



Educação, Pesquisa
e Inovação em Rede

RISC e Sirtfi em identidade federada

CT-GId

Shirlei Chaves

05/2025

<https://listas.rnp.br/mailman/listinfo/ct-gid>

Agenda

- 1 Visão Geral
- 2 Sirtfi
- 3 Shared Signals Framework
- 4 Considerações Finais



Visão Geral

Federação acadêmica

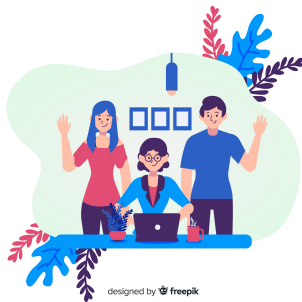
Baseada em confiança



- Provedores de Identidade (IdPs) e Provedores de Serviço (SPs) **confiam** no administrador da federação;
- SPs **confiam** que IdPs possuem uma base de usuários atualizada e que realizam corretamente o processo de autenticação de seus usuários;
- IdPs **confiam** que os SPs não irão abusar dos atributos obtidos de seus usuários.

Federação acadêmica

Resposta a incidente de segurança



- Incidentes de abrangência **interna** ao SP/IdP:
 - Resposta ao incidente tratado internamente pela equipe responsável.



Federação acadêmica

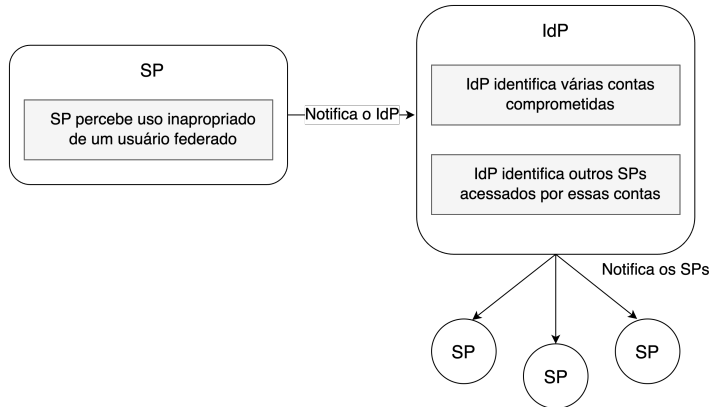
Resposta a incidente de segurança

- Incidentes de abrangência **externa** ao SP/IdP:
 - Qual o procedimento de resposta ao incidente?

Federação acadêmica

Resposta a incidente de segurança

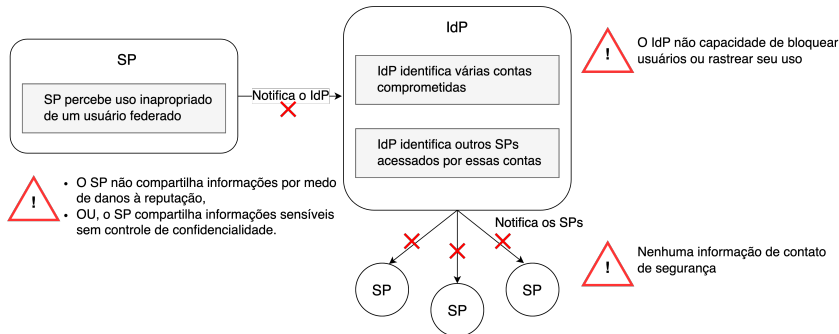
- Incidentes de abrangência **externa** ao SP/IdP:
 - Expectativa¹



Federação acadêmica

Resposta a incidente de segurança

- Incidentes de abrangência **externa** ao SP/IdP:
 - Realidade¹



¹ Figura adaptada de REFEDS - Introduction to Sirtfi



Sirtfi



- Objetivo: possibilitar uma **resposta a incidentes** de forma **coordenada**, na qual os **participantes** estejam **dispostos a colaborar** num incidente e **notificar terceiros** quando perceberem que o incidente impacta terceiros.

²<https://refeds.org/sirtfi>

- Controle de confidencialidade das informações³:

TLP:RED

TLP:AMBER+STRICT

TLP:AMBER

TLP:GREEN

TLP:CLEAR

- Marcações podem ser utilizadas em comunicações diversas, como e-mails, documentos, apresentações, chat e em trocas automatizadas de informações.

³ Traffic Light Protocol (TLP) - Centro Integrado de Segurança Cibernética do Governo Digital

- As entidades **autoatestam**⁴ a conformidade com o Sirtfi, adicionando elemento ao arquivo de metadados:

```
<ContactPerson xmlns:remd="http://refeds.org/metadata"
  contactType="other"
  remd:contactType="http://refeds.org/metadata/
    contactType/security">
  <GivenName>Security Response Team</GivenName>
  <EmailAddress>mailto:security@xxxxxxxxxxxxxx</
    EmailAddress>
</ContactPerson>
```

```
<md:Extensions>
  <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:
    names:tc:SAML:metadata:attribute">
    <saml:Attribute xmlns:saml="urn:oasis:names:tc:
      SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:
        attrname-format:uri"
        Name="urn:oasis:names:tc:SAML:attribute:
        assurance-certification">
      <saml:AttributeValue>https://refeds.org/sirtfi
    </saml:AttributeValue>
      <saml:AttributeValue>https://refeds.org/
        sirtfi2</saml:AttributeValue>
    </saml:Attribute>
  </mdattr:EntityAttributes>
</md:Extensions>
```

⁴O framework Sirtfi fornece um conjunto de afirmações, as quais a entidade autoatesta estar em conformidade.

- Obrigatório em algumas comunidades internacionais de e-Ciência, como a FIM4R (*Federated Identity Management For Research - FIM4R*)⁵:
 - Requisito para IdPs, Federações e eduGain, e proxies de comunidades de pesquisa:

Nota

Para ser aceitável pelas comunidades de pesquisa, um IdP deve atender aos requisitos do Sirtfi e afirmar isso nos metadados^a.

^a Federated Identity Management for Research Collaborations - 4.2 Requirement Matrix

- Dificuldades:
 - **Manual** - email, ligação, grupos de mensagens, etc.
 - **Demorado** - não é em tempo real e não há garantias que todos os interessados sejam informados de maneira rápida.
 - **Governança, não automatização** - ajuda a encontrar contatos, mas não automatiza o compartilhamento de eventos.

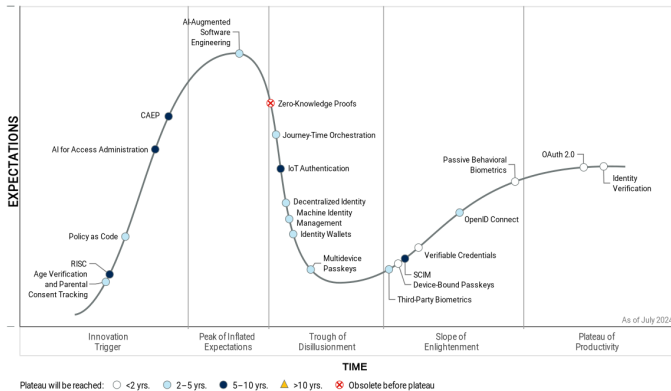


Shared Signals Framework

Gartner Hype Cycle™ para Identidade Digital 2024

RISC - Automatização do compartilhamento de informações sobre riscos e incidentes

Hype Cycle for Digital Identity, 2024



Gartner

Figura: Gartner Hype Cycle para Identidade Digital 2024⁶

⁶ <https://www.yubico.com/resource/2024-gartner-hype-cycle-for-digital-identity/>

Shared Signals Framework (SSF)

Building blocks

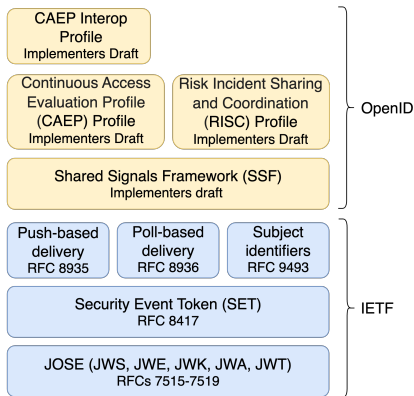


Figura: Pilha de protocolos framework SSF ^a

- Padrão em desenvolvimento pela OpenID Foundation^a.
- Compartilhamento (automatizado) de **eventos de segurança** entre organizações, relacionados aos seus usuários.
- Perfis para representação de dados:
 - CAEP: monitoramento e avaliação de acesso contínuos^b;
 - RISC: foco em mitigação de riscos e incidentes de segurança^c.

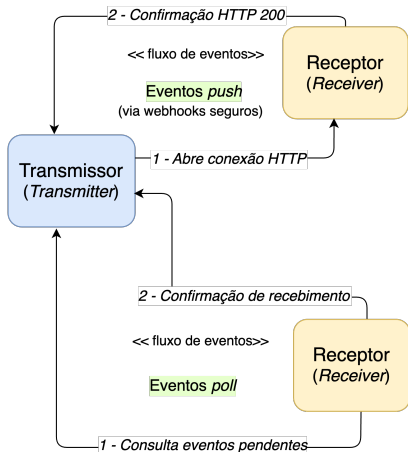
^aShared Signals Working Group - Overview

^bOpenID Continuous Access Evaluation Profile 1.0 - draft 03

^cOpenID RISC Profile Specification 1.0 - draft 02

Shared Signals Framework (SSF)

Building blocks



- Fluxo (*stream*) de eventos - canal de comunicação:
 - *Endpoints* do transmissor e do receptor;
 - Informações de autenticação;
 - Eventos suportados;
 - Configuração dos tipos de entrega (push/poll).
- Transmissor: gera e emite o evento de segurança (um IdP, por exemplo);
- Receptor: consumidor do evento, por exemplo, um SP.

Perfis RISC e CAEP

Eventos

Evento RISC	Descrição
<i>Account Credential Change Required</i>	A conta precisou trocar uma credencial (senha, por exemplo).
<i>Account Purged</i>	A conta foi excluída permanentemente.
<i>Account Disabled</i>	Conta desativada, o motivo pode ser informado em atributo do evento.
<i>Account Enabled</i>	Conta ativada.
<i>Identifier Changed</i>	O identificador (email ou telefone) foi alterado. De emissão apenas pelo provedor com autoridade sobre o identificador.
<i>Identifier Recycled</i>	O identificador foi reciclado e pertence agora a um novo usuário.
<i>Credential Compromise</i>	A credencial foi comprometida.
<i>Opt out</i>	Usuário opta por não haver emissão de eventos pra sua conta.
<i>Opt in</i>	Sinaliza emissão de eventos para a conta.
<i>Opt Out Initiated</i>	Sinaliza que o processo de opt out foi iniciado.
<i>Opt Out Cancelled</i>	Sinaliza que o processo de opt out foi cancelado.
<i>Opt Out Effective</i>	Opt out foi efetivado.
<i>Recovery Activated</i>	A conta ativou um fluxo de recuperação.
<i>Recovery Information Changed</i>	Alguma informação de recuperação da conta foi alterada.
<i>Session Revoked</i>	A sessão da conta foi revogada ^a .

Evento CAEP	Descrição
<i>Session Revoked</i>	O transmissor revogou a sessão.
<i>Token Claims Change</i>	O transmissor forneceu novos valores para declarações de tokens previamente enviados.
<i>Credential Change</i>	O transmissor tem uma nova credencial para o sujeito.
<i>Assurance Level Change</i>	O transmissor tem um novo nível de garantia para o sujeito.
<i>Device Compliance Change</i>	O transmissor determinou um novo valor de conformidade para o sujeito.
<i>Session Established</i>	O transmissor estabeleceu uma nova sessão para o usuário.
<i>Session Presented</i>	O transmissor identificou uma sessão presente em dado momento.

^a Este tipo de evento está obsoleto na especificação RISC. Novas implementações DEVEM usar o evento de sessão revogada definido na especificação CAEP.

Exemplo de um evento RISC para conta desabilitada:

```
{
  "iss": "https://idp.example.com/",
  "jti": "756E69717565206964656E746966696572",
  "iat": 1508184845,
  "aud": "636C69656E745F6964",
  "events": {
    "https://schemas.openid.net/secevent/risc/event-type/\
account-disabled": {
      "subject": {
        "format": "iss_sub",
        "iss": "https://idp.example.com/",
        "sub": "7375626A656374",
      },
      "reason": "hijacking",
    }
  }
}
```

Exemplo de um evento RISC/CAEP para sessão revogada:

```
{
  "iss": "https://idp.example.com/123456789/",
  "jti": "24c63fb56e5a2d77a6b512616ca9fa24",
  "iat": 1615305159,
  "aud": "https://sp.example.com/caep",
  "events": {
    "https://schemas.openid.net/secevent/caep/event-
type/\
session-revoked": {
      "subject": {
        "format": "email",
        "id": "subject@example.com"
      },
      "event_timestamp": 1615304991643
    }
  }
}
```



SSF - Adoção

Google Sign-in com RISC

- O Google implementa o RISC como parte do seu ecossistema de identidade⁷:
 - Se você, como desenvolvedor, oferece login com “Sign in with Google”, pode se inscrever para receber eventos RISC;
- Cenário:
 - Um usuário faz login no seu serviço usando o Google;
 - Posteriormente, o Google detecta que a conta foi comprometida, ou o próprio usuário altera sua senha;
 - O Google dispara um evento RISC do tipo session-revoked⁸ para todos os SPs (RISC *subscribers*) registrados para aquele usuário.

⁷ Protect user accounts with Cross-Account Protection

⁸ Evento RISC sessão revogada

SSF - Adoção

Google Sign-in com RISC

- Lado do SP:
 - Sistema recebe o evento via webhook (JWT assinado);
 - SP decide que ações tomar:
 - Invalidar a sessão ativa do usuário;
 - Forçar re-login;
 - Executar outras ações de mitigação de risco.

Nota

Tokens de eventos de segurança só são enviados para contas Google pessoais com escopos de perfil/e-mail autorizados. Contas do Google Workspace estão excluídas.

● SSF - Adoção

Outros exemplos

- Apple Business Manager/Apple School Manager: para utilizar um provedor de identidade próprio deve cumprir requisitos como⁹:
 - OpenID Connect para autenticação Federada;
 - OpenID SSF para eventos de segurança da conta.
- Okta é um provedor de identidade suportado no ecossistema da Apple¹⁰, além do google workspace e do Microsoft Entra ID.

⁹ Intro to federated authentication with Apple Business Manager

¹⁰ Integration with Okta and Apple Business Manager



Considerações Finais



Sirtfi vs SSF

Complementares ou concorrentes?

Aspecto	Sirtfi	SSF
Natureza	Framework de processos operacionais	Protocolo técnico para compartilhamento de eventos
Base Técnica	Humanos + processos + contatos	Webhooks + JWT + APIs
Integração	Usa metadata SAML (security contact)	Funciona em OIDC/SSF
Ação	Notificação manual, emails, telefonemas	Notificação automatizada, máquina para máquina
Escopo	Capacidade organizacional para resposta a incidentes de forma colaborativa	Notificação de eventos de risco em tempo real

Nota

Complementares: Sirtfi trata nível organizacional e humano (governança e processos), enquanto o SSF e seus perfis automatizam parte da comunicação de eventos de risco de contas.

Sirtfi vs SSF

Oportunidade de automação?

- A comunidade de e-Ciência exige que IdPs implementem o Sirtfi;
 - Garante que a entidade tenha capacidade mínima para colaborar na resposta a incidentes;
 - Porém, ainda há forte dependência de processos manuais, o que pode limitar a efetividade.
- O Shared Signals Framework (SSF), especialmente o perfil RISC, permite automatizar notificações de contas comprometidas;
 - Com isso, eventos críticos podem ser disseminados em tempo real;
 - A partir daí, os processos definidos no SIRTfI podem ser acionados de forma mais coordenada e eficaz.

- Base tecnológica diferente:
 - SAML não tem uma base natural para webhooks ou streams de eventos assíncronos, como no modelo do SSF.
 - OIDC tem especificações de segurança baseadas em JOSE¹¹ (JWT, JWS, etc.), o SAML depende de XML Signature e XML Encryption, considerados mais complexos e menos flexíveis para modelos *event-driven*.
- Porém:
 - Existem discussões sobre a evolução das federações acadêmicas para o modelo OIDC;
 - Algumas federações acadêmicas já oferecem suporte híbrido com OIDC e SAML.

¹¹ Javascript Object Signing and Encryption (JOSE)



SSF

Viável na CAFe?

- Camada Paralela?
 - IdPs da CAFe podem emitir sinais de segurança através de webhooks independentes;
 - Exigiria que os SPs na CAFe adotassem também um *endpoint* RISC fora do fluxo normal do SAML.
- Gateway?
 - Middleware ouve eventos no IdP (ex.: desativação de conta, revogação, etc.);
 - Traduza esses eventos para eventos RISC e envie para os SPs que suportem esse tipo de integração.

- Candidato "natural" para operar a infraestrutura: o operador da federação CAFe:
 - Já agrega e publica dados;
 - Possui relacionamento de confiança com IdPs e SPs da federação;
 - Capacidade de fornecer infraestrutura compartilhada.
- Desafios:
 - Gerenciamento de *streams* e entrega de eventos;
 - Manutenção de filas de eventos;
 - Segurança e autenticação mútua;
 - Auditoria e conformidade.

Referências

- 1 Shared Signals Working Group - Overview
- 2 OpenID Continuous Access Evaluation Profile 1.0 - draft 03
- 3 OpenID RISC Profile Specification 1.0 - draft 02
- 4 DevDay 2025: Strengthening Security: The Shared Signals Framework (Thomas Darimont)
- 5 sharedsignals.guide

Discussão

Contribuições? Dúvidas?

Muito obrigada!



ct-gid@listas.rnp.br
<https://listas.rnp.br/mailman/listinfo/ct-gid>



MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

