ETSI TR 103 603 V1.1.1 (2019-03)

User Group;
User Centric Approach;
Guidance for providers and standardization makers

Reference
DTR/USER-0048

Keywords
IoT, 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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

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 Technical Report (TR) 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 the STF 543 experts.

The concept of the full Project is to define a 5 dimension model called **ACIFO.** The 5 dimension model is based on 5 sub-models 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 [i.2] 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 (the present document) 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 meaning that an interaction "cursor" between the user and the supplier defines the freedom (GDPR [i.11]).

1 Scope

The present document defines guidance to the providers and standard makers to ensure that each service component is provided with the information needed by the user to make an informed choice. It addresses all the dimensions of ACIFO to the supplier, in order to produce the APIs according to the user expectations and whatever the number and types of additional suppliers.

The present document is designed in conjunction with the user guide, ETSI EG 203 602 [i.2]. Each recommendation which has been identified as important for the user finds its parallel for the supplier offer, as defined in the present document.

For each need and expectation, by user categories, the present document recommends relevant service information and functions. This is to facilitate, on the one hand, easy access for the user and on other hand, consistently create manageable services that are easily incorporated into a service definition that can support Service Level Agreement (SLA).

The recommendations are intended for the user to be able to compose own services according to the needs, the location and activities. The concept of this new vision is detailed 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 EG 203 602: "User Group; User Centric Approach: Guidance for users; Best practices to interact in the Digital Ecosystem".

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

[i.4] ETSI EG 202 009-1: "User Group; Quality of telecom services; Part 1: Methodology for identification of indicators relevant to the Users".

[i.5] ETSI TR 103 304: "CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services".

[i.6] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.7] ETSI EN 301 549: "Accessibility requirements for ICT products and services".

[i.8] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

[i.9] ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security controls".

[i.10] ISO 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

NOTE: Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[i.12] Arc Advisory Group: "Cybersecurity Maturity Model".

NOTE: Available at https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model.

[i.13] Dan Blum: "How to Assess Security Maturity and Make Improvements", Security Architects Partners.

NOTE: Available at http://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/.

[i.14] Gregory White: "The Community Cyber Security Maturity Model", Research Gate.

NOTE: Available at https://www.researchgate.net/figure/Community-Cyber-Security-Maturity-Model-CCSMM-5-Levels_fig1_235142909.

[i.15] NCSC: "Guidance B3 Data security".

NOTE: Available at https://www.ncsc.gov.uk/guidance/b3-data-security.

[i.16] Information Commissioner's Office: "Data protection by design and default".

NOTE: Available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.

[i.17] NCSC: "General Data Protection Regulation (GDPR)".

NOTE: Available at https://www.ncsc.gov.uk/GDPR.

[i.18] Federal Trade Commission: "US-EU Safe Harbour Framework".

NOTE: Available at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

[i.19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.20] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

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: distributed computing paradigm in which computation is largely or completely performed on distributed device nodes

equipment (terminal): user and provider equipments, including terminals, gateways, boxes, routers

fog: provides close 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 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:

ACIFO	Architecture, Communication, Information, Functionality, Organization
ACL	Access Control List
AES	Advanced Encryption Standard
AKA	Also Known As
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information/National Agency for Information Security Systems (France)
API	Application Programming Interface
BYOD	Bring Your Own Devices
CES	Customer Effort Score
CIA	Confidentially, Integrity and Availability (Model)
COOP	Continuity Of Operations Plan
CPU	Central Processing Unit
CX	Customer eXperience
DDOS	Distributed Denial-Of-Service
DMZ	DeMilitarized Zone
DPA	Data Protection Agency
DPO	Data Protection Officers

DRP	Disaster Recovery Plan
EN	European Standard
EU	European Union
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
ICE	Interactive Connectivity Establishment
ICS	Industrial Control Systems
ICT	Information and Communications Technology
ID	Identity Document
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
KPI	Keu Performance Indicator
M2M	Machine to Machine
MVP	Minimum Value Product
NCSC	National Cyber Security Centre (UK)
NGN	New Generation Network
NIS	Network and Information Security
NIST	National Institute of Standards and Technology (USA)
NPS	Net Promoter Score
OTTS	Over The Top Services
PaaS	Platform "as-a-Service"
PC	Personal Computer
PDA	Personal Digital Assistant
POC	Proof Of Concept
QoE	Quality of Experience
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RSA	Rivest-Shamir-Adleman (public-key cryptosystems)
SaaS	Software as a Service
SECaaS	Security-as-a-Service
SIEM	Security Incident and Event Management
SLA	Service Level Agreement
SLO	Service Level Objective
Vapp	Virtual application
VM	Virtual Machine
VoIP	Voice over Internet Protocol
WiFi	Wireless Fidelity
UMTS	Universal Mobile Telecommunications System
UX	User eXperience

4 Provider Service Platform

4.1 Open Service Platform

The generic model, as defined in ETSI TR 103 438 [i.1] is to design autonomic services, easing service composition to build a digital ecosystem where everything is offered in service.

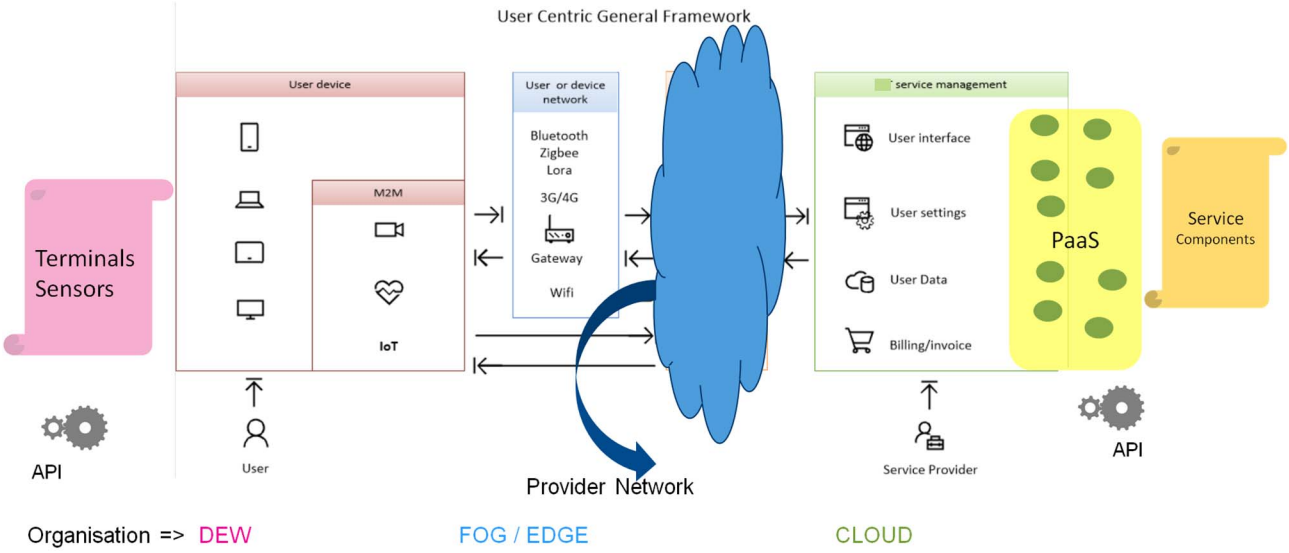

Figure 1: "User-Centric" Generic model

Nowadays cloud computing offers services over open platforms and changes the whole ecosystem of ICTs and telecommunications. This is a strong desire to change the way to offer, to manage and to pay the digital services. These systems are in an approach where "everything is service". They provide services accessible to a maximum of users who only pay for what they consume.

Enterprises and organizations strive to adapt themselves to this new digital ecosystem, the objectives of which is to provide services which are provided and managed in a transparent way with a relevant level of requested QoS.

The consumers' needs in QoS terms vary with their profiles (developer, service provider, final user), with the application domain (business, IoT and M2M) and with their strategies (green, effective cost, etc.). These open platforms need to have properties of elasticity, high availability, reliability, etc. to ensure SLAs (Service Level Agreements).

Furthermore, Quality of Service management all along service consumption needs a setting and dynamic adjustment of resources when running. This dynamic process is possible only if the system is able to have and use pertinent information to predict the relevant consumption of needed resources for the applications taken over. Monitoring techniques are therefore needed to obtain measurements able to highlight a potential event of degradation or failure. These measurements should also allow an autonomy of adaptation for each service.

The objective of the present document is to draw attention to expected properties for the management of user services (clause 4.2.1), security (clause 4.2.2) and to characterize the PaaS which collects the applicative offers (clause 4.2.3).

Clause 4.2.3 is about analysis and modelling "as a service". It describes the structuring choices in terms of "cloud" components to be built with functional and unfunctional parts. It presents a generic model to design autonomic services, easing service composition to build a digital ecosystem where everything is offered in service.

4.2 Providers

4.2.1 Provider services management

4.2.1.1 From QoS to QoE

Quality in the service area can be evaluated from different perspectives and therefore using different measurement methods:

a) the first is related to the reliability of the equipment and can be measured accurately via technical means, although these measurements might be expensive because of both the dispersion of the test results and the size of the sample to be tested;

b) the second is related to the service provision and is closely linked to the kind of use of the service. Therefore, appropriate indicators have to be defined according to use;

c) the last is intended to measure the subjective satisfaction of the customer and there is often no other means than a survey to get it.

In the two first categories, technical means can be used to perform the measurements and in such cases, standards are often useful to achieve a common approach; such standards are given as references where appropriate. They include a precise definition of what is meant as a failure: total failure, poor performance, back-up situation, etc. Assessing these different aspects is of paramount importance to the provider who endeavours to improve the offered QoS.

From a user viewpoint, the end-to-end QoS is the most relevant. Hence objective and subjective measurements may be usefully combined for a better assessment and the whole user approach and is called Quality of Experience (QoE). The subjective part is named User eXperience (UX) or Customer eXperience (CX).

The methodology for identification of indicators relevant to the users in order to measure the quality of telecom services is giving in an ETSI guide produced by the User Group: ETSI EG 202 009-1 [i.4].

This ETSI guide describes the methodology for evaluating the quality of service throughout a customer's journey: Pre-sales, Sales, Provisioning, Service Operation, Service Breakdowns & Interruptions, Claims, Billing/Payment and Termination. The concepts of service and supply are specified as well as that of "Service Level Objective". Finally, ETSI EG 202 009-1 [i.4] specifies the methods for analysing user expectations in terms of quality of service based on four criteria (availability, integrity, time and capacity) and three types of needs (flexibility, ergonomics and security).

4.2.1.2 The UX pyramid

On a subjective perspective named User Experience (UX), the gap between the expected quality and the perceived quality is evaluated.

Providers should consider 3 levels of user requirements:

- **The basic one is about the utility of the service:**

  As seen in the survey results available in ETSI TR 103 438 [i.1] if people do not understand the benefit of a service the users are not willing to use it and dissatisfied if the service has been subscribed. To ensure the usefulness of a service provider can make some pre-tests with users, as Proof of Concept (POC). It is interesting in this context to work on a minimum of high value functionality, generally named Minimum Value Product (MVP).

- **The second level focuses on the affordance (intuitive ergonomics) of the service:**

  The survey shows that setting a smartphone or a box is not very easy and that there are high expectations in the ergonomics of telecom services.

  A key indicator of the customer experience seen from the point of view of ease of use is the Customer Effort Score (CES) promoted at the Harvard Business Review in 2010 (https://hbr.org). It measures the level of pain to use a service, and it can be applied on the whole customer journey.

- **The last level regards the pleasure of use:**

  In the Kano model (https://www.kanomodel.com/) the user satisfaction is high when all customer requirements are perfectly performed, and, from this point it is possible to provide some non-expected services for a "positive surprise" effect.

The current and easy way to measure this level of satisfaction is to use the Net Promotor Score (NPS) indicator.

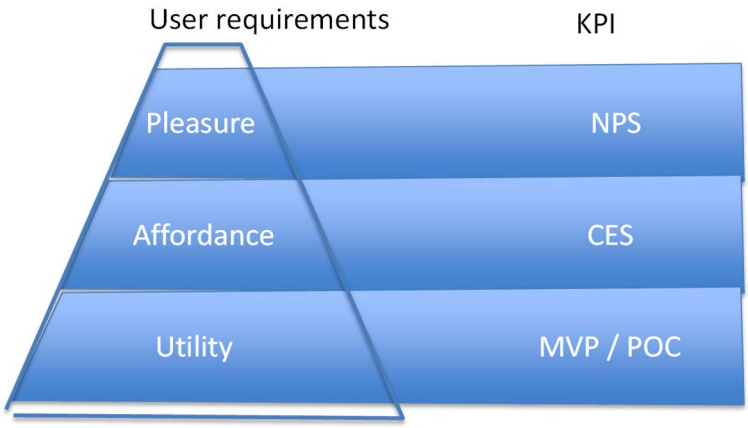

Figure 2: The UX pyramid

4.2.2 Security, data protection and privacy

4.2.2.1 Security

This clause aims to show what is expected of service providers to be compliant with regulation by ensuring they have sufficient measures in place to provide cybersecurity, data protection and maintain the privacy of sensitive information either their own or their customers data (Regulation (EU) 2016/679 [i.11]).

The Confidentially, Integrity and Availability (CIA) model is a guide for measures in information security. Information security is a key component within cybersecurity. Information security influences how information technology is used. Information technologies are already widely used in organizations and homes. This condition means that organizations and homes are subject to information security issues. Thus, it is necessary for such organizations and households to apply information security measures. These measures should protect valuable information, such as proprietary information of businesses and personal or financial information of individual users. Information security teams use the CIA triad to develop security measures. The CIA model shows the fundamental and mandatory goals that should be included in information security measures. The CIA model serves as a tool or guide for securing information systems and networks and related technological assets. This means the service or business provider has a responsibility with their actions and choices they undertake to protect data, information and assets also they need to be compliant with regulations and the law. This has become vitally important to a business or service provider wants to avoid being investigated and fined under GDPR if they fail to adequately take measures to protect data in their care. Cyber insurance is encouraging companies to become more compliant in order to secure lower premiums by implementing information and cybersecurity measures. User choice and responsibility - education and awareness/settings and permissions with applications and devices:

- Confidentiality - is the protection of information from unauthorized access. This is ensured by data or an information system is accessed by only an authorized person. User Id's and passwords, access control lists (ACL) and policy-based security are some of the methods through which confidentiality is achieved.

- Integrity - is the condition where information is kept accurate and consistent unless authorized changes are made. It is possible for information to change because of careless access and use, errors in the information system, or unauthorized access and use. This is ensured that it is edited by only authorized persons and remains in its original state when at rest. Data encryption and hashing algorithms are key processes in providing integrity. Also, version control may be used to prevent erroneous changes or accidental deletion by authorized users becoming a problem and backups or redundancies should be available to restore the affected data to its correct state. As well what often considered standard and basic security measures that can help maintain integrity are firewalls (control network access) and anti-malware/virus software.

- Availability - is the situation where information is available when and where it is rightly needed. The main concern in the CIA model is that the information should be available when authorized users need to access it. Availability is maintained when all components of the information system are working properly. This involves appropriate scheduling of hardware maintenance, software patching and/or upgrading and network optimization to ensure maximum availability for end-users. Also, providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur. Fast and adaptive disaster recovery is essential for the worst-case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan (DRP). Safeguards against data loss or interruptions in connections should include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as distributed denial-of-service (DDoS) attacks and network intrusions.

There are different Levels of Protection in cybersecurity they are presented below as a table and text description. While it focuses on the role of service providers and their responsibilities the awareness and their implementation of cybersecurity is relevant to end-user consumers as well. The content of Table 1 is ensembled thanks to the information derived from three sources [i.12], [i.13] and [i.14]. The table aims to provide an overview of the different levels of cybersecurity protection. Each level contains the elements of the one below it. They move from being passive, to being reactive and finally proactive in terms of cybersecurity. The cost of people and resources needed to implement each level increases in order for them to be implemented. For companies and individual end-users, not all aspects of these cybersecurity levels are valid to their requirements. There has to be a requirement for them to be implemented otherwise they can be an expanse of money and time that is wasted.

Table 1: Cybersecurity Implementation Levels

	Level 1 Initial	**Level 2 Advanced**	**Level 3 Self-Assessed**	**Level 4 Integrated**	**Level 5 Anticipate**
People	Minimal cyber awareness	Leadership aware of cyber threats - encourages training	Leadership promotes security awareness	End-users aware of cybersecurity issues	Awareness a business and community imperative
			A formal training program established	Education of cybersecurity is promoted by organisations	Culture supports continuous improvement of security skills, process and technology
	Minimal cyber info sharing	Informal info sharing/communication in the community	Formal info sharing/communication in the community	Analysis and sharing of collected info between different communities	Fully integrated info analysis to combine all physical and cyber info to create and share a near real-world picture of cyber events
			Defined roles to manage cybersecurity policy		
Process	Minimal cyber assessments and policy and procedure evaluations	Initial evaluation of policies and procedures	Routine audit programs but minimal verification	Verification of cyber plans and assessment to improvement	Continuous verification of plans through risked and quantitative tests
	Little inclusion of cyber into COOP	Aware of the need to integrate cybersecurity into COOP	Includes cyber in COOP	Integrate cyber in COOP and has an incident response and recovery plan	Continuous improvements of cyber in COOP and testing and verification of plans

	Level 1 Initial	Level 2 Advanced	Level 3 Self-Assessed	Level 4 Integrated	Level 5 Anticipate
Technology	Physical Security	Unidirectional Gateways	Zone Firewalls	SIEM software, device and service	Anomaly and Breach Detection
	Asset Inventory	DMZs	ICS Device Firewalls		
	Device Hardening	Firewalls and Anti-Malware	Application, device and network whitelisting	Automatic log and incident management	Threat Intelligence
	Patch Management	Access Control			

The cybersecurity implementation levels would be carried out mainly by the Service Provider within the User digital ecosystem to ensure their systems and data are protected from cyber-attack. For large service providers, they will be able to carry out many of these actions 'in-house' and working in partnership with select cloud network and cybersecurity providers to protect their systems and data. While smaller service providers, while they should be able to carry out basic cybersecurity process on their own, will pick and choose different cybersecurity packages which they can afford and/or meets their requirements from cloud network and cybersecurity providers.

Future Element - General Framework in Europe on Cybersecurity

The NIS (Network and Information Security) Directive, which requires some European companies to improve their ability to withstand cyber-attacks, has been adopted by the European Parliament in July 2016 and transposed by the Member States into their national laws before 9 May 2018. Member States have identified operators of essential services before 9 November 2018.

The NIS Directive [i.20] establishes common cybersecurity standards and strengthens cooperation between the countries of the Union and a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also, key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

The goal is to prevent cyber-attacks but also boost consumer confidence in the use of digital services.

4.2.2.2 Data protection

The methods for data protection are essential to providing the end-user with a secure and reliable service. The section of 'People' refers to the service provider employers and how they can inform the user about cyber threats. The section 'Process' is how Service Providers develop their cybersecurity strategy and its implementation. Also, how they certificate the different cybersecurity standards that include ISO/IEC 27001 [i.8] and ISO/IEC 27002 [i.9]. The NIST Cybersecurity Framework and ISO 15408 [i.10] also called "Common Criteria". Cybersecurity standards are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization. This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. The principal objective is to reduce the risks, including the prevention or mitigation of cyber-attacks. These published materials consist of collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies. The section 'Technology' are the tools that the service provider would need to implement to protect their systems and data from attack. Also, these tools ensure they are compliant with the implementation of cybersecurity standards. As well some of the elements of 'Technology' are relevant to the end-user device and network connections these include physical security, patch management (application/device updates), firewalls, anti-malware software and access control (usernames and passwords).

There is a need to achieve human-centric cybersecurity which means moving away from protecting devices and services from vulnerabilities towards designing cybersecurity around the behaviours and requirements of the end-user. These involve taking steps to improve user behaviour in cybersecurity through education, awareness and actions to active measures to ensure user take steps to improve their own cybersecurity on the devices, networks and services they use. As well as implementing secure by design or default as the standard method of incorporating cybersecurity to devices and services instead of adding cybersecurity on afterwards.

Data protection has become vital and will remain a cornerstone with a user-centric digital ecosystem. Data protection is about trust and confidence the end-user has in the companies and service provider they give their information to, in order to access chosen applications and services. ([i.17]) Companies now have an obligation to manage and protect data under the General Data Protection Regulation 2016/679 (GDPR) [i.11] and other related regulations including the NIS Directive [i.20] on cybersecurity and the upcoming European Union e-Privacy Regulation. GDPR supersedes the Data Protection Directive 95/46/EC [i.19] and it was adopted on 14 April 2016 and became enforceable beginning 25 May 2018.

GDPR enshrines into law for citizens their 'Data Subject Rights'. These include:

- Breach Notification - Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This mandatory action should 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, a mandatory statement of GDPR is that the controller should 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 his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure 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.

- Data Portability - GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine-readable format' and have the right to transmit that data to another controller.

- Privacy by Design (Data Protection by Design) - Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. This calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

4.2.2.3 Privacy

Privacy can be defined as freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one's personal data or information, as by a government, corporation, or an individual. Privacy in the context of online and connected services means the privacy and security level of personal data published via the Internet or held by a company. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences. Online privacy and anonymity are paramount to users, especially as e-commerce continues to gain traction. Privacy violations and threat risks are standard considerations for any website or online service under development. Privacy is linked to the confidentially of personal data between the user and the service provider. This is a different meaning of confidentially that is found within the CIA model which focuses on the service provider responsibility, though the methods to maintain confidentially are the same. Users know that in order to access a free service they are going to have to hand over some sort of personal information often they are willing to oblige as long as their data is not misused or sold on to a 3rd party. They expect confidentially to mean having another's trust or confidence when entrusted with secrets or private information.

Privacy means in the context of the user-centric digital ecosystem that end-user expect their personal data and information they hand-over to providers in exchange for a product or service that their information is stored safely, securely and will not be shared without their permission. This expectation is the goal of the GDPR [i.11] by clarifying the use of personal data and the need for companies to prove they are taking the necessary actions and steps to keep that data safe from attack or misuse.

In order to get further a proposal for a reinforced regulation in the field of electronic communications named e-Privacy is on the European agenda. Such directive will have to look at the need for special rules for the electronic communications sector including Over The Top Services (OTTS), the possible exemptions to consent for processing traffic and location data, and new solutions to cope with the cookie consent issue.

The survey described in ETSI TR 103 438 [i.1] reveals that 40 % never or rarely use a WiFi connexion for privacy and security reasons, and that is the main reason for not using WiFi.

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' , see also ETSI EG 203 602 [i.2].

This means in the context of designing a user-centric digital eco-system when it comes to privacy there is often a focus on optimizing the settings and permissions of an application or service. The part of the solution to the privacy paradox is privacy by design which is now part of the GDPR. Though it is called data protection by design. Data protection by design is ultimately an approach that ensures service providers consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle. As expressed by the GDPR, it requires the business to put in place appropriate technical and organizational measures designed to implement the data protection principles; and integrate safeguards into business processing so that they meet the GDPR's requirements and protect the individual rights. In essence, this means businesses have to integrate data protection into their processing activities and business practices.

4.2.3 Provider offers (PaaS)

Cloud Computing proposes a set of resources (e.g. devices, networks, storage, interfaces) shared and offered as services. These services are available at the users request and are billed depending on the rate of consumed and reserved resources. Reference is done to NIST to describe these services in 3 categories:

- **Infrastructure as a Service (IaaS):** consists of providing to user resources of processing, storage and networks as services. User may deploy and perform own applications regardless management of underlying infrastructure.
- **Platform as a Service (PaaS):** provides users (typically programmers) software platforms and development frameworks enabling automatic deployment of applications in Cloud.
- **Software as a Service (SaaS):** offers applications ready to use through web. SaaS applications are directly consumed by clients regardless of licences purchase, versions update and operating costs.

One of the promises of Cloud Computing is to offer "On-demand" services proposing a cost model aligned with users' consumption.

For that, Cloud proposes that data processing is sold "as a service".

The vision "X as a Service" should ideally permit composition of specific and personalized Cloud services, in a dynamic and agile manner depending on users' preferences and guaranteeing QoS.

In this context, it is important to be able to determine intrinsic properties of each Cloud provider in terms of elasticity, scalability, high availability and provisioning on demand.

Indeed, these properties translate the capabilities of a provider to correctly manage the services chosen by the user.

These management properties should also be exposed as services.

Elasticity: according to the definition from NIST, elasticity represents the capacity of a Cloud system to dynamically add or take off resources at the time of executing. The system reacts dynamically according to the real load.

The speed of elasticity system depends on two parameters:

- time required to take decision to add or take off a Virtual Machine (VM) or a Virtual application (Vapp).
- time needed to add or take off a VM or a Vapp.

Scalability: is the capacity of a Cloud system to maintain performance of application in case of increase or decrease of requests in the future.

High availability: means the resistance against systems a Cloud components failures (e.g. CPU, memory, VM, I/O, links, software).

It is mainly measured by uptime percentage.

On demand provisioning: as mentioned in NIST standard, Cloud providers should offer a lot of on-demand services.

They make available to consumers catalogs of standardized services and offers.

Provisioning automation depends on:

- management and monitoring technics of hypervisor;
- self-adaptation capacities of Cloud services and resources.

To manage service components three interfaces are necessary:

- **Usage interface** includes processing functions made by Cloud services and offered to consumers.
- **Control interface** contains mechanisms necessary to control service resources. It allows to reserve resources necessary for processing requests from user.
- **Management interface** contains mechanisms allowing self-management of Cloud service behaviour. This interface monitors the QoS offered by the service during consumption phase. It checks if this QoS is in accordance with QoS planned in the QoS contract.

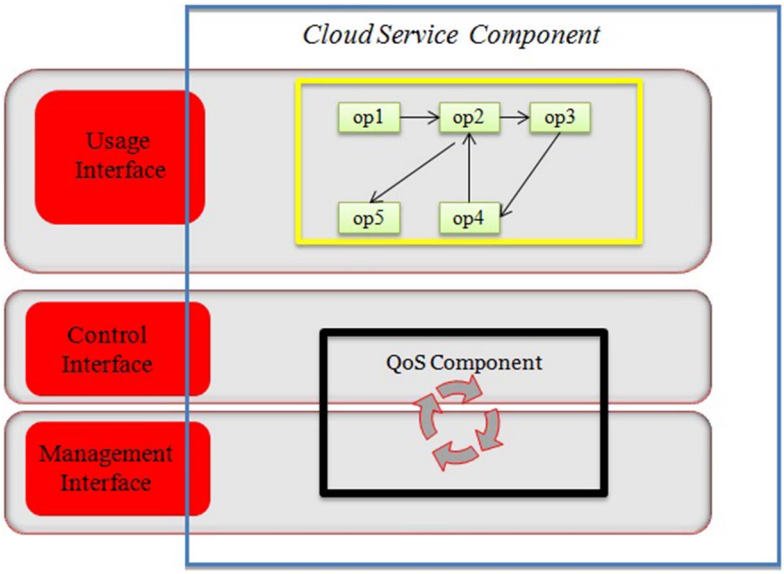

Figure 3: Service Cloud Service Component

The software design of services involves the software structure and the business service logic.

"as-a-Service" components should satisfy a set of requirements with a set of properties.

Properties are distinguished related to:

- The definition of the structure and the formal descriptions of service components, i.e. the nodes themselves.
- The definition or design of the service logic and functional architecture of service components, i.e. the interactions between service components.
- The management of the service components.

Properties related to service structure

- Cohesion: Service components should be consistent. The service logic offered should be relevant and recognized as a meaningful business service for potential customers. The service rendered by the component should find all its functionalities in a logical way internally. This feature is called: self-sufficiency, autonomy or even functional decoupling.

- Reuse: A service component should be reusable to build different services, in different compositions and different environments.

- Abstraction: Beyond service descriptions that should appear on service catalogs and SLAs, service components should abstract the internal service logic from outer service environments.

- Invariance: A service component should have an identical structure, that would not vary from a level to another in a hierarchy of service components. That means that the structure is invariant when scalability and elasticity are needed. This property is expressed in components construction, derived from the Fractal core principles.

- Statelessness: A service is stateless if it processes each received request as an independent transaction without any relationship with previous ones. A service component should then neither keep information regarding its state or its processing state nor handle information about previous requests. If it maintains its state for a long period, it will lose the "loose coupling" feature, its availability for other incoming requests and even its possibility to scale. Each component should handle data coming only from outside its area of responsibility i.e. from other service components so that its functional behaviour do not use data received from previous invocations. For that, it is needed to rely on transactions in unconnected mode that define well-specified formats of in-requests and out-responses. Here, the service component structure with its interfaces would help. It is also needed to delegate information handling and state management to external entities. This feature is crucial as it impacts the independency of a service component and thus the possibility to include it in compositions that need to be dynamic.

- Mutualisation: A service provider should offer the same service component instance as-a-Service to multiple users. In the present document, mutualisation means multi-tenancy. Service components should support multi-tenancy in order to be invoked by multiple users requiring the offered service either simultaneously or not. This reinforces the statelessness and the loose coupling features. Mutualization requirement calls for a need for loose bindings or connections between service components to have the capacity to provision multiple users and answer multiple service requests autonomously. Thus, mutualization will help realizing minimum functional coupling and loose coupling between functions.

Properties related to service interactions

- Loose Coupling: Service components should have no predefined sequence between them and should maintain relationship with minimized functional coupling.

- Invocation: A service component should be accessible and invoked based on service requirements in SLAs (invocation interface, function or service and QoS level). Three types of service contracts are distinguished: syntactical contract (service interface, function, service or process name, input/output parameters and structural constraints), semantic contract (informal description of the function or service with service use rules and constraints), and service-level contract with (defines the service commitments, i.e. QoS and SLA parameters like time to access, to process, to response, etc.).

- Composition: Multiple service components should be able to be chained as elementary entities (primitive or composite components) to create a service. They should be effective service composition participants, regardless of the size and complexity of the composition. This composition requirement feature is verified only if all of the features described are verified.

Properties related to service management

- Description: Service components should be describable based on meta-data in an independent manner from their implementation specificity. The formal description should have a logical and meaningful structure.

- Registration: Service components should be able to be registered in a Domain Registry. This registration can be made through a publication of its service offering, QoS level and state. It should also be able to discover its environment through service discovery.

- Exposition: This feature includes cohesion, description, registration and invocation. Exposition is providing the functional and non-functional description of service components as well as their inherent QoS level offered through catalogs on service portals to allow a third-party actor to select and/or build a service based on his profile and competences.

- Auto-management: Service components should be able to monitor and control their behaviours (non-functional aspects) using autonomic management approaches. Placing the monitoring of QoS very close around each service component and business logic helps to detect exactly the malfunctioning component.

- Ubiquity: Is the high equivalence between service components. Service components should be defined and described based on their core function and QoS level they offer (the values of QoS parameters). According to this definition, Service components may be grouped into communities of ubiquitous or identical service components where service components of a community provide the same service even if their business codes or algorithms are different, with the same QoS level. This feature goes with scalability issues, as the service provider may decide to scale the service by adding ubiquitous service components. It also enables higher service availability to find the requested service with the desired QoS level as this gathering in ubiquitous components community is an approach to set redundancy schemes.

These requirements apply to the software design of services on both, functional and non-functional aspects. Their generic nature allows a service architect to apply them on any service.

4.3 Service composition

As mentioned in clause 4.2 three interfaces are necessary to ensure autonomy and interworking of service components:

- **Usage interface** depending on data plane
- **Control interface** depending on control plane
- **Management interface** depending on management plane.

Service composition is based on the convergence of these three planes in order to ensure flexibility, dynamicity and adaptation. Service composition depends on the communication dimension of ACIFO model, defined in ETSI TR 103 604 [i.3].

5 Provider process for Smart Meter (functional model)

The digital eco-system for the provider process can be from a single primary provider to many end-users, as well including secondary providers who also serve as users themselves. The use case will focus on single household. And how they interact with services and software applications by using devices. The devices may be single use or multi-use. The digital eco-system is not confined to the geolocation of the home as many of services need access to external assets. Thus, whilst the eco-system may include smart home devices, home banking, entertainment, home shopping, the root of many of these services are outside the home.

The services can be solely in used in-house while others need access to resources outside the house. For example, smart metering 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. In theory they allow for better budgeting by allowing users to know accurately how much a household is spending on power or water. But a dedicated budgeting application needs to pull in data from households banking services and other financial services the user might use. Often this is from the outside the house and can also be used outside the house. The user(s) is (are) consumer(s) but may also be producer(s) (e.g. energy, applications, etc.) With the continuous exchange of data and always available networks the relationship between provider and user is no longer one way. It has become a two-way exchange of information. Within the User Centric General Framework, the actions and processes of the providers occur within the brackets in figure 4.

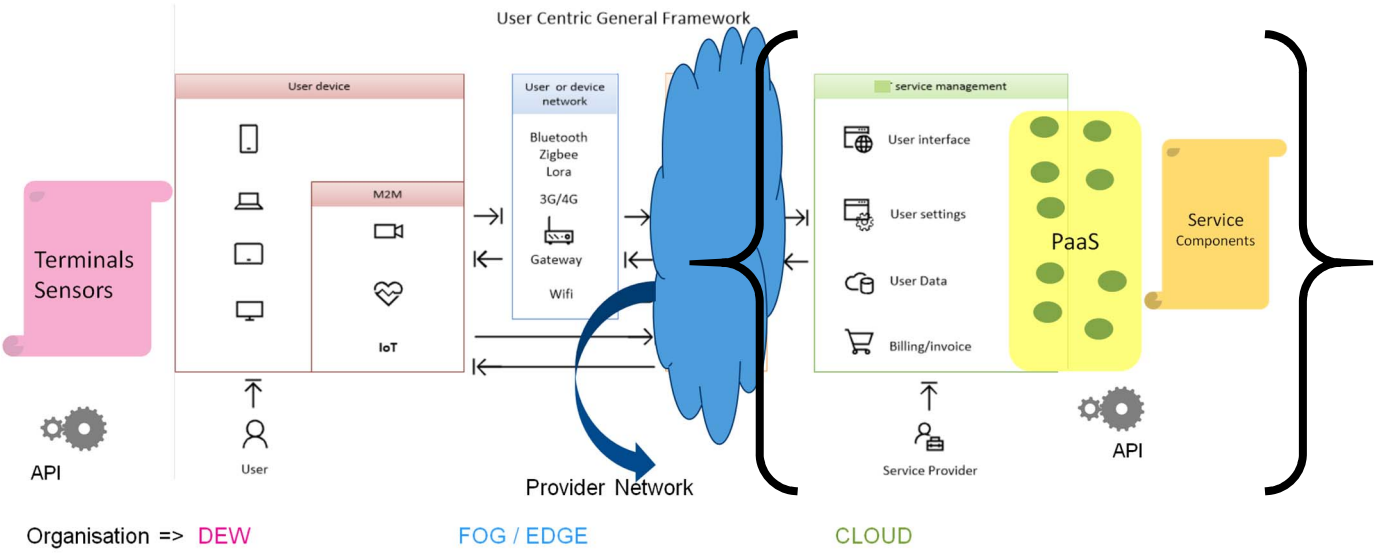

Figure 4: Generic model provider process

The provider process of smart meters is highlighted in figure 5. The primary provider is the utility company (gas, electricity and water) that serves the customer/end-user. They have a one-to-many relationships, but also between them and the customer as well as key secondary providers that include companies that support the functions of the smart meter within the digital eco-system. These include contractures providers, network providers and financial services, etc.

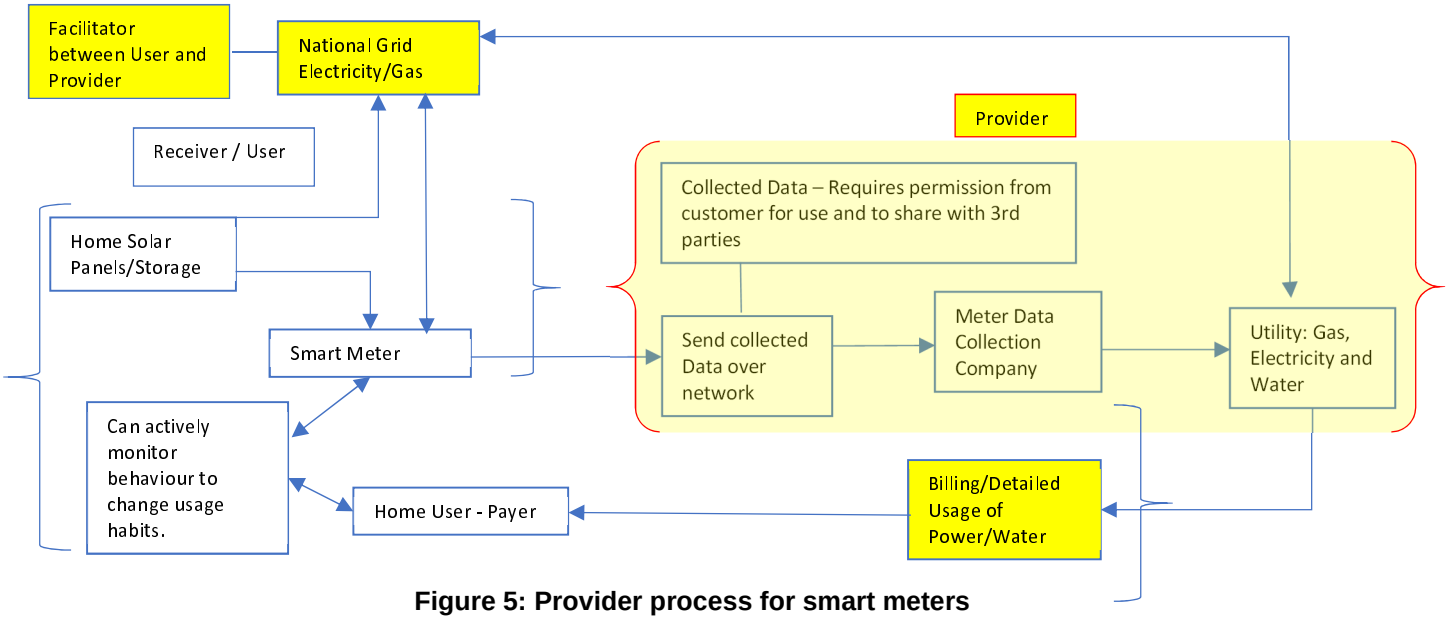

Figure 5: Provider process for smart meters

Types of Services for which providers should be responsible for:

- Energy/water usage. Billing: Involved are the Energy supplier(s), Water/Sewage suppliers and Metering companies that maintain and check that the meters are working correctly. Also, involved are the supply and support networks which are needed to for the billing process to work. The billing services require data to be collected. This requires permission from customer for use and to share with 3rd parties under the GDPR. Unless the user supplies metering, through readings themselves there is no direct interaction between the user and the service provider.

- Energy, use and production: The Energy supplier has a two-way relationship with Metering companies, they can part of the energy suppliers or be separate companies. They facilitate interaction between households and providers through data collection and analysis of users' consumption. Though the user should have control or knowledge of how their data is used by the provider.

- Security (of the home digital eco-system): The network provider and the device manufacture (secure-by-default) should be following the Standards and regulations set by Government bodies and NGOs. For example, ETSI TR 103 304 [i.5] and ETSI TR 103 309 [i.6]. The communication between the smart meter itself and the utility company is encrypted so it is highly unlikely an attacker will able to find out information from a user's habits. Also, all service providers should be following cybersecurity best practise to protect their user, employees, systems and data.

- Data protection and privacy: The companies that handle the metering, billing, data storage and transfer should follow data protection regulations of Directive on Security of Network and Information Systems and the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 [i.11]. The energy supplier should obtain permission/consent from the bill payer to use for a stated purpose.

- Special needs: Equipment and network providers should be following Standards such as ETSI EN 301 549 [i.7]. The interaction between the user and device in question depends on the type of impairments and the special needs of the user.

6 Profiles (Information Model)

6.1 User profile

To define the information necessary to provider operations in a generic and exploitable manner, the user profiles are required.

In provider Information model the user is represented by personal profile. Each user has at least one user profile. The user profile may change depending on time or environmental evolution. This profile should provide a relevant representation of the user, personal preferences and previous customizations and QoS needs. Two sets of information are distinguished: the information used to describe the user (e.g. name, age, etc.) and the information relative to personal preferences, including, when available, special needs to improve the accessibility of services. One remains valid under any circumstances while the second depends on the context (environmental and/or execution).

An identifier/password permits the provider to identify the user and to initiate the personal profile. A diary function might be implemented to help provider determine dynamically the proper preferences relative to each specific context. In user profile the links (pointer) to the existing customizations (personal environment, service customization, etc.) may also be found.

User profile could be composed of six following sub-profiles (figure 6):

- Personal information profile.
- Role profile.
- User resource profile.
- User agenda profile.
- Geo-spatial profile.
- Preferences profile.

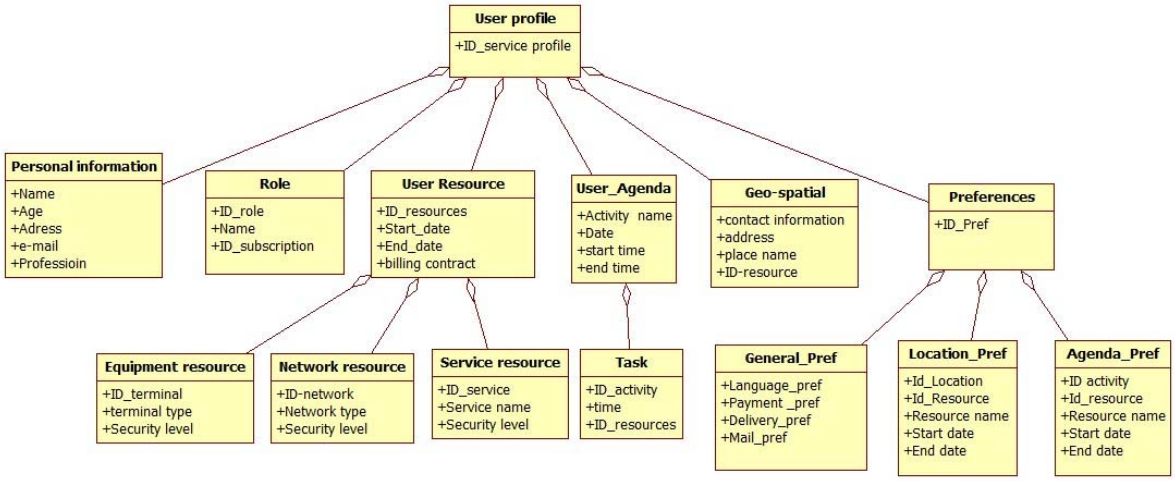

Figure 6: User profile

Personal information profile contains all the data directly linked to a user. This category includes some personal information: name, surname, profession, etc.

Role profile: this category 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, 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.

User resource profile represents all the resources authorized to the user regardless the location, role and agenda, special needs. This is implemented through a billing contract with a start date and end date of the contract. User resource profile should represent information about different types of resources: equipment, network, service. The level of security should be ensured for each resource type.

User agenda profile takes into consideration the user geo-spatial location by describing each activity according to the user agenda. Each activity is represented by a set of tasks linked with this task. For each task the user may select among a set of accessible resources that may be used when executing this task. As for the location profile the user may select among a set of accessible resources, the preferences linked to the agenda.

Geo-spatial profile represents information concerning locations, that is to say all the places where user is apt to be may be instantiated, e.g. at home and at the office. User may define a list of accessible resources depending on the place where the user is, by example the equipment (PC, mobile phones, PDA, etc.), the networks (WiFi, UMTS, Cable, etc.) and the service (sub-title language, browser) associated to a precise place. From this information the user may define the preferences: depending on the available resources at this place the user may choose the list of the subscribed networks, terminals and services.

Preferences profile identifies the user preferences in the NGN context in terms of terminals, networks and services according to the location (space), agenda (activities) and role (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 ambient surroundings of the user, with the aim of achieving personalization.

6.2 Resource profile

6.2.0 Introduction

To enable dynamic personalization of services according to user preferences and context information, resource profile provides facilities that are grouped under usage-oriented services as opposed to application-oriented services.

At the provider level resource profile plays the role of a middleware and provides an interconnection support and personalization facilities. It provides mechanisms to virtualize and to automate the access phase to relieve users of the service personalization tasks without any kind of human intervention.

The service personalization and the usage integration become possible only by developing an appropriately advanced profile management. These profiles are used by provider in order to provide necessary information to the integrated functions permitting establishment of the virtual organization and personalization of services. In order to have a dynamic usage-based access to services, an **active profile** is needed which dynamically maintains the information relative to each user and the context in which the user evolves. The active profile is dynamically updated when any of these three profiles changes. The provider uses this profile to interact with other users.

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

6.2.1 Equipment profile

The execution context describes the currently available resources of the equipment. It contains those hardware and software characteristics of the user equipment that are available. Equipment profile is composed of 4 sub-profiles able to describe all the needed information for the deployment of composed service that are connected and related to each other from different contexts (figure 7):

- general information.
- basic service.
- equipment service management.
- equipment service control.

General information contains all the attributes describing the equipment information (name, type, remote access, software, etc.).

Basic service contents ID service. The basic service is built from software services and hardware services information. For each service the offered QoS is associated.

Equipment service management defines the needed information for the equipment management during the user session.

Equipment service control defines all the information needed to equipment control for example:

- control policy.
- current QoS.
- threshold QoS.
- configuration.
- QoS status.

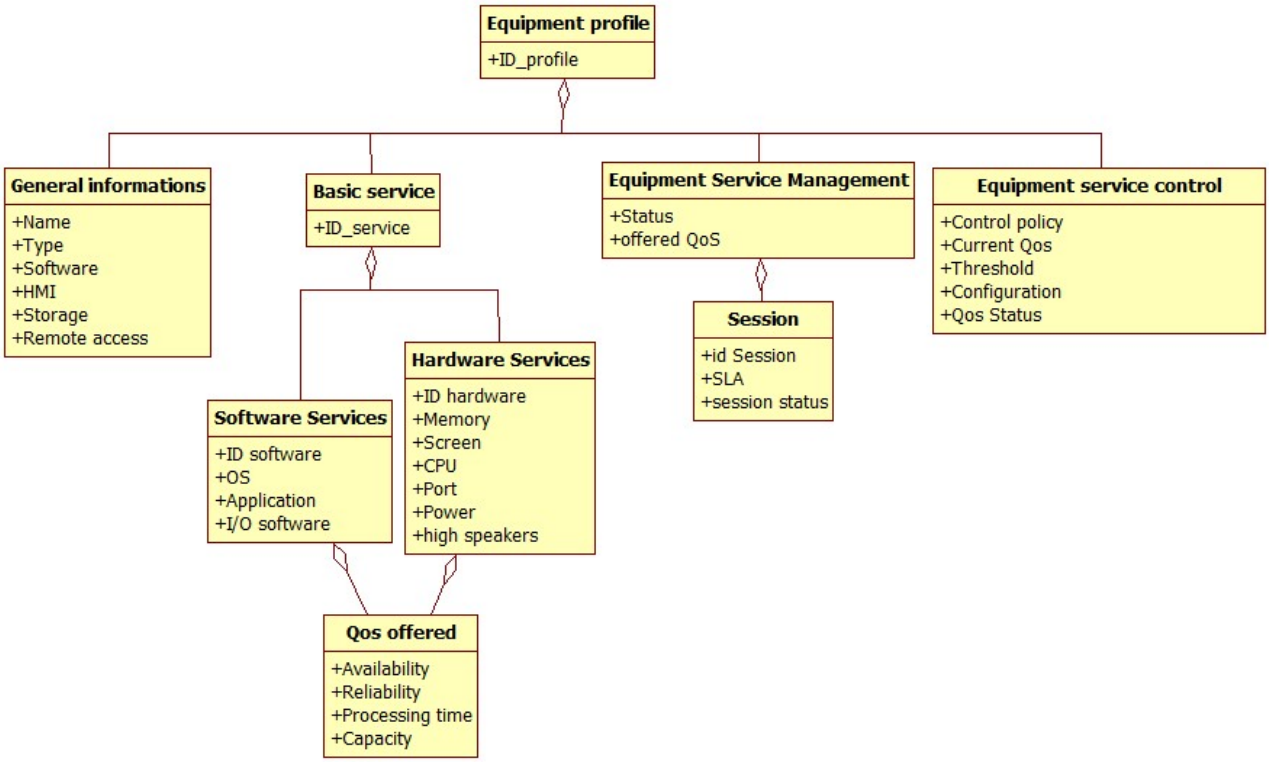

Figure 7: Equipment profile

Four QoS criteria Availability, Reliability, Processing time and Capacity should be used to represent offered QoS. Availability represents the accessibility rate of the service component. Integrity represents the capacity to run without alteration of information (for example: error rate). Processing time represents the time required for request processing (for example: response time). Capacity represents the maximum load the service component can handle (for example: processing capacity).

These criteria are associated with each function translating its behaviour at a given instant.

6.2.2 Network profile

Network profile is composed of 4 sub-profiles able to describe all the needed information for the deployment of composed service that are connected and related to each other from different contexts (figure 8):

- general information;
- basic service;
- equipment service management;
- equipment service control.

General information contains all the attributes describing the network information.

Basic service defines all the basic functionalities which compose a service. For each basic service one has to define the unique identifier, the name and the type. The basic service contains two descriptions: functional description and non-functional description (Offered QoS and Requested QoS).

Network service management defines the needed information for the network resources management during the user session.

Network service control defines all the information needed to network control. This control integrates the monitoring guaranteeing that the service composition should provide the predefined functionality and QoS.

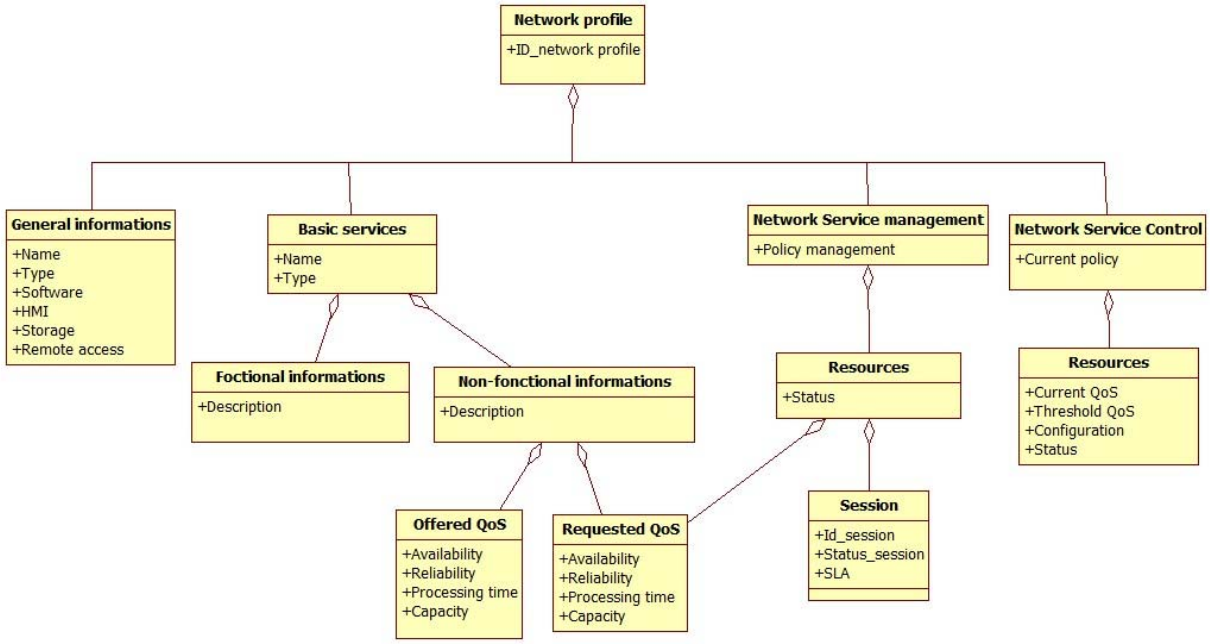

Figure 8: Network profile

The current QoS value is the value monitored during the service lifetime. The threshold value represents the limit the criterion should not exceed for the component to ensure the correct processing of requests.

SLA (Service Level Agreement) makes explicit on one hand the SLO user requirements and on the other hand the ensured provider offers including service and associated QoS.

6.2.3 Applicative service profile

The applicative service profile is a uniform information structure which contains both the description of service components (functional) and the knowledge of the service behaviour (non-functional aspect, QoS). It contains the different profiles to be sought during the different operational phases of a service component: provisioning and operation.

The definition of a service profile allows the quick creation of applications thanks to a composition of independent service components. These components provided by different providers may offer similar functionalities but with different QoS capabilities. This new generation of service is said autonomic because it is both autonomous and auto-manageable.

Applicative service profile is composed of 3 sub-profiles able to describe all the needed information for the deployment of composed service that are connected and related to each other from different contexts (figure 9):

- basic service.
- service management.
- service control.

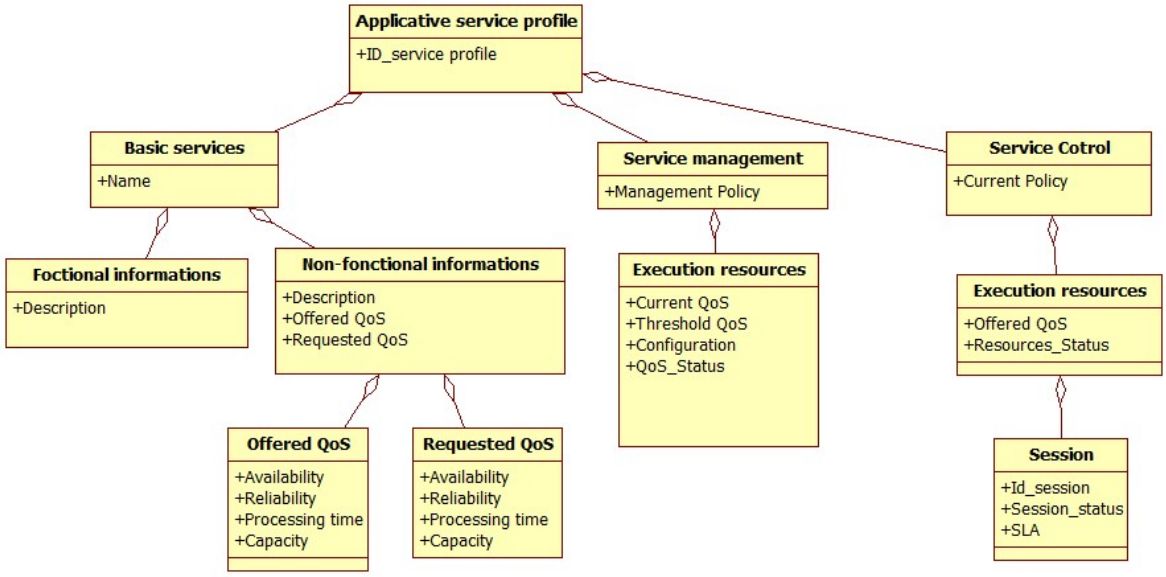

Figure 9: Applicative service profile

Basic service defines all the basic functionalities which compose a service. For each basic service are defined the ID, the name, the type, etc. The basic service is built from the functional and non-functional descriptions.

Functional description describes all the functionalities provided by this service (used audio-visual contents, protocols, ports).

Non-functional description describes the service QoS composed by an offered QoS and a requested QoS. The offered QoS represents the conception QoS and defines the maximal capacity that a service may offer in terms of availability, fiability, delay, capacity. The requested QoS represents the service requested QoS in order to be deployed in the user environment. It is the needed access network QoS, the terminal QoS for the service deployment. This information is necessary during terminal mobility (network roaming) and during user roaming (terminal change) when a user moves: change of the network service to which the terminal is attached, the network choice depends on the requested service QoS and the network preference indicated by the user at this place.

Service management defines the needed information for the service management during the deployment. The user global service compares the current QoS with the QoS values thresholds. If the result is positive this means that it fulfils the QoS contract and the QoS status becomes "IN-contract". If not, in case where the QoS agent detects a QoS degradation the QoS agent changes the QoS component and the QoS status becomes "OUT-contract".

Service management is composed of information linked to service component resources during the operation phase such as: the current resource QoS, the configuration and the QoS status may be:

- active: means that the service resources are in use.
- activable: means that the service component is potentially usable.
- available: means that the service component may be accessible.
- unavailable: means that the service component is temporally or finally unavailable.

The service component resources may represent the terminal or the access network.

Service control defines all the information needed to service control. It is composed of information linked to the resources reservation of the service components needed for the user request processing. Each component contains a waiting file which records the agreed requests of the different users. This represents a traceability of the number of service sessions attached to the same service. This permits to check if the resource has the required capacities to treat a new request from a new user, without violating the SLA request already accepted. To achieve that, the conception QoS is recorded and the number of sessions which share the resource, the SLA contract puts in place as well as the resource status in order to be able to update the condition of a resource which has been reserved or released.

6.3 Data protection

Data protection and safety is vital for company if they regularly process personal data [i.15]. If it is not already, data protection should be an integral part of their processes to ensure compliance with the GDPR [i.11].

Protecting data in transit: When using internet sites that require sensitive data to be entered (payment details/customer or personal information) checks are necessary to ensure the site is using secure connection, 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. Risk Assessments: The more sensitive the data, the more protection has to be implemented. Sensitive data should be closely guarded, whereas low-risk data can be afforded less protection. The major reason for such assessment is the cost benefit, as better data security equals greater expense. However, it is a good test to determine what data needs to be guarded more closely as this makes the whole data processing system more efficient.

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

a) Backups: Are a method of preventing data loss that can often occur either due to user error or technical malfunction. Backups should be regularly made and updated. Regular backups will impose an additional cost to service providers, but potential interruptions to their normal business operations will cost them more.

b) Encryption: High-risk data is the prime candidate for encryption every step on the way. This includes during acquisition (online cryptographic protocols), processing (full memory encryption) and subsequent storage (RSA or AES). Well-encrypted data is inherently safe; even in cases of a data breach, the data will be useless and irrecoverable to attackers, unless they obtained the keys that allow the data to be encrypted. For that reason, encryption is explicitly mentioned as a method of data protection in the GDPR. Which is why encryption should not be treated as a silver-bullet, as in order for it to be effective it has to be used alongside other methods of data protection.

c) Pseudonymisation: Is a method advocated in the GDPR that increases data security and privacy of the individuals. It works well with larger sets of data and consists of stripping identifying information from snippets of data. For example, service providers replace the names of persons with randomly generated strings. The identity of a person and data they supplied therefore should become impossible to link together.

d) Access Controls: Is a risk reduction method that works on the basis that the fewer people have access to the data, the lesser the risk of (inadvertent) data breach or loss. Service providers should ensure that they give access to sensitive data only to trustworthy employees who have a valid reason to access it. It is recommended they hold regular prior data handling education courses and refreshers, especially after hiring new employees. With their data protection officer, they should draft a clear and concise data protection policy outlining the methods, roles and responsibilities of each employee (or a group of employees).

Protecting data on mobile devices: The methods are similar to protecting data at rest. This means not installing unknown or untrusted 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 regular intervals.

Bring your own devices (BYOD): Companies should have policies and guidelines regarding their employees use of their own mobile devices when using them for official work and business. These include encrypt business data stored on personal devices with strong encryption. Full device encryption is best, but if that is not feasible, all business data should be stored in encrypted folders on the device. Routinely update hardware and apps to the latest versions to mitigate the risk of attackers exploiting a known vulnerability. Ensuring that devices are registered before they connect to the company network. This allows network administrators to detect unauthorized devices on the network. Authenticate devices using Secure Sockets Layer certificates before they are allowed to access network resources.

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. Destruction: Under the GDPR, they have the obligation to delete the data they do not need, and sensitive data warrants more comprehensive methods of destruction. Data destruction might not seem like a protection method at a first glance, but in fact it is. The data is being protected this way against unauthorized recovery and access.

7 Recommendations

7.1 End-to-end QoS

Move to a full "as the service" approach is a fundamental shift for providers in the way to create and deliver services. This is how users will be able to manage the complexity of a richer set of services without damage on quality and performance, and, in fine, the customer experience.

Virtualization promises to greatly improve service agility and scalability, that means make planning, configuration, and customization easier. It also accelerates the time to market for new services and applications, with capital and operational savings coming as an added benefit.

This means service providers can focus on the customer, making Quality of Service (QoS), Quality of Experience (QoE) and performance management top priority.

Providers can have a better user centricity approach, by allowing a bigger range of service options and a self-service and real time provisioning offer like bandwidth on demand.

When providers give QoS/QoE information to the customer, such information needs to be understood from a non-technical perspective.

Providers need to understand what drives overall customer perception of quality. Providers should well choose KPIs and the way to interpret them. For example, "Average" KPIs are meaningless.

To be sure that providers deliver a good service to customers, providers need to evaluate permanently the quality of the service according to the perception of the user, that means in an end to end perspective. **Entire chain determines the QoE. So providers should focus on how to intelligently combine KPIs.**

Providers should also use all the collected data about the quality of services in a way of continuous improvement, with some good engineering practices.

To have a look on the quality of experience, NPS (Net Promoter Score) and CES (Customer Effort Score) may be used.

7.2 Provider and digital Services

A micro-service architecture is recommended.

In a micro-service architecture, services should have different granularity and the protocols should be lightweight. A central micro-services property that appears in multiple definitions is that services should be independently deployable. The benefit of distributing different responsibilities of the system into different smaller services is that it enhances the cohesion and decreases the coupling. This makes it easier to change and add functions and qualities to the system at any time. It also allows the architecture of an individual service to emerge through continuous refactoring and hence reduces the need for a big up-front design and allows for releasing software early and continuously. Table 2 gives "as a service" features defined in clause 4.2.3.

Table 2: "As a service" features

Models / Features		as-a-Service
Structure	Cohesion	✓
	Reuse	✓
	Abstraction	✓
	Invariance	✓
	Statelessness	✓
	Mutualization	✓
Interactions	Loose coupling	✓
	Invocation	✓
	Composition	✓
Management	Description	✓
	Registration	✓
	Exposition	✓
	Auto-management	✓
	Ubiquity	✓

7.3 Provider and data

7.3.1 Knowledge base

Data are at the heart of the provider's strategy centered on the user. Data governance remains a fundamental issue for any company undergoing digital transformation. Data represent the Information System of company. The Information System is built of:

- Knowledge base, image of the digital eco-system (data bases, referential, catalogs, profiles, big data).
- A set of processes able to compute these data.

Speed and efficiency of decision making depends on the quality of the Information System and of predictive tools (machine learning, Artificial Intelligence, data analysis).

7.3.2 Security, Data protection and privacy

7.3.2.1 Security

The key areas where applying cybersecurity is critical in the user-centric digital eco-system include:

- User devices and User Networks.
- Machine to Machine communication (M2M).
- Service Provider Devices and Service Provider Networks.

The role of implementation by Service Providers is important and carried out by management using policies, guidelines, training and education to ensure end-users are protected by cybersecurity, and to encourage them to follow cybersecurity best practices.

oIn order t provide security services to end-users, key challenges include big data, IoT privacy and IoT Security. The UK NCSC and French ANSSI both provide guidelines as example of a model for applying best security practice within the environment of IoT and network connected systems. These include Technology which is Secure by Default and has the best security possible without the user even knowing it is there or having to turn it on. The elements which make up secure by default are: No default passwords; Keep software updated; Securely store credentials and security-sensitive data; Communicate securely; Minimize exposed attack surfaces; Ensure software integrity; Ensure that personal data is protected; Make systems resilient to outages; Monitor system telemetry data; Make it easy for consumers to delete personal data. These have to be implemented by device manufacturers and service providers.

7.3.2.2 Data protection

At the time of publication of the present document, companies should reason differently about the security of their IT, data and people. The most important thing is to detect threats as quickly as possible and secure what is essential, for example data and device assets. Most of the defence techniques are reserved for large companies that can afford them, and that does not change much across the different areas companies operate in. In the digital ecosystem, cybersecurity providers should offer a catalogue of services, adaptable to each case, pooling skills and defences at prices that meet the different expectations. This can only be through Security-as-a-Service (SECaaS). Formerly, security consisted of closing or severely limiting access to data, devices and applications. Currently, this is impossible for the modern businesses, hence they are transforming to adopt the same strategy according to current best practises. Firstly, because the infrastructure is virtualized and ends up in the cloud. Secondly, because the users are focused on mobility, and the companies haave their assets dispersed outside their own physical computing premises.

7.3.2.3 Privacy

List of good practices for Privacy by Design [i.16]:

- Businesses consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- Businesses make data protection an essential component of the core functionality of their processing systems and services.
- Businesses anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals.
- Businesses only process the personal data that they need for their purposes(s) and that they only use the data for those purposes.
- Businesses ensure that personal data is automatically protected in any IT system, service, product, and/or business practice so that individuals should not have to take any specific action to protect their privacy.
- Businesses provide the identity and contact information of those responsible for data protection both within their organization and to individuals.
- Businesses adopt a 'plain language' policy for any public documents so that individuals easily understand what they are doing with end-user personal data.
- Businesses provide individuals with tools, so they can determine how they are using their personal data, and whether their policies are being properly enforced.
- Businesses offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- Businesses only use data processors that provide sufficient guarantees of their technical and organizational measures for data protection by design.
- Businesses use other systems, services or products in our processing activities, they make sure that they only use those whose designers and manufacturers take data protection issues into account.
- Businesses use Privacy-Enhancing Technologies (PETs) to assist them in complying with their data protection by design obligations.

Annex A:
Additional Information for Security Recommendations

A.1 Acronyms and definitions for table of Cybersecurity Implementation levels

1) COOP - Continuity of Operations Plan: In the business world, a Continuity of Operations Plan AKA disaster planning or recovery plan. Businesses and agencies can create fault-tolerant systems and redundant storage so that sensitive data is maintained through an emergency. They can also invest in redundant hardware systems so that an office can still function if a local site is compromized. Other forms of COOP planning involve planning for individual business processes and applications to continue directly after a crisis. Planners can create systems for moving data and operations off-site. New data and document handling systems provide a lot of these features as a kind of insurance against emergencies.

2) DMZ - Demilitarized Zone: is primarily implemented to secure an internal network from interaction with and exploitation and access by external nodes and networks. DMZ can be a logical sub-network, or a physical network acting as a secure bridge between an internal and external network. A DMZ network has limited access to the internal network, and all of its communication is scanned on a firewall before being transferred internally. If an attacker intends to breach or attack an organization's network, a successful attempt will only result in the compromize of the DMZ network - not the core network behind it. DMZ is considered more secure, safer than a firewall, and can also work as a proxy server.

3) ICE- Interactive Connectivity Establishment (ICE) is a technique used in computer networking to find ways for two computers to talk to each other as directly as possible in peer-to-peer networking. This is most commonly used for interactive media such as Voice over Internet Protocol (VoIP), peer-to-peer communications, video, and instant messaging. In such applications, it is expected to avoid communicating through a central server (which would slow down communication, and be expensive), but direct communication between client applications on the Internet is very tricky due to network address translators (NATs), firewalls, and other network barriers.

4) SIEIM Software - Security Incident and Event Management: is implemented via software, systems, appliances, or some combination of these items. There are six main attributes of a SIEM system:

   a) Retention: Storing data for long periods so that decisions can be made off of more complete data sets.

   b) Dashboards: Used to analyse (and visualize) data in an attempt to recognize patterns or target activity or data that does not fit into a normal pattern.

   c) Correlation: Sorts data into packets that are meaningful, similar and share common traits. The goal is to turn data into useful information.

   d) Alerting: When data is gathered or identified that trigger certain responses - such as alerts or potential security problems - SIEM tools can activate certain protocols to alert users, like notifications sent to the dashboard, an automated email or text message.

   e) Data Aggregation: Data can be gathered from any number of sites once SIEM is introduced, including servers, networks, databases, software and email systems. The aggregator also serves as a consolidating resource before data is sent to be correlated or retained.

   f) Compliance: Protocols in a SIEM can be established that automatically collect data necessary for compliance with company, organizational or government policies.

5) Anomaly and Breach Detection - is mainly a data-mining process and is used to determine the types of anomalies occurring in a given data set and to determine details about their occurrences. It is applicable in domains such as fraud detection, intrusion detection, fault detection, system health monitoring and event detection systems in sensor networks. In the context of fraud and intrusion detection, the anomalies or interesting items are not necessarily the rare items but those unexpected bursts of activities.

6) Threat Intelligence - is the in-depth analysis of potential computer and network security threats to an organization. As with military intelligence, the goal is to get as much information as possible about threats so that a company can take proper action against them. The term implies anticipating and defending against attacks rather than just reacting with incident management techniques. Threat intelligence can examine threats facing one organization or it can cast an even wider net, involving the cooperation of other firms. As attacks become more sophisticated, professionals working to minimize threats should collaborate with each other.

The CIA model application to the User Centric General Framework ensures that a secure service is provided, and data is protected. The confidentiality methods of protecting information from unauthorized access of user IDs, passwords and access control lists would be used by the provider service management to ensure only the known authorized users can access user data and settings. Also, the User itself would have their own ID and password to access their accounts through the service provider. The integrity methods to ensure information is kept accurate and consistent unless authorized changes are made these would be implemented by the service provider on their hardware, software and networks. The availability methods would be implemented by the service provider to ensure their systems are kept up to date and in working order. They would aim to have a minimal amount of downtime, so end-users would not be overly affected. Often this means scheduled downtime is carried out either overnight or early in the morning.

A.2 Offers and regulation for Data Protection

Importantly, the Directive defines mandatory statements for the DPO:

- to be appointed on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices;
- to be provided with appropriate resources to carry out their tasks and maintain their expert knowledge;
- to report directly to the highest level of management;
- not to carry out any other tasks that could result in a conflict of interest;
- contact details to be provided to the relevant DPA.

The directive also indicates that the DPO:

- may be a staff member or an external service provider.

Annex B: Bibliography

- ETSI TS 103 426: "Publicly Available Specification (PAS); Smart Machine-to-Machine communications (SmartM2M) Home Gateway Initiative RD048-HG Requirements For HGI Open Platform 2.1".
- ETSI TR 184 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Types of numbers used in an NGN environment".
- ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

Annex C:
Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Associated Professor, Tatiana Aubonnet, CNAM

Other contributors:
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 Team Leader)

Emeritus Professor, Noemie Simoni, Telecom-Paritech

History

Document history		
V1.1.1	March 2019	Publication