UNIVERSITY OF OSLO

18th IFIP Summer School

on Privacy and Identity Management

Secure and Privacy-Preserving Authentication for Data Subject Rights Enforcement

Malte Hansen and Andre Büttner

University of Oslo

10th August 2023

Background

- Data Subject Rights (DSRs)
  - GDPR (Art. 12-23)

- Identifying DSs can be a challenging task
  - DSRs do not apply if DC can demonstrate that DS **cannot** be identified (cf. GDPR, Art. 11(2))

- Common DS authentication methods are
  - ID-document verification
  - Verification of corresponding email address or phone number

Source: https://advisera.com/articles/8-data-subject-rights-according-to-gdpr/

Motivation

- Violation of data minimisation principle
  - Often complete ID documents are requested

Home > News
> Dutch SA fines DPG Media Magazines for unnecessarily requesting copies of identity documents

Dutch SA fines DPG Media Magazines for unnecessarily requesting copies of identity documents

28 March 2022 Netherlands

Background information

Date of final decision: 14 January 2022
Cross-border case or national case: National
Controller: DPG Media Magazines B.V.
Legal Reference: article 12 (2) GDPR
Decision: Infringement of the GDPR, administrative fine
Key words: identity document; personal data; transparency

Source: https://edpb.europa.eu/news/national-news/2022/dutch-sa-fines-dpg-media-magazines-unnecessarily-requesting-copies-identity_en

Security Analysis of Subject Access Request Procedures

How to Authenticate Data Subjects Safely When They Request for Their Data

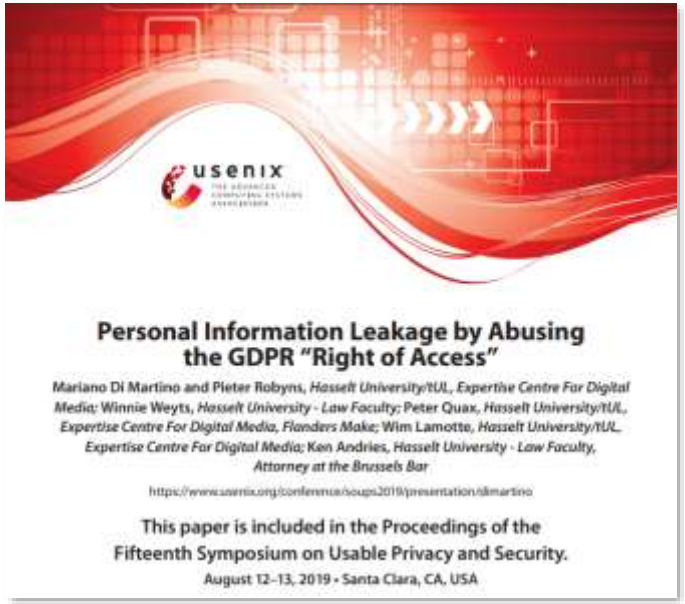
Coline Boniface[1], Imane Fouad[2], Nataliia Bielova[2], Cédric Lauradoux[1(✉)], and Cristiana Santos[3]

[1] Univ. Grenoble Alpes, Inria, France
{coline.boniface,cedric.lauradoux}@inria.fr
[2] Université Côte d'Azur, Inria, France
{imane.fouad,nataliia.bielova}@inria.fr
[3] School of Law, University Toulouse 1 Capitole, SIRIUS Chair, Toulouse, France
cristiana.santos@ut-capitole.fr

Boniface et al. "Security analysis of subject access request procedures: How to authenticate data subjects safely when they request for their data." *Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019*. Springer International Publishing, 2019.

Motivation

- Misuse of DSR requests to steal personal data
  - E.g., forged ID-documents or invalid email address



usenix

Personal Information Leakage by Abusing the GDPR "Right of Access"

Mariano Di Martino and Pieter Robyns, *Hasselt University/tUL, Expertise Centre For Digital Media;* Winnie Weyts, *Hasselt University - Law Faculty;* Peter Quax, *Hasselt University/tUL, Expertise Centre For Digital Media, Flanders Make;* Wim Lamotte, *Hasselt University/tUL, Expertise Centre For Digital Media;* Ken Andries, *Hasselt University - Law Faculty, Attorney at the Brussels Bar*

https://www.usenix.org/conference/soups2019/presentation/dimartino

This paper is included in the Proceedings of the Fifteenth Symposium on Usable Privacy and Security.

August 12–13, 2019 • Santa Clara, CA, USA

Di Martino et al. "Personal Information Leakage by Abusing the GDPR 'Right of Access'." *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019.

GDPiRated – Stealing Personal Information On- and Offline

Matteo Cagnazzo[1(✉)], Thorsten Holz[2], and Norbert Pohlmann[1]

[1] Institute for Internet-Security, University of Applied Sciences Gelsenkirchen, Gelsenkirchen, Germany
{cagnazzo,pohlmann}@internet-sicherheit.de

[2] Horst Görtz Institute (HGI), Ruhr-Universität Bochum, Bochum, Germany
thorsten.holz@rub.de

Abstract. The European *General Data Protection Regulation* (GDPR) went into effect in May 2018. As part of this regulation, the *right to access* was extended, it grants a user the right to request access to all personal data collected by a company about this user. In this paper, we present the results of an empirical study on data exfiltration attacks that are enabled by abusing these so called *subject access requests*. More specifically, our *GDPiRate attack* is performed by sending subject access

Cagnazzo et al. "GDPiRated–stealing personal information on-and offline." *Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security*. Springer International Publishing, 2019.

GDPArrrrr: Using Privacy Laws to Steal Identities

James Pavur*
DPhil Researcher
Oxford University

Casey Knerr
Security Consultant
Dionach LTD

Abstract

The General Data Protection Regulation (GDPR) has become a touchstone model for modern privacy law, in part because it empowers consumers with unprecedented control over the use of their personal information. However, this same power may be susceptible to abuse by malicious attackers. In this paper, we consider how legal ambiguity surrounding the "Right of Access" process may be abused by social engineers. This hypothesis is tested through an adversarial case study of more than 150 businesses. We find that many organizations fail to em-

about them.

In this paper, we consider the practical implementation of this right, with a particular focus on mechanisms to prevent its abuse to steal sensitive information about a third party. We find that GDPR itself provides little guidance on best practices and, more broadly, that little attention has been paid to the possibility of request abuse for the purpose of data theft. This lacuna is contextualized through a real-world experiments in which simulated fraudulent GDPR requests are sent to more than 150 organizations.

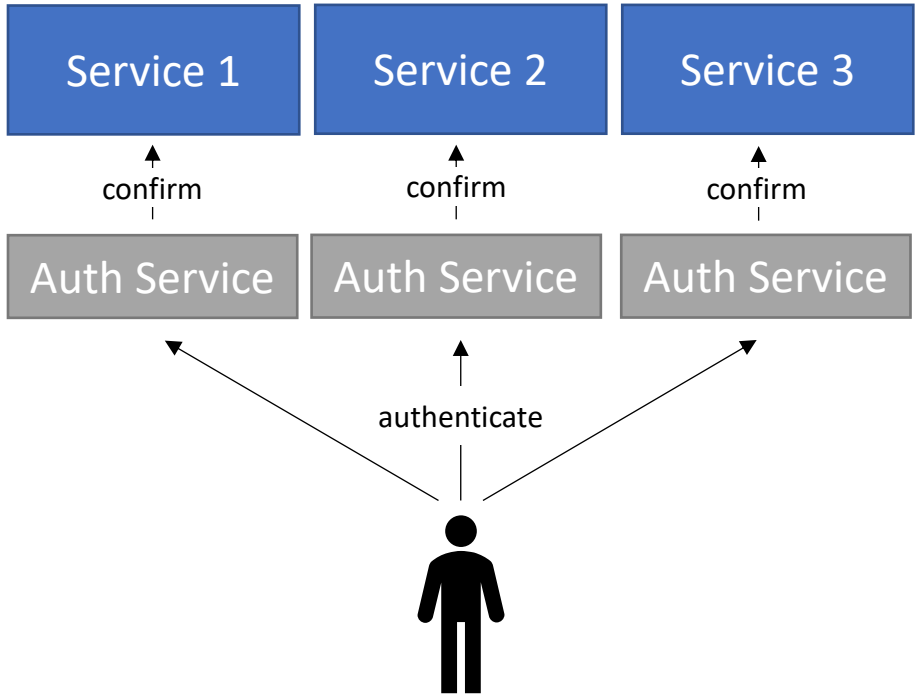
Pavur and Knerr. "Gdparrrrr: Using privacy laws to steal identities." *arXiv preprint arXiv:1912.00731* (2019).

Motivation

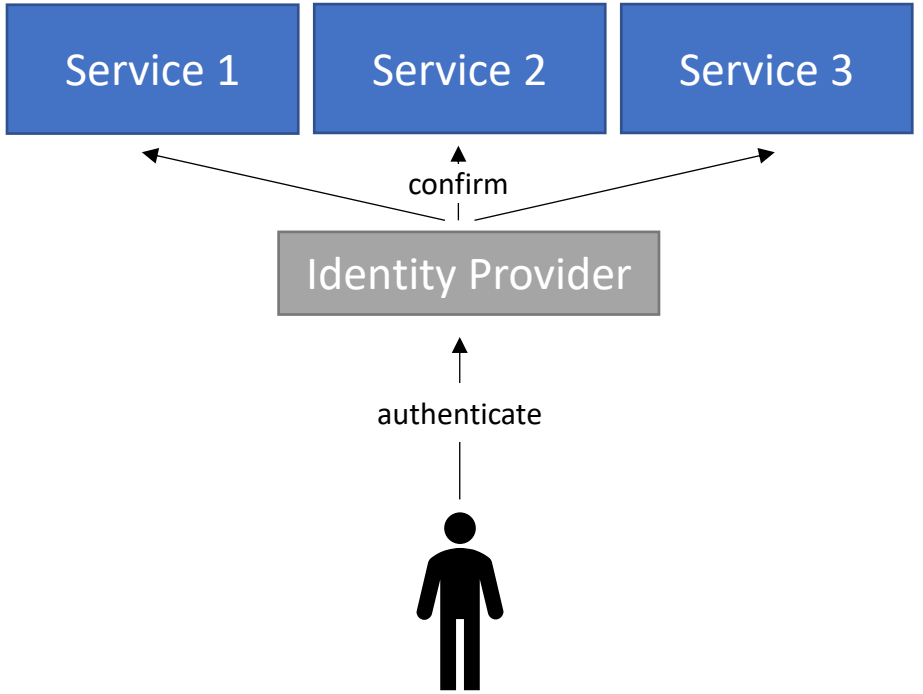
- Need for a better way to authenticate DSs
  - ➢No violation of privacy principles
  - ➢Without allowing illegitimate data access
  - ➢Ideally as a EU-wide solution that can be easily implemented

Authentication Models

Centralized Identity



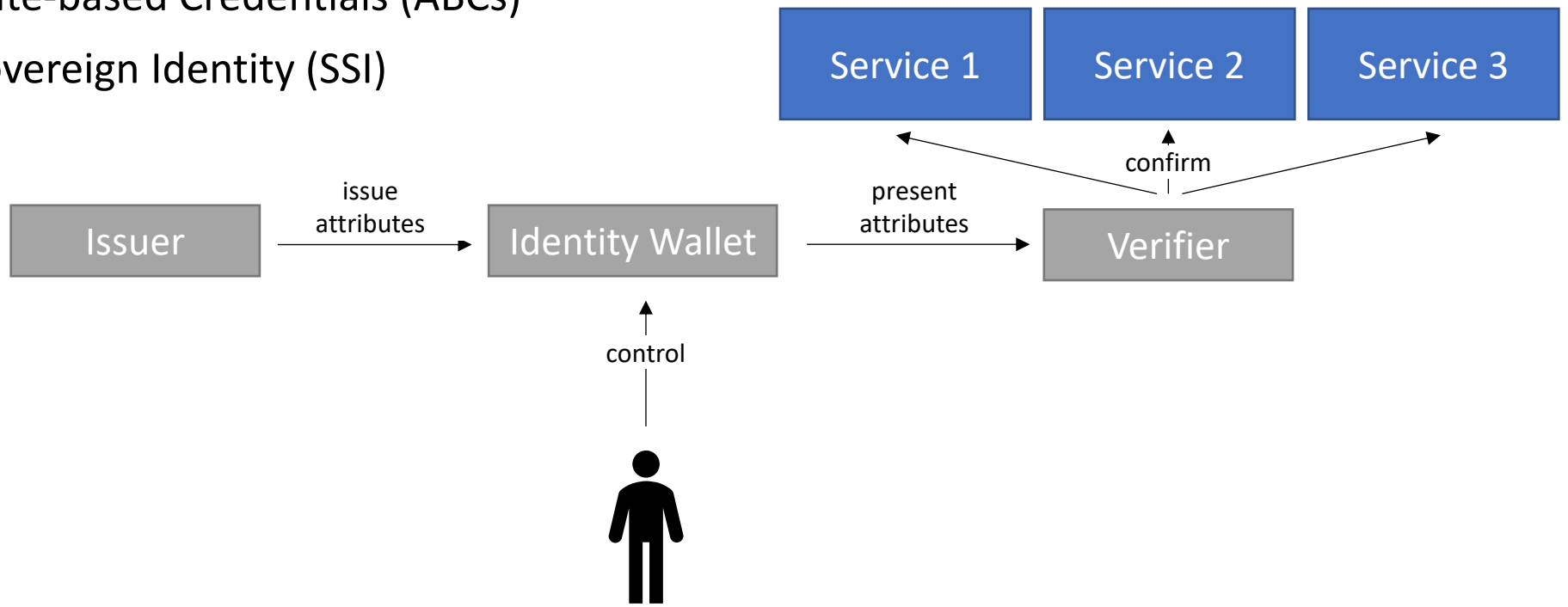
Federated Identity



Authentication Models

Decentralized Identity

- Attribute-based Credentials (ABCs)
- Self-Sovereign Identity (SSI)



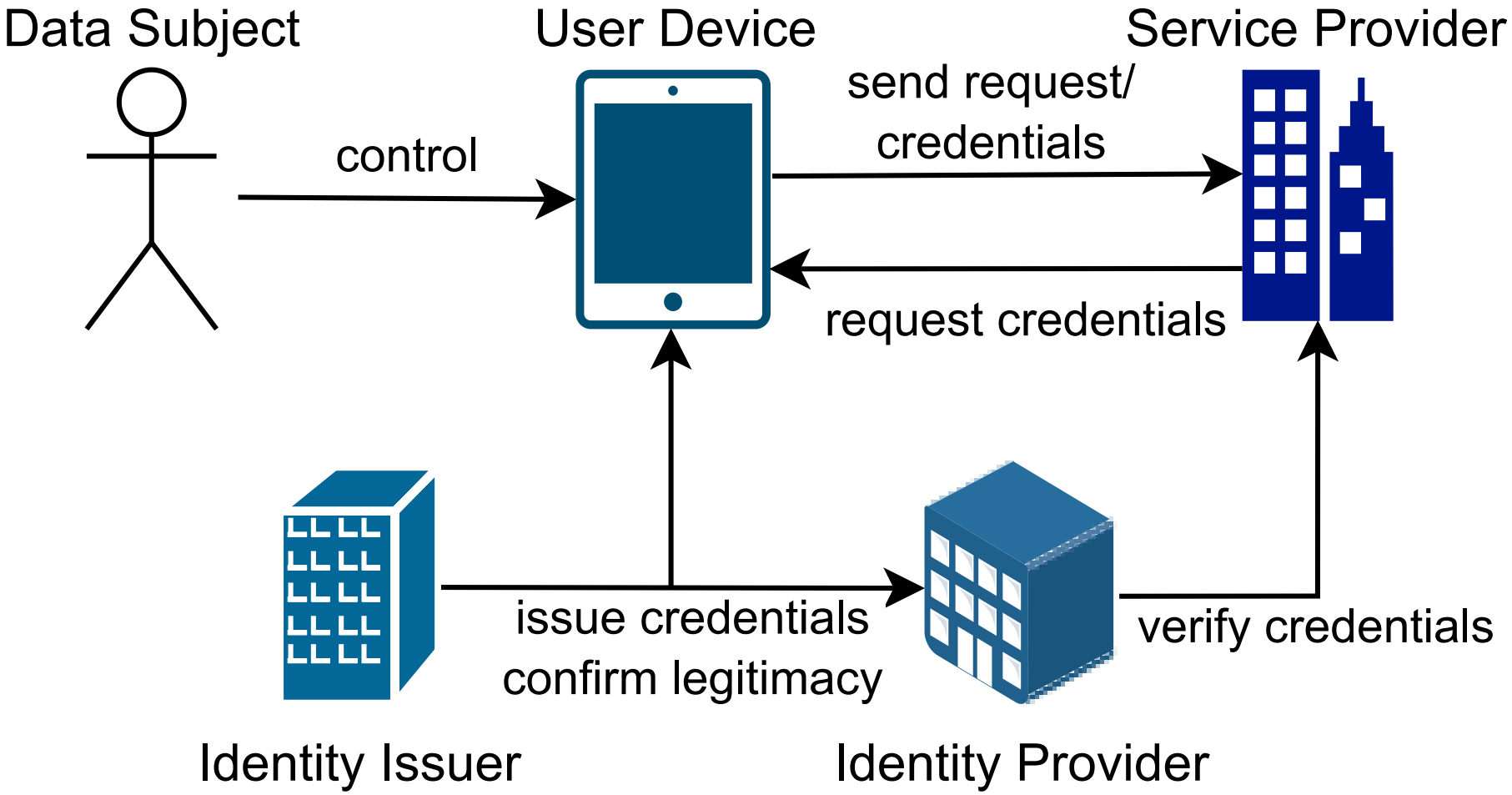
EU Digital Identity Wallet

- SSI-based infrastructure for eIDs within and across EU countries

Source: https://www.digdir.no/sites/sogn/files/styles/lg/public/2022-09/e-wallet-cards.png

- Verification of attributes
  - Personal Identifiable Data (PID)
    - e.g. *last name*, *first name*, *date of birth*, …
  - Qualified or non-qualified Electronic Attestations of Attributes (QEAA):
    - e.g. *driving license, transcript of records*, *payments*, …

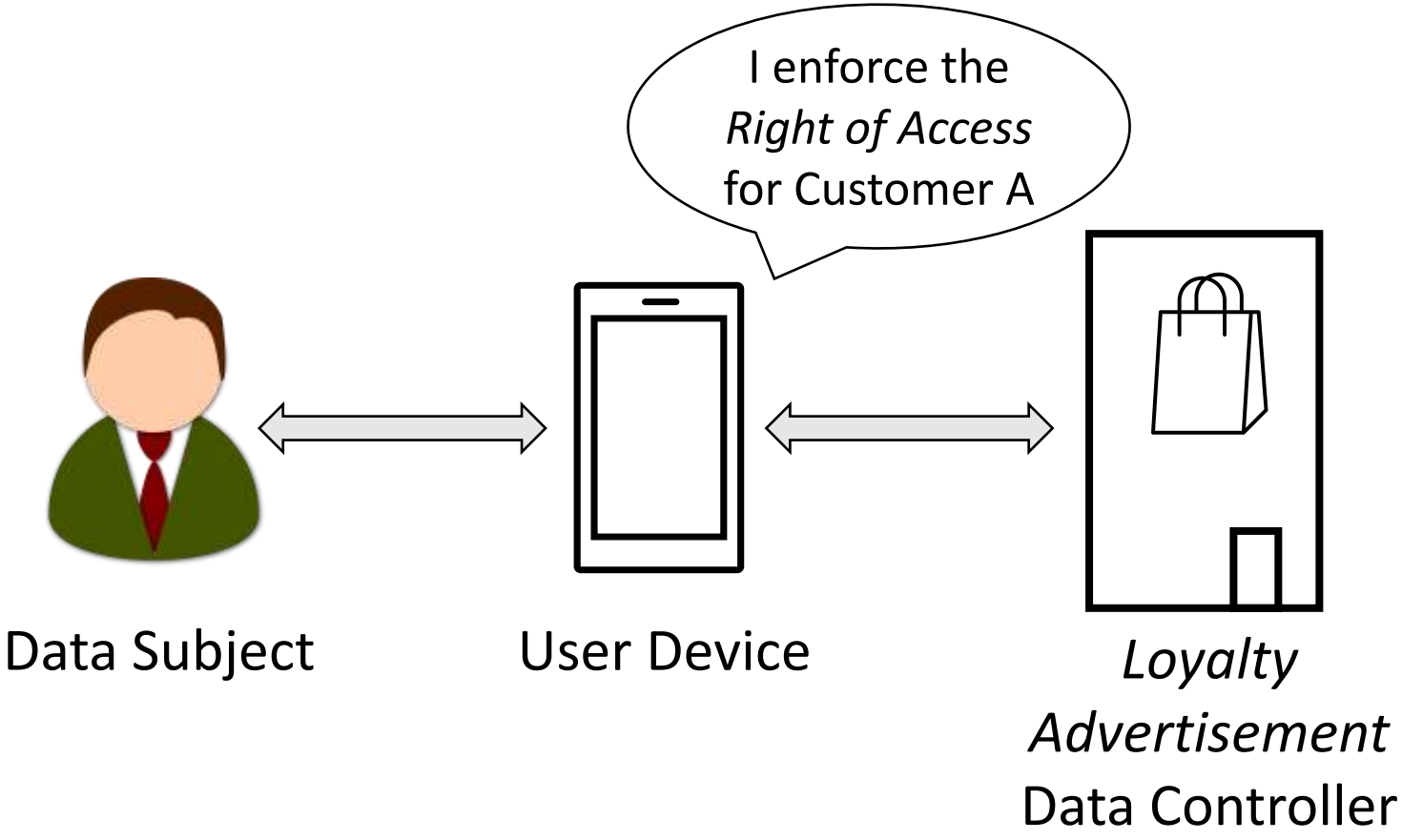
eID for Data Subject Rights Requests



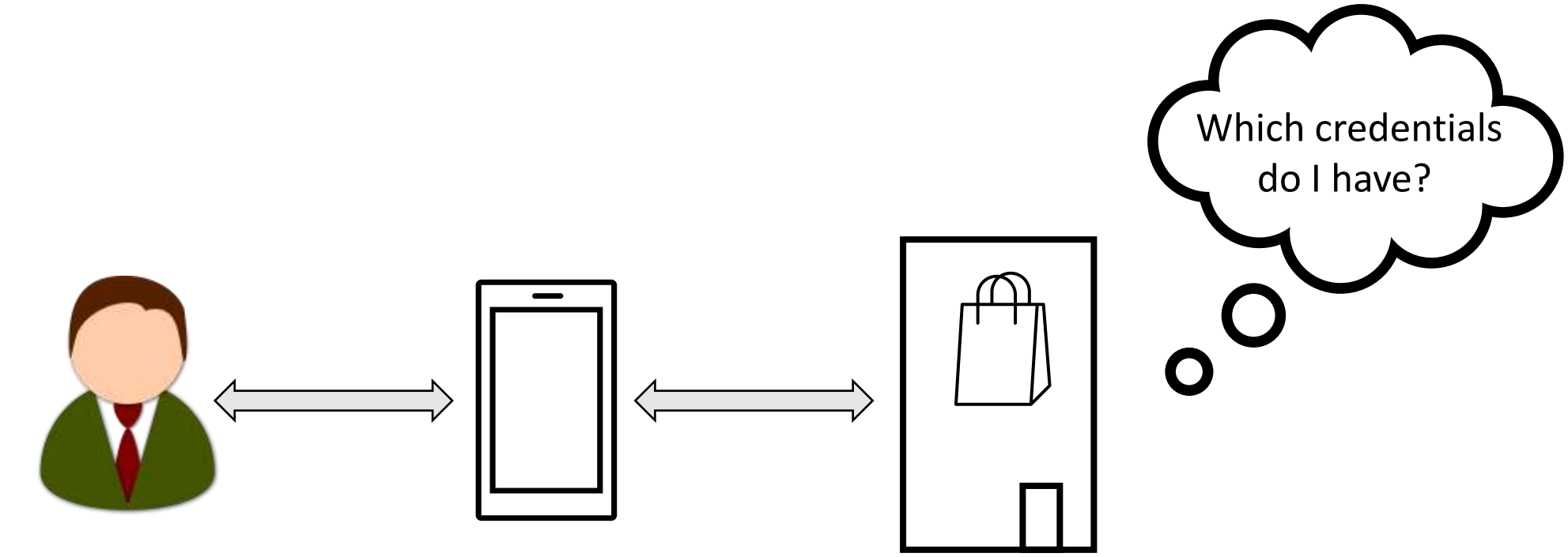
Self-Sovereign Identity Approach

Data Subject

Self-Sovereign Identity Approach

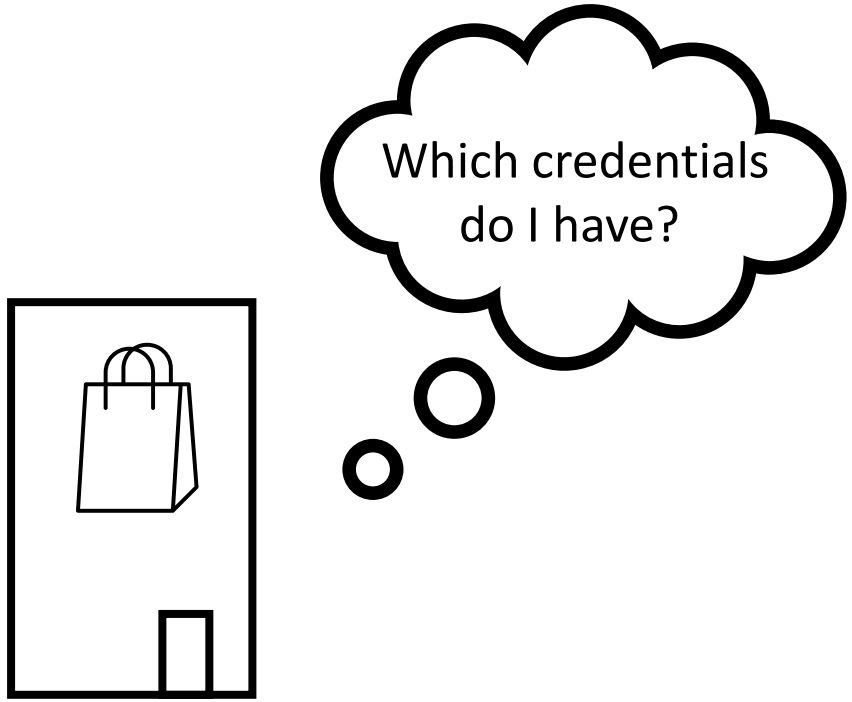


Self-Sovereign Identity Approach



Self-Sovereign Identity Approach

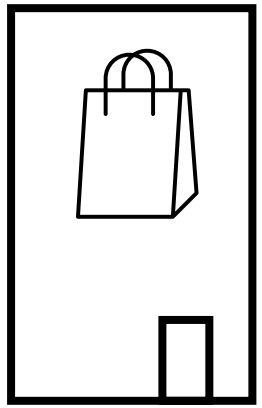
Possible Credentials
family name
first name
date of birth
address
gender
nationality



Loyalty
Advertisement
Data Controller

Self-Sovereign Identity Approach

Product Shipment	
customerNo	Customer A
productNo	491501
age verification	true
date of birth	1948-11-14
shipping name	George
shipping firstname	Anonymous
shipping address	London SW1A 1AA

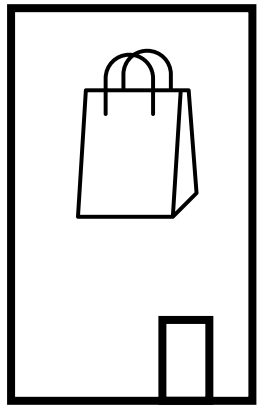


Loyalty
Advertisement
Data Controller

Product Shipment	
customerNo	Customer A
productNo	326773
age verification	false
shipping name	George
shipping firstname	Anonymous
shipping address	Llandovery SA20 0NQ

Self-Sovereign Identity Approach

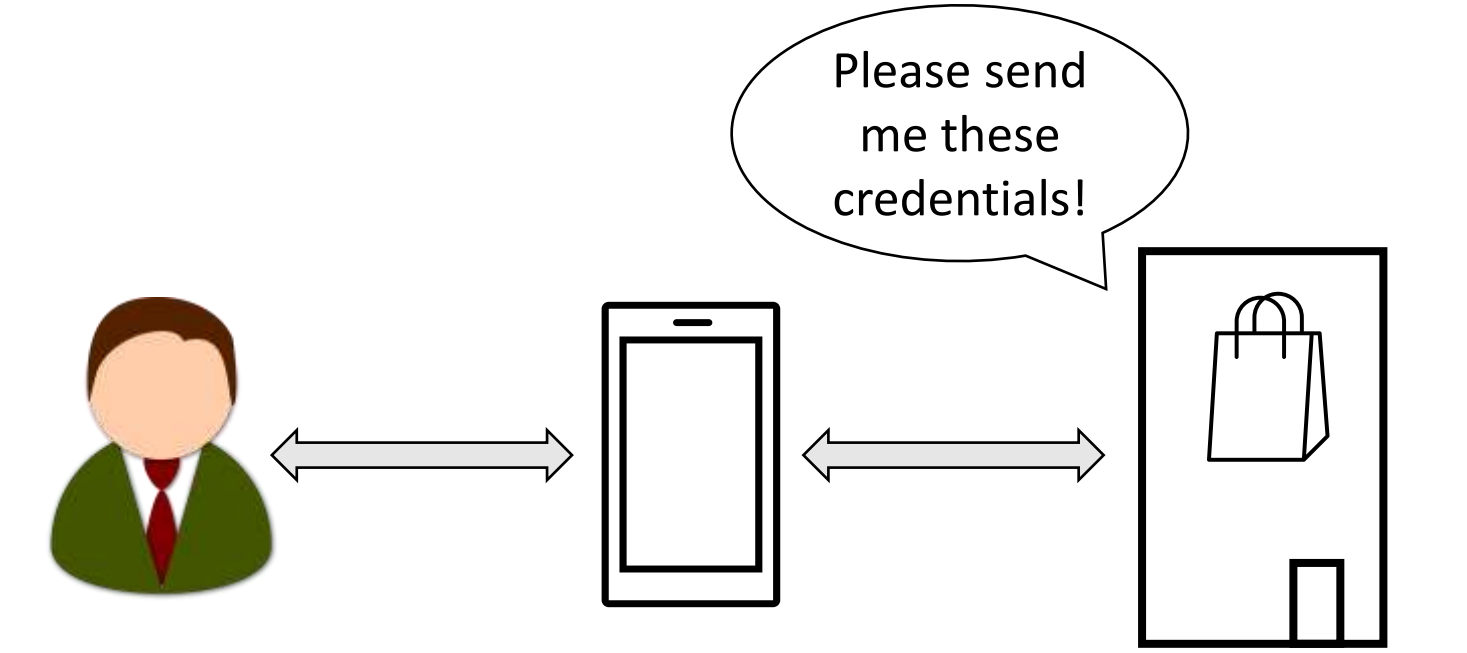
Product Shipment	
customerNo	Customer A
productNo	491501
age verification	true
date of birth	1948-11-14
shipping name	George
shipping firstname	Anonymous
shipping address	London SW1A 1AA



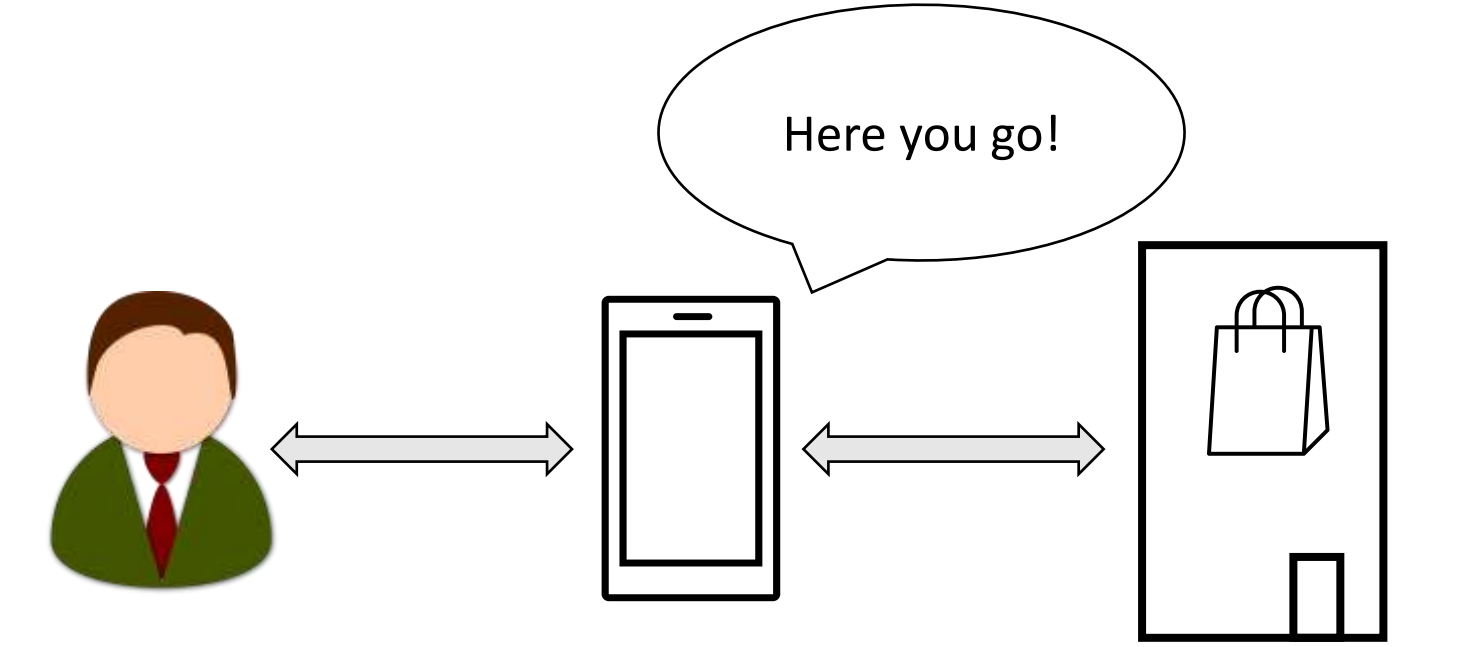
Loyalty
Advertisement
Data Controller

Product Shipment	
customerNo	Customer A
productNo	326773
age verification	false
shipping name	George
shipping firstname	Anonymous
shipping address	Llandovery SA20 0NQ

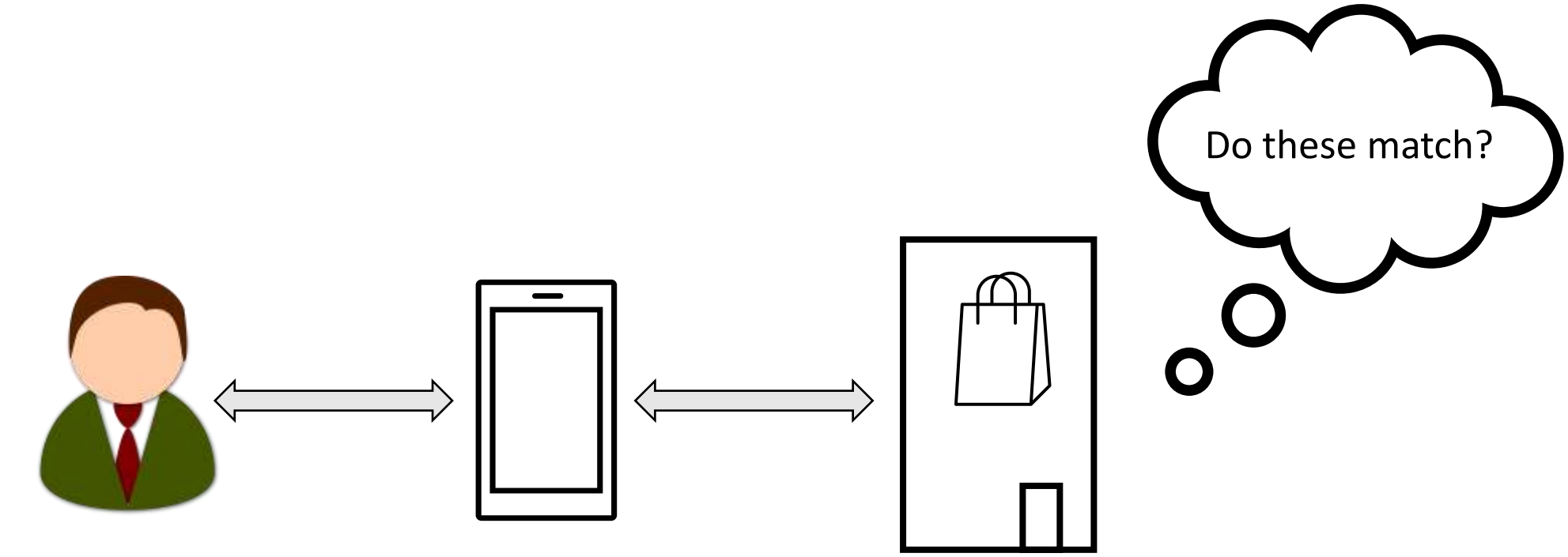
Self-Sovereign Identity Approach



Self-Sovereign Identity Approach



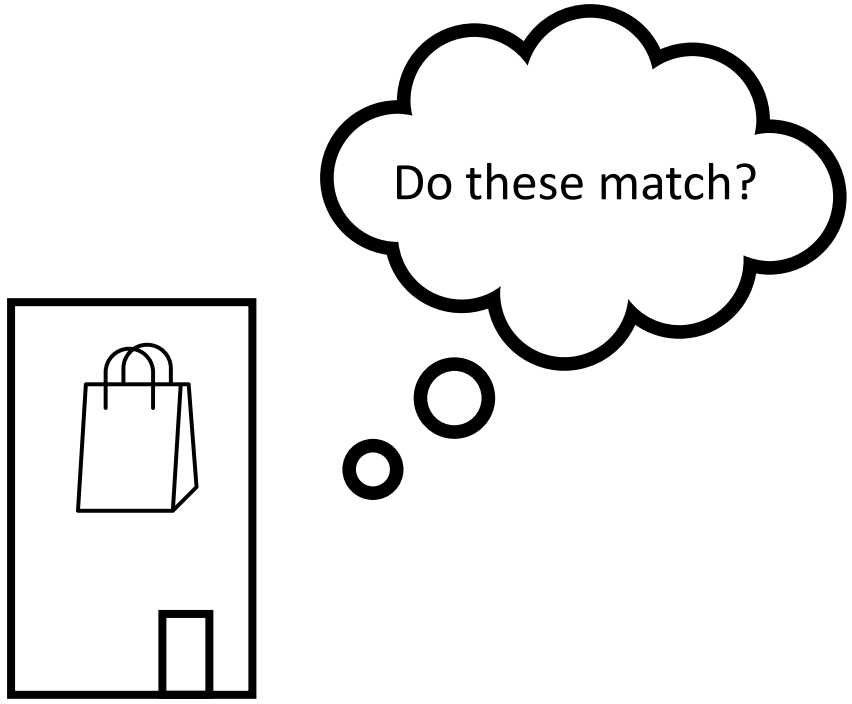
Self-Sovereign Identity Approach



Self-Sovereign Identity Approach

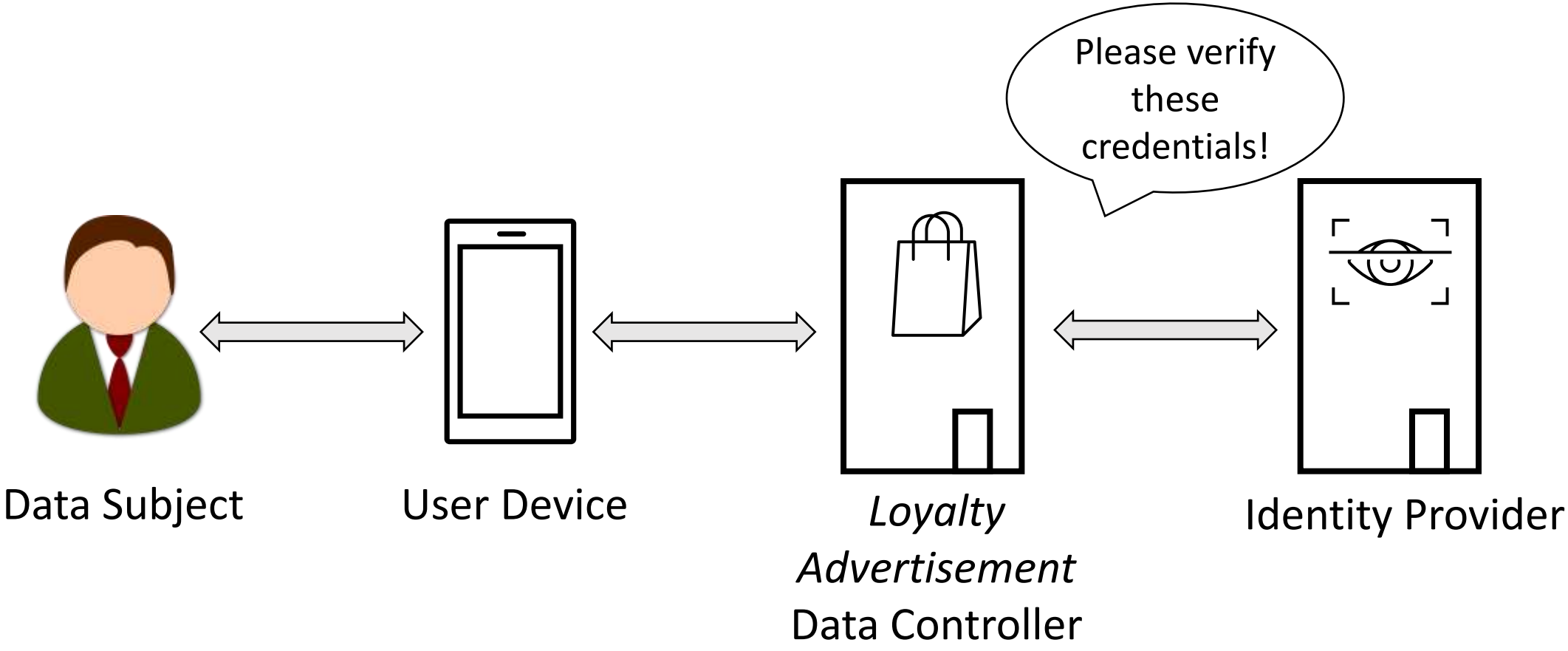
Loyalty Advertisement Credentials	
family name	George
date of birth	1948-11-14
address	London SW1A 1AA
address	Llandovery SA20 0NQ

Data Subject Credentials	
family name	George
first name	Charles
date of birth	1948-11-14
address	London SW1A 1AA
gender	male

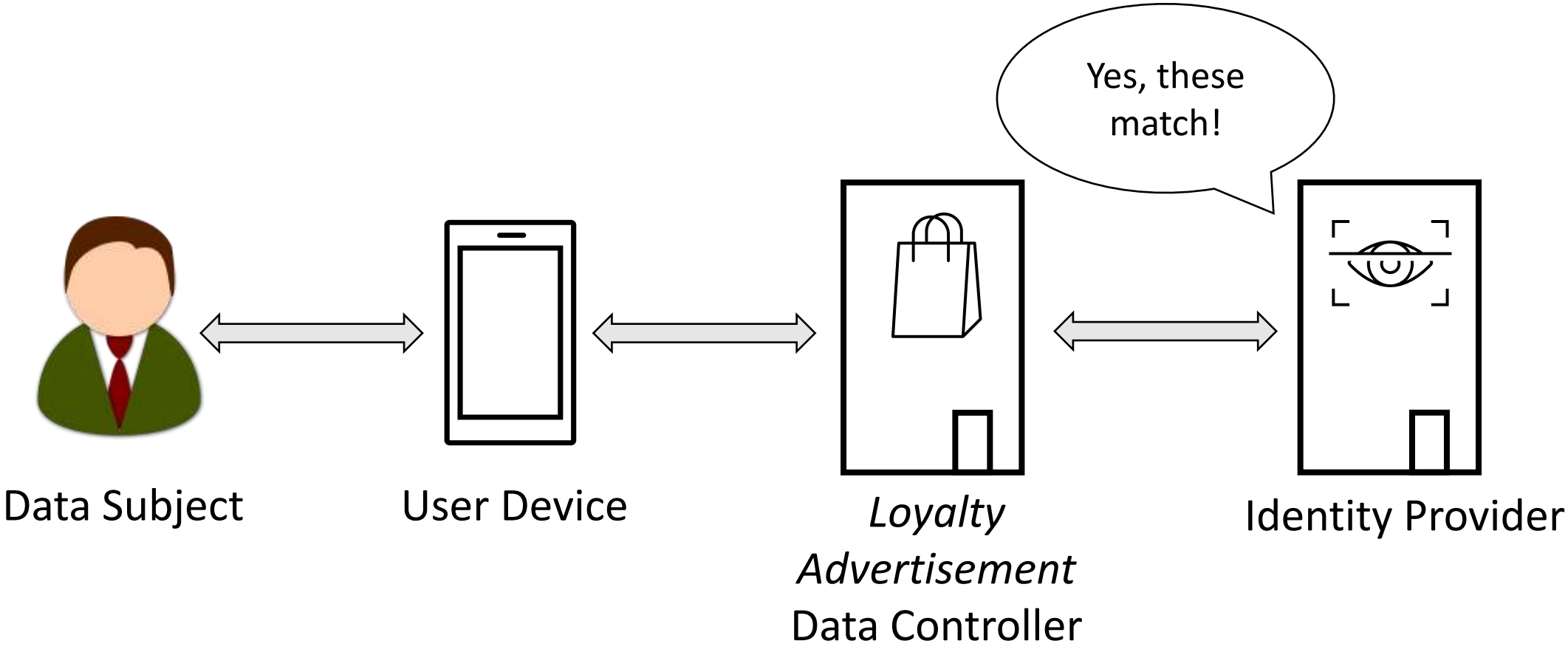


Loyalty Advertisement
Data Controller

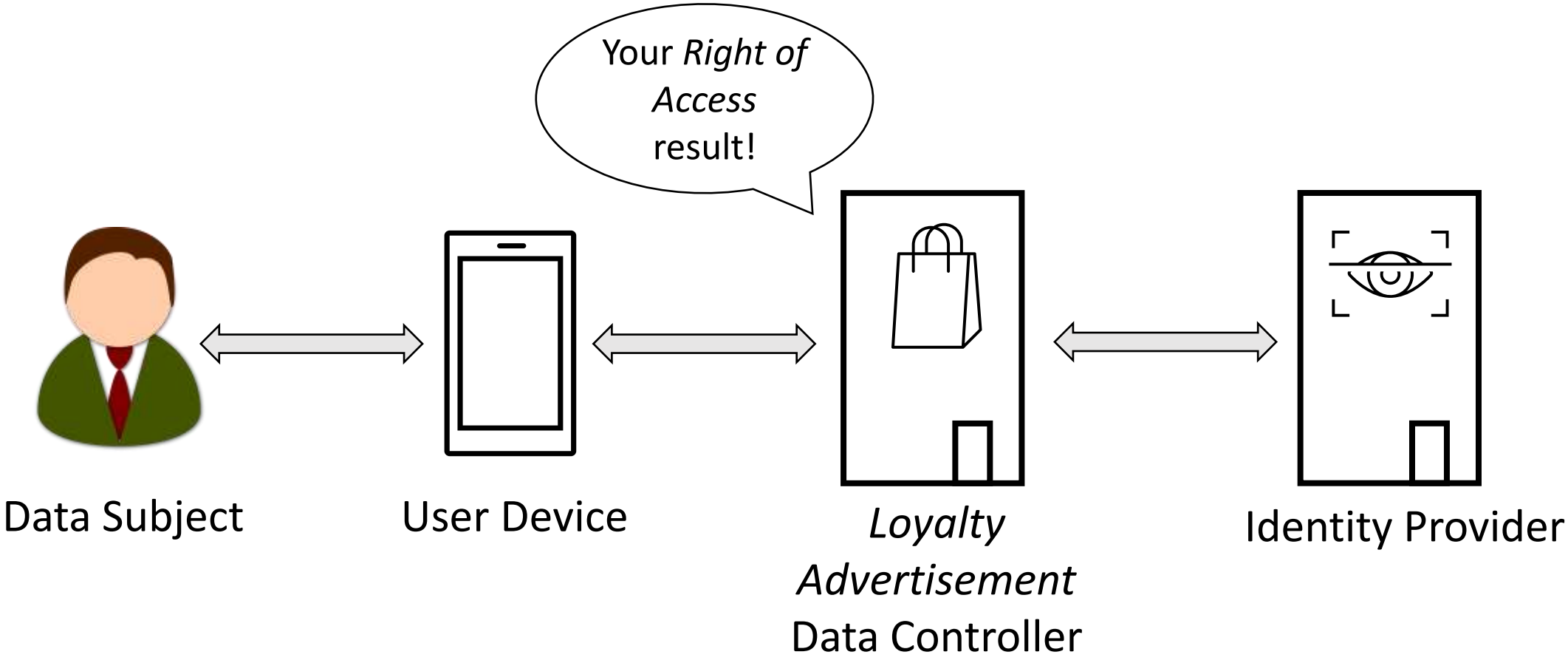
Self-Sovereign Identity Approach



Self-Sovereign Identity Approach



Self-Sovereign Identity Approach

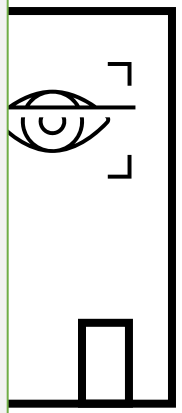


Self-Sovereign Identity Approach

Data Subject

What do we gain?

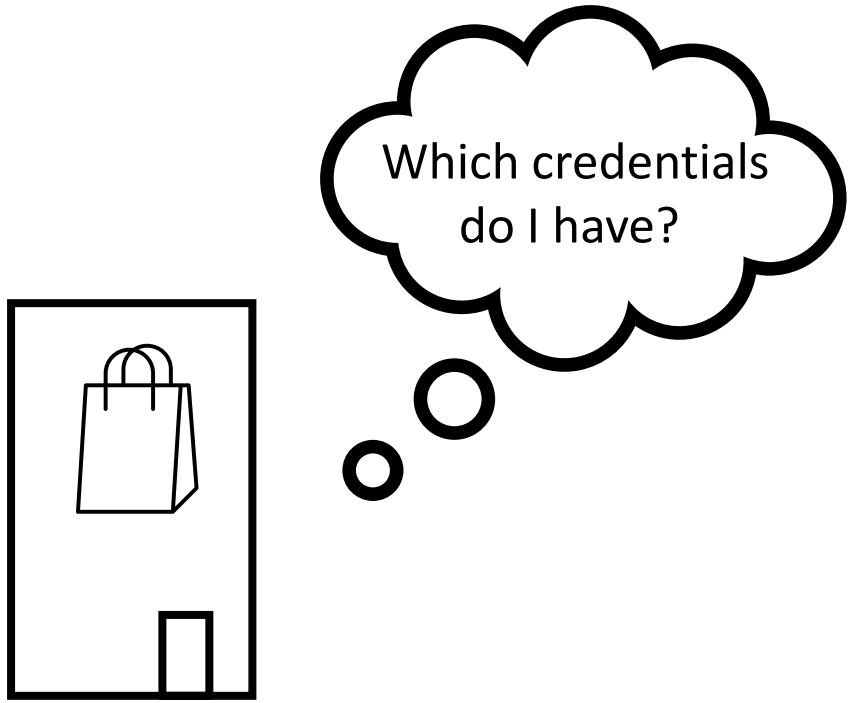
- Security
- Reliability
- Data minimisation
- Solution for EU Data Strategy
  - Data Intermediaries
  - Data Spaces & data sharing
- Anonymous Data Subject Right request



ty Provider

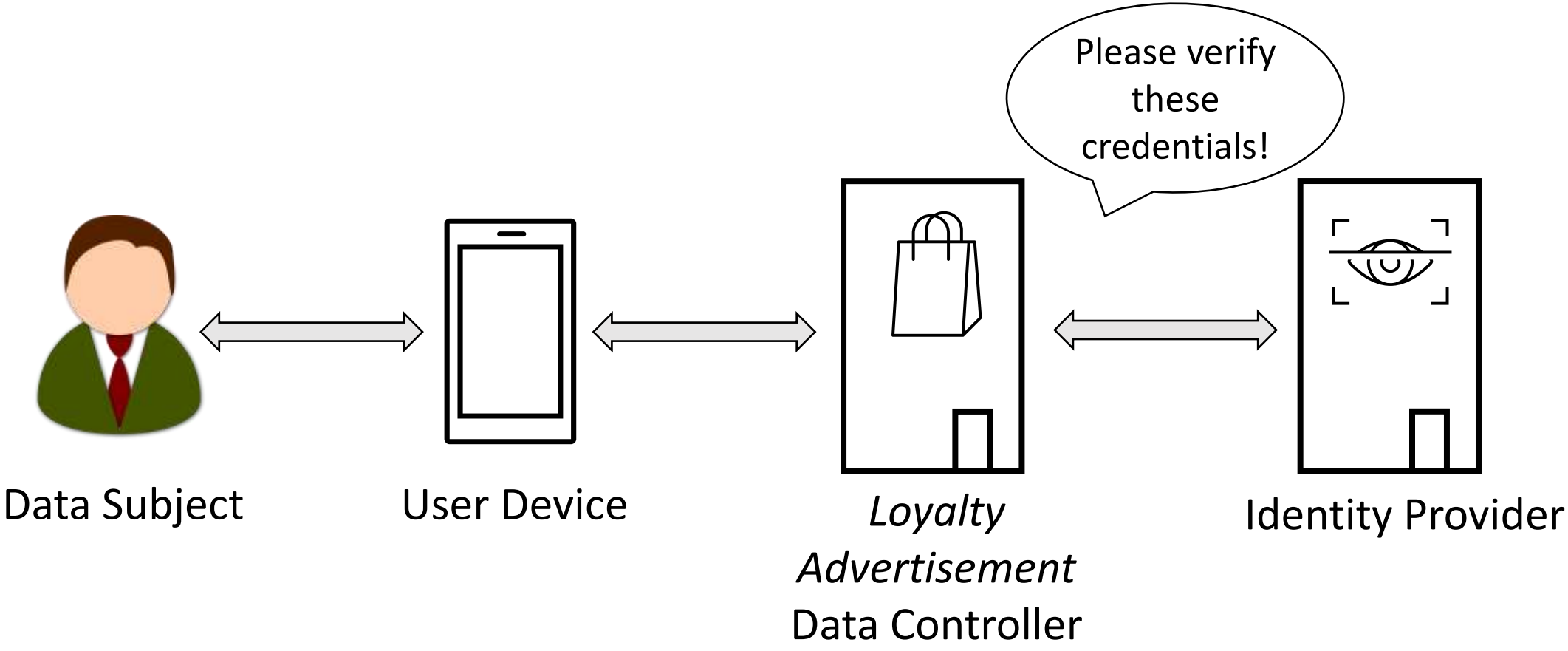
Federated Identity Management Approach

Possible Credentials
family name
first name
date of birth
address
gender
nationality

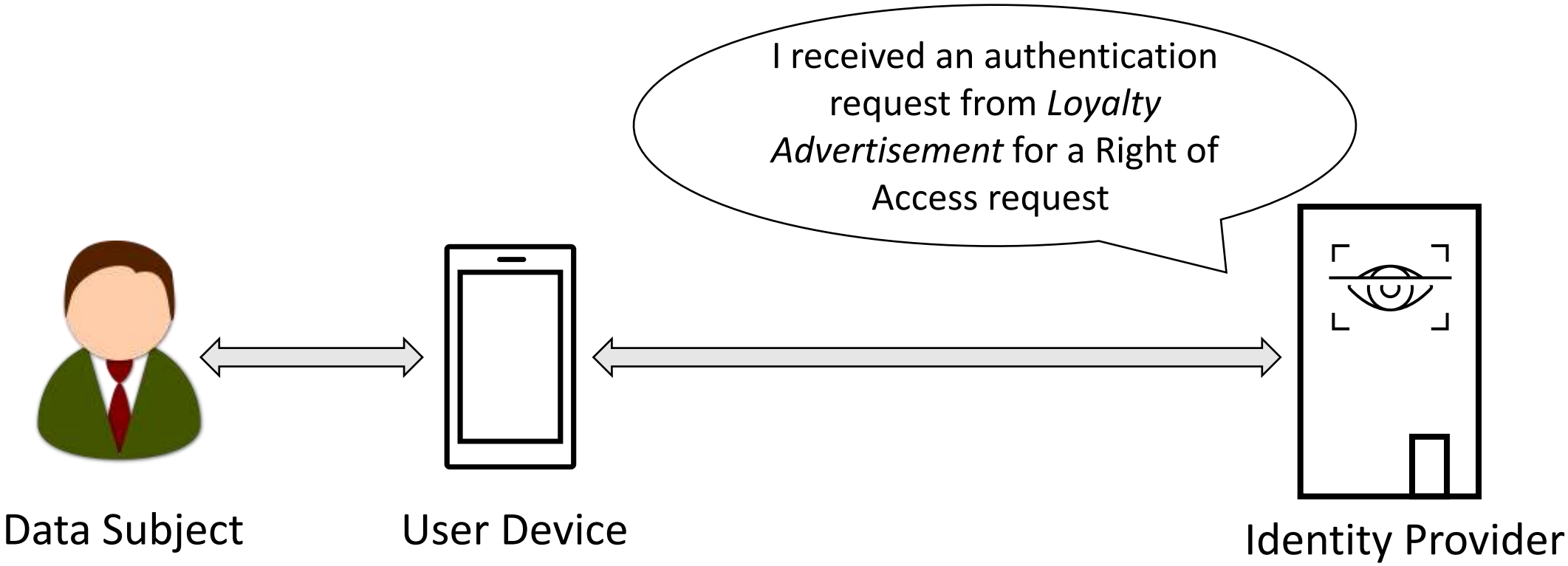


Loyalty
Advertisement
Data Controller

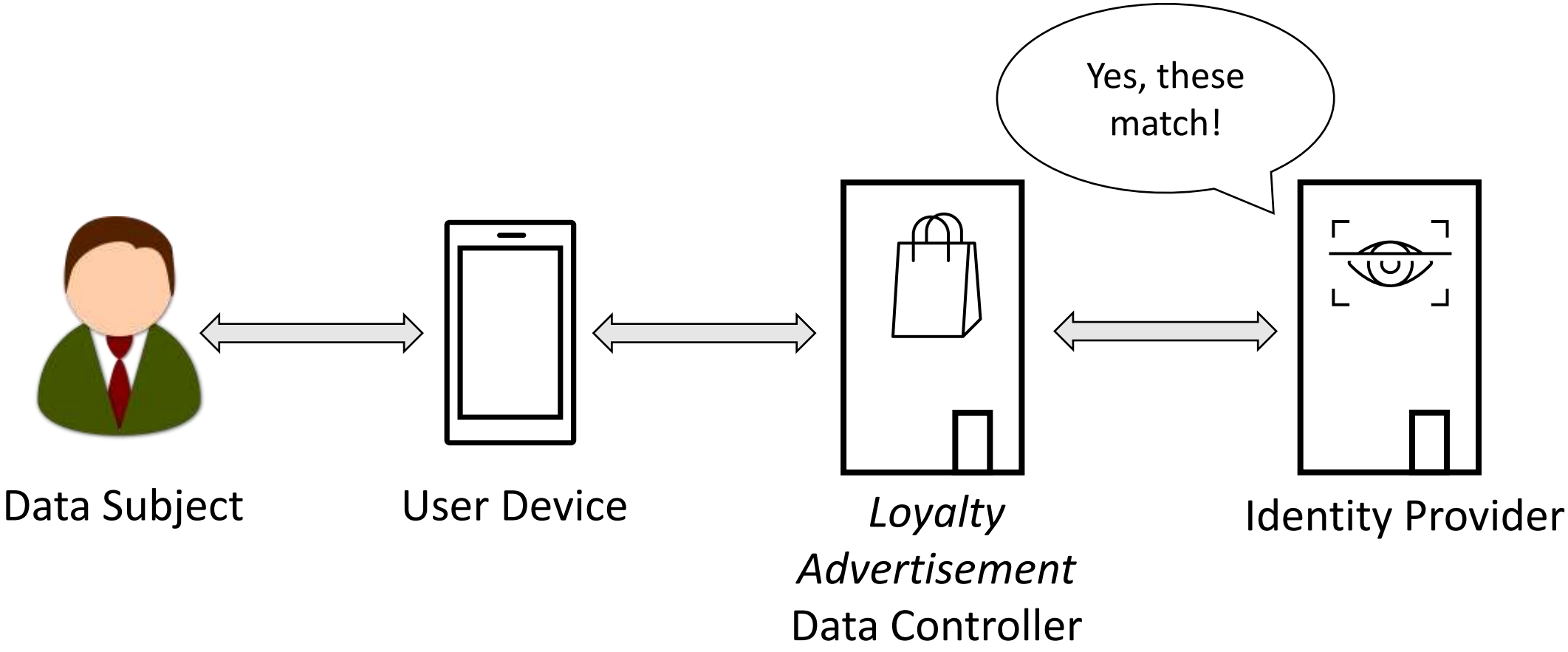
Federated Identity Management Approach



Federated Identity Management Approach



Federated Identity Management Approach

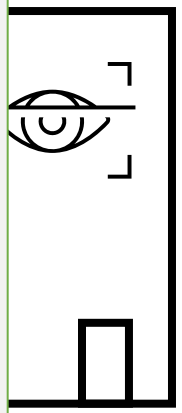


Federated Identity Management Approach

Data Subject

What do we gain?

- Alternative to eIDs
  - Transition period
- Shift of competencies to Identity Provider
  - Data Controller lacking resources
  - Untrusted Data Controller
  - Non-European Data Controller



ty Provider

Discussion

- Authentication threshold
  - How secure is any specific credentials?
  - How secure is any combination of credentials?
- Optional credentials
  - Additional actors?
  - Additional competences?
- Derived credentials
  - Reliability?
- Semantics
  - Standardization?

Conclusion

- Data Subject Rights can have specific demands:
  - Reliability
  - Data minimisation
  - Anonymity
- We must move away from centralized identity models
- eIDs and ABCs are crucial tools in this endeavor
- The European Data Strategy changes our landscape

Move forward with these points in mind!

Thank you!
Any questions?

Contact

Malte Hansen: maltehan@ifi.uio.no

Andre Büttner: andrbut@ifi.uio.no