ePaga - Sistema de Pagamento Electrónico

João Almeida, Paulo Ferreira, Carlos Ribeiro

joao.macedo@ist.utl.pt
paulo.ferreira@inesc-id.pt
carlos.ribeiro@ist.utl.pt
INESC-ID/Instituto Superior Técnico

Resumo. A possibilidade de utilizar dispositivos móveis para efectuar pagamentos tem vindo a prometer maior rapidez, conveniência e ubiquidade, em relação aos métodos actuais de pagamento. Por estas razões, o mercado dos pagamentos móveis evidencia um potencial elevado. No entanto, a falta de interoperabilidade entre sistemas de pagamento, em conjunto com a escassez de tecnologias apropriadas, tem atrasado o progresso na área dos pagamentos móveis. O objectivo deste trabalho é desenvolver um sistema de suporte a pagamentos electrónicos, focado nos pagamentos móveis, que permite tirar partido de vários protocolos de pagamento que convivam simultaneamente no mesmo dispositivo. A aplicação resultante deste suporte a múltiplos protocolos atinge assim uma maior universalidade, eficiência e interoperabilidade, quando comparada com um protocolo isolado. O sistema proposto baseia-se na tecnologia NFC (*Near Field Computing*). Este documento descreve ainda o protótipo implementado e a sua avaliação.

Palavras-chave: computação móvel, pagamentos electrónicos, pagamentos móveis, interoperabilidade, NFC.

1 Introdução

Durante a última década têm sido desenvolvidas diversas iniciativas com o objectivo de explorar o potencial dos pagamentos electrónicos em dispositivos móveis. No entanto, apenas uma pequena fracção dos projectos subsiste com relativo sucesso. Entre o variado leque de razões que conduzem ao fracasso de um sistema incluem-se a falta de universalidade e de interoperabilidade com outros sistemas, fraca percepção de segurança e elevado custo dos equipamentos compatíveis.

De modo a responder à elevada quantidade de projectos existentes no mercado, a solução proposta neste documento apresenta uma infra-estrutura que se adapta a este ambiente heterogéneo. Esta solução tem como objectivo desenvolver uma aplicação que suporte vários sistemas de pagamento. No momento de efectuar um pagamento, a solução proposta deve escolher o sistema mais apropriado, consoante os sistemas suportados pelo vendedor e os requisitos do cliente.

A aplicação proposta implica os requisitos que são referidos de seguida.

- Simplicidade: O sistema deve ser fácil de usar pelos clientes e vendedores.
- Universalidade: O sistema deve suportar o maior número de utilizações possível nos ambientes mais diversos, incluindo diferentes tipos de intervenientes e pagamentos de diversas quantias.
- Interoperabilidade: O sistema não deve estar limitado por uma marca de dispositivos, por um banco ou por uma operadora de telecomunicações. Também deve ser facilitada a interacção com outros sistemas de pagamentos electrónicos, assim como a integração com sistemas de pagamento tradicionais.
- Consistência: Apesar de funcionar num ambiente instável e heterogéneo, o sistema deve apresentar uma interface consistente ao utilizador e aos sistemas que suporta.

Um sistema de pagamento inclui requisitos adicionais como rapidez, custo ou segurança. Não cabe à aplicação proposta garantir que estes requisitos são respeitados por todos os protocolos; requer-se apenas que não dificulte o cumprimento destes requisitos por parte de cada protocolo.

2 Actores

Uma das razões que dificultam a criação de *standards* e reduzem o sucesso das iniciativas na área dos pagamentos móveis é a diversidade de entidades envolvidas, cada uma com perspectivas e objectivos distintos. Passa-se a enumerar as mais importantes [1]: clientes particulares, vendedores, bancos, operadoras de telecomunicações, fabricantes de dispositivos móveis e entidades governamentais ou reguladoras.

Clientes Particulares [2]: Para que um serviço de pagamentos móveis seja adoptado pelos utilizadores precisa de se diferenciar dos métodos de pagamento actuais, tais como dinheiro, cartões de crédito ou cheques. Os principais factores que influenciam a adesão de clientes a um sistema de pagamentos móveis são a facilidade de uso, percepção de segurança e o custo do serviço.

Vendedores: Para além de partilharem com os clientes preocupações como custo e segurança, os pontos que têm maior relevância são a rapidez da transacção e a facilidade de integração com os sistemas de pagamento existentes.

Bancos: Para os bancos, os pagamentos móveis representam uma oportunidade para oferecer um novo serviço, atraindo novos clientes, aumentando a lealdade dos mesmos e maximizando o lucro por cliente. Os bancos pretendem ter controlo sobre as aplicações de pagamento e desejam que o sistema seja independente das operadoras de telecomunicações.

Operadoras de Telecomunicações: As operadoras, à semelhança dos bancos, também encaram os pagamentos móveis como uma possibilidade de oferecer um novo serviço, com as vantagens referidas anteriormente. Qualquer serviço que necessite de comunicação através da sua rede representa uma fonte de rendimento extra para as operadoras. Tal como os bancos, também as operadoras ambicionam controlar as aplicações de pagamento, assim como a independência do sistema em relação aos bancos.

Fabricantes de dispositivos móveis: Os fabricantes influenciam o desenvolvimento de sistemas de pagamentos móveis através da inclusão de novas tecnologias nos dispositivos. Os atributos vistos como favoráveis, num serviço de pagamentos mó-

veis, são a escolha de uma tecnologia pouco dispendiosa e rápida introdução no mercado.

Entidades Governamentais ou Reguladoras: Estas instituições têm o papel de desenvolver legislação favorável, promover o desenvolvimento de *standards* e implementação de iniciativas como a criação de uma PKI (*Public Key Infrastructure*), atribuindo chaves e certificados aos cidadãos. As entidades governamentais desejam poder, no âmbito de uma investigação criminal, aceder à informação relativa às transacções que um individuo efectuou.

3 Tipos de Sistemas de Pagamento Móvel

Apesar da elevada quantidade e diversidade de sistemas desenvolvidos na área dos pagamentos móveis, estes podem ser caracterizados em categorias que representam os seus principais atributos. Estas categorias são enumeradas de seguida.

- Valor das transacções [2]: a relevância de requisitos como rapidez, custo por transacção e segurança varia consoante o valor da transacção.
- Tipo de interacção [4]: um pagamento pode ser feito à distância ou em proximidade. Estes tipos de interacções englobam diferentes cenários de utilização. Os pagamentos à distância incluem cenários como o ponto de venda virtual ou transferências C2C (*customer to customer*). Situações como pontos de venda (POS), P2M (pagamentos em maquinas automáticas) ou P2P (*peer to peer*) são alguns exemplos de pagamentos em proximidade.
- Momento do Pagamento [4]: o momento em que são cobradas as transacções influencia variáveis como o controlo sobre o saldo do cliente, ou a comunicação necessária para executar um pagamento. Um sistema pode ser pré-pago, pós-pago ou em tempo real.
- Tipo de Transacção: no cerne de um serviço de pagamentos electrónicos encontra-se o conceito de transacção. Uma transacção pode ser representada pela assinatura de um documento, à semelhança da utilização de cheques. Este tipo de sistemas é denominado *account-based* [5]. Uma transacção pode também ser representada pela troca de objectos criados por uma entidade confiável, de forma análoga à utilização de moedas e notas. Estes sistemas são categorizados como *token-based* [2].
- Necessidade de Intermediários [6]: nas transacções em proximidade pode existir uma interacção obrigatória com uma entidade central. Estas transacções podem ser categorizadas como *online*. As transacções em que esta interacção não é obrigatória são denominadas *offline*. As transacções *offline* são mais rápidas e baratas, para além de poderem ser executadas em zonas sem cobertura da rede telefónica móvel. No entanto, a falta de controlo da entidade central durante a transacção origina outros problemas. Em sistemas a*ccount-based,* nos pagamentos *offline* existe a possibilidade de o cliente efectuar pagamentos para os quais não tem saldo. No caso dos sistemas *token-based*, os pagamentos *offline* dão origem à dificuldade de detecção da reutilização indevida de *tokens*, que se traduz numa multiplicação indevida de dinheiro.

4 NFC

NFC (*Near Field Communication*) [7] é uma tecnologia relativamente recente, baseada no RFID *(Radio Frequency IDentification*) e compatível com este. O NFC opera na frequência dos 13,56 MHz e permite velocidades de transmissão até 424 Kbit/s. Um dispositivo NFC pode funcionar em três modos: em modo P2P para comunicar com outro dispositivo NFC, como leitor de etiquetas NFC, ou em modo de simulação de uma etiqueta NFC, para que um leitor o encare como um cartão *contactless*. Um dispositivo compatível com NFC tem de incluir os seguintes componentes: uma antena NFC, um chip NFC e um elemento seguro. O elemento seguro tem a capacidade de guardar dados e executar aplicações de forma segura.

Para além de apresentar consumos energéticos baixos, a principal característica do NFC é o alcance reduzido (3 a 30cm). Este factor torna intrusões extremamente difíceis, o que por sua vez torna desnecessários protocolos como o emparelhamento do *Bluetooth*. Assim, o estabelecimento de uma ligação é mais simples e rápido [8].

5 fairCASH

O fairCASH [9] é um sistema *token-based* e pré-pago que permite pagamentos à distância e pagamentos de proximidade *offline*. Os *tokens* deste sistema são transferíveis, isto é, podem ser transaccionados entre clientes várias vezes antes de serem depositados. O sistema permite anonimato inquebrável dos clientes, evitando que a identificação da aplicação de pagamento seja associada com o cliente. O cliente não fornece os seus dados ao sistema através de qualquer tipo de registo. Para carregar a aplicação com *tokens*, o cliente efectua uma transferência bancária da quantia desejada para o sistema. Para reduzir o risco de duplicação de *tokens*, cada cliente guarda um registo dos *tokens* recebidos que, com a sua permissão, é usado pelo sistema para calcular a origem de uma duplicação de *tokens*. O sistema refere também um número máximo de vezes que um *token* pode ser utilizado. Cada entidade é identificada pelo seu certificado digital. Para garantir a autenticidade dos *tokens*, estes são assinados pela entidade que os emite.

O sistema fairCASH foi o escolhido para servir de base ao protocolo implementado. Este sistema foi escolhido devido à simplicidade de implementação das técnicas descritas.

6 Arquitectura

O sistema de suporte a pagamentos móveis ePaga pretende comportar todos os tipos de pagamentos referidos. Em relação a tecnologias de comunicação de curto alcance, foi escolhida a tecnologia NFC, por ser a única que não limita o sistema a nível de segurança e usabilidade.

A Figura 1 representa a arquitectura da aplicação do dispositivo móvel. A camada superior implementa a interacção com o utilizador, de modo a que a aplicação lhe apresente uma interface consistente. A camada imediatamente abaixo aloja os vários

protocolos de pagamento. Esta é a única parte da arquitectura que varia entre sistemas de pagamento. O *middleware* do sistema visa oferecer uma camada de abstracção aos protocolos de pagamento que sejam implementados sobre ele. Este *middleware* deve também, no instante de receber ou efectuar um pagamento, escolher o protocolo da camada superior a ser usado. Os blocos da camada inferior representam funcionalidades disponibilizadas pelo dispositivo e que são utilizadas pelo *middleware*.
A camada de *middleware* está dividida nos seguintes módulos:

- Mecanismos de Escolha de Protocolo: escolhe um dos protocolos contido no Registo de Protocolos segundo a Política de Escolha de Protocolo.
- Registo de Protocolos: mantém a informação sobre os protocolos de pagamento instalados no dispositivo.
- Política de Escolha de Protocolo: conjunto de regras a serem seguidas pelos Mecanismos de Escolha de Protocolo, de modo a ser escolhido um protocolo.
- Comunicação Local: gere a comunicação NFC com outros dispositivos próximos. Gere também o acesso local ao elemento seguro do dispositivo.
- Comunicação Remota: gere a comunicação remota com base em *web services*.

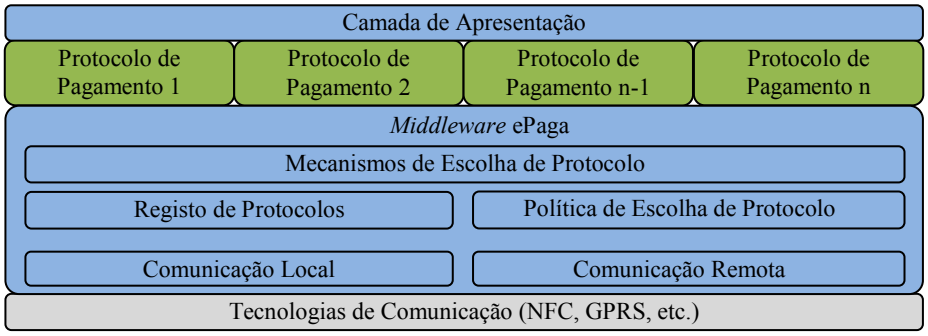

Figura 1. Arquitectura de *software* do sistema ePaga.

7 Protocolo *token-based*

Para a implementação do sistema ePaga foi adoptada uma abordagem na qual os primeiros passos consistem em implementar e testar individualmente protótipos de protocolos de pagamento. Estes protocolos exemplificam os protocolos que serão suportados pelo sistema. No passo seguinte estes protocolos servem de ponto de partida para a implementação de uma camada de apresentação unificada, seguida da camada de *middleware*.

Até a data de escrita deste documento foi implementado o primeiro dos protocolos de pagamento, que exemplifica um protocolo *token-based* e permite pagamentos em proximidade *offline*, nomeadamente transacções P2P e POS. Este protocolo partilha das vantagens e desvantagens deste tipo de sistemas. Por incluir pagamentos *offline* e *tokens* transferíveis, atinge um custo por transacção menor. No entanto, como cada *token* é representado por um objecto, o espaço de memória ocupado aumenta à medi-

da que o saldo aumenta (Tabela 1). Da mesma forma, a quantidade de dados transmitida aumenta em função do número de *tokens* utilizados numa transacção (Tabela 2).

Tabela 1. Memória do elemento seguro utilizada pelo protocolo.

Objecto	Espaço Ocupado (em *bytes*)
Applet sem saldo	14017
Applet com 10 *tokens* instalados	15397
Token	138
Certificado	220

Tabela 2. Quantidade de informação trocada entre os dispositivos, em função do número de *tokens* envolvidos.

Tokens transferidos	Informação transmitida (em *bytes*)
1	937
10	1784

8 Conclusões

A área dos pagamentos móveis continua a evidenciar um potencial tremendo, o que se verifica pelo constante investimento em novos projectos um pouco por todo o mundo. Este número elevado de iniciativas, deixa antever um mercado preenchido com sistemas propostos por entidades diferentes, muitos deles incompatíveis entre si. Como resposta a este cenário, foi proposto um sistema que suporta vários protocolos de pagamento na mesma aplicação. Este sistema permite aos intervenientes de uma transacção comunicarem através do protocolo mais adequado, seleccionado entre os protocolos suportados por ambos. O sistema maximiza assim a interoperabilidade entre dispositivos, de modo a explorar o verdadeiro potencial dos pagamentos móveis.

Referências

[1] Karnouskos, S. Mobile payment: A journey through existing procedures and standardization initiatives, Communications Surveys & Tutorials, IEEE, 6(4), 44-66, 2004
[2] N. Kreyer, K. Pousttchi, et al. Characteristics of Mobile Payment Procedures, Proceedings of the ISMIS 2002 Workshop on M-Services, 2002
[3] Andriew S. Lim, Inter-consortia battles in mobile payments standardisation, Electronic Commerce Research and Applications, 7(2), 202–213, 2008
[4] S. Karnouskos et al. Secure Mobile Payment — Architecture and Business Model of SEMOPS, Proceedings of the EURESCOM summit, 2003
[5] Xiaolin Zheng, Deren Chen, Study of Mobile Payments System, Proceedings of the IEEE International Conference on E-Commerce (CEC'03), 2003
[6] R. K. Balan, N. Ramasubbu, et al. mFerio: The design and evaluation of a peer-to-peer mobile payment system, Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services, 2009
[7] Diogo Simões, Sistema de Fidelização sobre NFC (Near Field Communication), 2008
[8] J. J. Chen, C. Adams, Short-range wireless technologies with mobile payments systems, The 6th International Conference on Electronic Commerce (ICEC), 2004
[9] H. Kreft, Cashing up with Mobile Money – the fairCASH Way, Euro mGov 2005, 2005