



THE ITALIAN
EDUCATION
& RESEARCH
NETWORK

Relazione del Servizio IDEM GARR AAI

Davide Vagheti <davide.vagheti@garr.it>

Assemblea dei Membri della Federazione IDEM
8 Marzo 2024



Agenda

- Stato della Federazione
- Statistiche di utilizzo
- Obiettivi e progetti del Servizio IDEM per il 2024

Nuovi Membri e Servizi (2023/01-2024-02)

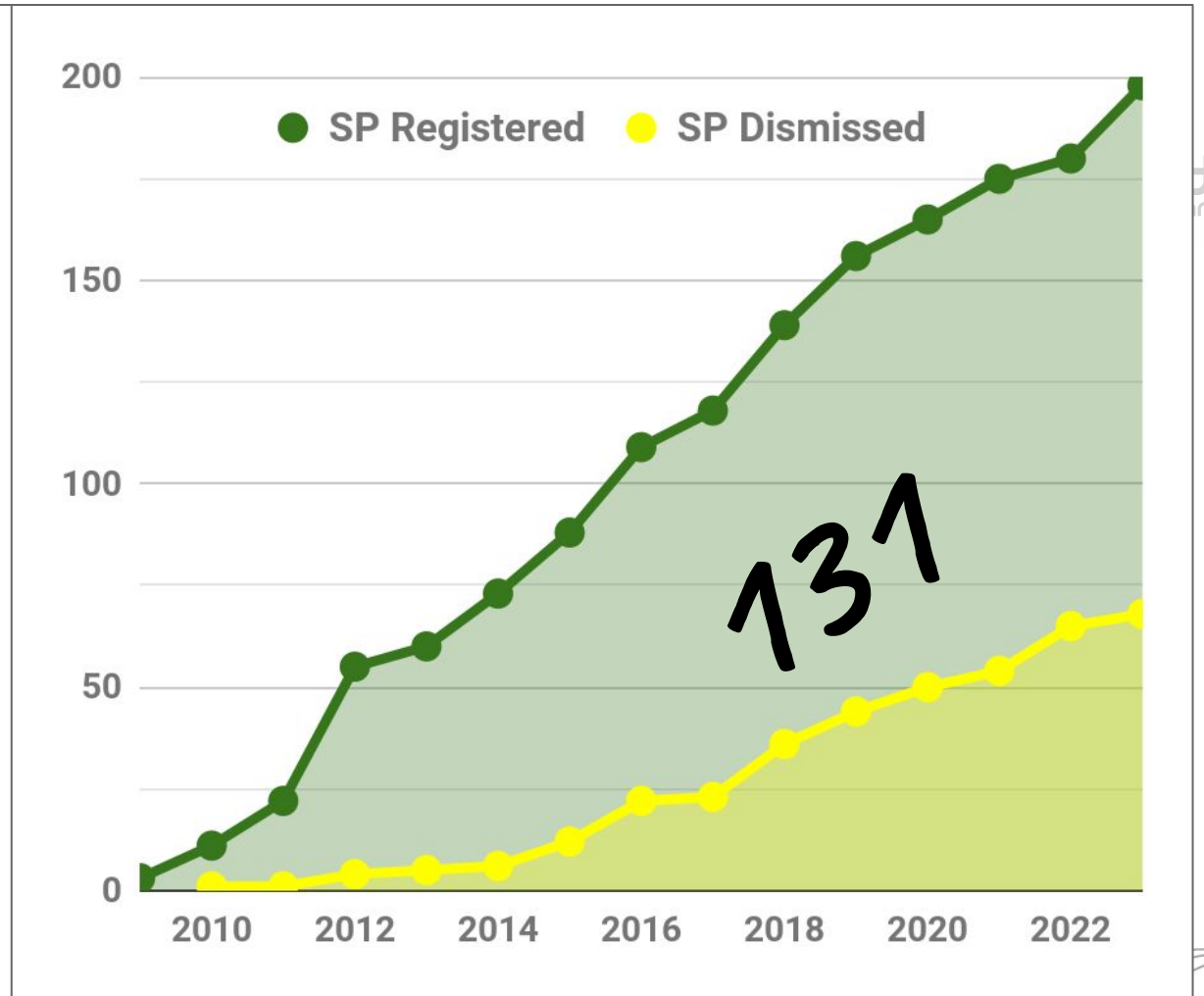
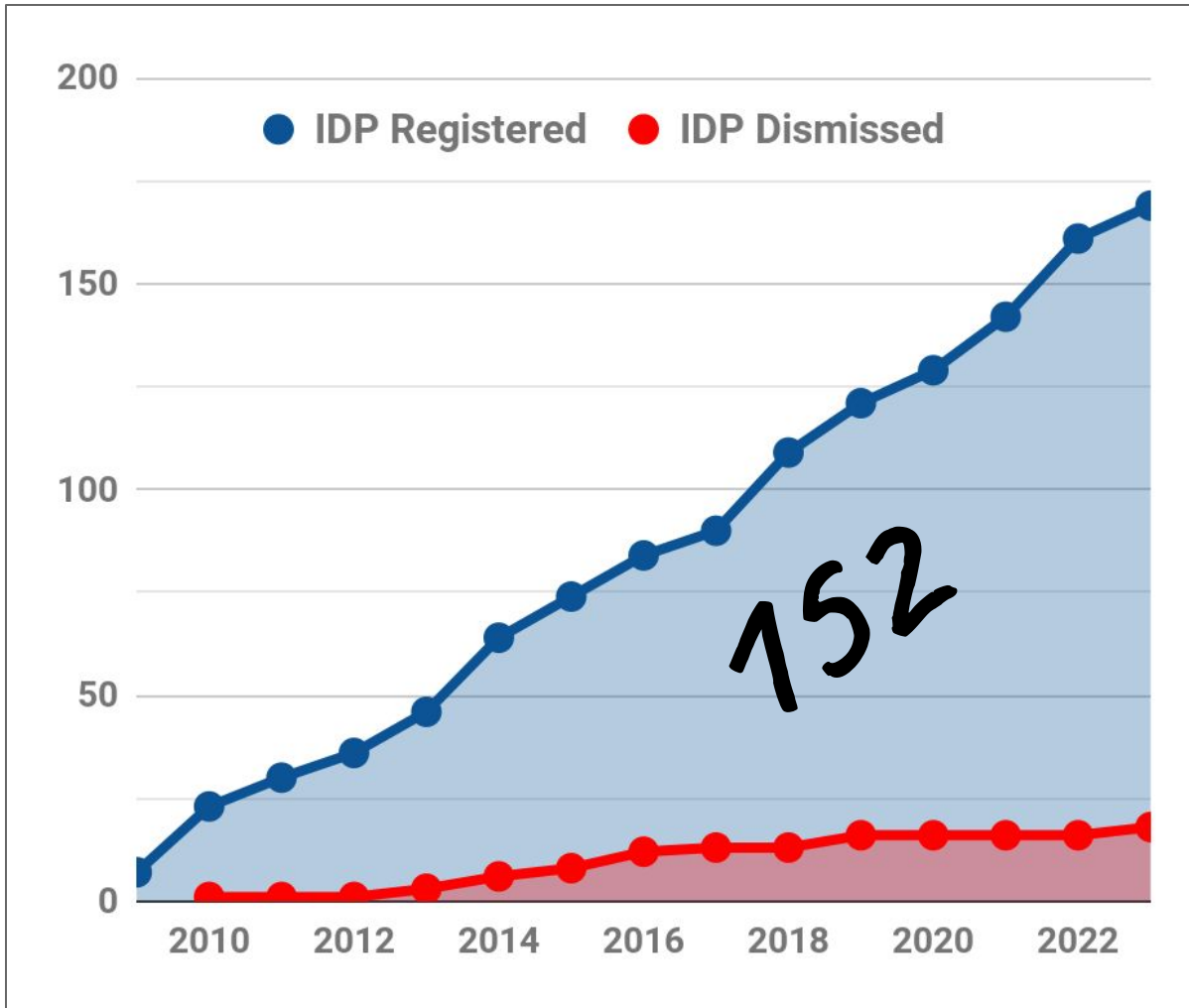
Membri

- Istituto Zooprofilattico Sperimentale della Sardegna
- Università degli Studi di Catanzaro "Magna Graecia"
- Università degli studi dell'Insubria e eduGAIN
- IRCCS Istituto di Candiolo - Fondazione del Piemonte per l'Oncologia
- IRCCS Fondazione G.B. Bietti
- ENEA
- Istituto Superiore di Studi Musicali "C.Monteverdi"
- IRCCS Ospedale Pediatrico del Bambin Gesù
- Università Vita-Salute San Raffaele
- Istituto Zooprofilattico Sperimentale delle Venezie (IZSVe)
- Università Campus Bio-Medico di Roma

Servizi

- Events GARR
- Egea
- Criterium
- INFN DARWIN Identity and Access Management Service
- AMS Identity and Access Management di INFN
- CTAO Identity and Access Management di INFN e eduGAIN
- International Lattice Data Grid (ILDG) di INFN

IDEM Identity Provider e Service Provider



eduGAIN Global Coverage



79 Federations

9109 Entities

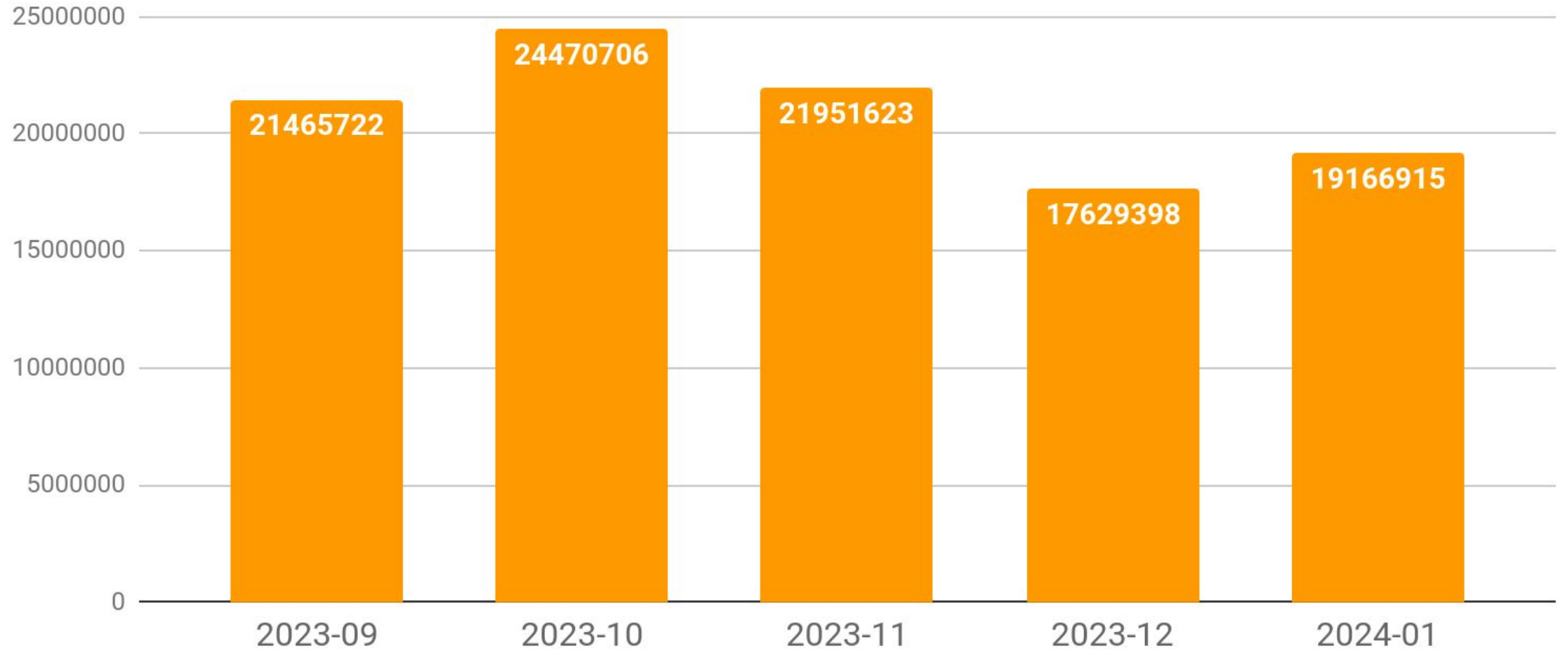
5554 Identity Providers

3637 Service Providers

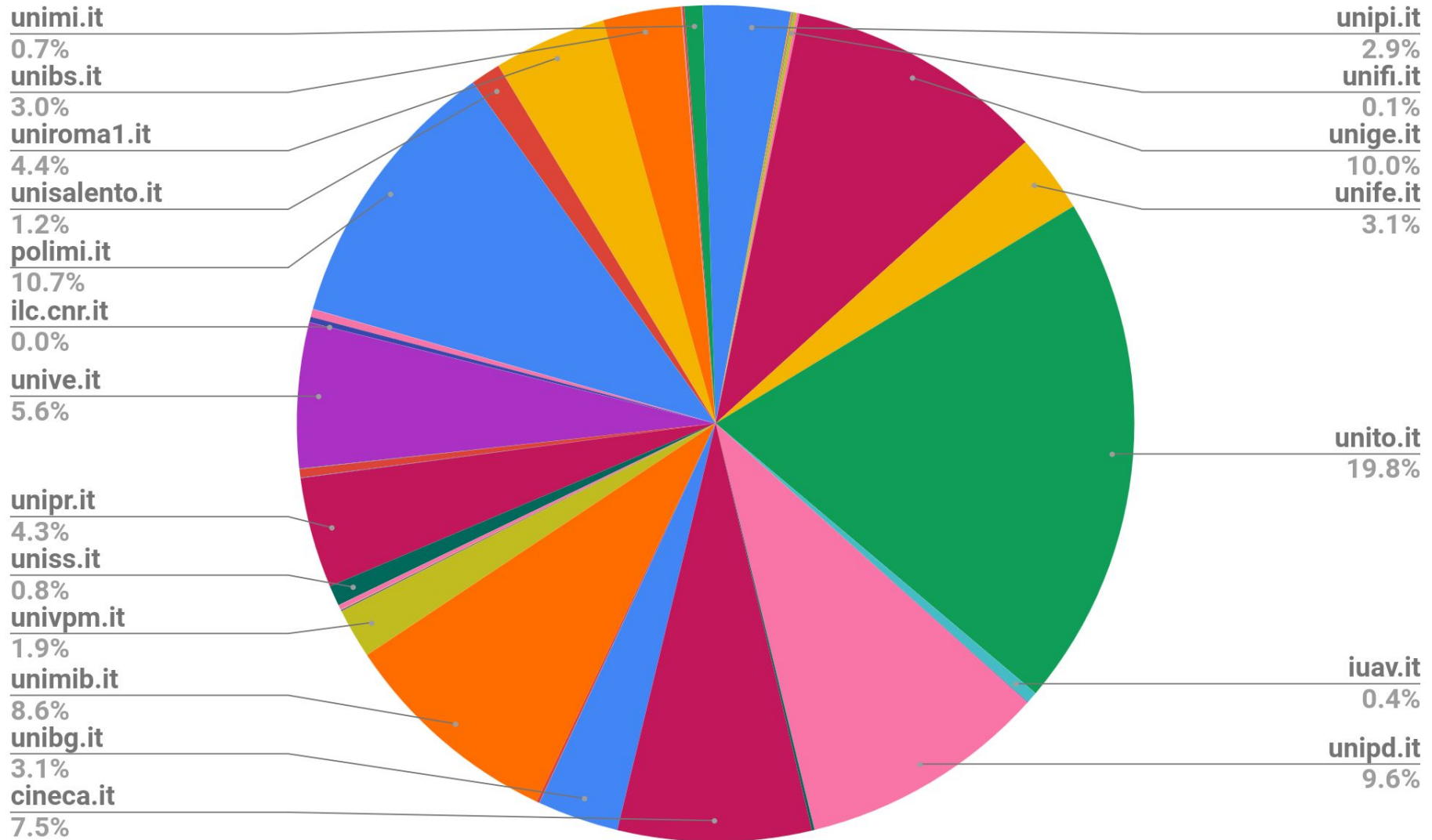
Statistiche

<i>Il campione</i>	
Organizzazioni Totali	75 (43 IdP in the Cloud)
Mesi considerati	da Settembre 2023 a Gennaio 2024

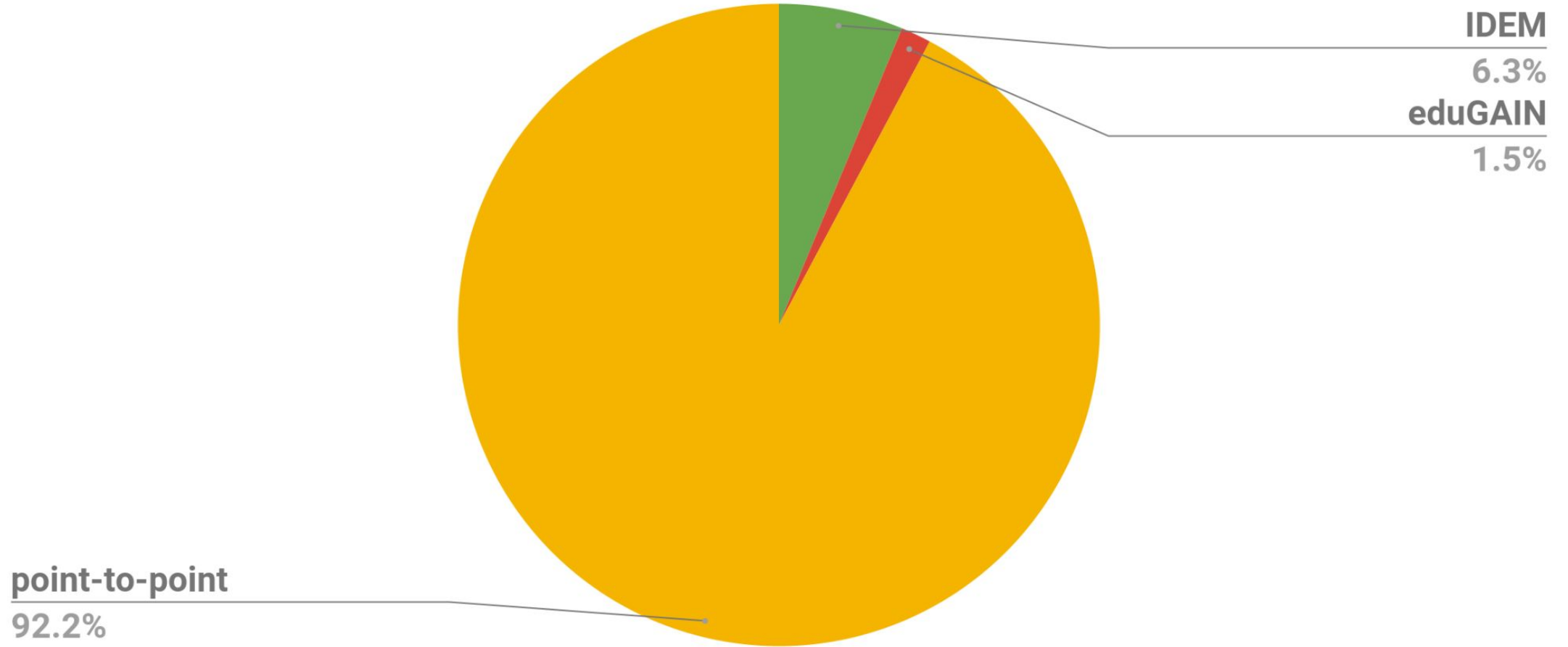
Login aggregati per mese



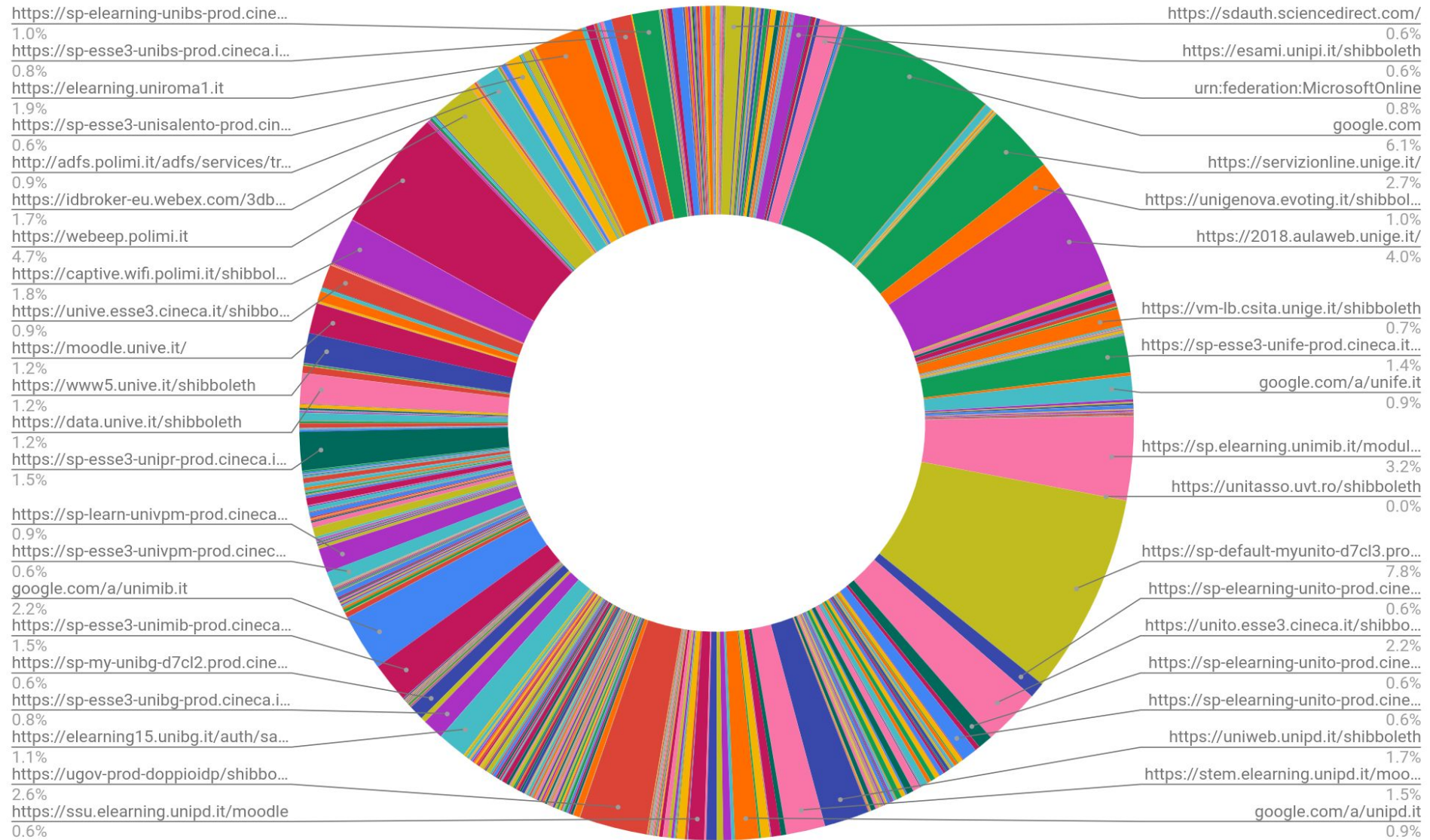
Login aggregati per organizzazioni



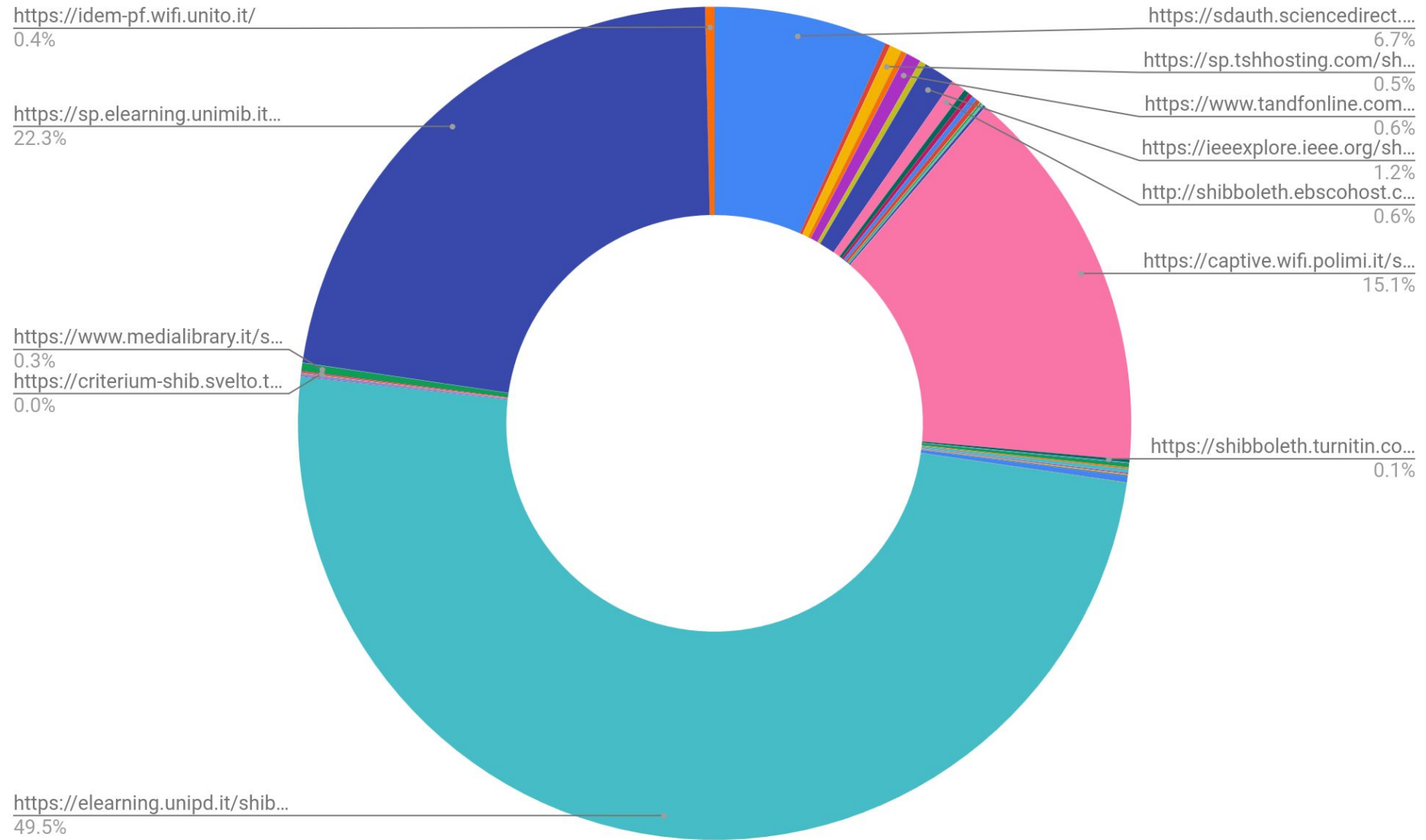
Login aggregati per provenienza delle risorse



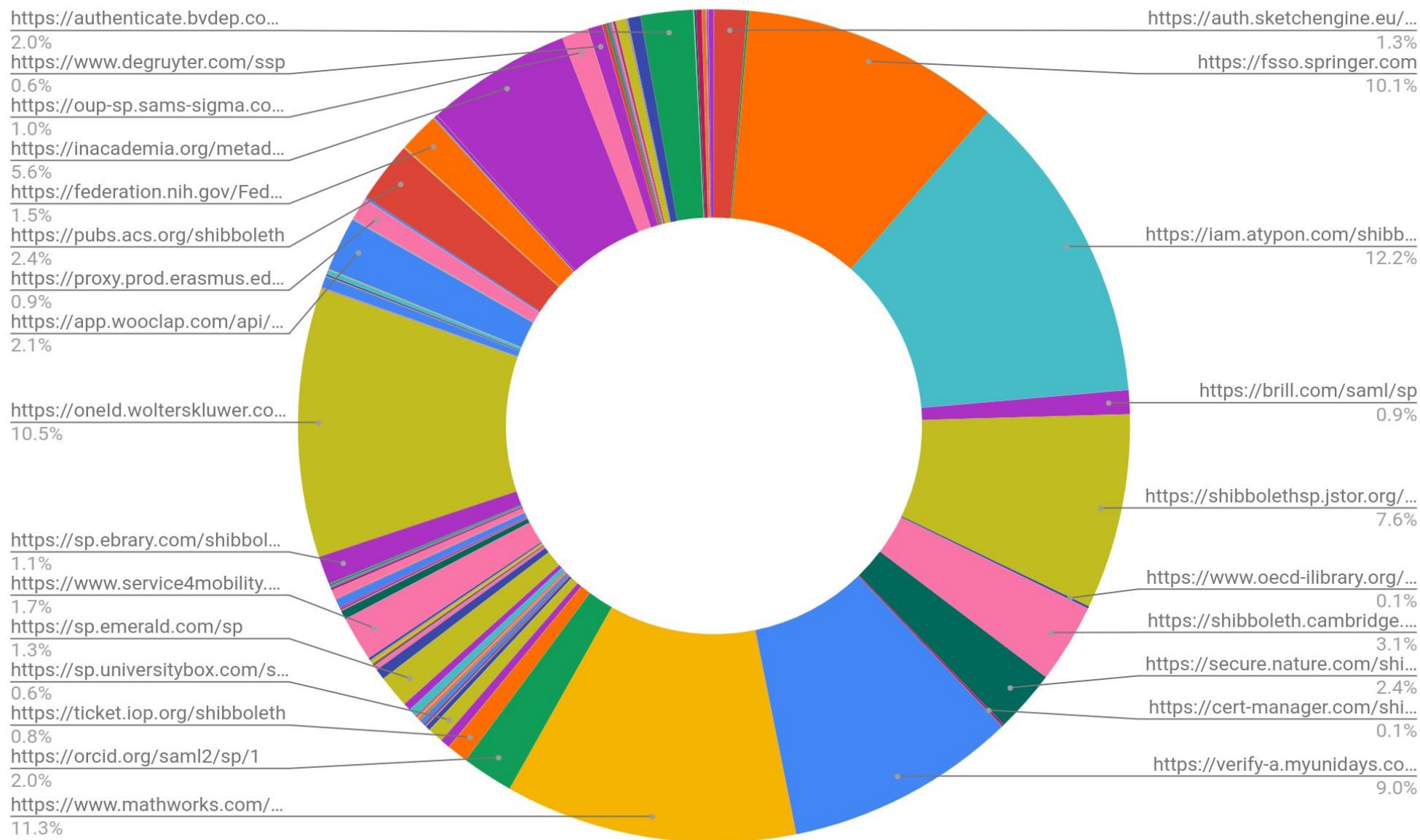
Login aggregati per risorse - Point to Point



Login aggregati per risorse - IDEM



Login aggregati per risorse - eduGAIN



Servizio IDEM GARR AAI Obiettivi e Progetti 2024

Formazione, ricerca e sviluppo

- Shibboleth IdP 5
 - OpenID Connect plugin
- Multi Factor Authentication
- Passwordless Authentication (WebAuthn/Passkey/Fido2)
- OpenID Federation

Supporto casi d'uso per la ricerca e l'istruzione

- Student Mobility
 - MyAcademicID
(<https://wiki.geant.org/display/SM/MyAcademicID+Identity+and+Access+Management+Service>)
 - European Student Identifier (<https://wiki.geant.org/display/SM/European+Student+Identifier>)
 - Guida IDEM: https://wiki.idem.garr.it/wiki/Erasmus_Plus_e_ESI
- HPC
 - MyAccessID (<https://wiki.geant.org/display/MyAccessID/MyAccessID+Home>)
 - LUMI EuroHPC
 - ICSC

Policy e standard

- Entity Attributes e Category
 - Storiche: Sirtfi/R&S/CoCo
 - Nuove: Anonymous Access, Pseudonymous Access, Personalized Access
- REFEDS MFA v1.2 (Strong/Passwordless Authentication)
- Profili di garanzia dell'identità digitale della Federazione IDEM
- REFEDS Identity Federation Baseline Expectations



THE ITALIAN
EDUCATION
& RESEARCH
NETWORK

Grazie

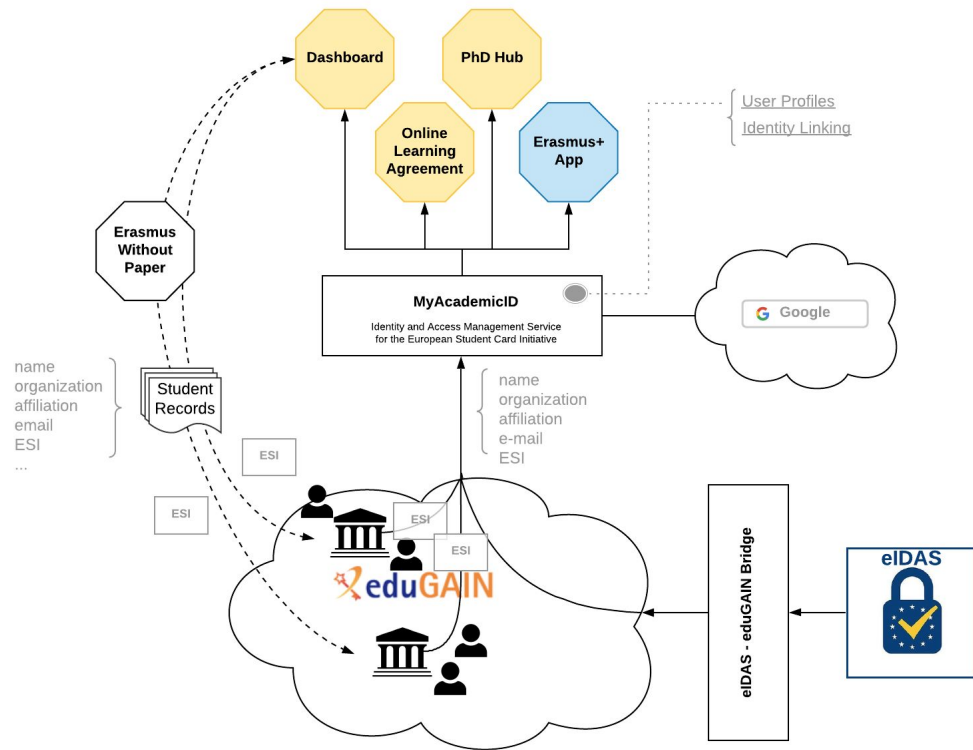
Daide Vagheti <davide.vagheti@garr.it>



BACKUP SLIDES

European Student Identifier

Guida del Servizio: [https://wiki.idem.garr.it/wiki/Erasmus Plus e ESI](https://wiki.idem.garr.it/wiki/Erasmus_Plus_e_ESI)



NEW

**Erasmus Without Paper
Administrator role**

Profili di garanzia IDEM: processo di adesione

1. Il membro IDEM compila l'autodichiarazione di conformità per il profilo richiesto.
2. Il Servizio verifica la correttezza formale ed effettua i controlli tecnici sull'identity provider (trasmette *assurance*? MFA?)
3. Su richiesta del CTS il Servizio effettua ulteriori controlli.
4. Il servizio pubblica il supporto del profilo nei metadata dell'IdP.
5. Ogni anno il membro IDEM deve rinnovare la dichiarazione di conformità.

Profili di garanzia IDEM: dichiarazione di conformità

INFORMAZIONI



Nome organizzazione
Nome del Referente Organizzativo
Data

DICHIARAZIONE

Conformità per ogni punto qualificante

AUTENTICITÀ

firma digitale del Referente Organizzativo

Dichiarazione di conformità per il profilo IDEM-P2

versione 1.0, 16 Agosto 2023

Tramite la presente dichiarazione di conformità l'organizzazione attesta il rispetto dei requisiti operativi indicati nella **sezione 4** del documento "Profili di garanzia delle identità digitali della Federazione IDEM" ([Profili di garanzia delle identità digitali della Federazione IDEM.pdf](#)) per il profilo IDEM-P2.



Per completare la dichiarazione è necessario spuntare per ogni elemento indicato qui sotto la relativa casella di controllo e far firmare digitalmente a cura del Referente Organizzativo.

La dichiarazione compilata e firmata deve essere trasmessa all'indirizzo idem-help@garr.it per approvazione e aggiornamento dei metadata.

Nome dell'Organizzazione: Inserire il nome dell'Organizzazione dichiarante
Nome e cognome del Referente Organizzativo: Inserire il nome e cognome del Referente Organizzativo
Data: Inserire la data di sottoscrizione

4. Requisiti operativi

	Casella di controllo
4.1. Organizzazioni L'organizzazione è conforme alla sezione 4.1	<input type="checkbox"/>
4.2. Identificatori L'organizzazione è conforme alla sezione 4.2.1 (Identificatori ammessi)	<input type="checkbox"/>
L'organizzazione è conforme alla sezione 4.2.2 (Persona fisica)	<input type="checkbox"/>
L'organizzazione è conforme alla sezione 4.2.3 (Contattabilità)	<input type="checkbox"/>
L'organizzazione è conforme alla sezione 4.2.4 (Riassegnazione)	<input type="checkbox"/>
4.3. Verifica dell'identità e gestione delle credenziali	
4.3.1 Registrazione e accreditamento L'organizzazione è conforme alla sezione 4.3.1	<input type="checkbox"/>

4.3.2. Controllo e verifica dell'identità
L'organizzazione è conforme alla sezione 4.3.2.3 (Profilo IDEM-P2)

4.3.3. Emissione, consegna e attivazione
L'organizzazione è conforme alla sezione 4.3.3.2 (Profili IDEM-P2 e IDEM-P3)

4.3.4. Sospensione, revoca e riattivazione
L'organizzazione è conforme alla sezione 4.3.4

4.3.5. Rinnovo e sostituzione
L'organizzazione è conforme alla sezione 4.3.5.1 (Profili IDEM-P0, IDEM-P1 e IDEM-P2)

4.4. Qualità degli attributi
L'organizzazione è conforme alla sezione 4.4.

4.5. Autenticazione

4.5.1. Ambito di applicazione
L'organizzazione è conforme alla sezione 4.5.1

4.5.2. Autenticazione a singolo fattore
L'organizzazione è conforme alla sezione 4.5.2

4.5.3. Autenticazione a più fattori
L'organizzazione è conforme alla sezione 4.5.3

Firma digitale del Referente Organizzativo

REFEDS Identity Federation Baseline Expectations

common set of expectations of all participant organisations to establish a baseline of trust in identity federations

REFEDS Baseline Expectations of Identity Provider Operators [IPO]

- [IPO1] Your Identity Provider is operated with organizational-level authority
- [IPO2] Your Identity Provider is trusted enough to be used to access your organization's own systems
- [IPO3] You publish contact information for your Identity Provider and respond in a timely fashion to operational issues
- [IPO4] You apply security practices to protect user information, safeguard transaction integrity, and ensure timely incident response
- [IPO5] You ensure the metadata registered in Federation is complete, accurate and up to date

REFEDS Baseline Expectations of Service Provider Operators [SPO]

- [SPO1] You ensure that controls are in place to protect user privacy in the service
- [SPO2] You do not share information received from Identity Providers with third parties without relevant notification and the information is stored only whilst necessary for operational purposes
- [SPO3] You publish contact information and respond in a timely fashion to operational issues
- [SPO4] You apply security practices to protect user information, safeguard transaction integrity, and ensure timely incident response
- [SPO5] You ensure the metadata registered in Federation is complete, accurate and up to date
- [SPO6] You publish requirements for any user information required to access your service and ensure these requirements are appropriate and respect privacy

REFEDS Baseline Expectations of Federation and Interfederation Operators [FO]

- [FO1] You focus on trustworthiness of Federation as a primary objective and are transparent about such efforts
- [FO2] You publish contact information and respond in a timely fashion to operational issues
- [FO3] You apply security practices to federation operations and ensure timely incident response
- [FO4] You follow good practices to ensure authentic, accurate and interoperable metadata to enable secure and trustworthy federated transactions
- [FO5] You implement and support frameworks that improve trustworthy and scalable use of Federation and promote their adoption by members and other participants
- [FO6] You collaborate with other organisations to promote realization of baseline expectations nationally and internationally