Liberty architecture framework for supporting Privacy Preference Expression Languages (PPELs)

Version 1.0

November 12, 2003

Editors and Contributors:

Robert Aarts, Nokia
Margareta Björksten, Nokia
Stephen Deadman, Vodafone
Bill Duserick, Fidelity Investments
Niina Karhuluoma, Nokia
Andrew Lindsay-Stewart, Vodafone
John Linn, RSA Security
Paul Madsen, Entrust
Paule Sibieta, France Telecom
Timo Skyttä, Nokia

Abstract:

The Liberty ID-WSF framework enables participants to associate a privacy policy, encoded in any privacy preference language, with a message using SOAP headers.

This document gives a high-level example of how privacy preferences can be handled using a multi-leveled policy approach in the communication between a Service Provider and Web Services Provider. In the multi-leveled policy framework, a limited, hierarchical set of privacy policies is used to describe the privacy practices of a Service Provider, and the privacy preferences of a Principal. When requesting attributes, the Service Provider or Web Services Consumer indicates its context specific privacy policy. The Web Services Provider acting on the Principal's behalf, then compares the requestor's privacy policy against the Principal's privacy policy preference for the attributes in question and decides whether to release the attributes. In case of a mismatch, the transaction is cancelled or the interaction service invoked.

This document does not intend to describe a detailed solution, only the principles of a multi-leveled policy approach. The privacy preference language and the actual attribute-sharing privacy policies for use within a 'circle of trust' should be designed with participating service providers, industry norms, and regulatory requirements in mind.

Table of contents

1. Overview

The objective of this paper is to provide an example of how to manage privacy preferences within Liberty Alliance's ID-WSF framework. It describes a candidate for the content of the "Usage Directives" message header, i.e. an example of a Privacy Preference Expression Language to handle attribute requests.

Like trust and security, privacy has become an increasingly important issue in web-based service environments. Consequently, privacy related issues should be taken into account with the design and implementation of new services. Privacy policies provide information about a provider's information handling practices. In order to foster end user trust, and increase the uptake of new services, it is important to ensure that user information is not disclosed without the user's permission. This requires methods to collect information about a user's privacy preferences and compare them against a service provider's privacy practices. A match of preferences and practices results in appropriate disclosure of the Principal's data; similarly, a failure to match them may prompt a response from the user as to how to proceed with the Service Provider (SP).

This document provides an example of a simplified way of handling privacy preferences, without going into specific implementation details. It does not, however, take a view as to how Service Providers must or should act with implementation trade-offs. This means, in practice, striking the right balance between end-user interaction and back-end server communication by, for example, limiting the policy permutations.

2. Liberty Privacy Management Framework

As the membership of Liberty Alliance spans the globe, Liberty employs a generic architecture for rights management based on the concept of a "Usage Directives Container". Employing the concept of a usage directives container helps a service provider (SP) to implement its privacy policy, respect the user's or Principal's privacy preferences and comply with certain aspects of applicable privacy laws.

In the ID-WSF framework, participants may indicate the privacy policy associated with a message by adding one or more <UsageDirective> header blocks to the SOAP header.[1] Essentially, the usage directives header contains elements that describe the privacy policy associated with the request. The usage directive in a request from a client can be understood as "intended usage" (SP's privacy policy). The usage directive in a response can be understood as a directive on how data is to be used (User's privacy preference/policy).

Liberty also provides the necessary protocols that allow an SP to communicate with a Principal to gain appropriate direction to use their data. A Web Services Provider (WSP) will strive to strike the right balance between interaction with the Principal at the user interface (e.g. browser) and leaving the negotiation to back-end servers, aiming for the optimum end-user experience.

3. Multi-leveled Policy Approach

The goal of the Liberty privacy policy framework is to enable the exchange of attribute information under end-user control and knowledge of the requestor's privacy policy. Both the Principal and the SP have their

[1] More information can be found in [LibertySOAPBinding] Hodges, Jeff, Aarts, Robert, eds. " Liberty ID-WSF SOAP Binding Specification ," Version 1.0, Liberty Alliance Project.
http://www.projectliberty.org/specs

own interpretation of just what is an appropriate use, i.e. they have their own policies. Consequently, to both ensure that the Principal's privacy preferences are met and that the SP can retrieve the attributes it desires, an 'intersection' must be found between these two policies. Whether the determination of this intersection is performed by the SP or the Principal (which in practice is likely to be the Web Services Provider (WSP) on behalf of the Principal), the SP must indicate its intended usages for the attributes and the Principal must indicate their allowed usages.

To facilitate this 'conversation', the SP and Principal must agree on the language they will use to communicate their policies to the other. The most flexible solution would be to simply define a syntax by which both entities can express the details of their policies to the other. For instance, the SP could indicate to the Principal all intended purposes for which the data will be used, how long it will be retained, etc. and the Principal could make similar statements to the SP. Such a system would be very flexible, allowing the SP and Principal to precisely specify the different aspects of their respective privacy policies. The price for this flexibility is that the task of determining an intersection of these two policies in an automated fashion (as would be necessary if a real-time decision were required on attribute release) is non-trivial. Additionally, most Principals would likely be unwilling to define their preferences to this level of detail.

These issues can be addressed through the introduction of a small number of 'standardized' privacy policies to which both SPs and Principals can refer. Calculation of a policy intersection becomes as simple as determining if both the SP and Principal indicate at least one of the standardized policies as acceptable and a Principal need only specify which of the standardized policies best approximate their preferences. This is the model Liberty advocates in this paper.

Consider the following example:

> A Principal would like to perform a transaction with the SP. Both the SP and the WSP are aware of a standard set of leveled or hierarchical privacy policies, where each policy within the set indicates a statement of privacy practices, ranging from conservative (strict), to broad (casual).
>
> When the Principal wants to perform a transaction with the SP, the SP will request attributes, such as name, address, and billing information, from the WSP holding the Principal’s attributes. Accompanying the request is one of the standard privacy policies - a statement of how the requested information will be used once in the hands of the SP. Previously, the Principal, upon entering an agreement with the WSP, declares a privacy preference for the release of his attributes by selecting one of the standard privacy policies.
>
> When the request for personal data from the SP is made, the request is accompanied by the reference to the privacy policy of the SP. If the privacy level of the SP matches or exceeds (i.e. is as strict or stricter than) the Principal’s, the requested data is disclosed. Otherwise, the Principal may receive a warning notifying him/her of the conflict. The transaction could then be cancelled, or the Principal could override the warning and allow the data to be released, completing the transaction.

4. Privacy policies

In the multi-leveled policy approach, the WSP and SP use a limited set of privacy policies. Five example policies, named *privacy strict, privacy cautious, privacy moderate, privacy flexible,* and *privacy casual* are described below. Each privacy policy is described using the following W3C P3P elements[2]:

- Purpose - describes the purposes of data collection or uses of data.
- Recipient –describes all intended recipients of the collected data.
- Retention -indicates the retention policy that applies to the data
- Access –indicates whether the SP provides access to the collected data
- Disputes – indicates dispute resolution procedures that may be followed for disputes about an SP's privacy practices
- Remedies -specifies the possible remedies in case a policy breach occurs

In the multi-leveled policy approach, the allowed element values at each policy level are set. There is an implied strictness to the element values, and they are slotted accordingly in the five privacy policies. The element values in the *'privacy strict'* policy are very restrictive, whereas the values of the *'privacy casual'* are very permissive.

There may be multiple values at each privacy level. As the privacy policy becomes less strict, more values are generally added to comprise the element definition. For example, this approach allows the SP to use data for more than one purpose and share it with more than one recipient at each privacy policy level.

The five policies are described in the following sections. Each description provides a high-level abstract of the policy (from the Principal's point of view) and lists element values that are allowed at each policy level.[3]

[2] For a detailed description of the P3P elements and associated values, please see the P3P specification: http://www.w3.org/TR/P3P/.

[3] It should be noted that the described policies are only examples, and that the used policies should be available also in human readable format in actual implementations.

4.1. Privacy Strict

Description: use my data for this activity only. Do not share my data with other entities. You may build statistical records based on my browsing habits as long as they do not contain identifying information. I have full access to my data, which you keep only as long as the identified purpose or the law requires. In case of disputes, I have access to your customer service or an independent organization.

POLICY NAME	ELEMENT	VALUE
1. *Privacy Strict*		
	PURPOSE	current, admin, develop, pseudo-analysis
	ACCESS	all
	RECIPIENT	ours
	RETENTION	stated-purpose, legal-requirement
	DISPUTES[@ resolution-type]	service, independent, law
	REMEDIES	correct, law

4.2. Privacy Cautious

Description: You may create an individually identifying profile of me based on the information I provide and my browsing habits. You may use my data to tailor services I use, and to promote products and services through means other than voice telephone. Only you and your business partners with equable privacy practices may use my data. You can keep my data as long as the identified purpose or the law requires. I will have access to my identified online and physical contact information. In case of disputes, I have access to your customer service or an independent organization.

POLICY NAME	ELEMENT	VALUE
2. *Privacy Cautious*		
	PURPOSE	current, admin, develop, pseudo-analysis, pseudo-decision, tailoring, individual-decision, individual-analysis, contact
	ACCESS	contact-and-other
	RECIPIENT	ours
	RETENTION	stated-purpose, legal-requirement
	DISPUTES[@ resolution-type]	service, independent, law
	REMEDIES	correct, law

4.3. Privacy Moderate

Description: You may create an individually identifying profile of me based on the information I provide and my browsing habits. You may use my data to tailor services I use, and to promote products and services. Only you and your business partners with equable privacy practices may use my data, and contact me for the promotion of your products or services. You can keep my data as long as the identified purpose or the law requires. I will have access to my identified online and physical contact information. In case of disputes, I have access to your customer service or an independent organization.

POLICY NAME	ELEMENT	VALUE
3. *Privacy Moderate*		
	PURPOSE	current, admin, develop, pseudo-analysis, pseudo-decision, tailoring, individual-decision, individual-analysis, contact, telemarketing
	ACCESS	contact-and-other
	RECIPIENT	ours
	RETENTION	stated-purpose, legal-requirement
	DISPUTES[@ resolution-type]	service, independent, law
	REMEDIES	correct, law

4.4. Privacy Flexible

Description: You may create an individually identifying profile of me based on information I provide, and my browsing habits. You may use my data to tailor services I use, and to promote your products and services. You may share my data with entities whose usage practices may be different from yours. You and the other entities may keep my data as long as your business practices require or the law allows. I will have access to at least my contact information.

POLICY NAME	ELEMENT	VALUE
4. *Privacy Flexible*		
	PURPOSE	current, admin, develop, pseudo-analysis, pseudo-decision, tailoring, individual-decision, individual-analysis, contact, telemarketing
	ACCESS	ident-contact, other-ident
	RECIPIENT	ours, same, other recipient, delivery
	RETENTION	business-practices, legal-requirement
	DISPUTES[@ resolution-type]	law
	REMEDIES	law

4.5. Privacy Casual

Description: You may create an identifying profile of me and use my data for the purposes specified in the human readable privacy policy. You may share my information with other unrelated entities whose usage practices are not known. You and the other entities can keep my information indefinitely or as long as the law allows. I may not have access to my data or be able to correct it.

POLICY NAME	ELEMENT	VALUE
5. ***Privacy Casual***		
	PURPOSE	current, admin, develop, pseudo-analysis, pseudo-decision, tailoring, individual-decision, individual-analysis, contact, telemarketing, other-purpose
	ACCESS	none
	RECIPIENT	ours, same, other-recipient, delivery, unrelated
	RETENTION	Indefinitely
	DISPUTES[@ resolution-type]	law
	REMEDIES	law

5. Attribute request with privacy policy

When requesting attributes, an SP/Web Service Consumer(WSC) should indicate its privacy policy. When a request is received, the WSP compares the SP's privacy policy against the Principal's privacy policy for the attributes in question. The following sections describe the general processing rules, and the messaging sequence related to three attribute requests; one where the SPs/WSC's privacy policy equals the Principal's policy requirements, and two where the SP's privacy policy differs from the one set by the Principal.

5.1. Processing rules

When receiving an attribute request, and comparing the requestor's (SP/WSC) privacy policy against the Principal's policy for the attributes in question, the WSP must check the following rules when deciding whether to release the requested attributes.

- The WSP is allowed to disclose attributes only when the UsagePolicy chosen by the Principal is equal to or LESS strict than the PrivacyPolicy that the SP/WSC used in request.
- In case the Usage Policy is LESS strict, the WSP MUST disclose attributes using the more STRICT Usage Policy equal to the Privacy Policy used in the SP/WSC request.
- The WSP can NOT change the Policy that relates to an attribute to a less strict policy without asking for the Principal's consent.

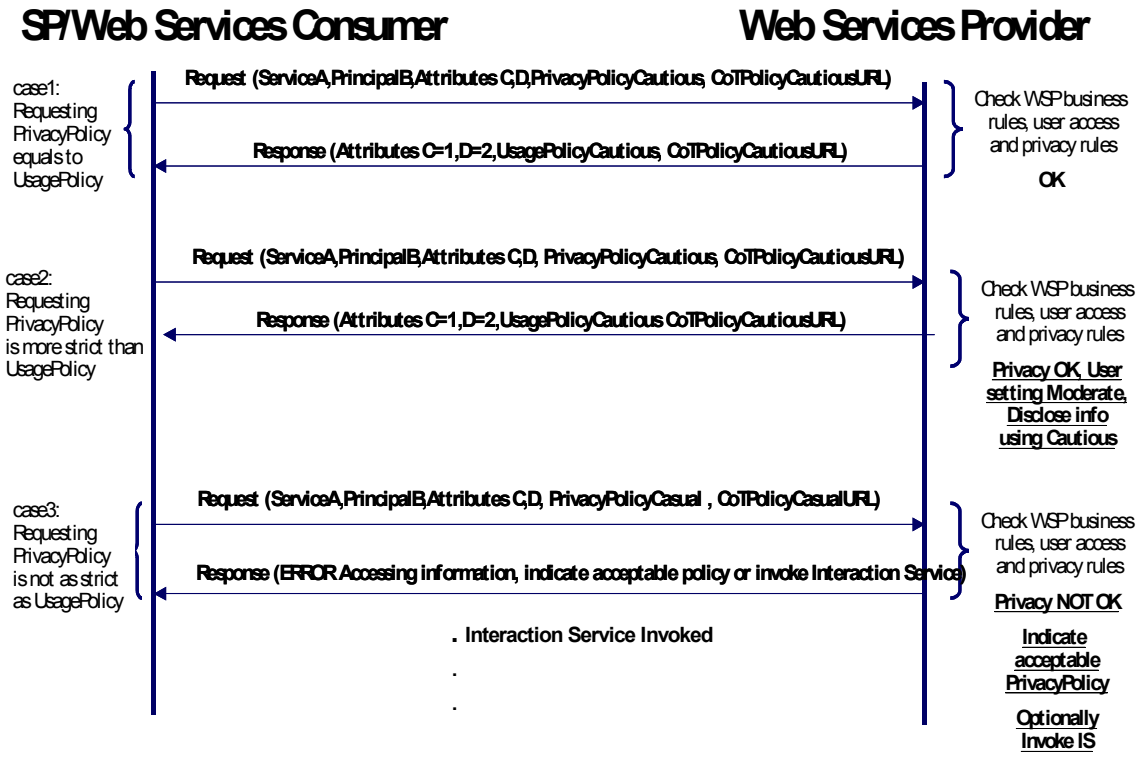
5.2. Example assumptions

Three alternative messaging sequences related to an attribute request are depicted in *Picture 1*. The following assumptions apply for the messaging sequences in question:

- The Principal has contacted the SP/Web Services Consumer (WSC) and has requested service.
- The WSP has previously collected Principal consent, access and privacy policies for the attributes in question, and represents the Principal in this transaction.
- The Circle of Trust (CoT) has a web site of its own, or uses an external "Policy Broker" web site, where the five privacy policies are available online. Thus the message carries either *CoTPrivacyPolicyXURL* or *PolicyBrokerPrivacyPolicyXURL*. The example uses the former.
- The SP/WSC sets the Privacy Policy and the Principal sets the Usage Policy.
- PrivacyPolicy_X = UsagePolicy_X. The naming difference is used to indicate WHO has decided to apply WHAT policy for WHAT attributes.

5.3. Messaging sequence

The messaging sequences in the picture depict three different attribute request scenarios; one where the requesting SP's policy is equal to the Principal's, one where the requesting SP's policy is stricter than the Principal's and one where the requesting SP's policy is less strict than the Principal's.



Picture 1

Case1 - Requesting policy equals usage policy:

- SP/WSC requests name and address with PrivacyPolicyCautious.
- Principal setting for UsagePolicy is UsagePolicyCautious.
- WSP (Principal) discloses name and address using UsagePolicyCautious.

Case2 - Requesting policy is stricter than the usage policy:

- SP/WSC requests name and address with PrivacyPolicyCautious.
- Principal setting for UsagePolicy is UsagePolicyModerate.
- WSP (Principal) MUST disclose name and address ONLY using UsagePolicyCautious.

Case 3 - Requesting policy is not as strict as the usage policy:

- SP/WSC requests name and address with PrivacyPolicyCausal.
- User setting for UsagePolicy is UsagePolicyCautious.
- WSP discloses only the acceptable policy or invokes the interaction service.

6. Regulatory Environment

This document describes the principles of a multi-leveled policy approach, using a limited set of privacy policies. It should be noted that the used policies are only examples. Actual privacy policies need to be designed with participating SPs, industry norms, and regulatory requirements in mind. In all cases, conformity with legal requirements will depend on the actual implementation of services and products. It should be noted that the communication of policies between the WSP and SP proposed in the framework cannot ensure legal conformity by itself. Moreover, legal requirements can be implemented in various ways, and developers and SPs should consult their legal counsel (and possibly their national privacy or data protection authorities) to ensure that the used policies are in line with the legal requirements of the jurisdiction in question.

The fundamental principle underlying the policies is that the Principal/WSP and the SP enter into a form of automated negotiation and that this is consensual by nature. However, there may be certain matters that are not legally negotiable (such as a Principal's right of access to, or correction of, their data, or rights to judicial redress and remedies). It should also be noted that not all interactions would necessarily require consent as the justification for collecting and using personal data; there may well be other legitimate legal grounds. Also, developers should consider whether (and if so, how) Principals are legally entitled to withdraw consent unilaterally and whether SPs are permitted to refuse access to services on the grounds that the Principal withholds consent. This may be particularly relevant to SPs in the public sector or subject to certain universal service obligations.

The general rule in many jurisdictions is that personal data shall only be collected and processed in conjunction with a specified and legitimate purpose. Issues such as the types of recipients to whom data may be disclosed or the period for which data may be retained may be regulated by reference to each of these specified purposes. For example, data may be retained for as long as it is needed to fulfill a particular purpose, but an SP may not be permitted to apply a standard retention period to all data and for all purposes, as different purposes are likely to necessitate different periods of retention. This may affect the structure of the policies used. Additionally, where an SP may wish to disclose or transfer data to a recipient in another country, there may be further legal requirements in relation to this cross border aspect. It may be possible for this to be based upon consent, provided that the transfer being contemplated is clear, but this ground may not be available if the SP wants to be able to make as yet undetermined transfers.

Developers should bring special care when dealing with data considered as sensitive or requiring special attention (e.g. information regarding a Principal's health or race, religious or political views, communications or location information), the collection and use of which may require consent to be given in a particular way (e.g. explicit consent, which may necessitate consent being given in writing and thereby limiting the use of these policies in such cases), or which may be subject to particular restrictions on the purposes and manner in which it can be used, regardless of whether or not the Principal provides consent.

Developers and SPs should also bring special attention when designing user and human readable interfaces. In particular, in many cases, the use of these privacy policies will not displace the legal requirement to provide human readable information about information handling practices and they should therefore be viewed as a supplemental tool.

For more general information on the legal framework in a number of jurisdictions and regions, please see the Liberty Alliance's documents: Privacy and Security Best Practices[4] and the ID-WSF Security and Privacy overview[5].

[4] [LibertyPrivSecBestPractices] Varney, Christine, ed. "Liberty Privacy and Security Best Practices", Version 2.0, Liberty Alliance Project. http://www.projectliberty.org/specs

[5] [LibertyWSFSecPrivOverview] Landau, S, Thompson, P, eds. "Liberty ID-WSF Security & Privacy Overview", Version 1.0, Liberty Alliance Project. http://www.projectliberty.org/specs

7. Conclusion

The Liberty ID-WSF framework enables participants to associate a privacy policy with a message by using the SOAP headers. The framework allows for the use of policies encoded in any privacy preference language. This document has described a high-level example of how privacy preferences can be handled within Liberty's ID-WSF framework using a multi-leveled policy approach, and illustrates how the P3P vocabulary may be deployed in a hierarchical manner within a hypothetical 'circle of trust'. This document does not intend to describe a final solution. The choice of privacy preference language and the actual attribute-sharing privacy policies for use within a 'circle of trust' should be designed with participating service providers, industry norms, and regulatory requirements in mind.