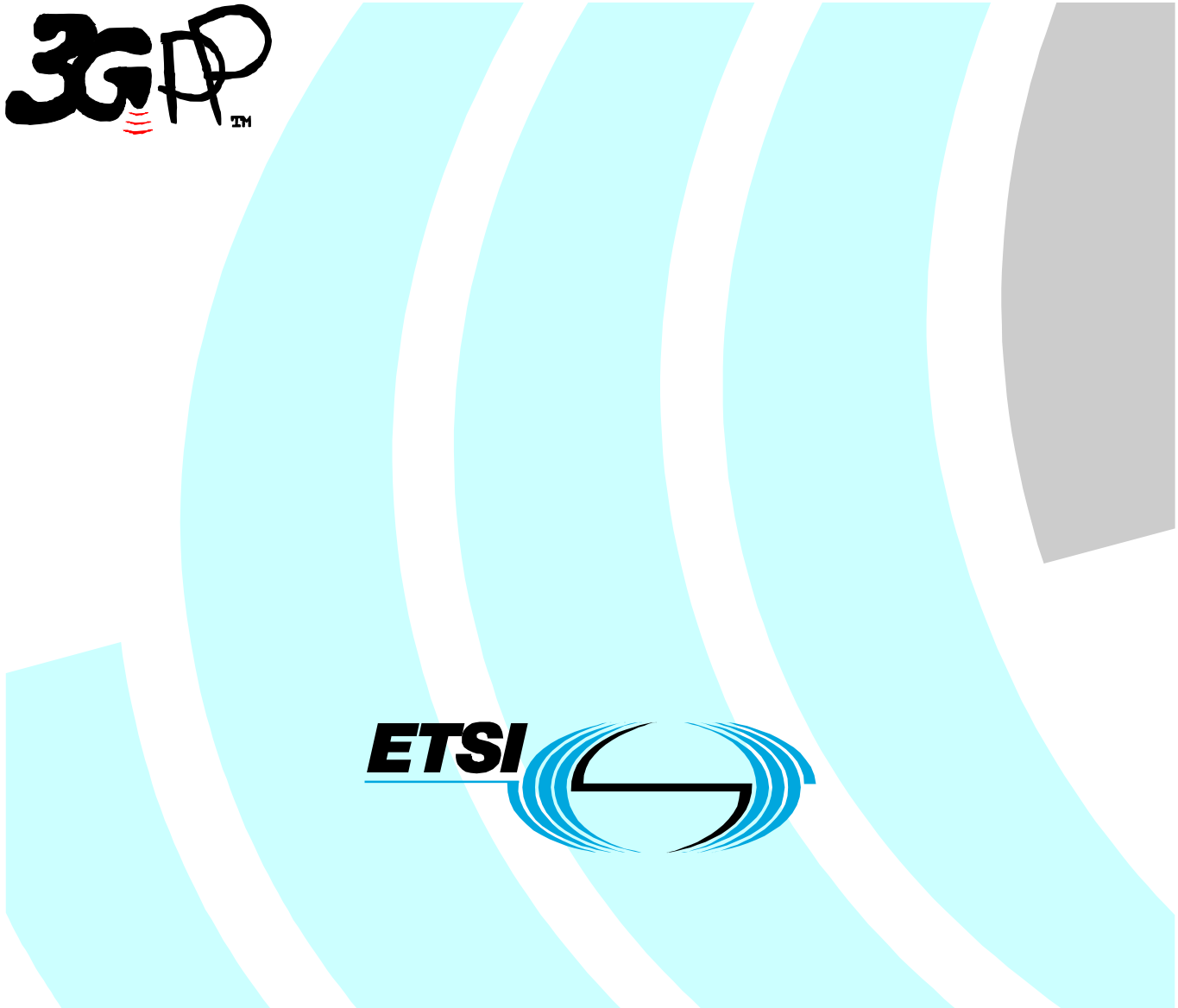
ETSI TR 122 949 V6.0.0 (2004-03)

Technical Report

Universal Mobile Telecommunications System (UMTS);
Study on a generalized privacy capability
(3GPP TR 22.949 version 6.0.0 Release 6)



Reference
DTR/TSGS-0122949v600

Keywords
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

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 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 .

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

Privacy in 3GPP is about the appropriate handling of privacy related information between the user and service provider and between users in accordance with the preferences of the user and regulatory policies.

Building and maintaining trust between users of 3GPP services and the network operator requires the careful consideration and deployment of capabilities that safeguard confidential information about the user. Privacy is therefore seen not only as a value added service but also as a risk-reduction mechanism in terms of service deployment.

From a 3GPP perspective, a generic way to handle privacy related information is desirable in order to provide as far as possible a common set of rules that can be used by any service that requires the protection of personal data or information about a user.

Privacy is protected by regulation usually in the form of directives enforced by regional or national authorities. Where specific legal requirements exist, these need to be considered by each application to assure compliance.

1 Scope

The present document aims to investigate and summarise the existing service requirements on privacy for 3GPP services. In order to ensure that these services and future 3GPP services will have a consistent set of rules that control the availability and usage of confidential information, it is the intention to identify a common way to handle privacy related information in the network.

Generic privacy requirements for the mobile industry are also being defined in [3] by the Open Mobile Alliance and it is the intention of this document to present the existing requirements and any alternatives to achieving the required functionality within 3GPP networks.

The scope of this study is to:

- Identify privacy related information that is used in the 3GPP system;
- Identify the existing 3GPP services that handle privacy related information;
- Identify the various stakeholders that handle, control or consume personal data, and to define their relationships;
- Document the definitions of the various functions, stakeholders and functions involved in a privacy capability;
- Identify the work being done by other organizations and the additional work to be done by 3GPP.

The types of data subject to privacy rules within the scope of this study include

- Privacy related information specific to an individual user;
- Privacy related information relating to entities such as corporations;
- Network data such as serving cell and broadcast area, e.g. data that relates to the user's location or presence in the network, and which could be used by applications to track the user.

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 41.101: "Technical Specifications and Technical Reports for a GERAN-based 3GPP system".

[2] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[3] Open Mobile Alliance: "OMA Draft Privacy Requirements", OMA-RD_Privacy-V1_0_0-20031104-A

[4] 3GPP TS 22.071 Location Services (LCS); Stage 1".

[5] 3GPP TS 22.141: "Presence service; Stage 1".

[6] 3GPP TS 22.127: "Service Requirement for the Open Services Access (OSA); Stage 1".

[7] 3GPP TS 22.240: "Service requirements for 3GPP Generic User Profile (GUP); Stage 1".

[8] 3GPP TS 22.174: "Push service; Stage 1".

[9] 3GPP TS 33.106: "Lawful interception requirements".

[10] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

[11] 3GPP TS 22.140: "Multimedia Messaging Service (MMS); Stage 1".

[12] 3GPP TS 22.088: "Call Barring (CB) supplementary services; Stage 1".

[13] 3GPP TS 22.228: "Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [2] and the following apply.

Personal Data: Any information relating to an identified or identifiable natural person ("data subject") (an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity).

NOTE: This definition is taken from Directive 95/46/EC [10]. Within the scope of the present document a 'data subject' is equivalent to a user. Only personal data collected and / or processed by a PLMN operator or service provider is within the scope of the present document.

Privacy: The appropriate handling of information that is deemed confidential between the user and service provider

Privacy Settings: Information relating to Personal Data of a user. Privacy Settings describe the rights and limitations of access to and processing of Personal Data.

Trust: Relationship between two entities that may be relied upon to ensure privacy

3.2 Abbreviations

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

BAOC	Barring of All Outgoing Calls
BOIC	Barring of Outgoing International Calls
BOIC-exHC	Barring of Outgoing International Calls except those directed to the Home PLMN Country
BIC	Baseline Implementation Capabilities
BIC-Roam	Barring of Incoming Calls when Roaming outside the home PLMN country
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CS	Circuit Switched
GUP	Generic User Profile
HLR	Home Location Register
IMS	IP Multimedia Subsystem
ISDN	Integrated Services Digital Network
LCS	Location Services
MSISDN	Mobile Station ISDN number
OMA	Open Mobile Alliance
OSA	Open Services Access
PLMN	Public Land Mobile Network
PPR	

SIP	Session Initiation Protocol
SMS	Short Message Service
UE	User Equipment
WLAN	Wireless Local Area Network

Additional definitions and abbreviations can be found in TR 21.905 [2].

4 Privacy models

4.1 Informative models

In the present document privacy is mainly considered as *privacy of user information*, i.e. privacy is considered as a requirement from an individual user. It should be noted, that privacy requirements may also arise from other parties involved in telecommunication. E.g. a PLMN operator could have the privacy requirement to hide its network topology from other operators, or a company (being a 3GPP subscriber for users, which are its employees) could have certain requirements for confidentiality of messaging among these employees, but privacy requirements from these parties are not covered the present document.

Already in its most general form one may observe that, from a user's perspective, there exist several flavors of privacy:

- **Protection of personal data**
  (I do not want my personal data being accessible to unauthorized parties)

- **Non-disclosure of identity**
  (e.g. I do not want to reveal my phone-number to my communication partner, or I want to remain anonymous towards a service provider)

- **Protection against tracking**
  (e.g. I do not want to be tracked, geographically or on my behavior)

- **Protection from unsolicited communication**
  (e.g. I want not to be bothered by spam-mail)

- **Access to undesirable information / kids-protection**
  (e.g. I want to block access of my kids to adult or gambling content)

From a Generalized Privacy capability point of view only *protection of personal data* and *non-disclosure of identity* seem to be within the scope of our work.

Privacy from unsolicited communication and *Access to undesirable information / Kids-protection* is considered as filtering of communication (incoming and outgoing) of the information being exchanged (e.g. originator, target, service, keyword search …). Filtering should be done on service level as separate service or enhancement to other services and is - generally - considered out of scope of our work. (exception: basic Call Barrings as in GSM, see below)

Tracking of a user is considered as collecting figures about that user and deduce information about the user. This can be a feature of a service (e.g. fleet management needs to track the location of a truck) or an unwanted misuse of data, for which the service provider can be made liable. In any case *Protection against tracking* seems to be out of scope of standardization.

4.2 Roles involved in Privacy

In the present document the following involved parties are considered:

- **The user:**
  In general it is assumed, that the user is provided with a 3GPP subscription.

Note 1: For the scope of this document it is considered irrelevant whether the user is also the subscriber or the subscriber is e.g. a company, which holds several 3GPP subscriptions for users, which are its employees.

Note 2: Within the context of some 3GPP services the notion of a "user" sometimes needs to be extended to service specific entities (e.g. "presentity" for the Presence Service)

- ***The home operator***:
  The PLMN operator, with whom the user has the subscription.

- ***A "visited" operator***:
  An operator of a PLMN, which is not the home operator. A visited operator may e.g. be the operator of a 3GPP network, in which the user currently is roaming.

- ***The service provider***:
  Privacy of user information may be specific to a particular service. A service is provided by a service provider which may be a 3GPP operator – home or visited – (e.g. location services) or a third party service provider.

Amongst these parties trust relationships exist:

- ***User – home operator***
  One of the most esteemed assets an operator has is the trust in protection of privacy, which is maintained by his customers. If a user communicates via the 3GPP system he considers this communication more "private" than communicating e.g. over the Internet.

- ***User – service provider***

  - *Service provider is the home operator, or the home operator acts on behalf of a (third party) service provider*:
    If a service or access to the service is offered by the home operator, then the same trust relationship exists as in the previous case.
    It should be noted that the term "offered by the home operator" only means that the user has the impression that the operator is responsible for that service. This impression could e.g. be implied by the fact that the user needs no separate contract with the service provider or that the service is advertised by the operator. In this case usually some kind of Service level agreement exists between operator and service provider.

  - *Service provider is a third party*:
    This is the case where the service provider is a third party (e.g. the user has a separate contract with the service provider, or a service is downloaded to the terminal from a website). A Service level agreement does not exist.
    While this case essentially is out of scope of 3GPP, some implications exist, if the third party service has some information exchange with the 3GPP system (e.g. the 3GPP identity of the user via CLIP/CLIR).

- ***Home operator - third party service provider***
  Depending on the trust relationship between the home operator and a third party service provider data about the user (e.g. location, presence, billing method, user preferences) may be exchanged between these parties.
  A Service level agreement exists between operator and service provider.

- ***Home operator - visited operator***
  Essentially, this trust relationship is manifested in the existence of a roaming agreement between the two parties. However, still this could require that enforcement of some user data privacy (e.g. for LCS in 3GPP Release 6) is performed in the home network and not on in the visited network.

4.3 Privacy related information

The present document is concerned with two types of privacy related information of a user:

- Personal Data

- Privacy Settings

4.3.1 Personal Data

Personal Data is any information, relating to an individual user, that is collected and / or processed by a PLMN operator or service provider. It is this information that is the subject of privacy protection, described in the present document.

Personal data is either:

- Related to a specific service or service capability - e.g. location information, presence information, accessibility to push services, service personalisation of third party provided services … ; or
- Non-service-specific information about the user - e.g. personal address, language, public identities (MSISDNs, SIP URLs) …

4.3.1.1 Access to and processing of Personal Data

The following kinds of access to and processing of Personal Data are within the scope of the present document:

- Read access to a user's Personal Data
- Modify a user's Personal Data

Out of scope of the present document are:

- Creation of a user's Personal Data
- Removal of a user's Personal Data

These actions are considered to be specific to individual service provisioning and are administrative tasks of the operator/service provider.

4.3.1.2 Types and granularity of Personal Data

Personal Data may consist of several types of information (e.g. location information, presence information) and may exist at several levels of granularity of information. E.g. a personal datum "personal address" (coarser granularity) may consist of "street", "number", "town", "zip-code", and "country" (finer granularity).

Note: The 3GPP Generic User Profile (GUP) 3GPP TS 22.240 [7] defines two levels of granularity of Personal Data: (a) GUP components (coarser granularity) and (b) GUP data elements (finer granularity).

4.3.2 Privacy Settings and access rules

Privacy Settings describe the rights and limitations of access to and processing of Personal Data. A user may have preferences for his privacy settings which should be taken into account by the operator / service provider.

Privacy settings may be expressed in terms of "access rules". Access rules can be used by any service that requires the protection of personal data or information about a user.

Access rules define who may access which personal data with what kind of processing rights.

- Who (accessor to Personal Data)
  Defines individual accessors or groups of accessors to Personal Data. The kind of identity used may be service specific. E.g. for the presence service these may be individual watchers or groups of watchers. For the push service this could be a list of service identities, that are allowed to push data to the user's terminal.
- Which Personal Data
  An access rule always refers to an identifiable personal datum. Again, the kind of personal datum (type, granularity level) may or may not be service specific.
- What kind of processing rights.
  An access rule may grant the right to access the Personal Data
  - not at all, or it may grant
  - the right to read, or
  - to modify the Personal Data.

The applicability of access rules may depend on additional parameters, e.g. time of day.

Note: There may exist additional – service specific – access rules (the presence service may e.g. display different presence information to different watchers), however these are out of scope of the present document.

5 Privacy Requirements

5.1 Existing Service Specific Requirements

5.1.1 LCS

Privacy requirements for LCS are contained in TS 22.071 [4]

- *Protection of personal data*
  It shall be possible for a Target UE Subscriber to subscribe to various types of privacy classes. The default treatment in the absence of the information to the contrary in the Target UE subscription profile shall be to assume that access is restricted to all LCS clients (unless using privacy overriding, or otherwise overridden by local regulatory requirements).

  The classes that can be included are as follows.

  - Universal Class: location services may be provided to all LCS Clients;
  - Call/session-related Class: location services may be provided to any or particular value added LCS clients that currently has a temporary association with the Target UE, i.e. call or session
  - Call/session-unrelated Class; location services may be provided to a particular, identified value added LCS Client or service
  - PLMN Operator Class – location services may be provided by particular types of LCS clients supported within the HPLMN or VPLMN.

  Privacy Attributes consist of:

  - Codeword: an additional level of security that may be set by a Target UE user to determine which Requestors are allowed to request location information;
  - Privacy Exception List: determines which LCS Clients, services and classes of LCS Clients may position a Target UE;
  - Service Type Privacy: determines whether the service type allows the LCS Clients to get the position of a Target UE;
  - Privacy Override Indicator: determines applicability of the Privacy Exception List.

  Means shall be provided for the UE subscriber to control privacy for value added services. (These means are not standardized).

  The privacy check shall be performed in the Home Environment of the target UE subscriber. This makes it possible for operators to ensure the privacy of their own subscribers i.e. the privacy settings that are used for privacy checks are always up to date and as specified by the Home Environment of the target UE subscriber.

  It shall be possible for privacy check to take into account Home Environment specific information such as time of day, subscriber location.

  It shall be possible for location services to support conditional positioning. Under these conditions, an application that is granted conditional positioning authorization must notify and obtain positioning authorization from the user of the target UE prior to performing the positioning process. Thus the user of the target UE shall be able to accept or reject the positioning attempt.

  Specific local, national, and regional privacy regulations must be complied with, and location information must always be available to the network service provider.

5.1.2 Presence

Privacy requirements for the Presence Service are contained in TS 22.141 [5].

Note that for Presence the "user" needs to be extended to the entities described there, namely a principal, a presentity or a watcher.

- Protection of personal data

  - Principal:
    A principal of a presentity shall, at any time, be able to control to whom, for how long and what (all or part of) presence information of the presentity is provided, and a principal of a watcher shall, at any time, be able to control to whom, for how long and what (all or part of) watcher information of the watcher is provided. The principal of the presentity can deny access to anonymous watchers.

  - Privacy override:
    Specific local, national, and regional privacy regulations shall be complied with. In particular, an operator shall, at any time, be able to override principal's privacy if required to do so.

  - Access rules:
    Access rules shall define:

    a) a watcher or groups of watchers allowed access to the presentity's presence information. For example: watchers x and y are allowed, or only watchers in group z are allowed, or all watchers and groups are allowed.

    b) the validity of the access authorization granted for a given watcher or groups of watchers. The access to the presentity's presence information can be restricted for a certain period (i.e. duration or number of requests), or during specific periods of the day.

    c) the attributes of the presentity's presence information that can be made available to a given watcher or groups of watchers.

    d) the ability to provide different presence information (i.e. both number of attributes and values of attributes) based on the watcher, and principal's preferences (e.g. its availability). For example: watcher x receives 'Online/Instant Messaging/im:a@there.com', while group y receives 'Offline/Instant Messaging/im:a@there.com'.

- Non-disclosure of identity

  - It shall be possible for watcher to request presence information anonymously (i.e. the watcher's identifier will not be revealed to the presentity).
    The access control mechanisms as listed above shall be able to cope with anonymous watchers.

Note: The mechanism to indicate the anonymity request of watchers (the initiator of a SIP dialogue can ask to remain anonymous to the receiver) is part of IMS-requirements when the watcher is an IMS subscriber.

5.1.3 OSA

Privacy requirements for OSA are contained in TS 22.127 [6].

- Non-disclosure of identity

  It shall be possible for the subscriber to hide his/her true identity from the OSA Applications and replace it with an alias. The alias shall be unique identification that has a one-to-one relationship with the true identity (e.g. MSISDN) of the subscriber and may be permanent or temporary (e.g. session based).

Note: In particular, subscriber anonymity is important in OSA charging functions

5.1.4 GUP

Privacy requirements for GUP are contained in TS 22.240 [7]

- Protection of personal data

It shall be possible for the user to define privacy requirements for components of the 3GPP Generic User Profile to determine access rights

Authorization of the requested action (create, read, modify or delete) on the user profile data depends on the following information:

- identification of the requesting application
- identification of the requesting subscriber (if delivered in the request)
- identification of the targeted user
- identification of the targeted user profile data

The targeted user profile data will be controlled as per the whole user profile and/or per different GUP components and/or per different GUP data elements.

5.1.5 Push Services

Privacy requirements for the Push Service are contained in TS 22.174 [8].

- Protection from unsolicited communication

  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, or
  - Unlimited, i.e. till modification or removal of the access rule.

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

5.1.6 Messaging

There is no explicit statement on privacy in TS 22.140 [11].

5.1.7 Call control and services in general

- Non-disclosure of identity

TS 22.081: "Line Identification Supplementary Services" (Supplementary Services for CS voice and data):

- CLIP/CLIR is the (implementation of) the requirement that a user at the originating side of a call wants to hide his identity (MSISDN) from the called party. This may be overridden by certain authorities (police, legal interception);

- COLP/COLR allows the user at the destination side to hide his identity.

In TS 22.228 equivalent requirements are expressed for IMS

- *Protection from unsolicited communication*
  TS 22.088 [12]: "Call Barring (CB) supplementary services"
  (BAOC, BOIC, BOIC-exHC, BIC, BIC-Roam) applicable to CS and SMS
  In TS 22.228 [13] equivalent requirements are expressed for IMS

5.2 General requirements

The following general (i.e. non-service-specific) requirements are identified:

- ***The user shall be allowed access to her Privacy Data in order for instance to review, or modify information***
  This requirement allows the user to monitor and control her Personal Data within the limitations set by the operator and / or service provider.

- ***The user shall be allowed to express preferences for her privacy settings on a per service basis.***
  This requirement allows the user to modify her privacy settings within the limitations set by the operator and / or service provider. User preferences shall include specific personal data items, who may or may not access those data items and the permitted kind of access.

- A generic privacy capability
  It shall be possible to use a common set of access rules that can be used by any service that requires the protection of personal data or information about a user.

- *Enforcement of privacy through the terminal*
  Terminals shall ensure that existing trust relationships and privacy controls, already established by network operators, are not bypassed.

- ***Enforcement of privacy through Home Network***
  This is the requirement that the means for enforcing privacy are located in the home network. Such a requirement exists e.g. in LCS Release 6.

- ***Requirement for control of access to the user's personal data by third parties or by third parties on behalf of the user***
  This is the requirement, that a third party (e.g. a service provider, a different subscriber) may access certain data about a user. This may be done

  - Upon request of the user (e.g. a user wants to employ an – eessentially untrusted – cityguide service, which needs to be authorized by the user to obtain the user's location from the network);

  - Without explicit request of the user (e.g. Push services).

- Roaming support

  Enforcement of user privacy shall be supported for services which are provided by the visited network for the roaming user.

  Like on the Internet, there is a fundamental legal problem related to how service providers deal with the laws of the various locations of its users. For roaming users, the privacy policies applied should relate to the regional/local directives of the users home PLMN. See also Annex A.

- call/session related authorisation

- The user shall be able to invoke defined access rules for a service in order to control how the user-specific/personal data is made available to those services

  Override (lawful intercept)
  Mandatory obligations, enforced by for instance national laws, for overriding privacy settings shall be complied with, e.g. lawful interception [9].

- Backward compatibility with existing standardized Privacy concepts

- Privacy settings are most effective if related to a user, not a piece of equipment. Therefore, it should be possible for the privacy settings of a user to be maintained when a user switches terminals.

- If some privacy settings for services offered by the Network Operator are resident within the terminal, then they should be consistent with equivalent privacy settings stored within the operator's network, e.g. the HLR flag, the privacy exception list, any settings in the PPR etc...

6 Work on privacy in other organizations

Privacy is important in 3GPP mobile communication networks, but privacy is of equal importance in many other telecommunication and service environments. There is work ongoing in the Liberty Alliance Project and in the Open Mobile Alliance (OMA), which is directly aimed at improving support for privacy, or which is very much related to privacy.

The OMA Privacy Requirements [3] mainly contains (a non-exhaustive list of) requirements that are mandated by legislation, and those that are not necessarily covered by legislation but are nevertheless considered industry best practices. Both the market/social expectations and legislative mandates are captured by use cases.

The present document tries to capture 3GPP requirements on privacy that are not contained in the OMA Privacy Requirements [3] and to minimize the overlap between the two documents.

NOTE: For ease of reading, some differences in terminology between the two documents should be noted, e.g. The OMA Privacy Requirements [3] calls the user a "data subject", while the operator / service provider is referred to as "controller" or "processor".

7 Security

Access to and use of privacy information shall be supported in a secure manner.
This is the requirement for third parties wishing to access the data to be authorized to do so.

8 Charging

Not applicable.

9 Regulatory framework

Relevant regulatory framework issues are covered in OMA Privacy Requirements, OMA-REQ-Privacy [3]. No additional requirements to those defined in the OMA Requirements Document have been identified.

10 Recommendations

It is seen as essential that 3GPP, Liberty and OMA are involved and coordinated in the development of privacy features and support for privacy in telecommunciation networks. The first step anyhow is to establish the service requirements that apply in different environments. Quite often the service requirements that are identified regarding privacy are related to corresponding regulatory requirements.

3GPP should seek to liase with Liberty and OMA and communicate service requirements on privacy that apply in 3GPP networks. As shown elsewhere in this document, there are many service requirements on privacy already documented in 3GPP's Specifications and many of these privacy requirements are quite relevant also for other organisations and similar services in other networks and environments.

The following steps of standardization are envisaged:

Step 1

3GPP to identify service requriements that apply in 3GPP networks.

OMA to identify service requirements that apply in OMA.

Liberty to identify service requirements that apply in Liberty.

Step 2

Specify and agree applicable functional requirements that are needed to fulfil the privacy service requirements in the corresponding standardization body together with OMA and Liberty. This work requires communication and coordination between the standardization bodies so that double work and potentially conflicting specifications can be avoided.

Step 3

Develop, specify and agree solutions on privacy (e.g. universal privacy classification and data formats) to resolve the service and functional requirements on privacy together with OMA and Liberty. Also this work requires communication and coordination between the standardization bodies so that double work and potentially conflicting specifications can be avoided.

Step 4

Specify and update service specific functions and architectural solutions (privacy related parts in service specific documents in 3GPP, OMA and Liberty) in accordance with the commonly agreed privacy requirements.

Annex A (informative): Roaming and Multi-jurisdiction support

The application of privacy by both the home and visited network, when a user is roaming in an area covered by a different jurisdiction to the users home requires careful consideration.

Typical use cases include, for instance a mobile user from the US who roams to Europe and buys goods using his mobile device. It should be assumed that the privacy policy applied should be that of the users home PLMN.

Editors note: Requirements on operators/service providers who serve users in multiple jurisdictions should be FFS.

Annex B (informative): Change history

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	WI
2003-03								Initial version		0.0.0	
2003-04								Updated based on inputs at SA1#20	0.0.0	0.1.0	
2003-05								Updated based on inputs at SA1#21 SWG	0.1.0	0.2.0	
2003-07								Updated based on inputs at SA1#21 (S1-030936, 937, 938 930, 931)	0.2.0	0.3.0	
2003-11								Raised to version 1.0.0 to present for information to SA #22	0.3.0	1.0.0	
2004-01								Raised to version 2.0.0 to present for Approval to SA #23	1.0.0	2.0.0	
SP-23	SP-040099	S1-040243	22.949			Rel-6		Approved at SA #23	2.0.0	6.0.0	

History

Document history		
V6.0.0	March 2004	Publication