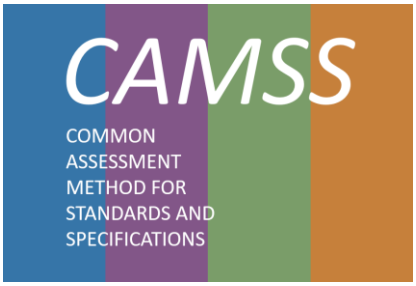

ASSESSMENT SUMMARY v1.0.0

Lightweight Directory Access Protocol (LDAP)[1]

Internet Engineering Task Force (IETF)[2]

[1] LDAP specification: RFC 4511 – Lightweight Directory Access Protocol (LDAP): The Protocol (ietf.org)

[2] IETF: IETF | Internet Engineering Task Force

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 **Lightweight Directory Access Protocol (LDAP)** carried out by CAMSS using the CAMSS Assessment EIF scenario[3]. The purpose of this scenario is to assess the compliance of a standard or specification with the European Interoperability Framework (EIF)[4].

2. ASSESSMENT SUMMARY

The **Lightweight Directory Access Protocol (LDAP)** The Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs on a layer above the TCP/IP stack. It provides a mechanism used to connect to, search, and modify Internet directories. The LDAP directory service is based on a client-server model. The function of LDAP is to enable access to an existing directory.

LDAP works on both public networks and private intranets and across multiple directory services, making it the most convenient language for accessing, modifying, and authenticating information in any directory.

LDAP has been developed by the Internet Engineering Task Force (IETF), an open standards organization that develops and promotes voluntary Internet standards, in particular the technical standards that comprise the Internet protocol suite (TCP/IP).

2.1. EIF 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 fully supports the principles setting context for EU actions on interoperability*:**

- **Subsidiarity and proportionality**
  According to the National Interoperability Framework Observatory (NIFO)[5] factsheets, LDAP is included in nine national catalogues of recommended specifications among which three countries are fully aligned with the European Interoperability Framework (EIF).

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

- **Openness**
  LDAP is a protocol that makes it possible for applications to query user information rapidly. The specification has been developed by the IETF, a standard developer organization whose work is

[3] CAMSS Assessment EIF scenario v5.0.0: https://ec.europa.eu/eusurvey/runner/EIFScenario_v500

[4] ISA2 Porgramme: https://ec.europa.eu/isa2/eif_en

[5] NIFO Factsheets: https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory-nifo/nifo-factsheets

accessible to all stakeholders and undergoes public reviews. The IETF is also in charge of maintaining the specification, nonetheless, some other communities offer assistance in its development and distribute the open-source version of the specification on their websites, such as OpenLDAP[6].

It is worth noting that LDAP is considered a standard protocol and has a wide market acceptance. It is excellent when it comes to authenticating Linux-based applications including many open-source solutions such as OpenVPN or Kubernetes and it is also used to complement Active Directory (AD)[7]as a directory services protocol. In terms of availability, LDAP is publicly available and it is licensed on a royalty-free basis for its implementation and study.

- **Transparency**
  Although the purpose of LDAP is other than enabling visibility of administrative procedures and does not enable the exposure of interfaces, it does tackle the comprehensibility of data as it is a tool that enables to access user information in the network in a human-readable manner. When it comes to the protection of personal information, LDAP foresees a set of security layers that require authentication mechanisms such as SASL and TLS. Furthermore, full conformity with LDAP demands the implementation of these security mechanisms.

- **Reusability**
  Being a standard protocol for maintaining and accessing directory services, LDAP can be used across business domains as long as they require the storage and management of user information. Moreover, it is publicly available for its use for free on the IETF website and it is also distributed in many developer communities.

- **Technological neutrality and data portability**
  It can be stated that LDAP is designed to be implemented across business domains and it is not dependent on a specific platform. Partial implementations of the specification, nonetheless, can only be implemented incrementally, to support some requirements and add-ons that are not mandatory but recommended. Therefore it allows for extensions, but its core principles are not meant to be customised. The wide use of LDAP makes it a source that enhances interoperability between systems since it allows many applications and services to connect to LDAP servers.

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

- **User-centricity**

[6] Open LDAP website: OpenLDAP, Main Page

[7] Active Directory Website: Azure Active Directory | Microsoft Azure

LDAP fosters the OOP in terms of accessibility by allowing the administration's stakeholders to keep the contact and access different distributed services without providing personal data for authentication more than strictly needed.

- **Inclusion and accessibility**
  The purpose of LDAP is not related to e-accessibility, therefore this criterion is considered not applicable to this specification.

- **Security and privacy**
  Given that one of the main purposes of LDAP is to help users connect to their IT resources safely, it has become a staple of the identity management industry, many mechanisms and solutions have been added to tackle secure exchange and processing of data issues. Moreover, LDAP can be developed to meet the highest standards of security when it is responsible for transporting sensitive information.

- **Multilingualism**
  The purpose of LDAP is not related to the delivery of multilingual European Public Services. Therefore, this criterion is considered not applicable to this specification.

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

- **Administrative Simplification**
  LDAP helps the administration simplification by easing the access of distributed directories information over a network. By ensuring access to different directory services, it fosters the implementation of digital services, supporting the principle of digital-first.

- **Preservation of information**
  The specification's purpose is not directly the long-term preservation of electronic records.

- **Assessment of effectiveness and efficiency**
  The maturity of the specification makes it prone to be subject to analysis and assessments. For that matter, there can be found a relatively large number of studies assessing LDAP's efficiency as well as its effectiveness.

2.2. EIF 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**
  LDAP can be mapped with EIRA, specifically with two ABBs in the technical view "Service Registry Component" and "Registration Service". Moreover, the specification is recommended and included in the ICT catalogue of nine member states including Spain, France and Germany. It is also included in the European List of ICT standards for e-procurement[8] and can be found in the Joinup repository. In terms of implementation conformity, IETF does not provide any tool, but there can be found many online documents that help validate LDAP when it is implemented.

- **Legal Interoperability**
  LDAP appears in the Commission Implementing Decision of 3 April 2014 on the identification of ICT technical specifications eligible for referencing in public procurement. The directive points out the urgency to set standards with the purpose of gaining interoperability between European member states.

- **Organisational interoperability**
  LDAP is a stable technology that has the potential to increase interoperability and constitutes a de-facto standard for authentication, For that matter, the LDAP standard can facilitate organisational interoperability agreements.

- **Semantic Interoperability**
  LDAP appears on many websites and is a subject of discussion among the communities implementing it. The OpenLDAP for instance operates two IRC channels focused on discussions related to LDAP development. At a European level, the Jinup platform holds many discussion topics about LDAP as well as it gives access to it.

[8]Commission Implementing Decision of 3 April 2014 on the identification of ICT technical specifications eligible for referencing in public procurement: EUR-Lex - 32014D0188 - EN - EUR-Lex (europa.eu)

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **LDAP**. 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
EIF Principle setting the context for EU actions on interoperability	100/100 (100%)	100%	Seamless
Core interoperability principles	2000/2100 (95,2%)	86%	Seamless
Principles related to generic user needs and expectations	500/500 (100%)	60%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	80%	Seamless
Interoperability layers*	1080/1100 (98,1%)	100%	Seamless
Overall Score	4180/4300 (92,7%)	86%	

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

With an 86% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 97,2% (4180/4300) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.