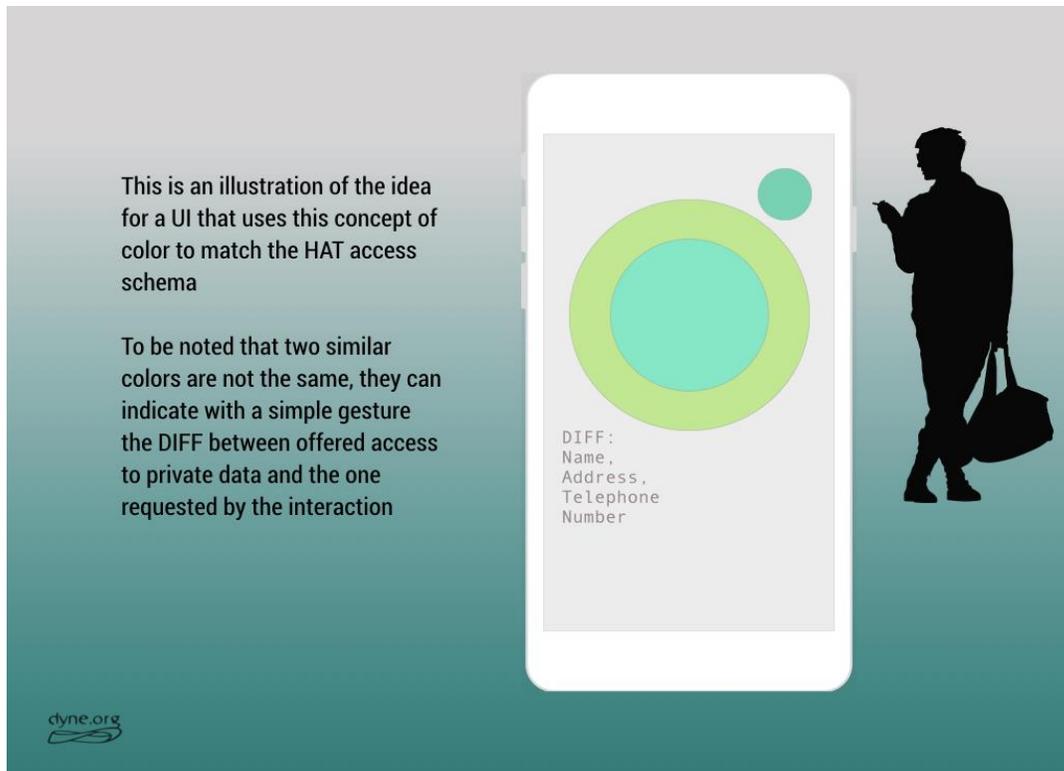


Figure 14

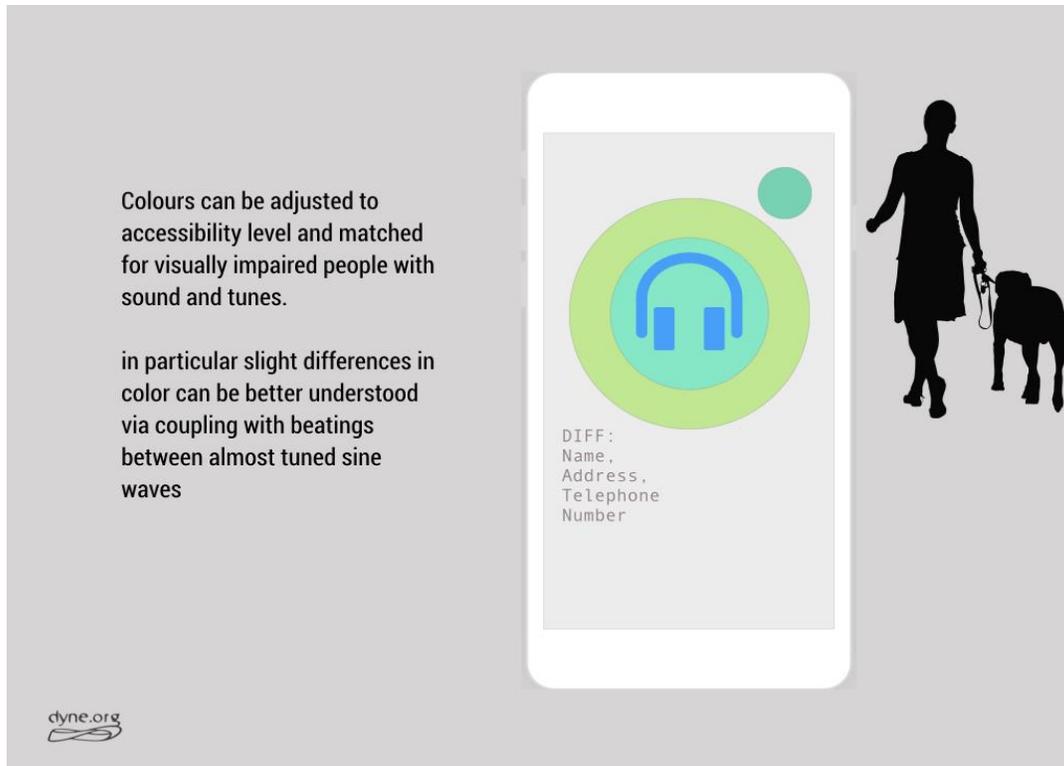


Figure 15

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

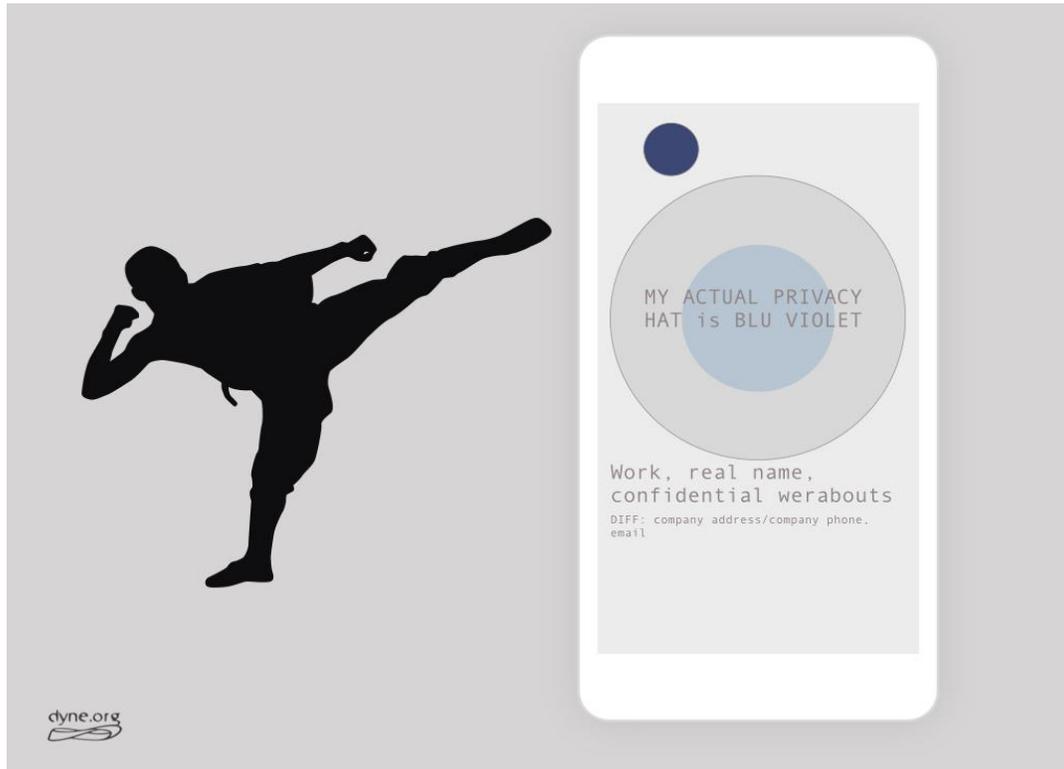


Figure 16

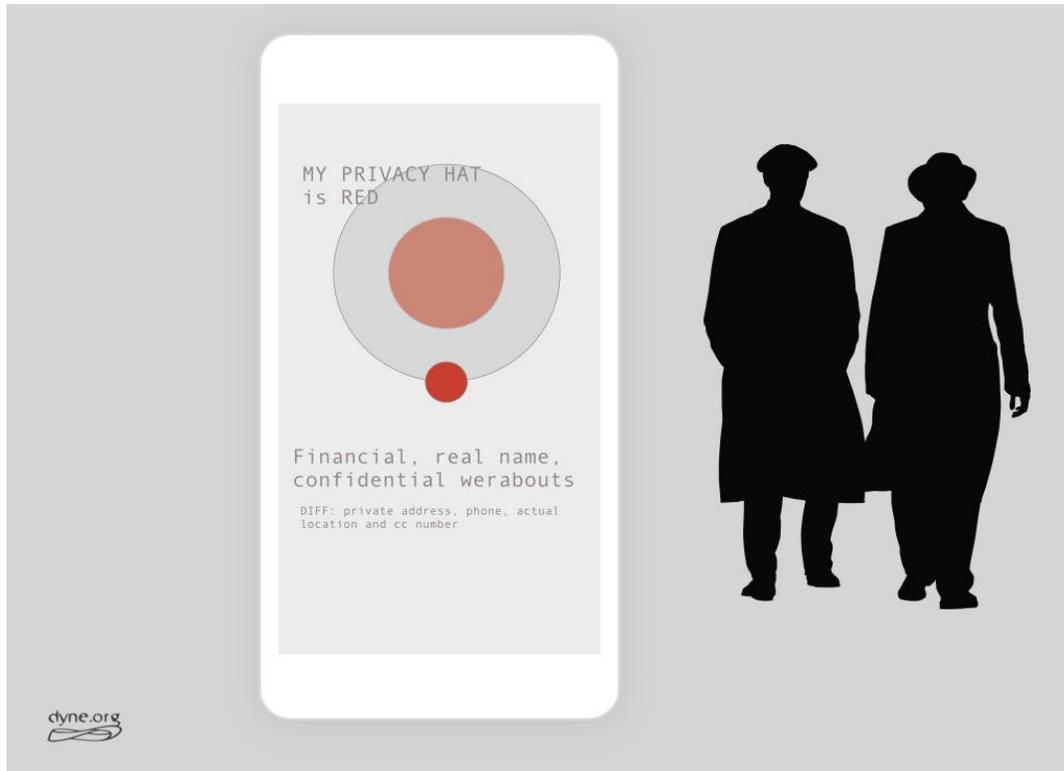


Figure 17

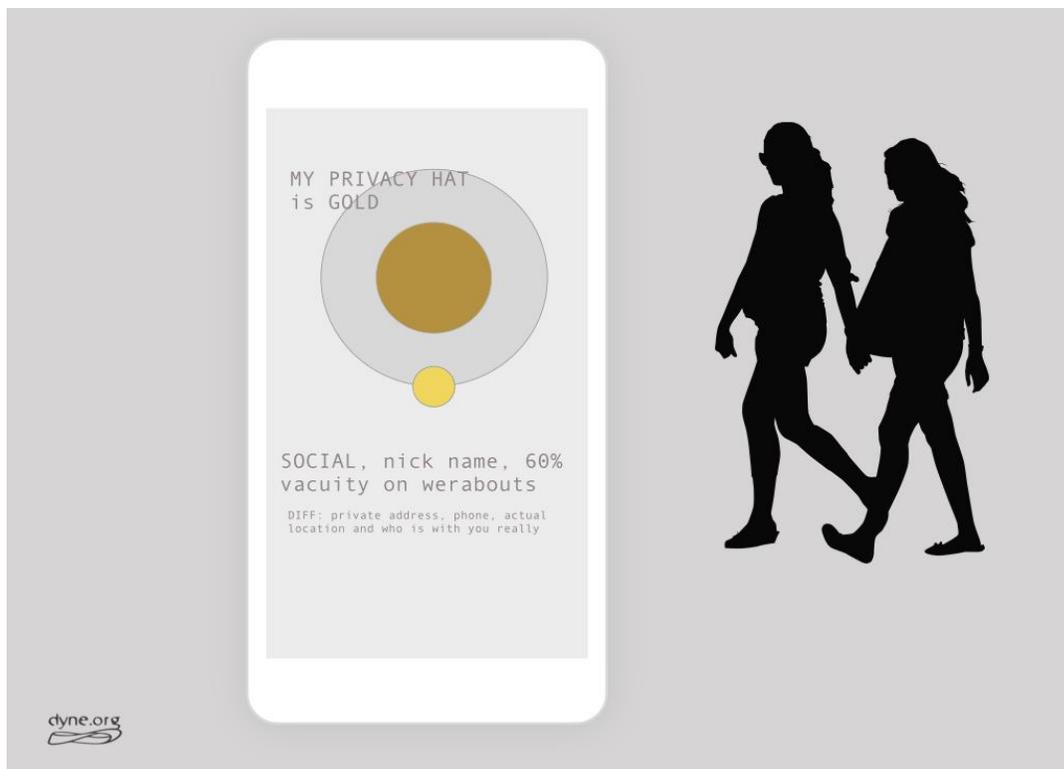


Figure 18

And settings that one may consider default:

CHOOSE 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 Wearing hats

A first implementation of the concepts explained above has been made conducting a development iteration in cooperation with DECODE partner Waag also in charge of this Task. The work lead to the data generator and a rough but effective implementation of the scheme using the visual language “Processing”, linked at the beginning of this document and here: <https://zenroom.dyne.org/entitlements-ux/entitlements.html>

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

Conceptually is relevant as well the idea of metadata DELTA, a sort of grain to be added for ex. to location and time data.

a sort of "storage duration" could as well be added, to ask the data (or the key to the data) to expire after a certain time, user defined...



dyne.org

Figure 20

In a similar fashion privacy settings can be evinced in many cases adding a delta on time, or better varying 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.