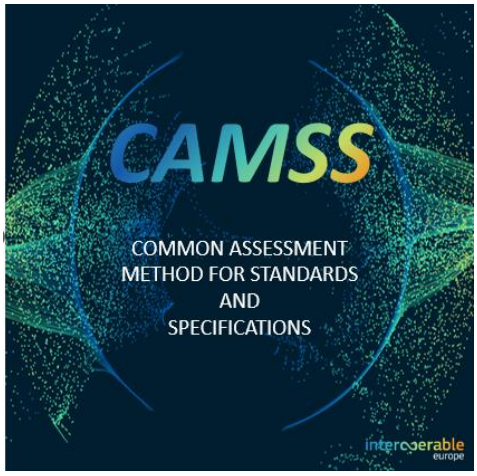

ASSESSMENT SUMMARY v1.0.0

System for Cross-domain Identity Management (SCIM)[1]

Internet Engineering Task Force (IETF)[2]

[1] SCIM: https://scim.cloud/

[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 **SCIM** 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 System for Cross-domain Identity Management (SCIM) specification is designed to make managing user identities in cloud-based applications and services easier. The specification suite seeks to build upon experience with existing schemas and deployments, placing specific emphasis on simplicity of development and integration, while applying existing authentication, authorization, and privacy models.

SCIM 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. In this case, this specification's intent is to reduce the cost and complexity of user management operations by providing a common user schema and extension model, as well as binding documents to provide patterns for exchanging this schema using standard protocols can be useful in the context of 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 fully supports the principles setting context for EU actions on interoperability*:**

- **Subsidiarity and proportionality**
  SCIM is listed in the national catalogue of the Netherlands[4]. The National Interoperability Framework (NIF) of these Member States is fully aligned with all the 3 sections of the European Interoperability Framework (EIF) according to the National Interoperability Framework Observatory (NIFO) factsheets[5].

[3] European Interoperability Framework (EIF): https://ec.europa.eu/isa2/eif_en
[4] CAMSS List of Standards: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards
[5] NIFO factsheets: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2023

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

- **Openness**

  SCIM 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 Internet Engineering Task Force (IETF) SCIM working group[6].

  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, SCIM has published documentation on its supporting processes and welcomes the critical evaluation of protocols and has provided guidance for it. Furthermore, SCIM implementations are directly used to create innovative solutions. For instance, Microsoft uses SCIM 2.0 to develop and plan provisioning for a SCIM endpoint in Microsoft Entra ID[7].

- **Transparency**

  SCIM is an HTTP-based protocol that makes managing identities in multi-domain scenarios easier to support via a standardized service. Therefore, its use improves the interoperability and standardization of the exchange of user identity information between identity domains, which can contribute to some extent for the visibility of administrative procedures, rules data, and services, the comprehensibility of Public Administrations data and exposure of interfaces to access public administration services.

- **Reusability**

  This specification refers to the System for Cross-domain Identity Management whose purpose is to securely automate the exchange of user identity data between a company's cloud applications and any service providers. It is inherently abstract and can be implemented and/or used in any domain as long as it fulfills the requirements. Therefore, its use goes beyond a specific business domain.

- **Technological neutrality and data portability**

  SCIM is a standardised protocol based on web standards, particularly RESTful principles, and JSON (JavaScript Object Notation) for data representation. The specification is designed to work across different technology stacks and platforms. SCIM is not tied to any specific programming language, operating system, or environment.

[6] IETF Working Groups: https://www.ietf.org/how/wgs/

[7] Azure Active Directory SCIM Provisioning: https://learn.microsoft.com/en-us/entra/identity/app-provisioning/use-scim-to-provision-users-and-groups

SCIM is designed to be flexible, and it does allow for partial implementations. It defines a set of core features, including the ability to create, read, update, and delete user identities and their associated attributes. In addition, customisation is also possible through extensions, the core SCIM specification defines a set of standard features for identity management, it also provides a framework for extending these capabilities to meet specific extension requirements. Besides, while SCIM is primarily designed for managing identity information, its features can contribute to data portability in the context of user identities within the European public services framework.

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

- **User-centricity**

  While SCIM primarily focuses on identity management, its features promote the efficient and consistent reuse of relevant identity information across systems. Organizations can tailor their SCIM implementations to meet their specific needs and ensure that relevant information is exchanged and reused effectively in their identity management processes.

- **Inclusion and accessibility**

  SCIM is not focused on enabling e-accessibility as it was designed to make identity management in cloud-based applications and services easier. Therefore, this criterion is considered not applicable to this specification.

- **Privacy**

  The SCIM protocol[8] explicitly addresses data protection and its alignment to relevant regulations. Some considerations include what to do in case of disclosure of sensitive information in URIs or secure storage and handling of sensitive data. In addition, to be able to make access control related decisions that are based on reliable identities and properties of Participants, a concept for Identity and Access Management (IdAM) is mandatory. The primary means for controlling access in SCIM are based on authentication and authorization mechanisms.

- **Security**

  SCIM itself does not provide encryption or security mechanisms at the protocol level. Nonetheless, it leverages underlying security features of the HTTP protocol and can be implemented in a secure manner. While SCIM defines mechanisms for authentication and authorization, the guarantee of authenticity and authentication of the roles involved in data transactions ultimately depends on the implementation of SCIM and the security practices adopted by the participating entities.

[8] SCIM Protocol: https://datatracker.ietf.org/doc/html/rfc7644

Identity management technologies like SCIM inherently include access control that allows organisations to define who has permissions to perform specific operations on user identities, which is indirectly enabling data integrity. Also, the use of secure transport mechanisms (such as HTTPS) contributes to data integrity during transmission, preventing unauthorized tampering and ensuring the accuracy of the exchanged data.

- **Multilingualism**
  While SCIM itself does not have explicit language-related features, its extensibility and flexibility allow organizations to adapt the implementation to meet multilingual requirements.

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

- **Administrative Simplification**
  SCIM could contribute to simplifying the delivery of European public services by providing a standardized and interoperable way to exchange identity information. In fact, its implementation can contribute to digital service delivery channels. Efficient identity provisioning and management through SCIM can support operations for creating, updating, and deactivating user identities, ensuring that users can quickly access and utilise digital services.

- **Preservation of information**
  SCIM does not foster the long-term preservation of electronic records nor other kinds of information. The purpose of the specification is not related to the preservation of information.

- **Assessment of effectiveness and efficiency**
  The effectiveness and efficiency of SCIM often evaluated through various means, including practical implementation and scalability. For instance, a 2023-paper[9] highlights how SCIM is a relevant industry standard for Identity and Access Management (IdAM) and another 2023-paper[10] talks about how SCIM can be a solution for the challenges presented in access management in centralized and decentralized identity governance.

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”.

[9] SCIM - Survey and Enhancement With RBAC: https://ieeexplore.ieee.org/abstract/document/10214272
[10] A Survey on IdAM for Cross-Domain Dynamic Users: https://ieeexplore.ieee.org/abstract/document /10132479

The Specification supports the implementation of digital public services complying with the EIF interoperability model:

- **Interoperability Governance**

  This specification is included in the Controlled Vocabulary ABB in the current European Library of Specifications (ELIS). SCIM enables the set of processes, policies and technologies used to manage and secure digital entities of individuals, devices and applications. Also, the specification has a compliance test[11] in GitHub where any user can access it and execute it to assure the specification's correct implementation.
  SCIM is recommended by Malta and the Netherlands according to the CAMSS List of Standards. In fact, SCIM is recommended by the Netherlands Standardisation Forum[12].

  This specification is mentioned in the European Union Agency for Cybersecurity (ENISA) 2022 study about Digital Identity[13] and in the Rolling Plan for ICT standardisation of 2023 by the European Commission. Specifically, it mentioned in the Cloud and Edge Computing Rolling Plan[14], which aims to establish a coherent framework and conditions for cloud computing in Europe.

- **Legal interoperability**

  SCIM is not a European Standard as it is not developed nor maintained by any European organisation nor initiative.

- **Organisational interoperability**

  . While SCIM may not be used for modelling broader business processes, it can be part of a larger ecosystem that includes business process modelling tools, identity and access management (IdAM). In this context, SCIM serves a specific role in handling identity-related tasks within the broader framework of business operations. For instance, SCIM provides a standardised protocol that helps ensure that different systems, even from different organizations, can understand and process identity data in a consistent manner.

- **Semantic Interoperability**

  SCIM encourages collaboration in the realm of identity management as it was created by IETF, a non-profit and open organisation dedicated to standardisation. IETF encourages collaborative efforts that extend beyond the specifications themselves and include discussions, forums, and knowledge-sharing platforms where users can exchange ideas, experiences, and best practices related to SCIM.

[11] SCIM 2.0 Compliance Test Utility: https://github.com/suvera/scim2-compliance-test-utility
[12] Netherlands Standardisation Forum: https://www.forumstandaardisatie.nl/open-standaarden/aanbevolen
[13] ENISA Digital Identity: https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust
[14] Cloud and Edge Computing Rolling Plan 2023: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/cloud-and-edge-computing-rp-2023

3. *ASSESSMENT RESULTS*

This section presents an overview of the results of the CAMSS assessments for **SCIM.** 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	100/100 (100%)	100%	Seamless
Core interoperability principles	1600/1700 (94%)	100%	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*	920/1000 (92%)	100%	Seamless
Overall Score	3720/4100 (91%)[15]	91%	

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

With a 91% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 91% (3720/4100) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[15] 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