Projeto de Formatura – 2023

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia Elétrica – Ênfase Computação

Tema:

Ampliando a Expressividade dos Tokens SPIFFE

SPIFFE e SPIRE

O SPIFFE é um framework de segurança específico para ambientes altamente distribuídos, como geralmente é o caso para sistemas "Cloud Native". Bastante consolidado e amplamente adotado por grandes empresas de tecnologia, ele tem como objetivo melhorar a gestão de identidades nestes ambientes onde recursos de hardware são voláteis, e podem ser alocados e desalocados rapidamente. Para isso, o framework define credenciais de curta duração, chamadas de Documento de Identidade Verificável SPIFFE (SVID), usadas quando as cargas de trabalho precisam se autenticar entre si. O SPIRE é uma implementação do SPIFFE, feita para ser facilmente usada em aplicações em produção, que gerencia a validação de identidade de plataforma e carga de trabalho, definindo APIs para gerenciar políticas, bem como emissão e rotação de certificados.

Nested Tokens e ID-Mode

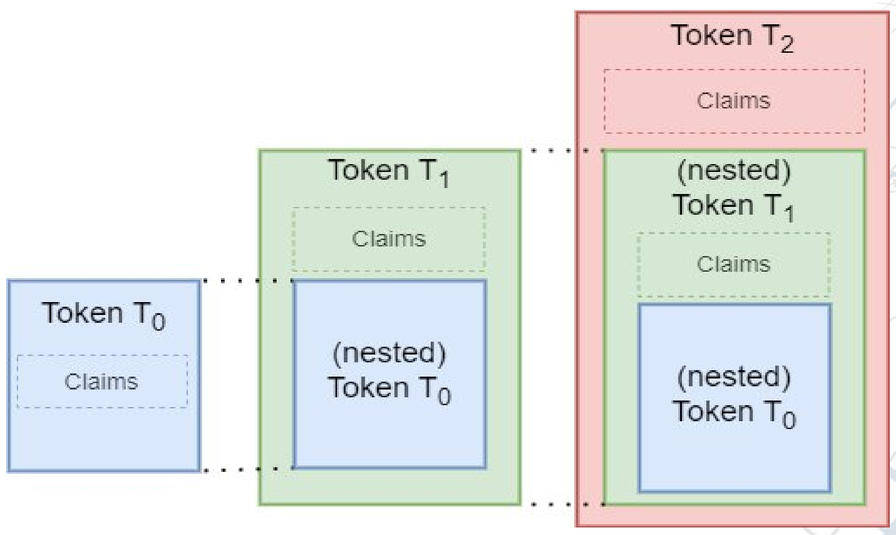

Figura: Exemplo de funcionamento dos Nested Tokens

Este projeto está sendo feito em parceria com o grupo de pesquisa "SVID-AttestedClaims", que tem por objetivo expandir a expressividade das credenciais dentro do framework do SPIFFE. Para isso, ele introduz o conceito de modelos aninhados, onde informações ou asserções adicionais podem ser adicionadas a uma asserção original sem modificá-la. Essa abordagem garante a integridade da afirmação original ao assinar o token inteiro, incluindo a carga útil acrescentada.

O objetivo deste projeto é criar uma maneira de manter a rastreabilidade dessas asserções distribuídas. Nomeado "ID-Mode", este modelo criado permite muita flexibilidade, e pode ter diversas utilidades dentro de projetos que já utilizam do SPIRE para a identificação de cargas de trabalho. Com ele, é possível criar lógicas de delegação de autenticação e autorização bastante seguras, dentro da lógica de identidades já provisionada pelo SPIRE, dentre outras diversas possíveis aplicações dada a flexibilidade do modelo baseado em asserções.

Prova de Conceito (PoC)

Uma prova de conceito (PoC) foi realizada para demonstrar a viabilidade do framework proposto para integrar ao SPIFFE uma lógica de asserções distribuídas. A prova de conceito foi feita simulando uma aplicação web altamente distribuída, e um usuário final que deseja utilizar técnicas de delegação de identidade para acessar recursos dentro da aplicação. Asserções são feitas pelas cargas de trabalho utilizando do modelo ID-Mode criado, e permitem o acesso aos recursos corretos de maneira bastante segura.

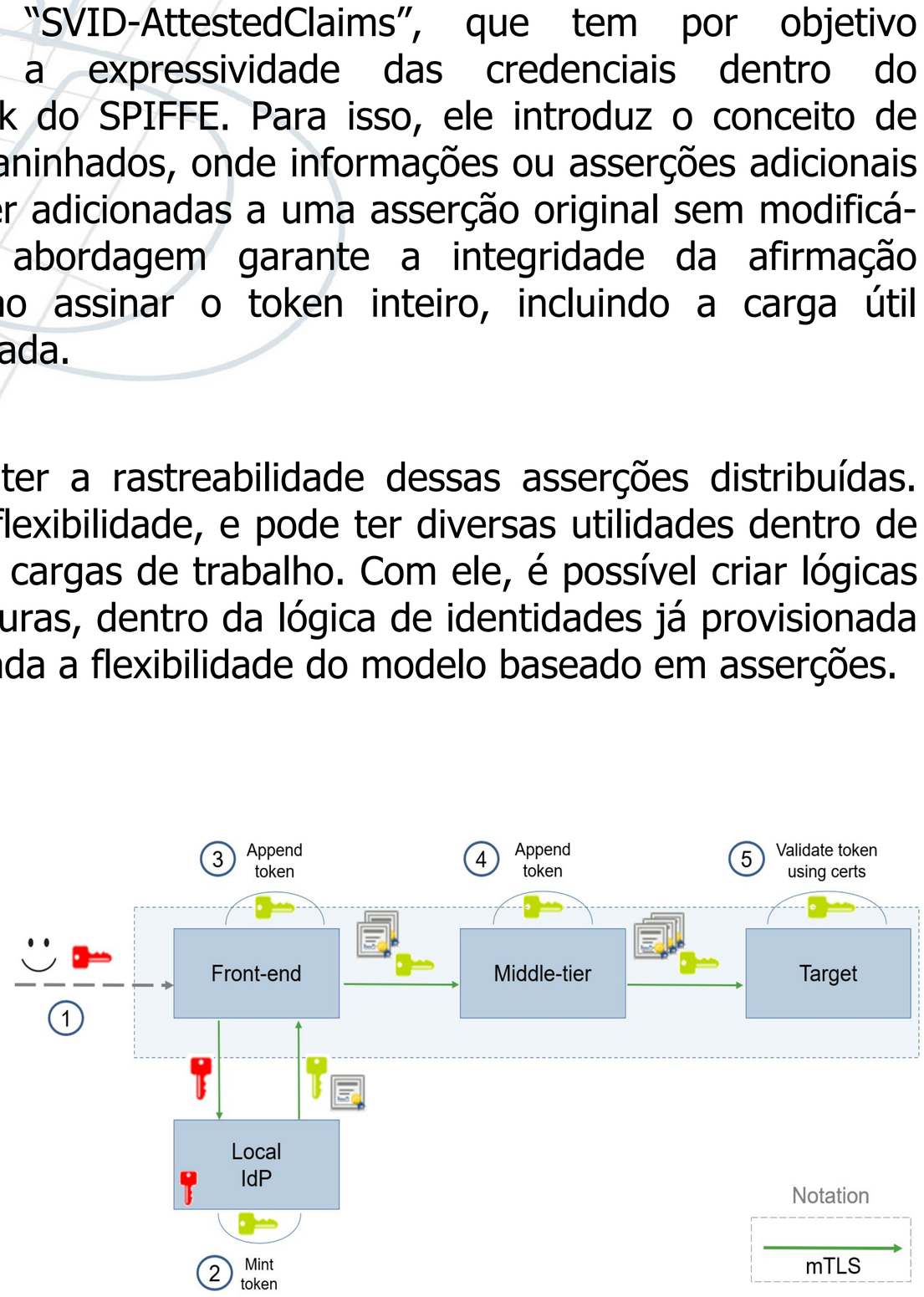

Figura: Fluxograma de uma aplicação utilizando o ID-Mode

Integrantes: David Henrique da Costa
Pedro Henrique Florio Mendes

Professor(a) Orientador(a): Prof. Dr. Marcos Antonio Simplicio Junior