# Liberty ID-SIS Employee Profile Service Implementation Guidelines

Version: 1.1

**Editors:**
Sampo Kellomäki, Symlabs, Inc.
Rob Lockhart, IEEE-ISTO

**Contributors:**
Carolina Canales-Valenzuela, Ericsson
Ariel Gordon, France Télécom
Vincent Guesdon, France Télécom
Jukka Kainulainen, Nokia Corporation
Lena Kannappan, France Télécom
John Kemp, IEEE-ISTO
Thomas Wason, IEEE-ISTO

**Abstract:**

The Liberty ID-SIS Employee Profile (ID-SIS-EP) is a web service. It offers profile information regarding employee. ID-SIS-EP provides basic employee information ID-SIS-EP is an instance of data-oriented identity web service. ID-SIS-EP is characterized by ability to query and update attribute data and incorporates from other specifications mechanisms for access control and conveying data validation information and usage directives.

**Filename:** liberty-idsis-ep–guidelines-v1.1.pdf

## Notice

This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact the Liberty Alliance to determine whether an appropriate license for such use is available.

Implementation of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. **This Specification is provided "AS IS", and no participant in the Liberty Alliance makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose.** Implementors of this Specification are advised to review the Liberty Alliance Project's website (http://www.projectliberty.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance Management Board.

Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane
Piscataway, NJ 08855-1331, USA
info@projectliberty.org

# Contents

# 1. Introduction

The Employee Profile (EP, previously referred to as the Employee Identity Profile, EIP) is a Liberty identity service that supports identity information regarding the Principal when in her job function.

The present document provides rationale and guidance for implementers of Employee Profile. A companion document Liberty Employee Profile Service Specification, [LibertyIDEP], normatively describes the ID-SIS-EP. In case of disagreement between present document and [LibertyIDEP] the latter is prescriptive.

## 1.1. Document Audience

This document is intended for application developers and implementers. The reader is presumed to be familiar with XML, SAML and SOAP. The reader should be familiar with the Liberty ID-FF Architectural Overview ([LibertyIDFFOverview]) and the Liberty D-WSF Web Services Framework Overview ([LibertyIDWSFOverview]). The [LibertyIDPPGuide] contains information of general application to Profiles.

## 1.2. Architectural Context of the ID-SIS-EP

The ID-SIS-EP service is an instance of a data-oriented identity service. The data-oriented aspect means that the service aims to provide attribute data structured in containers. This same approach is used by some other Liberty services, such as ID-SIS-PP, and they all share the methods and general framework as described in [LibertyDST].

The identity services in general require that Principal be directly or abstractly present in all transactions involving his identity or data, e.g., data that the Principal has gathered about other people. Thus the services that consult the ID-SIS-EP service use Liberty architectural framework to prove that they are acting on behalf of the Principal or that the Principal has somehow consented to sharing the data, for example, by means of a standing order or subscription. The identity services are further described in [LibertyIDWSFOverview].

### 1.2.1. ID-SIS-EP as an Interface

Although the essence of the ID-SIS-EP service is data expressed as attributes, it should be understood that the technical implementation is actually a process which handles data requests and computes responses. The fact that the services are dynamic allows many features such as flexible permission enforcement and supplying different data for same attributes to different service providers. Thus an implementation may choose to hold some of the attributes in a database while obtaining others on the fly or computing them. Please refer to [LibertyIDPPGuide] for a discussion on the nature of the interface.

### 1.2.2. Participants and Compliance Testing

See the discussion of this topic in [LibertyIDPPGuide].

## 1.3. XML Document Instantiation

See [LibertyIDPPGuide] for a discussion of this topic.

## 1.4. Extension Mechanisms

ID-SIS-EP is designed to be extensible in six ways which are discussed in [LibertyIDPPGuide]:

1. by adding more enumerator URIs to existing attributes,

2. by adding new attributes to existing containers,

3. by creating new containers,

4. by creating new discovery option keywords (URIs),
5. by extending the supported subset of XPATH expressions, or
6. by schema extension.

# 2. Overview of the Employee Profile Data Model

## 2.1. EP

**Table 1. Structure of the EP Data Model**

| Attribute | Example | Synopsis |
|---|---|---|
| `EmployeeID` | IT87T121 | Employee ID internal to enterprise (e.g., payroll number) |
| `AltEmployeeID` | IT87T121 | Alternate Employee ID internal to enterprise |
| `DateOfHire` | 2002-04-29 | Date of hiring |
| `JobStartDate` | 2002-05-30 | Job effective date |
| `EmployeeStatus` | `urn:liberty:id-sis-ep:employeeStatus:trial` | Status of the employee |
| `EmployeeType` | `urn:liberty:id-sis-ep:employeeType:contractor` | Type of the employee |
| `InternalJobTitle` | COO Special Operations | Job title that reflects actual function of the Principal |
| `OU` | Sales | Organizational unit, e.g., department where employee works |
| `CorpCommonName` | (container) | Usual every day name of the company or employer |
| `CorpLegalIdentity` | (container) | Official legal identification of the Principal |
| `ManagerEmployeeID` | IT87T121 | Internal Employee ID if the Principal's Manager |
| `SubalternateEmployeeID` | IT87T121 | Internal Employee ID if the Principal is a Manager |

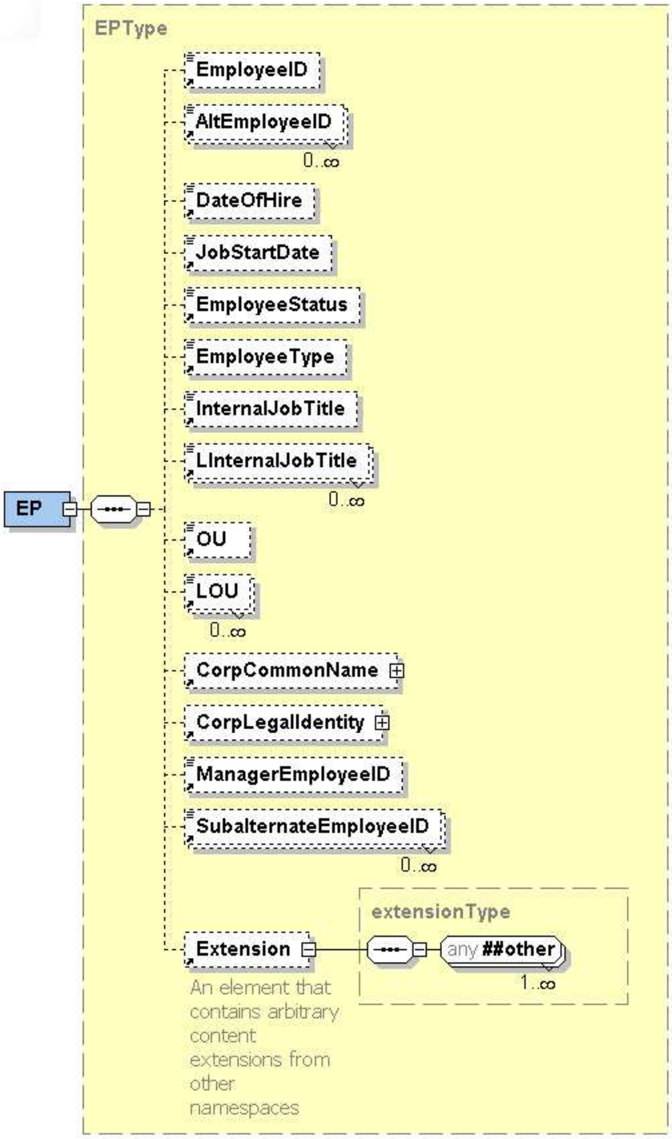

**Figure 1. Structure of the EP Data Model .**

## 2.2. CorpCommonName

**Table 2. CorpCommonName**

| Attribute | Example | Synopsis |
|---|---|---|
| `CN` | Mercnet Corp. | Organization’s every day name in latin writing system |
| `AltCN` | Mercnet Enterprises | Additional every day names in latin writing system |

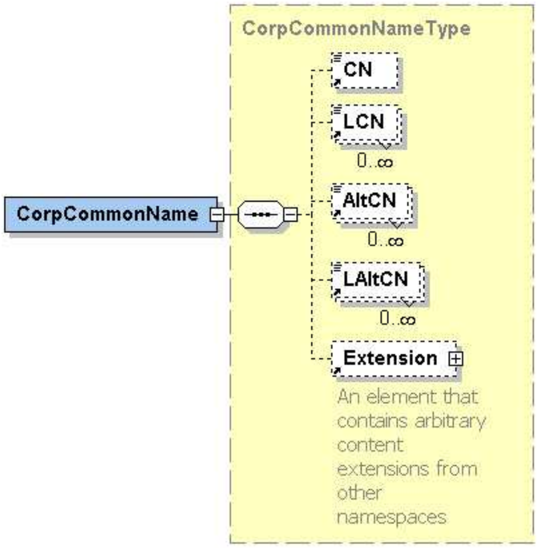
CorpCommonNameType
CN
LCN
0..∞
CorpCommonName
AltCN
0..∞
LAltCN
0..∞
Extension
An element that contains arbitrary content extensions from other namespaces

**Figure 2. Structure of CorpCommonName.**

## 2.3. CorpLegalIdentity

**Table 3. CorpLegalIdentity**

| **Attribute** | **Example** | **Synopsis** |
|---|---|---|
| `LegalName` | Mercnet - Com_io e Servi_ na Internet Lda. | Full legal name of the company or employer |
| `VAT` | (container) | Fiscal identification number |
| `AltID` | (container) | Other identification number(s) |

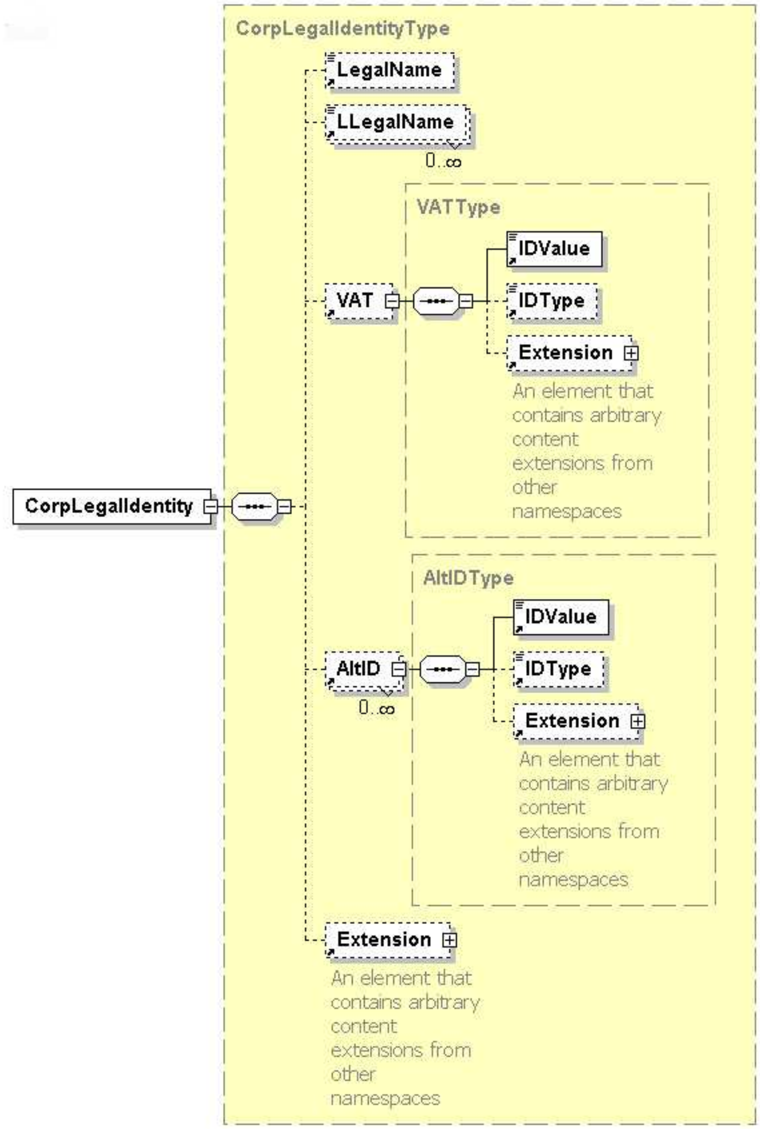
CorpLegalIdentityType
LegalName
LLegalName
0..∞
VATType
IDValue
VAT
IDType
Extension
An element that contains arbitrary content extensions from other namespaces
CorpLegalIdentity
AltIDType
IDValue
AltID
IDType
0..∞
Extension
An element that contains arbitrary content extensions from other namespaces
Extension
An element that contains arbitrary content extensions from other namespaces

**Figure 3. Structure of CorpLegalIdentity.**

## 2.3.1. VAT

**Table 4. VAT**

| **Attribute** | **Example** | **Synopsis** |
|---|---|---|
| `IDValue` | 502677123 | Identification number value |
| `IDType` | `urn:liberty:id-sis-pp:IDType:itcif` | Type of identification number stored in VAT or AltID attribute |

## 2.3.2. AltID

**Table 5. AltID**

| **Attribute** | **Example** | **Synopsis** |
|---|---|---|
| `IDValue` | 502677123 | Identification number value |
| `IDType` | `urn:liberty:id-sis-pp:IDType:itcif` | Type of identification number stored in VAT or AltID attribute |

# 3. Security Considerations

For the most part, ID-SIS-EP relies on standard privacy and security mechanisms provided by ID-FF and ID-WSF. Of these, the following are considered to be of paramount importance.

1. Ability to have several ID-SIS-EP service instances per principal so that a principal can have effective control about who holds which data about her and so that mere existence of some piece of data in one place does not imply that other pieces of data need to be kept in the same place. This is especially important considering that many principals are expected to want to maintain a certain separation between their work and private lives combined with the fact that employers are likely to mandate that the work-related profile be hosted on an attribute provider they control. The most important element in supporting several ID-SIS-EP service instances is the ID-WSF Discovery Service and especially its discovery option keyword registration feature.

2. Flexible permissions enforcement. It is important that Liberty recognizes that permissions enforcement will happen at all layers and is under control of the principal, even if, technically speaking, Liberty has framed permissions enforcement mechanisms as out of scope for the standardization effort.

3. Usage directives are a logical companion and, combined with digital signatures, provide the necessary audit trail and accountability so that abusers can be kept in check and a system can enjoy wide public confidence.

4. Solid architectural foundation so that the above-mentioned higher level mechanisms can be relied upon to work effectively. Solid foundation includes things like transport layer security, application of digital signatures to both requests and responses, as well as flawless crypto system and protocol design.

Most ID-SIS-EP specific privacy concerns can be addressed by properly configuring the permissions mechanisms.

1. Tight control needs to be maintained about who is allowed to see the various ID numbers that may be held in ID-SIS-EP. The permissions need to take into consideration both the principal's preference and the legal obligations that may vary from jurisdiction to jurisdiction.

2. Tight control also needs to be applied to the principal's full legal name, date of birth, gender, and other attributes that are customarily used for formal identification purposes.

3. Most services that request profile information have narrow scope and an administrator of the ID-SIS-EP provider should be able to determine what information can legitimately be needed for implementing a given service. The default permissions should take this into consideration so that information is only disclosed on a "need to know" basis rather than blanket disclosure.

4. Many pieces of information in the EmploymentInformation container may be of great interest, even outside a principal's job function. For example, JobStartDate may (adversely) affect an individual's private credit rating. Obviously, great care should be exercised in disclosing this type of information.

5. Some pieces of private life information may not be appropriate in working life. Again, permissions should reflect this.

# 4. Discovery and Queries

Issues relating to profiles discoveries and queries are discussed in [LibertyIDPPGuide] and will not be repeated here.

# 5. Processing Rule Rationale

Note that [LibertyDST] requires multiple `Modification` elements to behave in a transactional fashion, i.e., either all `Modification` elements must either succeed or fail as a group. If an implementation has difficulty in guaranteeing the transactional semantics, it may be better to only support one `Modification` element for which the transactional semantics are trivial.

# 6. Cultural Portability

An Internet environment is the underlying assumption for the systems designs; end users will venture to web sites outside their own culture and interact with other users and businesses in foreign countries. This calls for a common language. A large part of the world, but not the entire world, has standardized on the use of the Latin alphabet (character set) with some variations. A full discussion of issues relating to cultural portability is contained in [LibertyIDPPGuide].

The attributes that have parallel localized attributes in the Employee Profile, as designated with an "L" prefix are summarized below.

**Table 6. Global and Localized elements**

| Attribute | Localized | Type | Synopsis |
|---|---|---|---|
| `CN` | `LCN` | cis | Every day name in Latin writing system |
| `AltCN` | `LAltCN` | cis | Additional every day names in Latin writing system |
| `CorpCommonName` | `LCorpCommonName` | cis | Screen name of the Principal |
| `LegalName` | `LLegalName` | cis | Full legal name |
| `InternalJobTitle` | `LInternalJobTitle` | cis | Job title |
| `OU` | `LOU` | cis | Organizational Unit |

# References

## Informative

[LibertyIDFFOverview] Wason, Thomas, eds. "Liberty ID-FF Architecture Overview," Version 1.2-errata-v1.0, Liberty Alliance Project (12 September 2004). *http://www.projectliberty.org/specs*

[LibertyIDWSFOverview] Tourzan, Jonathan, Koga, Yuzo, eds. "Liberty ID-WSF Web Services Framework Overview," Version 1.1, Liberty Alliance Project (14 December 2004). *http://www.projectliberty.org/specs*

[LibertyIDWSFGuide] Weitzel, David, eds. (26 April 2004). "Liberty ID-WSF Impelmentation Guideline," Draft version 1.0-08, Liberty Alliance Project *http://www.projectliberty.org/specs/*

[LibertyIDEP] Kellomäki, Sampo, Lockhart, Rob, eds. "Liberty ID-SIS Employee Profile Service Specification," Version 1.1, Liberty Alliance Project (29 September, 2005). *http://www.projectliberty.org/specs*

[LibertyIDPP] Kellomäki, Sampo, Lockhart, Rob, eds. "Liberty ID-SIS Personal Profile Service Specification," Version 1.1, Liberty Alliance Project (29 September, 2005). *http://www.projectliberty.org/specs*

[LibertyIDPPGuide] Kellomäki, Sampo, Lockhart, Rob, eds. "Liberty ID-SIS Personal Profile Service Implementation Guidelines," Version 1.1, Liberty Alliance Project (29 September, 2005). *http://www.projectliberty.org/specs*

[LibertyDST] "Liberty ID-WSF Data Services Template Specification," Version 1.1, Liberty Alliance Project (14 December 2004). *http://www.projectliberty.org/specs* Kainulainen, Jukka, Ranganathan, Aravindan, eds.

[LibertyDisco] Sergent, Jonathan, eds. "Liberty ID-WSF Discovery Service Specification," Version 1.2, Liberty Alliance Project (12 December 2004). *http://www.projectliberty.org/specs*

[LibertyReg] Kemp, John, eds. "Liberty Enumeration Registry Governance," Version 1.1, Liberty Alliance Project (14 December, 2004). *http://www.projectliberty.org/specs*

[LibertyProtSchema] Cantor, Scott, Kemp, John, eds. "Liberty ID-FF Protocols and Schema Specification," Version 1.2-errata-v3.0, Liberty Alliance Project (14 December 2004). *http://www.projectliberty.org/specs*

[LibertyInteract] Aarts, Robert, eds. "Liberty ID-WSF Interaction Service Specification," Version 1.1, Liberty Alliance Project (14 December 2004). *http://www.projectliberty.org/specs*

[LDAP] Wahl, M., Howes, T., Kille, S., eds. (December 1997). "Lightweight Directory Access Protocol (Version 3), ," RFC2251, Internet Engineering Task Force *http://www.rfc-editor.org/rfc/rfc2251.txt [August 2003].*

[RFC2119] Bradner, S., eds. "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, The Internet Engineering Task Force (March 1997). *http://www.ietf.org/rfc/rfc2119.txt [March 1997].*

[XPATH] Clark , J., DeRose , S., eds. (16 November 1999). "XML Path Language (XPath) Version 1.0 ," Recommendation, W3C *http://www.w3.org/TR/xpath [August 2003].*