ETSI TR 103 369 V1.1.1 (2016-07)

CYBER;
Design requirements ecosystem

Reference
DTR/CYBER-0011

Keywords
cyber security, secure by default

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

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

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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.

Executive summary

The present document provides a high level structured ecosystem of multiple "by-design" requirements that are related to security and may be applicable to communication and IT networks and attached devices. All such networks and devices whether for public or private infrastructure use, are commonly subject to eleven kinds of obligations - imposed by regulation, contract, exposure to liabilities, societal expectation, or business necessity. At a more granular level, there are even more than the eleven. Those engineering and operating the networks and devices are expected to instantiate the capabilities for these obligations "by design". The present document is not intended to provide design details. It simply enumerates the eleven obligations as a kind of ontology and identifies where there may be synergies or conflicts among the design requirements, and provides a bibliography of reference information.

Introduction

Communication and IT networks in their most elementary form, consist of some network attached device used to exchange or receive information from some arbitrary set of other attached devices that generally packaged as services provided to user customers. Whether for physical or virtual capability instantiations, some design processes occur that are governed by requirements that allow those capabilities to meet expectations.

There are innumerable engineering methods, technical standards, and law that guide and govern this activity. When all of this guidance and governance is distilled, there emerge a set of recurring common capabilities that embedded "by design." They are there for users or operators to make use of as a function of the conditions and context of the devices and services.

Indeed, the term "by design" itself has been used in recent years to describe specific capabilities - perhaps the most notable being "privacy by design". It is also common throughout the world for public networks and devices to institute lawful inception or retained data capabilities by design. The ever growing enormous complexity of devices, software, and networks has resulted in exponential increases in exploited vulnerabilities that in turn has necessitated cyber security by design. When the recursive process of identifying all of these "by design" is undertaken, it appears there are ten of them with various sub-variants that emerge. These are enumerated and described here together with noting the synergies or conflicts that may exist among some of them.

1 Scope

The present document provides a high level structured ecosystem of security design requirements that may be applicable to communication and IT networks and attached devices. It identifies where there may be synergies or conflicts among the design requirements, and provides a bibliography of reference information.

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] Directive of the European Parliament and of the Council concerning measures with a view to achieving for a high common level of security of network and information security systems across the Union, Brussels, 18 December 2015.

[i.2] CPNI: "Threat Intelligence: Collecting, Analysing, Evaluating," Center for the Protection of National Infrastructure.

NOTE: Available at https://www.cpni.gov.uk/Documents/Publications/2015/23-March-2015-MWR_Threat_Intelligence_whitepaper-2015.pdf.

[i.3] ETSI TR 103 305: "CYBER; Critical Security Controls for Effective Cyber Defence".

3 Definitions and abbreviations

3.1 Definitions

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

by design: instantiation of an explicit technical or operational capability in a device, network or service offering

3.2 Abbreviations

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

ICT Information and Communications Technology
IT Information Technology

4 A "by design" ecosystem

4.0 Description

It is common today for those focussing on various specialities to independently describe a development or societal need or regulatory mandate as a "design for" construct imposed on developers and operators of communication and IT infrastructures. This piecemeal approach, however, ultimately leads to the obvious questions: what exactly are all the various requirements, how are they manifested as network capabilities, and what are the synergies or conflicts among them. The result is a kind of competition among all the "by design" that should be harmonized in order to design and operate real world networks and associated equipment and services at reasonable cost. Cyber security is among these requirements, and threaded through most other "by design" attributes.

4.1 Availability

4.1.0 Availability generally

Perhaps the most basic of all "by design" requirements is that of availability. Users of all kinds that make use of a device, network or service expect it to be functioning and available to meet their desired needs. That desired level of availability is often effected through various diverse legal mechanisms such as combinations of service level agreements, implied warranties, or regulatory requirements.

4.1.1 Public services

Some network infrastructures and services are either owned by governmental bodies or designated as "public" or "universal" pursuant to national regulatory or treaty requirements. Such networks and services may also be regarded as essential or critical and include a wide array of financial system, public utility, or industrial control uses ([i.1] and [i.2]). As a result, they may by government contract or law be deployed or subsidized so as to meet "by design," various availability requirements that may include, for example, underserved or rural areas.

4.1.2 Specific resilience and survivability requirements

An additional subset of public or private networks and services may also be subject to specific resilience and survivability design requirements - especially during national or local emergencies. These kinds of requirements often require an array of device level designs (e.g. special aerospace or military grade components and testing), multiple redundant systems, backup, failure isolation capabilities, elimination of any single-point failure components for failsafe purposes. Such requirements may include access and prioritization for authenticated users identified in conjunction with emergency and public safety communication in clause 4.2.3.

4.1.3 Bandwidth non-discrimination

Certain infrastructures and services - particularly where anticompetitive or "bottleneck" concerns may exist or public resources such as rights-of-way or radio spectrum - may be designated as "common carrier" and subject to design and operational constraints such as controls on bandwidth management. So-called "network neutrality" requirements are a prominent contemporary example.

4.1.4 Outage reporting

Certain infrastructures and services may be subject to outage auditing and reporting requirements that require additional capabilities by design. These services typically include public networks and services, or private ones that are subject to additional contractual requirements concerning availability.

4.2 Emergency and public safety communication

4.2.0 Emergency and public safety communication generally

Emergency and public safety communication requirements typically enjoy the highest of "by design" priorities. These capabilities support an array of critical national police, fire protection, and emergency management needs at all levels from local to global.

4.2.1 Authority to many

During public or even individual emergencies, at local, national, or international levels, a highly important need exists to reach different arrays of individuals through any available electronic communications. Tsunami warning capabilities have become prominent several years ago as global disaster conditions unfolded. Such needs vary from that breadth of users to national and city levels, down to local roadways for a wide array of circumstances that may include an impending natural disaster, a major accident, or even an abducted child or a disoriented elderly person. The design requirements include diverse structured information formats, interworking, authentication, and delivery methods including effective human interface requirements.

4.2.2 One to authority

The inverse of the authority to many design requirement occurs when an individual much reach local emergency departments for medical, police, or fire purposes. The capabilities are known by their telephony short number designations - e.g. 112 or 911. Increasingly these requirements include authentication and geolocation design capabilities, as well as alternative telecommunication transport and applications, which include text, images, and even video.

4.2.3 Access/prioritization during emergency

During the declaration of a serious emergency - especially a national one - the telecommunication networks and designated public services are typically subject to limited access and prioritization of traffic to serve government authorities. Private organizations may also enforce such a condition within their private networks for similar purposes. Such requirements necessitate significant "by design" capabilities that include substantial authentication requirements and control of switches and routers.

4.2.4 Device discovery/disablement

Large scale theft of mobile devices has produced requirements instituted by both regulatory authorities and consumer demand for the ability to remotely discover those devices and disable them. Such requirements impose an array of special design and authentication requirements both within the supporting networks and the devices themselves.

4.3 Lawful interception

4.3.0 Lawful interception generally

Essentially every nation as well as many private network owners require the electronic communication network and services within their jurisdiction or under their control to provide available forensics upon lawful authority. For many designated networks and services, including those available to the public, the requirement to support the interception provisioning capabilities "by design" is a condition of licensing or required by law through regulation or contractual agreement. Lawful interception as described here consists of the real-time "handover" of network forensics described in a legal instrument - usually pursuant to technical specifications and divided into three subtypes described below. Acquisition can occur anywhere in the communications path - from the end user device to the transport paths to the centres supporting the services. To the extent the provider or vendor in an investigation is able to handover the information unencrypted or to provide the associated keys or otherwise decrypt the information, they are obligated to do so. The boundary between real-time lawful interception and retained data handovers described below can be blurred. The virtualization of these capabilities is also producing new design challenges to meet requirements.

4.3.1 Signalling

All electronic communication networks function through signalling capabilities that set up and facilitate the transfer of information content. Those capabilities themselves generate information forensics concerning users, timeframes, locations, and the nature of the services provided. It is referred to by various other names such as Intercept Related Information, call-data, or metadata. Extensive sets of global design standards exist for acquiring, structuring, and conveying this information to lawful authorities such as law enforcement, or for a private network, the owning organization's security administrators or investigators.

4.3.2 Metadata analysis

The subsequent analysis of signalling information can itself produce extensive further data, including visualizations, that enable analysts to understand the forensics acquired. This includes the patterns that enable further investigation and mitigation of terrorist or criminal activity.

4.3.3 Content

Lawful interception may also include the production of the actual content of the communications - usually through some means of duplication at an access point, and its correlation with the signalling information. If content is encrypted through actions by the service provider, most jurisdictions require handover of either the unencrypted content or the encryption keys.

4.4 Retained data

4.4.0 Retained data generally

All electronic communication and IT networks and services create by design, generally significant amounts of information that is retained in temporary caches, log files, or auditing and accounting systems. This information is retained for diverse operational, business, or legal compliance purposes.

4.4.1 Criminal investigative

Data is retained and accessed for criminal evidentiary and investigative purposes either through law instituted in different jurisdictions (often referred to as Data Retention), or through preservation orders of different kinds and durations.

4.4.2 Civil investigative/eDiscovery

Data is also retained and accessed for civil evidentiary and investigative purposes through law or judicial rules instituted in different jurisdictions (referred to as eDiscovery).

4.4.3 Compliance, contractual requirements and business auditing

Data is also retained and accessed to meet a broad array of compliance (especially in finance and banking sectors) or to meet contractual requirement, or business auditing especially when there is a dispute among the parties.

4.5 Identity management

4.5.0 Identify management generally

Identity management encompasses an array of capabilities by design that enable any object, including a human user, to manifest an identifier at varying levels of trust and uniqueness in the context of the use or operation of an electronic communications or IT device, network, or service.

4.5.1 Access identity

Identifiers associated with individuals, service accounts and network end user devices are widely used in conjunction with access to a network infrastructure or service. Their use is implemented by design.

4.5.2 Communicating or process party identity

Object identifiers are used by design as part of all electronic communications and IT services to transport information between two end points.

4.5.3 Communicating or process party blocking

Object identifiers are used by design to prevent communication or information transfer from occurring.

4.6 Cyber Security

4.6.0 Cyber security generally

Cyber "by design" generally encompasses two sets of capabilities - the instantiation of defensive measures and the ability to exchange structured cyber security threat information.

4.6.1 Defensive measures

Defensive measures include an array of generally adaptive controls that are designed to be part of every lifecycle phase of a device, network, or service from its inception to its removal from service (ETSI TR 103 305 [i.3]). These controls produce and leverage forensic information, and themselves apply to maintaining the integrity of that information. Defensive measures depend significantly on timely exchange of structured threat intelligence.

4.6.2 Structured threat information exchange

Structured threat information exchange includes the ability by design for a device, network or service to continuously acquire, provide, and utilize current threat intelligence relevant to its use.

4.7 Personally Identifiable Information protection (Privacy)

Most jurisdictions and organizations have combinations of regional directives, national law, and organization policy requirements relating to the protection of personally identifiable information. These requirements are usually maintained to support privacy norms, although in some jurisdictions, additional content control requirements may exist as part of their privacy regimes - as described in clause 4.8.3. These requirements are generally met through cybersecurity measures, but can also impede availability of forensics needed for many other compliance requirements.

4.8 Content control

4.8.0 Content control generally

The content of electronic communications or provided by IT systems is usually subject to an array of legal requirements that can necessitate "by design" features to implement those requirements.

4.8.1 Intellectual Property Rights

Essentially every nation has requirements that provide for the maintenance of intellectual property rights associated with almost electronic communication and IT devices and content. Some of these requirements also arise pursuant to international treaties to which they are a party. Implementation of these rights can invoke a broad array of "by design" capabilities. Implementing these capabilities requires an array of identity management, auditing, and filtering design capabilities.

4.8.2 Societal or organization norms

Every nation and most organizations maintain limits on content arising from societal or organization norms. These may range from harassment or predatory behaviour to speech or depictions that are highly offensive to most people or can cause substantial harm. Implementing these capabilities requires an array of identity management, auditing, and filtering design capabilities.

4.8.3 Privacy

Some regional and national conceptualizations of privacy and instantiations in law allow for individuals to control the available public information about themselves through, for example, altering search engine results. These provisions have given rise to privacy by design principles, but the implementations may impede access to forensics for many other requirements.

4.9 Operations control

4.9.0 Operations control generally

The operation of almost all information and IT devices are subject to design requirements that arise from sharing a common resource such as the radio spectrum or safety of operators and users.

4.9.1 Emissions controls

All electronic communications and IT devices either intentionally or unintentionally generate electromagnetic energy. In the case of radiocommunication, the devices use allocation bands of the radio spectrum for transporting the communication between or among terminals. Where radiocommunication is not involved, the devices and equipment assemblies produce some level of incidental electromagnetic radiation that should be limited by design to levels that are generally specified by industry or regulatory authorities.

Emission controls are implemented through a combination of operator licensing, signal monitoring and national type approval regulations that give rise to many "by design" requirements.

4.9.2 Equipment characteristics

In addition to electromagnetic emissions, the physical, electrical, and user interface characteristics of communication and IT systems are usually subject to a wide array of context dependent design requirements that facilitate emission controls, support for disabled persons, and the health and safety of end users.

4.10 Support for persons with disabilities

Many end users have disabilities that include vision, hearing, and physical impairments arising from an array of causes. In many national and local jurisdictions, including private organization environments, electronic communication and IT networks and services are required by design to provide the ability for these classes of users to have effective access and use. The requirements may apply to the entire end-to-end infrastructure.

4.11 Network Management

4.11.0 Network management generally

The operation of ICT networks usually requires "by design" various systems essential to the management of network traffic and devices comprising the network, as well as capabilities that allow for charging and billing that are essential to many business and organization accounting models. These systems are often layered or nested within each other.

4.11.1 Traffic management

The acceptance of network traffic from customers or management systems, and the routing of that traffic among endpoints are generally essential "by design" capabilities for all networks.

4.11.2 Device management

Networks consist of large numbers of switching, transmission and other devices or equipment that are generally managed "by design" to ensure their operational status.

4.11.3 Charging and Billing

Most public ICT networks, and many private ones, maintain back-office systems for accounting and billing purposes that rely on raw information provided at the traffic or device management levels. The capabilities cover areas such post-paid (secure delivery and storage); pre-paid (real time metering); utility metering; tolls, etc. These systems require access to meta-data; retained data, and are essential to detect and mitigate fraud.

5 Synergies and conflicts among design requirements

Any number of the "by design" requirements described in the above clause may be concurrently applicable in the engineering and operation of electronic communication and IT networks and services. In some cases, the requirements support each other - producing a certain synergy among them. In other cases, there are inherent tensions among the requirements. These requirements are assembled in two groups in figure 1, and as noted, there are often significant synergies and essentially no conflicts within Group 1, while Group 2 requirements can diminish Group 1 capabilities. A dependency also exits between the protection of Personally Identifiable Information and Cyber Security.

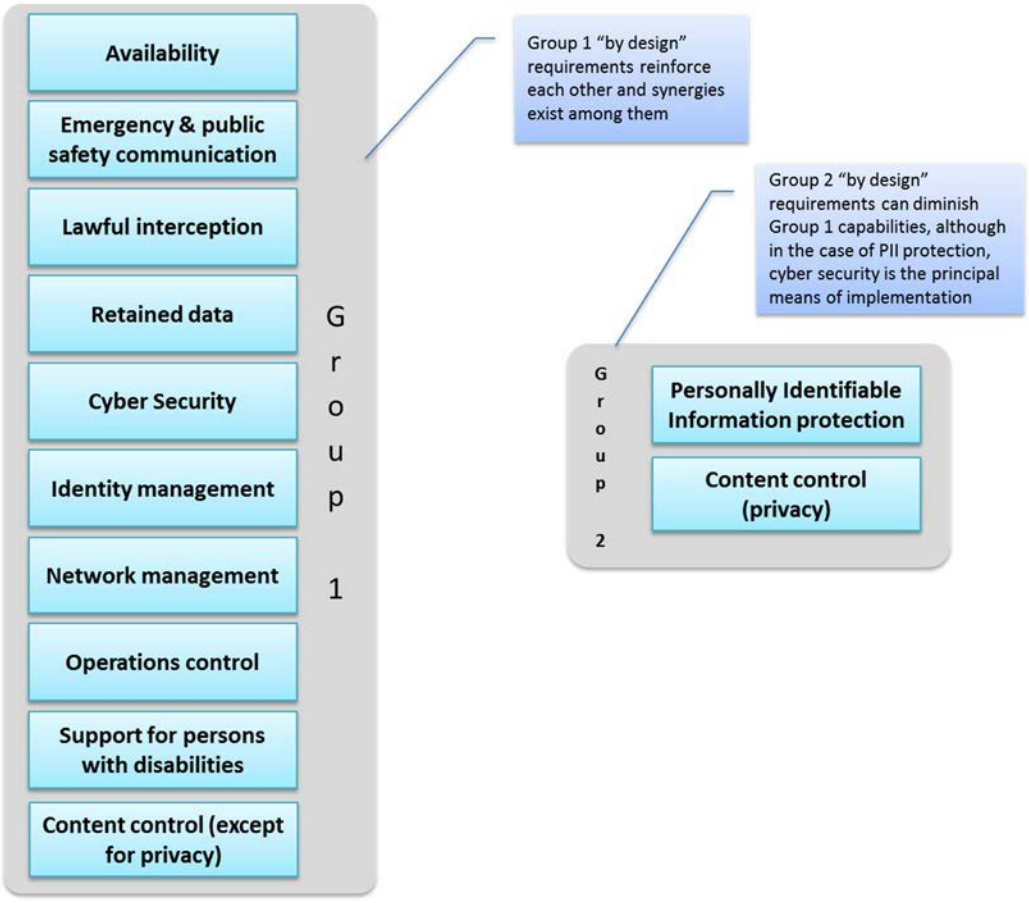

Figure 1: Enumeration and juxtaposition of "by design" requirements

History

Document history		
V1.1.1	July 2016	Publication