Authorization Systems as Privacy Enhancing Technology: An integrated Framework

Eda Marchetti
 ✓ Business process and Access Control
 ✓ BP-based Access control for GDPR compliance
   ✓ Procedural steps
   ✓ A possible integration
 ✓ Conclusions and future directions
BP is a graphic representation of a process, similar to flowchart, can be executable

AC ensures that only the intended people can access security-classified data and that these intended users are only given the level of access required to accomplish their tasks.
BP-based Access Control for GDPR
BP-based Access Control for GDPR
BP-based Access Control for GDPR
BP-based Access Control for GDPR

- SN Profile
  - Identity
- Health Data

Access Control
BP-based Access Control for GDPR

- SN Profile
- Identity
- Health Data

Access Control
BP-based Access Control for GDPR

Data Subject
- SN Profile
- Identity
- Health Data

New Rights

GDPR

Responsibilities & Fines

Data Controller

Access Control
BP-based Access Control for GDPR

New Rights

Data Subject

SN Profile

• Identity

Health Data

Responsibilities & Fines

Data Controller

GDPR-based Access Control*
Integrating AC and BP for GDPR Presumption of Compliance

- Identify required attributes
- Author the authorization policies
- Deploy the architecture
- Define the use case
- Gather authorization requirements
Possible scenario

- In case of already exiting BP, leverage the business process to be compliant with the GDPR
- Provide facilities to model business process compliant with the GDPR
Gather all the authorization and business requirements and the sources they come from.

Expressed in terms of statements or natural language authorization policies.
Extend/substitute BP activities with GDPR compliant ones

- pre-defined sets of sub-processes are provided for the different environments
- the sub-processes include specific activities allow the integration with GDPR-based access control systems
Tasks inception

Identify required attributes
Scenario 2 – model business process compliant with the GDPR

Identify required attributes

https://github.com/guerret/lu.uni.eclipse.bpmn2
Details about GDPR Model
Eclipse prototype

Plugin Prototype

ECLIPSE

Java

Data Protection Task
Identify required attributes
Transform the collected GDPR requirements, data and their purposes into machine-interpretable statements, so as to eliminate any ambiguity introduced by natural language.

Author the authorization policies
Specify the purposes

a.

b.

c.
Author the authorization policies

SPECIFY IMPLICIT ATTRIBUTES

a. 

b. 

c. 

Duration 30 Days
StartingDate 2018.11.14
Deploy the architecture:
list of XACML policies
encoding the GDPR principle
are specified and deployed into the architecture
Final integration
Where are we?

- GATHER AUTHORIZATION REQUIREMENTS
- DEFINE THE USE CASE
- IDENTIFY REQUIRED ATTRIBUTES
- AUTHOR THE AUTHORIZATION POLICIES
- DEPLOY THE ARCHITECTURE