HP OpenView Select Federation Premium Edition

LECP Service Overview and API

Software Version: 6.1

for HP-UX, Linux, Solaris, and Windows operating systems

April 2005

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

HP OpenView Select Federation includes software developed by third parties. The software in Select Federation includes:

- Software developed by Trustgenix, Inc. Copyright © Trustgenix, Inc. 2002-2005. All rights reserved.
- Apache Derby, Apache Xalan Library, Apache Xerces Library, and Apache XML Dsig Library.
- Software developed by the University Corporation for Advanced Internet Development <http://www.ucaid.edu>Internet2 Project.

Trademark Notices

- Trustgenix, IdentityBridge, and Trustgenix Federation Server are U.S. trademarks of Trustgenix, Inc.
- BEA and WebLogic are registered trademarks of BEA Systems, Inc.
- IBM, Tivoli, WebSphere are trademarks of International Business Machines in the United States, other countries or both.
- Linux is a U.S. registered trademark of Linus Torvalds.
- Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

- Oracle is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation.
- Sun, Sun Microsystems, Solaris, and Java™ are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.
- The Liberty Alliance project logos are trademarks of IEEE-ISTO.
- All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies/owners.

Support

Please visit the HP OpenView web site at:

http://www.managementsoftware.hp.com/

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

You can also go directly to the support web site at:

http://support.openview.hp.com/

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in.   Throughout the site, access levels are indicated by the following icons:

🔑 HP Passport

📝 Active contract

★ Premium contract

To find more information about access levels, go to the following URL:

http://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to the following URL:

https://passport.hp.com/hpp2/newuser.do

Contents

1

LECP Architecture and Interactions

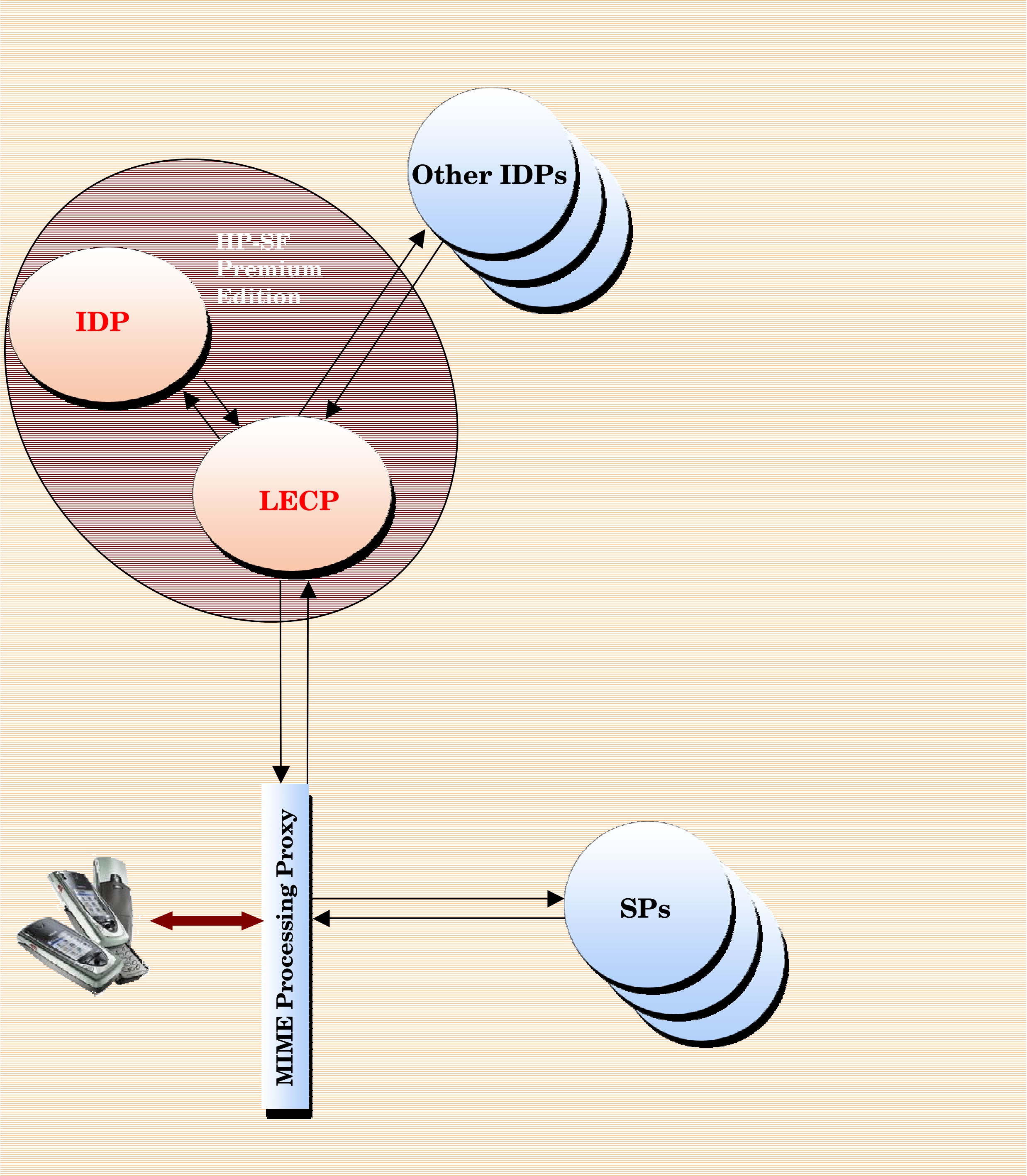
Introduction

The Select Federation LECP Service, bundled with the Premium Edition of Select Federation, implements the Liberty Enabled Client/Proxy profile (v1.1). The LECP profile provides for an enhanced user experience during Liberty authentication, especially in mobile environments. Using the Select Federation LECP Service, any WAP gateway can be easily extended to support the LECP profile.

See the "Liberty Bindings and Profiles Specification" for more information about the LECP profile:

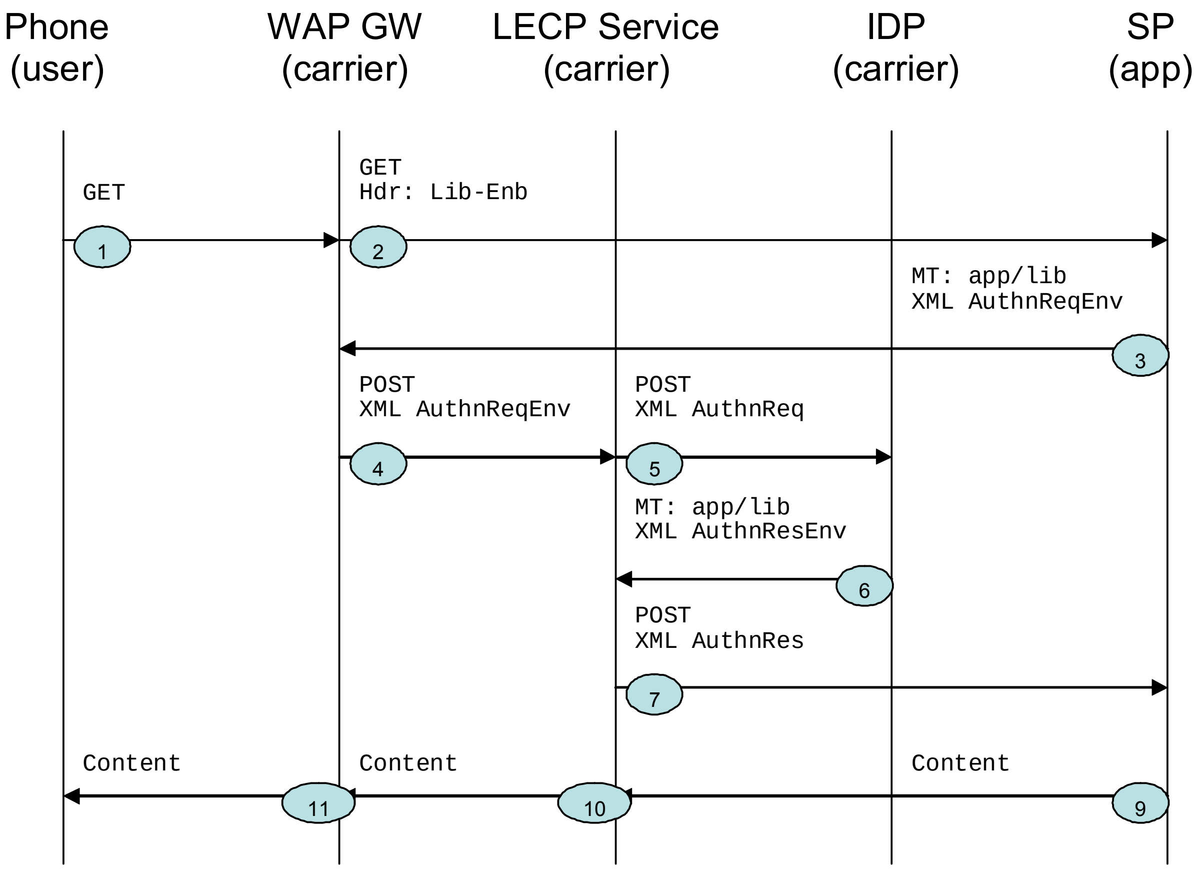
https://www.projectliberty.org/specs/archive/v1_1/index.html

LECP Architecture

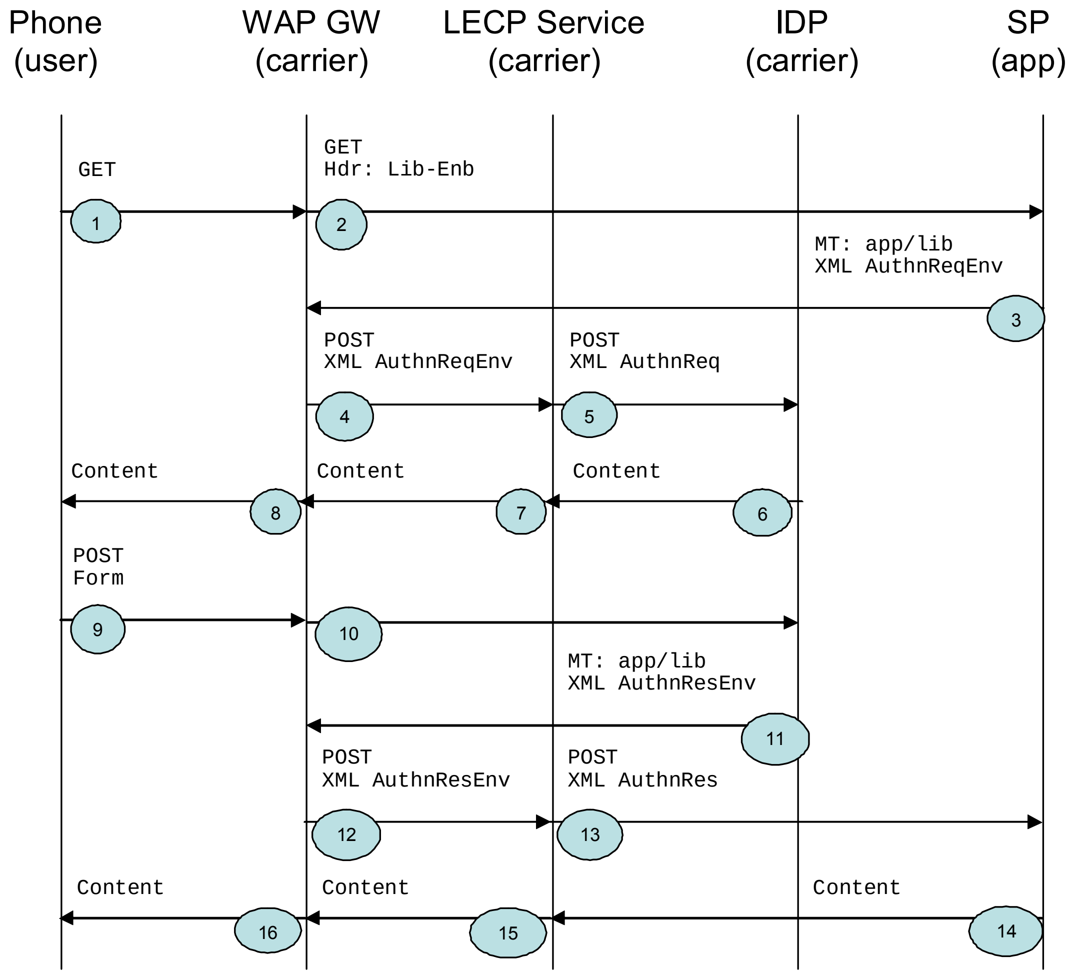


Message Flows

Basic Authentication



Authentication / Federation with User Interaction



2

WAP Gateway Integration

Liberty-Enabled Header

In order to activate the LECP profile, the WAP gateway must add the following header to every HTTP request:

Liberty-Enabled: LIBV=http://projectliberty.org/specs/v1

Handling Liberty Messages

For every request that includes the Liberty-Enabled header, the WAP gateway must check the response for Liberty messages requiring special processing. The messages are identified by their Content-Type:

application/vnd.liberty-request+xml

application/vnd.liberty-response+xml

The contents of HTTP responses of these MIME types must be dispatched to the LECP Service (see POSTing Liberty Messages below). The LECP Service will return a new response for return to the client.

3

LECP Service API

The Select Federation LECP Service is driven by a simple HTTP POST API to which the WAP gateway POSTs all Liberty messages received in HTTP responses -- the response from this POST is then returned to the client in place of the original response. The entry point for the LECP Service is:

<base url for Select Federation LECP WAR deployment>/tfsidp-lecp/IDPLECPService

Note:

Select Federation is a J2EE application, packaged as an Enterprise Application Archive (EAR). The LECP Service is packaged in its own Web Application Archive (WAR) within the Select Federation EAR (called `tfs.ear`).

Posting Liberty Messages

The contents of HTTP responses identified as Liberty messages are POSTed to the main entry point of the LECP service. All normal client request headers should be included in the POST, with the exception of cookie headers. In particular, any headers that may be needed by the IDP to authenticate the client must be included (the LECP service provides configuration parameters to control which URLs these headers will be passed on to).

To handle cookies set by an IDP or SP on Liberty messages, the following special headers should be included by the WAP gateway (if these headers are not included, support for session cookies on messages sent by the LECP service will be disabled):

Header	Description	Example
X-LECPSession	Opaque session id used by the LECP service to manage session cookies with Liberty SPs and IDPs as needed.	X-LECPSession: 1778 0654D5610F5A7C1E 43E11D231914
X-LECPURL	The URL of the request that returned the Liberty message being submitted for processing. This URL is used by the LECP service to manage any SP/IDP cookies set on the response (see X-LECPSetCookie header).	X-LECPURL: http://sp.com
X-LECPSetCookie	Used to pass the contents of any SetCookie headers included in the response containing the Liberty message.	X-LECPSetCookie: JSESSIONID=1142 5F119F968A9F14191 3F5C9E6E3B0;Path= /;Secure

Configuration

The following LECP service properties may be configured in the Select Federation configuration file (tfsconfig.properties):

Property	**Description**	**Example**
LecpDefaultIDPLoc	URL where a *default* IDP receives Liberty AuthnRequests. **Optional**: if provided, requests that do not specify an IDP will be forwarded to this URL. If not provided, the local IDP that is hosting the LECP will be used.	https://idp.com/tfsidp/IDPSingleSignOnService
lecpAllowIDPLocPrefixes	Space separated list of URL prefixes to which Liberty AuthnRequests will be forwarded. **Optional**: default is to allow all URLs.	https://goodidp1.com https://goodidp2.com
lecpDenyIDPLocPrefixes	Space separated list of URL prefixes to which Liberty AuthnRequests will NOT be forwarded. **Optional**: default is deny no URLs.	https://badidp1.com
lecpSessionHeader	Name of header that WAP gateway uses to pass opaque client session id to LECP Service, for use in managing cookies. **Optional**: default is X-LECPSession.	X-LECPSession

LecpStripHeadersIDP	Space separated list of HTTP headers which will be stripped in requests forwarded to IDPs. **Optional**: default is to pass all headers except those in a built-in list.	
LecpStripHeadersSP	Space separated list of HTTP headers which will be stripped in requests forwarded to SPs **Optional**: default is to pass all headers except those in a built-in list.	x-nokia-msisdn x-up-subno

Security Considerations

In order to avoid the overhead of establishing a mutually authenticated TLS HTTPS connection between the WAP gateway and the LECP service, it is recommended that the LECP service WAR be deployed behind a firewall that restricts access to connections made from the WAP gateway.