RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Educação, Pesquisa
e Inovação em Rede

CAEP

CT-GId

Shirlei Chaves

08/2024

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

Agenda

1. Visão Geral
2. CAEP
3. Conclusão

Visão Geral

Gartner Hype Cycle™ para Identidade Digital 2023

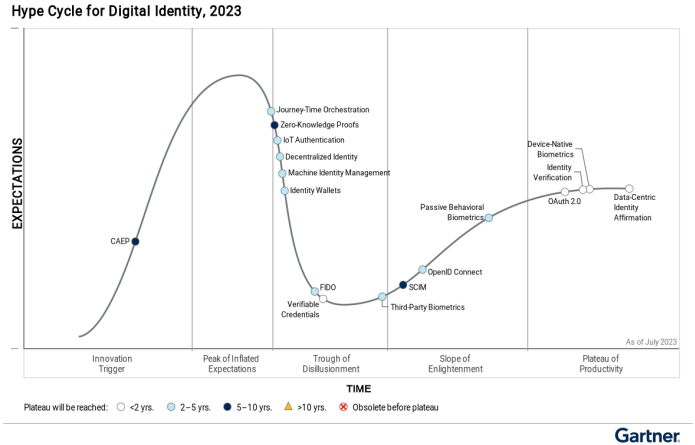


Figura: Gartner Hype Cycle para Identidade Digital 2023[1]

[1]https://wwps.microsoft.com/blog/digital-identity-gartner

Modelos de Controle de Acesso Tradicionais

Características [1][3][6]:

- O acesso é concedido durante o estabelecimento da sessão, considerando atributos como papeis e atributos do usuário, recurso ou do ambiente.
- A revogação de acesso pode ser lenta e exigir intervenção manual ou que a sessão expire.

O OAuth 2.0 fornece tokens de acesso e de atualização (*refresh tokens*), para manter as sessões atualizadas, mas não é suficiente para manter níveis de garantia sobre o usuário.

Modelos de Controle de Acesso Tradicionais

Problemas para ambientes dinâmicos [1][3][6]:

- Mudanças Contínuas no Contexto
- Sessões Longas
- Acessos a Múltiplos Serviços
- *Bring your own Device* (BOYD)
- Ambientes Híbridos e Remotos

Modelos de Controle de Acesso Tradicionais

Problemas para ambientes dinâmicos [1][3][6]:

- Mudanças Contínuas no Contexto
- Sessões Longas
- Acessos a Múltiplos Serviços
- *Bring your own Device* (BOYD)
- Ambientes Híbridos e Remotos

- Os métodos tradicionais não reavaliam o acesso após a autenticação inicial.

A segurança do dispositivo pode mudar durante uma sessão (p. ex.: instalação de *malware*).

Modelos de Controle de Acesso Tradicionais

Problemas para ambientes dinâmicos [1][3][6]:

- Mudanças Contínuas no Contexto
- Sessões Longas
- Acessos a Múltiplos Serviços
- *Bring your own Device* (BOYD)
- Ambientes Híbridos e Remotos

- Um usuário pode estar logado em múltiplos serviços durante um longo período.

Qualquer mudança de contexto durante a sessão (mudança de localização, comportamento suspeito) não é tratada adequadamente.

Modelos de Controle de Acesso Tradicionais

Problemas para ambientes dinâmicos [1][3][6]:

- Mudanças Contínuas no Contexto
- Sessões Longas
- Acessos a Múltiplos Serviços
- *Bring your own Device* (BOYD)
- Ambientes Híbridos e Remotos

- Usuários frequentemente acessam vários serviços e recursos simultaneamente.

Difícil garantir que o contexto de acesso é seguro para todos os serviços de forma contínua.

Modelos de Controle de Acesso Tradicionais

Problemas para ambientes dinâmicos [1][3][6]:

- Mudanças Contínuas no Contexto
- Sessões Longas
- Acessos a Múltiplos Serviços
- *Bring your own Device* (BOYD)
- Ambientes Híbridos e Remotos

- *Bring Your Own Device*: usuários utilizando dispositivos pessoais para acessar dados corporativos.

Variabilidade na segurança dos dispositivos pessoais.

Modelos de Controle de Acesso Tradicionais

Problemas para ambientes dinâmicos [1][3][6]:

- Mudanças Contínuas no Contexto
- Sessões Longas
- Acessos a Múltiplos Serviços
- *Bring your own Device* (BOYD)
- Ambientes Híbridos e Remotos
- Trabalho remoto e uso de infraestruturas de nuvem.

Aumento da superfície de ataque e necessidade de verificar continuamente a legitimidade do acesso.

Solução: Avaliação Contínua de Acesso

Continuous Access Evaluation (CAE) ou Avaliação Contínua de Acesso:

- Avaliação contínua se um cliente ainda tem autorização de acesso a um recurso.
- Desempenha um papel importante no modelo de Arquitetura de Confiança Zero (ZTA) [1].

> Um sistema de segurança de confiança zero deve autenticar e **autorizar cada solicitação de acesso de forma dinâmica e baseada em risco**, considerando fatores como identidade do sujeito, postura de segurança do dispositivo, tempo e localização, **em vez de confiar em uma única autenticação inicial para todas as solicitações subsequentes** [6].

CAEP

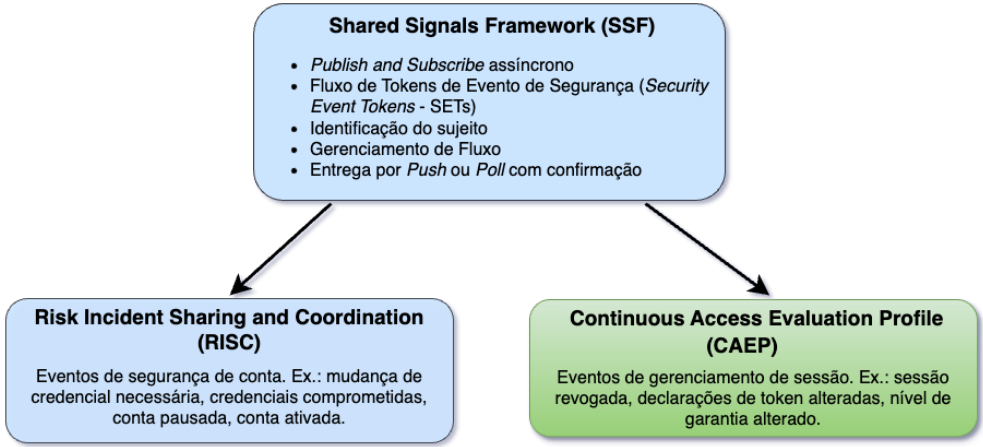
Shared Signals Framework (SSF)

Shared Signals Framework (SSF) ou Framework de Sinais Compartilhados:

- Novo padrão em desenvolvimento pela OpenID Foundation [5].
- Facilitar o compartilhamento de **eventos de segurança** entre organizações, relacionados aos usuários que utilizam seus sistemas.

Comunicação entre serviços de rede - provedores de serviço (SPs) e de identidade (IdPs), serviços de gerenciamento de dispositivos e IdPs ...

Shared Signals Framework (SSF)



Shared Signals Framework

Comunicação assíncrona no modelo *Publish and Subscribe*:

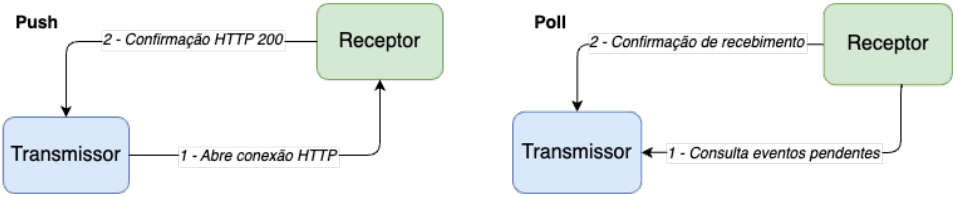
- *Publisher*: Transmissor (*Transmitter*)
- *Subscriber*: Receptor (*Receiver*)

Comunicação estabelecida via “fluxos” (*streams*):

- Unidade básica de comunicação: Tokens de Evento de Segurança (*Security Event Tokens*[2] - SETs)

[2] https://datatracker.ietf.org/doc/html/rfc8417

Entrega de Eventos



Continuous Access Evaluation Profile (CAEP)

Continuous Access Evaluation Profile (CAEP) ou Perfil de Avaliação Contínua de Acesso.

- Perfil especificado para descrever eventos relacionados à mudanças na **sessão** de um sujeito.
- Define um conjunto de tipos de eventos conforme o SSF.
  - Transmissores enviam atualizações contínuas para Receptores.
  - Receptores podem ajustar o acesso de usuários ou dispositivos de modo dinâmico e cooperativo.
- Especificação em desenvolvimento - versão 1.0, draft 02 [08].

CAEP - Eventos

Exemplo de um evento de 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
        }
    }
}
```

CAEP - Eventos

Tipos de Eventos conforme a especificação CAEP [1][4]:

Nome	Descrição
Session Revoked	O transmissor revogou a sessão.
Token Claims Change	O transmissor forneceu novos valores para declarações de tokens previamente enviados.
Credential Change	O transmissor tem uma nova credencial para o sujeito.
Assurance Level Change	O transmissor tem um novo nível de garantia para o sujeito.
Device Compliance Change	O transmissor determinou um novo valor de conformidade para o sujeito.

CAEP - Adoção

- Exemplo: Microsoft Entra ID (antigo Azure AD[3])[4]

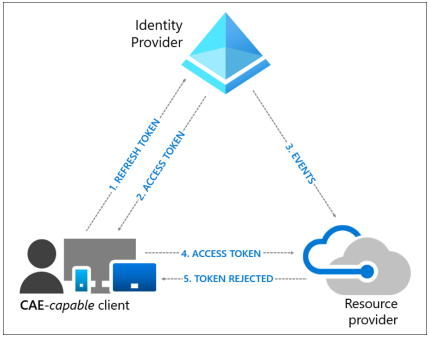


Figura: Fluxo de eventos de revogação de sessão

[3]Novo nome do Azure Active Directory
[4]Foco inicial no Exchange, Teams, e SharePoint Online.

CAEP - Adoção

- Exemplo: Microsoft Entra ID (antigo Azure AD[5])[6]

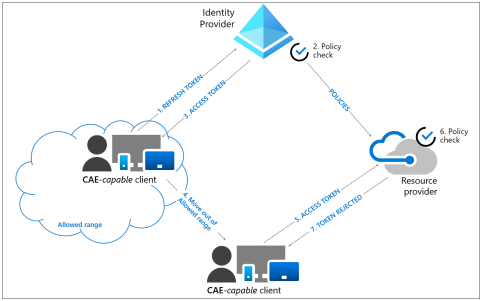


Figura: Fluxo de mudança de condição do usuário

[5]Novo nome do Azure Active Directory
[6]Foco inicial no Exchange, Teams, e SharePoint Online.

Conclusão

Resumindo

O CAEP possibilita:

- Lidar com desafios com tokens de longa duração
- Autenticação incremental (*step-up authentication*)
- Avaliação contínua da postura de um dispositivo
- Comunicação e resposta a eventos do ciclo de vida da identidade

Visa manter a segurança em ambientes de TI dinâmicos e serviços federados, permitindo a troca contínua de eventos de segurança e fornecendo uma abordagem contínua e adaptativa para a gestão de acessos.

Resumindo

- Especificado como um perfil do framework de sinais compartilhados (SSF) para eventos de sessão para facilitar o modelo de confiança zero.
- Considerado por relatório do Gartner como emergente, com um número de implantações crescendo, mas ainda limitado.
- O SSF e seus perfils como o CAEP são frutos de um grupo de trabalho em andamento, e portanto, ainda em desenvolvimento.

Referências

1. Hilbig, T., Serzantov, V. and Schreck, T., 2023, October. Protect the Gate–Not Only Once: Continuous Access Evaluation in Practice. In 2023 7th Cyber Security in Networking Conference (CSNet) (pp. 137-142). IEEE. DOI: 10.1109/CSNet59123.2023.10339788
2. OpenID Continuous Access Evaluation Profile 1.0 - draft 02
3. Re-thinking federated identity with the Continuous Access Evaluation Protocol
4. caep.dev
5. Shared Signals Working Group - Overview
6. Zero Trust Architecture - NIST Special Publication 800-207 - DOI: doi.org/10.6028/NIST.SP.800-207
7. OpenID Shared Signals and Events Framework Specification 1.0 - draft 01
8. OpenID Continuous Access Evaluation Profile 1.0 - draft 02

Discussão

Contribuições? Dúvidas?

Muito obrigada!

CC BY

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