Chapter 20
Policy Implementation in XACML

Slim Trabelsi and Akram Njeh

Abstract This chapter presents the implementation details of the PrimeLife policy engine (called PPL engine). This engine is primarily in charge of interpreting the policies and the preferences defined by the Data Controllers and the Data Subjects. Additionally, this engine is responsible for the enforcement of the privacy rules specified by the user. The enforcement is characterised by the application of the access control rules, the execution of the obligations and the generation/verification of the cryptographic proof related to the credentials. In this chapter we describe the architecture of this engine, the structure of policy language, and finally the data model of the implementation.

20.1 Introduction

Since the PPL language is specified as an extension of the XACML (eXtensible Access Control Markup Language) language, the PPL engine is designed to run together with any XACML engine (that only handles XACML access control rules). The architecture chosen for the deployment of the PPL engine is symmetric because Data Subjects and Data Controllers have similar requirements: Deciding whether a given piece of personal information (resp. collected data) can be shared with a Data Controller (resp. Third Party); handling obligations associated with data; storing data and associated preferences (resp. sticky policies). Using the same architecture everywhere to handle scenarios where one party can have multiple roles (e.g., collecting data and then disclosing it to third parties). The PPL engine executes multiple tasks in automated ways such as: Enforcing access control policies, generating and verifying cryptographic proofs related to credential requirements, matching between data handling preferences and data handling policies, generating and enforcing sticky policies, checking Authorisation, controlling the downstream usage of data, handling obligations, etc.
20.2 Architecture

In this section, we will present the design phase of the PPL engine. We present the architecture of the PPL system by defining a high level and a detailed architecture.

20.2.1 High Level Architecture

As presented in (Figure 20.1) below, the high level architecture presents an abstract overview of the PPL architecture and the interaction between the different entities; Data Subject, Data Controller and Third Party (Downstream usage).

![High Level Architecture Diagram](image)

Fig. 20.1: High level architecture.

20.2.1.1 Data Subject

*Policy engine*: This component is in charge of parsing and interpreting the privacy preferences of the Data Subject. This policy engine supports the entire PrimeLife Language capabilities (Preferences, Access control, DHP, Obligations, Credentials etc). For this reason, this module is replicated on the Data Controller side and the third party side.

*Repository*: Represents the PII and policy repositories. It is a database containing data owned by the Data Subject. This data could be composed of personal data, credentials, certificates, and other information that should be used during the interaction with the Data Controller application. It also contains the policy files representing his privacy preferences.

*Interface and communication*: This interface represents a communication interface with the Data Controller implementing the message exchange protocol.