ATIS STANDARD

ATIS-0200002

3RD PARTY SERVICE PROVIDER INTERFACES

TECHNICAL REPORT

ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' 17 Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Networked Car, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, please visit < http://www.atis.org >.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith.

ATIS-0200002, *3rd Party Service Provider Interfaces*

Is an ATIS Standard developed by the **ATIS Service Oriented Networks (SON) Forum**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright © 2011 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < http://www.atis.org >.

Printed in the United States of America.

ATIS-0200002

ATIS Standard on

3RD PARTY SERVICE PROVIDER INTERFACES

Alliance for Telecommunications Industry Solutions

Approved January 4, 2011

Abstract

Service Oriented Networks externally expose generic service capabilities over well-defined interfaces that can be re-used by higher-level service applications of Third Party Service Providers to offer services to end-users. There are a variety of standard interfaces that can be used, each addressing some particular set of capabilities. This Technical Report offers a directional perspective on such interfaces that indicates which are of greatest interest in the industry, especially in a converged IMS and web environment.

FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Service Oriented Networks Forum addresses work to enable the interoperability and implementation of Service Oriented Network (SON) applications and services by developing standards, providing coordination for the development of standards and practices, and facilitating related technical activities. This forum is placing an emphasis on telecommunications industry needs in collaboration with regional and international standards development programs in the telecommunications, IT, and Web industries.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, SON, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of initiation of this document, SON, which was responsible for its development, had the following leadership:

Andrew White, NSN, Chair of the SON Forum
Gary Munson, AT&T, Vice Chair of the SON Forum, and Technical Editor for this document

TABLE OF CONTENTS

1 SCOPE, PURPOSE, & APPLICATION 1

1.1 SCOPE 2

2 REFERENCES 4

2.1 PARLAY 3.0 VIA 3GPP TS SERIES 4
2.2 OMA PARLAYREST 2.0 APIS 6
2.3 OMA PROFILES FOR GSMA ONEAPI (PARLAY X AND RESTFUL)[3] 6
2.4 ADDITIONAL REFERENCES 7

3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS 8

3.1 DEFINITIONS 8
3.2 ACRONYMS & ABBREVIATIONS 8

4 WEB SERVICES INTERFACES 9

4.1 PARLAY X API SOAP AND RESTFUL BINDINGS 9
4.2 ADDITIONAL SOAP OR RESTFUL 3PSP INTERFACES 12

5 IMS AS FAMILY OF INTERFACES 12

6 IDENTITY MANAGEMENT 14

6.1 WS-SECURITY 14
6.2 OAUTH 2.0 15
6.3 SAML 2.0 16
6.4 FEDERATION 17
6.5 WS-TRUST AND WS-FEDERATION 17
6.6 SAML 2.0 18

7 DISTINCTION BETWEEN UE-SP INTERFACES AND 3PSP-SP INTERFACES 18

TABLE OF FIGURES

FIGURE 1: 3PSP INTERFACE 3
FIGURE 2: IMS AS FAMILY OF INTERFACES 13
FIGURE 3: WS-SECURITY MODEL ILLUSTRATION 15
FIGURE 4: OAUTH 2.0 MODEL ILLUSTRATION 16
FIGURE 5: IDENTITY MANAGEMENT ENTITIES 17

TABLE OF TABLES

TABLE 1: PARLAY X API BINDINGS 10

ATIS Standard on –

3RD Party Service Provider Interfaces

1 SCOPE, PURPOSE, & APPLICATION

The fundamental premise of Service Oriented Networks (SON) is exposure of generic capabilities, also referred to as "services", through well-defined interfaces that can be re-used by higher-level applications. Such exposure may occur across organizational domains. Control of network capabilities across an interface by external 3rd Party Service Providers (3PSP) to support end-user services is a well-known concept that fits within the SON context. There are a variety of such interfaces already defined that can be used, each addressing some particular set of capabilities. Some interfaces may be recognized in standards for that purpose. In fact, originally, the ATIS NGN architecture [1] had recognized Parlay, Parlay X, and SIP. However, it is important to re-assess what interfaces are of greatest interest for the following reasons:

- The emergence of additional potentially relevant interfaces that provide new capabilities.
- Industry experience with or level of support for particular interfaces.
- The emergence of new technology styles of interfaces.

While 3PSP control has historically been directed at network capabilities, it may be more generally thought of as control of Service Provider (SP) capabilities, where a SP may or may not be a network operator.

The purpose of this document is to offer a directional perspective on 3PSP-SP interfaces that indicates what is of greatest interest in the industry, especially in a converged environment of IMS and web services.

By offering such a perspective, vendors of relevant equipment or software can focus on a more limited set of options, and the 3rd party service provider community is encouraged to create more applications because there is no accompanying per-SP-specific interface work required.

This report is informative, not normative. SPs and 3PSPs may implement 3PSP interfaces as they deem appropriate.

Interfaces of different protocol types (SOAP or RESTful or SIP) may overlap in functionality offered. The perspective of this report is that such overlap is acceptable, since different interface technologies may be preferable to different developer/3PSP communities.

This report largely draws from one industry association, the Open Mobile Alliance (OMA), and two standards organizations, the Third Generation Partnership Project (3GPP) and the International Engineering Task Force (IETF). The OMA owns the Parlay X APIs and associated WSDL and RESTful interfaces, as well as additional OMA service enablers such as WAP Push that are of interest. The 3GPP defines an IMS Application Server (AS) functional element whose interfaces are based on IETF specifications. That AS role could be performed by a 3PSP.

This report captures a snapshot in time, based on what is currently or will be imminently available in the industry. The capability sets that the SPs choose to offer to 3PSPs and what the 3PSPSs may desire

to employ will surely expand over time. This environment is rapidly moving in two directions: one is the development of new capability sets and the second is the adaptation of existing capability sets to new protocols.

The new capability sets are driven by new and evolving market opportunities such as IPTV, machine-to-machine devices, social networking, and augmented reality.

The adaptation of existing capability sets results from new technologies such as LTE and software constructs such as REST. These technologies drive existing functionality into newer protocols.

1.1 Scope

As shown in Figure 1, the 3PSP is connected to a Service Provider that is supporting the 3PSP. The Service Provider may also be a Network Operator, or it may not be a Network Operator. The 3PSP is utilizing Service Provider-based capabilities, accessed across the 3PSP Interface, to provide services to end-users. An end-user of a 3PSP may be connected to a Network Operator that the 3PSP is also using for Service Provider capabilities, or may be connected to a Network Operator that the 3PSP is not using for Service Provider capabilities. An example of the latter case is an end-user with a web browser connection via an access service provider and the internet to the 3PSP, where the browser application has to do with accessing location information and the 3PSP is using a 3PSP Interface to some other Service Provider to collect location-based information.

The logical point of 3PSP connectivity to the Service Provider is the 3PSP Gateway, which has roles such as limiting what the 3PSP is allowed to do as per prior agreement, hiding Service Provider details from the 3PSP, and protecting the Service Provider from potential 3PSP misbehavior. The implementation of the 3PSP Gateway is out of scope of this document.

The SP may implement policies in the 3PSP GW or other functional elements that constrain what any particular 3PSP is allowed to do with or obtain from the SP – e.g., types of requests and their content, maximum interface load, scope or granularity of user profile and user presence information. Limitations on any specific 3PSP would typically be defined in a SLA. Such policy use would have at most only incidental impact on the interface specifications themselves (i.e., potentially to include explicit information on the nature of an SLA violation when the SP rejects a request from the 3PSP) and so is not further addressed in this document.

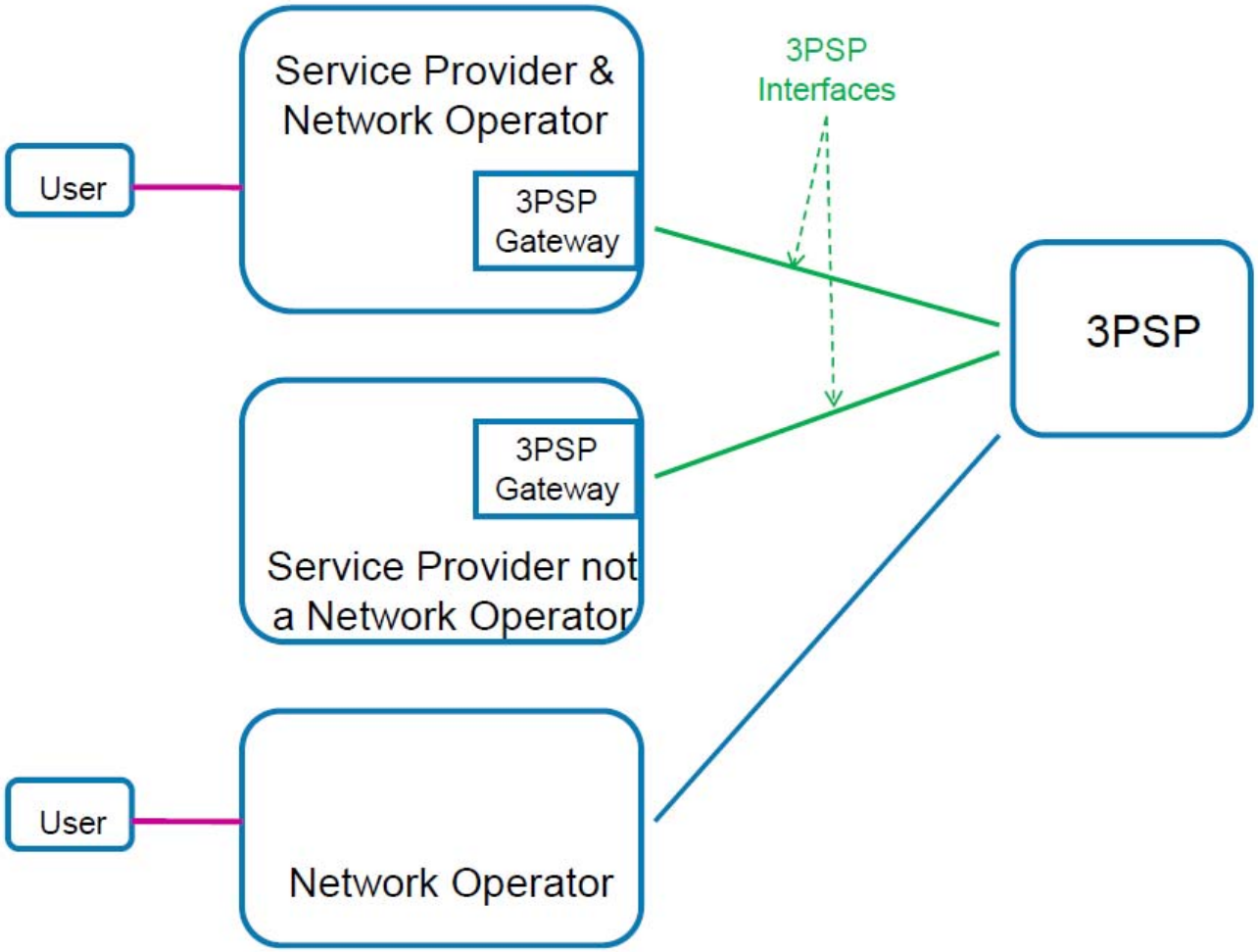

Figure 1: 3PSP Interface

The nature of the 3PSP-end-user relationship may vary. For example, end-users may be subscribers to services that the 3PSP has offered to the public, or it may be that the 3PSP is only offering services to end-users within a particular company, or it may be that the Service Provider has out-sourced services to the 3PSP.

The envisioned Network to which a 3PSP may attach is a Next Generation Network (NGN) that supports both IMS and web-based capabilities.

The kinds of control capabilities provided across the interface profile may include things like (the following list is not exhaustive):

- Multi-media session and conferencing control.
- Notification of various kinds of events.
- Supplementary session-related services (e.g., call screening or call forwarding).
- Obtaining information about end-users (e.g., location, presence, preferences).
- Content delivery (attachment, download, broadcast, multi-cast, etc.).

- Charging.
- Obtaining information on device capabilities or status.
- Managing user data (e.g., address book, preferences, media library).
- Messaging.

This report does not address PSTN/legacy network-oriented interfaces (e.g., CAP/CAMEL, TCAP, etc.) as part of the profile. This report does not address older, native protocols, some of which are widely used today and may remain in use for some time (e.g., SMPP or PAP).

This report does not address operations/management aspects of 3PSP interfaces.

There is a natural overlap between 3rd Party Service Provider – Service Provider interfaces and User Equipment – Service Provider interfaces. While this report does not directly address the latter, it discusses the relationship. See Section 7.

2 REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this ATIS Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[1] ATIS-1000018, *ATIS NGN Architecture Technical Report.*[1]

[2] 3rd Generation Partnership Project; *Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS), TS 23.228 V8.12.0.*

2.1 Parlay 3.0 via 3GPP TS series[2]

[3] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 1: Common (Release 8), 3GPP TS 29.199-1.*

[4] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 2: Third Party Call (Release 8), 3GPP TS 29.199-2.*

[5] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 3: Call Notification, 3GPP TS 29.199-3.*

[6] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 4: Short Messaging (Release 8), 3GPP TS 29.199-4.*

[7] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 5 (Release 8): Multimedia Messaging, 3GPP TS 29.199-5.*

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions, 1200 G Street N.W., Suite 500, Washington, DC 20005. < http://www.atis.org >

[2] These documents are available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

[8] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 6: Payment (Release 8), 3GPP TS 29.199-6.*

[9] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 7: Account Management (Release 8), 3GPP TS 29.199-7.*

[10] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 8: Terminal Status (Release 8), 3GPP TS 29.199-8.*

[11] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 9: Terminal Location (Release 8), 3GPP TS 29.199-9.*

[12] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 10: Call Handling (Release 8), 3GPP TS 29.199-10.*

[13] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 11: Audio Call (Release 8), 3GPP TS 29.199-11.*

[14] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 12: Multimedia Conference (Release 8), 3GPP TS 29.199-12.*

[15] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 13: Address List Management (Release 8), 3GPP TS 29.199-13.*

[16] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 14: Presence (Release 8), 3GPP TS 29.199-14.*

[17] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 15: Message Broadcast (Release 8), 3GPP TS 29.199-15.*

[18] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 16: Geocoding (Release 8), 3GPP TS 29.199-16.*

[19] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 17: Application Driven QoS (Release 8), 3GPP TS 29.199-17.*

[20] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 18: Device Capabilities and Configuration (Release 8), 3GPP TS 29.199-18.*

[21] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 19: Multimedia Streaming Control (Release 8), 3GPP TS 29.199-19.*

[22] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 20: Multimedia Multicast Session Management (Release 8), 3GPP TS 29.199-20.*

[23] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 21: Content Management (Release 8), 3GPP TS 29.199-21.*

[24] 3rd Generation Partnership Project; *Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 22: Policy (Release 8), 3GPP TS 29.199-22.*

2.2 OMA ParlayREST 2.0 APIs[3]

NOTE -- Regarding the OMA document references below:

- A "draft" or "D" in the name indicates a specification that is a work in progress.
- A "C" in the name is for "Candidate", indicating a specification that has reached a high degree of stability and is undergoing validation and review and/or public review.
- A reference with neither of the above indicators is past the Candidate phase and is an Approved document.

[23] Open Mobile Alliance, *RESTful Bindings for Parlay X Web Services – Common, Draft Version 1.1, OMA-TS-ParlayREST_Common-V1_1.*

[24] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Short Messaging, Draft Version 1.1, OMA-TS-ParlayREST_ShortMessaging-V1_1.*

[25] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Multi-Media Messaging, Draft Version 1.1, OMA-TS-ParlayREST_MultiMediaMessaging-V1_1.*

[26] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Payment, Draft Version 1.1, OMA-TS-ParlayREST_Payment-V1_1.*

[27] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Terminal Location, Draft Version 1.1, OMA-TS-ParlayREST_TerminalLocation-V1_1.*

[28] Open Mobile Alliance, RESTful bindings for Parlay X Web Services – Terminal Status, Draft Version 1.0, *OMA-TS-ParlayREST_TerminalStatus-V1_0 draft.*

[29] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Third Party Call, Draft Version 1.0, OMA-TS-ParlayREST_ThirdPartyCall-V1_0 draft.*

[30] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Call Notification, Draft Version 1.0, OMA-TS-ParlayREST_Call Notification-V1_0 draft.*

[31] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Audio Call, Draft Version 1.0, OMA-TS-ParlayREST_AudioCall-V1_0 draft.*

[32] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Device Capabilities, Draft Version 1.0, OMA-TS-ParlayREST_DeviceCapabilities-V1_0 draft.*

[33] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Presence, OMA-TS-ParlayREST_Presence-V1_0 draft.*

[34] Open Mobile Alliance, *RESTful bindings for Parlay X Web Services – Address List Management, Draft Version 1.0, OMA-TS-ParlayREST_AddressListManagement-V1_0 draft.*

2.3 OMA Profiles for GSMA OneAPI (Parlay X and RESTful)[3]

[35] Open Mobile Alliance, *OneAPI Profile of ParlayREST Web Services,* ***Draft*** *Version 2.0, OMA-TS-ParlayREST_OneAPIProfile-V***2***_0 draft.*

[36] Open Mobile Alliance, *OneAPI profile of Parlay X Web Services, Candidate Version 1.0, OMA-TS-PXPROF-V1_0.*

[3] See < http://member.openmobilealliance.org/ftp/Public_documents/ARCH/Permanent_documents/ > for OMA ParlayREST documents.

2.4 Additional References

[37] Open Mobile Alliance, *RESTful Bindings for OMA Push – Push Access Protocol, Draft Version 1.0, OMA-TS-PushREST-V1_0 draft.*
< http://member.openmobilealliance.org/ftp/Public_documents/CD/Permanent_documents/OMA-TS-PushREST-V1_0-20100810-D.zip >.

[38] Session Initiation Protocol (SIP) Event Package for OMA Content Push Delivery, IETF draft-mdolly-dispatch-oma-push < http://tools.ietf.org/html/ >.

[39] ATIS-1000035.2009, *ATIS NGN Identity Management Framework.*[1]

[40] ITU-T Recommendation Y.2720 (2009), *NGN Identity Management Framework.*[4]

[41] OASIS Web Services Security: *SOAP Message Security 1.1 (*WS-Security 2004) at
< http://docs.oasis-open.org/wss/v1.1/ >.

[42] OASIS *WS-Trust 1.4* at
< http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.doc >.

[43] OASIS *Web Services Federation Language* (WS-Federation) Version 1.2 at
< http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.doc >.

[44] WC3 XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008 at < http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/ >.

[45] WC3 XML Encryption Syntax and Processing W3C Recommendation 10 December 2002 at < http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/ >.

[46] The OAuth 2.0 Protocol, draft-ietf-oauth-v2-10 at
< http://tools.ietf.org/html/draft-ietf-oauth-v2-10 >.

[47] The Transport Layer Security (TLS) Protocol Version 1.2, IETF RFC 5246, at
< http://tools.ietf.org/html/rfc5246 >.

[48] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 OASIS Standard, 15 March 2005, at < http://docs.oasis-open.org/security/saml/v2.0/ >, and related documents.

[49] Open ID Foundation web site at < http://openid.net/foundation/ >.

[50] The Information Card Foundation web site at < http://informationcard.net >.

[51] The Kantara Initiative's Identity Assurance Work Group web site at
< http://kantarainitiative.org/confluence/display/idassurance/Home >.

[52] Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1, Cloud Security Alliance, at < http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf >.

[53] Domain 12: Guidance for Identity and Access Management, V2.1, Cloud Security Alliance, at
< http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf >.

[54] WC3 SOAP 1.2, at < http://www.w3.org/TR/soap12-part1/ >.

[55] Architectural Styles and the Design of Network-based Software Architectures, Roy Fielding Ph.D. dissertation, at < http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm >.

[4] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS

3.1 Definitions

3.1.1 3PSP interface: The actual exposed interface/protocol between the SP and the 3PSP, as opposed to some abstract representation of it -- for example, SOAP, RESTful, or SIP interfaces, which may also be referred to herein as bindings of abstract interface representations.

3.1.2 Application Programming Interface: An abstract representation of an interface -- e.g., a Parlay X API apart from and independent of its exposure as a SOAP interface. However, the reader is cautioned that industry use of "API" could mean either an abstract representation of an interface or a corresponding exposed interface (binding).

3.2 Acronyms & Abbreviations

3GPP	Third Generation Partnership Project
3PSP	Third Party Service Provider
API	Application Programming Interface
App	Application
AS	Application Server
ATIS	Alliance for Telecommunications Industry Solutions
CDF	Charging Data Function
GSM	Global System for Mobile Communications: originally from Groupe Spécial Mobile
GSMA	GSM Association
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IETF	International Engineering Task Force
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
LTE	Long Term Evolution
MS	Media Server
MRB	Media Resource Broker
NGN	Next Generation Network
OMA	Open Mobile Alliance
PCRF	Policy and Charging Rules Function
OASIS	Organization for the Advancement of Structured Information Standards
OCS	On-line Charging System
PAP	Push Access Protocol
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
REST	Representational State Transfer
RFC	Request For Comments
SAML	Security Assertion Markup Language
S-CSCF	Serving-Call Session Control Function

SIP	Session Initiation Protocol
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SLF	Subscription Locator Function
SMPP	Short Message Peer to Peer (protocol)
SON	Service Oriented Networks
SP	Service Provider
TLS	Transport Layer Security
WC3	World Wide Web Consortium
WS	Web Services
WSDL	Web Services Description Language

4 WEB SERVICES INTERFACES

There are two types of Web Services interfaces of special interest for 3PSP interfaces: interfaces employing SOAP [54] over HTTP, and interfaces that adhere to the principles of REST [55] and utilize HTTP. Both types of interfaces are widely used: SOAP more typically in enterprise/IT environments and REST in commercial internet environments. They have different strengths, and may appeal to different developer communities; this report acknowledges and allows for both approaches.

4.1 Parlay X API SOAP and RESTful Bindings

The set of Parlay X[5] APIs is the basis for providing functionality over 3PSP interfaces that is of greatest interest in the industry. There are two types of Parlay X API bindings included here: SOAP and RESTful. The latter is a recent exercise by the OMA and to date only covers some of the Parlay X APIs, but is indicative of the strong emerging interest in the use of the RESTful style. For a given Parlay X binding, there may be two included, reflecting different capability scopes:

1) The full binding (either SOAP or RESTful) as defined by OMA for a given Parlay X API.
2) A proper subset of the full SOAP or RESTful binding, as reduced to only cover the capabilities specified by the GSMA in their OneAPI specifications.

Some of the Parlay X APIs (and therefore the SOAP and RESTful bindings for 3PSP interfaces) are of relatively greater interest to SPs to offer and 3PSPs to employ than others. Table 1 indicates which presently appear to be of greatest interest, which is evidenced by corresponding OneAPI profiles and RESTful bindings already being specified. The table also indicates which are of relatively next higher interest, as evidenced by being included in the next phase of work in OMA to create RESTful bindings largely in common with GSMA interests. The remaining APIs are lumped into the category of ”relatively lesser interest”. Within each of the clusters in the table (highest interest, next highest interest, lesser interest), there is no intended ordering of the APIs.

[5] Parlay X as opposed to Parlay. The latter, commonly expressed as CORBA interfaces, offer even more functionality than Parlay X, but have gotten no real traction as 3PSP interfaces in their 10+ years of existence.

It remains to be seen, over the course of time, the actual popularity of each API/binding/profile.The Parlay X SOAP and ParlayREST bindings for the same Parlay X API may not in all cases provide exactly the same functionality.

"Part 1", "Part 2", etc., in the table below refer to the Part numbering as per the 3GPP Parlay X specifications. It is included here, as a reference aid for the reader. While the OMA now has taken over complete responsibility for Parlay X from the 3GPP, the Parlay X SOAP binding documentation is still kept by the 3GPP as 3GPP documents. The "N/A"s in the table, for Not Applicable, indicate that there are no such specifications, although OMA could conceivably take that on as work in the future.

Table 1: Parlay X API Bindings

Parlay X API	SOAP Binding Reference	RESTful Binding Reference	OneAPI scope SOAP Binding Reference	OneAPI scope RESTful Binding Reference
Necessary foundation APIs (to support any of the others)				
Part 1: Common	*[3]*	*[25]*		
APIs of relatively highest interest				
Part 9: Terminal Location	[11]	*[29]*	*[38]*	*[37]*
Part 4: Short Messaging	[6]	[26]	*[38]*	*[37]*
Part 5: Multimedia Messaging	[7]	[27]	*[38]*	*[37]*
Part 6: Payment	[8]	[28]	*[38]*	*[37]*
APIs of relatively next highest interest				
Part 2: Third Party Call	*[4]*	*[31]*	*N/A*	*[37]* *The OneAPI Call Control API is comprised of elements from ParlayREST Third Party Call, Call Notification and Audio Call*

Parlay X API	SOAP Binding Reference	RESTful Binding Reference	OneAPI scope SOAP Binding Reference	OneAPI scope RESTful Binding Reference
Part 3: Call Notification	*[5]*	*[32]*	*N/A*	*[37]* *The OneAPI Call Control API is comprised of elements from both ParlayREST Third Party Call, Call Notification and Audio Call*
Part 11: Audio Call	*[13]*	*[33]*	*N/A*	*[37]* *The OneAPI Call Control API is comprised of elements from both ParlayREST Third Party Call, Call Notification and Audio Call*
Part 8: Terminal Status	*[10]*	*[30]*	*N/A*	*[37]*
Part 13: Address List Management	*[15]*	*[36]*	*N/A*	*N/A*
Part 14: Presence	*[16]*	*[35]*	*N/A*	*N/A*
Part 18: Device Capabilities and Configuration	*[20]*	*[34]*	*N/A*	*[37]*
APIs of relatively lesser interest				
Part 7: Account Management	*[9]*	*N/A*	*N/A*	*N/A*
Part 10: Call Handling	*[12]*	*N/A*	*N/A*	*N/A*
Part 12: Multimedia Conference	*[14]*	*N/A*	*N/A*	*N/A*
Part 15: Message Broadcast	*[17]*	*N/A*	*N/A*	*N/A*
Part 16: Geocoding	*[18]*	*N/A*	*N/A*	*N/A*
Part 17: Application-driven Quality of Service (QoS)	*[19]*	*N/A*	*N/A*	*N/A*

Parlay X API	SOAP Binding Reference	RESTful Binding Reference	OneAPI scope SOAP Binding Reference	OneAPI scope RESTful Binding Reference
Part 19: Multimedia Streaming Control	*[21]*	*N/A*	*N/A*	*N/A*
Part 20: Multimedia Multicast Session Management	*[22]*	*N/A*	*N/A*	*N/A*
Part 21: Content Management	*[23]*	*N/A*	*N/A*	*N/A*
Part 22: Policy	*[24]*	*N/A*	*N/A*	*N/A*

4.2 Additional SOAP or RESTful 3PSP Interfaces

In addition to Parlay X APIs, many other "service enablers"/interfaces have been or are being defined within OMA, some of whose interfaces could serve as 3PSP interfaces offering additional functionality. Examples include the Next Generation Services Interface, Service User Profile Management, Contact Address Book, and Dynamic Content Delivery. (The OMA web site can be accessed for more information.) Thus, the OMA is a likely source for additional useful standard 3PSP SOAP- or RESTful-based interfaces. Such service enablers are not discussed further here, because SOAP- or RESTful-interfaces have not yet been specified and/or in some cases the service enabler work is in a relatively early stage.

One other OMA service enabler is of special interest; namely, Restful Push [39] for content delivery and asynchronous notifications. It is a technically mature service enabler, and a RESTful 3PSP interface for it is being defined (the original version of the interface was specified using PAP).

5 IMS AS FAMILY OF INTERFACES

It is natural to consider allowing the Application Server (AS) within the IMS part of the NGN architecture to be provided by a 3rd Party outside the domain of the rest of the NGN network operation -- i.e., a 3PSP AS.

Interest in this approach to providing 3rd party interfaces is primarily in the context of enterprise networks connected to commercial NGN network operators. The former may itself be a distributed IMS network, interconnected by the commercial network, with its own ASes supporting its own applications. Such a corporate network may want to have its own applications providing services to its end-users, including communications that originate into or terminate out of the commercial network. There appears to be little interest in using any part of the IMS AS family of interfaces to support 3rd party applications toward Consumer type end users, except for very focused capabilities such as SIP Push.

Figure 2 depicts the set of IMS AS interfaces,[6] [2] any of which could conceivably be exposed in whole or in part, with appropriate safeguards, by a commercial network. Currently, there is no direction in

[6] More formally, these are IMS *reference points* that are implemented by the respective interfaces. Those exposed interfaces associated with the reference points are of ultimate interest here.

standards activity to profile any particular subset of these interfaces for 3rd party support. At least in the near term, this kind of 3PSP connectivity will likely be supported only on a case-by-case basis, per enterprise network customer, as a given NGN operator deems worthwhile.

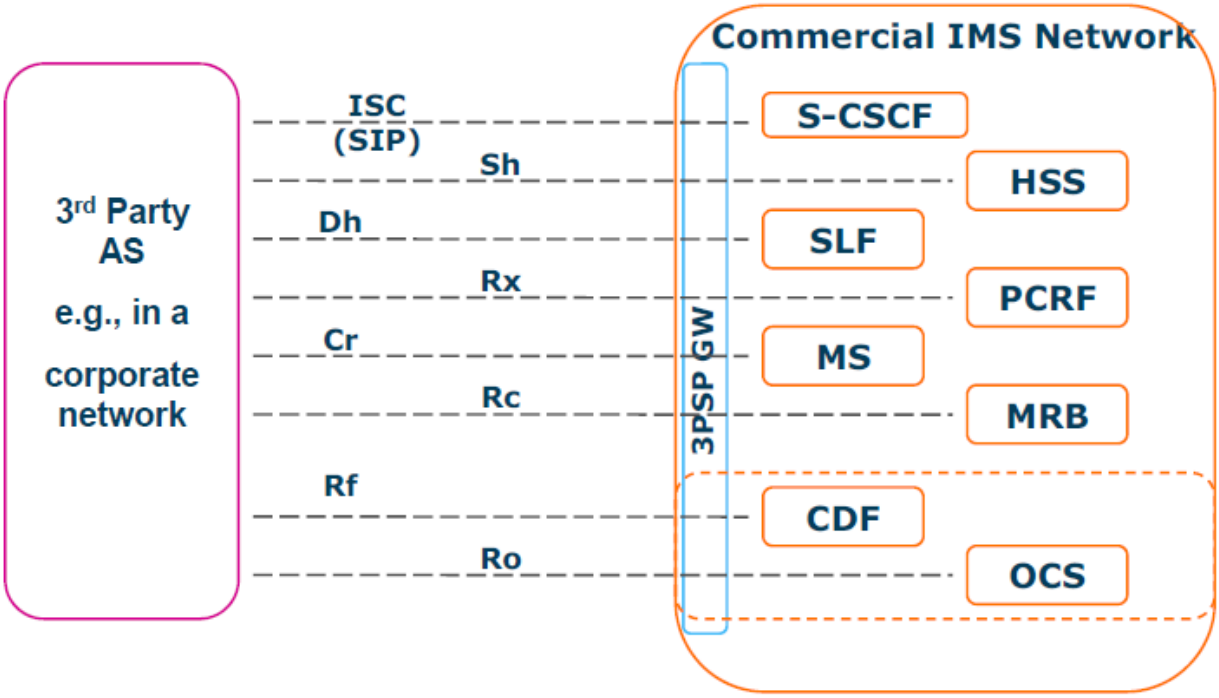

Figure 2: IMS AS Family of Interfaces

The interfaces between the AS and other IMS elements, and the nature of the protocols are:

- **ISC**: SIP, to the Serving-Call Session Control Function (S-SCSF)
- **Sh**: Diameter, to the Home Subscriber Server (HSS)
- **Dh**: Diameter, to the Subscription Locator Function (SLF)
- **Rx**: Diameter, to the Policy and Charging Rules Function /(PCRF)
- **Cr**: various* interfaces, to the Media Server (MS)
- **Rc**: HTTP or SIP, to the Media Resource Broker (MRB)
- **Rf**: Diameter, to the Charging Data Function (CDF)
- **Ro**: Diameter, to the On-line Charging System (OCS)

* RFC 5222, IETF mediactrl Control Framework and IVR and Mixer Control Packages, and others.

If any of the IMS AS family of interfaces were to be supported toward a 3PSP, minimally, it would begin with the ISC (SIP) interface, which is primarily for media session control. Allowing MS selection and control using the Rc and Cr interfaces, respectively, may be regarding by SPs as involving minimal

security risk. Likewise, the Ro and Rf interfaces for on-line and off-line charging, respectively, may be regarded by SPs as involving minimal security risk. Directly exposing any of the other interfaces may be viewed as less desirable by SPs.

Very specific functional areas within one of these interfaces may be of special interest for offering as a 3PSP interface. A key example is a SIP-based Push capability for content delivery or asynchronous notifications, motivated by the deployment of LTE, which is currently being specified in the IETF. [40]

6 IDENTITY MANAGEMENT

The ability of a 3PSP application to obtain an identity known to a SP, to authenticate to that SP, and to make specific authorized requests to the SP in a secure way are all critical to actually using a 3PSP interface. Those capabilities lie within the purview of Identity Management (IdM). [41], [42] Individual 3PSP interface SOAP and RESTful specifications do not explicitly define their own IdM or security mechanisms. Rather, those interfaces would be used in conjunction with a separately-defined IdM/security API layer.

There are a variety of IdM approaches/solutions that SPs may choose to employ with 3PSPs, depending on a variety of factors such as their own assessments of risk, complexity, etc.; the roles of proxy servers involved; or the expected sophistication of 3PSP environments or types operating systems they utilize. This is an unsettled area with various standards alternatives and sub-options within alternatives. This section provides some examples of IdM frameworks that can be used with 3PSP interfaces. For a broader perspective on security for virtualized services (an architectural framework, governance and operating domains, and associated considerations and guidelines), the Security Guidelines [54] and associated white paper on Identity and Access Management [55] from the Cloud Security Alliance (CSA) are good resources. There, the subject of 3PSP interfaces fits within the context of Software as a Service (SaaS).

It is worth noting that in an environment with 3PSPs that may be long-tail developers and SPs that may not be your traditional Telcos, *mutual* authentication will be a critical capability.

6.1 WS-Security

WS-Security [43] is a security framework defined use with SOAP interfaces. It involves a variety of companion specifications. Fundamentally, for authentication and authorization, WS-Security provides a means for passing security tokens of various kinds (e.g., X.509 certificates, username/password, SAML tokens) within SOAP messages.

WS-Security also specifies a way to include digital signatures of SOAP messages for assuring integrity, through the use of WC3 XML Signature [46] and a way to encrypt SOAP messages through the use of WC3 XML Encryption [47]

Looking at Figure 3, suppose a 3PSP application (3PSP App) wants to use 3PSP interface XYZ offered by a SP. For example, 3PSP interface XYZ may be a Presence interface whereby the 3PSP App may acquire from the SP presence information about end-users.

There is an initial step where the 3PSP App registers with the SP to obtain an App ID and credentials such as shared keys or PKI for use with interface XYZ.

There is a second step whereby the 3PSP App authenticates with the SP for use of the interface XYZ. The SP provides credentials to acquire an access token that can be used by the 3PSP App in the final step. In general, a 3PSP is acting on behalf of a user or a group of users for a request to the SP (e.g., the

3PSP having access to user Terry's address book kept by an SP, where then the 3PSP may have to have explicit permission from user Terry in order to access the address book). The 3PSP App needs to acquire and provide both user/goup tokens in addition to its own token according to the WS-Security specification. WS-Trust provides the Security Token Service on top of WS-Security. The Security Token Service is a well-established and well-vetted standard that can be used alongside the spectrum of 3PSP APIs types (SOAP, RESTful, SIP, etc.).

The third step involves actual use of the 3PSP interface XYZ. The 3PSP App sends a request to the SP. The request includes the access token in SOAP message, and the SOAP message may be encrypted and digitally signed. This step may be repeated over and over as the 3PSP App utilizes the 3PSP interface XYZ.

The access token may have a finite lifetime, and so the second step may need to be periodically repeated.

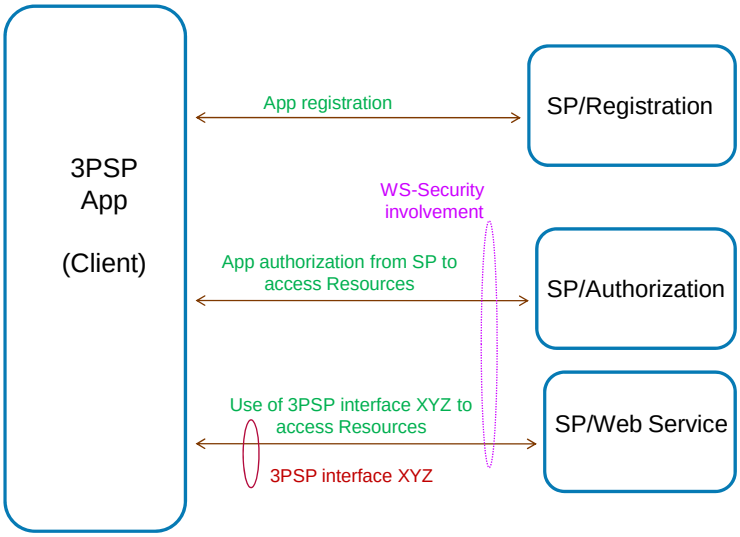

Figure 3: WS-Security Model Illustration

6.2 OAuth 2.0

OAuth 2.0 [48] is one approach that is useful especially for RESTful interfaces. It is, roughly speaking, an evolution/consolidation of OAuth 1.0 and WRAP. Looking at Figure 4, suppose a 3PSP application (3PSP App) wants to use 3PSP interface XYZ offered by a SP. For example, 3PSP interface XYZ may be a Presence interface whereby the 3PSP App may acquire from the SP presence information about end-users.

There is an initial step where the 3PSP App registers with the SP to obtain an App ID for use with interface XYZ. However, this is outside the scope of OAuth 2.0.

There is a second step where the 3PSP App requests the owner of the "Resources" (in OAuth 2.0 parlance) retrievable over interface XYZ for authorization to do just that. Depending on the nature of

the Resources, the Resource Owner could be the SP or could be an end-user. The Resource Owner provides authorization credentials to be used with the SP in the next step.

There is a third step whereby the 3PSP App authenticates with the SP and to receive an authorization code for use of the interface XYZ. After verifying the authentication code from the 3PSP, the SP provides an access token that can be used by the 3PSP App in the final step.

The fourth step involves actual use of the 3PSP interface XYZ. The 3PSP App sends a request to the SP. The request includes the access token in the HTTP Authorization header (the RESTful interface is HTTP-based, which is typical). This step may be repeated over and over as the 3PSP App utilizes the 3PSP interface XYZ.

The access token may have a finite lifetime, and so the third step may need to be periodically repeated. With OAuth 2.0, the access token in the fourth step is carried as cleartext, so typically TLS [49] would be utilized to encrypt the HTTP message. (Whereas, in contrast, OAuth 1.0 allows the access token to be digitally signed and so TLS wouldn't be needed if the desire was only to ensure the authenticity of the access token.)

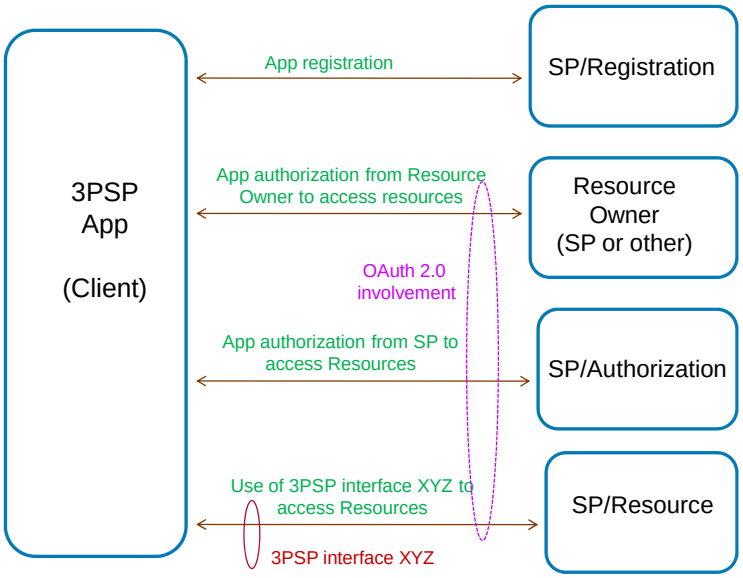

Figure 4: OAuth 2.0 Model Illustration

6.3 SAML 2.0

SAML [50] provides authentication/authorization capabilities more extensive from those of OAuth 2.0. However, OAuth2.0 provides a SAML profile to allow the exchange of a SAML assertion for an access token in the OAuth 2.0 context. SAML may be most relevant in environments where the 3PSP is an enterprise network using SOAP or SIP interfaces with the SP. SAML's purpose is especially to support single-sign-on in federated scenarios, but the size of SAML assertion is normally to big to fit in HTTP Headers in the RESTful environment.

6.4 Federation

A 3PSP application may wish to work in a common way toward multiple SPs, using a single identity and set of credentials, which lends itself to using some kind of federated IdM scheme. In that case, one can generally think of three types of entities as portrayed in Figure 5. An Identity Provider provides to 3PSP applications identities and related credentials to be used in requests from the 3PSP to the SP. When a request is sent from the 3PSP to the SP, the SP involves the Identity Provider to vouch for the 3PSP identity and credentials. Multiple 3PSPs and multiple SPs may utilize the same Identity Provider. In SAML/WS-Trust and OAuth Identity Federation contexts, the 3PSP is also called the Relying Party (RP). Also, as a simplified case, the Identity Provider and Service Provider can belong to the same entity -- i.e., the SP also provides the Identity Provider role.

Of course, SPs offering 3PSP interfaces may or may not be willing to opt in to a federation scheme.

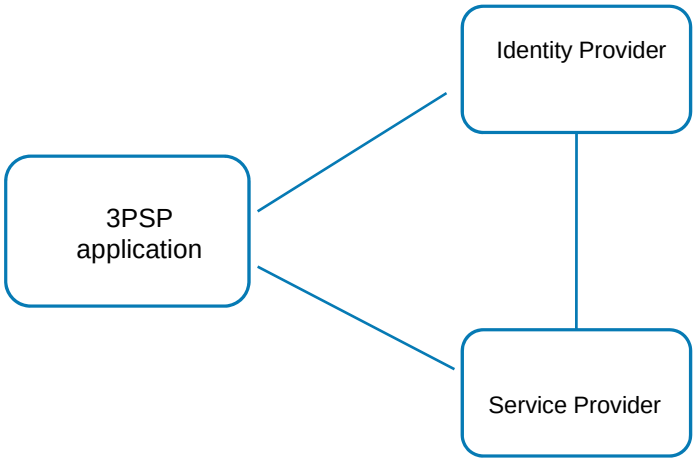

Figure 5: Identity Management Entities

A couple of the basic industry schemes that support the involvement of a separate Identity Provider are briefly highlighted below. Of course, SPs offering 3PSP interfaces may or may not be willing to involve a separate Identity Provider.

6.5 WS-Trust and WS-Federation

WS-Trust [44] is an extension of WS-Security that allows for a Security Token Service (what is labeled Identity Provider in Figure 5) to issue security tokens to the 3PSP application that can be used in requests to the SP. As an extension of WS-Trust, its protocols are SOAP. WS-Federation [45] extends the WS-Trust STS to support pseudonym, attribute, and claims-based authorization capabilities.

6.6 SAML 2.0

SAML 2.0, previously mentioned, also specifies a federated security framework. Within the scope of 3PSP interfaces security-related needs, SAML 2.0 and the WS- suite (Security, Trust, Federation, etc.) provide largely similar functionality.

There are many other aspects to federated IdM. As further examples of more recent capabilities, OpenID [51] and Information Cards [52] have been created to address needs around user-centric social networking. They are not intended for the general 3PSP-SP situation, but there may be some interoperability considerations. As one final example, the Identity Assurance Framework [53] has been specified to address needs around identifying different levels of security assurance.

7 DISTINCTION BETWEEN UE-SP INTERFACES AND 3PSP-SP INTERFACES

A natural question to ask is "what is the distinction between a UE-SP interface and a 3PSP-SP interface?"

There is no hard and fast, prescriptive distinction between the two. In theory, any functionality supported on a UE-SP interface could be supported on, and some kind of use case rationalized for, a 3PSP-SP interface or vice versa. Furthermore, business relationships or trust relationships between a SP and an End User could resemble those between the SP and 3PSPs or vice-versa.

However, in practice, there tends to be a difference in the nature of what would be appropriate toward or occur with UE versus 3PSP. Below are listed some examples that are intended to be illustrative and neither absolute nor exhaustive.

- *Termination of media sessions*. A 3PSP interface itself wouldn't terminate media sessions with End Users, whereas UE terminates media sessions.
- *Applicability of SP SEs*. A 3PSP would make use of certain network SEs, such as a Charging/Billing type SE or an Advertising Insertion/Formatting SE, that typically wouldn't make sense for a UE. Similarly, a UE may make use of a SE such as a Device Management/Diagnostics SE that typically wouldn't make sense for a 3PSP.
- *Directionality of information*. For example, a 3PSP would want to learn of UE device capabilities or location in order to provide service toward that UE, whereas the UE itself would provide information on its capabilities or location.
- *Regulatory*. Regulations for Emergency Services or Lawful Intercept may differ between 3PSPs and End Users.

It may be the case that some aspects of a *particular* interface specification may not be viable in some UE-SP settings, especially involving mobility devices, whereas they would be viable in a 3PSP-SP setting. One example would be a Parlay X API notification (such as for Terminal Location or SMS) expressed in a SOAP or RESTful binding. With a 3PSP application that resides on a statically situated server, the address to which to return notifications is not an issue. However, with a mobility device that when roaming moves its attachment point to the network, that is not achievable without some kind of alternative approach (such as using an additional push mechanism or resorting to polling).