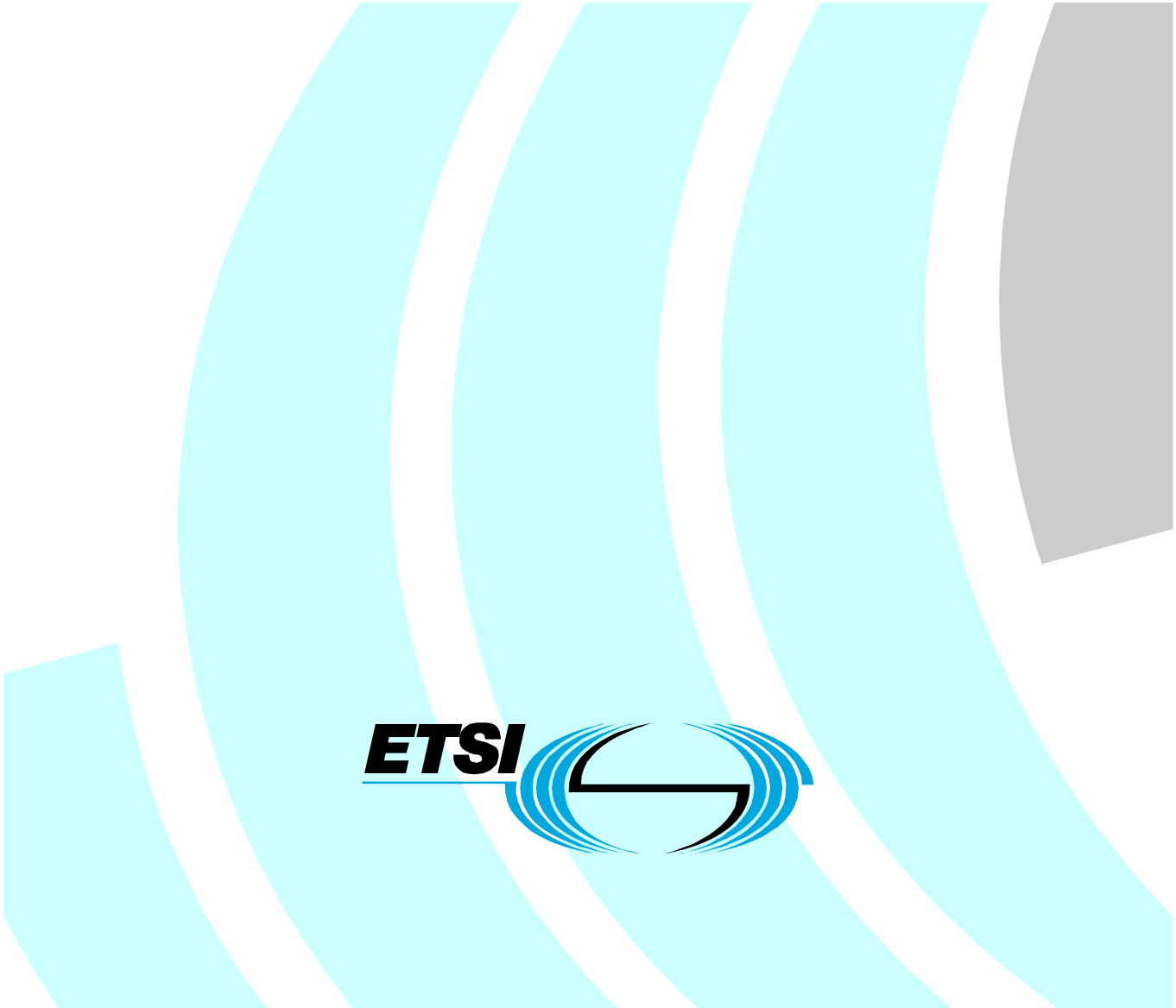
ETSI TR 102 659-2 V1.1.1 (2009-02)

Technical Report

GRID;
Study of ICT GRID interoperability gaps;
Part 2: List of identified Gaps



Reference
DTR/GRID-0001-2

Keywords
analysis; directory; ICT; interoperability; testing

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2009.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™, **TIPHON**™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 5
Foreword 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definitions and abbreviations 11
3.1 Definitions 11
3.2 Abbreviations 12
4 Methodology for Gap Analysis 14
5 Specification Areas selected for Analysis 14
5.1 Service Level Agreements 15
5.1.1 Introduction 15
5.1.2 SLA Terminology 15
5.1.3 Secondary Definitions 17
5.1.4 Discussion 17
5.1.5 Different types of SLA 18
5.2 Security 19
5.2.1 Introduction 19
5.2.2 Definitions 19
5.2.3 Authentication 19
5.3 Charging 21
5.3.1 Introduction 21
5.3.2 Charging Terminology 21
5.3.3 Offline Charging 21
5.3.4 Online Charging Service 22
5.4 Service Discovery 22
5.4.1 Introduction 22
6. Case Studies 22
7 Issues, Gaps and Overlaps 23
7.1 Architectural issues 23
7.2 Service capability and operational issues 24
7.2.1 Issues relating to SLA and QoS 24
7.2.2 Issues relating to security 25
7.2.3 Issues relating to Charging 25
7.2.4 Issues relating to Service Discovery 26
7.3 Gaps and overlaps arising from the EU FP6 Grids Survey 26
8 Way Forward 27
Annex A: Case Studies 28
A.1 Case Study 1 - Online Media and Entertainment 28
A.1.1 Scenario description 28
A.1.2 Video download in a Grid environment 28
A.1.2.1 Grid manager 30
A.1.2.2 Grid node 30
A.1.2.3 Grid client 30
A.1.3 Video download in an NGN environment 30
A.1.3.1 Service initialization 31
A.1.3.2 Functional entities and flows for the CoD service 32
A.1.4 Comparison 35
A.1.5 Gap analysis for the video download scenario 36

A.1.5.1 Authentication and Authorization 36
A.1.5.2 Service Discovery 39
A.1.5.3 Video Selection 40
A.1.5.4 Video Download 41
A.1.5.5 Video Control 41
A.1.5.6 Charging 41
A.1.5.7 SLA and QoS 42

A.2 Integrated Emergency Management (IEM) 43
A.2.1 Scenario description 43
A.2.2 IEM in a Grid environment 44
A.2.3 IEM in an NGN environment 45
A.2.4 Comparison 45
A.2.5 Gap analysis for the IEM scenario 46
A.2.5.1 Security 46
A.2.5.2 SLA and QoS 46
A.2.5.3 Charging 47
A.2.5.4 Reliability 47
A.2.5.5 Discovery 47
A.2.5.6 Workflow 47

A.3 High Performance Computing 47
A.3.1 Scenario description 47
A.3.2 HPC in a Grid environment 48
A.3.3 HPC in a NGN environment 49
A.3.4 Comparison 49
A.3.4.1 Database operating systems 49
A.3.4.2 NGN networking 50
A.3.4.3 Workflow management 51
A.3.4.4 Security policies 51
A.3.5 Gap analysis for the HPC scenario 51
A.3.5.1 Business vision 51
A.3.5.2 Grid middleware 51
A.3.5.3 User experience 51
A.3.5.4 Conclusion 52

A.4 e-Health 52
A.4.1 Introduction 52
A.4.2 e-Health in a Grid Environment 52
A.4.3 e-Health and NGN 52
A.4.4 SLA and QoS 53
A.4.5 Charging 53
A.4.6 Service Discovery 53
A.4.7 Security 54

Annex B: Bibliography 55

History 56

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee GRID (GRID).

The present document is part 2 of a multi-part deliverable covering the study of ICT GRID interoperability gaps, as identified below:

Part 1: "Inventory of ICT Stakeholders";

Part 2: "List of identified gaps".

1 Scope

The present document identifies interoperability gaps in existing and emerging Grid standards. It identifies shortcomings, overlaps and loopholes in current, proposed, and *de facto* Grid standards at all levels of the middleware/protocol stack (network to application interfaces), with specific consideration for large-scale commercialization and interoperability of standards/systems relevant to the ICT sector (i.e. the ETSI constituency), such as NGN.

This is part two of a two part document providing a study of ICT Grid interoperability gaps. The present document provides an initial gap analysis. The gaps have been identified through analysis of a series of scenarios, a summary of which can be found in the appendices. By selecting common themes across those scenarios it has been possible to identify specific requirements. These have directed the analysis of specific Grid standards. Standards identified may be Grid specific standards or other standards which support an integrated Grid NGN environment.

The present document addresses:

- Interoperability gaps in Grid Standards.
- Interoperability gaps between Grid and NGN standards in an integrated environment.

The present document does not address:

- Interoperability gaps between different Grid infrastructures due to custom software packages.
- Interoperability gaps between two implementations of the same standard (e.g. shortcomings and lack of precision).

TR 102 659-1 [i.21]captures the current state of Grid technologies and identifies the key stakeholders, including standards making bodies, research projects, production Grids and other initiatives. Additionally, it identifies a recommended base of standards and *de facto* standards in the form of a Grid ICT Profile, taking into account the requirements for interoperability in the ICT domain.

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.

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

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] OGF GFD.107: "Web Services Agreement Specification (WS-Agreement)", A.Andrieux et al, March 2007.

NOTE: http://www.ogf.org/documents/GFD.107.pdf

[i.2] "SLAM Overview", TM Forum.

NOTE: http://www.tmforum.org/browse.aspx?catID=2016

[i.3] "SLA Management Handbook: Volume 2 Concepts and Principles", Release 2.5, TeleManagement Forum, GB 917-2, July 2005.

[i.4] Telecoms & Internet converged Services & Protocols for Advanced Network, home page.

NOTE: www.etsi.org/tispan

[i.5] IETF RFC 2386: "A Framework for QoS-based routing in the Internet", E.Crawley et al, IETF, August 1998.

NOTE: http://www.faqs.org/rfcs/rfc2386.html

[i.6] OGF GFD.120: "Open Grid Services Architecture - Glossary of Terms", J.Treadwell, December 2007.

NOTE: http://www.ogf.org/documents/GFD.120.pdf

[i.7] OGF GFD.122: "Grid Network Services Use Cases from the e-Science Community", T.Ferrari, December 2007.

NOTE: http://www.ogf.org/documents/GFD.122.pdf

[i.8] ETSI TR 102 450: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Telecommunication Equipment Life Cycle".

[i.9] ETSI TR 102 479: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of available material on QoS requirements of Multimedia Services".

[i.10] ITU-T Recommendation E.800: "Terms and definition related to quality of service and network performance including dependability".

[i.11] ITU-T Recommendation G.1000: "Communications Quality of Service: A framework and definitions".

[i.12] ETSI TS 181 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service Layer Requirements to integrate NGN services and IPTV".

[i.13] ITU-T Recommendation M.1400: "Designations for interconnections among operators' networks".

[i.14] ITU-T Recommendation M.3320: "Management requirements framework for the TMN X-Interface".

[i.15] ETSI TS 188 003: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); OSS requirements; OSS definition of requirements and priorities for further network management specifications for NGN".

[i.16] ETSI TS 181 005: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".

[i.17] "Web Services Agreement Negotiation Specification (WS-Agreement Negotiation)", OGF (internally labelled GGF), draft, May 2008.

NOTE: http://forge.ogf.org/sf/docman/do/downloadDocument/projects.graap-wg/docman.root.current_drafts.ws_agreement_negotiation_specifi/doc6092/1

[i.18] "GT Information Services: Monitoring & Discovery System (MDS)", Globus Project.

NOTE: http://www.globus.org/toolkit/mds/

[i.19] "R-GMA: Relational Grid Monitoring Architecture", EGEE Project.

NOTE: http://www.r-gma.org/

[i.20] ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.21] ETSI TR 102 659-1: "GRID; Study of ICT Grid interoperability gaps; Part 1: Inventory of ICT Stakeholders".

[i.22] "Dynamic SLA negotiation based on WS-Agreement". A.Pichot, P.Wieder, O.Waldrich, W.Ziegler, CoreGrid Technical Report 82, June 2007.

NOTE: http://www.coregrid.net/mambo/images/stories/TechnicalReports/tr-0082.pdf

[i.23] IETF RFC 3820: "Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile".

[i.24] NCSA MyProxy.

NOTE: http://grid.ncsa.uiuc.edu/myproxy/

[i.25] ETSI TS 182 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; Dedicated subsystem for IPTV functions".

[i.26] IETF RFC 2782: "A DNS RR for specifying the location of services (DNS SRV)".

[i.27] ETSI TS 102 034: "Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks".

[i.28] ITU-T IPTV Focus Group Proceedings, ITU-T, 2008.

[i.29] ETSI TS 187 001: " Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[i.30] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[i.31] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment SubSystem (NASS)".

[i.32] IEEE 802.1X: "IEEE Standard for Port Based Network Access Control".

[i.33] IETF RFC 2933:"Internet Group Management Protocol MIB".

NOTE: http://www.faqs.org/rfcs/rfc2933.html

[i.34] IETF RFC 2069: "An Extension to HTTP: Digest Access Authentication", January 1997.

[i.35] ITU-T Recommendation P.910: "Subjective video quality assessment methods for multimedia applications" (04/08).

[i.36] DSL Forum Technical Report TR-126: "Triple-play Services Quality of Experience (QoE) Requirements".

[i.37] ETSI TS 102 005: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in DVB services delivered directly over IP protocols".

[i.38] IBM Tutorial - Building a grid using Web services standards.

[i.39] GFD-R.056: "Job Submission Description Language (JSDL) Specification", Open Grid Forum, November 2005.

NOTE: http://www.gridforum.org/documents/GFD.56.pdf

[i.40] ETSI TS 132 240: "Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);Telecommunication management; Charging management; Charging architecture and principles (3GPP TS 32.240 version 7.2.0 Release 7)".

[i.41] ETSI TS 132 200: "Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);Telecommunication management; Charging management; Charging principles (3GPP TS 32.200 version 5.9.0 Release 5)".

[i.42] ETSI TS 132 296: "Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);Telecommunication management; Charging management; Online Charging System (OCS): Applications and interfaces (3GPP TS 32.296 version 7.0.0 Release 7)".

[i.43] "Towards GLUE 2: Evolution of the Computing Element Information Model". S.Andreozzi et al.

NOTE: International Conference on Computing in High Energy and Nuclear Physics (CHEP'07), http://www.iop.org/EJ/article/1742-6596/119/6/062009/jpconf8_119_062009.pdf

[i.44] "GLUE Schema Specification: version 1.3", S.Andreozzi et al, 2007.

NOTE: http://forge.gridforum.org/sf/docman/do/downloadDocument/projects.glue-wg/docman.root.background.specifications/doc14185

[i.45] ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

[i.46] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905 version 8.6.0 Release 8)".

[i.47] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity management and their resolution in the NGN".

[i.48] "SAML Specifications".

NOTE: http://saml.xml.org/saml-specifications

[i.49] "XACML attribute profile schema".

NOTE: http://docs.oasis-open.org/security/saml/v2.0/saml-schema-xacml-2.0.xsd

[i.50] "Grid Access Control Language (GACL) Grid".

NOTE: http://www.gridsite.org/wiki/GACL

[i.51] GDF.98: "Usage Record - Format Recommendation".

NOTE: http://www.gridforum.org/documents/GFD.98.pdf

[i.52] ETSI TS 132 298: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Telecommunication management; Charging management; Charging Data Record (CDR) parameter description".

[i.53] "Web Services-Business Process Execution Language (WS-BPEL)".

NOTE: http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html

[i.54] "Common Information Model (CIM) Standards".

NOTE: http://www.dmtf.org/standards/cim

[i.55] "UDDI Version 3".

NOTE: http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm#uddiv3

[i.56] "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)".

NOTE: http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf.

[i.57] "Scalable Grid Service Discovery Based on UDDI". S. Banerjee, S. Basu, S. Garg, S.J. Lee, P. Mullan, and P. Sharma, Proc. Third Int'l Workshop Middleware for Grid Computing (MGC '05), pp. 1-6, Dec. 2005.

[i.58] "A Globus Toolkit Primer Or, Everything You Wanted to Know about Globus, but Were Afraid To Ask, Describing Globus Toolkit Version 4; A globus primer, An Early and Incomplete Draft". I. Foster. Technical report, Globus Alliance, 2005.

[i.59] "Personalized grid service discovery". S. Miles, J. Papay, V. Dialani, M. Luck, K. Decker, T. Payne, and L. Moreau, IEE Proc. Software, special issue on performance eng., vol. 150, no. 4, pp. 252-256, 2003.

[i.60] "Enhancing UDDI for Grid Service Discovery by Using Dynamic Parameters". B. Sinclair, A. Goscinski, and R. Dew, Proc. Int'l Conf. Computational Science and Its Applications (ICCSA '05), pp. 49-59, May 2005.

[i.61] "R-GMA Architectural Design".

NOTE: http://www.r-gma.org/arch-virtual.html

[i.62] GFD.80: "The Open Grid Services Architecture Version 1.5".

NOTE: http://www.ogf.org/documents/GFD.80.pdf

[i.63] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[i.64] IETF RFC 1321: "The MD5 Message-Digest Algorithm".

[i.65] ETSI ES 282 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Charging management [Endorsement of 3GPP TS 32.240 Release 7, 3GPP TS 32.260 Release 7, 3GPP TS 32.297 Release 7, 3GPP TS 32.298 Release 7 and 3GPP TS 32.299 Release 7, modified]".

[i.66] ITU-T Recommendation Y.1910: "IPTV architecture".

[i.67] "UBR Shutdown FAQ".

NOTE: http://uddi.microsoft.com/about/FAQshutdown.htm fetched on May 13th 2008.

[i.68] "ETSI eHEALTH TB".

NOTE: http://portal.etsi.org/portal_common/home.asp?tbkey1=eHEALTH

[i.69] "HealthGrid Association".

NOTE: http://www.healthgrid.org/

[i.70] "HealthGrid White Paper", November 2004.

NOTE: http://whitepaper.healthgrid.org/

[i.71] "NHS Connecting for Health IT restructuring project".

NOTE: http://www.connectingforhealth.nhs.uk/

[i.72] "US Connecting for Health network information sharing".

NOTE: http://www.connectingforhealth.org/

[i.73] GLUE Specification v2.0 (draft), Open Grid Forum, May 2008.

NOTE: http://forge.ogf.org/sf/projects/glue-wg

[i.74] "Condor Classified Advertisement Language and Processor", Condor Project, University of Wisconsin, USA, v7.0.1 February 2008.

NOTE: http://www.cs.wisc.edu/condor/manual/v7.0/condor_submit.html

[i.75] IETF RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

[i.76] ETSI SR 002 564 (V2.0.0): "Applicability of existing ETSI and ETSI/3GPP deliverables to eHealth".

[i.77] "Atlas computing technical design report". Tech. rep. CERN, ATLAS Collaboration, 2005.

[i.78] "Enabling Integrated Emergency Management: Reaping the Akogrimo Benefits". N.Briscombe et al.

NOTE: http://www.akogrimo.org/download/White_Papers_and_Publications/Akogrimo_whitePaper_DisasterCrisisMgmt_v1-1.pdf but also registered at ETSI http://docbox.etsi.org/grid/grid/50-Meetings/GRID04_20070920_Sophia-Antipolis/GRID04_02.pdf

[i.79] "Integrated Emergency Management", issued by the Milton Keynes Council Emergency Planning Department, 2004.

NOTE: http://www.mkweb.co.uk/emergencyplanning/documents/IEMv1_2.pdf

[i.80] "Civil Protection (1991) Home Secretary Announces Outcome of Emergency Planning Review; supplement to summer 1991 edition". Home Office Communications Directorate; London.

[i.81] "Civil Contingencies Act 2004: Emergency Preparedness", UK Cabinet Office, 2004.

NOTE: http://www.ukresilience.info/preparedness/ccact/eppdfs.aspx

[i.82] "OASIS Web Services Resource Framework (WSRF) TC".

NOTE: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrf

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

accounting: See note.

NOTE: This term has many definitions and should be avoided (e.g. can mean the whole topic of usage recording, charging and billing or the activity of dividing revenues between network operators and/or service providers).

billing: function whereby charging information is transformed into bills requiring payment (TS 132 240 [i.40])

chargeable event: activity utilizing resources and related services which may result in a charge

NOTE 1: As a minimum, a chargeable event characterizes the resource/service usage and indicates the identity of the involved end user(s).

NOTE 2: This is a generalized definition based on the telecom specific definition in TS 132 200 [i.41]

charging: function whereby information related to a chargeable event is collected, formatted, transferred and evaluated in order to make it possible to determine usage for which the charged party may be billed (offline charging) or the customer's account balance may be debited (online charging)

NOTE: This is a generalized definition based on the telecom specific definition in TS 132 296 [i.42].

Charging Data Record (CDR): formatted collection of information about a chargeable event for use in billing and accounting (synonymous with Usage Record)

NOTE: This is a generalized definition based on the telecom specific definition in TS 132 240 [i.40].

offline charging: charging mechanism where charging information does not affect, in real-time, the service rendered (TS 132 240 [i.40])

online charging: charging mechanism where charging information can affect, in real-time, the service rendered and therefore a direct interaction of the charging mechanism with bearer/session/service control is required (TS 132 240 [i.40])

Quality of Experience (QoE): See note.

NOTE: No single definition of Quality of Experience (QoE) is provided, however clause 5.1.2 identifies a number of candidate definitions.

Quality of Service (QoS): See note.

NOTE: No single definition of Quality of Service (QoS) is provided, however clause 5.1.2 identifies a number of candidate definitions.

Service Level Agreement (SLA):

NOTE: No single definition of Service Level Agreement (SLA) is provided, however clause 5.1.2 identifies a number of candidate definitions.

usage record: record of resources consumed

NOTE: Data is collected from individual resources at the fundamental or atomic level (synonymous with Charging Data Record (CDR)).

3.2 Abbreviations

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

A&E	Accident & Emergency
API	Application Program Interface
ATLAS	A Toroidal LHC ApparatuS
BOBO	Billing On Behalf of Others
BPEL	Business Process Execution Language
BPEL4WS	Business Process Execution Language for Web Services
B-SLA	Binding Service-Level Agreement
CA	Certificate Authority
CDDLM	Configuration Description, Deployment, and Lifecycle Management
CDR	Charging Data Record
CDS	Computerized Decision Support
CERN	Organisation Européenne pour la Recherche Nucléaire (European Organization for Nuclear Research)
CF	Customer Facing
CIM	Common Information Model
COD	Content on Demand
COP	Common Operational Picture
DB	Data Base
DHCM	Disaster Handling and Emergency Management
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name System

DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DVB	Digital Video Broadcasting
DVB	Digital Video Broadcasting
DVBSTP	DVB SD&S Transport Protocol
EAP	Extensible Authentication Protocol
EGA	please check
EGEE	Enabling Grids for E-sciencE
EPG	Electronic Programme Guide
FE	Functional Entity
GACL	Grid Access Control Language
GIIS	Grid Information Index Service
GRIS	Grid Resource Information Service
GT4	Globus Toolkit 4
HPC	High Performance Computing
HTTP	Hyper Text Transfer Protocol
ICT	Information & Communication Technology
IEM	Integrated Emergency Management
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGTF	International Grid Trust Federation
IP	Internet Protocol
IPI	Internet Protocol Infrastructure
IPI	please check
IPTV	IP Television
JSDL	Job Submission Description Language
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
LHC	Large Hadron Collider
MCF	Media Control Function
MDF	Media Delivery Function
MDS	Monitoring and Discovery Service
MPEG-2	Motion Picture Expert Group-2
MRI	Magnetic Resonance Imaging
NASS	Network Attachment SubSystem
NAT	Network Address Translation
NG	NorduGrid
NGN	Next Generation Network
NSP	NGN Service Provider
OASIS	Organization for the Advancement of Structured Information Standards
OGF	Open Grid Forum
OGSA	Open Grid Services Architecture
OS	Operating System
OSG	Open Science Grid
OWL	Object Windows Library
PANA	Protocol for carrying Authentication for Network Access
PKI	Public Key Infrastructure
PM	Patient Monitoring
PMA	Policy Management Authority
PPP	Point-to-Point Protocol
QoE	Quality of Experience
QoS	Quality of Service
RACS	Resource and Admission Control SubSystem
RDF	Resource Description Framework
REL	please check
RFC	IETF Request For Comments
R-GMA	Relational Grid Monitoring Architecture
RMS	Resource Management System
RMS	Resource Management System
R-SLA	Resource Service-Level Agreement
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol

RTSP	Real Time Streaming Protocol
SAGA	Simple API for Grid Applications
SAML	Security Assertion Markup Language
SD	Service Discovery
SD&S	Service Discovery and Selection
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SP	Service Provider
SQL	Structured Query Language
SRV	Service record
STQ	Speech and multimedia Transmission Quality
TCP	Transaction Control Protocol
TISPAN	ETSI Technical Committee for Telecoms & Internet converged Services & Protocols for Advanced Networks
T-SLA	Task Service-Level Agreement
UDAF	User Data Access Function
UDDI	Universal Description Discovery and Integration Service
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPSF	User Service Profile Function
URL	Uniform Resource Locator
USB	please check
USB	Universal Serial Bus
VCR	Video Cassette Recorder
VO	Virtual Organization
VOD	Video on Demand
WLAN	Wireless Local Area Network
WS	Web Services
WSDL	Web Services Description Language
WSDM	WS-Distributed Management
W-SLA	Workflow Service-Level Agreement
WSRF	Web Service Resource Framework
WSRM	Web Service Reliable Messaging
WSS	Web Service Security
XACML	eXtensible Access Control Markup Language
XDMS	XML Document Management Server
XML	Extensible Markup Language

4 Methodology for Gap Analysis

The methodology adopted to perform the gap analysis has been to:

- identify broadly applicable themes for gap analysis (the specific themes are described in clause 5);
- develop a number of case studies (summarized in clause 6 and described in Annex A) as a mechanism to identify gaps, etc.,
- bring together gaps, overlaps and issues based on these themes (see clause 7) and on more general architectural considerations.

Detailed proposals for the resolution of gaps, overlaps and issues are left for further study.

5 Specification Areas selected for Analysis

The present document identifies four major areas for requirements and standards analysis covering Grid and NGN. For each, key terminology is identified (and, where applicable, highlighting differences between Grid and NGN), a summary of the area is provided, and common challenges are outlined.

5.1 Service Level Agreements

5.1.1 Introduction

Many aspects of a Grid or NGN environment can be viewed as "services". For Grids this view is presented in the Open Grid Services Architecture (OGSA) [i.62]. When one part of the overall system interacts with such a service, it may wish to have measurable guarantees from the service provider concerning non-functional aspects of the given service. These may include properties such as communication latency, reliability, bandwidth, processing time, or privacy guarantees, to name a few. The properties in question will be specific to the capabilities provided by the given service, however the general requirement that those service properties somehow be specified remains the same.

Although overarching agreements may be made between the organizations responsible for the communicating services, the Grid concept also envisages automated processing and possibly dynamic negotiation of Service Level Agreements (SLA) (e.g. using ClassAds or the WS-Agreement protocol [i.1]). This is one step towards the Grid notion of achieving non-trivial Quality of Service (QoS).

QoS is a term used widely in telecommunications and networking and concerns multiple measurable aspects of the delivery of a service, such as network bandwidth and latency.

5.1.2 SLA Terminology

When considering SLAs in the context of Grids, NGN, and common Internet protocols, it is valuable to consider the different perspectives taken on key terms. The present document considers the following key organizations: TM Forum ([i.2] and [i.3]), ETSI TISPAN [i.4], IETF (responsible for Internet protocols - [i.5]) and OGF (concerning Grids - [i.6] and [i.7]).

Service Level Agreement (SLA):

- TM Forum [i.3]: A Service Level Agreement (SLA) is a formal negotiated agreement between two parties. It is a contract that exists between the Service Provider (SP) and the Customer. It is designed to create a common understanding about Quality of Service (QoS), priorities, responsibilities, etc. SLAs can cover many aspects of the relationship between the Customer and the SP, such as performance of services, customer care, billing, service provisioning, etc. However, although a SLA can cover such aspects, agreement on the level of service is the primary purpose of a SLA.

- TISPAN [i.4]: A Service Level Agreement (SLA): formal negotiated agreement between a Service Provider (SP) and a Supplier/several Suppliers. A Service Provider has the Customer role, buying equipments/software/services which are manufactured by one/several manufacturers [i.3] and [i.8].

- OGF [i.6]: A contract between a provider and a consumer that specifies the level of service that is expected during the term of the contract. An SLA typically includes one or more service-level objectives (a measurable objective for a service or for a set of one or more resources). SLAs are used by vendors and customers, as well as internally by IT shops and their end users. They might specify availability requirements and response times for normal operations and for problem resolution (network down, machine failure etc) and they might stipulate the payment and/or penalties associated with meeting or failing to meet the agreed criteria.

There is a broad similarity between the three definitions. They all involve two parties - albeit with different terminology which will be discussed in the following clause. They all introduce the link between the service level attained and payment/billing. The OGF introduces the notion that there can be multiple objectives in a single agreement, however this is also implicit in the TM Forum definition.

Quality of Service (QoS):

- OGF [i.6]: A measure of the service attained, such as security, network bandwidth, average response time or service availability.

- TISPAN: Quality of Service (QoS): the collective effect of service performance, which determine the degree of satisfaction of a user of the service [i.9]: which in turn references [i.10].

NOTE 1: The quality of service is characterized by the combined aspects of service support performance, service operability performance, serveability performance, service security performance and other factors specific to each service.

NOTE 2: The term "quality of service" is not used to express a degree of excellence in a comparative sense nor is it used in a quantitative sense for technical evaluations. In these cases a qualifying adjective (modifier) should be used [i.10].

NOTE 3: The definition above including notes 1 and 2 is from ITU-T Recommendation E.800 [i.10]. ITU-T Recommendation G.1000 [i.11] expands the definitions of QoS given in ITU-T Recommendation E.800 [i.10].

- IETF: A set of service requirements to be met by the network while transporting a flow [i.5].

The three definitions of QoS are similar in the sense of covering multiple measurable aspects of the delivery of a service. They differ, however, in their scope. The IETF definition focuses on network aspects, whereas the OGF definition is more general, covering aspects of the service, such as its computational characteristics.

Quality of Experience (QoE):

- TISPAN: User perceived experience of what is being presented by a communication service or application user interface [i.9].

- TISPAN : Purely subjective measure from the user's perspective of the overall value of the service provided [i.12].

While the term QoE is recognized in NGN, there is no such definition in Grid, since the concern in Grids has less emphasis on the user's perceived experience as such, but more on the mechanisms for supporting it.

User/Customer/Consumer:

ETSI TC TISPAN [i.45] defines the following "user oriented" terms:

- **User, End user:** The user is the actual user of the products or services offered by the Enterprise. The user consumes the product or service.

- **Subscriber:** The person or organization responsible for concluding contracts for the services subscribed to and for paying for these services.

- **Subscription:** A subscription describes the commercial relationship between the subscriber and the service provider [i.46].

- **Customer:** The customer buys products and services from the Enterprise or receives free offers or services. A Customer may be a person or a business.

It should be noted that in another TC TISPAN document [i.15], the following definition of "Customer" is provided:

- **Customer**: role that contracts for the services offered by a service provider based on a contractual relationship.

OGF defines a term "Service Consumer" [i.1]:

- A **Service Consumer** is an entity entering into an agreement with the intent of obtaining guarantees on the availability of certain services from the service provider. Service Provider (SP) is an entity entering into an agreement with the intent of providing a service according to conditions described by the agreement.

NOTE: Although the OGF Glossary [i.6] defines Service Requestor and OGSA [i.62] uses this term, WS-Agreement [i.1] uses Service Consumer, which therefore is used in this clause in the context of SLAs.

Despite the different terms used for customer in NGN and consumer in OGF the meaning of both definitions is broadly similar.

Service Provider

A term "Service Provider" is defined by the ITU-T as follows:

- **Service Provider (SP)**: A general reference to an operator that provides telecommunication services to Customers and other users either on a tariff or contract basis [i.13]. A Service Provider may or may not operate a network. A Service Provider may or may not be a Customer of another Service provider [i.14].

ETSI TC TISPAN defines the terms "Service Provider" and "NGN Service Provider":

- **Service Provider (SP) [**i.12**]:** entity providing a service to the subscriber.
- **NGN Service Provider (NSP) [**i.16**]:** An NGN operator role that offers NGN based services which share a consistent set of policies and common technologies. The NSP provides common functionalities e.g. user service authentication and identification, service control, charging, etc. Several Application Providers can use the same NSP to deliver applications to the Customers.

It should be noted that in another TC TISPAN document [i.47], the following definition of "NGN Service Provider" is provided:

- **NGN service provider:** entity offering IP based services, which shares a consistent set of policies and common technologies.

OGF defines Service Provider slightly differently in two different places. For the purpose of SLAs which is our concern here, we have this definition:

- **Provider (Service Provider) [**i.1**]:** A service provider is an entity entering into an agreement with the intent of providing a service according to conditions described by the agreement.

The term "Service Provider" is similar both for NGN and Grid in that sense it covers a contractual /agreement aspect with the customer (consumer).

5.1.3 Secondary Definitions

Having defined SLA, QoS and the parties involved, there is more detailed common terminology requiring consideration. These terms are largely taken from WS-Agreement [i.1]:

- **Agreement:** An agreement defines a dynamically-established and dynamically managed relationship between parties.
- **Business Value:** The business value is intended to represent the strength of an agreement in domain-specific terms. The value may be specified in terms of domain-specific qualities such as importance, cost and others.
- **Guarantee (Guarantee Terms):** Guarantee Terms define the assurance on service quality (or availability) associated with the service described by the service definition terms.
- **Initiator:** The agreement initiator is a party to an agreement. The initiator delivers an agreement offer to the responder.
- **Offer:** An offer is the description of the agreement relationship that is sent from initiator to the responder during agreement creation, indicating the relationship which the initiator would like to form. This offer is accepted or rejected by the responder.
- **Responder:** The agreement responder is a party to an agreement. The responder receives an agreement offer from the initiator and may accept or reject it.
- **Template (Agreement Template):** An agreement template is an XML document used by the agreement responder to advertise the types of offers it is willing to accept. In addition to the possible contents of an agreement document, a template may furthermore include information on constraints to describe a range of agreements it might accept.

5.1.4 Discussion

Agreement and negotiation

The fundamental concept is the SLA itself. This is established by means of a negotiation between the parties. Once the agreement is accepted by both parties, the association between them enters a usage phase in which the terms and objectives of the agreement are monitored and enforced. One standard for specifying an agreement in the Grid domain is WS-Agreement, standardized by the OGF in [i.1].

Negotiation has proven to be harder to standardize. The current status in the Grid domain is that a WS-AgreementNegotiation document [i.17] exists, but is not yet an OGF recommendation. Nonetheless WS-Agreement itself envisages the process of negotiation [i.22] including the ideas of offers, acceptance and rejection. It also includes the idea of a template, delivered by an agreement initiator, which contains the range of acceptable values of certain service description terms. The agreement responder may counter with a revised document which includes values within the ranges given in the first proposal. An alternative form of negotiation can be found in the Condor ClassAds Matchmaking mechanism, which is widely used within Grid infrastructures to provide a form of negotiation. Although the format of these contracts and the negotiation algorithm are specified, they have not been standardized.

Negotiation can of course be extremely simple - the Grid agreement initiator which can be the service provider or service consumer can make a single offer which the responder may simply accept or reject, which is negotiation only in the most trivial sense.

Service description terms

Service description terms are regarded as domain specific. It is the concern of the parties to agree on the meaning of these. The WS-Agreement specification envisages making use of other specifications to define the terms. Thus JSDL [i.39] is used in one of its examples to define such terms as FileSizeLimit and Individual CPUSpeed. As a more complicated situation and one with wide implications, there is no agreed way of enabling Grid services (provider and consumer) to come to an agreement about service description terms which concern the performance of the network such as latency, bandwidth and jitter. Examples of applications where this may be a concern can be found in the OGF document on Grid Network Services use cases from the e-science community [i.7].

It is relevant to mention here the GLUE Information Model, which is being widely used in Grid information systems (for example, in EGEE) to provide LDAP entries describing computational and storage resources in a Grid. The version used in production Grids is generally 1.3 [i.44] or earlier, but version 2.0 has just finished its Public Comment period in OGF [i.43]. GLUE may well be a good basis for defining service description terms.

5.1.5 Different types of SLA

We envisage formally four different types of SLA for operations of the Grid infrastructure over the NGN:

- Workflow Service-Level Agreements (W-SLAs), allows to negotiate for the performance of a workflow. This SLA is employed for the negotiation between the user and the Grid Service Provider as it characterizes a workflow in terms of QoS requirements and other execution constraints.

- Task Service-Level Agreements (T-SLAs) to negotiate for the performance of an activity or task within a workflow. This SLA is employed for the negotiation between the Grid Service Provider and the managers of resources providing services, such as the network service provider. It characterizes a task in terms of service steps and implicit or explicit resource requirements.

- Resource Service-Level Agreements (R-SLAs) to negotiate the right to consume a resource. This SLA might be negotiated without specifying the activity for which the resource will be used. The R-SLA characterizes a resource in terms of its abstract service capabilities and is employed for the negotiation between the Grid Service Provider, owned by the Network Operator, and the network service provider.

- Binding Service-Level Agreements (B-SLAs) to negotiate for the application of a resource to a task. In other word, an R-SLA promising network bandwidth might use a particular network session reserved and guaranteed with RSVP-TE, or a R-SLA promising parallel computer nodes might be applied to a particular task. The B-SLA associates a task, defined by its T-SLA with the R-SLA and the resource capabilities that should be met by exploiting the R-SLA. The B-SLA is suitable for the negotiation between the Grid service provider and the network service provider. In order to perform the described SLA management it is of fundamental to have local Grid Resource Management Systems (RMS) supporting the SLA negotiation.

5.2 Security

5.2.1 Introduction

Most interesting grid-specific interactions will involve a user, a client system, and a service provider. In this context, it is necessary that all three parties have a mechanism of identifying each other, and some policies around access controls, service level provision, data privacy, and data integrity. Furthermore, it may be necessary for third party services or intermediaries to become involved in a Grid interaction. There is also a consideration of establishing a contract or relationship between a user and service in advance, with an associated protocol and user profile. The scenarios will discuss how these issues are handled in each specific case: what is used as a user identifier; how do components authenticate each other; how is access control managed. Where possible, specific reference will be made to the relevant Grid standards.

5.2.2 Definitions

security principal: user, service, or computer which has one or more associated security identifiers.

security identifier: token (physical or digital) or piece of information which can be used to make decisions regarding the identity of the holder or access restrictions to a service, computer, or data.

5.2.3 Authentication

Given an X.509 [i.20] PKI infrastructure as the starting point for authorization, it would initially seem straight forward to perform authentication and authorization, however there remain many open aspects. It is necessary to decide what CAs are trusted, and what "domain" they are authorized to assert trust over, both in terms of identity namespace (known as the Distinguished Name, or DN, of an identity holder), and identity capability (such as user, service, and host certificates, or certificates authorized for particular actions such as data access or service execution). The International Grid Trust Federation (IGTF) http://www.igtf.net/ acts as a coordinating body for the three main Policy Management Authorities (PMAs) (Americas, Europe, Asia-Pacific) to establish standards for CA accreditation and CA-signing policies. The typical working mode is to simply accept this set of CAs and signing-policies without detailed review. Interestingly, these do not include common commercial CAs such as Thawte Consulting or VeriSign. The definition of "which CAs to trust" and "what do we trust this CA to sign" should, in theory, be decided by each autonomous site, however due to the plethora of CAs is typically accepted via a default package of CA certificates and signing policies which are loaded together at once. At the user-level, both from the command line and within browsers, this can be a difficult and confusing task. Furthermore, different CAs will have different policies regarding how strict they are about whose certificates they will sign. The strictness (or relative degree of security) provided by a particular CA is a matter of policy and not easily determined, measured, or compared. A difficulty for interoperability is the limited tools available for reviewing and verifying CA signing policies, leaving resource owners unsure as to whom they are allowing to access their systems. An impediment to usability (but not technical interoperability) of X.509 certificates is the burden and time delay of identity verification with Registration Authorities prior to the issuance of a signed digital certificate. This can often take several days to complete.

While Attribute Certificates, an extension to X.509 [i.20], are the standard mechanism for allocating roles to users in a Grid domain, there are no standards around the registration and issuing of these certificates. Furthermore, they are currently limited to users, however it is conceivable that services or hardware may need to be dynamically allocated roles in addition to a single static identifier. There are many opportunities to study more carefully the possible interaction patterns between users, systems, and services which make use of authentication, delegation, and roles.

A problem with X.509 is the fact that user certificates are more complicated than the typical username/password. Since many users will access the grid through multiple channels, digital certificates require the authenticator (typically the user, but possibly an third party service acting on the user's behalf) to possess the digital certificate and to be able to input that digital certificate to the authentication software chain. There are currently three models for doing this:

- via web-browser based digital certificates (over which the user and any server-side grid software has little or no control of the authentication protocol);
- via command line tools; and
- via proxy certificates stored in a "proxy server" and acquired by the user or a (possibly remote) application using a traditional username/password pair.

The interoperability of these three methods is limited, and users are often forced to use some combination of all three, where each authentication procedure will typically involve a "human in the loop". Users operating in a grid environment from multiple access points (i.e. multiple computers) will usually need to share the certificate between all participating systems. The process of moving certificates from browsers to the command line is complicated for the average user and time consuming, and yet still essential due to the limited capability afforded by purely browser-based X.509 authentication and grid infrastructure access. Users are often forced to place their certificate key pair on USB keys, copy them to multiple grid-enabled client machines (typically called "User Interface Node"), possibly in different administrative domains, and load the certificate into web-browsers on all client machines the user wishes to utilize for web-based access to grid resources requiring authentication.

Conversely, host certificates (and "standard" service certificates, discussed below) are "node-locked" and cannot be shared or moved between hosts without violating standard hard-coded rules regarding an association between a host and its identity contained within its X.509 digital certificate (as a matter of policy). Specifically, this constraint requires that the X.509 certificate contain an embedded hostname which matches the hostname of the machine which uses the certificate, and for services may require the certificate to contain a particular fixed identifier (for example, identifying it as an "email server" or "web server" certificate). There are several problems which arise from this:

- System administrators need to request new certificates if their network topology changes (i.e. when host names or domain names change).
- Many services do not support a standard service naming mechanism, and rather use "host" certificates. It is against best practice for a CA to sign multiple X.509 certificates with the same name (and valid for the same time period), therefore it is often the case that a single certificate is replicated multiple times within a given system, with one copy for each service. This consequently introduces maintenance issues when the certificates expire (typically on an annual basis).
- Certain network configurations (e.g. NAT, firewalls, and IP round-robin) make it difficult or impossible to verify a host name with a particular network request.
- It imposes the need to autonomously operate and administer a publicly accessible (i.e. Internet wide) server. In certain corporate settings and for smaller grid deployments this is often not practically possible.

Services have a range of different naming standards, and support for these "service" X.509 certificates varies. As mentioned earlier, in some instances it is necessary for services to share a host certificate between a set of services running on a single host. This has a technical implication/limitation that either the certificate is replicated for each service (inconvenient when certificate updates are performed, and services cannot be distinguished from each other by their digital certificate identity), or the services are run as the same operating system "user" in order for a single certificate to be shared.

A further variation on X.509 identity certificates are the use of proxy certificates, which violate the initial X.509 standard [i.20], but are accommodated by the IETF RFC 3820 standard [i.23]. Systems which accept proxy certificateswill, as a minimum, allow non-CA signing of certificates, and for full functionality will be prepared to equate a proxy certificate as an equivalent identifier as the primary certificate. There are many reasons why one or both of these variations may not be incorporated into services which provide X.509-based authentication, thus limiting the interoperability of such systems with grid services and users. Finally, an area which has not been extensively explored but which could have valuable properties is the use of service proxy certificates, perhaps associating a proxy certificate with a particular invocation or user-session of a service, or with a certain time-window. In summary, usage models for proxy certificates both within Grid and NGN environments could be studied more carefully to determine requirements and effective strategies or protocols.

The time-windowing of X.509 certificates is an essential property which is embedded within the certificate itself and therefore (like all other certificate properties) unchangeable. Use of these certificates requires reasonably precise time synchronization across all systems within a grid as any clock-skew may result in an erroneous rejection of a certificate due to an apparently invalid timestamp. This is particularly a problem near the creation and termination time points for a certificate. For proxy certificates, which are automatically generated and then immediately used for grid operations this is a critical issue. Other systems with a clock skew may see these proxy certificates as only being valid in the future and therefore refuse to accept them. A common problem is the expiry of a certificate after the start of a grouped set of grid operations but prior to its completion. Without a valid certificate it is impossible to continue to take actions to either roll back or resolve the inconsistent state the system will have entered. This implies the need to establish standards for time synchronization across a grid.

In order to address many of these issues with X.509 certificates and proxy certificates a system has been developed by NCSA called MyProxy [i.24] which allows proxy certificates to be stored in a central server and retrieved via different means by services or individuals using different means of authentication. The MyProxy API and capabilities are not standardized, and there is only one server implementation. The main risks introduced through the use of MyProxy are a centralized site holding numerous user certificates, and requiring (typically) only a username and password to retrieve a credential. The challenge is "getting a certificate into MyProxy". MyProxy server works by generating its own proxy key pair and then has the proxy public key signed by the user's local key pair. The generated proxy certificate is then held by the MyProxy server for a "medium" duration, typically measured in weeks, and is used to generate and sign "short lived" (hours to days) second generation proxy certificates which are then passed to users, services, and jobs which can successfully authenticate to the MyProxy server. The signing of the MyProxy public key cannot currently be done via a browser, therefore command line operations are required, including access to the user's key pair from the command line system. Due to the importance of the "MyProxy concept", it is seen as an essential area for further analysis, requirements capture, modelling, and standardization.

5.3 Charging

This clause provides an overview of charging concepts.

5.3.1 Introduction

Charging is a function whereby information related to a chargeable event is formatted and transferred in order to make it possible to determine usage for which the charged party may be billed. The charged party, for any chargeable event, may be an end customer or another service provider.

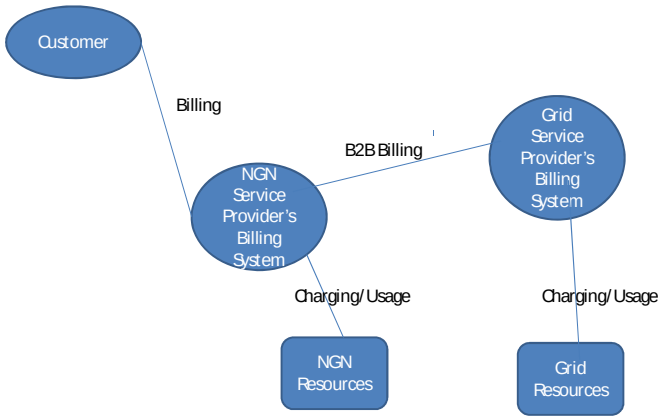


Figure 1: Example of a Charging Chain

5.3.2 Charging Terminology

The terms "Charging", "Billing" and "Accounting" are used, often interchangeably, thus causing confusion. Within the present document, the term "Charging" is used to describe the activity of collecting usage data from resources. This data may be used in the process of Billing customers, both end customers and other Network Operators/Service Provides. The actual Billing of a customer is a matter for the Service Provider and may be totally based on usage (charging data), partly based on usage or be totally independent of usage.

5.3.3 Offline Charging

Off line charging is a process where information on chargeable events and/or usage, are collected, concurrently with that resource usage, consolidated and made available for transfer to a billing system for processing at a later date.

5.3.4 Online Charging Service

Online charging is a charging mechanism where charging information can affect, in real-time the service rendered (e.g. prepay) and therefore a direct interaction of the charging mechanism with bearer/session/service control is required Charging information for resource usage is collected concurrently with that resource usage in the same fashion as in offline charging. However, authorization for the resource usage needs to be obtained prior to the actual resource usage. This authorization is granted by an online charging system upon request.

When receiving a resource usage request, the network assembles the relevant charging information and generates a charging event towards the online charging system in real-time. The online charging system then returns an appropriate resource usage authorization. The resource usage authorization may be limited in its scope (e.g. volume of data or duration), therefore the authorization may have to be renewed from time to time as long as the user's resource usage persists.

In conclusion, online charging is a mechanism where charging information can affect, in real-time, the service rendered and therefore a direct interaction of the charging mechanism with the control resource usage is required.

5.4 Service Discovery

5.4.1 Introduction

The decentralised, federated, and dynamic nature of a Grid computing environment requires directory services in order to locate data, services, and compute resources. There are many existing directory services which have been used in a grid environment (e.g. DNS, LDAP, UDDI), several which have been developed specifically for use in a Grid (e.g. MDS, R-GMA, GIIS/GRIS), and still more bespoke systems which are integrated into Grid computing environments.

5.4.2 Terminology

DNS Service Discovery: way of using standard DNS programming interfaces, servers, and packet formats to browse the network for services.

XML Web service discovery: process of locating, or discovering, one or more related documents that describe a particular XML Web service using the Web Services Description Language (WSDL). It is through the discovery process that XML Web service clients learn that an XML Web service exists and where to find the XML Web service's description document.

MDS (Monitoring and Discovery System): information services component of the Globus Toolkit and provides information about the available resources on the Grid and their status [i.18].

R-GMA (Relational Grid Monitoring Architecture): provides a service for information, monitoring and logging in a distributed computing environment [i.19].

GRIS (Grid Resource Information Service): holds resource properties, such as characteristics of a compute resource and network.

GIIS (Grid Index Information Service): configurable aggregate directory component. It accepts GRIS registry and provides aggregation services.

6. Case Studies

Case Studies are used to derive interoperability gaps by analysing several Grid infrastructures and comparative NGN scenarios in line with competitive business realities. The different use case scenarios focus on various aspects of interoperability. The list of these Case Studies is given in table 1 and the Case Studies are documented in annex A.

Table 1: Case Scenarios and focus of investigation

Case Scenario		Kind of application	Focus of investigation	Location of Case Study
1	Online media and entertainment	Content download, streaming	Authentication, Authorization Service Discovery, Video Selection, Video Download Video control, Charging, SLA and QoS	A.1
2	Integrated Emergency Management (IEM)	Integration of communication between people and transfer of information between people and control centres in a mixed fixed and mobile environment, for a critical application.	Security, SLA and QoS, Charging, Reliability, Discovery, Workflow	A.2
3	High Performance Computing	Data acquisition, data movement, pre-processing, processing, and visualization.	Security, SLA and QoS,	A.3
4	e-Health	Security, confidentiality, liability and ownership of data"	Security, SLA , QoS, charging and service discovery	A.4

The initial sections of each case study provide an introduction to the scenario and a possible instantiation in Grid and NGN contexts. The last section of each case study is devoted to the detailed gap analysis, where the NGN makes possible a core of higher-level Grid services supported by the network providers, in addition to meeting the basic requirements to network resources such as bandwidth, routing, and connectivity.

7 Issues, Gaps and Overlaps

This clause summarizes and brings together the issues that we have identified in previous clauses. Key issues, gaps and overlaps are identified by bold text.

7.1 Architectural issues

The issues here relate to the architecture of the overall distributed infrastructure: multiple layers, multiple network topologies, and, from different bodies of expertise, new overlapping ways of thinking about distributed services i.e. NGN and Grids.

- In the presence of a multiplicity of network technologies and the resulting integration problems, the vertical integration of network technologies is increasingly gaining in importance, since taken together, these elements are critical to NGNs and to the formation and operation of highly interactive, large-scale Grid infrastructure.

- Regarding end to end services, t**he quality of network services requested by Grid services need to be independent of the underlying networking technologies**. It is the responsibility of the network service provider to map and enforce the required QoS.

- Horizontal integration refers to the co-existence of multiple network service providers which may be required in order to underpin a single Grid application. These providers need to allow collaborative mechanisms for end to end service establishment. Each network service provider estimates what could be an efficient mapping of connectivity service requests to resources and then sets up the necessary resources for satisfying the required QoS and performance guarantees. If the mapping fails, it could try another mapping solution or reject the demand. Note that the network service provider will have to deal at the same time with online connectivity service requests, i.e. the mapping is done "in real time" and with the use available traffic engineering mechanisms in the network.

- **Reference model: While OGSA provides a software architecture model for Grids, it falls short of providing a complete system architecture.**

7.2 Service capability and operational issues

Based on the case studies captured in the annexes, this clause groups the gaps and overlaps by the topic areas introduced in clause 5. The areas currently selected are:

- Security, including authentication, authorization, protection and trust.
- Service Level Agreements and QoS.
- Charging, which includes the activity of collecting usage data from resources.
- Service Discovery.

Furthermore some gaps and overlaps which do not fall into the topics introduced in clause 5 are also described.

For each item, it is stated which of the case studies the gap or overlap is relevant to but for some cases an item may arise from knowledge and review of the current state of the art and not be related to any specific case study. It is also stated whether an identified deficiency is related to Grids or NGN or both.

7.2.1 Issues relating to SLA and QoS

- **There is no Grid standard for SLA negotiation available yet.** This is partly due to the complexity of assimilating different requirements for negotiation. As mentioned in clause 5.1, a draft specification WS-AgreementNegotiation is under discussion in OGF.
- For some long term distributed infrastructures, such as in the eHealth case study, there is a **requirement to maintain the SLA performance throughout the system's long lifetime**. This is true whether the system is based on Grid or NGN.
- For certain critical types of distributed infrastructure, such as in the eHealth and IEM case studies, the need is for **effective and timely alternative action when the terms of the SLA are violated**, in order to maintain a temporarily adequate level of service. This requires high reliability from the monitoring and metering services. This is true both for Grids and NGN.
- **For certain complex distributed systems, multiple applications may coexist and have different priorities**. For the eHealth case study, life support systems providing an active data feed monitoring a patient's condition would be prioritized above X-ray images for a broken arm. Since the geography, connections and computational/data resources of these different applications may overlap, effective network and other resource monitoring would be needed.
- **The structure of service description terms is defined, but the names and semantics of them are not.** In Grids, the style of working is that other specifications and models, such as JSDL for computational resources, are adopted in order define these properties. Some such description will be needed in order to agree the names and semantics of data transfer. Furthermore some such description will also be required when we come to consider the relationship with networks, where, for the sake of interoperability of Grid services deployed across a diversity of networks including NGN, it may be necessary to come to a decision about such terminology as throughput, jitter, round trip time and reliability. An alternative to the "adopt another specification such as JSDL" approach may be to move towards descriptive means offered by the semantic web.
- The Grid service consumer application should ideally not be concerned with low level information, such as CPU speed and network bandwidth etc. **The application service should be able to define QoS parameters at a high level, for example response time, etc.** The Grid infrastructure should be able to take care of mapping these high level parameters to low level ones and as discussed elsewhere this is mapped into specific network parameters for each network service provider.

- **There are many types of situation in which multiple providers may be required**. For instance the coexistence and interoperability of providers along the end to end service value chain include situations such as:
  - The provider selection process:
    - Multiple alternative providers from which one is chosen on the basis of some criteria, which could include SLA offers and business values.
    - Multiple alternative redundant providers for robustness.
  - Workflow intermediary: The service requestor comes to an agreement with the workflow service, which in turn comes to an agreement with its constituent services which may not be easily partitioned, if the constituents are a heterogeneous mix.
  - Virtual service provider: a service consumer may negotiate with a service provider which implements a distributed application. The service provider will then require a mix of on-demand computing capability from multiple providers and data transfer between them.

7.2.2 Issues relating to security

Authentication in Grids is primarily handled by X.509 [i.20] certificates and proxy certificates. NGN has proposed PKI mechanisms common in mobile units (e.g. SIM cards) to be expanded to all NGN User Equipment as a possible solution for authentication, in addition to a mechanism based on shared secrets [i.47]:

- The issue of key distribution, binding UE to a particular user, and trust of UE identity tokens has many similarities with user, host, and service identities in Grids, and both lack standards to guide development.
- **There are significant standards gaps around the issue of authorization in a Grid domain.** SAML (Security Assertion Markup Language) [i.48] and XACML (eXtensible Access Control Markup Language) [i.49] are the only two broadly applicable authorization standards, however their complexity makes them difficult to use in practice. **There is a need for a simplified authorization policy language,** perhaps similar to that provided by the Grid Access Control Language (GACL) [i.50]. **Furthermore, there is significant scope for standards concerning authorization policy management: sharing, merging, and updating security policies in an efficient, clear, and secure manner.**
- **There are limited standards related to the operation of a security infrastructure.** The International Grid Trust Federation (IGTF) http://www.igtf.net/ provides broad guidelines, and the Policy Management Authorities (PMAs) are responsible for accreditation of member Certificate Authorities (applicable within the X.509 PKI domain), however recent security incidents have suggested that accredited PMA members have widely varying operational standards. Standards concerning the operation and accreditation of "roots of trust" in PKI-based identity systems.
- Groups, Roles, and Attributes provide an important mechanism for providing flexible identity contexts within a Grid computing domain. Standards exist for defining these aspects, but **there is a lack of standards regarding their use as part of a dynamic Virtual Organization.** A standard model which defines a Virtual Organization, membership, capabilities, and policies would provide an operational framework to improve VO-centric services, in contrast to the current focus on either user or host/site centric services.
- **There are no standards for data provenance, an important issue in many domains: science, medicine, and financial services, to name a few. Only bespoke solutions for auditing data provenance are available.**

7.2.3 Issues relating to Charging

- Quite simply, how to bill for distributed services by providers discovered and selected dynamically is likely to be a problem. This applies both to NGN and Grid.
- In a situation where services are being offered by multiple providers and so too would networks, producing a single bill for the customer is an issue.

- Although it unlikely that Bills based on usage will be submitted to Integrated Emergency Management (IEM) users, the collection of usage data provides an important tool for Service Providers.

- It should be noted that the NGN model allows, but does not mandate, Billing On Behalf of Others (BOBO) [i.15]. Thus a customer of an NGN Service Provider could elect to enable users to purchase many products via her NGN account (e.g. communications, video download, books, soft drinks from vending machines, etc.).

- **Whilst standards exist for the structure of Grid usage records [**i.51**], these could be usefully being aligned with NGN Charging Detail Records (CDR) specifications [**i.52**] (OVERLAP).** This applies to all scenarios.

- **No standards exist for on line charging for Grid Services.** These could be developed jointly with the evolving NGN Standards (GAP).

- The use of these records for billing customers should not be the subject of standardization allowing Service Providers flexibility in developing and changing their business plan.

7.2.4 Issues relating to Service Discovery

- In a patient monitoring system (in the eHealth case study), a sensor network needs to coordinate the sensors and associate each with its functions, location and patient. Service registry mechanisms can be adapted for this purpose, but not typically used for device identification or where (such as a fast moving A&E situation) there is a high degree of dynamism. This illustrates **the need for a service/component coordination standard**, such possibly along the lines of the work undertaken by the OGF CDDLM Working Group, which has recently abandoned attempts to complete the CDDLM standard.

- In a Grid environment the usage of UDDI in assisting the discovery process has proven to be inadequate because of its static nature. GT4's MDS has gained much recent usage, as an alternative. There is also the potential for it to be combined with semantics though OWL. Given the inadequacy of UDDI, **a standard is required for grid service registry that can support VO-style authentication, a high level of dynamism, and the inclusion of service state rather than purely static details**.

- **The application of directory services such as LDAP to NGN services needs to be carefully considered.** While LDAP is currently the dominant standard, other standards or approaches may be more appropriate for NGN.

- **There is significant overlap of the capabilities provided by various Grid-domain directory services and service discovery mechanisms.** Some of these have been standardized, however most are bespoke solutions lacking any standard. There is significant scope to analyze the requirements of these different systems and work towards a common grid directory service standard.

7.3 Gaps and overlaps arising from the EU FP6 Grids Survey

A short questionnaire was sent to the selected key EU FP 6 projects. Selection criteria are listed in TR 102 659-1 [i.21]. The aim of this questionnaire was to identify whether IST projects with a Grid focus are interfacing with standards. If so and if they have some brief to focus on standards, whether there are interoperability concerns.

Ten responses were got out of 39 questionnaires sent by the STF 331. Responses were received from a wide range of projects including general infrastructure and specific application areas. The main application areas the projects aim to implement include eHealth, DHCM, aerospace, design and engineering, data mining, media, banking, medical imaging, bioinformatics, automotive industry, construction, pharmaceutical, metrological, oil & gas field, reactor safety. Some projects are testing on large grids. Others are not specifically directed at large grids or are testing ideas at a stage earlier than scaling up would be appropriate. One project tested on a mobile grid and another project is testing access to a Grid. Projects focus on a variety of standards which may be grouped to major topics such as foundation, SLA, job submission, security, and workflow.

Gaps and overlaps arising from the projects are summarized below:

- A few projects aim to work on interoperability between a wide range of standards. Several projects comment on **the need to interoperate with Grid middleware in general** (interoperability with a specific middleware stack, the gLite). A few projects focus on a small number of standards.

- Some projects do not address interoperability between implementations. 3 projects had to **face interoperability problems of different WSRF & WS-Notification implementations**. Other implementation **interoperability problems concerned workflow and SAGA**. Some projects mentioned interoperability as a future problem even if it was not a current focus.

8 Way Forward

NOTE: This clause will contain recommendations to address the issues, gaps and overlaps identified in clause 7. For example on the topic of a Grid Reference model.

While OGSA provides a software architecture model for Grids, it falls short of providing a complete system architecture. The next phase of the ETSI work could productively include developing a common understanding, possibly even a reference model. (The old EGA developed one, which has not been taken up in OGF). Such an RM would provide a common language for standards and goals.

Annex A:
Case Studies

A.1 Case Study 1 - Online Media and Entertainment

A.1.1 Scenario description

There are two main categories of entertainment experiences, depending on the amount of interaction: consumption and interaction. Consumption of content (e.g., video on demand) requires limited user interaction. Other user interaction intensive scenarios, such as online gaming, push more demand on the network based upon whether they are functional for guaranteeing, for instance, response times. In the following we concentrate on the consumption of content.

The content provider provides the media content that the consumer will experience. The integrator or publisher of the media service ties the offering together and exposes it to the consumer. The interactions between actors may change, and the entertainment content may change as well; therefore it is a key requirement to be able to autonomously manage resource allocation as well as enabling dynamic discovery and interaction of the provided infrastructure and services.

A simple case of content consumption is a video download, i.e. a service user wishes to download a video. In this scenario the user:

- is authenticated and authorized;
- discovers the services available;
- selects a video for download, and
- downloads the video.

The activities related to this scenario may not be undertaken in the given order. For example, authentication and authorization may be undertaken after service discovery and video selection.

In an extended scenario the following additional activities may be undertaken:

- the client negotiates, agrees, accepts QoS (especially if he selects a service that allows to consume a video or film immediately, i.e. video on demand, IPTV);
- service is declined due to User Profile restrictions (e.g. the User is under 18 and is restricted from downloading the video "Making ETSI Standards" as it is rated 18 due to the high level of violence and bad language);
- security, and
- billing.

For the moment we stick to the simple scenario. In the following we describe a video download in a Grid environment and the same service provided by an NGN enabled network.

A.1.2 Video download in a Grid environment

The flow of information for a simple video download in a Grid environment is shown in figure 2. A user using a Grid client has to be authenticated by a Grid manager before he can search in the database of the manager for a movie. The search result will include Grid nodes from where the requested video can be downloaded. The user selects a Grid node and downloads the video. The inscriptions in round brackets, i.e. WS-Security, WSRM and GridFTP, refer to the kind of Grid standards used in this scenario. The described scenario is based on the IBM tutorial "Building a grid using Web services standards" [i.38].

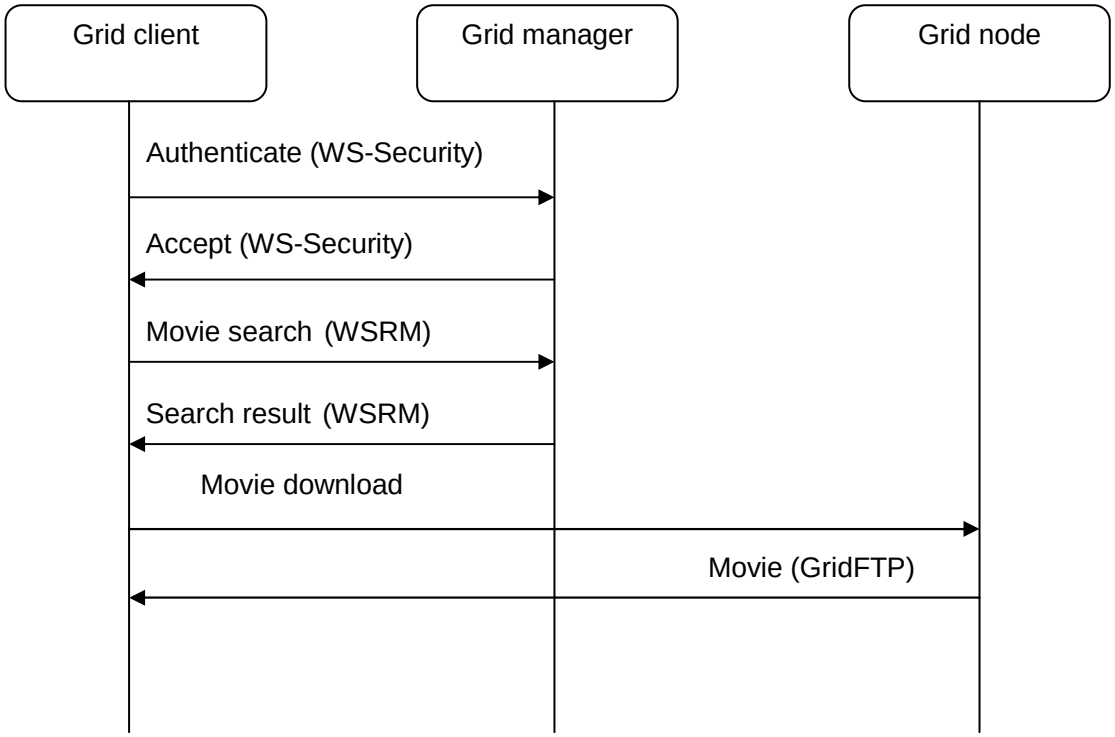


Figure 2: Information flow for a video download in a Grid environment

Figure 2 only shows the flow of information between three instances. However, in a Grid environment there may exist several Grid nodes that provide various services to the Grid users. This distributed character of Grid is indicated in figure 3.

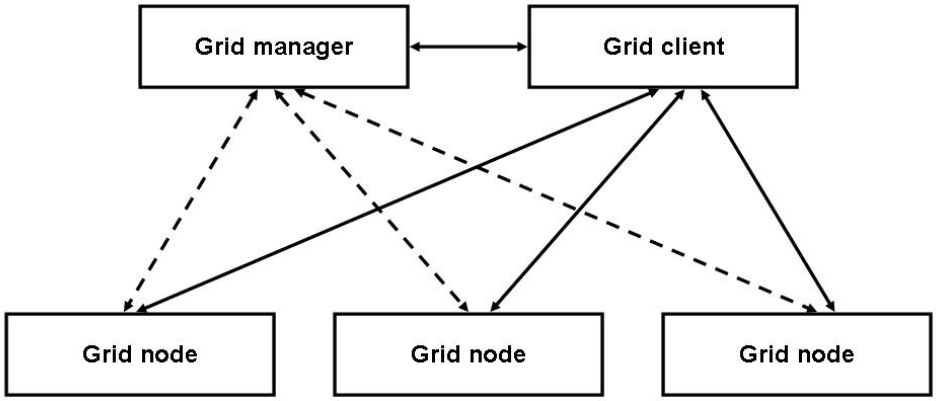


Figure 3: Distributed Grid environment

In the scenario, the Grid manager knows the available Grid nodes and the services, including the multimedia content, offered by this node. The Grid client only needs to know the Grid manager to find an appropriate service and the required multimedia content. Authorization and authentication is needed for all communication between Grid client, Grid manager and Grid nodes. In the following, we will describe roles and responsibilities of a Grid manager, a Grid node and a Grid client.

A.1.2.1 Grid manager

The Grid manager is responsible for **handling the security of the system** (through WS-Security and a token exchange mechanism), for **storing movie data**, for **accepting movie submissions and requests**, and for **validating these requests** to enable the Grid client to communicate directly with the Grid nodes. The Grid manager can also **respond to queries about Grid properties** (through the WS-Resource Framework) and through a basic concept of WS-Distributed Management (WSDM) control the availability of different nodes in the system and report their availability accordingly.

The Grid manager includes three roles:

1) Communication with the Grid client to provide client services.

2) Communication with the Grid nodes for exchanging movie data.

3) Management of the movie distribution to the Grid nodes, based on the status information of the individual Grid nodes.

Therefore, the Grid manager is both, a **Web service provider** (to the Grid client) and a **Web service user** (to the individual Grid nodes).

The Grid manager also plays a **secondary security role**, although one obviously intertwined with the other roles, both certifying connections with the Grid client and validating requests between the Grid client and Grid nodes during the operation of the Grid.

A.1.2.2 Grid node

The Grid node **accepts movie submissions** (and sends movies back) via the Grid client using WS-Reliable Messaging, a system that divides the communication of very large files into smaller pieces that can more easily be verified and acknowledged. The Grid node also supports basic WSDM, **resource properties** (for retaining information about available storage space and abilities), and WS-Security for ensuring that **requests are valid** at all times. Finally, the Grid node supports WS-Notification to enable a client to **monitor events** on each Grid node.

A.1.2.3 Grid client

The Grid client provides a complete **interface to all the components**, including using WS-Security, WSDM, WSRM, and WSDM to submit, retrieve, and exchange information status data about the Grid:

- **Login:** You need the client to log in to the Grid system so the client can start submitting, searching, and retrieving information. The purpose of Login is simply security. You need to be absolutely sure that only **certified users** can use the system.

- **Connect:** This creates a connection between your client and the Grid manager, which you use to exchange information between the client and the Grid manager during the course of a session.

- **Search Movie:** Search for an existing movie already submitted to the system.

- **Retrieve Movie:** Retrieve the movie from the Grid node storing it so you can play it on your client.

- **Submit Movie:** This submits a movie into the system for storage.

These operations are client-based. You obviously need to provide the functionality that supports these operations on the Grid manager, too.

A.1.3 Video download in an NGN environment

Video download in an NGN environment is provided as the Multimedia Content on Demand within the IPTV service and belongs to entertaining IPTV service categories [i.12].

Content on Demand (CoD) is a service provided for the users that can select their required content with the assistance of the Electronic Programme Guide (EPG) at the user preferred time.

NOTE: The content is transmitted uniquely (unicast) to that consumer who can usually use VCR-like functionalities (for example, fast-forward, rewind or pause) to control their viewing of the content. A special form of Content on Demand (CoD) is Video on Demand (VoD).

For this use case, the Content on Demand service provided by the **dedicated subsystem for IPTV functions in NGN** [i.25] has been selected.

A.1.3.1 Service initialization

The IPTV service initialization includes two functional phases:

1) UE start-up (the required functional steps are depicted in figure 4).

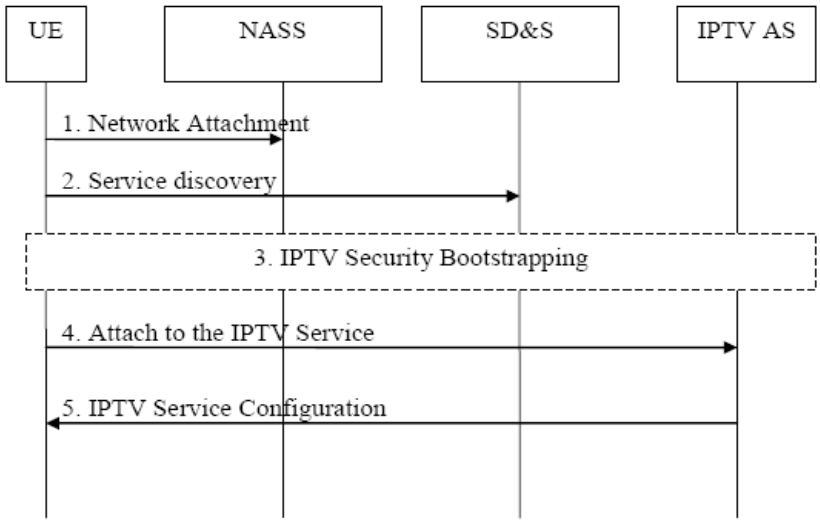


Figure 4: UE start-up procedure

In the first step, the UE attaches to the network (1). The UE may be passed data for service provider discovery. Then, the UE discovers service providers and services (2). In step 3 (IPTV security bootstrapping), the UE performs authentication, key management. During this procedure IPTV subsystem may register IPTV UE in other service level subsystems on behalf of UE. The UE is then attached to the IPTV Service (4). Finally, IPTV Service Configuration follows (5).

In steps 4 and 5, the UE navigates and selects a service from available service offers. IPTV AS may update IPTV user profile, presence of behalf of IPTV as a part of the SD&S process.

2) Service discovery and selection.

The service discovery and selection process is used by the UE to attach to the network, acquire list of service providers and make service selection from the selected service provider. There is a step preceding SD&S process including setup and initial UE configuration.

Figure 5 presents steps in the SD&S process.

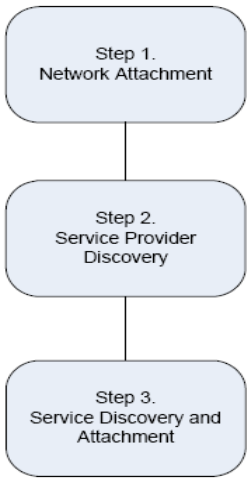


Figure 5: High Level SD&S Process

Step 1: **Network Attachment**: UE establishes connectivity to an IP-network and obtains network-based service configuration data (such as IP address, network mask, DNS, domain name, and others). During this step UE may be passed data for service provider discovery, e.g. a container option sent by DHCP server listing the source IP address of the Service Provider server or list of registered IPTV service provider servers using DNS SRV mechanism in accordance with RFC 2782 [i.26].

Step 2: **Service Provider Discovery**: UE collects the location (entry points) for discovering service providers and retrieves information about available IPTV Service Providers, learns the location of their one or more Service Discovery (SD) Server.

Step 3: **Service Discovery and Attachment**: during this step UE acquires information about available IPTV Services from one or more Service Discovery (SD) Servers, navigate, select service from the service offering and attach to the service. The procedure used to activate a particular IPTV service is typically service specific. Authentication is performed at this step.

Different mechanisms are available for Step 2 and Step 3, e.g. those defined in DVB-IP [i.27] can be used.

A.1.3.2 Functional entities and flows for the CoD service

In this clause the functional entities involved in CoD service and generic flows between them are described provided that the UE has been attached to the network (see figure 6). The figure does not mandate placement of functions. DRM flows are not included.

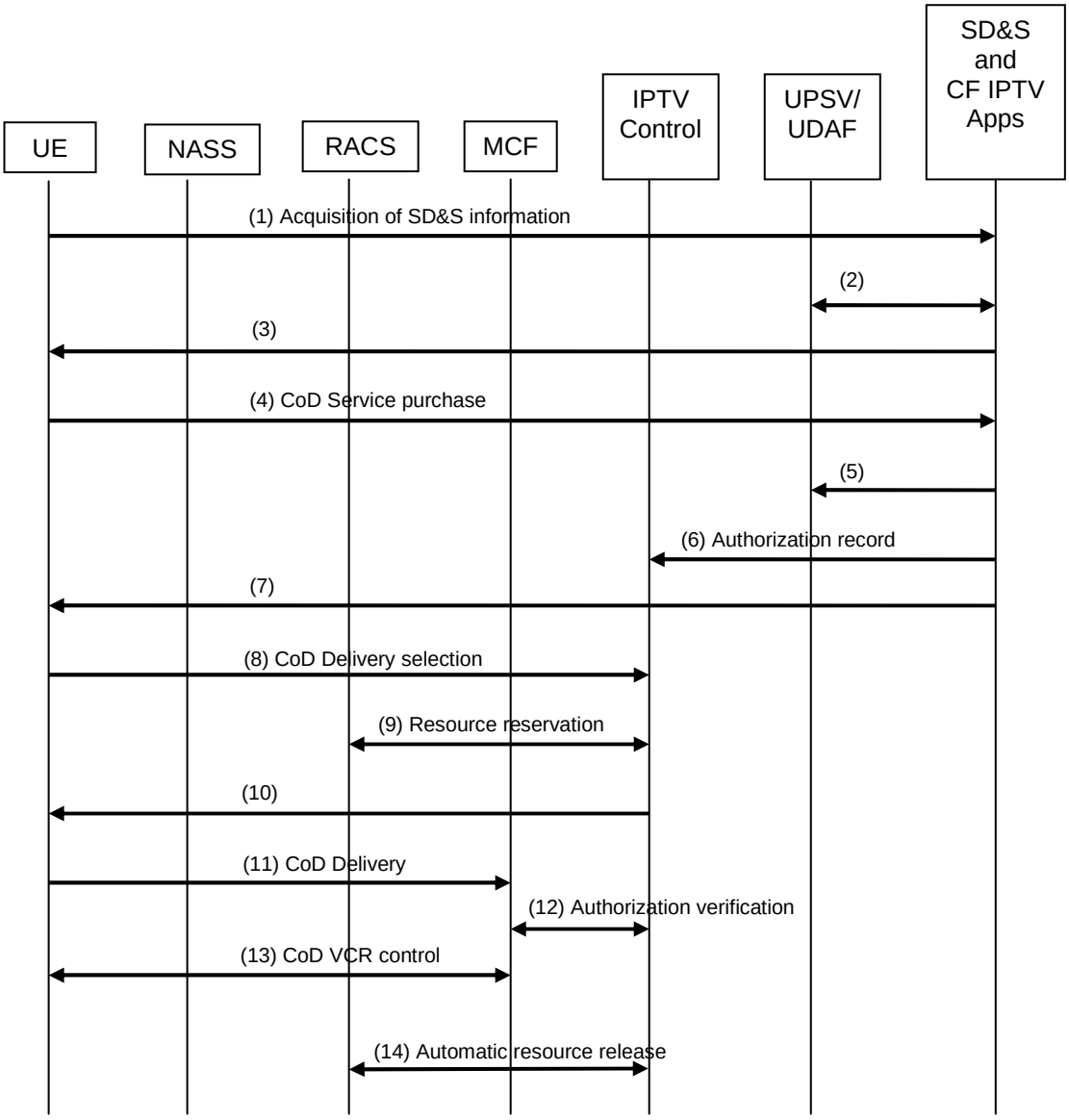


Figure 6: NGN IPTV CoD procedure

The following functional entities are involved in CoD service:

- **UE (User Equipment):**

  UE provides user interactions and control over delivery of IPTV and other NGN services. **User interactions** may include service discovery, selection and authorization.

  IPTV terminal processes serviced multimedia and presents it in user acceptable format. **Multimedia processing** may include requesting multimedia asset in supported encoded format, decoding and presenting it to the user in acceptable format, trick mode operators, channel change.

- **NASS (Network Attachment SubSystem) and RACS (Resource and Admission Control SubSystem)** provide Transport Control Functions in NGN such as:

  - policy control;
  - resource reservation and admission control;
  - IP address provisioning;
  - network level user authentication;
  - access network configuration as defined in TISPAN.

- **MCF (Media Control Function):**

  In IPTV dedicated subsystem MCF acts as UE point of contact for requested delivery of the selected IPTV service. It provides functions such as:

  - Handling media flow control of MDF (not applicable for multicast e.g. Linear TV).
  - Monitoring the status of MDF.
  - Managing interaction with the UE (e.g. trick mode commands).
  - Handling interaction with the IPTV control function.
  - Keeping an accurate view on status and content distribution related to the different MDFs that it controls.
  - Selecting an MDF, in the case an MCF controls multiple MDFs.

- **IPTV control:**

  - Checks if UE has been authorized by the Customer Facing IPTV Application to use IPTV Service Control and Delivery Functions.
  - Provides selection of the Media Control Function during the IPTV service selection (optional in case of one to one relationship between IPTV Control entity and Media Control Function entity).
  - May retrieve in NASS the geographical user localization, to select the Media Control Function entity.

- **UPSF (User Profile Server Function) / UDAF (User Data Access Function)**

  UPSF, as defined in ES 282 001 [i.30], is responsible for hosting a set of user related information, amongst:

  - service-level user identification,
  - numbering and addressing information,
  - service-level user security information: access control information for authentication and authorization,
  - service-level user location information at inter-system level,
  - service-level user profile information.

- **UDAF** knows the location and gives access to user data. An instance of it can be either GUP server if data federalization approach is selected, known NGN application, or other legacy solutions.

- **SD&S (Service Discovery and Selection) and CF (Customer Facing) IPTV Applications**

- **SD&S** provides description information for discovery of the service list for Live TV and selection of these services or on-demand IPTV services such as CoD.

- **CF IPTV applications** provide the server side functions to enable customer facing IPTV applications, expose IPTV services to other NGN application and manage IPTV subsystem. This includes service provisioning, service selection and authorization of IPTV services.

Generic flows between functional entities are described below:

1) UE (User Equipment) requests SD&S (Service Discovery and Selection) information from SD&S.
2) SD&S verifies user profiles from UDAF (User Data Access Function) / UPSF (User Profile Server Function).
3) SD&S replies service offers to UE.
4) User selects a service from the offers. UE requests the selected service from Customer Facing IPTV Applications.
5) Customer Facing IPTV Applications, optionally creates billing event, e.g. for on-line billing, and sends it to UDAF/UPSF.

6) Customer Facing IPTV Applications optionally creates authorization record (play ticket) to authorize content delivery.

7) Customer Facing IPTV Applications replies the location of IPTV control and optionally ticket data to UE.

8) UE requests IPTV control the location of MCF (Media Control Function). Optionally ticket data is supplied.

9) IPTV Control selects MCF based upon operator defined criterions and requests RACS to allocate resources between the end-points. Distributed RACS interfaces are allowed.

10) IPTV Controls replies MCF location to UE.

11) UE requests MCF to deliver media using reserved session and associated resources. Optionally ticket data is supplied and the ticket punched.

12) MCF optionally verifies user credentials to request multimode delivery.

13) UE utilizes VCR (Video Cassette Recorder) style control (e.g., fast-forward, rewind or pause, etc.) over media to MCF.

14) Automatic resource release follows session termination, which can be initiated either by end point UE or MCF, or by an IP network. Although it is not necessary to explicitly tear-down an old reservation, it is recommended that during normal operation MCF or IPTV Control send a teardown request to RACS as soon as the session has finished.

A.1.4 Comparison

The video download scenario in a Grid environment and in NGN includes the similar activities. These are authentication, authorization, service discovery, video selection and video download. An IPTV- or video on demand- environment may also offer video control functions. Even though the activities are similar, different mechanisms and standards are used for their realization. Table 2 provides an overview of the mechanisms and standards used for the different activities by both scenarios.

Table 2: Realization of activities in the video download scenario

Activity	Grid Protocols/Standards	NGN Protocols/Standards
Authentication, Authorization	WS Security	Combination of authentication and authorization is used. In some cases it may be performed separately on the IPTV terminal device and the end-user(s).
Service Discovery	WS Resource Framework WS Resource Properties	The information for service discovery and selection services is assembled according to the Service Discovery and Selection (SD&S) protocol, which for multicast (push) services is transported in IP packets according to the DVB SD&S Transport Protocol (DVBSTP) and for unicast (pull) services such as CoD is transported via HTTP.
Video Selection	WS Resource Framework WS Resource Properties, WS-Notification	RTSP (Real Time Streaming Protocol) is used to access such Content on Demand Services. The protocol used for unicast delivery (used for Content on Demand) of SD&S information is HTTP.
Video Download	WS Reliable Messaging, Grid FTP	MPEG-2 packets are encapsulated using the Real-Time Transport Protocol (RTP) or the packets are delivered directly over Internet protocols (that is, not involving an MPEG2 transport stream).
Video control (e.g. trick-mode (VCR) operation including pause, rewind, fast forward, resume, and stop.	*Not available*	RTSP (Real-Time Streaming Protocol) over TCP for the delivery of unicast on-demand content.

A.1.5 Gap analysis for the video download scenario

In order to provide a Grid-based video download service over NGN or an NGN-based video download service over Grid, the mechanisms used in both scenarios have to be compared. If for example, NGN requires more information for authentication and authorization than Grid, it might not be possible to offer a Grid service that is realized by NGN. Thus, a gap has been identified.

In the following, we compare the capabilities of the mechanisms used in Grid and NGN for the different scenarios and identify gaps and overlapping functionality.

A.1.5.1 Authentication and Authorization

NGN:

For managed NGN services involving CoD, it is typically the case that the end-user (subscriber) is authenticated and, subsequent to successful authentication, authorized to access service(s) and the content contained therein.

Depending upon circumstances, authentication and authorization functions may be performed separately on the IPTV terminal device and the end-user(s). In other cases, additional devices in end-user premises, such as a delivery network gateway and other end-user devices may require authentication before service access is authorized.

The combination of authentication and authorization can be considered to effect positive access control on the terminal device and end-user for purposes of service and content acquisition prior to use [i.28].

In general, the scope of the authentication in NGN includes [i.29]:

- **User Equipment (UE) authentication** (one or more devices allowing user access to network services delivered by TISPAN NGN networks).
- **Subscriber authentication** (the person or organization responsible for concluding contracts for the services subscribed to and for paying for these services).
- **User authentication** (the user is the actual user of the products or services).
- **Service authentication**.

For the IPTV service, i.e. including the CoD, the user and user equipment authentication and authorization take place at several layers:

- **User authentication at the network transport layer [**i.30**].**

  It provides the functions to identify, authenticate and authorize UE which connects to the Network Functions (NASS) (e1 interface - figure 7). Two authentication types are defined for NASS [i.31]: implicit authentication, for example based on line identification, and explicit authentication, for example based on EAP (Extensible Authentication Protocol). It is a matter of operator policy which form of authentication is applied. The applicable identities are: user identity and credentials provided by the user or UE identity. This procedure also involves the authorization for access to the network based on the user profile. A user specific configuration profile, related e.g. to QoS, may be downloaded from the home NGN network to the visited NGN network. When the authentication is successful and the UE is authorized to use access network resources, configuration of access network based on user profile is performed. The profile information includes at least the identity of the line (line ID), user identity and the user network QoS profile, which may be the QoS profile downloaded from the home NGN network or a default profile, and the identity of the IP edge (IP edge ID). It should be noted that this step may occur prior or during the IP address allocation procedure.

  The most prevalent automatic method currently used to attach to the network is the PPP (Point-to-Point Protocol) based authentication or DHCP (Dynamic Host Configuration Protocol) based network attachment with IEEE 802.1x [i.32]/PANA (Protocol for carrying Authentication for Network Access)/Implicit Access authentication.

- **User authorization at the service control and delivery layer:**

  At this layer, user authorization is done at Ct2 reference point (see figure 7). Ct2 is the optional reference point between UE and IPTV control. "Optional reference point" refers to a reference point only required in some of the operational modes: proxy, redirect, coupled or decoupled). One of its functions is to provide enough information for IPTV Control to check that UE has been authorized (by the Customer Facing IPTV Application) to access the requested resources.

  RTSP for interactive service control over IP multimedia delivery as defined in DVB-IPI [i.27] is used at the reference point between UE and IPTV control. Security considerations discussed in section DVP-IPI [i.27] apply. As this DVB specification is based on RTSP and HTTP, the same security considerations apply as with these protocols (see related RFCs). It should be noted that DVB-IPI has decided not to specify security and authentication for Phase 1.

  Optionally HTTP Digest Access Authentication can be applied to RTSP control messages as defined in RFC 2069 [i.34].

- **User authentication at the application layer:**

  It is used for UE authentication and authorization during initialization (Tr is the reference point between UE and Customer Facing IPTV Applications).

NOTE: UE authentication may also be done directly via e2 reference point (between NASS and Customer Facing IPTV Applications - see figure 7).

HTTP Digest (see RFC 2617 [i.63]) is recommended on the Tr interface. MD5 digest algorithm is recommended as defined in RFC 1321 [i.64].

Authentication at the application layer is required in the case of managed services for which an end-user (subscriber) has a direct relationship with the provider of the CoD service (e.g. pays for the service directly not via his/her contract with the NGN service provider). The service provider will typically require the terminal device and/or the end-user (subscriber) to be authenticated in a secure manner, in which case authentication means the produce of presenting some identity information in a secure manner that can be correlated with the service provider's subscriber database. Subsequent to end-user (subscriber) and/or terminal device authentication, a service authorization mechanism is used to authorize and grant access to specific services and content contained therein according to service and subscriber provisioning.

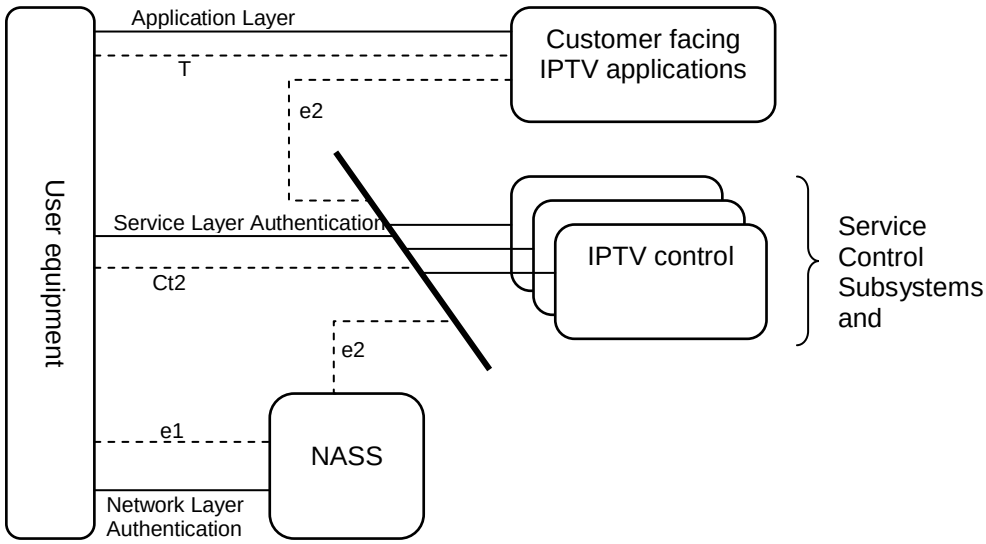


Figure 7: NGN CoD authentication layers and reference points

Grid:

Authentication and **authorization** in Grid systems are commonly realized through applying the Web Services Security4 SOAP Message Security 1.1 [i.56] which has been standardized and developed since 2004 via a committee in OASIS-Open (http://www.oasis-open.org/home/index.php). It ensures that individuals are entitled to use a particular resource or system. WSS allows embedding security into the requests exchanged between clients without affecting the request itself. WSS is a wrapper around all the other Web services solutions and forms a core part of all the Web services-based communication.

WSS includes details on the use of certificate formats such as **x.509 [**i.20**]**. In detail, the Grid utilizes public key or asymmetric cryptography for authentication of users, resources and services whereas each of them has a key pair, a public and a private key. The public key is made public and the private key is kept secret. While encryption and **authorization** is performed by means of the public key, decryption and digital signature, which are attached in the headers to SOAP messages, are realized with the private key. However, just generating a key pair does not allow accessing a resource in the Grid. A trusted authority of the Grid, the Certificate Authority (CA), has to sign the user's key pairs in order to confirm the user's identity. The certificate files are encoded with the **x.509 [**i.20**]** format. The binary security tokens of x.509 certificates are included to the exchanged messages. This ensures that movies are downloaded by valid users, whereas the user has to provide the user's signature in the communication. In addition, the grid client talks to the grid manager before downloading a requested movie file to the grid node. To ensure that the client is entitled to talk to the node, signatures are used to provide temporary authentication for the transaction. It should be noted that from the standard's point of view: Username Tokens, X.509 Tokens, SAML Tokens , REL Tokens and Kerberos Tokens can be included as well as how to include opaque encrypted keys as a sample of different binary token types.

The roles of users, administrators, and services are applied in Grid environment. Each role has to be authenticated in order to act in a Grid system. In addition, authorization rules for regulating the access to services have to be established. The services can be access through a portal that uses the certificate of the user to login into the Grid and lookups the services for which the user has been authorized by an administrator.

Gaps and Overlaps:

Similar roles:

The roles that have to be authenticated in the two systems are similar. In the following a number of elements of the NGN and Grid system are compared and concluded with possible overlaps and gaps between them:

- NGN user ↔ Grid user

  There are end users in both systems, but their authentication methods differ related to standards. The Grid user is authenticated through a certificate, the NGN user is authenticated at different layers corresponding to the NGN architecture, as described in clause A.1.5.1.

- NGN user equipment ↔ Grid portal

  The user equipment in NGN can be compared with the user portal in a Grid. Both hide and access the underlying layers of the system. However, the user in a Grid uses services provided by a Grid middleware to interoperate with the Grid. The user equipment of the NGN allows interoperating with the whole NGN system since the UE has been authorized related to a user's profile before. However, the methods of the authentication standards differ strongly, and may therefore do not interoperate.

- NGN service ↔ Grid service (or resource)

  The access of services in both systems has to be authorized by profiles that are related to users. The access of resources in Grid is authorized by the applying WSS. In NGN, the data related to user profiles can be located in several Functional Entities (FEs): Both, UDAF (NGN User Data Access) FE and UPSF (User Profile Server) FE may be used. Optionally, IPTV user profile information could be located in the IPTV Application server functions (i.e. IUDF (IPTV User Data FE)) hosting the IPTV applications, or in the UPSF as transparent data associated to the Application Server functions, or in an XDMS (XML Data Management Server) associated with the IPTV Application Function.

A.1.5.2 Service Discovery

NGN:

A Service Provider is identified uniquely by the name of the DNS (Domain Name System) it has registered and controls. The organizations administrating the Internet DNS domain names are used as a globally unique registration mechanism that allows these textual Service Providers identifiers to be globally unique names.

Each service has assigned one or more textual identifiers that take the form of an Internet DNS host name under the DNS domain that the SP controls. Thus a service can be uniquely identified by a concatenation of a service name (managed uniquely by the service provider) and the service provider's domain name.

It is the Service Discovery & Selection (SD&S) functional entity that provides description information for discovery of the service list for Live TV and selection of these services or on-demand IPTV services.

The information for service discovery and selection services is assembled according to the Service Discovery and Selection (SD&S) protocol, which for multicast (push) services is transported in IP packets according to the DVB SD&S Transport Protocol (DVBSTP) and for unicast (pull) services such as CoD is transported via HTTP (Hyper Text Transfer Protocol). As specified in TS 102 034 [i.27] a single HTTP request could retrieve the complete list of service providers providing DVB-IP services on the network. An SD&S entry point can be implemented using a DNS mechanism.

Once the service discovery has been done, user profiles in UDAF (User Data Access Function) / UPSF (User Profile Server Function) are verified.

It should be noted that IPTV profile information (content, service, and user) could be optionally located in:

- IPTV Application server functions (i.e. IUDF - IP User Data Function) hosting the IPTV applications,
- UPSF (User Profile Server Function) as transparent data associated to the Application Server functions,
- XDMS (XML Document Management Server) associated with the IPTV Application Function.

Grid:

Grid systems are evolving toward a service oriented computing infrastructure. Therefore, the discovery service gets in the focus of the grid community. Grid information services such as Globus Monitoring and Discovery Service (MDS) [i.18] and Relational Grid Monitoring Architecture R-GMA) [i.61](facilitate the discovery of resources and services in our case the discovery of a video download service.

R-GMA makes all the information appear like one large Relational Database that may be queried to find the information required. It consists of producers which publish information into R-GMA, and consumers which subscribe (http://www.r-gma.org/). However, the R-GMA has not been standardized, yet, and therefore, the video download scenario focuses the MDS functionality of the Globus Toolkit 4 (GT4).

For accessing resource properties via either pull mode (query) or push mode (subscription), a standardized mechanism for associating XML-based resource properties with network entities is implemented in GT4, the de-facto standard Grid middleware. These mechanisms are basically implementations of the WSRF and WSNotification specifications [i.58].

For collecting state information from registered information sources GT4 provides three *aggregator services.* Because not all interesting information sources will support WSRF/WS-notification interfaces, these aggregators can be configured to collect data from any arbitrary information source, whether XML-based or otherwise. The three aggregators implement a registry (MDS-Index), archiver (MDS-Archive), and event-driven data filter (MDSTrigger), respectively [i.58].

In addition, GT4 provides a range of browser-based interfaces, command line tools, and web service interfaces that allow users to query and access the collected information [i.58]. However, for further processing, the collected data should be use in automated ways. But this would belong to the domain/application layer.

Another approach, for the discovery of web services is the "Universal Description, Discovery and Integration" (UDDI) that has been specified by an industry initiative. It has been utilized for discovery of grid services by the grid community [i.57], [i.59] and [i.60]. The UDDI V2.0 and 3.0 specifications have been approved as OASIS Standards and are maintained by the OASIS UDDI Specification technical committee. However, the UDDI Business Registry (the public UDDI demonstration registry) is being discontinued and can be seen as the end of UDDI [i.67]. To enhance service discovery, various UDDI extension have been proposed.

In addition, semantic web technologies can be used to further enhance service discovery whereas services are annotated with metadata whose relationship are typically defined with a domain ontology.

For the video download scenario the basic GT4 approach is assumed. Therefore, the service "video download" has to register with service-associated properties within a service registry through the WS-Resourceproperties (Indexing).Within the Grid several service registries which can have a hierarchical order, can exist. In our example, the service registries are included in the Grid manager. The client requests the video download service at the Grid manager which has to look for the requested service. It returns the service trough an interface to the Grid client.

Gaps and Overlaps:

General principles of locating services are similar in both systems. The focus is on how meta-information about running services including their location can be advertised, gained, discovered, and evaluated. The services are indexed somehow with meta information about them. The meta-information has to be distributed throughout the system in order to advertise the service. Then, the meta information has to be collected for example in a hierarchal model so that the client (or the UE) can look up the service (discover, search for services) for which the user is looking for.

In NGN, the information for service discovery and selection is assembled according to the Service Discovery and Selection (SD&S) protocol, which for unicast (pull) services such as CoD is transported via HTTP (Hyper Text Transfer Protocol). The CoD Discovery Record provides all the necessary information to discover the CoD servers available on the network and the location of their catalogue of contents. It does not provide any information on individual contents. SD&S records information is represented and carried as XML records. Their syntax and grammar is described in XML schemas [i.33].

Within the Grid service discovery entity, properties of resources and of their belonging services have to be advertised throughout the Grid. The resource and service information can be indexed with XML within WSRF. This data has to be advertised.

The format of service information stored on nodes in Grid system as well as the information for service discovery and selection is provided by XML

A.1.5.3 Video Selection

NGN:

Video selection may be done by the either using RTSP (Real Time Streaming Protocol), or using IGMP (Internet Group Management Protocol) [i.33]. CoD Services are delivered using IP unicast and use RTSP for video selection.

The Service Discovery and Selection process as described in the clause A.1.5.2 provides the UE with the RTSP URL (Uniform Resource Locator) for accessing the RTSP based service in question. As an example the UE listens to a multicast address and port number to get the SD&S description, which is presented to the user and from which subsequently the user can make a selection. When the service is selected, the UE can use the associated URL to access the service. The URL indicates whether the session control is based on RTSP. When this is the case, the UE uses RTSP to access the service in question and the format of RTSP URL complies with [i.34].

Two mechanisms may be used to transport the Service Provider Discovery Information and the Service Discovery Information, one for multicast (DVB SD&S Transport Protocol (DVBSTP)) and one for unicast (HTTP). Since CoD services are delivering using IP unicast, HTTP is used.

Grid:

Once the user has been authenticated, the user has access to the directory service which includes a reference to an index service. The index service allows the user to search for desired media related to its authorization profile. While there are some meta-standards for searching (OWL, RDF, SQL, LDIF), this is usually a domain/application specific operation and therefore it is difficult to imagine this class of searching/indexing to be standardized "grid-wide". The index service may either return the location of media fragments or replicas (if the media is accessed in a client-driven "pull" mode), or provide a single media source reference which meets the requirements of the end user, and from which the end user can make a request to commence media access (in a "server-driven" push mode). The client will then collect the video data to store it for off-line access. The client may be responsible for asserting a policy around media retention, modification, and redistribution/replication.

In detail for the video download scenario, the Grid client sends a request with the video selected by the user to the Grid manager, which determines appropriate node for downloading the selected video. In order to avoid overloading of individual nodes, the Web Service Resource Framework (WSRF) [i.82] is used. The WSRF standard is responsible for retaining and recording information about availability and status of nodes. This information can be accessed by other nodes in the Grid to determine the state and act upon them. WSRF provides a standard way of maintaining data and state information about a web service and for retaining state and other persistent data across multiple Web services requests.

Gaps and Overlaps:

In both systems, a URL is returned for downloading the video.

A.1.5.4 Video Download

NGN:

The audio and video streams and the service information are multiplexed into an MPEG-2 transport stream. The resulting MPEG-2 packets are encapsulated using the Real-Time Transport Protocol (RTP), with Differentiated Services Code Point (DSCP) packet markings for QoS. TS 102 005 [i.37] specifies the use of video and audio coding in DVB services delivered directly over Internet protocols (that is, not involving an MPEG2 transport stream).

Real-Time Transport Control Protocol (RTCP) is used, for example, to send information to receivers about transmission statistics, and Internet Group Management Protocol (IGMP) to join and leave multicast streams.

Grid:

After an appropriate node has been selected and forwarded to the Grid client by the Grid manager, the client requests the video from this node. Before downloading, the node verifies with the Grid manager if the client is authorized to download this video. After confirmation by the Grid manager, the node accepts the transfer and copies the file with GridFTP and Web Service Reliable Messaging (WSRM). The video is divided in a predefined number of packets. Each packet is sent by the node to the client whereas each n packets, the node waits for an acknowledgement e.g. with a checksum of the transferred data in order to assure a correct transmission. After all packages have been received, the packages will be reassembled to the entire video on the client.

Gaps and Overlaps:

For downloading a video in an NGN system, the RTP is used. Traditional Grid systems traditionally focus batch job execution.

A.1.5.5 Video Control

Video control is context dependent functionality. The functionality is only usable/applicable for video streams. Context dependent functionality for video is only available in NGN but not in Grid.

GAP XX: NGN offers functionality applicable to Video streams, Grid does not.

A.1.5.6 Charging

The NGN provides mechanisms for on line and off line charging, including a file format for Charging Data Records (CDR) (TS 132 240 [i.40] endorsed by ES 282 010 [i.65]).

In dedicated IPTV subsystem [i.12], it is the IPTV subsystem itself that collects information related to billing and provides IPTV CDRs (including charging related elements), that can be collected by the billing system for the sake of off-line charging. These CDRs may also be used for other purposes than billing (such as QoS, statistics). IPTV subsystem integrates with the charging and accounting components of the management domain for having access to the user account (credit, balance, etc.) in order to allow IPTV user facing applications and optionally media delivery control to perform their role with.

The IPTV Architecture (ITU-T Recommendation Y.1910 [i.66]) identifies the "Application accounting functional block" which will record any transaction which is potentially chargeable.

For Grid, the OGF has a format recommendation for Usage Records which can be used to exchange basic accounting and usage data (GFD-R-P.098).

Gaps and overlaps

- Gaps.
- No on line (real time) charging specified for Grid.
- Overlaps.
- Offline Charging: It would be advantageous to align CDRs transferred from Grid/NGN resources to the Billing domain.

A.1.5.7 SLA and QoS

TISPAN does not specify the SLA for NGN. ETSI TC STQ is currently working on audiovisual QoS for communication over IP networks. The ES will address combination network performance parameters and user perceived media (audio and video) quality parameters for audiovisual communications on IP networks. The access technologies will include both wired (e.g. xDSL) and wireless (e.g. UMTS, WLAN) technologies. The ES will be applicable to:

- Broadcasting and streaming applications such as IPTV and VoD.
- Interactive point-to-pint applications such as videotelephony and videoconferencing.

ITU-T will publish soon the new recommendation on subjective video quality assessment methods for multimedia applications [i.35].

DSL Forum has defined QoE requirements for triple-play services [i.36].

A.2 Integrated Emergency Management (IEM)

A.2.1 Scenario description

IEM is short for Integrated Emergency Management. Although the term appears to be primarily prevalent in the UK, the integrated approach is common in Europe, the US and elsewhere under a variety of names. In the UK, the discipline has been formed in response to the observed inflexibility of response to emergencies in the past. The need for an approach that is integrated across multiple organizations became apparent in the early 1990's. According to [i.79], in 1991, the then Home Secretary announced that the post cold war review of Emergency Planning had identified (the need for) an "integrated approach to emergency management" [i.80]. This approach is currently embodied in the UK Civil Contingencies Act 2004 [i.81] and is adopted by local government authorities. IEM breaks the whole process down into phases and the guidance to the Act [i.81] defines the elements of these:

- planning which consists of:
  - anticipation;
  - assessment;
  - prevention;
  - preparation;
  - response;
  - and recovery.

The response phase concerns the effective response to disasters and crises and places severe demands on the communications and information processing infrastructure. This phase was the focus of the final demonstrator in the EU FP6 Akogrimo Project (referred to in that project as DHCM - Disaster Handling and Emergency Management). A summary of this is provided at [i.78]. The key organization in the design of the scenario was QinetiQ, which evolved from the research capability of the UK Ministry of Defence and has significant experience and expertise in IEM. We make use of that demonstrator to give an example of the roles and activities of the response phase, but they are in principle applicable to other types of emergency. First we consider the roles involved (the actors). Figure 8 shows the summarized demonstrator storyboard. The actors in this are as follows:

- An emergency call centre: this is often in a fixed place.
- Police officers, paramedics and fire fighters with mobile devices, who may have equipment not only for person to person communication but in some cases also for providing data entry in some form (e.g. situation and casualty assessment).
- A command centre (Silver Command): this is often in a fixed place, but one could also envisage a hierarchy of control rooms, some of which could be mobile

Each of the actors has software support and the totality of the software associated with all the actors could be considered to be a single distributed application. The command centre software maintains a Common Operational Picture. The Common Operational Picture (COP) includes information from a variety of sources: prior information from the planning phase; updates from the emergency sites which may include reports in the form of textual information (e.g. casualty information) and multimedia (e.g. audio/video of the emergency scene). Aspects of the COP may be delivered to whoever appropriately may receive them.

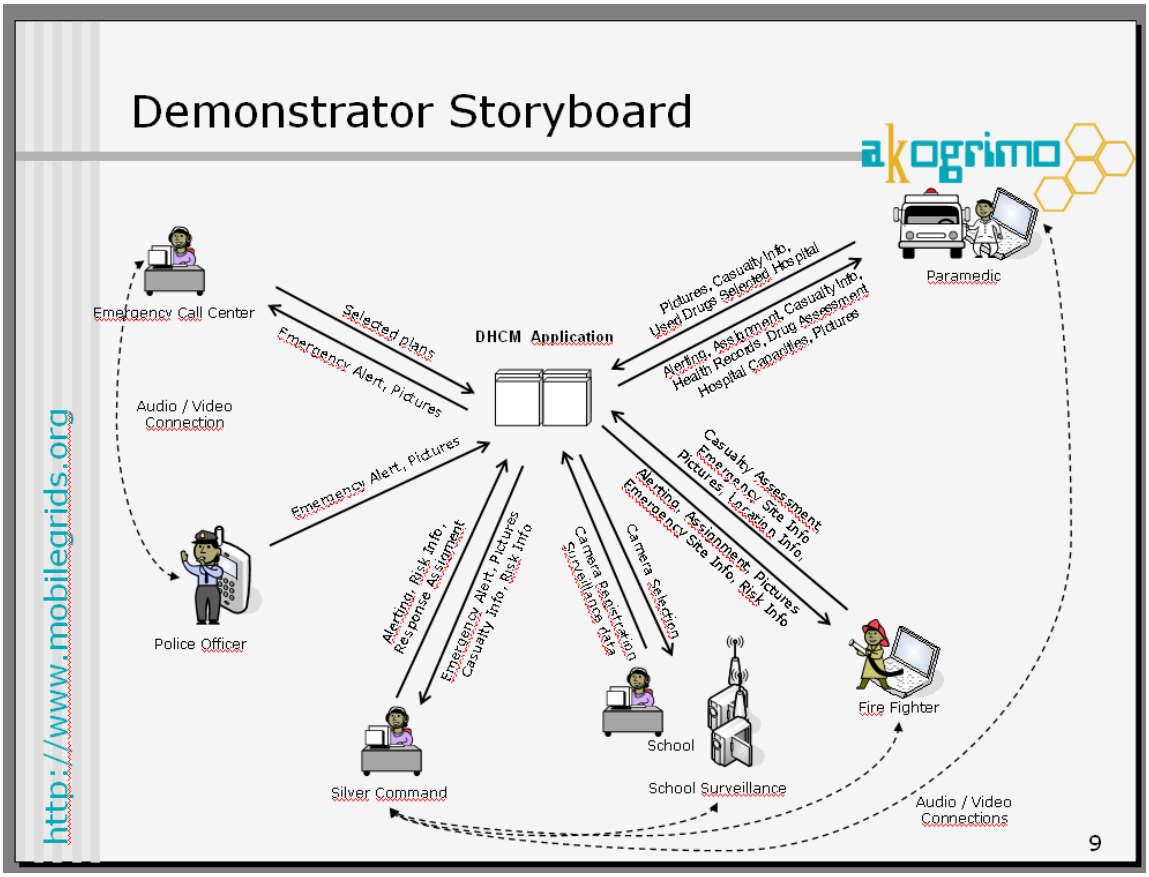


Figure 8: DHCM Demonstrator Storyboard from Akogrimo - an example of an IEM application in the response phase using mobile Grids

A.2.2 IEM in a Grid environment

The application involves not only communication between people, but also the sharing of information and in some types of crisis (infectious disease, flooding etc) may require significant computation. The application may require the bringing together of heterogeneous administrative organizations such as hospitals, police and local government together with utility computational and data intensive resources. The following aspects were, in [i.78], presented as technical barriers that the idea of mobile Grids could solve. In each case, the remark before the => symbol is taken from the paper and a further remark is added after the symbol:

- Simultaneous treatment of fundamental constraints such as resilience and agility => this suggests the loose coupling and redundancy aspects of the Grid concept, although this still remains to be fully realized on the Grid.
- Uncertainty of where/how to find resources => effective service discovery - this tool is a part of the Grid concept not fully realized as yet.
- Making trans-organizational resources secure, punctual, appropriate, auditable, (there are special cases relating to public/media information releases) => Making trans-organizational resources secure is the kind of situation for which Virtual Organizations (VOs) are intended and have been developed. Punctuality and auditability are not well served as yet.
- Provide insight of provenance, trust accuracy when conflicts in content are encountered => This requires appropriate access to knowledge sources, possibly using semantic capabilities.
- Preventing isolation due to organizational boundaries => This implies VOs and Grids.
- Address regional and political boundaries => There are several issues here, one of which is the different regulations across such boundaries.

- Optimizing the brokering of finite expert and specialist resources (including human) => Several implications here including the discovery of information about experts and services.
- Improving integration and interoperability of resources and workflows in extremely heterogeneous environments => Grid workflows, Grid heterogeneity.
- Safely handing control over of active workflows between phases and organizations => Grid workflows, Grid VOs.
- Detecting and managing context changes (often subtle and risk driven in IEM) => Delivery of current context about workers at emergency sites.
- Dealing with rapid shifts in priority and activity modes (through adaptive workflows) => Grid workflow responding to context.
- Identifying and obtaining best utilization of prior investment (training, infrastructure) for all activities in all phases => One implication here is the ability to acquire additional resources (computing, data communications) when required and not have then lying idle in silos.
- Exploit latent advantages of the number of skilled mobile resources => Implies mobility; multi-agency Grid VOs - thus some of the services in the VO are mobile. This leads to the idea of a VO which is dynamic and mobile to encompass mobile, changing resources.

A.2.3 IEM in an NGN environment

The IEM response scenario requires access to the overall distributed Grid application from diverse personnel in diverse situations with diverse means of communication. As NGN becomes more widely available, it will become one of the means of access and its associated capabilities such as real time access can be used. Subsequent versions of the present document will need to consider this further.

A.2.4 Comparison

NOTE: The following is placeholder text and will be updated in future versions of the present document.

Having discussed the IEM application and how it might be realized in a Grid environment and in an NGN environment, this clause provides a brief comparison (see table 3).

Table 3: Realization of activities in the video download scenario

Activity	Grid Protocols/Standards	NGN Protocols/Standards
Authentication	The application requires the ability to identify all users at the point of access to the Grid system. This authentication could be offered by the network that underlies the Grid. This could be IP with a present day Grid or the authentication could be offered by NGN - see the NGN entry. Between Grid services, authentication could be offered by means of X509 certificates.	ffs
Authorization	Based on the certificate offered by each user, each sensitive Grid service would be required to authorize attempts at access. Since there is a non-negligible probability of disruption, his application has a very strong requirement for protecting against this.	ffs
Information protection		ffs
Charging		ffs
Compute requirements		ffs
QoS - Priority usage in the response phase		ffs
reliability		ffs

A.2.5 Gap analysis for the IEM scenario

A.2.5.1 Security

- There is a requirement for trans-organizational information exchange, between authorized people and services in multiple conventional organizations. This is the kind of requirement that is fulfilled by Virtual Organizations (VO) which is not standardized. Individuals in the VO need to have their identity established from whatever authorized means of access they use, their role needs to established and the authorization for the services they can access needs to depend on this role.

- Confidentiality of both mobile and fixed communication is required, in some cases highly confidential.

A.2.5.2 SLA and QoS

- Infrastructure supporting this type of application needs to enable priority to be given to this application, both for computational and network resources, when an emergency is declared. In previous emergencies, it has happened that parts of a network have been shut off to allow for the emergency communications to continue and conventionally this has been done for the mobile phone network. This is however a very crude mechanism and could shut off some communications essential to the emergency response. It would also be necessary to prioritize data transmission required by the response phase and it would be more difficult to associate these with a specific network paths.

- Streaming may be required for video conferencing or for the delivery of video information from the emergency site to the control centre. Although the need for high quality may not be high (there might not be a need for cinema quality), there is a need for sufficiently low frame loss and low jitter.

- In advance of an actual emergency, the size of the requirement for networking resources is not known. This places a difficult demand on SLA negotiation.

- There needs to be a well understood relationship between an SLA agreement (such as may be specified by WS-Agreement) and network parameters such as reliable bandwidth and lack of jitter. WS-Agreement provides a framework for defining terms but does not standardize what those terms are.

A.2.5.3 Charging

- Although for this application, there should be no sense in which the services are terminated when "the money runs out", nonetheless there does need to be some transfer of money both for standby resources and for the actual use of resources when finished when the emergency response is completed.

A.2.5.4 Reliability

- Reliability of interworking between services produced and managed by different administrative entities.
- Reliable service operation (related to QoS).
- Reliable message passing - it is essential to know that a message has been delivered. This is probably not a gap for Grid/Web Services, as WS-RM is probably adequate here.
- In an emergency situation, there needs to be high robustness of services and of the means access to them, if necessary by redundancy in the presence of network paths being lost.
- Reliable service operation in the presence of potentially highly unreliable networks in the emergency situation. The ability to respond to dynamically changing situations is required. The response may include the substitution of alternative services to replace service instances which have impaired access.

Reliability is also related to SLA and QoS, since it is possible to set reliability metrics which can be the subject of an agreement.

A.2.5.5 Discovery

- Discovery of people with specific expertise and their availability.

A.2.5.6 Workflow

- The complexity of the emergency process requires some form of workflow across organizational boundaries, which requires all constituent services to be authorized for use.
- The emergency process workflow may control a situation at multiple locations and involving multiple individuals and will therefore need to respond to the context (location, connectivity status, etc) in which service providers exist at any time.

A.3 High Performance Computing

A.3.1 Scenario description

The purpose of this clause is to concentrate on one of the most usual computing Grids use cases. The initial ideas of Grid computing started from the need to link multiple geographically distributed High Performance Computing (HPC) installations - linked by high-speed networks - into a virtual supercomputer, also known as a metacomputer. Integrating data-driven scientific and engineering workflows onto HPC Grid, indeed, naturally enables scientific/technical applications.

Experiments such as the Large Hadron Collider (LHC), for instance, produce large volumes of data at one location to be distributed to three computational Grids for processing, namely the E-sciencE Grid (EGEE), Open Science Grid (OSG) and NorduGrid (NG)). On the other hand, different locations, changing parameters for each run, varying data formats and customized processing are also commonplace in the HPC community.

In HPC, high-performance compute resource-sharing is one of the Grid intrinsic properties. However, the application requirements from different scientific disciplines bring different sets of computational and data management challenges. Scientists and engineers conducting HPC simulations, for instance, often perform a sequence of tasks in a workflow pattern similar to that of a business process. For instance, in the LHC case, we speak about the ATLAS computing model [i.77].

A.3.2 HPC in a Grid environment

In a generic HPC scenario, the steps in a compute-intensive workflow might include setup, data acquisition, data movement, pre-processing, processing, and visualization. The data acquisition instruments, storage systems, and compute resources are often distributed within and across organizational boundaries. The HPC Grid user/application may have to deal with the complexity of the resource discovery, data movement, job scheduling etc. Some of the major prerequisites to be tackled while integrating scientific and engineering compute-intensive workflow onto Grid are:

- Data acquisition systems and their integration.
- Reliable and timely clusters for processing (often vector super-computers in HPC) and storage.
- High-performance networks between geographically remote sites.
- Supporting entire workflows while managing disparate data sources and formats.
- Enabling application-specific approaches to managing parameters, data management, processing, and analysis support.
- Usability by scientists and engineers with.

The requirements on HPC-type scenarios to realize workflows from different scientific domain are unique as their data, processing and functional characteristics vary to greater extent. The workflow is formerly defined as the automation of procedures where documents, information, or tasks are passed between participants according to a defined set of rules to achieve, or contribute to, an overall business goal. However, scientific workflow solutions can be grouped into two categories:

1) Domain-specific workflow systems: A domain-specific workflow solution poses challenges on extensibility to another application domain, since it does not address the sets of requirements responding to specific requirements.

2) Generic workflow system: A generic workflow solution requires further customization to be applicable to a particular application domain.

Application	Domain	Raw data (format) characteristics	Important functional requirements	Workflow requirements	I/O or data or CPU -intensive
LHC	Particle Physics	numerical, time-series data	large volume of data is to be transferred efficiently to other sites and interoperability between Grid middleware	workflow management services for data calibration and user analysis	compute as well as data-intensive
NEESgrid	Earthquake engineering	numerical data and video stream (for monitoring)	remote participation (telepresence) and steering of experiment	none	I/O intensive (hardware integration)
SDSS	Astronomy	Astronomical objects/ images represented as numerical data	MaxBCG algorithm search on astro objects	no explicit requirements - preprocessing pipeline can be modeled as workflow	data-intensive
GeWITTS	Aerospace	video stream	remote view of experiment	none	I/O intensive
LEAD	Atmospheric sciences	numerical, sensor data from Doppler radars	Real-time response to changing weather conditions	event-driven workflow	compute-intensive
*my*Grid	Molecular Biology	semi-structured, heterogenous and bespoke formats representing gene sequences, protein sequences etc.	construction and editing of service-based workflows	workflow steps to take input and output in domain-specific formats	experiment -dependent, some data-, some compute-intensive
DAME	Aircraft Maintenance	Engine sensor data - real valued variables monitored over time, historical data and non--declarative data such as procedures used	Data storage and mining - advanced pattern matching and data mining on large volume of data for engine fault diagnosis and prognosis	none	data-intensive, device integration

Figure 9: Comparison of some HPC application and workflow characteristics

In summary, core functional requirements of HPC applications in Grid environment (see figure 9) include a large source of variability in terms of data formats, the role of database management systems, the ability to compose workflows from loosely coupled services, the real-time response to changing events, the support for remote access to hardware, the computational requirements and the high-speed data transfer requirements.

The workflow integration based on Grid services is shown in figure 10. The typical grid workflow development stack is formed by, at the bottom, the Grid resources that include compute clusters, storage networks, data acquisition systems, licensed softwares and so forth. The Grid middleware, e.g., Globus, is responsible for services such as security, data management and job scheduling. The next layers include the Grid application toolkits and the Portal Interface. These development environments enable Grid applications to leverage continuously evolving class libraries supporting data processing, database access, network programming, Web Service integration, portal development and so on. The Scientific & Engineering workflows may access the infrastructure via a Portal Interface. Note that the different layers all need specific engineering development and operational maintenance.

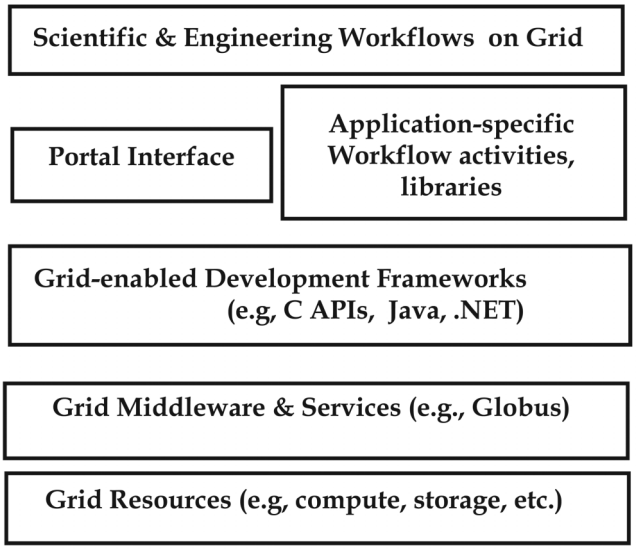


Figure 10: Usual Grid workflow development stack

A.3.3 HPC in a NGN environment

The IP-based NGN was not designed with the explicit goal to join the landscape of shared-memory multiprocessors, parallel vector machines and cluster of workstations, OS-bypass protocols and message passing software libraries. The high-speed, low-latency, and high-bandwidth communication as generally required in HPC would impose new challenges to the NGN. Some points are described below.

A.3.4 Comparison

A.3.4.1 Database operating systems

The majority of scientific applications in Grid environment rely on file systems for data management with very limited use of Relational Database Management Systems to retrieve metadata etc. Database replication can be performed, for instance, when HPC applications have to deal with distributed data and the availability of data is to be ensured in more than one location.

Given the evolution in database landscape, databases may be viewed as database operating systems with the support to other subsystems and applications plugging. The importance and the issues in integrating database systems into the Grid environment comes from the fact that databases are beginning to support native XML types and XML Web services, with the Master DB representing, on a per site basis, the manager to database information management, including local and remote client information management. The Master DB further load balances the database workflow activities by submitting requests to workers.

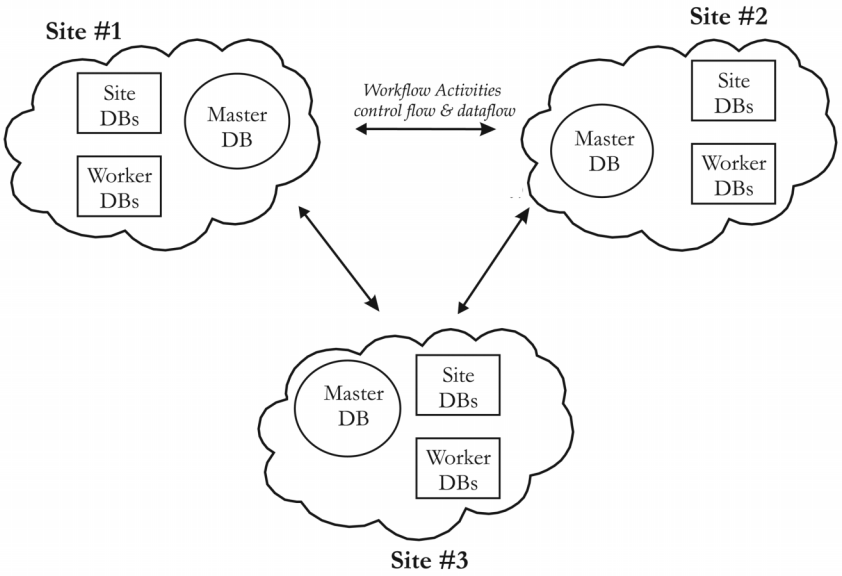


Figure11: Example of database usage in Grid environment

While usual HPC Grid environments were designed with the appropriate database facilities, the Grid over NGN does not meet the requirements for the management of NGN network-related information. For instance, the NGN may include its own databases as follows:

- Site databases (NGN SiteDB): Considering the importance of timely changes in network configuration, typically in network resource, the NGN SiteDB publishes the network resource information tables to the NGN MasterDB using transactional and push-style replication. This ensures immediate transfer of network status data to the NGN MasterDB as soon as the data imported into NGN SiteDB from the network's data acquisition system.

- Master database (NGN MasterDB): This maintains the network information user tables, and publishes them to sites and worker databases. It subscribes to network status data from all the sites. The master node also runs workflow services for users to register, run and monitor their application workflow.

- Worker databases (NGN WorkerDB): This set of databases is managed as a cluster of local "nodes". It carries out the processing work assigned by the NGN MasterDB.

In order to be compliant with usual Grid environment the NGN would run a set of databases in conformance with the database operating systems vision. The main issue for the NGN is in the mapping of the existing network management and operation framework, with the databases already built, in a way to fit the actual database workflow execution on the Grid.

A.3.4.2 NGN networking

Extending Grid service access to new platforms is different from extending Grid services to a network architecture such as NGN. Even though one of the main objectives of the existing Grid infrastructures is to integrate heterogeneous resources, generally no network services (and related resources) are considered.

Two types of network connections between connected entities such as client and server exist: control and data. One of the main issues in NGN networking for HPC, and in particular for data connections, is the potential need for high bandwidth pipes with the support of QoS and performance criteria. Further, the Grid messages and data moves are today generally routed through low latency and high bandwidth network technologies, such as InfiniBand and other high speed interconnects, to improve the performance.

This introduces a differentiation between network service and network resource. Without going to a hierarchical activity model for network service composition - a network service composition based on various, real-time selected network resources - customized network service setup is required in the NGN with reference to the current and future status of the network. The second issue is then the scheduled setup of network services and thereby network resources.

The evolution of Grid from an interoperable HPC computing infrastructure linked by high-speed networks into a service-oriented architecture based on Web Services standards running on the NGN will go probably through different phases.

A.3.4.3 Workflow management

There are many workflow principles used in business process automation that are relevant to scientific HPC workflows. Business workflows tend to be routine whereas scientific workflows are often exploratory, sometimes following a trial-and-error approach. The amount of data that are to be processed at each stage of the workflow is often greater in scientific workflows than business workflows.

Business workflows are usually well-defined in advance and executed in a routine fashion. A visually expressive workflow development environment is often a major requirement as scientific workflows are constructed by domain scientists; any requirement of BPEL expertise or major programming effort may not be an attractive option. The voluminous data that are to be acquired, moved, read and parsed at each stage of the scientific workflow can be far greater than in business workflows. Again the workflow system has to support appropriate data handling under the hood without expecting scientists to deal with it.

A.3.4.4 Security policies

The security policies for user authentication and authorization for scientific collaborations are different from the business process interactions, since the HPC Grid security policies required in a collaborative and resource sharing scientific environment are different from business environments. And this is case for the NGN operation, where business actors such as network operators and service providers interact with respecting a business agreement.

A.3.5 Gap analysis for the HPC scenario

A.3.5.1 Business vision

The business community has long been using some form of procedural automation for tasks that are routine in nature. Enterprises increasingly conduct their business in partnership and often, in order to meet a business request, services from partners are to be integrated. At the convergence of the business and scientific/engineering visions, specifications resulted in Business Process Execution Language for Web Services (BPEL4WS), supporting composition of services from different partners to achieve a business goal. BPEL is currently an OASIS draft specification under the name WS-BPEL [i.53].

A.3.5.2 Grid middleware

The Grid middleware as currently developed in the HPC practicing community seems to be very much directed by the requirements derived from the activities of a few number of intensive HPC users such as CERN. By choosing several application areas with somewhat different and complementary requirements, the Grid middleware software should ideally be driven towards a more general purpose Grid middleware platform. Examples include requirements for workflow, streaming, and real-time processing.

If successful, this would increase the value of the NGN operating platform, by being a significant research vehicle for other scientific domains as well.

A.3.5.3 User experience

As soon as the real NGN users start utilizing the Grid system over the NGN, it is important to get good user feedback and some kind of approval of functionality and system quality. In particular this may be the role of the service provider. Given the large extent of the NGN, the user experience supervision activity may face dead periods due to coordination problems across many different institutions, business partners, and even nations.

This is particularly true for network infrastructures. In such an intensive networking environment, the support of network Quality of Service requires the establishment of Service Level Agreements between users and network sand other service providers.

Another required functionality is authentication, authorization, and admission control as well as automated service provisioning and Traffic Engineering provided by the control plane. The availability of service guarantees allows flexible usage of the distributed infrastructure and enables considering end user application-controllable performance criteria.

A.3.5.4 Conclusion

As the Grid user application requirements may be quite diverse, the Grid over the NGN should be designed to serve a potentially infinite number of different applications and users.

A.4 e-Health

A.4.1 Introduction

The Healthgrid Association [i.69], formed in 2003, has gathered industry, researchers, and health care professionals together to consider the opportunities for applying Grid technology to the health care industry and to life sciences research. Their goals and objectives are outlined in their summary white paper, published in 2004 [i.70]. This scenario is primarily based on the HeathGrid model, with additions from the ETSI eHealth TC [i.68] and other major health care related Grid projects.

There are four primary targets for any e-Health initiatives:

i) to provide better health care for the public;

ii) to reduce the cost of providing health care;

iii) to seek innovative new ways to support medical professionals in providing health care; and

iv) to provide tools and infrastructure to facilitate and innovate medical research.

The HealthGrid white paper succinctly summarizes the key concerns of any new ICT into the world of health care: "security, confidentiality, liability and ownership of data" [i.70]. The importance of this area is also highlighted by Connecting for Health projects in the United Kingdom and United States [i.71] [i.72].

A.4.2 e-Health in a Grid Environment

A Grid environment which seeks to share patient or clinical study related information or provide electronic services for medical professionals will do so in a way that is secure, reliable, and traceable. From a patient-centric perspective, data records management is a key concern. A person wants accurate, timely, and complete diagnosis of any health issues. In emergency situations, it may be necessary to acquire medical records while the patient is unconscious. During a treatment regime, data is collected regarding the patient, and this data forms part of the medical history which is handled by a range of people and organizations. Broadly speaking, there are four classes of information which form a person's medical record: structured "persistent" data, such as name, date of birth, and contact information; un-structured textual entries from health professionals; structured "transient" data, such as blood pressure measurements, test results, heart rate; and imaging data, such as X-rays and MRIs. One goal of e-Health is to unify and streamline the management of this data. In the context of Grids and ICT, they key technology areas which this scenario touches on are: common data formats, authorization and authentication mechanisms, security policies, provenance, archival facilities, replica management, and data transport and sharing systems.

Health care services fall into two main categories: Computerized Decision Support (CDS) and Patient Monitoring (PM). For both, the distinguishing features from typical distributed information services are the issues of identity management, security, reliability, and service composition. CDS systems will authenticate the user and check authorization for access to multiple data sources either related to the patient or aggregated to enable a comparative diagnosis of a condition. Composing these data sources and a selection of services to present the healthcare professional with the necessary information requires interoperability. The PM system can also be seen as a "sensor network", an area of interest in Grid computing.

A.4.3 e-Health and NGN

NGN has an important role to play in e-Health. Systems which are part of critical patient care require reliable networking, secure (and possibly encrypted) data transmission, dynamic device identification and location, and automated-configuration. Many of these issues are common to mobile devices and also to NGN User Equipment. Diagnostic services both from the acquisition stage (e.g. at an imaging centre or laboratory) to the analysis and diagnosis stage may need to aggregate a significant quantity of data.

A.4.4 SLA and QoS

An e-Health environment has very demanding QoS requirements with a necessity that this is maintained continuously throughout the system lifetime. In this environment, SLAs are likely to be fixed in advance by policy rather than dynamically negotiated. What is required is an infrastructure which can track QoS for various aspects of a system and evaluate these against the policy SLA to take action when the SLA is violated. There are no e-Health specific SLA mechanisms for digital services. It is envisioned that policy based SLAs will be centrally managed and associated with given services or data artefacts based on the source, subject, and destination. For example, life support systems providing an active data feed monitoring a patient's condition would be prioritized above X-ray images for a broken arm. Furthermore the ongoing operation and availability of the life support and X-Ray systems would each be subject to an SLA which would require monitoring the QoS and responding to any failure to maintain the QoS specified in the SLA.

[i.1] is the primary mechanism for establishing SLAs within a Grid environment, however this is primarily designed for interaction of software services, or software services and end users, with dynamic negotiation and agreement of SLAs. It is also general and does not attempt to present any specific semantics for aspects which may be described within an SLA. SLA requirements and attributes for Grids are described using a range of mechanisms, some standardized and some not, which are generally closely tied to a particular workload management system (e.g. cluster scheduler and manager). Languages and models such as JSDL, [i.73], and [i.74] can be used to establish SLA properties and requirements between compute jobs and users, while CIM [i.54] provides an information model for physical devices forming the grid infrastructure. From NGN, the ETSI TC Speech, Transmission Planning, and Quality of Service group has worked with TISPAN to establish agreed QoS parameters, however these have primarily focused on speech and connection call quality metrics for existing systems, rather than considering QoS parameters for future NGN standard or value-added services. SLA within the telecoms industry has primarily been handled as a matter of policy between networks and contractual terms between the network provider and customer.

A.4.5 Charging

Within an e-Health environment, charging is an important consideration when accessing services from an external organization. Pay-at-use charging would imply some mechanism of providing a "pre-payment" receipt, "payment" token (analogous to cash), an external funding source (analogous to a credit card), or a service-internal billing account (analogous to a purchase order or credit line) in order to establish or complete an interaction with a remote service which requires payment. It is envisioned that many e-Health applications would operate outside a pay-at-use scheme, either operating within an enclosed environment (with requisite security requirements), or with a contractual payment scheme. A contractual payment scheme may either be fixed-rate, or based on usage (pay-per-use, debit or credit). For a pay-per-use scheme, some mechanism to account for usage would be required. Grid standards do not currently address payment mechanisms, although many bespoke "web service" payment schemes exist. Standards around Grid resource usage are at an early stage and focus on computational tasks. The telecoms industry relies on Charging/Call Detail Records [i.40] to track usage across networks in a standard way, then relying on provider-specific mechanisms to translate CDRs to charging information for a particular customer. It could be imagined that a similar system be used in an e-Health environment.

A.4.6 Service Discovery

In the e-Health use case, the key place for service discovery is in Patient Monitoring systems. These can be seen as a sensor network that needs to coordinate each sensor in their collection of data for a particular patient. Each sensor needs to be associated with its function(s), its location, and a patient. This can be controlled from the device or from a central management system. Service registries such as UDDI [i.57] can be adapted for this purpose, although they are not typically used for device identification or where there is a high degree of dynamism. TISPAN has been studying User Equipment device discovery and configuration.

A.4.7 Security

The security infrastructure for e-Health is the most complicated aspect to address. There is a need for advanced policy creation and verification tools, strong assurances against the risk of impersonation, protection of privacy, and a dynamic authentication and authorization mechanism based on identity and roles. The network infrastructure can support this by providing services which will handle secure, authenticated channels for data transmission. All services and devices within the system will require authentication, and patients and healthcare professionals will need to be allocated identities and roles. The policy management infrastructure will need to include overarching security assertions regarding service, device, and data access based on roles, as well as the ability to create and associate time limited policies granting access to specific individuals or positions/roles. To achieve this infrastructure, standards are required for identity tokens (their format, creation, and exchange), policies, and access control. The X509 standard [i.20] has currently shown the most promise and had the highest level of adoption for meeting these goals, although Shibboleth (based on SAML) and Kerberos systems have also been used. The UK NHS IT programme has adopted smart cards as a means of authenticating a particular user with an underlying X.509 certificate system. The US Connecting For Health project also, although to a lesser degree, recommends the use of an X.509 infrastructure.

Regarding security issues related to the telecommunications infrastructure and telecoms standards, ETSI has already produced a detailed special report which includes an entire section addressing this issue [i.76]. The reader is referred to the present document for further information.

Annex B: Bibliography

ETSI TR 133 919: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G Security; Generic Authentication Architecture (GAA); System description (3GPP TS 33.919)".

ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220)".

ETSI TS 133 221: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Support for subscriber certificates (3GPP TS 33.221)".

"HPC Job Scheduling: Base Case and Common Cases", OGSA HPC Profile WG, July 1, 2006.

"Mobile Grid Use Cases", G.Gallizo and J.Gallop.
http://docbox.etsi.org/grid/grid/50-Meetings/GRID04_20070920_Sophia-Antipolis/GRID04_10.pdf

IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

IETF RFC 3281: "An Internet Attribute Certificate Profile for Authorization".

IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

"OASIS Web Services Security (WSS) TC". http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss fetched on May 13th 2008.

OASIS home page. http://www.oasis-open.org fetched on May 13th 2008.

History

Document history		
V1.1.1	February 2009	Publication