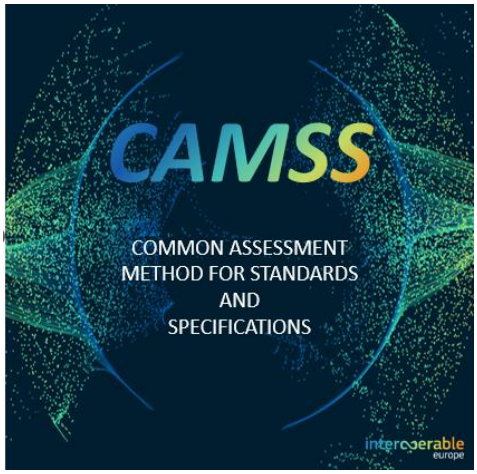

ASSESSMENT SUMMARY v1.0.0

The Syslog Protocol[1]

Internet Engineering Task Force (IETF)[2]

[1] The Syslog Protocol: https://datatracker.ietf.org/doc/html/rfc5424

[2] IETF: https://www.ietf.org/

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 **the Syslog Protocol** 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

The Syslog Protocol specification is a standard for message logging, which is used to convey event notification messages. This protocol utilizes a layered architecture, which allows the use of any number of transport protocols for transmission of syslog messages. It also provides a message format that allows vendor-specific extensions to be provided in a structured way.

The Syslog Protocol is developed by the IETF, which was founded in 1986, and aims to be the premiere standards development organization (SDO) for the Internet. The IETF makes voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, and it thus helps shape the trajectory of the development of the Internet. Thanks to this specification, logs can then be accessed by analysis and reporting software to perform audits, monitoring, troubleshooting, and other essential IT operational tasks, which can enhance interoperability and eGovernment.

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 specifically addresses interoperability in cloud computing, which can be extremely useful in eGovernment by enhancing data portability, increased efficiency and integrity.

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

- **Subsidiarity and proportionality**
  The Syslog Protocol is not included in any national catalogue of recommended specifications whose Member State NIF has a high performance on interoperability according to NIFO factsheets.

The specification fully supports the principles setting context for EU actions on interoperability:

- **Openness**

  The Syslog Protocol supports publication of data on the web with an open license and in a structured, machine-readable format. It is a free and open technical specification, built on IETF standards and licenses from the Open Web Foundation. The development and maintenance of this specification is carried out within the IETF Syslog Protocol working group[4].

[3] European Interoperability Framework (EIF): https://ec.europa.eu/isa2/eif_en
[4] IETF Working Groups: https://www.ietf.org/how/wgs/

This specification's development process includes a formal review and approval so that all the relevant stakeholders can formally appeal or raise objections to the development and approval of specifications. As a consensus-based group, IETF follows a specification development process in which both the review and the collected feedback is visible. In fact, the Syslog Protocol has published documentation on its supporting processes and welcomes the critical evaluation of protocols and has provided guidance for it. Furthermore, Syslog Protocol implementations are directly used to create innovative solutions. For instance, syslog-ng[5], developed byBalabit IT Security Ltd, is a log management solution that improves the performance Security Information and Event Management (SIEM) solution.

- **Transparency**

  The Syslog Protocol is a powerful tool for providing visibility into administrative procedures, rules data, and services within a networked environment. For example, it can be configured to log various administrative actions and commands executed on network devices, servers, or other systems. Also, it is a versatile logging protocol that allows for the comprehensive capture of administrative procedures by allowing standard user authentication and authorization, configuration changes, firewall and security rules, Intrusion Detection/Prevention Systems (IDS/IPS), network services, etc.

  The Syslog Protocol is not inherently designed for the purpose of exposing interfaces to access public administration services. However, it can indirectly contribute to the management and monitoring of public administration services by providing a standard in logging security events, providing an audit trail for security-related activities. This is essential for public administration services to identify and respond to potential security threats.

- **Reusability**

  The Syslog Porotocol is a widely used and standardized protocol for message logging, making it relatively versatile and applicable across different domains, including various business sectors. Its standardization allows different systems and devices to communicate using a common logging format. Therefore, it is abstract and can be implemented and/or used in any domain as long as it fulfills the requirements.

- **Technological neutrality and data portability**

  Syslog Protocol is designed to be flexible, and it does allow for partial implementations. It is technology-agnostic at the application layer as it operates at the network layer and focuses on the transport of log messages between devices and systems. Also, it is considered platform-agnostic, as it is designed to provide a standardized method for message logging and can be implemented on various operating systems, including Unix, Linux, Windows, and others.

[5] Syslog-ng: https://www.syslog-ng.com/

The specification is designed to be flexible, and partial implementations are possible based on the specific needs and requirements of a system or application. Furthermore, it allows for customisation to a significant extent. The Syslog Protocol is designed to be flexible, and various elements within syslog messages such as message content and facility codes can be customised based on specific needs and requirements. In this manner, it provides a message format that allows vendor-specific extensions to be provided in a structured way. Finally, The Syslog Protocol can contribute to data portability between systems and applications supporting the implementation or evolution of European public services as it provides a standardised protocol for message logging, which is crucial in security and traceability matters.

***The specification partially supports the principles related to generic user needs and expectations*:**

- **User-centricity**

  The Syslog Protocol provides a standardized framework for logging messages, and to a considerable extent, it supports the reuse of relevant information when needed. Some aspects of the syslog protocol that facilitate information include structured data, standardised message format, integration with logging systems, etc.

- **Inclusion and accessibility**

  While the Syslog Protocol itself does not have direct features related to e-accessibility, the way it is implemented and integrated within systems can have implications for accessibility considerations. For instance, log content accessibility can be improved through this specification. The content of syslog messages can be crafted in a way that is accessible to individuals with disabilities.

- **Privacy**

  While The Syslog Protocol itself does not inherently ensure the protection of personal data, its implementation and usage within public administrations can have implications for data protection. Having a standard way for event data logs can improve the protection of personal data. The specification does not have mechanisms to provide confidentiality for the messages in transit logging nor has been found included in any initiative neither at European nor on national level covering privacy aspects.

- **Security**

  The Syslog Protocol provides with security features for the exchange of data as all implementations of this specification MUST support a TLS-based transport, which also can support the authenticity of the roles involved in data transactions to a certain extent. The protocol does not mention any specific provision for data integrity, but it is specified that any syslog transport protocol must not deliberately alter the syslog message. Furthermore, the Syslog Protocol does not provide a built-in access control mechanism.

- **Multilingualism**

  Section 7.3.3[6] of the specification addresses language. It is mentioned that the "language" parameter may be specified by the originator to convey information about the natural language used inside the message.

The specification supports the foundation principles for cooperation among public administrations:

- **Administrative Simplification**

  While The Syslog Protocol itself is not directly designed for the delivery of public services, it can contribute to the overall efficiency, security, and reliability of IT systems, which may, in turn, impact European public services delivery. In comparison, the specification is not directly designed to enable digital service delivery channels.

- **Preservation of information**

  The Syslog Protocol, as a protocol for message logging, is not specifically designed for the long-term preservation of data, information, or electronic records. Its primary function is to transmit and store log messages related to system events, errors, and activities. However, organizations can leverage syslog in conjunction with other practices to contribute to the long-term preservation of relevant information.

- **Assessment of effectiveness and efficiency**

  The effectiveness and efficiency of the Syslog Protocol often evaluated through various means, including practical implementation and scalability. For instance, a 2013-paper[7] proposes the Syslog Protocol as a promising solution to Log Management and another 2020-paper[8] mentions how efficient and robust syslog parsing is for network devices in datacenter networks.

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”.

[6] Syslog Protocol Language: https://datatracker.ietf.org/doc/html/rfc5424#section-7.3.3
[7] Syslog a Promising Solution to Log Management:
https://www.researchgate.net/profile/Prasanta-Sahoo-3/publication/332780312_Syslog_a_Promising_Solution_to_Log_Management/links/5cc9415c4585156cd7bdf3c0/Syslog-a-Promising-Solution-to-Log-Management.pdf
[8] Efficient and Robust Syslog Parsing for Network Devices in Datacenter Networks:
https://ieeexplore.ieee.org/abstract/document/8988255

The Specification supports partially the implementation of digital public services complying with the EIFinteroperability model:

- **Interoperability Governance**

  At the time of elaborating this assessment, this specification is included in the Controlled Vocabulary ABB in the current European Library of Specifications (ELIS). The conformance of the Syslog Protocol implementations can be assessed against the requirements and specifications outlined in the protocol to ensure that it adheres to the standard. In addition, no Member States have been found recommending the Syslog Protocol in their ICT National Catalogues, their catalogues of recommended specifications nor an open repository/catalogue of standards at European level.

  In contrast, the Syslog Protocol has been selected for its use in the European Data Protection Supervisor (EDPS)[9]. It is the European Union's (EU) independent data protection authority, and they aim to monitor, advise, intervene, and cooperate in personal data and privacy matters regarding EU institutions. It is mentioned that the specification is the administrative management tool for training at the European Commission in three fields: informatics, language and general.

- **Legal interoperability**

  The Syslog Protocol is not a European Standard as it is not developed nor maintained by any European organisation nor initiative. It is developed by IETF, a standard development organisation based in the US. Moreover, the syslog protocol specification does not appear in any of the main European standard development bodies, therefore, the specification is not a European standard.

- **Organisational interoperability**

  The Syslog Protocol is not designed specifically for modelling business processes. It doesn't provide the necessary features or structures for representing business processes in a visual or diagrammatic way. However, syslog can indirectly contribute to organizational interoperability by providing a standardised communication format, thus improving cross-platform compatibility and secure information exchange.

- **Semantic Interoperability**

  The Syslog Protocol encourages collaboration in the field of message logging. For instance, IETF has created discussions lists[10] for their specifications that improve the development and specification of Internet technology through the general discussion of technical, procedural, operational, and other topics for which no dedicated mailing lists exist.

[9] EDPS: https://edps.europa.eu/_en

[10] IETF Discussion Lists: https://www.ietf.org/how/lists/discussion/

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for the **Syslog Protocol.** 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	1640/1700 (96%)	94%	Seamless
Principles related to generic user needs and expectations	1000/1200 (83%)	75%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	80%	Seamless
Interoperability layers*	580/1000 (58%)	90%	Essential
Overall Score	3140/3900 (80%)[11]	87%	

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

With a 87% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 80% (3140/3900) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[11] 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