ETSI

Master Tech Standardization
with ETSI

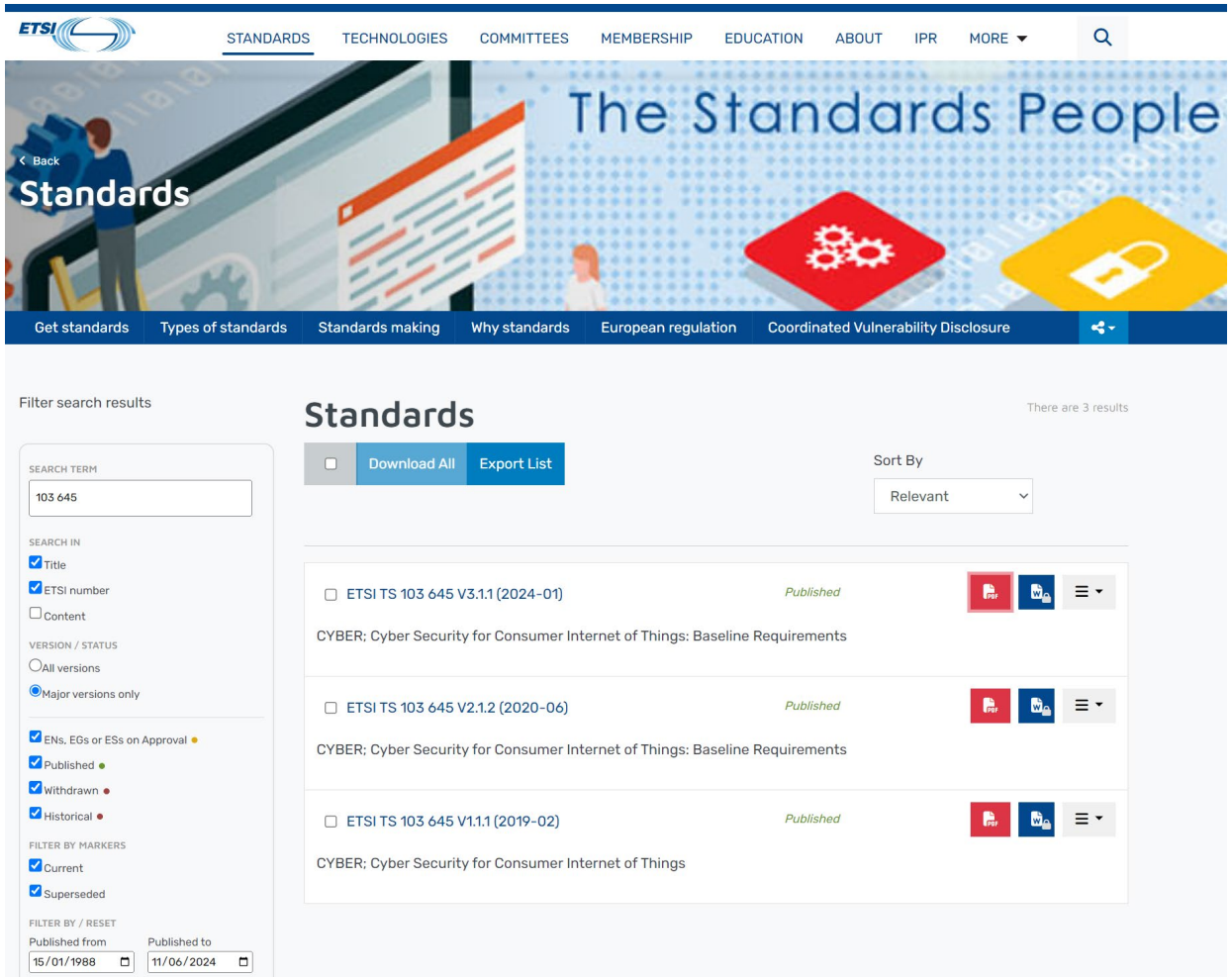
Module 5 – Let’s look at a standard

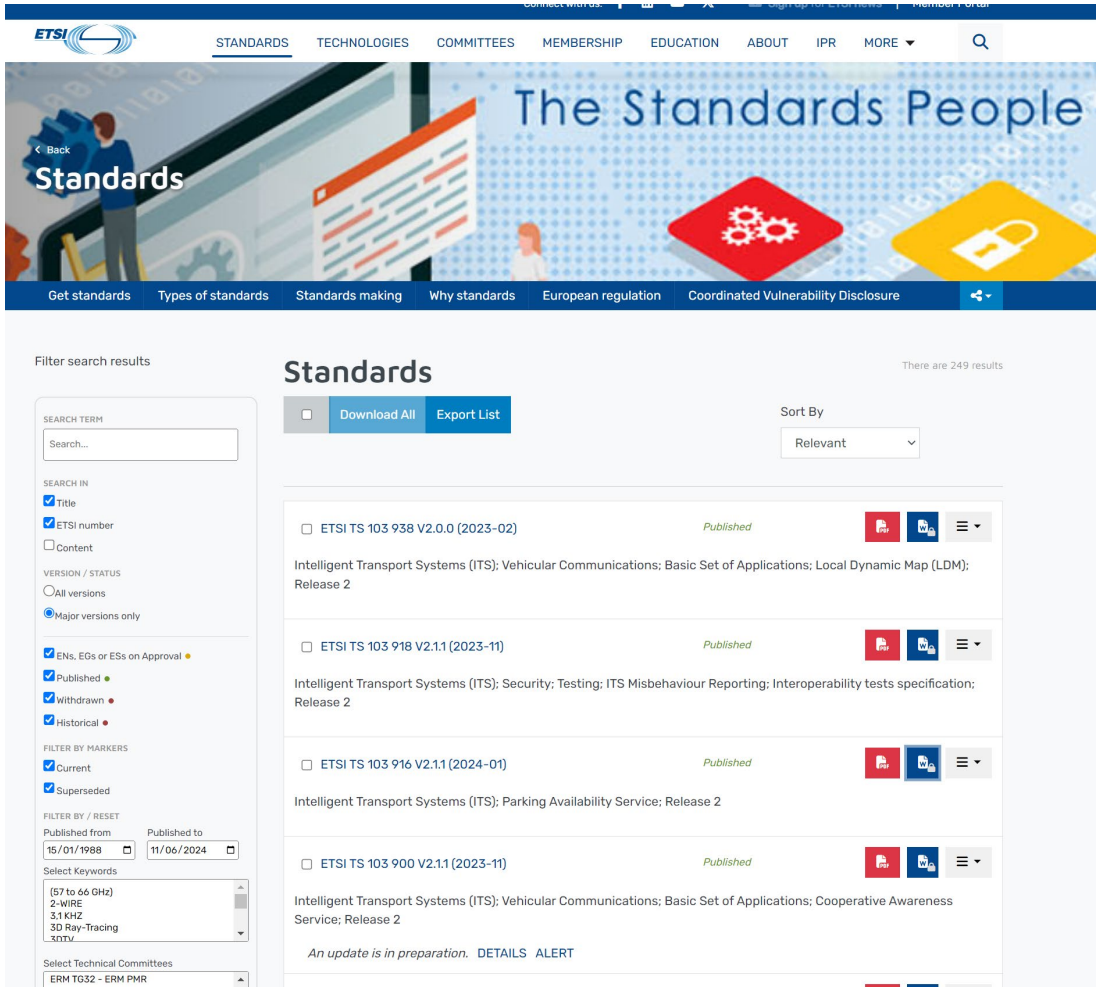
Section 5 – Real examples

- Let us take a look at 2 ETSI standards
- One for connected cars
- One for Cyber Security
- You can download them free of charge from the ETSI Website
- https://www.etsi.org/deliver/etsi_ts/103900_103999/103916/02.01.01_60/ts_103916v020101p.pdf
- https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/03.01.01_60/ts_103645v030101p.pdf

Search for standards on ETSI.ORG

Master Tech Standardization with ETSI





Connected car parking service

- The scope tells us what the Specification is all about

1 Scope

The present document specifies the facility layer service responsible for the generation of dynamic parking availability information in various transport environments (on street, off street, in parking facilities and park & ride stations). The dissemination is intended from a roadside or any other appropriate node, for example a central station.

- The references tell us what else to read
- And the long list of Abbreviations

AVP	Automated Valet Parking
AVPS	Automated Valet Parking System
BTP	Basic Transport Protocol
CCH	Control Channel
CDD	Common Data Dictionary
FCP	Functional Configuration Profile
FL-SDU	Facilities-Layer - Service Data Unit
IF-App	Interface of the Facility to Application
IF-OFa	Interface of the Facility to Other Facilities
IF-Mng	Interface of the Facility to the Management plan
IF-N&T	Interface of the Facility to the Network & Transport layers
IF-Sec	Interface of the Facility to the Security protocol
ITS	Intelligent Transport Systems
ITS-S	ITS Station
MAC	Medium Access Control
MAPEM	MAP (topology) Extended Message
MCI	MCO Control Information
MCO	Multi-Channel Operation
MIB	Management Information Base

2.1 Normative 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.

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

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 necessary for the application of the present document.

[0] ETSI TS 102 894-2: "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary; Release 2".

[0] ETSI TS 103 141: "Intelligent Transport Systems (ITS); Facilities layer function; Multi-Channel Operation (MCO) for Cooperative ITS (C-ITS); Release 2".

[0] ETSI TS 103 836-5-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol; Release 2".

[0] ETSI TS 103 836-4-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality; Release 2".

[0] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".

[0] Recommendation ITU-T X.691/ISO/IEC 8825-2 (1997-12): "Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)".

[0] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2".

[0] ETSI TS 103 836-6-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols; Release 2".

Informative information

- Some sections provide background material
- This is useful for understanding the more detailed normative sections

4.1 Background

Mobility services are users' value-added services which support the mobility of users in their various mobility activities contexts. These services are necessary to maintain the user' mobility system operational (e.g. its vehicle), to facilitate the transition between various transport modalities, and to support the transition of the user toward other users' offered services which are of interest to them (Point Of Interest (POI)).

Point Of Interest are multiple and are related to the user activity and its present needs.

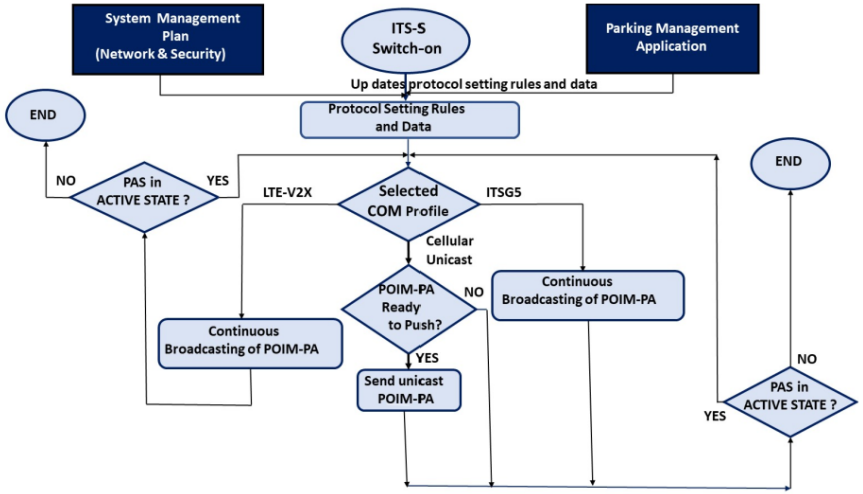
Parking places are often associated to these various points of interest as users need to park their vehicles when accessing a new service facility (e.g. hotel, restaurant, public transport station, rest area, energy supply station, etc.).

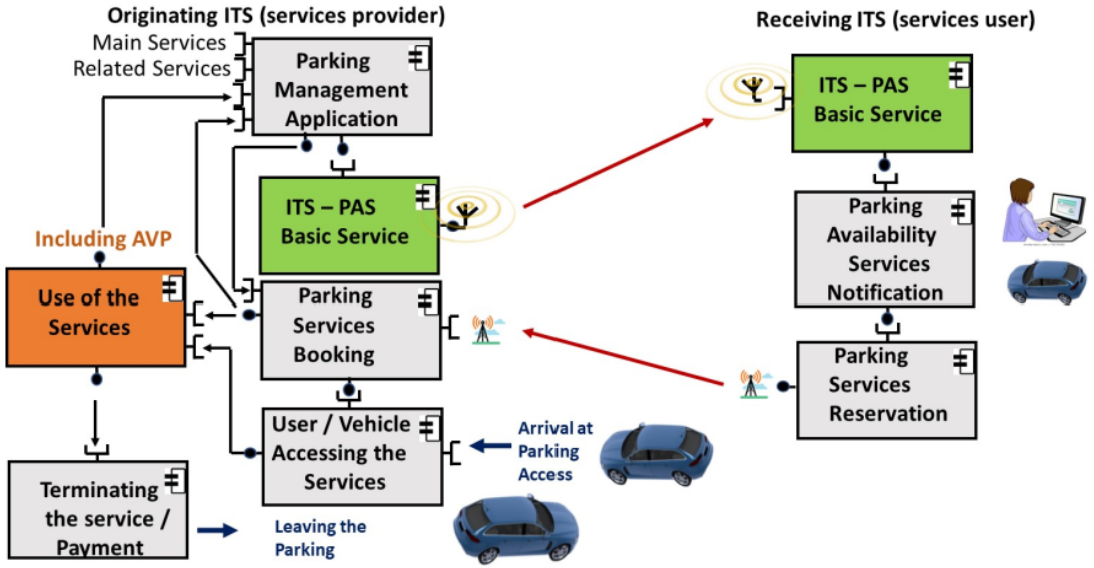
In a parking area, it is possible to access other services which can be supplied by specific related POIs. For example:

- A Valet Parking (human or automated) which may take in charge the vehicle to park it or take care of it for requested other services (e.g. energy loading, washing, tyres pressure gauging and refiling, goods transfer, etc.).
- An Energy supply station (petrol/gas, hydrogen, electric, etc.) which can be at the level of the parking place or at the level of parking space (e.g. electrical supply (connected or inductive)) ETSI TS 101 556-1 [i.0] and ETSI TS 101 556-3 [i.0].
- A vehicle tyres pressure gauge and filing system, see ETSI TS 101 556-2 [i.0], enabling to control vehicles tyres pressure and adjust their pressures when necessary.
- A vehicle washing system.
- Vehicle security system (e.g. for trucks and their payload).
- Mobility Services which are required for Park & Rides.
- Etc.

Diagrams

- Diagrams can vary from high level overviews of the system to detailed flow charts
- They are normally informative
- Specifications are corrected over time but change control (track changes) on diagrams is harder than text





Tables

- Tables are often used to describe parameters passed over interfaces
- They also indicate if parameters are mandatory/conditional/optional
- Normally normative – look at the words “shall” and specific requirements “Maximum Latency Time”

Table 5: PCI from PAS to GeoNetworking/BTP at the originating ITS-S

Category	Data	Data requirement	Mandatory/Conditional/Optional
Data passed from the PAS to GeoNetworking/BTP	BTP type	BTP header type B ETSI TS 103 836-5-1 [0], clause 7.2.2	Conditional. The data shall be passed if the value is not provided by the ITS-S configuration, e.g. defined in a Management Information Base (MIB) or if the value is different from the default value as set in the MIB.
	Destination port	As specified in ETSI TS 103 836-5-1 [0]	Conditional. The data shall be passed if the value is not provided by the ITS-S configuration, e.g. defined in a Management Information Base (MIB) or if the value is different from the default value as set in the MIB.
	Destination port info	As specified in ETSI TS 103 836-5-1 [0]	Conditional. The data shall be passed if the value is not provided by the ITS-S configuration, e.g. defined in a Management Information Base (MIB) or if the value is different from the default value as set in the MIB.
	GN Packet transport type	GeoNetworking SHB	Conditional. The data shall be passed if the value is

Table 3: Maximum E2E latency time requirements relatively to selected communication mode

Communication Mode	Transmission Triggering Conditions	Reception	Max E2E Maximum latency time	Comments
Continuous broadcast	Service provider application	All users present in the wireless ad-hoc local area network covered area	1 to 10 seconds according to information dynamic evolutions and network load	False positive and false negative are related to the selected time-period of broadcasting
Pushed unicast	Push unicast is triggered by the service provider when this one considers that the addressed user needs to receive updated parking availability information	The addressed user receives an unsolicited parking availability information which can be repeated according to parking load evolution	During peak hours, the maximum latency time between repeated unicast messages needs to be adjusted between 1 to 10 seconds	The latency time can be measured by comparing the message reception time value to the time stamp value provided in the POIM-PA
NOTE: During peak hours, it is then recommended to select the maximum time-period of 1 second excepted if the used channel is saturated.				

Text

- In the majority of specifications requirements are written in text
- Again, the magic words are used
- “shall” a requirement you must comply with
- “can” an optional requirement

6.6.2 Interface to MCO_FAC

If the ITS-S supports MCO, the PAS shall exchange information with the MOC_FAC via the interface IF.MCO specified in ETSI TS 103 141 [0] which is a facility layer function accessible via IF.OFa interface (see Figure 6). This interface can be used to configure the default MCO settings for generated POIM-PAs and can also be used to configure the MCO parameters on a per message basis.

If the ITS-S supports MCO, the PAS shall provide the POIM-PA embedded in a Facility-Layer Service Data Unit (FL-SDU) together with protocol control information (PCI) to the MCO_FAC. In addition, it can also provide MCO Control Information (MCI) following ETSI TS 103 141 [0] to configure the MCO parameters of the POIM-PA being provided. At the receiving ITS-S, the MCO_FAC shall pass the received POIM-PA to the PAS.

The data set that is passed between the PAS and the MCO_FAC for the originating and receiving ITS-S is specified in Table 4.

7.5.2 GeneralParkingPlace container

The general parking place container contains the following information:

- The geographical position of the parking place (mandatory).
- The name of the parking place (mandatory).
- The opening periods (optional).
- The address of the parking place (optional).
- The phone number of the parking place (optional).
- The WEB Site link of the parking place (optional).

For more details see the clause A.3.

Annexes

- Used for additional information
- May be informative or normative
- Here it points to machine readable versions of the standard
- ASN.1 is a bit like code for protocols

A.3 POIM-PA ASN.1 module

This clause provides the normative ASN.1 modules (see Recommendation ITU-T X.691/ISO/IEC 8825-2 [0]) containing the syntactical specification of the *ParkingAvailabilityBlock*, its containers, data frames, and data elements defined in the present document. This module, together with modules specified in clause A.2 provides the POIM-PA specification.

The semantical specification of the *ParkingAvailabilityBlock* components, its containers, the data frames, and the data elements are contained in the same module, in the form of ASN.1 comments. For readability, the same semantical specification is presented in a different format in annex B.

The POIM-ParkingAvailability module is identified by the Object Identifier {itu-t (0) identified-organization (4) etsi (0) itsDomain (5) wg1 (1) poi(103916) parkingAvailability(1) major-version-1 (1) minor-version-1 (1)}. The module can be downloaded as a file as indicated in Table A.0. The associated SHA-256 cryptographic hash digest of the referenced file offers a mean to verify the integrity of that file.

Table A.0: POIM ParkingAvailability ASN.1 module information

Module Name	POIM-PDU-Descriptions
OID	{itu-t (0) identified-organization (4) etsi (0) itsDomain (5) wg1 (1) poi (103916) parkingAvailability (1) major-version-1 (1) minor-version-1 (1)}
Link	https://forge.etsi.org/rep/ITS/asn1/pa_ts103916/-/raw/v2.1.1/POIM-ParkingAvailability.asn
SHA-256 hash	dd05938e201c7f10a3aaf2021f4983e5d481e0401d413b62203a253db97e6966

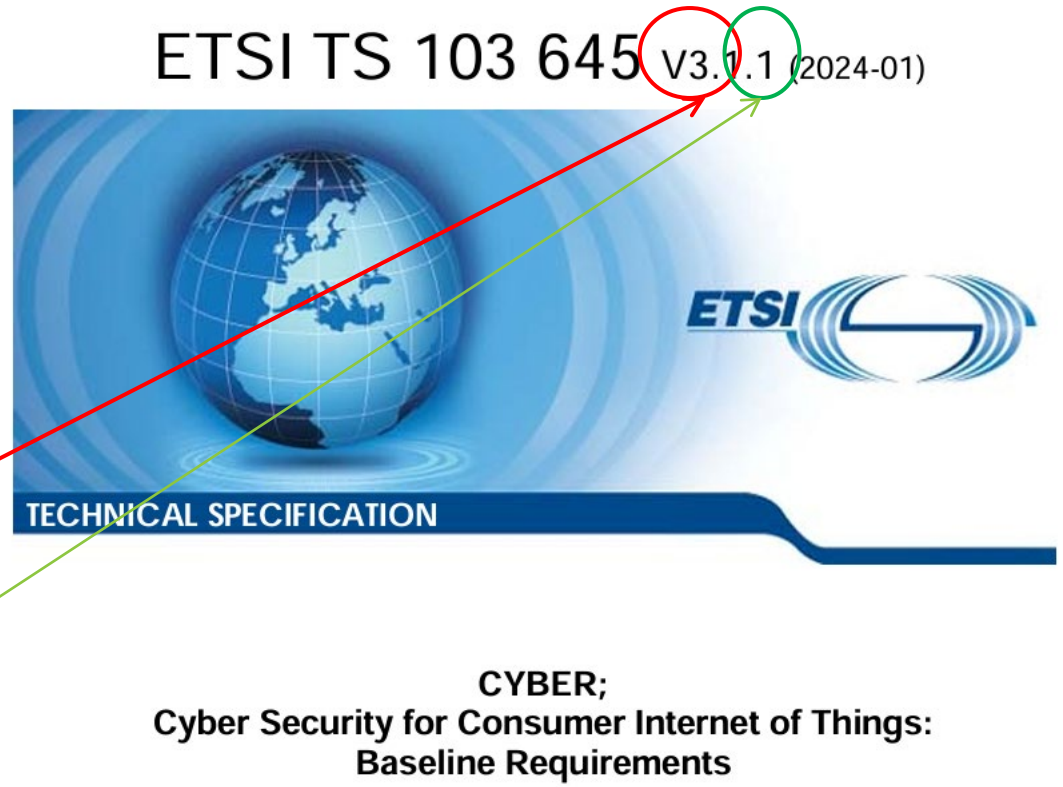
ETSI Forge - https://forge.etsi.org/

- ETSI Forge is a platform where users of ETSI standards can download software produced collaboratively by ETSI delegates
- It is home to machine readable versions of a specification
- ASN.1 – the protocols that run over interface
- OpenAPI – APIs to connect to services
- Open source code
- YAML - a data serialisation language

```
/**
 * This DE indicates the type of a reservation of a parking space/area.
 *
 * The value shall be set to:
 * - `0` to indicate that it is reserved to disabled persons,
 * - `1` to indicate that it is reserved to pregnant women,
 * - `2` to indicate that it is reserved to women,
 * - `3` to indicate that it is reserved to parents with small children,
 * - `4` to indicate that it is reserved for loading and unloading of goods,
 * - `5` to indicate that it is reserved for manual charging of electric vehicles,
 * - `6` to indicate that it is reserved for automated charging of electric vehicles,
 * - `7` to indicate that it is reserved for vehicles carrying out refrigerated transport
 * - `8` to indicate that it is reserved for VIPs,
 * - `9` to indicate that it is reserved for pre-booked reservations only,
 * - `10` to indicate that it is not reserved and can still be reserved,
 * - `11` to indicate that it cannot be reserved,
 * - `12` to indicate that it reserved for drop-off and pick-up of vehicles for automated
 * - `13` to indicate that it is reserved for vehicles with a permit,
 * - 14-31  - reserved for future usage.
 *
*/
ParkingReservationType ::= INTEGER {
   disabled(0),
   pregnant(1),
   womenOnly(2),
   parentAndChild(3),
   loadAndOffloadGoods(4),
   manualElectricVehicleCharging (5),
   automatedElectricVehicleCharging (6),
   refriferatedTransport(7),
   vip(8),
   preBooking (9),
   freeToBeReserved (10),
   reservationNotPossible (11),
   automatedValetparking (12),
   permit (13)
}(0..31)
```

Version handling

- Specifications change over time
- A complex system of version numbers ensures you can get the latest version
- Or an earlier version for reference
- Functions are added in major releases
- Corrections in minor releases



Informative references

- A valuable source of information when starting to work in a new area
- Many have hyperlinks to speed up the discovery process

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 103 305-3: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 3: Internet of Things Sector".

[i.2] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.3] NIST Special Publication 800-63B: "Digital Identity Guidelines - Authentication and Lifecycle Management".

[i.4] ISO/IEC 29147: "Information technology - Security techniques - Vulnerability Disclosure".

[i.5] OASIS: "CSAF Common Vulnerability Reporting Framework (CVRF)".

[i.6] ETSI TR 103 331: "Cyber Security (CYBER); Structured threat information sharing".

[i.7] 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).

[i.8] ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", November 2017, ISBN: 978-92-9204-236-3, doi: 10.2824/03228.

[i.9] UK Department for Digital, Culture, Media and Sport: "Secure by Design: Improving the cyber security of consumer Internet of Things Report", March 2018.

[i.10] IoT Security Foundation: "IoT Security Assurance Framework", Release 3.0November 2021.

[i.11] GSMA: "GSMA IoT Security Guidelines and Assessment".

[i.12] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.13] Commission Notice 2016/C 272/01: "The "Blue Guide" on the implementation of EU products rules 2016" (Text with EEA relevance).

[i.14] Copper Horse: "Mapping Security & Privacy in the Internet of Things".

[i.15] ENISA: "Baseline Security Recommendations for IoT - Interactive Tool".

[i.16] IoT Security Foundation: "Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies".

[i.17] F-Secure: "IoT threats: Explosion of 'smart' devices filling up homes leads to increasing risks".

[i.18] W3C®: "Web of Things at W3C".

[i.19] ETSI TS 103 701: "CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

[i.20] DIN SPEC 27072: "Information Technology - IoT capable devices - Minimum requirements for Information security".

[i.21] GSMA™: "Coordinated Vulnerability Disclosure (CVD) Programme".

[i.22] IoT Security Foundation: "Vulnerability Disclosure - Best Practice Guidelines".

[i.23] OWASP Internet of Things (IoT) Top 10 2018.

[i.24] IEEE 802.15.4-2015™/Cor 1-2018: "IEEE Standard for Low-Rate Wireless Networks, Corrigendum 1".

[i.25] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[i.26] GSMA: "SGP.22 Technical Specification v2.2.1".

[i.27] ISO/IEC 27005:2022: "Information technology - Security techniques - Information security risk management".

[i.28] Microsoft® Corporation: "The STRIDE Threat Model".

[i.29] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.30] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.31] ETSI TR 103 621: " Guide to Cyber Security for Consumer Internet of Things".

[i.32] FIRST: "Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure".

[i.33] ISO/IEC TR 5895: "Cybersecurity - Multi-party coordinated vulnerability disclosure and handling".

[i.34] ISO/IEC 16500-6:1999: "Information technology Generic digital audio-visual systems".

Testing and certification

- Standards often have test specifications that help ensure compliance
- ETSI does not perform certification testing
- Specialist test organisations will help with both testing and certification
- ETSI provides support on the application of testing and validation techniques in standards-making

4 Implementation of the standard

The implementation of provisions in the present document is informed by risk assessment and threat modelling (such as ISO/IEC 27005 [i.27] and STRIDE Threat Model [i.28]) and data protection and privacy impact assessments; that are performed by the device manufacturer and/or other relevant entities and are out of scope of the present document. For certain use cases and following risk assessment, it can be appropriate to apply additional provisions as well as those contained within the present document. In all cases, security, data protection and privacy by design and by default should be used to inform the product development process, following risk assessment, but that is out of scope of the present document.

The present document sets a security and data protection baseline; however, due to the broad landscape of consumer IoT it is recognized that the applicability of provisions is dependent on each device. The present document provides a degree of flexibility through the use of non-mandatory "should" provisions (recommendations).

The present document defines the security requirements for the device, it does not define a testing or certification method to assess the requirements against. Some methods of fulfilling the requirements in the present document can impact testing and certification making it very difficult, or even impossible, to demonstrate compliance in certain test regimes.

Testing and certification involving third party assessment is likely to require documentation, including architectural design documentation, security requirements capture and analysis, threat models and environmental assumptions, policy documentation for lifecycle management (including supply chain management), assessment certificates for any components that are used to implement functionality required in the present document. These documentation requirements will be defined by the testing regime and are out of scope of the present document. A way to assess conformance to the present document is specified in ETSI TS 103 701 [i.19].

https://www.etsi.org/about/our-expertise

Defining requirements

- Some requirements are easy to define
- Think about how you would test it
- Others are a lot harder
- How would you test if something is simple?

- You may see a few voids – these used to be requirements but have been removed – without affecting the following section numbers

5.1 No universal default passwords

Provision 5.1-1 Where passwords are used to authenticate users against the device or for machine-to-machine authentication, and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.

NOTE 1: There are many mechanisms used for performing authentication, and passwords are not the only mechanism for authenticating a user to a device. However if they are used, following best practice on passwords is encouraged according to NIST Special Publication 800-63B [i.3].

NOTE 2: Standard pairing codes are not considered as passwords used for machine-to-machine authentication.

Many consumer IoT devices are sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. Continued usage of universal default values has been the source of many security issues in IoT [i.17] and the practice needs to be discontinued. The above provision can be achieved by the use of pre-installed passwords that are unique per device and/or by requiring the user to choose a password that follows best practice as part of initialization, or by some other method that does not use passwords.

Provision 5.3-3 An update shall be simple for the user to apply.

The degree of simplicity depends on the design and intended usage of the consumer IoT device. Some examples can be given as follows, but are not exhaustive. An update that is simple to apply will be automatically applied, initiated using an associated service (such as a mobile application), or via a web interface on the consumer IoT device. If an update is difficult to apply, then that increases the chance that a user will repeatedly defer updating the consumer IoT device, leaving it in a vulnerable state.

Provision 5.3-4 Void.

Summary

- The best way to learn how standards are written is to read a few
- They are surprisingly interesting
- Think of a topic you love and find a standard
- If it is behind a paywall, check with your University Library
- SDOs want to help. Go to the website and ask

Master Tech Standardization

with ETSI

Thank you for your attention

Follow us on: