IdM – Método Baseado em Chaves para Autenticação Única em IOT

EDUARDO ALBERTO SCHMOLLER

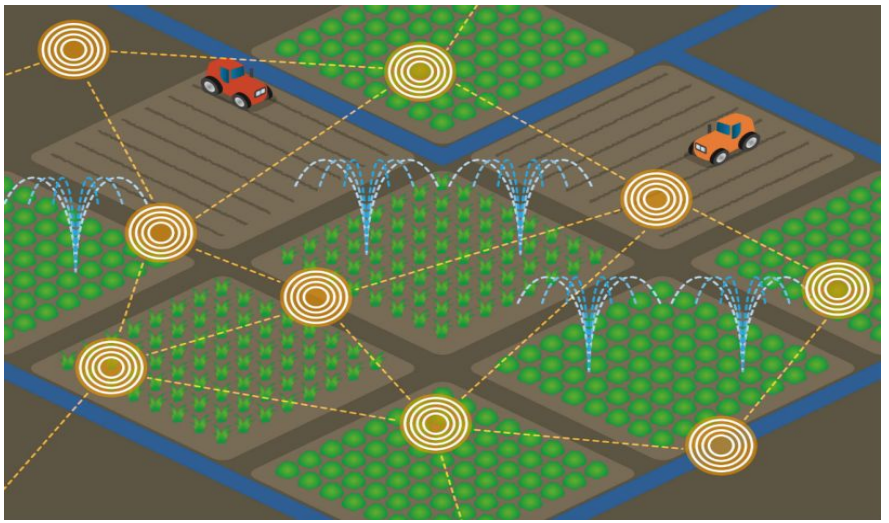
AUTORES: MSc. Adriano Witkovski, Prof. Dr. Altair O. Santin (Orientador)

Pato Branco, 08 de Junho de 2017

Internet da Coisas (IoT)

"*Na sua essência, a IoT significa apenas um ambiente que reúne informações de vários dispositivos (computadores, veículos, smartphones, semáforos, e quase qualquer coisa com um sensor) e de aplicações (qualquer coisa desde uma aplicação de mídia social como o Twitter a uma plataforma de comércio eletrônico, de um sistema de produção a um sistema de controle de tráfego), não necessáriamente conectado à internet.*"

Aplicações de IoT



Internet das Coisas (IoT)

→ **Limitações: poder computacional, sem suporte a HTTP e SSL.**

→ **Problemas: Confidencialidade, autencidade, integidade dos dados.**

→ **Necessidades: Cominicação segura, acesso seguro a rede, gestão de indentidade, manutenção, atualização, "coisas" isoladas da internet.**

Segurança

→ Criptografia chave simetrica: Utiliza poucos recursos, descoberta da chave, controle de usuários, manutenção da chave em diversos “Appliances”.

→ Criptografia chave pública: duas chaves, dificuldade deobter a chave privada baseado na chave pública.

→ Autenticação e autorização de acesso.

Protocolos IoT

→ CoAP: Constrained Application Protocol

→ DTLS: Datagram Transport Layer Security

→ Parser: tradução HTTP ↔ CoAP / DTLS

Utilização de comunicação segura entre “Appliance” e gateway e entre o serviço do fabricante e o gateway.

SSO possiblitando autenticação única para o técnico acessar vários “Appliances”.

Topologia Proposta

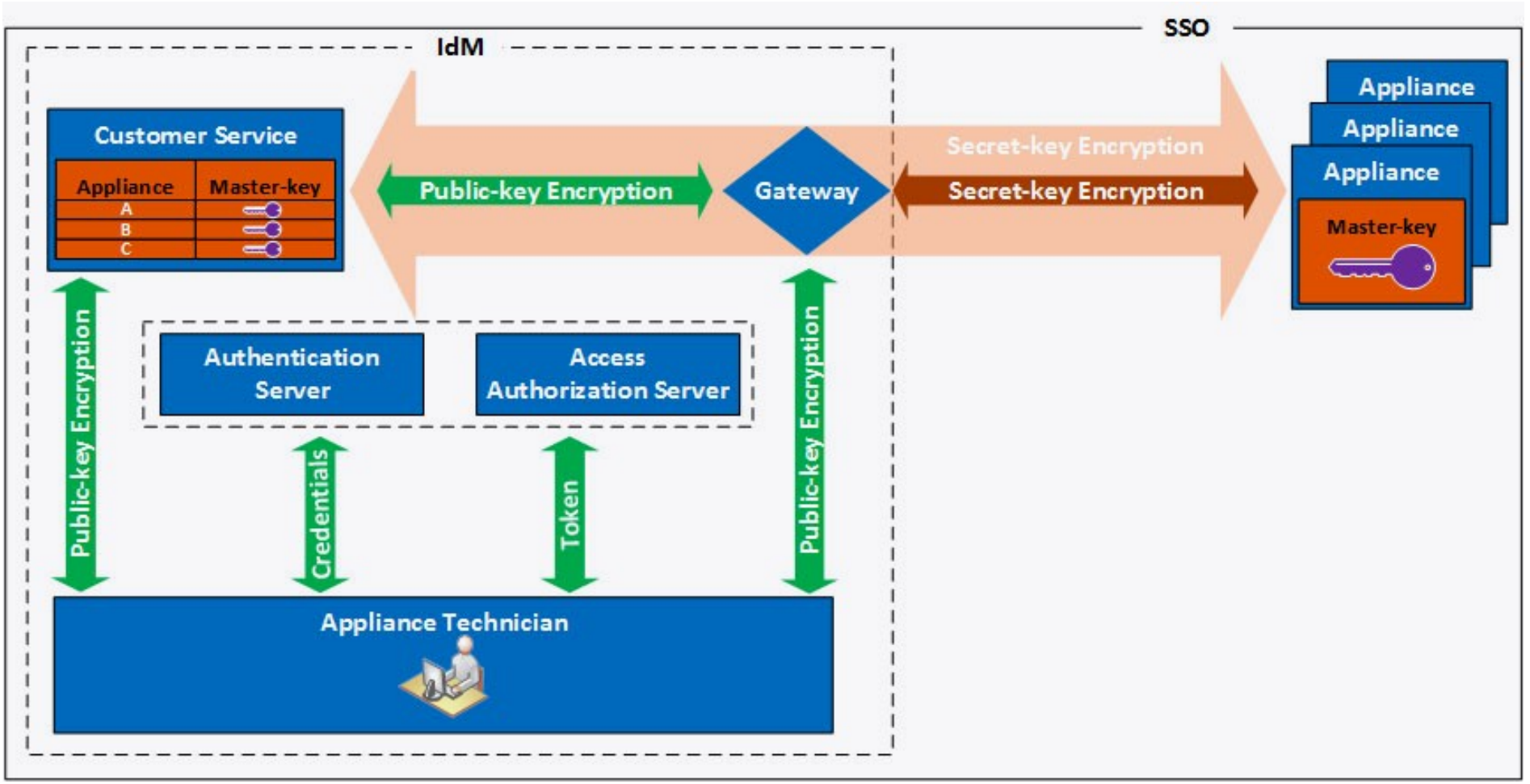


Figura 1 - Proposta

Requisição do Appliance

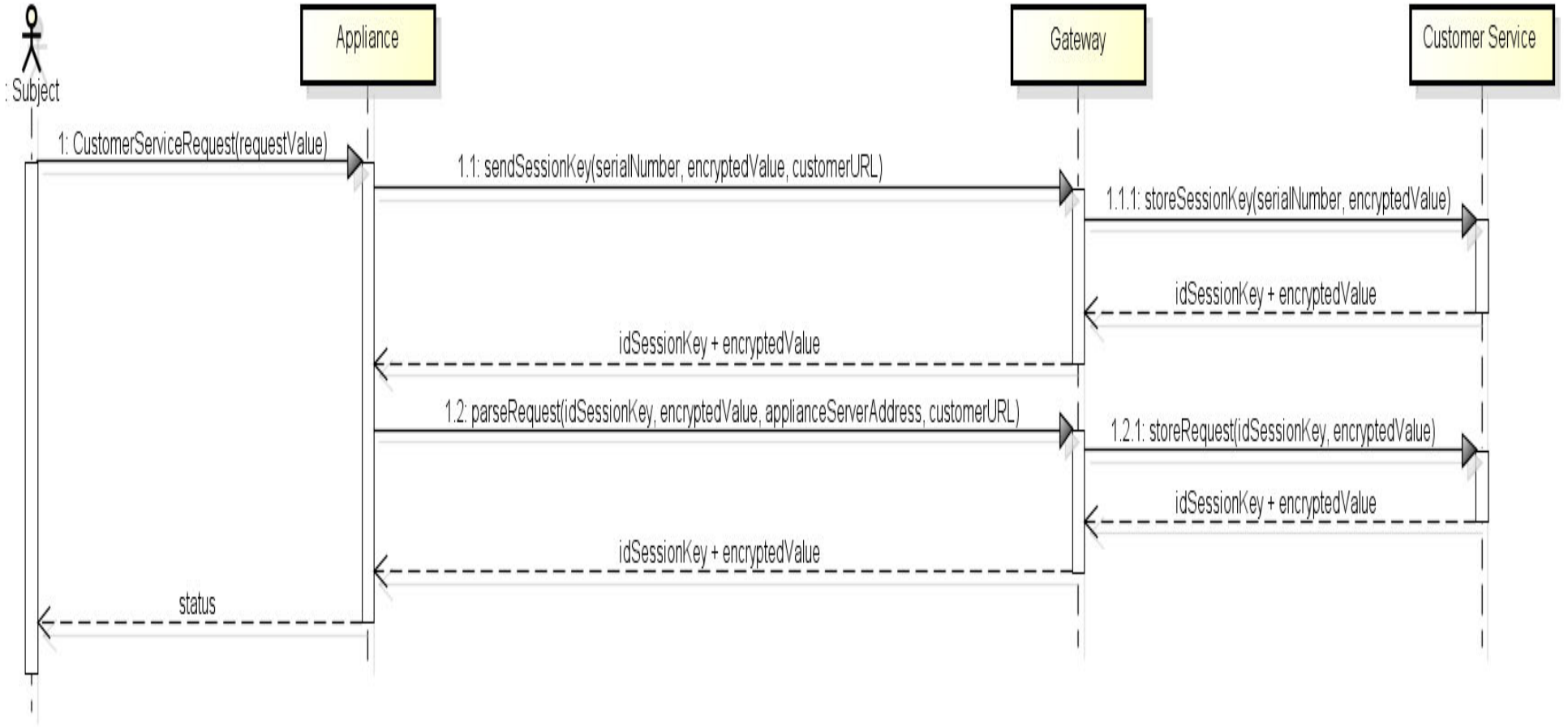


Figura 2 – Troca de mensagens Appliance

Autenticação Técnico

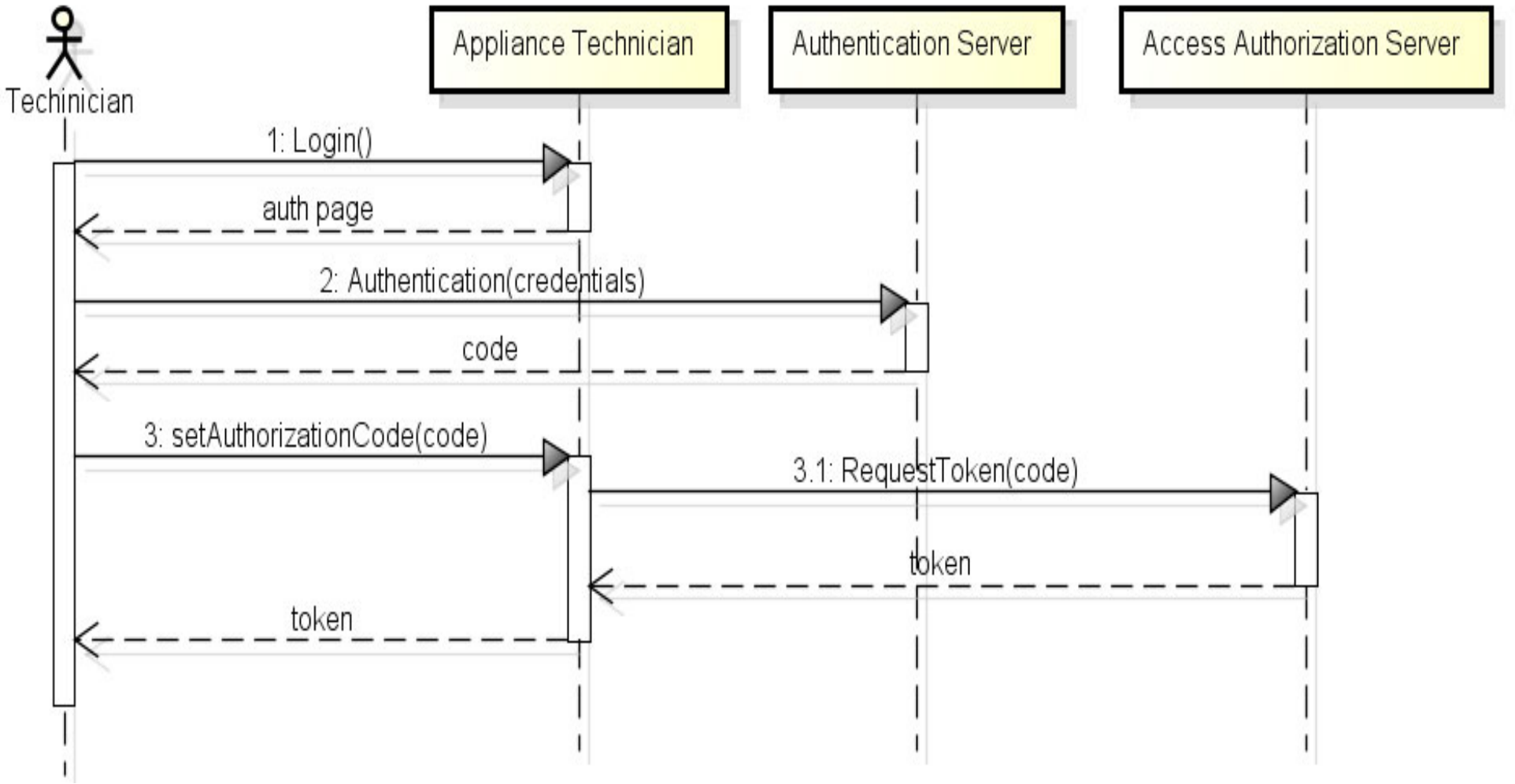


Figura 3 – Autenticação técnico

Acesso do Appliance pelo Técnico

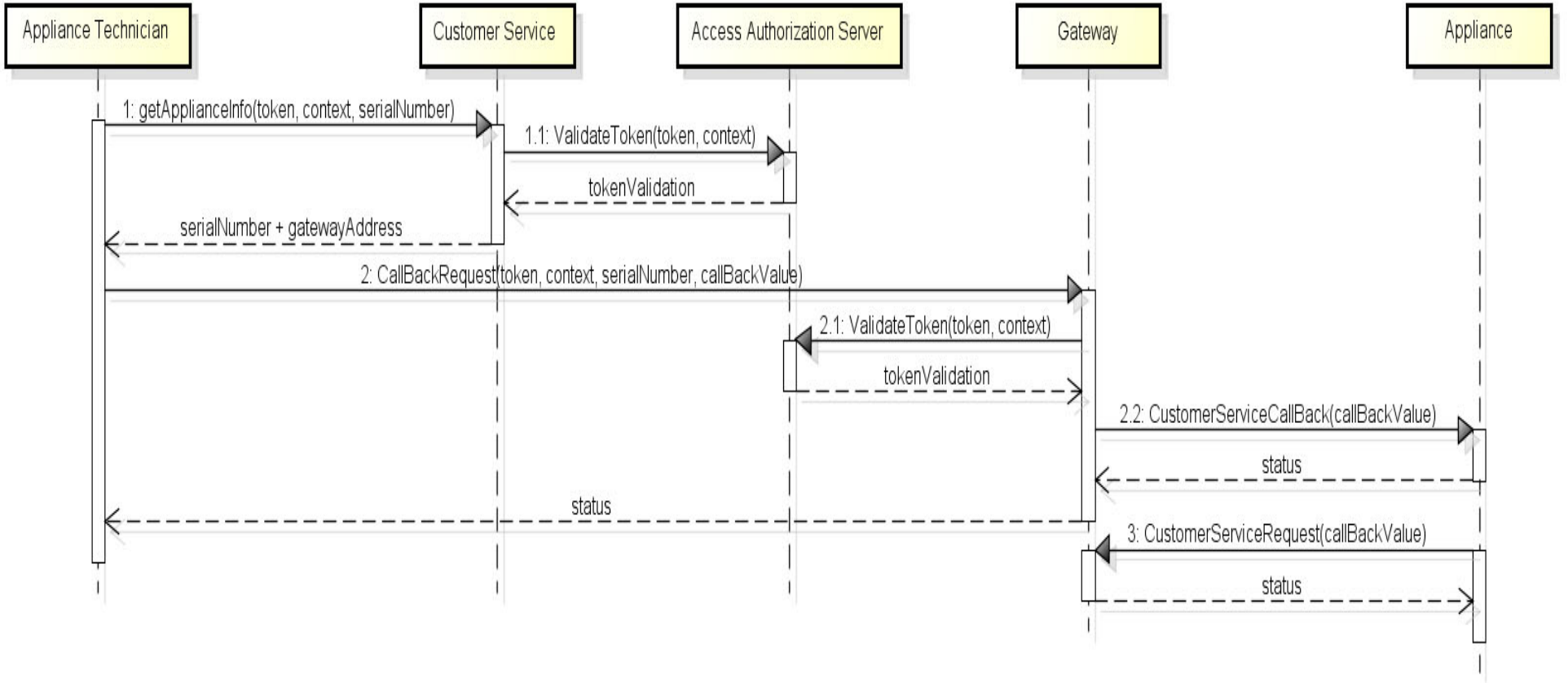


Figura 4 – Acesso appliance pelo técnico

Protótipo

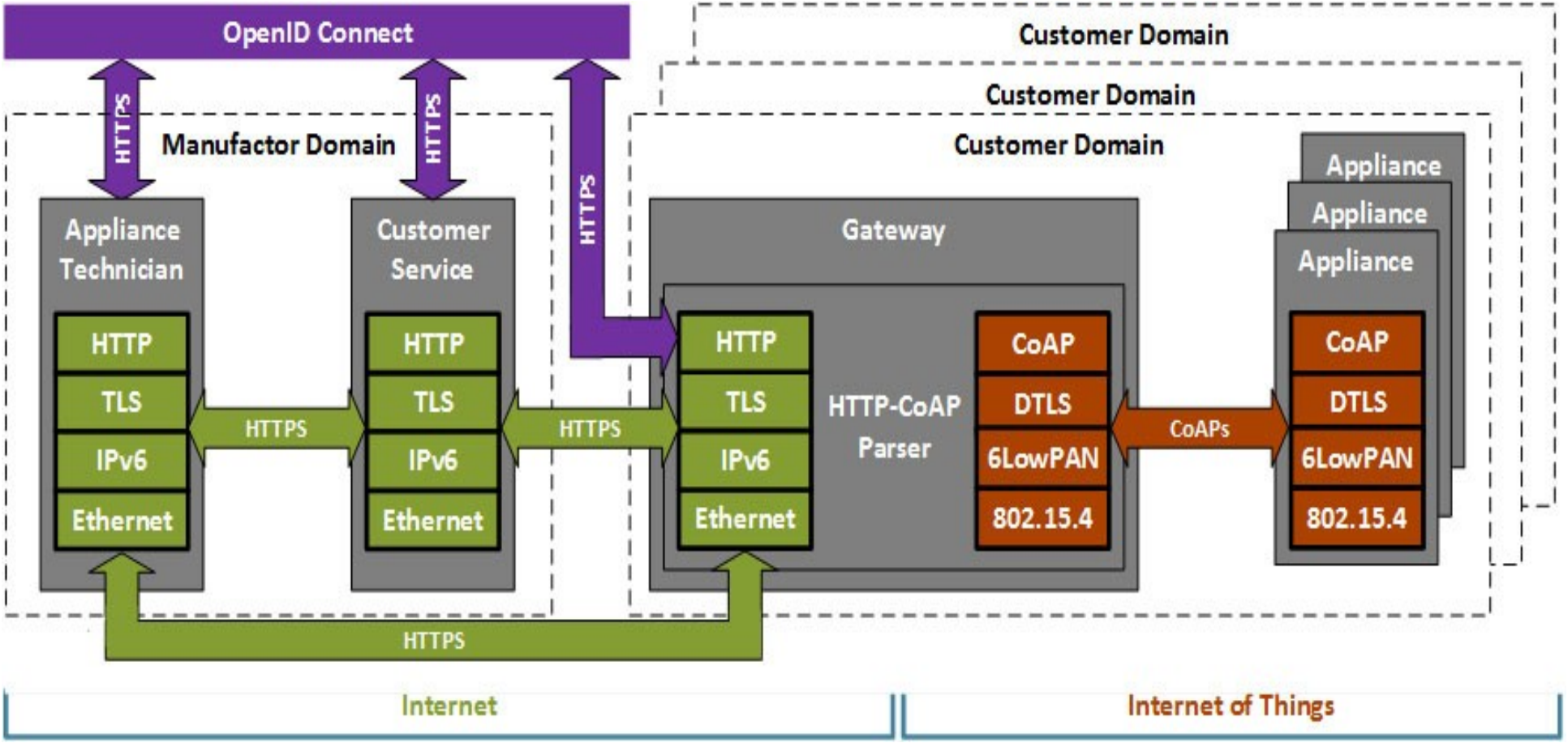


Figura 5 - Protocolos

Implementação - Simulação

O protótipo utiliza padrões de tecnologias conhecidas e bibliotecas de código aberto. O Manufactor Domain consiste em dois componentes, AppTec e CS. O AppTec foi implementado usando o framework Vaadin. O CS foi implementado como um Web Service RESTful usando a API JAX-RS. O Customer Domain consiste em um GW e vários Apps. As interfaces com o GW que representam o contexto Internet foram implantadas usando Java em um servidor HTTP. A interface da IoT foi construída num servidor CoAP usando a biblioteca Californium, que também foi usada para o App. Para cifragem foi utilizado o algoritmo AES de 128 bits, a fim de obter as chaves KKM e KEK, usando o Scandium, um subprojeto do Californium. O Scandium com suporte ao DTLS na versão 1.2 no contexto da IoT. O servidor de autenticação (AS) foi implementado seguindo a especificação do OpenID 2.0 usando a biblioteca Nimbus. O Nimbus fornece um IdM para AppTec, CS e GW, e também assegura que somente usuários autenticados e autorizados acessam os App. A autorização de acesso (AAS) foi implementada seguindo especificação do protocolo OAuth 2.0 e Nimbus, a fim de emitir tokens de acesso para o AppTec autenticado.

Resultados

Figura 6 - Resultados

Conclusões

→ Proteção de mensagens fim – a – fim.

→ Gateway e Appliances não expostos.

→ Serviço de autenticação evita ataques da internet.

→ IdM retira o esforço do appliance para interação com a internet.

→ Possibilita multiplos acessos com uma única autenticação, sem necessidade de saber a senhas de cada appliance e sem utilizar a mesma senha.

→ Tempo de resposta aceitável entre 10 e 50 Apps e mensagem de 32 a 4096 Bytes.

REFERÊNCIAS

→ Witkovski, Adriano; Santin, Altair. Um IdM e Método de Autenticação baseado em chaves para prover autenticação única em Internet das Coisas. SBSeg 2016.

→ http://computerworld.com.br/tecnologia/2014/11/25/iot-e-um-grande-e-confuso-campo-a-espera-de-explodir

→ Shelby Z., Hartke K., and Bormann C., “The Constrained Application Protocol (CoAP)”, IETF RFC 7252.

→ Rescorla E., Modadugu N., “Datagram Transport Layer Security Version 1.2.”, IETF RFC 6347.

IdM – Método Baseado em Chaves para Autenticação Única em IOT

EDUARDO ALBERTO SCHMOLLER

AUTORES: MSc. Adriano Witkovski, Prof. Dr. Altair O. Santin (Orientador)

Pato Branco, 08 de Junho de 2017