ETSI TR 104 196 V1.1.1 (2026-02)

TECHNICAL REPORT

Considerations for using portals to support requests from Authorized Organizations

Reference
DTR/LI-00287

Keywords
lawful disclosure, lawful interception,
security requirements

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo 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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

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.

1 Scope

The present document describes considerations for situations in which providers choose to adopt web-based portal solutions to respond to requests from Authorized Organizations. The present document describes portals and explains how existing ETSI TC LI specifications can be used to improve portal design. The present document shows how portals can become a stepping stone towards adoption of interfaces defined by an ETSI TC LI Technical Specification. The present document highlights some caveats around portals and makes it clear that portals are not a substitute for meeting ETSI TC LI Technical Specifications.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TS 103 976: "Interface for Lawful Disclosure of vehicle-related data".

[i.2] ETSI TS 103 120: "Lawful Interception (LI); Interface for warrant information".

[i.3] ETSI TS 103 307: "CYBER; Security Aspects for LI and RD Interfaces".

[i.4] ETSI TS 103 280: "Lawful Interception (LI); Dictionary for common parameters".

[i.5] ETSI TS 103 705: "Lawful Interception (LI); Data Structures for Lawful Disclosure".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 976 [i.1] and the following apply:

Authorized Organization (AO): any organization legally authorized to make requests and receive results

provider: organization responding to a request (the organization that includes the Request Processing System)

Request Processing System (RPS): system within an organization which holds the data that is subject to the request where there is a lawful reason for it to respond to requests for information

3.2 Symbols

Void.

3.3 Abbreviations

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

AO	Authorized Organization
API	Application Programming Interface
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
RPS	Request Processing System
VIN	Vehicle Identification Number

4 Core concepts

4.1 Goal

The goal of the present document is to help people to adopt ETSI TC LI Technical Specifications i.e. full computer-to-computer API (Application Programming Interface). It is acknowledged that initially people might not be able to move to a full computer-to-computer system, and so portals can be a useful stepping stone. The present document aims to assist with the design of portal solutions, and in the longer term to facilitate the move towards adoption of ETSI TC LI Technical Specifications. The present document is neither encouraging nor discouraging the use of portals alongside an API system for the long term. Further details are given in clause 4.5.

4.2 Definition of a portal

A portal is defined to be a website hosted by, or on behalf of the provider which allows an Authorized Organization to type in requests and then receive results either through the website or delivered over other channels (not specified here).

4.3 Caveat

Adoption of the present document does not imply that a system is compliant with any ETSI TC LI Technical Specification; it is not a substitute for compliance with other ETSI TC LI standards.

4.4 Reference design

The approach in Figure 4.4-1 is recommended. The key point is to run one system with two front ends (one for meeting an ETSI Technical Specification, and one for a portal). The goal is to make the front end systems as thin as possible i.e. to put most of the functionality in the main Request Processing System.

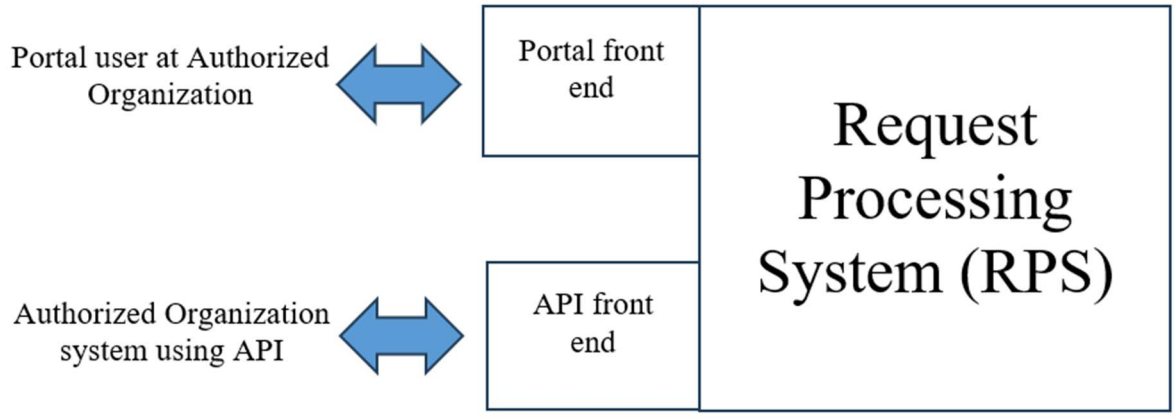

Figure 4.4-1: Approach to portal design

The design in Figure 4.4-1 is not a strict architecture or design and is not intended to constrain data flows or security boundaries.

The functionality in the smaller boxes (labelled front end in Figure 4.4-1) is likely to be different between APIs and portals. This would typically include the following:

- The portal needs a User Interface design; the API needs to terminate API connections.
- The security is different (see clause 4.6).

The functionality in the larger box (labelled Request Processing System in Figure 4.4-1) would typically be created once and could be accessed via both the portal and API solutions. It would typically include:

- Single workflow engine: each request follows the same path regardless of whether it came from the portal or API.
- Single way to submit query into the provider database.
- Single way to create the results (meaning that the results are identical whether requested through a portal or through a API).
- Single approach to supplying integrity information such as hashing (e.g. see also ETSI TS 103 307 [i.3]).
- Single audit log.

4.5 Use of portals alongside systems with full APIs

It is clear that the full API is the best long-term solution for high volume uses, but the present document does not advise in favour or against running portals alongside an API solution. Clause 4.5 notes some benefits and drawbacks of doing this, in order to help people make decisions about use of portals.

Considerations around offering both an ETSI-compliant API and a portal (designed in line with the present document):

- It is credible to state that this is a solution that can meet the needs of any AO globally. If the AO has a high volume of requests, they can use the ETSI-compliant API (designed to meet a wide range of requirements and agreed by a broad community). If an AO has a low volume of requests, or does not want to build a ETSI solution, then they can use the provider portal. With an API and a portal (producing identical results, from the same underlying system), it is realistic to state that no other solution needs to be offered or will be offered by the provider.

Considerations around offering an API (without a portal):

- If a provider offers an API, then it would incur some extra cost to build a portal as well. The present document is not implying it is a requirement to build portals in addition to APIs; in some scenarios the extra expense of a portal might not be justified. The security will be easier without portal access, because then the user management issues (i.e. which users are allowed to access the system) are taken care of by the AO. Further details are given in clause 4.6. The onboarding process is harder for smaller AOs, which can introduce a higher barrier to entry.

4.6 Security

4.6.1 General

The present document does not contain a full analysis of portal security, instead.it identifies some risks and issues to consider.

4.6.2 Clear boundaries of responsibility

The Responsible Owner at an AO is the person who takes responsibility for a request that is issued (Was it lawful? Was it correct? Did it go to the right place? Can I justify it?).

The Responsible Owner at a Provider is the person who takes responsibility for how the request is handled (Did I check it was correct and authorized? Was it lawful to release this data? Can I justify it?).

In order to meet their responsibilities, it is important for a Responsible Owner to understand exactly where their responsibility starts and ends. This point will be called the Front Door. The AO Front Door is the point where a request is issued (under the authority of the AO Responsible Owner). The Provider Front Door is the point where a Provider issues the results (under the authority of the Provider Responsible Owner).

The Responsible Owners may wish to get suppliers or vendors to build systems which help the Responsible Owner meet their responsibilities, i.e. to perform tasks behind the relevant Front Door. The appropriate legislation determines whether risks or obligations can be transferred to suppliers or vendors (it might be the case that risks and obligations ultimately still sit with the Responsible Owner). The Responsible Owners should make sure they know how their obligations are being met. This might include:

- Knowing where their Front Door is and exactly when/why information leaves/enters.
- Factors such as retention periods, user verification, data localization (where is data stored) should be clearly understood by the Responsible Owner.

Care should taken about functionality that sits between the AO Front Door and the Provider Front Door (i.e. is not inside either Front Door). It is likely to be best to minimize any functionality that sits here. It might be unclear who is responsible for anything that is between the Front Doors. The following examples might be relevant:

- Having stateful functionality between the Front Doors risks having a different understanding of the status of requests in AO and Provider. The Responsible Owner might have issued a request which they think has reached its destination but it has not, which might carry serious legal consequences.
- Having processing between the Front Doors might cause an issue when material is used in court. It also creates a risk of differing understandings of the data at AO and Provider. It introduces the risk of mistakes taking place between one Front Door and the other.
- Having storage between the Front Doors could create a data security issue. Who can see the data? Who can access it? Who is responsible for the data if compromised. Ultimately the Responsible Owner at AO or Provider (or both) will carry various consequences here.
- Care should be taken about routeing or proxying between the Front Doors. Basic network-level routeing is often necessary. It is important that the choice of destination for a request was made inside the AO Front Door. Care should be taken about routeing or proxying that could result in requests going to a different place from the Front Door that the Responsible Owner chose.
- There are risks about functionality which could be used by more than one AO or Provider. This carries risk of information going to the wrong place, or data being shared with people who are not entitled to see it.
- Generating requests anywhere other than within the AO runs the risk of the request being unlawful as it might not have been approved and fully understood by the Responsible Owner.

4.6.3 Management of users

An important issue for portals is that the provider is responsible for management of the list of accredited users.

In general, for a portal solution, the provider would be responsible for managing risks arising when users join or leave the Authorized Organization (AO), or where privileges are revoked. Verification of new AO users can be difficult with risks around e-mail spoofing. It is recommended to use a range of techniques (beyond looking at the email domain) in order to build confidence in AO users. The Responsible Owner at the Provider (see clause 4.6.2) is responsible for data released by the Provider and therefore this is the person who needs to understand what assurances were received, so they can decide if they are sufficient. Risks can be introduced if particular AO staff are on leave and so need to allocate certain functions to others. The risks are increased if two different AO organizations are involved.

4.6.4 Other security points

Standard cyber security risks (e.g. Distributed Denial of Service attack) should be considered. It should be noted that an attack through either front end (see figure 4.4-1) can affect the central Request Processing System i.e. care should be taken around the security of both front ends.

If a separate results channel is created, it is important to consider the security of this channel too.

5 Parts of ETSI TC LI Technical Specifications that are applicable to portal design

5.1 List of parts of ETSI TC LI Technical Specifications

It is recommended that the following parts of an ETSI Technical Specification are used (where appropriate) as part of designing portals:

1) Fundamental model. The ETSI model has a clear boundary between what is AO-managed and what is provider-managed. There are strong reasons to have clear boundaries of responsibility: it is fundamental to many legal and policy requirements in various jurisdictions.

2) Definitions: explaining that terms from the relevant specifications (e.g. ETSI TS 103 120 [i.2], ETSI TS 103 280 [i.4] and ETSI TS 103 976 [i.1]) should be used where suitable.

3) Identifiers and house-keeping. This would include using provider and AO identifiers.

4) Request types: for certain situations (e.g. vehicles), there is a clear set of request types (see ETSI TS 103 976 [i.1]). It is recommended that these are used where they are suitable.

5) Results: where a standardized request type has been used (as described in the point about request types), it is recommended to use the corresponding response structures (e.g. see ETSI TS 103 976 [i.1]).

6) Workflow: it is recommended to follow the Workflow steps from an ETSI TS (mostly this is defined in ETSI TS 103 120 [i.2] e.g. see the Simple Workflow in ETSI TS 103 120 [i.2], clause H.2). This gives a structure for when results are delivered and when error responses are sent, etc.

7) Look at ways that ETSI TC LI data structures (ETSI TS 103 705 [i.5]) can be used to help portal design.

User interface design can help support the above points. For example, it would be helpful for a user interface to guide an AO user through the ETSI-defined fields, enforcing the strongly-typed definitions from the very start of the process and using ETSI-defined terminology. It would be helpful for the user interface to guide users through the ETSI-defined workflow.

5.2 Use of ETSI TC LI specifications in a vehicles context

5.2.1 Explanation

Clause 5.2 contains illustrations of the points listed in clause 5.1, specifically for a vehicles context.

5.2.2 Fundamental Model

This point relates to ensuring that the boundaries of responsibility are clearly demarcated. The following transitions should be clear to all parties:

- The point when the AO submits a request (i.e. an obligation is created on the provider). The AO user should be asked to confirm the submission of a request (with clarity about where the request will be sent).
  It is helpful for everyone to be able to see and understand which stage of the workflow (described in clause 5.2.7) is in progress.

- The point when the response is delivered (the end of the obligation on the provider).

5.2.3 Definitions

For vehicles, it is recommended to use the standardized definitions for these concepts (and others where appropriate):

- VIN.
- Location.
- Time and date.
- IMSI and IMEI.

5.2.4 Identifiers

It is helpful to have a clear system of identifiers for every party (AO or provider). It is useful to have a unique name for each organization to prevent confusion. For example, the AOs involve should work together to ensure that they do not re-use common acronyms. It is out of scope to describe personal details for any individuals on either side of the interface. It is helpful to have a unique reference number for each request that is made. There are different ways to create the reference number (either the AO creates it, or the provider does). For a portal it is recommended that there is an option for the AO to include a reference number as it submits the request. The provider is responsible for creating a unique request number (unique within that provider). The provider may use the AO reference number in their request numbering.

5.2.5 Request types

It is recommended that a portal uses any of the request types from ETSI TS 103 976 [i.1], clause 7, that are appropriate.

5.2.6 Results

Wherever one of the ETSI TS 103 976 [i.1] request types has been used, it is recommended to use the accompanying results format.

5.2.7 Workflow

It is recommended to follow the steps in ETSI TS 103 120 [i.2], clause H.2.4. The benefit is that it is clear at all items who is supported to be responding next.

5.2.8 Use of ETSI TC LI data structures

No additional comments on this topic are made in the present document.

Annex A:
Change history

Status of Technical Report ETSI TR 104 196 Considerations for using portals to support requests from Authorized Organizations		
TC LI approval date	**Version**	**Remarks**
January 2026	1.1.1	First publication of the TR after approval at ETSI TC LI#71 in Sophia Antipolis (France)

History

Version	Date	Status
V1.1.1	February 2026	Publication