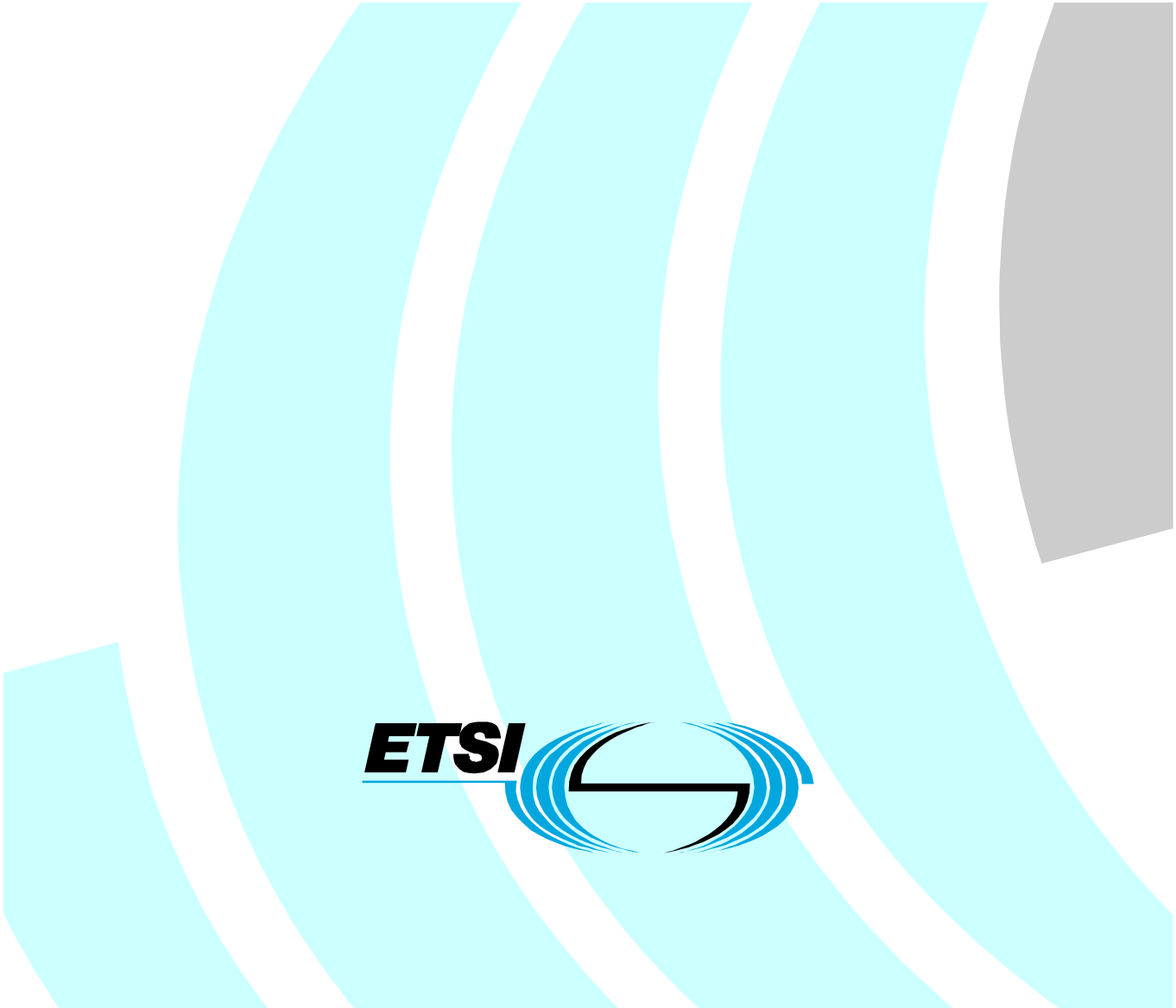
ETSI EG 202 325 V1.1.1 (2005-10)

ETSI Guide

Human Factors (HF);
User Profile Management



Reference
DEG/HF-00059

Keywords
profile, user

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

Contents

Intellectual Property Rights 7
Foreword 7
Introduction 7
1 Scope 8
2 References 8
3 Definitions and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 11
4 Concept and benefits 11
4.1 What is a profile? 11
4.1.1 General profile concept 11
4.1.2 Descriptive information 12
4.1.3 Generic settings and preferences 12
4.1.4 Service and device specific data 13
4.1.5 Interpretation of profile data 13
4.2 Profile types 14
4.2.1 Base profile 14
4.2.2 Device and service profiles 14
4.2.3 Situation dependent profiles 14
4.3 Templates 15
4.4 Profile tool 15
4.5 Active/inactive profiles 15
4.6 Profile agent 15
4.6.1 Agent components 15
4.6.2 Storage agent and components 16
4.6.3 Processing agent 17
4.6.4 Activation agent 18
4.6.5 Viewing/editing agent 18
4.7 Benefits 19
4.8 Need for standardization 19
5 Stakeholders and roles 19
5.1 User and administrator roles 19
5.1.1 User role 19
5.1.2 Administrator role 20
5.1.3 Usability issues related to roles 20
5.2 User 21
5.2.1 Managing activation of profiles 21
5.2.2 Range of categories 21
5.2.3 Independent adult 21
5.2.4 Supervision and ownership of responsibility 22
5.2.4.1 Parent - Child relationships 22
5.2.4.2 Teacher - Student relationships 22
5.2.4.3 Employer - Employee relationships 23
5.2.4.4 Caregiver - Care Recipient relationships 23
5.2.5 User with impaired or underdeveloped functions 23
5.2.6 First-time user 23
5.2.7 User in emergency situations 23
5.2.8 Law enforcement 24
5.3 Profile provider 24
5.3.1 Provides the profile and associated services 24
5.3.2 One or several profile providers 25
5.3.3 Profile portability 25
5.4 Service developers and manufacturers 25

6 Scenarios 27
6.1 A typical working day 27
6.2 Initial profile set-up for a child 29
6.3 Buying a new mobile phone 31
6.4 A person with a severe hearing loss 32
6.5 Public access terminal 33
6.6 Car crash 33
6.7 Hospital stay 34
6.7.1 Profile accessible with a personal device 34
6.7.2 Profile accessible with a hospital provided personal device 35
6.7.3 Lucy desires not to share any electronic access with the hospital 35

7 Profile contents 35
7.1 Profile data 35
7.2 Representing and defining profile data 36
7.3 General operations 37
7.4 Generic or specific preferences and settings 37
7.5 Capability and preference negotiation 37
7.6 Overview of a selection of profile objects 38
7.6.1 Rule 38
7.6.2 Date and time 38
7.6.3 Group 38
7.6.4 Service 39
7.6.5 Terminal 39
7.6.6 Accessory 39
7.6.7 Contact information 40
7.6.8 Presence information and activity 40
7.6.9 Language preferences and regional settings 40
7.6.10 Accessibility settings 41
7.6.11 Content preferences 41
7.6.12 Settings for management of other users' profiles 41
7.6.13 Mood 41
7.6.14 Network 41

8 Rules 42
8.1 The concept of a rule 42
8.2 Conditions and actions 42
8.3 References to objects 42
8.4 Rule building tool and rule base 43
8.4.1 Rule building tool 43
8.4.2 Rule definition language 43
8.4.3 Rule base 44
8.4.4 Active and inactive rules 44
8.4.5 Rule exceptions 44
8.4.6 Prevention of conflicting rules and rule bases 45

9 Default values and templates 45
9.1 Creation of profiles 45
9.2 Creation of templates 46
9.3 When defaults are not appropriate 47
9.4 Live and creation templates 47
9.5 Privacy 47
9.6 Inheritance 47
9.7 Templates for different types of users and situations 48
9.7.1 Adult 48
9.7.2 Companies 48
9.7.3 Clubs and affinity groups 48
9.7.4 Accessibility templates 49
9.7.5 Child template 49
9.7.5.1 Settings and preferences proposed in child templates 49

10 Set-up and maintenance of profiles 50
10.1 Who can create and update profiles? 50

10.2 Who initiates profile updates? 50
10.3 Scope of profile data values 50
10.4 Profile tool 51
10.4.1 Design for All approach 51
10.4.2 Various versions of profile tool 53
10.4.3 Available in various terminals 53
10.4.4 Online profile management 54
10.4.5 Offline profile management 54
10.4.6 Language and vocabulary 54
10.5 Creation 55
10.5.1 Starting values 55
10.5.2 Linking services and devices with existing settings and preferences 56
10.5.3 Base profile creation 56
10.5.4 Situation dependent profile creation 56
10.5.5 Device profile creation 56
10.5.6 Service profile creation 56
10.6 Update 57
10.7 Deletion 57
10.7.1 Profile data deletion 57
10.7.2 Base profile deletion 58
10.7.3 Situation dependent profile deletion 58
10.7.4 Device profile deletion 58
10.7.5 Service profile deletion 58
10.8 Information acquisition 59
10.8.1 Explicit methods 59
10.8.2 Implicit methods - adaptive personalization 60
10.8.3 Combination of implicit and explicit methods 61
10.9 Configuration methods 62
10.9.1 Pre-configuration 62
10.9.2 Guided configuration 62
10.9.3 Manual configuration 63
10.10 Data storage, synchronization and back-up 63
10.10.1 Storage 63
10.10.2 Synchronization 63
10.10.3 Revision handling and undo functionality 63

11 Profile activation 64
11.1 User states 64
11.2 Automatic identification of current user state 64
11.3 Transitions between user states 65
11.4 Presentation of profile state 65
11.5 Activation and deactivation of profiles 66
11.6 Different means of triggering the automatic activation of profiles 66
11.7 Activation rules 67
11.7.1 Default precedence order of activation/deactivation rules 67
11.7.2 Different types of activation rules 67

12 Address book management 68
12.1 The function of the address book 68
12.2 Content of the address book 68
12.2.1 Content address book records 68
12.2.1.1 Services available 69
12.2.1.2 Charging information 69
12.2.2 Postal address data 70
12.2.3 vCards and e-business cards 70
12.2.4 Additional content of address book records 70
12.2.5 Shared address books 70
12.2.6 Availability in various tools 71
12.2.7 Synchronization of distributed address books 72
12.3 Operations on address books 72
12.3.1 Add to address book 72
12.3.2 Modify 73

12.3.3 Group and arrange 74
12.3.4 Search 74
12.3.5 Send 75
12.3.6 Move, copy, remove records....75

13 Information sharing and privacy 75
13.1 Personal information privacy 75
13.1.1 General privacy issues 75
13.1.2 Templates....76
13.2 Access to profile data 76
13.3 Vendor and provider interactions 77
13.4 Privacy levels 77
13.5 Privacy policies 78
13.6 Access control and authentication 79
13.7 Trusted third parties....80
13.8 Privacy regulations 80
13.9 Access control methods....81

14 Log 82

Annex A (informative): Collective table of goals and guidelines....83

A.1 Concept and benefits 83

A.2 Stakeholders and roles....85

A.3 Profile contents....86

A.4 Rules....87

A.5 Default values and templates....88

A.6 Set-up and maintenance of profiles 89

A.7 Profile activation 93

A.8 Address book management 94

A.9 Information sharing and privacy 96

A.10 Log 98

History 100

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 ETSI Guide (EG) has been produced by ETSI Technical Committee Human Factors (HF).

Intended readers of the present document are:

- standards developers;
- profile providers;
- service providers;
- terminal manufacturers (including mobile phone, PC, and public access point manufacturers);
- software developers.

Introduction

The concept of a user profile usually refers to a set of preferences, information, rules and settings that are used by a device or service to deliver a customized version of capabilities to the user. In practice, most devices and services already contain profiles specific to that product and unrelated to any other. These profiles are frequently sub-divided into a number of profile components.

Commercial and technical constraints currently dictate having profile components associated with each device or service, and is likely to remain a common model for profiles. This model is reflected in proposed system architectures such as the 3GPP GUP (see references [4], [5] and [6]).

There will be a number of user characteristics and preferences that will apply independently of any particular product (e.g. a user's preferred language or their need for enlarged text). The guidance given in the present document reflects one key objective, that users should not be required to provide this information more times than is necessary.

Users move from one situation to another throughout the day (e.g. at home, driving, working). In each of these situations, users will have different needs for how they would like their ICT resources arranged. At present, an increasing number of products already provide the user with ways of tailoring their preferences to these different situations. The present document identifies and suggests ways which make it easy for users to specify their situation dependent needs in ways that require the minimum need to understand the wide range of products that contain unique situation dependent preferences and access methods.

In addition, common user profile management holds the promise of improving the uptake of new technologies and allowing greater access to the benefits of technologies. The present document focuses on presenting guidelines to service providers and manufacturers in shaping their product requirements in ways to maximize human and social benefit.

1 Scope

The present document provides guidelines relevant to users' needs to manage their profiles for personalisation of services and terminals. Effective user profile management will be critical to the uptake and success of new and advanced communication services and it is therefore important to focus on the users' requirements in this area.

Key areas that are addressed in the present document are:

- the user profile concept;
- the benefits of user profiles to different parties;
- scenarios in which user profiles bring benefits;
- administering profiles that reflect users' lifestyles and situations;
- administering automatic activation of user profiles;
- optimizing the presentation of user profile management guidelines to enable easier compliant product development.

Profile solutions considered to be within the scope of the present document:

- that are provided for the primary benefit of the user;
- where the user has rights to modify the majority of the profile contents;
- where the user has the right to accept or reject proposed changes to the profile.

"User Profiling" is **not** within the scope of the present document. "User Profiling" employs profiles:

- that are created and owned by other parties, invisible to the user, to enable the other parties to tailor the services they offer to a user;
- where the user is given little or no opportunity to check, modify or reject changes made to the profile;
- based on the background collection of information about users derived from their actions.

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI EG 202 249: "Universal Communications Identifier (UCI); Guidelines on the usability of UCI based systems".

[2] ETSI EG 202 301: "Universal Communications Identifier (UCI); Using UCI to enhance communications for disabled, young and elderly people".

[3] ETSI EG 202 067: "Universal Communications Identifier (UCI); System framework".

[4] ETSI TS 122 240: "Universal Mobile Telecommunications System (UMTS); Service requirements for 3GPP Generic User Profile (GUP); Stage 1 (3GPP TS 22.240 Release 6)".

[5] ETSI TS 123 240: "Universal Mobile Telecommunications System (UMTS); 3GPP Generic User Profile (GUP) requirements; Architecture (Stage 2) (3GPP TS 23.240 Release 6)".

[6] ETSI TS 129 240: "Universal Mobile Telecommunications System (UMTS); 3GPP Generic User Profile (GUP); Stage 3; Network (3GPP TS 29.240 Release 6)".

[7] OMA-UAProf-v2-0-20030520-C: "User Agent profile".

NOTE: See http://www.openmobilealliance.org/release_program/docs/UAProf/OMA-UAProf-V2_0-20030520-C.PDF

[8] OMA-ERELD-UAProf-v2-0-20030520-C: "Enabler Release Definition for User Agent Profile Version 2.0".

NOTE: See http://www.openmobilealliance.org/release_program/docs/UAProf/OMA-ERELD-UAProf-V2_0-20030520-C.PDF.

[9] W3C Recommendation (15 January 2004): "Composite Capability/Preference Profiles (CC/PP): Structure and Vocabularies 1.0".

NOTE: See http://www.w3c.org/Mobile/CCPP/.

[10] ISO 8601: "Data elements and interchange formats - Information interchange - Representation of dates and times".

[11] Wireless Village initiative: "Presence Attributes DTD and Examples V1.1".

NOTE: See http://www.openmobilealliance.org/tech/affiliates/wv/wv_pa_dtd_v1.1.pdf

[12] CWA 13987-1: "Smart Card Systems - Interoperable Citizen Services - User Related Information (based on DISTINCT) - Part 1: Definition of User Related Information".

[13] ISO 639-2: "Codes for the representation of names of languages - Part 2: Alpha-3 code".

[14] "Service Scenarios and Specifications", ePerSpace.

NOTE: See http://www.ist-eperspace.org/.

[15] ETSI EG 202 116: "Human Factors (HF); Guidelines for ICT products and services; "Design for All"".

[16] ETSI EG 202 423: "Human Factors (HF); Guidelines for the design and deployment of ICT products and services used by children".

[17] ETSI EG 202 132: "Human Factors (HF); User Interfaces; Guidelines for generic user interface elements for mobile terminals and services".

[18] ETSI TR 102 133: "Human Factors (HF); Access to ICT by young people: issues and guidelines".

[19] The Center for Universal Design (1997): "The Principles of Universal Design, Version 2.0. Raleigh, NC: North Carolina State University".

NOTE: See http://www.design.ncsu.edu:8120/cud/univ_design/principles/udprinciples.htm.

[20] W3C Recommendation (16 April 2002): " The Platform for Privacy Preferences 1.0 (P3P1.0) Specification".

NOTE: See http://www.w3c.org/TR/P3P/.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

accessibility: ensuring that all sectors of the community have equal access to communications and online information

active profile, active user profile: set of all active profile components related to a user

address book: entity that contains a number of records describing contacts of the user

administrator: person who defines profiles with settings and rules

NOTE: also known as profile administrator.

base profile: rules and settings that are always active in the profile

base profile component: subset of the profile which contains rules and settings that are always active

creation template: template where modifications made to the template will not affect any rules or settings in profiles that were previously created from that template

Design for All: design of products to be usable by all people, to the greatest extent possible, without the need for specialized adaptation

feedback: information presented to users that relates to an action that the user has requested

inactive profile: profile that does not currently apply but that may apply to a user when the circumstances change

live template: template where modifications made to the template will affect all rules or settings in profiles that were previously created from that template

log: entity that contains a number of records that describe instances of an activity

object: profile data with attributes, values and operations that the user can refer to when defining their profiles

profile: total set of user related information, preferences, rules and settings which affects the way in which a user experiences terminals, devices and services

NOTE: The use of the word profile in the present document implies user profile unless otherwise stated.

profile component: part of a profile

NOTE: Also known as component.

profile tool: tool that enables a user to view and modify information in profiles

profile provider: entity (e.g. company such as a service provider, organisation such as a special interest or affinity organization) that provide profiles and associated services

Personal User Agent (PUA): functional entity (probably implemented as a software object) with a one-to-one relationship to a specific UCI

NOTE: It stores or has access to information on all of a person's communication services and their service identifiers (e.g. telephone numbers, email addresses, etc.).

rule: statement that can be interpreted by the profile agent to produce or limit an action

scope: the limit on the range of information and activities with which a profile agent is associated

state information: information about the current state of some aspect of the user and their devices and services

template: set of rules and settings provided by an entity as a starting point for the user for the creation of their profiles

usability: extent to which a product can be used by specific users to achieve specific goals with effectiveness, efficiency and satisfaction in a specified context of use

user: person using ICT services

user profile: see profile

3.2 Abbreviations

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

GPS	Global Positioning System
GSM	Global System for Mobile communication
GUP	3GPP Generic User Profile
ICT	Information and Communications Technologies
IP	Internet Protocol
PIN	Personal Identification Number
PUA	Personal User Agent
RNIB	Royal National Institute of the Blind
SIM	Service Identity Module
SMS	Short Message Service
UCI	Universal Communications Identifier
URL	Uniform Resource Locator

4 Concept and benefits

4.1 What is a profile?

4.1.1 General profile concept

When users wish to have the behaviour of devices or services personalized to their requirements a profile will be required. A profile may apply to a single simple device or service, more complex devices or services, or any combination that the user may wish to use. The entire set of saved information, preferences, rules and settings a user may want to apply is their "user profile". In addition, a user may choose to have multiple profiles.

Profiles reflect a user's unique lifestyles and situations. Profiles may be related to the various situations that a user experiences in their lives. If users view these situations in a hierarchical way, it should be possible for users to have a hierarchy of profiles that reflect the relationship between these hierarchical situations. For example, a user may have a number of profiles related to different work situations such as "Work meeting" and "In my office" with a general "At work" profile at the top of this hierarchy of work related profiles and that would apply if none of the other more specific situations applied. Where profiles are organized in a hierarchical way the lower level profiles can inherit profile data from the higher-level ones. Templates (see clause 9) may also be organized in a hierarchical way. Users may find hierarchical organization of profiles and templates as useful as the beneficial concept of organizing documents on a computer in a hierarchy of folders.

Any profile will contain details of the user and their personal requirements in a form that can be used by the system to deliver the required behaviours. Information in a profile may also be included for sharing with another person, device or service.

The profile is merely a conceptual entity. Users could use a profile viewing tool to see and edit all aspects of any profile whether or not that profile is active. Alternatively, they could see and edit a component of any profile by only looking at device specific elements of the profile from a device's user interface. As it is only a conceptual entity for the user, the descriptions used in the present document should not be read as implying a particular way of storing and accessing profile data.

In particular, device profile data may be stored and initially processed within the device and service profile data may be stored and initially processed within the service environment. However, the user profile concept described in the present document should ensure that there are links between all of the places where the user's profile data is handled to ensure that users can have the concept of centralised profiles which cover all of their devices and services.

User convenience and access to their resources

Goal 4.1.1.a: The use of profiles should not limit the access a user might otherwise have to their services and devices.

Goal 4.1.1.b: However the user's profile data is distributed amongst devices and services, it should be possible to ensure that users can have the concept of centralised profiles which cover all of their devices and services.

Guideline 4.1.1.c: Users should be provided with a mechanism that allows them to organize profiles and templates in a hierarchical way.

The following clauses describe the different categories of user information and preferences.

4.1.2 Descriptive information

The first category of user information is descriptive information about the user. This information is likely to include such things as the user's name and address, and may, if the user wishes, include information such as birthday and nickname information. Some of this information may not be applicable for processing by profile rules and is most likely to be intended for identification and transmission to other people or services, according to the user's privacy requirements.

4.1.3 Generic settings and preferences

The user may wish to express a wide range of preferences which may be applicable when using a number of different devices and services. These may include:

- generic service preferences (e.g. people with hearing difficulties may express a preference for receiving information and communications in a text format);
- time-dependent preferences (e.g. not accepting voice communications between 23:00 and 07:00);
- location and situation based preferences (e.g. requirements related to communications when driving a car);
- depending on the context of use, combinations of service, location and time preferences (e.g. wanting text information translated to voice when driving a car);
- affinity based preferences, such as a templates (see clause 9) provided by an organization such as the RNIB, Royal National Institute of the Blind, which gives a wide range of default preferences that have been shown to be suitable for people with visual disabilities.

The user may also wish to have preferences related to the sensory aspects of user interfaces of information and communications. This information could include preferences such as:

- audio information should be presented at a "very loud" volume;
- text information should be presented with "large text".

For terms like "very loud" or "large text" to be useful, the user would wish them to always result in the same standardized (see clause 4.8, "Need for standardization") user experiences. For this to be achieved, these terms would need to map to technical descriptions that have universal applicability across a wide range of usage scenarios and device connections. The technical descriptions would need to take into account the many varieties of terminals and usage environments. So "very loud" might be expressed as a sound level value at a certain listening distance and "large text" might need to be expressed in a distance independent measure such as angle of arc subtended at the eye. This can be approximated very well where applications and devices are used in pre-defined combinations. Where multiple applications and devices from different sources are working together, and where no precise interface standards between these are agreed, the user experience will not necessarily be precisely as the user expected (e.g. if headphones of different sensitivities are connected to the same audio output the perceived volume will be different).

4.1.4 Service and device specific data

In order for a device or service to be personalized in ways that suit individual users, it is necessary to set a number of parameters that relate to device/service features in ways that ensure that the device or service will deliver the capabilities that the user desires. Dependent on the complexity of the device or service there may only be a few user settable parameters or there may be a very large number. Examples of some of the very wide range of device/service parameters that may need to be set include:

- the loudness of a telephone ring tone;
- which of a number of telephone ring tones is used to indicate a call from a particular category of users;
- the frequency with which new email message delivery is checked;
- the communication method used for mobile data services.

NOTE: EG 202 132 [17] contains details on specific user interface criteria for mobile telecommunication devices and services. See also OMA-UAProf ([7] and [8]) and W3C CC/PP [9].

In the majority of cases, the range of parameters that can be set by users and the values that may be set will not be consistent between different devices or services. Where such diversity exists it makes it impossible to transfer the settings that have been set for one device or service to another similar device or service in a way that ensures that the same outcome will be achieved. This problem would be overcome if:

- different devices or services of the same type had consistent sets of parameters which had value ranges that produced identical effects;
- settings in one proprietary form on one device or service can be converted to settings in another proprietary form on a similar device or service from a different supplier (either directly or via intermediate conversion to a standardized form).

In most cases, devices use qualitative rather than quantitative designations, such as "very loud" or "large text". These qualitative designations could be followed and the resulting settings would fall into an approximate range desired by the user.

Sharing of profile data between user resources

Guideline 4.1.4.a: If specific data in part of a profile relating to a device or service has been specified by the user, then it should be possible for the equivalent fields for other devices or services of the user to be populated with the same data.

4.1.5 Interpretation of profile data

In order to avoid the user having to understand the internal attributes and detailed behaviours of every device or service with which they may need to interact, it is necessary for a user's individual information and preferences to either be directly usable by a device or service or for it to be translated into a form that a device or service can understand.

Many of the device/service specific settings relate to similar factors as some of those specified in the device/service independent user information and preferences (e.g. a mobile telephone may have user selectable character sizes that relate very closely to a user preference setting such as "very large text"). Users will benefit greatly where mechanisms exist to set many device/service specific parameter settings to values that are based upon the data stored in the user information and preferences. The realisation of this objective will depend on standardization (see clause 4.8, "Need for standardization") of profile parameters and the ways in which these parameters are expressed.

It is important that, if data in part of a profile relating to a device or service has been specified by the user, then related profile fields for other devices or services can be directly populated by the same data or data translated to produce the same effects. Similarly, reuse of parameter settings between different devices and services of a similar class can only be achieved if there is standardization of profile parameters and the ways in which these parameters are expressed.

Interpretation of profile data

Guideline 4.1.5.a: In order to avoid the user having to understand the internal attributes and detailed behaviours of every device or service with which they may need to interact, it is necessary for a user's individual information and preferences to either be directly usable by a device or service or for it to be translated into a form that a device or service can interpret.

Guideline 4.1.5.b: If data in part of a profile relating to a device or service has been specified by the user, then related profile fields for other devices or services can be directly populated by the same data or data translated to produce the same effects.

4.2 Profile types

4.2.1 Base profile

A base profile contains rules and settings that are always active such as users' name and birth date. It will typically contain descriptive information (see clause 4.1.2) and some categories of generic settings and preferences (see clause 4.1.3).

4.2.2 Device and service profiles

Profile data that only relates to a specific device or service (see clause 4.1.4) is contained in a device or service profile. Frequently, the profile data may be closely associated with the device or service (i.e. it may be stored within the device or service). Also one device or service profile may, in fact, contain a group of related profiles for sub-elements of that device or service. For example, the profile for a mobile phone may contain profiles for the mobile phone calendar, the mobile phone email application, etc.

New devices will be delivered with predefined settings in a pre-set device profile. The device profile may be instantiated with data from users' settings related to a similar device and also with data from their base profile (such as high audio volume, large text or contact book entries, see clause 10.5, "Creation").

Similarly, a new service will have predefined settings in an initial, pre-set service profile. This service profile may be instantiated with data from the user's settings related to a similar service and also with data from their base profile.

There may be devices or services that are shared between a number of users. For example, both the fixed telephones and the fixed telephony service in a family home will be shared between all members of that family. Each person who makes use of these shared devices or services may incorporate the shared device/service profiles as part of their own user profile. A profile for a shared device or service, associated with more than one person's profiles would raise issues such as conflicting preferences when used simultaneously by several people.

For intelligent homes or offices, the home or office could be considered to be a shared device that may be used in the profiles of the family members or the employees.

4.2.3 Situation dependent profiles

A user will require different behaviours for their devices and services and for the way in which these interact according to the user's different circumstances. For instance, when in a meeting, users will usually want their mobile phone to be in silent mode. They may also prefer calls to their fixed office telephone to be directed to their mobile phone as they will be unable to answer their office phone. In order to achieve this, the user should have access to or be able to define situation dependent profiles.

Each situation dependent profile will identify which devices and settings are needed in the situation and what device and service specific settings will be required. How this is achieved can vary depending on the technologies being used, but typically many devices and services may contain predefined, situation-specific sets of settings and rules and these just need to be activated each time the situation occurs. Situation dependent profile may contain information, settings and preferences from all of the categories described in clauses 4.1.2 to 4.1.4.

4.3 Templates

Profiles can contain a very large number of settings and preferences which would be difficult to set up unaided. When a user first obtains profiles, the creation task can be greatly simplified if the profiles are created from templates. The template provides a set of rules and settings that act as a starting point for the user in creating their profiles. Templates can be provided for the user from a number of different sources. Further more detailed information on templates can be found in clause 9.

4.4 Profile tool

Users will require a tool to view and amend the contents of any of their profiles. Each device or service should provide a user interface that allows the user to view and modify (at least) the profile data associated with that device or service. In order for users to benefit from their accumulated experience in viewing and modifying profiles it will be beneficial if all of the user interfaces adopt a consistent set of information presentation and interaction models. When profiles are presented to users for viewing or editing, the presentation of the information should only reflect the ways in which the information is distributed where it is helpful for the user to know this (e.g. it may be helpful for the user to know that the device volume setting applies to the specific device and not to all their devices).

Many users would benefit from having a tool that allows them to have an integrated view of the profile data associated with the full range of appropriate devices and services. The present document discusses characteristics of such a profile tool. The existence of a profile tool would avoid users having to access many different profile tools, devices and services in order to obtain an overview of what settings have been specified and what behaviours may be expected. A "Design for All" approach is encouraged (see [15], clause 4.3, "Design For All") so as to make the profile tool accessible to as many people as possible, including elderly people and persons with disabilities, without the need for adaptation or specialized design.

4.5 Active/inactive profiles

A profile can either be currently unused (an "inactive profile") or it can be in current use (an "active profile"). The present document assumes that a separate profile may be used for each common user situation (e.g. "At home", "In the car"). When the situation changes the required behaviour is that a new situation-dependent profile is activated and the previous one is de-activated. This model is very easy to describe and is used in the remainder of the present document. Technical solutions may use profiles that have different sub-sections that are utilised in different situations.

In order for users to experience the ICT environments that they desire, it is essential that the situation dependent subsets of profile data in the various devices and services are all activated when the specified situation occurs. Notification that a situation applies can occur in two ways:

- the user specifies that the situation is occurring (e.g. by pressing an appropriate key or making an appropriate menu selection);
- a device or service detects that the situation is occurring (e.g. because a phone has been put in a car handsfree unit or because a user's location is detected inside the user's home).

In either case, where one device or service has information that a specific situation is now occurring, this information needs to be made available to every device or service that may be involved with the particular profile. To achieve this, some form of information subscription or information dissemination mechanism should be available.

More details of profile activation are given in clause 11.

4.6 Profile agent

4.6.1 Agent components

In order for a profile to be effective the profile providers need entities that:

- store the profile data;
- process the profile data and initiate achievement of the behaviours encoded in the profile rules;

- activate and de-activate the profile in the appropriate circumstances.

When all of these functions are performed by a single entity, that entity can be referred to as a "profile agent". When these functions are performed by different entities these profile agent entities are referred to as:

- a profile storage agent;
- a profile processing agent;
- a profile activation agent.

These terms can also be used to refer to the separate functions within an integrated profile agent. All of the entities described in this clause are conceptual entities. In profile management implementations these entities may not be separate processes but could be groups of functions within a single larger process.

In many cases, each device or entity that is involved with a particular person's communications may have its own profile agent and, because of the scope of the device, the profile agent may have limited scope relative to those in other active entities. Profile agents will need an inquiry mechanism that allows active agents to be aware of any other profile activity that may affect or override their normal behaviour. In the case of conflicts between the various profile agents, there should be methods for resolving the conflict, and these methods may potentially involve active user decisions. Profile agents need to have access to location and presence information when it is available.

Access to location and presence information

Guideline 4.6.1.a: Profile agents need to have access to location and presence information when it is available.

Multiple profile agents

Guideline 4.6.1.b: Profile agents should have methods that allow them to be aware of each others' activities.

Guideline 4.6.1.c: There should be mechanisms to resolve conflicts when the activity of one profile agent potentially affects or overrides another's behaviour.

Guideline 4.6.1.d: Conflict resolution mechanisms may involve user decisions.

4.6.2 Storage agent and components

The profile storage agent is the entity that stores information about the profile data and the locations of data repositories of profile data related to users, which might be compared to 3GPP GUP server [5]. Note that there may very well be multiple profile storage locations. These locations will probably not store the total profile but only components that apply to a device or service, and the various locations may have different persistence and priority levels. Users require the data to be stored in a secure manner with user agreed levels of privacy applied to the availability and distribution of that data (see clause 13, "Information sharing and privacy"). Ideally, profile data should always be available, over all networks, from all supported devices and services, including fixed and mobile services allowing service continuity and the optimal user experience. Changes of data at different locations should be consistent, which may be ensured by synchronization of data and transaction security (see clause 10.10, "Data Storage, synchronization and back-up"). There is a risk that data stored and handled by different providers may become inconsistent.

Practical and operational reasons are likely to dictate that profile data will be stored in close association with the device or service to which it relates (e.g. profile data relating to a specific mobile phone will be likely to be stored in that phone or on a SIM-card in that phone). Information that may be useful for several devices or services should be centrally available. However, in order to ensure that profile data is available for restoration in case of loss, copies of profile data for devices, subject to data loss or erasure, may be stored in a more secure location or backed up to a user selected file storage. Profile information relating to one or more users may be stored on the same device or service if that device or service is available to multiple users.

Devices and services may have groups of settings and rules that are, within the domain of that device or service, called "profiles", but within the scope of the present document these "profiles" would be called "profile components".

Storing, maintaining and restoring profile data

Goal 4.6.2.a: Users should be able to assume that storage of data is working correctly and no user activity is required.

Goal 4.6.2.b: Users do not need to be aware about where the profile data is stored and how it is synchronized.

Goal 4.6.2.c: Profile data should be stored securely.

Goal 4.6.2.d: A synchronization mechanism should be used to ensure that when changes are made to profile data, the data held at different locations is always consistent.

Guideline 4.6.2.e: Profile data should be easily restorable if the data is deleted or corrupted.

Guideline 4.6.2.f: The profile provider should offer the user different options related to storage, such as backup and synchronization frequency. The user may also be allowed to further customize these options.

Guideline 4.6.2.g: Any solution which makes use of profile data should contain a fallback mechanism if the desired profile data is unavailable. This could take the form of a last used profile, default template contents, or an attempt to re-create the required profile elements through querying other resources in the user's personal area network.

Guideline 4.6.2.h: There should be a mechanism warning users when inconsistent data has been discovered by the profile agents or tools.

Guideline 4.6.2.i: An appropriate action for resolving inconsistent data should be proposed to the user.

4.6.3 Processing agent

In order that the rules (see clause 8, "Rules") in a profile can be translated into the behaviours the user desires, it is necessary for the profile processing agent to operate upon the rules. The profile processing agent is responsible for ensuring that all the operations required by the profile rules are carried out. The profile processing agent will need to initiate operations on a variety of devices and services referred to in the profile. For efficiency and effectiveness it is likely that the processing agent will have functionality distributed between multiple devices and services.

Users will not only be able to use their own devices but they could also use devices shared with other users. In those cases the device settings should be automatically set for the user who is currently logged into the device or service.

Availability and reliability of the communications channel will affect the quality of the user experience, especially the ability of the profile agent to act quickly and give feedback to users.

The profile processing agent will also have security and privacy requirements (more information on privacy can be found in clause 13).

Persistence and availability of profile data

Guideline 4.6.3.a: The profile processing agent should be able to access relevant profile data at all times when a profile is active.

Guideline 4.6.3.b: The profile processing agent should be able to access the devices and services referred to in the profile rules in order to ensure that the actions in the device or service are carried out.

Guideline 4.6.3.c: If the device or service has features that access external resources but those resources are unavailable, the user should be provided with alternative solutions.

Guideline 4.6.3.d: When communicating with devices and services, the profile processing agent should have the necessary permissions to successfully request and achieve the desired behaviours from the device or service.

Visibility of external interactions

Guideline 4.6.3.e: If any part of the profile or a profile agent needs to make any interactions outside the user's personally controlled service environment, the user should be given the opportunity to be made aware of these external interactions. Typical interactions would be external requests for information or responses to any external events or changes.

Guideline 4.6.3.f: The user should be given the opportunity to make a decision about accepting or rejecting these requests by external entities.

4.6.4 Activation agent

When a profile is inactive, the profile activation agent will be responsible for activating it when needed. This activation may be rule driven, as a result of a user request or as a result of an event such as when the device is turned on. The profile activation agent will also be responsible for the de-activation of profiles. A scenario illustrating automatic activation is explained in clause 6.1, "A typical working day". More details of profile activation are given in clause 11,"Profile activation".

Activation agent

Guideline 4.6.4.a: A user should be able to have multiple profiles available if they choose to maintain separate sets of preferences that can be selected in a single step.

Guideline 4.6.4.b: The user should be able to manually order the activation agent to activate a different profile across all affected devices and services, without having to use multiple devices or applications.

Guideline 4.6.4.c: A profile activation agent should be able to access the profile processing agent at all times when it is required to activate or de-activate the profile.

Guideline 4.6.4.d: A profile activation agent should be able to receive requests from a profile processing agent to activate or de-activate either the profile belonging to the profile processing agent or another appropriate profile.

4.6.5 Viewing/editing agent

A user should be provided with mechanisms to view or edit all or part of their profile. In order that users are able to get a clear view of their complete profile many users would find a single mechanism that allowed them to view or edit the complete profile very valuable. There may be components of the profile that are not accessible to the user, for a variety of reasons. The provision of such a tool (see clause 10.4, "Profile tool") should be considered where the results of using it can be relied upon by the user. To achieve this, profile information will need to be transmitted through different networks and be used on different devices and services in a way that is transparent to the user.

Viewing/editing agent

Goal 4.6.5.a: Users should be provided with mechanisms that allow them access to all components of their profile.

Goal 4.6.5.b: The profile implementations should allow as much user access as possible, within legal and business constraints.

Goal 4.6.5.c: Users should have mechanisms that allow them to edit profile data and have the changes automatically propagated to all components where that data is used.

Guideline 4.6.5.d: A user should be provided with mechanisms to view or edit all or part of their profiles.

4.7 Benefits

Helps users to personalize services and devices: The ability to customize a device or service allows users to maximize their benefit from the services while minimizing the hard work frequently required to understand them.

Wider demand for ICT services: The decrease in cost and increase in variety of services has led to much wider demand for ICT devices, but also a bewildering variety of implementations. With the increase in services and devices comes increasing usage in more areas of human activity. Users are employing ICT services in many more areas with many more devices, and relying on them more. Profiles are required to allow the users to more easily tailor their services to their needs, not tailor their behaviour to their devices and services.

Emerging social requirements for management of personal information: With the wider deployment and wider variety of ICT services, with the necessary distribution of certain user information, the potential for both beneficial personalized user services and detrimental access to personal information exists. Because of the broad use of ICT services, there is greater interest in their appropriate use by the various social and governmental organizations in the protection of individual privacy and liberties. User profiles can be used to help the user express their requirements about the privacy of their information.

Avoids users repeatedly specifying their preferences: Common solutions to the problem of customizing services allow users to acquire and use new technologies and products as they are created, reducing the need to completely re-learn methods of access and employment of the new products.

Convenience: Most of the users are not, or do not desire to be, technically astute when it comes to the underlying technologies of their devices and services. Manufacturers and service providers endeavour to satisfy as wide a market as possible with their offerings. If users have a common set of expectations as to how their devices and services may be set up, at least for basic services, they will be more likely to take advantage of new offerings.

Help users to access content in an appropriate form: The convergence of many formerly discrete devices – the ability of cars to communicate, the use of mobile phones to buy from vending machines, the interaction of personal devices via personal area networks, the rise of multimedia messaging, presents users with a wide variety of options for accessing content.

4.8 Need for standardization

User descriptions of settings and preferences (see also clauses 4.1.4 and 4.1.5) can differ significantly between different profile agents and even between different contexts of use within the same profile agent. However, the formal internal object descriptions will need to conform to standardized naming conventions, to enable profiles to be migrated between profile agents (see clauses 5.3.3 "Profile portability" and 8.4.2 "Rule definition language").

If data in profile components relating to a device or service have been specified by the user, then related profile fields for other devices or services can be directly populated by the same standardized data or data translated to produce the same effects. Whereas it will be essential to have standardized descriptions of these objects in order that profiles can be migrated from one provider to another, this does not imply that users will need to understand these descriptions.

The present document will therefore be considered as input for further standardization work.

5 Stakeholders and roles

5.1 User and administrator roles

5.1.1 User role

A person is in a user role when they are using their existing profiles, including activation or deactivation of their profiles. It is likely that some people, for instance very young children, would only be allowed the user role.

5.1.2 Administrator role

A person needs to be in an administrator role to define new profiles or to modify existing profiles. Administrators' rights to access and modify profile data is described in detail in clause 13.2. The most straightforward case is that the same person is in a user role most of the time and may be in an administrator role when there is a need to create a new profile or update existing ones. The administrator can also be someone else, for example when a company administers profiles for employees or when parents administer profiles for their children (see clause 5.2.4, "Supervision and ownership of responsibility"). In that case, the employees or the children might be granted some rights to administer some aspects of their profiles. A mechanism would then allow levels of administrator roles such as super-administrator role and self-administrator role.

Alternatively users may call upon a third party service to administer their profiles either all of the time, or when the administration task is awkward to perform at the current time. This is useful when a person is using a terminal with limited capabilities or simply is not interested in, or sure about, how to perform modifications. People with disabilities and older people might also find a third party useful for managing their profiles.

A profile administrator in a company would be expected to perform a very wide range of tasks, many of which might be quite complex. It could be expected that people in such a role would have experience of technical systems and be trained in profile administration. In contrast many profile users cannot be expected to have any specific technical knowledge and experience and may only be required to perform quite simple tasks. Given this wide range of variability, it is likely that the tools provided to these profile administrators could be significantly different.

NOTE: A person addressed in the present document, whether in a user role or in an administrator role, is most often called "user" in the present document.

5.1.3 Usability issues related to roles

The task complexity of managing a profile will vary greatly between corporate profile administrators managing many people's profiles and individual profile users managing their own profiles. The level of knowledge and experience will also vary greatly between these groups. For this reason the user interfaces presented to different roles will need to be designed separately to take account of these differences. Examples of factors that will need to be considered are:

- Optionally, and depending on factors such as legislation, it may be necessary to request authentication when changing from the user role to administrator role and thus getting administrator privileges for configuration of profiles. This would improve the user's feelings of trust and security. At the end of the configuration, the administrator should be reminded to change role again, from administrator role to user role. That would minimize the risk of unwanted configurations.

- Privacy levels will need to be defined for various operations and for access to certain information in the profile. Making these privacy levels easy for users to understand and/or control will need careful planning according to the type of user e.g. the solution chosen for a novice user will be very different to that for a corporate profile administrator. Privacy related issues are described in more detail in clause 13.

- The task complexity of managing profiles will vary greatly between a corporate profile administrator and a novice profile user. The structure of the user interface dialogues and the complexity of the user interface screens are likely to vary significantly between these extremes.

- Users should receive a clear notification when they move from the user role to the administrator role. This notification should warn the user that changes made in the administrator role may be irreversible. Users should have the ability to turn off this warning mechanism.

- Users should receive a clear notification when they move from the administrator role to the user role. Users should have the ability to turn off this notification mechanism.

Users may sometimes make use of a corporate administrator or other 3rd party to perform some of their administration tasks. Factors that will need to be taken into account in these circumstances are:

- the ways in which profile setup and modifications are fed back to the user;

- what methods of interaction between the 3rd party and a person requesting changes are appropriate for various tasks.

User and administrator roles

Guideline 5.1.3.a: There should be a mechanism informing users whether they are in a user role or in an administrator role.

Guideline 5.1.3.b: Users should receive a clear notification when they move from the user role to the administrator role. This notification should warn the user that changes made in the administrator role may be irreversible. Users should have the ability to turn off this warning mechanism.

Guideline 5.1.3.c: Users should receive a clear notification when they move from the administrator role to the user role. Users should have the ability to turn off this notification mechanism.

Guideline 5.1.3.d: There should be a mechanism allowing levels of administrator roles such as super-administrator role and self administrator-role. These levels of administrator roles would require user authentication.

Guideline 5.1.3.e: Users may call upon a third party service and allow the third party service be in an administrator role and administer their profiles.

Guideline 5.1.3.f: Certain important profile administration operations will require special privileges. These operations would require users to authenticate themselves.

Guideline 5.1.3.g: At the end of the configuration, the administrator should be reminded to change role again, from administrator role to user role. That would minimize the risk of unwanted configurations.

5.2 User

5.2.1 Managing activation of profiles

Information in profiles may be divided into profiles that relate to specific situations in which users find themselves (e.g. "Office", "Meeting", "Driving" "Travelling", "Home"). When a user starts a new activity or another situation occurs, then the corresponding profile needs to be activated. A scenario illustrating this is explained in clause 6.1, "A typical working day".

If a wrong profile is active then it may completely or partly fail to meet the user's needs. Users should not have to remember and be willing to spend time and effort on manually activating profiles. It is therefore important that profiles are activated automatically (see clause 11).

5.2.2 Range of categories

Profiles are likely to apply to almost any person that requires or is offered personalized operation of devices and services. In many respects it is impossible to elaborate a comprehensive set of categories of users that could have differing profile needs. The following clauses divide users into a small number of generic categories that are distinguished by the way in which profiles are managed rather than by any other categorization.

5.2.3 Independent adult

The independent adult can be considered to be the most straightforward category of profile user. Independent adults will have the greatest freedom to manage their profiles. The only constraints on the user's ability to modify profile data will be limits and constraints imposed for operational reasons by profile providers, device manufacturers and service providers.

A wizard could guide the independent adult when setting up their profiles by explaining and proposing a set of templates that suit typical roles (e.g. private, work) and situations (e.g. home, out, in car, office, meeting). A scenario illustrating the use of profiles in these typical roles and situations can be found in clause 6.1, "A typical working day".

5.2.4 Supervision and ownership of responsibility

The supervisory nature of some users applies to parent-child, employer-employee, teacher-student, and expert-beginner types of relationships. We will call this generically a supervisor – supervised user relationship. The main characteristic of the supervising relationship is that the user to which the profile applies does not have financial or other responsibility but some one else does, such as parents managing their children's profiles or an agent of an employer who is responsible for maintaining and supporting employee profiles. In many cases, their devices and services may need to be able to share profile data of each other's profiles and provide events to each others devices or services.

As communicating devices become more ubiquitous, their use by some in the population (particularly those with reduced social expectations of responsibility) may need to be supervised or controlled in various ways by their particular parent, employer, or care giver. Profiles need to be able to provide the potential ability to control or delegate selected elements, activities, or capabilities.

While there may be more categories of relationships, the present document identifies three major types. These guidelines are then based on the abstracted requirements from these relationships, and should allow the flexibility for user profile management to cope successfully with other types of relationships.

Management of another person's profiles

Guideline 5.2.4.a: The supervisor should be able to set the privacy levels for any other user for whom they are legally or financially responsible, within the scope of their responsibilities.

Guideline 5.2.4.b: The supervisor should be able to select profile elements of the person being supervised to control alerting, user permission, or complete blocking, under the control of the supervisor.

Guideline 5.2.4.c: The supervisor should be able to individually set the profile information elements of the person being supervised, within the scope of their responsibilities.

Guideline 5.2.4.d: A supervised user should be able to differentiate between parts of their private profile they have rights to manage and those maintained by the supervisor, and be aware of any intersection or conflict.

Guideline 5.2.4.e: Profiles should help the user or their care giver, parent or affinity group to customize services and devices in order to maximise the usability of technologies available.

5.2.4.1 Parent - Child relationships

Initially, the profile of a dependent child (see [16] and [18]) will most likely be owned by the parent or guardian of the child. This child may be allowed to change a restricted set of the profile that the parent or guardian has decided as being suitable for management by the child. The relationship between the child and parent or guardian is similar in principle to that between the employee and the company.

As children develop, and if they assume responsibility for payment for their ICT services, the parent or guardian of the child may selectively allow the child to control increasing parts of their profile. In certain countries there may be legal frameworks that determine when children have the right to fully control their profile.

A scenario illustrating the parent - child relationships is explained in clause 6.2, "Initial profile set-up for a child", see also clause 9.6.6, "Child template".

5.2.4.2 Teacher - Student relationships

The teacher-student relationship also has specific unique demands on profile management. The most recent and obvious case is the desired ability of schools to disable certain functioning of students devices. The current mechanisms are to either prohibit all communications or to make the use of many devices illegal in school. Unfortunately this interferes with many of the benefits that many parents value. A well-formed profile management system will allow a much more controlled and deterministic mechanism for limiting device functionality without interfering with the desired benefits.

5.2.4.3 Employer - Employee relationships

Dependent on the particular management choices made, employees of certain companies may find that much of the content of their professional profiles are managed by their employer and not by themselves. Companies may chose to adopt such a strategy both to relieve their employees of unwanted configuration complexity as well as to enforce certain company policies regarding communication behaviours and security, and optimize the personal devices to the needs of the company's business applications and services.

In such cases, the user will only be free to change a restricted set of options that the company is happy to allow the user to alter, depending of course on the ownership of the various devices and services.

5.2.4.4 Caregiver - Care Recipient relationships

The relationships between a care giver and a care recipient are especially important when each are making use of multiple devices and services, as some of them might be required for the monitoring of health or for alerting when additional aid is required. One complexity in this relationship as well is that, in some cases, the care giver might be the employee of the care recipient or a third party such as a hospital.

5.2.5 User with impaired or underdeveloped functions

Although elderly people, people with disabilities and young children are frequently identified and treated as separate categories, it can be very limiting to assume that specialized profiles will be required to suit people who fall into these categories. Any individual may have their unique preference for their own setting of some aspect of how information is presented to them or the ways in which they wish to communicate. Many people would be tempted to presume that a blind person would prefer information and communication by audio means and not by text - but this would be wrong as, with the use of modern screen reading techniques, many blind people prefer to carry out the majority of their communication using text based services such as email.

What many elderly people, people with disabilities and young children share is that they may need to take account of impairment or lack of development of certain sensory or mental functions. For example, as people age they will gradually experience some loss of hearing and young children will not have developed their abilities in skills such as reading. Because of these impairment or underdevelopment, some people in these categories may wish to define requirements that other people in the population may be content to leave undefined and, hence, set to some typical norm.

The conclusion of this analysis is that it will be fruitless to try to create rigid profiles that are supposed to meet the supposed needs of people who fall into one of the categories previously listed. What is needed is sufficient flexibility in profiles to allow any user to specify their individual needs. What may be of benefit to users is that some of the options in a sufficiently flexible profile can be pre-set to defaults that have been demonstrated to be popular options for many people in some broad category (e.g. people with impaired vision may prefer an initial option that presents them with large fonts on displays). With in-built flexibility of profiles, such pre-setting will not be a mistake as the user will always have the flexibility to reset any specially set option to a more typical or a more extreme setting to suit their individual need.

5.2.6 First-time user

A user who is about to create their first set of profiles is called a first-time user. All people in a user role discussed in clause 5.2 can be considered to be first-time users when creating their first set of profiles. A wizard could guide the first-time users when setting up their profiles by explaining and proposing a set of templates that would suit their needs, see clauses 9.6.1 and 10.5.

5.2.7 User in emergency situations

Heightened fear of terrorism, along with the instantaneous global nature of information and the ubiquity and usefulness of mobile devices, highlights the importance of flexible and assured communications between users and emergency personnel.

In emergency situations, the following information in profiles may be useful:

- preferences such as language preferences - important in the selection of first responders or for using automated translation tools;

- user address or location information - particularly useful if young children are involved or when people have difficulties giving information;
- emergency contact information - specifies who to contact such as parent, husband or wife;
- important medical information - for those requiring special consideration during treatment.

The use of Universal Communications Identifiers (UCIs) [1], [2] and [3]) could greatly assist in the resolution of some emergency situations by ensuring that appropriate communication may be automatically set up and provide a more efficient access to a caller's profile.

User in emergency situations

Guideline 5.2.7.a: Profiles should have the ability to change the behaviour of devices and services in response to emergency situations.

Guideline 5.2.7.b: There should be the potential for a profile to contain emergency related information that could be accessed by emergency personnel in emergency situations.

Guideline 5.2.7.c: Every device and service should provide a potential emergency capability for negotiating priority, identifying a user as a first responder, and lowering its impact on a network infrastructure possibly overloaded due to a regional emergency.

5.2.8 Law enforcement

There may be the need for a third party, with appropriate legal approval and documentation, to access a user's profile without their knowledge.

Law enforcement

Guideline 5.2.8.a: There should be a mechanism for profiles to be accessed by a third party who has the appropriate legal approval and documentation.

Guideline 5.2.8.b: The profile provider should retain complete and secure records of a request to access an individual's profile in emergency situations.

5.3 Profile provider

5.3.1 Provides the profile and associated services

An entity, such as a company, that provides the profile and associated services is called a profile provider. The profile provider may offer different versions of profile tools that are designed with respect to the context of use for different users, tasks, equipment and the physical and social environments. In addition to profile tools, the profile provider may also offer 3rd party services for administrating the profiles. Different types of profile providers include:

- Profile provider providing the whole profile or a major part of the profile: the profile data may be distributed at different locations, or reside at one centralized location. Profile providers should be offered a means, under control of the user's profile agent and therefore the user, of synchronizing their part of the profile with other parts of the profile. The level of availability should be guaranteed.
- Device or service specific profile providers: a device manufacturer, a device, or a service provider may provide a profile, related to the particular device or service.
- Self providers: where users set up their own environment, providing their entire profile, or parts of it. The level of availability of such profiles cannot be guaranteed as the availability of the device or service which hosts the profile is unknown.

The requirements for the above types of profile providers may vary. The present document is primarily addressing profile providers (e.g. telecommunication operators) providing the whole or a major part of the profile.

Profile provider

Guideline 5.3.1.a: Profile providers should be offered a means, under control of the user's profile agent and therefore the user, of synchronizing their part of the profile with other parts of the profile.

5.3.2 One or several profile providers

Users may have one or several profile providers, depending on different requirements, preferences or different user roles (leisure, professional etc.). Users who set up their personal profiles may choose to configure a profile to suit both leisure time and business hours. Other users may have one private profile and another corporate profile, provisioned by the same or by different profile providers.

As a user will wish to have a single integrated view of their profile, even when they have several profile providers, the different parts of their profile should be synchronized.

One or several profile providers

Guideline 5.3.2.a: Users should be able to have a single integrated view of their profile, even when they have several profile providers.

5.3.3 Profile portability

Users may wish to change their profile provider for a variety of reasons such as the provision of better or cheaper services. With any such change, users would find it inconvenient if they lose the profile preferences, settings and rules that they have accumulated over a long period. Therefore, it will be necessary to export profiles including profile tool settings and import them to the new profile provider and new profile tools. The outcome and the user experience should still be the same and the profiles should keep similar behaviour when having a new profile provider and/or using new profile tools. To allow this, the profile information including objects and the internal language implementing the rules need to be standardised (see clause 4.8 "Need for standardization"). The profile information can thus be exported from the original profile provider and imported by the new profile provider.

Profile portability

Goal 5.3.3.a: Users will expect a similar user experience when the profile is moved to a new profile provider.

Guideline 5.3.3.b: Users should be able to change their profile provider when desired, keep their existing profiles and export them to the new profile provider.

Guideline 5.3.3.c: It should be easy to duplicate or import the profile (or parts of the profile) and export it to another profile provider and other profile tools.

Guideline 5.3.3.d: When changing profile provider, there should be no need to redefine existing profile components.

Guideline 5.3.3.e: When the profile provider is changed, the previous profile provider should still guarantee that the user's data is kept private or deleted.

5.4 Service developers and manufacturers

The present document describes issues related to personalization of services and devices, and presents guidelines that are useful when creating services and devices. Service developers and manufacturers have a wide range of requirements depending on the range of devices and scope of their markets.

Several aspects of a service or device may be personalized, depending on:

- characteristics of the service and device;
- specific goals of the service provider or manufacturer (e.g. a public service may want to provide features that appeal to the broadest market whereas a niche provider will wish to provide very specialised features relevant to users in that niche market);
- categories of users (e.g. working, children, hearing impaired) who will use the device/service;
- different individual lifestyles (e.g. frequent traveller) and situations (e.g. babysitting);
- existing profile data that can be used to set initial values for new device or service start-up.

Service developers and manufacturers decide (based on their market knowledge) about:

- in what way personalization can take place;
- which parts of the service are candidates for personalization;
- available settings (identifying which are standardized and which are service or device unique);
- produce templates that reflect these points.

In order to effectively create and manage profiles, service developers and manufacturers would benefit by understanding and applying the applicable guidelines contained within the present document.

Context of use will vary as the individual uses the device or service, and will depend on factors such as:

- time of day;
- geographic location of use;
- type of location such as classroom, office, airplane;
- environmental aspects such as background, noise, light;
- immediate task history, such as search topics.

In order to decide the best way to deliver the device or service to the intended users, service developers will need to obtain information about those users. Prior to the launch of a product, a number of methods can be employed to obtain such information. Although it is out of scope for the present document, these techniques can include:

- results of market surveys;
- feedback from users about previous versions of the device or service;
- usability and focus group testing of prototypes of the new device or service;
- users may define which aspects are relevant, or they may become clear from the way the individual uses the service.

To identify the requirements of individual users of the device or service prior to creating or updating their profile, a number of methods may be used to determine relevant information (see clause 10.8, "Information acquisition"). Personal privacy should be considered when selecting and applying the method.

Service developers and manufacturers

Goal 5.4.a: Service providers and manufacturers should decide which parts of the service or terminal are candidates for personalization, e.g. some profile data owned by the service provider or manufacturer cannot be viewed and/or updated by the user such as charging data.

Goal 5.4.b: Service providers and manufacturers should make settings available for external sharing and control by profile providers and end-users (identifying which are standardized and which are service or device unique).

Goal 5.4.c: Service providers and manufacturers should decide in what ways personalization can take place, e.g. by the provision of suitable profile management tools.

Goal 5.4.d: Service providers and manufacturers should produce templates.

6 Scenarios

This clause contains scenarios which illustrate the way that profiles benefit users and illustrate many of the key concepts in user profile management. They scenarios will highlight some interesting concepts and are not intended to illustrate all alternative solutions. At the beginning of each scenario, there is list of issues that are covered in the scenario.

6.1 A typical working day

Issues addressed in this scenario include:

- situation dependent profiles;
- profile hierarchy with several more specific profiles building on a less specific profile;
- transitions between states;
- automatic activation;
- events;
- profile agent;
- intelligent house and house profiles;
- sensor;
- intelligent car.

The following scenario about a typical day in the life of a business woman, Anne, illustrates how states, including default states, might be activated and how the transitions between these states might be triggered.

Anne has defined a set of profiles that she finds very useful. Her profiles cover both her private role and her professional role (see clause 9.6.1, "Adult"). She found it easy to define her profiles as she was guided by a wizard (see clause 10.9.2, "Guided configuration") that asked her some questions in order to propose appropriate templates related to her lifestyle. These templates proposed some default values based on the choices she made during the guided tour provided by the wizard. She decided to accept some of the proposed defaults and she decided to select her own values for other preferences and settings. The wizard also proposed options for activation of her profiles (see clause 11, "Profile activation").

At home

Anne is at home and her profile is in the "at home (awake)" state. There are sensors in the house that can detect Anne's presence.

Leaving home - Outside

When Anne leaves the house and locks the door behind her, her "smart key" sends a message to her smart home that she has left the house. At this transition of the smart home state, the profile agent checks all the entities associated with Anne to determine Anne's current state. As the current state of the entities does not match those described for any of the defined user states the profile agent needs to select one of the default states. Anne has previously defined that the "outside" profile should be activated after leaving the house, leaving work and leaving the car (i.e. when all of the "at home" states, all of the "at work" states or any of the "car" states suddenly cease to be valid). As Anne is the last person leaving the house, the house's "All left" profile is activated resulting in that the heating is be set to Economy mode, the alarm is turned on and the shutters are closed. The house profile could be considered as a "device" profile associated with a shared "device", see clause 4.2.2. A set of profiles suiting different situations (e.g. "All left", "People at home", "Night"), could be associated with the house. Typically, house profiles may be associated with more than one person's profiles. A house profile associated with more than one person's profiles would raise issues such as conflicting preferences when used simultaneously by several people.

As Anne is leaving the house, her state is changed to "outside" and the "outside" profile is activated which results in calls being directed to her mobile phone.

In car

When Anne enters the car she places her mobile phone in the car handsfree/charger mount. Placing the phone in the handsfree/charger generates a change of entity state that is notified to the profile agent. The profile agent again checks the state of the entities associated with Anne and tries to find a match to a current user state. In this case the "driving my car" state only requires that the mobile phone is in the handsfree/charger, so the profile agent chooses the "driving my car" state and activates the "driving my car" profile. Seat and mirrors are adjusted to her preferences, calls are directed to the car handsfree, she will listen to incoming emails and her favourite radio channel is selected and the volume is set to her preferred level.

Leaving car

When Anne removes the phone from the handsfree/charger, this state change is communicated (as an event) to the profile agent and the profile agent again checks the state of the entities. The "driving my car" state no longer applies and the states of the various entities do not match those defined for any of the other states. As previously described, Anne agreed that the profile agent should select the "outside" state when she leaves the car, so the state is now set to "outside" and the "outside" profile is activated again which results in calls being directed to her private mobile phone.

At work - at office

As soon as Anne enters her work premises by using her smart badge, her profile agent is notified of this event. Anne's state is set to "at work" as this state is the default state that is activated when the event from the smart badge has been received (the state of the entities do not match those required for any of Anne's other more specific at work states). As soon as Anne enters her own office and places her mobile phone in the desk charger, the charger sends an event to her profile agent. The profile agent checks entity states and determines that the "in my office" state applies, as this only requires the phone to be in the desk charger. The "large fonts" preference is activated on her PC, her preferred language is set and her calls are directed to her office fixed phone.

At work - default

When Anne leaves her office and is not yet at a meeting, her profile agent sets the default "at work" state which results in calls being directed to her work mobile phone.

At work - meeting

Anne has a meeting scheduled for 14:00 and this has been entered into the calendar application on her PC. The PC notifies her profile agent 5 minutes before the meeting is due to start that she should be in a meeting. The profile agent sends an instant message to Anne asking if the meeting is still taking place (Anne has said that she wishes to confirm scheduled meetings as they are often cancelled or postponed). When she confirms that the meeting is taking place, her state is set to "in a meeting" at 13:58.

As she enters the smart meeting room at 13:59 the room detects her smart badge and sends an "entering meeting" event to her profile agent. As the profile agent has already set the state to "in a meeting" it does not need to take any new action but it notes that the meeting is in a smart meeting room. As not all meetings will be in smart meeting rooms the profile agent needs to look at two sources of meeting related events - calendar based and smart room based.

The meeting profile sets her mobile phone to silent mode, calls will be directed to her voice mail but an exception is made that allows her most important client to phone her as she hopes to sign an important contract very soon.

The meeting ends later than scheduled but the profile agent maintains the "in a meeting" state longer than was indicated in the calendar schedule as it has not received a "leaving a meeting" event from the smart room.

At work - default

When Anne eventually leaves the meeting the profile agent receives the "leaving a meeting" event and examines the state of the entities associated with Anne. As the state of the entities do not match those specified in any of Anne's states, and because no event saying that she has left her work premises has been received, the profile agent restores the default state "at work" which results in calls being directed to her work mobile phone.

Leaving work

As it is now so late, Anne wants to go home. As she leaves the work premises the building detects her smart badge leaving and notifies Anne's profile agent. The profile agent sets the default "outside" state.

In car

When Anne enters her car and plugs in her mobile phone the "driving my car" state is set again. As usual, seat and mirrors are adjusted to her preferences, calls are directed to the car handsfree, she will listen to incoming emails and her favourite radio channel is selected and the volume is set to her preferred level. She has defined a rule (in her "driving my car" profile) that determines that she is returning home as it detects that she is driving the car after having left work. The outcome of that rule is to set the heating of her home to a comfortable temperature when she arrives.

Outside and later Wi-Fi indoors

On the way home she picks up her husband from the airport. As she leaves the car the "outside" state is re-established. As Anne enters the airport her smart mobile phone detects a Wi-Fi network. Anne has a default profile called "Wi-Fi indoors" and the presence of the Wi-Fi network triggers this state. With the "Wi-Fi indoors" set Anne's profile now gives her the option of routing her communications via a broadband Wi-Fi connection.

Sleeping

Anne's journey home from the airport goes through the same familiar states - "outside", "driving my car", "outside" and "at home (awake)". After a busy day it will soon be time for Anne's state to be "asleep" which results in no calls being allowed, heating is being set to "Energy saving mode", shutters are being closed.

6.2 Initial profile set-up for a child

Issues addressed in this scenario include:

- child (see [16]);
- parent;
- managing profiles on behalf of someone else (see clause 5.2.4.1, "Parent - Child relationships");
- roles - administrator and user;
- default values and templates for guided configuration (see clause 9.7.5, "Child template" and clause 10.9.2 "Guided configuration");
- wizard for guided configuration;
- Universal Communications Identifier (UCI) (see [1], [2] and [3]).

Karen and Peter have decided that their son Michel, 12 years, will get his own profiles as he is frequently using his mobile phone and the internet. Karen and Peter feel worried as they have read about paedophiles lying about their age and identity when contacting children in internet chat rooms. However, they have been informed that an increasing number of chat rooms for children have enhanced the security by demanding a Universal Communications Identifier, UCI, for ensuring that the users of the chat rooms have an authenticated age (see [2]). As profiles and UCI work perfectly well together, Karen and Peter decide to give profiles and a UCI to their son. Yesterday they all went to their profile/UCI provider. As UCI is an authenticated identifier, they had to prove Michel's identity to the provider by bringing Michel personally with his identity card to the provider. The profile provider, who is also a certified UCI authority with rights to give people a UCI, entered Michel's personal data such as name, address and birth date in his base profile, and associated it to his UCI.

Today Michel and his parents sit together in front of the PC and they feel a bit curious and excited to use the CD they got from their profile provider. The CD contains a wizard for configuring child profiles. The wizard shows them Michel's personal data entered by the profile provider and proposes to show a very short film explaining the profile concept and the benefits for children and parents. The wizard explains that it will ask the parents which statements are applicable to their situation. Depending on the answers to these questions, the wizard can investigate further with more questions to get a more detailed picture of their needs. The further questioning by the wizard do not be described in this scenario. Based on the parents' choices, the wizard will propose templates that assist in the definition of Michel's profiles. For some data entries, parents will typically accept the default values proposed in the template, but for other entries, they will prefer to fill in values.

The wizard asks the parents: "Which of the following statements do you agree with?"

Statement: "My child has limited abilities reading text or understanding complex text."

If the parents reply "yes", further questioning would identify ways in which profiles could provide enhanced accessibility to information by providing options such as:

- listen to text;
- large fonts;
- adapted conceptual content (e.g. text, images and sounds).

Statement: "My child should be protected from accessing and downloading unsuitable content."

If the parents reply "yes", profiles that provide content limitations would be proposed. The profiles may contain the child's age or other data that could be used for filtering services or access control, allowing only suitable content.

Statement: "I wish to prevent my child from communicating with some people."

Due to children's social development they may not be aware of the risks when communicating with some people. If the parents reply "yes", profiles that provide filtering services that limits the communications could be proposed. The profiles might contain:

- list of allowed communications (incoming and outgoing);
- service provider's identifications of unsuitable adult chat rooms;
- the UCI concept of "authentic date of birth", used to allow access to age-controlled services such as children's chat rooms (see [2]);
- masking the child's location, number, or other data, or substituting the parent's, for calls to or from unknown or known dangerous addresses.

Statement: "I wish to limit costs".

Many parents complain about the communication costs, and sometimes prevent their children from using mobile phones. In addition, parents may want to limit their children's ability to buy online. If the parents reply "yes", profiles that provide filtering services that reduces costs could be provided. These could contain the following:

- List of allowed communications such as:
  - phone;

- internet (allowed sites, not buying online).

- Rules that allow only local communication (no international, no expensive services).

- Rules that enforce cost limitations such as "I give my children 50 Euros to spend on communication. When 5 Euros is left, then they can only phone their parents".

Statement: "I wish to create a "School" profile."

Many schools do not allow children to use or even bring mobile phones to school as teachers do not want their lessons to be disturbed. Yet many parents insist their children have mobile phones for their safety, security, and convenience. If parents reply "yes", they could be offered a "School" profile which could contain:

- a rule that limits usage to appropriate types of communication (e.g. limiting functionality to making emergency calls and allowing calls to or from parents);

- activation rules to automatically activate or deactivate the "In Class" profile. The child's mobile phone could detect standardized location dependent labels such as "Classroom" or "Silent" associated with classrooms.

Statement: "I wish to know where my child is."

Parents may get worried if they do not know where their children are. If the parent wishes to have this option, profiles could provide data from location based services to the parents' profiles, giving the parents information about their children's location.

Statement: "I wish to define a profile for emergency situations."

Children may not be able to give important information in emergency situations. Profiles for emergency situations could contain private information that would only be provided to appropriate enquiries from emergency personnel (e.g. doctors, nurses and police). The information could include:

- contact details of the child and parents;

- location of the child;

- special health information (haemophilia, allergies, diabetics, medicines, contact information to the child's doctor etc);

- child's age so that the emergency operator may give instructions adapted to the child's age.

Statement: "I wish that we, the parents, have full privileges of our child's profiles and related tools and that our child has user privileges".

If this option were chosen, the parents would have administrator privileges and the children would have privileges to use the profiles, but not to manage them (see clause 5.1, "User and administrator roles").

6.3 Buying a new mobile phone

Issues addressed in this scenario include:

- device profile creation, see also clause 10.5, "Creation";

- centralized backup of profiles;

- use of settings, preferences and information from another device.

Anders has used his mobile phone for three years. He has set up the phone to meet his personal preferences and he had a lot of information stored in his address book and calendar. Unfortunately he lost his mobile phone yesterday in deep water while he was sailing. He decides to buy a new mobile and he wishes to have the same information and settings as in his lost phone.

As the profile information of his mobile phone, also including calendar and address book, was always synchronized with his centralized profile, he has not lost that information from his mobile phone.

The shop assistant asks Anders if he wishes to use pre-set default values or whether he wants to use the information stored in his profile. He says that he wants to use as much as possible from his lost phone and the shop assistant helps him to do that by using his profile data.

6.4 A person with a severe hearing loss

Issues addressed in this scenario include:

- using data from the address book to determine the role of the person being called (e.g. business or friend);
- choosing the communication solution dependent on the role of the person being called;
- UCI which supports negotiation to help set up a call that suits the user's preferences;
- language preferences;
- assisting people with hearing loss, optimized by the use of personal video;
- invocation of human or automated relay service offering sign language translation.

This scenario is about Bill who is 37 years old and who has a severe hearing loss. Bill uses:

- a mobile video phone to communicate in sign language via an automated service;
- an automated system which recognises his sign language and converts to speech in a choice of languages.

From this it is clear that Bill has access to two alternative ways of using sign language to communicate with people or services that expect spoken communication. Without a profile, Bill will have to make a decision about which of the services to use each time he makes a communication to a person or service that expects spoken communication. Having made the decision, he will have to remember how to access each of these services and then enter details of the person or service he wants to communicate with.

If Bill has a profile, this can contain details of the method for accessing each of the sign-language to speech services. This profile can also contain rules that express Bill's preferences for when he uses each service. These rules can be used to automatically choose the appropriate service to use, based on Bill's judgement about when it may be worth using the more costly human-mediated relay service and when the cheaper automatic service would be best. The rules about which service to use may take into account a large range of factors, including:

- the role that Bill is currently in (e.g. if he is in his business role and his company wishes Bill to have the best possible communication with business customers the company will be willing to pay for the dearer relay service);
- the identity of the person Bill is communicating with (e.g. Bill's best friends may understand and tolerate the inferior quality of communications via the automated service as they realise that it is saving him money);
- the language preference of the person Bill is contacting (e.g. if Bill's relay service is an English language service and the person Bill is contacting is German, then it will be essential to use the multi-language service).

In the above examples, the profile agent that processes the rules in Bill's profile will need to communicate with various communications services and networks to achieve what Bill requires.

If a Universal Communications Identifier (UCI) (see [1], [2] and [3]) is used, the Personal User Agent (PUA) that controls Bill's communications would take care of all of the communications complexities. In particular, in the example in the last bullet, Bill's PUA would communicate with the PUA of Bill's German contact and discover that this contact speaks German but not English. Without this PUA to PUA communication, specifying the correct output language would be something that Bill would have to do himself (if he was aware that the person he was contacting only spoke German). If Bill and the person he was contacting did not use UCI and Bill did not know that he only spoke German, then he might choose to use the English language relay service. In such a case, everybody involved in the attempted communication would be very frustrated and embarrassed.

6.5 Public access terminal

Issues addressed in this scenario include:

- identification;
- language selection;
- dyslexia;
- base profile;
- delivery of preferred settings;
- globally available bookmarks.

Roberto from Italy is on holiday in Höllviken in Sweden where he is invited by his old friend Ingrid. One day, they decide to visit Copenhagen and Roberto remembers that he read some interesting information about places he wanted to visit. The problem is that he does not remember the names of the places, neither does he remember on which websites he read the interesting information. Fortunately, he bookmarked the websites containing information about places to visit. When Ingrid shows him the nice library in Kungsparken, he gets the brilliant idea to use the library PC to read the websites he has previously bookmarked.

His profile is automatically activated when he logs on. As Roberto is dyslexic, he finds it difficult to read when having certain coloured backgrounds, but he likes to read with a light cyan background. The background colour of the PC is automatically set to light cyan as this preference is defined in his base profile.

Roberto only knows how to say "Hello" and "I love you" in Swedish, but luckily, he automatically gets information in Italian, when available, or otherwise in English, thanks to the language preferences in his base profile. He finds all the interesting websites he bookmarked in Italy thanks to the possibility of including bookmarks in profiles, and thus making them accessible wherever the internet is available. He shows the websites to Ingrid and they plan which places they will visit tomorrow.

6.6 Car crash

Issues addressed in this scenario include:

- emergency situation;
- sensor in car activating the emergency profile;
- profile data made available to emergency personnel;
- medical data in profile;
- other people's contact information in profile;
- language preferences.

Catherine moved from France to Sweden three months ago due to her new job. She lives with her husband Pierre near Malmö. She is interested in learning Swedish, but has not yet progressed very far with her Swedish lessons. She thinks it is OK to speak English at work and in most other situations.

As Catherine will fly from Copenhagen to Nice on a very early flight, she has to get up at five. Unfortunately it has been very cold and her car skids, crashes and she looses consciousness. Luckily, Catherine's car has a crash sensor that detects the crash and calls for help. As the intelligent car knows who is driving, it automatically activates the part of her profile associated with emergency situations.

Thanks to Catherine's profile the following happens:

- An ambulance will be sent to the place where the accident took place. Her profile says that she does not speak Swedish, but is very good in English. All ambulance personnel speak English, but they prefer to bring a French speaking nurse as Catherine's language preference for emergency situations is French. It is very common that people prefer their native language when they are in a state of shock.

- The ambulance personnel receive the information that she is seriously allergic to the acetylsalicylic acid (commonly used in pain killers) and might die if given it.
- When the ambulance personnel realise that Catherine is injured, they decide that she needs to be sent to the closest hospital.
- Catherine is in the ambulance and regaining consciousness but she is still in great pain. Unfortunately, she is unable to phone her husband as she is in a state of shock. Her profile contains information about who to contact in an emergency situation: her husband Pierre and it also indicates that his preferred language is French but English is also OK. The French speaking nurse initiates a call to her husband and tells him about the accident and his wife's condition. The nurse suggests that he talks to her to help her recover from her state of shock. After having talked to him for a while, Catherine calms down a bit, especially as he has told her that he will soon arrive at the hospital where they will meet.

6.7 Hospital stay

Issues addressed in this scenario include:

- information sharing;
- profile storage and accessibility choices;
- limited transport of personal information;
- description of identification processes;
- temporary delegation to a supervisor.

Lucy Van Epers needs to go to the hospital for some elective surgery, see ePerSpace scenarios [14]. The various devices and services she uses, along with those of the hospital, work together to make her stay more comfortable and efficient, and more reliable and accurate for the medical personnel. Together, they increase Lucy's confidence in this usually stressful event. While the entire scenario will not be described here, there are a few elements of the scenario which illustrate some important profile issues related to the transport of user data.

Lucy carries a personal digital device, which could actually just be an enhanced mobile phone. She is able to use this device to answer a myriad of questions from the hospital, such as her preferred diet, choice of music and television, setting up the phone service in her room. She can also use it to carry her music, and any certificates she has for licensed content, such as an on-line movie she has been meaning to watch.

She starts by sending the hospital permission (during their on-line registration session) to inquire of her profile about her relevant settings, which of course is much easier than spelling each one out on-line or to a hospital employee.

Technologies used in this scenario include a personal digital device, network services and content management. The alternative solutions, described below, are solely to illustrate that there will be multiple solutions to each issue.

6.7.1 Profile accessible with a personal device

Lucy carries her personal device with her to the hospital. She has her profile provided by her favourite profile provider, who offers enough storage space for all her required files such as an entire year on her calendar, her favourite songs, books she refers to or intends to read someday, and space for a movie.

Her device carries a secure identification token (such as a SIM card) which she has password protected, and she can provide an authentication token based on that, along with the categories of data it applies to, to the hospital, which then sets up a limited access method for the data they need in her profile and the data she will want access to, such as her movie.

6.7.2 Profile accessible with a hospital provided personal device

The hospital prefers that it has more control over the devices brought into the hospital (for example mobile phones), and provide Lucy with a device she can use to bring her "connectedness" into the hospital with her. It executes a Web application that collects any of her data that the hospital stay requires, asking her permission to download any secure elements. It also allows her to copy the movie from her home server, but may limit her eventual access to it (and other services), depending on her condition. It also allows her to transfer her phone number and other access addresses, so that she can stay in touch, but again the hospital desires to exercise some control on when she may receive communications. It will not hide them from her, but may redirect them to a number or mailbox of her choosing.

In this case, Lucy needs to have a mechanism to allow another, temporarily used device, to be associated with her for the length of the hospital stay, so her overall profile related services and their logical connection to her can remain intact. This also illustrates the supervisor – supervised case in health care, that Lucy delegates some level of control of the relevant parts of her profile over to a temporary supervisor.

6.7.3 Lucy desires not to share any electronic access with the hospital

Lucy does not feel comfortable sharing any profile data with the hospital. Instead, she has her home network ask her the relevant questions. Using her secure access at home, she then emails the relevant data to the hospital. When the hospital receives this, they do ask her to allow access if a justifiable emergency arises. She brings her movie with her on a secure memory card that she can insert in the television of her hospital room. Although this is more time consuming, the hospital recognizes the privacy desires of their patients.

This alternative describes the need for adaptation to various levels of individual security and confidence in technology. Lucy still has profile data but chooses to share it manually. This case also applies to those who have no desire or need to use mobile technology. The profile mechanisms available to her and the hospital should allow her to do so.

7 Profile contents

7.1 Profile data

Profiles need to be set-up and maintained in order to offer personalized services and devices. This clause provides an overview of what profile data (see also clause 4.1) is contained within profiles.

For each profile, the following need to be defined:

- **profile name:** The profile name is used for identifying profiles. In addition, the profile may have a voice or sound label, an icon and a colour. These are described in more detail in clause 7.2.
- **core functional profile data:** This is the most essential part of the profile. It contains preferences, settings and rules that are valid when the profile is active.

In order to automatically activate or deactivate profiles, the following will be defined:

- **activation criteria:** In order to let the profile be automatically activated, activation criteria need to be defined. If no activation rule is defined, the profile has to be activated manually.
- **deactivation criteria:** In order to let the profile be automatically deactivated, deactivation criteria can be defined. If no deactivation criteria is defined, the profile will automatically be deactivated when another profile is activated and it can also be deactivated manually.
- **user confirmation of activation/deactivation of profiles:** Users may choose whether they prefer automatic activation/deactivation to take place with or without having to confirm it.

In addition, the following might be defined:

- **comment:** The profile can be described in the free text comment.

- **inheritance information:** Defines inheritance relations between profiles such as when the user has defined the "Work" profile with several related profiles including "At my desk", "Business travel", "Meeting", "Default" (when none of "At my desk", "Business travel", "Meeting" are active).

- **association to a live template:** If there is an association to a live template then the profile will automatically be modified when the live template is modified.

- **lifetime:** When the profile is created, it is possible to assign it a Lifetime (e.g. to be applied once, a user defined length of time, or until the user decides to delete the profile). The lifetime of a profile is not to be confused with the time a profile is active. A profile that is deactivated still exists and can be activated again. A profile is automatically deleted and will not be activated again when the Lifetime is ended.

Some of the profile data can be predefined and/or in templates. Some information, settings and preferences are more or less permanent and are preferably defined in a base-profile containing information such as the user's name and birth date. Other settings are more suited to a certain situation and it might be relevant to define those settings in a situation dependent profile corresponding to that specific situation e.g. "meeting", "travel" and "office".

The following clauses define the contents of a profile from the user's point of view. Objects and settings needed for delivering services that are not visible by the users are not described.

7.2 Representing and defining profile data

The way in which users wish to see objects or define their values to objects may be complex. Some of these values could be represented or defined in absolute terms (e.g. 24th December 2005) or in relative terms (e.g. 2 weeks from now). In other cases, there may currently be no generally agreed common standard for expressing such objects (e.g. there is no commonly agreed standard for quality of communication between voice communications and video communications).

The grouping of profile data should be consistent and logically related to the task the user wishes to achieve. It may be necessary to provide entry points in different parts of the user interface to the same set of profile data.

Representing and defining profile data

Goal 7.2.a: The way objects are represented to users should be dependent on user's preferences and the specific context of use.

Guideline 7.2.b: Some values could be represented or defined in absolute terms (e.g. 24th December 2005) or in relative terms (e.g. 2 weeks from now), depending on the user's preferences.

Guideline 7.2.c: Users should be able to access their profile information and profile tools in a selectable language.

Guideline 7.2.d: The grouping of profile data should be consistent and logically related to the task the user wishes to achieve.

Guideline 7.2.e: It may be necessary to provide entry points in different parts of the user interface to the same set of profile data.

Profile data presented to users should be described to the user in a language that they can understand. In practice, they may have a very different internal representation. Further details about this can be found in clause 4.1.5, "Interpretation of profile data".

Profile data may have a number of attributes that help users to manage their profiles. The following attributes are some of the most common and useful ones that make objects visible to users in the profile management tool:

- **name as a text label:** The name of the profile is defined as a text label. The user can choose whether to see the text label or not. Instead of seeing the text label, the profile can be identified by an icon or a voice/sound label, as described below.

- **colour:** The user can select a colour for displaying the name. It may be useful to use colours to more easily distinguish between individual objects.

- **icon:** The user can select an icon that can be displayed together with the name or instead of the name. This can be useful when a small screen is being used and for enhancing accessibility for those users where the use of icons is easier than reading the text name.
- **voice/sound label:** The user can record a sound or spoken word and associate it with the name or use it instead of the text label. This can be useful when using spoken commands, when using a terminal without a screen or with a small screen and for blind or partially sighted people.
- **Comment:** The user can write a comment that can be useful later for understanding or remembering the use of the object.

7.3 General operations

There are a number of operations needed to maintain and employ profiles. The profile data will be manipulated by different actors such as profile providers, service providers and end users. The operations could also be done remotely.

The following operations exist for most profile data:

- create new;
- assign values to the attributes;
- view;
- modify;
- copy;
- paste;
- delete.

The complexity of the open communications environment impacts the planning for profile operations. Different services on different devices supported by different protocols may be required to fulfil user needs. Profiles should allow users to take full advantage of all available technologies.

7.4 Generic or specific preferences and settings

Preferences and settings can be generic such as "high audio volume" or service/device specific. Generic preferences and settings contain information that is relevant to all available personalized services/terminals or groups of them. Service/device-specific preferences and settings contain information that can be utilised by one specific service/device only. Further information on this subject can be found in clauses 4.1.3 and 4.1.4.

Generic or specific preferences and settings

Guideline 7.4.a: Users could define whether preferences and settings are specific or generic e.g. if settings are related to specific terminals/services or to groups of terminals/services.

7.5 Capability and preference negotiation

Users may wish to set values, but it may not always be possible for an exact match to their preference to be achieved. To resolve such situations, negotiation can take place in order to try and achieve a good, but not perfect, match. Where the relevant capability is supported (see also OMA-UAProf [7]), negotiation will take place between:

- user's preferences - terminal capabilities;
- user's preferences - service capabilities;
- terminal - service capabilities;

- preferences of two communicating parties;
- terminal capabilities of two communicating parties;
- service capabilities of two communicating parties.

7.6 Overview of a selection of profile objects

This clause provides an overview of a selection of objects that are useful to define and refer to when defining profiles. Other objects, not listed in this clause, may also be useful in profiles.

7.6.1 Rule

One of the most important components of many profiles is rules. These enable various forms of conditional behaviour to be specified in a profile. Many of the objects described in this clause will be referred to in rules. A detailed description of rules is contained in clause 8.

7.6.2 Date and time

Profiles may be activated or deactivated at a certain date and time. Users can define time in different ways and name the defined time, e.g. Night: 22.00-07.00, so that it can easily be referred to in rules, see ISO 8601 [10]. Time can be defined in different ways such as always, start time, end time, according to a schedule, or as a one single time or date. The calendar functionality within the profile tool can be synchronized with an external calendar. A time schedule can also be automatically defined as the complement to another time schedule.

EXAMPLE: A user defines "work time" as Monday to Friday 8.00 to 17.00. She sets "spare time" to be the rest of the week hours. "spare time" is automatically made the complement to work time. When the user redefines "work time", the will, knowing that "spare time" is the complement to "work time", ask the user to confirm that "spare time" should also be automatically modified.

7.6.3 Group

Users may want to address a group of items such as people, or other objects, when defining rules. The profile tool could offer some predefined groups to help the user take advantage of the concept, but of course, the user would have to add members to the groups. Examples of groups are family, friends, colleagues, customers/business, club/association, email, place/activity. White list is a concept that could include all records in the address book, and could be used for filtering incoming communication so that only persons in the address book are allowed access to the user. It is possible to separately add users in one group to another group or add a group in a group to create a hierarchy of nested groups inside group.

Users could get a list of objects and rules referring to a group so that they may better understand the consequences of performing operations on the group.

Defining groups and adding members to groups

Guideline7.6.3.a: The profile tool could offer some predefined groups to help the user take advantage of the concept. The user would then only have to add members to each group.

Guideline7.6.3.b: There should be a mechanism helping users defining their own groups.

Guideline7.6.3.c: For every individual group, users could get a list of objects and rules that refer to that group so that users may better understand the consequences of performing operations on that group.

7.6.4 Service

Information provided by services will need to be adapted to the user's needs using the information contained within the profile. One group of services that is particularly useful to address in profiles is communication services such as filtering of incoming and outgoing communications. Profile operations related to communications services are further described in documents describing the Universal Communications Identifier concept (see [1], [2] and [3]).

Services will not only provide information to the users but also receive feedback from them. When users are able to interact with the service they can customize it by defining their user preferences. To be able to customize new services and new features of existing services, the users need to receive information about them. Service discovery and service feature discovery would allow users to be notified about new services and when new service features have been made available.

7.6.5 Terminal

Users will need to define their terminals such as fixed phone, mobile phone, computer etc. and associate them with their profiles. This is useful when defining their personal settings and preferences related to that terminal, when defining automatic activation rules or when defining source or destination in communication rules. Terminals can be associated with services, accessories, places and activities. Users may want to define their phone and associate it with home or work. They may also define a profile and call it "work" or "home" and then associate it with a phone.

Relations with terminals can be in both directions terminal to profile and profile to terminal:

Terminal to profile: Terminals and accessories will provide data (such as events for synchronization) to the profiles. A user initiated change of profile in the mobile phone could be synchronised with the profile in the network, with potentially more benefits for the user. Events from terminals can be used for synchronization and trigging different actions in profiles such as when a user arrives at work and places the mobile in the desk charger, which would result in an automatic activation of the "Office" profile. This might happen:

1) the mobile phone detects that it is connected to the desk charger, which sends this event (e.g. SyncML) to the profile agent;

2) the profile agent receives the event with the information about which charger is used. This information can be used to activate the "Office" profile.

Profile to terminal: Terminals and services might change behaviour when a profile is activated. Example: A meeting profile might result in the following settings in the mobile phone: Silent mode, Set Alert to Vibrating, Divert to Voicemail, Call Filtering will be activated.

7.6.6 Accessory

Accessories may be used together with terminals to offer more functionality. Different accessories may be associated with specific places or activities, to trigger automatic activation of profiles related to those places or activities. The user may associate rules with events such as attachment/detachment of terminal accessories. The profile agent may subscribe to events and take different actions depending on the rules associated with those events. For instance, when a mobile phone is placed in a desktop charger at the office, the "Office" profile will be activated resulting in automatic diversion of incoming calls to the fixed phone in that office.

Accessory

Guideline 7.6.6.a: When an accessory is used the first time, the profile tool should automatically be updated in order to provide the user with the ability to address that accessory and the events associated with it, when defining their profiles.

Guideline 7.6.6.b: Automatic accessory discovery will help the user address new accessories in rules, e.g. for defining automatic activation of profiles.

7.6.7 Contact information

An important element to address in profiles will be a person or organization. This type of information is usually found in the form of contact records in an address book (which may be a separate application to the profile agent). Contact information is covered in more detail in clause 12.

7.6.8 Presence information and activity

Situation dependent profiles are often associated with places and activities. Different types of location information (see Wireless Village version 1.1 [11]) may be useful such as:

- time zone/local time;
- geolocation (gives the measured position of the client device. It may be either sensor based, e.g. GPS or network based or a combination of both);
- postal address;
- freetext location (e.g. Nice Airport, Terminal 2);
- devices and accessories.

Places referred to when using services for example when a travel booking is made online, may be used for activating a "Travel" profile. Another example is when people are using automatic teller machines or using their credit cards which might give an indication of where they are.

Users may also associate their devices and accessories to certain places or activities, for instance when a mobile phone or a mobile handsfree is used in a specific environment such as in a car.

Place and activity are words that can have a similar meaning to users as a specific activity is often related to a specific place, e.g. work is an activity that is often associated with a specific place. Objects related to place/activity are useful when defining personal preferences or source and destination in rules. They are also useful for activation and deactivation of profiles.

Presence attributes contains presence information intended for the user and may also contain meta-information for machine-to-machine communication between the publishing client and receiving clients. The location can be given using different methods and should be given with accuracy information indicating the average positioning accuracy achieved by the method.

Presence attributes can be divided into the following classes:

- client, (e.g. application or terminal) status describes the availability of the client for communication, location information and client capabilities;
- user status describes the declared availability of the user;
- extended presence information that is specific to the vendor or service provider, non-standard presence attributes that need to be passed through standard presence servers.

7.6.9 Language preferences and regional settings

Users may define their language preferences and regional settings corresponding to where they spend most of their time. They may have alternative regional settings in profiles used when travelling abroad. See ISO 639-2 [13]: "Codes for the representation of names of languages - Part 2: Alpha-3 code" for standard language codes.

7.6.10 Accessibility settings

Profiles can be used to improve communications both for people with various functional impairments (e.g. people with different disabilities and elderly people), for very young people and for all people in situations when the context requires specific settings or services. CEN Workshop Agreement 13987-1: "Smart Card Systems - Interoperable Citizen Services - User Related Information (based on DISTINCT) - Part 1: Definition of User Related Information" [12] provides examples of accessibility settings. The term "special needs" is most commonly used to refer to the needs of disabled people. It is also useful to broaden the definition to include people in situations when they temporarily have special needs.

EXAMPLE 1: Visually impaired people and young children who cannot yet read could define "listen to text"' as a permanent preference in their base profile.

EXAMPLE 2: The special need "listen to text" could also be useful for people wanting to listen to their emails while driving a car. A situation-dependent profile "Driving" could provide them with this service. The situation-dependent profile "Driving" might be automatically activated when the driver uses their car mobile handsfree or when opening the car door with a smart key.

7.6.11 Content preferences

Domain specific terminology may be used for defining content preferences. Implicit and explicit methods (see clause 10.8, "Information acquisition") may be used for definition of content preferences. To obtain the maximum benefits, domain specific terminology should be standardized (see clause 4.8, "Need for standardization").

A concept called bookmarks exists in web browsers. Bookmarks can be used for storing URL's to web sites the user wishes to revisit. An extension of the current concept would be to have the bookmarks stored in the profile rather than in a specific browser on a specific terminal. This would mean that these bookmarks would then be available from any browser and from any suitable terminal.

7.6.12 Settings for management of other users' profiles

This functionality is targeted at profile administrators managing other people's profiles such as corporate profile administrators, parents managing their children's profiles or care givers. Most users managing their own profiles do not in general need user management. Templates providing help to define these profiles may be very useful.

This functionality can be seen as an extension to normal profile management and includes:

- management of multiple users and their profiles;
- log management for multiple users;
- security including authentication, confidentiality and privileges;
- template operations.

7.6.13 Mood

Moods may also be referred to in profiles and rules. Some users might want to define their mood and communicate it to other users.

7.6.14 Network

The fast evolution of telecommunication networks and services gives new management possibilities. Different networks have different rates depending on factors such as time, quality, and availability. Users may define Network settings, preferences and rules in their profiles.

8 Rules

8.1 The concept of a rule

Users often express conditional phrases in their everyday life. When doing so, they express rules (even if they do not call them rules) such as "WHEN it rains, THEN I bring the umbrella". This concept is also useful when defining profiles and the profile tool thus will require a rule editor. The rules are processed by the rule engine.

Rules can be used for defining:

- profile activation criteria (e.g. "WHEN my mobile phone is attached to the car handsfree THEN activate "Driving" profile), clause 11, "Profile activation";
- filtering criteria;
- diverting communications;
- communication priority;
- privacy rules;
- log information.

8.2 Conditions and actions

Rules consist of one or more conditions (e.g. "When it rains") and one or more actions (e.g. "bring the umbrella"). A condition can be defined in different ways, such as a specific word (e.g. "When"), graphic sign or position to the left. An action can also be defined in different ways such as a specific word (e.g. "Then"), graphic sign or position to the right.

There are different types of conditions, for example:

- event driven, when an event occurs such as an accessory has been attached to a terminal, "WHEN my mobile phone is attached to the car handsfree". The condition will be followed by an appropriate action such as "THEN activate "Driving" profile.";
- filtering incoming calls such as "When incoming call is from Family";
- filtering outgoing calls such as "When outgoing call is to Customers";
- something is equal to a specific value or range such as the current time is "Mondays at 19.00 to 21.00".

Conditions and actions

Guideline 8.2.a: The user should be able to choose active events from a set of possible events.

Guideline 8.2.b: When the user associates rules with events, then the profile will automatically subscribe to the events.

Guideline 8.2.c: State-changes related to a user's terminals or services need to be communicated to the profile agent in an accurate and timely fashion.

8.3 References to objects

The user may refer to different types of objects such as terminals, communications, services, people, the time of day, the day of the week, etc. It is often convenient to group people and refer to the group e.g. friends, family, colleagues, customers etc. Further information on objects can be found in clause 7.6. Conditions in communication rules and security rules usually contains source (e.g. who is calling) and destination (e.g. who is called) objects, see table 1.

EXAMPLE: Alice wants to assign a special melody when someone in her family calls. That rule should always be active, so no additional conditions need to be defined. Alice has previously defined the group "Family" including her husband and two children. She has also previously defined the group "My phones". The rule may then refer to "Family" as communication source and "My phones" as destination as she wants that ring signal whatever phone she uses (given that the phone supports customized ring tones).

Table 1: The use of groups in rules

Rule Name	Source	Destination	Action
Family ring signal	Family	My phones	Ring signal is "I am sailing by Rod Stewart".

References to objects

Guideline 8.3.a: The profile tool should provide a rule editor that is well-integrated and objects should be easily referred to (e.g. direct manipulation).

Guideline 8.3.b: The user needs to be able to understand the consequences when there are any changes made to objects and they should be informed which rules are affected when objects are deleted or renamed.

Guideline 8.3.c: The user should be able to express and view objects in different ways.

When objects are deleted or renamed, the consequences in rules referring to them may be difficult to understand, especially as the effects may take place a long time afterwards. It is therefore necessary to let the user see a list of all rules referring to the deleted or renamed objects. The tool may propose different actions to take.

8.4 Rule building tool and rule base

8.4.1 Rule building tool

The definition of rules may be complex task. It is therefore necessary to provide the user with at rule building tool that helps the user achieve the intended outcome of the rules. The rule building tool is most likely to be tightly integrated into the tool described in clause 10.4, "Profile tool". Consequently, the guidelines provided in clause 10.4 would also apply to the rule building tool. Mechanisms to assist users in the task of creating and modifying rules should be provided. These would include pre-defined rules and rule templates, see also clause 9, "Default values and templates". Further information and guidelines related to the rule building tool is provided in the following clauses.

Rule building tool

Guideline 8.4.1.a: Rule building tools and engines should have a mechanism for testing rule changes before incorporating them.

Guideline 8.4.1.b: The user should be able to express and view the rules in different ways such as with words, filling in a table, filling in a form or graphically.

Guideline 8.4.1.c: The rule building tool should propose appropriate rules for the most common uses in rule templates and users should be given a mechanism to choose these templates.

8.4.2 Rule definition language

It is preferable that rules are entered in an intuitive graphical user interface, for example in a table, and they are internally translated to a rule definition language. Whereas most users would probably prefer an intuitive graphical user interface, an administrator managing a large number of profiles might prefer using the command line editor where the rules can be entered by using a rule definition language.

The rule definition language should be standardized (see clause 4.8, "Need for standardization") to allow profile portability which ensures that, when changing profile provider, users can bring their profiles and maintain the same behaviour. The actual syntax varies depending on the chosen language.

The rule definition language should have language extension capabilities and be syntax optimized for:

- parseability;
- human readability;
- non-redundancy.

8.4.3 Rule base

A rule base is an important part of the profile. It contains a set of rules and one rule may refer to other rules. As the rule-base may contain a large number of rules, referring to a large number of objects, the rule base may easily become very complex. It is thus important to provide a rule building tool that helps the user creating rules that ensures the desired outcome.

Rule base

Guideline 8.4.3.a: Users may define nested rules, that is, rules referring to other rules.

Guideline 8.4.3.b: Synchronization of the rule bases should be done when there are multiple rule bases and multiple profile providers.

8.4.4 Active and inactive rules

Rules may be active or inactive. Only active rules will be processed by the rule engine. Some rules need to always be active and could be defined in a base profile. Other rules are active only when the situation dependent profile with which they are associated is active.

Active and inactive rules

Guideline 8.4.4.a: Users should be given an option that lets them see which rules are active and which are not.

Guideline 8.4.4.b: Users should be given an option that lets them activate and deactivate rules where appropriate.

8.4.5 Rule exceptions

Users may define a rule and then define zero, one or several exceptions (circumstances where that rule does not apply).

EXAMPLE: Mark needed a "Meeting" profile to avoid being disturbed during meetings. However, he still wanted to be available for his most important customer Alice and his manager Peter. The primary rule contained in the first line in table 2 defines that, when he is at a meeting, he does not want to be disturbed. The following two lines define the exception rules (circumstances when he still wants to be reached).

Table 2: Rule exceptions

Name	Source	Destination	Action
Meeting	All	My Phones	Use my voice mail
Meeting exception	Alice	My Phones	Allow
Meeting exception	Peter	My Phones	Allow

When defining communication rules, most users would probably prefer most communications to be allowed, but may define rules that deny some communication. Some users such as victims who want to avoid threats may prefer that most communications are denied with only trusted communications being allowed.

Rule exceptions

Guideline 8.4.5.a: Users may define a rule and then define zero, one or several circumstances where that rule does not apply.

Guideline 8.4.5.b: One principle is to define what is allowed and then define one or several exceptions. The opposite principle is to define what should be denied and then define the exceptions. Users should be allowed to decide which principle they wish to be applied.

8.4.6 Prevention of conflicting rules and rule bases

Rule bases may contain conflicting rules, but this should be avoided. If conflicting rules are detected then the profile tool may propose to users one or more solutions from which they may choose. Synchronization of the rule bases is needed when there are multiple rule bases and multiple profile providers.

When users define rules or when objects referred to in rules are deleted or renamed, there is a risk that conflicting rules will be created or unexpected side-effects will occur such as:

- the specified action does not define the intended outcome;
- some rules will never be used and their actions will never happen due to the conditions being specified in such a way that they may never become true;
- a rule will inadvertently negate another rule.

The user will need support from the profile tool in preventing or solving conflicts and side-effects. The profile tool may for example:

- monitor activities to detect abnormal behaviour;
- propose strategies to avoid or correct problems;
- detect if rules have not been applied for a certain amount of time;
- provide an undo mechanism to allow users to revert to a situation before the problem occurred.

Prevention of conflicting rules and rule bases

Guideline 8.4.6.a: The profile agent should make a plausibility test to detect if there might be conflicting rules, even when more than one profile provider provides profiles for the user.

Guideline 8.4.6.b: If conflicting rules are detected then the profile tool may propose one or more solutions from which the user may choose.

9 Default values and templates

9.1 Creation of profiles

Templates that contain typical rules and settings will be of particular benefit in the initial configuration of profiles. First-time users could set up their profiles by using a wizard and templates. The wizard guides the user by explaining and proposing a set of templates that suit different group of users, roles and situations. These different types of templates may propose relevant settings and rules as default values. Users may decide to use the proposed default values or they may prefer choosing among alternative values.

The use of templates is useful as it is easier if information is already filled in as suggestions or default values as starting points and the user can choose to accept it or otherwise select available alternatives. A wizard could ask the user some questions in order to suggest templates that suit various categories of user in their different roles and situations.

9.2 Creation of templates

Templates may be provided by profile providers, service providers, device manufacturers, affinity groups, corporate and club administrators, and by the users themselves. It should be possible for users to create new templates by customizing existing ones.

When creating templates, the following will need to be considered:

- Which preferences, settings and rules can be assumed to be appropriate defaults for a target set of users, roles and situations. These default parameters should be acceptable to a maximum (such as "at least 90 %") of the target communities.
- Which default values could be set by values in the user's base profile (if specified in the base profile).
- The scope of application of a template and the granularity of information. The range is from a very detailed and comprehensive template for a very specific purpose to more general templates that apply to a wide variety of applications.
- Methods used for the creation and modification of templates.
- If a template needs to be a creation template or a live template (see clause 9.4).
- In what way changes to live templates will affect existing profiles that were based on these templates.
- What privacy issues need to be reflected in the templates.
- Which items in the template define things that the user can subsequently alter and which items will have fixed values.
- Which preferences and settings are related and may be grouped together.

Templates could be enhanced as a result of anonymous feedback from real usage of profiles derived from the template (e.g. if the template say the default value of <Setting X> is 5 but everyone using it has set the value to 10, then the value 10 will be set as a new default value. Users should be offered the option of not allowing the changes they make to their profiles to be used by the profile provider in enhancing templates.

Defaults and templates

Guideline 9.2.a: For first time definition of profiles, users should be provided with a ready-to-use profile containing relevant default values.

Guideline 9.2.b: Profile providers should provide templates that relate to a range of types of users and situations.

Guideline 9.2.c: The predefined default parameters in templates provided for users should be acceptable to a maximum (such as "at least 90 %") of the target communities.

Guideline 9.2.d: Users could be provided with a mechanism that allows them to create a new template by customizing an existing one.

Guideline 9.2.e: Users should be able to determine which settings have default values and which do not.

Guideline 9.2.f: If profile providers wish to obtain feedback on changes that users make to the defaults provided by a template, they should always ask the user's permission to obtain that feedback.

Guideline 9.2.g: Provide appropriate default values and allow the user to fine-tune these later if they wish to.

9.3 When defaults are not appropriate

There may be parameters for which defaults are not appropriate and where the profile agent will force the user to set their own value e.g. where it is legally required for the user to make an explicit decision for themselves. An example might be where a user should be asked to give permission for their personal medical history to be shared with a specified user or organisation (e.g. a hospital). When prompting the user for a value, the profile agent may:

- request explicit user input;
- propose a range of options from which the user will have to chose one;
- propose a value to accept or reject and give the user a mechanism to specify an alternative value if they reject the proposed value.

If there is any doubt that the user's action is an explicit choice or accept/reject action, then the legal status of the choice made may be questionable (e.g. tick-boxes presented at the end of a large amount of written information may not be acceptable proof of an explicit decision).

When defaults are not appropriate

Guideline 9.3.a: Where there is a potential legal liability related to a user choice or value, a default should not be used and the user should be asked to make an explicit decision about that choice or value.

9.4 Live and creation templates

There are two types of templates:

- creation templates, where modifications made to them will not affect any rules, settings or profiles that were previously created from those templates;
- live templates, where modifications made to them will affect all rules, settings or profiles that are created from those templates. This could be of benefit in a corporate environment where a company wished to make changes to all of its profiles as a result of a corporate change of policy.

Live templates and creation templates

Guideline 9.4.a: When a change is made to a live template, users of profiles derived from that template should be informed that changes have been made and they should be able to discover what those changes are.

Guideline 9.4.b: Subsequent updates of settings resulting from changes to a live template or from updates issued by the profile provider should form the default entries for profile resets.

9.5 Privacy

Templates provide an excellent opportunity to support users in controlling their privacy. Templates can have many default settings related to privacy that will avoid the user needing to understand the often complicated details related to the detailed management of their privacy. Guidelines on the many privacy related issues are presented in clause 13.

9.6 Inheritance

Some commonly used settings such as privacy settings may be defined in live templates. Other templates and profiles could then be built on these extracted parts contained within a live template. The user would then only have to change these settings once in the live template and have these preferences propagated to all templates and profiles derived from that live template. Where templates are organized in a hierarchical way (see clause 4.1.1) the lower level templates can inherit profile data from the higher-level templates.

9.7 Templates for different types of users and situations

9.7.1 Adult

Templates proposed to the independent adult would typically relate to their different roles and situations within their roles. User will be guided how to define activation criteria for each of the situation dependent profile related to the situations listed below. A scenario illustrating activation and use of similar profiles is explained in clause 6.1 "A typical working day".

A user in the private role might need templates appropriate for the following situations:

- **Home template** could propose diverting calls to private fixed line phone. The wizard could ask if the user wishes to define settings related to the management of a smart home.
- **Out template** could propose diverting calls to private mobile phone.
- **Driving template** could propose diverting calls to the car handsfree. The wizard could ask if the user wishes to define settings related to the management of an intelligent car.
- **Unavailable template** could propose diverting calls to private voice mail. The wizard could ask if the user wishes to define exceptions, for instance a list of people (e.g. family and certain friends) who would be able to contact the user.

A wizard could ask users if they are working, and if so propose profiles appropriate to situations in the working role. Corporate administrators may also find Work profiles useful and might also need a wizard and templates for security management and rules for restriction of outgoing calls such as pay services and international calls.

A user in the professional role might need templates appropriate for the following situations:

- **Office template** could propose diverting all calls to work fixed line phone. Let private calls be diverted to voice mail and professional calls be diverted to work fixed line phone.
- **Out template** could propose diverting calls to work mobile phone.
- **Unavailable/meeting template** could propose diverting calls to work voice mail. The wizard could ask if the user wishes to define exceptions, for instance a list of people (e.g. boss and family) who would be able to contact the user.

9.7.2 Companies

Predefined templates for different sizes and types of companies may be available for company profile administrators. There could be predefined templates using an appropriate vocabulary for different sizes and types of companies.

Benefits when using templates:

- templates that can be applied to many employees at the same time;
- modification to a live template will affect all employees profiles created from this live template;
- the company's security policy and communication policy can easily be defined in company templates.

9.7.3 Clubs and affinity groups

Predefined templates for different sizes and types of clubs and affinity groups may be available for club or group profile administrators. There could be predefined templates using an appropriate vocabulary for different types of clubs or groups.

Benefits when using templates:

- templates that can be applied to many club or group members at the same time;
- modification to a live template will affect all member profiles created from this live template;

- club security policy and communication policy can easily be defined in club templates.

9.7.4 Accessibility templates

The need for access to ICT is increasing - we are rapidly moving towards an e-society. However, there is a risk that many new ICT technologies may exclude large groups of consumers from participating fully in this e-society. Furthermore, as the population of Europe is ageing it is important not to exclude this growing population who may suffer from age related impairments and disabilities. Templates are useful for improving conditions and services for these groups. Doctors or affinity organizations could propose suitable templates depending on the user's needs.

Users could choose among templates proposing needs and preferences suitable for the following three basic categories:

- sensory needs and preferences (sight, hearing, touch, taste/smell, balance);
- physical needs and preferences (speech, dexterity, manipulation, mobility, strength/endurance);
- cognitive needs and preferences (intellect, memory, language/literacy).

Characteristics of these disabilities and their relationship with ICT devices and services are described in [15].

9.7.5 Child template

Parents (see clause 5.2.4.1, "Parent - Child relationships") have many ICT related concerns, including protecting their children from potentially dangerous people, limiting their access to certain content, monitoring their location, exercising some control over their use of costly commercial services or content, and security of family related confidential information (see [16]).

In many families, parents to young children or teenagers will define their children's profiles. Parents may want to limit the ways in which their children can modify their profiles. A scenario illustrating how parents set up a profile for their child is explained in clause 6.2, "Initial profile set-up for a child".

Issues that need to be dealt with when creating templates for children:

- How much information the parents should be able to get about their children's communications and location.
- Abilities and requirements depending on age:
  - how children's profiles could adapt to children's social, cognitive and physical development;
  - step by step development.
- The need for manual activation of profiles should be minimized.
- Settings for fun such as child adapted ring tones.

9.7.5.1 Settings and preferences proposed in child templates

Settings and preferences proposed in child templates could reflect the issues described below (including but not limited to):

Privileges related to children:

- Children have no privilege to use the profile tool, and therefore they are unable to modify their templates.
- Children have read privilege but no delete privilege for their log tool.
- Children have limited privileges to update their contact book.
- Children may activate profiles, if the parents give their child this privilege.

Privileges related to parents:

- Parents have full privileges to use the profile tool.

- Parents may be interested in their children's log data.
- Parents have full privileges to use and update the child's contact book.

Content filtering:

- Profiles could provide content limitations. The profile may contain the child's age or other data entered by parents that could be used for filtering services or access control, allowing only suitable content.

Communications:

- Communication profiles such as "Home" and "Out" could be similar to those described in clause 9.7.1.
- Outgoing call options may be limited, to one or more of the following alternatives:
  - calls to a list of allowed contact book entries (e.g. parents, grand parents, neighbours and some friends);
  - only local calls are permitted;
  - no calls to special and/or expensive categories services are permitted;
  - no calls to individually specified services are permitted;
  - outgoing call limitations may depend on communication costs so that there will be more restrictions on calls from a mobile phone than from a fixed phone.

10 Set-up and maintenance of profiles

10.1 Who can create and update profiles?

Profiles may be created or updated by the users themselves or by profile providers. Third party services may update profiles on behalf of the users or assist them if problems occur. Profiles that are related to specific services may be updated by the service provider.

10.2 Who initiates profile updates?

Profile operations may be initiated on users' initiative or as a result of the profile agent proposing updates due to changes in the environment (e.g. new services or service features, new devices or accessories). The profile agent should be notified when changes occur to the environment so that the profile tool may propose suitable profile updates.

10.3 Scope of profile data values

Users may define different values of their profile data that suits various situations. Support should be provided to allow users to define generic values for profile data elements and methods that will allow them to define other values that are specific to particular scopes.

In specifying the scope of the profile data values, users should be able to make use of pre-defined contexts or define contexts that cover devices, services and situations. The scopes may make reference to specific objects such as "my work mobile phone" or classes of objects such as "my telephony services".

These scopes can include the following:

- roles e.g. for my private role, name = my nickname;
- services e.g. for my home e-mail, store messages in the "Personal" folder;
- devices e.g. for my home phone, volume = medium;
- groups of services/devices e.g. for all my telephony services, ring tone from "family" = Tune A;

- locations e.g. at work, role = business;
- situation e.g. for meeting, alerting mode = vibrate;
- environment e.g. for noisy environment, volume = maximum.

Scope of profile data values

Guideline 10.3.a: Users should be able to select or define the scope of their profile data values.

10.4 Profile tool

10.4.1 Design for All approach

A profile tool is used to view, create and modify profiles. The requirements of a profile tool depend on if it is intended to be used for managing single user private profiles or managing profiles for a great number of persons for example a corporate profile administrator managing profiles for employees at a company. The present document is focusing on profile tools intended for users managing their own profiles or on behalf of someone else such as parents managing their children's profiles.

The user requirements of the profile tool depend on the user's preferences and abilities, the tasks to perform, the available terminal and the environment. A "Design for All" approach is encouraged (see [15], clause 4.3 "Design For All") so as to make the profile tool accessible to as many people as possible, including elderly people and persons with disabilities, without the need for adaptation or specialized design. In practice adopting the "Design for All" approach means considering the needs and requirements of people at the ends of the population continuum rather than just those in the middle. The "Design for All" approach is summarized by the following seven basic principles (identified by the Center for Universal Design at North Carolina State University [19]):

1) **Equitable use:** The design is useful and marketable to people with diverse abilities.
2) **Flexibility in use:** The design accommodates a wide range of individual preferences and abilities.
3) **Simple and intuitive use:** Use of the design is easy to understand, regardless of the user's experience, knowledge, language skills or current concentration level.
4) **Perceptible information:** The design communicates necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities.
5) **Tolerance for error:** The design minimizes hazards and the adverse consequences of accidental or unintended actions.
6) **Low physical effort:** The design can be used efficiently and comfortably and with a minimum of fatigue.
7) **Size and space for approach and use:** Appropriate size and space is provided for approach, reach, manipulation and use, regardless of the user's body size, posture or mobility.

NOTE: Copyright © 1997 NC State University, The Center for Universal Design [19].

As users do probably not manage their profiles every day, the profile tool need to be designed to minimise the users' memory load. Users should not be expected to enter information manually. Information should, where possible, be automatically retrieved in other applications and used transparently in profile tools. It is better to choose among relevant alternatives in a menu instead of having to type it manually. Profile tools should be easy to use and too much complexity should be avoided.

A guided configuration process (see clause 10.9.2) proposing templates (see clause 9) will help users configuring their profiles. Provision of defaults for many preferences in a user's profile will help to minimize the amount of profile configuration that the user will be required to do. The user will always be able to fine-tune the values set as defaults at a later time if they wish to. Where users are required to or wish to enter information, they can be helped by being given examples of the correct format for the required preferences and support for handling the formats. Also the profile tool can prevent or help the user avoid incorrect input of entries.

Users will expect to see information in the profile tool in their own language, e.g. non-English speaking users should not have to learn English to be able to use the profile tool. Ensuring that the user gets the correct language can be achieved by inspecting the user's own profile data to see if it contains a language preference. Where this is not available it should be easy for the user to select the correct language from a set of languages when first using the tool. As well as using the correct language, it is also important to consider that first-time users will be unfamiliar with technical terminology so that a mechanism that allows users to see synonyms for the terms should be provided where possible.

It is important that the terminology used should be consistent across all profile tools. It is unlikely that the user will have sufficient knowledge to be able to decipher and translate between different terms that denote the same concept, in order to be able to configure the preferences correctly. Language and terminology issues and guidelines are further provided in clause 10.4.6.

Profile tool in a "Design for All" approach

Goal 10.4.1.a: A "Design for All" approach is encouraged so as to make the profile tool accessible to as many people as possible, including elderly people and persons with disabilities, without the need for adaptation or specialized design.

Guideline 10.4.1.b: The profile tool should provide equitable use - The design must be useful and marketable to any group of users - avoiding segregation or stigmatization of any users.

Guideline 10.4.1.c: The profile tool should be flexible in use - The design must accommodate a wide range of individual preferences and abilities.

Guideline 10.4.1.d: The profile tool should be simple and intuitive to use - The design must be easy to use and understand, regardless of the user's experience, knowledge, skills or concentration level.

Guideline 10.4.1.e: The profile tool should provide perceivable information - The design must communicate necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities.

Guideline 10.4.1.f: The profile tool should support tolerance for error - The design must minimize hazards and the adverse consequences of accidental or unintended actions.

Guideline 10.4.1.g: The profile tool should demand only low physical effort - The design must be usable efficiently and comfortably and with minimum fatigue.

Guideline 10.4.1.h: The profile tool should provide size and space for approach and use - Appropriate size and space must be provided for approach, reach, manipulation and use, regardless of the user's body size, posture or mobility.

Guideline 10.4.1.i: Where the user's profile contains information on personal user interface related preferences and settings, these can be used by the profile tool to configure its own settings.

Guideline 10.4.1.j: It should be possible to export and import some personal settings of the profile tools such as preferred language, accessibility settings, notification settings, user defined use of icons, log settings. This is useful, for example, when changing profile provider.

Information about profile data

Guideline 10.4.1.k: Users should be informed about what profile data need to be configured and what effect configuring these will have.

Guideline 10.4.1.l: Users should be given examples of the correct format for the required profile data and support for handling the formats.

10.4.2 Various versions of profile tool

Users should have a maximum of choices concerning the use of profile tools. All users should be able to install, uninstall and upgrade their profile tools. A user can have different versions, on different terminals of the profile tool that are synchronised. If an older revision of a profile tool is used, it should not be able to change profile data known only to newer tool revisions. If a newer revision of a profile tool exists, the user can be encouraged to download and install that newer version.

The user should be able to install and run different versions of a profile tool:

- from any terminal (e.g. PC, PDA, mobile phone, fix phone);
- on different operating systems;
- as a web application or installed on the terminal;
- using any browser (e.g. Internet Explorer, Firefox, WAP browser);
- using a graphical user interface, voice command interface or a human being;
- using preferred language;
- for use by private profile administrators;
- for use by corporate profile administrators.

Various versions of profile tool

Goal 10.4.2.a: Users should have a maximum of choices concerning the use of profile tool.

10.4.3 Available in various terminals

Various terminals may be used for managing profiles. Different types of terminals are more or less suitable for different tasks depending on terminal capabilities and user interfaces. Devices and services may provide a mechanism that allows the user to view or edit the profile data that relates to that device or service, or even offer the ability to read and edit other discovered profile elements on other devices or services.

An important difference between terminals is if there is a screen or not and the size of the screen:

- **Full screen:** Full screen user interfaces such as a PC are suitable for activation/deactivation of profiles and for managing profiles.
- **Small display:** The profile tool offers a user interface for small displays (e.g. of a mobile phone). It can be used for activation/deactivation of profiles and for managing profiles. Many users may prefer the use of icons as they demand less space than words.
- **No display:** Terminals without display such as fix line phones can be used for activating and deactivating profiles. Most users would find them less suitable for managing profiles, although spoken menus and the use of 12-key pad could be used. Users may also ask third party services to manage their profiles.

It would be beneficial to users if they can associate icons to different objects such as profiles, persons, groups, times, activities, places etc. It would also be beneficial if they can choose among three presentation modes: only icon, icon and name and only name. Users would benefit from options that allow them to set the presentation mode settings generally, per object type or specific object or attribute.

Tool available in various terminals

Goal 10.4.3.a: All terminals can be used for activation and deactivation of profiles.

Guideline 10.4.3.b: Alternative interfaces should be available for managing profiles such as display, spoken menus, 12-key keypad.

Guideline 10.4.3.c: Within any type of interface, users should, where feasible, be able to choose between a range of alternative presentation modes (e.g. text or icon).

Guideline 10.4.3.d: Profile providers could offer their services or third party services for managing profiles.

10.4.4 Online profile management

Users may manage their profiles while being online with their profile agent. The advantage is that the profile tool would be able to give the most up to date view of the profile data and the environment including devices and services related to their profiles. The feedback to the user would be immediate so as the effects of the profile updates.

10.4.5 Offline profile management

Users may use their profile tool while they are offline. It is recommended that the local profile data is synchronised before using the tool offline, to minimise the risk of managing data that differs from the online (master) version. The profile tool should indicate offline mode and that the local and the online version of the profile data may differ.

After changing the local version of profiles, it will be necessary to go online and upload the modifications to the appropriate profile agent. The user should be warned about possible inconsistencies if the synchronization has not yet been done, or if any of their changes are incompatible with their current services.

Offline profile management

Guideline 10.4.5.a: The profile tool should make it clear to the user whether they are using their profile tool online or offline.

Guideline 10.4.5.b: If users are updating their profiles offline, the profile tool should inform them about the risk that data in the profile tool might not be up to date.

Guideline 10.4.5.c: If users are using their profile tool offline, the profile tool should inform them that updates to the profile will not be verified by the profile agent until they go online and make the updates available to their profile agent.

Guideline 10.4.5.d: If users are updating their profiles offline, the profile tool should inform them that the outcome of their updates may not produce the intended outcome until they go online and make the updates available to their profile agent.

Guideline 10.4.5.e: If users have been updating their profile tool offline, the profile tool should ask them the next time they go online if they wish to make the updated profile data available to their profile agent.

10.4.6 Language and vocabulary

The tool's user interfaces will need to be localized for the language of the different national groups of users. However, whatever language is used, it is important to use a vocabulary within that language which is familiar and acceptable to the user. Different groups of users may require the same concepts described in different terms according to their experience and understanding. For example, a profile administrator managing multiple users may wish to see the rules that control how a user's communications behave as "rule" objects, whereas the ordinary user may only be aware of these rules in terms of the communication outcomes that are required.

The vocabulary used in the profile tool's user interface should be consistent whether used as written or spoken text, and when used in different versions of the profile tools. Consistent terminology in the profile tool is also needed for ensuring the expected user experience when moving from one profile provider to another. The vocabulary used should be appropriate to the intended target audience. "Wizards" should follow real-world conventions, making information appear in a natural and logical order and use words, phrases and concepts familiar to the user, rather than system-oriented terms.

Language and vocabulary

Goal 10.4.6.a: The profile tools should offer different end user views of the basic profile management functionality that are tailored to the knowledge and experience of the specific groups of users. The vocabulary used should be appropriate to the specific group of users.

Goal 10.4.6.b: A set of user terms, symbols and icons, covering at least a set of key objects (such as listed in clause 7.6, "Overview of a selection of profile objects") should be defined. User terms for at least the major European languages should be standardized.

Goal 10.4.6.c: Where necessary, provide explanations of terminology and concepts that need to be understood by the user.
Goal 10.4.6.d: Terminology and technical concepts that the user does not need to understand should be avoided.

Goal 10.4.6.e: The vocabulary used in profile tool user interfaces should be consistent whether used as written or spoken text, and when used in different profile tools and different terminals.
Goal 10.4.6.f: All tools and services involved in profile management should exhibit the same behaviour in relation to the key profile concepts represented by the user terms, symbols and icons (including at least those listed in clause 7.6 "Overview of a selection of profile objects").

Guideline 10.4.6.g: Users should be able to access their profile information and profile tools in a selectable language.

Guideline 10.4.6.h: The profile tool should determine its initial default language setting from language preferences contained in the user's profile if this preference exists.

10.5 Creation

10.5.1 Starting values

Start values of objects in a profile can be predefined (defaults) and/or set in templates (see clause 9, "Default values and templates"). This can be compared to the situation when a newly purchased mobile phone already contains pre-set values.

Users may also use wizards (see clause 10.9.2 "Guided configuration") that propose defaults and help the users define their own starting values. Profile providers could provide some profile information as start values when users first use or open a new service or device, such as:

- user's name;
- terminals;
- services;
- accessibility settings;
- localization settings, preferred language;
- security settings, electronic signature;

set of predefined profiles templates suiting different roles and situations such as work, spare time, out.

Starting values

Guideline 10.5.1.a: The profile should self-populate with the most appropriate default values for user privacy and security.

Guideline 10.5.1.b: A new profile element should self-populate with matching information in the base profile, when available.

10.5.2 Linking services and devices with existing settings and preferences

When users have been using devices or services for a while, before linking them to their profiles, data will already be set in those devices or services. For each settable data item, the user will be given options how that data will be handled:

- which data should be linked to the profile agent;
- in which direction synchronization of service/device values should be provided (service/device to profile or profile to service/device).

10.5.3 Base profile creation

A base profile (see clause 4.2.1) is created and instantiated when the user purchases or gets a profile service and can be updated by the user at any time.

10.5.4 Situation dependent profile creation

When purchasing the profile service, the profile provider offers a profile tool containing a wizard for creating their first set of profiles. It proposes templates with options that suit different lifestyles and situations from which the user may choose (see clause 9). These templates contain default settings and activation rules that users may modify in order to adapt them to their personal needs and situations. Third party services may also offer an initial set of profiles.

10.5.5 Device profile creation

New devices will be delivered with predefined settings in a pre-set device profile. Some of the default values are more or less globally used whereas some, such as predefined language, depend on where the mobile phone is purchased. When a user's profile specifies a language preference, the preferred behaviour could be to set the language setting in the mobile phone to the one specified in the profile. This capability might be useful for people living abroad who purchase a mobile phone locally.

The device profile may be instantiated with data from users' settings related to a similar device (see scenario in clause 6.3) and also with data from their base profile (such as high audio volume, large text or contact book entries). While the device may have some level of basic connectivity before first use (for requirements such as emergency calling), a current example of "profile creation" is the addition of a user's existing SIM card into a new cell phone.

Device profile creation

Guideline 10.5.5.a: In the case of first time use of a replacement device, the new device should be able to take advantage of the user's settings (which are contained within a profile) for the prior device, or other devices.

Guideline 10.5.5.b: Always start with the option to explain fully each information field required for device-specific settings.

10.5.6 Service profile creation

A new service will have predefined settings in an initial, pre-set service profile. This service profile may be instantiated with data from the user's settings related to a similar service and also with data from their base profile.

Service profile creation

Guideline 10.5.6.a: In the case of first time use of a replacement service, the new service should be able to take advantage of the user's settings (which are contained within a profile) for the prior service, or other services.

Guideline 10.5.6.b: Always start with the option to explain fully each information field required for service-specific settings.

10.6 Update

Profiles need to be updated regularly to adapt to new services, terminals, accessories and user preferences. Some updates will be made directly by the user. Non-user initiated updates may need to occur immediately after a change is notified to the profile agent, after which the user may also be notified of the change. For other updates, the user may need to confirm that they wish the update to take place before the update is made.

Updating profile data may result in unwanted consequences if other profile data refers to it. It is therefore necessary to let the user see a list of all profile data referring to the updated profile data. The tool may propose different actions to take.

Update notification and confirmation

Guideline 10.6.a: For each object in a profile, the user should be able to select whether they wish to receive notification of any updates made to that object.

Guideline 10.6.b: For each object in a profile, the user should be able to select whether they wish to receive a request for update before they confirm that they wish the update to the object to be made.

Guideline 10.6.c: The user should be provided a list of all profile data referring to the updated profile data. The tool may propose different actions to take to resolve any potentially unwanted consequences.

Update operations include:

- updating data to the base profile;
- updating situation dependent profiles e.g. an update to a "School" profile will be needed when a child changes school and many details including the school location will need to be updated;
- update to device profiles e.g. updating a device profile when a new accessory that might be addressed in an activation rule is added;
- updating a service profile e.g. updating the service profile when the service is used with another device.

Updates to devices or services could be made using the profile tool in the device or service or by using a profile tool that allows any profile data to be updated.

10.7 Deletion

10.7.1 Profile data deletion

From an operational point of view there should always be a copy of the profile, even when it is wholly or partially deleted. Users would be able to recreate a profile similar to the deleted profile by recovering the copy of the deleted profile and updating it as necessary. This will also prevent the user from losing functionality if problems are encountered after deletion. There can also be situations where users may want all the profile information deleted. In those cases that information must be deleted and no backup copy should be maintained.

Deletion of profile data may result in be unwanted consequences if other profile data refers to the deleted data. It is therefore necessary to let the user see a list of all profile data referring to the deleted profile data. The tool may propose different actions to take.

Deletion

Guideline 10.7.1.a: When a profile is wholly or partially deleted, a copy of the original profile should be kept in a place that allows future reuse of that profile.
Guideline 10.7.1.b: Users should be provided with a mechanism that allows them to permanently delete stored copies of deleted profiles.

Guideline 10.7.1.c: The user should be provided a list of all profile data referring to the deleted profile data. The tool may propose different actions to take, to avoid any unwanted consequences.

Guideline 10.7.1.d: When deleting a profile object, the user should be informed about which other objects and profiles that might be affected.

10.7.2 Base profile deletion

The base profile should not be deleted unless the user decides to stop using the profile service. The minimum information (the user's name etc.) will normally be deleted by the profile provider.

Base profile deletion

Guideline 10.7.2.a: The base profile should not be deleted unless the user decides to stop using the profile service. The minimum information (the user's name etc.) will normally be deleted by the profile provider.

10.7.3 Situation dependent profile deletion

A situation dependent profile can be deleted by the user at any time. Deleting a situation depended profile will have the following results:

- the reference to the profile (e.g. its name) will be deleted;
- the profile tool will ask the user whether to keep the activation rule or delete it. The user may want to keep it for future use as it might be useful for activating another situation dependent profile;
- objects referred to by the profile may still be set to values in other profiles, so these objects will not be deleted.

Situation dependent profile deletion

Goal 10.7.3.a: A situation dependent profile can be deleted by the user at any time.

Guideline 10.7.3.b: When a situation dependent profile is deleted, the objects referred to by the profile should not be deleted.

10.7.4 Device profile deletion

Device profiles will not be deleted from the devices, but they may be made unavailable from the profile tool.

Device profile deletion

Goal 10.7.4.a: Device profiles will not be deleted from the devices, but they may be made unavailable from the profile tool.

10.7.5 Service profile deletion

The service profiles will not be deleted from the services, but they may be made unavailable from the profile tool.

Service profile deletion

Goal 10.7.5.a: The service profiles will not be deleted from the services, but they may be made unavailable from the profile tool.

10.8 Information acquisition

In order to offer personalized services and devices, information on the user needs to be gathered. Profiles are usually composed and managed at the start and/or in the course of using the services and devices.

This information may be acquired by asking the user to provide information, or by tracking the user's actions and choices when using services or devices. The key to a successful profile implementation is to gather a user's personal information in ways that are acceptable to users.

Many different aspects play a role in how information should be gathered, such as:

- user tasks;
- generic or specific preferences;
- privacy;
- context of use such as location, time, used devices/accessories/services;
- initiative (whether the information acquisition is initiated by the user or profile agent);
- content selections.

The different methods for gathering user information may be more suitable in some situations and less suitable in others. When a user is first supplied with a profile, it is important that appropriate initial defaults are provided for all of the settings in that profile, Following that, there are two major mechanisms for applying personalization to a service or device; explicit or implicit.

10.8.1 Explicit methods

The user of the service/device actively defines the settings of the service. They may be asked to actively provide information by filling in questionnaires and online forms.

Users should be able to set personal preferences by answering questions or selecting options, but in practice, unless there is a well-understood benefit, few users invest much effort in setting preferences.

Examples of methods for explicit collection of preferences:

- creating a list of settings/items that the user likes;
- creating a list of settings/items that the user dislikes;
- users ranking a collection of settings/items from favourite to least favourite;
- users choosing the preferred setting/item out of two or more settings/items.

Explicit methods

Goal 10.8.1.a: Keep customization quick and easy to set up.

Guideline 10.8.1.b: Invite the user to customize their profile, and outline the advantages of doing so.

10.8.2 Implicit methods - adaptive personalization

Implicit methods, also referred to as adaptive personalization, are mechanisms that more or less continuously adapt profile data to match user requirements that have been inferred as a result of continuously monitoring user behaviour. Adaptive profile agents can relieve users of the burden of personalizing their profiles and so may overcome the limitations of explicit methods of customization. Whether adaptive personalization is seen as a pure benefit to a user or a violation of their freedom and privacy will depend largely on why the user's behaviour is being monitored, and what control the user has over what is done as a result of the behaviour monitoring.

Systems that create a profile related to a user and make inferences about a user's preferences and that do not offer the user opportunities to inspect, modify or reject these inferences are considered to be examples of "user profiling" and are, as stated in clause 1 of the present document, outside the scope of User Profile Management. Frequently, commercial services use such "user profiling" techniques with the primary aim of enhancing their selling opportunities. Whereas such systems may well be seen by users to benefit to them, the lack of ownership and control of the profile data by the user means that they will not be subject to all of the requirements specified in the present document.

Where the user is able to observe and control the way in which adaptive personalization is used to modify their profile, adaptive personalization can minimize the frequency with which the user needs to explicitly modify their profile. A common way in which adaptive personalization can be implemented is by means of recommender systems.

Recommender systems attempt to predict users' needs and recommend helpful suggestions which, if the user agrees, would result in a change to the user's profile. For example, a recommender system might, at midday, recommend that "you may wish to read your email", as the profile agent has noticed that the user has read email by that time on all other days.

Other examples of implicit collection of preferences include:

- Suggesting a list of internet sites that the user may wish to place at the top of their listing of favourite internet sites.

- Suggesting a good time to telephone one of the user's contacts based upon an analysis of previous successful and unsuccessful calls to that contact.

As well as basing recommendations on the behaviour of a single user, recommender systems may also make use of information on how groups of users behave. For example, a recommender system might suggest to a blind user having trouble booking a hotel over the internet that they might try a hotel booking web site that has been shown, from previous observation of other blind users, to be very easy for blind users to navigate. Such techniques are frequently referred to as collaborative filtering or social filtering. This technique is useful for recommending options on which the specific user has not (yet) expressed any personal opinion or where no previous behaviour can be used for making inferences.

In some circumstances (e.g. when configuring profiles for very young children), users can take part in tests that will be used for defining users' levels and abilities. However, it is important to be aware of exactly what is being tested. It is important to separate different tests such as cognitive test, motor skills and colour blindness, to ensure that the tester knows what is tested. For example, someone might use an educational game where the child plays a game of catching letters that are falling down a computer screen to evaluate letter recognition skills. However, the test might conclude that a child that does poorly in the test has poor letter recognition skills when it may just be that their motor skills are not well developed. It is clearly necessary to be careful what the test is measuring; the letter recognition or motor skills.

Pros of implicit methods:

- Relieve users of the burden of personalizing services and devices.

Cons of implicit methods:

- Good human-factors practice is to expect computer interfaces to be more-or-less predictable. There is a risk that a system which suddenly or autonomously changes may be confusing and inconsistent. Consistency is one important goal and adaptive systems do not fully follow that principle.

- Users have to learn a new interfaces and system behaviour.

- There is often a significant cost associated with the implementation of adaptive systems, and this cost would need to be justified.

- Adaptive personalisation tends to have a connotation of "Big Brother is watching you". This impression largely relates to "user profiling", which is outside the scope of the present document. For this reason users may wish to turn adaptive personalisation off.

- The system may misunderstand the user's wishes. This could occur when the user is doing something on behalf of someone else or when another person is using one of the user's devices.

Implicit methods - adaptive personalization

Goal 10.8.2.a: Customizing the interface based on the user's role or subject area can save their time and produce results more closely matching their needs. It is important to be careful not to antagonise users by making incorrect assumptions.

Guideline 10.8.2.b: Users should be able to turn adaptive personalization off.

Guideline 10.8.2.c: Users should be able to be informed about the acquired information, assumptions and changes made when implicit methods are used and have the opportunity to allow, deny or override them.

Guideline 10.8.2.d: Where implicit methods are used, it is necessary to identify the user before collecting behaviour information, not make assumptions based on the use of a specific terminal, as more than one person may use the same terminal.

Guideline 10.8.2.e: The profile agent should explain the advantages of personalization for enhancing the user experience.

Guideline 10.8.2.f: Users should be allowed an option as to whether or not they wish to be made aware that an implicit method has made an assumption about their user preferences. They should also be offered the option about whether or not they wish to confirm the assumption. The user should be allowed to change the options that they have selected at any time.

Guideline 10.8.2.g: Automatic personalization should be avoided unless it can consistently and accurately match users' needs and expectations.

Guideline 10.8.2.h: Users should be able to define if preferences that are explicitly set may or may not be updated by implicit methods.

Guideline 10.8.2.i: Profile agents must limit their implicit data collection to user actions completely within their own scope.

10.8.3 Combination of implicit and explicit methods

Combining explicit and implicit methods can be highly beneficial for users. The profile tool, or another application that communicates with the profile tool, will continually search for patterns in the user's behaviour. When a pattern is detected, the user would be asked an explicit question to check the assumptions made about the user. Alternatively, the profile tool may initially ask users to provide information (explicit method), and then update this information based on patterns in the user's subsequent behaviour (implicit method). The profile agent should avoid asking users questions while they are actively engaged in other tasks.

Combination of implicit and explicit methods

Guideline 10.8.3.a: Users should not be asked to enter information that can be acquired by the profile agent from other sources.

Guideline 10.8.3.b: A well-designed profile agent needs to limit the effort required from users in defining their profiles.

10.9 Configuration methods

The types of configuration methods (also described in [17]) referred to in the present document, in increasing order of user involvement, are:

- pre-configuration;
- guided configuration;
- manual configuration.

In addition to information being pre-configured into the profile or entered by the user, as described in this clause, implicit methods may be used to provide profile information. The implicit methods of updating profiles can be found in clause 10.8.

Before the configuration, users may need to authenticate themselves when changing from the user role to administrator role (see clause 5.1, "User and administrator roles"). At the end of the configuration, the user should be reminded to change back to the user role.

10.9.1 Pre-configuration

Pre-configuration provides a useful starting point before further personalization. A description of what may be set up and guidelines relating to pre-configuration can be found in clause 9 on default values and templates and clause 10.5.1 on starting values.

It can be assumed that pre-configuration of profiles related to services and devices will remove a barrier that may inhibit usage. An example of this from the field of mobile communications was the increased uptake of SMS that resulted from the pre-configuration on the SIM card of the SMS Centre phone number, which previously had to be entered manually by users.

If pre-configuration cannot be achieved, some means for guided and/or manual configuration should be provided.

10.9.2 Guided configuration

If pre-configuration cannot be achieved or if the user wishes to further personalize their profiles, some means of guided configuration should be provided, taking into consideration the needs of all users (including young, elderly or disabled users, see clause 10.4.1. For example, users with visual or motor impairments would benefit from a web site or software on a PC that could offer speech input/output, or simply the larger keyboard and display for better text input/output capabilities.

The user may be required to walk through a sequence of instructions and choices, and to input certain entries. Based on the user's input, the profile will then be automatically configured. An example of guided configuration is the use of a setup wizard (see for example the scenario in clause 6.2). Templates (see clause 9) will usually define which parts of the profile are pre-set as defaults and which require responses from the user in the guided configuration process.

Guided Configuration

Goal 10.9.2.a: There should be a balance between the number of steps and the complexity within each step. Any additional number of steps or complexity within each step introduces the potential for errors.

Guideline 10.9.2.b: Users should be informed about what information they need to have ready to hand during the configuration procedure, and if necessary, how to obtain it.

Guideline 10.9.2.c: There should be a clear overview of the steps of the configuration sequence.

Guideline 10.9.2.d: The user should be presented with information about the progress of the configuration.

Guideline 10.9.2.e: Provide a logical and consistent order of the configuration steps. For instance, group together related settings and preferences.

Guideline 10.9.2.f: Navigation should be under user control throughout the configuration. There should be no time-outs that automatically continue to the next configuration step.

Guideline 10.9.2.g: "Back", "next", "cancel", and "finish" as well as "help" functionality and controls should be provided. The "cancel" and "help" controls are especially important when the user is not able to proceed for whatever reason.

Guideline 10.9.2.h: At each step of the configuration the user should receive clear instructions about what type of information is required, i.e. what input information is expected from the user. Illustrative examples could be provided.

Guideline 10.9.2.i: The user should receive clear feedback when the configuration procedure ends.

Guideline 10.9.2.j: If the configuration fails or is aborted the state of the profile should revert to previous step of the configuration, i.e. no preferences and settings within the aborted step should be modified. In some cases, it may be necessary to revert to where the configuration started. The user should be informed on how to proceed in order to complete the configuration.

10.9.3 Manual configuration

Users may configure their profiles by manually entering profile data. Manual configuration is initiated by the user who actively decides which profile data to update and in which order (within certain limits). Manual configuration is not done in a context determined by any guided configuration procedure. However, the user interface should provide information related to the particular profile data they are about to define or update.

10.10 Data storage, synchronization and back-up

10.10.1 Storage

User preferences should be stored in profiles on the server and handled by the storage agent, see clause 4.6.2. Users should be able to assume that storage of data is working correctly and no user activity is required. Users should be able to rely on automatic handling of:

- backup of different data;
- synchronization;
- data consistency.

10.10.2 Synchronization

The overall user requirement for synchronization is to have all profile data up-to-date, wherever the data was entered and wherever it is stored. If the format of stored data varies between storage locations, the synchronization mechanism in the storage agent should be able to handle this to ensure data consistency. The storage agent should be able to remember previously synchronized versions of their profiles data. Through a user interface or their profile tool, users should be able to select profile data they want to be synchronized.

Synchronization of data has been described in clauses 4.6.2, "Storage agent and components", 10.5.2, "Linking services and devices with existing settings and preferences" and 10.4.5, "Offline profile management".

10.10.3 Revision handling and undo functionality

The user should be able to make changes and try them before deciding to commit the changes where feasible. Changes could be stored as deltas so that the user can have undo and redo functionality. Storing deltas may also be helpful to reduce the amount of information stored. An exception to the need to hold a series of deltas may be when a profile is deleted. The deletion of a profile may be the point where a whole set of deltas are deleted and only the last profile is saved (possibly as part of a user commanded clean-up procedure). This last profile may be stored for future use if any kind of problem or accident occurs.

Undo functionality

Guideline 10.10.3.a: The profile agent should always maintain a copy of the last deleted profile in case the users have any problem when creating or updating a new one. This will prevent the user from losing functionality if problems arise.

Guideline 10.10.3.b: Users should be able to make changes and try them before deciding to commit the changes.

Guideline 10.10.3.c: The profile provider should keep a number (may be defined in a contract) of previous revisions of the profiles.

11 Profile activation

Automatic activation of situation dependent profiles is seen as a key method of relieving users of the task of manually activating different profiles as their situation changes. This form of support could be a significant factor in deploying profiles in a way that makes self-management of communications easy to understand and implement.

Users could define activation rules according to their activities and make use of different means (e.g. events from time schedules, accessories and external applications) to trigger the automatic activation of their profiles. Rules for automatic activation and deactivation can be customised and it is important to find a balance of simplicity, but also offer enough richness and options so that users feel that the profiles suit their needs.

11.1 User states

At any particular time, a user can be considered to be in a particular user state that relates to the user's situations. To enable effective user profile management, it is necessary to define a number of user states that are meaningful to the user and that relate to the ways that the user wishes to manage their services and devices. Some examples of states that many users might find convenient include at home (awake), asleep, in the office or a meeting, driving the car or travelling by public transport, abroad, etc.

Most users would prefer to have a number of pre-defined states to select from, with the option of adding to or changing those states to suit their own individual preferences. Profile providers (see clause 5.3) could, when the user first sets up their profile, provide users with a basic set of user states from which they can select those that they think will be significant. Profile templates for different types of users would be a good way for profile providers to provide users with an appropriate set of user states. The profile tool can provide the user with a mechanism for modifying or adding to these pre-defined states as the user identifies states that are more helpful to them. For each user state there will be a corresponding situation dependent profile (see clause 4.2.3).

The Profile Agent (see clause 4.6) can be informed about what state the user is in by the user manually selecting their current state from a list of possible states. This method of specifying and changing user states is a significant load for users and may frequently result in the user forgetting to activate a new state (or deactivate an existing state). It is better if the profile agent could identify when a user enters or leaves a state, especially where the user is allowed to confirm or reject the inferred state change (if they wish to).

Once the current user state is correctly determined, the profile agent will activate the situation dependent profile that corresponds to that state.

11.2 Automatic identification of current user state

In order for the profile agent to automatically determine what the current user state is, the profile agent must have access to information on the state of entities that are closely associated with the user. The precise entities that are utilised to determine user state is something that is the joint responsibility of the profile agent (which decides which entities it can possibly monitor) and the users (who decide which of these entities they wish the profile agent to monitor). Examples of entities that the profile agent could monitor to determine the current user state are:

- the state of the user's devices and accessories;
- the state of any or all of the user's communications networks;

- the state of any or all of the user's communications services;
- the state of any or all of the user's communications applications;
- the state of external devices and services that are closely linked with user activity (e.g. use of an Automated Teller Machine (ATM) to withdraw money from one of the user's bank accounts);
- location sensors and location services.

By getting information on the current or recent state of a number of these entities, the profile agent could make accurate inferences about the likely user state (e.g. if the user withdraws money from an ATM machine they are in the "out" state and that if the user's GSM service shows that they are roaming in a foreign country they are in the "abroad" state.

At any particular time, all of the user's terminals, services and applications will be in one of a finite number of possible states (e.g. "active", "no connectivity", "switched off"). At any time, the sum of these terminals, service and application states can be considered to be the current state of the user's environment. A key activity for the profile agent will be to examine the state of the user's environment and try to use this to infer the likely "user state".

Where the current state of the user's environment does not match the state associated with one of the user states, the profile agent should propose that it sets the user state to one of a number of default states. Which default state is chosen will be subject to rules in the profile and these rules will typically indicate which default state to choose based upon the last user state that the user was in. These default states will also be provided by the profile provider and will also be subject to updating by the user.

Event subscription and notification

Guideline 11.2.a: Profile tools should be provided with all state and location change events available.

11.3 Transitions between user states

Whenever the profile agent is informed about a change in the state of an entity associated with the user, it should examine the rulebase in the user's profile to see if changes in the state of this entity may be associated with changes of user state. Where state changes to the entity may be associated with changes to the user state, the profile agent examines the current state of all of the entities associated with a user state in order to determine whether the current user state still applies.

Where the profile agent determines that the current states of entities associated with the user are no longer those associated with the current user state, the profile agent should initiate a user state change process. If the current states of entities associated with the user correspond to those defined for another user state the profile agent should identify the need to change the user state to that other state. Where the user has requested that they authorize all changes of user state the profile agent should ask the user to agree to a change to the newly identified state. Where the user has not requested that they authorize changes to user state, the profile agent should change the user state and notify the user that the state has been changed if the user has requested to be notified.

Where the new states of entities do not correspond to those associated with another user state, the profile agent should initiate a change to one of the default user states. The profile agent should seek user authorization and notify the user according to the same rules described in the previous paragraph.

11.4 Presentation of profile state

In order that the users do not experience unexpected communication behaviour, it is desirable that they know which profile is active.

The presentation mode depends on the terminal capability and the user's preference settings. If there is a screen then the name of the profile and/or the associated icon can be shown. If there is no screen or if the user has defined the preference of audible notification then a spoken word or sound could inform the user about which profile is active.

The user should be able to select a type of alerting when a profile is activated or deactivated. They should be able to select from at least "No alerting, do it automatically", "Do it automatically, but alert me", "Alert me and ask my permission first", and "Do not do anything, I will select it manually".

User awareness of profile state

Goal 11.4.a: Users should be able to get information about profile state from any terminal.

11.5 Activation and deactivation of profiles

Profiles may be in an active or an inactive state. The profile can be activated either manually by the user or automatically as defined in activation rules.

Normally, a currently active profile is inactivated the moment another profile is activated. Users can always choose a profile manually, even if another profile has automatically been activated. Users define the conditions. The rules, for activation and deactivation are described in clause 11.7.

Activation and deactivation of profiles

Goal 11.5.a: Users should be able to get information about which profile is active from any terminal.

Guideline 11.5.b: Users should be offered the option of being notified of automatic profile activation.

Guideline 11.5.c: Users should be offered the option to choose whether they prefer activation/deactivation to take place with or without having to confirm it.

11.6 Different means of triggering the automatic activation of profiles

Users can define activation rules according to their activities and make use of different means to trigger the automatic activation of their profiles. For example, activation rules may specify that the "Driving" profile is activated if the user has attached their mobile phone to the car hands-free unit.

An automatic activation of a profile may be triggered by events from:

- a time schedule in the profile tool;
- synchronization with an external application (e.g. a calendar application);
- terminals and accessories (e.g. a mobile phone being placed in a desktop charger may automatically activate a profile associated with the location of the desktop charger);
- services such as location based services or an instant message sent from the user's home PC;
- distributed event publish and subscribe mechanisms.

The activation will be dependent on the capabilities of the underlying technologies in use.

Different means of triggering the automatic activation of profiles

Goal 11.6.a: Users should be able to activate profiles from any terminal.

Guideline 11.6.b: Users can define activation rules according to their activities and make use of different means to trigger the automatic activation of their profiles.

Guideline 11.6.c: Users should be able to manually activate and deactivate a profile.

Guideline 11.6.d: Manual activation overrides the automatic activation of a profile.

11.7 Activation rules

Different rules can apply for automatic activation of a profile. It is clear that this flexibility in definition of profiles might also augment the complexity. When defining a profile, the user should be able get information about possible state changes of other profiles when the new profile is activated and also which other profiles may be activated when the new profile gets deactivated. Users can choose if the profiles should change state to an active or an inactive state with or without asking the user to confirm. Users should be able to get clearly presented real time information on profiles, in the way that is specified in their preferences.

11.7.1 Default precedence order of activation/deactivation rules

Profiles may be activated due to one or more activation rules. The following default precedence rules may apply:

1) user activates a profile manually;
2) automatically by an accessory or environment trigger that is synchronised with a profile;
3) automatically by a user-employed service;
4) automatically by profile time schedule or by a calendar that is synchronised with a profile.

An action with lowest precedence number has the highest priority. When the user performs an action such as selecting a profile or uses an accessory synchronised with a profile, this will result in a change to that profile even if a time schedule defined activation of another profile.

Users may change precedence of numbers 2 to 4. They can also define that they want to be asked for confirmation before activating another profile.

Activation precedence order

Guideline 11.7.1.a: There should be standardized activation precedence defaults.

Guideline 11.7.1.b: Manual activation takes precedence over automatic activation.

Guideline 11.7.1.c: Users may define user-defined activation precedence.

11.7.2 Different types of activation rules

Users may choose among different types of activation rules such as:

Previous

The profile that was active before is activated again. An example is when a person had the profile "Office" set and goes to a meeting. When the meeting is ended the "Meeting" profile is automatically deactivated at 16:00 because the agenda said "Meeting 14:00-16:00". The Profile that is automatically activated is the previous profile "Office".

EXAMPLE 1: Office → Meeting → Office.

Default Always

Users can define a Default Always profile that is always automatically activated when another is deactivated.

EXAMPLE 2: Any Profile → Default Always.

Default when nothing else is defined

Users can define a default profile that is automatically activated if no other activation rule is applicable. All devices and services should have a well-known default profile, and the default values should be set for user privacy and control.

According to a time schedule

Users can define a time schedule for activation of profiles.

Defined order

EXAMPLE 3: Users can define the order. Example Apple → Banana means that Banana will automatically be activated when Apple is deactivated.

EXAMPLE 4: One → Two → Three → Four → Back to first item in list.

Combination of the above activation rules

Users may combine the different activation rules.

Different types of activation rules

Guideline 11.7.2.a: Users may choose among different types of activation rules.

12 Address book management

In this clause, the word "address book" is used to indicate the address book that is part of, or associated with, a profile agent, unless otherwise stated.

This clause is based on the address book clause in EG 202 249 [1] which focused primarily on address book issues related to UCI.

The address book may be an integrated part of the profile agent, which is available from the profile tool when managing profiles. It may also be a third-party address book which is made available in the profile tool in a transparent way.

12.1 The function of the address book

An address book as part of, or associated with, a profile agent is a vital part of the profile tool. It is needed:

- to provide a list of contacts with whom the user may wish to communicate;
- to give the profile agent a source of information upon which its filtering rules can be based;
- to control rules surrounding a user's "Buddy Lists";
- to provide identification links for any authentication required for sharing of the user's resources.

12.2 Content of the address book

12.2.1 Content address book records

At a minimum, the address book should contain a list of people with their name and contact information stored against each person. An address book record should have fields for:

a) name;

b) UCI (including all its parts);

c) an indication of the presence of a UCI (e.g. symbol, icon, or abbreviation);

d) phone number;

e) email address;

f) nicknames and nickname venues;

g) user permissions;

h) logs and notes.

An identifier that is permanently associated with a person and all of their services (e.g. UCI or an ENUM number) eliminates the dual problems of a large number of identifiers per person in an address book and identifiers in address books that cease to be valid as people change services and service providers. For this reason, it is very desirable to provide support for the storage of such numbers in address books.

Support for both UCI and non-UCI address book records

Guideline 12.2.1.a: Address books should be capable of holding records for contacts that have UCIs and for contacts that do not. For this reason, fields for UCI and non-UCI contact information should be provided.

Indicating the presence of a UCI in address book records

Guideline 12.2.1.b: A visual distinction to indicate the presence of a UCI is required (e.g. symbol, icon, or abbreviation). This could be placed with the other UCI data in a displayed address book record. Such a symbol might be as simple as "UCI" if, indeed, this name becomes established.

12.2.1.1 Services available

An address book record should provide a simple representation of what services are available (as it may help the user to decide the most effective type of communication to request). The most obvious way to do this will be to use universally accepted icons or abbreviations representing each available service.

Information stored in the address book about preferred services could be kept up-to-date by information communicated by the profile agent.

Presentation of preferred services in address book records

Guideline 12.2.1.1.a: If there are preferred services then these should be made clear by means of appropriate symbols or icons that can be displayed with the data record. In UCI systems, this will be derived from information that the owners of UCIs provide in the additional information field of their UCIs.

Correlation of address book entries

Guideline 12.2.1.1.b: Many address book entries are derived from the record of individual communications. The address book tools should have an interactive mechanism to attempt to correlate communications identifiers from different sessions with the same individuals.

12.2.1.2 Charging information

It may be thought necessary to indicate the level of charging which the user should expect. At the very least it might be necessary to consider how to indicate:

- free communication;
- mobile rate;
- premium rate;
- international rate;
- reverse charges;
- shared charges on sessions not established by the user;
- in-session changes to rates.

The charging that users experience may well also be a function of the communication service that they request. Any information relating to charges will be supplied as part of the additional information field of a UCI. Charging could also be accumulated as a historical record for estimation of costs.

Presentation of charging information in address book records

Guideline 12.2.1.2.a: Information about the charging rate for communication should be imparted by means of a symbol or text placed after the preferred service symbol, icon or abbreviation. For UCI, this will be derived from information that the owners of UCIs provide in the additional information field of their UCIs.

12.2.2 Postal address data

The address book may also contain additional information such as postal address. In addition to the postal address, entry codes could be added, which may be used for automatically opening gates and doors.

12.2.3 vCards and e-business cards

The user should be able to designate outgoing vCards or e-business cards for manual or automatic distribution to a community selected in their profiles.

12.2.4 Additional content of address book records

Address book records may also contain a number of additional attributes (not just restricted to those in the UCI "additional information" field). Some of these attributes may be related to alternative ways of highlighting the address book record. Such attributes could include:

- a voice label;
- a visual image;
- date of last communication;
- associated sounds (e.g. ring signals);
- associated icons (e.g. to indicate membership of the "Family" group);
- text characteristics - colour; text weight (e.g. italic, upper-case);
- assistive technologies (necessary or available);
- a notes field (e.g. for recording things such as a preferred carrier pre-select code to use when communicating with that contact).

Additional content of address book records

Guideline 12.2.4.a: Consideration should be given to the inclusion of fields for additional information. This additional information could include a voice label or a graphic image, as well as a visible version of some of the additional information fields that are stored for UCIs.

12.2.5 Shared address books

There are many circumstances in which two or more people will wish to communicate with the same set of people. Typical examples are members of the same family or employees of the same company. In these circumstances it is very desirable that these people (the shared interest group) can access contact data contained in a shared address book.

One or more of the people in the shared interest group may be given the rights to add to and modify the records in the shared address book. However, records from the shared address book can be presented to members of the shared interest group as either a separate list of contacts or as contacts that appear as part of their own private set of stored contact data. Sharing items in a family address book in no way overrides the access privileges assigned to directory records. Some members of a family will not be able to view records belonging to the company address books of other members of the family unless they have been assigned explicit rights to view these records. Sharing of address book records is illustrated in figure 1.

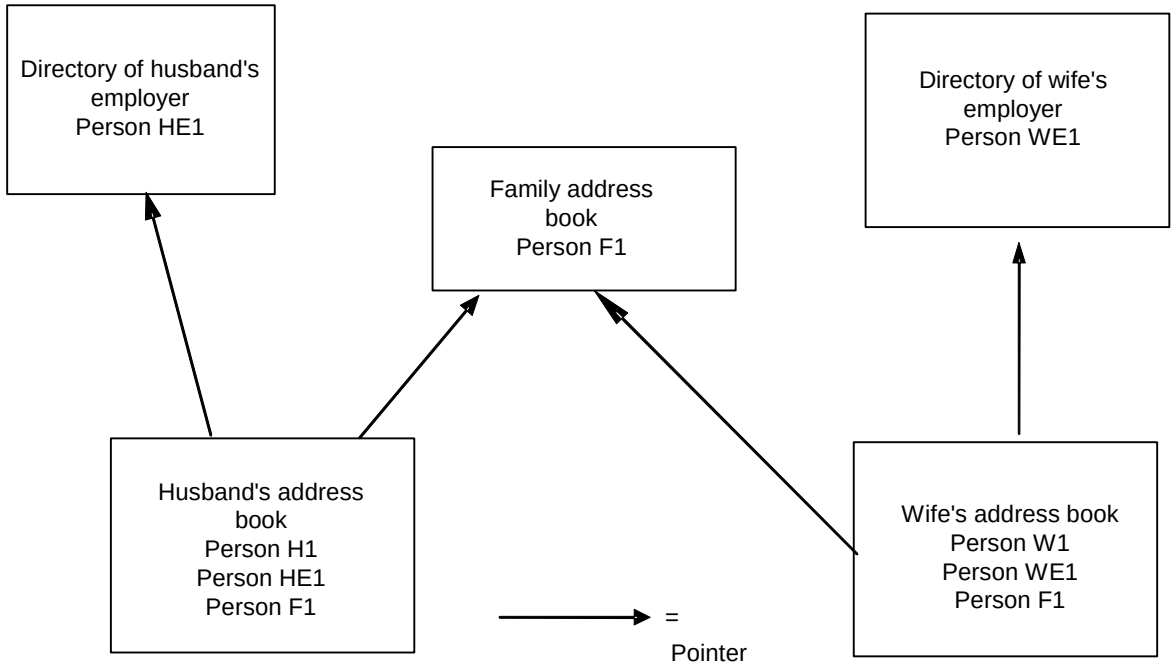


Figure 1: Shared address books

Shared address books

Guideline 12.2.5.a: The capability to allow a number of users to share one or more common address books as well as their personal address book should be provided.

12.2.6 Availability in various tools

Address book data should be available in various tools such as profile tools. The stored address book data and user interfaces used to present and manipulate that data need to be separated. Address book data and operations need to be available for developers of tools by offering operations such as:

- authenticate;
- search by different search criteria;
- sort by different sort criteria;
- read;
- create;
- update;
- delete;
- notification when updates have occurred;

- communities of interest.

When relevant, the operations may be on:

- parts of address book records;
- entire address book records;
- set of address book records;
- members matching a certain criteria.

12.2.7 Synchronization of distributed address books

Address books contained in terminals (or on smart cards) might be a subset of those available to the profile agent(s) in terms of:

- the number of records held;
- the number of fields held per record.

The constraints on what is held in a terminal address book will be determined by limitations of storage format in the terminal (restricted number of records and fields) and by user preferences.

Users should be able to express their personal preferences for what gets stored in terminals - making a selection of which records and which fields.

When address books in terminals and profile agent address books are synchronized, users will not wish to be disturbed by requests to resolve differences in storage capacity and record sizes.

Synchronization of distributed address books

Guideline 12.2.7.a: All address lists associated with different terminals and smart cards may be synchronized with a master list held by the profile agent.

Guideline 12.2.7.b: Dependent on local storage capacity it should be possible to download any record to a terminal address book from the master address book.

12.3 Operations on address books

It is likely that a number of address book record operations will be provided. The following clauses refer to the most common and relevant operations and assume that all operations are performed online.

Users may, from time to time, modify address book records on offline versions of their address book (e.g. in a mobile telephone address book that is out of signal range). When editing of the address book occurs offline there may be problems of synchronization with the online version. These problems, and the approaches to solving them, will be almost identical to those with offline editing of the profile agent profile. Therefore, reference to clause 7.2.4 in EG 202 249 [1] should be made when addressing issues related to offline editing of address books.

12.3.1 Add to address book

There are a number of different ways in which users may wish to have records added to their address books. These include the following:

- The user may wish to manually add a contact to the address book by entering all of the data themselves.
- The contact data of someone the user has just replied to may be added automatically to the address book (sometimes referred to as "contact data capture") if the user has opted for such a feature.

- The profile agent may, as a result of certain user behaviours, offer information suggesting additions to the address book. For example, if a number of communications have been made to or received from a contact that is not in the address book, the profile agent may ask whether the user wishes to have that contact added to the address book.

- Users will require that the master address book in the profile agent is synchronized with all of their terminals (with the profile agent information being considered the master version of the data). Where a new contact has been added to a terminal address book, this synchronization should create a new record in the profile agent address book. The capabilities, in particular the different storage capacity of each terminal, will need to be taken into account.

- Where the profile agent acquires new contact data, users may wish to be notified and given the opportunity to add this contact data to one or more local terminal address books.

- A user may designate certain groups of users, such as members of one's employer or club, fellow travellers, for example, to trigger an automatic sharing of address book data without user interaction.

It is expected that all of these methods of adding records to the address book could be quite common. As such, they should be supported in such a way that it is quick and easy for users to make such additions.

Add to address book

Guideline 12.3.1.a: Users need to be given a mechanism to manually add contact data to the address book.

Guideline 12.3.1.b: Users will require the ability to set special conditions which will automatically add an identifier into the address book (or flag up the need for a decision on whether to place the identifier into the address book).

Guideline 12.3.1.c: Where records are added automatically, the user will require the capability of personalizing the label received as part of the contact data. This could be necessary because of duplication (two "John Smith" labels) or because the contact is not normally known by that label to the user.

12.3.2 Modify

The modification of address book records is likely to be a frequent operation if these records contain information other than the name and contact information of the contact. Whereas an individual's name is unlikely to change frequently, other information in the address book such as postal addresses or non-UCI communication identifiers could change quite frequently. For this and other reasons, data in an address book record will sometimes be incomplete or out-of-date (e.g. a user has changed their name by marriage).

Where UCIs are used, completion and/or modification of the UCI information can occur as part of the PUA to PUA handshake process that occurs in UCI communication setup.

Attempts to modify address book records that are referred to by profile rules or that are members of various lists (e.g. a "friends" list) could cause problems in the way that these rules or lists operate.

Automatic completion and correcting of address book records

Guideline 12.3.2.a: Part of the "handshake" between PUAs should include the identification and updating of incomplete or out-of-date UCI address book data.

Guideline 12.3.2.b: Subject to the user's choices on the amount of feedback that they wish to receive, the user should be kept informed of the changes made, and possibly given the opportunity to accept or refuse them.

Changing address book records

Guideline 12.3.2.c: Attempts to remove or modify address book records that are referred to by profile rules or that are members of various lists (e.g. privacy "white list") should be flagged to the user.

12.3.3 Group and arrange

The user may wish to group and arrange address book records. A number of alternative grouping mechanisms may prove acceptable (dependant on the target group of users). These methods include:

- Address book categories – in this method, one or more categories may be assigned as attributes of each contact (e.g. named categories such as "Work", "Friend", "Family").
- Address book sub-sections – in this method the address book is considered as a single entity, but it can contain different sub-sections assigned to different categories (e.g. different address book sub-sections for "Work", "Friends", "Family").
- Different address books – this is a variant of the address book sub-sections described in the previous bullet. In this method it should also be possible to have the same contact in more than one of the address books. Although the user may perceive the address books as separate entities, the danger of multiple conflicting contact records for the same contact must be avoided.

Different methods for allowing the user to vary the way in which they control the order of records in the address book(s) should be provided.

Address book record organization

Guideline 12.3.3.a: Users should be able to view their address book records according to different criteria such as group, alphabetic listing of surname, first names, etc.

12.3.4 Search

Users will have different knowledge and different strategies when searching for contacts in the address book. Search mechanisms that are likely to be helpful for users include:

- a scrolling list;
- name entry:
  - field search;
  - all fields search;
  - specified fields search;
  - whole word or part word searches;
- group search (where the user can enter or select the name of a group).

For searches beyond the scope of the address book, different search strategies will probably be required to searches made on the address book (e.g. more information about the desired contact would be required from the user to make the search sufficiently specific).

Searching for contact data across different sources

Guideline 12.3.4.a: Users should be provided with a search mechanism that is consistent across multiple sources (e.g. personal address books, group address books and white pages) and when accessed from different terminal types.

12.3.5 Send

Users may wish to send contact records from their address book to other users.

Sending or updating contact data details

Guideline 12.3.5.a: The facility should be available to send contact data details from the user's address book to others address books. Where restrictions have been applied to the transfer or broadcasting of the contact data then this should be made apparent to the person attempting to send the contact data and should not be permitted by the profile agent.

12.3.6 Move, copy, remove records

In addition to the operations already mentioned, users will need the ability to move, copy and remove records from address books.

Automatic housekeeping operations may assist the user in managing the move, copy and removal operations. The profile agent might prompt the user about moving a contact from their personal address book to a family address book if it detects that other members of the user's family also frequently contact the person in the user's address book.

In looking at these methods, the principle that the user should always have ultimate control should be taken into account (e.g. by allowing the user to turn various prompting options on and off).

Moving, copying or removing records

Guideline 12.3.6.a: In addition to user initiated moving, copying or removal of records, consideration should be given to allowing the profile agent to prompt the user about when it may be beneficial to move, copy or remove an address book record.

13 Information sharing and privacy

13.1 Personal information privacy

13.1.1 General privacy issues

As personalized services become more common, personal privacy issues will become an increasingly important factor in their acceptance.

Increasing threats (see [17]) to both privacy and security are emerging due to factors such as:

- the large amount of personal information that is now being collected in order to personalize devices and services;
- communication convergence (the moving of data across different domains and the usage of transport mechanisms of lower security such as Wi-Fi);
- the storage of personal information on remote customer databases and the weak controls on how that information may subsequently be used;
- the low and misconceived level of understanding of privacy and security threats in the general public;
- the almost inevitable trade-off between security and usability (e.g. multiple security levels such as PINs, shared-secrets; etc.).

To ensure that users are confident that their information is not used in ways of which they disapprove, they will need standardized ways to both control how and to whom their information is made available. They also need status visibility e.g. to be warned when there is a risk that information is about to be shared in ways which they may find unacceptable.

If profile data is made available to the wrong people, then users will lose confidence in the profile provider who allowed that profile data to be misused. However, too restricted access to profile data should be avoided, as it may reduce the usability and the number of available services.

Privacy requirements of stored or transmitted data vary among different users, companies, countries, and service- and profile providers. It is therefore impossible to define a set of privacy guidelines that meet the needs of all users while still conveying any useful information. However, careful application of the guidelines in the following clauses can help to ensure the correct balance between privacy and functionality.

13.1.2 Templates

A number of privacy related factors need to be considered in templates. Users need to be able to limit the availability of individual pieces of information to those entities that they desire to share it with. Templates could provide pre-configured privacy options that meet their expected needs of their users depending on users and context. Other templates will also be likely to have an impact on privacy.

A set of predefined templates can be used for privacy management. They may meet different needs and could be used for defining privileges, authentication methods and privacy preferences according to:

- user individuals;
- user roles;
- security levels;
- services;
- devices and accessories;
- objects and operations.

13.2 Access to profile data

Profile data exchange may depend on:

- the privacy level desired by the user;
- the authenticated identity of the person, organization, device or service attempting to access the profile data;
- legal limitations on specific data available externally (see clause 13.8);
- service provider restrictions on release or modification of profile data.

Administrators of profiles (clause 5.1.2) have rights to read their profiles and get information about the use of their profiles irrespective of any privacy controls placed on the rights of others to access their profile data. Profile administrators have read, update and delete privileges on profile data. Where there is data related to the administrator of a profile that the administrator is unable to read or write (e.g. billing data), then that data is outside the scope of the present document and no guidance is given on access to and privacy of such data.

In many cases the user of a profile is also the administrator of the profile, but in other cases, someone else is the administrator (see clause 5.2.4). An example that is very likely to be common is parents managing their children's profiles. Parents will then be the administrators of the information in their children's profiles. In a corporate profile, the employer is generally the administrator of the profile and has access rights to information in the profile. It is important to ensure that the user may easily get information about who is able to know what.

Service providers may add, update and delete information related to their services. Service providers, in the role of administrator, may allow the user the right to view some service related profile data but deny them the right to directly modify that data. The service provider might require the user to send an e-mail or to make phone call to request a change to some elements of the profile. This type of change request would most frequently be required when the change to the profile involves a change to the user's service subscription.

Users may also let third party services manage their profiles, see clause 13.7, , "Trusted third parties".

Some data is unsuitable to be copied and shared with other users, e.g. security and privacy information (passwords, certificates etc) or personal details (name, address, year of birth, credit card number, etc) and this information should be automatically excluded from any copying to another person or organization.

Where information is shared, users should be able to monitor and audit accesses to that data by examining their profile activity log (see clause 14).

Access to profile data

Guideline 13.2.a: A user should be able to differentiate between their own private profiles and those maintained by their employer or organization.

Guideline 13.2.b: Users should be in control over access to and distribution of their user profile data.

Guideline 13.2.c: Only the minimum user profile data requested by an entity should be provided to that entity.

Guideline 13.2.d: For any item of profile data, users should be able to specify that they wish to be asked whether they want that data to be released. Users would expect to be given an explanation why the data is required by external resources or other people.

Guideline 13.2.e: A service shall only share information with another service if the other service is also "trusted"' by the user.

Guideline 13.2.f: If a user action incurs an external request for profile information which the user has set as unavailable to the requesting entity, the user should be provided an immediate option to share the requested information on a regular or single time basis.

Guideline 13.2.g: Where information is shared, users should be able to monitor and audit accesses to that data by examining their profile activity log.

13.3 Vendor and provider interactions

In order that their devices and services can be personalized, users need to allow profile providers, devices and communication service provider's access to profile data related to the operation of the device or service. Users may be also be happy to entrust other services, such as an academic service, with preferences for work-related research and teaching information but not information related to bank details, health, leisure, political activities etc. Users should also be able to share information in their profile with others, such as with a user's affinity group or buddy list, and it should also be possible for users to send entire profiles or parts of profiles to other users.

Profile data may be distributed over different devices, networks and services and belong to different administrative domains. These administrative domains may be closed against external access. However, in order to enable a seamless service experience for the user, a controlled transparency to exchange profile data is needed (see [4]).

Vendor and provider interactions

Guideline 13.3.a: Profile providers, network operators and value added service providers require a mechanism for exchanging profile data in order to enable a seamless service experience for the user.

13.4 Privacy levels

Security mechanisms that are appropriate to the level of confidentiality should be available for the transfer of profile data to, from or between authorised entities. Users should be offered default settings at a sufficient level of security that is appropriate to the data stored or transmitted. However, a level of security that is higher than necessary should be avoided as it increases costs and may contribute to poor system usability.

An important consideration is that users will expect:

- a set of security levels together with a simple explanation of what these levels mean;

- an explanation of what could happen to their data in different security contexts;
- the option to be informed of visibility of or access to their profile data;
- the option to be asked for permission to allow visibility of or access to their profile data.

Users may assign privacy levels to different entities such as service providers, and related to specific services. There will also be some information that the user will want to share with every company and with every service.

The privacy levels can vary depending on the situation and role of the user and as defined in the currently active situation dependent profile. For instance, the users might want to share their work-related preferences with their colleagues, but they might not want to share what is related to their hobbies.

Privacy levels

Goal 13.4.a: Users should be offered default settings at a sufficient level of security that is appropriate to the data stored or transmitted.

Goal 13.4.b: There should be a common security level at which user identity needs to be verified. The authentication can be controlled in different ways such as one or more of a range of alternative authentication schemes, restrictions to passwords, and choice of authentication method.

Guideline 13.4.c: There should be a mechanism to inform a user whenever any information in their profile above a selected privacy level is read by an external entity, along with identification of that entity.

Guideline 13.4.d: When communicating with devices and services, the profile processing agent should respect user and legally required privacy requirements (see clause 13.8).

Guideline 13.4.e: There should be a mechanism for the user to be informed about any changes of security level.

Guideline 13.4.f: All elements of any profile need to have selectable levels of information sharing to specific single entities or to a well-known sharing group, such as Friends, Family, Business Associates, Buddy Lists.

Guideline 13.4.g: Security levels should have common definitions between entities, so that users can share a common expectation.

Guideline 13.4.h: A new user's default start-up security profile should be preconfigured with default security levels. The user may redefine the security levels at any time.

Guideline 13.4.i: The users should be able to easily understand, chose and apply their desired security policies.

Guideline 13.4.j: The profile provider should apply the appropriate level of security to the transfer of the data.

Guideline 13.4.k: Access to profile data should be limited to the subset of data required to perform the given service or function.

Guideline 13.4.l: There should be a mechanism for informing the user about any identified security breaches.

13.5 Privacy policies

Users may not wish to make explicit choices on whether their privacy preferences are being respected each time they use a communication or information service. For this reason, mechanisms (such as the W3C's P3P initiative [20]) that attempt to compare users' privacy preferences against a web site's published privacy policy present a potential model that ensures users' privacy preferences are being respected.

As users will not want to define independent privacy preferences for every service that they use, there is a need for a common way to define privacy preferences such that they apply across the widest possible range of services. What is also needed is an assurance that any claims made by service providers are accurate and can be trusted. Whatever method is adopted, there needs to be mechanisms for providing users with both positive and negative feedback on whether their privacy preferences are being respected. Where it is determined that a user's privacy preferences are not being respected, users will need a mechanism to ensure that they do not participate in ways that compromise their privacy preferences.

Privacy policies

Guideline 13.5.a: Mechanisms that respect user's personal preferences with respect to the privacy of their personal information should be used. At this time, mechanisms that are based upon the W3C's P3P recommendation [20] should be used for web-based services.

Guideline 13.5.b: Users should be provided with feedback on whether their privacy preferences are being respected. Users should be given positive indications that their privacy preferences are being met. Where their privacy preferences cannot be met, users should be informed and offered an option that ensures that their privacy preferences will not be violated.

Guideline 13.5.c: Users should be provided a mechanism to request details of any information stored about or relating to them.

13.6 Access control and authentication

Access to most profile data will only be permitted in an authorised and secure manner and there need to be methods available to check that the service, person or organisation accessing the data has the appropriate authorisation to do so. The access to any item of profile data may be granted to the public, a defined group or list of people, to a single person or organization and these access criteria may vary. Except for those items of profile data that the profile user intends to be fully publicly available, access to profile data will require authenticated identification of the user, organisation, service or application wishing to access the profile data.

Authorisation of the requested action (create, read, modify or delete) on the profile data [4] depends on identification of the:

- requesting person or organisation (if delivered in the request);
- requesting application;
- targeted user;
- targeted profile data.

Authentication attributes can only be set by a person with administrative privileges. A profile user should not normally have to manage authentication as the criteria would normally be set during initial profile creation. However people with responsibility for managing other people's profiles need to manage authentication criteria, such as corporate administrators for employee profiles, club administrators for member profiles, or parents managing their children's profiles may need to manage authentication criteria for these users. Administrators should be able to use authentication templates that suit their administrative role.

The following authentication settings may be defined in templates and they may be defined and modified by the administrator:

- Password expiration, defines how often passwords must be changed as well as who may change them.
- Password strength.
- Lockout, to prevent password attacks by limiting the number of password failures permitted within a period of time.

- There are multiple authentication schemes such as password, token etc., and with different strengths. There are different authentication methods such as:
  - User authentication provides access privileges on a per user basis.
  - Client authentication allows access from a specific IP address or terminal. The user performs the authentication by successfully meeting an authentication challenge, but it is the client terminal that is granted access. Authentication may be based on service contracts based on SIM cards or MAC addresses.
  - Session authentication can be used to authenticate on a per-session basis. The user is challenged for a proper authentication response.
  - Traditional line identification, as used for traditional basic telephony service.

If any part of the user profile or a user profile agent needs to make any external requests or responses to any external events, the user needs to have the opportunity to be made aware of these external interactions and be given the option to allow or deny them.

Access control and authentication

Guideline 13.6.a: Access to profile data should only be permitted in an authorised and secure manner.

Guideline 13.6.b: Transmitting profile data should be done ensuring that any non-authorised person may not read or modify the profile data.

Guideline 13.6.c: The validity of an authentication should, if required, be subject to a maximum time limit.

13.7 Trusted third parties

There may be situations where users need to make use of services previously unknown to them and with which they have no previous formal relationship e.g. no service subscription. For effective operation of these services it may be necessary for the service to have access to some of a user's profile data. As, in many circumstances, the service might only be used once for a short period it would be impractical to established a trusted relationship between the user and the service. The use of trusted third parties is an effective solution that enables appropriate sharing of profile data with a wide range of similar services.

One option is for the user to have a direct relationship with the trusted third party and for the trusted third party to take responsibility for ensuring that access to profile data by services related to the trusted third party is done in an appropriate way. However, as relationships between trusted third parties and service providers are often already established for various types of service, the management of access to a user's profile data may often make use of these existing relationships and agreements. In this case, parts of a user's profile related to a use of a service to which the user already subscribes to can be shared with other providers of a similar service via the trusted third party. This is precisely what currently happens when a person is roaming with a mobile phone. An additional advantage of this option is that service operators can have confidence that there will be no interchange of profile information that will compromise their own commercial interests as the arrangement between the service provider and the trusted third party will ensure that such commercially sensitive issues are always addressed in the agreements.

Trusted third parties

Goal 13.7.a: Trusted third party services may provide the authentication of identity.

13.8 Privacy regulations

The privacy requirements need to fulfil local privacy regulations. Lawful interception and other regulator requirements may imply that profile data is delivered to authorities (e.g. emergency services), despite the privacy settings.

Privacy regulations

Goal 13.8.a: Lawful interception and other regulator requirements may imply that profile data is delivered to authorities (e.g. emergency services), despite the privacy settings.

13.9 Access control methods

Terminals and services will provide a mechanism for people to gain access to users' confidential information and to gain access to their means of communication. For this reason, users may need mechanisms to allow them to exercise access control to their profile. Mechanisms such as password control, smartcard access and biometric monitoring can all be used as mechanisms for providing a level of access control security.

Mechanisms that heavily rely on users memorizing passwords and PINs may appear to be very secure, but such mechanisms may frequently be undermined by users writing down their passwords and PINs to avoid forgetting them. Many service providers attempt to increase the security of their services by increasing the number of elements that a user has to enter in an access control procedure (e.g. username, password plus one of a number of personal secrets), by putting constraints on the format of these elements (e.g. insisting that a password has a defined mixture of letters and numbers) and by insisting that some of these elements should be changed on a regular basis. Each new requirement appears to reduce the chance that an unauthorized person can access the service. However, as the complexity of the procedure increases, so does the chance that users are unable to memorize the necessary information and this results in many users resorting to writing down this information. Once the information is written down, the security of the access control procedure will be totally compromised. Thus, attempts to increase the security of an access control procedure by adding input fields and constraints can very easily lead to the procedure being less secure in practice.

Replacing elements of access control procedures with methods that do not rely on users memorizing passwords and personal secrets will tend to make these procedures easier for users and will reduce the risk that users will resort to writing the information down. The use of smartcards (or information beamed from terminals that have smartcards) and biometric methods (e.g. iris recognition, voice-prints, fingerprints) will all reduce the chance that users will compromise system security by writing down security information.

Access control methods

Guideline 13.9.a: The methods of access control provided should be appropriate to the context in which it is used. Thus, it would be inappropriate to require a very difficult and secure access procedure if no valuable or personal information is potentially under threat.

Guideline 13.9.b: Where a terminal, service or application has distinct sub-applications within it, different access control mechanisms should be considered for some or all of the sub-applications as well as for the terminal, service or application itself (e.g. a user should be free to choose to use the access control procedure provided for their contact information but not to use the access control for all terminal data).

Guideline 13.9.c: Mechanisms that require explicit user presence or intervention but that do not rely heavily on user memory should be considered for use when important security validations are required.

Guideline 13.9.d: Avoid increasing the number of elements that a user has to enter in an access control procedure (e.g. username, password plus one of a number of personal secrets) and putting constraints on the format of these elements (e.g. insisting that a password has a defined mixture of letters and digits).

Guideline 13.9.e: Replacing elements of access control procedures that rely on human memory with other methods such as smartcards or biometric methods will reduce the risk of users compromising security by writing down security information.

Guideline 13.9.f: Where there is a possibility for a password to be stored on a user's terminal, users should be asked whether they wish to enter the password every time or whether they wish to have the terminal remember it for future usage. Where such an option is presented, the user should be warned of the ability of other users of the terminal gaining access to the service or application.

Guideline 13.9.g: Any requirements or limitations of a password (e.g. on the content and/or length) should be clearly indicated to the user when the user is first asked to generate the password.

14 Log

Users can choose what they would like to see logged and how it should be displayed (e.g. what objects, activities, or more complex combinations of these). The user might choose to have different logs related to their different roles (e.g. private or business roles).

Logs can contain information such as:

- creation, update and deletion of profiles;
- activation and deactivation of profiles;
- rules applied;
- services and devices addressed in profiles.

Profile agents will keep a log of the changes made to the profile. These would also be available to the user who may or may not choose to use them. Profile administrators may also indicate what logs they are interested to see and the various events that may need to be tracked (e.g. the changes that users have made to their profiles). Certain logs (e.g. record of profile changes) may have certain restrictions such as the prevention of individual record deletion.

Users will require flexibility with regards to the way in which the log is displayed on each of their terminals. For instance, it may be appropriate that the log presented on a phone without a screen includes only voice-based communications. Users may use rules for defining their log preferences.

Log

Goal 14.a: Users should have access to the communication log (or a filtered version of it) from any terminal.

Guideline 14.b: The content of the log information presented would be subject to rules defined in each user's profile (e.g. the profile rules might specify that logs presented when the user is using a basic voice terminal should only list the last 5 log records).

Guideline 14.c: The profile agent should maintain a log of a core set of operations such as create, update and delete.

Guideline 14.d: Users can choose what they would like to see logged (e.g. what objects, activities, or more complex combinations of these).

Guideline 14.e: Each log will have a minimum set of parameters that will be stored for each log record. Users should be given options to control how much additional details each log should contain.

Guideline 14.f: Users should be given control of how logs should be displayed, including control of the sorting order (increasing/decreasing) of defined item such as date or service. Users could also be offered pre-defined settings suitable for different terminal capabilities, which they could subsequently modify.

Guideline 14.g: Users should be given control of the lifetime of log data. This control could be in terms of the age of the data or in terms of the overall storage space limits to be imposed upon the log data.

Guideline 14.h: Users should be able to view the log data chronologically.

Guideline 14.i: The user should be able to transfer the entire log or parts of a log record between the log tool and another tool or service.

Annex A (informative): Collective table of goals and guidelines

A.1 Concept and benefits

User convenience and access to their resources

Goal 4.1.1.a: The use of profiles should not limit the access a user might otherwise have to their services and devices.

Goal 4.1.1.b: However the user's profile data is distributed amongst devices and services, it should be possible to ensure that users can have the concept of centralised profiles which cover all of their devices and services.

Guideline 4.1.1.c: Users should be provided with a mechanism that allows them to organize profiles and templates in a hierarchical way.

Sharing of profile data between user resources

Guideline 4.1.4.a: If specific data in part of a profile relating to a device or service has been specified by the user, then it should be possible for the equivalent fields for other devices or services of the user to be populated with the same data.

Interpretation of profile data

Guideline 4.1.5.a: In order to avoid the user having to understand the internal attributes and detailed behaviours of every device or service with which they may need to interact, it is necessary for a user's individual information and preferences to either be directly usable by a device or service or for it to be translated into a form that a device or service can interpret.

Guideline 4.1.5.b: If data in part of a profile relating to a device or service has been specified by the user, then related profile fields for other devices or services can be directly populated by the same data or data translated to produce the same effects.

Access to location and presence information

Guideline 4.6.1.a: Profile agents need to have access to location and presence information when it is available.

Multiple profile agents

Guideline 4.6.1.b: Profile agents should have methods that allow them to be aware of each others' activities.

Guideline 4.6.1.c: There should be mechanisms to resolve conflicts when the activity of one profile agent potentially affects or overrides another's behaviour.

Guideline 4.6.1.d: Conflict resolution mechanisms may involve user decisions.

Storing, maintaining and restoring profile data

Goal 4.6.2.a: Users should be able to assume that storage of data is working correctly and no user activity is required.

Goal 4.6.2.b: Users do not need to be aware about where the profile data is stored and how it is synchronized.

Goal 4.6.2.c: Profile data should be stored securely.

Goal 4.6.2.d: A synchronization mechanism should be used to ensure that when changes are made to profile data, the data held at different locations is always consistent.

Guideline 4.6.2.e: Profile data should be easily restorable if the data is deleted or corrupted.

Guideline 4.6.2.f: The profile provider should offer the user different options related to storage, such as backup and synchronization frequency. The user may also be allowed to further customize these options.

Guideline 4.6.2.g: Any solution which makes use of profile data should contain a fallback mechanism if the desired profile data is unavailable. This could take the form of a last used profile, default template contents, or an attempt to re-create the required profile elements through querying other resources in the user's personal area network.

Guideline 4.6.2.h: There should be a mechanism warning users when inconsistent data has been discovered by the profile agents or tools.

Guideline 4.6.2.i: An appropriate action for resolving inconsistent data should be proposed to the user.

Persistence and availability of profile data

Guideline 4.6.3.a: The profile processing agent should be able to access relevant profile data at all times when a profile is active.

Guideline 4.6.3.b: The profile processing agent should be able to access the devices and services referred to in the profile rules in order to ensure that the actions in the device or service are carried out.

Guideline 4.6.3.c: If the device or service has features that access external resources but those resources are unavailable, the user should be provided with alternative solutions.

Guideline 4.6.3.d: When communicating with devices and services, the profile processing agent should have the necessary permissions to successfully request and achieve the desired behaviours from the device or service.

Visibility of external interactions

Guideline 4.6.3.e: If any part of the profile or a profile agent needs to make any interactions outside the user's personally controlled service environment, the user should be given the opportunity to be made aware of these external interactions. Typical interactions would be external requests for information or responses to any external events or changes.

Guideline 4.6.3.f: The user should be given the opportunity to make a decision about accepting or rejecting these requests by external entities.

Activation agent

Guideline 4.6.4.a: A user should be able to have multiple profiles available if they choose to maintain separate sets of preferences that can be selected in a single step.

Guideline 4.6.4.b: The user should be able to manually order the activation agent to activate a different profile across all affected devices and services, without having to use multiple devices or applications.

Guideline 4.6.4.c: A profile activation agent should be able to access the profile processing agent at all times when it is required to activate or de-activate the profile.

Guideline 4.6.4.d: A profile activation agent should be able to receive requests from a profile processing agent to activate or de-activate either the profile belonging to the profile processing agent or another appropriate profile.

Viewing/editing agent

Goal 4.6.5.a: Users should be provided with mechanisms that allow them access to all components of their profile.

Goal 4.6.5.b: The profile implementations should allow as much user access as possible, within legal and business constraints.

Goal 4.6.5.c: Users should have mechanisms that allow them to edit profile data and have the changes automatically propagated to all components where that data is used.

Guideline 4.6.5.d: A user should be provided with mechanisms to view or edit all or part of their profiles.

A.2 Stakeholders and roles

User and administrator roles

Guideline 5.1.3.a: There should be a mechanism informing users whether they are in a user role or in an administrator role.

Guideline 5.1.3.b: Users should receive a clear notification when they move from the user role to the administrator role. This notification should warn the user that changes made in the administrator role may be irreversible. Users should have the ability to turn off this warning mechanism.

Guideline 5.1.3.c: Users should receive a clear notification when they move from the administrator role to the user role. Users should have the ability to turn off this notification mechanism.

Guideline 5.1.3.d: There should be a mechanism allowing levels of administrator roles such as super-administrator role and self administrator-role. These levels of administrator roles would require user authentication.

Guideline 5.1.3.e: Users may call upon a third party service and allow the third party service be in an administrator role and administer their profiles.

Guideline 5.1.3.f: Certain important profile administration operations will require special privileges. These operations would require users to authenticate themselves.

Guideline 5.1.3.g: At the end of the configuration, the administrator should be reminded to change role again, from administrator role to user role. That would minimize the risk of unwanted configurations.

Management of another person's profiles

Guideline 5.2.4.a: The supervisor should be able to set the privacy levels for any other user for whom they are legally or financially responsible, within the scope of their responsibilities.

Guideline 5.2.4.b: The supervisor should be able to select profile elements of the person being supervised to control alerting, user permission, or complete blocking, under the control of the supervisor.

Guideline 5.2.4.c: The supervisor should be able to individually set the profile information elements of the person being supervised, within the scope of their responsibilities.

Guideline 5.2.4.d: A supervised user should be able to differentiate between parts of their private profile they have rights to manage and those maintained by the supervisor, and be aware of any intersection or conflict.

Guideline 5.2.4.e: Profiles should help the user or their care giver, parent or affinity group to customize services and devices in order to maximise the usability of technologies available.

User in emergency situations

Guideline 5.2.7.a: Profiles should have the ability to change the behaviour of devices and services in response to emergency situations.

Guideline 5.2.7.b: There should be the potential for a profile to contain emergency related information that could be accessed by emergency personnel in emergency situations.

Guideline 5.2.7.c: Every device and service should provide a potential emergency capability for negotiating priority, identifying a user as a first responder, and lowering its impact on a network infrastructure possibly overloaded due to a regional emergency.

Law enforcement

Guideline 5.2.8.a: There should be a mechanism for profiles to be accessed by a third party who has the appropriate legal approval and documentation.

Guideline 5.2.8.b: The profile provider should retain complete and secure records of a request to access an individual's profile in emergency situations.

Profile provider

Guideline 5.3.1.a: Profile providers should be offered a means, under control of the user's profile agent and therefore the user, of synchronizing their part of the profile with other parts of the profile.

One or several profile providers

Guideline 5.3.2.a: Users should be able to have a single integrated view of their profile, even when they have several profile providers.

Profile portability

Goal 5.3.3.a: Users will expect a similar user experience when the profile is moved to a new profile provider.

Guideline 5.3.3.b: Users should be able to change their profile provider when desired, keep their existing profiles and export them to the new profile provider.

Guideline 5.3.3.c: It should be easy to duplicate or import the profile (or parts of the profile) and export it to another profile provider and other profile tools.

Guideline 5.3.3.d: When changing profile provider, there should be no need to redefine existing profile components.

Guideline 5.3.3.e: When the profile provider is changed, the previous profile provider should still guarantee that the user's data is kept private or deleted.

Service developers and manufacturers

Goal 5.4.a: Service providers and manufacturers should decide which parts of the service or terminal are candidates for personalization, e.g. some profile data owned by the service provider or manufacturer cannot be viewed and/or updated by the user such as charging data.

Goal 5.4.b: Service providers and manufacturers should make settings available for external sharing and control by profile providers and end-users (identifying which are standardized and which are service or device unique).

Goal 5.4.c: Service providers and manufacturers should decide in what ways personalization can take place, e.g. by the provision of suitable profile management tools.

Goal 5.4.d: Service providers and manufacturers should produce templates.

A.3 Profile contents

Representing and defining profile data

Goal 7.2.a: The way objects are represented to users should be dependent on user's preferences and the specific context of use.

Guideline 7.2.b: Some values could be represented or defined in absolute terms (e.g. 24th December 2005) or in relative terms (e.g. 2 weeks from now), depending on the user's preferences.

Guideline 7.2.c: Users should be able to access their profile information and profile tools in a selectable language.

Guideline 7.2.d: The grouping of profile data should be consistent and logically related to the task the user wishes to achieve.

Guideline 7.2.e: It may be necessary to provide entry points in different parts of the user interface to the same set of profile data.

Generic or specific preferences and settings

Guideline 7.4.a: Users could define whether preferences and settings are specific or generic e.g. if settings are related to specific terminals/services or to groups of terminals/services.

Defining groups and adding members to groups

Guideline7.6.3.a: The profile tool could offer some predefined groups to help the user take advantage of the concept. The user would then only have to add members to each group.

Guideline7.6.3.b: There should be a mechanism helping users defining their own groups.

Guideline7.6.3.c: For every individual group, users could get a list of objects and rules that refer to that group so that users may better understand the consequences of performing operations on that group.

Accessory

Guideline 7.6.6.a: When an accessory is used the first time, the profile tool should automatically be updated in order to provide the user with the ability to address that accessory and the events associated with it, when defining their profiles.

Guideline 7.6.6.b: Automatic accessory discovery will help the user address new accessories in rules, e.g. for defining automatic activation of profiles.

A.4 Rules

Conditions and actions

Guideline 8.2.a: The user should be able to choose active events from a set of possible events.

Guideline 8.2.b: When the user associates rules with events, then the profile will automatically subscribe to the events.

Guideline 8.2.c: State-changes related to a user's terminals or services need to be communicated to the profile agent in an accurate and timely fashion.

References to objects

Guideline 8.3.a: The profile tool should provide a rule editor that is well-integrated and objects should be easily referred to (e.g. direct manipulation).

Guideline 8.3.b: The user needs to be able to understand the consequences when there are any changes made to objects and they should be informed which rules are affected when objects are deleted or renamed.

Guideline 8.3.c: The user should be able to express and view objects in different ways.

Rule building tool

Guideline 8.4.1.a: Rule building tools and engines should have a mechanism for testing rule changes before incorporating them.

Guideline 8.4.1.b: The user should be able to express and view the rules in different ways such as with words, filling in a table, filling in a form or graphically.

Guideline 8.4.1.c: The rule building tool should propose appropriate rules for the most common uses in rule templates and users should be given a mechanism to choose these templates.

Rule base

Guideline 8.4.3.a: Users may define nested rules, that is, rules referring to other rules.

Guideline 8.4.3.b: Synchronization of the rule bases should be done when there are multiple rule bases and multiple profile providers.

Active and inactive rules

Guideline 8.4.4.a: Users should be given an option that lets them see which rules are active and which are not.

Guideline 8.4.4.b: Users should be given an option that lets them activate and deactivate rules where appropriate.

Rule exceptions

Guideline 8.4.5.a: Users may define a rule and then define zero, one or several circumstances where that rule does not apply.

Guideline 8.4.5.b: One principle is to define what is allowed and then define one or several exceptions. The opposite principle is to define what should be denied and then define the exceptions. Users should be allowed to decide which principle they wish to be applied.

Prevention of conflicting rules and rule bases

Guideline 8.4.6.a: The profile agent should make a plausibility test to detect if there might be conflicting rules, even when more than one profile provider provides profiles for the user.

Guideline 8.4.6.b: If conflicting rules are detected then the profile tool may propose one or more solutions from which the user may choose.

A.5 Default values and templates

Defaults and templates

Guideline 9.2.a: For first time definition of profiles, users should be provided with a ready-to-use profile containing relevant default values.

Guideline 9.2.b: Profile providers should provide templates that relate to a range of types of users and situations.

Guideline 9.2.c: The predefined default parameters in templates provided for users should be acceptable to a maximum (such as "at least 90 %") of the target communities.

Guideline 9.2.d: Users could be provided with a mechanism that allows them to create a new template by customizing an existing one.

Guideline 9.2.e: Users should be able to determine which settings have default values and which do not.

Guideline 9.2.f: If profile providers wish to obtain feedback on changes that users make to the defaults provided by a template, they should always ask the user's permission to obtain that feedback.

Guideline 9.2.g: Provide appropriate default values and allow the user to fine-tune these later if they wish to.

When defaults are not appropriate

Guideline 9.3.a: Where there is a potential legal liability related to a user choice or value, a default should not be used and the user should be asked to make an explicit decision about that choice or value.

Live templates and creation templates

Guideline 9.4.a: When a change is made to a live template, users of profiles derived from that template should be informed that changes have been made and they should be able to discover what those changes are.

Guideline 9.4.b: Subsequent updates of settings resulting from changes to a live template or from updates issued by the profile provider should form the default entries for profile resets.

A.6 Set-up and maintenance of profiles

Scope of profile data values

Guideline 10.3.a: Users should be able to select or define the scope of their profile data values.

Profile tool in a "Design for All" approach

Goal 10.4.1.a: A "Design for All" approach is encouraged so as to make the profile tool accessible to as many people as possible, including elderly people and persons with disabilities, without the need for adaptation or specialized design.

Guideline 10.4.1.b: The profile tool should provide equitable use - The design must be useful and marketable to any group of users - avoiding segregation or stigmatization of any users.

Guideline 10.4.1.c: The profile tool should be flexible in use - The design must accommodate a wide range of individual preferences and abilities.

Guideline 10.4.1.d: The profile tool should be simple and intuitive to use - The design must be easy to use and understand, regardless of the user's experience, knowledge, skills or concentration level.

Guideline 10.4.1.e: The profile tool should provide perceivable information - The design must communicate necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities.

Guideline 10.4.1.f: The profile tool should support tolerance for error - The design must minimize hazards and the adverse consequences of accidental or unintended actions.

Guideline 10.4.1.g: The profile tool should demand only low physical effort - The design must be usable efficiently and comfortably and with minimum fatigue.

Guideline 10.4.1.h: The profile tool should provide size and space for approach and use - Appropriate size and space must be provided for approach, reach, manipulation and use, regardless of the user's body size, posture or mobility.

Guideline 10.4.1.i: Where the user's profile contains information on personal user interface related preferences and settings, these can be used by the profile tool to configure its own settings.

Guideline 10.4.1.j: It should be possible to export and import some personal settings of the profile tools such as preferred language, accessibility settings, notification settings, user defined use of icons, log settings. This is useful, for example, when changing profile provider.

Information about profile data

Guideline 10.4.1.k: Users should be informed about what profile data need to be configured and what effect configuring these will have.

Guideline 10.4.1.l: Users should be given examples of the correct format for the required profile data and support for handling the formats.

Various versions of profile tool

Goal 10.4.2.a: Users should have a maximum of choices concerning the use of profile tool.

Tool available in various terminals

Goal 10.4.3.a: All terminals can be used for activation and deactivation of profiles.

Guideline 10.4.3.b: Alternative interfaces should be available for managing profiles such as display, spoken menus, 12-key keypad.

Guideline 10.4.3.c: Within any type of interface, users should, where feasible, be able to choose between a range of alternative presentation modes (e.g. text or icon).

Guideline 10.4.3.d: Profile providers could offer their services or third party services for managing profiles.

Offline profile management

Guideline 10.4.5.a: The profile tool should make it clear to the user whether they are using their profile tool online or offline.

Guideline 10.4.5.b: If users are updating their profiles offline, the profile tool should inform them about the risk that data in the profile tool might not be up to date.

Guideline 10.4.5.c: If users are using their profile tool offline, the profile tool should inform them that updates to the profile will not be verified by the profile agent until they go online and make the updates available to their profile agent.

Guideline 10.4.5.d: If users are updating their profiles offline, the profile tool should inform them that the outcome of their updates may not produce the intended outcome until they go online and make the updates available to their profile agent.

Guideline 10.4.5.e: If users have been updating their profile tool offline, the profile tool should ask them the next time they go online if they wish to make the updated profile data available to their profile agent.

Language and vocabulary

Goal 10.4.6.a: The profile tools should offer different end user views of the basic profile management functionality that are tailored to the knowledge and experience of the specific groups of users. The vocabulary used should be appropriate to the specific group of users.

Goal 10.4.6.b: A set of user terms, symbols and icons, covering at least a set of key objects (such as listed in clause 7.6, "Overview of a selection of profile objects") should be defined. User terms for at least the major European languages should be standardized.

Goal 10.4.6.c: Where necessary, provide explanations of terminology and concepts that need to be understood by the user.

Goal 10.4.6.d: Terminology and technical concepts that the user does not need to understand should be avoided.

Goal 10.4.6.e: The vocabulary used in profile tool user interfaces should be consistent whether used as written or spoken text, and when used in different profile tools and different terminals.

Goal 10.4.6.f: All tools and services involved in profile management should exhibit the same behaviour in relation to the key profile concepts represented by the user terms, symbols and icons (including at least those listed in clause 7.6, "Overview of a selection of profile objects").

Guideline 10.4.6.g: Users should be able to access their profile information and profile tools in a selectable language.

Guideline 10.4.6.h: The profile tool should determine its initial default language setting from language preferences contained in the user's profile if this preference exists.

Starting values

Guideline 10.5.1.a: The profile should self-populate with the most appropriate default values for user privacy and security.

Guideline 10.5.1.b: A new profile element should self-populate with matching information in the base profile, when available.

Device profile creation

Guideline 10.5.5.a: In the case of first time use of a replacement device, the new device should be able to take advantage of the user's settings (which are contained within a profile) for the prior device, or other devices.

Guideline 10.5.5.b: Always start with the option to explain fully each information field required for device-specific settings.

Service profile creation

Guideline 10.5.6.a: In the case of first time use of a replacement service, the new service should be able to take advantage of the user's settings (which are contained within a profile) for the prior service, or other services.

Guideline 10.5.6.b: Always start with the option to explain fully each information field required for service-specific settings.

Update notification and confirmation

Guideline 10.6.a: For each object in a profile, the user should be able to select whether they wish to receive notification of any updates made to that object.

Guideline 10.6.b: For each object in a profile, the user should be able to select whether they wish to receive a request for update before they confirm that they wish the update to the object to be made.

Guideline 10.6.c: The user should be provided a list of all profile data referring to the updated profile data. The tool may propose different actions to take to resolve any potentially unwanted consequences.

Deletion

Guideline 10.7.1.a: When a profile is wholly or partially deleted, a copy of the original profile should be kept in a place that allows future reuse of that profile.

Guideline 10.7.1.b: Users should be provided with a mechanism that allows them to permanently delete stored copies of deleted profiles.

Guideline 10.7.1.c: The user should be provided a list of all profile data referring to the deleted profile data. The tool may propose different actions to take, to avoid any unwanted consequences.

Guideline 10.7.1.d: When deleting a profile object, the user should be informed about which other objects and profiles that might be affected.

Base profile deletion

Guideline 10.7.2.a: The base profile should not be deleted unless the user decides to stop using the profile service. The minimum information (the user's name etc.) will normally be deleted by the profile provider.

Situation dependent profile deletion

Goal 10.7.3.a: A situation dependent profile can be deleted by the user at any time.

Guideline 10.7.3.b: When a situation dependent profile is deleted, the objects referred to by the profile should not be deleted.

Device profile deletion

Goal 10.7.4.a: Device profiles will not be deleted from the devices, but they may be made unavailable from the profile tool.

Service profile deletion

Goal 10.7.5.a: The service profiles will not be deleted from the services, but they may be made unavailable from the profile tool.

Explicit methods

Goal 10.8.1.a: Keep customization quick and easy to set up.

Guideline 10.8.1.b: Invite the user to customize their profile, and outline the advantages of doing so.

Implicit methods - adaptive personalization

Goal 10.8.2.a: Customizing the interface based on the user's role or subject area can save their time and produce results more closely matching their needs. It is important to be careful not to antagonise users by making incorrect assumptions.

Guideline 10.8.2.b: Users should be able to turn adaptive personalization off.

Guideline 10.8.2.c: Users should be able to be informed about the acquired information, assumptions and changes made when implicit methods are used and have the opportunity to allow, deny or override them.

Guideline 10.8.2.d: Where implicit methods are used, it is necessary to identify the user before collecting behaviour information, not make assumptions based on the use of a specific terminal, as more than one person may use the same terminal.

Guideline 10.8.2.e: The profile agent should explain the advantages of personalization for enhancing the user experience.

Guideline 10.8.2.f: Users should be allowed an option as to whether or not they wish to be made aware that an implicit method has made an assumption about their user preferences. They should also be offered the option about whether or not they wish to confirm the assumption. The user should be allowed to change the options that they have selected at any time.

Guideline 10.8.2.g: Automatic personalization should be avoided unless it can consistently and accurately match users' needs and expectations.

Guideline 10.8.2.h: Users should be able to define if preferences that are explicitly set may or may not be updated by implicit methods.

Guideline 10.8.2.i: Profile agents must limit their implicit data collection to user actions completely within their own scope.

Combination of implicit and explicit methods

Guideline 10.8.3.a: Users should not be asked to enter information that can be acquired by the profile agent from other sources.

Guideline 10.8.3.b: A well-designed profile agent needs to limit the effort required from users in defining their profiles.

Guided Configuration

Goal 10.9.2.a: There should be a balance between the number of steps and the complexity within each step. Any additional number of steps or complexity within each step introduces the potential for errors.

Guideline 10.9.2.b: Users should be informed about what information they need to have ready to hand during the configuration procedure, and if necessary, how to obtain it.

Guideline 10.9.2.c: There should be a clear overview of the steps of the configuration sequence.

Guideline 10.9.2.d: The user should be presented with information about the progress of the configuration.

Guideline 10.9.2.e: Provide a logical and consistent order of the configuration steps. For instance, group together related settings and preferences.

Guideline 10.9.2.f: Navigation should be under user control throughout the configuration. There should be no time-outs that automatically continue to the next configuration step.

Guideline 10.9.2.g: "Back", "next", "cancel", and "finish" as well as "help" functionality and controls should be provided. The "cancel" and "help" controls are especially important when the user is not able to proceed for whatever reason.

Guideline 10.9.2.h: At each step of the configuration the user should receive clear instructions about what type of information is required, i.e. what input information is expected from the user. Illustrative examples could be provided.

Guideline 10.9.2.i: The user should receive clear feedback when the configuration procedure ends.

Guideline 10.9.2.j: If the configuration fails or is aborted the state of the profile should revert to previous step of the configuration, i.e. no preferences and settings within the aborted step should be modified. In some cases, it may be necessary to revert to where the configuration started. The user should be informed on how to proceed in order to complete the configuration.

Undo functionality

Guideline 10.10.3.a: The profile agent should always maintain a copy of the last deleted profile in case the users have any problem when creating or updating a new one. This will prevent the user from losing functionality if problems arise.

Guideline 10.10.3.b: Users should be able to make changes and try them before deciding to commit the changes.

Guideline 10.10.3.c: The profile provider should keep a number (may be defined in a contract) of previous revisions of the profiles.

A.7 Profile activation

Event subscription and notification

Guideline 11.2.a: Profile tools should be provided with all state and location change events available.

User awareness of profile state

Goal 11.4.a: Users should be able to get information about profile state from any terminal.

Activation and deactivation of profiles

Goal 11.5.a: Users should be able to get information about which profile is active from any terminal.

Guideline 11.5.b: Users should be offered the option of being notified of automatic profile activation.

Guideline 11.5.c: Users should be offered the option to choose whether they prefer activation/deactivation to take place with or without having to confirm it.

Different means of triggering the automatic activation of profiles

Goal 11.6.a: Users should be able to activate profiles from any terminal.

Guideline 11.6.b: Users can define activation rules according to their activities and make use of different means to trigger the automatic activation of their profiles.

Guideline 11.6.c: Users should be able to manually activate and deactivate a profile.

Guideline 11.6.d: Manual activation overrides the automatic activation of a profile.

Activation precedence order

Guideline 11.7.1.a: There should be standardized activation precedence defaults.

Guideline 11.7.1.b: Manual activation takes precedence over automatic activation.

Guideline 11.7.1.c: Users may define user-defined activation precedence.

Different types of activation rules

Guideline 11.7.2.a: Users may choose among different types of activation rules.

A.8 Address book management

Support for both UCI and non-UCI address book records

Guideline 12.2.1.a: Address books should be capable of holding records for contacts that have UCIs and for contacts that do not. For this reason, fields for UCI and non-UCI contact information should be provided.

Indicating the presence of a UCI in address book records

Guideline 12.2.1.b: A visual distinction to indicate the presence of a UCI is required (e.g. symbol, icon, or abbreviation). This could be placed with the other UCI data in a displayed address book record. Such a symbol might be as simple as "UCI" if, indeed, this name becomes established.

Presentation of preferred services in address book records

Guideline 12.2.1.1.a: If there are preferred services then these should be made clear by means of appropriate symbols or icons that can be displayed with the data record. In UCI systems, this will be derived from information that the owners of UCIs provide in the additional information field of their UCIs.

Correlation of address book entries

Guideline 12.2.1.1.b: Many address book entries are derived from the record of individual communications. The address book tools should have an interactive mechanism to attempt to correlate communications identifiers from different sessions with the same individuals.

Presentation of charging information in address book records

Guideline 12.2.1.2.a: Information about the charging rate for communication should be imparted by means of a symbol or text placed after the preferred service symbol, icon or abbreviation. For UCI, this will be derived from information that the owners of UCIs provide in the additional information field of their UCIs.

Additional content of address book records

Guideline 12.2.4.a: Consideration should be given to the inclusion of fields for additional information. This additional information could include a voice label or a graphic image, as well as a visible version of some of the additional information fields that are stored for UCIs.

Shared address books

Guideline 12.2.5.a: The capability to allow a number of users to share one or more common address books as well as their personal address book should be provided.

Synchronization of distributed address books

Guideline 12.2.7.a: All address lists associated with different terminals and smart cards may be synchronized with a master list held by the profile agent.

Guideline 12.2.7.b: Dependent on local storage capacity it should be possible to download any record to a terminal address book from the master address book.

Add to address book

Guideline 12.3.1.a: Users need to be given a mechanism to manually add contact data to the address book.

Guideline 12.3.1.b: Users will require the ability to set special conditions which will automatically add an identifier into the address book (or flag up the need for a decision on whether to place the identifier into the address book).

Guideline 12.3.1.c: Where records are added automatically, the user will require the capability of personalizing the label received as part of the contact data. This could be necessary because of duplication (two "John Smith" labels) or because the contact is not normally known by that label to the user.

Automatic completion and correcting of address book records

Guideline 12.3.2.a: Part of the "handshake" between PUAs should include the identification and updating of incomplete or out-of-date UCI address book data.

Guideline 12.3.2.b: Subject to the user's choices on the amount of feedback that they wish to receive, the user should be kept informed of the changes made, and possibly given the opportunity to accept or refuse them.

Changing address book records

Guideline 12.3.2.c: Attempts to remove or modify address book records that are referred to by profile rules or that are members of various lists (e.g. privacy "white list") should be flagged to the user.

Address book record organization

Guideline 12.3.3.a: Users should be able to view their address book records according to different criteria such as group, alphabetic listing of surname, first names, etc.

Searching for contact data across different sources

Guideline 12.3.4.a: Users should be provided with a search mechanism that is consistent across multiple sources (e.g. personal address books, group address books and white pages) and when accessed from different terminal types.

Sending or updating contact data details

Guideline 12.3.5.a: The facility should be available to send contact data details from the user's address book to others address books. Where restrictions have been applied to the transfer or broadcasting of the contact data then this should be made apparent to the person attempting to send the contact data and should not be permitted by the profile agent.

Moving, copying or removing records

Guideline 12.3.6.a: In addition to user initiated moving, copying or removal of records, consideration should be given to allowing the profile agent to prompt the user about when it may be beneficial to move, copy or remove an address book record.

A.9 Information sharing and privacy

Access to profile data

Guideline 13.2.a: A user should be able to differentiate between their own private profiles and those maintained by their employer or organization.

Guideline 13.2.b: Users should be in control over access to and distribution of their user profile data.

Guideline 13.2.c: Only the minimum user profile data requested by an entity should be provided to that entity.

Guideline 13.2.d: For any item of profile data, users should be able to specify that they wish to be asked whether they want that data to be released. Users would expect to be given an explanation why the data is required by external resources or other people.

Guideline 13.2.e: A service shall only share information with another service if the other service is also "trusted" by the user.

Guideline 13.2.f: If a user action incurs an external request for profile information which the user has set as unavailable to the requesting entity, the user should be provided an immediate option to share the requested information on a regular or single time basis.

Guideline 13.2.g: Where information is shared, users should be able to monitor and audit accesses to that data by examining their profile activity log.

Vendor and provider interactions

Guideline 13.3.a: Profile providers, network operators and value added service providers require a mechanism for exchanging profile data in order to enable a seamless service experience for the user.

Privacy levels

Goal 13.4.a: Users should be offered default settings at a sufficient level of security that is appropriate to the data stored or transmitted.

Goal 13.4.b: There should be a common security level at which user identity needs to be verified. The authentication can be controlled in different ways such as one or more of a range of alternative authentication schemes, restrictions to passwords, and choice of authentication method.

Guideline 13.4.c: There should be a mechanism to inform a user whenever any information in their profile above a selected privacy level is read by an external entity, along with identification of that entity.

Guideline 13.4.d: When communicating with devices and services, the profile processing agent should respect user and legally required privacy requirements (see clause 13.8).

Guideline 13.4.e: There should be a mechanism for the user to be informed about any changes of security level.

Guideline 13.4.f: All elements of any profile need to have selectable levels of information sharing to specific single entities or to a well-known sharing group, such as Friends, Family, Business Associates, Buddy Lists.

Guideline 13.4.g: Security levels should have common definitions between entities, so that users can share a common expectation.

Guideline 13.4.h: A new user's default start-up security profile should be preconfigured with default security levels. The user may redefine the security levels at any time.

Guideline 13.4.i: The users should be able to easily understand, chose and apply their desired security policies.

Guideline 13.4.j: The profile provider should apply the appropriate level of security to the transfer of the data.

Guideline 13.4.k: Access to profile data should be limited to the subset of data required to perform the given service or function.

Guideline 13.4.l: There should be a mechanism for informing the user about any identified security breaches.

Privacy policies

Guideline 13.5.a: Mechanisms that respect user's personal preferences with respect to the privacy of their personal information should be used. At this time, mechanisms that are based upon the W3C's P3P recommendation [20] should be used for web-based services.

Guideline 13.5.b: Users should be provided with feedback on whether their privacy preferences are being respected. Users should be given positive indications that their privacy preferences are being met. Where their privacy preferences cannot be met, users should be informed and offered an option that ensures that their privacy preferences will not be violated.

Guideline 13.5.c: Users should be provided a mechanism to request details of any information stored about or relating to them.

Access control and authentication

Guideline 13.6.a: Access to profile data should only be permitted in an authorised and secure manner.

Guideline 13.6.b: Transmitting profile data should be done ensuring that any non-authorised person may not read or modify the profile data.

Guideline 13.6.c: The validity of an authentication should, if required, be subject to a maximum time limit.

Trusted third parties

Goal 13.7.a: Trusted third party services may provide the authentication of identity.

Privacy regulations

Goal 13.8.a: Lawful interception and other regulator requirements may imply that profile data is delivered to authorities (e.g. emergency services), despite the privacy settings.

Access control methods

Guideline 13.9.a: The methods of access control provided should be appropriate to the context in which it is used. Thus, it would be inappropriate to require a very difficult and secure access procedure if no valuable or personal information is potentially under threat.

Guideline 13.9.b: Where a terminal, service or application has distinct sub-applications within it, different access control mechanisms should be considered for some or all of the sub-applications as well as for the terminal, service or application itself (e.g. a user should be free to choose to use the access control procedure provided for their contact information but not to use the access control for all terminal data).

Guideline 13.9.c: Mechanisms that require explicit user presence or intervention but that do not rely heavily on user memory should be considered for use when important security validations are required.

Guideline 13.9.d: Avoid increasing the number of elements that a user has to enter in an access control procedure (e.g. username, password plus one of a number of personal secrets) and putting constraints on the format of these elements (e.g. insisting that a password has a defined mixture of letters and digits).

Guideline 13.9.e: Replacing elements of access control procedures that rely on human memory with other methods such as smartcards or biometric methods will reduce the risk of users compromising security by writing down security information.

Guideline 13.9.f: Where there is a possibility for a password to be stored on a user's terminal, users should be asked whether they wish to enter the password every time or whether they wish to have the terminal remember it for future usage. Where such an option is presented, the user should be warned of the ability of other users of the terminal gaining access to the service or application.

Guideline 13.9.g: Any requirements or limitations of a password (e.g. on the content and/or length) should be clearly indicated to the user when the user is first asked to generate the password.

A.10 Log

Log

Goal 14.a: Users should have access to the communication log (or a filtered version of it) from any terminal.

Guideline 14.b: The content of the log information presented would be subject to rules defined in each user's profile (e.g. the profile rules might specify that logs presented when the user is using a basic voice terminal should only list the last 5 log records).

Guideline 14.c: The profile agent should maintain a log of a core set of operations such as create, update and delete.

Guideline 14.d: Users can choose what they would like to see logged (e.g. what objects, activities, or more complex combinations of these).

Guideline 14.e: Each log will have a minimum set of parameters that will be stored for each log record. Users should be given options to control how much additional details each log should contain.

Guideline 14.f: Users should be given control of how logs should be displayed, including control of the sorting order (increasing/decreasing) of defined item such as date or service. Users could also be offered pre-defined settings suitable for different terminal capabilities, which they could subsequently modify.

Guideline 14.g: Users should be given control of the lifetime of log data. This control could be in terms of the age of the data or in terms of the overall storage space limits to be imposed upon the log data.

Guideline 14.h: Users should be able to view the log data chronologically.

Guideline 14.i: The user should be able to transfer the entire log or parts of a log record between the log tool and another tool or service.

History

Document history		
V1.1.1	August 2005	Membership Approval Procedure MV 20051014: 2005-08-16 to 2005-10-14
V1.1.1	October 2005	Publication