ASSESSMENT SUMMARY v1.0.0

OpenTelemetry[1]

Cloud Native Computing Foundation (CNCF)[2]

---

[1] OpenTelemetry: https://opentelemetry.netlify.app/docs/specs/otel/

[2] CNCF: https://www.cncf.io/

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

1. INTRODUCTION

The present document is a summary of the assessment of **OpenTelemetry** carried out by CAMSS using the CAMSS EIF assessment scenario. The purpose of this scenario is assessing the compliance of a standard orspecification with the European Interoperability Framework (EIF)[3].

2. ASSESSMENT SUMMARY

OpenTelemetry is an observability framework and toolkit designed to create and manage telemetry data such as traces, metrics, and logs. Crucially, OpenTelemetry is vendor- and tool-agnostic, meaning that it can be used with a broad variety of observability backends, including open source tools like Jaeger and Prometheus, as well as commercial offerings.

Cloud Native Computing Foundation (CNCF) as part of the Linux Foundation, they provide support, oversight and direction for fast-growing, cloud native projects, including Kubernetes, Envoy, and Prometheus[2]. Cloud native technologies empower organisations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.

2.1 Interoperability Principles

Interoperability principles are fundamental behavioural aspects that drive interoperability actions. They are relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented.

***The specification does not support the principles setting context for EU actions on interoperability*:**

- **Subsidiarity and proportionality**
  OpenTelemetry has not been found included within the catalogue of any Member State.

***The specification fully supports the principles setting context for EU actions on interoperability*:**
- **Openness**
  OpenTelemetry is an open source, vendor-neutral observability framework supports methods for monitoring browser applications and publishing telemetry data on the web. All major and minor releases foresee a public review in the OpenTelemetry GitHub[4], where anyone can contribute. The specification is in its 33rd version and is licensed under its Apache 2.0 License[5], whose main conditions require preservation of copyright and license notices.

---

[3] European Interoperability Framework (EIF): https://ec.europa.eu/isa2/eif_en
[4] OpenTelemetry GitHub: https://github.com/open-telemetry/opentelemetry-collector
[5] Apache 2.0 License: https://www.apache.org/licenses/LICENSE-2.0.html

As an industry-standard, OpenTelemetry is supported by more than 40 observability vendors, integrated by many libraries, services, and apps, and adopted by numerous end users. Moreover, there is a mailing list communicating updates, community meetings are held regularly and even special interest groups (SIGs) for specific if one is interested in being part of the specification's community.

- **Transparency**
OpenTelemetry significantly enhances the visibility of administrative procedures by providing comprehensive observability tools that offer deep insights into system performance, reliability, and behaviour. In addition, it can be comprehensively scoped to provide significant insights into administrative procedures. For instance, by instrumenting each step of an administrative procedure, OpenTelemetry captures detailed information about the execution flow, including the time taken at each step and any errors encountered. By leveraging OpenTelemetry, public administrations can ensure their services are robust, efficient, and user-friendly, leading to better service delivery.

- **Reusability**
OpenTelemetry is highly usable beyond any specific business domain due to its standardised, extensible, and flexible design. Its broad ecosystem support and applicability to various industries make it a powerful tool for achieving comprehensive observability. By enabling detailed monitoring and analysis of applications and services, OpenTelemetry facilitates improved performance, reliability, and efficiency across diverse business domains.

- **Technological neutrality and data portability**
The OpenTelemetry specification is technology- and platform-agnostic, enabling it to be used across diverse technology stacks, platforms, and programming languages. Its standardised protocols, broad language support, modular architecture, and extensive integration capabilities make it a versatile and powerful tool for achieving comprehensive observability in any environment.

OpenTelemetry's design allows for flexible, partial implementations, making it highly adaptable to varying organizational needs and constraints. In addition, the OpenTelemetry specification allows extensive customisation and extensions to meet the specific needs and requirements of different applications and environments. OpenTelemetry significantly enhances data portability between systems and applications. In fact, one of the main functionalities regarding OTel is to export telemetry data to back-end systems and platforms like ElasticSearch or Prometheus.

The specification partially supports the principles related to generic user needs and expectations:
- **User-centricity**
OpenTelemetry empowers organisations to capture and reuse relevant information effectively through its standardised data collection, interoperability, and supportive community ecosystem. In addition, context propagation helps to reuse context data as centralised data collection ensure that there are no duplicates and it is collected only once.

- **Inclusion and accessibility**

  OpenTelemetry's observability capabilities can indirectly support the development, monitoring, and improvement of accessible digital services. By providing insights into performance, errors, user behaviour, compliance, and integration with accessibility tools, OpenTelemetry contributes to creating a more inclusive digital environment where individuals with disabilities can access and interact with services effectively.

- **Privacy**

  OpenTelemetry is not related to any privacy matter. Therefore, this criterion is considered not applicable to this specification.

- **Security**

  The OpenTelemetry Collector defaults to operating in a secure manner, even though it is configuration driven[6]. OTel configuration should ensure sensitive configuration information is managed securely. The Collector should be configured to obfuscate or scrub sensitive data before exporting. Furthermore, some components may require privileged access and care should be taken before enabling these components. Component developers should minimise privileged access requirements and must document what requires privileged access and why. OpenTelemetry explicitly addresses and guarantees data accuracy through data sampling. The idea behind sampling is to control the spans sent to an observability backend, resulting in lower ingest costs.

- **Multilingualism**

  While not a direct feature of OpenTelemetry, applications instrumented with OpenTelemetry can incorporate internationalisation (i18n) support to handle multilingual content and user interfaces effectively. OpenTelemetry can capture telemetry data related to user interactions with multilingual content, providing insights into how different language versions of an application are used.

The specification fully supports the foundation principles for cooperation among public administrations:
- **Administrative Simplification**

  OpenTelemetry can improve the delivery of public services as monitoring telemetry data can help improve the systems used to provide citizens with public services. Furthermore, by providing essential observability and monitoring capabilities, OpenTelemetry can ensure the effective delivery of digital services through various channels, including web applications, APIs, mobile apps, and IoT devices.

---

[6] OTel Security Best Practices: https://github.com/open-telemetry/opentelemetry-collector/blob/main/docs/security-best-practices.md

- **Preservation of information**

    While the primary focus of OpenTelemetry is on observability and monitoring of digital systems, OpenTelemetry can improve long-term preservation of electronics resources through the integration with storage backends.

- **Assessment of effectiveness and efficiency**

    The effectiveness and efficiency of OpenTelemetry is often evaluated through various means, including practical implementations and scalability. For instance, a 2024-paper[7] about network insights in OpenTelemetry explores the integration of network telemetry data into OpenTelemetry, aiming to provide a holistic understanding of application performance and detect network-related issues. On the other hand, another 2024-paper[8] about the development of an OpenTelemetry extension for call graphs highlights OTel agents to automatically collect data required for call graph creation.

2.2 Interoperability Layers

The interoperability model which is applicable to all digital public services includes:
- Four layers of interoperability: legal, organisational, semantic, and technical.
- A cross-cutting component of the four layers "integrated public service governance".
- A background layer, "interoperability governance".

The Specification supports the implementation of digital public services complying with the EIF interoperability model:
- **Interoperability Governance**

    OpenTelemetry is associated with EIRA ABB's in the EIRA Library of Interoperability Specifications (ELIS). More specifically, it is associated with the "Artificial Intelligence" and "Audit" ABBs from the "Technical-Application" View and the "Analytics" and "Telemetry" ABBs from the "Technical-Infrastructure" View of the current European Library Of Specifications (ELIS).

    The conformance of OpenTelemetry implementations can be assessed through various means. For instance, some supported languages such as Erlang/Elixir have a testing section where it is specified how to validate spans and attributes. The specification is included in the Spanish National Institute of Cybersecurity (INCIBE)[9]. OpenTelemetry-Go Contrib is a collection of third-party packages for OpenTelemetry-Go. An attacker can easily flood the peer address and port for requests. Version 0.46.0 contains a fix for this issue. However, OTel is not part of any national catalogue of standards of any Member State nor any European initiative.

---

[7] Network insights in OpenTelemetry: https://eprints.ost.ch/id/eprint/1165/
[8] OpenTelemetry Extension for Supporting Call Graphs: https://www.tdcommons.org/dpubs_series/6992/
[9] INCIBE-CERT Vulnerabilities: https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-47108

- **Legal interoperability**

    OpenTelemetry is developed by the Cloud Native Computing Foundation (CNCF), an organisation based in the US that hosts and promotes open source projects for cloud native computing. Moreover, OTel does not appear in any of the main European standard development bodies, therefore, the specification is not a European standard.

- **Organisational interoperability**

    Modelling business processes typically involves higher-level concepts and frameworks that go beyond the scope of network protocols like OTel. However, by adopting OpenTelemetry, organisations can ensure consistent observability practices, seamless integration of monitoring tools, and enhanced collaboration across diverse IT environments.

- **Semantic Interoperability**

    OpenTelemetry is an open source project that anyone in the community[10] can use and improve. The community uses GitHub discussions[11] for most communications. For those who are brand new to OpenTelemetry and want to chat or get redirected to the appropriate place for a specific question, they can join the CNCF OTel Slack channel[12].

---

[10] OpenTelemetry Community: https://opentelemetry.io/community/
[11] OTel GitHub Discussions: https://github.com/open-telemetry/community/discussions
[12] CNCF OpenTelemetry Slack channel: https://opentelemetry.io/community/end-user/slack-channel/

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for the **OpenTelemetry.** The CAMSS "Strength" indicator measures the reliability of the assessment by calculating the number of answered (applicable) criteria. On the other hand, the number of favourable answers and the number of unfavourable ones is used to calculate the "Automated Score" per category and an "Overall Score".

Category	Automated Score	Assessment Strength	Compliance Level
Principles setting the context for EU actions on interoperability	20/100 (20%)	100%	Ad-hoc
Core interoperability principles	1680/1700 (99%)	100%	Seamless
Principles related to generic user needs and expectations	940/1200 (78%)	75%	Sustainable
Foundation principles for cooperation among public administrations	480/500 (96%)	100%	Seamless
Interoperability layers*	740/1000 (74%)	80%	Sustainable
Overall Score	3360/4000 (84%)[13]	89%	

The technical interoperability layer is covered by the criteria corresponding to the core interoperability principle ''Openness''.

With an 89% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 84% (3360/4000) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

---

[13] See the "results interpretation" section of the CAMSS Assessment EIF Scenario Quick User Guide: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-eif-scenario/results-visualisation-and-interpretation