Technical Information On Bluewin Identity Provider

Technical Description On Bluewin Service Identity Provider

V2.3 dated 4th June 2004

Content:

1 Introduction 2

2 Liberty as Base Technology 3
   2.1 Liberty Alliance And Liberty Module Overview 3
   2.2 ID-FF: Identity Federation Framework 4
   2.3 Extension Of Industrial Standards 4
   2.4 ID-WSF: Identity Web Services Framework 4
   2.5 ID-SIS: Identity Services Interface Specifications 5
   2.6 Liberty Status Q4 2003 5

3 Process Overview Bluewin Identity Provider Service 6
   3.1 Standard Federation Process 8
   3.2 Extended Federation Process 8
   3.3 SSO Process 9
   3.4 Defederation Process 11
   3.5 Logout Process 12

4 Technical Requirements for Service Providers 13
   4.1 Liberty Framework 14
   4.2 OASIS And SAML 14

5 Appendix A: The Bluewin B2B Products 16
   5.1 Referenced Documents 16

6 Appendix B: International Standards 17

....
1 Introduction

Two options of the Bluewin Identity Provider service (abbreviated as IdP) are available for service providers:

a) **IdP_Basic:**
   IdP_Basic is a SSO package ideal for service providers who run their own separate user administration and will maintain this in the future. With this you can offer your customers “Single-Sign-On” functionality.

b) **IdP_Complete:** *(planned; not yet up and running):*
   IdP_Complete is an integral package designed for service providers that wish to run their operation without any user administration. The entire login and registration process is performed in an outsourcing method via Bluewin. Your customers benefit from the "Single-Sign-On". The **IdP_Complete** package will be available in 2005.

Bluewin is also offering the following supplementary package:

c) **IdP_Report:**
   IdP_Report is an offline interface for exchanging user data from Bluewin IdP.

d) **IdP_ProjMgmt:**
   IdP_ProjMgmt includes the entire Consulting and Project Management package, ensuring that the service provider's infrastructure is adapted to conform to Liberty and is compatible with Bluewin IdP.

The Identity Provider service is described in more detail in the document [1] *IdP_Public_WhitePaper* (Title: "Your Clients Benefit With Bluewin Identity Provider "). This paper describes the technical processes for **IdP_Basic**.
2 Liberty as Base Technology

The Bluewin service **Identity Provider** is based on the specifications of the **Liberty Alliance** (cf. [http://www.projectliberty.org/](http://www.projectliberty.org/)).

The Liberty Alliance is an alliance of renowned international companies (cf. excerpt from list of members at right-hand side), which have set the goal of using a federative structure to enable the user to use the "Single-Sign-On" feature, with privacy adherence in mind. The detailed list of "Founder Members", "Sponsor Members" and "Affiliates" is available for viewing on the Liberty Alliance web site.

Additional information on Liberty and its specifications can be found on the Liberty web site.

2.1 Liberty Alliance And Liberty Module Overview

The **LAP_Introduction** document ("Introduction to the Liberty Alliance Identity Architecture") provides an overview of the activities for Liberty and the corresponding standardisation endeavours. The Liberty specifications are made up of four modules:

1. **Module 1**: ID-FF: Identity Federation (base for all the Liberty processes)
2. **Module 2**: Standards of OASIS, W3C and IETF, or the extension of relevant standards from this committee
3. **Module 3**: ID-WSF: Identity Web Services Framework, allowing diverse identity services to be set up interoperably
4. **Module 4**: ID-SIS: Identity Services Interfaces for diverse services such as calendar, alarm, eWallet, etc. (future services)
The diagram opposite shows the four Liberty modules: ID-FF, Standards, ID-SIS and ID-WSF.

Today (2004), ID-FF and ID-WSF have been defined, as well as a few of the ID-SIS services.

2.2 ID-FF: Identity Federation Framework

The Liberty ID-FF module enables the federation of identities, including the corresponding management. This framework enables the interoperability of the most varied of platforms and defines the federation for PCs and mobile devices (mobile phones, PDAs etc.). With ID-FF, the user has access to Single-Sign-On in his/her personal CoT ("Circle of Trust"). The ID-FF module also defines the exchange of metadata.

The ID-FF module is the central module of the Liberty specifications. The Liberty document LAP_Architecture ("Liberty Architecture Overview") gives an overview on the basic mechanism of the process of identity federation.

2.3 Extension Of Industrial Standards

Module 2 is not actually a Liberty module. Rather it represents a collection of international standards relevant to Liberty. In other words, ID-FF, ID-WSF and ID-SIS are based on these standards. These refer to existing standards; as necessary and when required they will be extended and approved with the appropriate standardisation organisations. Some of the organisations with which Liberty Alliance works include:

1. Organisation for the Advancement of Structured Information Standards (OASIS)
2. World Wide Web Consortium (W3C)
3. Internet Engineering Task Force (IETF)

The following are used as standards:

<table>
<thead>
<tr>
<th>SAML</th>
<th>HTTP</th>
<th>WS-Security</th>
<th>WSDL</th>
<th>XML-ENC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAP</td>
<td>XML</td>
<td>SSL/TLS</td>
<td>SOAP</td>
<td>XML-DSIG</td>
</tr>
</tbody>
</table>

2.4 ID-WSF: Identity Web Services Framework

ID-WSF is based on ID-FF and forms the basis to provide personified services. ID-WSF comprises:

- the exchange of individual attributes ("permission-based attribute sharing")
- the collection of identity elements in a distributed environment ("identity service discovery")
- interaction services ("interaction services")
• additional security profiles, which are to be observed during data exchange ("security profiles")
• SOAP binding ("Simple Object Access Protocol Binding")
• extended support for end devices, not IP/HTTP specific ("extended client support")
• personality profiles specification ("identity services templates")

2.5 ID-SIS: Identity Services Interface Specifications

Module 4 (ID-SIS) is based on ID-WSF and contains specifications for functions such as user registration, address book, calendar, location-specific services, and alarms ("alerts").

2.6 Liberty Status Q4 2003

The following diagram shows the status of Liberty Alliance specifications as of August 2003:
3 Process Overview Bluewin Identity Provider Service

A basic idea of Liberty is that an individual user (in Liberty documents referred as the "Principal") can federate various accounts ("local identities"), which he or she uses at various web sites. This in turn means that the user only has to login once to a single web site in order to have access to all of these federated web sites. Liberty describes two roles to provide this functionality:

1. **Identity Provider**: This is the web site on which the user (naturally) logs in. Bluewin assumes this role in Switzerland. The concept of Bluewin is open to the presence of additional Identity Providers.

2. **Service Provider**: This refers to the remaining web sites with which the user has federated ("Federation of local identity with identity of Identity Provider").

These two roles are the basis for Single-Sign-On (SSO) for the user. In other words, the individual person registers at Bluewin with his/her account (using his/her identity as a private person) and then has SSO access to all the service providers which he/she has previously federated. The user is automatically logged in at these service providers sites as soon as the corresponding page of the service provider is accessed. Bluewin Identity Providers together with the federated service providers then form a personal "Circle of Trust" (CoT) for the individual user ("principal"): What exactly is federation? A federation of two accounts, one at an identity provider and one at a service provider, is defined by a common key. This common key has to be filed in the two databases (IdP and SP) as an add-on to the user data. This key is called an "Opaque Handle", an unambiguous string which does.

The Bluewin service Identity Provider (IdP) supports the following processes in combination with the service provider (SP):

1. **Standard Federation Process** (according to Liberty):
   In this process the user is given the option to define the federation between his/her global identity (at Bluewin IdP) and the local identity at the SP. The user only has to do this once in order to subsequently enjoy the benefits of SSO.
   Details are available in Section 3.1 "Standard Federation Process".
2. **Extended Federation Process** (according to Liberty):
   This process is an enhancement to the federation process (see above): When the user is not yet registered at the service provider, the user defines which of his/her attributes (of his/her global identity at Bluewin IdP) may be used automatically for registration at the service provider. Afterwards the standard federation process is executed.
   Details are available in Section 3.2 "**Extended Federation Process** .

3. **SSO Process** (according to Liberty):
   This process contains the automatic login (SSO) at the SP when the user has been previously registered at Bluewin IdP and if the two identities have been previously federated. Details are available in Section 3.3 "**SSO Process** .

4. **Defederation Process** (according to Liberty):
   This process terminates a federation to an SP. Details are available in Section 3.4 "**Defederation Process** .

5. **Logout Process** (according to Liberty):
   This process logs the user out from Bluewin IdP and from all federated SPs.
   Details are available in Section 3.5 "**Logout Process** .
3.1 Standard Federation Process

The Liberty Single Sign-On and Federation Protocol enables the principal to federate his/her account at the SP with the Bluewin account. This is done by initialising a Redirect from the SP to Bluewin and the subsequent exchange of an Opaque Handle via Redirect to the SP and a reciprocal Authentication Assertion via SAML.

The following flow chart shows the federation process for two principal accounts:

The goal of this process, therefore, is to ensure that both the Bluewin IdP and the SP possess a common key ("Opaque Handle"). This "Opaque Handle" clearly references the user ("principal").

3.2 Extended Federation Process

Bluewin gives the SP the opportunity of simplifying its client registration process for Bluewin clients by making personal Bluewin user data available to the SP. The Bluewin user, however, must confirm this step.

The following flow chart displays the federation sequence for two accounts with previous registration of the principal at the SP:
The goal of this process is a simplified and user-friendly registration process at the SP. This is done through data exchange of user ("principal") attributes.

Remark: The final Liberty specifications for the exchange of identity attributes (ID-WSF) have not yet been incorporated into the framework SourceID. SourceID is a multi-protocol federation framework from Ping Identity Corporation. The Bluewin Identity Provider service is based on SourceID and will be adapted as soon as SourceID fully supports ID-WSF.

3.3 SSO Process

Through Liberty Alliance specifications, Single Sign On is enabled, allowing the principal to access an SP service via SSO. The principal must have previously authenticated at Bluewin for an SSO service. Via a Redirect from the SP to Bluewin and the subsequent return of an authentication artifact via Redirect to the SP and a reciprocal authentication assertion via SAML, the principal can start the SP service without having to be authenticated at the SP.

The following flow chart displays the process for a Single Sign On access to an SP service:
The goal of this process is to enable the user ("principal") to be automatically logged in at the SP (without any user interaction at all) if 1) the user has already logged in at Bluewin IdP and 2) the user has previously defined the federation with the SP.
3.4 Defederation Process

Liberty defines the Liberty Identity Federation Termination Process, allowing the principal to terminate a defined federation with an SP. The principal has to invoke a defederation function at Bluewin, which then notifies the SP via SOAP of the termination request.

The following flow chart displays the defederation process:

The goal of this process is to terminate an existing federation with an SP. In doing so the common key ("Opaque Handle") is made invalid.
3.5 Logout Process

Liberty specifications also define the Liberty Single Logout Process, which permits the principal to end all open sessions at all SPs. The principal at Bluewin can initiate this by simply using the Bluewin logout function.

The following flow chart displays the logout process:

The goal of this process is to logout the principal from all open sessions both at the SPs and at Bluewin IdP.
4 Technical Requirements for Service Providers

In order to use Bluewin to create a federation for the purpose of a Single Sign On under the Liberty specifications, the service provider needs a separate client administration with registration, etc., and its own web-based services. The user database must be enhanced to support the user handles. In addition, the SP must also extend its existing infrastructure with the Liberty processes for the role of SP, as described in Chapter 3.

An SP architecture extended with Liberty could look like this:
4.1 Liberty Framework

Bluewin is currently using a Liberty Framework prototype development called **SourceID for Java**. SourceID is a public source toolkit which enables rapid implementation of a Liberty solution. The toolkit is available as a version for Java and .net and it can be downloaded at [http://www.sourceid.org](http://www.sourceid.org). A brief overview is provided here of the most important components and the operating principle of the Java Toolkit.

The Java Toolkit encapsulates the following functionalities and makes them available in a high-level Servlet/JSP API:

- XML parsing
- XML data binding
- SOAP
- Digital signatures
- SAML
- Liberty protocols.

In other words, developers do not have to worry about Liberty protocol implementation details.

SourceID.Java is based on different Apache Tools and Libraries, which are supplied along with the Toolkit. The required versions are written in Toolkit. Standard Apache installations have to be patched if necessary.

SourceID.Java is not a persistent framework to edit and save account and federation data. It requires a pre-defined way in which it then processes the provider’s account database. For this purpose a so-called Account Handler, an adapter on the client database, has been developed. SourceID.Java defines the interface that has to be implemented by such an Account Handler.

SourceID.Java does not assume any user authentication. It only delegates temporarily the process control to the existing JSPs or provider Servlets for the authentication.

The deployment of a Liberty enhancement using the SourceID.Java Toolkit encompasses the following main activities for the developers:

- configuration of the SourceID.Java by means of editing the sourceid-sso.xml files and listing of the services to be federated in the sourceid-sso-providers.xml file
- writing of an Account Handler Adapter to your own client database and extension of the client database to include federation attributes
- development of user interfaces, which represent the Liberty interactions. To this end the Toolkit provides several JSP and Servlets for adaptation and integration into the existing services.

SourceID is a possible Liberty Framework variant. Of course a service provider can also use another Liberty Framework or Liberty product.

4.2 OASIS And SAML

The Liberty Alliance does not intend to define any new protocol standards, but rather to incorporate the Liberty ideas into existing specifications. Therefore the key element for federation is the existing SAML (Security Assertion Markup Language) protocol. SAML is based on XML and was developed by the OASIS Group.
SSTC (Security Services Technical Committee). OASIS refers to “ Organisation for the Advancement of Structured Information Standards”.

SAML pursues the concept of two parties: “Asserting Party” (equivalent to Liberty role of identity provider) and the “Relying Party” (equivalent to Liberty role of service provider).

Between the Bluewin Identity Provider (SAML: Asserting Party) and the service provider (SAML: Relying Party), so-called artifacts are exchanged within the SAML protocol. An artifact consists of an identifier for Bluewin IdP and a so-called assertion handle. The latter is a non-ambiguous reference to the so-called assertion.

SAML requests and responses are packed by the SOAP protocol and transmitted by HTTP. With regard to security, SAML 1.1 requires at least SSL 3.0 or TLS 1.0.

Additional useful details on SAML are available on the OASIS homepage:

- [http://www.oasis-open.org](http://www.oasis-open.org)
5 Appendix A: The Bluewin B2B Products

Bluewin is the leading Internet service provider in Switzerland and provides a broad range of services for Internet users. Bluewin also provides a range of services geared at business clients. This enables business clients to provide innovative services on their own as a service provider. These services for business clients from Bluewin encompass the following:

- ADSL Internet access for small businesses
- HostCentre, in order to operate company web sites in a secure environment
- HomepageTool, in order to be able to create your own homepage easily
- Advertising, for efficient advertising on Bluewin
- 3rd Party Billing (3pb) for the billing of content via existing billing options at Bluewin (telephone invoice Swisscom Fixnet)
- Identity Provider (IdP), to enable personalised offerings to be created and in order to eliminate important registration barriers for users willing to buy
- Content Delivery & Protection, to generate sales from the new services through protection of the content and assurance of its distribution (streaming)

Bluewin operates its infrastructure in two secure computing centres in Switzerland. At both sites the most important components are designed redundantly, enabling Bluewin to achieve a high degree of availability and safety against failure.

5.1 Referenced Documents

<table>
<thead>
<tr>
<th></th>
<th>Reference</th>
<th>Description</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>[4]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[5]</td>
<td>LAP_WWW</td>
<td>Additional Liberty documents as under Liberty Alliance</td>
<td>V1.1</td>
<td></td>
</tr>
<tr>
<td>[6]</td>
<td>SourceID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[7]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Appendix B: International Standards

## HTTP

HyperText Transport Protocol

[KFC2616]: HTTP is the transport protocol for HTML documents. HTML and HTTP are the basis of WWW. HTTP or “Hypertext Transport Protocol” is an application-level protocol for distributed, collaborative, hypermedia information systems.

## SAML

Security Assertion Markup Language

SAML (Security Assertion Markup Language) is an XML standard for exchanging authentication and authorization data between security systems. SAML is an XML-based specification describing authentication, attributes, and authorization decision objects (assertions) that can be exchanged between partners.

An (SAML) artifact is a small, random number designed to point to full SAML assertions. SAML artifacts are passed between sites by the browser on URL query strings.


## SOAP

Simple Object Access Protocol

Originally SOAP was a protocol invented by Microsoft and used for the first time under Windows 98 and Windows NT: The SOAP protocol allows process calls between remote objects. SOAP DCOM objects on remote nodes can interwork with each other.

Now SOAP is a generic protocol that allows the communication of programs on different servers. SOAP is based on XML and HTTP. Therefore SOAP does work thru different networks, including firewalls. In other words: SOAP is an XML envelope and data encoding technology used to communicate information and requests across the Web. It is typically considered the protocol used by Web services. It is actually an envelope encapsulation format that can be used with lower level Web protocols such as HTTP and FTP.

See also [http://www.w3.org/TR/SOAP](http://www.w3.org/TR/SOAP).

## SSL

Secure Socket Layer

[KFC2828]: SSL or “Secure Sockets Layer (protocol)” originally was developed by Netscape Communications, Inc. SSL is a protocol layer between TCP/IP and HTTP, FTP or Gopher for secure transportation of HTTP data.

HTTP data is ciphered by SSL and than handed over to TCP. TCP than hands over the data to IP. In this way SSL together with TCP/IP is forming an Internet tunnel: „Normal“ TCP/IP packets are transported over the Internet. But the content of the TCP/IP packets are ciphered HTTP packets. Thus SSL is an Internet protocol that uses connection-oriented end-to-end encryption to provide data confidentiality service and data integrity service for traffic between a client (often a Web browser) and a server and that can optionally provide peer entity authentication between the client and the server.

All the browsers that are supporting SSL are displaying “HTTPS:” when SSL encoding is used. When S/HTTP encoding is used they display “SHTTP:”. SSL is the common security standard that is used since the 1990ies. Although at the beginning the importance of S/HTTP was small, it was the source to form an Internet standard out of SSL. This standard is called TLS (Transport Layer Security).

During the second half of the 1990ies the Netscape (NS) and Microsoft (MS) browser had supported SSL only with 40 bit encoding (due to US government restrictions for export). The Microsoft browser had also supported the MS standard PCT (Private Communication Technology). In Switzerland during this time the products SecureNet and SafeLine from the Swiss company R3 have been designed (and produced) to support 128-bit SSL implementation (IDEA and TDES). SecureNet and SafeLine have been used for Telebanking over Internet (by CS, UBS, ZKB and others). Since the early 2000s there is no export restriction anymore and US browsers also support 128 bit encryption.

The term “Sockets” refers to the Berkeley interprocess communications model. A socket specifies the end points of a two-way communications channel, which connects two
processes together so they can exchange information.

**TLS**

**Transport Layer Security**

[RFC 2246, 3546]: TLS is a “generic SSL” that is an (official) Internet standard (RFC) since 1999. The specification for the TLS protocol was developed under the auspices of the Internet Engineering Task Force (IETF) to allow client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

TLS is the open, standards-based evolutionary replacement for the Secure Sockets Layer (SSL) protocol developed by Netscape Communications Corporation. Beginning of 1998 industry experts expect TLS to quickly replace SSL as the primary protocol used to encrypt real-time communication over the Internet.

Related to TLS is the PPP EAP TLS Authentication Protocol: Transport Level Security (TLS) provides for mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. PPP EAP TLS describes how EAP-TLS, which includes support for fragmentation and reassembly, provides for these TLS mechanisms within EAP.

**WAP**

**Wireless Application Protocol**

WAP is a protocol suggested by Nokia, Ericsson, Unwired Planet and Motorola dedicated for Internet and email access with mobile (wireless) devices (e.g. PDAs, mobile phones etc.) Until end of 1997 proprietary protocols such as HDML, HDTP, TTML and ITTP have been used for the same purpose.

WAP defines a set of protocols: WAE (Wireless Application Environment) for the application layer, session layer, transport layer based on WTP (Wireless Transport Protocol).

*See also* [http://www.wapforum.org](http://www.wapforum.org).

**WSDL**

**Web Services Description Language**

WSDL is an XML based meta language to define a web service of a company that wants to allow access to this web service for other companies in the world. WSDL and UDDI (Universal Description, Discovery, and Integration) are the kernel technologies for web services.

WSDL is a popular technology for describing the interface of a Web service.

*See also* [http://www.w3.org/TR/wsd](http://www.w3.org/TR/wsdl).

**WSS**

**Web Services Security**

WSS or WS-Security describes enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies.

WS-Security also provides a general-purpose mechanism for associating security tokens with messages. No specific type of security token is required by WS-Security. It is designed to be extensible (e.g. support multiple security token formats). For example, a client might provide proof of identity and proof that they have a particular business certification.

Additionally, WS-Security describes how to encode binary security tokens. Specifically, the specification describes how to encode X.509 certificates and Kerberos tickets as well as how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the credentials that are included with a message.

**XML**

**eXtensible Markup Language**

XML is a very flexible so called meta language: XML defines the structure of a document or data. Simple example: XML can be used to describe the structure of an ordinary purchase order (“PO”).

Similar to IBM’s SGML, XML is a (generic) language to define a document description language, e.g. to define HTML. XML is the base for Microsoft’s “push technology” CDF.
But XML is also the base for the new technology “Web Services” (WS).

1998: XML is widely seen as a possibility to migrate from EDI thru a conversion from EDI to XML based DTDs (Document Type Definition).

With XML it is possible to exchange non HTML files and data (but not program code or objects) over the Internet. Objects have to be exchanged through XMI. Since 1998, XML is an accepted standard by W3C.

XML is a W3C technology for encoding information and documents for exchange over the Web. See also http://www.w3.org/XML.

XML-DSig XML Digital Signature
XML-DSig or “XML Digital Signature” is a W3C working group to develop an XML compliant syntax used for representing the signature of Web resources and portions of protocol messages (anything that may be referenced by a URI) and procedures for computing and verifying such signatures.

XML Encryption
XML Encryption is a W3C working group to develop a process for encrypting/decrypting digital content (including XML documents and portions thereof) and an XML syntax used to represent the (1) encrypted content and (2) information that enables an intended recipient to decrypt it.