INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA
Área Departamental de Engenharia de Electrónica e Telecomunicações
ISEL

WPAC - Wireless Payment and Access Control
Dispositivos Móveis no Pagamento de Serviços e Controlo de Acessos

Pedro Miguel Alves Henriques

Dissertação de natureza científica realizada para obtenção do grau de Mestre em Engenharia Informática e de Computadores

Resumo:

A rápida evolução dos dispositivos móveis e das tecnologias de comunicação sem fios transformou o telemóvel num poderoso dispositivo de computação móvel. A necessidade de estar sempre contactável, comum à civilização moderna, tem aumentado a dependência deste dispositivo, sendo transportado pela maioria das pessoas num ambiente urbano e assumindo um papel talvez mais importante que a própria carteira. A ubiquidade e capacidade de computação dos telemóveis aumentam o interesse no desenvolvimento de serviços móveis, além de tradicionais serviços de voz. Um telemóvel pode em breve tornar-se um elemento activo nas nossas tarefas diárias, servindo como um instrumento de pagamento e controlo de acessos, proporcionando assim novas interfaces para serviços existentes. A unificação de vários serviços num único dispositivo é um desafio que pode simplificar a nossa rotina diária e aumentar o conforto, no limite deixaremos de necessitar de dinheiro físico, cartões de crédito ou débito, chaves de residência e de veículos automóveis, ou inclusive documentos de identificação como bilhetes de identidade ou passaportes.
O interesse demonstrado pelos intervenientes, desde os fabricantes de telemóveis e operadores de rede móvel até às instituições financeiras, levaram ao aparecimento de múltiplas soluções de serviços móveis. Porém estas soluções respondem geralmente a problemas específicos, apenas contemplando um fornecedor de serviços ou uma determinada operação de pagamento, como seja a compra de bilhetes ou pagamento de estacionamento. Estas soluções emergentes consistem também tipicamente em especificações fechadas e protocolos proprietários. A definição de uma arquitectura genérica, aberta interoperável e extensível é necessária para que os serviços móveis possam ser adoptados de uma forma generalizada por diferentes fornecedores de serviços e para diversos tipos de pagamento. A maior parte das soluções actuais de pagamento móvel depende de comunicações através da rede móvel, algumas utilizam o telemóvel apenas como uma interface de acesso à internet enquanto outras possibilitam o envio de um SMS (*Short Message Service)* para autorizar uma transacção, o que implica custos de comunicação em todas as operações de pagamento. Este custo de operação torna essas soluções inadequadas para a realização de micropagamentos e podem por isso ter uma aceitação limitada por parte dos clientes. As soluções existentes focam-se maioritariamente em pagamentos à distância, não tirando partido das características do pagamento presencial e não oferecendo por isso uma verdadeira alternativa ao modelo actual de pagamento com cartões de crédito/débito. As capacidades computacionais dos telemóveis e suporte de diversos protocolos de comunicação sem fio local não têm sido aproveitadas, vendo o telemóvel apenas como um terminal GSM (*Global System for Mobile*

Communications) e não oferecendo serviços adicionais como seja a avaliação dinâmica de risco ou controlo de despesas.

Esta dissertação propõe e valida, através de um demonstrador, uma aquitectua aberta para o pagamento e controlo de acesso baseado em dispositivos móveis, intitulada WPAC (*Wireless Payment and Access Control*). Para chegar à solução apresentada foram estudadas outras soluções de pagamento, desde o aparecimento dos cartões de débito até a era de pagamentos electrónicos móveis, passando pelas soluções de pagamento através da internet. As capacidades dos dispositivos móveis, designadamente os telemóveis, e tecnologias de comunicação sem fios foram também analisadas a fim de determinar o estado tecnológico actual. A arquitectura WPAC utiliza padrões de desenho utilizados pela indústria em soluções de sucesso, a utilização de padrões testados e a reutilização de soluções com provas dadas permite aumentar a confiança nesta solução, um destes exemplos é a utilização de uma infra-estrutura de chave pública para o estabelecimento de um canal de comunicação seguro. Esta especificação é uma arquitectura orientada aos serviços que utiliza os Web Services para a definição do contracto do serviço de pagamento. A viabilidade da solução na orquestração de um conjunto de tecnologias e a prova de conceito de novas abordagens é alcançada com a construção de um protótipo e a realização de testes.

A arquitectura WPAC possibilita a realização de pagamentos móveis presenciais, isto é, junto do fornecedor de bens ou serviços, seguindo o modelo de pagamento com cartões de crédito/débito no que diz respeito aos intervenientes e relações entre eles. Esta especificação inclui como aspecto inovador a avaliação dinâmica de risco, que utiliza o valor do pagamento, a existência de pagamentos frequentes num período curto de tempo, e a data, hora e local do pagamento como factores de risco; solicitando ao cliente o conjunto de credenciais adequado ao risco avaliado, desde códigos pessoais a dados biométricos. É também apresentada uma alternativa ao processo normal de pagamento, que apesar de menos cómoda permite efectuar pagamentos quando não é possível estabelecer um canal de comunicação sem fios, aumentando assim a tolerância a falhas. Esta solução não implica custos de operação para o cliente na comunicação com o ponto de venda do comerciante, que é realizada através de tecnologias de comunicação local sem fios, pode ser necessária a comunicação através da rede móvel com o emissor do agente de pagamento para a actualização do agente de software ou de dados de segurança, mas essas transmissões são ocasionais. O modelo de segurança recorre a certificados para autenticação dos intervenientes e a uma infra-estrutura de chave pública para cifra e assinatura de mensagens. Os dados de segurança incluídos no agente de software móvel, para desabilitar a cópia ou corrupção da aplicação mas também para a comparação com as credenciais inseridas pelo cliente, devem igualmente ser encriptados e assinados de forma a garantir a sua confidencialidade e integridade. A arquitectura de pagamento utiliza o standard de Web Services, que é amplamente conhecido, aberto e interoperável, para definição do serviço de pagamento. Existem extensões à especificação de Web Services relativas à segurança que permitem trocar itens de segurança e definem o modo de cifra e assinatura de mensagens, possibilitando assim a sua utilização em aplicações que necessitem de segurança como é o caso de serviços de pagamento e controlo de acesso. O contracto de um Web Service define o modo de invocação dos serviços, transmissão de informação e representação de dados, sendo normalmente utilizado o protocolo SOAP que na prática não é mais que um protocolo de troca de mansagens XML (eXtensible Markup Language). O envio e recepção de mensagens XML; ou seja, a transmissão de simples sequências de caracteres, é suportado pela maioria dos protocolos de comunicação, sendo portanto uma solução abrangente que permite a adopção de diversas tecnologias de comunicação sem fios. O protótipo inclui um agente de software móvel, implementado sobre a forma de uma MIDlet, aplicação Java para dispositivos móveis, que implementa o protocolo de pagamento comunicando sobre uma ligação Bluetooth com o ponto de venda do comerciante, simulado por uma aplicação desenvolvida sobre a plataforma .NET e que por isso faz prova da heterogeneidade da solução. A comunicação entre o comerciante e o seu banco para

autorização do pagamento e transferência monetária utiliza o protocolo existente para a autorização de pagamentos, com base em cartões de crédito/débito.
A definição desta especificação aberta e genérica em conjunto com o forte interesse demonstrado pelos intervenientes, proporciona uma boa perspectiva em termos de adopção da solução, o que pode impulsionar a implementação de serviços móveis e dessa forma simplificar as rotinas diárias das pessoas. Soluções móveis de pagamento reduzem a necessidade de transportar vários cartões de crédito/débito na nossa carteira. A avaliação dinâmica de risco permite aumentar a segurança dos pagamentos, com a solicitação de mais credenciais ao cliente para pagamentos com um maior risco associado, sendo um ponto importante quer para os clientes quer para as instituições financeiras pois diminui o risco de fraude e aumenta a confiança no sistema. Esta solução de pagamento electrónico pode também facilitar a consulta de pagamentos efectuados e saldos, mantendo um histórico dos movimentos, o que não é possível nos cartões de crédito/débito sem uma visita a uma ATM (*Automated Teller Machine*) ou utilização de *homebanking*.

Palavras-Chave – Pagamento sem fios, Controlo de acessos, Comércio electrónico, Serviços móveis, Dispositivos nómadas, Segurança, Avaliação dinâmica de risco.

Novembro de 2009