Faculty of Health, Science and Technology

Michael Oggolder

A Privacy-Policy Language and

a Matching Engine for U-PrIM

Computer Science
C-level thesis

Date/Term: 12-12-12
Supervisor: Tobias Pulls
Examiner: Donald F. Ross
Serial Number: C2013:06

Karlstads universitet 651 88 Karlstad
Tfn 054-700 10 00 Fax 054-700 14 60
Information@kau.se www.kau.se

A Privacy-Policy Language and a Matching Engine for U-PrIM

Michael Oggolder

This thesis is submitted in partial fulfillment of the requirements for the Bachelors degree in Computer Science. All material in this thesis which is not my own work has been identified and no material is included for which a degree has previously been conferred.

Michael Oggolder

Approved, 12/12/2012

Opponent: Stefan Gehring

Advisor: Tobias Pulls

Examiner: Donald F. Ross

Abstract

A privacy-policy matching engine may support users in determining if their privacy preferences match with a service provider's privacy policy. Furthermore, third parties, such as Data Protection Agencies (DPAs), may support users in determining if a service provider's privacy policy is a reasonable privacy policy for a given service by issuing recommendations for reasonable data handling practises for different services. These recommendations need to be matched with service provider's privacy policies, to determine if a privacy policy is reasonable or not, and with user's privacy preferences, to determine if a set of preferences are reasonable or not.

In this thesis we propose a design of a new privacy-policy language, called the U-PrIM Policy Language (UPL). UPL is modelled on the PrimeLife Policy Language (PPL) and tries to improve some of PPL's shortcomings. UPL also tries to include information deemed mandatory for service providers according to the European Data Protection Directive 95/46/EC (DPD). In order to demonstrate the features of UPL, we developed a proof-of-concept matching engine and a set of example instances of UPL. The matching engine is able to match preferences, policies and recommendations in any combination. The example instances are modelled on four stages of data disclosure found in literature.

Keywords: privacy, privacy policies, policy matching engine, data protection

Contents

List of Figures

Listings

List of Tables

List of Abbreviations

PPL PrimeLife Policy Language

P3P Platform for Privacy Preferences Project

XACML eXtensible access control markup language

U-PrIM Usable Privacy-enhancing Identity Management for smart applications

UPL U-PrIM Policy Language

DPA Data Protection Agency

DPD European Data Protection Directive

Chapter 1

Introduction

The Internet and mainly so-called Web 2.0 applications have taken a major part in the life of millions of people all over the world. Facebook[1], one of the biggest social network sites on the Internet, has more than one billion registered and over 580 million daily active users [Fac12]. The fact that it has become very common for people to share a lot of detailed information about their private and professional lives has also caused serious privacy concerns [TNR11]. For users of social network sites, and other kinds of Internet services, it is hard to keep track of the information that is shared with several platforms on the Internet. The Eurobarometer analytical report of 2008, "Data Protection in the European Union: Citizens' perceptions" [Org08], shows the trend that users are more concerned about privacy than five years ago. Two-thirds of survey participants said they were concerned whether organisations that held their personal data handled this data appropriately. Furthermore, more than a third of Internet users do not read privacy policies at all and 24% read them without fully understanding them [Soc11]. Therefore, it would be helpful to support users with understanding privacy polices and accordingly reduce their privacy concerns.

[1] Facebook, `https://www.facebook.com` (accessed 20/11/2012)

1.1 Motivation and Goals

Legal regulations concerning data privacy, such as the European Data Protection Directive (DPD) [Eur95], compel service providers to provide privacy policies that explains, among other things, how they will use the personal data that they collect. Privacy policies are usually long and written using legal terms, resulting in them rarely being fully understood, or even read at all, by users [TNR11]. Consequently, users are not aware how their data actually will be treated when they disclose data to websites. One proposed solution to this problem is to provide automated support for users in their decision if they actually want to disclose specific private information for getting access to a particular service under the stated privacy policy of the service provider.

In order to support users in such a decision with automated tools, both, the user's privacy preferences and the privacy policy of the service provider need to exist in a machine-readable form, such as privacy policy language. Before a user discloses data to a service the user's privacy preferences and the service's privacy policy needs to be matched. The result of the match tells the user if a match between both privacy statements could be found or not.

The goal of this thesis is to design a privacy policy language that comes up to all state-of-the-art requirements, and to develop a proof-of-concept policy matching engine for this privacy policy language, in order to support a user in determining if two privacy statements are matching or not.

1.2 Disposition and Scope

In Chapter 2 we introduce relevant related work in the area of privacy policies. The chapter ends with pointing out some shortcomings of the data handling part of the PrimeLife Policy Language (PPL). Based on the discussion in Chapter 2, Chapter 3 starts with proposing requirements for the design of a new privacy-policy language. The scope of the design

is limited to the data handling part of a privacy-policy language. Next, we present our privacy-policy language: the U-PrIM Policy Language (UPL). The chapter ends with describing some sample instances of our policy language. In Chapter 4 a proof-of-concept prototype of a privacy-policy matching engine for UPL is presented. The chapter ends with a presentation of sample input and output, based upon the sample instances of the language described in Chapter 3. In Chapter 5 we evaluate the result of the work done. Finally, Chapter 6 closes the thesis with a conclusion. Appendix A contains the XML schema of UPL and sample instance based on the stages discussed in Chapter 3. Furthermore, there can be found the full sample input files for the test case presented at the end of Chapter 4.

Chapter 2

Background

This chapter discusses relevant related work in the area of privacy policies. First, we introduce the Platform for Privacy Preferences Project (P3P). Next, we discuss the data handling part of the PrimeLife Policy Language (PPL) and compare it to P3P. The chapter ends with identifying new requirements for our policy language (presented in Chapter 3), that stem from both the DPD [Eur95] and identified shortcomings of PPL's data handling part.

2.1 Platform for Privacy Preferences Project (P3P)

The P3P standard was issued in April of 2002 by the World Wide Web Consortium (W3C). It enables websites to express their privacy policies in a standard, machine-readable format which can be interpreted easily by user agents [LL03, CES+08].

The W3C created P3P to increase the user understanding of website privacy policies. P3P policies are eXtensible Markup Language (XML) documents, that provide information about the website owner (the `entity` element), types of information that may be collected (the `categories` element), how information may be used (the `purposes` element), if and how information is shared with third parties (the `recipient` element), data retention poli-

cies (the `retention` element), and options for a possible dispute resolution (the `disputes` element). A website can have different privacy policies for different parts of the website or just one policy for the whole website. In a so-called *policy reference file* it is listed which policy applies to which part of a website. There are three ways how a website can indicate that privacy practices are expressed in a P3P policy: The most common way is to place the reference file in a standard *well-know location*: `/w3c/p3p.xml`. Alternatively, it is possible to add either a HTTP response header or a `<link>` tag in the HTML content that advertises the location of the policy reference file [CDE+06]. For describing a user's privacy preference the W3C issued a language called APPEL (A P3P Preference Exchange Language) accordingly. The matching of the website's privacy policy against the user's privacy preference is usually done at the client's user agent before accessing the website. P3P has been implemented in two web browsers and in several dedicated P3P user agents [CES+08, TNR11].

One of the first P3P clients was Microsoft's *Internet Explorer 6* (IE6), which allows users to specify personal privacy preferences regarding the conditions under which the browser will accept cookies from websites. IE6 does not consider full P3P polices in its decision, but allows the user to access the human-readable parts of a P3P policy. Also *Netscape Navigator 7* includes P3P functionality which allows the user to specify his or her privacy preferences regarding the acceptance of cookies. A better exploitation of the capabilities of P3P is offered by At&T's *Privacy Bird*[1]. Users can either choose from three pre-packed preferences or define their own individual privacy preference in an APPEL file. Before visiting a website the At&T privacy bird will match the user's preferences against the website's policy and shows the result in form of a either green (in case of a match) or a red (in case of a mismatch) bird icon. If there is no policy present, the bird icon is shown in yellow [CES+08, TNR11].

[1] At&T Privacy Bird, `http://www.privacybird.org/` (accessed 26/10/2012)

2.2 PrimeLife Policy Language (PPL)

In the context of the European ICT research project *PrimeLife*[2], between March 2008 and October 2011, the consortium proposed a privacy-friendly language for access control: the PrimeLife Policy Language (PPL) extends the eXtensible access control markup language (XACML)[3] with data handling, credential capabilities, a new obligation handling mechanism, and a downstream usage authorization system [ABdV+09].

As XACML is language for access control consisting of access rules, policies and policy sets, PPL extensions apply to these components. Next to the target element describing the resource, the subject and environment variables, the main components of a rule are the *credential requirements* and the *data handling* part. Credential requirements are intended for providing an authenticated statement about an attribute value. This mechanism should enable user-centric and privacy-friendly access control within PPL, primarily through the use of anonymous credentials, such as identity mixer (idemix) or U-Prove [CL01, CH02, BCP11, CL04, IBM12, Bra00].

Furthermore, each rule may contain a number of *data handling policies*, describing which information needs to be revealed to come up to the access control conditions and how the revealed data will be handled. Additionally, a *data handling preference* describes how the resource that is protected by the rule has to be treated [ABdV+09]. As PPL is designed to be used on the one hand by the operator of a website (called *data controller*) and on the other hand by the user (called *data subject*[4]), data handling preferences are mainly used to let the data subject specify how he/she wants his/her personal data to be treated while the data controller expresses how he/she will use collected data in the

[2]PrimeLife, `http://www.primelife.eu/` (accessed 26/10/2012)

[3]OASIS eXtensible Access Control Markup Language (XACML), `https://www.oasis-open.org/committees/xacml/` (accessed 30/10/2012)

[4]The terms *data controller* and *data subject* in PPL originates from the EU Data Protection Directive, where a data controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. This personal data is any information relating to an identified or identifiable natural person, called the data subject [Eur95, Article 2].

data handling policy. This data includes implicitly collected data (such as IP addresses and connection time) as well as data explicitly reveal by the user (such as name or e-mail address). [ABdV+09]

For comparing PPL to P3P, the most relevant area of PPL to focus on is its data handling part. A PPL data handling policy contains two elements which allow to express how personal data is proposed to be treated: *authorizations* and *obligations*. In order to specify actions that the data controller is allowed to perform for particular personal data, authorizations are used in PPL. There are two types of authorizations:

1. The first concrete authorization type is a set of *purposes* that restricts—like in P3P—the data usage to these.

2. The second concrete authorization type is called *downstream usage* and describes if and how data may be passed on to third parties, to so-called downstream data controllers.

While authorizations specify which actions are allowed to be performed, obligations express actions that are required to be performed in particular conditions by the data controller. Trabelsi et al. [TNR11] define obligations for PPL as follows:

> *A promise made by a data controller to a data subject in relation to the handling of his/her personal data. The data controller is expected to fulfill the promise by executing and/or preventing a specific action after a particular event, e.g. time, and optionally under certain conditions.*

Consequently the structure of an obligation could be defined as Event-Condition-Action [ABdV+09, TNR11]:

`On` **`Event`** `If` **`Condition`** `Do` **`Action`**

To facilitate the comparison of obligations the authors of PPL considered triggers as events filtered by conditions. The resulting structure of an obligation is a set of events (triggers) that result in an action [ABdV+09, TNR11]:

```
Do Action when Trigger
```

As it is not possible to cover all real-life events with triggers and actions the authors of PPL tried to find a generic, extensible form, describing *how* an obligation should look like, rather than describing *which* obligations should be part of the language. An example for a triggered action could be: *When personal data of a data subject is passed on to a downstream controller, notify the data subject.*

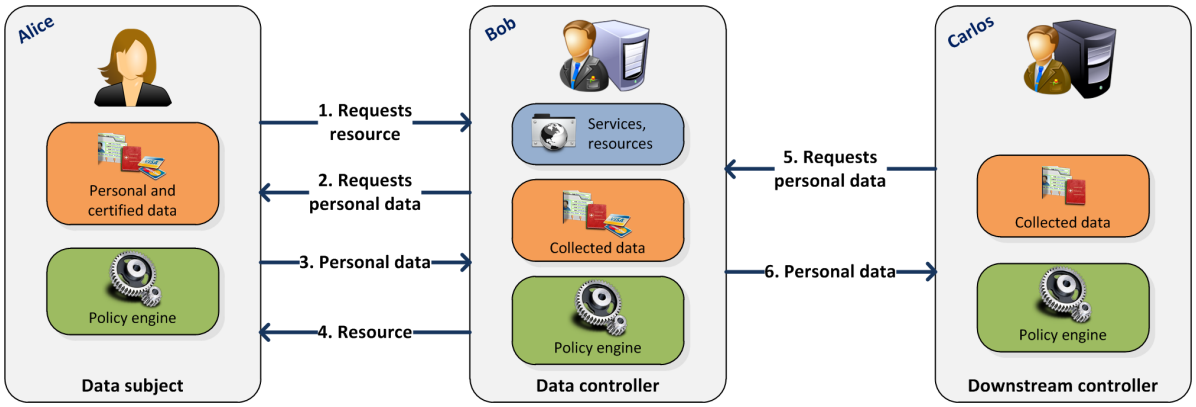

Figure 2.1: The data subject requests access to a resource hosted by the data controller. The data subject needs to reveal personal data as well as certified data to the data controller. The collected personal data may be passed on to the downstream controller.

Figure 2.1 illustrates a typical usage scenario. The data subject *Alice* requests access to a resource hosted by the data controller *Bob*. In order to be granted access she has to reveal some personal data, including data certified by credentials. Furthermore, Bob may want to forward Alice's personal data to to a third party, such as the downstream controller *Carlos*[5]. Alice specifies in PPL's data handling preference which data she wants to reveal, how they should be treated and if the data controller may pass them downstream. The data controller specifies in PPL's data handling policy how he intends to use the requested data. The privacy policy and the privacy preference are matched in the policy engine.

[5]From now on the user in the role of the *data subject* is represented by Alice, the *data controller* by Bob and the *downstream controller* by Carlos. In terms of political correctness each of these three parties can be either male or female. The example characters are used to facilitate reading.

In accordance with Trabelisi et al. [TNR11] the main features and the main contributions over prior arts of PPL are:

- **Two-sided data handling policies/preferences with automated matching** Both, the data controller and the data subject specify in a policy file how collected data will be treated (in case of a privacy policy) respectively should be treated (in case of a privacy preference). A policy matching engine detects if a match can be found comparing both files.

- **Credential-based access control** The access control condition specifies the credentials that need to be presented by a data subject. The concept of credentials acts as useful abstraction for many authentication technologies, including especially anonymous credentials.

- **Language symmetry** Both, a data controller's privacy policy and a data subject's privacy preference can be expressed by using the same language schema. This allows easy matching.

- **Downstream usage** The data subject may specify if and how her collected data (or just parts of it) may be passed downstream.

- **Event based obligations** With the combination Trigger/Action events can be attached to the execution of an obligation.

In summary, the main innovation of PPL compared to P3P in terms of data handling is the *language symmetry*, which allows personal data to be viewed as a special type of resource. Hence the data subject can express to whom and under which condition she is willing to reveal her resource (the personal data), as well as the data controller restricts the access of his actual resource in the same way. As a result the *two-sided data handing* allows automated matching of policies and preferences. By exploiting this language symmetry it is also easy to express possible *downstream usage* practices. Furthermore, *credential-based*

access control allows to request access, e.g. via anonymous credentials in a privacy-friendly way.

2.3 Space for Future Work

In this section, we discuss some shortcomings of PPL, primarily with regard to data handling. Most components of P3P and PPL (such as purposes, downstream usage and obligations) are also necessary to obey to data privacy laws like the Data Protection Directive[6] (DPD) of the European Union. The DPD [Eur95, Articles 10 & 11] states that the data controller has to provide the data subject whose personal data is processed among others the following information:

- the identity of the controller and of his representative, if any;
- the purposes of the processing for which the data are intended;
- the recipients or categories of recipients of the data.

Furthermore, the draft legislative package of the European Commission which was unveiled on the 25th of January 2012 adds among others two main innovations to the DPD [vB12]: the first alteration is the so-called *"right to be forgotten"* which commits the data controller to erase all personal data of data subject, for retaining, if the data subject requests it. The second alteration is the *data breach notification*, which commits the data controllers to notify data subjects about any breach of personal data without undue delay. Both new requirements could be expressed with obligations in PPL. The previously mentioned *purposes of the processing* can be expressed with the purpose authorization component in PPL. However, it not possible to provide further identity information of the data controller nor of any downstream data controller within the policy.

[6]Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Eur95]

The "right to be forgotten" can be modelled in PPL by using obligations, where the data subject triggers the deletion of her data. In order to express data retention in PPL, obligations triggered by time are needed. Though, the data retention time for several purposes, for what that data may be used, could be different. *For example, the contact details of a web store customer's have to be retained for accounting purposes several years while the customer may wish that the same data may not be used anymore for marketing purposes after one year.* The concrete privacy policy would become very complex when trying to express this scenario in PPL. In order to avoid this issue the data retention time needs to be bound to the purpose of data usage, not to the whole attribute.

Another point to discuss about privacy policies are security aspects, like integrity, authenticity and non-repudiation. As it is common for security topics, in the following the worst-case example: *A malicious data controller Mallory asks the data subject for a bunch of very personal data, in order to grant access to the resource the data subject requested. Later on, when the data subject notices that the requested resource was not worth to reveal all this personal data and complaining at e.g. the national data protection agency, the malicious data controller just could repudiate that he requested this data and present a different policy.* A digitally signed policy would meet each of the security targets and solve this issue. The digital signature would tell a data subject that the privacy policy verifiable applies to data controller he is trying to connect (*authenticity*) and no one modified the policy in transit if the signature and the certificate of the signature is valid too (*integrity*). Hence, the data subject may save the signed policy and the corresponding certificate for the reason of *non-repudiation.*

However, the fact that a policy is signed (it could also be self-signed) does not say anything about the content of the privacy policy. The data controller could ask for more data than he actually needs to process the request of the data subject for a certain purpose, i.e., diverge from the privacy principle of *data minimisation.* In order to guarantee that a data controller is asking for the minimum of data for a legitimate purpose an authenticated

statement from a trusted third-party is needed. This statement could be specific or generic.

A generic statement could take the form of a *recommendation* from the trusted third-party, such as a data protection agency. The recommendation would have to be bound to a particular *context*, i.e., the *higher level purpose* of the request for data. For example, the data needed by a data controller for shopping shoes online differs from the data needed when shopping for a new house.

A specific recommendation could be realised through a privacy *seal*, such as is already issued by for example TRUSTe[7]. This privacy seal could take the form of a signature on a data controller's policy.

2.4 Summary

In this chapter we discussed and compared P3P and the data handling part of PPL. The discussion of the shortcomings regarding special scenarios and the requirements of the DPD [Eur95] in the data handling of PPL gives a basis for a design of a new policy language, described in the following chapter.

[7]TRUSTe, `http://www.truste.com/` (accessed 05/11/2012)

Chapter 3

Design of a New Privacy-Policy Language

Usable Privacy-enhancing Identity Management for smart applications (U-PrIM) is the name of a research project involving the departments of Computer Science, Information Systems and Psychology at Karlstad University (KaU)[1], in collaboration with industry partners Nordea Bank[2] in Denmark and Gemalto[3] in Sweden. The purpose of the project is to find ways of using future mobile technologies that are secure, privacy-friendly and easy to use [Ang11]. Part of the research project is to implement a new privacy policy language that enable users (assuming the role of data subjects) to validate that data requests made by a service provider (data controller) complies with the privacy principle of data minimisation.

[1]Karlstad University, `http://www.kau.se` (accessed 02/11/2012)
[2]Nordea Bank, `http://www.nordea.com/` (accessed 02/11/2012)
[3]Gemalto, `http://www.gemalto.com/` (accessed 02/11/2012)

3.1 Requirements for a new Privacy-Policy Language

Considering the discussion on space for further work discussed in Section 2.3 the requirements for a new privacy policy language—named the U-PrIM Policy Language (UPL)—will be examined in this section.

The *language symmetry* brought appreciable advantages in PPL. Hence, UPL should be considered to be designed as a symmetric language too. Easy matching of privacy practices of different parties would be possible consequently. The data subject specifies in a *preference* file how her personal data may be treated. The data controller specifies in a *policy* file how he intends to used the collected personal data. Beside the data subject and the data controller, a trusted third party should be considered in UPL. This third party issues *recommendations* for how data should be handled. Good examples of third parties would be Data Protection Agencys (DPAs) or non-governmental organisations such as the Electronic Frontier Foundation (EFF)[4]. A recommendation is a general statement bound to a particular *context*, i.e., the *higher level purpose*. It should state what is a reasonable request in terms of data to be revealed, for which purpose the data should be processed, and at least what obligations the data controller should adhere to.

Internet users (for our intents and purposes, data subjects) are often not aware what data they actually should reveal for different services. In addition, data controllers tend to ask for more information than they actually need for their core task. In order to release users from thinking a lot about their privacy preferences they could just adapt them to agree with a recommendation from a third party they trust. Consequently, in order to present themselves to customers (data subjects) in a trustworthy way data controllers could adjust their privacy policy to comply with a recommendation. As illustrated in Figure 3.1 policies for data controllers, preferences for data subjects, and recommendations by third parties (such as DPAs) could be matched against each other to determine if they match or not.

In accordance to the European Data Protection Directive [Eur95], and to enable giving

[4]Electronic Frontier Foundation, `https://www.eff.org/issues/privacy` (accessed 05/11/2012)

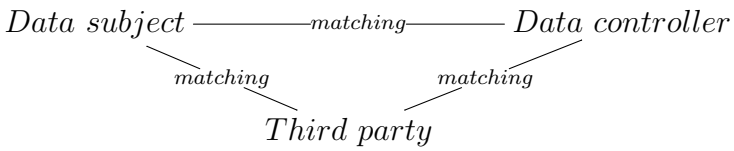

Figure 3.1: Overview of required matching by the policy matching engine.

more contact details than e.g. an X.509 certificate offers, adding an identity element to the language should be considered. These further identity information could be for example the postal address, a name of a representative or an emblem of the organisation.

As discussed in Section 2.3, a digital signature is essential for security reasons, hence it should be considered in UPL. Furthermore, it would be good to consider in addition to the indirect way of showing trustworthiness (adjust a data controller's policy to comply with a recommendation) a direct way, like it is possible in PPL and P3P. Therefore a policy should be able to get a seal from a third party, such as a DPA. This seal could be another digital signature attesting that the data controller will request only the minimum data for a certain purpose.

In general, users are willing to reveal different amount of personal data depending on what service they are using. For example, for a governmental citizen service page users a more willing to give their personal data than for a discussion board for pet owners. Therefore users would define varying privacy preferences for different *"higher purposes"*. Data controllers, that offers different services may wish to define policies under different "higher purposes", as well as different recommendations from a third party can be issued for different "higher purposes".

For some applications it might be essential for the data controller that the collected data is certified (compare credentials in PPL [TNR11]). Therefore, it should be considered to be able to certify attributes using the policy language. In accordance to Section 2.3, it can be necessary to have different data retention times for different purposes. This should be considered in the design of the new policy language. Moreover, the obligations used in

PPL should be considered to be adopted in order to have the ability express obligations demanded by the DPD.

Summing up the functional requirements for the design and implementation for a new privacy-policy language are as follows:

1. Keep language symmetries as in PPL.
2. Besides preferences and polices, recommendations should be considered.
3. Comply to requirements of the European Data Protection Directive [Eur95]; especially about the identity element and the elements in the new draft legislative package of the European Commission [vB12], such as the "data breach notification" and the "right to be forgotten".
4. Consider a digital signature and a possibility to certify a policy with a seal from a third party.
5. Consider a way to have different data retention times for different purposes.
6. Policies, recommendations and preferences should have a "higher purpose".

An additional non-functional requirement is to facilitate an easy matching procedure for the policy language instances.

3.2 Design of a New Privacy-Policy Language

Based on the the requirements collected in Section 3.1, we created a language schema for UPL based upon primarily the design of the data handling part of PPL. The complete schema can be found in Appendix A.1.

The heart of the language schema is a `Container` element typified by a `type` attribute. The type of a container can be either policy, preference or recommendation. We require

that a policy and recommendation are digitally signed, so a `Signature` element is added next to the `Container` element. In order to come up the language symmetry the `Signature` element is also mandatory for a preference, but the signature itself may then be empty. Furthermore, an additional element for seals from third parties should be considered; hence a `CertifiersSetForSeals` is added on the same level, which is intended to contain a set of certifiers. The schema specification of the `UPL` element (which is the XML document root), depicted in Listing 3.1, shows that the `Container` and `Signature` element are mandatory while the `CertifiersSetForSeals` element is optional. The `Signature` element contains the Base64 encoded string of the signature over the container.

```
1   <!-- UPL-Root -->
2   <xs:element name="UPL">
3     <xs:complexType>
4      <xs:sequence>
5        <xs:element ref="Container"/>
6        <xs:element ref="Signature"/>
7        <xs:element ref="CertifiersSetForSeals" minOccurs="0"/>
8      </xs:sequence>
9     </xs:complexType>
10  </xs:element>
```

Listing 3.1: The specification of the `UPL` root element. The child elements `Container` and `Signature` are mandatory, while the `CertifiersSetForSeals` is optional.

Listing 3.2 shows the `type` attribute specification of the `container` element. The type has to be either policy, preference or recommendation.

```
1   <!-- Container-Type-Attribute -->
2   <xs:attribute name="type">
3     <xs:simpleType>
4       <xs:restriction base="xs:string">
5         <xs:pattern value="policy|preference|recommendation"/>
6       </xs:restriction>
7     </xs:simpleType>
8   </xs:attribute>
```

Listing 3.2: The specification of the `type` attribute, which is used within the `Container` element. The type has to be either policy, preference or recommendation.

The first child of the container should be an element specifying the “higher purpose” of the `container`. Since a container could have several higher purposes a set element should be considered (compare Listing 3.3). The authors of PPL reused the purposes described

in P3P [CDE+06, Section 3.3.5]. These purposes also fit for the `HigherPurpose` element in UPL.

```
1   <!-- HigherPurposesSet -->
2   <xs:element name="HigherPurposesSet" type="HigherPurposesSet"/>
3   <xs:complexType name="HigherPurposesSet">
4       <xs:sequence>
5           <xs:element name="HigherPurpose" minOccurs="1" maxOccurs="unbounded"
                type="xs:string"/>
6       </xs:sequence>
7       <xs:attribute name="semantics">
8     <xs:simpleType>
9       <xs:restriction base="xs:string">
10        <xs:pattern value="and|or"/>
11      </xs:restriction>
12    </xs:simpleType>
13  </xs:attribute>
14  </xs:complexType>
```

Listing 3.3: The specification of the `HigherPurposesSet` element. One or many `HigherPurpose` child elements are allowed. The `semantics` attribute may be either *AND* or *OR*.

Purposes are specified by standard URIs specified in agreed-upon vocabularies. They can be either organised as flat lists or hierarchically [ABdV+09]. Furthermore, it is possible to specify the semantics of several higher purposes by using the `semantics` attribute within the `HigherPurposesSet` element. This can by either an *AND* or an *OR* semantic. The AND semantic is more restrictive in terms of matching, saying that it will only be a match if the complete set of higher purposes match. Unlike for the OR semantic it would be a match too if any of e.g. the three data subject's higher purposes (*communicate*, *account*, and *marketing*) are used by a data controller. This means that also a subset of the higher purpose would be a match.

The next element inside the container is the `Identity` element which gives information about the identity of either the data controller (in case of a policy) or the third party which issues recommendations (in case of a recommendation). In case of a preference, the `Identity` element exists but is empty (compare line 6 in Listing 3.6). Therefore all child elements need to be optional. The Listing 3.4 shows an example `Identity` element. The `CertificateURL` element refers to the location of the certificate that corresponds to the

private key used to sign the `Container` element.

```
<Identity>
    <Identifier>Data Protection Agency of Sweden</Identifier>
    <Representative>Mrs. Jane Gustafsson</Representative>
    <Country>SE</Country>
    <Email>contact@dpa.gov.se</Email>
    <Phone>+46 1 234 56 78 90</Phone>
    <URI>www.dpa.gov.se</URI>
    <HumanReadablePolicyURL>http://dpa.gov.se/privacy-seals/en/</
        HumanReadablePolicyURL>
    <CertificateURL>http://dpa.gov.se/imprint/policy_seal_certificate.pem</
        CertificateURL>
    <EmblemURL>http://dpa.gov.se/imprint/logo.svg</EmblemURL>
</Identity>
```

Listing 3.4: An example for an `Identity` element with all child elements filled out.

The actual data handling is specified within the `AttributesSet` element. An `AttributesSet` contains a set of attributes whereupon each `Attribute` is about exactly one particular data subject's attribute (e.g. her e-mail address, compare Listing 3.5) requested by the data controller. The `AttributeValue` child element entitles this attribute. Since the data controller may use each attribute for different purposes the `Attribute` element contains another child element called `PurposesSet`. The `PurposesSet` is a list of several purposes under which the specific attribute may be used. Each `Purpose` element comes with an `expirationTime` attribute. This expiration time specifies for how long (from the point of data disclosure) the attribute may be used for the particular purpose.

If a data controller requests that certain information is certified by a third party he can set the `certifiedBy` attribute of the `Attribute` element to a key that corresponds to a certifier specified in the policy. The `certifiedBy` attribute is an identifier for an entry in `CertifiersSetForAttributes` for a particular certifier (`CertifierForAttribute`). This `CertifierForAttribute` element is identified by the attribute `certifierId`. In order to give further details about the certifier the previous specified `Identity` element is reused for the `CertifierForAttribute` element.

```
<Attribute certifiedBy="SE-GOV-CA">
    <AttributeValue>Email</AttributeValue>
    <PurposesSet>
```

```
4         <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/account</
              Purpose>
5         <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/marketing</
              Purpose>
6     </PurposesSet>
7     <ObligationsSet>
8         <Obligation>
9             <TriggersSet>
10                <TriggerPersonalDataDeleted>
11                    <MaxDelay>P1D</MaxDelay>
12                </TriggerPersonalDataDeleted>
13                <TriggerOnViolation>
14                    <MaxDelay>P5D</MaxDelay>
15                </TriggerOnViolation>
16            </TriggersSet>
17            <ActionNotifyDataSubject/>
18        </Obligation>
19    </ObligationsSet>
20 </Attribute>
```

Listing 3.5: An example for an `Attribute` element. The `AttributeValue` specifies the value of the attribute. In case of a policy, i.e., a request for data, the value is the type of the attribute, such as Email. Within the `PurposesSet` several purposes with an appropriate data retention time are listed. The `ObligationsSet` element contains several obligations consisting of triggers and actions. Each trigger has `MaxDelay` child element indicating the maximum delay for an action after the trigger event occurred.

Besides the intended purposes of data usage (expressed by the `PurposesSet` element) the `Attribute` element contains an `ObligationsSet` element. As discussed in Section 2.2, obligations are commitments made by the data controller. Like in PPL, obligations in UPL are defined as (event) triggered actions. The `ObligationsSet` element may contain several `Obligation` elements whereupon each obligation consists out of one ore more `Trigger` elements and one `Action` element. Moreover each `Trigger` element contains an element `MaxDelay` saying in which time frame the specified action has to be triggered. The following list describes example triggers and actions that can be used in UPL:

- **TriggerPersonalDataDeleted** Triggers an action if any personal data of the data subject has been deleted;
- **TriggerPersonalDataSent** Triggers an action if any personal data of the data subject has been passed on to a third party;

- **TriggerOnViolation** Triggers an action if a violation regarding the personal data of the data subject has been noticed;
- **TriggerOnDataSubjectRequests** Triggers an action if the data subject sends a request (including an action) to the data controller;
- **ActionDeletePersonalData** All personal data of the data subject has to be deleted;
- **ActionNotifyDataSubject** The data subject has to be notified about the event that trigger this action.

In reference to the example in Listing 3.5 it could happen that the data subject has to be notified (*action*) about the deletion of her e-mail address (*trigger*) by the data controller. If the e-mail address is the only way for communicating with the data subject the, the ability of the data controller to live up to such an obligation is questionable.

```
1  <!-- Container (abstract) -->
2  <xs:element name="AbstractContainer"/>
3  <xs:complexType name="AbstractContainer" >
4    <xs:sequence>
5      <xs:element ref="HigherPurposesSet"/>
6      <xs:element ref="Identity"/>
7      <xs:element ref="AttributesSet"/>
8      <xs:element ref="CertifiersSetForAttributes" minOccurs="0"/>
9      <xs:element name="DownstreamUsage" type="AbstractContainer" minOccurs="0"/>
10   </xs:sequence>
11 </xs:complexType>
```

Listing 3.6: The abstract `Conatiner` element is the basis for the actual `Conatiner` and the `DownstreamUsage` element.

The last element within the `Container` (see Listing 3.6) element is the `DownstreamUsage` element. In order to express in-depth how the collected data may be used by a downstream controller the `DownstreamUsage` element is of the type *abstract container*. In other words, for specifying downstream usage another `Container` element (including all child elements introduced above) can be used. If the optional `DownstreamUsage` element is left out, the implications are that data are not allowed to be shared with any third party at all.

In order to reuse specified elements within the XML schema definition (XSD) abstract elements were used. Since the `DownstreamUsage` element does not need the `type` attribute (used by the `Container` element) an *abstract container* type is specified. The actual `Container` element has the abstract container as basis just adding the `type` attribute.

As mentioned in the beginning of this section, and shown in Listing 3.1, the optional `CertifiersSetForSeals` element enables certifiers to give a seal for a policy; or in case of a recommendation or preference to demand a seal for a policy that is matched against them. As depicted in Listing 3.7, there can be one or more `CertifierForSeal` child elements, whereupon each contains a `Signature` and an `Identity` element.

```
1  <!-- CertifiersSetForSeals -->
2     <xs:element name="CertifiersSetForSeals">
3         <xs:complexType>
4             <xs:sequence>
5                 <xs:element name="CertifierForSeal" minOccurs="1" maxOccurs="
                      unbounded">
6                   <xs:complexType>
7                     <xs:sequence>
8                         <xs:element ref="Identity"/>
9                         <xs:element ref="Signature"/>
10                    </xs:sequence>
11                  </xs:complexType>
12                </xs:element>
13            </xs:sequence>
14        </xs:complexType>
15    </xs:element>
```

Listing 3.7: The specification of the `CertifiersSetForSeals` element. One or more `CertifierForSeal` child elements are allowed. Each of them contains an `Identity` and a `Signature` child element.

In the case of a recommendation, the `Signature` element within the `CertifierForSeal` element is present, but empty. Meaning, the `CertifierForSeal` element is used to recommend that a policy needs to be certified by a certain third party (e.g. a DPA), that is identified by the `Identity` element. However, it should be possible to express that a policy should be certified by any DPA or by a particular group of DPAs. In order to come up to this requirement some hierarchy and/or ontology needs to be set up. Also in terms of matching a function is needed that is aware of this ontology. *For example the function*

should return a match when the "DPA of Sweden" certified a policy and "Any DPA within the EU" is recommended. Setting up this hierarchy and/or ontology is not in the scope of this thesis.

Both, the `Signature` element next to the `Container` and the `Signature` element within a `CertifierForSeal` element contain digital signatures on the `Container` element. As mentioned above, the corresponding certificates including the public key to verify these signatures are located at the `CertificateURL` which is part of the appropriate `Identity` element.

3.3 Creation of Example Instances

In order to analyse the necessary data processing for the new German identity card (which was introduced in November of 2010) Zwingelberg [Zwi11] used a staged model, which correlates with the stages of typical contract negotiations. In accordance to Zwingelberg [Zwi11, Section 2.2] the staged model could also provide a basis for future discussion on the assessment of which personal data is necessary for different usage scenarios. A short description of the four stages follows [Zwi11, Section 2.2]:

Stage 1 The data subject only seeks information about the data controller's service, therefore no personal information needs to be revealed at all and the data subject acts anonymously.

Stage 2 At this stage a proof is needed that the same data subject is acting at a later point of time. As long as the data subject only seeks information about the data controller's service, she may stay anonymous. This phase is called *early contact*. If she later on decides to close a contract she needs to reveal personal data. Where at the early contact phase just a pseudonym was used, later on this pseudonym needs to be connected to the real identity of the data subject. Technically this can be achieved by using any kind of session identifiers, such as browser cookies.

Stage 3 This stage requires some kind of authentication by the data subject. That is to say the data subject does not need to reveal a certain requested attribute; just the information if the data subject's attribute passes the "challenge" imposed by the data controller. *For example, a data controller wishes to know if the data subject's age is over 18 or if she is an European citizen—but he does not need to know the actual age or nationality.* For this kind of *zero-knowledge proof* cryptographic methods are needed and the requested attributes need to be certified by a third party.

Stage 4 At this stage the data subject needs to be identified by her personal data. Therefore the requested data needs to be certified and disclosed to the data controller. This can be necessary for any applications where identification is required by law.

Based on the stages described above, example scenarios and appropriate instances for each of the three container types of UPL—policy, preference and recommendation—were created. Next, we describe the created scenarios and point out some essential characteristics. The complete instance files can be found in appendix A.2.

3.3.1 Stage 1: Anonymous Access

Referring to the instance files in appendix A.2.1 this example has the `HigherPurpose` *browsing*. The data controller is an online newspaper service. For browsing through the news a data subject does not need to reveal any personal data at all, hence the `AttributesSet` element is empty. However, the policy is signed in order to come up to the security target of non-repudiation. The URLs for the human-readable policy and the policy's respectively recommendation's certificate can be found within the `Identity` element.

3.3.2 Stage 2: Early Contact Negotiation

Referring to the instance files in appendix A.2.2, in this example the data controller is represented by an insurance company. The data subject may browse anonymously through the products and services offered by the data controller. In order to facilitate the data subject arranging an individual insurance package an `Attribute` named *SessionIdentifier* is used and may be disclosed to the data controller. This session identifier can be seen as a pseudonym for the data subject's identity. It is used for the `Purposes` *login*, *state* and *tailoring* which comes up to the arrangement of the insurance package. As it would make no sense to pass on that session identifier to a third party no downstream usage is permitted. Furthermore, since the data controller is an insurance company his policy has been certified by the *Data Protection Agency of Sweden*. The `Signature` and `CertificateURL`, as well as further contact details about the certifier, can be found within the `CertifierForSeal` element. The recommendation, which is issued by the *Data Protection Agency of Sweden* as well, says that a policy needs to be certified by *Any Data Protection Agency*. The `Signature` element within this certain `CertifierForSeal` element is left empty, requesting that the seal needs to be digitally signed. Compared to the recommendation, the preference is more restrictive, requesting a certification merely by the *Data Protection Agency of Sweden*. If the data subject finally wants to place a contract more personal data needs to be revealed—however this is not in the scope of this scenario.

3.3.3 Stage 3: Zero-Knowledge Proof

Referring to the instance files in appendix A.2.3, in this example the data controller is a hosting provider for video clips. The `HigherPurpose` for that privacy policy is both *arts* and *marketing*. The `HigherPurposesSet` element has set the `semantics` attribute (*AND* semantics), that means when matching e.g. a recommendation with a policy, it would be a match only if the policy is issued under the same combination of higher purposes.

The `Attribute` *SessionIdentifier* is used as in Section 3.3.2 to enable a login function and to tailor the platform regarding the data subject's previous behaviour. Moreover, the attribute *Country* is used for further tailoring and decide which video clips are suggested. Referring to Listing 3.8, the `Attribute` *Age* is used for further tailoring and an individual decision as well. The attributes `relation` and `value` are indicating that not the age of the data subject needs to be reveal but just a proof that her age is over or equal to 18. The `relation` *GTE* means *"greater than or equal"*. But also *LTE* (for *"less than or equal"*), *GT* (for *"greater than"*), *LT* (for *"less than"*) and *CONTAINS* (for saying that the value needs to be within a comma separated list) may be used.

```
1 <Attribute certifiedBy="SE-GOV-CA">
2     <AttributeValue relation="GTE" value="18">Age</AttributeValue>
3     <PurposesSet>
4         <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/individual-
              decision</Purpose>
5         <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/tailoring</
              Purpose>
6     </PurposesSet>
7 </Attribute>
```

Listing 3.8: An example `Attribute` with zero-knowledge proof. This example says that the *Age* has to be *greater or equal* ("GTE") to *18*.

If only the `relation` attribute is set for a preference or a recommendation, the data controller may ask for any relation (e.g. any minimum age). If the `value` attribute is set too, he may ask just for this certain age; for every other age there is a mismatch. This behaviour avoids that a malicious data controller could challenge the data subject with a list of ages, just to find out her correct age. As PPL has a dedicated component for credential handing, there are no zero-knowledge proof elements within PPL's data handling part.

That proof about the data subject's age and her home country needs to be certified. This is indicated by the `certifiedBy` attribute within the `Attribute` element (see Listing 3.8). This key corresponds to a `CertifierForAttribute` element within the `Container` element. This certifier is identified by this key using the `certifierId` attribute (see List-

ing 3.9).

```
<CertifiersSetForAttributes>
    <CertifierForAttribute certifierId="SE-GOV-CA">
        <Identifier>Government Offices of Sweden</Identifier>
        <Representative>Mr. John Gustavsson</Representative>
        <Email>contact@ca.gov.se</Email>
        <Phone>+46 8 405 10 00</Phone>
        <URI>www.ca.gov.se</URI>
    </CertifierForAttribute>
</CertifiersSetForAttributes>
```

Listing 3.9: An example `CertifierForAttribute` element which is the form of a previously specified `Identity element`. The certifier is identified by `certifierId` attribute.

Considering that the marketing content (in form of small video clips) is provided by a third party (the downstream controller), and the content is tailored for different nationalities, this downstream controller needs to know the nationality of the data subject. The `DownstreamUsage` element including the `HigherPurpose` *marketing* and the single `Attribute` *country* expresses this fact, see lines 59-61 in Listing A.8 on page 67.

3.3.4 Stage 4: Identification Required

Referring to the instance files in Appendix A.2.4, in this example the data controller is represented by the Government Offices of Sweden. For governmental services it is required that *first name* and *last name* of the data subject have been certified and are presented for identification. The e-mail address is not needed to be certified in this scenario. However, the data controller commits to certain obligations for the e-mail address. Referring to Listing 3.5, the data controller commits to the data subject, she will be notified within one day respectively five days (action `ActionNotifyDataSubject`) if her data is deleted (trigger `TriggerPersonalDataDeleted`) or if there is any violation regarding her data detected (trigger `TriggerOnViolation`), respectively.

As the e-mail address may be used only one month for *accounting* and *marketing* purposes, the notification could still be sent via e-mail (since notifications match the `Purpose` called *communicate*) after that. For notifying the data subject about the deletion of his

e-mail address for the last purpose, a different way of communication has to be used.

3.4 Summary

In this chapter, we discussed the design of UPL. UPL is modelled on P3P, the data handling part of PPL, and the requirements of the DPD [Eur95] as well as the new draft legislative package of the European Commission [vB12]. Moreover, we created example instances based on the staged approach by Zwingelberg [Zwi11].

Chapter 4

Implementation of a Matching Engine

In this chapter, we discuss the implementation of a prototype for a policy matching engine for UPL, as described in Chapter 3. In Section 4.1 we collect the requirements for such a policy matching engine. Section 4.2 discusses the architecture, and different approaches for parsing and comparing XML. The chapter ends with a presentation of the matching engine, including some examples of sample input and output.

4.1 Requirements for a UPL Matching Engine

As discussed in Section 3.1, UPL may be used by three parties; by the data controller issuing his privacy *policy*, by the data subject specifying her privacy *preferences*, and by a third party issuing *recommendations*. A policy matching engine is a tool to support any of these parties by deciding if two privacy statements are matching or not. For example, a data subject may wish to know if her privacy preference matches the privacy policy of data controller before accessing his website, or a data controller wants to match his privacy policy with a recommendation issued by a DPA. Figure 3.1 on page 17 depicts all ways of

matching between these three parties. To determine if two privacy statements (in the form of policies, preferences or recommendations) are matching, the terms *match* and *mismatch* need to be defined.

In general, a privacy statement is a set of statements about the treatment of personal data. Consequently two statements are matching not only if these sets are totally equal but also if one set is a subset of the other. To decide which statements needs to be a subset and which a superset a *matching order* is essential. By way of example, if a data subject's preference states that certain attributes may be used for the purposes *account*, *marketing*, and *communicate*[1], and a data controller intends to use that particular attribute just for the purposes of *account* and *communicate*, then the data controller's policy is a subset of the data subject's preference. Thus, when matching both statements the result should be positive. Although, if the data controller intended to use the data subject's personal data for more purposes than the data subject stated, the result should be a mismatch.

Consequently the following considerations can be done in terms of the matching order:

- When matching a policy X with a preference Y, the policy has to be a subset of the preference. If the policy has additional elements or longer (less restrictive) durations (e.g. for data retention), that is a mismatch. We state that $X \subseteq Y$.

- When matching a policy X with a recommendation Z, the policy needs to be a subset of the recommendation to comply and give a positive matching result. We state that $X \subseteq Z$.

- For preference Y and recommendation Z matching, for a match the recommendation has to be a subset of the preference. We state that $Z \subseteq Y$.

- For matching two equal container types, there has to be an exact match for a positive result.

[1]These example purposes are modelled on the purposes specified by P3P [CDE+06, Section 3.3.5].

In accordance to the statements above and in terms of the matching order we consider the following matching condition:

$$preference \supseteq recommendation \supseteq policy$$

In other words, if a data subject's preference is less restrictive than a recommendation or a data controller's policy, a match can be found. This also means a recommendation may be more restrictive than a data subject's preference, but not less restrictive. And a data controller's policy has to be at least as restrictive as a preference or a recommendation in order to find a match. The smallest set of privacy statements is the most restrictive one.

This consideration is valid in terms of a set of a data subject's attributes, purposes under which personal data may be used and data retention times (as a lower data retention time may be seen as a subset of a higher data retention time). However, for obligations and for seals (`CertifierForSeals`) the largest set is the most restrictive one. For instance is a privacy statement more restrictive if it defines more obligations or has more seals than another. Consequently, for *obligations* and for *seal certifiers*, we consider the following matching condition:

$$preference \subseteq recommendation \subseteq policy$$

The input for the matching engine are two arbitrary files of a UPL container type (preference, policy, recommendation), hence the matching engine needs to be aware of these conditions to ensure the correct matching order. In general, it may be assumed that the input files are well-formed and valid, regarding the schema file. Furthermore, all signatures may be assumed as valid. For real implementations the validation of input files and certificates is essential and has to be done before the actual matching.

Since this implementation is a proof-of-concept prototype, the output format has not yet determined. The output format of PPL's matching engine is a so-called *annotated sticky-policy*. This sticky policy is the agreed-upon set of granted authorizations and promised

obligations with respect to a resource [TNR11]—however the derivation of a matching result to a sticky policy is out of the scope of this thesis. For evaluating the matching engine a human-readable output is useful, however it should be considered that a policy matching engine may be a part of a so-called policy decision point (PDP) (compare "Detailed architecture of PPL" in Figure 2 on page 19 of the report by Trabelsi et al. [TNR11]). Therefore, the output should be parsable by any other component in a larger architecture. For the proof-of-concept implementation it is helpful if the output is as verbose as possible and to enable easy modifications on the output format.

4.2 Implementation of a UPL Matching Engine

In this section we discuss the proof-of-concept implementation of the matching engine. The programming language of choice was Java for the following reasons: Java applications are cross platform, i.e., Java applications may be run on any platform or operating system, which has a Java runtime environment (JRE) installed. Since the focus of the U-PrIM project [Ang11] is on privacy aspects for mobile platforms, the matching engine may be used in mobile applications for the Android[2] platform too.

The prototype of the matching engine is designed as a command line application, awaiting two arguments (two file paths, each pointing at a UPL privacy statement). While matching these two files, each found difference between both files are printed to standard output. The final result, if a match could be found or not, is printed to standard output too.

4.2.1 Architecture of the Matching Engine

The first action the matching engine has to take is to parse the given XML files into memory. For parsing XML in Java there are several different libraries, such as the Simple API for

[2]Android mobile platform, `http://www.android.com/` (accessed 10/11/2012)

XML (SAX)[3] and the Document Object Model (DOM)[4]. The main difference between these libraries is the parsing paradigm they follow. It may be distinguished between *event-based* and *tree-based* parsing. Event-based parsers are modelled on the data-push principle, i.e., while parsing a file different elements within this file trigger events which are pushed to a so-called handler. An example for an event-based parser is *SAX*. Tree-based parsers are modelled on the data-pull principle. For example, *DOM* is a tree-based parsing library, which at first reads the whole document tree into memory enabling the other components to pull the desired data out of this tree. Since it is helpful when comparing two objects to have them both in memory the XML parser of choice for the matching engine prototype was the DOM interface of the Java API for XML Processing (JAXP).

To map the tree structure of UPL onto Java objects each UPL element was created as a Java class (see Figure 4.1). Child elements are represented by attributes within the particular classes. Sets are represented by an extended Java collection.

The second action the matching engine needs to take, after parsing the UPL files, is to map the document tree on the Java classes within the package `se.kau.upl.me.model`. As shown in Figure 4.2, the matching engine's entry point is the `Main` class. This class accesses the two files and parses their XML content using the *DOM* library. If this is successful, the `Engine` object is invoked. The `Engine` object is aware of the matching order discussed in Section 4.1 and is in charge of mapping the UPL tree onto Java objects. Next, the actual matching (done by the `ContainerEngine` and the `CertifierForSealsEngine`) is invoked. The `ContainerEngine` is invoked at first for the actual UPL `Container` element and next for the `DownstreamUsage` elment, if present. Any results found by these components are printed to the standard output by using a static method of the `Logger` class.

The matching engine prototype is segmented into four Java packages:

`se.kau.upl.me.core` The `<core>` package contains the classes that would take the part

[3]Simple API for XML, `http://www.saxproject.org/` (accessed 11/11/2012)
[4]Document Object Model, `http://www.w3.org/DOM/` (accessed 11/11/2012)

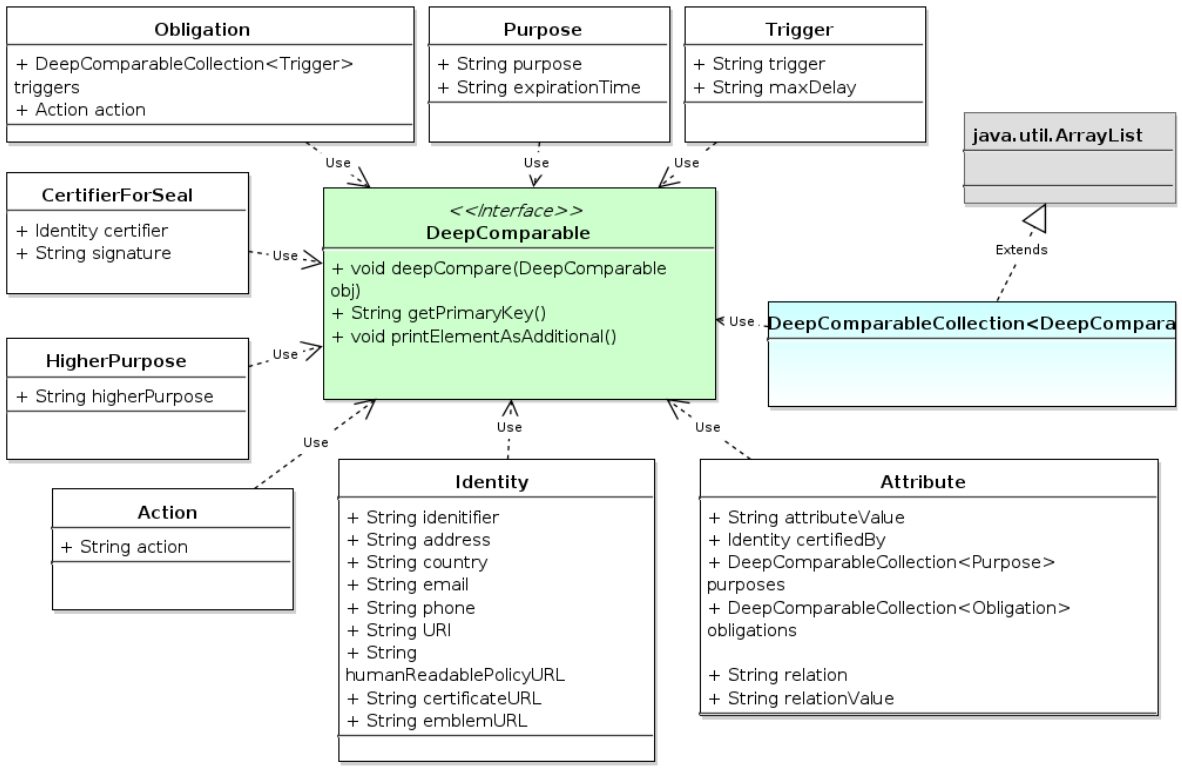

Figure 4.1: A class diagram of the package `se.kau.upl.me.model` within the matching engine implementation. Each UPL element modelled into a Java class implements the interface `DeepComparable`.

of the *controller* in the Model-View-Controller (MVC) design pattern. Figure 4.2 illustrates the call hierarchy of this packages, starting with the `Main` class, called by the user.

`se.kau.upl.me.exceptions` This packages contains user-specific exceptions which may be thrown by the matching engine. The `ElementNotFoundException` is thrown if a mandatory element was not found within a given privacy statement.

`se.kau.upl.me.model` The classes within this package represent the *model* in the MVC design pattern. The tree structure of an UPL privacy statement is mapped onto these classes. However, each single class implements the `DeepComparable` interface, which demands to bring some business logic to these model classes.

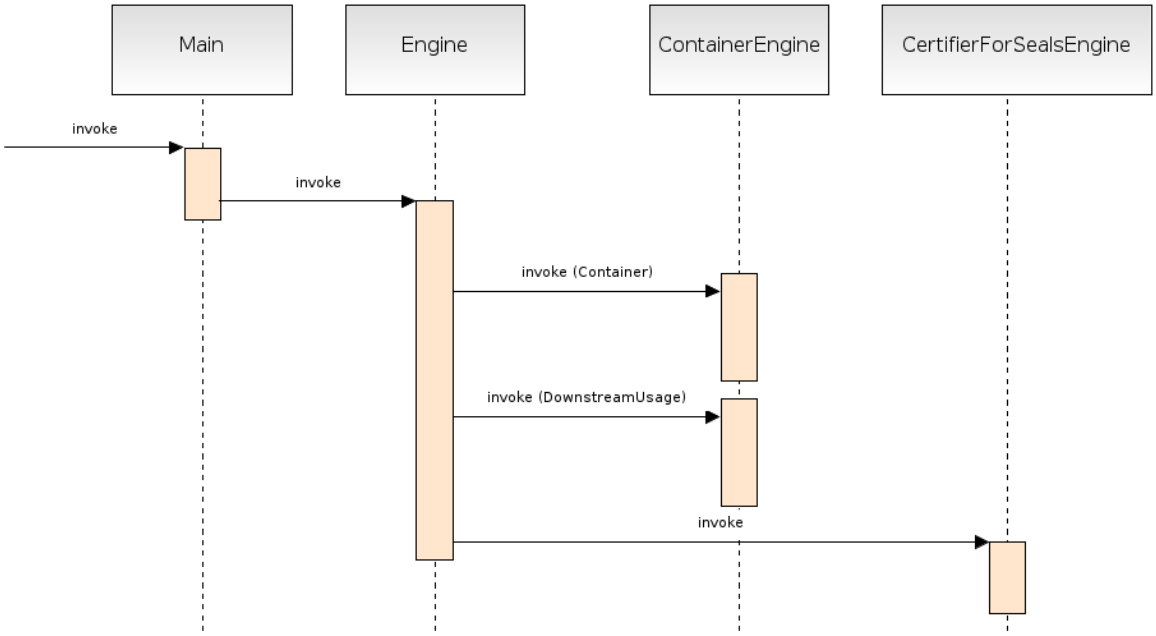

Figure 4.2: A call diagram of the package `se.kau.upl.me.core`. The class `Main` is the entry point of the matching engine invoked by the user. The `Engine` class invokes the `ContainerEngine` once with the UPL `Conainter` and once with the `DownstreamUsage` element, if present. Last the `CertifierForSealsEngine` is invoked from the `Engine`.

`se.kau.upl.me.utils` This package contains two classes which support the matching engine with statical utility methods. On the one hand the `Logger` class represents the *view* part of the MVC design pattern. On the other hand the class `UPLUtils` contains static methods which are used by the classes of the `se.kau.upl.me.core` package.

4.2.2 Matching of Java Objects

As mentioned above, the actual matching is done within the `se.kau.upl.me.model` classes mainly by using two methods. The method `void deepCompare(DeepComparable obj)` is specified in the interface `DeepComparable`, which each of these classes in the package `<model>` needs to implement. The method `boolean equals(Object obj)` is inherited from `java.lang.Object` and needs to be overridden by each class. It returns true if the

given object is totally equal (including each of its child elements) compared to the current object.

An UPL privacy statement is a tree structure containing several sets. This tree of sets needs to be compared in terms of the conditions about the matching order developed in Section 4.1. To represent these sets within Java objects a class `DeepComparableCollection` is created. Referring to Figure 4.1, this class extends the collection `java.util.ArrayList` and implements the interface `DeepComparable`. Moreover, as the class is *generic* it may be only typified by objects implementing the interface `DeepComparable`.

Each element within one of these sets in UPL needs to have a *primary key* in order to enable matching. By the way of example, the primary key of the UPL element `Attribute` is the `AttributeValue` and for the element `Purpose` it is the purpose itself. This primary key is returned by the method `String getPrimaryKey()` which is required by the `DeepComparable` interface.

The heart of the matching engine is the implementation of the method `void deepCompare(DeepComparable obj)` required by the `DeepComparable` interface. If the current object contains child elements the `void deepCompare(DeepComparable obj)` method is called for each of them. Otherwise the differences between the current and the given object are printed out directly by using a static method of the `Logger` class. On the one hand, these child elements of an object could be represented by attributes of a Java class (e.g. the attribute `certifiedBy` within the object `Attribute`). On the other hand, if the current object is a `DeepComparableCollection` (representing a set like a `PurposesSet` containing several `Purpose` elements), these child elements are the elements of the collection. For comparing the child elements of two collections we developed an algorithm. This algorithm (see pseudocode in Algorithm 1) is implemented in the the method `void deepCompare(DeepComparable obj)` of the `DeepComparableCollection` class. The algorithm is matching each element of the first collection with each element of the second collection. There are three possible results for each compared element pair:

- Two elements are totally equal. There is no further action on these elements required.
- Two elements have an equal primary key (e.g. the same `AttributeValue`) but the are differences regarding their child elements. These elements need to be "deep-compared".
- There are additional elements in the collection that is supposed to be the subset of the other collection. These elements need to be printed as *additional*. Therefore the method `void printElementAsAdditional()` required by the interface `DeepComparable` is called.

Algorithm 1 Algorithm for comparing of two collections in pseudocode

```
1: for each element1 ∈ collection1 do
2:     for each element2 ∈ collection2 do
3:         if element1 == element2 then
4:             remove element1 from collection1
5:             remove element2 from collection2     ▷ if elements are totally equal they are removed
6:         end if
7:         if element1.primaryKey == element2.primaryKey then
8:             deepCompare elment1 with element2    ▷ deep-compare elements and print differences
9:             remove element1 from collection1
10:            remove element2 from collection2
11:        end if
12:    end for
13: end for
14: print remaining elements of collection2    ▷ The remaining elements are additional in the second collection.
```

For every difference which is printed by using the method `static void log(String message)` a variable named `differenceCounter` is incremented. Finally, the counter value is printed to standard out, stating the result of the matching. If it is zero, a match could be fond—otherwise it is a mismatch.

4.2.3 Test Cases and Example Output

To generate test cases the UPL instances developed in Section 3.3 are used (the full XML instance files can be found in Appendix A.2). In the following we show two output examples of the proof-of-concept matching engine. Listing 4.1 shows a mismatch and the differences which caused the mismatch. Listing 4.2 shows the result of the matching of two files where a match could be found.

```
1  *** Matching {sample-recommendation_stage4.xml} vs. {sample-policy_stage3.xml}
       ***
2  {policy} has an additional higher purpose: http://www.w3.org/2006/01/P3Pv11/arts
3  {policy} has an additional higher purpose: http://www.w3.org/2006/01/P3Pv11/
       marketing
4  {policy} has an additional attribute: SessionIdentifier
5  {policy} has an additional attribute: Age
6  {policy} has an additional attribute: Country
7  {downstream-policy} has an additional higher purpose: http://www.w3.org/2006/01/
       P3Pv11/marketing
8  {downstream-policy} has an additional attribute: Country
9  {policy} has no seals while {recommendation} has
10 *** RESULT: 8 difference(s) was/were found. ***
```

Listing 4.1: The output of the matching engine when matching the recommendation of stage 4 and the policy of stage 3 (compare to Appendix A.2).

```
1  *** Matching {sample-preference_stage2.xml} vs. {sample-policy_stage2.xml} ***
2  Exact match for the container element.
3  *** RESULT: Match okay ***
```

Listing 4.2: The output of the matching engine when matching the preference of stage 2 and the policy of stage 2 (see Appendix A.2).

Since the different stages were designed for different scenarios these test cases do not exhaust all capabilities of the matching engine prototype. Therefore, the policy file of stage 3 and the recommendation file of stage 4 were modified in order to create more differences in detail (find the modified files in Appendix A.2.5).

Listing 4.3 shows a mismatch because of a preference's shorter expiration time at the `Purpose` element, the policy which is not using the `relation` attribute for the age, and an additional higher pupose in the policy's `DownstreamUsage` element. Listing 4.4 shows a mismatch because of the attribute *email* which is certified within the recommendation

but not in the preference, a longer (less restrictive) `MaxDelay` at a certain obligation, and an additional trigger for an obligation within the preference. The fourth difference printed out may be actually ignored when using this prototype. Since there is no ontology in place which can say that the *Data Protection Agency of Sweden* would match with *Any Governmental Office of Sweden*.

```
1 *** Matching {sample-preference_stage3.xml} vs. {sample-policy_stage3_modified.
      xml} ***
2 {preference} has a shorter (more restrictive) expiration time at the attribute
      SessionIdentifier for the purpose:
3     http://www.w3.org/2006/01/P3Pv11/login
4 {policy} is requesting the attribute Age, but not just the GTE-relation
5 {downstream-policy} has an additional higher purpose: http://www.w3.org/2006/01/
      P3Pv11/gaming
6 *** RESULT: 3 difference(s) was/were found. ***
```

Listing 4.3: The output of the matching engine when matching the preference of stage 3 and a modified policy based on the example policy stage 3 (see Listing A.14 in Appendix A.2.5).

```
1 *** Matching {sample-recommendation_stage4_modified.xml} vs. {sample-
      preference_stage4.xml} ***
2 {recommendation} has at attribute Email a certifier while {preference} has none
3 {preference} has a longer (less restrictive) max delay for the obligation
      ActionNotifyDataSubject at the attribute Email
4 {preference} has has an additional trigger TriggerOnViolation for the obligation
       ActionNotifyDataSubject at the attribute Email
5 {preference} has additional certifiers for seals: Data Protection Agency of
      Sweden
6 *** RESULT: 4 difference(s) was/were found. ***
```

Listing 4.4: The output of the matching engine when matching the preference of stage 4 and a modified recommendation based on the example recommendation stage 4 (see Listing A.15 in Appendix A.2.5).

In order to enable easy modification of the output format, all text output is stored as parameterised strings in a property file.

4.3 Summary

In this chapter, we discussed the implementation of a prototype for a policy matching engine for UPL. This prototype is able to match policies, preferences and recommendations

in each possible combination. Since it is a prototype the output format is designed to be human-readable, but it may be changed by editing the appropriate property file.

Chapter 5

Evaluation

In this chapter, we evaluate the result of the work described in the previous two chapters. In the first section we discuss the design of UPL. The second section evaluates the proof-of-concept implementation of the matching engine for UPL.

5.1 Evaluation of UPL

With UPL we improved some shortcomings of PPL's data handling part, discussed in Section 2.3. Table 5.1 depicts which features of PPL were adapted in UPL, which new contributions could be made with UPL, and which features are possible areas of future work.

Language feature	PPL	UPL
Symmetric language	✔	✔
Features event based obligations, in order to come up to requirements by the DPD [Eur95] and the draft legislative package of the European Commission [vB12], such as the "right to be forgotten" or the "data breach notification".	✔	✔

— *Continued on next page* —

Language feature	PPL	UPL
Features the possibility to express if and how personal data may passed on to a downstream controller by the data controller (downstream usage).	✔	✔
Third parties may issue recommendations which may be used by, both, data controllers and data subjects to model their privacy statements on them.	✖	✔
A signature element ensures authenticity and integrity of policies (and recommendations).	✖	✔
Features an identity element within the language in order to come up to the requirement of the DPD [Eur95].	✖	✔
Each privacy statement is created under a “higher purpose” which describes the context of data usage.	✖	✔
The data retention time is bound to the purposes of an attribute and not to the whole attribute.	✖	✔
Features a defined output format, associated to a resource.	✔	✖
Features full credential-based access control capabilities.	✔	✖
Features the possibility to define the type and value of an attribute in the same privacy statement.	✖	✖
Features an ontology for purposes of data usage (and “higher purposes”).	✖	✖
Features an ontology for seal certifiers.	✖	✖

Table 5.1: A comparison between the language features of PPL and UPL

The first three rows of Table 5.1 show features of PPL that were adapted in UPL. One of these features is the language symmetry which allows a data controller's privacy policy and a data subject's privacy preference to be expressed in the same language schema. Consequently, this also allows easy matching.

Adding the notion of *recommendations* issued by third parties is one of the main contributions in UPL. This enables users (in the role of data subjects) to adapt their privacy preferences to a third party's recommendation, which they hopefully trust. Data controllers may also adapt their privacy policies in order to adhere to a recommendation of a trusted third party, such as a DPA. Users can also compare a data controller's privacy policy with a third party's recommendation to determine if the data controller's request is reasonable or not. Each of these UPL privacy statement types—policy, preference, recommendation—is issued under a certain "higher purpose". A user, and a third party issuing privacy recommendations, may specify several different privacy statements for different higher purposes (e.g. *shopping* or *gaming*).

By exploiting all the language features that could be adapted from PPL, and those additional features we incorporated in this thesis, UPL can handle all the use-cases described in Section 3.3. However, since the scope of UPL was on the data handling part of a policy language, use-cases which require authentication with credentials are not fully supported in UPL. The `relation` attribute described in Section 3.3.3 allows to express that a zero-knowledge proof is required. This proof could be realised by using anonymous credentials. The integration of credential-based access control capabilities to UPL is a possible area of future work.

Furthermore, the case that a data subject has e.g. more than one e-mail addresses, such as one private personal e-mail address and another e-mail address for work, whereupon she wants her different email addresses to be treated differently, should be considered in future work done on UPL. Since the current version of UPL does not specify a type for an attribute, the e-mail addresses can not be distinguished. A way to work around this

shortcoming would be that the data subject creates two privacy preferences with different "higher purposes" to have different privacy statements for the work e-mail address and the private e-mail address. This shortcoming may be solved in a better way by using attribute types, such as the vCard format [Per11] or the schemas issued by *schema.org*[1]. Moreover, it could be helpful if the ontology for "higher purposes" and for purposes within the `Attribute` element are organised hierarchically. The current version of UPL uses the purposes specified by P3P [CDE+06], which are organised as a flat list. This ontology and the specification of attribute types in UPL are potential areas of future work.

As introduced in Chapter 3, the `HigherPurpose` element specifies a `semantics` attribute, which can be either AND or OR. The AND semantic is more restrictive when matching two privacy statements, saying that it will only be a match if the complete set of higher purposes match. However, scenarios may be found where it is hard to say whether it is a match or a mismatch. For example, a preference specifies three higher purposes—such as *marketing* AND *gaming* AND *communicate*—with the AND semantics attribute set and a policy is issued for two of these higher purposes—such as *marketing* AND *gaming*—also with an AND semantics attribute set. This scenario would be a mismatch as only the complete combination of higher purposes would match. A way to express that each one-and-one-combination (such as *marketing* AND *gaming* or *communicate* AND *gaming*) of a data subject's preference should match, for each of these combinations a separate privacy preference needs to be created. However, this matching rule is not specified in the current version of UPL and is a possible are of future work.

The output format of PPL's matching engine is an *annotated sticky-policy*. This sticky policy is the agreed-upon set of granted authorizations and promised obligations with respect to a resource [TNR11]. The current version of UPL does not define any output format. Hence, that is another potential area of future work.

Yet another potential area of future work is to define an ontology for the `CertifierFor-`

[1]Properties from a person specified by *schema.org*, `http://schema.org/Person` (accessed on 20/11/2012)

`Seals` element. This ontology could be for instance a hierarchy defining groups of certifiers, such as *Any Data Protection Agency within Europe* which contains all European DPAs.

Moreover, elaborating on the usage of recommendations, especially from a usability standpoint, is another possible are of future work. For example, how much would users make use of such a feature and if it would lead to users actually trusting service providers more, or not at all, are interesting topics for further research.

5.2 Evaluation of the UPL Matching Engine Prototype

The proof-of-concept matching engine for UPL is able to match preferences, policies and recommendations in any combination. However, it assumes that the input files are well-formed, valid and plausible. Furthermore, all certificates used in UPL are assumed as valid by the matching engine prototype. For real implementations the validation of input files and certificates is essential and has to be done before the actual matching. Implementing this validation component is an area of future work. Moreover, the output for the proof-of-concept matching engine is in a more human-readable format, than it would be needed for easy parsing. For implementations where the matching engine is part of a PDP, the output format needs to be parsable. The specification of a parsable output format is a possible area of future work.

Since the current version of UPL does not define an ontology for seal certifiers, the proof-of-concept matching engine is not able to find matches in terms of a possible ontology. For example, if a preference requires a seal from *Any Data Protection Agency within Europe* and a policy has a seal from *Data Protection Agency of Sweden* the prototype prints out a mismatch, since the matching engine is not aware of this implicitly assumed ontology. Adding this feature to the matching engine is a potential area of future work.

Furthermore, the test cases discussed in Section 4.2.3 are only examples and not in

any way exhaustive with regard to the full capabilities of the language. In order to gain confidence in that the matching engine is able to handle all special cases, test cases need to be developed methodically. That could be a further potential area of future work.

Also the integration of UPL, which is in the current version merely about data handling, into a standardized access control policy such as XACML and the integration of the matching engine into a policy decision point (PDP) of a privacy-enhanced access control system are possible areas of future work.

5.3 Summary

In this chapter, we discussed the the main contributions as well as areas left for future work of, both, the design of UPL and the proof-of-concept matching engine for UPL. Next to the the definition of attribute types for UPL, the definition of ontologies for, both, the `Purpose` element and the seals certifiers are key areas of future work. The methodical development of test cases and integration of the mentioned ontologies into the matching engine are areas of future work regarding the implementation.

Chapter 6

Conclusion

We have examined relevant related work in the area of privacy policies to identify shortcomings in the state of the art. Based on the discussion about shortcomings found in PPL, and respecting legal demands regarding data protection, requirements for a new privacy-policy language were collected. These requirements were used to design a new privacy-policy language, called UPL. The current version of UPL focuses on data handling, that is, how data is to be handled by a data controller. Integrating UPL into an access control language, such as XACML, is a potential area of future work. In order to depict the features of the policy language in real-life scenarios, sample instances were created. These sample instance are modelled on the staged approach by Zwingelberg [Zwi11].

In Chapter 4 we described the implementation of a proof-of-concept prototype privacy-policy matching engine for UPL. This prototype is able to match preferences, policies and recommendations in any combination. The output format for the prototype is human-readable. For real implementations the output format needs to be parsable, since the matching engine may be part of a PDP. The specification of a parsable output format is a possible area of future work. Furthermore, the creation of ontologies for, both, the purposes of data usages and seals certifiers, and the integration of these ontologies into the matching engine were out of scope of this thesis and therefore suggested as future work.

We hope our contribution is a step forward in reducing the privacy concerns of Internet users and may support them in determining if it is worth to reveal their personal data to different service providers.

References

[ABdV+09] Claudio A. Ardagna, Laurent Bussard, Sabrina De Capitani di Vimercati, Gregory Neven, Stefano Paraboschi, Eros Pedrini, Franz-Stefan Preiss, Dave Raggett, Pierangela Samarati, Slim Trabelsi, and Mario Verdicchio. Primelife policy language, 2009. `http://www.w3.org/2009/policy-ws/papers/Trabelisi.pdf`, accessed 12/10/2012.

[Ang11] Julio Angulo. U-PrIM - Usable Privacy-enhancing Identity Management for smart applications, 2011. `http://www.kau.se/en/computer-science/research/research-projects/u-prim`, accessed 12/10/2012.

[BCP11] Patrik Bichsel, Jan Camenisch, and Franz-Stefan Preiss. A comprehensive framework enabling data-minimizing authentication. In *Proceedings of the 7th ACM workshop on Digital identity management*, DIM '11, pages 13–22, New York, NY, USA, 2011. ACM.

[Bra00] Stefan A. Brands. *Rethinking public key infrastructures and digital certificates: building in privacy.* Mit Press, 2000.

[CDE+06] Lorrie Cranor, Brooks Dobbs, Serge Egelman, Giles Hogben, Jack Humphrey, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle, Matthias Schunter, David A. Stampley, and Rigo Wenning. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, 2006.

[CES+08] Lorrie Faith Cranor, Serge Egelman, Steve Sheng, Aleecia M. McDonald, and Abdur Chowdhury. P3P deployment on websites. *Electronic Commerce Research and Applications*, 7(3):274 – 293, 2008.

[CH02] Jan Camenisch and Els Van Herreweghen. Design and implementation of the *idemix* anonymous credential system. In Vijayalakshmi Atluri, editor, *ACM Conference on Computer and Communications Security*, pages 21–30. ACM, 2002.

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In

Birgit Pfitzmann, editor, *EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, 2001.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Matthew K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 56–72. Springer, 2004.

[Eur95] European Parliament, Council. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Directive, 1995. `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT`, accessed 24/10/2012.

[Fac12] Facebook Inc. Facebook Newsroom, Key Facts, 2012. `http://newsroom.fb.com/Key-Facts`, accessed 20/11/2012.

[IBM12] IBM Research – Zurich. Specification of the identity mixer cryptographic library – version 2.3.4, 2012. `https://prime.inf.tu-dresden.de/idemix/`, accessed 20/11/2012.

[LL03] Helena Lindskog and Stefan Lindskog. *Web Site Privacy with P3P*. John Wiley & Sons, 2003.

[Org08] The Gallup Organization. Flash Eurobarometer 225: Data Protection in the European Union - Citizens' Perceptions. Analytical report, European Commission, February 2008.

[Per11] S. Perreault. vCard Format Specification. RFC 6350 (Proposed Standard), August 2011.

[Soc11] TNS Opinion & Social. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. Report, European Commission, June 2011.

[TNR11] Slim Trabelsi, Gregory Neven, and Dave Raggett. Report on design and implementation. Technical report, PrimeLife, May 2011.

[vB12] Dr. Florian von Baum. New draft european data protection regime to apply also to all us companies processing data of european residents. *Business & Technology Transactions*, February 2012. `http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227`, accessed 25/10/2012.

[Zwi11] Harald Zwingelberg. Necessary Processing of Personal Data: The Need-to-Know Principle and Processing Data from the New German Identity Card. In *Privacy and Identity Management for Life*, pages 151–163, 2011.

Appendix A

XML Language Files

A.1 UPL Schema Description

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
3
4    <!-- List of Obligations -->
5    <xs:element name="ObligationsSet">
6        <xs:complexType>
7          <xs:sequence>
8            <xs:element ref="Obligation" minOccurs="0" maxOccurs="unbounded" />
9          </xs:sequence>
10       </xs:complexType>
11   </xs:element>
12
13   <!-- Obligation -->
14   <xs:element name="Obligation">
15       <xs:complexType>
16         <xs:sequence>
17           <xs:element ref="TriggersSet" minOccurs="1" maxOccurs="1" />
18           <xs:element ref="Action" minOccurs="1" maxOccurs="1" />
19         </xs:sequence>
20       </xs:complexType>
21   </xs:element>
22
23
24   <!-- Trigger (abstract) -->
25   <xs:element name="Trigger" abstract="true" />
26   <xs:complexType name="Trigger">
27     <xs:sequence/>
28
```

```
29  </xs:complexType>
30
31
32    <!-- List of Triggers -->
33  <xs:element name="TriggersSet">
34      <xs:complexType>
35        <xs:sequence minOccurs="1" maxOccurs="unbounded">
36          <xs:element ref="Trigger" />
37        </xs:sequence>
38      </xs:complexType>
39  </xs:element>
40
41
42   <!-- TriggerPersonalDataDeleted -->
43  <xs:element name="TriggerPersonalDataDeleted" substitutionGroup="Trigger">
44   <xs:complexType>
45    <xs:complexContent>
46      <xs:extension base="Trigger">
47        <xs:sequence>
48          <xs:element name="MaxDelay" type="xs:duration"/>
49        </xs:sequence>
50      </xs:extension>
51    </xs:complexContent>
52   </xs:complexType>
53  </xs:element>
54
55    <!-- TriggerPersonalDataSent -->
56  <xs:element name="TriggerPersonalDataSent" substitutionGroup="Trigger">
57   <xs:complexType>
58    <xs:complexContent>
59      <xs:extension base="Trigger">
60        <xs:sequence>
61          <xs:element name="Id" type="xs:anyURI"/>
62          <xs:element name="MaxDelay" type="xs:duration"/>
63        </xs:sequence>
64      </xs:extension>
65    </xs:complexContent>
66   </xs:complexType>
67  </xs:element>
68
69  <!-- TriggerOnViolation -->
70  <xs:element name="TriggerOnViolation" substitutionGroup="Trigger">
71   <xs:complexType>
72    <xs:complexContent>
73      <xs:extension base="Trigger">
74        <xs:sequence>
75          <xs:element name="MaxDelay" type="xs:duration"/>
76        </xs:sequence>
77      </xs:extension>
78    </xs:complexContent>
79   </xs:complexType>
```

```
80  </xs:element>
81
82  <!-- TriggerOnDataSubjectRequests -->
83  <xs:element name="TriggerOnDataSubjectRequests" substitutionGroup="Trigger">
84   <xs:complexType>
85    <xs:complexContent>
86      <xs:extension base="Trigger">
87        <xs:sequence>
88          <xs:element name="MaxDelay" type="xs:duration"/>
89        </xs:sequence>
90      </xs:extension>
91    </xs:complexContent>
92   </xs:complexType>
93  </xs:element>
94
95
96      <!-- Action (abstract) -->
97  <xs:element name="Action" abstract="true" />
98      <xs:complexType name="Action">
99        <xs:sequence/>
100     </xs:complexType>
101
102
103   <!-- ActionDeletePersonalData -->
104 <xs:element name="ActionDeletePersonalData" substitutionGroup="Action">
105     <xs:complexType >
106       <xs:complexContent>
107         <xs:extension base="Action">
108           <xs:sequence/>
109         </xs:extension>
110       </xs:complexContent>
111     </xs:complexType>
112 </xs:element>
113
114   <!-- ActionNotifyDataSubject -->
115 <xs:element name="ActionNotifyDataSubject" substitutionGroup="Action">
116     <xs:complexType>
117       <xs:complexContent>
118         <xs:extension base="Action">
119           <xs:sequence/>
120         </xs:extension>
121       </xs:complexContent>
122     </xs:complexType>
123 </xs:element>
124
125 <!-- Purposes -->
126   <xs:element name="PurposesSet">
127       <xs:complexType>
128           <xs:sequence>
129               <xs:element name="Purpose" minOccurs="1" maxOccurs="unbounded">
130                 <xs:complexType>
```

```
131                     <xs:simpleContent>
132                       <xs:extension base="xs:string">
133                           <xs:attribute name="expireTime" type="xs:duration" use
                                ="required"/>
134                       </xs:extension>
135                     </xs:simpleContent>
136                 </xs:complexType>
137               </xs:element>
138           </xs:sequence>
139       </xs:complexType>
140     </xs:element>
141
142     <!-- AttributeValue (including zero-knowledge proof) -->
143     <xs:element name="AttributeValue">
144       <xs:complexType>
145         <xs:simpleContent>
146             <xs:extension base="xs:string">
147                   <xs:attribute name="relation">
148                   <xs:simpleType>
149                     <xs:restriction base="xs:string">
150                       <xs:pattern value="GT|GTE|LT|LTE|E|CONTAINS"/>
151                     </xs:restriction>
152                   </xs:simpleType>
153               </xs:attribute>
154               <xs:attribute name="value" type="xs:string"/>
155           </xs:extension>
156         </xs:simpleContent>
157       </xs:complexType>
158     </xs:element>
159
160
161     <!-- Attributes -->
162     <xs:element name="Attribute">
163       <xs:complexType>
164         <xs:sequence>
165             <xs:element ref="AttributeValue"/>
166             <xs:element ref="PurposesSet"/>
167             <xs:element ref="ObligationsSet" minOccurs="0" maxOccurs="unbounded"/
                  >
168         </xs:sequence>
169         <xs:attribute name="certifiedBy" type="xs:string"/>
170       </xs:complexType>
171     </xs:element>
172
173
174     <xs:element name="AttributesSet">
175       <xs:complexType>
176         <xs:sequence>
177           <xs:element ref="Attribute" minOccurs="0" maxOccurs="unbounded"/>
178         </xs:sequence>
179       </xs:complexType>
```

```
180     </xs:element>
181
182     <!-- Identity (abstract) -->
183     <xs:element name="AbstractIdentity" abstract="true" />
184       <xs:complexType name="AbstractIdentity" >
185         <xs:sequence>
186           <xs:element name="Identifier" type="xs:string" minOccurs="0" maxOccurs=
                "1"/>
187           <xs:element name="Representative" type="xs:string" minOccurs="0"
                maxOccurs="1"/> <!-- Full Name of the representative person -->
188           <xs:element name="Address" type="xs:string" minOccurs="0" maxOccurs="1"
                />
189           <xs:element name="Country" type="xs:string" minOccurs="0" maxOccurs="1"
                />
190           <xs:element name="Email" type="xs:string" minOccurs="0" maxOccurs="1"/>
191           <xs:element name="Phone" type="xs:string" minOccurs="0" maxOccurs="1"/>
192           <xs:element name="URI" type="xs:anyURI" minOccurs="0" maxOccurs="1"/>
193           <xs:element name="HumanReadablePolicyURL" type="xs:anyURI" minOccurs="0
                " maxOccurs="1"/>
194           <xs:element name="CertificateURL" type="xs:anyURI" minOccurs="0"
                maxOccurs="1"/>
195           <xs:element name="EmblemURL" type="xs:anyURI" minOccurs="0" maxOccurs="
                1"/>
196         </xs:sequence>
197       </xs:complexType>
198
199     <!-- Identity -->
200     <xs:element name="Identity">
201       <xs:complexType>
202         <xs:complexContent>
203         <xs:extension base="AbstractIdentity">
204             <xs:sequence>
205             </xs:sequence>
206         </xs:extension>
207         </xs:complexContent>
208       </xs:complexType>
209     </xs:element>
210
211
212     <!-- HigherPurposesSet -->
213     <xs:element name="HigherPurposesSet" type="HigherPurposesSet"/>
214     <xs:complexType name="HigherPurposesSet">
215         <xs:sequence>
216             <xs:element name="HigherPurpose" minOccurs="1" maxOccurs="unbounded"
                  type="xs:string"/>
217         </xs:sequence>
218         <xs:attribute name="semantics">
219       <xs:simpleType>
220         <xs:restriction base="xs:string">
221           <xs:pattern value="and|or"/>
222         </xs:restriction>
```

```
223       </xs:simpleType>
224     </xs:attribute>
225     </xs:complexType>
226
227     <!-- CertifierForAttribute -->
228     <xs:element name="CertifierForAttribute">
229       <xs:complexType>
230         <xs:complexContent>
231         <xs:extension base="AbstractIdentity">
232             <xs:sequence>
233             </xs:sequence>
234             <xs:attribute name="certifierId" type="xs:string" use="required"/>
235          </xs:extension>
236         </xs:complexContent>
237
238       </xs:complexType>
239     </xs:element>
240
241     <xs:element name="CertifiersSetForAttributes">
242         <xs:complexType>
243             <xs:sequence>
244                 <xs:element ref="CertifierForAttribute" minOccurs="1" maxOccurs="
                        unbounded"/>
245             </xs:sequence>
246         </xs:complexType>
247     </xs:element>
248
249     <!-- Signatature -->
250     <xs:element name="Signature" type="xs:base64Binary" />
251
252     <!-- CertifiersSetForSeals -->
253     <xs:element name="CertifiersSetForSeals">
254         <xs:complexType>
255             <xs:sequence>
256                 <xs:element name="CertifierForSeal" minOccurs="1" maxOccurs="
                        unbounded">
257                   <xs:complexType>
258                     <xs:sequence>
259                         <xs:element ref="Identity"/>
260                         <xs:element ref="Signature"/>
261                     </xs:sequence>
262                   </xs:complexType>
263                 </xs:element>
264             </xs:sequence>
265         </xs:complexType>
266     </xs:element>
267
268
269
270     <!-- Container-Type-Attribute -->
271     <xs:attribute name="type">
```

```
272       <xs:simpleType>
273         <xs:restriction base="xs:string">
274           <xs:pattern value="policy|preference|recommendation"/>
275         </xs:restriction>
276       </xs:simpleType>
277     </xs:attribute>
278
279     <!-- Container (abstract) -->
280     <xs:element name="AbstractContainer"/>
281       <xs:complexType name="AbstractContainer" >
282       <xs:sequence>
283           <xs:element ref="HigherPurposesSet"/>
284           <xs:element ref="Identity"/>
285           <xs:element ref="AttributesSet"/>
286           <xs:element ref="CertifiersSetForAttributes" minOccurs="0"/>
287           <xs:element name="DownstreamUsage" type="AbstractContainer" minOccurs="
                0"/> <!-- if left out, no downstreamUsage is not allowed -->
288         </xs:sequence>
289       </xs:complexType>
290
291     <!-- Container -->
292     <xs:element name="Container">
293         <xs:complexType>
294             <xs:complexContent>
295               <xs:extension base="AbstractContainer">
296                 <xs:sequence>
297                 </xs:sequence>
298                 <xs:attribute ref="type" use="required"/>
299               </xs:extension>
300             </xs:complexContent>
301         </xs:complexType>
302     </xs:element>
303
304     <!-- UPL-Root -->
305     <xs:element name="UPL">
306       <xs:complexType>
307        <xs:sequence>
308           <xs:element ref="Container"/>
309           <xs:element ref="Signature"/>
310           <xs:element ref="CertifiersSetForSeals" minOccurs="0"/>
311         </xs:sequence>
312       </xs:complexType>
313     </xs:element>
314 </xs:schema>
```

Listing A.1: UPL schema file

A.2 UPL Example Instances

A.2.1 Instances for Stage 1

```
<?xml version="1.0" encoding="UTF-8"?>

<UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
    <Container type="policy">

        <HigherPurposesSet>
            <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/browsing</
                HigherPurpose>
        </HigherPurposesSet>
        <Identity>
            <Identifier>Example Newspaper</Identifier>
            <Address>SE-65 636 Karlstad, Sweden</Address>
            <Country>SE</Country>
            <Email>contact@example-karlstad-news.se</Email>
            <Phone>+46 8 405 10 00</Phone>
            <URI>example-karlstad-news.se</URI>
            <HumanReadablePolicyURL>http://example-karlstad-news.se/terms/privacy
                /en/</HumanReadablePolicyURL>
            <CertificateURL>http://example-karlstad-news.se/imprint/
                policy_certificate.pem</CertificateURL>
        </Identity>
        <AttributesSet/>
    </Container>
    <Signature>
        QXQgZ3BsLCB3ZSBob2xkIG91ciBjbGllbnRzIHRvIGluZHVzdHJ5LWxlY
        aXZhY3kgc3RhbmRhcmRzLiBncGwgZG9lcyBldmVyeXRoaW5nIHBvc3NpY
        IGNsaWVudCBXZWIgc2l0ZXMgcHJvdGVjdCB0aGUgcHJpdmFjeSBvZiB5b
        Zm9ybWF0aW9uLCBidXQgd2UgYWxzbyByZWx5IG9uIHlvdXIgdmlnaWxhb
        IHRoZSBpbnRlZ3JpdHkgb2Ygb3VyIHNlYWwgcHJvZ3JhbXMgd2l0aCBvd
        dGUgUmVzb2x1dGlvbiBwcm9ncmFtLCB3aGljaCBsZXRzIHVzZXJzIGhvb
        YWNjb3VudGFibGUuDQoNCmdwbJJzIERpc3B1dGUgUmVzb2x1dGlvbiBGb
        ZSB0b29sIHRoYXQgbGV0cyB5b3UgcmVwb3J0IHZpb2xhdGlvbnMgb2Ygc
        c3RhdGVtZW50cyBhbmQgc3BlY2lmaWMgb25saW5lIHByaXZhY3kgaXNzd
        biB0byBncGwgY2xpZW50cyBXZWIgc2l0ZXMuIGdwbCBpbnZlc3RpZ2F0Z
        IGNvbXBsYWludHMgYW5kIG1lZGlhdGVzIHNvbHV0aW9ucyBiZXR3ZWVuI
        c2l0ZXMuDQo=
    </Signature>
</UPL>
```

Listing A.2: UPL example policy on stage 1

```
<?xml version="1.0" encoding="UTF-8"?>

<UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
4       xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
5       <Container type="preference">
6
7           <HigherPurposesSet>
8               <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/browsing</
                    HigherPurpose>
9           </HigherPurposesSet>
10          <Identity/>
11          <AttributesSet/>
12      </Container>
13      <Signature/>
14  </UPL>
```

Listing A.3: UPL example preference on stage 1

```
1   <?xml version="1.0" encoding="UTF-8"?>
2
3   <UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4       xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
5       <Container type="recommendation">
6
7           <HigherPurposesSet>
8               <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/browsing</
                    HigherPurpose>
9           </HigherPurposesSet>
10          <Identity>
11                  <Identifier>Example Community for Data Privacy</Identifier>
12                  <Representative>Mrs. Jane Doe</Representative>
13                  <Country>DE</Country>
14                  <Email>contact@example-open-privacy-board.org</Email>
15                  <URI>www.example-open-privacy-board.org</URI>
16                  <HumanReadablePolicyURL>http://example-open-privacy-board.org/
                        privacy-seals/en/</HumanReadablePolicyURL>
17                  <CertificateURL>http://example-open-privacy-board.org/imprint/
                        policy_seal_certificate.pem</CertificateURL>
18                  <EmblemURL>http://example-open-privacy-board.org/imprint/logo.svg
                        </EmblemURL>
19          </Identity>
20          <AttributesSet/>
21      </Container>
22      <Signature/>
23  </UPL>
```

Listing A.4: UPL example recommendation on stage 1

A.2.2 Instances for Stage 2

```
1   <?xml version="1.0" encoding="UTF-8"?>
2
```

```
3  <UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4      xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
5      <Container type="policy">
6
7          <HigherPurposesSet>
8              <HigherPurpose>https://www.kau.se/upl/early-contact</HigherPurpose>
9          </HigherPurposesSet>
10         <Identity>
11             <Identifier>Example Insurance Company AB</Identifier>
12             <Address>SE-21 010 Malm??weden</Address>
13             <Country>SE</Country>
14             <Email>contact@example-insurance.se</Email>
15             <Phone>+46 8 405 10 00</Phone>
16             <URI>example-insurance.se</URI>
17             <HumanReadablePolicyURL>http://example-insurance.se/terms/privacy/en/
                   </HumanReadablePolicyURL>
18             <CertificateURL>http://example-insurance.se/imprint/
                   policy_certificate.pem</CertificateURL>
19         </Identity>
20         <AttributesSet>
21             <Attribute>
22                 <AttributeValue>SessionIdentifier</AttributeValue>
23                 <PurposesSet>
24                     <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                           login</Purpose>
25                     <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                           state</Purpose>
26                     <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv1/
                           tailoring</Purpose>
27                 </PurposesSet>
28             </Attribute>
29         </AttributesSet>
30
31     </Container>
32     <Signature>
33         QXQgZ3BsLCB3ZSBob2xkIG91ciBjbGllbnRzIHRvIGluZHVzdHJ5LWxlYWRpbm
34         aXZhY3kgc3RhbmRhcmRzLiBncGwgZG9lcyBldmVyeXRoaW5nIHBvc3NpYmxlIH
35         IGNsaWVudCBXZWIgc2l0ZXMgcHJvdGVjdCB0aGUgcHJpdmFjeSBvZiB5b3VyIH
36         Zm9ybWF0aW9uLCBidXQgd2UgYWxzbyByZWx5IG9uIHlvdXIgdmlnaWxhbmNlLi
37         IHRoZSBpbnRlZ3JpdHkgb2Ygb3VyIHNlYWwgcHJvZ3JhbXMgd2l0aCBvdXIgb2
38         dGUgUmVzb2x1dGlvbiBwcm9ncmFtLCB3aGljaCBsZXRzIHVzZXJzIGhvbGQgZ3
39         YWNjb3VudGFibGUuDQoNCmdwbJJzIERpc3B1dGUgUmVzb2x1dGlvbiBGb3JtIG
40         ZSB0b29sIHRoYXQgbGV0cyB5b3UgcmVwb3J0IHZpb2xhdGlvbnMgb2YgcG9zdG
41         c3RhdGVtZW50cyBhbmQgc3BlY2lmaWMgb25saW5lIHByaXZhY3kgaXNzdWVzIH
42         biB0byBncGwgY2xpZW50cyBXZWIgc2l0ZXMuIGdwbCBpbnZlc3RpZ2F0ZXMgYW
43         IGNvbXBsYWludHMgYW5kIG1lZGlhdGVzIHNvbHV0aW9ucyBiZXR3ZWVuIHVzZX
44         c2l0ZXMuDQo=
45     </Signature>
46     <CertifiersSetForSeals>
47         <CertifierForSeal>
48             <Identity>
```

```
                <Identifier>Data Protection Agency of Sweden</Identifier>
                <Representative>Mr. John Doe</Representative>
                <Country>SE</Country>
                <Email>contact@dpa.gov.se</Email>
                <Phone>+46 1 225 14 77 00</Phone>
                <URI>www.dpa.gov.se</URI>
                <CertificateURL>http://example-insurance.se/imprint/
                    policy_seal_certificate.pem</CertificateURL>
            </Identity>
            <Signature>
                UVhRZ1ozQnNMQ0IzWlNCb2IyeGtJRzkxY2lCamJHbGxiblJ6SUhSdklHbHVaSF
                V1JwYm1jZ2IyNXNhVzVsSUhCeQ0KYVhaaFkza2djM1JoYm1SaGNtUnpMaUJuY0
                ZG1WeWVYUm9hVzVuSUhCdmMzTnBZbXhsSUhSdklHaGxiSEFnYjNWeQ0KSUdOc2
                Z2MybDBaWE1nY0hKdmRHVmpkQ0IwYUdVZ2NISnBkbUZqZVNCdlppQjViM1Z5SU
                SUdsdQ0KWm05eWJXRjBhVzl1TENCaWRYUWdkMlVnWVd4emJ5QnlaV3g1SUc5dU
                bmFXeGhibU5sTGlCWFpTQmlZV05ySUhWdw0KSUhSb1pTQnBiblJsWjNKcGRIa2
                TmxZV3dnY0hKdlozSmhiWE1nZDJsMGFDQnZkWElnYjI1c2FXNWxJRVJwYzNCMQ
                MngxZEdsdmJpQndjbTluY21GdExDQjNhR2xqYUNCc1pYUnpJSFZ6WlhKeklHaH
                TnNhV1Z1ZEhNZw0KWVdOamIzVnVkR0ZpYkdVdURRb05DbWR3YkpKeklFUnBjM0
                MngxZEdsdmJpQkdiM0p0SUdseklHRnVJRzl1YkdsdQ0KWlNCMGIyOXNJSFJvWV
                YjNVZ2NtVndiM0owSUhacGIyeGhkR2x2Ym5NZ2IyWWdjRzl6ZEdWa0lIQnlhWF
                aGRHVnRaVzUwY3lCaGJtUWdjM0JsWTJsbWFXTWdiMjVzYVc1bElIQnlhWFpoWT
                SUhSb1lYUWdjR1Z5ZEdGcA0KYmlCMGJ5Qm5jR3dnWTJ4cFpXNTBjeUJYWldJZ2
                d2JDQnBiblpsYzNScFoyRjBaWE1nWVd4c0lHVnNhV2RwWW14bA0KSUdOdmJYQn
                NWtJRzFsWkdsaGRHVnpJSE52YkhWMGFXOXVjeUJpWlhSM1pXVnVJSFZ6WlhKek
                ZwOKYzJsMFpYTXVEUW89
            </Signature>
        </CertifierForSeal>
    </CertifiersSetForSeals>
</UPL>
```

Listing A.5: UPL example policy on stage 2

```
<?xml version="1.0" encoding="UTF-8"?>

<UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
    <Container type="preference">

        <HigherPurposesSet>
            <HigherPurpose>https://www.kau.se/upl/early-contact</HigherPurpose>
        </HigherPurposesSet>
        <Identity>
            <Country>SE</Country>
        </Identity>
        <AttributesSet>
            <Attribute>
                <AttributeValue>SessionIdentifier</AttributeValue>
                <PurposesSet>
                    <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        login</Purpose>
```

```
                    <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        state</Purpose>
                    <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv1/
                        tailoring</Purpose>
                </PurposesSet>
            </Attribute>
        </AttributesSet>

    </Container>
    <Signature/>
    <CertifiersSetForSeals>
        <CertifierForSeal>
            <Identity>
                <Identifier>Data Protection Agency of Sweden</Identifier>
                <Representative>Mr. John Doe</Representative>
                <Country>SE</Country>
                <Email>contact@dpa.gov.se</Email>
                <Phone>+46 1 225 14 77 00</Phone>
                <URI>www.dpa.gov.se</URI>
                <CertificateURL>http://example-insurance.se/imprint/
                    policy_seal_certificate.pem</CertificateURL>
            </Identity>
            <Signature/>
        </CertifierForSeal>
    </CertifiersSetForSeals>
</UPL>
```

Listing A.6: UPL example preference on stage 2

```
<?xml version="1.0" encoding="UTF-8"?>

<UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
    <Container type="recommendation">

        <HigherPurposesSet>
            <HigherPurpose>https://www.kau.se/upl/early-contact</HigherPurpose>
        </HigherPurposesSet>
        <Identity>
                <Identifier>Data Protection Agency of Sweden</Identifier>
                <Representative>Mr. John Doe</Representative>
                <Country>SE</Country>
                <Email>contact@dpa.gov.se</Email>
                <Phone>+46 1 225 14 77 00</Phone>
                <URI>www.dpa.gov.se</URI>
                <HumanReadablePolicyURL>http://dpa.gov.se/privacy-seals/en/</
                    HumanReadablePolicyURL>
                <CertificateURL>http://dpa.gov.se/imprint/policy_seal_certificate
                    .pem</CertificateURL>
                <EmblemURL>http://dpa.gov.se/imprint/logo.svg</EmblemURL>
        </Identity>
```

```
21          <AttributesSet>
22              <Attribute>
23                  <AttributeValue>SessionIdentifier</AttributeValue>
24                  <PurposesSet>
25                      <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                            login</Purpose>
26                      <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                            state</Purpose>
27                      <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv1/
                            tailoring</Purpose>
28                  </PurposesSet>
29              </Attribute>
30          </AttributesSet>
31
32      </Container>
33      <Signature>
34          QXQgZ3BsLCB3ZSBob2xkIG91ciBjbGllbnRzIHRvIGluZHVzdHJ5LWxlYWRpbmc
35          aXZhY3kgc3RhbmRhcmRzLiBncGwgZG9lcyBldmVyeXRoaW5nIHBvc3NpYmxlIHR
36          IGNsaWVudCBXZWIgc2l0ZXMgcHJvdGVjdCB0aGUgcHJpdmFjeSBvZiB5b3VyIHB
37          Zm9ybWF0aW9uLCBidXQgd2UgYWxzbyByZWx5IG9uIHlvdXIgdmlnaWxhbmNlLiB
38          IHRoZSBpbnRlZ3JpdHkgb2Ygb3VyIHNlYWwgcHJvZ3JhbXMgd2l0aCBvdXIgb25
39          dGUgUmVzb2x1dGlvbiBwcm9ncmFtLCB3aGljaCBsZXRzIHVzZXJzIGhvbGQgZ3B
40          YWNjb3VudGFibGUuDQoNCmdwbJJzIERpc3B1dGUgUmVzb2x1dGlvbiBGb3JtIGl
41          ZSB0b29sIHRoYXQgbGV0cyB5b3UgcmVwb3J0IHZpb2xhdGlvbnMgb2YgcG9zdGV
42          c3RhdGVtZW50cyBhbmQgc3BlY2lmaWMgb25saW5lIHByaXZhY3kgaXNzdWVzIHR
43          biB0byBncGwgY2xpZW50cyBXZWIgc2l0ZXMuIGdwbCBpbnZlc3RpZ2F0ZXMgYWx
44          IGNvbXBsYWludHMgYW5kIG1lZGlhdGVzIHNvbHV0aW9ucyBiZXR3ZWVuIHVzZXJ
45          c2l0ZXMuDQo=
46      </Signature>
47      <CertifiersSetForSeals>
48          <CertifierForSeal>
49              <Identity>
50                  <Identifier>Any Data Protection Agency</Identifier>
51                  <URI>any.dpa.eu</URI>
52              </Identity>
53              <Signature/>
54          </CertifierForSeal>
55      </CertifiersSetForSeals>
56  </UPL>
```

Listing A.7: UPL example recommendation on stage 2

A.2.3 Instances for Stage 3

```
1   <?xml version="1.0" encoding="UTF-8"?>
2
3   <UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4       xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
```

```
5     <Container type="policy">
6
7         <HigherPurposesSet semantics="and">
8             <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/arts</HigherPurpose>
9             <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/marketing</
                  HigherPurpose>
10        </HigherPurposesSet>
11        <Identity>
12            <Identifier>Example Video Plattform AB</Identifier>
13            <Address>SE-40 010 Gothenburg, Sweden</Address>
14            <Country>SE</Country>
15            <Email>contact@example-film3000.se</Email>
16            <Phone>+46 8 405 10 00</Phone>
17            <URI>example-film3000.se</URI>
18            <HumanReadablePolicyURL>http://example-film3000.se/terms/privacy/en/<
                  /HumanReadablePolicyURL>
19            <CertificateURL>http://example-film3000.se/imprint/policy_certificate
                  .pem</CertificateURL>
20        </Identity>
21        <AttributesSet>
22            <Attribute>
23                <AttributeValue>SessionIdentifier</AttributeValue>
24                <PurposesSet>
25                    <Purpose expireTime="P1D">http://www.w3.org/2006/01/P3Pv11/
                          login</Purpose>
26                    <Purpose expireTime="P1D">http://www.w3.org/2006/01/P3Pv11/
                          state</Purpose>
27                    <Purpose expireTime="P1D">http://www.w3.org/2006/01/P3Pv1/
                          tailoring</Purpose>
28                </PurposesSet>
29            </Attribute>
30
31            <Attribute certifiedBy="SE-GOV-CA">
32                <AttributeValue relation="GTE" value="18">Age</AttributeValue>
33                <PurposesSet>
34                    <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                          individual-decision</Purpose>
35                    <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                          tailoring</Purpose>
36                </PurposesSet>
37            </Attribute>
38
39            <Attribute certifiedBy="SE-GOV-CA">
40                <AttributeValue>Country</AttributeValue>
41                <PurposesSet>
42                    <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                          individual-decision</Purpose>
43                    <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                          tailoring</Purpose>
44                </PurposesSet>
45            </Attribute>
```

```
46          </AttributesSet>
47
48          <CertifiersSetForAttributes>
49              <CertifierForAttribute certifierId="SE-GOV-CA">
50                  <Identifier>Government Offices of Sweden</Identifier>
51                  <Representative>Mr. John Gustavsson</Representative>
52                  <Email>contact@ca.gov.se</Email>
53                  <Phone>+46 8 405 10 00</Phone>
54                  <URI>www.ca.gov.se</URI>
55              </CertifierForAttribute>
56          </CertifiersSetForAttributes>
57
58          <DownstreamUsage>
59              <HigherPurposesSet>
60                  <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/marketing</
                        HigherPurpose>
61              </HigherPurposesSet>
62              <Identity>
63                  <Identifier>DownstreamController.com</Identifier>
64                  <Address>SE-40 010 Gothenburg, Sweden</Address>
65                  <Country>SE</Country>
66                  <Email>contact@datacenter.downstreamcontroller.com</Email>
67                  <URI>datacenter.downstreamcontroller.com</URI>
68                  <HumanReadablePolicyURL>http://datacenter.downstreamcontroller.
                        com/terms/privacy/en/</HumanReadablePolicyURL>
69              </Identity>
70
71              <AttributesSet>
72                  <Attribute certifiedBy="SE-GOV-CA">
73                      <AttributeValue>Country</AttributeValue>
74                      <PurposesSet>
75                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                                individual-decision</Purpose>
76                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                                tailoring</Purpose>
77                      </PurposesSet>
78                  </Attribute>
79              </AttributesSet>
80              <CertifiersSetForAttributes>
81                  <CertifierForAttribute certifierId="SE-GOV-CA">
82                      <Identifier>Government Offices of Sweden</Identifier>
83                      <Representative>Mr. John Gustavsson</Representative>
84                      <Email>contact@ca.gov.se</Email>
85                      <Phone>+46 8 405 10 00</Phone>
86                      <URI>www.ca.gov.se</URI>
87                  </CertifierForAttribute>
88              </CertifiersSetForAttributes>
89          </DownstreamUsage>
90
91      </Container>
92      <Signature>
```

```
93          QXQgZ3BsLCB3ZSBob2xkIG91ciBjbGllbnRzIHRvIGluZHVzdHJ5LWxlYWRp
94          aXZhY3kgc3RhbmRhcmRzLiBncGwgZG9lcyBldmVyeXRoaW5nIHBvc3NpYmxl
95          IGNsaWVudCBXZWIgc2l0ZXMgcHJvdGVjdCB0aGUgcHJpdmFjeSBvZiB5b3Vy
96          Zm9ybWF0aW9uLCBidXQgd2UgYWxzbyByZWx5IG9uIHlvdXIgdmlnaWxhbmNl
97          IHRoZSBpbnRlZ3JpdHkgb2Ygb3VyIHNlYWwgcHJvZ3JhbXMgd2l0aCBvdXIg
98          dGUgUmVzb2x1dGlvbiBwcm9ncmFtLCB3aGljfCBsZXRzIHVzZXJzIGhvbGQg
99          YWNjb3VudGFibGUuDQoNCmdwbJJzIERpc3B1dGUgUmVzb2x1dGlvbiBGb3Jt
100         ZSB0b29sIHRoYXQgbGV0cyB5b3UgcmVwb3J0IHZpb2xhdGlvbnMgb2YgcG9z
101         c3RhdGVtZW50cyBhbmQgc3BlY2lmaWMgb25saW5lIHByaXZhY3kgaXNzdWVz
102         biB0byBncGwgY2xpZW50cyBXZWIgc2l0ZXMuIGdwbCBpbnZlc3RpZ2F0ZXMg
103         IGNvbXBsYWludHMgYW5kIG1lZGlhdGVzIHNvbHV0aW9ucyBiZXR3ZWVuIHVz
104         c2l0ZXMuDQo=
105     </Signature>
106 </UPL>
```

Listing A.8: UPL example policy on stage 3

```
1  <?xml version="1.0" encoding="UTF-8"?>
2
3  <UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4      xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
5      <Container type="preference">
6
7          <HigherPurposesSet semantics="and">
8              <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/arts</HigherPurpose>
9              <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/marketing</
                   HigherPurpose>
10         </HigherPurposesSet>
11         <Identity/>
12         <AttributesSet>
13             <Attribute>
14                 <AttributeValue>SessionIdentifier</AttributeValue>
15                 <PurposesSet>
16                     <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                           login</Purpose>
17                     <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                           state</Purpose>
18                     <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv1/
                           tailoring</Purpose>
19                 </PurposesSet>
20             </Attribute>
21
22             <Attribute certifiedBy="SE-GOV-CA">
23                 <AttributeValue relation="GTE">Age</AttributeValue>
24                 <PurposesSet>
25                     <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                           individual-decision</Purpose>
26                     <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                           tailoring</Purpose>
27                 </PurposesSet>
28             </Attribute>
```

```
29
30              <Attribute certifiedBy="SE-GOV-CA">
31                  <AttributeValue>Country</AttributeValue>
32                  <PurposesSet>
33                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                            individual-decision</Purpose>
34                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                            tailoring</Purpose>
35                  </PurposesSet>
36              </Attribute>
37          </AttributesSet>
38
39          <CertifiersSetForAttributes>
40              <CertifierForAttribute certifierId="SE-GOV-CA">
41                  <Identifier>Government Offices of Sweden</Identifier>
42                  <Representative>Ms. Carina Gustavsson</Representative>
43                  <Email>contact@ca.gov.se</Email>
44                  <Phone>+46 8 405 10 00</Phone>
45                  <URI>www.ca.gov.se</URI>
46              </CertifierForAttribute>
47          </CertifiersSetForAttributes>
48
49          <DownstreamUsage>
50              <HigherPurposesSet>
51                  <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/marketing</
                        HigherPurpose>
52              </HigherPurposesSet>
53              <Identity>
54                  <Identifier>DownstreamController.com</Identifier>
55                  <URI>datacenter.downstreamcontroller.com</URI>
56              </Identity>
57
58              <AttributesSet>
59                  <Attribute certifiedBy="SE-GOV-CA">
60                      <AttributeValue>Country</AttributeValue>
61                      <PurposesSet>
62                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                                individual-decision</Purpose>
63                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                                tailoring</Purpose>
64                      </PurposesSet>
65                  </Attribute>
66              </AttributesSet>
67
68              <CertifiersSetForAttributes>
69                  <CertifierForAttribute certifierId="SE-GOV-CA">
70                      <Identifier>Government Offices of Sweden</Identifier>
71                      <Representative>Ms. Carina Gustavsson</Representative>
72                      <Email>contact@ca.gov.se</Email>
73                      <Phone>+46 8 405 10 00</Phone>
74                      <URI>www.ca.gov.se</URI>
```

```
75                </CertifierForAttribute>
76            </CertifiersSetForAttributes>
77        </DownstreamUsage>
78
79    </Container>
80    <Signature/>
81 </UPL>
```

Listing A.9: UPL example preference on stage 3

```
1  <?xml version="1.0" encoding="UTF-8"?>
2
3  <UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4      xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
5      <Container type="recommendation">
6
7          <HigherPurposesSet semantics="and">
8              <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/arts</HigherPurpose>
9              <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/marketing</
                   HigherPurpose>
10         </HigherPurposesSet>
11         <Identity>
12                 <Identifier>Data Protection Agency of Sweden</Identifier>
13                 <Representative>Mr. John Doe</Representative>
14                 <Country>SE</Country>
15                 <Email>contact@dpa.gov.se</Email>
16                 <Phone>+46 1 225 14 77 00</Phone>
17                 <URI>www.dpa.gov.se</URI>
18                 <HumanReadablePolicyURL>http://dpa.gov.se/privacy-seals/en/</
                       HumanReadablePolicyURL>
19                 <CertificateURL>http://dpa.gov.se/imprint/policy_seal_certificate
                       .pem</CertificateURL>
20                 <EmblemURL>http://dpa.gov.se/imprint/logo.svg</EmblemURL>
21         </Identity>
22         <AttributesSet>
23             <Attribute>
24                 <AttributeValue>SessionIdentifier</AttributeValue>
25                 <PurposesSet>
26                     <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                           login</Purpose>
27                     <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                           state</Purpose>
28                     <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv1/
                           tailoring</Purpose>
29                 </PurposesSet>
30             </Attribute>
31
32             <Attribute certifiedBy="SE-GOV-CA">
33                 <AttributeValue relation="GTE" value="18">Age</AttributeValue>
34                 <PurposesSet>
35                     <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
```

```
                    individual-decision</Purpose>
36                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                        tailoring</Purpose>
37              </PurposesSet>
38          </Attribute>
39
40          <Attribute certifiedBy="SE-GOV-CA">
41              <AttributeValue>Country</AttributeValue>
42              <PurposesSet>
43                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                        individual-decision</Purpose>
44                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                        tailoring</Purpose>
45              </PurposesSet>
46          </Attribute>
47      </AttributesSet>
48
49      <CertifiersSetForAttributes>
50          <CertifierForAttribute certifierId="SE-GOV-CA">
51              <Identifier>Government Offices of Sweden</Identifier>
52              <Representative>Mr. John Gustavsson</Representative>
53              <Email>contact@ca.gov.se</Email>
54              <Phone>+46 8 405 10 00</Phone>
55              <URI>www.ca.gov.se</URI>
56          </CertifierForAttribute>
57      </CertifiersSetForAttributes>
58
59      <DownstreamUsage>
60          <HigherPurposesSet>
61              <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/marketing</
                    HigherPurpose>
62          </HigherPurposesSet>
63          <Identity/>
64
65          <AttributesSet>
66              <Attribute certifiedBy="SE-GOV-CA">
67                  <AttributeValue>Country</AttributeValue>
68                  <PurposesSet>
69                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                            individual-decision</Purpose>
70                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                            tailoring</Purpose>
71                  </PurposesSet>
72              </Attribute>
73          </AttributesSet>
74
75          <CertifiersSetForAttributes>
76              <CertifierForAttribute certifierId="SE-GOV-CA">
77                  <Identifier>Government Offices of Sweden</Identifier>
78                  <Representative>Ms. Carina Gustavsson</Representative>
79                  <Email>contact@ca.gov.se</Email>
```

```
                    <Phone>+46 8 405 10 00</Phone>
                    <URI>www.ca.gov.se</URI>
                </CertifierForAttribute>
            </CertifiersSetForAttributes>
        </DownstreamUsage>

    </Container>
    <Signature>
        QXQgZ3BsLCB3ZSBob2xkIG91ciBjbGllbnRzIHRvIGluZHVzdHJ5LWxlYWRpbmcg
        aXZhY3kgc3RhbmRhcmRzLiBncGwgZG9lcyBldmVyeXRoaW5nIHBvc3NpYmxlIHRv
        IGNsaWVudCBXZWIgc2l0ZXMgcHJvdGVjdCB0aGUgcHJpdmFjeSBvZiB5b3VyIHBl
        Zm9ybWF0aW9uLCBidXQgd2UgYWxzbyByZWx5IG9uIHlvdXIgdmlnaWxhbmNlLiBX
        IHRoZSBpbnRlZ3JpdHkgb2Ygb3VyIHNlYWwgcHJvZ3JhbXMgd2l0aCBvdXIgb25s
        dGUgUmVzb2x1dGlvbiBwcm9ncmFtLCB3aGljfCBsZXRzIHVzZXJzIGhvbGQgZ3Bs
        YWNjb3VudGFibGUuDQoNCmdwbJJzIERpc3B1dGUgUmVzb2x1dGlvbiBGb3JtIGlz
        ZSB0b29sIHRoYXQgbGV0cyB5b3UgcmVwb3J0IHZpb2xhdGlvbnMgb2YgcG9zdGVk
        c3RhdGVtZW50cyBhbmQgc3BlY2lmaWMgb25saW5lIHByaXZhY3kgaXNzdWVzIHRo
        biB0byBncGwgY2xpZW50cyBXZWIgc2l0ZXMuIGdwbCBpbnZlc3RpZ2F0ZXMgYWxs
        IGNvbXBsYWludHMgYW5kIG1lZGlhdGVzIHNvbHV0aW9ucyBiZXR3ZWVuIHVzZXJz
        c2l0ZXMuDQo=
    </Signature>
</UPL>
```

Listing A.10: UPL example recommendation on stage 3

A.2.4 Instances for Stage 4

```
<?xml version="1.0" encoding="UTF-8"?>

<UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
    <Container type="policy">
        <HigherPurposesSet>
            <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/government</
                HigherPurpose>
        </HigherPurposesSet>
        <Identity>
            <Identifier>Government Offices of Sweden</Identifier>
            <Address>SE-103 33 Stockholm, Sweden</Address>
            <Country>SE</Country>
            <Email>contact@sweden.gov.se</Email>
            <Phone>+46 8 405 10 00</Phone>
            <URI>sweden.gov.se</URI>
            <HumanReadablePolicyURL>http://sweden.gov.se/terms/privacy/en/</
                HumanReadablePolicyURL>
            <CertificateURL>http://sweden.gov.se/imprint/policy_certificate.pem</
                CertificateURL>
            <EmblemURL>http://sweden.gov.se/imprint/logo.svg</EmblemURL>
```

```
19          </Identity>
20          <AttributesSet>
21              <Attribute certifiedBy="SE-GOV-CA">
22                  <AttributeValue>First Name</AttributeValue>
23                  <PurposesSet>
24                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                            government</Purpose>
25                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                            communicate</Purpose>
26                      <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                            account</Purpose>
27                  </PurposesSet>
28              </Attribute>
29
30              <Attribute certifiedBy="SE-GOV-CA">
31                  <AttributeValue>Last Name</AttributeValue>
32                  <PurposesSet>
33                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                            government</Purpose>
34                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                            communicate</Purpose>
35                      <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                            account</Purpose>
36                  </PurposesSet>
37              </Attribute>
38
39              <Attribute>
40                  <AttributeValue>Email</AttributeValue>
41                  <PurposesSet>
42                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                            communicate</Purpose>
43                      <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                            account</Purpose>
44                      <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                            marketing</Purpose>
45                  </PurposesSet>
46                  <ObligationsSet>
47                      <Obligation>
48                          <TriggersSet>
49                              <TriggerPersonalDataDeleted>
50                                  <MaxDelay>P1D</MaxDelay>
51                              </TriggerPersonalDataDeleted>
52                              <TriggerOnViolation>
53                                  <MaxDelay>P5D</MaxDelay>
54                              </TriggerOnViolation>
55                          </TriggersSet>
56                          <ActionNotifyDataSubject/>
57                      </Obligation>
58                  </ObligationsSet>
59              </Attribute>
60          </AttributesSet>
```

```
61
62
63          <CertifiersSetForAttributes>
64              <CertifierForAttribute certifierId="SE-GOV-CA">
65                  <Identifier>Government Offices of Sweden</Identifier>
66                  <Representative>Mr. John Gustavsson</Representative>
67                  <Email>contact@ca.gov.se</Email>
68                  <Phone>+46 8 405 10 00</Phone>
69                  <URI>www.ca.gov.se</URI>
70              </CertifierForAttribute>
71          </CertifiersSetForAttributes>
72
73          <DownstreamUsage>
74              <HigherPurposesSet>
75                  <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/government</
                        HigherPurpose>
76              </HigherPurposesSet>
77              <Identity/>
78
79              <AttributesSet>
80                  <Attribute>
81                      <AttributeValue>First Name</AttributeValue>
82                      <PurposesSet>
83                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11
                                /government</Purpose>
84                      </PurposesSet>
85                  </Attribute>
86
87                  <Attribute>
88                      <AttributeValue>Last Name</AttributeValue>
89                      <PurposesSet>
90                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11
                                /government</Purpose>
91                      </PurposesSet>
92                  </Attribute>
93              </AttributesSet>
94          </DownstreamUsage>
95      </Container>
96      <Signature>
97          QXQgZ3BsLCB3ZSBob2xkIG91ciBjbGllbnRzIHRvIGluZHVzdHJ5LWxlYWRpbmcgb
98          aXZhY3kgc3RhbmRhcmRzLiBncGwgZG9lcyBldmVyeXRoaW5nIHBvc3NpYmxlIHRvI
99          IGNsaWVudCBXZWIgc2l0ZXMgcHJvdGVjdCB0aGUgcHJpdmFjeSBvZiB5b3VyIHBlc
100         Zm9ybWF0aW9uLCBidXQgd2UgYWxzbyByZWx5IG9uIHlvdXIgdmlnaWxhbmNlLiBXZ
101         IHRoZSBpbnRlZ3JpdHkgb2Ygb3VyIHNlYWwgcHJvZ3JhbXMgd2l0aCBvdXIgb25sa
102         dGUgUmVzb2x1dGlvbiBwcm9ncmFtLCB3aGljaCBsZXRzIHVzZXJzIGhvbGQgZ3BsI
103         YWNjb3VudGFibGUuDQoNCmdwbJJzIERpc3B1dGUgUmVzb2x1dGlvbiBGb3JtIGlzI
104         ZSB0b29sIHRoYXQgbGV0cyB5b3UgcmVwb3J0IHZpb2xhdGlvbnMgb2YgcG9zdGVkI
105         c3RhdGVtZW50cyBhbmQgc3BlY2lmaWMgb25saW5lIHByaXZhY3kgaXNzdWVzIHRoY
106         biB0byBncGwgY2xpZW50cyBXZWIgc2l0ZXMuIGdwbCBpbnZlc3RpZ2F0ZXMgYWxsI
107         IGNvbXBsYWludHMgYW5kIG1lZGlhdGVzIHNvbHV0aW9ucyBiZXR3ZWVuIHVzZXJzI
108         c2l0ZXMuDQo=
```

```
109     </Signature>
110     <CertifiersSetForSeals>
111         <CertifierForSeal>
112             <Identity>
113                 <Identifier>Data Protection Agency of Sweden</Identifier>
114                 <Representative>Mr. John Doe</Representative>
115                 <Country>SE</Country>
116                 <Email>contact@dpa.gov.se</Email>
117                 <Phone>+46 1 225 14 77 00</Phone>
118                 <URI>www.dpa.gov.se</URI>
119                 <CertificateURL>http://sweden.gov.se/imprint/
                        policy_seal_certificate.pem</CertificateURL>
120             </Identity>
121             <Signature>
122                 UVhRZ1ozQnNMQ0IzWlNCb2IyeGtJRzkxY2lCamJHbGxiblJ6SUhSdklHbHVaSFZ
123                 V1JwYm1jZ2IyNXNhVzVsSUhCeQ0KYVhaaFkza2djM1JoYm1SaGNtUnpMaUJuY0d
124                 ZG1WeWVYUm9hVzVuSUhCdmMzTnBZbXhsSUhSdklHaGxiSEFnYjNWeQ0KSUdOc2F
125                 Z2MybDBaWE1nY0hKdmRHVmpkQ0IwYUdVZ2NISnBkbUZqZVNCdlppQjViM1Z5SUh
126                 SUdsdQ0KWm05eWJXRjBhVzl1TENCaWRYUWdkMlVnWVd4emJ5QnlaV3g1SUc5dUl
127                 bmFXeGhibU5sTGlCWFpTQmlZVO5ySUhWdw0KSUhSb1pTQnBiblJsWjNKcGRIa2d
128                 TmxZV3dnY0hKdlozSmhiWE1nZDJsMGFDQnZkWElnYjI1c2FXNWxJRVJwYzNCMQ0
129                 MngxZEdsdmJpQndjbTluY21GdExDQjNhR2xqYUNCc1pYUnpJSFZ6WlhKeklHaHZ
130                 TnNhV1Z1ZEhNZw0KWVdOamIzVnVkR0ZpYkdVdURRbO5DbWR3YkpKeklFUnBjM0I
131                 MngxZEdsdmJpQkdiM0p0SUdseklHRnVJRzl1YkdsdQ0KWlNCMGIyOXNJSFJvWVh
132                 YjNVZ2NtVndiM0owSUhacGIyeGhkR2x2Ym5NZ2IyWWdjRzl6ZEdWa0lIQnlhWFp
133                 aGRHVnRaVzUwY3lCaGJtUWdjM0JsWTJsbWFXTWdiMjVzYVc1bElIQnlhWFpoWTN
134                 SUhSb1lYUWdjR1Z5ZEdGcA0KYmlCMGJ5Qm5jR3dnWTJ4cFpXNTBjeUJYWldJZ2M
135                 d2JDQnBiblpsYzNScFoyRjBaWE1nWVd4c0lHVnNhV2RwWW14bA0KSUdOdmJYQnN
136                 NWtJRzFsWkdsaGRHVnpJSE52YkhWMGFXOXVjeUJpWlhSM1pXVnVJSFZ6WlhKekl
137                 ZW0KYzJsMFpYTXVEUW89
138             </Signature>
139         </CertifierForSeal>
140     </CertifiersSetForSeals>
141 </UPL>
```

Listing A.11: UPL example policy on stage 4

```
1  <?xml version="1.0" encoding="UTF-8"?>
2
3  <UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4      xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
5      <Container type="preference">
6          <HigherPurposesSet>
7              <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/government</
                   HigherPurpose>
8          </HigherPurposesSet>
9          <Identity/>
10         <AttributesSet>
11             <Attribute certifiedBy="SE-GOV-CA">
12                 <AttributeValue>First Name</AttributeValue>
13                 <PurposesSet>
```

```
14                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        government</Purpose>
15                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        communicate</Purpose>
16                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        account</Purpose>
17              </PurposesSet>
18          </Attribute>
19
20          <Attribute certifiedBy="SE-GOV-CA">
21              <AttributeValue>Last Name</AttributeValue>
22              <PurposesSet>
23                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        government</Purpose>
24                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        communicate</Purpose>
25                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        account</Purpose>
26              </PurposesSet>
27          </Attribute>
28
29          <Attribute>
30              <AttributeValue>Email</AttributeValue>
31              <PurposesSet>
32                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        communicate</Purpose>
33                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        account</Purpose>
34                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        marketing</Purpose>
35              </PurposesSet>
36              <ObligationsSet>
37                  <Obligation>
38                      <TriggersSet>
39                          <TriggerPersonalDataDeleted>
40                              <MaxDelay>P1D</MaxDelay>
41                          </TriggerPersonalDataDeleted>
42                          <TriggerOnViolation>
43                              <MaxDelay>P5D</MaxDelay>
44                          </TriggerOnViolation>
45                      </TriggersSet>
46                      <ActionNotifyDataSubject/>
47                  </Obligation>
48              </ObligationsSet>
49          </Attribute>
50      </AttributesSet>
51
52
53      <CertifiersSetForAttributes>
54          <CertifierForAttribute certifierId="SE-GOV-CA">
55              <Identifier>Government Offices of Sweden</Identifier>
```

```
56                  <URI>www.ca.gov.se</URI>
57              </CertifierForAttribute>
58          </CertifiersSetForAttributes>
59
60          <DownstreamUsage>
61              <HigherPurposesSet>
62                  <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/government</
                        HigherPurpose>
63              </HigherPurposesSet>
64              <Identity/>
65
66              <AttributesSet>
67                  <Attribute>
68                      <AttributeValue>First Name</AttributeValue>
69                      <PurposesSet>
70                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11
                                /government</Purpose>
71                      </PurposesSet>
72                  </Attribute>
73
74                  <Attribute>
75                      <AttributeValue>Last Name</AttributeValue>
76                      <PurposesSet>
77                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11
                                /government</Purpose>
78                      </PurposesSet>
79                  </Attribute>
80              </AttributesSet>
81          </DownstreamUsage>
82      </Container>
83      <Signature/> <!-- Requesting signed policy -->
84      <CertifiersSetForSeals>
85          <CertifierForSeal>
86              <Identity>
87                  <Identifier>Any Governmental Office of Sweden</Identifier>
88                  <URI>.*\.gov\.se</URI>
89              </Identity>
90              <Signature/>
91          </CertifierForSeal>
92      </CertifiersSetForSeals>
93  </UPL>
```

Listing A.12: UPL example preference on stage 4

```
1   <?xml version="1.0" encoding="UTF-8"?>
2
3   <UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4       xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
5       <Container type="recommendation">
6           <HigherPurposesSet>
7               <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/government</
```

```
            HigherPurpose>
8       </HigherPurposesSet>
9       <Identity>
10              <Identifier>Example Community for Data Privacy</Identifier>
11              <Representative>Mrs. Jane Doe</Representative>
12              <Country>DE</Country>
13              <Email>contact@example-open-privacy-board.org</Email>
14              <URI>www.example-open-privacy-board.org</URI>
15              <HumanReadablePolicyURL>http://example-open-privacy-board.org/
                    privacy-seals/en/</HumanReadablePolicyURL>
16              <CertificateURL>http://example-open-privacy-board.org/imprint/
                    policy_seal_certificate.pem</CertificateURL>
17              <EmblemURL>http://example-open-privacy-board.org/imprint/logo.svg
                    </EmblemURL>
18      </Identity>
19      <AttributesSet>
20          <Attribute certifiedBy="SE-GOV-CA">
21              <AttributeValue>First Name</AttributeValue>
22              <PurposesSet>
23                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        government</Purpose>
24                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        communicate</Purpose>
25                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        account</Purpose>
26              </PurposesSet>
27          </Attribute>
28
29          <Attribute certifiedBy="SE-GOV-CA">
30              <AttributeValue>Last Name</AttributeValue>
31              <PurposesSet>
32                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        government</Purpose>
33                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        communicate</Purpose>
34                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        account</Purpose>
35              </PurposesSet>
36          </Attribute>
37
38          <Attribute>
39              <AttributeValue>Email</AttributeValue>
40              <PurposesSet>
41                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        communicate</Purpose>
42                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        account</Purpose>
43                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        marketing</Purpose>
44              </PurposesSet>
45              <ObligationsSet>
```

```
46                  <Obligation>
47                      <TriggersSet>
48                          <TriggerPersonalDataDeleted>
49                              <MaxDelay>P1D</MaxDelay>
50                          </TriggerPersonalDataDeleted>
51                          <TriggerOnViolation>
52                              <MaxDelay>P5D</MaxDelay>
53                          </TriggerOnViolation>
54                      </TriggersSet>
55                      <ActionNotifyDataSubject/>
56                  </Obligation>
57              </ObligationsSet>
58          </Attribute>
59      </AttributesSet>
60
61
62      <CertifiersSetForAttributes>
63          <CertifierForAttribute certifierId="SE-GOV-CA">
64              <Identifier>Government Offices of Sweden</Identifier>
65              <Representative>Mr. John Gustavsson</Representative>
66              <Email>contact@ca.gov.se</Email>
67              <Phone>+46 8 405 10 00</Phone>
68              <URI>www.ca.gov.se</URI>
69          </CertifierForAttribute>
70      </CertifiersSetForAttributes>
71
72      <DownstreamUsage>
73          <HigherPurposesSet>
74              <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/government</
                    HigherPurpose>
75          </HigherPurposesSet>
76          <Identity/>
77
78          <AttributesSet>
79              <Attribute>
80                  <AttributeValue>First Name</AttributeValue>
81                  <PurposesSet>
82                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11
                            /government</Purpose>
83                  </PurposesSet>
84              </Attribute>
85              <Attribute>
86                  <AttributeValue>Last Name</AttributeValue>
87                  <PurposesSet>
88                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11
                            /government</Purpose>
89                  </PurposesSet>
90              </Attribute>
91          </AttributesSet>
92      </DownstreamUsage>
93  </Container>
```

```
94      <Signature>
95          QXQgZ3BsLCB3ZSBob2xkIG91ciBjbGllbnRzIHRvIGluZHVzdHJ5LWxlYWRpbmc
96          aXZhY3kgc3RhbmRhcmRzLiBncGwgZG9lcyBldmVyeXRoaW5nIHBvc3NpYmxlIHR
97          IGNsaWVudCBXZWIgc2l0ZXMgcHJvdGVjdCB0aGUgcHJpdmFjeSBvZiB5b3VyIHB
98          Zm9ybWF0aW9uLCBidXQgd2UgYWxzbyByZWx5IG9uIHlvdXIgdmlnaWxhbmNlLiB
99          IHRoZSBpbnRlZ3JpdHkgb2Ygb3VyIHNlYWwgcHJvZ3JhbXMgd2l0aCBvdXIgb25
100         dGUgUmVzb2x1dGlvbiBwcm9ncmFtLCB3aGljaCBsZXRzIHVzZXJzIGhvbGQgZ3B
101         YWNjb3VudGFibGUuDQoNCmdwbJJzIERpc3B1dGUgUmVzb2x1dGlvbiBGb3JtIGl
102         ZSB0b29sIHRoYXQgbGV0cyB5b3UgcmVwb3J0IHZpb2xhdGlvbnMgb2YgcG9zdGV
103         c3RhdGVtZW50cyBhbmQgc3BlY2lmaWMgb25saW5lIHByaXZhY3kgaXNzdWVzIHR
104         biB0byBncGwgY2xpZW50cyBXZWIgc2l0ZXMuIGdwbCBpbnZlc3RpZ2F0ZXMgYWx
105         IGNvbXBsYWludHMgYW5kIG1lZGlhdGVzIHNvbHV0aW9ucyBiZXR3ZWVuIHVzZXJ
106         c2l0ZXMuDQo=
107     </Signature>
108     <CertifiersSetForSeals>
109         <CertifierForSeal>
110             <Identity>
111                 <Identifier>Data Protection Agency of Sweden</Identifier>
112                 <Representative>Mr. John Doe</Representative>
113                 <Country>SE</Country>
114                 <Email>contact@dpa.gov.se</Email>
115                 <Phone>+46 1 225 14 77 00</Phone>
116                 <URI>www.dpa.gov.se</URI>
117                 <CertificateURL>http://sweden.gov.se/imprint/
                        policy_seal_certificate.pem</CertificateURL>
118             </Identity>
119             <Signature/>
120         </CertifierForSeal>
121     </CertifiersSetForSeals>
122 </UPL>
```

Listing A.13: UPL example recommendation on stage 4

A.2.5 Modified Files for Test Cases

```
1   <?xml version="1.0" encoding="UTF-8"?>
2
3   <UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4       xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
5       <Container type="policy">
6
7           <HigherPurposesSet semantics="and">
8               <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/arts</HigherPurpose>
9               <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/marketing</
                    HigherPurpose>
10          </HigherPurposesSet>
11          <Identity>
12              <Identifier>Example Video Plattform AB</Identifier>
```

```
13              <Address>SE-40 010 Gothenburg, Sweden</Address>
14              <Country>SE</Country>
15              <Email>contact@example-film3000.se</Email>
16              <Phone>+46 8 405 10 00</Phone>
17              <URI>example-film3000.se</URI>
18              <HumanReadablePolicyURL>http://example-film3000.se/terms/privacy/en/<
                    /HumanReadablePolicyURL>
19              <CertificateURL>http://example-film3000.se/imprint/policy_certificate
                    .pem</CertificateURL>
20          </Identity>
21          <AttributesSet>
22              <Attribute>
23                  <AttributeValue>SessionIdentifier</AttributeValue>
24                  <PurposesSet>
25                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                            login</Purpose>
26                      <Purpose expireTime="P1D">http://www.w3.org/2006/01/P3Pv11/
                            state</Purpose>
27                      <Purpose expireTime="P1D">http://www.w3.org/2006/01/P3Pv1/
                            tailoring</Purpose>
28                  </PurposesSet>
29              </Attribute>
30
31              <Attribute certifiedBy="SE-GOV-CA">
32                  <AttributeValue>Age</AttributeValue>
33                  <PurposesSet>
34                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                            individual-decision</Purpose>
35                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                            tailoring</Purpose>
36                  </PurposesSet>
37              </Attribute>
38
39              <Attribute certifiedBy="SE-GOV-CA">
40                  <AttributeValue>Country</AttributeValue>
41                  <PurposesSet>
42                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                            individual-decision</Purpose>
43                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                            tailoring</Purpose>
44                  </PurposesSet>
45              </Attribute>
46          </AttributesSet>
47
48          <CertifiersSetForAttributes>
49              <CertifierForAttribute certifierId="SE-GOV-CA">
50                  <Identifier>Government Offices of Sweden</Identifier>
51                  <Representative>Mr. John Gustavsson</Representative>
52                  <Email>contact@ca.gov.se</Email>
53                  <Phone>+46 8 405 10 00</Phone>
54                  <URI>www.ca.gov.se</URI>
```

```
55              </CertifierForAttribute>
56          </CertifiersSetForAttributes>
57
58          <DownstreamUsage>
59              <HigherPurposesSet>
60                  <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/marketing</
                        HigherPurpose>
61                  <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/gaming</
                        HigherPurpose>
62              </HigherPurposesSet>
63              <Identity>
64                  <Identifier>DownstreamController.com</Identifier>
65                  <Address>SE-40 010 Gothenburg, Sweden</Address>
66                  <Country>SE</Country>
67                  <Email>contact@datacenter.downstreamcontroller.com</Email>
68                  <URI>datacenter.downstreamcontroller.com</URI>
69                  <HumanReadablePolicyURL>http://datacenter.downstreamcontroller.
                        com/terms/privacy/en/</HumanReadablePolicyURL>
70              </Identity>
71
72              <AttributesSet>
73                  <Attribute certifiedBy="SE-GOV-CA">
74                      <AttributeValue>Country</AttributeValue>
75                      <PurposesSet>
76                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                                individual-decision</Purpose>
77                          <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv1/
                                tailoring</Purpose>
78                      </PurposesSet>
79                  </Attribute>
80              </AttributesSet>
81              <CertifiersSetForAttributes>
82                  <CertifierForAttribute certifierId="SE-GOV-CA">
83                      <Identifier>Government Offices of Sweden</Identifier>
84                      <Representative>Mr. John Gustavsson</Representative>
85                      <Email>contact@ca.gov.se</Email>
86                      <Phone>+46 8 405 10 00</Phone>
87                      <URI>www.ca.gov.se</URI>
88                  </CertifierForAttribute>
89              </CertifiersSetForAttributes>
90          </DownstreamUsage>
91
92      </Container>
93      <Signature>
94          QXQgZ3BsLCB3ZSBob2xkIG91ciBjbGllbnRzIHRvIGluZHVzdHJ5LWxlYWRp
95          aXZhY3kgc3RhbmRhcmRzLiBncGwgZG9lcyBldmVyeXRoaW5nIHBvc3NpYmxl
96          IGNsaWVudCBXZWIgc2l0ZXMgcHJvdGVjdCB0aGUgcHJpdmFjeSBvZiB5b3Vy
97          Zm9ybWF0aW9uLCBidXQgd2UgYWxzbyByZWx5IG9uIHlvdXIgdmlnaWxhbmNl
98          IHRoZSBpbnRlZ3JpdHkgb2Ygb3VyIHNlYWwgcHJvZ3JhbXMgd2l0aCBvdXIg
99          dGUgUmVzb2x1dGlvbiBwcm9ncmFtLCB3aGljfCBsZXRzIHVzZXJzIGhvbGQg
100         YWNjb3VudGFibGUuDQoNCmdwbJJzIERpc3B1dGUgUmVzb2x1dGlvbiBGb3Jt
```

```
        ZSB0b29sIHRoYXQgbGV0cyB5b3UgcmVwb3J0IHZpb2xhdGlvbnMgb2YgcG9z
        c3RhdGVtZW50cyBhbmQgc3BlY2lmaWMgb25saW5lIHByaXZhY3kgaXNzdWVz
        biB0byBncGwgY2xpZW50cyBXZWIgc2l0ZXMuIGdwbCBpbnZlc3RpZ2F0ZXMg
        IGNvbXBsYWludHMgYW5kIG1lZGlhdGVzIHNvbHV0aW9ucyBiZXR3ZWVuIHVz
        c2l0ZXMuDQo=
    </Signature>
</UPL>
```

Listing A.14: Modified UPL policy based on the example policy on stage 3

```
<?xml version="1.0" encoding="UTF-8"?>

<UPL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="upl_shema_v1.xsd">
    <Container type="recommendation">
        <HigherPurposesSet>
            <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/government</
                HigherPurpose>
        </HigherPurposesSet>
        <Identity>
                <Identifier>Example Community for Data Privacy</Identifier>
                <Representative>Mrs. Jane Doe</Representative>
                <Country>DE</Country>
                <Email>contact@example-open-privacy-board.org</Email>
                <URI>www.example-open-privacy-board.org</URI>
                <HumanReadablePolicyURL>http://example-open-privacy-board.org/
                    privacy-seals/en/</HumanReadablePolicyURL>
                <CertificateURL>http://example-open-privacy-board.org/imprint/
                    policy_seal_certificate.pem</CertificateURL>
                <EmblemURL>http://example-open-privacy-board.org/imprint/logo.svg
                    </EmblemURL>
        </Identity>
        <AttributesSet>
            <Attribute certifiedBy="SE-GOV-CA">
                <AttributeValue>First Name</AttributeValue>
                <PurposesSet>
                    <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        government</Purpose>
                    <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        communicate</Purpose>
                    <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        account</Purpose>
                </PurposesSet>
            </Attribute>

            <Attribute certifiedBy="SE-GOV-CA">
                <AttributeValue>Last Name</AttributeValue>
                <PurposesSet>
                    <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        government</Purpose>
                    <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
```

```
                    communicate</Purpose>
34                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        account</Purpose>
35              </PurposesSet>
36          </Attribute>
37
38          <Attribute certifiedBy="SE-GOV-CA">
39              <AttributeValue>Email</AttributeValue>
40              <PurposesSet>
41                  <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11/
                        communicate</Purpose>
42                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        account</Purpose>
43                  <Purpose expireTime="P1M">http://www.w3.org/2006/01/P3Pv11/
                        marketing</Purpose>
44              </PurposesSet>
45              <ObligationsSet>
46                  <Obligation>
47                      <TriggersSet>
48                          <TriggerPersonalDataDeleted>
49                              <MaxDelay>P0DT1H</MaxDelay>
50                          </TriggerPersonalDataDeleted>
51                      </TriggersSet>
52                      <ActionNotifyDataSubject/>
53                  </Obligation>
54              </ObligationsSet>
55          </Attribute>
56      </AttributesSet>
57
58
59      <CertifiersSetForAttributes>
60          <CertifierForAttribute certifierId="SE-GOV-CA">
61              <Identifier>Government Offices of Sweden</Identifier>
62              <Representative>Mr. John Gustavsson</Representative>
63              <Email>contact@ca.gov.se</Email>
64              <Phone>+46 8 405 10 00</Phone>
65              <URI>www.ca.gov.se</URI>
66          </CertifierForAttribute>
67      </CertifiersSetForAttributes>
68
69      <DownstreamUsage>
70          <HigherPurposesSet>
71              <HigherPurpose>http://www.w3.org/2006/01/P3Pv11/government</
                    HigherPurpose>
72          </HigherPurposesSet>
73          <Identity/>
74
75          <AttributesSet>
76              <Attribute>
77                  <AttributeValue>First Name</AttributeValue>
78                  <PurposesSet>
```

```
79                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11
                            /government</Purpose>
80                  </PurposesSet>
81              </Attribute>
82              <Attribute>
83                  <AttributeValue>Last Name</AttributeValue>
84                  <PurposesSet>
85                      <Purpose expireTime="P1Y">http://www.w3.org/2006/01/P3Pv11
                            /government</Purpose>
86                  </PurposesSet>
87              </Attribute>
88          </AttributesSet>
89      </DownstreamUsage>
90  </Container>
91  <Signature>
92      QXQgZ3BsLCB3ZSBob2xkIG91ciBjbGllbnRzIHRvIGluZHVzdHJ5LWxlYWRpbmc
93      aXZhY3kgc3RhbmRhcmRzLiBncGwgZG9lcyBldmVyeXRoaW5nIHBvc3NpYmxlIHR
94      IGNsaWVudCBXZWIgc2l0ZXMgcHJvdGVjdCB0aGUgcHJpdmFjeSBvZiB5b3VyIHB
95      Zm9ybWF0aW9uLCBidXQgd2UgYWxzbyByZWx5IG9uIHlvdXIgdmlnaWxhbmNlLiB
96      IHRoZSBpbnRlZ3JpdHkgb2Ygb3VyIHNlYWwgcHJvZ3JhbXMgd2l0aCBvdXIgb25
97      dGUgUmVzb2x1dGlvbiBwcm9ncmFtLCB3aGljaCBsZXRzIHVzZXJzIGhvbGQgZ3B
98      YWNjb3VudGFibGUuDQoNCmdwbJJzIERpc3B1dGUgUmVzb2x1dGlvbiBGb3JtIGl
99      ZSB0b29sIHRoYXQgbGV0cyB5b3UgcmVwb3J0IHZpb2xhdGlvbnMgb2YgcG9zdGV
100     c3RhdGVtZW50cyBhbmQgc3BlY2lmaWMgb25saW5lIHByaXZhY3kgaXNzdWVzIHR
101     biB0byBncGwgY2xpZW50cyBXZWIgc2l0ZXMuIGdwbCBpbnZlc3RpZ2F0ZXMgYWx
102     IGNvbXBsYWludHMgYW5kIG1lZGlhdGVzIHNvbHV0aW9ucyBiZXR3ZWVuIHVzZXJ
103     c2l0ZXMuDQo=
104 </Signature>
105 <CertifiersSetForSeals>
106     <CertifierForSeal>
107         <Identity>
108             <Identifier>Data Protection Agency of Sweden</Identifier>
109             <Representative>Mr. John Doe</Representative>
110             <Country>SE</Country>
111             <Email>contact@dpa.gov.se</Email>
112             <Phone>+46 1 225 14 77 00</Phone>
113             <URI>www.dpa.gov.se</URI>
114             <CertificateURL>http://sweden.gov.se/imprint/
                    policy_seal_certificate.pem</CertificateURL>
115         </Identity>
116         <Signature/>
117     </CertifierForSeal>
118 </CertifiersSetForSeals>
119 </UPL>
```

Listing A.15: Modified UPL recommendation based on the example recommendation on stage 4