Multipass: Autenticação Mútua em Cenários Heterogéneos

Rui Ferreira[1], André Tomás[1], Pedro Estima[1], Rui Aguiar[1], Ricardo Azevedo[2]

[1]Instituto de Telecomunicações
[2]PT Inovação

***Resumo*— A utilização de dispositivos móveis como dispositivos computacionais de uso geral é uma tendência crescente, com especial enfase para o mercado dos Smartphones. Esta tendência levou ao aparecimento de serviços que exploram o uso de dispositivos móveis como mecanismos de autenticação do utilizador, ou mesmo como mecanismo de pagamento de transações.**

Este artigo descreve a arquitetura e implementação que foram desenvolvidas para suportar os cenários de autenticação do projeto Multipass2 que visa explorar o uso de dispositivos móveis como mecanismos de autenticação do utilizador, num cenário multi-canal. Um dos objetivos primordiais é a garantia de mecanismos de autenticação mútua entre o utilizador e o serviço, num cenário heterogéneo em que as tecnologias de rede IP (Wifi ou 3G) se misturam com tecnologias de comunicação em proximidade (Bluetooth, NFC). O artigo apresenta ainda a implementação desenvolvida como prova de conceito e os resultados obtidos no decorrer do projeto.

***Palavras Chave*— Segurança, Gestão de Identidades, Android, Autenticação**

I. INTRODUÇÃO

OS dispositivos móveis têm vindo a desempenhar um papel cada vez mais preponderante como ferramentas do dia-a-dia cujo propósito vai muito para além de simples dispositivos de comunicação. Esta utilização tem sido explorada pelos Smartphones, que dispõem de recursos computacionais consideráveis, várias tecnologias de comunicação (3G, Wifi, Bluetooth) e que executam aplicações que se afastam dos tradicionais serviços providenciados sobre telefones móveis.

Esta tendência ganha novos contornos quando se considera que estes dispositivos podem substituir completamente as carteiras e chaves tradicionais no bolso do utilizador. Um Smartphone pode ser usado como sistema de autenticação do seu portador para abrir portas ou outros sistemas de controlo de acesso, ou ainda como sistema de pagamento de serviços, através de uma carteira digital, como é o caso do Google Wallet.

O projeto Multipass tem como principal objetivo explorar o uso de dispositivos móveis como mecanismo de autenticação do utilizador em ambientes quotidianos com diferentes tipos de serviços e tecnologias de acesso; sendo que se coloca especial enfase nos seguintes quatro aspetos:

1) Assegurar a autenticação mútua, confidencialidade e integridade entre o dispositivo móvel e os serviços com os quais comunica.
2) Operar tanto com base em mecanismos de autenticação com chave pública/privada, assim como com sistemas de gestão de identidades federadas como OpenID[1] e SAML[2].
3) Suportar mecanismos de simplificação de autenticação que suportem autenticação multi-canal.
4) Funcionar em ambientes heterogéneos, recorrendo tanto a tecnologias de comunicação sobre IP (Wifi ou 3G) como comunicação em proximidade (NFC e Bluetooth).

O projeto foca-se em particular em dois cenários distintos. O primeiro cenário, focado em ambientes de domótica ou Internet of Things (IoT) permite que um dispositivo móvel se autentique e interaja de forma segura com outros dispositivos nas suas imediações, e.g. para abrir a porta de uma casa, ou para comandar remotamente outros dispositivos. O segundo cenário envolve a utilização de um terminal público (quiosque), em que o dispositivo móvel é utilizado para autenticar um utilizador junto de um quiosque e autorizar o quiosque a agir em seu nome junto de outros serviços, recorrendo para isso a sistemas de gestão de identidade que garanta a autenticidade de todas as partes envolvidas.

No âmbito do projeto Multipass foi implementado um protótipo para instanciar os cenários do projeto. Este protótipo é composto por três componentes: i) uma aplicação Android que permite ao utilizador fazer a gestão dos tokens de autenticação que transporta consigo e interagir com serviços nas imediações; ii) serviços para gerar e consumir tokens baseados em chave pública/privada; iii) e um mecanismo de autenticação que permite a sistemas de Identity Management (IdM) recorrer a mecanismos multi-canal, mantendo as mensagens de autenticação num canal separado e recorrendo a mecanismos do operador para autenticar o dispositivo móvel.

Este artigo está estruturado da seguinte forma. Na secção II é apresentado o estado de arte relevante, na secção III são descritos os dois cenários que se pretende instanciar. A secção IV apresenta a arquitetura que foi criada para suportar ambos os cenários e na secção V é descrito o protótipo desenvolvido e são discutidos os desafios associados à sua implementação.

Por fim na secção VI são apresentadas as conclusões.

II. Estado da Arte

O uso de telemóveis como mecanismos de autenticação antecede o aparecimento dos Smartphones. São bastante comuns os sistemas de bilhetes eletrónicos enviados por SMS, como é o caso de [3], em que um identificador único é enviado num SMS, armazenado no telemóvel e apresentado no ato de consumo onde é verificado contra uma lista de identificadores válidos. Outros serviços recorrem a soluções semelhantes, diferindo na tecnologia de transporte e formato de armazenamento, por exemplo em [4] é descrito uma solução em que são usados códigos de barras para registar e apresentar os bilhetes e para permitir a leitura automática dos mesmos.

No entanto este tipo de sistemas não protege adequadamente o utilizador/consumidor ,porque o processo de autenticação não garante nem que o dispositivo adquiriu de facto aquele identificador, nem que o serviço é de facto fidedigno. Um ataque contra este tipo de sistemas consistiria em extrair o código único do telemóvel, ou em efetuar um ataque de man-in-middle. No sentido de melhorar a segurança deste tipo de sistemas alguns serviços implementaram mecanismos que autenticam o dispositivo móvel com base em mecanismos criptográficos. Por exemplo [5] fornece um serviço para entrada sem check-in em hotéis, que usa tokens únicos transmitidos na forma de sinal sonoro para abrir fechaduras. Mas mesmo neste caso a autenticação não é mútua, é apenas o terminal móvel, e não o serviço, que é autenticado.

O aparecimento dos Smartphones promove o uso de aplicações especializadas para cada tarefa, pelo que a disponibilidade de ferramentas no dispositivo não é uma limitação. Se considerarmos ainda que estes dispositivos possuem mecanismos de comunicação sem fios como Wifi e Bluetooth, ficam preenchidos os requisitos para implementar protocolos de autenticação nestes dispositivos.

Esforços no sentido de explorar o uso de Smartphones para este propósito têm sido particularmente vincados na área dos pagamentos eletrónicos, onde as iniciativas[6] da Google Wallet e Isis começam a promover este tipo de utilização. Estas iniciativas têm ainda resultado em alterações aos novos dispositivos móveis no mercado (pelo menos dos financiados pelo Google), promovendo a adoção de Near Field Communication (NFC) como mecanismo preferencial de comunicação de curto alcance para este tipo de transações, e adicionando chips para armazenamento seguro (semelhante ao Trusted Platform Module(TPM) ou Smartcard). O operador de telecomunicações desempenha um papel fundamental, que pode ir muito além do simples encaminhamento de bits. Nos tradicionais cenários, em que o dispositivo já tem um SIM Card, do qual o operador é dono, a autenticação pode ser baseada nesse elemento seguro e delegada para o Operador. Esta funcionalidade garante os níveis desejados de segurança, a autenticação é baseada em certificados e não é *phishable*. As garantias são bastante elevadas.

No âmbito do projecto Mutipass, pretende-se preencher algumas das lacunas identificadas anteriormente, providenciando um misto destes mecanismos, estabelecendo como requisito mínimo a necessidade de autenticação mútua – independentemente da tecnologia de transporte em utilização – e suportando tanto soluções análogas às de bilhetes eletrónicos como soluções integradas suportadas pelo operador.

III. Cenários

O projeto Multipass considera dois cenários distintos para efeitos de autenticação do utilizador. O primeiro cenário foca-se em ambientes em que o utilizador carrega no seu telemóvel tokens para se autenticar com dispositivos com os quais poderá interagir; simultaneamente esses tokens são capazes de autenticar também os dispositivos, garantindo assim que está a interagir com serviços que pretende. O segundo cenário implica uma terceira entidade (IdP – Identity Provider) na qual ambos os intervenientes confiam para autenticação das partes envolvidas com base em conhecimento prévio do utilizador e serviços.

A. Domótica e Ambientes Inteligentes

Em Ambientes Inteligentes, tipicamente demonstrados em cenários de domótica, o utilizador interage com múltiplos dispositivos em seu redor. Estas interações são normalmente de curta duração, com baixa complexidade para o utilizador, e com consequências diretas no contexto atual onde o utilizador se encontra.

Em casa são exemplos deste tipo de cenários o uso do telemóvel para a abertura de portas, controlar pequenos dispositivos ou iniciar tarefas comuns no ambiente envolvente, por exemplo, controlar pequenos eletrodomésticos como sistemas de ar-condicionado. Em ambientes empresariais, haverá cenários em que poderá ser usado para marcar presenças, fazer controlo de acesso a espaços, desbloquear o terminal de trabalho ou ativar a máquina do café – podendo depois interagir com sistemas de pagamentos.

Internamente este tipo de cenário pode estar circunscrito a apenas um dispositivo, ou integrado com Gateways especializadas em integração de serviços de domótica. A complexidade é invisível aos olhos do utilizador, facilitando a adoção. O que se pretende neste contexto é fortalecer estas interações, assegurando que o utilizador é sempre autenticado e está a interagir com dispositivos que já conhece.

B. Terminais Públicos

Os sistemas de gestão de identidades, têm como objetivo unificar a identidade do utilizador de forma reduzir o esforço de gestão de credenciais por parte do utilizador, ou orquestrar o uso de múltiplos serviços pelo mesmo utilizador. Estes sistemas permitem ao utilizador e serviços delegar o processo de autenticação noutra entidade. A forte ligação entre telemóvel e os sistemas IdM já fornecidos pelo operador potencia o uso do dispositivo como chave de acesso a sistemas fora da área de influência do utilizador – mas ligados de alguma forma ao operador.

Neste tipo de cenários o dispositivo móvel funciona como mecanismo de acesso a outros serviços, mas delegando o processo de autenticação no sistema de gestão de identidades. Mas de maior interesse no contexto deste projeto é o uso do dispositivo móvel para autenticar o utilizador em serviços que são acedidos a partir de dispositivos que não lhe pertencem. São exemplos disto quiosques públicos para acesso à internet ou outro tipo de terminais dedicados, para utilização pública.

No caso especifico do operador, há uma miríade de dispositivos pertencentes ao operador com os quais o utilizador interage diariamente. São exemplos disto, terminais nas lojas aderentes do operador, boxes televisivas e terminais públicos. Ou seja equipamentos que acedem a serviços do operador em nome do utilizador, para os quais a posse do dispositivo poderia dispensar o uso de credenciais, desde que usado o telemóvel como dispositivo para se autenticar.

IV. Arquitetura

A arquitetura do projeto Multipass suporta dois mecanismos de autenticação distintos. O primeiro faz uso de tokens de autenticação, baseados em criptografia de chave pública que são um conjunto de chaves assinadas por um gerador. O segundo consiste na integração com sistemas de IdM, através de um mecanismo de autenticação adicional, que recorre ao operador para autenticar o telemóvel e o seu portador por forma a iniciar sessões autenticadas noutros dispositivos. Estes dois mecanismos suportam respetivamente os cenários descritos na secções III-A e III-B.

A. Pressupostos

O pressuposto fundamental que suporta esta arquitetura é o uso de mecanismos de comunicação com garantias de confidencialidade (e mediante o cenário, autenticação). Na prática as troca de mensagens iniciadas pelo dispositivo móvel são feitas sobre túneis TLS (independentemente do protocolo de transporte), que se necessário, implementam autenticação com recurso a certificados, e nos permitem estender o sistema com recurso a verificação de certificados numa PKI ou mecanismos de revogação.

Apesar de se tentar garantir a confidencialidade dos dados armazenados (e.g. tokens) durante o processo de transferência, o problema de armazenamento seguro no dispositivo móvel não é abordado, já que consideramos que existem outras soluções de uso geral com este fim, por exemplo envolvendo cifragem do armazenamento ou dispositivos TPM, para proteger os dados do utilizador em caso de perda ou roubo do dispositivo.

B. Autenticação com recursos a tokens

Neste contexto o dispositivo móvel funciona como sistema de armazenamento de tokens do utilizador. Estes tokens são estruturas assinadas criptograficamente que associam as chaves públicas do dispositivo que armazena o token com os certificados do gerador do token, e também dos consumidores que podem autenticar o dispositivo com base no token.

Cada token é composto pelos seguintes campos (Fig. 1):

Fig. 1. Estrutura de um token.

1) B_P: é a chave pública do dispositivo Multipass, à qual corresponde uma chave privada (B_K) disponível apenas no dispositivo. Esta chave (B_K) é usada pelo dispositivo para se autenticar.
2) *Metadata*: é um campo que contém dados adicionais específicos para a aplicação que gerou o token.
3) *E*: é um certificado que pode ser usado pelo dispositivo para autenticar o sistema que consome o token.
4) *V*: é um certificado associado ao sistema de controlo de acesso que gerou o token
5) *Sig(Vk)*: é uma assinatura feita pelo detentor da chave privada correspondente a *V*, ou seja o gerador do token.

O processo de criação de tokens consiste na associação de uma chave pública, armazenada no dispositivo móvel, a um conjunto de metadata fornecido por um gerador de confiança. Não consideramos no entanto mecanismos para estabelecer essa relação de confiança, e assumimos que esta já existe, por intermédio de outros protocolos. Por exemplo no primeiro cenário (secção III-A) assumimos que existe uma associação segura com recurso a Bluetooth que foi estabelecida previamente pelo utilizador, ou que existe outro mecanismo de confiança pré-estabelecido entre o utilizador e o gerador de tokens.

A informação incluída em cada token é suficiente para que todas as partes se autentiquem mutuamente, após a criação do mesmo. O dispositivo móvel usa o certificado *E* incluído no token para verificar se está a entregar o token a um serviço em quem o gerador confia. Já o consumidor do token verifica a assinatura e certificado do gerador, para assegurar que o token é de confiança e com base na chave *Bp*, autentica o dispositivo que entrega o token.

Esta solução pode ser usada tanto em situações ad-hoc em que os certificados colocados no token são assinados pelo próprio detentor, assim como em cenários em que existe uma PKI para verificar a confiança nos consumidores e geradores de tokens.

C. Integração com sistemas de IdM

A segunda parte da arquitetura do Multipass dedica-se a lidar com integração com serviços de IdM. Esta integração tem fundamentalmente dois objectivos:

1) Suportar o uso de Security Assertion Markup Language (SAML) como protocolo de autenticação em serviços, juntamente com mecanismos do operador para autenticar o dispositivo móvel.
2) Permitir o uso destes protocolos em cenários onde o browser (que é autenticado para aceder ao serviço) não se encontra em execução no dispositivo móvel.

Usar os recursos do operador para autenticar o dispositivo móvel permite-nos separar as comunicações, fazendo que os dados relativos aos serviços passem pelo canal de dados IP (Wifi ou 3G), mas os dados relativos ao processo de autenticação com o IdP sejam transmitidos de forma segura sobre o canal de controlo do operador. Isto pode ser

conseguido recorrendo aos mecanismos de comunicação Over the Air (OTA) que podem iniciar um processo de autenticação no telemóvel, por intermédio de um pedido de PIN pelo cartão SIM – o arranque da aplicação SIMToolkit, instalada no cartão SIM é conseguida através de uma mensagem que é enviada entre do operador diretamente para o SIM card, através de uma plataforma OTA do operador. A integração de ambos os protocolos, faz-se com recurso a inserção de um cabeçalho adicional, que contém o identificador do utilizador, em todas mensagens HTTP enviadas ao IdP do utilizador (que é pré-configurado no browser). Este cabeçalho é então utilizado pelo IdP para identificar o utilizador e iniciar o processo de autenticação, comunicando diretamente com o dispositivo móvel através da OTA. O utilizador recebe um pedido de PIN iniciado pelo cartão, semelhante aquele que é usado para desbloquear o dispositivo.

Desta forma é possível integrar protocolos de IdM, como o SAML (Fig. 2), com um mecanismo de autenticação disponibilizado pelo OTA, e aplicação SIMToolKit. No entanto o processo é igualmente válido para OpenID[1].

Este mecanismo permite separar fisicamente o dispositivo em que o utilizador se autentica (terminal móvel) do dispositivo em que o browser que estabelece a sessão está em execução. É com recurso a esta solução que se pretende instanciar o segundo cenário descrito, em que o dispositivo móvel autentica um quiosque público para agir em nome do utilizador.

Para que se possa separar os dois componentes é necessário adicionar algumas condições para manter o pré-requisito de autenticação mútua:

1) Tem de existir um canal de comunicação entre o terminal móvel e o browser com garantias de confidencialidade
2) Se possível o IdP utilizado no processo de autenticação deve autenticar também o dispositivo onde o browser é executado

O canal seguro entre o terminal móvel e o browser, serve para transmitir o identificador do utilizador entre o telemóvel e o browser, e para manter estado sobre a associação do entre os dispositivos.

O ponto 2) visa minimizar o risco de ataques de Man-in-the-Middle que embora nunca pudessem capturar o PIN do utilizador (já que este passa num canal diferente), poderiam permitir que um atacante tomasse controlo da sessão. Caso não seja possível faze-lo, o IdP pode ainda tomar outro tipo de medidas para gerir o risco, como restringir os privilégios da sessão que foi autenticada para só permitir algumas operações.

Este tipo de soluções é funcionalmente muito semelhante aos cenários designados de "split-terminal" [7], existentes na Generic Bootstrap Architecture (GBA). A grande diferença prende-se com os protocolos utilizados tanto para iniciar a autenticação como para autenticar o dispositivo, que aqui pretendemos evitar, favorecendo a integração com um sistema de IdM e protocolos mais fáceis de implementar.

D. Descoberta de Serviços

Em qualquer um dos cenários descritos o processo de autenticação é sempre iniciado pelo dispositivo móvel. Embora seja possível que o dispositivo notifique o utilizador da presença de serviços nas imediações, o processo de autenticação é sempre iniciado de forma explícita pelo utilizador.

Para descobrir serviços é possível recorrer-se a três tecnologias distintas:

1) Pesquisa de serviços Bluetooth, recorrendo ao protocolo SDP
2) Interação com códigos de barras QR
3) Interação com tags NFC

Nem todos os mecanismos de pesquisa de serviços são práticos para todas as situações, em ambientes em que existem vários serviços do mesmo tipo é normalmente preferível tags ou códigos de barras, para que não exista ambiguidade sobre o dispositivo com que se está a interagir.

O resultado de qualquer uma destas opções é um endereço de destino, que pode ser um IP e porto TCP, ou um endereço e canal RFCOMM (Bluetooth). No caso particular dos serviços de tokens, é incluído no resultado da pesquisa de serviços, um

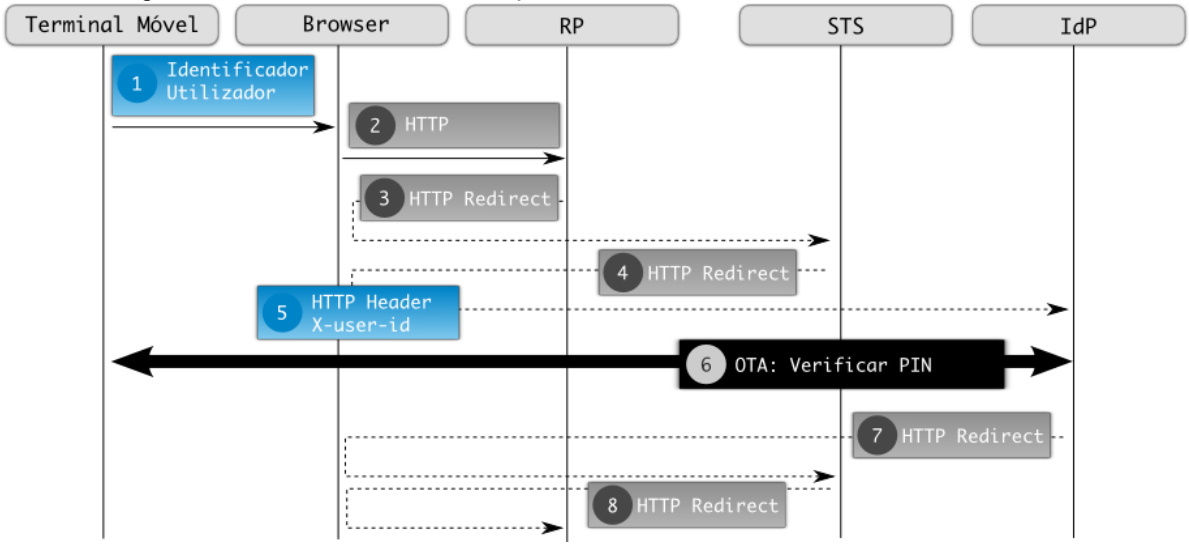

Fig. 2. Integração de Autenticação Over the Air com SAML

identificador que pode ser mapeado no certificado (*E*) que está incluído em cada token. Esta informação permite associar tokens a serviços descobertos, e ignorar serviços para os quais o dispositivo não possui tokens.

V. Implementação e Resultados

O principal objetivo deste projeto é desenvolver um protótipo capaz de demonstrar as interações de um dispositivo móvel com outros elementos do meio envolvente de forma segura e sem fios, instanciando os cenários descritos na secção III.

A implementação está dividida em três componentes (Fig. 3): uma aplicação Android que gere os tokens do utilizador no dispositivo, e controla o processo de autenticação; um serviço que instancia tokens e autentica o dispositivo com base nos mesmos; e um quiosque de acesso público onde o utilizador se pode associar com o seu dispositivo móvel para aceder a outros serviços através de um browser.

A. *Ambiente de desenvolvimento*

O ambiente de desenvolvimento considerado é baseado em ferramentas Java (versão 1.6 da Standard Edition) em execução em ambiente Linux. A implementação no dispositivo móvel Android é feita sobre a versão 2.3.3 (API 10) e compatível com superiores, não requerendo permissões especiais de acesso ao dispositivo.

O conteúdo trocado entre componentes é baseado em mensagens codificadas e com uma estrutura pré definida e conhecida pelos vários intervenientes da comunicação. A codificação de mensagens trocadas entre o dispositivo móvel e os restantes serviços é feita utilizando recorrendo à biblioteca de serialização de mensagens *Protocol Buffers*.

B. *Abstração de camada de transporte*

A interação entre componentes pode ocorrer sobre diversos mecanismos de transporte, sendo que uma rede IP pode não estar disponível como é o caso de Bluetooth.

Para permitir abstrair o protocolo de transporte da rede foi criado um proxy transparente para interligar clientes que utilizem diferentes protocolos de comunicação sem fios, com serviços implementados sobre TCP/IP.

Desta forma todos os serviços são implementados como servidores TCP/IP comuns, e apenas a implementação do terminal móvel e deste proxy é que tem lidar com as especificidades de cada protocolo de comunicação sem fios. De momento este componente lida apenas com dois protocolos orientados à conceção, TCP/IP e RFCOMM/Bluetooth e para além de fazer o mapeamento entre sockets nos dois protocolos, cria também as entradas para descoberta de serviços sobre Bluetooth. Apesar de ser feito uso de NFC para descoberta de serviços, o uso de NFC como protocolo de transporte ainda não foi considerado.

C. *Serviço de Tokens*

O serviço de tokens é responsável por negociar novos tokens com o dispositivo móvel, e consumir os tokens no processo de autenticação. Estas duas funcionalidades são funcionalmente independentes, ou seja uma instância do serviço de tokens pode criar um token que deve ser consumido por uma outra instância, desde que o consumidor confie no certificado do gerador do token.

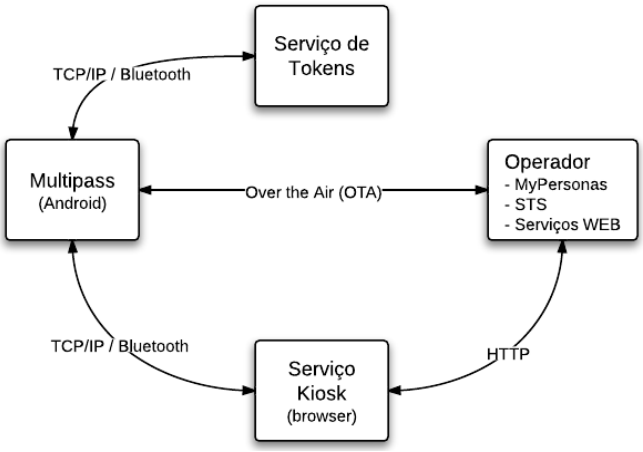

Fig. 3. Diagrama de componentes desenvolvidos.

O protótipo desenvolvido associa aos tokens gerado, e a metadata, com instruções arbitrárias para serem executados pelo consumidor do token. Neste caso o protótipo exige interação com o utilizador para escolher a ação que vai ser associada ao token. Isto permite controlar remotamente um dispositivo com recurso a estes tokens de autenticação mútua, despoletando ações como desbloquear o ecrã de um computador, ou desligando um terminal a partir do dispositivo móvel.

D. *Serviço Quiosque*

Este serviço pretende fornecer um terminal público de acesso à internet para consulta de serviços por parte das entidades que disponibilizem autenticação por intermédio do operador. O quiosque não é mais que um terminal público com um browser, que o utilizador pode usar.

Para suportar a autenticação do utilizador no quiosque foi implementada uma extensão para o browser Firefox que recebe o identificador do utilizador, enviado pelo dispositivo móvel que se liga ao quiosque, e o reenvia para um IdP pré-configurado no quiosque.

Quando o utilizador se liga ao quiosque com o seu dispositivo móvel, este inicializa um browser para ser utilizado. Apenas quando o utilizador tenta usar o browser para aceder a um serviço que requer autenticação através do IdP é que a extensão do browser reenvia o identificador. Uma vez enviado este identificador o processo é transparente para o serviço de quiosque, sendo o IdP a gerir o processo de autenticação com o dispositivo do utilizador.

Para garantir que a sessão do utilizador não permanece em funcionamento depois de terminado o uso no quiosque, foram implementados mecanismos que mantêm a sessão ativa enquanto existir uma ligação entre o dispositivo do utilizador e o quiosque. A ligação entre ambas as partes é mantida ativa com base na troca constante de mensagens em intervalos regulares e ao qual a falha na troca destas mensagens (e.g. se o utilizador se afastar do quiosque) resulta numa interrupção do sistema de comunicação de ambos os lados, voltando tanto a aplicação como o terminal ao seu estado inicial.

E. *Aplicação Multipass*

A aplicação Multipass é responsável por fazer uso dos dois serviços implementados, serviço de tokens e serviço quiosque. Com esta aplicação no dispositivo móvel, o utilizador pode fazer gestão dos seus tokens (aquisição, entrega e armazenamento) e interagir com serviços de quiosque.

A pesquisa de serviços nas imediações pode ser efetuada com recurso a Bluetooth, códigos QR ou tags NFC, embora em ambientes em que coexistam múltiplas instâncias destes serviços seja preferível recorrer às tags e códigos de barras.

Após a fase de pesquisa de serviços recorrendo a um dos protocolos disponíveis, a aplicação permite despoletar uma das seguintes ações:

1) Adquirir um token gerado por um dispositivo próximo
2) Usar um token gerado anteriormente, para se autenticar com um consumidor de tokens
3) Associar o dispositivo móvel a um quiosque para posteriormente autenticar uma nova sessão no quiosque

Mais ainda, a aplicação pode ser configurada para efetuar ela própria pesquisa autónoma de serviços de quiosque e lançar uma notificação ao utilizador sempre que seja encontrado algo nas redondezas. Esta pesquisa de serviços necessita obrigatoriamente de uma ligação Bluetooth constantemente ativa de forma a realizar as pesquisas.

Por fim para permitir instanciar túneis TLS sobre sockets Bluetooth foi desenvolvido um mecanismo que permite utilizar sockets não IP em APIs que usam sockets IP, permitindo desta forma utilizar a implementação de TLS existente nos dispositivos Android sobre outros tipos de sockets, como sendo Bluetooth. Internamente esta solução funciona como um proxy invertido, instanciado dentro da aplicação Android que reencaminha as mensagens através de outro tipo de sockets e mapeia os diferentes sockets. Esta solução sofre de algumas limitações resultantes da API de Android, uma vez que as sockets Bluetooth não suportam operações assíncronas, é necessário implementar esta solução numa thread separada.

F. *Resultados*

Um dos objetivos do projeto consistia na produção de um protótipo, que demonstrasse os cenários do projeto. No entanto interessa ainda medir o impacto da utilização de túneis TLS sobre o protocolo Bluetooth.

Os testes realizados medem o tempo de ida e volta de uma mensagem de 100KBytes. Embora este valor seja pelo menos uma ordem de grandeza acima de uma transação de um token Multipass (que ocupa menos de 10KB), consideramos este valor antevendo o uso de grandes quantidades de metadata nos tokens e futuras extensões à arquitetura.

O dispositivo móvel é o iniciador da ligação e os tempos incluem o estabelecimento e término das ligações. Não nos sendo possível medir com exatidão o custo temporal de cada um dos protocolos para a mesma ligação, optou-se por repetir esta experiência para três situações distintas:

1) Uma ligação Bluetooth através das APIs normais de Android
2) Uma ligação Bluetooth através do sistema de mapeamento de sockets, mas sem instanciar os mecanismos de TLS

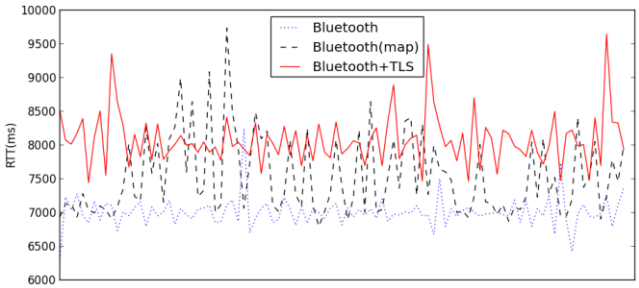

Fig. 4. RTT para um para envio e receção de 100KB sobre Bluetooth

3) Uma ligação TLS sobre um socket Bluetooth

O gráfico apresentado na Figura. 4, contém o tempo da ligação para um total de 98 experiências, para cada um dos casos. O tempo médio gasto por uma ligação Bluetooth normal, uma ligação Bluetooth mapeada e uma ligação TLS sobre Bluetooth foi respetivamente de 7009, 7527 e 8077 milissegundos.

Destes valores retira-se que a utilização de TLS sobre Bluetooth resultou na introdução (para esta operação) de um tempo adicional médio de 1069 milissegundos. Deste tempo, em média 518 milissegundos são resultantes da nossa implementação para mapear sockets, enquanto os restantes resultam do uso de TLS.

Face ao tempo total médio para esta operação (7009ms) houve uma degradação média de cerca de 15%, sendo que metade desse agravamento resulta da implementação que foi produzida.

VI. Conclusões

Neste artigo foram descritas a arquitetura e implementação desenvolvidas no decorrer do projeto Multipass2, cujo objetivo é recorrer a dispositivos móveis como mecanismo privilegiado para interação com serviços recorrendo a autenticação mútua.

A arquitetura apresentada visa suportar dois cenários distintos. O primeiro cenário incide sobre ambientes em que o dispositivo móvel é usado para interagir e controlar múltiplos dispositivos na proximidade do utilizador, como é o caso de ambientes de domótica e Internet of Things. O segundo cenário ambiciona usar o telemóvel como mecanismo para autenticar sessões noutros dispositivos, recorrendo aos sistemas de IdM, para autenticar o utilizador e aos serviços do operador para que as transações referentes ao processo de autenticação ocorram num canal separado da rede de dados.

Para instanciar os cenários pretendidos foi implementado um protótipo com o propósito de validar a arquitetura. Foi desenvolvida uma aplicação Android para gerir tokens de autenticação armazenados no dispositivo e interagir com outros serviços, através de redes IP ou Bluetooth e utilizando códigos QR ou tags NFC para facilitar o processo. Foram também criados componentes para integração com outros serviços, em particular com vista à integração com o IdP e mecanismos de comunicação diretamente com o SIM Card do operador.

AGRADECIMENTOS

O trabalho aqui apresentado decorre do projeto Multipass2 financiado pela PT Inovação, e desenvolvido em colaboração com grupo de investigação ATNoG no pólo de Aveiro do Instituto de Telecomunicações.

REFERÊNCIAS

[1] D. Recordon, J. Bufu, J. Hoyt, B. Fitzpatrick, and D. Hardt, OpenID Authentication 2.0 http://openid.net/specs/openid-authentication-2_0.html, December 2007.

[2] Cantor, S., Kemp, J., Philpott, R., and E. Maler. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard saml-core-2.0-os, March 2005.

[3] http://www.mobile.se

[4] http://web.twelvehorses.com/technology/ticketing/

[5] http://www.openways.com/

[6] Ross, P.E., "Phone-y money," Spectrum, IEEE , vol.49, no.6, pp.60-63, June 2012 doi: 10.1109/MSPEC.2012.6203971

[7] 3GPP TS 33.220; Generic Authentication Architecture (GAA); Generic bootstrapping architecture http://www.3gpp.org/ftp/Specs/html-info/33220.htm, June 2006.