

Sirtfi: un nome complicato per la gestione degli incidenti di sicurezza in ambito federato

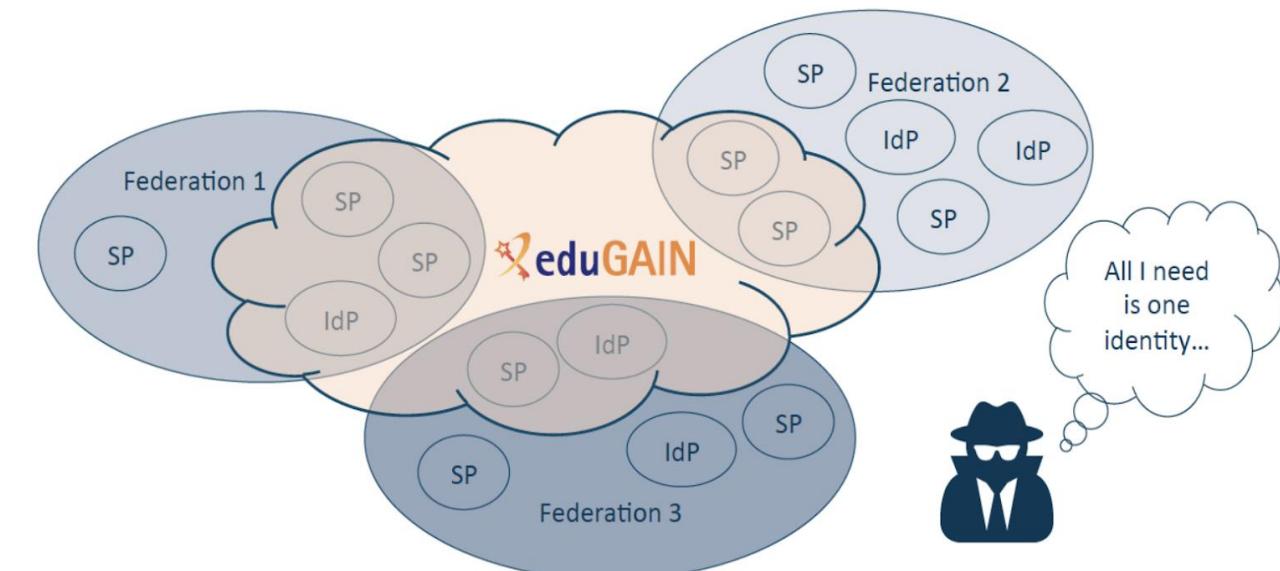
Barbara Monticini
GARR



**NET
MAKERS**

Gli incidenti di sicurezza in ambito federato

- eduGAIN rappresenta un'ampia superficie di attacco
- Mancanza di un CSIRT centralizzato
- Tutti i partecipanti devono collaborare per gestire gli incidenti di sicurezza
- Il caso SHEER ID



A Security Incident Response Trust Framework for Federated Identity

- [Sirtfi-1.0.pdf](#)
 - *This document identifies practices and attributes of organizations that may facilitate their participation in a trust framework called Sirtfi purposed to **enable coordination of security incident response across federated organizations.***
- <https://refeds.org/sirtfi>
 - Sito web ufficiale
- <https://wiki.idem.garr.it/wiki/EntityAttribute-Category>
 - Wiki IDEM con workflow operativo di adesione al framework

Sezioni del framework REFEDS Sirtfi

Operation security

*information resources ...
availability and integrity ...
confidentiality of sensitive information*

Traceability

*be able to answer the basic questions
"who, what, where, and when"
concerning a security incident*

Incident Response (*)

*a security incident response capability
exists within the organization*

Participant Responsibilities

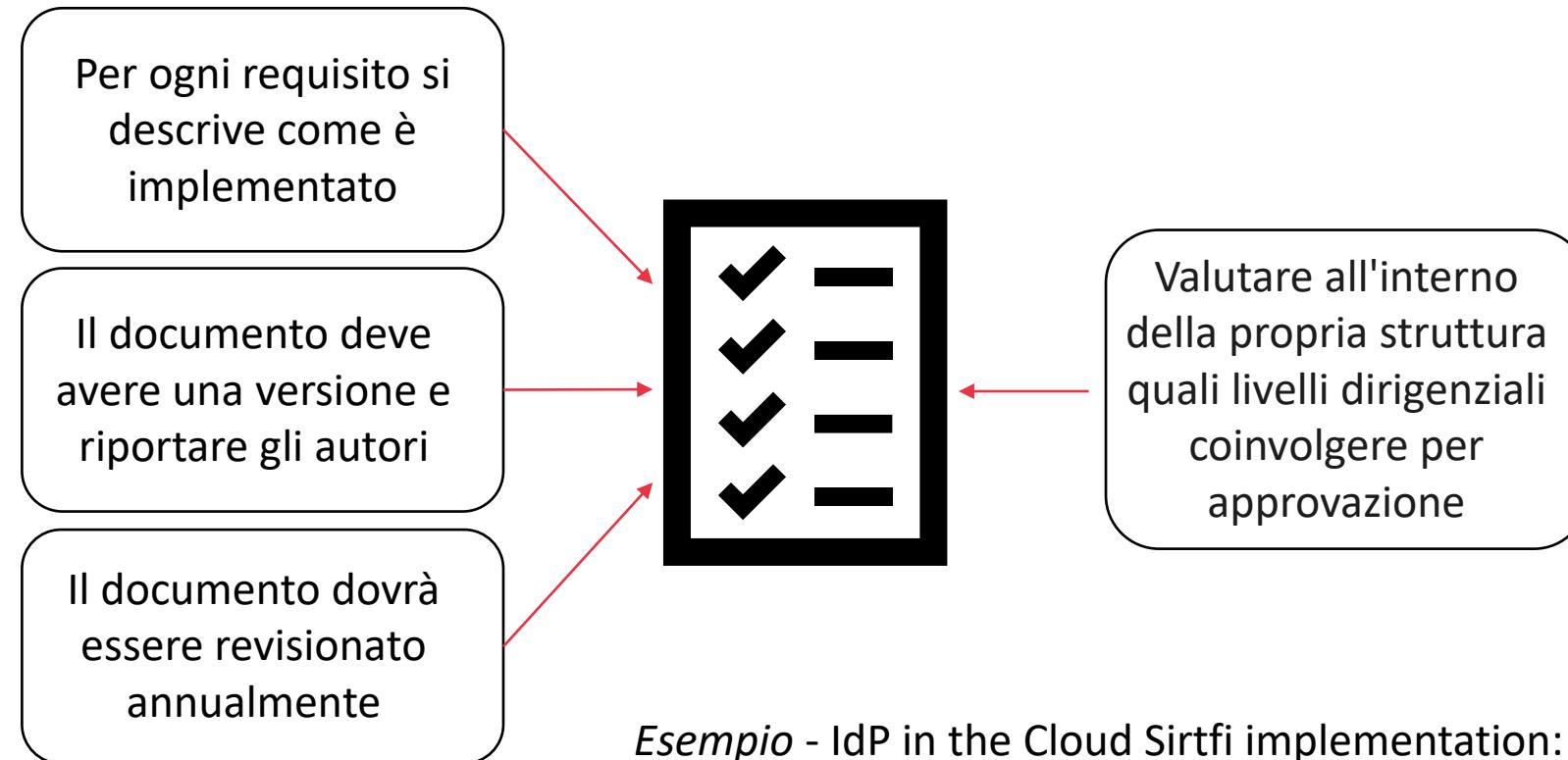
*All participants (IdPs and SPs) in the
federations need to rely on appropriate
behavior.*

(*) uso di TLP nelle comunicazioni relative agli incidenti di sicurezza e presenza di un security incident response contact

Sirtfi @ IDEM

- Security contact per ogni entità:
 - A meno che non sia disponibile un *incident response security contact* presso l'Istituzione, **GARR-CERT** è il contatto Sirtfi designato da IDEM per la gestione degli incidenti di sicurezza in ambito federato
- La base per l'adesione a Sirtfi è un'**autovalutazione** fondata su tutti i requisiti indicati dal framework
- Istruzioni operative nel **wiki** di IDEM (tramite **Metadata Registry**)
- **Corso di formazione** IDEM Sirtfi (17 novembre 2021)

Autovalutazione Sirtfi



Sirtfi: i numeri nella Federazione IDEM

SIRTFI present The Higher The Better

This federation: 9.76%(eduGAIN avg: 29%)

16  148

- Solo 16 entità su 148 in IDEM hanno aderito a Sirtfi
- In percentuale è il **9.76%** delle entità totali
- La media delle altre Federazioni in eduGAIN è del **29%**
- E' così grave?



Il futuro di eduGAIN e il peso di Sirtfi



REFEDS
Baseline
Expectations

This document defines a common set of expectations of all participant organisations to establish a **baseline of trust in identity federations**.

To **review the REFEDS Baseline Expectations document** and **make proposals for changes to eduGAIN to support the baseline.**

Need to enforce standards like **CoCo, R&S, Sirtfi** more

Starting from **April 2022**: implementation of changes within eduGAIN

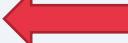
Servizi accessibili solo con Sirtfi già oggi

CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

Sign in with your organization or institution account

 Enter the name of the organisation you are affiliated with...

Why is my organisation not listed?   La HO non è nella lista

The Security Incident Response Trust Framework for Federated Identity

You need Sirtfi to access CERN! Look for your home organisation below and click to email them a request.

Your home organisation must comply with security best practices in order for you to have access to certain research services. Want more information? Visit the [Sirtfi Homepage](#).



Servizi accessibili solo con Sirtfi già oggi

The screenshot shows the Globus Web App login interface. At the top, there's a blue header bar with the Globus logo (a white 'g' inside a white cloud) and the word "globus". Below the header, the text "Log in to use Globus Web App" is displayed. A horizontal line separates this from the next section. The text "Use your existing organizational login" is followed by the placeholder "e.g., university, national lab, facility, project". A dropdown menu is open, showing "GARR - Direzione" with a downward arrow icon. Below the dropdown is a blue "Continue" button. To the left of the "Continue" button is a green CILogon logo (two arrows forming a circle). To the right of the logo is a text box containing the following text: "Globus uses CILogon to enable you to Log In from this organization. By clicking Continue, you agree to the [CILogon privacy policy](#) and you agree to share your username, email address, and affiliation with CILogon and Globus. You also agree for CILogon to issue a certificate that allows Globus to act on your behalf." The entire interface is set against a background with various small, semi-transparent icons related to technology and data.

Log in to use Globus Web App

Use your existing organizational login
e.g., university, national lab, facility, project

GARR - Direzione

Continue

 Globus uses CILogon to enable you to Log In from this organization. By clicking Continue, you agree to the [CILogon privacy policy](#) and you agree to share your username, email address, and affiliation with CILogon and Globus. You also agree for CILogon to issue a certificate that allows Globus to act on your behalf.

Servizi accessibili solo con Sirtfi già oggi

CILogon Supports Sirtfi

Post date: Apr 17, 2017 8:34:53 PM

CILogon now officially supports the Security Incident Response Trust Framework for Federated Identity ([Sirtfi](#)). As part of InCommon's Sirtfi Proof of Concept (see: [FAQ](#)), [InCommon](#) tagged [CILogon](#) as Sirtfi-compliant in [federation metadata](#). Hosted by NCSA at the University of Illinois, CILogon benefits from the operational security and incident response capabilities of [NCSA Cybersecurity](#). CILogon's compliance with [Interoperable Global Trust Federation](#) standards helped to prepare for meeting the Sirtfi standards. As a Sirtfi-compliant service provider, CILogon checks for a corresponding tag of [Sirtfi-compliance in metadata for identity providers](#). Visit the [eduGAIN Entities Database](#) to see if your identity provider supports Sirtfi. If it does, CILogon thanks you! If not, please don't delay! As always, contact help@cilogon.org for assistance.

Servizi accessibili solo con Sirtfi già oggi



Test Your Identity Provider

To test that your identity provider works with CILogon, please select it from the list below and Log On.

Select an Identity Provider

GARR ▾ ?

Log On

By selecting "Log On", you agree to [CILogon's privacy policy](#).

Servizi accessibili solo con Sirtfi già oggi

Verify Attribute Release ▼

Thank you for your interest in the CILogon Service. This page enables you to verify that all necessary attributes have been released to the CILogon Service Provider (SP) by your selected Identity Provider (IdP). Below you will see the various attributes required by the CILogon Service and their values as released by your IdP.

 All required attributes have been released by your IdP. For details of the various attributes utilized by the CILogon Service and their current values, see the sections below.

[Proceed to the CILogon Service](#) [Logout](#)

Sirtfi nelle altre federazioni

The screenshot shows the InCommon website. The top navigation bar includes links for SOLUTIONS, HELP, ABOUT, and NEWS. Below this is a secondary navigation bar with links for FEDERATION, EDUROAM, CERTIFICATES, SOFTWARE, ACADEMY, and COMMUNITY. The FEDERATION link is highlighted. The main content area features a news article titled "Baseline Expectations 2 Take Effect" dated Nov. 06, 2020. The article discusses what is changing in BE2 and lists three requirements for Identity Providers and Service Providers.

06
Nov.
2020

FEDERATION

Community

Baseline Expectations 2 Take Effect

What is changing in Baseline Expectations 2?

BE2 adds 3 additional elements to Baseline Expectations:

- All Identity Providers (IdP) and Service Providers (SP) service endpoints must be secured with current and community-trusted transport layer encryption
- All entities (IdP and SP) meet the requirements of the SIRTFI v1.0 trust framework when handling security incidents involving federation participants
- All IdP metadata must include an errorURL; if the condition is appropriate, SPs should use the IdP-supplied errorURL to direct the user to proper support.

Visit the [Baseline Expectation wiki home page](#) to see the changes in Baseline Expectations 2.

Riferimenti

- REFEDS Sirtfi: <https://refeds.org/sirtfi>
- REFEDS Baseline Expectations: <https://refeds.org/baseline-expectations>
- eduGAIN Futures Working Group:
<https://wiki.geant.org/display/eduGAIN/eduGAIN+Futures+Working+Group+Charter>
- IDEM wiki: <https://wiki.idem.garr.it/wiki/EntityAttribute-Category>
- Autovalutazione Sirtfi «GARR Idp in the Cloud»:
https://wiki.idem.garr.it/w/images/0/0b/Sirtfi_IdP_in_the_Cloud_v1.0.pdf