



**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;**

**Liberty Alliance and 3GPP security interworking;
Interworking of Liberty Alliance Identity Federation Framework
(ID-FF), Identity Web Services Framework (ID-WSF) and
Generic Authentication Architecture (GAA)
(3GPP TR 33.980 version 13.0.0 Release 13)**



Reference

RTR/TSGS-0333980vd00

Keywords

GSM,LTE,SECURITY,UMTS

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 noticeThe present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI 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.

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 (<https://ipr.etsi.org>).

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 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
3 Definitions, symbols and abbreviations	7
3.1 Definitions	7
3.2 Abbreviations	8
4 Interworking of Liberty Alliance ID-FF/ ID-WSF and Generic Authentication Architecture.....	9
4.1 Introduction	9
4.2 Architectural Description – Use of GBA within ID-FF / ID-WSF.....	9
4.2.1 Architecture for collocation of NAF with Liberty Alliance Authentication Function	12
4.2.1.1 Collocation of IdP/NAF in Liberty Alliance ID-FF (alternatively SAML v2.0).....	12
4.2.1.2 Collocation of AS/NAF in Liberty Alliance ID-WSF.....	13
4.2.2 Architecture for collocation of BSF with Liberty Alliance authentication function.....	15
4.2.2a Logical data model of the Liberty Alliance Authentication Function (IdP/AS)	16
4.2.3 User Registration to Interworking Service.....	16
4.2.3.1 Registration with Operator.....	17
4.2.3.2 Registration with IdP.....	17
4.2.4 Provisioning of User Data for Interworking Service	17
4.2.4.1 Service based on standard user data.....	18
4.2.4.2 Service based on pre-provisioned interworking data	18
4.2.4.3 Service based on explicitly added interworking data	18
4.3 Co-hosting of NAF and IdP.....	18
4.3.1 Federation Concept in GBA.....	19
4.3.2 Session Concept at IdP	19
4.3.2a Single-Logout Concept	20
4.3.3 SSO scenario: ID-FF with <lib:AuthnResponse> transfer.....	20
4.3.3.1 HTTPS with conventional TLS.....	20
4.3.3.2 HTTPS with PSK TLS	22
4.3.4 SSO scenario: ID-FF with artefact transfer.....	23
4.3.5 SSO scenario: ID-WSF Authentication Service	25
4.3.6 SSO scenario: SAML v2.0 with <samlp:Response> transfer	27
4.3.6.1 HTTPS with TLS	27
4.3.6.2 HTTPS with PSK TLS	28
4.3.7 SSO scenario: SAML v2.0 with artefact transfer (resolution)	29
4.3a Co-hosting of BSF and IdP	30
4.3a.1 General.....	30
4.3a.2 UE behaviour	31
4.3a.3 IdP/BSF behaviour.....	31
4.3a.4 Federation Concept in GBA with IdP/BSF collocation	31
4.3a.5 Session Concept at the IdP.....	32
4.3a.6 SSO scenario: ID-FF with <samlp:AuthnResponse> transfer	32
4.4 Use of GUSS / USS in Support of ID-FF and ID-WSF	34
4.4.1 GAA-LAP Interworking Service	35
4.4.2 GAA-LAP Interworking USS.....	35
4.4.2a GUSS / USS when IdP/AS is collocated with BSF	35
4.5 Liberty Alliance Authentication Context and GBA	35
Annex A: Digest Authentication within SASL for Ua protocol between UE and AS/NAF	37

A.1	HTTPS deployment.....	37
A.2	Digest challenge	37
A.3	Digest response	38
A.4	Response auth.....	38
A.5	Subsequent authentication.....	38
Annex Z:	Change history	39
History		41

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

3GPP defined the Generic Authentication Architecture (GAA) independent of the Liberty Alliance Identity Federation and Web Service Framework. Both systems were designed to be deployed independently of each other. The Liberty Alliance Identity Federation and Web Service Framework offers simplified sign-on and session management for complex web service business interaction protocols. The GAA offers a mechanism to provide a shared secret and certificates to two communicating entities for mobile applications, based on GSM and UMTS authentication and key agreement protocols.

1 Scope

The present document provides guidelines on the interworking of the Generic Authentication Architecture (GAA) and the Liberty Alliance architecture. The document studies the details of possible interworking methods between the Security Assertion Markup Language v2.0, SAML v2.0 (or alternatively the Liberty Alliance Identity Federation Framework, ID-FF), the Identity Web Services Framework (ID-WSF), the Security Assertion Markup Language (SAML) and a component of GAA called the Generic Bootstrapping Architecture (GBA). This document only applies if Liberty Alliance and GBA or SAML v2.0 and GBA are used in combination.

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".
- [2] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".
- [3] 3GPP TS 33.221: "Generic Authentication Architecture (GAA); Support for subscriber certificates".
- [4] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".
- [5] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".
- [6] Liberty Alliance Project, ID-WSF v2.0: "Liberty ID-WSF Security Mechanisms".
- [7] Liberty Alliance Project, ID-FF v1.2: "Liberty ID-FF Architecture Overview".
- [8] Liberty Alliance Project, ID-WSF v2.0 "Liberty ID-WSF Authentication Service Specification and Single Sign-On Service".
- [9] Liberty Alliance Project, ID-WSF v2.0: "Liberty ID-WSF SOAP Binding Specification".
- [10] Liberty Alliance Project, ID-WSF v2.0: "Liberty ID-WSF Discovery Service Specification".
- [11] Organization for the Advancement of Structured Information Standards (OASIS), SAML v2 Core "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0".
- [12] Liberty Alliance Project, ID-FF v1.2: "Liberty ID-FF Bindings and Profiles Specification".
- [13] Organization for the Advancement of Structured Information Standards (OASIS), "Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0".
- [14] Liberty Alliance Project, ID-WSF v1.2: "Security Mechanisms".
- [15] Liberty Alliance Project Support Documents: "Authentication Context Specification" v2.0.
- [16] Liberty Alliance Project, ID-WSF "Profiles for Liberty enabled User Agents and Devices" v2.0.