

## Identity and access management for Networks and Services; IdM Interoperability between Operators or ISPs with Enterprise

---

### *Disclaimer*

This document has been produced and approved by the Identity and Access Management for Networks and Services (ETSI INS) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG. It does not necessarily represent the views of the entire ETSI membership.

<https://standards.iteh.ai>  
Document Preview

[ETSI GS INS 001 V1.1.1 \(2011-03\)](https://standards.iteh.ai/catalog/standards/etsi/b6b899c2-33d7-449d-b3e1-6df7e401fe79/etsi-gs-ins-001-v1-1-1-2011-03)

<https://standards.iteh.ai/catalog/standards/etsi/b6b899c2-33d7-449d-b3e1-6df7e401fe79/etsi-gs-ins-001-v1-1-1-2011-03>



---

**Reference**

DGS/INS-001

---

**Keywords**access, ID, interoperability, management,  
network, service, use case**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

<https://standards.iteh.ai>  
Document Preview

---

**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/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/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 2011.  
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
Introduction .....	5
1 Scope .....	6
2 References .....	6
2.1 Normative references .....	6
2.2 Informative references.....	6
3 Abbreviations .....	7
4 IdM Overview: authentication and attribute exchange.....	7
4.1 Operators/ISPs.....	7
4.1.1 Authentication.....	7
4.1.2 Attribute Exchange .....	8
4.2 Enterprise (and Home Network) .....	9
4.2.1 Authentication.....	9
4.2.2 Attribute Exchange .....	10
5 Operator/ISP-Enterprise Use Cases.....	10
5.1 SSO for small enterprises and home network users .....	10
5.1.1 Description.....	10
5.1.2 Actors.....	10
5.1.2.1 Actors specific Issues .....	10
5.1.2.2 Actors specific benefits .....	11
5.1.3 Pre-Condition.....	11
5.1.4 Post-Condition .....	11
5.1.5 Normative Flow .....	12
5.2 Attribute Sharing between Operator and Web Enterprise .....	12
5.2.1 Description.....	12
5.2.2 Actors.....	12
5.2.2.1 Actors specific Issues .....	13
5.2.2.2 Actors specific benefits .....	13
5.2.3 Pre-Condition.....	13
5.2.4 Post-Condition .....	13
5.2.5 Normative Flow .....	14
5.3 Outsource billing to operator.....	14
5.3.1 Description.....	14
5.3.2 Actors.....	14
5.3.2.1 Actors specific Issues .....	15
5.3.2.2 Actors specific benefits .....	15
5.3.3 Pre-Condition.....	15
5.3.4 Post-Condition .....	15
5.3.5 Normative Flow .....	16
5.4 Integration of XaaS and multi-stage IdM systems .....	17
5.4.1 Description.....	17
5.4.2 Actors.....	17
5.4.2.1 Actors specific Issues .....	17
5.4.2.2 Actors specific benefits .....	18
5.4.3 Pre-Conditions .....	18
5.4.4 Post-Condition .....	18
5.4.5 Example Flow .....	19
5.5 Authentication as a service.....	20
5.5.1 Description.....	20
5.5.2 Actors.....	20
5.5.2.1 Actors Specific Issues .....	20
5.5.2.2 Actor Specific Benefits .....	21

5.5.3	Pre-conditions .....	21
5.5.4	Post-conditions .....	21
5.5.5	Example Flow .....	22
5.6	Summary Table of Use Cases.....	22
6	Functional requirements .....	23
7	Functional Requirements: Impact on current architectures .....	23
8	Functional architecture definition .....	24
8.1	General .....	24
8.1.1	Authentication relationship .....	25
8.1.2	Attribute exchange relationship .....	26
8.1.3	Functional elements description .....	27
8.1.3.1	Identity Provider .....	27
8.1.3.2	Attribute Provider .....	27
8.1.3.3	Authorization Authority .....	27
8.1.3.3.1	Authorization Enforcement .....	27
8.1.3.3.2	Authorization Validation/Decision .....	28
8.1.3.4	Authentication Authority .....	28
8.1.3.4.1	Authentication Enforcement .....	28
8.1.3.4.2	Authentication Validation/Decision .....	28
8.1.3.5	Charging Provider .....	28
8.1.3.6	Identity Provisioning .....	29
8.1.3.7	Identity Broker .....	29
8.2	Interfaces .....	29
8.2.1.1	IdentityResolution.....	29
8.2.1.2	IdentityManagement .....	30
8.2.1.3	AttributeManagement .....	30
8.2.1.4	IdentityAuthentication .....	31
8.2.2	IdentityCharging interface .....	32
8.3	Protocols.....	32
8.3.1	Interface c .....	32
8.3.2	Interface d .....	32
8.3.3	Interface e1 .....	32
8.3.4	Interface e2 .....	32
9	Operator/ISP-Enterprise IdM Interoperability instantiation.....	33
9.1	Instantiation SSO for small enterprises and home network users.....	33
9.1.1	Instantiation Video On Demand System.....	33
9.1.2	Instantiation Local IdM (e.g. Home or Enterprise IdM).....	33
9.1.3	Instantiation Operator IdM .....	33
9.1.4	Use of Interfaces .....	33
9.2	Instantiation Authentication as a Service .....	34
9.2.1	Instantiation Enterprise .....	34
9.2.2	Instantiation Mobile Operator.....	35
9.2.3	Use of Interfaces .....	36
<b>Annex A (informative):</b>	<b>Authors and contributors.....</b>	<b>37</b>
History .....	.....	38

---

## 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 Group Specification (GS) has been produced by ETSI Industry Specification (ISG) Identity and access management for Networks and Services (INS).

---

## Introduction

In the present document we present an architecture and its instantiation for use cases where interoperability exists between Operators and Enterprises in terms of authentication and attribute exchange. Historically both domains were seen as separated, without any kind of interactions. The demand for new scenarios, i.e. Software as a Service, implies that some interactions need to be in place. This cooperation can be achieved either by exchanging data about the user or reusing the authentication context.

The first part of the present document provides a brief overview of the actual authentication and attributes exchange within the Operator and the Enterprise. Next, a set of use cases which demand for cooperation between Enterprise and Operators are presented. These use cases are the ground to collect the requirements and the impact of such requirements in the actual architectures.

The second part of the present document presents the architecture in terms of functions and its relationships, which answers the collected requirements. Moreover it describes the interfaces and the protocols such interfaces can use. Finally two examples of its instantiation are presented.