# 3GPP TR 22.895 V2.0.0 (2012-02)

*Technical Report*

# 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Service aspects of integration of Single Sign-On (SSO) frameworks with 3GPP operator-controlled resources and mechanisms (Release 12)


Keywords
Sign-On, Identity

*3GPP*

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

# Contents

# 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

To ensure competitiveness in a longer time frame an evolution of the overall 3GPP system needs to be considered.

This document investigates the functionality and requirements needed to integrate Single Sign-On (SSO) and identity management capabilities within the 3GPP network and their corresponding offered services. The Single Sign-On (SSO) feature enables a 3GPP operator to become an Identity Provider and leverage existing 3GPP services and authentication mechanisms to grant access to Affiliated Application Services located outside the operator's domain without additional user intervention.

The Single Sign-On (SSO) framework is characterized by:

- positioning the operator as the preferred Identity Provider;
- executing user authentication for Affiliated Application Services using 3GPP authentication mechanisms and infrastructure;
- providing reliable and robust secure credential handling;
- cost-efficient deployment and operation; and
- delivering convenience and ease of use for the consumer accessing Application Services (on a mobile device).

# 1 Scope

The Single Sign-On (SSO) framework integration with 3GPP network resource and services intends to execute a comprehensive set of use cases and service requirements to serve various operator authentication configurations.

The scope of the Single Sign-On (SSO) integration study is to:

- provide service and deployment scenarios for 3GPP operators adopting an integrated approach to SSO, including web, person-to-person and M2M service scenarios;
- provide transparent identification and seamless authentication to Application Services on behalf of the user;
- support a comprehensive set of use cases of integration of different Identity and SSO frameworks (e.g OpenID) for various operator authentication configurations;
- define use cases and provide service requirements for Operators sharing controlled user credentials with Affiliated Application Service Providers;
- define use cases and service requirements associated with ensuring that the intended user is making use of the associated SSO capability (including the case when the UE has been stolen or lost);
- realize the Identity Provider role within the 3GPP network ecosystem and its influence among outside internet web service providers; and
- provide an enhanced user experience with secure, reliable access and authentication to Affiliated Application Services.

# 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] OpenID Foundation "OpenID Authentication 2.0", http://openid.net/specs/openid-authentication-2_0.html.

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**Affiliated Application Service Provider:** An Application Service Provider having a trust relationship with the IdP and/or SSO Provider. The Affiliated ASP is referred to as the Relying Party in the OpenID Specification [2].

**Application Service:** A network-based service delivered to the user through an application that resides on the UE. The Application Service may be web-based or non-web-based.

**Application Service Provider:** A party that offers Application Services.

**Credentials:** Evidence that proves the identity of a user and is critical to the process of authentication.

**Identity Provider:** A party that provides the service of asserting a user's identity to an Application Service and to an SSO Provider.

**OpenID Provider:** An OpenID Authentication server on which a Relying Party relies for an assertion that the end user controls an Identifier (see OpenID Specification "OpenID Authentication 2.0" [2]).

**SSO Authentication:** Authentication between a UE and SSO Provider using Operator- or SSO Provider-controlled credentials and without requiring user involvement.

**SSO Provider:** A party receiving identity assertions from an Identity Provider and providing authentication of users to Application Service Providers.

**SSO Service:** A service in which a user is authenticated once (i.e., "single sign-on") and provided with seamless access to multiple Application Services.

**User Authentication:** Authentication that establishes the presence of the rightful user by requiring an input of credentials (e.g., PIN, password, biometric characteristic) which only the rightful user would be able to provide.

NOTE: User authentication is not achieved if the credentials are provided automatically (e.g., by storing them in a Web browser for automatic entry onto an HTML form). However, such automated use of credentials may still be regarded as a form of authentication of varying strength when presented together with data, which may include the freshness of the authentication and assurance level, that establishes the user was present when the authentication was carried out and the result stored locally.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

| | |
|---|---|
| AASP | Affiliated Application Service Provider |
| ASP | Application Service Provider |
| IdP | Identity Provider |
| OP | OpenID Provider |
| RP | Relying Party |
| SSO | Single Sign-On |

# 4 Use cases, services and user groups

## 4.1 Introduction

This clause investigates a set of use cases for integration of different Identity and SSO frameworks (e.g., OpenID) with the 3GPP networks set up for various authentication configurations (e.g. with and without GAA/GBA via TR 33.924) . It also explores service requirements for operators that enable authenticated access to Affiliated Application Service Providers.

The following common pre-conditions are assumed for all use cases:

- The Operator provides an SSO Service.
- The user has a service subscription with SSO support.
- The user has at least one data service account.
- The user agrees to the terms and condition to use SSO with the Operator.
- The user agrees to the terms and condition to use SSO with the Affiliated Application Service.

- Service agreements and charging schemes are already in place between Affiliated Application Service Providers and Operators.

- The user is able to access the Application Service via devices registered with the operator.

## 4.2 Use case 1: Affiliated Application Service access

### 4.2.1 Pre-conditions

A user has purchased a subscription plan that includes an operator managed SSO Service. The user has multiple Application Service accounts and IMS-based domain services already established. The user's device is a non-3GPP device (e.g., fixed consumer device or a WiFi-only mobile device) and does not use a UICC/smartcard for network access.

- Operator acting as an SSO Provider has pre-provisioned the SSO credentials within the network and non-3GPP device.

### 4.2.2 Service flows

A user has an established service with an operator and relies on his operator to provide a SSO Service. The user wishes to use a 3rd party movie service such as Netflix, to access his personal account to select and view a movie of his choice, on a consumer device. Immediately upon entering the service, the user is seamlessly and transparently connected to his AASP account without performing user authentication (e.g., being prompted for login and password credentials). The user freely selects a movie and watches it using an application on his device, without interruption.

The user is transparently authenticated by an SSO Service, which is provided by the operator. The absence of a UICC in this scenario necessitates the use of non-UICC based credentials for authentication. More specifically the means of network access for this scenario could, for example, employ the use of SIP-Digest or PKI based credentials, which may be reused for SSO authentication.

### 4.2.3 Requirements

- The SSO Service provided by the operator shall provide secure seamless and transparent access to Affiliated Application Services for non-3GPP devices which do not use a UICC/smartcard for network access.

## 4.3 Use case 2: Seamless SSO access between Operator service and multiple Affiliated Application Services

### 4.3.1 Pre-conditions

A user has purchased a subscription plan that includes the SSO Service. The user has multiple Application Service accounts and operator services such as IMS-based domain services or mobile data services already established.

- Credentials required for authentication are already secured within the network and UE.

- Applications are installed on the UE if needed to access a service.

### 4.3.2 Service flows

A user has been authenticated for and is using an operator service such as IMS messaging services and wishes to access an Affiliated Application Service, such as a social website. Immediately upon accessing the Affiliated Application Service, the user is transparently connected to his account at the AASP without providing login and password credentials. Later, the user can get the same seamless SSO experience when accessing the services of a different AASP.

## 4.4 Use case 3: Seamless mobility access to an Affiliated Application Service Provider across Operator/IdP domains

### 4.4.1 Pre-conditions

A user has purchased a subscription plan that includes the SSO Service. The user has multiple Application Service accounts and operator services such as IMS-based domain services or mobile data services already established.

- Credentials required for authentication are already secured within the network and UE.
- Applications are installed on the UE if needed to access a service.

### 4.4.2 Service flows

A user is on a train watching an Internet TV show provided by his AASP on his laptop using LTE. The viewing mechanism can be any application used for accessing the AASP's internet TV service. As the user travels and moves from the coverage area of one Operator/IdP network to the coverage area of another Operator/IdP with whom the first Operator/IdP has a roaming agreement, the SSO Service manages the change in IdPs seamlessly, transparently and without noticeable delay. The user watches the TV show without any interruption caused by the change of IdPs.

## 4.5 Use case 4: Accessing an Affiliated Application Service using OpenID

### 4.5.1 Pre-conditions

- The user's network operator is also an *OpenID* identity provider.
- The *OpenID* identifier has been established by the network operator.
- The online photo service is an Affiliated Application Service that supports *OpenID*.
- The online photo service trusts the user's network operator for the user authentication.

### 4.5.2 Entities involved in the use case

The following entities are involved in the authentication procedure:

- User with the user equipment (UE), which is capable of running a web client or a dedicated application and communicating with the appropriate operator credentials.
- Application Web server — an entity providing an online photo service. It plays the role of a Relying Party.
- *OpenID* identity providing service (OP), which is controlled by the operator.
- Operator's HSS.

### 4.5.3 Service flows

A user, who has a subscription with a mobile network operator, accesses an Affiliated Application Service which supports *OpenID*, for example an online photo service. The user's network operator is also an *OpenID* identity provider. Upon making a request, which contains the user's *OpenID* identifier to the online photo service, the user gains an authenticated access to the photo service for viewing access-protected photographs without being involved in the authentication procedure.

### 4.5.4 Requirements

- The UE shall be capable of authentication with the use of Operator-controlled credentials.

- The application web server (Relying Party) shall be able to support the *OpenID* specification [2].
- The OP shall be able to perform authentication based on Operator-controlled credentials.

## 4.6 Use case 5: User authentication

### 4.6.1 Pre-conditions

The following pre-conditions apply to this use case:

- The UE is equipped to recognize a certain pre-defined condition (e.g., an event such as power-up of the UE, request from network) to trigger authentication of the user.
- The UE securely stores the user's SSO authentication credentials.
- The UE is provisioned with an operator's or SSO Provider's policy that governs triggering of the user authentication.

### 4.6.2 Service flows

According to Operator or SSO Provider provisioned policies, the user is authenticated by the UE. Upon successful user authentication, the UE then securely stores the time when the authentication was carried out. Later, the user proceeds to access an OpenID supported Application Service. The UE retrieves and presents the identity and evidence of local authentication (e.g., time of successful authentication, assurance level of the authentication) to the Application Service. Assurance level could take into account what type of user authentication was performed (e.g., number of authentication factors such as password, token, biometric). The Application Service receives the evidence, and upon inspection, grants the user access to the service transparently (i.e., without requiring the user to be further involved in the authentication procedure).

### 4.6.3 Requirements

NOTE: These requirements may be combined with other use cases if policy requires that user authentication must be established or checked/refreshed for access to the AASP's service.

- The Operator shall be able to configure policies which govern the user authentication procedures.
- Affiliated Application Service Providers shall be able to request a user re-authentication.
- The user shall be authenticated according to the service providers' authentication assurance level and freshness of the authentication.
- The UICC may be capable of recording, securely storing and relaying to the network evidence of user authentication, the time at which the user authentication was carried out and the assurance level of that authentication.
- The UE shall be able to carry out user authentication according to Operator provisioned policies or user preference on the UE.

## 4.7 Use case 6: Automation of authentication method

### 4.7.1 Pre-conditions

The following pre-conditions apply to this use case:

- The UE supports more than one option of access network-based SSO authentication method (e.g., 3GPP GBA, 3GPP AKA, 3GPP ISIM, 3GPP SIP-Digest, EAP variants).
- The UE supports methods which include user-entered SSO credentials (e.g., identity and password) for user authentication.

### 4.7.2 Service flows

A user accesses an SSO (e.g., OpenID) supported Affiliated Application Service on a UE. The UE and IdP or SSO Provider agree on an SSO authentication method to be used to access the service without requiring further user involvement in the processes of agreement or the subsequent usage of the agreed method. The user proceeds to seamlessly access the service accordingly.

### 4.7.3 Requirements

- When a user accesses an Affiliated Application Service, the UE and SSO Provider shall be able to agree on an authentication method to be used without requiring user involvement in the processes of agreement or the subsequent usage of the method.
- A different authentication method may be selected each time the user is to be authenticated for access to an Affiliated Application Service.

## 4.8 Use case 7: Seamless service detection, redirection and supply of credentials by a UE

### 4.8.1 Pre-conditions

The following pre-conditions apply to this use case:

- A user has registered his SSO identifier(s) with appropriate IdP(s).
  NOTE: There may be multiple SSO methods and IdPs supported by the UE (e.g., OpenID, Liberty Alliance).
- The user has registered his SSO credentials for authentication (e.g., identity and password) with the IdP(s) and stored them in the UE.
- User authentication has been established or checked/refreshed according to Operator policy provisioned on the UE.

### 4.8.2 Service flows

Current SSO services require the user to view a screen and recognize when credentials are being sought and supply manually the credentials upon request. In order for the user to avoid having to recognize and enter his or her credentials manually, possibly having to repeat this process for each and every service, the process is automated by the UE.

### 4.8.3 Requirements

- The UE is required to automatically detect a request for credentials from the AASP and SSO Provider, possibly requiring this action for several such providers, and supply the credentials automatically without user intervention.

## 4.9 Use Case 8: Seamless transition between 3GPP access and non-3GPP access to a service via the SSO of a single IdP

### 4.9.1 Pre-conditions

- A user has a subscription with the mobile network operator that includes SSO Service.
- The user's UE supports access via 3GPP and non-3GPP networks.
- The social network is a web service of an AASP.

- The AASP trusts the user's network operator for authentication of the user for access to this service.

### 4.9.2 Service flows

A user has a User Equipment (UE) that is able to establish a connection to the AASP both via 3GPP networks and via non-3GPP networks (e.g., public or private WLAN). The user has a subscription that includes an SSO Service with a mobile network operator/IdP and accesses an Affiliated Application Service, for example a social network. The user gains an authenticated access to his social network account without being involved in the authentication procedure. The SSO Service asserts authentication to the AASP regardless of the access technology over which the user may be connected. A subsequent transition from or to non-3GPP access is seamless and transparent to the user.

### 4.9.3 Entities involved in the use case

The following entities are involved in the authentication procedure:

- User with the user equipment (UE), which is capable of establishing an IP connection via both 3GPP access and non-3GPP access.
- AASP – an entity providing a social network service. It plays the role of a Relying Party.
- SSO Service, which is controlled by the operator.
- Operator's HSS.

### 4.9.4 Requirements

- The SSO framework shall be able to support seamless transitions between 3GPP access and non-3GPP access technologies during the same SSO Service session (i.e., during a session with the same IdP).
- Transitions between 3GPP access and non-3GPP access technologies shall be transparent to the user from an SSO service perspective.

## 4.10 Use case 9: User identity acknowledgement for SSO usage

A user submits a notification to the operator when he becomes aware that his UE is stolen or lost. Subject to the user's request, the operator pauses SSO support for the user. When he want to access an Affiliated Application Service, he is requested to perform user authentication, which may involve credentials supplied independently from those previously supplied for the SSO Service. Additionally, if he submits evidence that he is the intended user the SSO support can be resumed by the operator.

### 4.10.1 Requirements

When an operator receives a notification from a user that his UE is lost or stolen, the operator shall pause the SSO support for that user until evidence is provided by that user to resume the SSO support.

When the SSO support for a user is paused, any further attempt to access a service shall require the user to be authenticated via credentials which may be supplied independently from those previously supplied for use with the SSO Service.

## 4.11 Use case 10: Using the 3GPP SSO Service by another (non-MNO or other MNO) SSO Provider

### 4.11.1 Pre-conditions

- A user has a subscription with the mobile network operator that includes SSO Service.
- The user also subscribes to an SSO Service that uses a 3rd party IdP, such as Facebook.

- The user has a subscription with YouTube that was created using Facebook as the IdP (subscription is identified by Facebook ID).
- YouTube trusts Facebook for user identity and authentication.
- Facebook and the user's network operator trust each other for the user identity and authentication. Facebook and the network operator's SSO Provider have created an interworking relationship between them.
- The SSO Provider configuration has already happened between the 3GPP SSO Service and the 3rd party IdP.

### 4.11.2 Service flows

A user is registered to a web based SSO service, for example Facebook that he uses to connect to web application servers (RPs). The user has already established subscriptions with numerous AASPs, among them YouTube, using Facebook's IdP as its SSO Service. The user's 3GPP network operator has established an SSO Service based on 3GPP credentials for SSO authentication and makes an offer to the user to join this service. The user, seeing the value in this service, wishes to make use of this service but wants to be sure he will be able to seamlessly access all his existing subscriptions (that were created using his Facebook Identity) using the operator's SSO Service (without the need to re-open and/or re-configure all his existing subscriptions in the different web services/RPs). The operator offers the user the possibility of using the 3GPP 3rd Party SSO Service. This means that: the 3GPP SSO Service can be utilized to seamlessly sign on to a subscription which was created using a Facebook Identity. This requires only a simple one-time set-up session which configures the existing interworking relationship between the Facebook IdP and the 3GPP SSO Service for that specific user.

The user joins the 3GPP SSO Service and during the registration process configures all his existing IdPs (such as Facebook) to be part of the interworking services.

The user, having joined the 3GPP SSO Service, requests to access YouTube with the subscription that was created using the Facebook SSO Service. The SSO authentication request is identified to be part of the "SSO Service interworking with the 3rd party IdP identified as Facebook", and uses the 3GPP SSO Service to validate the user identity followed by connecting the user, seamlessly (without any request to authenticate to Facebook), to YouTube to watch his favorite clip.

### 4.11.3 Entities involved in the use case

The following entities are involved in the authentication procedure:

- User with the user equipment (UE), which is capable of establishing an IP connection.
- Application Web server (e.g., an entity providing an online book store service). It plays the role of an AASP and a Relying Party.
- A 3rd Party SSO Provider (in this case, Facebook) – an entity which provides SSO and Identity management service to the user and which acts as an IdP (e.g., for YouTube).
- 3GPP SSO Service, which is controlled by the operator and includes the interworking with the 3rd Party SSO Service functionality.
- Operator's HSS.

### 4.11.4 Requirements

- The SSO framework shall support an interworking relationship between the 3GPP SSO Service and SSO Service from other providers.
- Login to a subscription created using a 3rd Party SSO Service using the 3GPP SSO Service shall be transparent to the User (looks the same as login to a subscription created using a 3GPP operator provided SSO Service).
- The user shall be able to request that his SSO subscriptions are recognized by both parties in the interworking relationship between the 3GPP SSO Service and the 3rd party IdP.
- The user shall be able to maintain his or her other SSO identities registered to the original IdPs.

## 4.12 Use case 11: SSO-provided attribute exchange and associated user consent

### 4.12.1 Pre-conditions

A user has purchased a subscription plan that includes the SSO Service. The user already has Application Service accounts and operator services such as IMS-based domain services or mobile data services already established. The user has upgraded the UE (e.g., from a small smart phone to tablet PC with 3GPP access) with additional applications.

- Credentials required for authentication are already secured within the network and UE.
- User has specified attributes for attribute exchange.
- New applications are installed on the UE if needed to access a service.

### 4.12.2 Service flows

A user is using an operator service and wishes to add a new Affiliated Application Service, such as a business application in the cloud for the first time. Upon accessing the new Application Service, the Application Service requires an initial registration based on user-specified attributes. The SSO Service supports the initial registration by exchange of user-specified attributes and asks the user for consent of the attribute exchange to the new Application Service.

### 4.12.3 Requirements

- The SSO Service shall provide the exchange of user-specified attribute to Affiliated Application Service for initial registration of the user at Affiliated Application Service according to user-specified attributes.
- The SSO Service shall enable the user to be notified of an attribute exchange and to provide consent on the content of attribute exchange being requested.

## 4.13 Use case 12: User management of the association between an Application Service and the SSO Service

### 4.13.1 Pre-conditions

A user has purchased a subscription plan that includes the SSO Service. The user already has Application Service accounts and operator services such as IMS-based domain services or mobile data services already established. The user has upgraded the UE (e.g., from a small smart phone to tablet PC with 3GPP access) with additional applications.

- Credentials required for authentication are already secured within the network and UE.
- New applications are installed on the UE if needed to access a service.

### 4.13.2 Service flows

A user is using an operator service and wishes to add a new Affiliated Application Service, such as a business application in the cloud for the first time. Upon accessing the new Application Service, the SSO Service manages a first-time user verification of the authentication at the new Application Service to prevent risk of unauthorized background usage of the SSO authentication.

### 4.13.3 Requirements

- The SSO Service shall support the ability of the user to manage the association between an Application Service and the SSO Service. In this case user authentication is required.

# 5 Business Models

The mobile operator may become an SSO Provider, interworking with the user-centric services provided outside of that operator's domain. This clause studies the potential business models for the mobile operator and the AASPs.

The mobile operator provides the SSO functionalities for the AASP either directly or via cooperation with an independent SSO Provider and the SSO Provider may pay the mobile operator with a fixed rate or based on the number of service users. The mobile operator has a business agreement with an AASP to provide SSO services.

This model offers the following benefits:

- The user may access the third party service via operator's network with SSO support.
- The mobile operator may provision more attractive services for the users.
- Subscribers of the mobile operators and the AASPs rely on a trusted IdP and SSO Provider.

# 6 Deployment Scenarios

All use cases described in clause 4 need to take into account that Operators may or may not support various authentication capabilities which could potentially be used for SSO, e.g., GBA, AKA, SIP DIGEST, username/password or other capabilities.

# 7 Service Aspects

This clause studies Service requirements for operator-centric SSO interworking with current state of the art identity management systems (e.g. OpenID, OAuth, SAML).

# 8 Charging Aspects

The mobile operator may become a SSO provider. This clause studies Charging requirements for operator-centric SSO interworking with current state of the art identity management systems (e.g. OpenID).

# 9 Security Aspects

A mobile operator may become a SSO provider, interworking with the user-centric Web services provided outside of that operator's domain. This clause studies Security requirements for operator-centric SSO interworking with current state of the art identity management systems (e.g. OpenID, OAuth, SAML).

# 10 Privacy Aspects

This clause studies Privacy requirements for operator SSO interworking with the Application Services provided outside of that operator's domain.

# 11 Suggested Requirements

## 11.1 Requirements for the UE

REQ_UE_001: The UE shall support SSO authentication without user intervention based on operator-controlled credentials.

REQ_UE_002: The UE shall support a request for user re-authentication from Affiliated Application Service Providers or the SSO Provider.

REQ_UE_003: For the UE that supports non-3GPP access, transitions between 3GPP access and non-3GPP access technologies shall be transparent to the user from an SSO Service perspective.

REQ_UE_004: The UE shall be able to initiate the SSO Service regardless of the access technologies supported by the UE.

REQ_UE_005: The UICC may be capable of recording, securely storing and relaying the evidence of user authentication, the time at which the authentication was carried out and the assurance level of that authentication.

## 11.2 Requirements for an SSO Service

REQ_SSO_001: The SSO Service provided by the SSO Provider shall provide secure seamless and transparent access to Affiliated Application Services to the user.

REQ_SSO_002: The SSO Service provided by the SSO Provider shall provide secure seamless and transparent access to Affiliated Application Services for subscribers to the SSO Service using devices that support either 3GPP access or non-3GPP access.

REQ_SSO_003: The SSO Service shall be able to support the OpenID specification [2].

REQ_SSO_004: The SSO Service shall support authentication based on operator-controlled credentials and policies.

REQ_SSO_005: The SSO Service may support negotiation and use of an agreed authentication method between the Operator and the SSO Provider. The negotiation of an authentication method may be repeated each time the user accesses an AASP's service.

REQ_SSO_006: The SSO Service shall support seamless service continuity between 3GPP access and non-3GPP access technologies during the same Affiliated Applications Service session.

REQ_SSO_007: Login to a subscription created through a 3rd party IdP using the 3GPP SSO Service shall be transparent to the user. The user shall be able to configure which 3rd party SSO identities are used with the 3GPP SSO Service.

# 12 Summary and conclusions

This Technical Report analyzes use cases and provides requirements for integrating Single Sign-On Service frameworks with 3GPP operator-controlled resources and mechanisms.

New potential requirements for the SSO Service have been identified in clause 11 of this Technical Report. It is therefore recommended that this clause is used as a basis for introducing new requirements into 3GPP Technical Specifications.

This report further recommends that a set of SSO requirements limited to operational and service aspects are captured in SA1 specifications (e.g., a new clause in TS 22.101).

# Annex <A> (informative): Change history

*It is usual to include an annex (usually the final annex of the document) for reports under TSG change control which details the change history of the report using a table as follows:*

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New |
| *8/11/11* | *SA1#55* | *S1-112269* | | | *Addressed Vodafone comment to change REQ_SSO_003 from "shall" to "shall be able to"* | *0.2.0* | *0.2.1* |
| *Sept 2011* | *SA#53* | *SP-110587* | | | *Raised to v.1.0.0 by MCC for presentation to SA* | *0.2.1* | *1.0.0* |
| *11/16/11* | *SA1#56* | *S1-113450* | | | *Incorporated agreed documents S1-113275, S1-113280, S1-113281, S1-113282, S1-113283, S1-113284* | *1.0.0* | *1.1.0* |
| *11/18/11* | *SA1#56* | *S1-113462* | | | *Addressed Vodafone objections at SA1 Plenary* | *1.1.0* | *1.2.0* |
| *01/31/12* | *SA1#57* | *S1-120093* | | | *Rapporteur editorial cleanup* | *1.2.0* | *1.2.1* |
| *02/16/12* | *SA1#57* | *S1-120323* | | | *Incorporated agreed documents S1-120271, S1-120328* | *1.2.1* | *1.3.0* |
| *02/2012* | *SA#55* | *SP-120108* | - | - | *Raised to v.2.0.0 by MCC for approval at SA#55 (no technical change)* | *1.3.0* | *2.0.0* |