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

Barbara Monticini

GARR

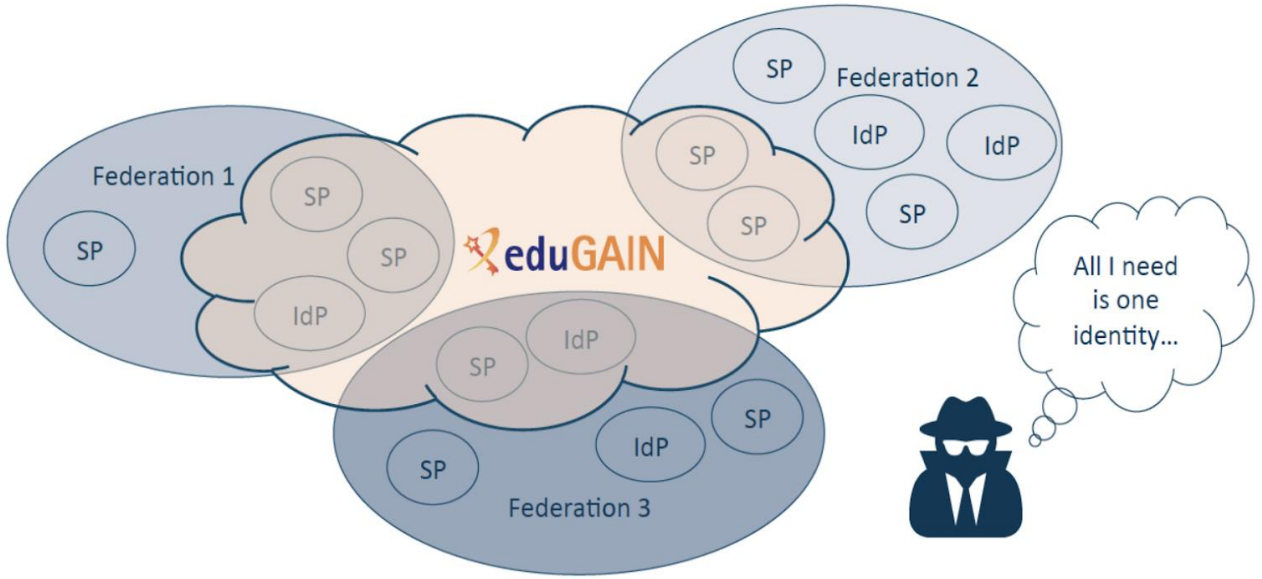
WORKSHOP GARR 2021

NET MAKERS

Consortium GARR

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

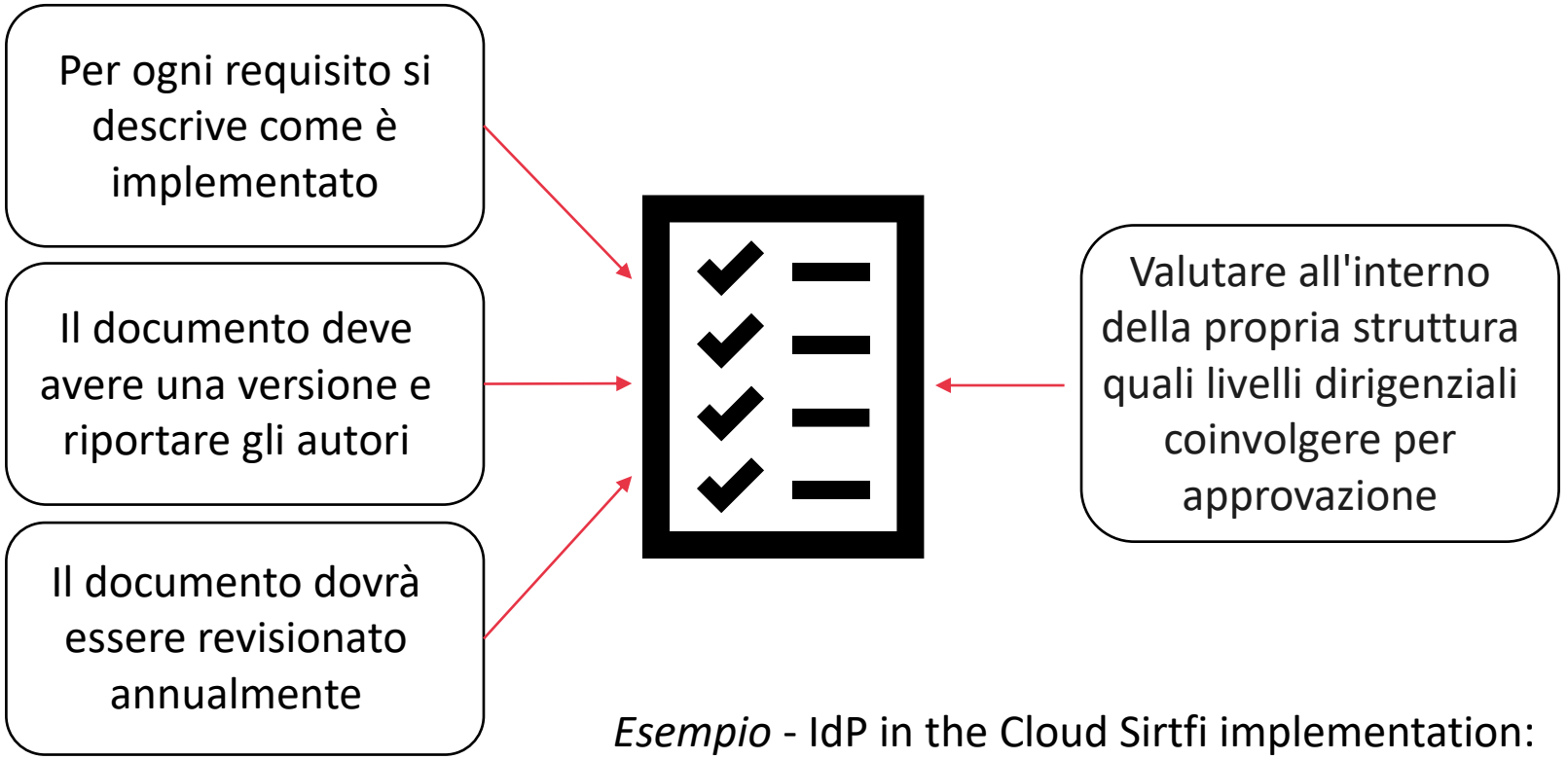
All participants (IdPs and SPs) in the federations need to rely on appropriate behavior.

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

Sirtfi @ IDEM

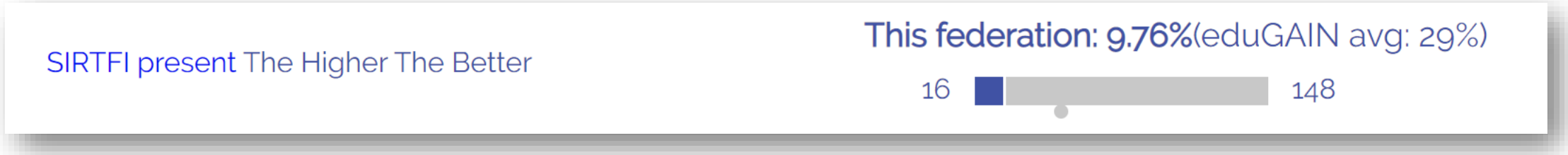
- Security contact per ogni entità:
  - A meno che non sia disponibile un *incident response security contact* presso l'Istituzione, **GARR-CERT** è il contatto Sirtfi designato da IDEM per la gestione degli incidenti di sicurezza in ambito federato
- La base per l'adesione a Sirtfi è un'**autovalutazione** 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



Esempio - IdP in the Cloud Sirtfi implementation:
https://wiki.idem.garr.it/w/images/0/0b/Sirtfi_IdP_in_the_Cloud_v1.0.pdf

Sirtfi: i numeri nella Federazione IDEM



- 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

EduGAIN Futures Working Group

eduGAIN 2.0

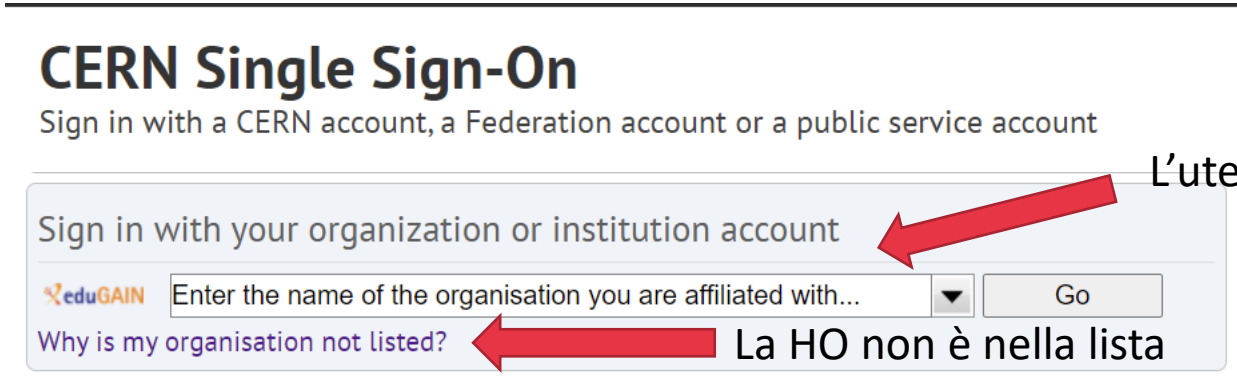
This document defines a common set of expectations of all participant organisations to establish a **baseline of trust in identity federations**.

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

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

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

Servizi accessibili solo con Sirtfi già oggi



L'utente cerca la propria HO

La HO non è nella lista

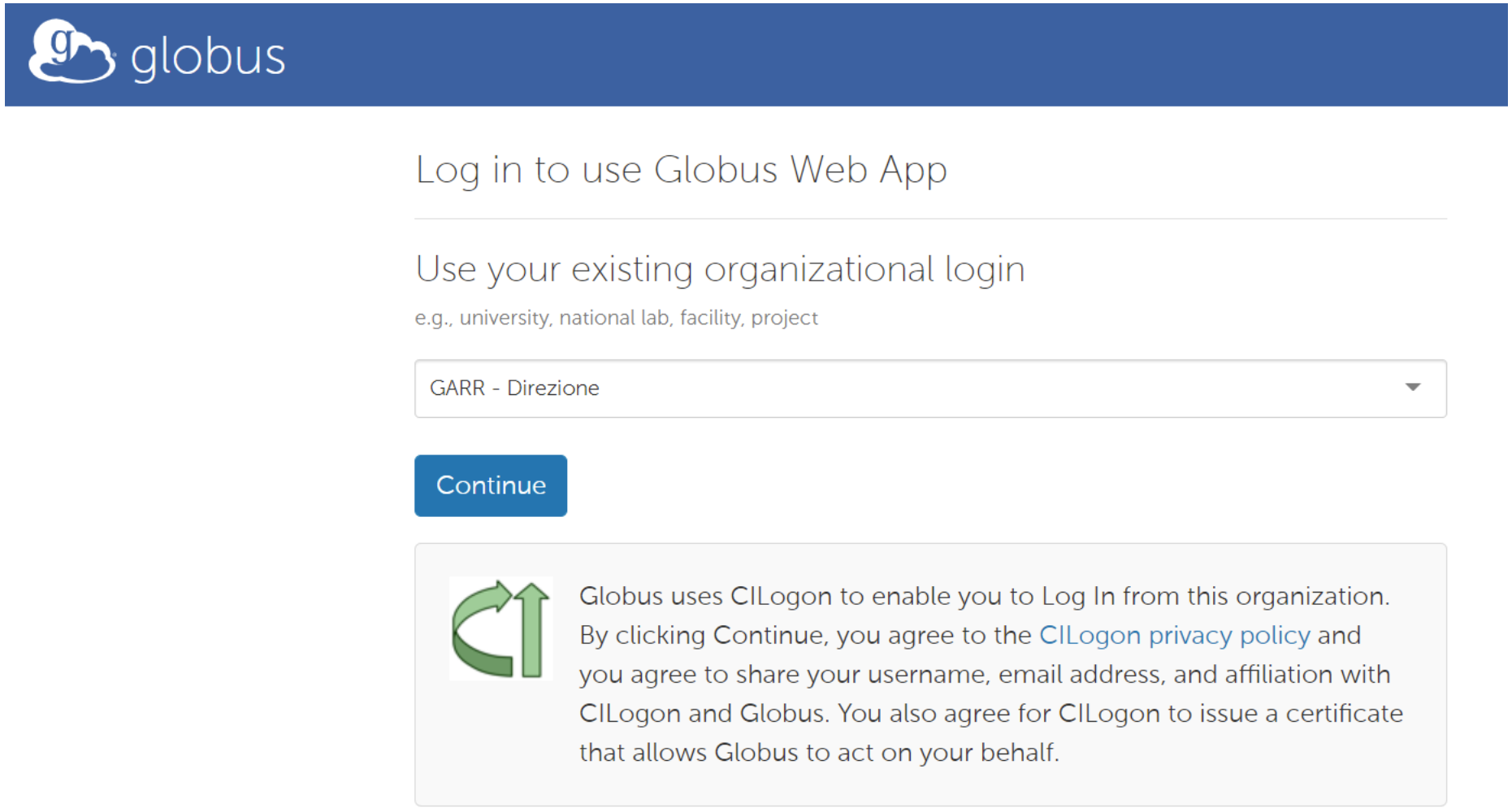
The Security Incident Response Trust Framework for Federated Identity

SIRTFI

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



Servizi accessibili solo con Sirtfi già oggi

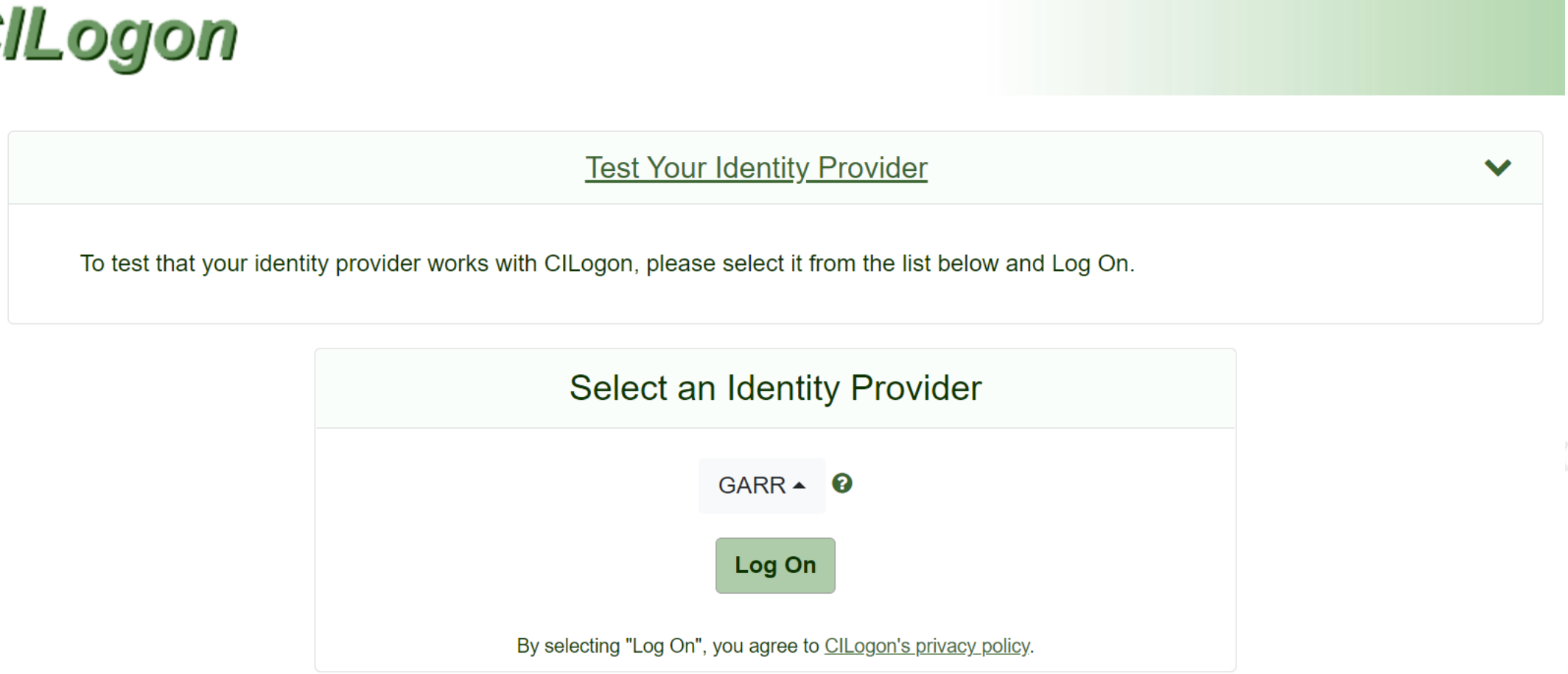
CILogon Supports Sirtfi

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

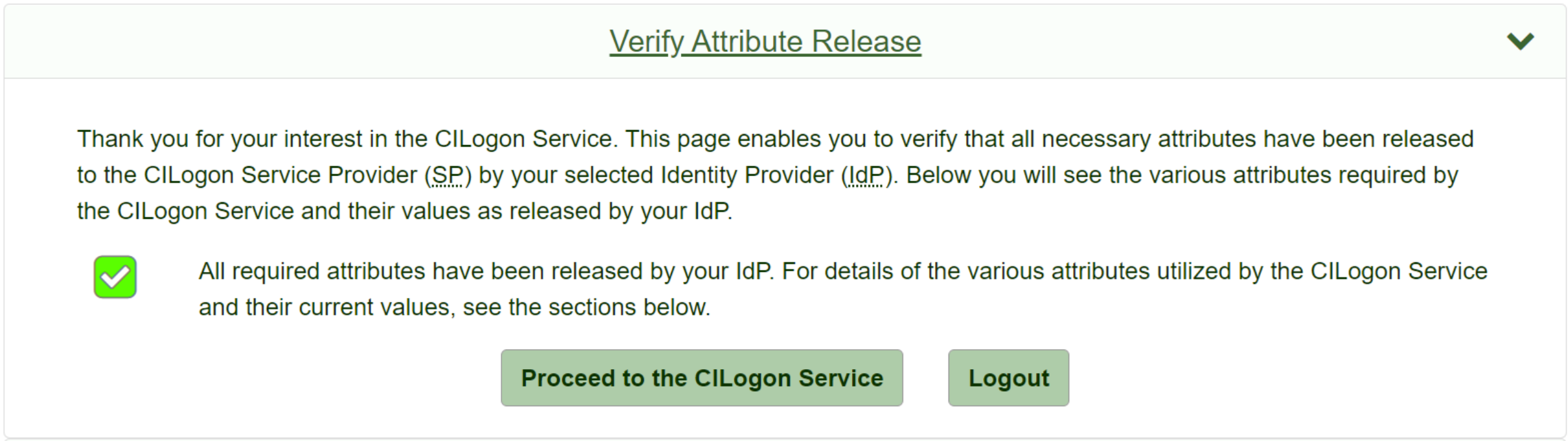
CILogon now officially supports the Security Incident Response Trust Framework for Federated Identity (Sirtfi). As part of InCommon's Sirtfi Proof of Concept (see: FAQ), InCommon tagged CILogon as Sirtfi-compliant in federation metadata. Hosted by NCSA at the University of Illinois, CILogon benefits 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

CILogon



Servizi accessibili solo con Sirtfi già oggi



Sirtfi nelle altre federazioni

FEDERATION Community

06 Nov. 2020

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