
TSG-SA WG1 #17
Durango, USA, 12-16th August 2002

S1-021734
Agenda Item: 10.10

Title: Reply LS on Push Security
Response to: S3-020403 on Reply LS on Push Security from SA3 (S1-021511)
Release:
Work Item:

Source: SA1
To: SA3
Cc: SA2, T2

Contact Person:
Name: George Bumiller
Tel. Number: +1 519 722 7312
E-mail Address: gbumiller@rim.net

Attachments: S1-021622 (Draft TS 22.174 v1.2.1)

1. Overall Description:

SA1 thanks SA3 for their comments on security for Push stage 1 [draft TS 22.174]

SA1 wishes to advise that the LS was brought in by one of the Push SWG members before it had been formally received. The comments were reviewed and used in updating the Push stage 1, which has been further advanced at the current meeting to v.1.2.1.

2. Actions:

To SA3 group.

ACTION: SA1 wishes to provide SA3 with the current draft of the TS for their comments.

SA1 would be pleased to have further comments on the current draft TS 22.174 that SA3 may wish to make.

3. Date of Next TSG-SA1 Meetings:

SA1 SWGs	14-18 October 2002,	Beijing, co-located with SA2
SA1#18	11-15 November 2002,	Busan, Korea, hosted by Samsung

TSG-SA1-#17
Durango, U.S.A, 12 – 16 July 2002

S1-021622
Agenda Item: Push 10.10

3G TS 22.174 v.1.2.1

Technical Specification

**3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Push Service
Service aspects (Stage 1)
(Release 6)**



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPP Organisational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organisational Partners' Publications Offices.

Keywords

UMTS, service, push

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>

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.

© 2000, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Contents	3
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
3 Definitions and abbreviations	6
3.1 Definitions.....	6
3.2 Abbreviations	6
4 Overview of the Push Service	6
5 Requirements.....	8
5.1 General.....	8
5.2 Provisioning	8
5.3 Subscription	9
5.4 Addressing and Routing	9
5.5 Delivery.....	10
5.6 Service Management	10
6 Security.....	10
7 Privacy.....	11
8 Access rules.....	11
Charging	12
10 Push Subscription Profile Information.....	12
11 Roaming	13
12 Inter-working.....	13
12.1 Inter-working with the Internet.....	13
12.2 Service Independence.....	13
12.2.1 Forwarding	13
12.2.2 Barring.....	13
13 Feature Interactions	13
14 Annex B: Change history	13

556677799101011121313

Foreword

This Technical Specification has been produced by the 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 this TR, 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 specification.

Introduction

The Push Service introduces a means to transmit push data from a push initiator to a push recipient (e.g. a UE) without a previous user action. The push concept, as provided by the SMS teleservice, has been very successful in the GSM second generation, both for text messaging (for user viewing) and for other unstandardized data to the SIM (as a building block used for OTA and other purposes). This TS introduces the Push Service as a generalization of existing network capabilities plus the development of new capabilities. The Push Service should therefore be understood as a building block (network capability), which can be used for new services, both public and private, in 3GPP.

In the normal client/server model, a client requests a service or information from a server, which then responds in transmitting information to the client. This is known as the “pull” technology, the user pulls information from the content provider. The World Wide Web is a typical example of pull technology, where a user enters a URL (the request) that is sent to a server and the server answers by sending a Web page (the response) to the user.

In contrast to this there is also the “push” technology where there is no explicit request from the user before the content provider (push initiator) initiates an information transfer to a user. Another way of saying this is that whereas “pull” transactions of information are always initiated from the user, “push” transactions are content provider initiated. The welcome message received after registration with a visited network whilst roaming is an example of information transfer that has been initiated without a request from the user. Typically, a user signs up with the push initiator and defines their interest, volume of information acceptable and other factors in the push subscription profile. As information becomes available that satisfies the user’s push subscription profile, the push initiator delivers it to the user using the Push Service.

The Push service may be used to implement high level services such as IP multimedia services, MMS, etc., and new services including public safety, government, corporate IT, transfer of push data to machines and devices, in addition to infotainment type services.

Another common use for push services is the delivery of notification from e.g. MMS to the user while the user has the

option of “pulling” the actual push data from the push initiator.

The PLMN Push function provides the push data to the user agent in the UE. The user agent interprets and presents the push data to a person, device or machine using the UE.

NOTE: The requirements of services such as streaming, conversational services and broadcast are independent from push. Therefore they are not considered appropriate for inclusion here. Push will be available for use in appropriate applications of all high level services.

1 Scope

This Technical Specification defines the Stage 1 description of the Push Service and is the set of requirements that shall be supported for the provision of push, seen primarily from the subscriber’s, service providers’ and delivery network points of view.

This TS includes information applicable to network operators, service providers, terminal and network manufacturers. It is of use to manufacturers and organisations, which have devices or machines benefiting by availability of push service.

This TS contains the core requirements for the Push Service, for operator and external Push Initiators, which are sufficient to provide a complete service capability and service capability feature.

This TS defines the requirements for the Push Service to enable delivery of push data, including such functionality as:

- Transfer of push data from a Push Initiator to a Push Recipient
- Latency and Priority classes,
- Delivery class
- Definition of handling of undeliverable push data

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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] 3G TS 21.133: “3G Security; Security Threats and Requirements”

[2] 3G TS 21.905: “Vocabulary for 3GPP Specifications”

3 Definitions and abbreviations

Definitions and abbreviations used in the present document are listed in TR 21.905 [2]. For the purposes of this document the following definitions and abbreviations apply:

3.1 Definitions

Push Data: data sent by the push initiator to the push recipient, of a format known to the receiver (push recipient), and not otherwise defined by the push service.

PLMN: the 3GPP network that receives the push data from the push initiator and ensures the delivery of push data to the push recipient. The delivery of the push data may involve other networks.

Push function: the function in the PLMN that receives the Push Data from the Push initiator. The push function is responsible for delivering the push data to the Push recipient.

Push initiator: the entity that originates push data and submits it to the push function for delivery to a Push recipient. A Push initiator may be e.g. an application providing value added services.

Push recipient: the entity that receives the push data from the Push function and processes or uses it. This may include the UE with which the PLMN communicates with, the user agent with the application level address, and the device, machine or person which uses the push data. A Push recipient is controlled by an individual user .

Push service: a service capability offered by the PLMN. The Push Service is initiated by a Push Initiator in order to transfer push data (e.g. data, multimedia content) from the Push Initiator to the Push Recipient without a previous user action. The Push Service could be used as a basic capability or as component of a value added service.

Push User agent: is any software or device associated with a Push recipient that interprets Push Data to the user. This may include textual browsers, voice browsers, search engines, machine or device interface software, etc.

Push Subscription Profile: a set of parameters indicating the Push recipient’s settings and preferences for the Push Service.

3.2 Abbreviations

For the purposes of this document the following abbreviations apply:

URL – Uniform Resource Locator.

4 Overview of the Push Service

The overview of push is followed by a summary of the relationships among the entities involved (operators, users, push recipients and push initiators).

NOTE: these are functional descriptions: multiple functions may, depending on business arrangements, be performed by a single entity.

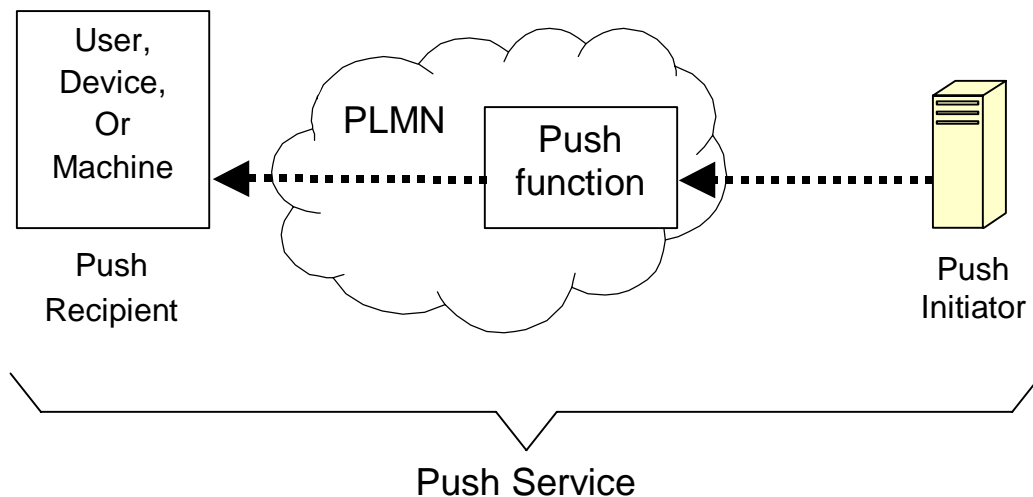


Figure 1: Push Service Overview

The Push Service is a service whereby the Push Initiator sends push data through a Push Server to a Push Recipient, without interaction from the Push Recipient.

The typical mode of operation is as follows:

- A Push Recipient (e.g. user, receiving device like a meter) explicitly or implicitly subscribes to a set of value added services offered by various Push Initiators and allow these Push Initiators to send it push data that meet the Push Recipient's configured criteria. (This configured criteria is part of the Push user profile.)
- A Push Initiator identifies information matching the criteria set by the Push Initiator and package it up into the push data
- The Push Initiator delivers the push data to the Push function, identifying the Recipient's address, and optionally delivery class, priority, delivery time parameters, etc.
- The Push function takes the responsibility of delivering the push data, optionally following the delivery class, priority and delivery time parameters, to the Push Recipient and for providing feedback to the Push Initiator regarding delivery of the push data if requested by the Push Initiator.

Key characteristics of the Push Service include:

- The Push Initiator may, but is not required to deal with the specifics of the wireless transport, selection of appropriate bearers, out-of-coverage or roaming issues, and other wireless network anomalies. These are all managed by the Push Service and hence can be optimised at the network level rather than being handled by all applications. Using an available bearer the push service offers as many capabilities that are available to delivery of the push data following the requested push services requested by the push initiator.
- The push initiator shall be provided with a means to query the push server for a specific recipient's push user profile subject to privacy considerations.
- The push server shall not change the push data (contents). Any transformations that the Push Server provides shall be compliant with user privacy requirements as defined in the push subscriber profile.
- The push service shall be able to handle user groups (i.e. have the ability to target a certain group of push recipients).
- The push service is capable of supporting asynchronous communication between a Push Initiator and the push recipient on a wireless device.

- The privacy of the user is important and the introduction of the push services should in no way result in unwanted information “spam” being sent to mobile users.

The Push data could contain:

- Application specific data exchanged between a server and its client e.g. ERP, CRM, Field Service management, m-commerce transaction data or a meter reading
- Provisioning or configuration control data
- MMS content data

The entities shown in Figure 1 are Push Initiator, Push Server (PLMN) and the Push Recipient. The Push Initiator may be outside the Operators network and hence will require well-defined relationships amongst them.

For example, a Push Initiator can be within the Operator domain (e.g. an operator portal) or an external VASP. A Push Recipient (e.g. a User) will need to be part of the Operators network and will require allowing the network to pass through push data and also subscribing to the Push Initiator to generate the data it wants pushed. To support flexible billing models, it becomes necessary for the Operator to have a defined commercial relationship with the Push Initiator.

5 Requirements

The following list gives the high level requirements for the Push service:

5.1 General

The Push Service shall allow a Push Initiator (which may be external to the PLMN) to initiate delivery of push data to the Push recipient. It shall be possible to deliver push data to the push recipient without any user intervention, subject to settings in the push subscription profile. The Push Initiator may interrogate the push subscription profile, if available, in order to establish the user preference related to the Push Service.

- The push mechanism shall be efficient in the use of network resources and terminal resources.
- It shall be possible to support Push Service independently over CS (including CS data and SMS), PS domains or IMS.

NOTE: Operators should be able to choose which of these options they use to deliver Push services, and it should be possible to use these options independently from each other. E.g. delivery over the PS domain would allow operators who are not planning to introduce IMS and SMS to offer Push Services.

- It shall be possible to deploy Push Services independently of other services defined by 3GPP.
- The quality of service delivery shall be able to include time-sensitive as well as reliable delivery choices
- It shall be possible to use all available access networks (e.g. GERAN, UTRAN,).
- It shall be possible for the Push Initiator to specify a bearer for the Push Service, as a default the push service shall identify the bearer. The Push Initiator may, however, require certain grade of service for delivery, e.g. speed of delivery or delivery acknowledgement.

5.2 Provisioning

The operator shall be able to provision a user or organisation-user (e.g. a subscriber or a VASP) with the Push Service. The provision may include usage of the Push Service as a Push initiator, as a Push recipient or both.

The provision may be:

- general: where the service is made available to all user or organisation-users (subject to compatibility restrictions enforced) without prior arrangements being made with the operator;
- pre-arranged: where the service is made available to an individual user or organisation-user only after the necessary arrangements have been made with the operator.

If the user is provisioned with the Push Service as a Push initiator he may use the Push Service in order to transfer push data to the Push Recipient, subject to settings in the push subscription profile of the Push Recipient.

If the user is provisioned with the Push Service as a Push recipient he may use the Push Service in order to receive push data from a Push initiator.

The push subscription profile parameters (user's settings and preferences) are managed by the user or the operator on behalf of the user.

The operator shall be able to withdraw the provision of the Push service. Withdrawal may be general or pre-arranged.

NOTE: Provisioning with – or subscription to – value added services, that make use the Push service are out of scope of this specification.

NOTE : the concept of organisation user may apply to GUP and if so will not be duplicated here.

5.3 Subscription

The usage of the Push Service to deliver push data from a Push Initiator to a Push Recipient requires as a precondition either an explicit or implicit subscription to the Push Service

Explicit Push Subscription:

A subscriber subscribes to the Push Service together with the Push service provider, i.e. the home PLMN operator. Home PLMN Push service providers may then use the Push service to deliver content to the subscriber.

Implicit Push Subscription:

A Value added service provider shall be able to subscribe to the Push Service on behalf of a subscriber to a value added service provided by this VASP. From a Push service point of view the subscriber becomes a push recipient. From now on the Value added service provider shall be able to use the Push Service capabilities to deliver content to this particular subscriber, i.e. the push recipient.

The Push service subscription is valid for the subscriber to receive push data from the VASP that has subscribed to the Push service as long as the subscription is valid.

5.4 Addressing and Routing

It shall be possible to uniquely identify push recipients.

It shall be possible for push recipients to uniquely identify push initiators.

The addressing model shall include addresses of the device (e.g. IP address, SIP-URI, MSISDN) and application level addressing (i.e. user agents). The addressing model shall be compatible with Internet specifications when applicable.

It shall be possible to deliver push data to a push recipient with a dynamically allocated IP address.

The Push service shall be able to deliver a push data to a push recipient that does not have an IP address currently assigned.

Both telecom and internet numbering and addressing schemes shall be supported.

It shall be possible to address push recipients without allocating E.164 numbers.

5.5 Delivery

The PLMN may set restrictions including maximum size of Push data.

The Push Service may offer classes of priority and service delivery. When offered this shall include support for the following:

- Delivery time constraints (timing window, i.e. allow the push initiator to specify "deliver after" and "deliver before" parameters)
- Requested delivery priority (different priorities dependent on for example push initiator, or allowing the push initiator to specify the desired priority)
- If neither delivery time nor priority is set then a single attempt shall be made to deliver the push data without unnecessary delay.
- The push service shall be able to send a delivery report to the push initiator, which includes information about a specific submission's final outcome (delivered, expired, etc.). The report is sent only if the push initiator requested it in the initial push submission or has requested it for all push submissions.
- It shall be possible to deliver push data both in an acknowledged and an un-acknowledged manner between the push service and the push recipient
- It shall be possible for the push initiator to request that only one delivery attempt is made.

In case the push recipient declines a specific instance of push data, it shall be provided with means to indicate whether the push service is allowed to re-send it or not.

In the case that classes of priority and service delivery are not offered an attempt to deliver push data to the push recipient shall be made without unnecessary delay.

5.6 Service Management

The basic principle of service management is "the user is in control".

The user is provisioned with the Push Service by a Network Operator. If a user is provisioned with the push service, the provisioning data shall include a push subscription profile for push service settings and push service preferences. .

The push subscription profile of a Push Recipient shall at least contain:

- General settings, independent of individual Push initiators
this may include:
 - Permissible minimal QoS per data format for receiving push data
 - Permissible maximum size of push data permitted to be pushed
 - Permissible charging thresholds to receive push data
- A mechanism for screening push initiators

NOTE: Parameters may be bearer sensitive.

6 Security

The "Security Threats and Requirements" specified in 21.133 [1] shall not be compromised.

It shall be possible for the Push Service Operator to be assured of the identity of the Push Initiator.

It shall be possible for the Push Recipient to be assured of the identity of the Push Initiator.

Mechanisms shall be provided to ensure that the push data is sent to and accessed only by the intended addressed entity.

It shall be possible for the Push Service or the user to deny unauthorized push data.

An authorization may be based on the following:

- identity of the Push Initiator
- the destination user, device or user agent
- push related attributes such as priority and content type

It shall be possible for the user to control acceptance of push data sent to the user based on the trust level of the Push Initiator.

The Push Service shall provide data integrity and data confidentiality of the push data.

Push Initiators must have authorization (e.g. service level agreement) with the Push Service Operator (e.g. PLMN Operators) in order to use the Push Service.

7 Privacy

The Push Service shall ensure compliance with the Push Recipient's privacy requirements as described below. Specific local, national, and regional privacy regulations shall be complied with. An operator shall, at any time, be able to override a Push Recipient's privacy preferences if required to do so by legal authorities.

The privacy of the user is important and the introduction of the push services should in no way result in unwanted information "spam" being sent to mobile users.

8 Access rules

The Push Recipient shall be able to define access rules, in order to control how her privacy requirements shall be handled by the Push function.

It shall be possible for the Push Recipient to define the following access rules:

- The Push Recipient shall be able to allow push data from individual push initiators or groups of Push Initiators to transmit push data to the Push recipient
- It shall be possible for the Push Recipient to uniquely identify a Push initiator and the addressed User Agent prior to accepting or declining a request to receive push data from that Push Initiator.
- The Push Recipient shall be able to automatically decline push data from individual push initiators or groups of Push Initiators to transmit push data to the Push recipient
- At any time it shall be possible for the Push Recipient to stop receipt of push data from a Push Initiator. This may include any push data from this Push Initiator or only push data addressed to a particular User Agent of the Push Recipient.
- The Push Recipient shall be able to allow individual push initiators or groups of Push Initiators to transmit push data without user interaction at the Push Recipient's side.

It shall be possible for the Push Recipient to define these access rules based on:

- The identity of the Push Initiator
- The addressed User Agent

In addition it shall be possible for the Push Recipient to specify the validity of these access rules

- Only for the next request of the Push Initiator or
- For a pre-defined period e.g. next hour
- Unlimited, i.e. till modification or removal of the access rule.

NOTE: A set of default access rules may be defined by the operator.

9 Charging

This paragraph specifies charging requirements for the Push service.

NOTE: Value added services, that use the push service as a service capability, may have additional charging requirements. These are out of scope of this specification.

The Push service shall support various charging mechanisms (e.g. reverse, prepaid and reply charging etc.).

The following charging scenarios shall be supported:

1. Charging for the push service can be subscription based.
Different charging options shall be permissible whether the user is provisioned with the Push Service as a Push initiator or as a Push recipient.
2. Charging for the push service can be based on the push data, the resources used and time needed to carry out the push service.
3. Charging for the push service can be based on the size of the push data pushed to a receiver.
4. It shall be possible to charge the **Push recipient** only, the Push Initiator only, or both.
5. It shall also be possible to mix and match the various different charging scenarios outlined above.
6. One-off charging for subscription and cancellation of Push Service should be possible –FFS
7. It shall be possible to charge a Push initiator for an attempt to send push data to a push recipient, even if the push recipient rejects the push data

It shall be possible to include the following data in the CDRs as charging information if available:

- message types, length, storage time in the network, etc
- delivery time, upload / download method,
- Push service sender / -recipient
- the amount of the push data sent
- the amount of the push data received.
- roaming conditions (e.g. in a visited network)
- location conditions
- media.

10 Push Subscription Profile Information

For each Push recipient the Push Service shall keep a Push subscription profile. This Push subscription profile shall

contain the Push recipient's access rules as described in chapter 7.2.

Optionally (as an operator's option) the Push subscription profile may contain additional Push personalization settings of the Push recipient, e.g.

- Permissible minimal QoS per data format for receiving push data
- Permissible maximum size of data packages permitted to be pushed
- Permissible charging thresholds to receive push data
- ...

At any time the Push Service shall permit a Push recipient to modify her Push subscription profile information.

A Push initiator shall be able to interrogate any Push Recipient's Push subscription profile information. However only information relevant to this Push Initiator shall be revealed by the Push Service

NOTE: The Push subscription profile may be realized as part of the 3GPP Generic User Profile (TS 22.240) [3]

11 Roaming

Push services shall be available when roaming.

The push recipients shall be able to select and receive pushed local services, subject to the user profile settings.

12 Inter-working

This section describes the inter-working between 3GPP networks and other networks (e.g. the internet) and 3GPP services.

12.1 Inter-working with the Internet

12.2 Service Independence

12.2.1 Forwarding

12.2.2 Barring

It shall be possible to provide push service to a user regardless of barring status of other services.

It shall be possible for user to bar a push service regardless of barring status of other services.

13 Feature Interactions

14 Annex A: Change history

V. 0.1.0	February 2001	First Draft (Presented at TSG-SA-WG1 6 th – 9 th February 2001)
----------	---------------	---

V. 0.2.0	July 2001	Second Draft (from SA1 ad-hoc, 9 July 2001)
V. 0.3.0	November 2001	Third Draft (presented at SA1 5 th – 9 th November 2001)
V. 0.3.1	January 2002	Highlighting removed as basis for Phoenix SWG (13-18 January 2002)
V. 0.5.0	January 2002	Output of Phoenix Push SWG (15-16 January 2002).
v. 0.6.0	February 2002	Output from Saalfelden (11 th – 15 th February 2002)
v. 0.7.0	April 2002	Output from Sophia Antipolis (9 th April 2002)
v. 0.7.1	April 2002	Clean copy of output from Sophia Antipolis
v. 0.8.0	May 2002	Output of Victoria (15 th May 2002)
v. 0.8.1	May 2002	Clean copy of output from Victoria
v. 1.0.0	May 2002	Submission to SA for information
v. 1.1.0	July 2002	Output of Rome (8 – 12 July 2002)
v. 1.1.1	July 2002	Clean copy of output from Rome
v. 1.2.0	August 2002	Output of Durango (12 – 16 August 2002)
v. 1.2.1	August 2002	Clean copy of output from Durango

Change history										
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New