Enhancing Transparency and Consent in the IoT

Victor Morel

Sustainable Computing Lab

contact@victor-morel.net

25^{th} June 2021

Outline

The Internet of Things

- Growing infrastructure
- Numerous devices, various uses
- Limited capacities and interfaces
- Different types of data collected

Privacy concerns in the IoT

Personal data collection

- → Risks of surveillance and abuse of targeted advertising
- → Specific issues raised with the IoT
- → Difficult to comply with regulations

General Data Protection Regulation

GDPR

- Most recent legal framework for personal data protection in Europe
- Extra-territorial scope: impact outside Europe as well
- Introduces rights for data subjects (DS)
- And obligations for data controllers (DC)

Bundle of principles:

- Lawful, fair, and transparent processing
- Purpose limitation
- Data minimization
- Safe storage
- Accountability of DC

Emphasis on information and consent

Information

Information must be:

- Accessible and intelligible
- Concise
- Transparent

Content:

- Identity of DC
- Type of data
- Purpose of processing
- Legal ground
- Recipients of data
- Third parties
- Retention time
- Rights of DS

Consent

Consent

- One of the six legal grounds
- Unlike other legal grounds, requires DS implication
- DC must be able to demonstrate its obtention

Valid if the following conditions are met:

- Informed
- Free
- Specific
- Unambiguous

Of the difficulty to comply

It is difficult to comply with regulations in IoT environments

- IoT devices are numerous, ubiquitous, with heterogeneous uses
- Low computational capacities, passivity, inappropriate interfaces

Information issues

- Declaration of devices
- Reception of information
- Intelligibility of information

Consent issues

- Expression of choices
- Communication of consent
- Demonstration of valid consent

Our objectives

Objectives for information

1. Systematic declaration
2. Reception of information
3. Intelligible presentation

Objectives for consent

4. Expression of choices
5. Communication of consent
6. Demonstration of consent

Global approach

- Using machine-readable privacy policies for information and consent
- DC privacy policies for commitment (DCP)
- DS privacy policies to define choices (DSP)

Outline

User-friendly information

Limited number of solutions for the IoT

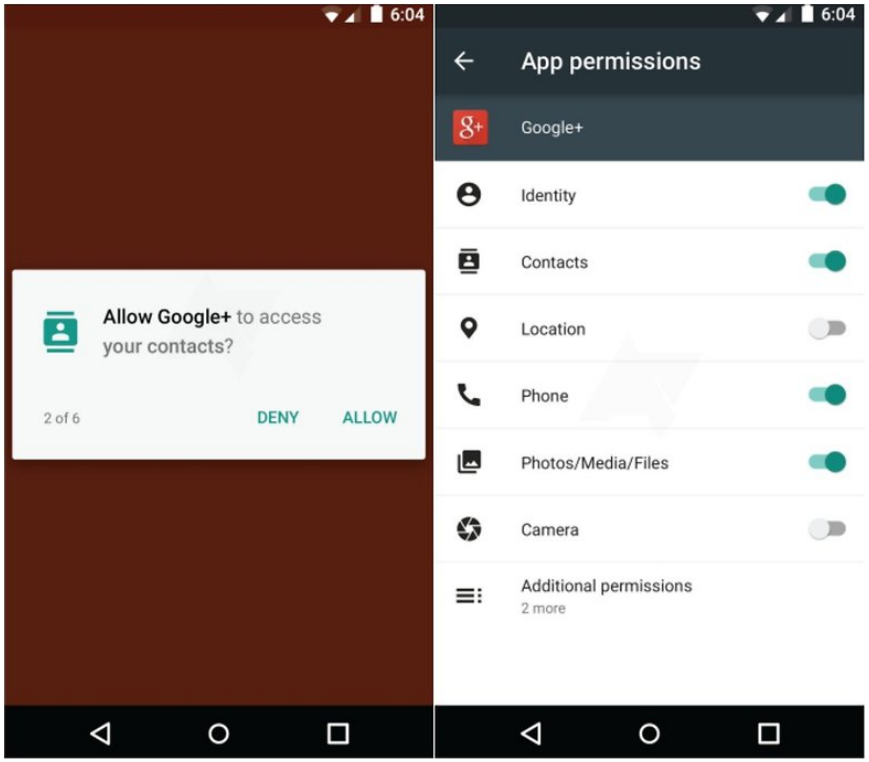


Figure: Android Permissions

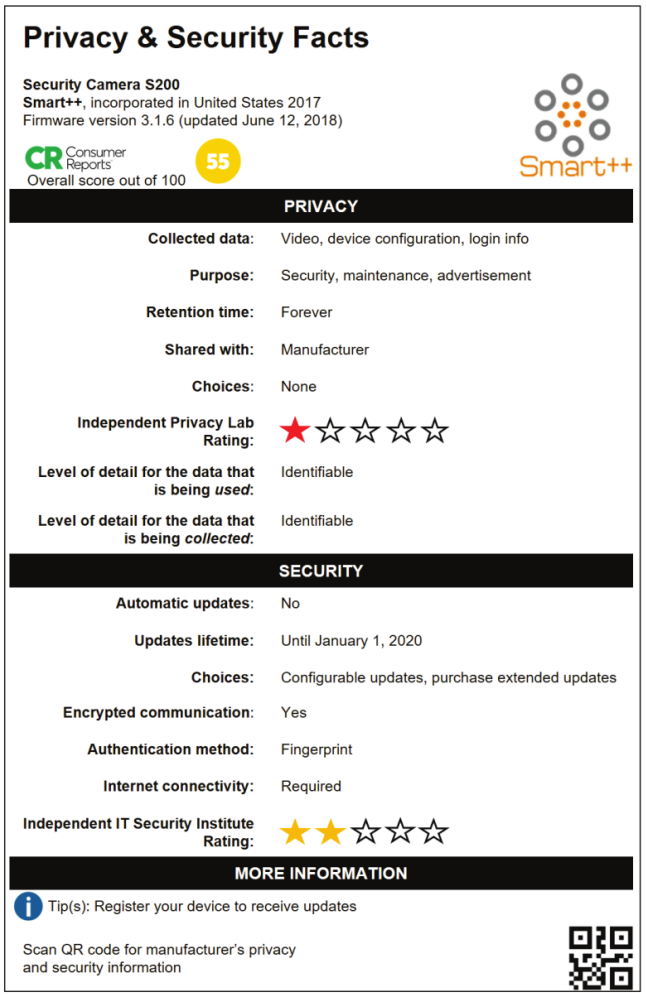


Figure: Prototype IoT Label

Machine-readable information

Often privacy languages

- Set of syntax and semantics used to express policies
- Not always formally defined

P3P

- Privacy preferences in XML format
- Did not meet the expectations
  - $\rightarrow$ Notably because of ambiguities and coarse policies

Pilot

- Tailored to the IoT
- Formal semantics

Outline

Privacy assistants

In a nutshell

- Agents acting on behalf of DS
- Communicate with the environment (other devices)
- Privacy preferences are in a structured format

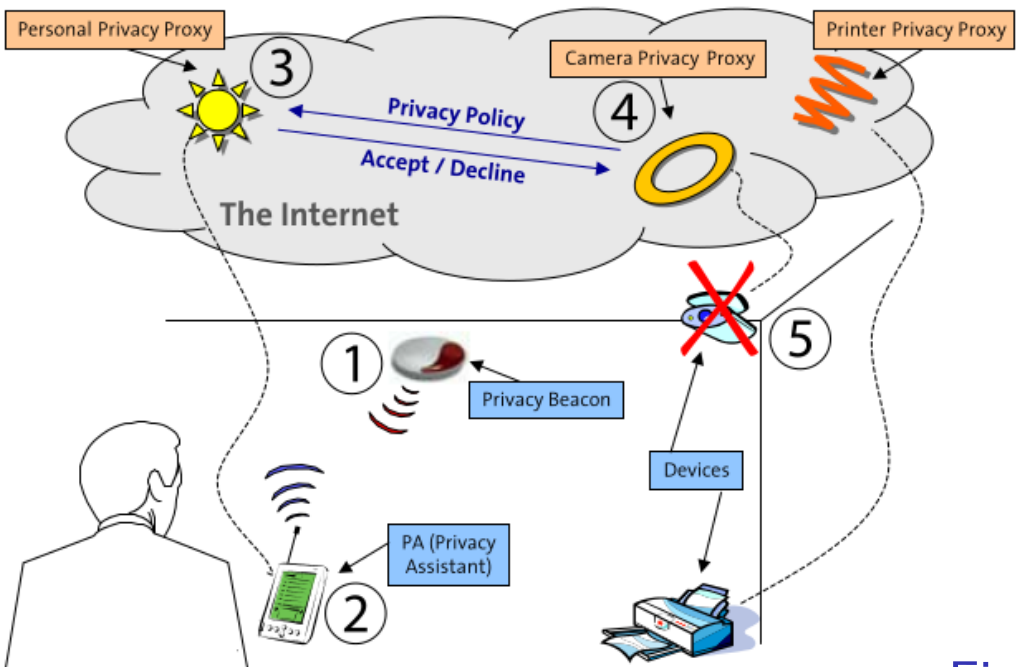


Figure: PawS by Langheinrich, 2002

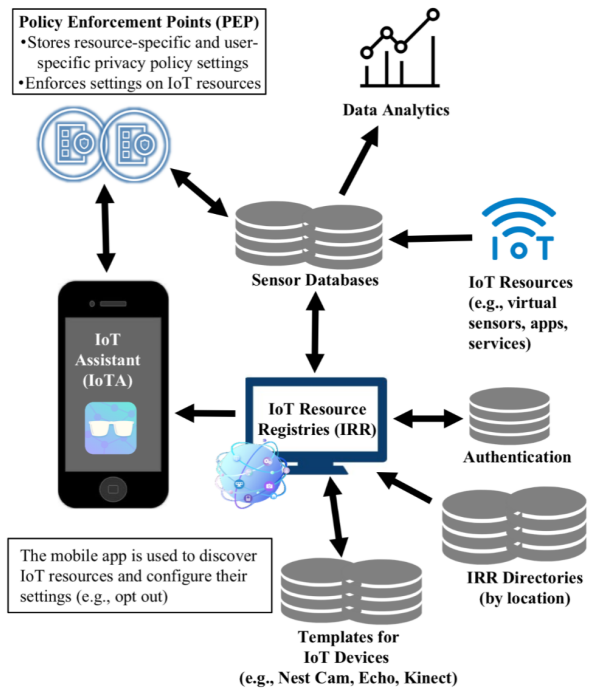


Figure: Personalized Privacy Assistant by CMU

Opt-out facilities

Opt-out

- Weak version of consent
- "Yes or No" to data collection
- Yes by default
- Not compliant with the GDPR

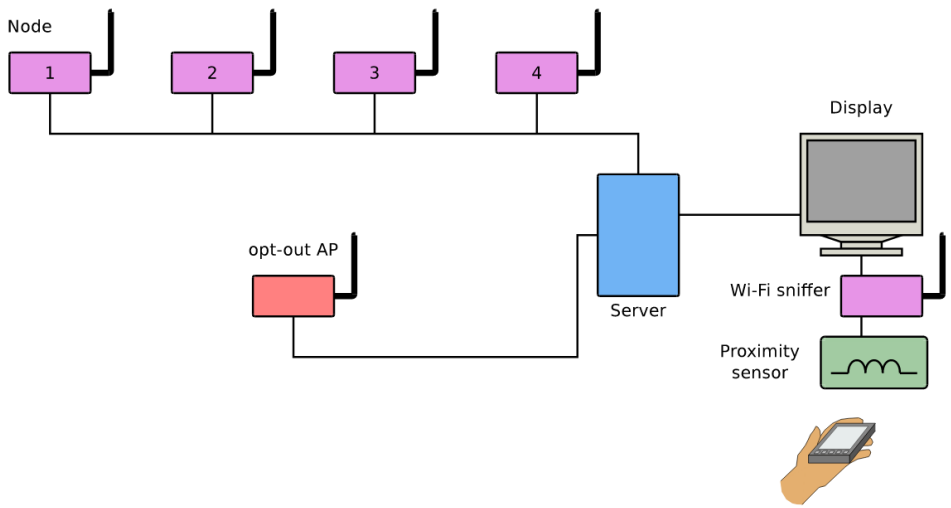


Figure VII.1 – Architecture of the Wombat system in a demonstration configuration.

Figure: Wombat by Matte and Cunche[1]

[1] "Wombat: An Experimental Wi-Fi Tracking System".

Outline

Framework

A framework for information and consent in the IoT

- Generic (different possible implementations)
- User-friendly
- Addresses legal compliance
- Does not require heavy modifications of existing infrastructures
- Composed of mandatory and optional requirements

Global functioning

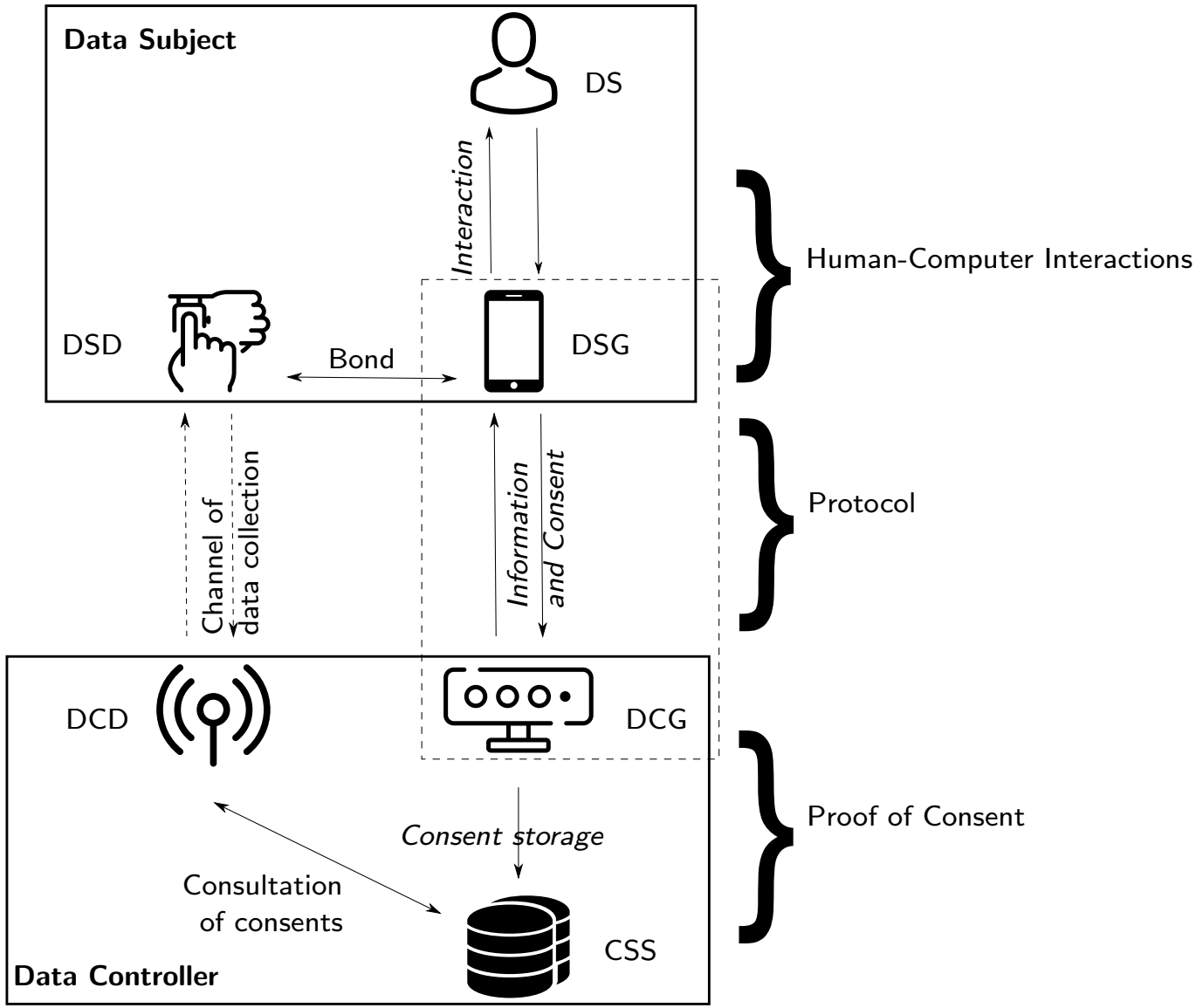


Figure: Explanatory diagram of the framework.

Messages exchanged

Privacy policies

- A DCP is a commitment, a DSP is a set of requirements
- $policy ::= (rule_1, rule_2, \ldots, rule_i)$
- DCP rule: *"Interparking requests your license plate for improvement of service purposes, and stores it for 14 days"*
- DSP: *"I agree that my license plate is collected for improvement of service purposes by interparking, and stored no more than 7 days."*
- Operations must be permitted: comparison and intersection

Other messages can be communicated

- Consent: {hash(policy), (ID_1, ID_2, ..., ID_i), signature}
- Dissent: $\equiv$ consent to a nil privacy policy
- Refusal, deny, and accept

Outline

Global presentation of the protocol

Privacy Policy Negotiation Protocol (PPNP)

- Defines the way communication happens between devices
- DS can negotiate the policy
- Defined through state diagrams
- And using sequence diagrams

Policies match

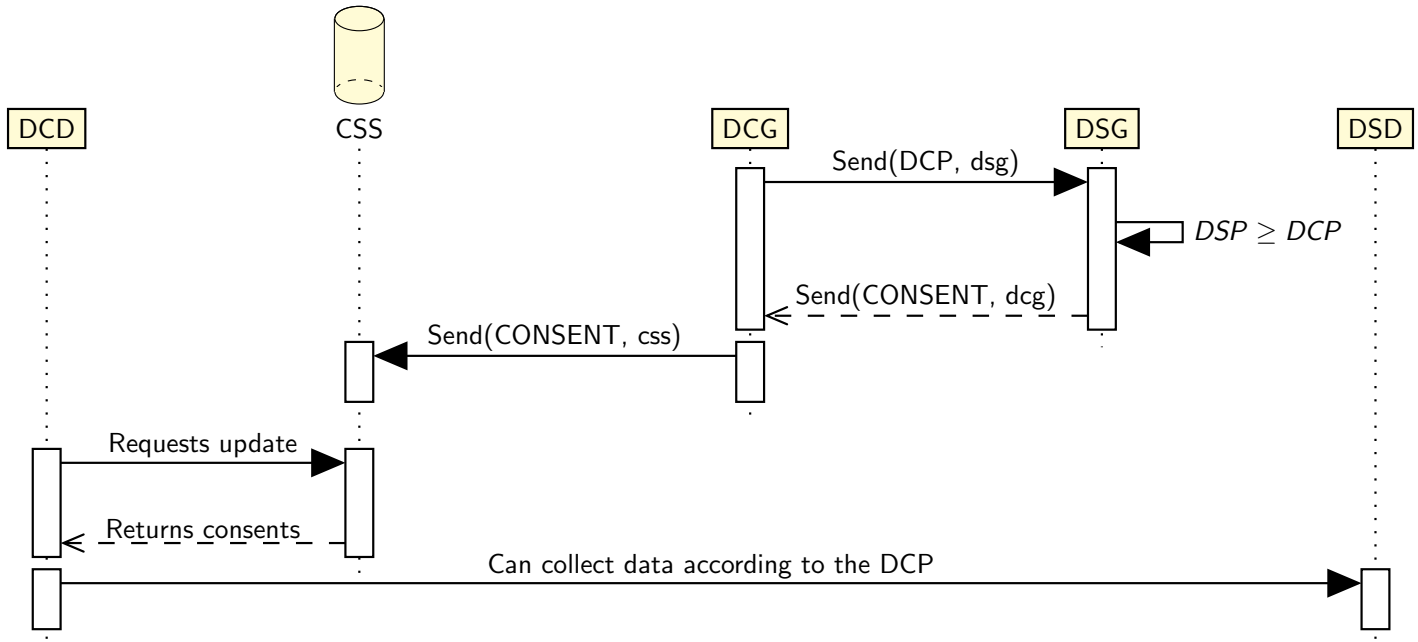


Figure: The policies match

Intersection

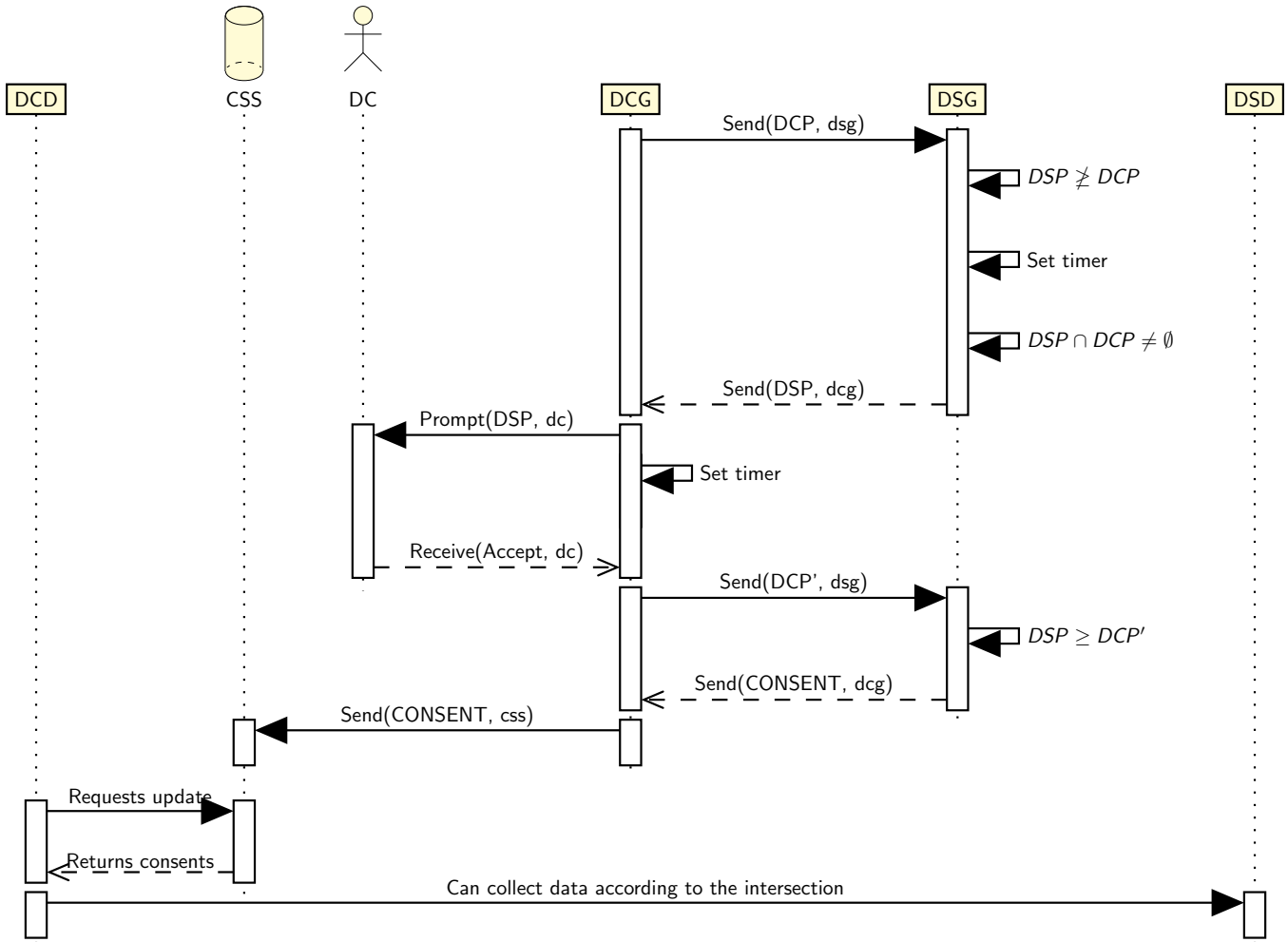


Figure: (Optional) The policies do not match, but an agreement is made on the intersection of policies

Dissent

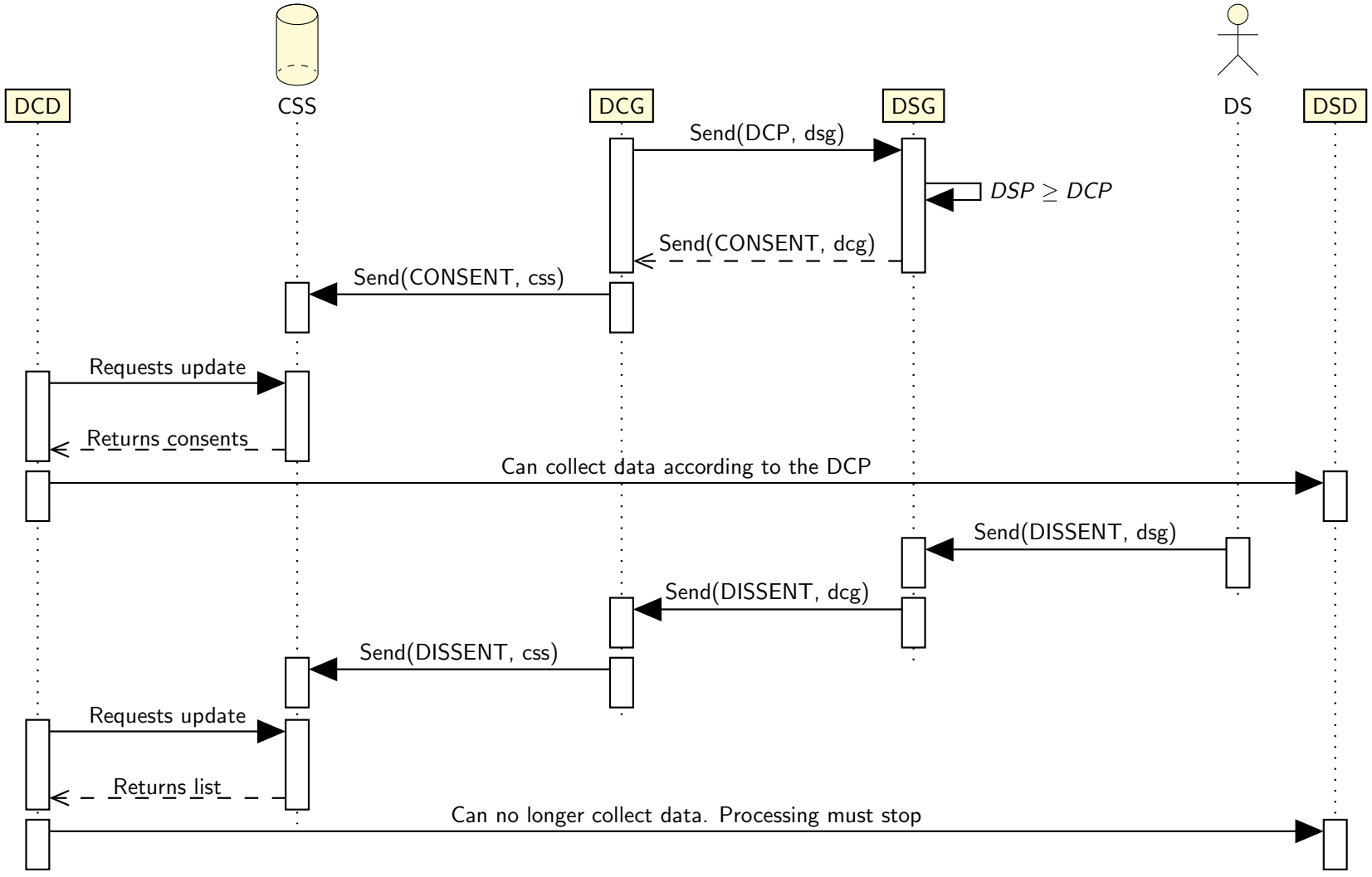


Figure: The data subject dissents

Outline

Personal Data Custodian

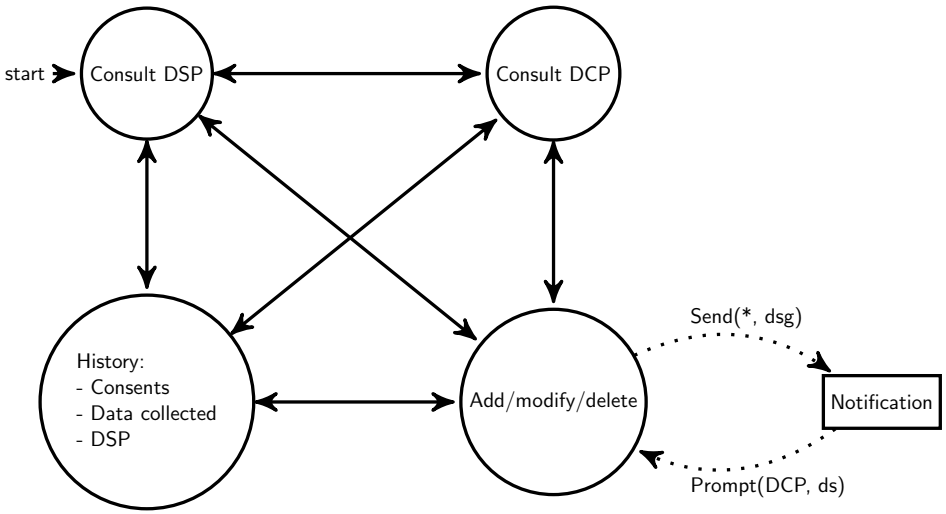


Figure: Global functioning of the *Personal Data Custodian*.

Consult DCP

Intelligibly presents privacy policies retrieved

Consult DSP

Consultation of one's own privacy policy

Add/modify/delete

Add, modify, or delete a privacy rule in one's DSP

Notifications

Considers interactions between device and data subject

History (optional)

To raise awareness about data collection

Outline

Direct communications

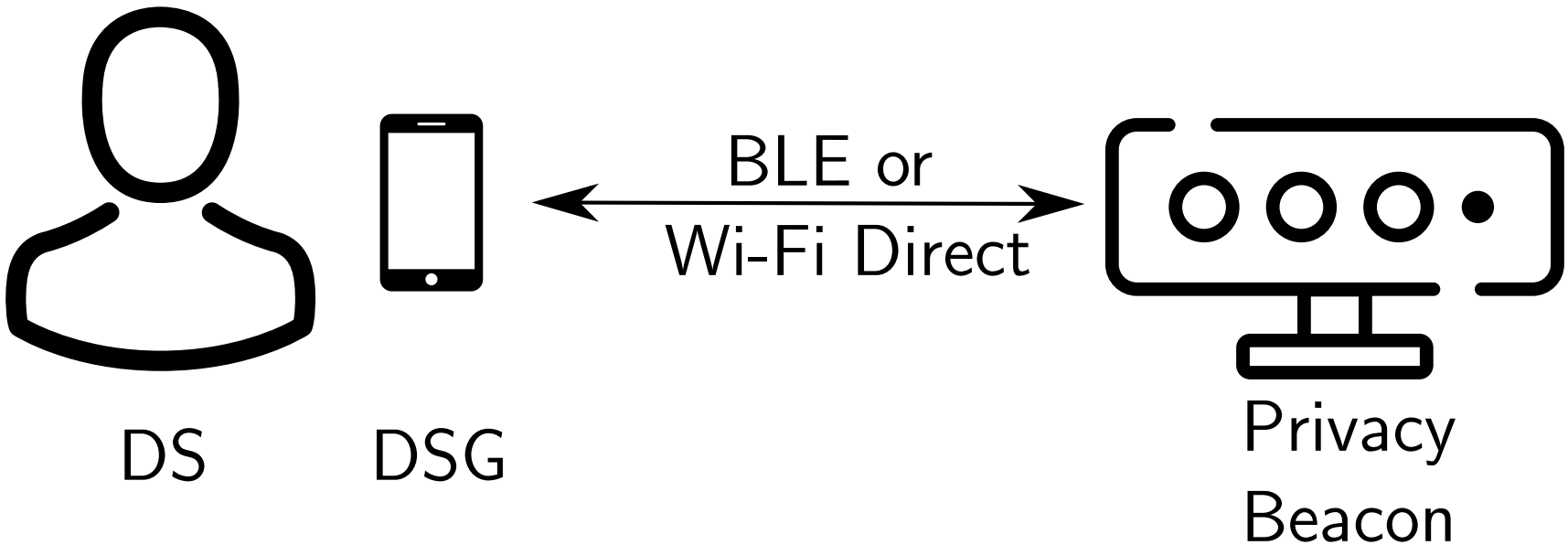


Figure: Example of direct communications.

Indirect communications

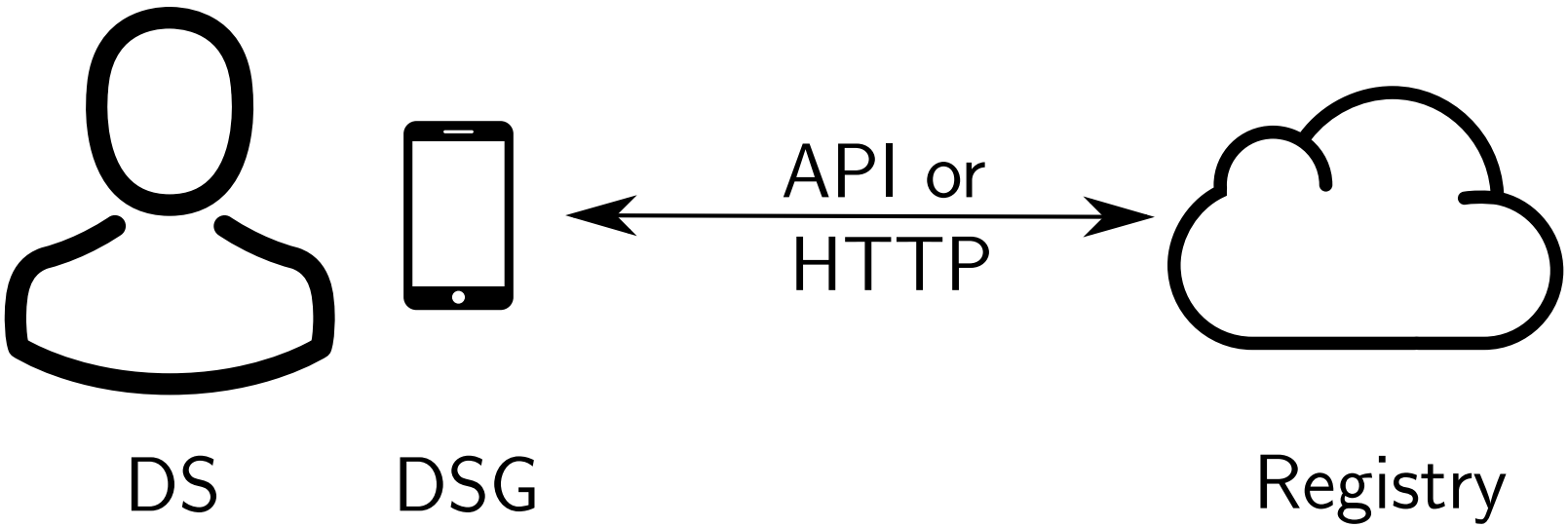


Figure: Representation of indirect communications.

Personal Data Custodian

The PDC can typically be implemented as an app

Figure: Google's Android

Figure: Apple's iOS

Abstract syntax of Pilot

$$
\begin{array}{rcl}
\textit{Pilot Privacy Policy} & ::= & (\textit{datatype}, \textit{dcr}, \textit{TR}) \\
\textit{Data Communication Rule}\,(\textit{dcr}) & ::= & \langle \textit{condition}, \textit{entity}, \textit{dur} \rangle \\
\textit{Data Usage Rule}\,(\textit{dur}) & ::= & \langle \textit{Purposes}, \textit{retention\_time} \rangle \\
\textit{Transfer Rules}\ (\textit{TR}) & ::= & \{\textit{dcr}_1, \textit{dcr}_2, \ldots\}
\end{array}
$$

Outline

Map of Things

`https://mapofthings.inrialpes.fr/map`

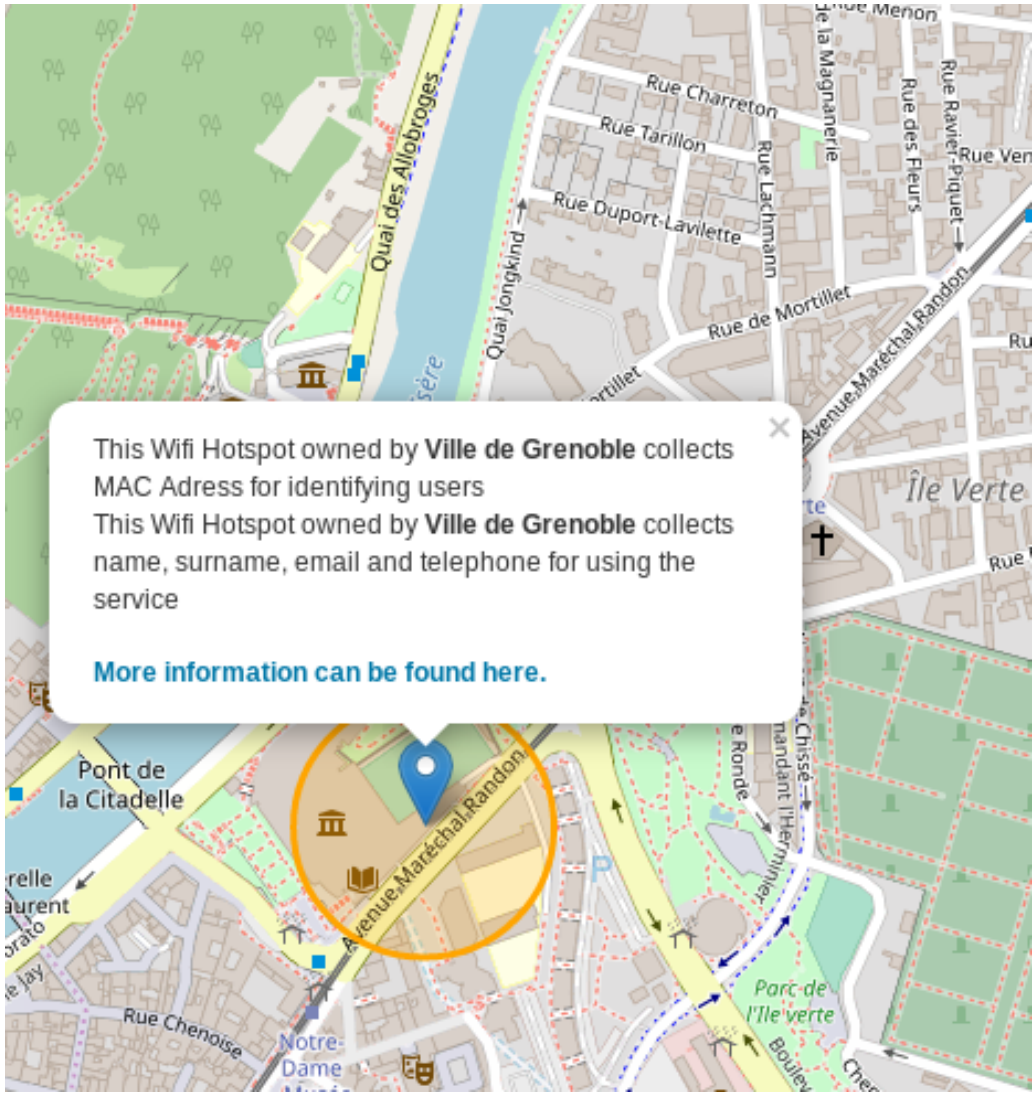


Figure: MoT short notice

ColoT

Figure: ColoT logo

A mobile app

- Works on Android
- Implements:
  - Direct and indirect information
  - Direct consent
  - Proof of consent
- Video time!

Outline

Contributions I

Genericity

- Does not depend on specific technology
- Addresses the heterogeneity of the IoT

Legal compliance

- Addresses legal compliance
- Designed for informed consent in the GDPR

User- and privacy-friendly

- Minimizes required interactions
- Optional features for usability
- No data disclosed by default

Contributions II

Implementation

- Ease of implementation
- Inexpensive to field
- PDC runs on smartphones
- Under free licences

Discussion on ePrivacy Regulation

- Will supersede the ePrivacy Directive
- Will consider metadata such as cookies
- This work demonstrates that consent can be easily managed in a privacy-preserving way

Publications

IWPE2018

Enhancing Transparency and Consent in the IoT (position paper)

SPIoT2019

UPRISE-IoT: User-centric Privacy & Security in the IoT (book section)

TRUSTCOM2019

A Generic Information and Consent Framework for the IoT

WISEC2020

DEMO: CoIoT: A Consent and Information assistant for the IoT

WPES2020

SoK: Three Facets of Privacy Policies (survey paper)

Outline

Limitations

Theoretical limitations

- Consent is intrinsically imperfect
- Data can be unlawfully collected: enforcement rests on the DC side
- Other legal grounds are unfit for technological solutions

Technical limitations

- Due to time shortage
- MoT does not restrict access
- ColoT does not implement all optional features
- Other limitations such as MAC address retrieval...

Outline

Perspectives

Standardization of consent

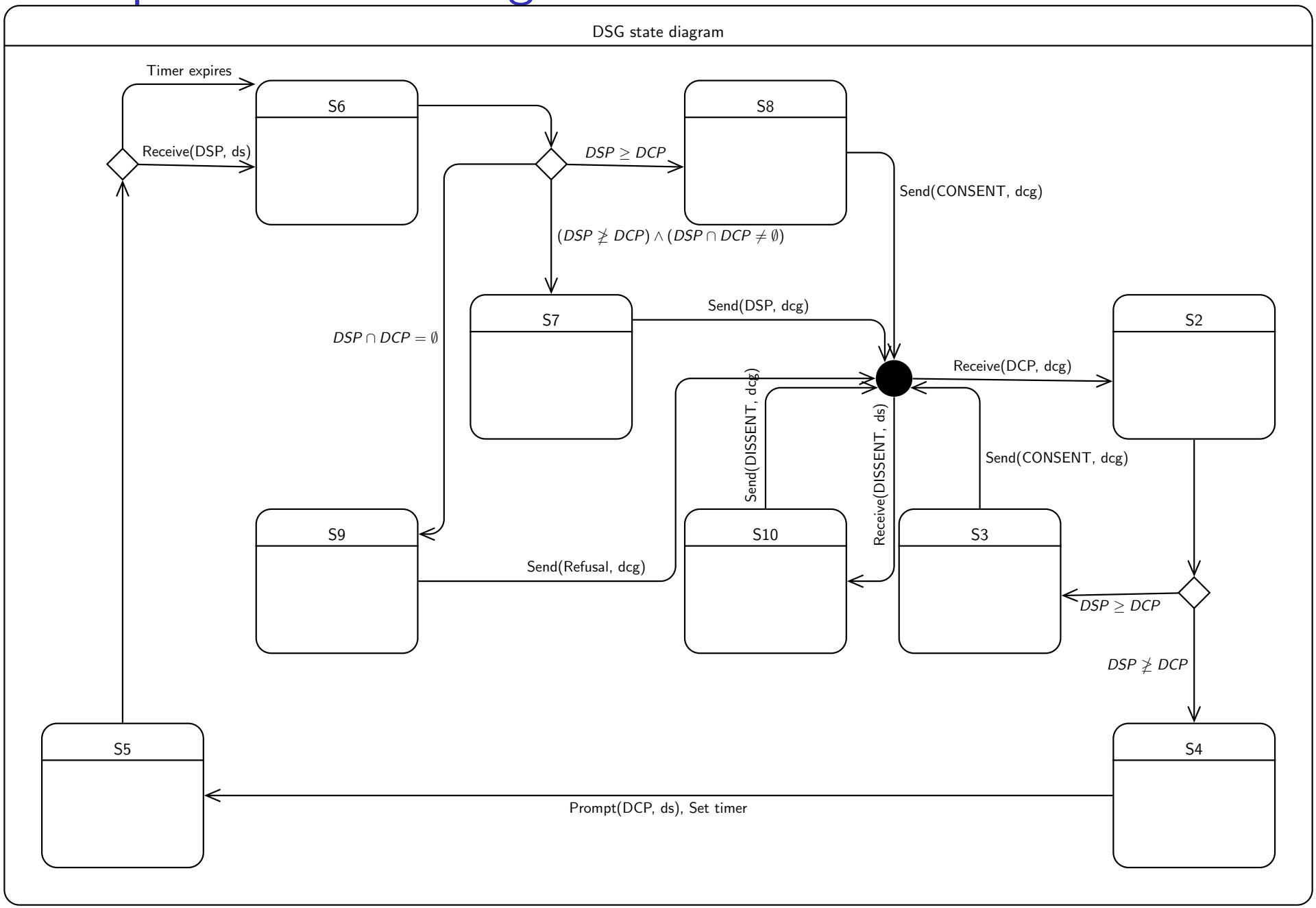
- Prevents deception of DS with unlawful interfaces
- Facilitates technical implementations of the law
- Paves the way to large-scale versions of the PoC presented here

Toward collective consent

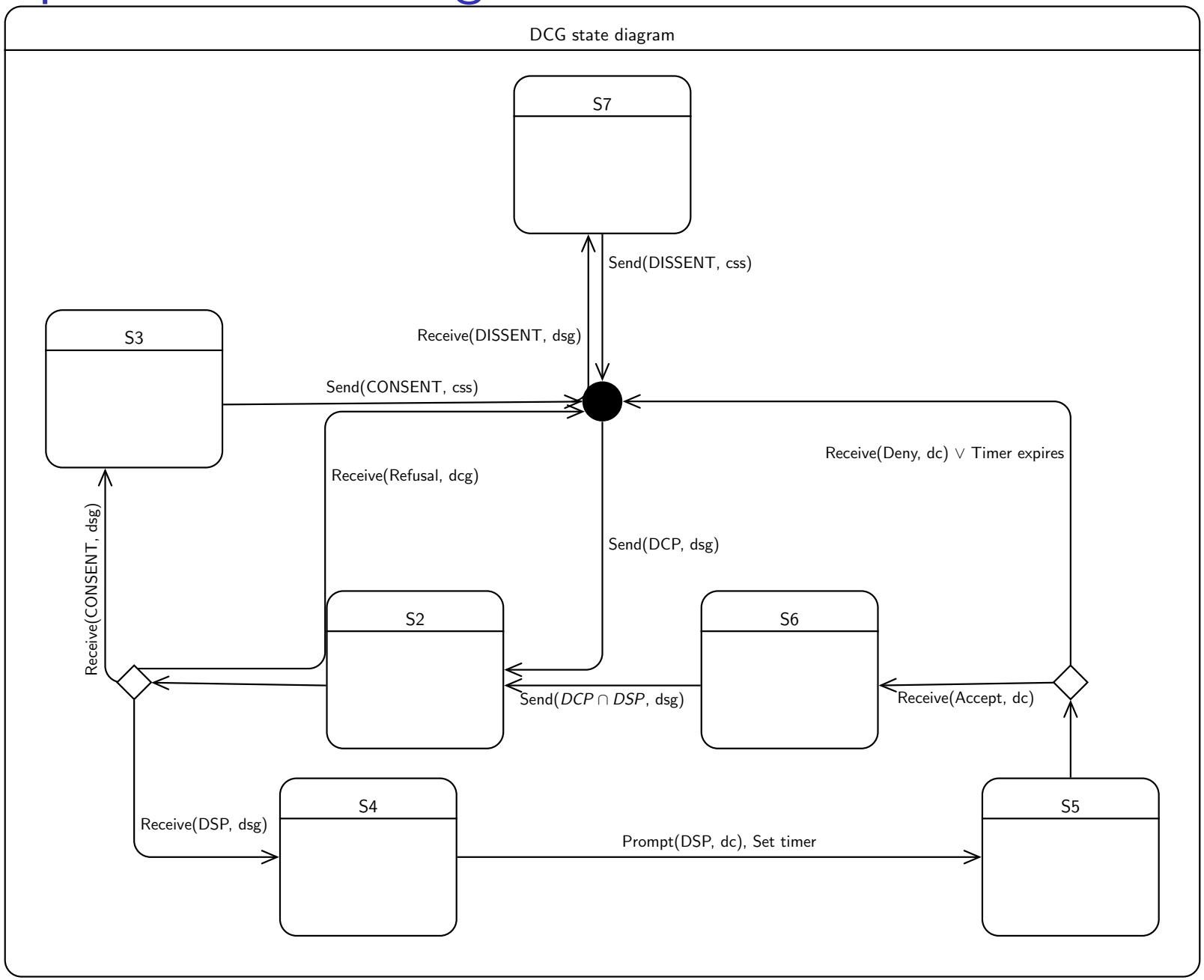
- Personal data is a collective issue
- Collective approach to personal data management can restore balance between parties
- Framing (un)lawful consent

Questions?

Backup: DSG state diagram



Backup: DCG state diagram



Backup: Proof of consent

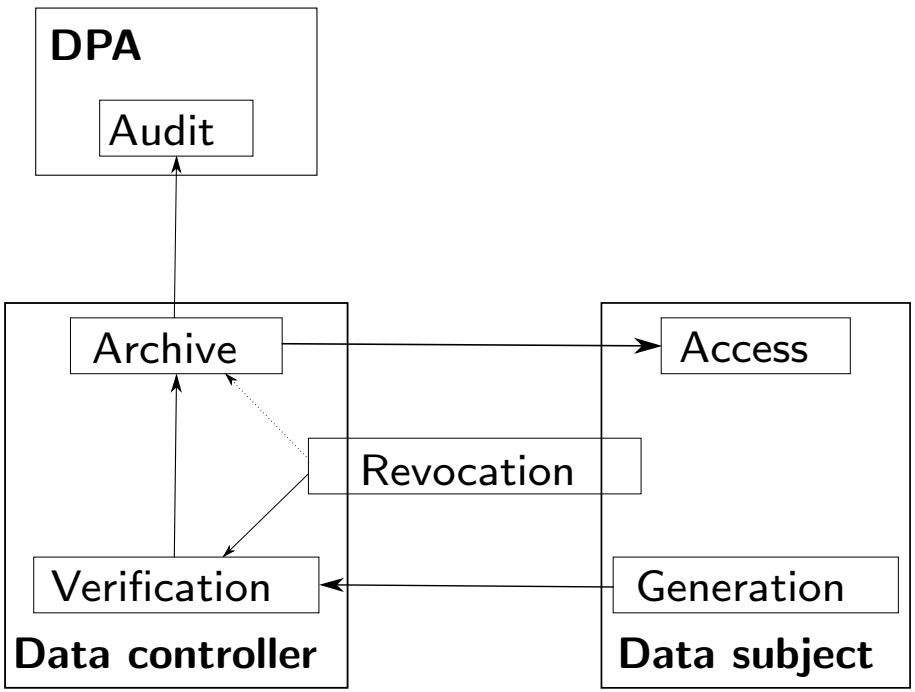


Figure: High-level requirements for the proof of consent.

Data subject requirements

Generation Steps for consent production

Revocation Steps for communication of consent withdrawal

Access (optional) Access to previously given consents

Data controller requirements

Archive Steps during which consents are stored

Verification Steps to assess the well-formedness of consents

Revocation Steps for reception and accounting of consent withdrawal

Audit Highest-level goal of the proof of consent

Backup: Cryptographic properties for the proof of consent

Completeness All consents must be stored.

Tamper-evidence Ability to detect any unwilling modification on a ledger.

Unforgeability Resistance against the fabrication of a digital signature.

Non-impersonation Attack in which an adversary assumes the identity of one of the legitimate parties.

Non-repudiation Prevents a party from denying the performance of a contract.

Backup: Technical options for the proof of consent

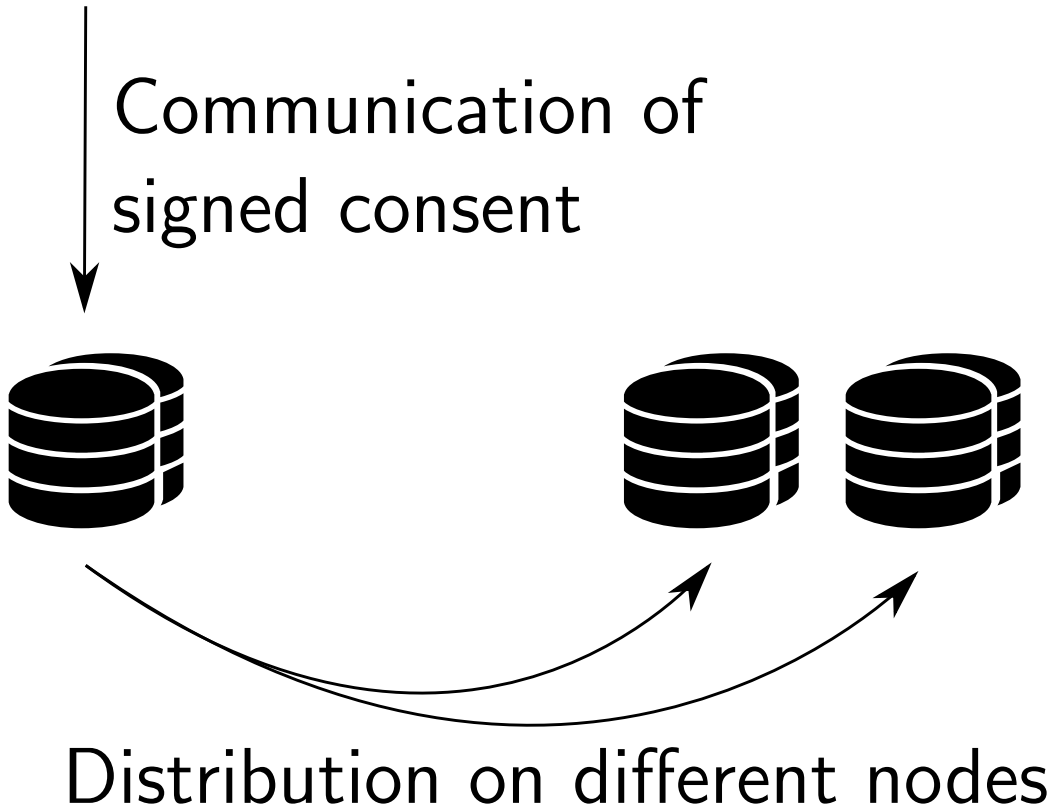


Figure: Distributed ledger

Backup: The Hypercore ledger

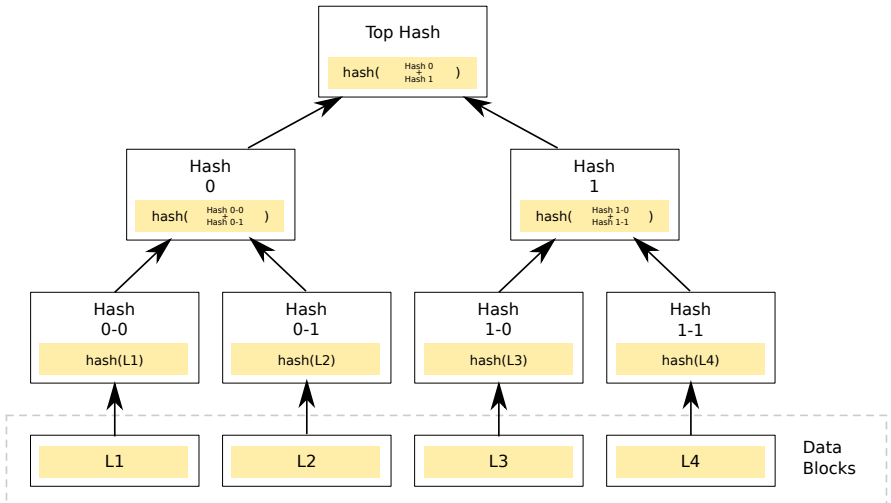


Figure: Illustration of a Merkle Hash Tree by Azaghal

Dat Protocol

- P2P protocol for distributed data
- Storage and content integrity are stored in Hypercore registers
- In our context, consents are stored in such a register

Backup: Signed and ordered

Cryptographic signatures

- Consents must be signed for authentication and non-repudiation
- Android and iOS implement cryptographic signatures

Order of entries

- Necessary for a correct implementation of consent withdrawal
- Consents and dissents must be ordered in the ledger
- The last entry prevails

Backup: Pilot

Syntax

$$
\begin{aligned}
\textit{Pilot Privacy Policy} &::= (\textit{datatype}, \textit{dcr}, \textit{TR}) \\
\textit{Data Communication Rule}\,(\textit{dcr}) &::= \langle \textit{condition}, \textit{entity}, \textit{dur} \rangle \\
\textit{Data Usage Rule}\,(\textit{dur}) &::= \langle \textit{Purposes}, \textit{retention\_time} \rangle \\
\textit{Transfer Rules}\ (\textit{TR}) &::= \{\textit{dcr}_1, \textit{dcr}_2, \ldots\}
\end{aligned}
$$

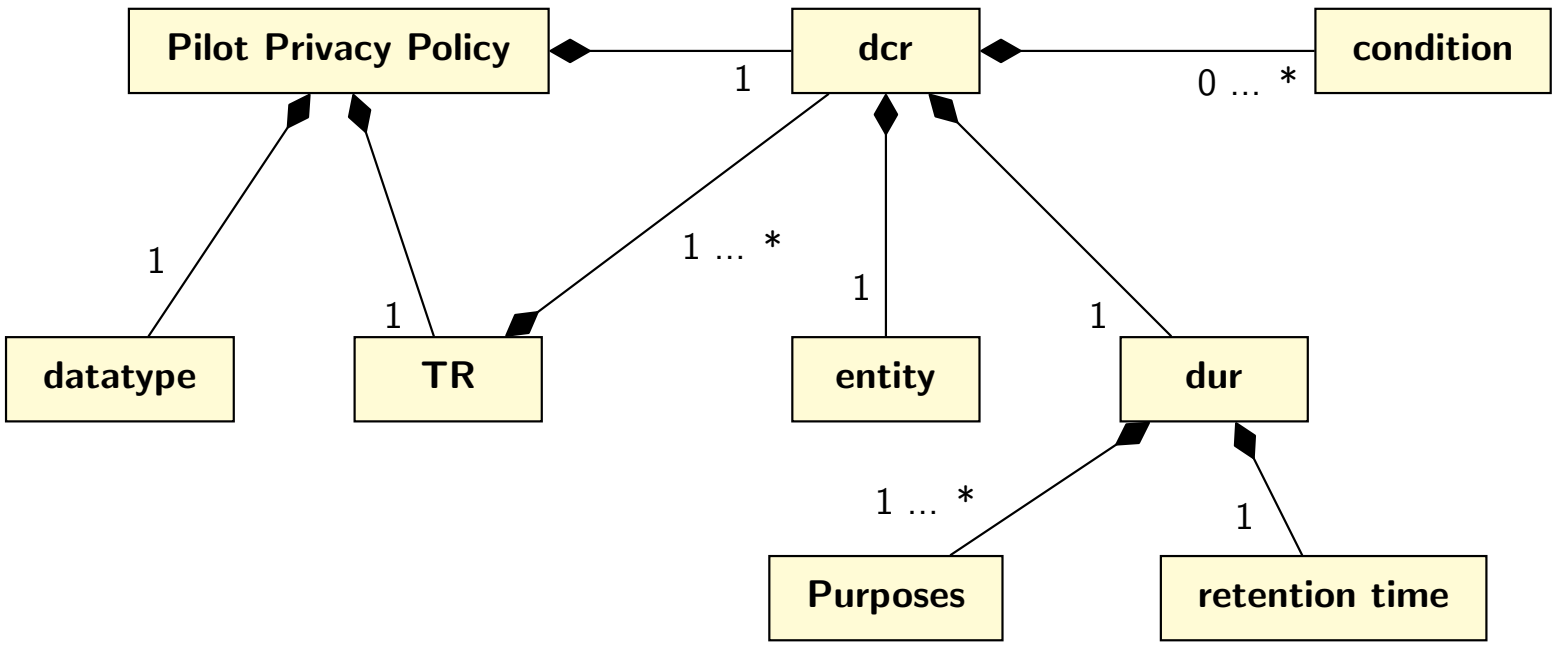


Figure: Pilot high-level structure in a UML fashion.