ETSI EG 203 602 V1.1.1 (2019-04)

User Group;
User Centric Approach: Guidance for users;
Best practices to interact in the Digital Ecosystem

Reference
DEG/USER-0047

Keywords
IoT, QoE, 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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This ETSI Guide (EG) has been produced by ETSI User Group (USER).

Modal verbs terminology

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

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

Introduction

The present document has been produced by STF 543 experts.

The concept of the full Project is to define 5 dimension model called **ACIFO.** The 5 dimension model is based on 5 submodels defined as:

- Architectural Model **A**cifo: defines the global structure, including semantics and is optimized for the stated objectives.
- Communication Model a**C**ifo: defines the exchange protocols, including APIs and HMIs, over three planes:
  - Management (Monitoring)
  - Control
  - Usage
- Information Model ac**I**fo: defines the information of the whole ecosystem (equipment, network, applications, services, HMIs, User, etc.) from the offer to the availability of resources for Users, Providers and any other partners. It is a knowledge data base representing the whole ecosystem.
- Functional Model aci**F**o: defines the functionalities (the process) to compose any service based on "micro-services".

- Organization Model acif**O**: defines the role of any actor and which actor is responsible of each action. ("Who is doing what?").

These five dimensions should be shared by the user and the supplier/provider. For the user, it should be possible to define (or to choose) the level of autonomy and control for the personalized composition of services.

The four deliverables produced by STF 543 define the different dimensions:

- ETSI TR 103 438 [i.1] focuses on the Architecture and the Organization. It includes the use cases and the results of the survey.
- ETSI EG 203 602 (the present document) focuses on the information and the functionalities. It is dedicated to the user. It provides analysis and recommendations from the information and functionalities.
- ETSI TR 103 603 [i.2] addresses all the dimensions to the supplier, in order to produce the APIs according to the user expectations and whatever the number and types of additional suppliers.
- ETSI TR 103 604 [i.3] focuses on the communication and in particular on the HMIs.

For example, for Energy (production, distribution, consumption), the supplier will create an API for the user. The information will be exchanged between the supplier and the user, but will not be used only by the supplier: the user will have access to all the information and will be able to use this information to optimize their energy consumption. This data base is a source to provide new services and new applications (for the user and for the supplier). One major challenge and constraint is to ensure that all the private data may be checked and monitored by the user (the contract needs to define clearly these points). The data are not used only by the supplier, the user should have access to the data and may refuse that the data be used or known → an interaction "cursor" between the user and the supplier defines the freedom (GDPR).

1 Scope

The present document defines guidance to the user in order to build its own service composition with the expected and relevant Quality of Experience (QoE) and to ensure their data privacy.

It focuses on analysis of functionalities and information from the user point of view.

It provides recommendations from functional and informational elements.

The present document defines the intersection of the "user centric" and the "user interface" which contains the different profiles of the user and equipment to adapt to user's new needs. Thus according to the possibilities offered by the equipment, the networks and the software platforms, a personalization is possible.

The present document includes the results of an additional survey that complete the results obtained in the initial survey, defined in ETSI TR 103 438 [i.1].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 438: "User Group; User centric approach in Digital Ecosystem".

[i.2] ETSI TR 103 603: "USER Guidance for providers and standardization makers".

[i.3] ETSI TR 103 604: "USER; User centric approach Qualification of the interaction with the digital ecosystem".

[i.4] ETSI EN 301 549: "Accessibility requirements suitable for public procurement of ICT products and services in Europe".

[i.5] Directive on Security of Network and Information Systems and the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

ACIFO: 5-dimension model, based on recommendations and common objectives for Users and Providers, giving the capability for the User to compose the needed services

NOTE: The 5-dimension model creates one unique and integrated solution.

cloud: network of remote servers hosted on the Internet and used to store, manage, and process data in place of local servers or personal computers

dew: programming model for enabling ubiquitous, pervasive, and convenient ready-to-go, plug-in facility empowered personal network

NOTE: Dew computing is a new computing paradigm appeared after the widely acceptance of cloud computing. Dew computing has two key features: first, local computers (desktops, laptops, tablets, and smart phones) provide rich micro-services independent of cloud services; second, these micro services inherently collaborate with cloud services. Dew computing concerns the distribution of workloads between cloud servers and local computers, and its focus is the software organization of local computers. The goal of dew computing is to fully realize the potentials of local computers and cloud services.

edge: computation largely or completely performed on distributed devices

equipment (terminal): in the present document, large range of user and provider equipment, including terminals, gateways, boxes, routers

fog: decentralized computation, data storage and application services

NOTE: Fog computing, also known as fog networking or fogging, is a decentralized computing infrastructure in which data, processing, storage and applications are distributed in the most logical, efficient place between the data source and the cloud. Fog computing essentially extends cloud computing and services to the edge of the network, bringing the advantages and power of the cloud closer to where data is created and acted upon.

micro-service: basic and simple service (with SoA properties) that can be combined for the composition of services as expected by the User

NOTE: The basic concept behind this term is that each service performs a unique feature (e.g. for security, "authentication" is a micro-service, for discovery, "find" is a micro-service).

profile: information template (model) to provide or to access to personalized services

user-centric: user who is the heart of the ecosystem

NOTE: This means that the user constrains the whole environment, unlike other contexts where that is the application (application-centric), or network (network-centric) or the system (system-centric) which constrains the context.

3.2 Symbols

Void.

3.3 Abbreviations

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

API	Application Programming Interface
AV	AntiVirus
CD	Compact Disc
DVD	Digital Versatile Disc
EU	European Union
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
https	hypertext transfer protocol secure
ID	IDentity
IMEI	International Mobile Equipment Identity
MIPs	Microprocessor without Interlocked Pipeline stages
NGN	New Generation Network
OS	Operating System
PaaS	Platform as a Service

QoS	Quality of Service
QoE	Quality of Experience
RFID	Radio Frequency IDentification
SD	Secure Digital
SLO	Service Level Objective
SMS	Short Message Service
USB	Universal Serial Bus
UX	User eXperience
VOD	Video On Demand
Wi-Fi	Wireless Fidelity

4 User in front of the service platform

4.1 From settings to personalized service composition

4.1.1 Generic model

The generic model from the User point of view, as defined in ETSI TR 103 438 [i.1], is shown in figure 1.

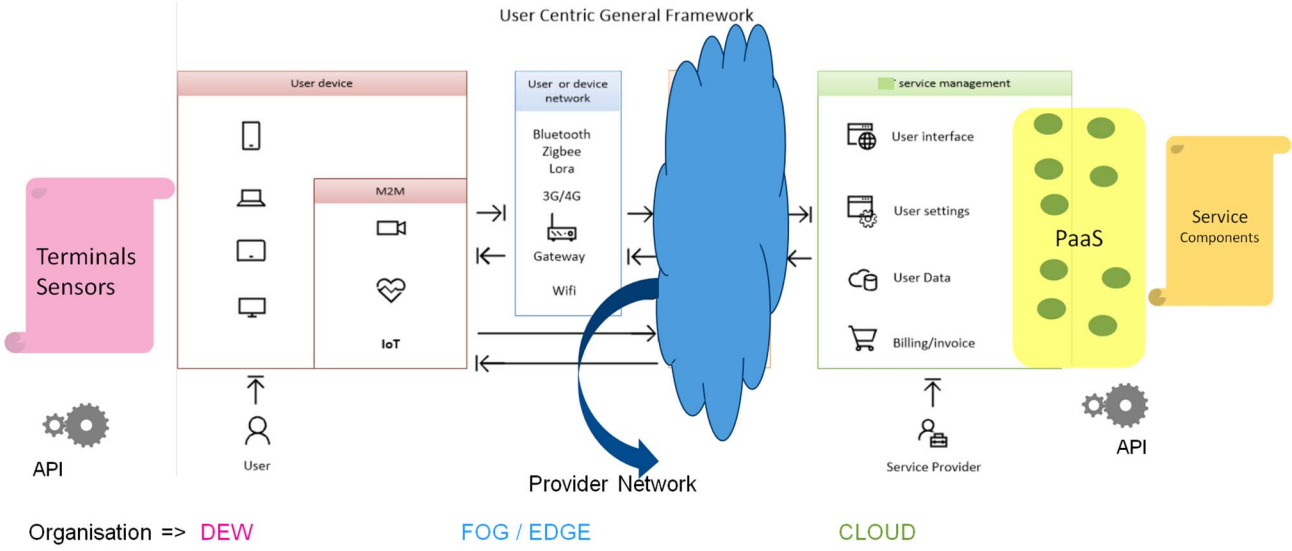

Figure 1: "User-Centric" generic model

What are the reading keys of this generic model of the digital ecosystem as proposed in ETSI TR 103 438 [i.1]?

The emerging usages and the providers' strategies will be put in perspective with the new emerging paradigms:

- On one hand, the human dimension, the more active role of users, the consumers behavior (mobility, social networks, interest groups, groups of customers, etc.), the need of service personalization, the wish that all the technologies are available for everyone and that the virtual reality is supporting the human reality.
- On the other hand, services are dematerialized, which changes the way to design services, the assembly of services, the way to deliver services to consumers and to ensure service continuity and even the consumption modes of the user who becomes more and more the " master of the game".

The global objective is to facilitate access to usages in providing personalized information at the right time.

That means that the relationship between users and providers are evolving significantly. From the passive client incurring offers to the active user who takes ownership of the central role, applicant of innovation, personalization and freedom.

This "user-centric" evolution implies to provide contents and personalized services to the user, depending on location, agenda, preference, at the right time, without technical, spatial and temporal constraints, in a framework of confidence and of shared freedom.

4.1.2 User point of view

First, user has a more and more thorough of the offers. User expects to dispose of rich and pertinent information within the environment, including opinions coming from social networks, from comparison tools and measurement tools. User may also expect to be able to use real engineering and personalized tools. The price based on usage offers a wide flexibility to the user. Per share offers are replaced by packages of customizable services.

Services offers should be adjusted to lifestyle changes, users' habits, especially in urban environment, but also in rural environment which create insulation.

Services operating hours reach out to 24 hours a day, 7 days a week. Dematerialization may reduce user trips and enables home delivery services, signatures of contracts, invoices which is an economy source for users and providers. Dematerialization goes together with eco-attitude.

Personalization means exploitation of client personal data. This situation may be paradoxical because on one hand the client may wish a " user centric" offer and on the other hand the user is sensitive to risks on personal digital privacy. The sensitivity level is variable depending on cultures. The challenge of personal data protection is consequently important and personal data exploitation should have a sufficient counterpart, in terms of added value in services delivery.

This information personalization may be more than the use of collaborative filtering. It may use the users browsing behaviors to offer predictable contents. The proposals remain targeted and coherent, independently of the channel.

Personalization is contextual and uses in particular the location in order to meet expectations of customers who are looking for local services (agencies, shops, cinemas, public services, car parks, etc.).

Secondly, dematerialization results in fully digital managing of data and professional documents (contracts, invoices, flyers, technical contents, administrative supports, mailing and messaging) which transit inside companies and/or in the context of exchanges between partners (administrations, clients, providers, etc). Dematerialization is the replacement of printed documents by digital supports, leading to the paperless office. Beyond supports dematerialization, the commercial activities which have been during a long time supported by physical agencies are dematerialized via web, mobile web, call centers or video call centers.

Moreover "user experience" becomes "multichannel", that means, a coherent service delivery, whatever the access mode to information system and in particular that any done operation, whatever the equipment (terminal) and all the channels.

Additionally a process initiated via one of the channels may be carried over another or several others.

A strong decoupling is needed between the business functions delivered by the heart of the distribution system and the presentation layers.

The evolution of economical organizations including the specialization by profession will need an orchestration of the specific contributions to propose a high added value to the user, a seamless offer rather than an incoherent juxtaposition. Inevitably this leads to design an architecture-oriented service and platforms "as a service" (PaaS).

To complete it should be noted that users grant a very high importance to own mobile phone, which includes a lot of possibilities ("a real swiss knife"), providing comfort, cocooning in the private life, affect, professional efficiency, but also perceived as intrusive.

4.2 User expectations

4.2.1 User experience (UX)

A good digital user experience is based on:

- always on line;

- services easily accessible anytime and everywhere;
- on demand;
- at real-time;
- available in self-service along with a fast helpdesk service response.

For the user, that means a good level of flexibility and control of his digital environment.

People need to find easily and quickly information about a service:

- How to order it?
- How going to pay for it?
- How to configure it?
- How to keep the control on it?

Users also need to be in a relationship of trust with their providers. That means that users benefit of transparency and proofs of security and privacy protection.

As part of the development of the present document a survey has been conducted in order to understand what is the current level of flexibility control, or trust, as perceived by the users themselves, and what should be expected for the future.

Four pillars for a good quality of user experience were identified:

- **Control:** the ability to manage the device or the subscription.

  i.e.: connection priority, control of applications in the background, battery life, etc.

- **Privacy and security:** the need of transparency security and privacy protection.

  i.e.: cookies control, localization control, the ability to hide the text of sms received, etc.

- **Flexibility and customization:** people want to have services adapted to their profile, and the context of use.

  i.e.: setting according to the location, smart synchronization, senior applications or parameters, etc.

- **Affordance:** in relation with user friendly conception of the services.

  i.e.: plug and play concept, clarity and contextual menu, banishment of technical vocabulary, some help notice or bubble information, etc.

All these expectations are the same whether for private or professional use.

Figure 2 shows the respective weight of each pillar according to the customer as a result of the survey.

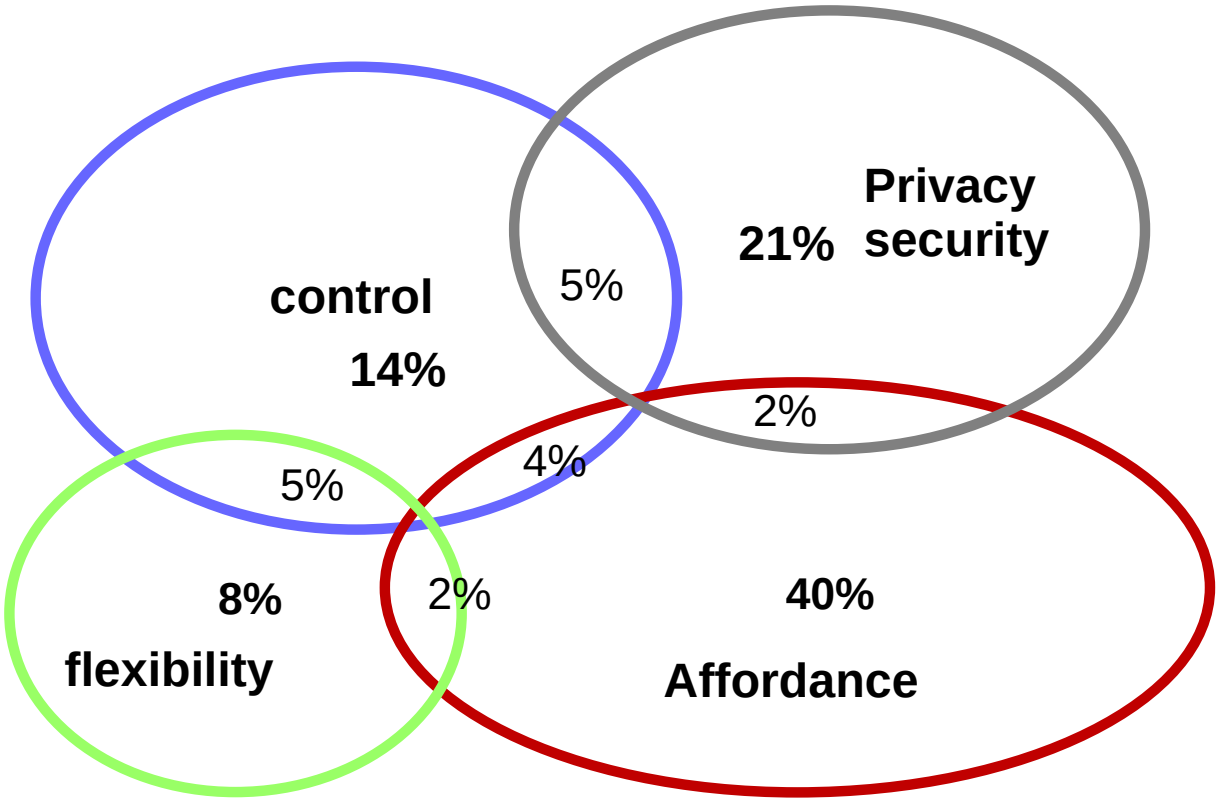

Figure 2: The 4 pillars for a good quality of user experience

Affordance is the most important for user. The requirement to obtain a good level of satisfaction is linked with the user-friendly interface.

Today the situation is not very good on this point and the survey reveals the difficulties to set up smartphones and boxes: the average score is below 5 out of 10 for the smartphone and around 5 out of 10 for the box.

The lack of knowledge about the successive mobile generations (and consequently of the respective capabilities) is also point out.

Today a very large majority of people would like to be able to much more flexibility and indicates difficulty to make the own composition of services because of the low scalability of the offers.

There is also a lack of information or accurate information about the service or the level of quality or availability of the service (mobile coverage knowledge for example).

When looking at digital future, customers declare themselves confident for more friendly, more customized and flexible environment (around 60 % with positive opinion on this matter for the future).

On the contrary, people are not very reassured about safety and respect of individual freedom in the future (more than one in three have a doubt or do not know).

Users have shared opinions about what they will be able to control within their digital environment in the future.

The user centric approach promoted in the present document has the goal to provide more quality of experience within the next generation network and digital services provisioning.

4.2.2 Security: data protection and privacy

4.2.2.1 User expectations of Data Protection

Most user experience of GDPR is the consent to receive emails and the terms and conditions they automatically consent to. Findings from the additional survey showed that 46,8 % of respondents support strong regulation of digital services. This aligns with the goals of GDPR to improve the confidence users will have in companies who handle sensitive and personal data, but the survey also showed when asked 'How do you see your digital future?' 54,8 % believed there will less respect for individual freedom. Though due to GDPR being still a recent development there is still time for companies and service providers to implement policies and measures which will ensure respect for an individual's online digital freedom. Key elements that user should be aware of under GDPR.

Breach Notification - Under the GDPR, breach notification will become mandatory in all EU member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". There is a mandatory statement from GDPR Directive to be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access - Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them are being processed, where and for what purpose. Further, another mandatory statement of GDPR Directive: the controller to provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten - Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17 of GDPR Directive [i.5], include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests. From the additional survey when asked if users had exercised this right only 14,7 % said they had while 66,7 % said they might consider it in the future. Overtime more people will likely exercise this right.

Data Portability - GDPR introduces data portability - the right for a data subject (the user) to receive the personal data concerning them, which have previously been provided in a 'commonly use and machine-readable format' and for which the right to transmit that data to another controller has been given. This has yet to be fully implemented with only limited testing by different companies. An example is the Data transfer Project which is an open-source initiative which features data portability between multiple online platforms made by large technology companies. Some of the expected use cases for users porting data directly between digital services and platforms include the means to transfer contacts, messages and media between platforms without losing access to them or having to recreate them or a user does not agree with the privacy policy of their music service. Users want to stop using it immediately but do not want to lose the playlists that have been created by users. Using this open-source software, users could use the export functionality of the original Provider to save a copy of personal playlists to the cloud. This enables users to import the lists to a new Provider, or multiple Providers, once on a new service that have been decided.

4.2.2.2 User expectations of Privacy

In this context of designing a user-centric digital eco-system, when it comes to privacy, there is often a focus on optimising the settings and permissions of an application or service.

To obtain views from citizens, a Euro-barometer survey on e-Privacy was conducted by the Commission throughout the EU. The key findings are the following:

- 78 % say it is very important that personal information on their computer, smartphone or tablet can only be accessed with their permission.
- 72 % state that it is very important that the confidentiality of their e-mails and online instant messaging is guaranteed.
- 89 % agree with the suggested option that the default settings of their browser should stop the sharing of their information.

When the survey conducted in this project shows:

- 76 % of people claim they have not enough tools or means to challenge their provider on the privacy respect.

- 87 % would like to hide their location by themselves and dynamically depending application or situation.
- 71 % say they use an add-blocker on their PC.
- 40 % never or rarely use a Wi-Fi connexion for privacy and security reasons, and that is the main reason for not using Wi-Fi.

Also, there is the issue of free or very low-cost service which users are willing to use but do not want companies to take advantage of personal data which pays for those free services this is the 'privacy paradox'.

This privacy paradox is a consequence of the competing demand to use information technologies (including social technology and social software) and have an online persona, while simultaneously having to guard against potential threats to personal safety and privacy resulting from the misuse of available information either by companies or individuals.

The privacy paradox is illustrated in the survey results available in ETSI TR 103 438 [i.1].

To the question 7 "would you like to be informed when you are risking entering into an area with low or no coverage?" a large majority of users replied "yes".

Within the questions 12 related to the battery life, a large majority of users would require information on the data collected and the possibility to monitor it in order to get the most out of the battery life.

The question 31 "do you want more pro-active assistance from your telecom operator?" is also very revealing about the privacy paradox. At this question a majority says "yes" for more pro-active assistance as long as the security and privacy are ensured. On the other hand users are very reluctant to give access to their personal agenda. This means that only with a complete trust in their service providers, the end-user would like greater pro-active assistance.

To the question 32 "do you think you have enough tools or means to challenge your provider?" the majority of users did not trust the level of security or privacy respect of the providers as already seen.

4.3 Service composition

4.3.0 Introduction

"User Centric" context involves providing the user the ability to compose:

- content and personalized services according to user's location, agenda and preference;
- without technical, spatial or temporal constraints;
- in an trusted environment and shared freedom.

In the digital ecosystem it is necessary to consider users as communicating entities that are connected to the network not only occasionally but permanently. The new context is "always connected". Users should be able to access the services from anywhere, at any time and using any means of access. This is the principle of "anytime, anywhere and anyhow". The two concepts are complete only if the notion of use is integrated. A user should be able to use the same service (offer) in different desired ways.

The composition of services according to the structuring of the user's information and preference is presented in clause 4.3.1. The adaptation and customization of services according to the representation of all the ambient resources are represented in clause 4.3.2.

4.3.1 Services offered by composition

The user profile provides the image of the user with user's preference, possibilities and constraints, in a structured and uniform format. This profile provides an easy access to all necessary data and relevant selection of each service component according to the user's preference.

In this context the user services composition can be based on:

- service discovery in an environment;

- service preference;
- continuity of services according to user's location and agenda;
- the degree of service security (authentication, authorization, confidentiality, cryptography, etc.).

Each service composition proposed by the provider may be linked to a user service session.

4.3.2 Adaptation and personalization of services

The location-based service adaptation, personalization and user context are three new highly correlated terms that are important in the new digital ecosystem.

Figure 3 shows the adaptation and customization of services according to the location of the user (temporal / spatial). Intersections connect and limit the choice of resources: equipment, networks and service. The central intersection in figure 3 includes usable solutions.

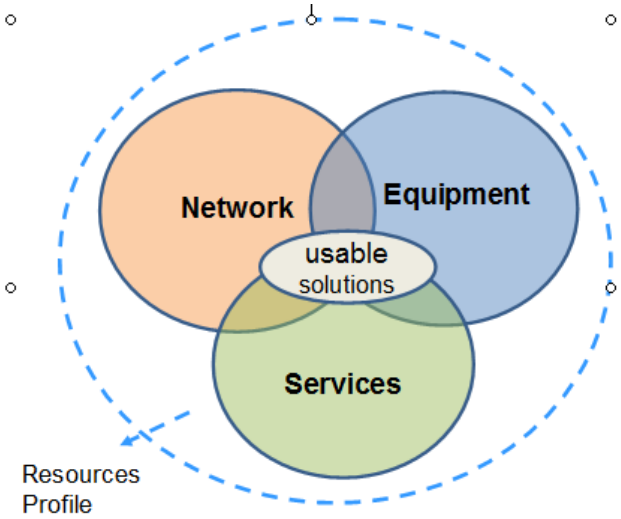

Figure 3: Adaptation et personalization of services

The usage may change according to the location and time.

As an example, a user subscribed to a video on demand (VoD), when the user is at home (broadband access), the preference is to receive the movie on high-resolution television. If the user is travelling and would like to watch a movie on the train using the same VoD service on a computer, the conditions will not be the same. In the absence of a broadband connection it will not be possible to keep the same quality of service if the real time is requested.

5 User process for Smart Meters (functional model)

This clause is based on the use case studied in ETSI TR 103 438 [i.1] to explain the process of digital service, from the point of view of the user. "Smart meter" is chosen as it broadly represents the presence of digital services at home.

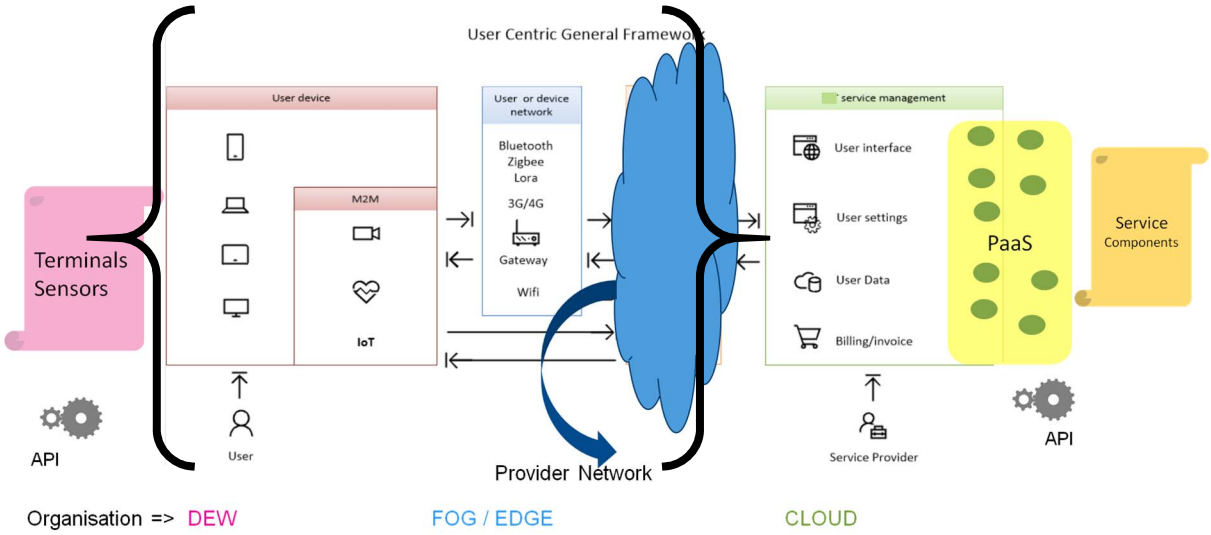

Figure 4: Generic Model for User process

Within in the functional model of the smart meter, the user has control over a few key elements. These are mostly related to the billing process. With Gas and Electricity suppliers there have been efforts made to make it easier for Users to move between different suppliers in order to achieve the best value for money. While for Water and Sewage companies the user often cannot change supplier most companies now make it as easy as possible to change details or keep the same accounts for example if users move home but are still within the catchment area for that company to minimise disruption for the User. For bills and payments, utility companies aim to allow customers control over how users pay for example monthly direct debit, traditional quarterly bills, use feed-in-tariffs, etc. Users are able to change payment details, if by direct debit the date the money is paid on or if the users believe that they have over-paid users can apply for refunds from the company (some countries require this to be done automatically) and finally with the switch to online accounts users are generally able to better see the own history of payments and bills which allows users to track how much they are spending but also compare to other deals and offers users may receive.

Within the User Centric General framework, the user process for smart meters occurs within the brackets on the diagram below. The smart meter functions are managed by a single user and include the utilities meters themselves which measure the amount of water, gas or electricity that has been used. The smart device that displays the amount of power or water has been used and the cost of them. This smart device will also contain the means to communicate wirelessly with the physical meters themselves and send a regular meter reading to the utility or meter company.

The services can be solely in used in-house whiles others need access to resources outside the house. Smart metering functions for utilities are stand-alone in that they report usage of resources and how much money has been spent. Apart from when they send meters updates to the utility company. They enable budgeting by allowing the users to know accurately how much they are spending on gas and/or electricity or water. The user(s) is (are) consumer(s) but may also be producer(s) (e.g. energy, applications, etc.)

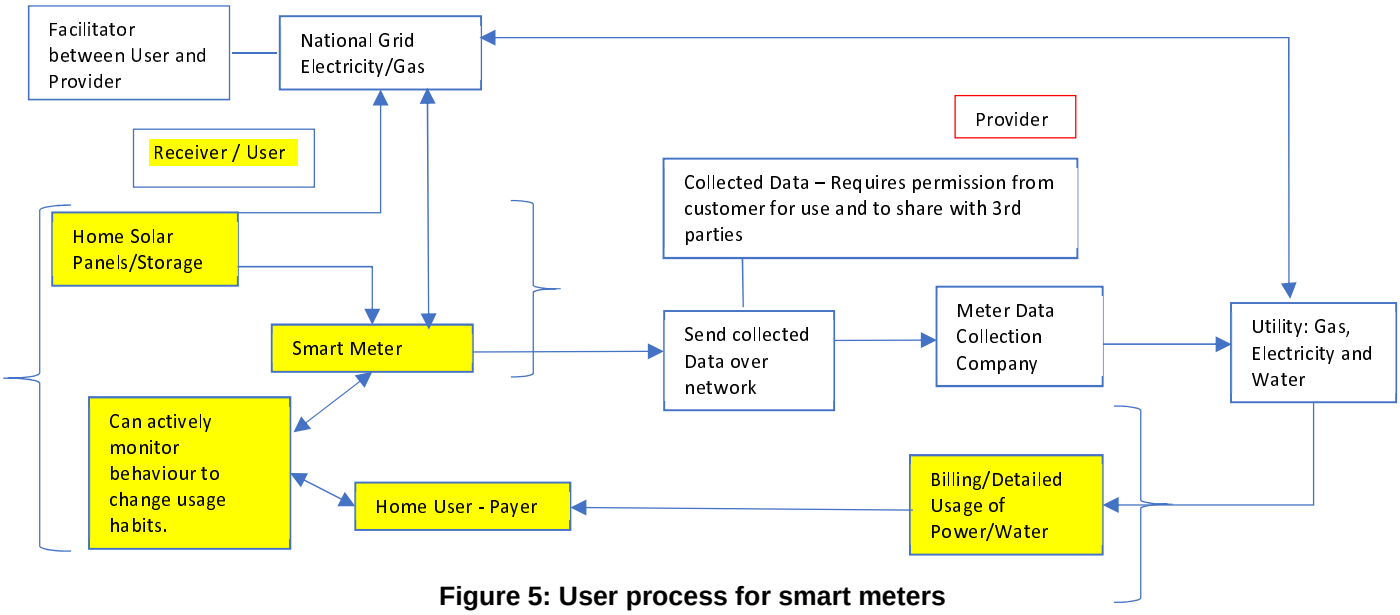

Figure 5: User process for smart meters

Highlighted in the process flow diagram in figure 5 is the areas where the user has a degree of control over within the User centric general framework. The provider part (in red brackets on figure 4) may be found in ETSI TR 103 603 [i.2].

When interacting with the control interface of the smart meter the user may change some settings and parameters within allowances set by the service provider. For example, the frequency of alerts the user wants to receive e.g. how much money the user has spent for a given time period. Also, the user would like to take some action on the information sent to the service provider, e.g. frequency of meter readings, from every hour to once a day for example. Finally, the user may have the option to customize the user interface to personalize the experience e.g. background, colour of text, screen brightness, etc.

Types of services the User should control over within their digital eco-system.

- Budget control: Home user can be a single or multi-person household. With Meters moving from 'dumb' to 'smart' when they are smart it should allow Users to better monitor energy and water usage and cost. Though it should be noted that it is still possible when meters are dumb but it requires greater effort to estimate cost and usage.

- Data protection and privacy: The companies that handle the metering, billing, data storage and transfer of data, should follow data protection regulations. These include Directive on Security of Network and Information Systems and the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 [i.5]. The energy supplier should obtain permission/consent from the bill payer which is the User to use their data for a stated purpose. Also, under GDPR a User has the right to obtain any data held on them therefore the service companies should maintain data in an easy to access and read format.

- Energy/water usage. Billing: Energy supplier; Water/Sewage suppliers; Metering companies; Supply networks. All of these collect Data about their User or customers. Therefore, they requires permission from customer for using and to share data with 3rd parties. A user has the right to know under GDPR what their data is being collected for and how it is going to be used. Also, since smart waters allow real-time monitoring of use by the user, they can change their habits and identify points of waste quickly which has the potential to save the user money while it allows the companies to also save resources, they need to maintain supplies. Decreased water and energy use overall is better for the user, companies and the environment.

6 Profiles (Information model)

6.1 User profile

6.1.1 User profile representation

The user profile is a key element of the proper functioning of digital ecosystem. User Profile provides information about the user in private and professional life, habits and preferences. In fact, the knowledge of the digital ecosystem relating to the user and user preference is strongly linked (limited) to the information collected in the user's profile.

That is why the proposed modelling and profile structuring have been guided by, on one hand, concerns to satisfy the "anywhere, anytime" and on the other hand, real-world modelling according to four levels of visibility. Namely the levels are "User, Service, Network, Equipment (Terminal)". For people with special needs, additional information are available in ETSI EN 301 549 [i.4].

To define the information necessary to User Profile representation in a generic and exploitable manner the following information may be required:

- **Personal information:** contains all the attributes describing the user's personal and / or business information.
- **Role information:** represents the user role.
- **User Geo-spatial information:** includes the attributes that are particularly attached to a given location, which should satisfy the need "anywhere." Information pertains to equipment, networks, and services related to the user's known location.
- **User agenda information:** traces the user's schedule with user's communication needs and user's intended location. This criterion should satisfy the "anytime" needs.
- **User preference information:** contains the user's different choices regarding equipment (terminals), networks and services based on spatial (location) and time (agendas) parameters. These preferences may constrain the various existing possibilities to a reduced set according to the user wishes.
- **User resource information:** includes services, networks and equipment capacities.

6.1.2 Personal information

This part collects all information related specifically to the user. Depending on the desired visibility, the forms contain all the information describing the user in a specific community. The data in each form is attached to the user regardless of time or location.

This information is classified into two subsets "Personal" and "Business". Mechanisms are provided to allow the user to define the information that will be visible in different communities. The data visibility (public, private, protected) can be defined manually by the user as well as by a deduction using self learning mechanisms.

The "personal contact" includes the attributes giving access to all the information concerning the user's personal life (see figure 6). These attributes are attached to the user regardless of user's location, time, usage or special needs when applicable. The visibility of these information can be chosen by the user. Indeed, if needed, the user would be able to define for example a pseudonym which will replace in another form the name and the first name, when the user expresses the obligation to remain them confidential. As a result, the user has the opportunity to define as many "personal contacts" as wanted to be able to use them in different communities.

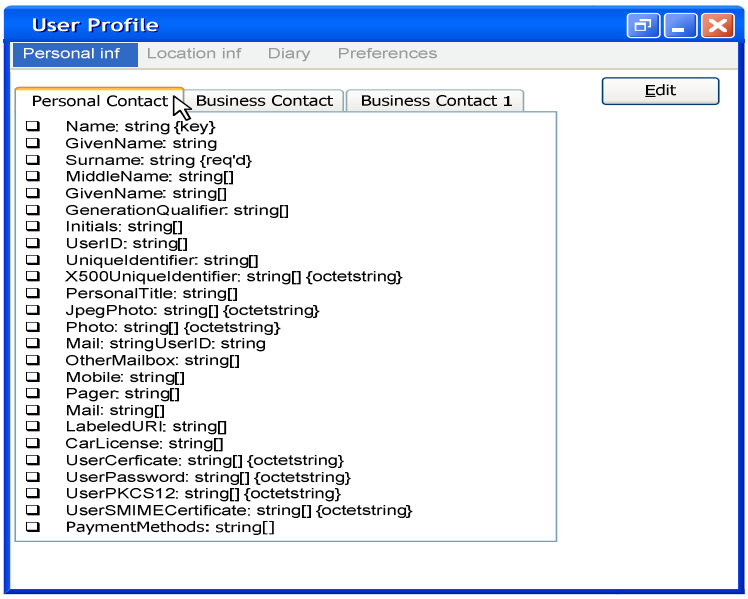

Figure 6: User personal information

Figure 7 illustrates the attributes that provide information about the user's business life. Business contact includes information only valid within a given organization. However, in the case where the user performs several jobs in different and independent organizations, it would be possible to define separate business forms for the user within each organization.

Note the presence of information on personal laptop, which does not depend on a particular location.

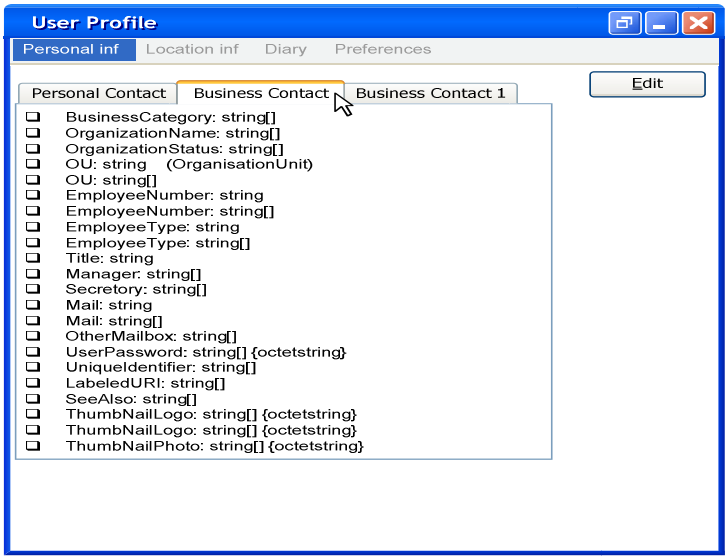

Figure 7: User business information

However, if necessary, the user can define other records that contain attributes describing a specific set of information relating to a particular use, to differently represent the user in different communities, or if there are special needs.

6.1.3 Role information

Role information represents the role played by each user when initiating the session. The user may play several roles which give the possibility to open or close some privileges or some service offers.

The user plays different roles in different situations, and consequently may have different responsibilities, by example at home a user may be a parent of children, and in the office may be a manager of employees. So, for the different roles a user may have different responsibilities. User has the possibility to swap from a role to another during the same session.

6.1.4 User geo-spatial information

6.1.4.0 Introduction

Some of the user-related information is strongly related to a particular location. Indeed, depending on the user's location, a set of possibilities is offered to him. Once the user leaves this location the possibilities are no longer accessible.

To enable the digital ecosystem to make the most of the environmental possibilities, means are provided so that the user may record the characteristics of the frequently visited locations: home, office, car, etc.

The characteristics of the user's work environment and house should be specified and the information recorded in two different entries ("Home" and "Office") relating to the location.

Note the structure that describes the information about the description of the location, then the equipment (terminals), networks and services available in this location. Subsequently, once the user is located, the digital system should take into account this information to customize the user's request according to the specificities of the location and the specific preference.

6.1.4.1 Information about the residence

To be able to dynamically account for all the possibilities of access to information in a location where the user is, the information may be recorded in separate records relating to a specific location.

Figure 8 shows the information to describe in detail all the specificities of the user's residence. For each residence the relevant information at the residence will be collected and recorded. This information includes the attributes that are used to describe the actual location (e.g. address) as well as all the service, network and equipment options that the user has the right to access inside the residence.

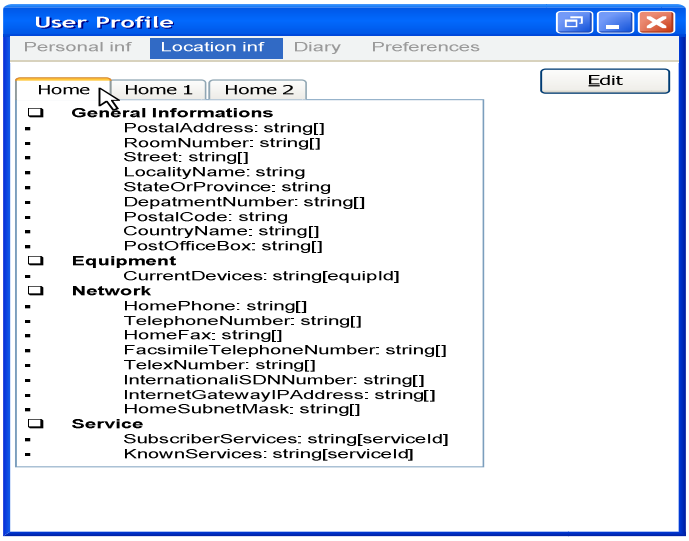

Figure 8: Location-dependent information, Home

6.1.4.2 Information about the workplace

Figure 9 shows a form that gives access to information about the user's workplace. Like any information sheet about a physical location, it is formatted in four parts that give access to all the attributes describing the general information about the location and the possibilities offered in terms of equipment (terminals), networks and services.

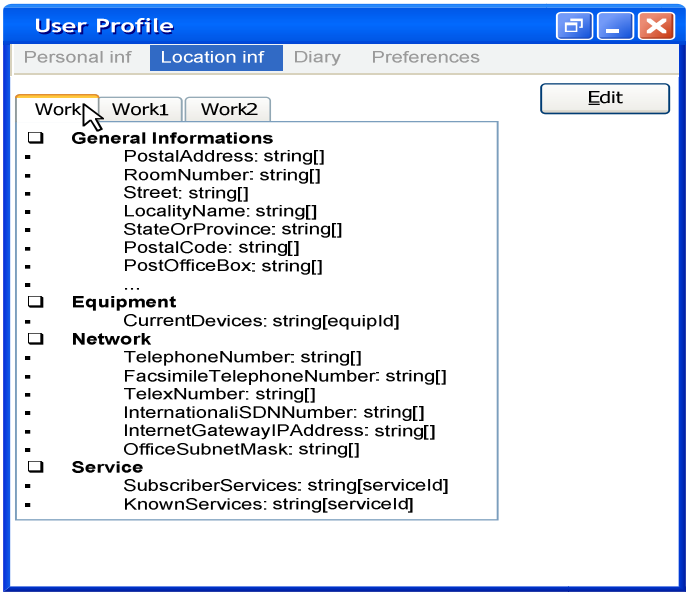

Figure 9: Location-dependent information, Office

As illustrated in figure 8 and figure 9, it would be possible to save several forms each describing a different location in a given category. In the presented example, two categories may be seen. They are defined as "home x" and "work y" and each contains several forms. However, the user may add other (e.g. the car, meeting room, etc.).

6.1.5 User agenda information

The agenda maps the user's needs in terms of communication and intended location. The user has the possibility to define in separate forms the information and temporal preference that should be taken into account by the digital system. Indeed, this criterion should make it possible to take into account the preference of the user at any time and thus satisfy the need for "anytime".

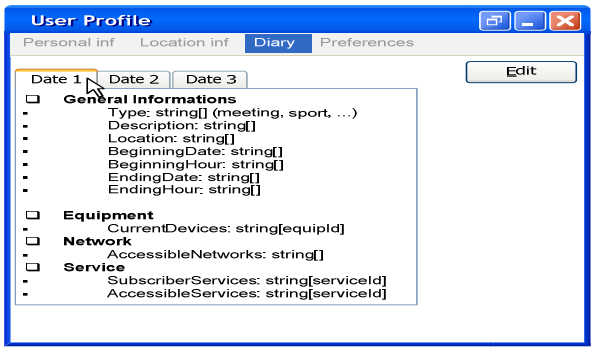

Figure 10: User agenda

Figure 10 shows an example of an agenda form and the information it contains.

6.1.6 User preference information

6.1.6.0 Introduction

This profile identifies the user preference in the NGN (Next Generation Networks) context in terms of equipment (terminals), networks and services according to the location (space), agenda (activities) and role (e.g. Parent/child).

The general preferences are also recorded such as language or payment modes preference.

The user preferences are loaded at each time. A set of accessible resources are ready to be deployed in the user ambient surrounding.

6.1.6.1 General preference

General preference attributes express the wishes of the user without limiting them to a specific scope. These attributes are indeed high-level constraints set by the user.

Figure 11 shows an example of general preference attributes. These attributes allow users to specify a constraint that limits all of the existing possibilities for a given attribute. For example, if the user has previously defined several payment methods (credit form, direct transfer and check) the one to be used in priority should be specified.

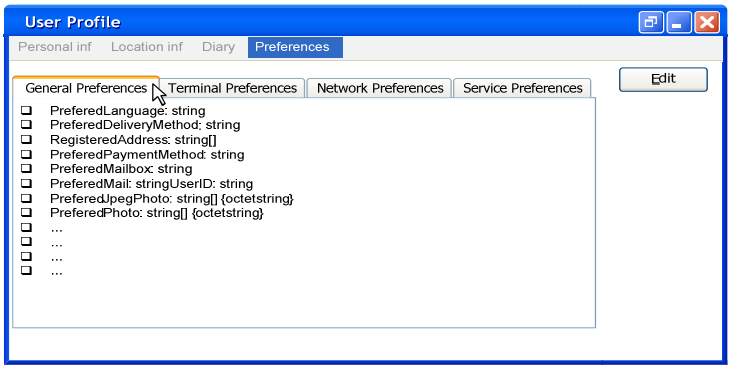

Figure 11: User general preference

6.1.6.2 Equipment (terminal) preference information

Equipment preference allows users to specify which equipment should be used first in each case. When the user has special needs, the equipment should fulfil the characteristics as defined in ETSI EN 301 549 [i.4]. The present document then allows the choice of one of several available equipment when the requested service can be rendered by several of them.

Figure 12 shows some attributes that can be used to express the user's preference for the equipment. As illustrated, the user may define for each specific location the equipment that should be used in priority. Indeed, the fields of this form make it possible to give priority to the equipment when the user has several. Thus, for example when in the office profile there are several equipment for display, the user could specify the one to be used in priority.

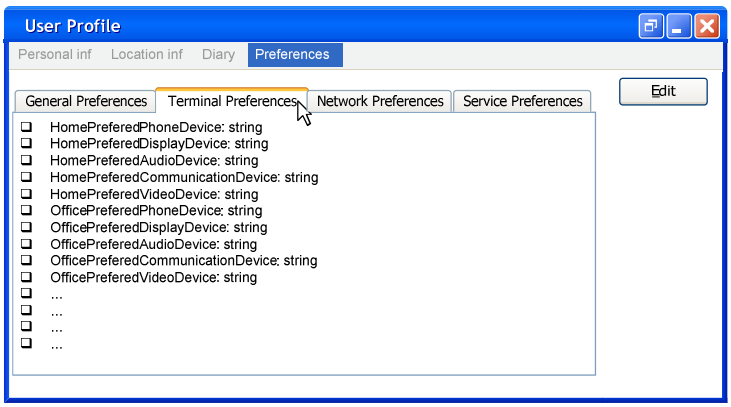

Figure 12: Equipment preference

In the case of example, the user can define priorities of use for all available equipment (depending on the location and special needs) in the workplace ("Work" form) and in the personal residence ("Home" form).

6.1.6.3 Network preference

The digital system should allow users through network preference to choose in their profile which preferred networks to be used to access services among the available networks.

Figure 13 illustrates network preference that can be specified by the user. Indeed, the user using this form has the means to choose the order in which the networks will be used primarily.

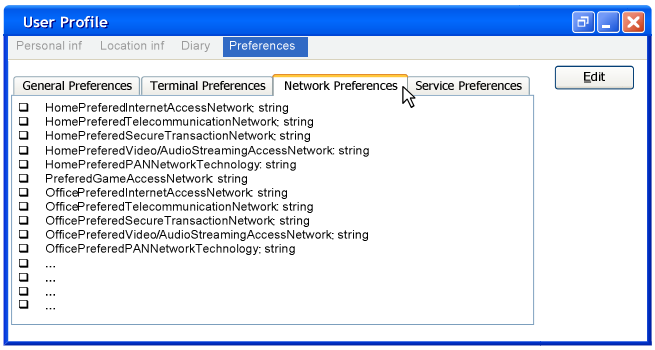

Figure 13: Network preference

6.1.6.4 Service preference

Like the equipment and network preference users can specify the service preference.

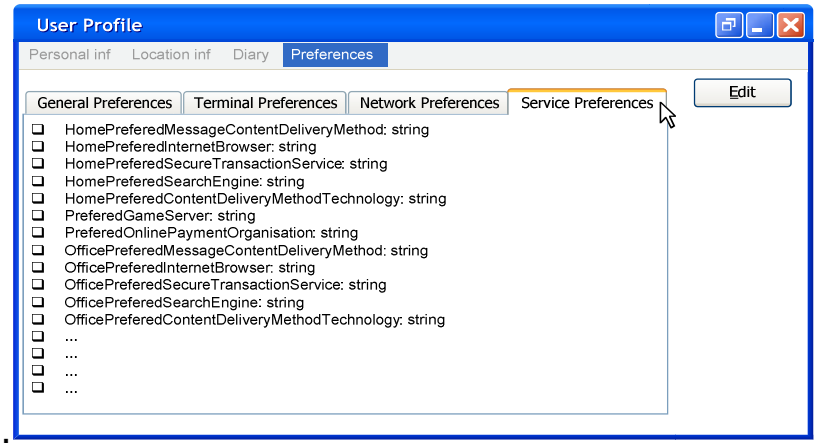

Figure 14: Services preference

Figure 14 shows some attributes of "service preference". As illustrated, the user has the opportunity to choose among all similar applications (services), those wanted to be used in priority. Thus, the user has the possibility to define, for example, the non-paying services or those included in his package as services that should be used in priority.

6.2 User resource profile (equipment, network, service)

6.2.0 Introduction

To provide generic and personalized access to services, features and capacity of the user's equipment should be taken into account. Indeed, the rendered service and its QoS (Quality of Service) are limited by the capacity of the user's terminals. Service components can be distributed across multiple devices. Therefore, the logic of the personalized service can depend heavily on the equipment capabilities. The term equipment is used to refer to any "support component" that takes part in the access procedure and the implementation of the service (functional dimension). Accessibility services may be defined as service preference.

The equipment profile (terminal, box, router, etc.) should include information to identify it, and then determine its performance (QoS). If all the equipment does not support all the functionalities provided by a service, the QoS will be strongly limited by the most restrictive equipment.

In addition, access to the service should to be taken into account. Embedded software capabilities and equipment access interfaces also play an important role in the customization and adaptation phase of the service. Therefore, they should also be taken into account to select the appropriate service components in order to build a personalized service that meets the user's request.

User resource profile includes three parts: equipment (clause 6.2.1), network (clause 6.2.2), and service (clause 6.2.3).

6.2.1 Equipment resource profile

The generic equipment resource profile should contain the following attributes:

- ID (Identifier)
- Hardware Capabilities
- Software Capacities
- Input / Output Capabilities.

ID (Identifier) to uniquely identify a device. The IMEI (International Mobile Equipment Identity), number for portable terminals or the serial number and the manufacturer's name for laptops are two examples.

Hardware capabilities include information about the physical capabilities of the equipment. This is the QoS offered by the provider defined by criteria like availability, capacity, and reliability. Therefore essentially Memory, Power Supply and the Central Unit may be found. In a first approach, the Memory covers the availability criterion, the duration of the service rendered by the equipment depends on the Power Supply and the MIPS of the Central Unit (processing capacity). Reliability is evaluated based on the number of erroneous instructions per second.

The embedded equipment software builds a runtime environment for the user's services (software capabilities). The type and version of the embedded OS, the embedded platforms (software / middleware) and the software associated with the Input / Output belong to this category. Information on the execution context and services already available locally (shared or not) can be obtained.

Input/output capabilities includes the means of communication of the equipment with his entourage (the human-machine interface (HMI) and Storage). It can be quoted:

- HMI:
  - Keyboard (yes, no, special), mouse (yes, no, 2 or 3 buttons), etc. For people with special needs, the equivalent or alternative to the keyboard, mouse, screen, sound should be taken into account.
  - Screen (resolution, colour, number of sequences per second), printer (resolution, colour, number of pages per second), sound (compression, buffer size, number of output channels, special processing), etc.
- Storage:
  - USB key (yes, no, special format);
  - the card (yes, no, type of interface: SD, micro SD);
  - CD / DVD reader / writer (yes, no, speed, format, etc.).

6.2.2 Network resource profile

The generic network resource profile should contain the following attributes:

- Access Types:
  - Long range: 4G, 5G, Ethernet, Wi-Fi
  - Low range: Bluetooth, RFID, etc.
- Bandwidth
- Download Capacity

6.2.3 Service resource profile

The generic service resource profile should contain the following attributes:

- Service types:
  - Security services: authentication, authorization, cryptography.
  - Billing services.
  - Preference services.
  - Notification services.
- Validity period.
- SLO (Service Level Objective).

The Service Level Objective is the means for the user to express his needs. The objectives expressed by the user may be linked to the end-to-end SLO. Indeed, if the user requires a service composition, the conditions linked to their operation such as capability, availability, scalability may be specified.

6.3 Data protection

This is more often associated with businesses and service providers when they are implementing cybersecurity methods. But the general principles of data protection are relevant to the end-user when they use their devices and use those devices to access services over the internet. These solutions are good universal practises for data protection which all users should aim to follow. For users with special needs, information are available in ETSI EN 301 549 [i.4]:

1) Protecting data in transit: When using internet sites that require sensitive data (bank details/payment cards) to be entered check that it is using secure which often is indicated by a https prefix. This means that a secure connection means a user's information is private when sent to a site. Over open and public networks Virtual Private Networks (VPNs) are one of the most common and effective cryptographic methods used to assure the confidentiality and integrity of data when transmitted. These are designed to protect Data in transit that may be at risk of attacks such as interception, traffic replay, manipulation or jamming.

2) Protecting data at rest: Wherever data is stored, even temporarily, it may be vulnerable to unauthorised access, tampering or deletion. The most common methods of cybersecurity will ensure these risks are minimised. These include enabling firewalls, having anti-virus software, encryption of storage drive and enabling regular backups of data and systems.

3) Protecting data on mobile devices: The methods are similar to protecting data at rest. This means not installing unknown or un-trusted applications. Recent smartphones and mobile operating systems also support data encryption which should be enabled. Also, if the device supports back-ups these should also be done at regularly intervals.

4) Secure Disposal: Any data which is sensitive to the user should be removed from the media which stored it; just hitting 'Delete' is not enough. It is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of disposal will allow the user to re-use the media, while others are destructive in nature and render the media unusable. This can be achieved by either rewriting or formatting the storage media until the old data cannot be recovered in a meaningful way. Also, a destructive method is shredding the storage media so data recovery becomes impossible.

7 Recommendations

7.1 QoE

Already today, and much more tomorrow, users have the ability to access a large number of digital services applications and contents covering almost every time and everywhere a big part of daily life, for personal or professional activities.

In order to get the most benefit of all the services people have to develop own know how, that means improve the level of maturity.

The degree of maturity of the user is partly due to user's involvement, control expectations, and of course the diversity and frequency of the used services:

- Today 34 % of people change the setting of smartphone less than once a year.
- 56 % of survey respondents never or rarely get on line to the personal page of their fix subscription and it is quite the same for the mobile (53 %). Obviously, for these people, it is difficult to have a good level of knowledge and control.

The architecture and software oriented of next generation networks are able to improve the flexibility and dynamic management and control of the services.

If this user centric approach is correctly performed the user will be able to develop skills and ability to choose the right services and compose them in the own digital environment.

User should challenge much more providers and ask himself some important questions, as in figure 15, about the wanted level of customization, the privacy and security requirements, the part of personal information the user is willing to give for a contextual service delivery, the desired monitoring tools to have in order to control the used services.

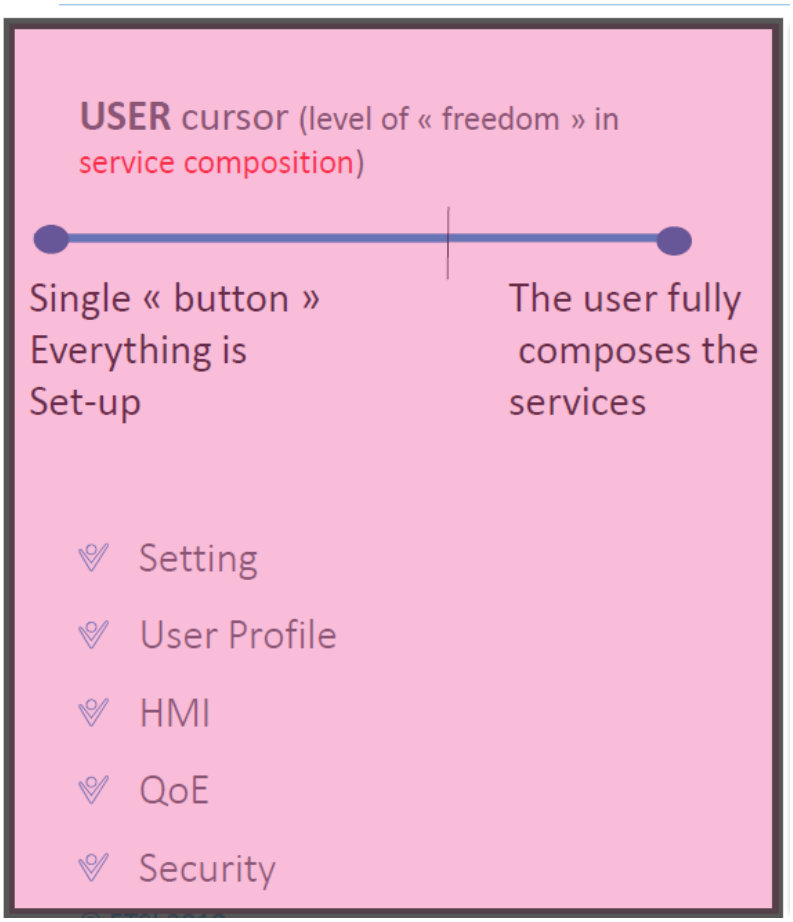

Figure 15: Illustration of the User "cursor"

The degree of maturity of the user is partly due to personal involvement, expectations of control, and the diversity and frequency of the used services.

But in an affordable, easy to use and ubiquity digital environment the user know-how should quickly be developed, and really obtained according to the expectations.

7.2 User and digital services

7.2.1 User Services best practices

7.2.1.0 Introduction

The user view is mainly translated by requirements of " offer understanding/service discovery" and " service personalization" which get along with a "service continuity (for the mobility)" (clause 7.2.1.1). This personalization may only be done that through functionalities (clause 7.2.1.2) based on the user profile (identity, preferences, special needs if any, location, agenda) and on resources profile (service, network and equipment), and depending on the execution context and environment context. This knowledge base requests good security practices (clause 7.2.1.3).

7.2.1.1 User Process best practices

How to make a request or to choose or accept a service?

In an ecosystem where everything is service, a service as seen by the user is necessarily a composition of elementary services that has to be learned to distinguish. The good practice, the good reading grid is to:

- Distinguish the different levels of service which differ in the nature of the service rendered. There are at least four levels of visibility. Each level (figure 16) proposes the abstract image of an autonomous network, able to analyse and deal with problems in the limits of own responsibility.
- Each level includes components (nodes) and put in relation these components (links) in order to build a network (meaning enchainment) which offers a transparent service.

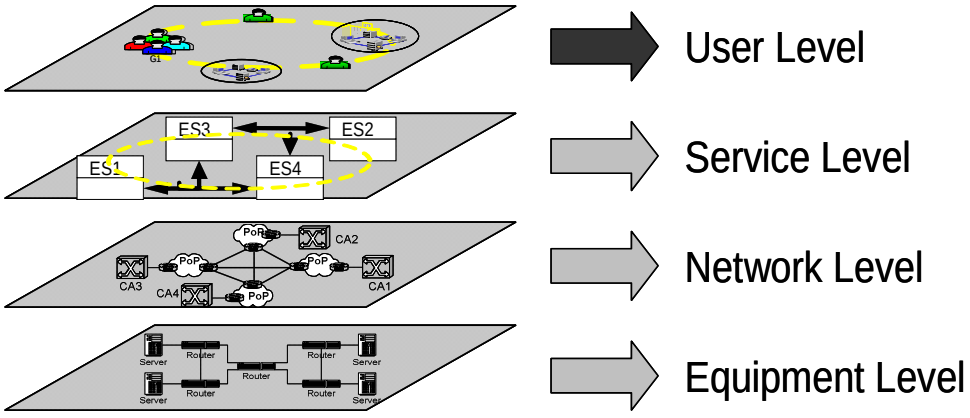

Figure 16: Visibility levels

So, depending on the QoE, the user may, either operate at once the whole process which makes the service in a transparent way, or translate the request by selecting and setting the desired composition.

7.2.1.2 User Management Services best practices

Regardless of the organization (Cloud, Fog, Edge or Dew -smartphone or PC-), the platform places at the disposal of the user the tools for all the use cases.

Good practices include the following management tools:

- Request Process: this service allows the user to request a commercialized service without needing to take care of the way the service, setting and personalization are provided.

- Service choice: this service allows the user to choose a commercialized service without having to take care of the way the service, setting and personalization are provided.
- Profile preference: this service allows the users to define preferences and to enter personal information. A form (model) is needed.
- Environment knowledge: This service updates, dynamically, the knowledge data base which contains information about the environment context and location.

7.2.1.3 Security best practices

There are certain steps and actions that home users can take in order to minimise or prevent them from becoming victims of cyber-attack. From the additional survey when asked the main concerns of digital services the primary concern with 49,2 % was to identify theft and coming second with 20,4 % the unauthorised use of personal data by a 3rd party. This indicated that users have an understanding that cyber threats exist and with encouragement should willing or able to follow cybersecurity best practices.

End-User cybersecurity best practise can only be encouraged through education and awareness programs that promote good security behaviour. Technology Companies, Service Providers and Governments carry out education and awareness campaigns to achieve this but when dealing with human behaviour there is always uncertainty that people will always adhere to good security practice. This means secure by design and secure by default are needed to protect against users who fail to follow good security practices:

- Patch regularly. The user should update their software and devices as often as they can. By patching user can prevent or minimise the chance of successful attacks. Most modern software have automatic patching programs. The user should turn them on and say "yes" whenever they ask for update.
- Use antivirus (AV) software and update it. It does not matter which one a user chooses or whether it's a free or full version, user should be using some form of AV software and let it update automatically. This includes all users, whatever the implemented OS. AV software is like the hand washing of the computer age; in the ever-increasing connected environments, there is a for need basic sanitation to help prevent the spread of infection.
- The User needs to think before clicking. Use common sense before interacting with links or attachments. Does something sound too good to be true? Are Users wondering why someone sent them a file? Does the link look weird when a User hover over it? If users are asking themselves these questions, they probably should avoid clicking it. This relies on continuous education and awareness programs or campaigns to ensure user remains engaged with cybersecurity.
- Users should only use trusted software from official sources. Many platforms use certificate schemes and managed sources to ensure that users are downloading safe applications or software. Though often there are cases where users will download and use software that comes from 3rd party sources either as part of their work or hobby. If they follow good security practices they should remain safe.
- For Network Security User should only allow trusted and known devices to connect to their home networks to present an unknown device spreading malware to other devices. Also, firewalls should always be enabled on devices that support them. If the device does not support firewalls the router can be set-up to provide limited protection for all devices that are connected to it.

In the digital ecosystem in a perfect world if service providers follow security by design and secure by default methods there should be no need for users to worry about cybersecurity as all data and devices would be protected from cyber-attack. Also, if the user were fully aware and alert they would never fall for social engineering attacks that aim to steal personal detail to allow the attackers to either steal money from bank accounts or infiltrate devices and demand a ransom to stop them releasing personal information or give access back to the victim. Though these security practices rarely happen therefore a user has to take basic steps to implement security on devices and networks. Service providers have made it easier and simpler so generally, the security is on by default for devices and applications. Governments and technology companies have also stepped measures to educate and make people aware of the different type of cyber-threats/attacks and the measures that if taken will minimise the chance of them becoming victims. The need to develop good security behaviour in users is vital in an ever more connected world as data, information and services become entwined if one part of this connected web is compromised it can lead to a cascade of problems for victims from stolen money, identity theft and fraud.

With the high-profile case of cyber-attacks that include ransomware, chip security vulnerabilities of Spectre and Meltdown, to the Cloud storage hack which led to many actors and celebrities have pictures of them leaked. These incidents have brought the issues of cybersecurity to people's minds and shown them the need to understand and implement cybersecurity procedures.

With GDPR coming into force in Europe has led to service providers and users to better examine their protection from cyber-attacks and how their data is collected, used and protected. Though this does not mean all users are following cybersecurity best practises and there is still a long way go before this happens.

7.3 User and data

7.3.1 User profile

The user profile is a key element of the proper functioning of digital ecosystem. User Profile provides information about the user in private and professional life, habits and preferences. To define the information necessary to User Profile in a generic and exploitable manner the following information should be available:

- Personal information (personal and / or business information)
- Role information
- User Geo-spatial information
- User agenda information
- User preference information

This information identifies the user preferences in the NGN **(Next Generation Networks)** context in terms of equipment (terminals), networks and services according to the location (space), agenda (activities) and role (e.g. Parent/child).

The general preferences are also recorded such as language or payment modes preferences.

The user preferences are loaded at each time. A set of accessible resources are ready to be deployed in the user ambient surrounding.

Each information should specify two types of data:

- shareable data;
- sensitive data (non-shareable).

7.3.2 User resource profile

To provide generic and personalized access to services, features and capacity of the user should be taken into account in following levels:

- equipment (equipment resource profile);
- network (network resource profile);
- service (service resource profile).

The rendered service and its QoS (Quality of Service) are limited by the capacity of the user's terminals. Embedded access interfaces should by play an important role in the personalization and adaptation phase of the service.

Access network to the service (5G, Wi-Fi) will have to be taken into account in network resource profile.

In service resource profile the Service Level Objective (SLO) is the means for the user to express his needs.

Furthermore, each user resource level should contain security requirements. For example:

- equipment (fire wall);

- networks (cryptography);
- service (authentication, authorization).

7.3.3 Data protection

Most users' experience of GDPR is the consent to receive emails and the terms and conditions they automatically consent to. The goal of GDPR is to improve the confidence users will have in companies who handle sensitive and personal data. Key elements that user should be aware of under GDPR: Breach Notification; Right to Access; Right to be Forgotten and Data Portability.

Sensitive data should be signalled in user profile for all information contained, as defined in clause 7.3.1.

The degree of security should be signalled in each user resource profile level: equipment, network, service, as defined in clause 7.3.2.

The general principles of data protection are relevant to the end-user when using own devices and using those devices to access services over the internet.

These include:

- Data Integrity.
- Protect data in transit (network).
- Protecting data at rest.
- Protecting data on mobile devices (equipment, service).
- Secure Disposal.

There are key privacy elements and principles that users should be aware of when choosing a service in order to be confident that the provider is following the best privacy by design practices:

- The service provider provides the identity and contact information of those responsible for data protection both within their organisation and to individuals.
- The service provider adopts a 'plain language' policy for any public documents so that individuals easily understand what they are doing with end-user personal data.
- The service provides provider's individuals (user or customer) with tools, so they can determine how they are using personal data, and whether personal policies are being properly enforced.
- The service provider offers strong privacy defaults, user-friendly options and controls, and respect user preference.

Annex A:
Additional Survey

An initial survey has been described and analysed in ETSI TR 103 438 [i.1]

An additional survey is contained in archive eg_203602v010101p0.zip which accompanies the present document.

Annex B: Bibliography

Harvard Business Review in 2010. https://hbr.org.

ETSI EG 202 009-1: "User Group; Quality of telecom services; Part 1: Methodology for identification of indicators relevant to the Users".

Annex C:
Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Emeritus Professor, Noemie Simoni, Telecom-Paritech

Other contributors:
Associated Professor, Tatiana Aubonnet, CNAM

Alex Cadzow, Cadzow Communications Consulting Ltd.

Bernard Dupré, AFUTT Chair

Qostic Chair, Pierre-Yves Hébert, AFUTT

Graduate Engineer, Frédéric Lemoine, PHD CNAM

Doctor-Engineer, Jean-Yves Monfort, AFUTT (STF 543 Team Leader)

History

Document history		
V1.1.1	February 2019	Membership Approval Procedure MV 20190406: 2019-02-05 to 2019-04-08
V1.1.1	April 2019	Publication