ETSI TR 181 020 V1.1.1 (2008-03)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Exposing TISPAN NGN Services and Capabilities; Requirements, Technical Approaches and Next Steps

Reference

DTR/TISPAN-01053-NGN

Keywords

analysis, interface, interworking, OSA, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 5
Foreword 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definitions and abbreviations 11
3.1 Definitions 11
3.2 Abbreviations 11
4 Service development and deployment requirements 13
4.1 Business requirements 13
5 Technical approaches and industry efforts 14
5.1 General 14
5.2 SOA 14
5.3 Web Services 15
5.4 W3C 17
5.5 OASIS 17
5.6 WS-I 18
5.7 Liberty Alliance Project 18
5.8 OSA/Parlay 19
5.8.1 Overview of OSA/Parlay 19
5.8.2 Technical Information 19
5.8.2.1 OSA APIs 19
5.8.2.2 OSA/Parlay Framework 20
5.8.2.3 Parlay X 20
5.8.3 Specification References 21
5.9 OMA 22
5.10 ITU-T 22
6 Management Frameworks 23
6.1 General 23
6.2 NGN Management 23
6.3 TMF 23
6.3.1 NGOSS 23
6.3.1.1 Overview 23
6.3.1.2 NGOSS Views 24
6.3.1.3 Web Service / Service Orientated Architecture Implementation of NGOSS 25
6.3.2 SID 25
6.3.3 MTOSI / MTNM 25
6.4 DMTF 27
6.4.1 CIM 27
6.4.2 WS-Management 27
6.5 WSDM by OASIS 28
6.6 Service Modeling Language (SML) 28
7 Conclusions and Next Steps 28
Annex A: Sources of Further Information 30
A.1 Organization URLs 30
Annex B: Bibliography 31

History 32

Intellectual Property Rights

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

Introduction

The focus of the present Technical Report is on identifying the emerging requirements for exposing NGN services and capabilities and on summarizing some of the technologies for accomplishing the goal.

At the current time, NGN services and capabilities are being exposed by different technological means. There have been a number of causes for using a wide range of technologies. The most notable include:

- Historical usage of certain protocols in certain networks.
- Varying considerations in protocols' timing, bandwidth consumptions, and extensibility.
- Different security requirements.

The drives and imperatives behind the present effort include:

- NGN (including IMS) is on its way to become the global reference architecture encompassing different networks and technologies.
- Realization that in competitive reality, the design, implementation, integration and the deployment stages of both NGN and external to NGN services and applications continue to shorten, become more automated and of ad-hoc nature.
- The NGN boundaries, many times in the past defined by regulatory rules and assumptions, are a moving target and vary greatly worldwide.

As a result, the present Technical Report identifies new emerging requirements and, in the same time, analyzes the relevance of some previous working assumptions.

1 Scope

The present document:

- Identifies requirements for flexible and agile service development and deployment for a multi-provider and multivendor environment.
- Surveys the technical approaches available (e.g. Web services) to expose the functionalities and identify any possible impacts in the evolution of the TISPAN architecture and management.
- Surveys the existing industry efforts in this domain (e.g. TISPAN/NGN (protocols), Parlay/X, OSA, OMA, ITU-T, OASIS, WS-I, W3C, among others) and relationship with management frameworks (e.g. DMTF/TMF)
- Identifies next steps.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

[1] ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

[2] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[3] W3C: "Simple Object Access Protocol (SOAP)".

NOTE: Available at http://www.w3.org/TR/soap/.

[4] W3C: "Web Services Description Language (WSDL)".

NOTE: Available at http://www.w3.org/TR/wsdl.

[5] W3C: "Web Services Architecture".

NOTE: Available at http://www.w3.org/TR/ws-arch/.

[6] OASIS (2004-10-19): "Universal Description Discovery & Integration (UDDI)", Version 3.0.2 UDDI Specification Technical Committee Draft,.

NOTE: Available at http://uddi.org/pubs/uddi-v3.htm.

[7] OASIS: "Web Services Security (WS-Security)".

NOTE: Available at http://docs.oasis-open.org/wss/v1.1/.

[8] OASIS: "Web Services Secure Conversation (WS-SecureConversation)".

NOTE: Available at http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.3/ws-secureconversation.pdf.

[9] OASIS: "Web services Trust (WS-Trust)".

NOTE: Available at http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/ws-trust.pdf.

[10] OASIS: "Web Services Security Policy (WS-SecurityPolicy)".

NOTE: Available at http://www.oasis-open.org/committees/download.php/15979/oasis-wssx-ws-securitypolicy-1.0.pdf.

[11] IBM: "Web Services Federation Language (WS-Federation)" Version 1.1, December 2006. (c) 2001-2006 BEA Systems, Inc., BMC Software, CA, Inc., International Business Machines Corporation, Layer 7 Technologies, Microsoft Corporation, Inc., Novell, Inc. and VeriSign, Inc. All rights reserved.

NOTE: Available at http://www.ibm.com/developerworks/library/specification/ws-fed/.

[12] OASIS: "Web Services Reliable Messaging (WS-ReliableMessaging)".

NOTE: Available at http://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.1-spec-os-01.pdf.

[13] OASIS: "Web Services Atomic Transaction (WS-AtomicTransaction)".

NOTE: Available at http://docs.oasis-open.org/ws-tx/wstx-wsat-1.1-spec.pdf.

[14] OASIS: "Web Services Coordination (WS-Coordination)".

NOTE: Available at http://docs.oasis-open.org/ws-tx/wstx-wscoor-1.1-spec.pdf.

[15] OASIS: "Web Services Business Activity (WS-BusinessActivity)".

NOTE: Available at http://docs.oasis-open.org/ws-tx/wstx-wsba-1.1-spec-cd-01.pdf.

[16] W3C Recommendation (2005-01-25): "SOAP Message Transmission Optimization Mechanism (MTOM)".

NOTE: Available at http://www.w3.org/TR/soap12-mtom/.

[17] W3C: "Web Services Addressing (WS-Addressing)".

NOTE: Available at http://www.w3.org/Submission/ws-addressing/.

[18] W3C (2007-09-04): "Web Services Policy 1.5 - Framework", W3C Recommendation.

NOTE: Available at http://www.w3.org/TR/ws-policy/.

[19] WS-I (2006-04-10): "Basic Profile", Version 1.1.

NOTE: Available at http://www.ws-i.org/Profiles/BasicProfile-1.1.html.

[20] WS-I (2007-03-28): "Basic Profile", Version 1.2.

NOTE: Available at http://www.ws-i.org/Profiles/BasicProfile-1.2.html.

[21] WS-I (2004-08-24): "Simple SOAP Binding Profile", Version 1.0.

NOTE: Available at http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0-2004-08-24.html.

[22] WS-I (2007-10-25): "Basic Profile", Version 2.0.

NOTE: Available at http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile.

[23] WS-I (2007-03-30): "Basic Security Profile", Version 1.0.

NOTE: Available at http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html.

[24] WS-I (2006-01-20): "REL Token Profile", Version 1.0.

NOTE: Available at http://www.ws-i.org/Profiles/RELTokenProfile-1.0.html.

[25] WS-I (2006-01-20): "Kerberos Token Profile", Version 1.0.

NOTE: Available at http://www.ws-i.org/Profiles/KerberosTokenProfile-1.0.html.

[26] WS-I (2006-01-20): "SAML Token Profile", Version 1.0.

NOTE: Available at http://www.ws-i.org/Profiles/SAMLTokenProfile-1.0.html.

[27] WS-I (2006-11-06): "RSP WG Usage Scenarios", Working Group Draft, Version 1.

NOTE: Available at http://www.ws-i.org/profiles/rsp-scenarios-1.0.pdf.

[28] Liberty Alliance: "Liberty ID-WSF Data Services Template Specification", Version 2.0.

NOTE: Available at http://www.projectliberty.org/liberty/content/download/1068/7307/file/liberty-idwsf-dst-v2.0.pdf.

[29] Liberty Alliance: "Liberty Alliance ID-WSF 2.0" Specifications including Errata v1.0 Updates.

NOTE: http://www.projectliberty.org/liberty/content/download/3433/22925/file/liberty-idwsf-2.0-20070709.zip.

[30] IETF RFC 3261: "SIP: Session Initiation Protocol".

[31] Void.

[32] ETSI ES 204 915 (all parts): "Open Service Access (OSA); Application Programming Interface (API)".

[33] Void.

[34] ETSI ES 202 504 (all parts): "Open Service Access (OSA); Parlay X Web Services".

[35] OMA: "OMA Web Services Enabler Release V1.0".

NOTE: Available at http://www.openmobilealliance.org/release-program/owser-v10.html.

[36] WS-I (2004-04-16): "Basic Profile Version 1.0".

NOTE: Available at http://www.ws-i.org/Profiles/BasicProfile-1.0.html.

[37] ITU-T Recommendation Y.2201: "NGN Release 1 Requirements".

[38] ITU-T Draft Recommendation: "Open service environment capabilities for NGN applications and user services (Y.ngn-openenv)".

[39] ITU-T Recommendation Y.2232 (January 2008): "NGN convergence service model and scenario using Web Services".

[40] DMTF CIM: "Common Information Model".

NOTE: Available at http://www.dmtf.org/spec/cims.html.

[41] TM Forum: "NGOSS Shared Information/Data (SID) model".

NOTE: Available at http://www.tmforum.org/SIDDatasheets/SIDDatasheet/32723/article.html.

[42] ETSI TS 188 001: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN management; Operations Support Systems Architecture".

[43] TM Forum: "eTOM Solution Suite (GB921) Release 7.0".

NOTE: Available at http://www.tmforum.org/page32701.aspx.

[44] ITU-T Recommendation M.3050: "Enhanced Telecommunications Operations Map".

[45] TM Forum: "NGOSS Release 7.0 SID Solution Suite (GB922 & GB926)".

NOTE: Available at http://www.tmforum.org/page32555.aspx.

[46] TMForum: "NGOSS Architecture Technology Neutral Specification Distribution Transparency Framework Services - TMF053F v1.0".

NOTE: http://www.tmforum.org/browse.aspx?catID=1157&linkID=28756.

[47] TMForum: "NGOSS Compliance/Conformance Strategy GB940 v6.1 r6.0".

NOTE: Available at http://www.tmforum.org/page31893.aspx.

[48] TMForum: "The ICON Catalyst projects".

NOTE: Available at http://www.tmforum.org/browse.aspx?catID=2595&linkID=31223.

[49] TMForum: "The NGOSS Cookbook projects".

NOTE: Available at http://www.tmforum.org/browse.aspx?catID=1608&linkID=28765.

[50] TMForum: "Multi-Technology Operations System Interface (MTOSI) Release 1.0".

NOTE: Available at http://www.tmforum.org/page30792.aspx.

[51] ITU-T Recommendation M.3170.0: "Multi-Technology Network Management MTNM".

[52] Sun 2002-04-12: "JavaTM Message Service Specification ", Version 1.1.

NOTE: Available at http://java.sun.com/products/jms/.

[53] TMForum: "TMF608 Version 3.4 Information Agreement for MTNM Release 3.5".

NOTE: Available at http://www.tmforum.org/browse.aspx?catID=4359&linkID=32958.

[54] ITU-T Recommendation G.805: "Generic functional architecture of transport networks".

NOTE: Available at http://www.itu.int/rec/T-REC-G.805/en.

[55] ITU-T Recommendation G.809: "Functional architecture of connectionless layer networks".

NOTE: Available at http://www.itu.int/rec/T-REC-G.809/en.

[56] IETF RFC 2616: "HTTP Hypertext Transfer Protocol -- HTTP/1.1".

NOTE: Available at http://tools.ietf.org/html/rfc2616.

[57] OMG (Object Management Group) (2004-03-12): "Common Object Request Broker Architecture: Core Specification (CORBA)", Version 3.0.3.

NOTE: Available at http://www.omg.org/docs/formal/04-03-12.pdf.

[58] Distributed Management Task Force DSP0226 (2006-04-05): "Web Services for Management (WS-Management)", Version: 1.0.0a.

NOTE: Available at http://www.dmtf.org/standards/published_documents/DSP0226.pdf.

[59] Distributed Management Task Force DSP0201 (2007-09-25): "Specification for the Representation of CIM in XML", Version 2.3.0.

NOTE: Available at http://www.dmtf.org/standards/published_documents/DSP0201-2.3.0.pdf

[60] IETF RFC 2817: "Upgrading to TLS Within HTTP/1.1".

NOTE: Available at http://tools.ietf.org/html/rfc2817.

[61] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

NOTE: Available at http://tools.ietf.org/html/rfc2617.

[62] IETF RFC 4120: "The Kerberos Network Authentication Service (V5)".

NOTE: Available at http://tools.ietf.org/html/rfc4120.

[63] HP, IBM, Intel and Microsoft whitepaper (2006-03-15): "Toward Converging Web Service Standards for Resources, Events, and Management", Version 1.0.

NOTE: Available at http://download.boulder.ibm.com/ibmdl/pub/software/dw/webservices/Harmonization_Roadmap.pdf.

[64] BEA, BMC, Cisco, Dell, EMC, HP, IBM, Intel, Microsoft, and Sun (2006-07-25): "Service Modeling Language, Draft Specification", Version 0.5.

NOTE: Available at http://www.serviceml.org/SML-200607.pdf.

[65] ETSI TS 132 150: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Telecommunication management; Integration Reference Point (IRP) Concept and definitions (3GPP TS 32.150 version 7.2.0 Release 7)".

[66] ETSI TS 122 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1 (3GPP TS 22.228 version 8.3.0 Release 8)".

[67] IETF RFC 3460: "Policy Core Information Model (PCIM) Extensions".

[68] IETF RFC 2778: "A Model for Presence and Instant Messaging".

[69] ETSI TS 129 198 (V7.1.1): "Universal Mobile Telecommunications System (UMTS); Open Service Access (OSA) Application Programming Interface (API); (3GPP TS 29.198 Release 7)".

[70] ETSI ES 203 915: "Open Service Access (OSA); Application Programming Interface (API)".

[71] ETSI ES 202 391: "Open Service Access (OSA); Parlay X Web Services".

[72] ETSI TS 129 199: "Universal Mobile Telecommunications System (UMTS); Open Service Access (OSA); Parlay X web services; (3GPP TS 29.199 version 7.4.1 Release 7)".

[73] ETSI TS 122 127: "Universal Mobile Telecommunications System (UMTS); Service requirement for the Open Services Access (OSA); Stage 1 (3GPP TS 22.127 version 7.1.0 Release 7)".

[74] ETSI EG 201 988: "Services and Protocols for Advanced Networks (SPAN); Service Provider Access Requirements (SPAR); Open Service Access for API requirements".

[75] ETSI TS 123 198: "Universal Mobile Telecommunications System (UMTS); Open Service Access (OSA); Stage 2 (3GPP TS 23.198 version 7.3.0 Release 7)".

[76] ETSI TR 102 397: "Open Service Access (OSA); Mapping of Parlay X 2 Web Services to Parlay/OSA APIs".

[77] ETSI TS 129 198 (V6.3.0): "Universal Mobile Telecommunications System (UMTS); Open Service Access (OSA) Application Programming Interface (API); (3GPP TS 29.198 Release 6)".

[78] ETSI TS 129 199 (V6.1.0): "Universal Mobile Telecommunications System (UMTS); Open Service Access (OSA); Parlay X web services (3GPP TS 29.199 Release 6)".

[79] ETSI TS 123 127: "Universal Mobile Telecommunications System (UMTS); Virtual Home Environment (VHE)/Open Service Access (OSA) (3GPP TS 23.127 version 6.1.0 Release 6)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 180 000 [1] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP CT5	3GPP Core Network & Terminals Working Group 5 (Open Service Access)
3GPP	3rd Generation Partnership Project
API	Application Program Interface
AS	Application Server
ATM	Asynchronous Transfer Mode
BP	Basic Profile
BPEL	Business Process Execution Language
BSP	Basic Security Profile
CAMEL	Customized Application for Mobile Enhanced Logic
CAPEX	CAPital EXpenditure
CDG	CDMA Development Group
CDMA	Code Division Multiple Access
CIM	Common Information Model
CIMOM	CIM Object Manager
CLP	Command Line Protocol
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off The Shelf
CRUD	Create Read Update Delete
CSAIL	Computer Science and Artificial Intelligence Laboratory
DCOM	Distributed Component Object Model
DDP	Document Delivery Package
DMTF	Distributed Management Task Force
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVB	Digital Video Broadcasting
EML	Element Management Layer
EM-NM	Element Management - Network Management
ERCIM	European Research Consortium for Informatics and Mathematics
eTOM™	enhanced Telecom Operations Map
ETSI	European Telecommunications Standards Institute
GPRS	General Packet Radio Service
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
ICON	Implementing Contract-based services in NGN

ID	Internet Draft
IDL	Interface Definition Language
ID-WSF	IDentity Web Services Framework
IETF	Internet Engineering Task Force
IIOP	Internet Inter ORB Protocol
IM	Instant Messaging
IMS	Internet protocol Multimedia Subsystem
IOC	Information Object Class
IP	Internet Protocol
IRP	Integration Reference Point
ISC	IP multimedia Subsystem Service Control
IT	Information Technology
ITU-T	ITU - Telecom sector
IVR	Interactive Voice Response
J2EE	Java™ 2 Platform, Enterprise Edition
J2SE	Java™ 2 Standard Edition
JCP	Java Community Process
JMS	Java Messaging Service
LAI	Location Area Identifier
MIT	Massachusetts Institute of Technology
MMCC	Multi-Media Call Control
MPA	Motion Picture Association
MPCC	Multi-Party Call Control
MPLS	Multi-Protocol Label Switching
MQ	Message Queue
MTNM	Multi-Technology Network Management
MTOM	Messsage Transmission Optimization Mechanism
mTOP	multi Technology OSS Program
MTOSI	Multi-Technology Operation Systems Interface
MTOSSJ	Multi-Technology Operation Support Systems thru Java
NASS	Network Attachment SubSystem
NGN	Next Generation Network
NGOSS	Next Generation Operations Systems & Software
NML	Network Management Layer
OASIS	Organization for the Advancement of Structured Information Standards
OMA	Open Mobile Alliance
OPEX	OPErational EXpenditure
ORB	Object Request Broker
OSA	Open Service Architecture
OSE	Open Service Environment
OSS	Operations Support Systems
OSS/J	OSS through Java
PAM	Presence and Availability Management
PDH	Plesiochronous Digital Hierarchy
PDP	Packet Data Protocol
PON	Passive Optical Network
QoS	Quality of Service
RACS	Resource and Admission Control Subsystem
REL	Rights Expression Language
REST	REpresentational State Transfer
RFC	Request For Comments
RFI	Request For Information
RIAA	Recording Industry Association of America
ROI	Return On Investment
RPC	Remote Procedure Call
RSP	Reliable Secure Profile
SAML	Security Assertion Markup Language
SDH	Synchronous Digital Hierarchy
SDO	Standards Development Organization
SID	Shared Information/Data model
SIP	Session Initiation Protocol
SMASH	Systems Management Architecture for Server Hardware

SML	Service Management Layer
SML	Service Modelling Language
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNIA	Storage Networking Industry Association
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SONET	Synchronous Optical NETwork
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TM	TeleManagement
TMF	TeleManagement Forum
TNA	Technology Neutral Architecture
TS	Technical Specification
UAProf	User-Agent Profile
UDDI	Universal Description Discovery and Integration
UML	Unified Modelling Language
W3	World Wide Web
W3C	World Wide Web Consortium
WAP	Wireless Access Protocol
WBEM	Web Based Enterprise Management
WDM	Wavelength Division Multiplexing
WiMAX	Worldwide Interoperability for Microwave ACCess
WLAN	Wireless Local Area Network
WS	Web Services
WS-*	All Web Services Specifications
WSDL	Web Services Description Language
WSDM	Web Services Distributed Management
WSF	Web Services Framework
WS-I	Web Services Interoperability Organization
WS-RX WG	Web Services Reliable eXchange Working Group
WS-SX WG	Web Services Secure eXchange Working Group
WS-TX WG	Web Services Transaction eXchange Working Group
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol
XSD	XML Schema Definition

4 Service development and deployment requirements

In competitive reality, the design, implementation, integration and the deployment stages of both NGN [2] and external to NGN services and applications continue to shorten, become more automated and of ad-hoc nature. The resultant emerging requirements for flexible and agile service development and deployment for a multi-provider and multi-vendor environment are presented in the clauses below.

4.1 Business requirements

Communication Service Providers are investing in new networking technologies driven by the need to drive down CAPEX and OPEX costs. Moreover industry changes are driving Communications service providers towards agile rapid and economical provision of new service in order to drive up their top-line revenues.

The Business drivers include:

- Collision of IT Media and Telecoms industry where modern IP networks and applications running on them are replacing traditional solutions.
- Regulatory changes.
- Falling margins on traditional Telco products.

Requirement 1: Service Providers need to use Web Service and XML based solutions for management interfaces to control the TISPAN functional entities: Core IMS, RACS and NASS [2].

Rationale: Modern IT platforms are moving to XML and web service technologies and these are the essential foundation for Service Orientated Architecture (SOA). SOA is the method that has mainstream IT vendor endorsement for moving to agile software development. SOA architecture uses the find-bind-execute mechanism that allows dynamic re-use of software components and applications, of which management application are an example.

Requirement 2: Service providers need to converge on the main stream Web Service specification stacks that are being developed and delivered by the IT industry especially the main IT platform vendors.

Rationale: There is a very disparate set of Web Service standards and Service Providers can only afford to target one Web Services platform as they will be used for both management applications and the IMS Applications Environment Platform. These WS platforms need to interoperate Out of the Box.

Requirement 3: ETSI standards need to demonstrate a roadmap for convergence on main stream WS and XML standards from OASIS and W3C

Rationale: The IT industry stakeholders are working in OASIS and W3C to agree service standards stack that will be used to support IT Servers and virtualized Computing and Storage. The alternative of ETSI defining its own WS stack in isolation from OASIS and W3C will be counter productive since telecom is only one relative small part of the overall IT marketplace.

5 Technical approaches and industry efforts

5.1 General

This clause provides an overview of the current technical approaches and the latest industry efforts applicable for exposure the identified NGN functionalities. The clause also examines the impacts they may have on the evolution of the TISPAN architecture and management.

5.2 SOA

Service orientation is an approach to defining distributed, interface-oriented systems that deliver functionality as services. These services are accessed through the interfaces they expose.

A Service Oriented Architecture (SOA) is a software architecture of services, policies, practices and frameworks in which components can be reused and repurposed rapidly in order to achieve shared and new functionality. This enables rapid and economical implementation in response to new requirements thus ensuring that services respond to perceived user needs.

SOA uses the object-oriented principle of encapsulation in which entities are accessible only through interfaces and where those entities are connected by well-defined interface agreements or contracts.

SOA principles require that relationships between Service Interfaces and Service Interface Consumers can be established dynamically at run time to perform activities in support of requirements. However, for early deployment reasons, this relationship may initially also be established manually by configuration rather than by the services themselves at run time.

The following guiding principles define the ground rules for development, maintenance, and usage of the SOA:

- Reuse, granularity, modularity, composition, componentization, and interoperability.
- Compliance to standards (both common and industry-specific).
- Services identification and categorization, provisioning and delivery, monitoring and tracking.

The following specific architectural principles for design and service definition focus on specific themes that influence the intrinsic behaviour of a system and the style of its design:

- Service Encapsulation.
- Service Loose coupling: Services maintain a relationship that minimizes dependencies and only requires that they maintain an awareness of each other.
- Service contract: Services adhere to a communications agreement, as defined collectively by one or more service description documents.
- Service abstraction: Beyond what is described in the service contract, services hide logic from the outside world.
- Service reusability: Logic is divided into services with the intention of promoting reuse.
- Service composition: Collections of services can be coordinated and assembled to form composite services.
- Service autonomy: Services have control over the logic they encapsulate.
- Service statelessness: Services minimize retaining information specific to an activity.
- Service discoverability: Services are designed to be outwardly descriptive so that they can be found and assessed via available discovery mechanisms.

SOA is not tied to a specific technology. It may be implemented using a wide range of technologies, including REST, RPC, DCOM, ORB or Web Services but also without any of these protocols.

5.3 Web Services

In recent years, the imperative to connect people, information, and processes has changed the way software is being developed. Successful IT systems increasingly require interoperability across platforms and flexible services that can easily evolve over time. This has led to the prevalence of XML as the universal language for representing and transmitting structured data that is independent of programming language, software platform, and hardware.

Building on the broad acceptance of XML, Web services are applications that use standard transports, encodings, and protocols to exchange information. With broad support across vendors and businesses, Web services enable computer systems on any platform to communicate over corporate intranets, extranets, and across the Internet with support for end-to-end security, reliable messaging, distributed transactions, and more.

Web services are based on a core set of standards that describe the syntax and semantics of software communication: XML provides the common syntax for representing data; the Simple Object Access Protocol (SOAP) [3] provides the semantics for data exchange; and the Web Services Description Language (WSDL) [4] provides a mechanism to describe the capabilities of a Web service. Additional specifications, collectively referred to as the WS-* architecture [5], define functionality for Web services discovery, event handling, attachments, security, reliable messaging, transactions, and management.

The most important attribute of the WS-* architecture [5] is composition. Protocol composition enables incremental development of Web services solutions only as individual requirements (such as security, reliable messaging, attachments, discovery, etc.) are needed. In isolation, each of these requirements solves an elemental need. In composition, they address higher-level functionality commonly required by distributed applications. As such, the WS-* specifications can be used either independently or in combination with one another. This eliminates the complexity and overhead associated with specifications that attempt to define multiple capabilities or are tightly coupled with other specifications. It also enables developers to apply only the specific functionality needed to solve the immediate need. As new application requirements arise, new specifications can be authored without compromising backwards compatibility.

The high level Web services protocols stack is presented in figure 1.

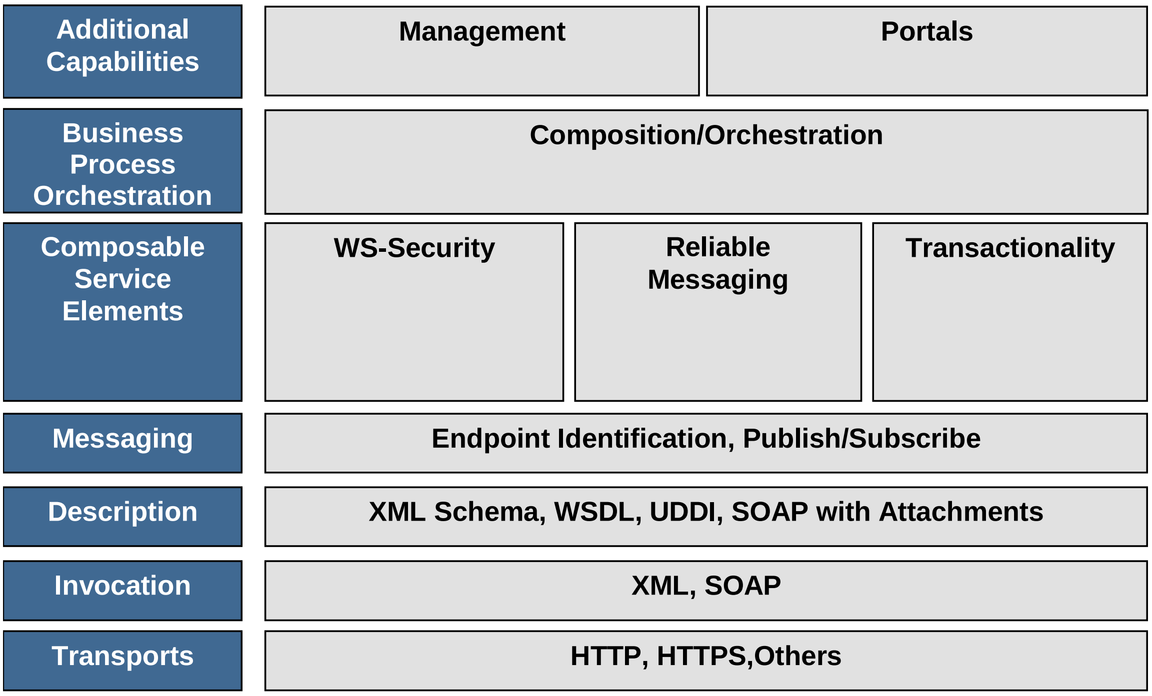

Figure 1: The Web services protocols stack (by WS-I)

Below is a partial list of the commonly used Web services specifications:

- SOAP: An XML-based, extensible message envelope format, with "bindings" to underlying protocols (e.g., HTTP, SMTP and XMPP) [3].
- WSDL: An XML format that allows service interfaces to be described, along with the details of their bindings to specific protocols. Typically used to generate server and client code, and for configuration [4].
- UDDI: A protocol for publishing and discovering metadata about Web services, to enable applications to find Web services, either at design time or runtime [6].
- WS-Security [7], WS-SecureConversation [8]: WS-Trust [9] and WS-SecurityPolicy [10], WS-Federation [11] - enable the trusted exchange of single or multiple SOAP messages, potentially across multiple trust domains.
- WS-ReliableExchange [12]: A protocol for reliable messaging between two Web services.
- WS-AtomicTransaction [13]: WS-Coordination [14] and WS-BusinessActivity [15]: Protocols for coordinating the outcome of distributed application actions.

Broad vendor agreement on standards and proven interoperability have set Web services apart from integration technologies of the past. During the ongoing process of interoperability and standardization, multiple industry and standardization bodies have driven efforts to create both horizontal as well as industry-specific Web services standards.

Typically, the lower protocols in the "Web services stack" are standardized at W3C, while the higher application-oriented protocols are standardized at OASIS. Additionally, WS-I develops profiles, sample applications and test tools that "glue" the specifications together and further promote Web services interoperability.

5.4 W3C

The World Wide Web Consortium (W3C) is the main international standards organization for the World Wide Web (W3). The Consortium is jointly administered by the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) in the USA, the European Research Consortium for Informatics and Mathematics (ERCIM) (in Sophia Antipolis, France), and Keio University (in Japan).

Among the relevant Web services W3C Standards are SOAP, WSDL, MTOM, WS-Addressing, WS-Policy, XML, XML Information Set, and XML Schema.

- SOAP [3].
- WSDL [4].
- MTOM (SOAP Message Transmission Optimization Mechanism) [16]: Describes the mechanism for optimizing the transmission and/or wire format of a SOAP message by selectively re-encoding portions of the message while still presenting an XML Infoset to the SOAP application.
- WS-Addressing [17]: Provides transport-neutral mechanisms to address Web services and messages. Defines XML elements to identify Web service endpoints and to secure end-to-end endpoint identification in messages. This specification enables messaging systems to support message transmission in a transport-neutral manner through networks that include processing nodes such as endpoint managers, firewalls, and gateways.
- WS-Policy [18]: Defines a base set of constructs that can be used and extended by other Web services specifications to describe a broad range of service requirements, preferences, and capabilities.

See annex A for URL Links to Websites.

5.5 OASIS

The Organization for the Advancement of Structured Information Standards (OASIS) is a global consortium that is engaged with the development, convergence and adoption of e-business and Web Service standards.

Among specifications under development by OASIS technical committees and are potentially relevant to the topic of the present document are:

- WS-Security [7]: Defines how to use XML Encryption and XML Signature in SOAP to secure message exchanges. It also defines various XML security token formats for use with the WS-Security protocol, including Username/Password, X.509, SAML, Kerberos, and REL (Rights Expression Language) Token Profiles.
- WS-ReliableMessaging [12] (WS-RX WG): A protocol for reliable message exchange using Web services.
- WS-AtomicTransaction [13], WS-Coordination [14] and WS-BusinessActivity [15] (WS-TX WG): Protocols for coordinating the outcome of distributed application actions through atomic and/or long-running transactions.
- WS-SecureConversation [8], WS-Trust [9] and WS-SecurityPolicy [10] (WS-SX WG): Define WS-Security extensions and policies to enable the trusted exchange of multiple SOAP messages.
- WS-Federation [11]: Defines mechanisms that are used to enable identity, attribute, authentication, and authorization federation across different trust realms.

See Annex A for URL Links to Websites.

As of November 2007, OASIS is considering to establish a new "Telecom Member Section" to provide a focus on telecoms services in a SOA framework. Its target is to address the technical challenges to providing robust and scalable time-sensitive services in a SOA environment, including issues related to performance and others specifically associated with service orchestration.

5.6 WS-I

Web Services Interoperability (WS-I) is an open industry organization with member companies throughout North America, South America, Europe, Asia and the Pacific Rim. WS-I is chartered to promote Web services interoperability across platforms, operating systems and programming languages. Its goal is "to provide guidance, recommended practices and supporting resources for "generic protocols for the interoperable exchange of messages between Web services. In this context, "generic protocols" are protocols that are independent of any action indicated by a message, other than those actions necessary for its secure, reliable and efficient delivery, and "interoperable" means suitable for multiple operating systems and multiple programming languages."

Among the important WS-I deliveries are:

- The Basic Profile (BP) 1.1 [19] provides interoperability guidance for a core set of non-proprietary Web services specifications, such as SOAP [3], WSDL [4] and UDDI [6], along with interoperability-promoting clarifications and amendments to those specifications.
- The Basic Profile (BP) 1.2 (work in progress) [20] builds on Basic Profile 1.1 by incorporating Basic Profile 1.1 errata, requirements from Simple SOAP Binding Profile 1.0 [21], and adding support for WS-Addressing [17] and MTOM [16].
- The Basic Profile (BP) 2.0 (work in progress) [22] builds on Basic Profile 1.2 by adding support for SOAP 1.2.
- The Basic Security Profile (BSP) [23] provides guidance on the use of WS-Security and the REL [24], Kerberos [25], SAML [26], UserName and X.509 security token formats.
- The Reliable Secure Profile (RSP) [27] provides guidance on using WS-ReliableMessaging [12] with WS-SecureConversation [8].

See annex A for URL Links to Websites.

5.7 Liberty Alliance Project

The Liberty Alliance Project was formed to establish an open standard for federated network identity. As such, the Liberty Alliance Data Service Template [28] and Liberty Web Services Framework (Liberty ID-WSF 2.0) [29] specifications propose a framework for web services that offer access to data in general and enable to expose user information in a secured and privacy enabled way.

Liberty Alliance ID-WSF 2.0 specifications [29] are composed of the following specifications:

- Liberty ID-WSF2.0 security and policy overview.
- Discovery service specification.
- Soap binding specification.
- Security mechanisms specification.
- Interaction service specification.
- Data service template.

The Data Service Template [28] defines:

(1) abstract definitions about messages that are sent and received by the web service; and

(2) guidelines regarding the structure of the data offered through the service. The Liberty Alliance Data Service Template specification offers a set of XML schemas with placeholders (for data types) that are filled based on the nature of the data offered by the data service.

The Liberty Alliance project has also defined a set of APIs to expose user related information with privacy, such as a location API, a presence API, a contact book API, a personal profile API, a messaging API, etc.

See annex A for URL Links to Websites.

5.8 OSA/Parlay

5.8.1 Overview of OSA/Parlay

OSA (Open Service Access) [32] is a set of APIs which enable network operator or 3rd party applications to access telecoms network functionality. The OSA APIs were originally developed by The Parlay Group, and today the terms OSA and Parlay are synonymous - often the term OSA/Parlay is used to indicate this. The OSA/Parlay APIs are (generally) network agnostic, and raise the level of abstraction compared with SIP [30] or IN-based applications.

OSA/Parlay is standardized in a joint activity between ETSI TISPAN's OSA Project, 3GPP CT5 and The Parlay Group. OSA/Parlay specifications are published by ETSI, and are also part of 3GPP's specification set. OSA/Parlay is integrated into the 3GPP IMS architecture, and is also referred to by 3GPP2. The intention of OSA/Parlay is to have the same APIs used for applications in both fixed and mobile networks.

5.8.2 Technical Information

In the IMS architecture [66], the OSA Service Capability Server is integrated via the ISC and Sh interfaces, as the IMS Application Server (AS) function. The OSA Service Capability Server provides the OSA API interface to the OSA Application Server.

The OSA/Parlay APIs are available at two different levels of abstraction: the full-function base OSA/Parlay APIs [32], developed initially, and the more abstracted Parlay X APIs [34].

5.8.2.1 OSA APIs

The base OSA/Parlay APIs [32] are a set of APIs which offer access to a full set of telecoms network functionality. The APIs are defined using UML, and a choice of technical realizations is provided as part of the specifications

- Corba, using IDL code provided in the specifications.
- Web Services, using the WSDL code provided.
- J2SE, using the J2SE code provided.
- J2EE, using either the J2EE Local or J2EE Remote code provided.

The OSA/Parlay specifications [32] include the following APIs (Service Capabilities):

- Generic Call Control (Part 4, Sub-Part 2):
  simple 2-party call control, no call leg manipulation
- Multi-Party Call Control (Part 4, Sub-Part 3):
  more complex, providing multi-party and leg manipulation features
- Multi-Media Call Control (Part 4, Sub-Part 4):
  adds media management to MPCC
- Conference Call Control (Part 4, Sub-Part 5):
  adds conference management to MPCC or MMCC
- User Interaction (Part 5):
  call-based and non-call based, for IVR type applications, also for message-based (SMS) interaction with users
- User Location (Part 6):
  single shot, triggered or periodic user location information reports, including provision of geodetic co-ordinates
- User Location Camel (Part 6):
  as User Location, but also providing Cell ID or LAI location information, as available in CAMEL
- User Location Emergency (Part 6):
  location information reports suitable for North American emergency location services

- User Status (Part 6):
  user status information reports, triggered or single-shot: reachability, terminal type, connection type and status, roaming status etc.

- User Binding (Part 6):
  triggered notification of user requests to bind to a network.

- Terminal Capabilities (Part 7):
  reports terminal capabilities, or changes of capabilities. Uses WAP UAProf format.

- Data Session Control (Part 8):
  user data session (e.g. GPRS PDP context) management.

- Account Management (Part 11):
  basic account management: balance reports, account updates, voucher management.

- Charging (Part 12):
  time or volume based charging, using units or currency amounts. Offers direct credit or debit to/from accounts, charge reservation, rating, split charging.

- Policy Management (Part 13):
  access to a policy management system which follows RFC 3460 [67] Policy Core Information Model

- Presence and Availability Management (Part14):
  management and sharing of presence and availability information. Based on PAM Forum specifications and using concepts from RFC 2778 [68].

- Multi-Media Messaging (Part 15):
  comprehensive messaging API, supporting many messaging types (e.g. SMS, IM, e-mail) in session and non-session based communication. Offers mailbox access.

- Service Broker (Part 16):
  simple API permitting an application to register with a service broker function.

Two further API specifications are also available, but are considered obsolete: Generic Messaging and Connectivity Management (QoS management).

5.8.2.2 OSA/Parlay Framework

The OSA/Parlay APIs [32] include a Framework specification (Part 3), which provides APIs for access and authentication of applications, for management of service contracts, and for application access to Service Capabilities provided by the network. The Framework also provides lifecycle management of Service Capabilities, and load and fault management.

As with the other OSA/Parlay APIs, the Framework has realizations provided in IDL, WSDL, J2SE and J2EE.

5.8.2.3 Parlay X

The Parlay X APIs [34] are written as an abstraction of the OSA/Parlay APIs. Rather than offering the rich and detailed functionality required by developers of telecoms applications, they offer discreet APIs with few methods, stateless behaviour, single-shot methods more suited to the needs of web services developers, or developers of non-telecoms applications who need to add some basic telecoms-related functionality to their application.

The Parlay X APIs are only available as Web Services APIs. While Parlay X APIs map onto functionality provided in the base OSA/Parlay APIs, Parlay X can be deployed independently of the base APIs.

The Parlay X 3.0 specifications [34] include the following APIs:

- 3rd Party Call (Part 2).

- Call Notification (Part 3).

- Short Messaging (Part 4).

- Multimedia Messaging (Part 5).
- Payment (Part 6).
- Account Management (Part 7).
- Terminal Status (Part 8).
- Terminal Location (Part 9).
- Call Handling (Part 10).
- Audio Call (Part 11).
- Multimedia Conference (Part 12).
- Address List Management (Part 13).
- Presence (Part 14).
- Message Broadcast (Part 15).
- Geocoding (Part 16).
- Application-driven QoS (Part 17).
- Device Management (Part 18).
- Multimedia Streaming Control (Part 19).
- Multimedia Multicast Control (Part 20).

5.8.3 Specification References

ETSI publishes the master specifications of the APIs. The Parlay Group point to this published ETSI specification instead of re-publishing it. 3GPP maintain their own specifications, which have the same structure as the ETSI specification. Each part of the 3GPP specification is a subset or a copy of the ETSI specification.

The OSA/Parlay APIs are published by ETSI as ES 20x 915 series . These correspond to 3GPP TS 29.198 [69] series of specifications. The 3GPP specifications are a subset of the ETSI specifications - they contain no additional functionality, but some of the functionality in the ETSI series of specifications is not available in the 3GPP series, due to differing scopes.

For example, ETSI ES 203 915 [70] series corresponds to 3GPP TS 29.198 Release 6 [77] series. ETSI ES 204 915 [32] corresponds to 3GPP TS 29.198 Release 7 [69] series.

Parlay X APIs are being developed in two phases at ETSI. Parlay X 2 is standardized in ETSI ES 202 391 [71] series, which corresponds to 3GPP TS 29.199 Release 6 [78]. Parlay X 3 is standardized in ETSI 202 504 series [34], which corresponds to 3GPP TS 29.199 Release 7 [73].

Requirements for the OSA APIs are produced both by 3GPP and by ETSI: the 3GPP requirements are in 3GPP TS 22.127 [73], while the ETSI requirements are in EG 201 988 [74]. The stage 2 Architecture for OSA is described in 3GPP TS 23.198 [75] (also in 3GPP TS 23.127 [79] prior to Release 6).

Mapping documents have also been produced. 3GPP TS 29.199 [72] contains a suggested mapping between the base OSA/Parlay APIs and network protocols. A suggested mapping between Parlay X and the base OSA/Parlay APIs is being developed in TR 102 397 [76].

See annex-A for a list of URL links to these organizations.

5.9 OMA

Open Mobile Alliance is an international organization developing open, market driven interoperable specifications for global adoption. It was created in 2002 by leading mobile operators, device and network suppliers, information technology companies, content and service providers - the entire mobile value chain. It was formed by combining many existing smaller industry organizations to work under the OMA umbrella.

The focus of OMA is to promote interoperability at the application level for service enables such as Mobile Broadcast Service, Digital Rights Management, Mobile Location Services, and Games Service.

OMA specifications are designed to be network agnostic (e.g., hiding the complexity for access methods) and span across different types of networks, e.g., fixed, mobile, cable, xDSL, broadcast, WLAN, WiMAX, etc.

As a principle, OMA aims to re-use existing technologies avoiding duplication, divergence and fragmentation. OMA has an extensive network of 35 formal liaison relationships with other standards bodies, including those dealing with fixed and broadcast networks: ETSI, IETF, W3C, DVB, ITU-T, RIAA, MPA, CDG and JCP.

Current OMA work is built upon combinations of protocols including Web services, SIP, IMS and other from 3GPP.

In 2004, OMA published the OMA Web Services Enabler [35] to establish a base-line for developing Web services within OMA. It provides a framework for designing Web services that emphasizes the need to be consistent with Web service development outside OMA and, as such, requires conformance to the Web Services Interoperability Base Profile 1.0 [36] and WS-Security [7].

See annex A for URL Links to Websites.

5.10 ITU-T

The following work developed in ITU-T SG13 is relevant for the present document:

1) ITU-T Recommendation [37]. This Recommendation provides high level requirements for services and capabilities of Next Generation Network (NGN) release 1. Among others, this includes high level requirements and associated capabilities for an open service environment in NGN.

2) ITU-T Draft Recommendation [38]. The objective of this Recommendation is to provide service and functional requirements, service architecture and implementation scenarios of Open Service Environment (OSE) capabilities based on NGN release 1.

   The document builds, and extends, work developed in ITU-T Recommendation Y.2201 [37] as far as requirements and associated capabilities for an open service environment in NGN are concerned. The document includes text on open service environment use cases, on relationship of SOA concepts with open service environment capabilities, and on relationship of some current standardization efforts with OSE capabilities.

3) ITU-T Recommendation Y.2232 [39]. The objective of this document is to cover the following topics for convergence service scenarios in NGN using Web Services:

   - Requirements of convergence services scenario in NGN.
   - Web Services deployment model for NGN.
   - Web Services based convergence service scenarios in NGN.
   - Value proposition of Web Services in Convergence service scenarios.
   - Security and Interoperability considerations of Web Services based Convergence service scenarios.

See annex A for URL Links to Websites.

6 Management Frameworks

6.1 General

This clause contains an overview of existent advanced management standards and technologies. The main reason for inclusion of this information is due to experience accumulated in the area of interfaces' design for network entities and distributed systems by multiple standardization bodies, specifically for the purpose of management. This experience and the corresponding techniques could to some extent be applicable for exposure of NGN services and capabilities beyond the traditional management functions. The present document will examine the applicability of some of these management frameworks to the broader objective in hand. An additional positive factor to consider would be the ability to use common tools and infrastructure for both the management and the execution of the NGN services.

Among the included management standards and technologies are DMTF/CIM [40] and TMF/SID [41] addressing different management domain areas. DMTF/CIM is focusing primary on the IT resource management (systems, storage) and IP networks, while TMF/SID aims to describe information about the telecom service provider's overall technical and business system.

6.2 NGN Management

The "TISPAN NGN Management" specification [42] defines the Functional/Information view of the NGN OSS Architecture for the management of the NGN network and services and its specific security aspects. The NGN OSS Functional/ Information view is based on the concepts of TeleManagement Forum's New Generation Operations System and Software (NGOSS).

From the Overview of [42]:

"The NGN OSS Service and the NGN OSS Service Interface are the main basic entities used in the description of the NGN OSS View. An NGN OSS Service Interface provides access to functionality for managing the NGN in a way that supports the eTOM operational processes. NGN OSS Service Interfaces are the target of standardization and shall be specified as well-defined sets of related behaviours that together deliver necessary and sufficient functionality to be provided by an NGN OSS. Each behaviour is specified as an operation with a well-defined name, data, and pre- and post-conditions. NGN OSS Service Interfaces and Service Interface Consumers are grouped into NGN OSS Services. For a given NGN OSS Service, NGN OSS Service Interfaces and Service Interface Consumers may be defined as mandatory or as optional. The NGN OSS Service can be profiled: a profile of an NGN OSS Service indicates which of its Service Interfaces and Service Interface Consumers are present in a given specification used in the description of a possible realization of an NGN OSS system. All NGN OSS Operations within an NGN OSS Service Interface/Service Interface Consumer must be provided if the NGN OSS Service Interface/Service Interface Consumer is present in the specification. i.e. individual operations cannot be profiled. The basic NGN OSS Architecture principles require that NGN OSS Service Interfaces are made publicly available for use by NGN OSS Service Interface Consumers."

6.3 TMF

6.3.1 NGOSS

6.3.1.1 Overview

NGOSS is a comprehensive, integrated framework for developing, procuring and deploying operational and business support systems and software. It is available as a toolkit of industry-agreed specifications and guidelines that cover key business and technical areas including:

- Business Process Automation delivered in the enhanced Telecom Operations Map (eTOM™) - refer to TMF GB921 series [43] or to ITU-T Recommendation M.3050 [44].
- Systems Analysis & Design delivered in the Shared Information/Data Model (SID) - refer to TMF GB922 series [45]; more detailed explanation in clause 6.3.2.
- Solution Design & Integration delivered in the Contract Interface and Technology Neutral Architecture (TNA) - refer to TMF 053 series [46].

- Conformance Testing delivered in the NGOSS Compliance Tests [47].
- Procurement and Implementation delivered in ROI Model, RFI Template, and Implementation Guide documents.

NGOSS-based solutions use mainstream IT concepts and technologies to deliver a more productive development environment and efficient management infrastructure. NGOSS is prescriptive for only those few "cardinal points" where interoperability is key, while enabling ease of customization across a wide range of functionality. This allows NGOSS-based systems to be tailored to provide a competitive advantage while also working with legacy systems.

6.3.1.2 NGOSS Views

NGOSS recognizes, in general, four views in OSS development: business requirements, system design & modelling, solution implementation and service operations. The purpose of the NGOSS Lifecycle is to bridge the knowledge, activity of interests and inputs/outputs produced within each of the four views and make them a traceable and re-useable asset to the company. The definition of the four views and applicable NGOSS artefacts for each view is described below.

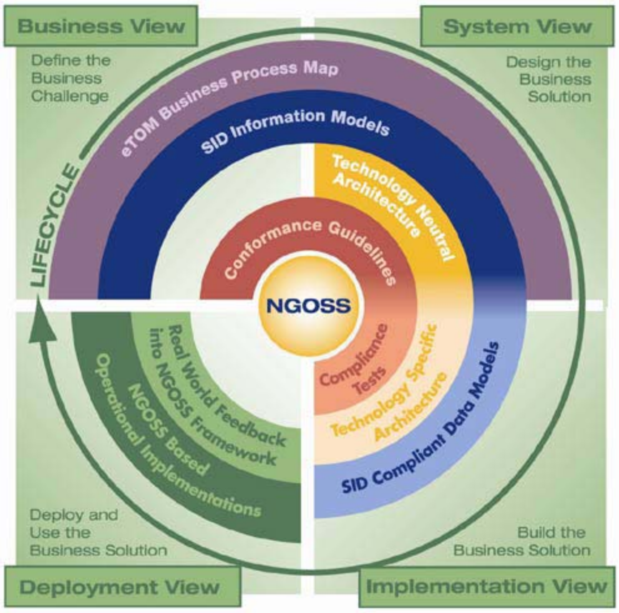

Figure 6.1: TMF NGOSS Lifecycle Views

Business View

This View is about "identification of the business need". The purpose of the View is to document the business requirements and all associated business activities that help to define the business requirements, such as process definition, policies, stakeholders, resource, etc.

System View

This is about "modelling the system solution". In this View there is formal information modelling of business needs and the desired system solution, done using a "grey box" perspective that places a focus on the points of interoperability (interactions). There are items relating to system Contracts, COTS capabilities and policy, process flow in terms of systems, information model, data specification, built s/w components and built COTS components.

Implementation View

This is about "validating the proposed solution". The Implementation View maps the System View solution models onto target technologies, potentially including a COTS component base assembly. There are items relating to Contract implementations, Class instance diagrams, Data models, Execution environments, Trial/pilot of system solution and Technology Neutral guidelines.

NGOSS Artefacts used/produced:

- Proposed solution model (built using the SID) and proposed distributed computing harness (specified using the TNA);
- NGOSS Input: NGOSS Lifecycle Use Case for the Implementation View plus the Artefacts produced in the Business and System Views;
- NGOSS Output: NGOSS Contract for the Implementation View + Artefacts from the Business View + System View + NGOSS components built from the Business View and System View contracts and SID.

Deployment View

This is about "realizing the solution". Here there is the observable behaviour of the solution operating in the "real world". There are items relating to Contract Instances, Components, full-scale run-time solution and technology specific guidelines.

6.3.1.3 Web Service / Service Orientated Architecture Implementation of NGOSS

NGOSS recognizes three styles of implementation of which one is based on Service orientated architecture using Web Services.

Many TMF Catalyst demonstration projects have built NGOSS Solutions based on Web Services. Of particular note are:

- The ICON Catalyst projects [48].
- The NGOSS Cookbook projects [49].

In each of these catalyst projects, industry standard Web Service toolkits have been used to create Web Service realizations of NGOSS Architecture Implementation and Deployment Views.

6.3.2 SID

TMF, within its NGOSS (Next Generation Operations Systems and Software) program, has produced the SID (Shared Information/Data Model) [45], which is recognized as the over-arching information model for the Service Provider. The SID is intended to provide an overarching information model that enables coverage of the entire network management and operations problem space. The SID provides the fundamental entities needed to manage and operate an information/telecommunications network starting from a set of core abstractions and including customer, product, service, and resource domains (to name a few). The current coverage of the SID in the resource domain does not include an adequate cellular network resource model.

The activity of SID specification is ongoing, and the current version of the model is now release 7.0, included within NGOSS release 7.0. [45].

Since 2005 there is an ongoing activity led by TMF which has the objective of proposing the SID for adoption by ITU-T Recommendation SG.4 as the umbrella Information Model for integrating domain specific models such as network transport, DTMF CIM, etc. At the ITU-T SG4 meeting in February 2007, it was agreed to work together to identify the additional work required to continue with the SID model submission to ITU-T.

6.3.3 MTOSI / MTNM

Within the TMF, the mTOP (multi Technology OSS Program) program provides coordination and planning for the TM Forum interface specification work in the area of resource and service management with respect to the fulfilment and assurance processes. It is specifying the MTOSI (Multi-Technology Operation Systems Interface) [50] and MTNM (Multi-Technology Network Management) Interfaces [51].

MTOSI is an OSS-OSS interface specification where "OSS" applies to any management system that supports Element Management Layer (EML), Network Management Layer (NML) and/or Service Management Layer (SML) functionality. The scope is resource management and specific aspects of service management concerning the fulfilment and assurance processes. MTOSI covers most layer 1 technologies such as Synchronous Optical NETwork (SONET), Synchronous Digital Hierarchy (SDH), Wavelength Division Multiplexing (WDM), Plesiochronous Digital Hierarchy (PDH) and many layer 2 technologies such as Asynchronous Transfer Mode (ATM), Digital Subscriber Line (DSL) and Ethernet. There are plans to extend MTOSI to layer 3 technologies such as IP and to additional layer 2 technologies such as WiMax, Passive Optical Network (PON) and Multi-Protocol Label Switching (MPLS). Note that MPLS is sometimes classified at layer 2.5.

Further, the TMF MTOSI team has proposed joint work with 3rd Generation Partnership Project (3GPP™) concerning mobile network management specifically on the subject of best practice and guidelines on definition of XML OSS interfaces.

MTOSI explicitly supports realization on Web Services and Java Messaging Service(JMS) technologies [52].

The MTOSI program builds on the TMF MTNM (Multi Technology Network Management) program, which specifies EM-NM interfaces. The MTOSI work extends MTNM to cover the general OSS-OSS situation The information model adopted by MTOSI is an extension of the MTNM information model for the Resource domain, while it is claimed (by TMF) to be compatible to the SID information model for the Service Domain. Moreover within the TMF a specific mTOP-SID mapping activity is ongoing to guarantee interoperability between the MTOSI Resource Layer and the SID Resource Layer.

Features are the way the TMF captures MTOSI business requirements. A MTOSI feature is defined around TMF608 [53] which is an implementable UML model (analogous to a NGOSS system view) catering for the eTOM resource domain. It has grown from the layer 2 domain but has currently been extended to cater for connectionless networks such as Ethernet and is being extended to cater for physical inventory. It is aligned with ITU-T Recommendations G.805/809 [54], [55] which may be considered to be the NGOSS business view model for the resource domain. This is the basis for the current harmonization work between mTOP, SID and DMTF CIM (models. In addition MTOSI and OSS/J (OSS through Java Initiative, included within TMF since Q2 2006) are working closely together under the banner of a "MTOSSJ" study group to promote future harmonization and greater alignment in terms of implementation.

In order to make the implementation process easier for adopters, each MTOSI Feature has been broken down into individual self contained packages called DDPs (Document Delivery Package) similar to the 3GPP IRP (Integration Reference Point) concept [65] such that each DDP contains both the implementation aspects of the API but also the full documentation aspects of the API. A DDP can be considered to be equivalent to a Service Oriented Architecture Service Interface and sets the granularity for realization and deployment of MTOSI implementations.

When defining a specific feature against requirements MTOSI defines both the operations (verbs) and the associated data (nouns). The operations are not restricted to basic CRUD (Create, Read, Update, Delete) but can be more complex operations such as get data according to a filter mechanism etc. The nouns themselves are based on the identified classes defined in the UML such that each class may be mapped into an XSD complex type. MTOSI uses a design paradigm called ‘contract first' which means that API's are defined by WSDL (Web Services Description Language) documents. As such the WSDL is a contract between multiple applications defining both the operations and the data to be used. Currently the XSD (XML Schema Definition) schemas are produced manually using common industry tools to directly translate the UML classes. The operations are created in the WSDL as per business requirement, as per use case, along with any required exception handling. The XSD Schema is then accessed as import references in the WSDL.

A feature of the WSDL is that it may be implemented in any supporting technology, e.g. Java, C++, C# and deployed over any supported SOAP binding, currently HTTP [56] or JMS [52] but this does not exclude other middleware technologies in future such as CORBA IIOP [57] or MQ subject to a standard binding becoming available. (Proprietary bindings do exist but interoperability becomes a consideration - W3C currently only defines SOAP for HTTP).

The method of implementing the MTOSI web-service is to take the WSDL and parse it with an implementation program such as wsdl2java or wsdl2c++ which translates the WSDL into a server side implementation containing the required operations, a proxy object for the client which is used to remotely call these operations, plus a set of packaged data binding objects. The data binding objects are just the class objects identified in the UML at design time and packaged as XSD Schema objects. These objects must be integrated manually at both client and server sides of the API according to the internal data representation of the respective applications.

Ideally there will be a close resemblance between the application data model and TMF 608 [53] otherwise standard techniques such as "Gang of Four's Façade pattern" need to be used to map the API data onto the internal data model. In addition to the WSDL definition MTOSI also defines middleware relationships called Message Exchange Patterns which may be synchronous or asynchronous point to point between two applications or more complex middleware relationships such a message brokering and potentially in future BPEL (Business Process Execution Language) based for complex interactions.

6.4 DMTF

6.4.1 CIM

The Common Information Model (CIM) [40] is a mechanism to provide standardized schemas for management instrumentation expressed as object oriented classes. CIM is comprised of a core modeling infrastructure that defines syntax and semantics for modeling a resource, as well as a series of resources modeled with that infrastructure. Various committees in the DMTF have modeled a wide assortment of classes for things like Network Adapters, Storage Devices, Services, etc.

Instrumentation providers are typically written to plug into a CIM Server, also known as a CIM Object Manager (CIMOM). There are implementations of CIMOMs for Unix, Windows and other operating systems.

Access to CIM resources is done via one of the existing "Web Based Enterprise Management" (WBEM) Protocols [58], which provide operations like Enumerate, Get, Set, Invoke, etc. The DMTF has standardized CIM-XML [59], an http+xml protocol, Command Line Protocol (CLP), a text based user oriented "shell" style protocol, as well as WS-Management, a Web Services based protocol.

CIM is being leveraged for Operating System, Application, Hardware and Storage Management. Recent initiatives like SMASH provide instrumentation for embedded management controllers which exist on servers and workstations. These embedded controllers which will emerge as part of Server Hardware platforms in 2007 will include CIM instrumentation, CLP and WS-Management.

In addition, Storage Networking Industry Association (SNIA) has adopted CIM as their modeling language for Storage Management. Existing products use CIM-XML, although upcoming products are beginning to move to WS-Management to leverage Web Services.

6.4.2 WS-Management

WS-Management is a Web Services based protocol intended to access Management Instrumentation [58].

The Web services architecture is based on a suite of specifications that define rich functions and that may be composed to meet varied service requirements. WS-Management leverages many of these Web Services "Infrastructure Specifications" to provide core functionality as well as profile it to make it suitable for management purposes.

A crucial application for these services is in the area of systems management. To promote interoperability between management applications and managed resources, the specification identifies a core set of Web service specifications and usage requirements that expose a common set of operations central to all systems management. This comprises the abilities to:

- Get, put (update), create, and delete individual resource instances, such as settings and dynamic values;
- Enumerate the contents of containers and collections, such as large tables and logs;
- Subscribe to events emitted by managed resources; and
- Execute specific management methods with strongly typed input and output parameters.

To provide a secure mechanism of management, WS-Management supports multiple security models and profiles as well as allows extensibility to allow new or special purpose mechanisms to be supported. Popular supported security profiles are TLS/HTTP [60], HTTP Digest [61], Kerberos [62], and HTTP Basic [56]. The specification has also been authored to allow the use of WS-Security [7] as it becomes popular.

In each of these areas of scope, the specification defines minimal implementation requirements for conformant Web service implementations. An implementation is free to extend beyond this set of operations, and may also choose not to support one or more areas of functionality listed above if that functionality is not appropriate to the target device or system.

WS-Management is currently supported by a community of products. Open Source WS-Management implementations have been created by companies including HP, Intel and Sun. There exist both standalone WS-Management implementations which allow integration into existing applications and systems as well as implementations intended to work with CIM Servers (CIMOMs) such as OpenPegasus and OpenWBEM. These implementations provide a wide set of choices for heterogeneous operating systems including Unix and Linux. WS-Management is also implemented in Microsoft Windows Server 2003 R2 and Windows Vista. In addition, hardware manufacturers including, but not limited to, HP, Intel and AMD have publicly announced WS-Management support directly in their hardware products.

6.5 WSDM by OASIS

Web Services Distributed Management and its dependent specifications have been standardized by OASIS. See Annex-A for a list of URL links to this organization and specifications.

In order to seek a unified Web Services Management Protocol, an effort is underway to achieve this long term goal. A join whitepaper has been published by the participants which outlines the roadmap. The unified protocol effort will be based on the WS-Management infrastructure specifications, but will provide additional layers to include certain features from WSDM. More information can be found in the "Toward Converging Web Service Standards for Resources, Events, and Management" whitepaper [63].

6.6 Service Modeling Language (SML)

SML [64] is a new emerging effort which is attempting to define mechanisms for applying constraints to managed systems. It can be used in conjunction with modeling languages like CIM to provide a higher level abstraction for things like service availability and deployment.

The Service Modeling Language (SML) specification is used to model complex IT services and systems, including their structure, constraints, policies, and best practices. SML is based on a profile on XML Schema and Schematron.

SML was created by the SML working group whose members are BEA, BMC, Cisco, Dell, EMC, HP, IBM, Intel, Microsoft and Sun.

SML will allow for the creation of best practices and policies that automate the services' validation, development, operations, updates and end-of-life - the full lifecycle. SML does not prescribe a specific IT model or set of models; instead, it defines the syntax and semantics that all SML models must follow: their base vocabulary, the rules of composition, the grammar and the syntax. SML Specifies:

- Profiles for the use of XML 1.0 Schema and Schematron to define service models.
- Extensions to support and constrain inter-document references in those models.
- Inter-document uniqueness and key definitions plus the ability to use them across documents.
- Rules to capture best practices and policies.

7 Conclusions and Next Steps

The present document has identified a number of disparate activities in progress in a number of different SDOs. Various Standards Development Organizations (SDOs) are working on the application of SOA frameworks to the telecoms sector, but since the focus of each SDO is different, the current status of SOA standards for telecoms is fragmented.

In addition the existing SOA and Web Services standards do not completely address all of the needs of the telecoms operators or vendors to provide flexible and agile service development and deployment for a multi-provider and multi-vendor environment.

The conclusion of the present document is that there are considerable technical benefits that would accrue from the increased collaboration of the IT and telecommunications industries to provide a rich service development and deployment environment fully utilizing the capabilities that an NGN can offer.

Annex A: Sources of Further Information

A.1 Organization URLs

OASIS	Organization for the Advancement of Structured Information Standards	http://www.oasis-open.org
W3C	World Wide Web Consortium	http://www.w3.org
WS-I	Web Services Interoperability Organization	http://www.ws-i.org
Liberty Alliance		http://www.projectliberty.org/
Parlay Group		http://www.parlay.org
OMA	Open Mobile Alliance	http://www.openmobilealliance.org
TMF	TeleManagement Forum	http://www.tmforum.org
ITU	International Telecommunication Union	http://www.itu.int
OMG	Object Management Group	http://www.omg.org
DMTF	Distributed Management Task Force	http://www.dmtf.org
OSA/Parlay JWG	OSA/Parlay Joint Working Group	http://portal.etsi.org/docbox/TISPAN/Open/OSA/osa.htm
OpenPegasus		http://www.openpegasus.org/
Schematron		http://www.schematron.com/

Annex B: Bibliography

- Oasis specifications can be found at: http://www.oasis-open.org/specs/index.php
- More information on WSDM Web Services Distributed Management can be found at: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsdm.
- WS-I profile specifications can be found at: http://www.ws-i.org/deliverables/Default.aspx
- Liberty Alliance specifications can be found at: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications
- OSA/Parlay (ETSI Joint Working Group) specifications can be found at: http://portal.etsi.org/docbox/TISPAN/Open/OSA/Overview.html
- TMF specifications can be found at: http://www.tmforum.org/library
- As of 2007, the ITU allows immediate access to pdf formats of in-force, posted ITU-T Recommendations: http://www.itu.int/ITU-T/publications/recs.html
- OMG specifications can be found at: http://www.omg.org/technology/documents/spec_catalog.htm
- DMTF specifications can be found at: http://www.dmtf.org/standards/published_documents

History

Document history		
V1.1.1	March 2008	Publication