RP4: Proposta de Fase 2

GT-AMPTo - Segunda Fase

Autenticação Multi-fator para Todos

Emerson Ribeiro de Mello (IFSC)

30 de março de 2018

1. Visão geral

1.1. Descrição do produto/serviço resultante do piloto

Como resultado dessa fase de piloto, espera-se ter uma solução que permita aos provedores de identidade (IdP) da Comunidade Acadêmica Federada (CAFe) oferecerem autenticação com dois fatores para seus usuários. A solução permitirá a cada usuário dos IdPs determinar se deseja habilitar a autenticação com mais de um fator e quais opções, dentro das seguintes, poderão ser ativadas e combinadas, como fatores extras de autenticação:

- **Diálogo de confirmação**
  - Solução dependente de telefone inteligente (Android ou iOS) e de conectividade com a Internet no momento da autenticação, mas que possui a melhor usabilidade.
- **Senhas descartáveis (*One-Time Password* – OTP)**
  - Solução dependente de telefone inteligente (Android ou iOS), porém não precisa ter conectividade com a Internet no momento da autenticação.
- **FIDO U2F**[1]
  - Solução dependente de *tokens* físicos FIDO U2F [Srinivas et al., 2014], que devem estar conectados (via porta USB, ou NFC ou *bluetooth*) no dispositivo que o usuário está utilizando para se autenticar (primeiro fator).

Adicionalmente, durante a fase piloto, espera-se que seja completado um produto mínimo viável (*Minimal Viable Product* - MVP) baseado no cenário de manifestação das credenciais do usuário para o controle de acesso físico com IoT. Deste modo, vislumbramos como resultado principal da evolução deste estudo de caso um MVP para uma solução de controle de portas inteligente baseado em NFC e FIDO UAF [Machani et al., 2014]. Tal solução, integrada à CAFe, será capaz de obter os atributos de usuários para serem utilizados nos mecanismos de controle de acesso baseado em atributos. Além disso, a solução proverá o gerenciamento de dispositivos (ex: portas e sensores) e de políticas de controle de acesso que controle os mesmos.

1.2. Identificação do público alvo

Para o piloto espera-se ter uma solução completamente funcional, validada e testada em provedores de identidade (IdP) Shibboleth versão 3.3 ou superior[2]. Sendo assim, toda instituição que possuir um provedor de identidade Shibboleth poderá usufruir do produto dessa fase de piloto, o que inclui todas as instituições usuárias da Comunidade Acadêmica Federada (CAFe). Por consequência, todos os usuários desses provedores de identidade poderão usufruir da solução, ou seja, habilitar e usar o segundo fator de autenticação.

Cabe frisar que algumas instituições delegam a autenticação de seus sistemas internos (i.e. sistema acadêmico, webmail, *service desk*, etc.) para seu provedor de identidade Shibboleth, seguindo assim o modelo de gestão de identidade centralizado [Jøsang et al., 2005]. Ou seja, esses sistemas internos não atuam como provedores de serviços na federação CAFe, contudo são provedores de serviço privados da instituição e que só possuem relação de confiança com o provedor de identidade da instituição. Sendo assim, a solução resultante desse piloto irá beneficiar os usuários desses sistemas internos também.

[1] https://fidoalliance.org/about/what-is-fido [2]Se houver a manutenção da retrocompatibilidade.

2. Definição do piloto

2.1. Arquitetura do piloto

Para o desenvolvimento do protótipo na Fase 1, foram utilizados provedores de identidade e provedores de serviços disponibilizados pelo Laboratório de Experimentação em Gestão de Identidade (GIdLab) da RNP. Para o desenvolvimento do piloto, pode-se fazer uso de provedores de identidade das instituições parceiras, ou ainda, continuar usufruindo GIdLab, porém, neste caso, será solicitado um provedor de identidade específico para cada instituição parceira.

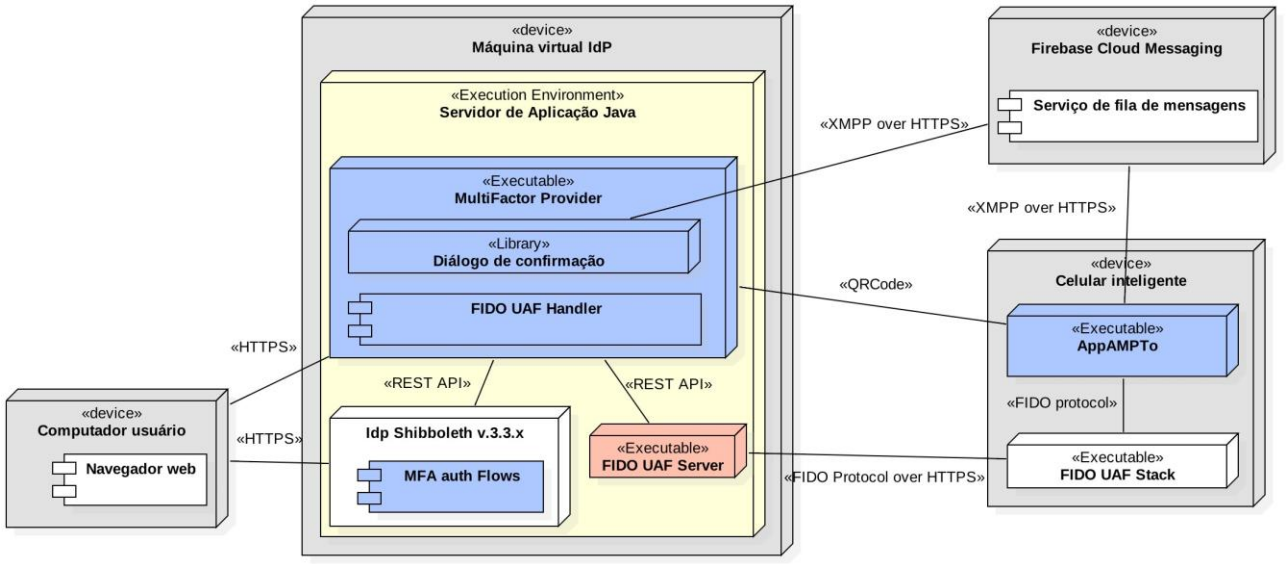

Figura 1: Diagrama de implantação do protótipo na Fase 1

A Figura 1 apresenta um diagrama de implantação UML do protótipo já desenvolvido e que será evoluído na fase de piloto. Os blocos em azul consistem em componentes de software desenvolvidos pelos proponentes. O nó *Firebase Cloud Messaging* representa o serviço de fila de mensagens fornecido gratuitamente pela Google e é usado na presente solução somente no cenário que se faz uso do **Diálogo de Confirmação** como segundo fator de autenticação.

O *Multi-Factor Provider* (MFaP) é o principal componente da solução e o mesmo será evoluído para permitir, além do Diálogo de Confirmação, o uso de senhas descartáveis (OTP) [Haller et al., 1998] e FIDO U2F [Srinivas et al., 2014]. A arquitetura do MFaP será projetada para que o mesmo possa ser estendido para agregar outras tecnologias como fatores extras de autenticação e sua configuração permitirá ao administrador do IdP indicar quais fatores extras de autenticação estarão disponíveis para seus usuários. Por exemplo, caso um administrador de IdP queira oferecer somente OTP como fator extra de autenticação, a solução permitirá que ele desabilite o diálogo de confirmação e FIDO U2F.

Na Fase 1 deste grupo de trabalho, foram propostos dois cenários de uso. O **primeiro cenário** teve como foco a autenticação multi-fator em provedores de identidade *Shibboleth*. O **segundo cenário** teve como foco a transposição da autenticação federada para a Internet das Coisas (IoT), além de desenvolver uma solução de controle de acesso baseado em atributos.

Os componentes e nós relacionados com FIDO UAF [Machani et al., 2014], ilustrados naFigura 1, foram desenvolvidos exclusivamente para permitir a execução do segundo cenário voltado para IoT. De acordo com a especificação do FIDO UAF, este pode ser usado como o único fator de autenticação de um usuário, tornando-o adequado para o cenário de transposição da autenticação e controle de acesso físico. Dessa forma, cabe frisar que no protótipo desenvolvido na Fase 1 os componentes do FIDO UAF não foram empregados no primeiro cenário.

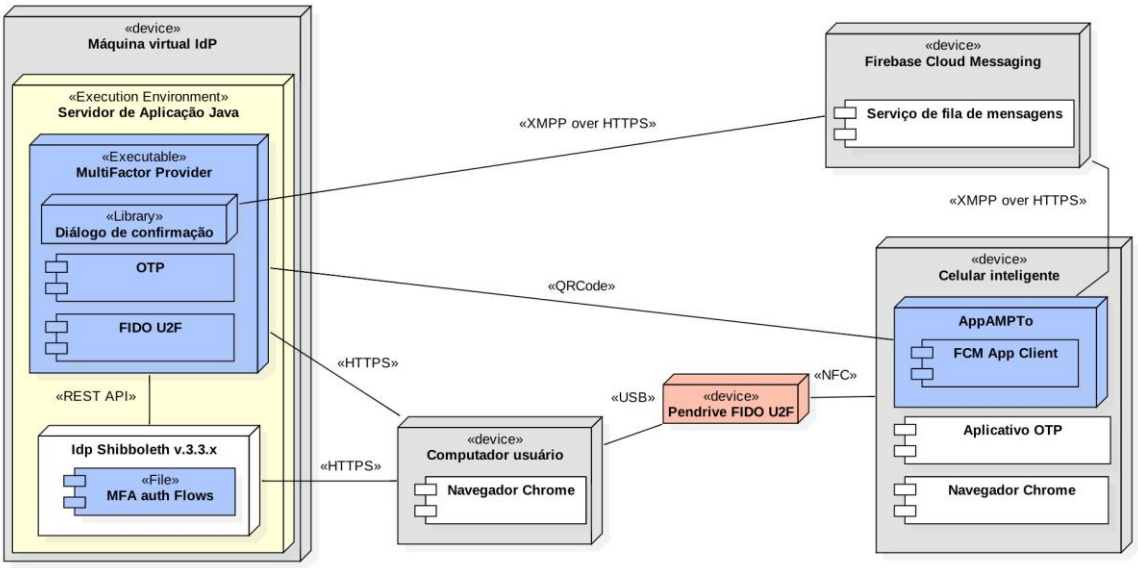

Figura 2: Diagrama de implantação para o piloto na Fase 2

A Figura 2 apresenta o cenário a ser desenvolvido na fase de piloto. Para o cenário com senhas descartáveis (OTP), será desenvolvido um módulo específico no MFaP e verificado se haverá necessidade de adicionar ou modificar os fluxos de autenticação (Auth Flows) que já foram implementados no protótipo da Fase 1. Para este cenário, partimos do pressuposto que o usuário já tem um aplicativo em seu celular para gestão das senhas descartáveis (OTP) [M'Raihi et al., 2011], como por exemplo, *Google Authenticator* ou Authy[2].

Para o cenário com FIDO U2F [Srinivas et al., 2014], também haverá o desenvolvimento de um módulo específico no MFaP, bem como a verificação sobre a necessidade de adicionar ou alterar os fluxos de autenticação no IdP. Neste cenário, como requisito, o usuário deverá acessar a página de autenticação do IdP por meio de um navegador *web* que tenha suporte ao FIDO U2F API ou a nova API de autenticação robusta chamada de *Web Authentication*[3]. No momento da escrita dessa proposta, os seguintes navegadores atendem a este requisito: Google Chrome, Mozilla Firefox e Opera. Este cenário tem como premissa que cada usuário deverá possuir um *token* físico U2F (*pendrive*) e o mesmo poderá ser usado no computador por meio de uma porta USB. Contudo, essa solução ainda assim estaria adequada para usuários que só possuem o celular como dispositivo de acesso ao IdP. Nesse caso, o pendrive FIDO U2F poderia se comunicar com o celular por meio de NFC ou *bluetooth* [Alliance, 2015].

Na fase de protótipo, o cenário com **Diálogo de confirmação** foi implementado para telefones com o sistema operacional Android. Para o piloto, pretende-se evoluir o aplicativo Android, agregando novas funcionalidades, além do desenvolvimento de um aplicativo específico para o sistema operacional iOS. Sendo assim, o cenário com Diálogo de Confirmação estará adequado para os dois principais sistemas operacionais embarcados nos telefones inteligentes, que segundo a Gartner[4], detinham 99,2% da participação no mercado em 2017 (Android - 84,8% e iOS - 14.4%).

Para o piloto, pretende-se implementar todos os componentes apresentados na Figura 2 em provedores de identidade das instituições parceiras. Como pode ser observado na Figura 1, a interação entre MFaP e IdP se dá por meio de uma API REST (*Web Service*) e por fluxos de autenticação nativos do IdP, que na prática são arquivos de configuração XML. Ou seja, a solução desenvolvida possui baixo acoplamento com o IdP, evitando assim amarras que dificultariam a evolução e manutenção do IdP ou MFaP.

[2] https://authy.com/

[3] https://www.w3.org/TR/webauthn

[4] https://www.gartner.com/newsroom/id/3859963

Todos os componentes de software já desenvolvidos na fase de protótipo e aqueles que serão desenvolvidos na fase piloto, estão sobre licenças de software livre ou código aberto. Ou seja, a solução proposta não requer o pagamento de licenças ou *royalties* e pode ser usada pelos provedores de identidade de forma gratuita.

Como mencionado anteriormente, o segundo cenário de uso considerado pelo GT explorou, na fase de protótipo, a especificação do FIDO UAF como único mecanismo de autenticação federada. Este cenário considerou a transposição das credenciais do usuário paro mundo físico, como fonte de atributos para a avaliação de políticas de controle de acesso baseada em atributos (ABAC). Para tal, foi definida uma arquitetura para o desenvolvimento de soluções IoT com controle de acesso através de um protótipo de fechadura inteligente que explora as características de segurança das tecnologias NFC e FIDO.

Para a segunda fase, pretende-se evoluir a solução desenvolvida baseada na arquitetura apresentada na Figura 3. Nesta figura, demos ênfase ao desenvolvimento da solução empregando FIDO UAF, de forma que os outros mecanismos de autenticação suportados pelo *MultiFactor Provider* estão sendo abstraídos (representados pelo estereótipo *Library* no componente *Diálogo de confirmação*).

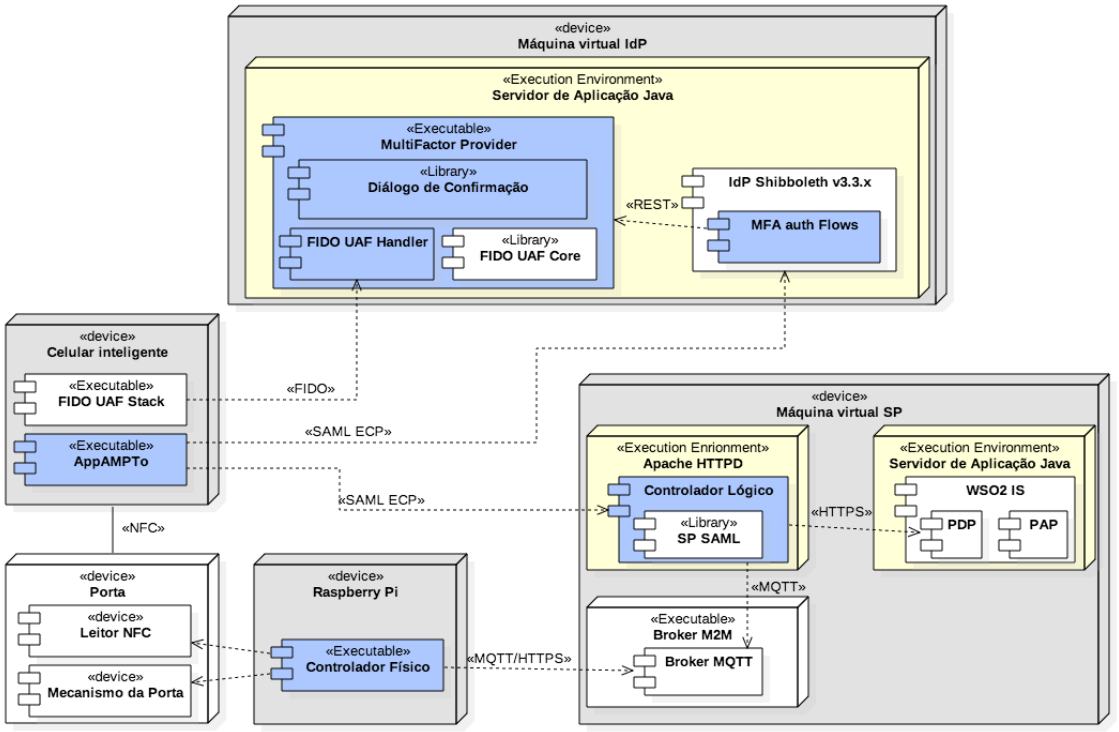

Figura 3: Diagrama de implantação para o cenário de controle de acesso físico na fase 2.

O exemplo considerado nesta arquitetura é o de uma porta inteligente. A porta possui um leitor NFC e um mecanismo de trava elétrica solenoide, ambos conectados a um *Controlador Físico*, que neste exemplo, consiste em um Raspberry Pi. É importante mencionar que o Raspberry Pi pode ser substituído por uma plataforma micro-controlada, como o Arduino. O papel do *Controlador Físico* é atuar como *gateway* para dispositivos IoT com baixo poder de processamento, permitindo a utilização de protocolos M2M (*Machine-to-Machine*) para a comunicação com um servidor que hospeda o provedor de serviço (SP).

O principal componente do SP é o *Controlador Lógico*, responsável pelo gerenciamento dos diversos dispositivos, incluindo uma implementação do SAML para permitir o uso de autenticação federada. Para suportar a definição de políticas de controle de acesso, foi seguida uma arquitetura nos quais os componentes responsáveis pelos mecanismos de autorização são externalizados da aplicação sendo protegida, através da noção de servidor de autorização. Deste modo, o *Controlador Lógico* também atua como *PEP* (*Policy Enforcement Point*), consultado o *PDP* (*Policy Decision Point*) do WSO2 Identity Server (IS) para decisões de autorização baseada em políticas de controle de acesso. O WSO2 IS é uma solução aberta

para serviços de autorização, mantida por uma empresa que oferece serviços pagos relacionados a este produto. O *PAP* representa a interface para gerenciamento e especificação de políticas de controle de acesso ABAC oferecida pelo WSO2 IS. Uma vez que se utiliza uma arquitetura modularizada para os mecanismos de autorização, a solução de autorização baseada em atributos da CAFe pode ser facilmente substituída por uma solução já existente na instituição onde será implantada.

No tocante a arquitetura de suporte a IoT, nossa proposta é de utilizar um *broker* que suporte protocolos M2M (*Machine-to-Machine*) como o MQTT. Um opção para tal são os componentes da plataforma Fiware. O Fiware é uma plataforma para o desenvolvimento de soluções inteligentes baseado em um conjunto de especificações e implementações de referência. Apesar de ser uma plataforma com diversas funcionalidades, cada componente Fiware pode ser utilizado de maneira independente. Os componentes Fiware oferecem uma API bem definida de acordo com uma especificação padrão (sempre utilizando protocolos da indústria). Deste modo, o componente *IDAS* é um candidato a *broker* para protocolos M2M como MQTT e CoAP. Nossa proposta é que o uso destes componentes permita ao *Controlador Lógico* abstrair detalhes de protocolos de comunicação com dispositivos IoT, ao mesmo tempo em que baseamos nossa solução em protocolos utilizados pela indústria. Opcionalmente, é possível substituir os componentes Fiware por outros produtos disponíveis no mercado que também suportam os protocolos mencionados, como o Mosquitto[5].

2.2. Instituições participantes

Para a condução desse piloto seria interessante contar com instituições que fazem de seu IdP como solução de autenticação centralizada para seus sistemas internos ou que seus usuário sejam frequentes utilizadores de provedores de serviço na CAFe, como por exemplo, do portal de periódico CAPES.

A Universidade Federal do Rio Grande Sul (UFRGS) é um bom exemplo de instituição que faz uso de seu provedor de identidade *Shibboleth* como solução de autenticação centralizada para seus sistemas internos. A participação da UFRGS seria interessante devido a diversidade de usuários que poderiam testar a solução, algo desejável para um piloto. Outro fato relevante é que o analista de TI da UFRGS, Rui Ribeiro, atua ativamente junto à RNP para manutenção e evolução da federação CAFe.

A Rede Nacional de Ensino e Pesquisa (RNP) também seria um boa candidata para participar do piloto, tendo em vista que alguns de seus funcionários fazem uso da autenticação no IdP Shibboleth para acessar serviços federados, como o serviço de conferência *web* MConf[6].

A Universidade do Vale do Itajaí (UNIVALI) é uma instituição cliente da CAFe é tem interesse de participar da fase de piloto deste GT. A Universidade Federal de Juiz de Fora é outro exemplo de instituição que poderia ser envolvida nos testes com o piloto. O professor Edelberto Franco Silva possui ampla experiência em federação de identidades e controle de acesso, de forma que o piloto poderia ser implantado no contexto do grupo de pesquisa do professor Edelberto.

Qualquer outra instituição que possua um provedor de identidade na CAFe também poderia ser uma candidata a participar do piloto. Contudo, o pouco número de provedores de serviços na CAFe, pode resultar em um pequeno número de usuários que efetivamente participarão do piloto.

Para essa fase de piloto espera-se que as instituições parceiras possam ajudar a testar e validar a autenticação com segundo fator, bem como a gestão do ciclo de vida desses fatores extras de autenticação. Entre os testes, poderia ser verificado o comportamento da solução em um cenário com vários usuários se autenticando ao mesmo tempo; a usabilidade das páginas de configuração e ativação do segundo fator junto ao IdP, bem

[5] https://mosquitto.org/

[6] https://conferenciaweb.rnp.br

como dos aplicativos móveis para Android e iOS. Além disso, pretendemos também utilizar as próprias instituições da equipe do GT para fins de teste e validação do piloto.

2.3. Objetivos e evoluções

A Figura 2 apresenta os componentes que serão desenvolvidos na fase de piloto para o cenário de autenticação multi-fator. Pretende-se realizar as seguintes evoluções:

- **Gerência de todo o ciclo de vida do segundo fator**
  - No protótipo, preocupou-se apenas em permitir cadastrar e ativar o segundo fator para os usuários de um IdP. Contudo, para que a solução possa ser de fato colocada em produção é necessário conceber uma solução que permita aos usuários: cadastrar, ativar, desativar, renovar e revogar o segundo fator. Nessa fase de piloto, será desenvolvida uma solução para gerenciar esse ciclo de vida.
- **Multi-Factor Provider (MFaP)**
  - **Página *web* para ativar segundo fator** – Na fase de protótipo, preocupou-se em ter uma página que fosse possível cadastrar e ativar o segundo fator. Na fase de piloto, essa página será totalmente refatorada para atender os seguintes requisitos: (1) interface mais intuitiva e integrada com a página do provedor de identidade. Dessa forma, espera-se que o administrador de IdP, que queira implantar o MFaP, não tenha que se preocupar com a personalização dessa página para adequar com a identidade visual de sua instituição; (2) apresentar todos os fatores extras de autenticação que foram habilitados pelo administrador o IdP, como diálogo de confirmação, OTP e FIDO U2F.
  - **Refatorar interface para ser implementada para cada fator extra de autenticação** – Criar uma interface de software que possa ser implementada para cada fator extra de autenticação. Dessa forma, a solução permitirá que novos fatores extras de autenticação sejam acrescentados futuramente no MFaP. Por exemplo, apesar de não propormos o SMS como um fator extra de autenticação, o administrador de um IdP poderia implementar essa interface genérica para oferecer esse fator para seus usuário;
  - **Senhas descartáveis (OTP)** – implementar interface para permitir que o OTP seja usado como fator extra de autenticação;
  - **FIDO U2F** – implementar interface para permitir que o FIDO U2F (*pendrive*) seja usado como fator extra de autenticação;
  - **Refatorar camada de persistência de dados** – Na fase de protótipo, as informações adicionais sobre o segundo de fator de cada usuário foram persistidas em um banco não relacional. Para a fase de piloto, pretende-se desenvolver um conjunto de interfaces para persistência para permitir o uso de banco de dados relacionais, não relacionais e até mesmo serviço de diretórios, como o LDAP.
- **Fluxos de autenticação**
  - Evoluir ou adicionar nos fluxos de autenticação (arquivos XML) para permitir o uso de senhas descartáveis e FIDO U2F como fatores extras de autenticação.
- **Aplicativo para telefones com Android**
  - Adicionar funcionalidades no aplicativo, desenvolvido na fase de protótipo, para permitir que o usuário possa ter um maior gerência sobre os fatores extras de sua conta, diminuindo a dependência da página *web* do MFaP para realizar tais ações;

  - Agregar mais informações na notificação com pedido de autenticação na solução de Diálogo de Confirmação. Por exemplo, adicionar o nome do provedor de serviço, do provedor de identidade, endereço IP do computador onde o usuário se autenticou com o primeiro fator, etc.

- **Aplicativo para relógios com Wear OS**
  - Na Fase 1, foi solicitado a compra de relógios inteligentes com Android Wear, agora recentemente rebatizado de Wear OS. Contudo, os equipamentos chegaram tardiamente e não foi possível explorá-los da forma que estava planejada. Para o piloto, pretende-se desenvolver um aplicativo para relógio com Wear OS e que esteja integrado com o telefone, Android ou iOS, para permitir o uso do Diálogo de Confirmação.

- **Aplicativo para telefones com iOS**
  - Devido as limitações orçamentárias e de tempo, na fase de protótipo, só foi possível desenvolver um aplicativo para Android. Esse foi suficiente para validar a solução. Na fase de piloto, pretende-se também desenvolver um aplicativo para o iOS. Dessa forma, a solução aqui proposta estará adequada para mais de 99% dos usuários que possuem um telefone inteligente.

A Figura 3 apresenta a proposta de arquitetura para o cenário de controle de acesso físico com IoT.
Neste contexto, pretende-se realizar as seguintes atividades:

- **Gerenciamento do ciclo de vida de dispositivos IoT**
  - Durante a fase de protótipo, considerou-se a existência de somente uma porta sendo controlada pela solução desenvolvida. Entretanto, se faz necessário evoluir o *Controlador Lógico* para considerar atividades relacionadas ao gerenciamento dos dispositivos IoT permitindo, por exemplo, o cadastro de novas portas a serem gerenciadas.

- **Registro de atividades (*logging*)**
  - Uma solução de controle de acesso precisa incluir mecanismos de registros (*logging*) para fins de auditoria. Adicionalmente, tais mecanismos podem ser utilizados para alimentar um *Security Information and Event Management* (SIEM), que por ventura esteja instalado na instituição.

- **Gerenciamento de políticas de acesso**
  - Enquanto que a definição e gerenciamento de políticas de controle de acesso devem ser questões decididas por cada instituição, é importante demonstrar como tais funcionalidades podem ser alcançadas.

- **MVP de fechadura inteligente baseada nas tecnologias exploradas**
  - O mecanismo de controle de uma porta inteligente proposto pelo GT emprega tecnologias de ponta, que não são encontradas em produtos disponíveis no mercado. Deste modo, pretende-se desenhar um MVP para fechadura inteligente com o objetivo de se ter um produto para apresentar a alguma empresa da área.

3. Modelo de negócios proposto para o piloto

Como mencionado anteriormente, o GT vem atuando em dois cenários de uso: autenticação multifator em provedores de identidade Shibboleth e controle de acesso físico, demonstrando a transposição de autenticação federada para IoT. Deste modo, apresentamos a seguir dois modelos Canvas, um para cada cenário.

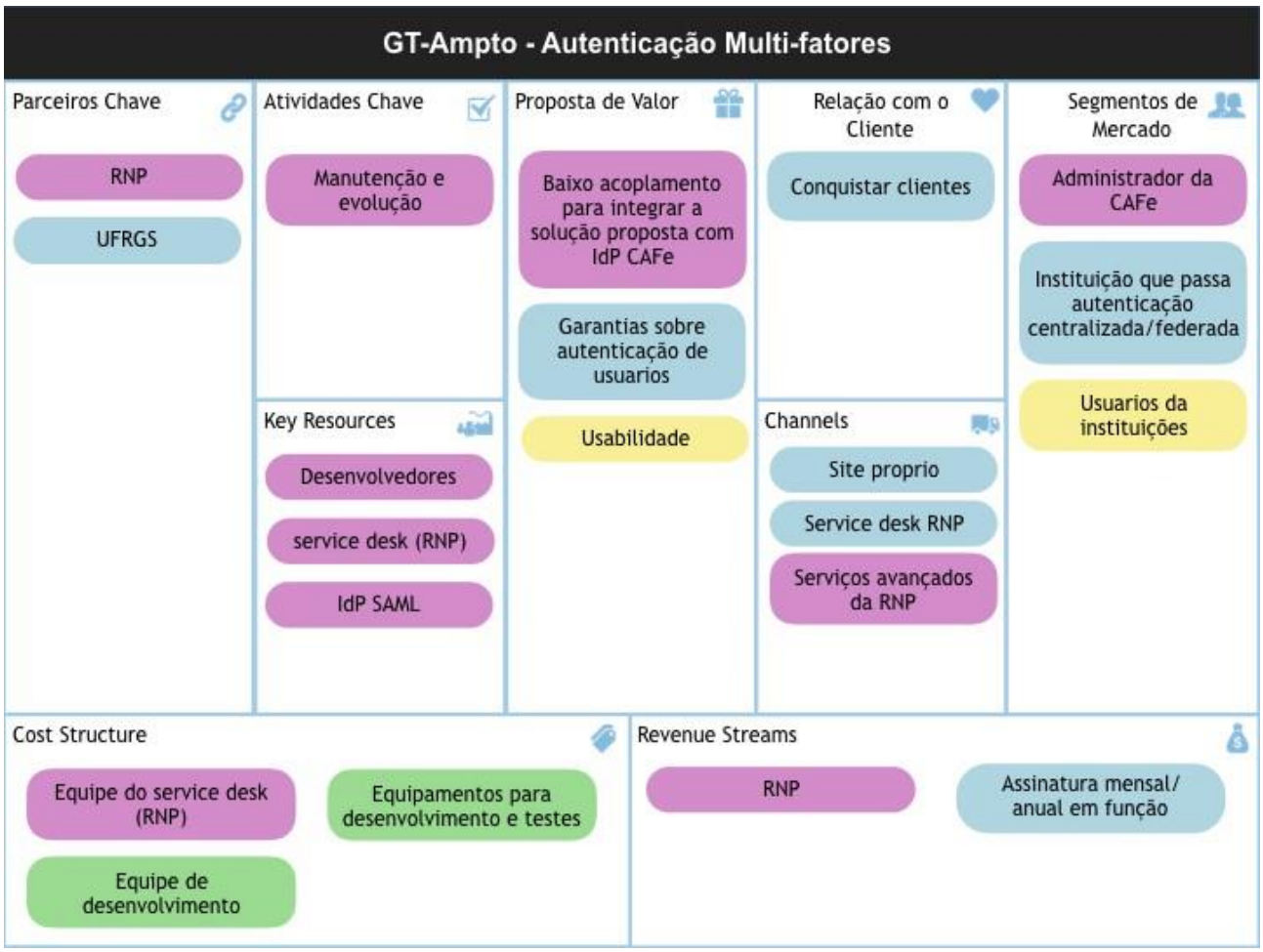

Figura 4: Canvas para o produto que agrega autenticação nos provedores de identidade na CAFe

O resultado deste grupo de trabalho pode ser entendido como uma nova funcionalidade a ser adicionada nos provedores de identidade da Comunidade Acadêmica Federada (CAFe) que é mantida pela RNP. Como consequência, esse produto poderia ser entregue pela RNP para todas suas instituições clientes.

Na Figura 4 é apresentada a modelagem do negócio no formato de canvas. No **segmento de mercado (*Customer Segments*)**, entendeu-se que a solução aqui proposta poderia interessar a RNP, como mantenedora da CAFe; as instituições que fazem uso de modelo de autenticação centralizada, mesmo não usufruindo do modelo federado; e os usuários das instituições que participam da CAFe.

A **proposta de valor (*Value Propositions*)** da solução está fundamentada em possuir um baixo acoplamento com IdP. Essa característica visou garantir que a solução pudesse ser instalada facilmente nos IdPs que já estão em operação, além de possibilitar atualizações futuras, seja do IdP ou da solução aqui desenvolvida. Para as instituições a solução proposta ainda agregará valor em seus sistemas, pois oferecerá um maior nível de certeza sobre as autenticações de seus usuários. Ou seja, a solução poderá minimizar problemas com ataques de força bruta para descoberta de senha (eficaz com senhas consideradas fracas) e *phishing*. Por fim, do ponto de vista do usuário dessas instituições, colocamos a usabilidade como proposta de valor, pois a solução aumenta a robustez do processo de autenticação de uma forma não tão complexa e que seria adequada até mesmo para usuários não tão avançados.

Para os **canais de relacionamento (*Channels*)**, considerou-se como clientes as instituições que possuem um provedor de identidade na CAFe, ou mesmo que fazem uso do modelo de autenticação centralizada fundamentado sobre o SAML. Dessa forma, imaginamos que a forma de divulgar o produto seria por meio da própria RNP, em seu portfólio de serviços avançados, podendo esse produto ser visto como um

componente opcional para aquelas instituições que estão ou querem ingressar na CAFe. Considerou-se também manter um *site* próprio para que outras instituições possam conhecer e até mesmo experimentar o produto. Por fim, imaginou-se que o *service desk* da RNP seria o ponto de interação para os clientes que estão fazendo uso da solução e precisam de algum tipo de apoio.

Na **relação com o cliente *Customer Relationship*)**, entendeu-se que a solução irá conquistar clientes, fazendo com que aqueles que já implantaram a solução, continuem gostando de ter a solução e fazendo com que aqueles que ainda não tenham implantado, sintam interesse em conhecer. Para tal, imaginou-se para a fase de divulgação a participação em *workshops* voltados para gerentes de TI (i.e. FORUM RNP), divulgação em listas de e-mail de gestores de TI de Universidades e Institutos. Para a fase de atendimento, o *service desk* com um acordo de nível de serviço (*Service Level Agreement* – SLA) que possua um tempo adequado para a característica crítica do serviço.

Como **fontes de receita (*Revenue Streams*)**, considerou-se a RNP, pois a mesma poderia ser responsável por manter o serviço para suas instituições usuárias, como já o faz para a própria federação CAFe. Contudo, imaginou-se que a solução poderia ser usada por instituições que não fazem parte da CAFe. Sendo assim, considerou-se um modelo de assinatura mensal em função do número de usuários que serão beneficiados pela solução.

Para os **recursos chave (*Key Resources*)** da solução, considerou-se IdP SAML, pois a solução foi feita exclusivamente para essa tecnologia. Desenvolvedores são fundamentais para o lançamento do produto e para sua manutenção e evolução. O *service desk* da RNP como principal canal de relacionamento com os clientes, situando-o como nível 1 de suporte. Isso ajudaria minimizar a interrupção da equipe de desenvolvimento com pedidos de suporte, podendo assim manter uma pequena equipe de desenvolvimento.

A **atividade chave (*Key Activities*)** do modelo está na manutenção e evolução da solução. É importante manter uma frente de prospecção de novas tecnologias que poderiam ser usadas como fatores extras de autenticação, além de garantir que a solução continue funcionando mesmo diante de atualizações de softwares de terceiros, como do provedor de identidade *Shibboleth*, especificações SAML, navegadores *web*, etc.

Para os **parceiros chave (*Key Partnerships*)** considerou-se uma parceira entre comprador e fornecedor. RNP e instituições com IdP são possíveis compradores da solução e poderiam ajudar na concepção ou mesmo evolução da solução.

Por fim, a **estrutura de custos (*Cost Structure*)** da solução é composta pela aquisição de equipamentos para desenvolvimento e testes (i.e. telefones de diferentes marcas, pendrive FIDO U2F, etc.), pagamento da equipe de desenvolvimento e o custo implícito do *service desk* da RNP. Imagina-se aqui que não será preciso ter uma infraestrutura própria de TI, mesmo que terceirizada, para oferta da solução, tampouco fazer ações de *marketing* para venda.

De forma a englobar os dois cenários sendo considerados pelo GT, foi feito um modelo Canvas considerando o cenário de controle de acesso físico, apresentado na Figura 5.

Sobre o **segmento de mercado (*Customer Segments*)**, a solução proposta tem potencial para alcançar diversos segmentos de mercado, indo desde instituições participantes da comunidade acadêmica federada, incluindo casos específico de controle de acesso em ambiente universitário como controle em restaurantes universitários, acesso a laboratórios (por motivos diversos), e controle de acesso em prédios públicos (principalmente fora do horário comercial). Adicionalmente, vislumbramos a possibilidade de uso da solução vinculada a identidades estudantis (como compra de entradas em cinemas ou teatros com desconto para estudantes) e em situações que exijam um controle de acesso físico mais rigoroso como acesso a arsenal de armamentos em empresas de vigilância, ou até mesmo em órgãos de segurança pública.

A principal **proposta de valor (*Value Propositions*)** da solução de controle de acesso físico é o fato de não existir no mercado hoje uma solução com o nível de segurança garantido pelas tecno-

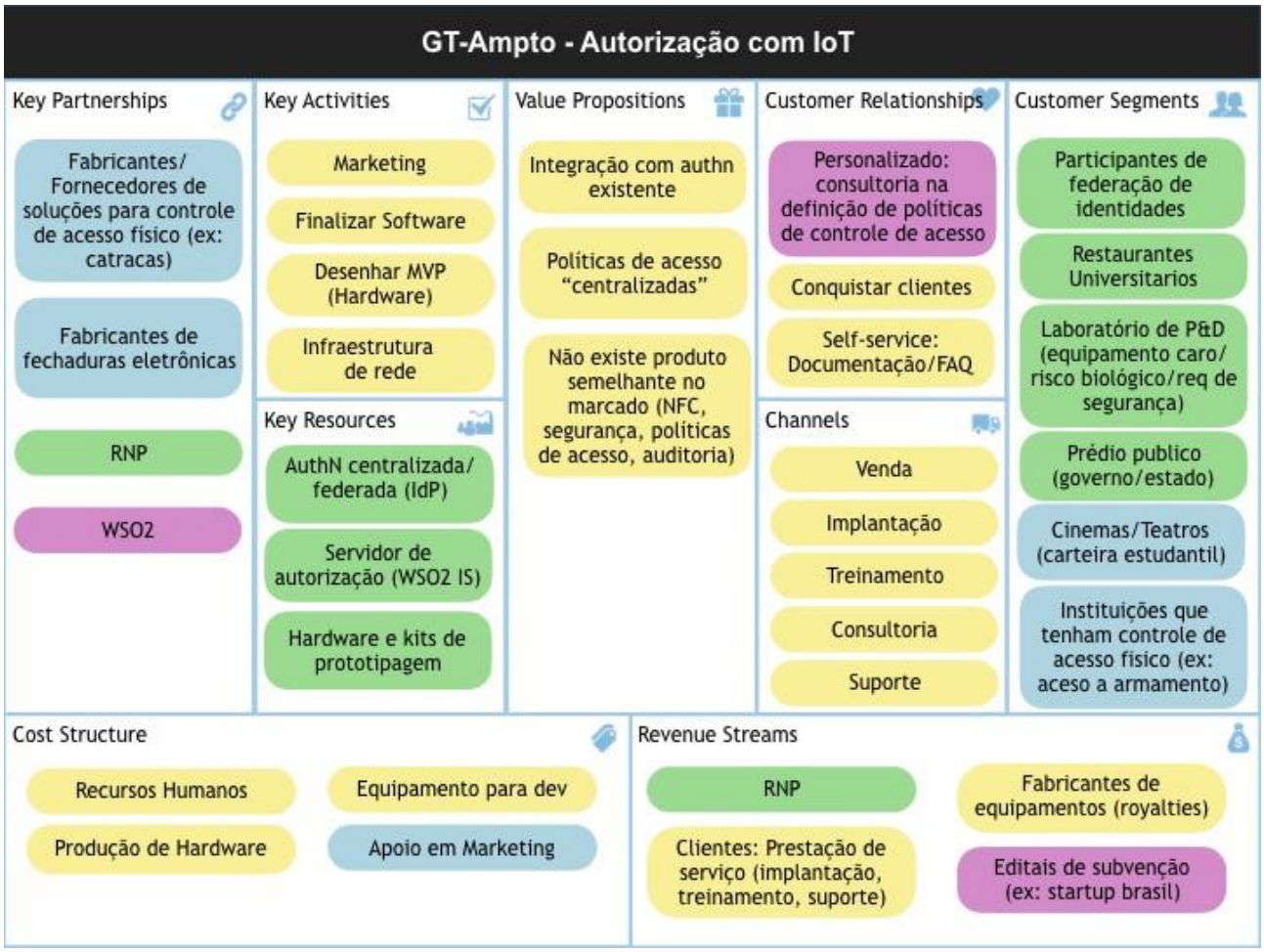

Figura 5: Canvas para o produto de controle de acesso físico.

logias exploradas por este GT. O uso de NFC, em conjunto com protocolos FIDO, no contexto de autenticação e autorização traz um nível de garantia (*Level of Assurance* - LoA) a mais do que as soluções tradicionais baseadas em RFID e listas de controle de acesso. Outra proposta de valor é o fato da solução ser facilmente integrada com a infraestrutura de autenticação existente na instituição destino. Além disso, o uso de um mecanismo centralizado para a definição de políticas de controle de acesso que pode ser aplicadas em diversos pontos de aplicação (por exemplo, um único console para gerenciar as políticas de acesso de todas as portas de um departamento), ao invés de ser necessário configurar cada porta individualmente (como são as soluções mais populares hoje em dia).

Os **canais de relacionamento (*Channels*)** para a solução de controle de acesso incluem canais de vendas e a prestação de serviços como implantação, treinamentos, suporte e consultorias para a definição de políticas de controle de acesso.

O **relacionamento com o cliente *Customer Relationship*)** tem como foco principal a conquista de novos clientes, adotando duas categorias de relacionamento: uma abordagem personalizada na forma de consultorias para a definição de políticas de acesso que se adequem ao ambiente do cliente; e a exploração de *self-service* através de documentação técnica que pode ser utilizada pelos administradores e operadores de infraestrutura da instituição cliente.

A **principal fonte de receita (*Revenue Streams*)** durante as fases iniciais consiste na RNP através do seu programa de P&D, apoiando a prospecção de novas tecnologias e o desenvolvimento de soluções inovadoras.

Vislumbramos duas fontes vinculadas aos clientes diretos da solução, através de vendas e prestação de serviços, e dos fabricantes de equipamento que produziriam a solução de hardware em larga escala. Adicionalmente, vemos também a possibilidade de participar em editais de subvenção do governo (como o programa *startup* brasil e outros similares).

Dentre os **recursos chaves (*Key Resources*)** para o desenvolvimento da solução temos a necessidade de um mecanismos de autenticação centralizada (ou federada), e de um servidor de autorização. Adicionalmente, também é necessário a disponibilidade de hardwares e kits para prototipagem rápida, tais como ambientes de desenvolvimento baseado em micro-controladores, leitores NFC, fechaduras elétricas ou eletro-mecânicas, entre outros.

As **atividades chaves (*Key Activities*)** identificadas neste momento incluem um esforço de desenvolvimento para finalização do software da solução, o desenho de um MVP para o hardware proposto, assim como esforço de infraestrutura de rede para montar o ambiente de desenvolvimento/implantação. Identificamos também a necessidade de uma atividade de marketing de forma a auxiliar na elaboração de demonstrações e de uma estratégia para aproximação de clientes potenciais.

Os **parceiros chaves (*Key Partnerships*)** para esta solução inclui RNP, fornecendo o apoio para a etapa de desenvolvimento da solução. Também vislumbramos fabricantes de fechaduras eletrônicas e de soluções de controle de acesso físico (como catracas) como possíveis parceiros, principalmente na fase de produção da solução de hardware. As instituições participantes do piloto fornecerão um apoio fundamental ao realizarem os primeiros testes com a solução. Adicionalmente, a WSO2 pode vir a se tornar um parceiro baseado nos serviços oferecidos na area de servidores de gestão de identidades e de autorização.

A **estrutura de custo (*Cost Structure*)** é composta majoritariamente de recursos humanos, principalmente ,desenvolvedores de software e hardware. Vislumbramos também um custo associado à produção do hardware proposto pelo GT, o que se relaciona também com a necessidade de equipamentos para desenvolvimento da solução. Adicionalmente, consideramos que existirá um custo associado com as atividade relacionadas a marketing.

4. Aproveitamento dos resultados do piloto

Como resultado do piloto espera-se ter um componente de *software* que possa ser acoplado junto ao provedor de identidade, agregando a esse último a possibilidade de autenticar seus usuários com mais de um fator. Esse componente poderá ser incluído pela RNP em sua máquina virtual padrão de Provedor de Identidade. Dessa forma, toda nova instituição, ao ingressar na CAFe, já poderá usufruir do resultado desse piloto. As instituições que já possuem um provedor de identidade Shibboleth, podendo esse estar na CAFe ou não, poderiam baixar esse componente isolado e fazer a instalação do mesmo.

Na concepção do piloto, imaginou-se que nas lojas de aplicativos *Google Play* e *Apple Store* haverá um único aplicativo o qual poderá ser usado por qualquer usuário de qualquer instituição pertencente a CAFe. Esse aplicativo seria assim mantido, por exemplo, pela RNP e evitaria que as instituições clientes precisassem manter e evoluir um aplicativo para dispositivos móveis, algo que pode ser custoso. Contudo, se a instituição possuir uma equipe de desenvolvimento, essa terá a possibilidade de pegar o aplicativo resultante desse piloto para fazer suas personalizações e evoluções, cabendo a essa instituição publicar seu aplicativo nas lojas *Google Play* e *Apple Store*.

No tocante ao cenário de controle de acesso físico, espera-se que o MVP de uma tranca de porta inteligente, e um sistema de software para seu gerenciamento, que sirva como base para o uso em diversos cenários. Dentre os cenários vislumbrados para a fase piloto, consideramos a instalação do equipamento para controlar acesso a laboratórios de pesquisa, utilizando-se da federação CAFe como fonte de autenticação e atributos. Adicionalmente, a tecnologia desenvolvida pode servir de base para outros usos dentro do

ambiente universitário (por exemplo, controle de acesso a restaurante universitário), vinculado à identidade estudantil, ou até mesmo como base para sistemas de ponto eletrônico. Além disso, o software desenvolvido poderá ser explorado pela RNP como um cliente da plataforma Fiware.

5. Macro cronograma de desenvolvimento do piloto

Macro atividades		1º Trim.			2º Trim.			3º Trim.			4º Trim.		
		1	2	3	4	5	6	7	8	9	10	11	12
		05/18	06/18	07/18	08/18	09/18	10/18	11/18	12/18	01/19	02/19	03/19	04/19
Entregas pré-definidas pela RNP	Relatórios	**RP5 RP6 RP7**	**RT4 RT5**	**RA5**		**RP7**	**RA6**			**RA7 RT6 RT7**		**RP8**	**RA8**
	(**E1**) Início da implantação do piloto			**E1**									
	(**E2**) Entrega de documentação e código fonte				**E2**								
	(**E3**) Workshop de disseminação							**E3**					
	(**E4**) Apresentação final dos resultados										**E4**		
	(**E5**) Entrega final do código e documentação											**E5**	
(**MA1**) Modelo de gestão de ciclo de vida do segundo fator													
(**MA2**) Refatoramento do código do MFaP													
(**MA3**) Evolução e desenvolvimento de aplicativos para telefones e relógio													
(**MA4**) Testes e Avaliação													
(**MA5**) Documentação e divulgação dos resultados													
(**MA6**) Desenho do MVP da tranca eletrônica													
(**MA7**) Produção do MVP da tranca eletrônica													
(**MA8**) Implantação da tranca eletrônica													
(**MA9**) Modelo de gestão de dispositivos IoT													
(**MA10**) Evolução e desenvolvimento do Controlador Lógico													

As Macro Atividades (MA) listadas estão intimamente relacionadas com os objetivos apresentados na Subseção 2.3. A **MA1** consiste na concepção do modelo de gestão do ciclo de vida dos fatores extras de autenticação. Para a **MA2** entende-se que será evolução do código já desenvolvimento na fase protótipo, o que inclui correções e melhorias que já são conhecidas, além de adicionar novas funcionalidades, como a gestão do ciclo de vida e adição de novos fatores, conforme ilustrado pela Figura 2. A **MA3** compartilha a mesma ideia descrita para a **MA2**, contudo aqui tem-se previsto o desenvolvimento de aplicação completamente nova para o sistema operacional iOS, algo se quer foi previsto na fase de protótipo. Sendo

assim, a **MA3** é a que possui maior risco. De acordo com o cronograma da RNP, a entrega do código fonte deve acontecer em agosto de 2018 (**E2**).

Entendemos que nessa data será uma entrega preliminar, ou seja, ainda haverá desenvolvimento das **MA3** e **MA4**. Para a **MA4**. entende-se que serão realizados os testes de softwares que serão apresentados no **RT5**. Por fim, na **MA5** foram concentradas todas atividades de documentação do projeto.

As Macro Atividades 6 a 10 estão relacionadas com o cenário de controle de acesso físico. A **MA6** envolve o desenho de um MVP para o equipamento de tranca eletrônica, que será então explorado na **MA7** para a produção de algumas unidades do equipamento para implantação (atividade **MA8**) nas instituições parceiras que irão se envolver nos testes com o cenário de controle de acesso físico. A **MA9** corresponde na definição de um modelo para o gerenciamento de dispositivos IoT pela nossa solução. O propósito é permitir a um administrador realizar o cadastro e gerenciamento de outras trancas eletrônicas dentro de sua instituição. Por fim, a **M10** concentra o esforço de desenvolvimento do Controlador Lógico, incluindo a criação de interfaces Web para gerenciamento da solução, questões relacionadas ao registros dos acessos e a incorporação do modelo de gerenciamento de dispositivos definido pela **MA9**. Todas as macro atividades serão sincronizadas com as entregas pré-definidas pela RNP.

6. Recursos para o desenvolvimento do piloto

6.1. Aquisição de equipamentos para o desenvolvimento do piloto

Descrição	**Justificativa**	**Valor Unitário**	**Qtde**	**Valor Total**
Celular iPhone 8	Para desenvolvimento do aplicativo para iOS	R$ 3.999,00	1	R$ 3.999,00
iMac 21” /macBook	Para desenvolvimento do aplicativo para iOS	R$ 13.000,00	1	R$ 13.000,00
Pendrive FIDO U2F	Para testes com FIDO U2F	R$ 240,00	6	R$ 1.440,00
Desktop s/ monitor (Core i7 - 8GB - 500GB)	Para desenvolvimento da solução de controle de acesso	R$ 3.600,00	1	R$ 3.600,00
Mini Trava Elétrica Solenóide	Para desenvolvimento da tranca eletrônica	R$ 34,90	3	R$ 104,70
Kit Módulo Leitor NFC PN532	Para desenvolvimento da tranca eletrônica	R$129,90	3	R$ 389,70
Placa Wemos D1 R2 Wifi ESP8266	Para desenvolvimento da tranca eletrônica	R$ 49,90	1	R$ 49,90
Módulo WiFi ESP8266 NodeMcu ESP-12	Para desenvolvimento da tranca eletrônica	R$ 42,90	1	R$ 42,90
Kit Raspberry Pi Start	Para desenvolvimento da tranca eletrônica	R$ 339,90	2	R$ 679,80
Fonte DC Chaveada 12V 5A	Para desenvolvimento da tranca eletrônica	R$ 59,90	3	R$ 179,70
Módulo Relé 5V 1 Ca-nal	Para desenvolvimento da tranca eletrônica	R$ 8,90	3	R$ 26,70
Total				R$ 23.512,40

6.2. Recursos oferecidos pela RNP para execução do piloto

Recurso	Especificação	Justificativa	Qtde
IdP no GIdLab	IdP Shibboleth v3.3.x com as especificações padrões do GIdLab	Será reservado um IdP para cada instituição participante e mais 2 IdPs para atividades de desenvolvido do GT	4
SP no GIdLab	SP Shibboleth com as especificações padrões do GIdLab	Será reservado um SP para cada instituição participante e mais 2 SPs para atividades de desenvolvido do GT	4

Referências

[Alliance, 2015] Alliance, F. (2015). Bluetooth & nfc transport for fido u2f.

[Haller et al., 1998] Haller, N., Metz, C., Nesser, P., and Straw, M. (1998). Rfc 2289: A one-time password system. Technical report, Technical report, IETF.

[Jøsang et al., 2005] Jøsang, A., Fabre, J., Hay, B., Dalziel, J., and Pope, S. (2005). Trust requirements in identity management. In *Australasian workshop on Grid computing and e-research (CRPIT'44)*, pages 99–108, Darlinghurst, Australia. Australian Computer Society, Inc.

[Machani et al., 2014] Machani, S., Philpott, R., Srinivas, S., Kemp, J., and Hodges, J. (2014). Fido uaf architectural overview. *FIDO Alliance, December*.

[M'Raihi et al., 2011] M'Raihi, D., Machani, S., Pei, M., and Rydell, J. (2011). Totp: Time-based one-time password algorithm. RFC 6238, RFC Editor. http://www.rfc-editor.org/rfc/rfc6238.txt.

[Srinivas et al., 2014] Srinivas, S., Balfanz, D., and Tiffany, E. (2014). Fido universal 2nd factor (u2f) overview. *Version v1. 0-rd-20140209, FIDO Alliance, February*.