GT-CoFee
Um esquema de gestão de identidade federada para IoT

EQUIPE

Coordenador-geral
Leonardo Barbosa e Oliveira
Universidade Federal de Minas Gerais (UFMG)

Coordenador-adjunto
Marco A. A. Henriques
Universidade Estadual de Campinas (Unicamp)

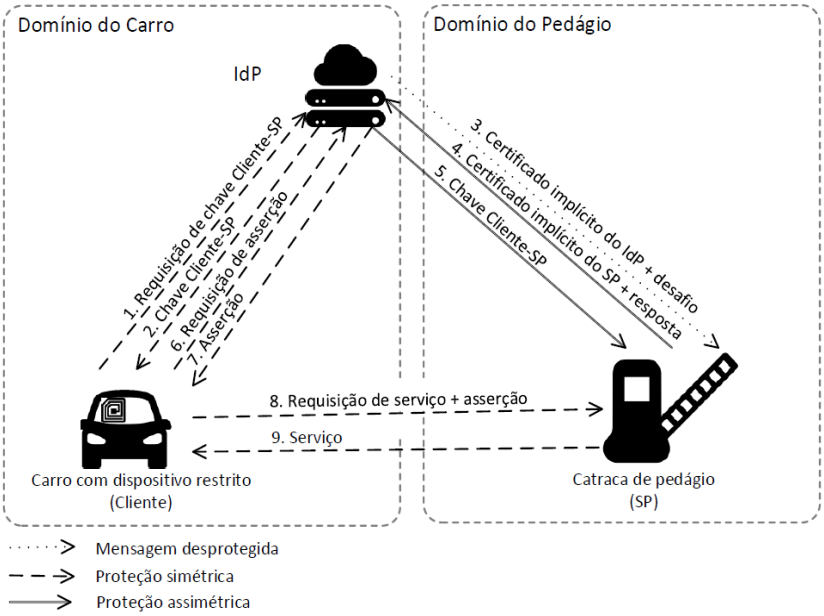
Colaboradores
Maria Luiza Burgarelli A. Santos
Universidade Federal de Minas Gerais (UFMG)
Jéssica C. Carneiro
Universidade Federal de Minas Gerais (UFMG)
Fernando A. Teixeira
Universidade Federal de São João del-Rei (UFSJ)
Antônio M. R. Franco
Universidade Federal de Minas Gerais (UFMG)

SITE
leob.dcc.ufmg.br/cofee

CONTATO
pd@rnp.br

DESCRIÇÃO

Um aspecto crítico no uso de sistemas modernos, sobretudo na Internet das Coisas (*Internet of Things – IoT*), é a autenticação de usuários e controle de acesso aos recursos disponíveis. A gestão de identidades (*Identity Management – IdM*) é essencial nesse sentido, pois provê meios para que essas tarefas possam ser realizadas de maneira segura.



Protocolo de Autenticação FLAT – Pagamento de pedágio.

Abordagens amplamente utilizadas em IdM, no entanto, não são adequadas para o ambiente IoT, uma vez que normalmente se baseiam nas credenciais de acesso dos usuários dos dispositivos, e não dos próprios dispositivos, o que é uma prática insegura, pois muitas vezes os dispositivos não deveriam ter as mesmas permissões de acesso que seus usuários. Além disso, abordagens em IdM existentes baseiam-se em criptografia assimétrica e, portanto, requerem uma carga significativa de processamento e armazenamento, o que é inadequado para dispositivos com recursos reduzidos encontrados comumente em ambientes IoT.

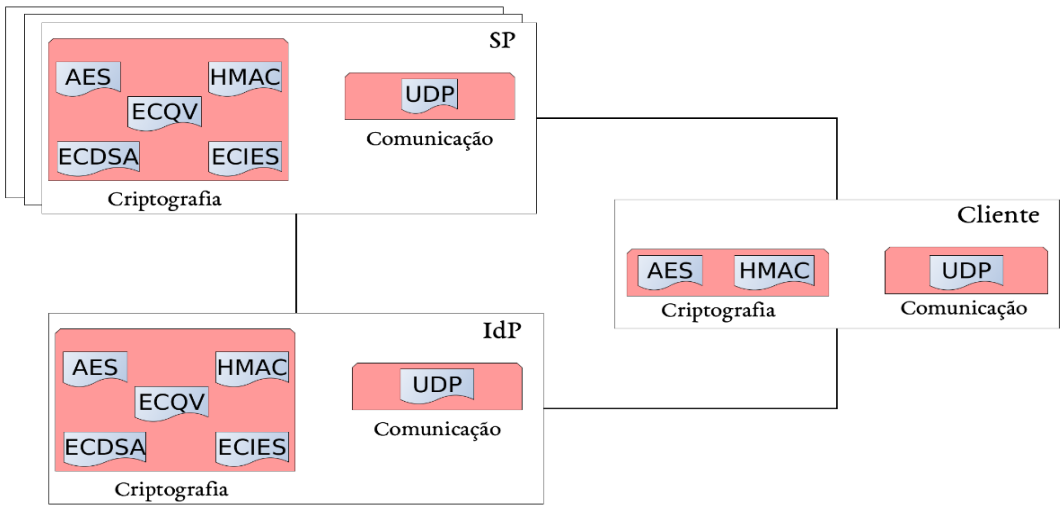
FLAT – Autenticação Federada Leve para a Internet das Coisas

Como solução para esse problema, propomos uma alternativa leve para a autenticação de dispositivos restritos, o FLAT (*Federated Lightweight Authentication of Things*). Modelamos, desenvolvemos e avaliamos um protótipo de nosso protocolo federado de autenticação em dispositivos restritos, aplicando o FLAT a cenários reais de utilização: um sistema de pagamento automático de pedágio e um sistema de controle de acesso aos estacionamentos de universidades. O FLAT baseia-se nas seguintes estratégias: (i) utilização de apenas primitivas criptográficas simétricas no cliente IoT, (ii) utilização de certificados implícitos na comunicação entre SP e IdP e (iii) substituição de criptossistemas como RSA/DSA por criptossistemas baseados em curvas elípticas (ECIES/ECDSA).

Protótipo - Controle de acesso a estacionamentos

FLAT pode ser utilizado em diversos cenários em que seja necessária a autenticação de dispositivos de diferentes domínios, com aplicações na indústria e no meio acadêmico:

- Autenticação para liberação e pagamento automático de pedágio de outro domínio;
- Controle automático de estacionamento em universidades;
- Conexão autenticada de equipamentos de diagnóstico e reparo de uma empresa em equipamentos que precisem de reparos de uma outra empresa;
- Drone fotografando regiões e descarregando fotos em sistemas que residem em domínios fora do seu domínio de origem.



Arquitetura do FLAT