ASASP – ACTUALIZAÇÃO SEGURA DE APLICAÇÕES EM SISTEMAS POS

Manuel José Ferreira Carneiro Mendonça

Dissertação submetida para obtenção do grau de

MESTRE EM INFORMÁTICA

Orientador:

Nuno Fuentecilla Maia Ferreira Neves

Júri:

Maria Teresa Caeiro Chambel

Paulo Jorge Pires Ferreira

Outubro de 2004

ASASP – ACTUALIZAÇÃO SEGURA DE APLICAÇÕES EM SISTEMAS POS

Manuel José Ferreira Carneiro Mendonça

Dissertação submetida para obtenção do grau de
MESTRE EM INFORMÁTICA

pela

Faculdade de Ciências da Universidade de Lisboa

Departamento de Informática

Orientador:

Nuno Fuentecilla Maia Ferreira Neves

Júri:

Maria Teresa Caeiro Chambel

Paulo Jorge Pires Ferreira

Outubro de 2004

Agradecimentos

Está terminada mais uma etapa da minha vida. Não seria justo nesta hora deixar de reconhecer todos aqueles que de forma desinteressada contribuíram para que a pudesse concluir.

O meu primeiro agradecimento é dirigido ao meu orientador o Professor Nuno Ferreira Neves. Desde o primeiro momento manteve o interesse, empenho, disponibilidade e o encorajamento nos momentos mais difíceis. A ele, o meu sincero agradecimento por tudo. Fica a esperança de com ele poder iniciar e finalizar outras etapas.

Em segundo lugar, mas não menos importante, à minha família, sem distinção, pelo constante apoio, motivação e paciência.

Um agradecimento muito especial à SIBS pela inspiração.

Por último a todos aqueles que se têm cruzado no meu caminho e que me ajudaram a ser quem sou.

“A sabedoria é como um anel, um tesouro, preciosa.”

Resumo

Ao longo dos últimos vinte anos tem aumentado a importância dos sistemas de pagamento electrónico. Actualmente, a esmagadora maioria das transacções electrónicas são efectuadas usando cartões de crédito ou débito em terminais POS (*Point of Sale*) localizados nos estabelecimentos comerciais. O sucesso desta forma de pagamento tem, no entanto, custos associados à gestão e manutenção dos muitos equipamentos existentes, de diversas gerações e fabricantes. Em particular, existe um importante custo relacionado com a actualização das aplicações desses equipamentos, uma vez que na maior parte dos casos é necessária a intervenção humana.

Nesta tese é descrita uma solução para este problema, onde os terminais POS são informados da existência de novas versões de aplicações, e depois são capazes de se actualizarem de uma forma automática e segura. Embora a arquitectura e protocolos propostos sejam relativamente genéricos, optou-se por criar uma solução que pudesse ser aplicada num ambiente bancário real. Escolheu-se assim, para servir de base ao trabalho, a rede Portuguesa de pagamentos electrónicos – o Multibanco. O sistema desenvolvido consegue alcançar os seguintes objectivos: encontra-se bem integrado com a arquitectura existente, mas ao mesmo tempo minimiza a interferência com as operações de pagamento, através da delegação de alguma funcionalidade num conjunto de novos componentes; automatiza o processo de actualização desde o momento da produção da aplicação (numa qualquer empresa) até à sua instalação num terminal; e possibilita o controlo completo das actualizações por parte da entidade que gere o sistema de pagamentos. A tese apresenta ainda uma simulação e avaliação da solução proposta numa rede de computadores.

PALAVRAS-CHAVE: Segurança, Sistemas de Pagamento Electrónico, Terminais de Venda (POS), Actualização Automática de Aplicações

Abstract

During the past twenty years the importance of electronic payment systems has progressively increased. Currently, a large number of transactions are performed with credit or debit cards at terminals located in merchant stores, such as Point of Sale Devices (POS). The success of this form of payment, however, has an associated cost due to the management and maintenance of the many types of equipment from different generations and manufacturers. In particular, there is an important cost related to the deployment of new software upgrades for the devices, since in most cases human intervention is required.

This thesis describes a secure solution for this problem, where terminals are informed about the existence of more recent versions of the applications, and then they automatically upload the updates. Even tough the proposed architecture and protocols are relatively generic, we wanted to build a solution that could be applied in a real banking environment. Therefore, we decided to base our work on the Multibanco payment network. The adopted model achieves several objectives: it is tightly integrated with the existing system, but at the same time it minimizes interference with the payment operations, by delegating some functionality on a new set of components; it automates the update process from the moment of software production (at a manufacturer) until its installation at some POS; and it gives complete control of the upgrades to the entity managing the payment network. The thesis also describes a simulation and evaluation of the proposed solution on a network of computers.

KEY-WORDS: Security, Electronic Payment Systems, Point of Sale Devices, Automatic Software Upgrades.

Índice Geral

Índice de Figuras

Índice de Tabelas

Capítulo 1 Introdução

Nos últimos anos tem-se verificado em todo o mundo um grande aumento no número de utilizadores da Internet. Essa evolução tem sido observada por muitos como uma nova oportunidade para negociar, comprar e vender. Embora tenham vindo a ser efectuados fortes investimentos e investigação em soluções na área dos pagamentos electrónicos para essa tecnologia, verifica-se que tanto o número de transacções como o volume monetário transaccionado é diminuto, quando comparados com os números existentes nos sistemas desenvolvidos pelas redes bancárias de pagamentos.

O sucesso dessas redes fechadas de pagamento deve-se entre outras coisas, ao suporte de um número bastante elevado de terminais, quer sejam *Automatted Teller Machines* (ATM) ou *Point of Sale* (POS), e à comodidade e divulgação do cartão de débito/crédito.

Ao contrário dos outros países da Europa, em Portugal, a evolução do sistema de pagamento bancário deu-se de forma abrupta. Durante o período de atonia que durou de 1974 a 1983, a forma de operação da banca e dos seus serviços estava completamente estagnada e desactualizada face à realidade internacional. A negociação da entrada de Portugal na União Europeia, com critérios de entrada exigentes, como a redução da inflação para valores pouco vulgares face ao historial português, e o controlo rigoroso das operações realizadas pela banca, entre outros factores, resultaram na necessidade de uma rápida revolução de todo o sistema bancário.

Beneficiando da conjuntura de uma forte evolução tecnológica no sector das telecomunicações, principalmente no serviço público de transmissão de dados, que ao mesmo tempo oferecia melhores preços e melhor qualidade de serviço, do facto da banca na altura se encontrar nacionalizada e da análise dos sistemas de pagamento estrangeiros, o sector bancário português criou um sistema de pagamento automático assente numa plataforma tecnológica comum reconhecido internacionalmente como um dos mais seguros e avançados do mundo: a rede Multibanco [1].

1.1 Actualização do Software dos POS

Em Portugal o Operador do Sistema de Pagamentos (OSP) é a SIBS - Sociedade Interbancária de Serviços, que representa e actua em todas as transacções electrónicas em nome do Banco de Portugal.

Não foi no entanto a primeira rede de pagamentos automáticos introduzida em Portugal, existiram outras iniciativas como por exemplo a rede Chave 24 gerida pelo Banco Montepio Geral. No entanto, o investimento exigido para disponibilizar esse tipo de serviços a todo o país levado a cabo por uma única instituição criou uma oportunidade de negócio para que a rede Multibanco, apoiada por várias instituições, se implantasse com maior rapidez e menor esforço individual numa lógica de economia de escala.

No início da sua implantação, a rede Multibanco só colocou à disponibilidade do público terminais ATM, cujos serviços oferecidos incluíam: o levantamento de numerário, requisição de cheques, consultas de saldo e movimento. Progressivamente os serviços foram alargados à alteração do código secreto, depósito de valores e numerário, pagamentos de serviço e serviços específicos para bancos, até chegar aos nossos dias com a possibilidade carregar o telemóvel, adquirir bilhetes para espectáculos e transportes públicos.

A revolução no tipo e duração do atendimento oferecido pela rede, e pelos seus caixas automáticos, quando comparada com as práticas de atendimento nos balcões dos bancos na altura, justificam em grande parte o seu sucesso imediato.

Depois da introdução dos ATM, foram instalados os terminais POS. No início o número destes equipamentos era reduzido e forneciam uma pequena lista de serviços. O preço por equipamento era bastante elevado. Ao contrário dos ATM que eram financiados pela rede, o custo dos POS era suportado directamente por quem os adquirisse. Este facto levou a uma fraca adesão da maioria dos pequenos e médios comerciantes devido ao elevado investimento necessário para obterem o serviço de pagamentos.

Nesta altura, o aparecimento de um terminal simples e de preço acessível, desenvolvido pela SIBS e fabricado em Portugal, visando as necessidades estratégicas do sistema de pagamentos electrónico português, que sobretudo se prendiam com a expansão e maior utilização do serviço criado, abriu as portas à popularização do serviço de pagamento automático. Este facto obrigou os outros fabricantes a praticarem preços significativamente mais baixos chegando a ser cerca de dez por cento do seu valor inicial.

Com sucessivas evoluções tecnológicas e preços cada vez mais reduzidos, rapidamente o número de terminais foi aumentando existindo hoje em operação cerca de 140.000 unidades de vários fabricantes.

Os POS podem existir em diversos ambientes e configurações. No caso das caixas de pagamento, como acontece em algumas grandes superfícies comerciais, o POS assume a configuração dum computador que integra a aplicação *Electronic Founds Transfer* (EFT). Nestes casos é comum os equipamentos estarem ligados em rede numa arquitectura do tipo cliente-servidor. A parte cliente da aplicação EFT encontra-se na caixa junto do operador e a parte servidor num único equipamento algures no estabelecimento do comerciante. Desta forma optimiza-se o processo de comunicação, sendo apenas necessário um canal para a transmissão de todas as mensagens entre o servidor da empresa e o Servidor do Sistema de Pagamentos (SSP) mantido pela SIBS. No caso dos terminais mais simples, é muito frequente observarem-se arquitecturas bastante diversificadas.

Cada terminal POS está ligado à rede de pagamentos por intermédio dum operador de comunicações, público ou privado, sendo possível comunicar com o SSP por intermédio de vários tipos de infra-estruturas de comunicação, como por exemplo: modem de linha comutada, DOV e GSM. Por intermédio destas infra-estruturas, as mensagens enviadas pelo POS são processadas pelo SSP que lhe responde informando o resultado da transacção desencadeada.

A realização duma transacção num POS começa pela selecção do tipo de serviço de pagamento automático: compra, devolução ou outro. Escolhido o serviço são introduzidos os dados necessários para a realização da transacção: cartão do cliente, o montante a pagar e o *Personal Identification Number* (PIN). O terminal envia uma mensagem ao SSP para ser processada. No final do processamento o SSP produz uma mensagem de resposta para o POS indicando o resultado da transacção. Como prova de confirmação da realização da operação é impresso um talão, ficando o cliente com uma cópia e o comerciante com o original.

O modo de funcionamento dum terminal ATM é semelhante. O utilizador começa por introduzir o cartão, digita o PIN, selecciona o serviço e introduz os dados necessários à realização do serviço. O ATM envia uma mensagem ao SSP que a processa enviando

depois a resposta para o ATM indicando o resultado do processamento. Como forma de confirmação da realização da operação pode ou não ser impresso um talão.

Em qualquer destes casos a iniciativa do contacto é sempre dos terminais e nunca do SSP.

1.1 Actualização do Software dos POS

Se por um lado o desenvolvimento do hardware termina na maior parte dos casos com o lançamento do produto no mercado, ou pelo menos estabiliza rapidamente, por outro as aplicações EFT que correm nos POS e ATM podem sofrer várias transformações ao longo da vida útil do equipamento. A criação de novos serviços, o uso de novas tecnologias de cartões ou acontecimentos recentes como a passagem do ano 2000, a entrada em vigor da nova moeda ou a adesão à norma EMV [35][36][37][38], são exemplos práticos do dinamismo exigido a estas aplicações. A globalização inevitável da economia europeia promove as condições ideais para que se instalem novos fabricantes e equipamentos oferecendo outros serviços, que consequentemente trarão maior dinamismo às aplicações.

Para além destes desafios, existem outros factores que no dia a dia contribuem para que aconteçam frequentes alterações do software: problemas não detectados nas fases de teste e descobertos durante a sua utilização, compromissos internacionais e fraude.

1.2 Processo de Actualização

Devido aos diversos requisitos exigidos para assegurar a qualidade e segurança da rede de pagamentos, qualquer empresa que tencione comercializar e colocar em funcionamento um POS, ATM ou uma nova aplicação EFT, numa rede de pagamentos, é obrigada a certificar o equipamento e a aplicação EFT junto da entidade que gere o serviço. A certificação visa garantir que a aplicação cumpre a especificação fornecida por essa entidade reportando ao fornecedor do equipamento/aplicação as correcções necessárias.

Findo o processo, com sucesso na certificação, é apenas com base num compromisso de honra que muitas vezes o fabricante se compromete a fornecer os equipamentos ou a distribuir as novas aplicações sem quaisquer alterações em relação ao que foi certificado.

Os actuais processos de actualização de aplicações em POS em muitas redes de pagamentos é efectuado por empresas de manutenção e requer a deslocação dum técnico ao local de instalação do equipamento para ai fazer a substituição da aplicação EFT. Na

maior parte das vezes implica desmontar o equipamento para substituir o circuito integrado que possui o programa. Para poupar tempo por vezes é substituído o próprio equipamento por outro igual que foi entretanto actualizado. Noutros casos a actualização do software é feita ligando o terminal a um computador para trocar ficheiros.

1.3 Necessidade de Actualização Automática

Se considerarmos que a substituição duma aplicação pode rondar os vinte minutos por terminal POS, para um parque de 140.000 equipamentos, significa que são necessárias cerca de 46.666 horas/homem para a substituição integral do parque. Se essa tarefa fosse executada por um único técnico a trabalhar ininterruptamente, seriam necessários cerca de 5.3 anos, isto sem contar com os tempos de deslocação. Se cada intervenção técnica custar à banca 50€ e se cada cópia da aplicação custar também 50€ significa que a actualização do parque de POS envolve um custo da ordem de 14.000.000€.

A inexistência de um processo automático, global que faça a distribuição e substituição remota das aplicações EFT representa custos de manutenção e demora que em última análise reflectem a ineficiência do processo.

Os aspectos económicos de manutenção são sem dúvida importantes, mas esse processo também não garante que a aplicação que foi certificada seja efectivamente a que vai ser instalada no terminal.

Por estas razões justifica-se a necessidade duma solução que permita a actualização periódica das aplicações nos POS que seja segura e automática, e que ao mesmo tempo permita ao OSP manter sob seu controlo as aplicações que são executadas em cada um dos seus terminais.

O custo associado à manutenção das aplicações EFT pode ser reduzido se, em vez do técnico se deslocar ao local de instalação do POS para a substituição da aplicação, o terminal possa descarrega-la remotamente do OSP.

As especificações relativas à Europay, Master Card & Visa (EMV) [35][36][37][38] focam a necessidade de criação da possibilidade dos terminais de pagamento automático descarregarem o seu próprio software. Mas nada refere quanto à arquitectura do sistema nem ao modo de operação ou como fazer a integração nos diversos sistemas de pagamentos existentes.

Durante a investigação que foi elaborada para a realização deste trabalho foram identificadas duas empresas fabricantes de POS que afirmaram possuir uma solução proprietária para a substituição das aplicações EFT de forma remota. As duas foram contactadas na tentativa de obter detalhes sobre a implementação do processo mas os pedidos foram ignorados.

1.4 Contribuição

Com este trabalho pretende-se apresentar uma solução para o problema da actualização das aplicações EFT que estão em funcionamento nos POS de forma a que esta seja efectuada de forma rápida e segura. Embora a solução possa ser usada nos ATM, não os vamos tratar aqui por terem requisitos de segurança e de manutenção diferentes dos POS, que só por si justificam um estudo separado.

No desenvolvimento desta solução pretendeu-se alcançar os seguintes objectivos:

- Diminuir os custos associados à manutenção das aplicações nos POS;
- Aumentar a rapidez e segurança do processo de actualização;
- Actualizar de forma remota as aplicações dos terminais POS;
- Usar no processo de actualização a mesma infra-estrutura de comunicações do sistema de pagamentos;
- Integrar no sistema de pagamentos a capacidade de controlar o processo de actualização;
- Minimizar a intrusão do processo de transmissão da aplicação no funcionamento do sistema de pagamentos delegando do SSP essa tarefa;
- Dar garantias de que a aplicação não sofre quaisquer alterações durante todas as fases do percurso da aplicação, desde a sua produção até à execução.

Neste trabalho houve o cuidado de garantir que a solução proposta poderia empregar-se nos POS mais simples, que dotam os pequenos estabelecimentos comerciais do serviço de pagamento automático, e nos sistemas mais complexos das grandes superfícies comerciais. Num caso extremo esta solução poderá ser empregue em situações em que os POS são adquiridos sem qualquer aplicação EFT. Na primeira transacção (e única que

conseguem efectuar nestas circunstâncias) recebem do SSP instruções para procederem ao carregamento da aplicação. Não se deixou de lado a possibilidade de, para casos especiais em que há necessidade do técnico se deslocar ao local, este poder solicitar directamente através da interface do POS o carregamento de uma nova aplicação EFT dando assim início ao processo de forma manual.

O principal requisito para que um POS possa implementar esta funcionalidade é a possibilidade de carregar uma nova aplicação EFT sem necessidade de alteração física do terminal, ou seja, a aplicação EFT tem que residir num suporte de leitura/escrita como seja uma EEPROM ou disco rígido, e ter espaço de memória suficiente para alojar as duas aplicações EFT, a que se encontra em funcionamento e a nova aplicação.

Actualmente nem todos os terminais em funcionamento podem implementar as funcionalidades requeridas pela proposta descrita nesta tese, no entanto, a evolução tecnológica e a renovação do parque de terminais que tem sido uma constante ao longo do tempo sugere que no espaço de 1 a 3 anos seja possível reunir as condições para empregar a solução de forma universal.

A ideia base consiste na transferência da aplicação EFT do fornecedor de software para os terminais POS tendo o OSP como intermediário. Resumidamente o processo inicia-se com a certificação da aplicação. Findo esse processo com sucesso, por decisão do OSP a aplicação EFT é enviada para um ou mais Servidores de Descarga de Aplicações (SDA) dedicados a procederem à transferência da aplicação EFT para os POS.

Como a iniciativa de comunicação é sempre do POS, qualquer transacção electrónica começa pelo envio duma mensagem do POS para o SSP. De alguma forma estabelece-se uma relação entre a aplicação e o modelo de POS para os quais a aplicação se destina por forma a poder ser detectada no âmbito da realização dum serviço de pagamento automático a necessidade de dar início ao processo de actualização. Uma vez dado o início ao processo o POS comunica com o SDA e recebe a nova aplicação.

Este trabalho serviu de base para a elaboração dos artigos Secure Updates on Point of Sale Devices, apresentado na 1st International Conference on E-business and Telecommunication Networks [46] e a sua extensão Actualização Segura e Automática de Aplicações em Terminais de Venda [47], apresentado na 7ª Conferência de Redes de Computadores.

1.5 Estrutura da Tese

Este documento encontra-se organizado da seguinte forma: no Capítulo 2 é mostrado o funcionamento genérico dum sistema de pagamento electrónico, focando a sua constituição com especial detalhe em relação aos POS, serviços disponibilizados, protocolo da rede de pagamentos electrónico e infra-estrutura de segurança. Como trabalho relacionado apresenta-se uma abordagem à norma EMV 2000 que servirá de suporte à escolha da infra-estrutura de segurança utilizada por este trabalho. A transferência segura de ficheiros como é descrita na norma ISO 15668 também é aqui apresentada como suporte à realização deste trabalho.

No Capítulo 3, procede-se à descrição da arquitectura do sistema proposto, as fases e o funcionamento global do processo de actualização.

O Capítulo 4 é dedicado à concepção do sistema. Descreve-se o modelo adoptado e cada um dos protocolos necessários à sua implementação, nomeadamente, o protocolo de instalação, protocolo de transferência da aplicação, protocolo de gestão interna, e o protocolo de actualização.

No capítulo 5 faz-se a descrição da implementação dum protótipo do sistema e a avaliação do protocolo com base nos resultados obtidos em experiências com o protótipo.

Finalmente o capítulo 6 é dedicado às conclusões e trabalho futuro.

Capítulo 2 Sistema de Pagamento Electrónico

Neste capítulo, apresentamos o funcionamento duma rede de pagamentos uma vez que vamos desenvolver uma solução para o problema da actualização das aplicações dos POS. Nessa apresentação será descrito em detalhe cada um dos seus componentes, protocolos e serviços que se encontra num sistema de pagamento automático. No final do capítulo são apresentados dois trabalhos com os quais esta tese se relaciona, a especificação EMV para sistemas de pagamento e a transferência segura de ficheiros tal como se encontra descrita na norma ISO/FDIS15668.

2.1 Pagamento Electrónico

Um pagamento consiste na transferência de moeda de um agente económico (cliente) para outro (comerciante) a troco de um bem ou serviço. A troca é efectuada porque existe confiança no sistema, o cliente confia que a moeda emitida pelo Estado é aceite pelo comerciante e o comerciante confia que a moeda entregue pelo cliente será aceite por outra pessoa inclusivé o próprio Estado.

Ao longo da história os governos têm sucessivamente aumentado as medidas de segurança para impedir a falsificação da moeda que emitem. No caso da moeda cunhada, os metais são cuidadosamente escolhidos e cunhados por forma a tornar difícil e economicamente inviável a sua duplicação. Para as notas, fazem parte dessas medidas a emissão de moeda em papel especial, usando marcas de água, com elementos impressos de difícil reprodução, hologramas e outras medidas com vista à dissuasão da falsificação, para além de leis com sanções que implicam a pena de prisão.

Nos sistemas de pagamento electrónico existe também a necessidade de se proteger as transacções contra as fraudes, tendo a experiência demonstrado que com o devido cuidado no seu desenho se conseguem soluções pelo menos tão seguras como os métodos empregues nas moedas e notas de papel.

Num pagamento electrónico a moeda física é substituída por uma mensagem que ordena o débito da conta bancária do cliente e o crédito da conta bancária do comerciante. A mensagem é enviada do estabelecimento do comerciante, através de um equipamento

POS, para o SSP. O SSP comunica com o banco do cliente para que lhe seja debitado um determinado montante. Comunica também com o banco do comerciante para que lhe seja creditado o mesmo montante.

As primeiras precauções vão no sentido de dar garantias da autenticidade e integridade das mensagens que permitem que modificações não autorizadas sejam detectadas, de tal forma que as transacções de pagamento fraudulentas possam ser impedidas de serem concretizadas antes que ocorram estragos.

2.1.1 Exemplo dum Pagamento Electrónico

Como exemplo vamos considerar que um cliente deseja pagar uma conta de mercearia no valor de 200€ e receber 300€ em dinheiro usando o seu cartão bancário. Vamos assumir que a conta do comerciante está no Banco Comerciante e que a conta do cliente está no Banco Cliente (ver Figura 1).

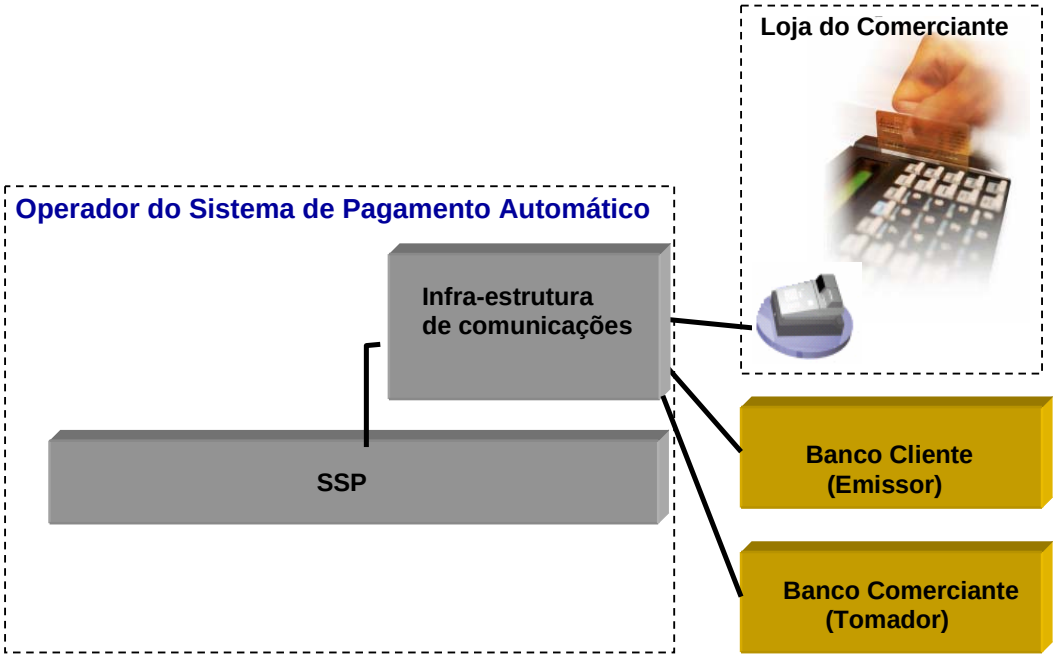


Figura 1 : Arquitectura de suporte a um pagamento electrónico.

Os dados do cartão do cliente são lidos pelo POS e o operador do terminal introduz o montante a pagar de 500€ (200€ para o pagamento da conta da mercearia e 300€ para ser dado ao cliente). O cliente insere o *Personal Identification Number* (PIN) por intermédio dum *Pin Entry Device* (PED). O POS constrói uma mensagem de compra que inclui a identificação do terminal, o montante do pagamento, o PIN e a informação constante na pista magnética do cartão do cliente. É estabelecida uma ligação com o SSP e entregue a

mensagem criptograficamente assinada pelo terminal. Dependendo do sistema de pagamentos essa mensagem pode ou não ser cifrada.

O SSP recebe a mensagem e verifica se esta é autêntica com base no seu formato, dimensão, terminal de origem e assinatura. O PIN do cliente é verificado contra a informação do cartão recebido.

Caso a validação de qualquer um dos elementos da mensagem falhe, o SSP rejeita o pedido do POS e envia-lhe uma mensagem de recusa. Nos casos em que a validação do PIN falha, normalmente o sistema permite ao cliente mais duas tentativa para introduzir o PIN correcto antes de bloquear a utilização do cartão. Se depois das tentativas adicionais a validação do PIN falhar, o SSP recusa permanentemente todas as mensagens que foram originadas com esse cartão, colocando-o em lista negra.

Assumindo que todas as validações foram bem sucedidas, o SSP identifica o Banco do Cliente pelos dados do cartão. O SSP formata uma mensagem com os dados recebidos do POS e envia-a ao Banco do Cliente. O Banco do Cliente verifica a validade da conta e, se o saldo for suficiente para cobrir os 500€, o Banco do Cliente responde com sucesso ao SSP. Caso contrário, o Banco do Cliente recusa o pedido do SSP.

Supondo que o pedido de débito é aprovado, o Banco Cliente debita o saldo da conta especificada na mensagem em 500€. Uma vez recebida autorização de débito, o SSP envia uma mensagem ao Banco do Comerciante, identificado pelo terminal de origem da mensagem, para crédito na conta do comerciante. Depois de receber a resposta do Banco do Comerciante a confirmar o crédito na conta, o SSP envia finalmente uma mensagem ao terminal POS a indicar que a transacção foi aceite e que o pagamento foi efectuado. O talão impresso pelo equipamento faz prova do sucesso da transacção.

2.2 Componentes do Sistema de Pagamentos

O sistema de pagamentos electrónico conforme utilizado no exemplo anterior pode ser decomposto nos seguintes componentes:

- OSP;
- Bancos;
- Cartões bancários;

- Terminais de pagamento;
- Elos de comunicação;
- Comerciante;
- Cliente.

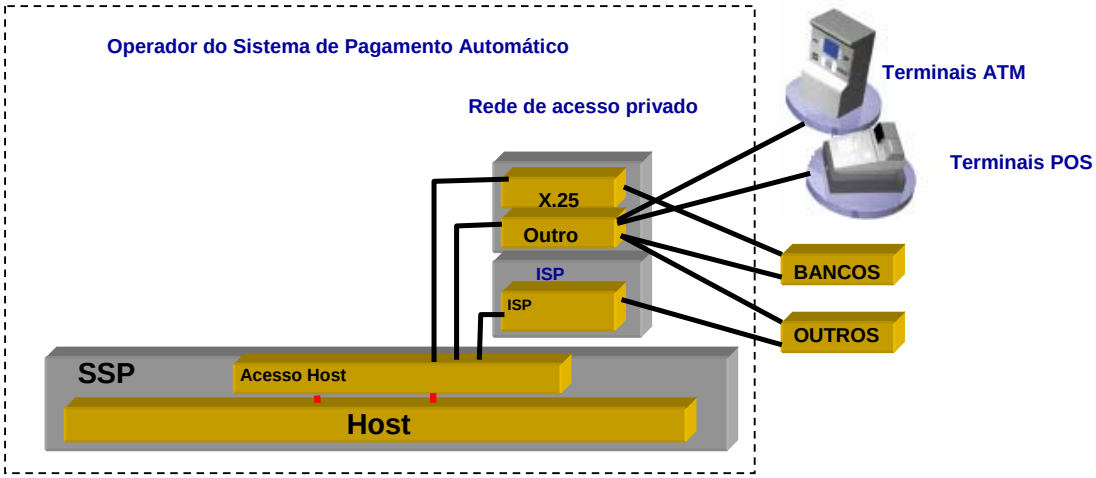


Figura 2 : Arquitectura dum Sistema de Pagamentos.

Cada um destes componentes encontra-se interligado através de uma rede de comunicações que pode pertencer a um operador de comunicações público ou privado (ver Figura 2).

2.2.1 Operador do Sistema de Pagamentos

O OSP é responsável pela disponibilidade dos serviços, interagindo com todos os outros intervenientes e monitorando o estado das comunicações e terminais. É o componente que gere os terminais POS e ATM tanto ao nível das infra-estruturas como dos serviços disponibilizados, recebendo e processando as mensagens enviadas pelos terminais, garantindo e supervisionando a segurança e integridade da informação recebida e processada.

Ao nível do processamento de serviços, com base nos dados do cartão (magnético ou *chip*) extraí o *Bank Identification Number* (BIN) para determinar qual o banco e respectivo centro de autorizações para onde as mensagens de autorização (suponhamos débito ou crédito de uma conta) devem ser encaminhadas e qual a natureza dos contratos a usar para aplicação de eventuais taxas de utilização, de câmbio ou outras.

2.2 Componentes do Sistema de Pagamentos

Como é facilmente perceptível poderão existir diversos protocolos de comunicação envolvidos, dependendo dos componentes intervenientes na comunicação com o OSP.

O OSP estabelece acordos com outras entidades homólogas ou bancos para a aceitação mútua de serviços de pagamentos com base nos cartões por eles emitidos, possibilitando a aceitação de um serviço desencadeado por um cartão emitido por qualquer banco em qualquer parte do mundo.

No caso Português, no início da década de 80, a comunidade bancária portuguesa criou um modelo de cooperação interbancária em que o primeiro projecto desenvolvido foi a rede de ATMs que iniciou o seu funcionamento em 1985. Após o período de lançamento, que durou cerca de dois anos, a rede aumentou significativamente não só em números de terminais, como também em serviços disponibilizados.

A rede de ATMs funciona totalmente em *online* (sempre ligado) o que permite uma maior segurança das transacções e verificar o estado de funcionamento dos equipamentos. Neste último caso é possível disponibilizar às empresas de manutenção um serviço automático de comunicação de avarias oferecendo ao cliente final uma maior qualidade e disponibilidade dos serviços.

O segundo serviço com grande impacto junto do grande público, o Pagamento Automático, foi lançado em 1987 com um terminal de origem francesa num conjunto restrito de ambientes. Pela primeira vez foi possível efectuar transferências electrónicas de fundos no ponto de venda, onde, até aí, só era possível utilizar cartões de crédito reservados a uma elite.

A evolução do número de terminais ao longo dos anos apresenta dois períodos de forte crescimento: nos primeiros anos da década de 90 em que o Pagamento Automático foi alargado à aceitação de cartões de crédito e aos telefones públicos, e em 1995 com o lançamento do Porta Moedas Multibanco (PMB) que acelerou novamente a contratação de POS em ambientes em que o pagamento com dinheiro era preponderante.

O serviço de Pagamento Automático é também usado de forma popular no pagamento de portagens e serviço de Via Verde.

2.2.2 Bancos

A abertura do sector bancário aos investidores bancários em 1983 e a privatização parcial dos bancos detidos pelo Estado Português iniciada em 1989 proporcionaram um novo ímpeto à diversificação, modernização e competição do mercado financeiro. A perspectiva de adesão ao mercado único e a instalação de um crescente número de bancos estrangeiros levou à expansão de novos sectores de mercado.

Desde 1986 que a legislação Portuguesa sofreu alterações para se adaptar à legislação comunitária. Fundamentalmente tais alterações focaram-se nos seguintes aspectos: definição das instituições de crédito; regras de operação, concessão e revogação de licenças para o estabelecimento de instituições de crédito; regras de supervisão e controlo das instituições de crédito; regras de solvência e rácios de liquidação; e promoção da competição.

Devido à natureza da sua actividade, as instituições de crédito e as companhias financeiras são os principais fornecedores dos serviços de pagamento. Esta actividade é explicitamente identificada em regulamentos estabelecidos pelo Governo e pelo banco central no seu papel de autoridade de política monetária.

O decreto-lei 298/92, que regula as instituições de crédito e as companhias financeiras, estipula que as instituições de crédito são instituições cuja actividade consiste em receber depósitos e outros fundos monetários do público em geral e em conceder crédito por sua conta.

Em 30 de Dezembro de 1994, foi constituído um fundo de garantia no qual todas as instituições que recebem depósitos fazem parte, e que protege os depositários mais pequenos e por sua vez a estabilidade do sistema bancário.

Os bancos fazem a gestão e controlo das contas dos seus clientes e no âmbito do sistema de pagamentos, podem tomar os seguintes papeis:

Banco Emissor (*Issuer*) – O cliente que deseja aceder à rede de pagamentos efectua o seu pedido de adesão e recebe um cartão de plástico emitido pelo banco que contem uma banda magnética e/ou *chip* que identifica por um lado a instituição financeira dentro da rede de pagamentos e por outro lado o cliente dentro da própria instituição. Efectua o débito/crédito da conta do cliente em função das transacções recebidas do OSP.

Banco Tomador (*Acquirer*) – Certifica perante a entidade que gere o sistema de pagamentos que o seu sistema de processamento está conforme as regras especificadas. Efectua contratos e distribui os terminais POS aos comerciantes que desejam aderir ao sistema de pagamentos. Processa as transacções dos terminais credita/debita a conta do comerciante e participa nas acções de compensação interbancária.

2.2.3 Cartões Bancários

Os primeiro cartões de crédito em plástico surgiram no inicio dos anos 70. Estes eram dotados de uma gravação em relevo na qual constava um número que identificava a instituição emissora do cartão, o número de conta do cliente, o número e data de expiração do cartão. Para a realização de um pagamento era utilizada uma nota de crédito que teria que ser preenchida pelo comerciante. Desta constavam o montante e a identificação do estabelecimento comercial. O comerciante colocava o cartão num "gravador" manual juntamente com a nota de crédito. Ao passar o "gravador" sobre o cartão, a gravação em relevo no cartão impressionava a nota de crédito através de um papel de carbono, ficando registado os dados do cartão. O possuidor do cartão assinava a nota de crédito e o comerciante validava a assinatura constante no verso do seu cartão e contra a constante no bilhete de identidade.

Sensivelmente no ano de 1986 surgem os primeiros cartões bancários de plásticos contendo toda a informação relativa à instituição de emissão do cartão, data de expiração do cartão, número de conta e número de cartão numa banda magnética [2]. Desta forma os dados poderiam ser lidos de forma automática por leitores de pistas magnéticas.

Até agora o método mais conveniente para a identificação ou autenticação em uso pelas instituições financeiras é a combinação de algo que o cliente do banco possui, o cartão bancário, com algo que só o cliente sabe, o PIN. A correspondência única entre o número da conta do cliente contida na pista magnética do cartão com o PIN memorizado serve para a identificação do cliente. A posse do cartão sem o PIN ou o conhecimento do PIN sem o cartão correspondente, é insuficiente para que um impostor ganhe acesso ao sistema. A norma ANSI X9.8 [14] estabelece o standard para a gestão e segurança dos PIN.

Hoje em dia, a segurança com base em cartões com pista magnética está a ser posta em causa porque é fácil obter a tecnologia que permite a cópia do conteúdo da pista do cartão para outro cartão. Mesmo que o conteúdo esteja cifrado, a criptografia não protege quanto

a este tipo de exposição dos dados. No entanto, os avanços recentes na tecnologia tornaram possível incorporar um microprocessador num cartão de plástico, permitindo efectuar os cálculos necessários à identificação e autenticação directamente no cartão em vez do ponto de entrada do sistema. Além disso, a capacidade adicional obtida com esta tecnologia permite guardar no cartão outro tipo de informação referente à conta do cliente. O efeito conseguido é a produção de um cartão que para além de inteligente é seguro. A Europay, Mastercard & Visa através da especificação EMV **Error! Reference source not found.** disponibilizam a informação para o desenvolvimento de um sistema de pagamentos electrónico baseado em cartões inteligentes.

Em Portugal até 1995 predominavam os cartões bancários com banda magnética, desde então a esta parte a tecnologia *chip* tem vindo a ganhar importância, nomeadamente no uso do PMB, em aplicações de fidelidade (ClubSmart) ou de caracter administrativo como é exemplo o cartão para abastecimento de gasóleo agrícola. Com o compromisso assumido pela banca portuguesa na adopção do standard EMV, brevemente a tecnologia *chip* terá tanta ou mais importância do que a tecnologia baseada em pista magnética.

2.2.4 Terminais de Pagamento

Os terminais de pagamento são a interface humana do sistema de pagamentos para o cliente e o comerciante. São os típicos terminais ponto de venda POS que permitem a um comerciante dotar o seu estabelecimento da capacidade de aceitar pagamentos electrónicos.

Os POS podem ser classificados segundo:

- Ambiente de operação: atendidos ou *self-service* (não atendidos);
- Comunicação: *online* ou *offline*;
- Controlo de operação: instituição financeira, comerciante ou detentor do cartão.

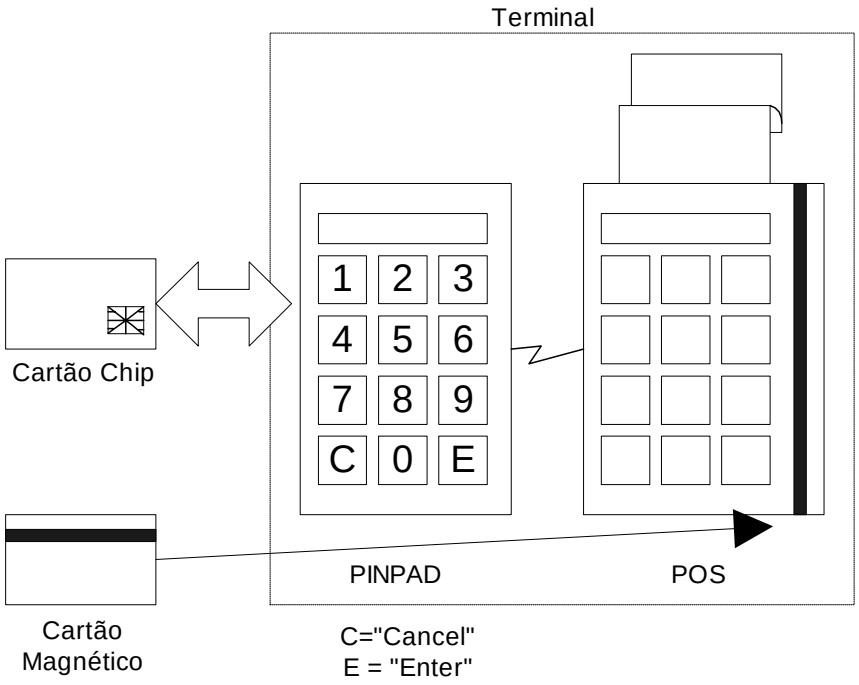


Figura 3 : Exemplo dum terminal POS atendido.

Um terminal atendido (ver Figura 3) é caracterizado por necessitar de um operador para realizar os serviços de pagamento electrónico. A escolha do serviço é seleccionada pelo operador recorrendo ao teclado e ao ecrã da interface humana disponibilizada pelo terminal. São exemplo deste tipo de terminais os POS que equipam as caixas registadoras dos supermercados e lojas do comércio a retalho.

Os terminais não atendidos caracterizam-se pelo oposto, isto é, não necessitam de operador e possuem um leque de serviços mais reduzidos, normalmente resumindo-se ao serviço de compra. Os terminais mais comuns deste tipo são os que equipam os postos de abastecimento de combustível *self-service* 24 horas por dia, em que, é o próprio utilizador que manipula o terminal.

Quanto ao tipo de comunicação, os terminais que oferecem maior segurança são os terminais *online*. Caracterizam-se por comunicarem com o SSP sempre que realizam operações do cliente, fazendo depender a conclusão da operação do resultado transmitido pelo SSP.

Os terminais *offline*, são caracterizados por fazer depender o resultado das operações do SSP sempre que possuem ligação, mas também de dados internos quando não tiverem ligação. Para que tal seja possível, o SSP transmite para o POS uma tabela designada de

"lista negra", na qual são colocados todos os cartões aos quais se deve recusar serviços. Este tipo de solução apresenta um problema de segurança pois o intervalo de tempo que separa a inserção de um cartão em lista negra e a sua transmissão para o POS pode ser suficiente para que um cartão realize dezenas de operações.

Os serviços disponibilizados pelo POS podem ser controlados de três formas diferentes:

- Pode ser controlado pela instituição financeira recusando ou aceitando os serviços solicitados pelo POS;
- O comerciante pode controlar que serviços disponibiliza aos seus clientes;
- O detentor do cartão pode contratar mais ou menos serviços disponibilizados pelo cartão, fazendo depender a concretização da operação dos serviços contratados.

2.2.4.1 Características Físicas

As características físicas dos terminais de pagamento são determinadas por normas internacionais **Error! Reference source not found.** e dependem dos serviços prestados pelo terminal, o meio ambiente onde opera e a configuração do terminal. De acordo com tais normas, um terminal POS no mínimo deve possuir:

- Visor para apresentações de mensagens ao cliente e operador com pelo menos 36 caracteres (2 linhas de 16 caracteres);
- Teclado para introdução de montantes da operação e outras teclas adicionais como confirmação, anulação e correcção;
- Equipamento de comunicações para ligação à rede de pagamentos;
- Módulo de segurança para o armazenamento de chaves e realização de operações criptográficas;
- Protecção de memória por forma a não apagar ou alterar os dados no terminal, incluindo chaves criptográficas;
- Teclado para a introdução de PIN (ou Pinpad);
- Leitor de cartões magnéticos e/ou chip;
- Impressora de talões;
- Relógio capaz de manter um desvio de até 1 minuto por mês.

2.2.4.2 Módulo de Segurança

O módulo de segurança é o dispositivo que efectua todas as operações criptográficas do terminal POS. É nele que residem as chaves criptográficas que assinam e autenticam as mensagens trocadas entre o POS e o SSP e que cifram o PIN do cliente dando origem ao *Pinblock* ou PIN cifrado. Um módulo de segurança é construído de forma a não possibilitar a observação dos dados internos, estando dotado de tecnologia que detecta diferentes níveis de intrusão, destruindo por completo a informação guardada no seu interior sempre que ameaçado.

Cada módulo de segurança possui a sua própria memória, processador e bateria. Os componentes electrónicos estão protegidos por várias grelhas de metal mergulhados num banho de resina epóxica que os sela por completo. Caso seja forçado mecanicamente, a grelha parte, activando o mecanismo de autodestruição. Normalmente exige-se que o núcleo destes equipamentos seja baseado num micro-controlador *tamper proof* possuindo diferentes níveis de detecção de intrusão e protecção de dados [4]. Alguns destes equipamentos utilizam o algoritmo standard NBS DEA [40]. A gestão do PIN deve ser feita de acordo com as normas ISO 9564 parte 1 e 2 [18]. A autenticação de mensagens é efectuada de acordo com a norma ISO 8731 parte 1 e 2 [19] e a gestão de chaves é efectuada de acordo com a norma ISO 11568 parte 1, 2 e 3 [21].

O módulo de segurança está fisicamente ligado ao POS. Um canal de comunicações entre ambos permite a troca de comandos para a realização das diversas operações de cifra, decifra, gestão de chaves e captura de PIN.

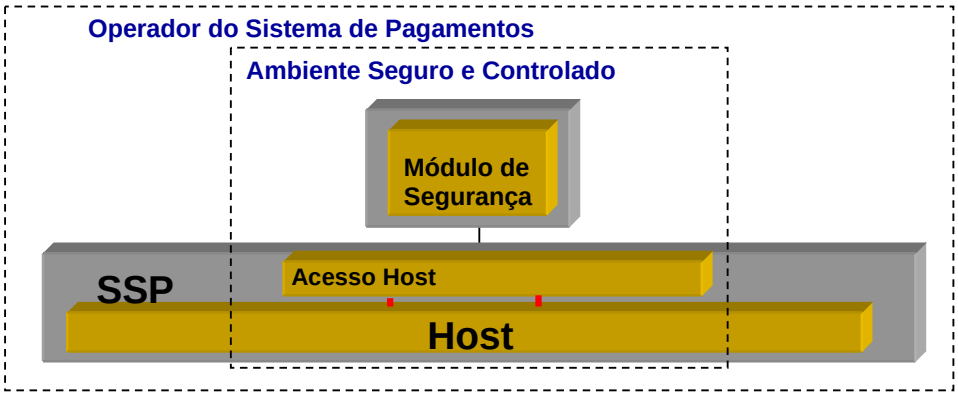


Figura 4 : Carregamento de chaves no módulo de segurança.

Na primeira fase do ciclo de vida, o módulo de segurança é ligado directamente ao SSP num ambiente seguro e controlado (ver Figura 4). Um conjunto de mensagens trocadas

entre estes dois equipamentos permite atribuir ao módulo de segurança um identificador lógico único e as chaves iniciais do sistema. As chaves são transferidas para o módulo de segurança por mensagens que organizam a informação em blocos de dados contendo: a chave propriamente dita, a sua identificação e a versão.

O módulo de segurança armazena diversas chaves. Entre elas as chaves para cifrar o PIN, e as chaves para assinar e verificar a assinatura das mensagens. São identificadas por um identificador único e todas as operações usam este identificador para que se possa aceder à chave apropriada. O identificador do POS em conjunto com o identificador do módulo de segurança permite ao SSP identificar as chaves a aplicar para verificar e gerar as assinaturas das mensagens trocadas.

O SSP pode actualizar as chaves guardadas no módulo de segurança trocando mensagens com o POS nas quais são incluídas as novas chaves. O POS por intermédio de comandos apropriados actualiza as chaves no módulo de segurança.

Um dos pontos mais sensíveis de um sistema de pagamentos é a integridade do código PIN. Colocando um teclado como parte integrante do módulo de segurança consegue-se com que o PIN nunca viaje em claro fora do módulo, assegurando um maior grau de privacidade e protecção das pessoas.

O teclado para a introdução de PIN deve obedecer à norma ISO 9564 [18] (ver Figura 5).

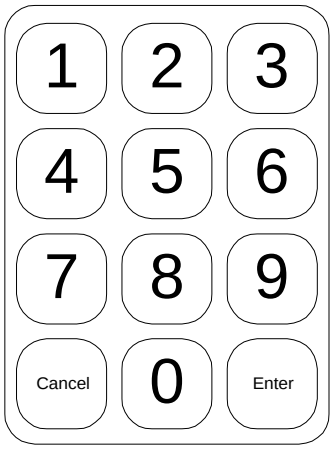


Figura 5 : *Layout* do PED segundo a norma ISO 9564.

2.2.4.3 Ciclo de Vida

O ciclo de vida de um POS é essencialmente constituído por quatro fases: iniciação, instalação, operação e abate.

- **Iniciação** - A primeira fase ocorre no momento da contratação do serviço de pagamentos. O terminal é registado na base de dados do SSP sendo-lhe atribuído um identificador único na rede de pagamentos. São lhe fornecidos parâmetros específicos de comunicação em função do local onde é instalado e do tipo de comunicação utilizado.

- **Instalação** - A segunda fase ocorre no momento da instalação do POS no seu local definitivo. Nessa altura o terminal é configurado com os dados atribuídos para que possa comunicar com o SSP e identificar o comerciante associado.

- **Operação** - A terceira fase corresponde à actividade do terminal durante a qual são realizados os serviços de pagamento electrónico.

- **Abate** - A fase de abate ocorre quando o terminal é removido do local para onde foi contratado. Nessa altura, quaisquer mensagens originadas desse POS são rejeitadas pelo SSP e todas as chaves residentes no módulo de segurança são destruídas.

2.2.4.4 Requisitos de Segurança

Existem diversos requisitos de segurança associados aos terminais de pagamento. Por exemplo, os materiais de construção usados no seu fabrico devem ser de difícil aquisição para dificultar ao máximo a construção de equipamentos que possam ser confundidos com os originais. Um oponente pode obter o PIN, fazendo os clientes usarem um equipamento que possui o comportamento funcional equivalente ao de um legítimo terminal, mas que está sobre o seu controlo. Neste caso, o falso terminal revela o PIN inserido e regista a informação do cartão bancário. Esta informação pode depois ser utilizada num terminal legítimo para efectuar transacções. Em relação a este tipo de ataques a criptografia não providência uma solução eficaz para o problema da protecção da informação, uma vez que essa informação pode ser atacada antes de entrar no sistema.

Em relação ao armazenamento das chaves criptográficas que residem no terminal também é necessário um nível de segurança elevado. Um adversário poderia roubar o terminal e

procurar as chaves ou alterar o seu valor podendo forjar mensagens falsas, assinando-as correctamente, fazendo-as passar como mensagens legítimas. Apesar de em sistemas bem desenhados este tipo de ataque possa levar muito tempo a ser realizado, não é infinito. Medidas de segurança, como sensores que detectam a penetração no terminal, podem ser ultrapassados ao ter o tempo e os recursos disponíveis para o efeito. Por outro lado a detecção do roubo do terminal e a resposta apropriada para invalidar o terminal podem salvaguardar dados futuros.

Os ataques desferidos pelos que têm autorização de operar com o terminal, têm vantagem sobre os outros atacantes, somente em relação ao tempo disponível. Pois não necessitam de roubar o terminal evitando o levantamento de suspeitas.

Como os terminais são em número elevado e construídos de forma económica, e como normalmente são instalados em locais pouco seguros, os segredos guardados no terminal devem ser muito poucos e sempre que possível o terminal deve estar dotado de mecanismos de destruição dessa informação quando ameaçado.

2.2.5 Elos de Comunicação

Os elos de comunicação interligam os equipamentos da rede de pagamentos, nomeadamente os POS localizados nos estabelecimentos comerciais, o SSP e os servidores das instituições bancárias. Tradicionalmente tem sido utilizada exclusivamente a rede pública de dados, a funcionar em X.25 [6]. Mais recentemente com as diversas evoluções tecnológicas, tornaram-se vulgares outros tipos de comunicação como *Data Over Voice* (DOV) [28], GSM [29] ou mesmo TCP/IP [3].

Todos os dias os sistemas de pagamentos transferem milhões de Euros de forma electrónica entre diversas instituições e indivíduos. Essas transacções só podem ser processadas de forma segura se for garantida a integridade das mensagens. Os meios de comunicação são sensíveis à intercepção de mensagens por um grande número de técnicas que permitem ataques passivos (escuta) e/ou ataques activos (alteração/substituição do conteúdo das mensagens). Quando se usa uma rede fixa de comunicações, nem sempre é necessário interpor um equipamento na linha de comunicações para captar os dados. Por exemplo, no caso em que se usa comunicação por satélite ou microondas basta uma antena. Se for permitida a alteração do conteúdo das mensagens, pode-se facilmente modificar os dados para beneficiar o infractor. Por

exemplo, aumentando a quantia da transferência, alterando a conta de destino do crédito ou transformando uma mensagem negativa em positiva.

As técnicas de autenticação de mensagens tentam eliminar a exposição a estes factores. Permitem ao receptor verificar onde a mensagem foi originada, se é actual, qual o seu destino e se foi ou não alterada [5].

2.2.6 Comerciante

O comerciante participa na actividade do serviço de pagamentos a diversos níveis:

- Obtem o terminal POS para aceitação do serviço de pagamentos junto do banco tomador;
- Aceita para pagamento os cartões aderentes ao serviço;
- Obtem os fundos resultantes da realização das transacções de pagamento electrónico.

2.2.7 Cliente

O cliente efectua todas as actividades associadas com a utilização do cartão. Nelas incluem-se:

- A adesão ao serviço de pagamento pela contratação junto do banco emissor;
- Escolha, memorização e alteração do PIN associado;
- Apresentação do cartão nos dispositivos que aceitam o serviço de pagamentos (ATM, POS, maquinas de venda automática, telefones, etc.).

2.3 Serviços Disponíveis na Rede de Pagamentos

Os serviços disponibilizados pela rede de pagamentos dependem do sistema e do modelo de negócio associado. No caso particular da rede Multibanco os serviços podem ser classificados em quatro categorias diferentes, nomeadamente: serviços de manutenção, de gestão, de cliente e de actualização e segurança.

2.3.1 Serviços de Manutenção

Os serviços de manutenção são usados no contexto da manutenção do POS. Possibilitam ao pessoal técnico fazer a configuração do equipamento, instalação, testes de comunicação e a realização de consultas ao SSP sobre o estado do POS.

2.3.2 Serviços de Gestão

Os serviços de gestão possibilitam ao operador do POS a realização de consultas sobre as operações dos clientes que foram efectuadas, nomeadamente, conhecer os totais de pagamentos efectuados, de devoluções, de comissões a pagar e outras consultas genéricas. Nesta categoria incluem-se também os serviços de abertura e fecho de período contabilístico que permitem a utilização do POS.

Os serviços de abertura e fecho do período contabilistico definem a janela temporal de actividade do POS. Normalmente coincide com a abertura e fecho do estabelecimento comercial ao público. Este conceito permite controlar o nível de risco do POS, podendo o SSP recusar transacções se a janela temporal estiver aberta à muito tempo.

A realização destes serviços exigem o uso de um cartão magnético com características especiais que contém entre outros dados a instituição bancária e a conta do comerciante para onde são creditados ou debitados os montantes associados aos serviço de cliente.

2.3.3 Serviços de Cliente

A operação de compra é universalmente encontrada em todos os POS. A rede Multibanco disponibiliza outros serviços nesta categoria, nomeadamente, consulta de saldos, consulta de movimentos, pagamento de serviços e pedidos de livros de cheque.

2.3.4 Serviços de Actualização e Segurança

Estes serviços fazem a actualização dos parâmetros do terminal e a gestão dos parâmetros de segurança do POS. Incluem-se a actualização dos dados de comunicação e a evolução dinâmica de chaves, para a cifra do PIN, assinatura e verificação das mensagens.

O comportamento do terminal para a realização destes serviços é diferente dos restantes uma vez que a iniciativa de comunicação parte sempre do POS. Assim, sempre que há necessidade da realização de uma actualização, o SSP incluí, na mensagem de resposta a

um serviço pedido pelo POS, o pedido de realização de um serviço de actualização e segurança. Desta forma o SSP pode gerir remotamente alguns dos parâmetros mais críticos do POS.

2.4 Infra-estrutura de Segurança

A infra-estrutura de segurança do OSP, baseado em técnicas e conceitos do uso de criptografia simétrica, permite a realização de transacções seguras entre o POS e o SSP.

O hardware, software, políticas e procedimentos desenvolvidos garantem a autenticidade das mensagens trocadas bem como a emissão, distribuição e revogação das chaves do sistema.

2.4.1 Serviços de Segurança

A base de toda a confiança é o SSP e toda a infra-estrutura é dependente da sua chave secreta. A infra-estrutura de segurança suporta uma série de serviços que permitem de forma eficaz garantir a fiabilidade das chaves emitidas.

Entre os serviços disponibilizados incluem-se:

Geração, armazenamento seguro e revogação de chaves de sessão;

- Geração de chaves para transporte, autenticação de mensagens e geração de *Pinblock* com base na chave mestra;
- Distribuição de chaves;
- Armazenamento de chaves, que assegura a recuperação das chaves entretanto actualizadas quando se detectam falhas nas actualizações;
- Revogação de chaves;
- Gestão do modo de geração do *Pinblock*;
- Iniciação e abate dos módulos de segurança e *Pinpad*.

Conforme já foi referido anteriormente, esta infra-estrutura usa o algoritmo standard NBS DEA. A gestão de PIN está de acordo com as normas ISO 9564 parte 1 e 2, a autenticação

de mensagens é efectuada de acordo com a norma ISO 8731 parte 1 e 2 e a gestão de chaves efectuada de acordo com a norma ISO 11568 partes 1, 2 e 3.

Numa infra-estrutura de chave secreta a segurança do sistema depende da protecção da chave secreta, que deve ser protegida da melhor forma possível. Daí a necessidade de hardware especial para a proteger.

A rede de pagamentos fechada não admite quaisquer outros elementos que não os mencionados. E não existe senão um único nível de hierarquia, sendo que o SSP ocupa o lugar de topo e os terminais, módulos de segurança e Pinpad o lugar imediatamente inferior

2.5 Protocolo da Rede de Pagamentos Electrónico

O sistema de pagamentos electrónico disponibiliza a execução de serviços requisitados através dos terminais POS. A cada serviço ou transacção corresponde um par de mensagens designadas por *pedido* e *resposta*. As mensagens de pedido são sempre originadas pelo POS e as mensagens de resposta sempre originadas pelo SSP.

A maioria dos sistemas de pagamentos segue a norma ISO 8583 [17] na implementação do protocolo EFT, mas é comum existirem sistemas de pagamentos que seguem implementações proprietárias, como é o caso de Portugal, Espanha e Itália.

Segundo esta norma, cada mensagem é composta por um *Message Transaction Identifier* (MTI), um ou dois *Data Element Bitmaps* seguido dos *Data Elements* propriamente ditos.

Cada mensagem é univocamente identificada pelo valor do MTI. Cada *bit* nos *Bitmap* refere a presença ou ausência na mensagem de determinado *Data Element*. Numa transacção de compra o *Primary Bit Map* e o *Secondary Bit Map* indicam a presença na mensagem dos elementos: identificador lógico do POS, identificador lógico do módulo de segurança, data e hora do pedido do serviço, conta do cartão, número de sequência da mensagem, o montante, a pista do cartão e o *Pinblock* do cliente.

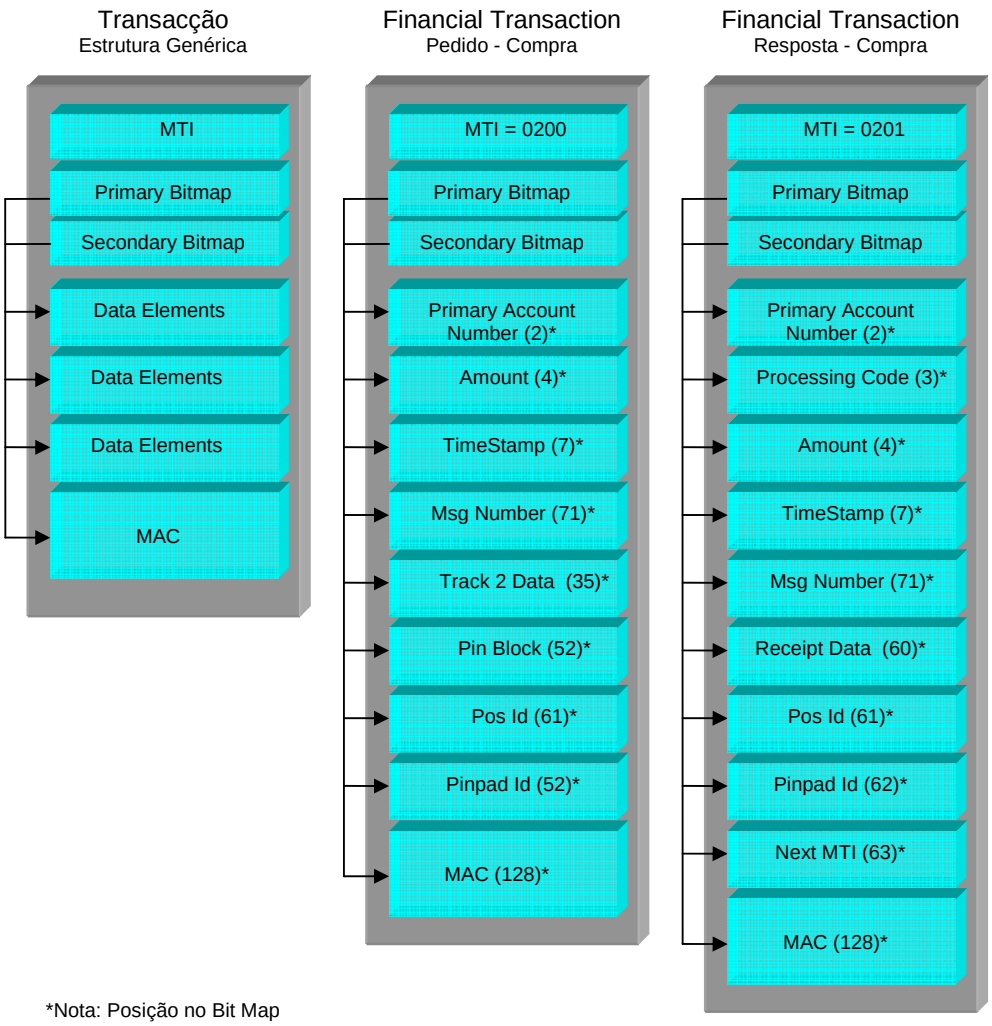


Figura 6 : Estrutura genérica da mensagem segundo a norma 8583

A mensagem de resposta inclui entre outros *Data Elements* o resultado do processamento da transacção (*Processing Code* bit 3) e a próxima transacção a ser executada pelo POS (*Next MTI* bit 63). As mensagens são protegidas com *Message Authentication Codes* (MAC) [12][13] que assegura protecção contra ataques de integridade e autenticidade. Como exemplo mostra-se na Figura 6 a estrutura genérica das mensagens segundo a norma 8583.

2.6 A Especificação EMV

Em 1996 as empresas Europay, MasterCard e Visa lançaram em conjunto um grupo de documentos conhecidos por especificação EMV'96. Actualmente designados por EMV2000, estes documentos descrevem para os cartões *chip* e terminais EMV compatíveis:

- O conjunto mínimo de funcionalidades para assegurar a correcta operação e compatibilidade, independentemente da aplicação a usar num ambiente transaccional EMV compatível [35];

- O conjunto mínimo de funcionalidades de segurança para garantir a correcta operação e compatibilidade [36];

- A definição dos procedimentos necessários para a execução duma transacção de pagamento num ambiente de interacção internacional [37];

- A definição dos requisitos obrigatórios, recomendados e opcionais para suportar a aceitação de cartões *chip* EMV compatíveis [38].

Entre as principais motivações para a criação desta especificação encontram-se:

- A redução da fraude e o aumento da confiança dos utilizadores na utilização dos sistemas de pagamento, baseando-se na experiência da utilização dos cartões *chip* em sistemas de pagamento em funcionamento (como por exemplo o sistema francês);

- Estender a utilização dos cartões de pagamento para ambientes inseguros (como por exemplo a Internet) onde as medidas actuais de segurança baseadas em cartões magnéticos não se aplicam;

- Alcançar um maior universo de utilizadores;

- Aumentar a presença da tecnologia do cartão *chip* com a integração de múltiplas aplicações para além dos produtos bancários.

2.6.1 Modelo do Sistema de Pagamentos EMV Compatível

O modelo do sistema de pagamentos EMV compatível é composto pelas seguintes entidades:

- **Cliente** (*Cardholder*) – O detentor do cartão bancário EMV compatível;

- **Comerciante** (*Merchant*)– O detentor do terminal que aceita cartões EMV compatíveis como forma de pagamento;

- **Emissores** (*Issuer*) – Os emissores das aplicações que constam no cartão EMV compatível;
- **Tomador** (*Acquirer*)[1]– A entidade que processa as transacções dos terminais e que paga aos comerciantes;
- **Esquema de Pagamentos** (*Schemes*) - Marcas de esquemas de pagamentos, nas quais se incluem a Eurocard/Mastercard e Visa.
- **Operador do Sistema de Pagamentos –** A entidade que gere a rede de pagamentos.

Cada uma destas entidades está relacionada da forma como se mostra na Figura 7.

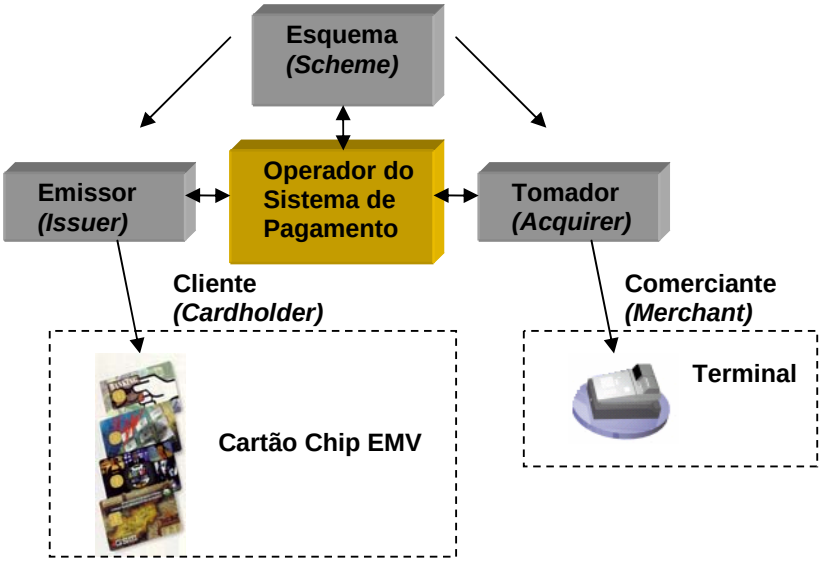


Figura 7 : Modelo do Esquema de Pagamentos EMV.

2.6.2 Aplicações EMV

O cartão bancário com *chip* EMV permite a coexistência de várias aplicações no mesmo suporte. No momento da emissão dum cartão, são inseridas no *chip* as aplicações que a entidade emissora coloca à disposição do cliente de acordo com o contrato efectuado, por exemplo, aplicações de crédito, débito, fidelidade, saúde, seguros, etc.. Cada aplicação é caracterizada por um identificador (AID – *Application Identifier*) e pela entidade emissora dessa aplicação, responsável pelos dados constantes no cartão.

[1] No caso do sistema bancário português, o operador do sistema de pagamentos acumula as funções do tomador.

Entre esses dados constam os elementos criptográficos que permitem ao terminal e ao emissor autenticar o cartão que está a ser apresentado como meio de pagamento.

Os terminais de pagamento, dependendo do país, do sistema de pagamentos e do ambiente de operação, suportam um determinado conjunto de aplicações do universo de todas as aplicações EMV existentes. O terminal informa o sistema de pagamentos sobre as aplicações que suporta. O sistema de pagamentos envia por sua vez a lista dos AIDs que está autorizado a processar. A intersecção destes dois conjuntos determina as aplicações que cada terminal pode executar.

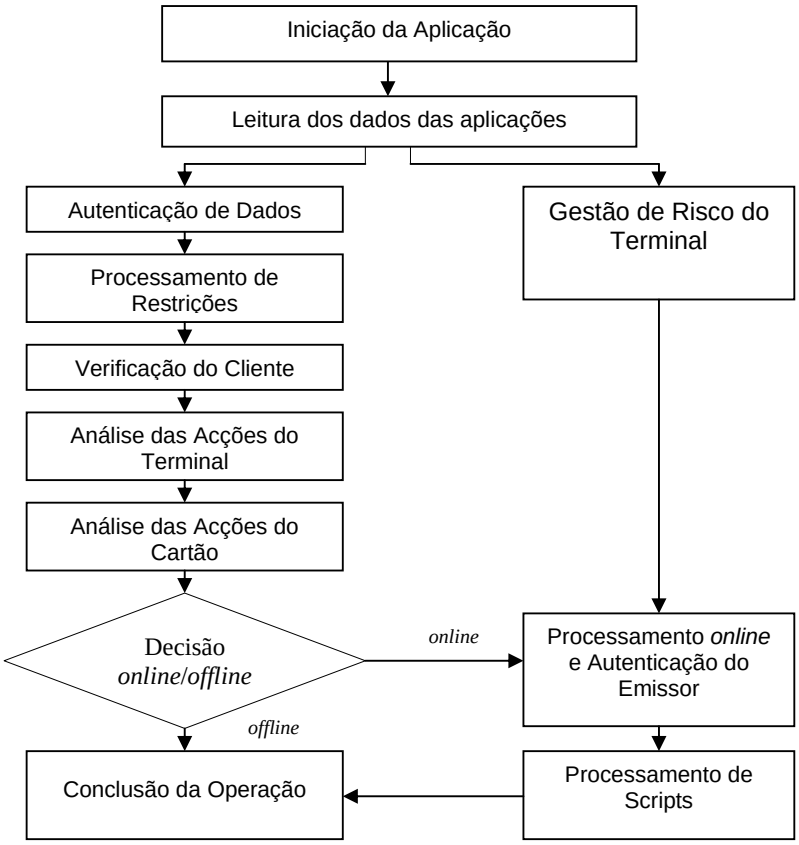


Figura 8 : Exemplo do Fluxo de Execução duma Transacção EMV.

2.6.3 Realização duma Transacção EMV

Resumidamente a sequência de acções envolvidas na realização duma transacção de compra entre um terminal e cartão EMV, são as seguintes (ver Figura 8) [37]:

- **Iniciação da Aplicação** – O terminal informa o cartão que se vai iniciar o processamento duma nova transacção e fornece-lhe informações sobre essa transacção. O terminal obtém do cartão a lista dos ficheiros que contêm os dados a

serem usados durante a realização da transacção e determina se esta é ou não autorizada;

- **Leitura dos dados da aplicação** – O terminal obtém do cartão dados dos ficheiros necessários para que se possa efectuar diversas funções usadas no processamento da transacção;

- **Autenticação de dados –** Nesta fase é determinado se é efectuada a autenticação de dados em *offline*, que tipo de autenticação é efectuada, e de que modo o sucesso ou insucesso dessa autenticação afecta o fluxo da transacção. A capacidade do chip suportar a autenticação de dados em *offline* é opcional, mas se simultaneamente o terminal e o cartão suportarem a autenticação em *offline* então esta acção deve ser executada. Dependendo das capacidades do terminal e do cartão pode ser efectuada a autenticação estática ou dinâmica;

- **Processamento de Restrições** – O objectivo desta acção é determinar o nível de compatibilidade da aplicação no terminal com a aplicação existente no *chip* e efectuar se possível os ajustes necessários para a sua execução ou se por outro lado se deve rejeitar a transacção. O processamento das restrições inclui a verificação do número da versão das aplicações e a verificação das datas de expiração;

- **Verificação do cliente** – A verificação do cliente é executada por forma a garantir que a pessoa que apresenta o cartão como forma de pagamento é o legítimo detentor do cartão para quem este foi emitido. O cartão e o terminal determinam o tipo de verificação a efectuar que pode incluir: processamento do PIN em *offline*, processamento do PIN em *online*, assinatura ou uma combinação dos métodos anteriores;

- **Gestão de Risco do Terminal** – Esta acção é realizada pelo terminal para proteger de fraudes o tomador, o emissor e o sistema de pagamentos. Garante que no caso de estarem envolvidas grandes quantias é efectuado um pedido de autorização ao emissor para a conclusão da transacção. Assegura que as transacções realizadas por um cartão são validadas periodicamente em *online* para proteger o sistema de ameaças não detectadas no ambiente *offline*;

- **Análise das Acções do Terminal** – Depois de estarem concluídas a Gestão de Risco do Terminal e todas as funções relacionadas com a realização duma transacção *offline*, o terminal toma a primeira decisão sobre se a transacção deve ser aprovada em *offline*, recusada em *offline* ou se deve ser transmitida *online* por forma a que seja o sistema de pagamentos a decidir sobre a aceitação ou recusa da transacção;

- **Análise das Acções do Cartão** – O cartão pode efectuar a sua própria análise de risco para proteger o emissor de fraude ou risco de crédito excessivo. Os detalhes dessa gestão é dependente do emissor, mas o cartão pode decidir que se complete a transacção em *online*, em *offline*, que se peça directamente a confirmação ao emissor (*referal*) ou que se rejeite a transacção;

- **Processamento Online** – O processamento *online* é executado para garantir que o emissor pode rever a decisão de autorização ou rejeição da transacção por esta se encontrar fora dos limites de risco definidos pelo emissor, sistema de pagamento ou tomador. Do ponto de vista transaccional, o conteúdo das mensagens diferem das utilizadas para a realização duma transacção baseada em pista magnética, nos elementos de dados específicos ao cartão chip. A decisão do emissor é posteriormente comunicada ao cartão para concluir a transacção;

- **Processamento de Scripts** – Um emissor pode enviar um conjunto de comandos sob a forma dum *script* para serem enviados pelo terminal ao cartão para executar acções que não sendo necessariamente relevantes para a transacção actual podem selo para a continuidade do funcionamento da aplicação no cartão;

- **Conclusão do Processamento** – Esta acção termina o processamento da transacção.

2.6.4 Autenticação do Cartão

A especificação EMV utiliza uma infra-estrutura de segurança baseada em chave pública para efectuar a autenticação dos cartões EMV.

As chaves públicas dos bancos emissores e respectivos certificados são usados para a execução de Métodos de Autenticação do Cartão (CAM – *Card Authentication Method*) onde é possível realizar para as aplicações nele existentes a Autenticação de Dados Estáticos (*Static Data Authentication*) ou a Autenticação de Dados Dinâmicos (*Dynamic*

Data Authentication). A escolha entre cada um dos métodos pode ser determinada pelo esquema de pagamento em função da importância da aplicação.

2.6.4.1 Autenticação de Dados Estáticos

Neste tipo de autenticação o emissor assina previamente um conjunto de dados estáticos do cartão para garantir a detecção de alterações ao cartão após a personalização. Durante a realização duma transacção o terminal é instruído pelo emissor do cartão da lista de dados que deve pedir ao cartão para verificar a sua autenticidade [36].

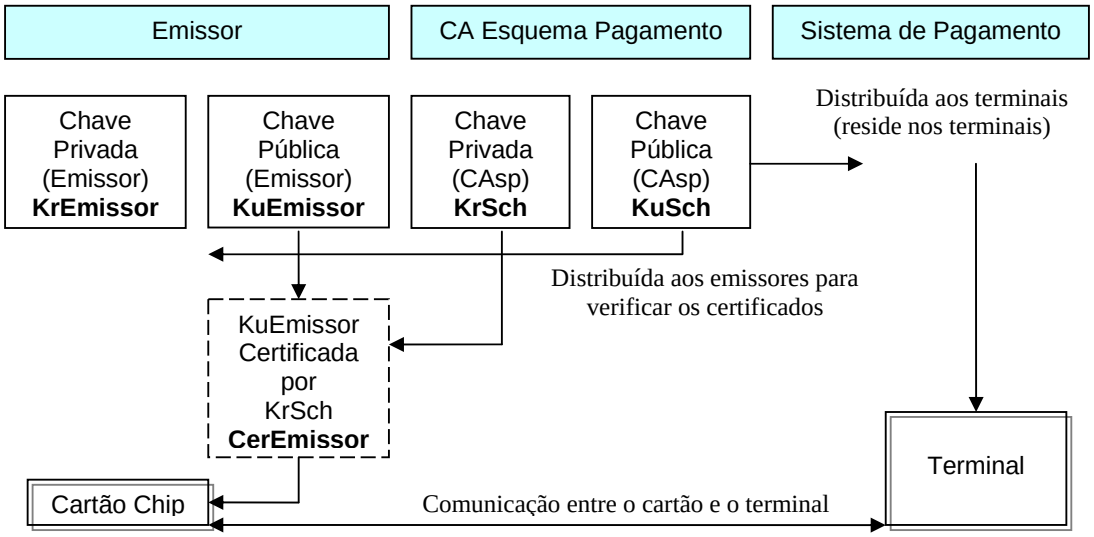


Figura 9 : Diagrama da Autenticação de Dados Estáticos.

Neste esquema de autenticação (ver Figura 9), o cartão disponibiliza ao terminal:

- *KuEmissor* (que é certificada pela CA do esquema de pagamento);
- Dados do cartão com assinatura digital assinadas pela *KrEmissor*.

O terminal:

- Usa a chave *KuSch* para verificar que a chave *KuEmissor* foi certificada pela CA do esquema de pagamento;
- Usa a chave KuEmissor para verificar a assinatura digital dos dados do cartão.

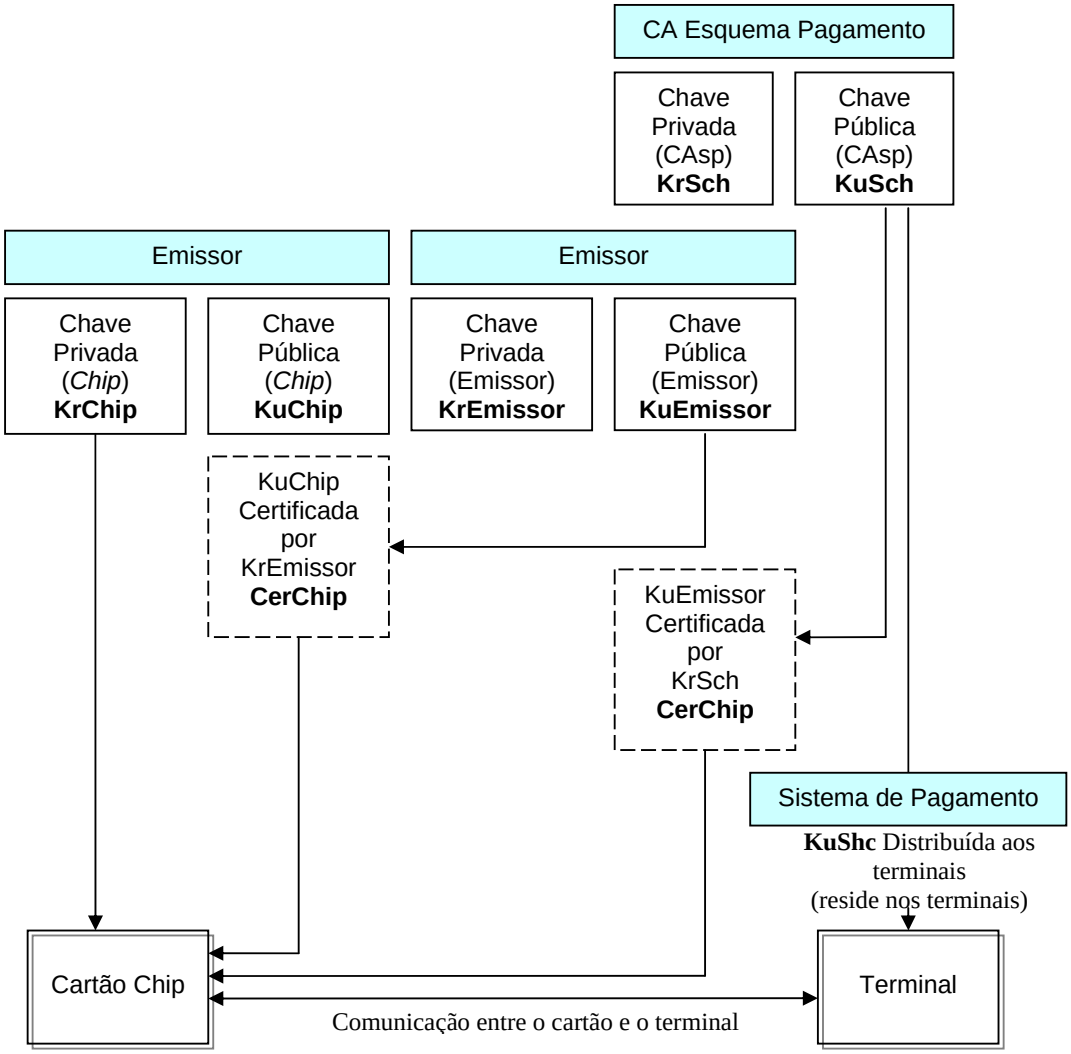


Figura 10 : Diagrama para a Autenticação de Dados Dinâmicos.

2.6.4.2 Autenticação de Dados Dinâmicos

Neste esquema de autenticação (ver Figura 10) [36], durante a realização duma transacção o cartão *chip* produz uma assinatura dinâmica sobre um desafio aleatório que recebeu do terminal. Pela verificação desta assinatura o terminal pode autenticar o cartão *chip* e confirmar a legitimidade de dados críticos no cartão.

O cartão disponibiliza ao terminal:

- *KuChip* que é certificada pelo Emissor;
- *KuEmissor* que é certificada pela CA do esquema de pagamento;
- Dados do cartão com assinatura digital.

O terminal usa:

- A chave *KuSch* para verificar que a chave *KuEmissor* foi certificada pela CA do esquema de pagamento;
- A chave *KuEmissor* para verificar que a chave *KuChip* foi certificada pelo emissor;
- A chave *KuChip* para verificar a assinatura digital dos dados do cartão.

2.6.5 Criptogramas Aplicacionais

Durante a realização duma transacção EMV, tanto o cartão como o terminal efectuam decisões sobre a aceitação da transacção, decidindo se esta deve ser processada em *offline*, em *online* ou se deve ser rejeitada.

As decisões efectuadas pelo cartão são sempre acompanhadas por um criptograma que permite ao terminal e ao emissor validar que a decisão foi efectuada por um cartão legítimo.

Por outro lado, as decisões do emissor são comunicadas ao cartão acompanhadas por um criptograma gerado pelo próprio emissor.

O criptograma aplicacional consiste na geração dum MAC (segundo a norma ISO/IEC 9797) [12] gerado sobre um dos seguintes conjuntos de dados:

- Dados referidos pelo terminal transmitidos ao cartão no comando GENERATE AC ou outro comando;
- Acedidos internamente pelo *chip.*

O algoritmo utiliza uma chave de sessão derivada da chave mestra *ICC Application Cryptogram Master Key* (MK_{AC}) [36]. Esta chave pode ser derivada a partir de dois dados do conhecimento do terminal, o número da conta primária do cartão (PAN – *Primary Account Number)* e do seu número de sequência (PAN *Sequence Number*). A gestão desta chave é da responsabilidade do emissor.

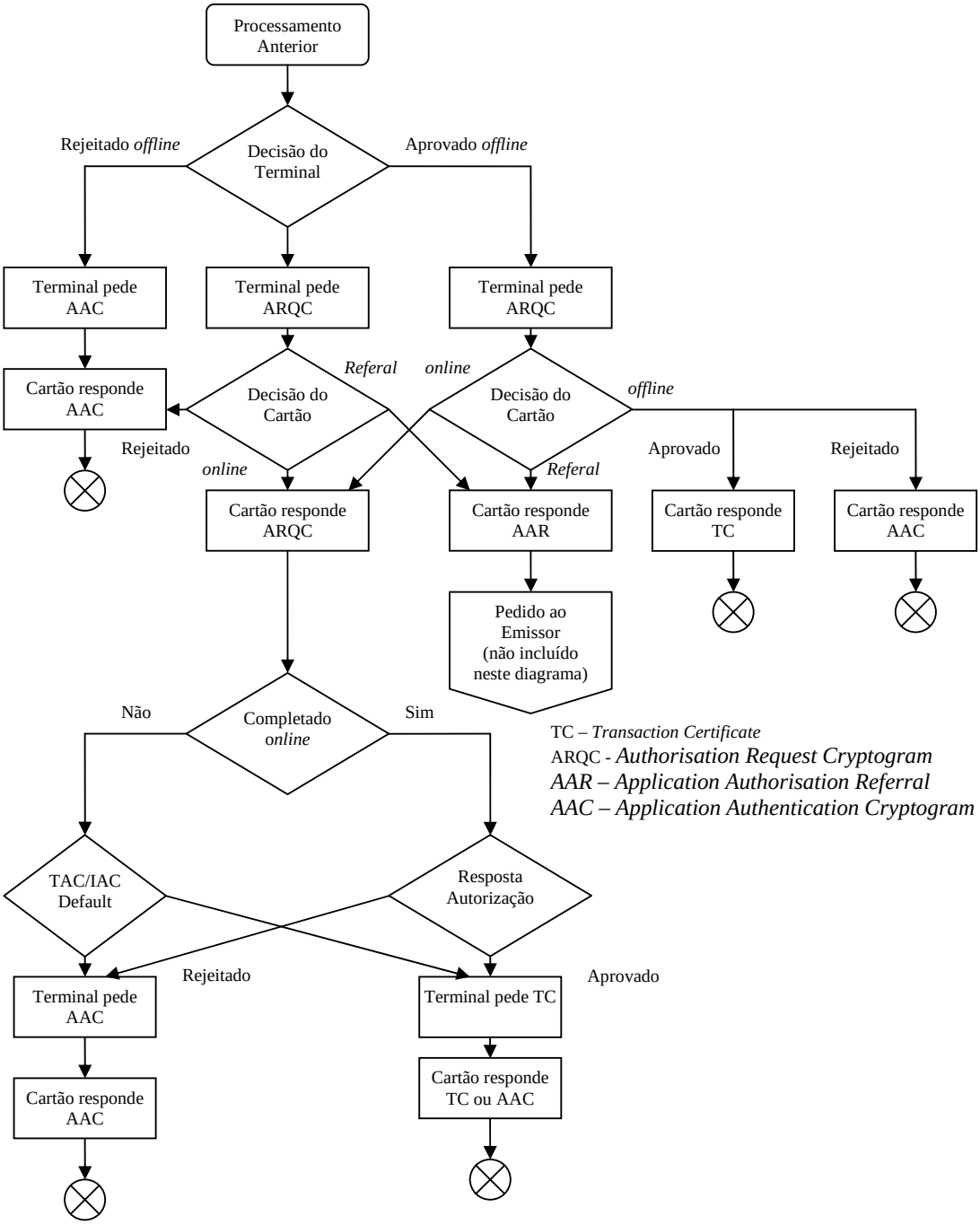


Figura 11 : Uso do comando GENERATE AC.

O fluxo de execução associado às decisões do cartão (isto é a geração do criptograma aplicacional) pode ser entendido pela análise do diagrama representado na Figura 11 no qual se apresenta o esquema de utilização do comando GENERATE AC.

Durante o processamento duma transacção o terminal executa um ou dois comandos GENERATE AC. O cartão responde a esse comando com um dos seguintes criptogramas:

- *Transaction Certificate* (TC) – Transacção Aprovada;
- *Authorisation Request Cryptogram* (ARQC) – É necessário aprovação *online*;
- *Application Authorisation Referral* (AAR) – O comerciante deve pedir a confirmação directamente ao emissor (por exemplo por telefone);
- *Application Authentication Cryptogram* (AAC) – Transacção Recusada.

O terminal em função do criptograma devolvido pelo cartão determina o fluxo de execução a atribuir ao processamento da transacção.

2.6.6 Arquitectura de Gestão de Chaves

Neste ambiente transaccional os terminais da rede de pagamentos (POS, ATM, máquinas de venda automática, etc.) podem efectuar a autenticação em *offline* ou *online* do cartão apresentado como meio de pagamento.

O esquema de pagamento EMV é utilizado como CA do ambiente de pagamento EMV. Esta entidade cria certificados para cada banco emissor de cartões assinando as respectivas chaves públicas. A chave pública desta CA é então distribuída por todos os sistemas de pagamento que se encarregarão de as distribuir aos terminais dessa rede de pagamentos para que estes possam verificar os certificados dos bancos emissores.

2.6.6.1 Ciclo de Vida da Chave Pública da CA

O ciclo de vida da chave pública da CA em circunstâncias normais pode ser dividida nas seguintes fases:

- Planeamento;
- Geração;
- Distribuição;
- Uso;
- Revogação (planeada).

2.6.6.2 Planeamento

Durante esta fase o esquema de pagamento investiga os requisitos para a introdução dum novo par de chaves assimétricas num futuro próximo. Estes requisitos relacionam-se com o número de chaves necessárias e com os parâmetros das mesmas. Uma parte importante desse planeamento é a revisão da segurança do algoritmo de segurança utilizado, o RSA [7][9], para determinar a expectativa de vida das chaves existente e das que serão criadas. Esta revisão leva à determinação do tamanho das chaves, à sua data de expiração, e às possíveis modificações a efectuar às datas de expiração das chaves existentes bem como a decisão de distribuir as chaves de substituição.

2.6.6.3 Geração de Chaves

Após a decisão de criação das chaves, a CA gera o novo par de chaves de forma segura assegurando a integridade da CA e das chaves.

2.6.6.4 Distribuição

Nesta fase a CA distribui as chaves geradas aos membros do sistema, os emissores e tomadores (operadores dos sistemas de pagamentos) com o seguinte propósito:

- **Emissores** – Para verificar os certificados emitidos pela CA durante a fase de uso das chaves;

- **Tomadores** (operadores do sistema de pagamentos) – Para o carregamento seguro das chaves públicas da CA nos terminais dos comerciantes.

Para prevenir a introdução de chaves públicas de CAs fraudulentas, as interfaces entre a CA e os emissores e tomadores devem assegurar a integridade de distribuição das chaves públicas da CA.

No ambiente EMV quando o esquema de pagamento decide que é necessário introduzir no sistema uma nova chave pública da CA, é executado um processo que assegura a distribuição da nova chave a todos os intervenientes. É da responsabilidade do sistema de pagamentos assegurar que a nova chave da CA e os dados relacionados (isto é, o certificado digital) são distribuídos a todos os terminais da rede.

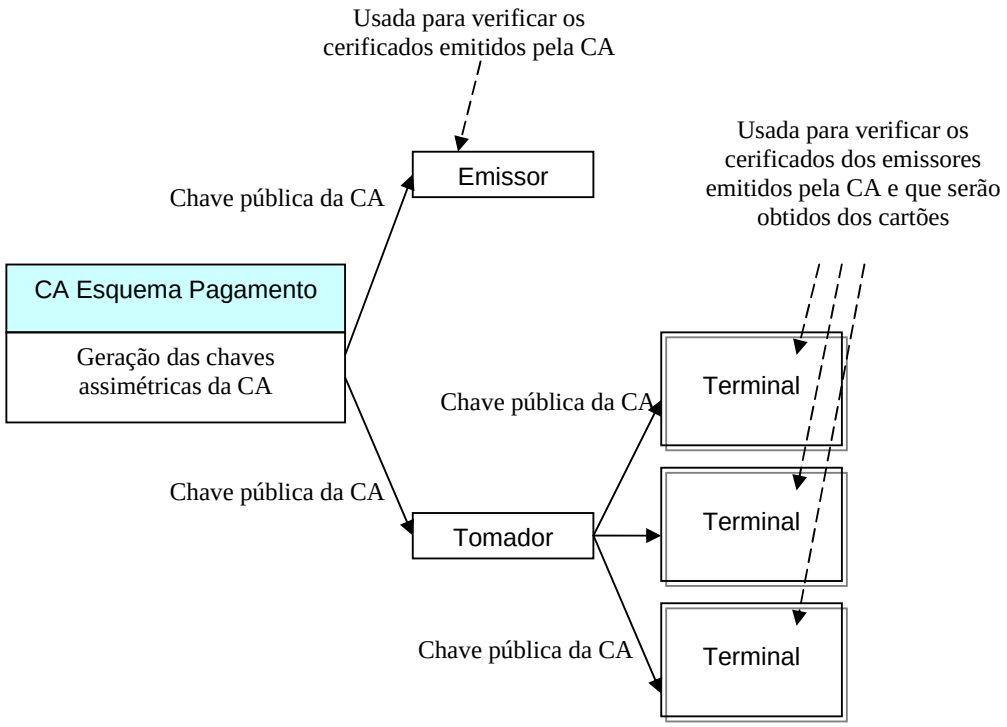


Figura 12 : Distribuição da chave pública da CA.

No ambiente EMV quando o esquema de pagamento decide que é necessário introduzir no sistema uma nova chave pública da CA, é executado um processo que assegura a distribuição da nova chave a todos os intervenientes. É da responsabilidade do sistema de pagamentos assegurar que a nova chave da CA e os dados relacionados (isto é, o certificado digital) são distribuídos a todos os terminais da rede (ver Figura 12).

Nesse sentido, o sistema de pagamentos deve obedecer aos seguintes princípios:

- O terminal deve ter a capacidade de receber a nova chave da CA livre de erros;
- O terminal deve ter a capacidade de verificar que os certificados foram provenientes do sistema de pagamento onde está inserido;
- O sistema de pagamentos deve ter a capacidade de confirmar que a nova chave da CA foi correctamente transferida para os terminais.

2.6.6.5 Uso das Chaves

A chave pública da CA é usada pelos terminais para efectuar a autenticação estática ou dinâmica do cartão. A chave privada da CA é usada pela CA para a geração dos certificados da chave pública dos emissores através das seguintes acções:

- O emissor gera a sua chave pública e envia-a à CA;
- A CA assina a chave pública do emissor com a chave privada da CA obtendo-se assim o certificado da chave pública do emissor que lhe é devolvido;
- Com a chave pública da CA, o emissor verifica a exactidão do seu certificado recebido da CA. Se estiver correcto o emissor pode incluí-lo como parte dos dados de personalização dos cartões.

Para prevenir a introdução de chaves públicas de emissores fraudulentas, as interfaces entre os emissores e a CA devem garantir a integridade das chaves públicas submetidas a certificação.

2.6.6.6 Revogação (Planeada)

O par de chaves da CA tem que ser retirada de serviço quando atingir a data de expiração conforme determinado na fase de planeamento. Em termos práticos significa que:

- Os certificados produzidos para as chaves públicas dos emissores passam a partir dessa data a ser inválidos. Por isso os emissores devem garantir que os cartões emitidos com essa chave privada expiram antes da data de expiração do par de chaves da CA;
- Um tempo antes da data de expiração das chaves da CA, a CA deve deixar de emitir certificados para os emissores utilizando essa chave;
- Os tomadores devem garantir que na data de expiração das chaves da CA os terminais já não possuem a chave pública da CA.

Quando o esquema de pagamento decide revogar uma das chaves da CA, os sistemas de pagamentos devem garantir que essa chave jamais pode ser usada nos seus terminais para a realização da autenticação estática ou dinâmica.

Para a remoção das chaves da CA devem ser aplicados pelos sistemas de pagamento os seguintes princípios:

- O terminal deve ter a capacidade de verificar que recebeu a notificação para retirar a chave da CA isenta de erros;

- O terminal deve ter a capacidade de verificar que essa notificação foi proveniente do seu sistema de pagamento;

- O sistema de pagamento deve ter a capacidade de confirmar que a chave da CA foi efectivamente removida dos seus terminais.

2.6.6.7 Compromisso das Chaves da CA

Caso os pares de chaves da CA sejam comprometidos, deve ser colocado em acção um processo de emergência que acelere o processo de revogação do par de chaves da CA antes da data de expiração planeada. Neste caso são adicionadas as seguintes fases ao ciclo de vida das chaves da CA:

- **Detecção -** O comprometimento das chaves da CA pode ser alcançado pela confirmação duma brecha na segurança da CA ou pela confirmação da quebra da chave por criptoanálise. Adicionalmente o compromisso pode ser:
  - **Suspeito** – A monitorização do sistema ou a queixa dum dos membros do sistema indicam a ocorrência de transacções fraudulentas que podem ter a haver com o compromisso das chaves, mas isso ainda não se encontra confirmado;
  - **Potencial –** As técnicas de criptoanálise, por exemplo factorização, foram desenvolvidas de tal forma que com os recursos disponíveis qualquer chave de qualquer comprimento pode ser comprometida, mas não existe evidência de que tal tenha ocorrido.
- **Confirmação** – A confirmação dum potencial compromisso das chaves da CA incluem os impactos técnicos, no risco e fraude, e no negócio para o sistema de pagamento e para os seus membros. O resultado da confirmação incluem a determinação das possíveis acções nos custos e riscos do compromisso para a tomada de decisão;

- **Decisão -** Baseado nos resultados da fase de confirmação, o sistema de pagamentos decide as acções a serem tomadas em relação ao compromisso das chaves. No pior dos casos, esta decisão consiste na

revogação não planeada da chave pública da CA antes da sua normal data de expiração;

- **Revogação (Acelerada) -** A decisão de revogação da chave pública da CA levará à comunicação a todos os membros do sistema de pagamentos da nova data de expiração da chave. O processo de revogação decorrerá de forma semelhante ao da revogação planeada.

2.6.7 Funcionalidades do Emissor

O emissor é responsável pela gestão das chaves relacionados com os dois esquemas de autenticação mencionados anteriormente [36]. Entre as suas atribuições contam-se as seguintes funcionalidades:

- A geração, manutenção e armazenamento seguro das chaves assimétricas do emissor;
- A transferência das chave pública do emissor para a CA do sistema de pagamentos;
- O armazenamento da chave pública do sistema de pagamentos e os certificados para as chaves públicas do emissor;
- A geração e transferência segura do par de chaves dos cartões emitidos (chaves RSA);
- O uso da chave privada do emissor para certificar as chaves públicas dos cartões chip, ou para assinar dados aplicacionais;
- A geração e armazenamento seguro das chaves secretas do emissor.

Estas funcionalidades complementam as da CA do sistema de pagamentos:

- A geração, manutenção e armazenamento seguro do par de chaves assimétricas do sistema de pagamentos;
- O uso da chave privada do sistema de pagamentos para certificar as chaves públicas do emissor;

- A transferência segura (com a respectiva integridade) da chave pública do sistema de pagamentos para todos os terminais.

2.7 Transferência Segura de Ficheiros

Tipicamente a transferência de ficheiros entre entidades bancárias é caracterizada pela troca entre sistemas de grandes volumes de informação num ambiente relativamente seguro. Em contraste, as transferências de ficheiros entre os terminais e o sistema de pagamentos é caracterizada pela transferência de pequenos volumes de informação num ambiente bastante mais inseguro do que o anterior.

A norma ISO/FDIS 15668 [22] aplica-se à transferência de diversos tipos de ficheiros no âmbito da actividade bancária, como por exemplo:

- Software;
- Transferência das transacções que foram realizadas em *offline*;
- Dados técnicos relacionados com o sistema de pagamentos (ou banco tomador);
- Dados aplicacionais (por exemplo, listas negras de cartões).

Independentemente do tipo de ficheiros a transmitir, todos eles apresentam as seguintes características:

- Os dados podem ser ou não secretos;
- O número de entidades que pode receber o ficheiro pode ser uma ou várias;
- O canal de comunicações pode pertencer à rede pública ou a uma rede privada;
- A natureza da transferência pode ser de conexão directa (tempo real – *circuit switching*) ou orientada à mensagem (*store and forward – message switching*).

Esta norma interessa-nos em particular na sua aplicação à transferência de software entre o OSP e os terminais de pagamento.

Genericamente, os intervenientes do processo de transferência são:

- **Originador** – A entidade que possui os dados a serem transmitidos;
- **Emissor** – A entidade responsável por transferir os dados provenientes do Originador com destino ao Receptor;
- **Receptor** – A entidade a quem os dados se destinam.

É assumido que entre as entidades envolvidas no processo de transferência segura existe uma relação preestabelecida de confiança que cobre em especial os aspectos comercias e legais associados com essa transferência. É assumido também que todos os dados provenientes do Originador foram confirmados como legítimos e correctos até ao momento da transferência.

Podemos pensar que o processo de transferência depende de entre outras de duas camadas aplicacionais:

- **Camada de Comunicações** – A camada que trata do processo de transmissão de dados;
- **Camada de Segurança** – A camada que disponibiliza serviços de segurança.

2.7.1 Formas de Transferência Segura de Ficheiros

São identificadas as seguintes formas de transferência segura de ficheiros:

- **Transferência de ficheiros protegidos** – Nesta forma de transferência (ver Figura 13), a camada de transferência não utiliza quais quer serviços de segurança, apenas inclui os serviços de comunicações. Neste caso o ficheiro deve ser protegido antes da transferência. A segurança é gerida pelo Originador e pelo Receptor. Não existe segurança adicionada ao nível das comunicações;

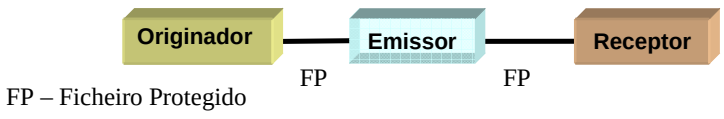


Figura 13 : Transferência de Ficheiros Protegidos.

- **Transferência segura de ficheiros** – Neste caso (ver Figura 14) a segurança é tida em conta entre o Emissor e o Receptor. O Originador confia plenamente no Emissor. Neste caso a camada de transferência utiliza os serviços de segurança. Não é necessário que o ficheiro seja protegido antes da transferência.

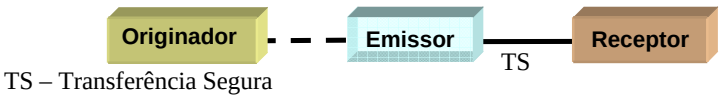


Figura 14 : Transferência Segura de Ficheiros.

- **Transferência segura de ficheiros protegidos** – As funções de segurança podem ser divididas entre a camada de segurança e a camada de comunicações. Por exemplo, o Originador cria um ficheiro, assina-o com a sua chave para assinatura, e cifra o ficheiro com a chave secreta partilhada com o Receptor. A principal preocupação vai no sentido de prevenir que alguém dentro da organização do Emissor possa ver o conteúdo do ficheiro, contudo, o Originador confia no processo de transferência na medida em que o Emissor efectuará a autenticação do Receptor e garantirá a integridade do ficheiro transmitido (ver Figura 15).

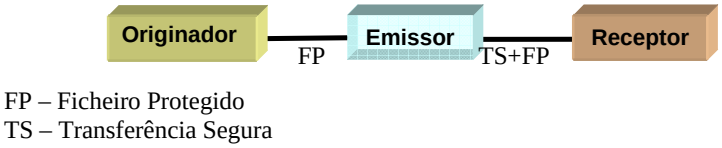


Figura 15 : Transferência Segura de Ficheiros Protegidos.

2.7.2 Download de Software

Conforme já foi referido anteriormente, a aplicação desta norma tem particular interesse no caso da transferência de software para terminais de pagamento. Para ser aplicada esta norma refere a necessidade de decompor o software dum terminal em diferentes elementos aplicacionais, nomeadamente:

- ***Loader*** - Software seguro e de confiança, previamente carregado no terminal antes da transferência segura de ficheiros. É responsável pela implementação dos mecanismos de segurança para a transferência segura do Gestor de Aplicações e a sua execução segura;

- **Gestor de Aplicações** - Aplicação de gestão que é responsável pela implementação dos mecanismos de segurança para o carregamento de aplicações e a sua execução segura;

- **Aplicações** – São aplicações para serem usadas pelo terminal no âmbito dos pagamentos electrónicos constituídas por código objecto executável ou código objecto interpretável.

2.7.3 Serviços de Segurança

Genericamente a realização duma transferência segura de ficheiros necessita dos seguintes serviços de segurança:

- **Autenticação da Origem da mensagem** – A autenticação da origem tem como objectivo assegurar o Receptor de que o alegado Originador é de facto o pretendido. Pode também assegurar o Receptor de que o ficheiro recebido é o ficheiro pretendido. Este tipo de autenticação pode ocorrer simultaneamente com a transferência do ficheiro mas também pode ocorrer antes da transferência do ficheiro no momento do estabelecimento da ligação. As técnicas que proporcionam a autenticação do conteúdo do ficheiro transferido também podem proporcionar a autenticação do Originador mas para isso é necessário que o ficheiro seja totalmente transmitido. Existem situações onde é desejável efectuar a autenticação da origem antes de iniciar o processo de transferência. Por exemplo, pode ser desejável prevenir que um impostor se faça passar por um legítimo Originador e tomar o canal de comunicações por muito tempo na transferência dum ficheiro muito longo, ainda que a sua ilegitimidade seja detectada e o ficheiro rejeitado;

- **Autenticação do Receptor** – Este serviço de segurança autentica a identidade do Receptor antes de iniciar o processo de transferência. Alguns Receptores só estão autorizados a receber certo tipo de ficheiros. Faz parte do controlo do Originador a determinação dos direitos do Receptor de receber certo tipo de ficheiros. Este serviço também impede que um falso Receptor possa ocupar o canal de comunicações enquanto o ficheiro é transferido. Este serviço de segurança não impede que outra entidade possa "escutar" o canal de comunicações e obter uma cópia do ficheiro. Para impedir que isso aconteça terá que ser usado outro serviço de segurança: Confidencialidade. Existe um serviço relacionado com a

Autenticação do Receptor, o serviço de Não Repudiação da Entrega, que confirma, depois da transferência, que o Receptor efectivamente recebeu o ficheiro;

- **Integridade** – Este serviço controla o ficheiro como um todo ou individualmente nos seus segmentos de forma a detectar alterações acidentais ou intencionais do ficheiro durante e após o processo de transferência;

- **Confidencialidade** – Quando necessário a confidencialidade dos ficheiros transferidos assegura que só o intencionado Receptor tem acesso ao conteúdo do ficheiro;

- **Não Repudiação da Origem** – Este serviço proporciona evidência de que o alegado Originador efectivamente gerou o ficheiro transferido. Sem este serviço o Originador mais tarde pode alegar que o Receptor criou o ficheiro e que afirma ter sido criado pelo Originador;

- **Não Repudiação da Recepção** – Este serviço proporciona evidência de que o alegado Receptor efectivamente recebeu o ficheiro. Sem esta evidência o Receptor pode alegar que não recebeu o ficheiro. Este serviço é obtido pelo envio ao Originador duma mensagem que mostra que: o legítimo Receptor recebeu o ficheiro e que o conteúdo do ficheiro não sofreu alterações;

- **Auditoria** – Pode ser necessário para o Emissor/Originador e/ou Receptor manter um registo com os detalhes da transferência (data e hora, tipo de ficheiros, volume de ficheiros, números de versão, etc.). Tal registo pode manter informação sobre as falhas e sucesso de transferência. No caso de tentativas de fraude os registos de falhas na transferência podem auxiliar a identificar a fonte de tais tentativas.

Do conjunto de serviços anteriores na transferência de software são utilizados os seguintes serviços:

- Autenticação (mútua ou unilateral) do Originador/Emissor;

- Verificação da Integridade do ficheiro transferido.

- Não Repudiação da Recepção.

A confidencialidade pode ser necessária no caso da transferência de dados sensíveis, como por exemplo, chaves criptográficas.

2.7.3.1 Autenticação da Origem

O processo de autenticação pode usar um algoritmo simétrico ou assimétrico. No caso da utilização dum algoritmo simétrico o Emissor e o Terminal partilham as mesmas chaves. As chaves iniciais devem ser carregadas no Terminal antes da realização de qualquer transferência. A mesma chave pode ser utilizada na autenticação do Emissor pelo Receptor e na autenticação do Receptor pelo Emissor, mas é recomendado que para o processo de autenticação mútua se use uma chave diferente por terminal para impedir que um terminal se possa fazer passar por outro. Além disso esta solução impede também a criação de um falso Emissor com possibilidade de transferir ficheiros para qualquer terminal no caso de se comprometer as chaves dum terminal. Por cada elemento aplicacional (*Loader*, Gestor de Aplicações e Aplicações) devem existir chaves diferentes.

No caso da utilização dum algoritmo assimétrico, associado a cada elemento aplicacional do terminal (*Loader*, Gestor de Aplicações e Aplicações) deve existir um par de chaves diferente. No terminal reside a chave privada. A correspondente chave pública é transmitida ao Emissor para que este possa autenticar o terminal. A chave pública usada para autenticar o Emissor do Gestor de Aplicações deve ser transmitida em segurança para o terminal, nele residir de forma segura e ser protegida contra substituições.

2.7.3.2 Integridade do Ficheiro

A integridade do ficheiro transferido é assegurada acrescentando um *File Verification Value* (FVV) ao conteúdo do ficheiro. O FVV é calculado apenas uma única vez, pois é independente da operação de transferência e da entidade que recebe o ficheiro.

Depois da transferência do ficheiro e antes da sua activação, o terminal deve verificar o FVV.

O FVV pode ser calculado usando um algoritmo simétrico ou assimétrico. No caso dos algoritmos simétricos, as chaves usadas para a verificação da integridade de cada um dos elementos aplicacionais do terminal devem ser diferentes. A chave usada para verificar a

integridade do Gestor de Aplicações deve ser instalada de forma segura antes de disponibilizar o terminal.

As chaves usadas para a verificação da integridade das aplicações transferidas podem ser:

- Instaladas antes de disponibilizar o terminal;
- Transferidas para o terminal de modo seguro ao mesmo tempo que se transfere o Gestor de Aplicações;

A integridade e confidencialidade destas chaves devem ser protegidas usando um conjunto de chaves previamente instaladas.

No caso da utilização dum algoritmo assimétrico, existe um único par de chaves privada/pública do Emissor cuja chave pública é comum a todos os terminais.

A chave pública usada para a verificação da integridade do Gestor de Aplicações transferido deve residir em cada um dos terminais e protegida contra substituições. A chave pública usada para a verificação da integridade das aplicações transferidas devem ser transferidas de forma segura ao mesmo tempo que se transfere o Gestor de Aplicações ou então terem sido previamente instaladas.

2.7.3.3 Não Repudiação da Recepção

Depois de receber e verificar a integridade do software recebido o terminal deve enviar a confirmação de forma segura ao Emissor (quer tenha havido sucesso ou insucesso na transferência ou verificação da integridade).

A confirmação segura consiste no envio duma mensagem enviada pelo terminal ao Emissor protegida por uma chave e que inclui o resultado da transferência.

2.8 Sumário

Neste capítulo descreveu-se o funcionamento dum sistema de pagamento electrónico exemplificado com um serviço de compra. Com base nessa descrição apresentou-se a constituição dum sistema de pagamentos electrónicos semelhante ao existente em Portugal, focando os seus componentes com especial detalhe nos terminais POS. Descreveu-se sucintamente o protocolo de funcionamento dessa rede na componente dos

serviços disponibilizados aos POS. Não foi esquecido o papel fundamental da segurança para garantir a integridade e autenticidade das transacções.

Como referências de trabalho relacionado apresentou-se uma breve descrição da norma EMV e da Transferência Segura de Ficheiros. Da norma EMV destacou-se a sua infra-estrutura de segurança, os esquemas de autenticação e a forma de integração com os sistemas de pagamento já existentes. Da Transferência Segura de Ficheiros descreveram-se os intervenientes do processo de transferência, as diversas formas de transferência segura de ficheiros e os serviços de segurança envolvidos no processo. Da totalidade dos serviços de segurança genericamente presentes nas transferência de ficheiros restringiu-se essa lista para o caso da transferência de software e descreveu-se como podem esses serviços serem realizados.

Capítulo 3 Sistema de Actualização

O Sistema de Actualização permite automatizar e acelerar o processo de manutenção das aplicações que são executadas nos equipamentos POS. Os objectivos a atingir por este sistema são:

- Automatizar o processo de manutenção e substituição de aplicações no POS;
- Aumentar a segurança do sistema de pagamentos;
- Disponibilizar mais rapidamente ao público os novos serviços;
- Poupar recursos materiais e humanos;
- Exercer maior controlo sobre a qualidade dos serviços existentes;
- Obter maior controlo sobre as versões das aplicações instaladas;
- Tornar difícil a adulteração de aplicações entre o produtor das aplicações e o terminal;
- Definir e atribuir responsabilidades aos intervenientes no processo;
- Controlar todo o processo através de um único ponto, o OSP.

Na sua essência, a actualização de aplicações resume-se à transferência de ficheiros entre dois sistemas, o Produtor de Software e o terminal POS, através do OSP.

Relacionando este trabalho com a norma ISO 15668 interessa pois determinar qual a forma de transferência segura que deve estar presente no sistema de actualização, quais os serviços de segurança envolvidos e como estes podem ser implementados. A mesma norma sugere a possibilidade de se implementar os serviços de segurança recorrendo a algoritmos de criptografia simétrica ou assimétrica. Como a especificação EMV utiliza criptografia assimétrica, e uma vez que é expectável que esta norma seja adoptada em breve pela maioria dos países europeus, optou-se por basear o esquema de segurança desta solução também neste tipo.

3.1 Processo de Actualização

No âmbito do processamento de transacções electrónicas, como já foi referido, a iniciativa de comunicação é exclusiva dos terminais. A uma transacção electrónica corresponde um par de mensagens, pedido (feito pelo POS) e resposta (dada pelo SSP). A determinação da necessidade de actualizar a aplicação do POS que está nesse momento a solicitar um serviço, faz-se no SSP através do cruzamento da informação do identificador do POS com a existência de uma aplicação certificada compatível com esse modelo de terminal e já distribuída aos SDA. Se for determinada a necessidade de dar início à actualização, na mensagem de resposta ao serviço solicitado, o SSP indica através dum código que esta deve ser executada. Quando o POS terminar o processamento do serviço que o levou a contactar o SSP, o POS inicia o processo de actualização enviando ao SSP a mensagem de início deste serviço. O SSP envia na resposta os dados de comunicação do SDA disponível para efectuar a transferência da aplicação (ver Figura 16).

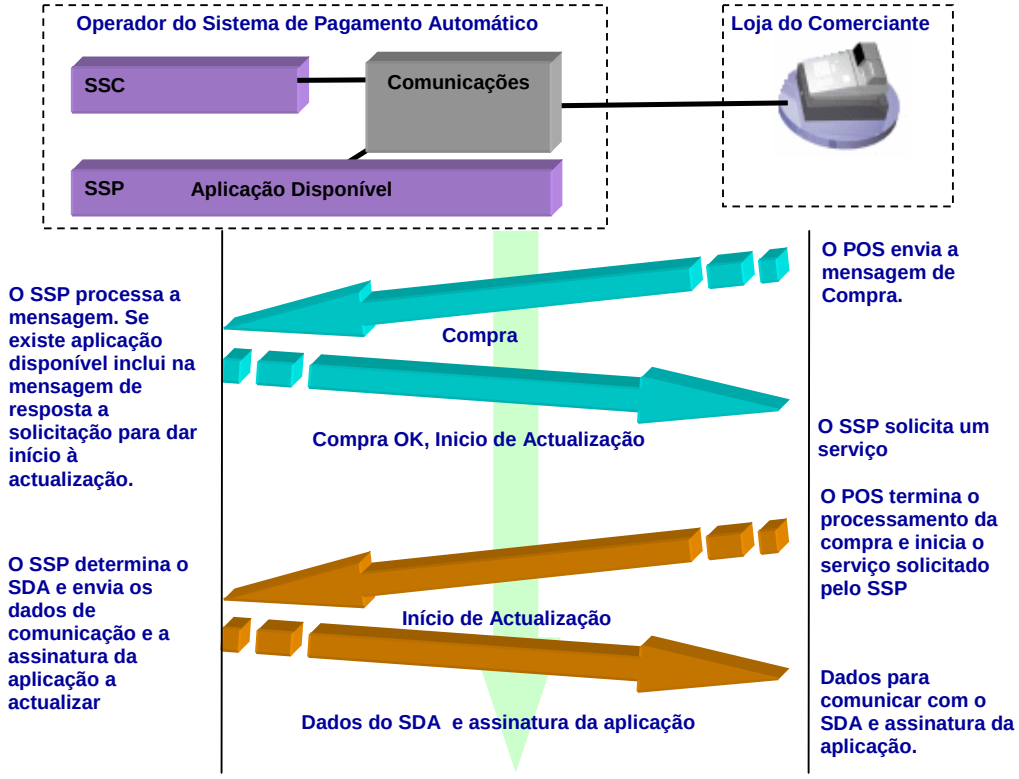


Figura 16 : Início do Processo de Actualização.

O POS na posse dos dados de comunicação só necessita de determinar o momento mais oportuno para iniciar a transferência da nova aplicação. Nessa altura o POS deve estabelecer uma sessão de transferência e autenticar o SDA em todas as mensagens que

trocar com ele, uma vez que só deverá receber aplicações de entidades credenciadas pelo SSP.

Finalizada a transferência e antes de colocar a nova aplicação em execução, o POS deve verificar a integridade da aplicação recebida contra a assinatura da aplicação recebida do SSP. No final do processo o POS deve informar o SDA e o SSP do resultado da actualização.

3.2 Transferência Segura

Conforme descrito no capítulo anterior, genericamente os intervenientes num processo de transferência segura de ficheiros são: o Originador, o Emissor e o Receptor. No sistema de actualização pretende-se transferir de forma segura o software produzido pelos Produtores de Software para os POS compatíveis através do OSP.
Para atingir esse objectivo, uma vez conhecida a arquitectura do sistema de pagamentos, podemos identificar nesse processo de transferência as referidas entidades:

- **Produtor de Software (Originador)** – A entidade que produz o software para o POS;
- **Operador do Sistema de Pagamento (Emissor)** – A entidade responsável por transferir o software proveniente do Produtor de Software com destino aos POS compatíveis;
- **Terminais POS (Receptor)** – O equipamento para o qual se destina o software.

Neste processo de transferência não se deseja que dentro da organização do Emissor exista a possibilidade de se efectuar modificações ao software, pelo que o ficheiro terá que ser protegido para que o POS possa detectar quaisquer alterações efectuadas. Adicionalmente deseja-se também que o POS só possa receber ficheiros enviados pelo OSP e originados do Produtor. Estes requisitos sugerem que se esteja perante a transferência segura de ficheiros protegidos (ver Secção 2.7.1).

3.3 Emissor

Do ponto anterior verificamos a necessidade do OSP disponibilizar pelo menos duas interfaces para o exterior: a interface com o Produtor de Software e a interface com os POS.

Para a interface com o Produtor é criado no OSP o Servidor do Sistema de Certificação (SSC) que é responsável por:

- Autenticar os Produtores de Software que pretendam certificar novas aplicações;
- Verificar a integridade e a assinatura do software recebido;
- Enviar relatórios por si assinados aos Produtores de Software notificando-os do resultado da certificação.

Para a interface com os POS, à primeira vista, poderíamos ser levados a pensar que o SSP poderia constituir a interface natural, no entanto, o processo de actualização de aplicações deve ser transparente ao normal funcionamento dos serviços de pagamento electrónico disponibilizados pelo SSP aos POS, não podendo em caso algum, verificar-se uma degradação da qualidade, segurança ou desempenho do serviço existente.

A operação de actualização é uma tarefa morosa que a ser executada pelo SSP o ocupa com tempo de processamento dedicado a uma actividade que não é o principal negócio e razão da sua existência - o processamento de transacções. Para nos ajudar a compreender a dimensão do problema, fez-se o cálculo do tempo que pode demorar a concretizar uma operação deste tipo segundo as condições normais de funcionamento (ver

Figura 17).

Dados iniciais:

- Velocidade de comunicação: 9600bps.
- Tamanho da aplicação :780Kbytes
- Protocolo da camada Ligação de Dados: Send and wait.
- Dimensão máxima da mensagem de Confirmação (POS): 70bytes
- Dimensão máxima da mensagem de dados (SSP): 70bytes(cabeçalho) + 2048bytes(dados)=2108bytes
- Tempo de processamento das mensagens : 250 ms

Cálculo do Tempo de Telecarregamento:

- Número total de tramas: 780x1024/2048= 390
- Dimensão da trama de dados = (2108)x8 = 16944bits
- Tempo de transmissão da mensagem de dados (SSP -> POS) = 16944/9600 = 1,795s
- Tempo de transmissão da mensagem de Confirmação (POS -> SSP) = 70x8/9600 = 58ms
- Tempo de transmissão da transacção (SSP->POS + POS->SSP) = 1,795 + 0,058 = 1,853s
- Duração do telecarregamento = 1,853*390/60 = 12,1min

Figura 17 : Cálculo do tempo total de carregamento duma aplicação EFT.

Se for tido em consideração que por exemplo na rede Multibanco existem cerca de 140000 terminais POS, facilmente se conclui que a ser o SSP a efectuar a tarefa de transmissão da aplicação para os POS, existe efectivamente o risco de se degradar a qualidade do serviço de pagamentos.

Os riscos de intrusão ao normal funcionamento da rede são diminuídos delegando esta tarefa para servidores dedicados, os SDA, que se ocuparão de transferir a aplicação para os POS.

Assim, propõe-se que a arquitectura do sistema de actualização representada na Figura 2 seja reconfigurada conforme a que se mostra na Figura 18.

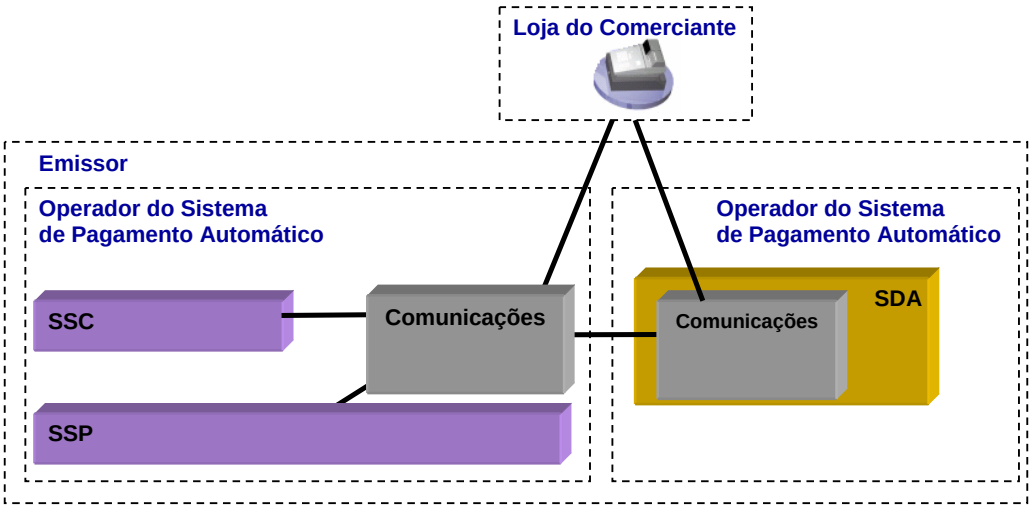


Figura 18 : Arquitectura do Emissor do Sistema de Actualização.

3.4 Ciclo de Vida da Aplicação

O ciclo de vida da aplicação no âmbito do processo de actualização compreende todas as fases que uma aplicação EFT percorre desde a sua produção até ao momento em que é eliminada do POS:

1. Entrega;
2. Certificação;
3. Distribuição;

4. Transmissão;
5. Execução;
6. Abate.

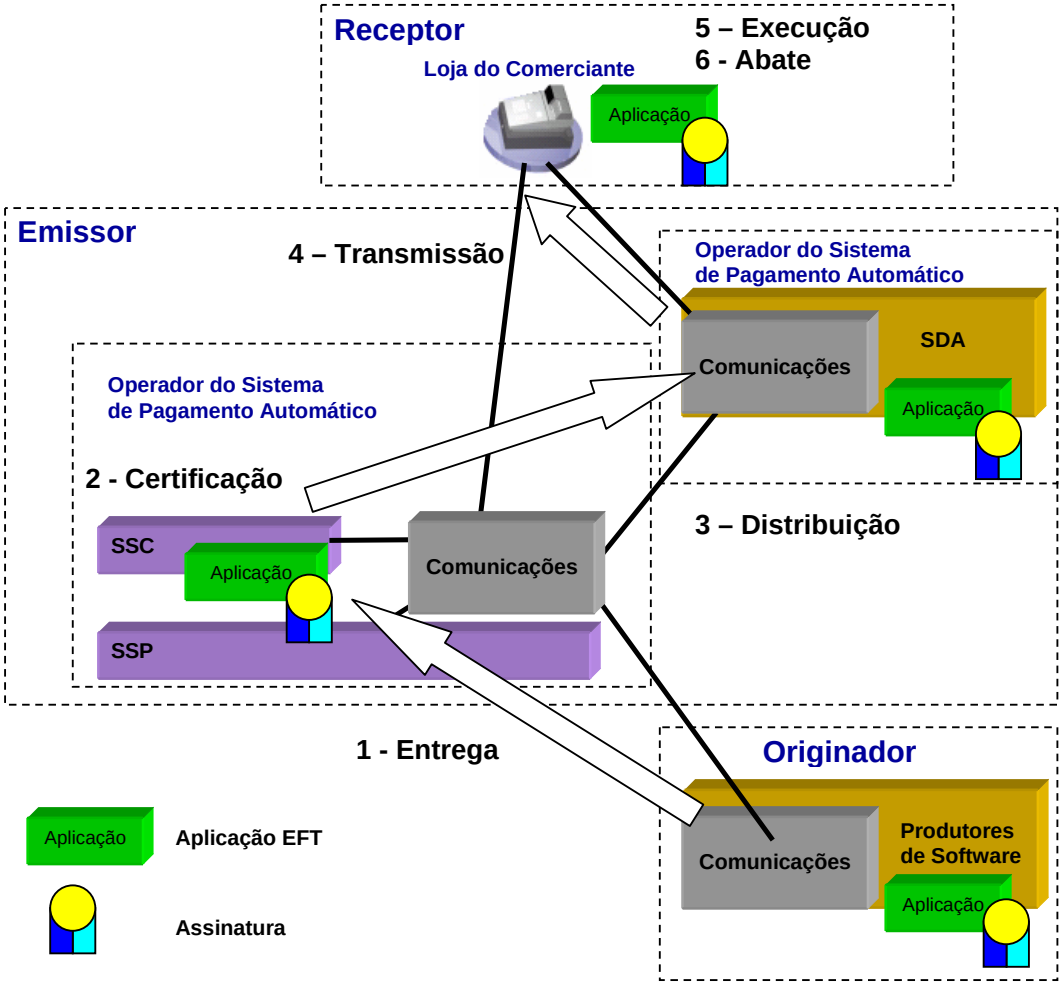


Figura 19 : Ciclo de vida da aplicação no processo de actualização.

A Figura 19 representa as fases do ciclo de vida da aplicação.

3.4.1 Entrega

Nesta fase o Produtor de Software entrega a nova versão da aplicação para actualização e realiza as seguintes acções:

- Autenticam o SSC;
- Entregam as aplicações assinadas com a sua chave privada, *KrProd*.

O SSC realiza as seguintes acções:

- Autentica o produtor da aplicação;
- Verifica a autenticidade e integridade da aplicação recebida.

3.4.2 Certificação

A certificação visa testar o funcionamento da aplicação recebida na fase anterior sobre um equipamento POS com o qual é compatível, para verificar a sua conformidade com as especificações funcionais produzidas pelo OSP. No fim do processo de certificação é entregue ao Produtor do Software um relatório em formato digital, assinado pelo SSC, que descreve o resultado desta operação. No caso da detecção de erro ou inconformidade é solicitada a entrega duma nova aplicação e o processo de actualização é abortado. Caso contrário a aplicação pode ser actualizada nos POS.

3.4.3 Distribuição

Após a conclusão da certificação com sucesso, a aplicação reúne as condições necessárias para que possa ser instalada em todos os POS com os quais é compatível. Por decisão interna da gestão do OSP, a aplicação é distribuída pelo SSC a todos os SDA seleccionados para efectuarem essa actualização. A determinação de quais os SDA que são disponibilizados para a transferência do software pode basear-se em critérios específicos com os objectivos de reduzir por um lado a redundância da informação, ao copiar-se o software para o menor número de SDAs possível, e por outro controlar a carga de terminais POS que a eles se ligarão para a transferência do software. Pode considerar-se para isso a distribuição geográfica dos terminais POS, a distância destes aos SDA, ou qualquer outro critério mais adequado.

Entre o SSC e os diversos SDA são efectuadas as seguintes acções:

- Autenticação mútua;
- Transferência segura do software.

O SDA é responsável por

- Realizar uma política de segurança que permita a autenticação dos terminais que pretendam carregar aplicações;
- Sincronizar o processo de transferência com os terminais que acedem ao serviço;

- Fornecer estatísticas sobre o funcionamento do processo de carregamento.

3.4.4 Transmissão

A fase de transmissão compreende todas as acções necessárias para a transferência segura da aplicação do SDA para o POS. Resumidamente as actividades envolvidas nesta fase, são:

- Contacto do POS com o SDA;
- Autenticação mútua entre o POS e o SDA;
- Transmissão do ficheiro contendo o software com possibilidade de sincronismo em caso de falhas de transmissão;
- Verificação da integridade do ficheiro, verificação da assinatura e autenticação do Produtor do Software por parte do POS. Isto significa que o POS só deve receber software do produtor do equipamento. Só assim o produtor do equipamento pode ser responsabilizado em caso de incorrecto funcionamento do equipamento.

3.4.5 Execução

Nesta fase do ciclo de vida da aplicação o POS coloca em execução a aplicação recebida substituindo a aplicação anterior. Dependendo da estrutura funcional da aplicação, do sistema operativo e da arquitectura física do terminal POS, o equipamento poderá ter que executar procedimentos específicos para que nenhuma informação necessária ao correcto funcionamento do POS se perca com a transição, como por exemplo, conversão de dados, *restart* à aplicação e ao hardware.

Ainda que a aplicação recebida seja autêntica e se encontre certificada, no processo de substituição das aplicações poderão ocorrer erros, pelo que é prudente estabelecer no POS um mecanismo de regressão à aplicação anterior caso algo corra mal na execução da nova aplicação.

3.4.6 Abate

O abate consiste na eliminação do código da aplicação substituída e todos os dados associados, libertando todos os dispositivos envolvidos na sua execução.

3.5 Sumário

Neste capítulo começou-se por determinar o tipo de transferência de ficheiros envolvido no processo de actualização identificando as entidades intervenientes.

Relativamente ao Emissor foi descrita a arquitectura mais conveniente para que o sistema de actualização possa ser integrado pelo sistema de pagamentos com vista à menor intrusão possível no processamento de transacções.

Definimos também as fases do ciclo de vida das aplicações EFT no âmbito do processo de actualização e terminámos este capítulo com a descrição genérica do funcionamento do processo de actualização.

Capítulo 4 Concepção do Sistema

Nos capítulos anteriores identificaram-se os objectivos a atingir com esta solução e descreveu-se genericamente o funcionamento do processo de actualização. Este capítulo é dedicado à concepção do sistema, nomeadamente identifica e caracteriza a infra-estrutura de segurança a utilizar na implementação do sistema, define e descreve em detalhe o protocolo de actualização.

4.1 Infra-estrutura de Segurança de Chave Pública

O desenvolvimento duma infra-estrutura de segurança de chave pública (PKI), permite definir uma arquitectura que reúne um grupo de componentes que interagem entre si, com o objectivo comum de constituírem um ambiente seguro assente em conceitos e técnicas de criptografia assimétrica.

O hardware, software, políticas e procedimentos desenvolvidos garantem a autenticidade das mensagens trocadas bem como a emissão de pares de chaves, distribuição e revogação dos correspondentes certificados digitais.

4.1.1 Requisitos

A infra-estrutura de segurança utilizada pela solução proposta deve cumprir os seguintes requisitos:

- **Estrutura escalável** – A estrutura tem que ser escalável uma vez que o sistema tem necessidade de suportar um número crescente de componentes, nomeadamente: Produtores de Software EFT, SDAs e POS;

- **Pedidos de emissão de certificados online** – Os elementos que pertencem à infra-estrutura de segurança devem ter possibilidade de pedir, obter, revogar e publicar os certificados em tempo real;

- **Utilização de "*Certification Revocation List*"(CRL)** – Deve existir um CRL para que os vários elementos possam verificar o estado dos certificados;

- **Assinatura e verificação de assinatura** – Alguns elementos do sistema devem possuir a capacidade de gerar chaves para assinar e verificar as assinaturas das mensagens trocadas entre os diversos interlocutores;

- **Assinatura de mensagens de correio electrónico** – Uma solução simples para a troca de ficheiros entre os produtores de aplicações e o SSC, quer sejam aplicações EFT ou os relatórios de certificação, é o uso do *e-mail*. Neste caso as mensagens trocadas devem ser assinadas;

- **Assinatura de ficheiros –** Nos casos em que se opte por transferir quer as aplicações EFT como os relatórios de certificação por suporte físico como CD, *memory stick* ou outro dispositivo, deve existir forma de verificar a autenticidade do conteúdo do suporte. Todos os ficheiro devem ser assinados. Para isso deve ser calculado o *Hash* de cada ficheiro e posteriormente ser assinado com a chave privada do seu produtor.

- **Hardware de Segurança –** Deve ser utilizado hardware seguro para guardar as chaves.

4.1.2 Componentes

Uma estrutura deste género é composta por elementos que permitem a realização do objectivo da PKI, cada um deles com funções específicas:

- **Autoridade de Certificação (CA)** – A sua assinatura é a base de toda a confiança da infra-estrutura. Disponibiliza os meios para a geração dos pares de chaves e certificados digitais. Entre outras funções recebe os pedidos de certificação e de revogação efectuados pela Autoridade de Registo (ou aplicações de cliente) e emite certificados e listas de certificados digitais revogados. Procede à assinatura de todos os certificados emitidos, tanto para utilizadores, quer para outras CAs. Disponibiliza num repositório público toda a informação referente à revogação de certificados sob a forma de CRL e *Authority Revocation List* (ARL). Mantém sob a forma de arquivo todos os dados gerados;

- **Autoridade de Registo (*Registration Authority* – RA)** – Este componente disponibiliza a interface entre a CA e a aplicação cliente. Recebe os pedidos de emissão de certificados digitais e verifica a autenticidade dos requerentes. Numa PKI este elemento é facultativo pois os serviços por si disponibilizados podem ser

realizados pela CA. A sua utilização permite a divisão de tarefas permitindo aliviar a carga funcional da CA e repartir responsabilidades;

- **Aplicação do utilizador (ou sistema) final** – A aplicação do cliente (ou sistema) final, deve estar preparado para processar, originar e reagir a todos os acontecimentos decorrentes do funcionamento da infra-estrutura. Deve conseguir requerer os serviços de certificação, de revogação, processar os historiais de chaves e ainda determinar quando efectuar uma actualização ou uma recuperação de chaves;

- **Directoria PKI** – Este repositório de dados armazena todos os certificados emitidos pela CA e está disponível *online*.

Associado a esta infra-estrutura deve existir um documento detalhado que contém a descrição de todos os procedimentos que satisfazem as regras definidas pela Política de Segurança da PKI. Inclui entre outras informações, as definições de como a CA foi construída e a forma como opera, o modo como os certificados são aceites, emitidos e revogados, o modo como as chaves são geradas, registadas, certificadas e armazenadas, para além do modo como são disponibilizadas aos utilizadores.

4.1.3 Hierarquia

Em termos práticos uma PKI faz a gestão das relações entre os que necessitam dos seus serviços e estabelece um nível de confiança num ambiente distribuído. Permite criar uma relação de confiança entre duas entidades que não se conhecem, assente na base de confiança que cada uma dessas entidades individualmente possuem com uma terceira entidade, neste caso a CA. A partir do momento em que se confia numa CA, confia-se em todos os certificados por si emitidos.

Numa PKI é comum encontrarem-se sistemas organizados em hierarquias de CAs, situando-se no topo dessa hierarquia a *root* (raiz) CA. Esta CA é a base de confiança para todos os elementos que se encontram hierarquicamente abaixo.

Podem existir diversos níveis hierárquicos, em cada um desses níveis encontram-se CAs intermédias designadas por sub-CAs (CAs subordinadas). O último nível corresponde ao nível da aplicação do utilizador final.

Independentemente do tamanho da cadeia hierárquica e dos certificados dos utilizadores finais serem emitidos por uma CA intermédia, continua a ser a *root* CA a base de toda a confiança.

4.1.4 Armazenamento Seguro de Chaves

O elemento mais sensível duma PKI é a chave privada que deve ser protegida o melhor possível, seja a chave privada do utilizador final ou duma CA. Ambas estão expostas ao mesmo perigo, mas a revelação da chave privada da CA destroi toda a hierarquia de segurança por ela sustida.

Actualmente o mercado disponibiliza três dispositivos de armazenamento de chaves considerados seguros:

- **Smart card –** Existem diversos tipos de *smartcards*: cartões de memória ou com microprocessador. Os cartões de memória limitam-se a armazenar informação e não têm capacidade para suportar algoritmos de segurança. Os cartões com microprocessador dificultam a cópia da informação neles armazenada por conterem eles próprios mecanismos de autenticação para acesso a essa informação. Possuem a capacidade de gerar internamente a chave privada e de a manter num ficheiro secreto, a sua construção impede a sondagem de informação e a detecção de ataques;

- ***USB Token*** – Este dispositivo possui as mesmas propriedades e funcionamento dum *smart card* diferindo deste no nível físico;

- ***Hardware Security Module* –** Este dispositivo é utilizado em sistemas criptográficos como método que assegura a segurança duma série de operações. É normalmente utilizado para o armazenamento da chave privada das CAs e desempenha as funções de: assinatura de certificados, geração de números aleatórios e geração de chaves dentro do módulo. Realiza operações criptográficas com grande rapidez e efectua o armazenamento seguro de chaves. É à prova de alterações pois o material considerado mais sensível é destruído em caso de intrusão.

4.2 Modelo Adoptado

Identificadas as funcionalidades que se desejavam alcançar com o desenvolvimento do sistema de actualização de aplicações para POS, identificado o modelo de transferência de software e definidos os requisitos necessários à implementação duma PKI, chegou a altura de definir o modelo da solução que se propõe, quanto a:

- Infra-estrutura de segurança;
- Arquitectura;
- Protocolos.

4.2.1 Infra-estrutura de Segurança

Para a concretização da infra-estrutura de segurança baseada em chave pública são criados os seguintes componentes:

- **CA** - A CA é a base de confiança de toda a hierarquia. Toda a infra-estrutura depende da sua assinatura. A sua principal função é gerar e/ou fornecer pares de chaves e emitir certificados digitais. Tem como principais actividades receber pedidos de certificados, revogar certificados, devolver certificados já revogados e listas de certificados revogados. Todos os nós finais e intermédios desta cadeia de confiança têm que possuir uma cópia da chave pública da CA;
- **Repositório de Certificados** - Este elemento destina-se a armazenar os certificados;
- **Sistema utilizador** - É definido como elemento utilizador dos serviços da CA para que a infra-estrutura resulte. Deve por isso responder e gerar adequadamente acontecimentos relacionados com o funcionamento da infra-estrutura. Utiliza os serviços de certificação, revogação ou actualização de chaves. Os elementos que se enquadram nesta categoria são: Produtores de Software, SDA, SSC e SSP e POS.

4.2.2 Arquitectura

A arquitectura do modelo compreende todos os elementos que pertencem ao sistema de pagamentos electrónico acrescido dos elementos necessários à actualização das aplicações EFT e dos elementos necessários à construção da infra-estrutura de segurança. Assim o modelo para a solução proposta assume a configuração representada na Figura 20:

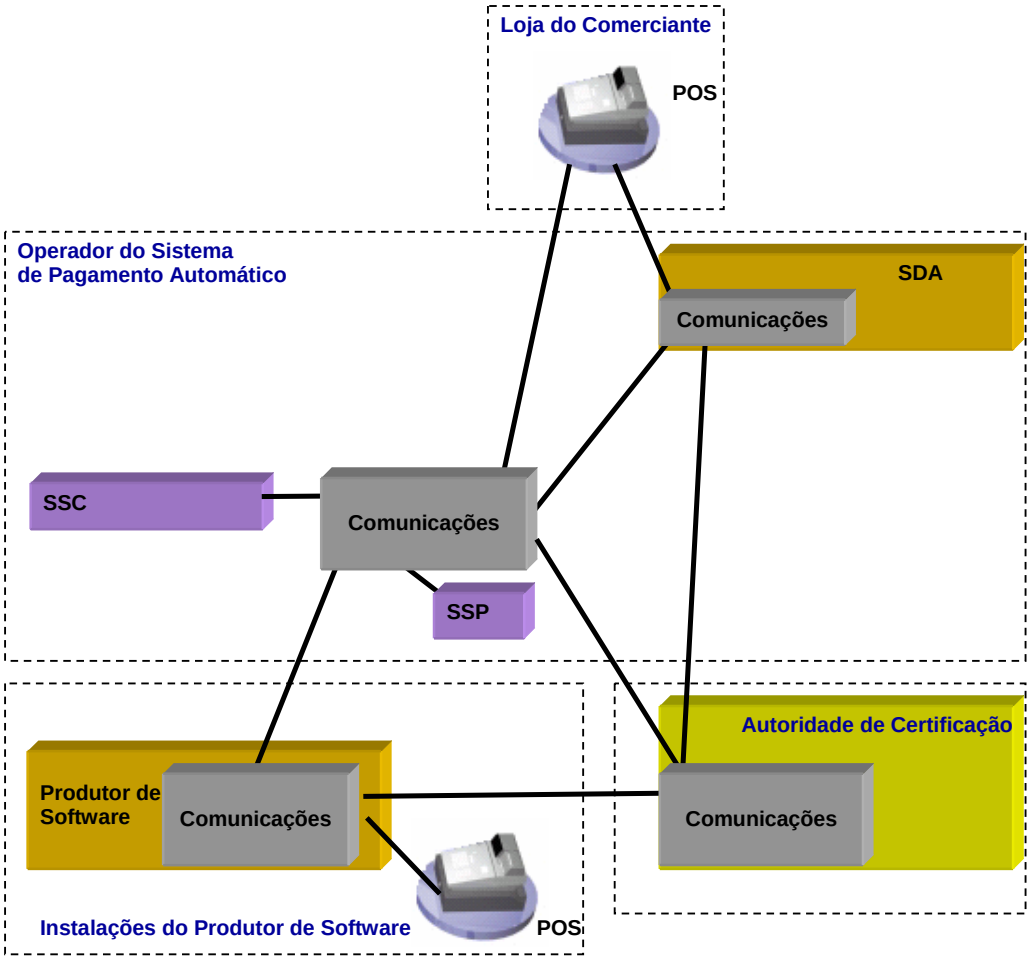


Figura 20 : Arquitectura do modelo adoptado.

4.3 Protocolos

O protocolo de actualização foi organizado num grupo de sub-protocolos, cabendo a cada um deles a realização duma função específica:

- **Protocolo de Autenticação** – Este protocolo aplica-se aos Produtor de Software, o SSC e todos os SDAs e define as regras que permitem obter e validar os certificados digitais emitidos pela CA de forma a realizarem o processo de autenticação;

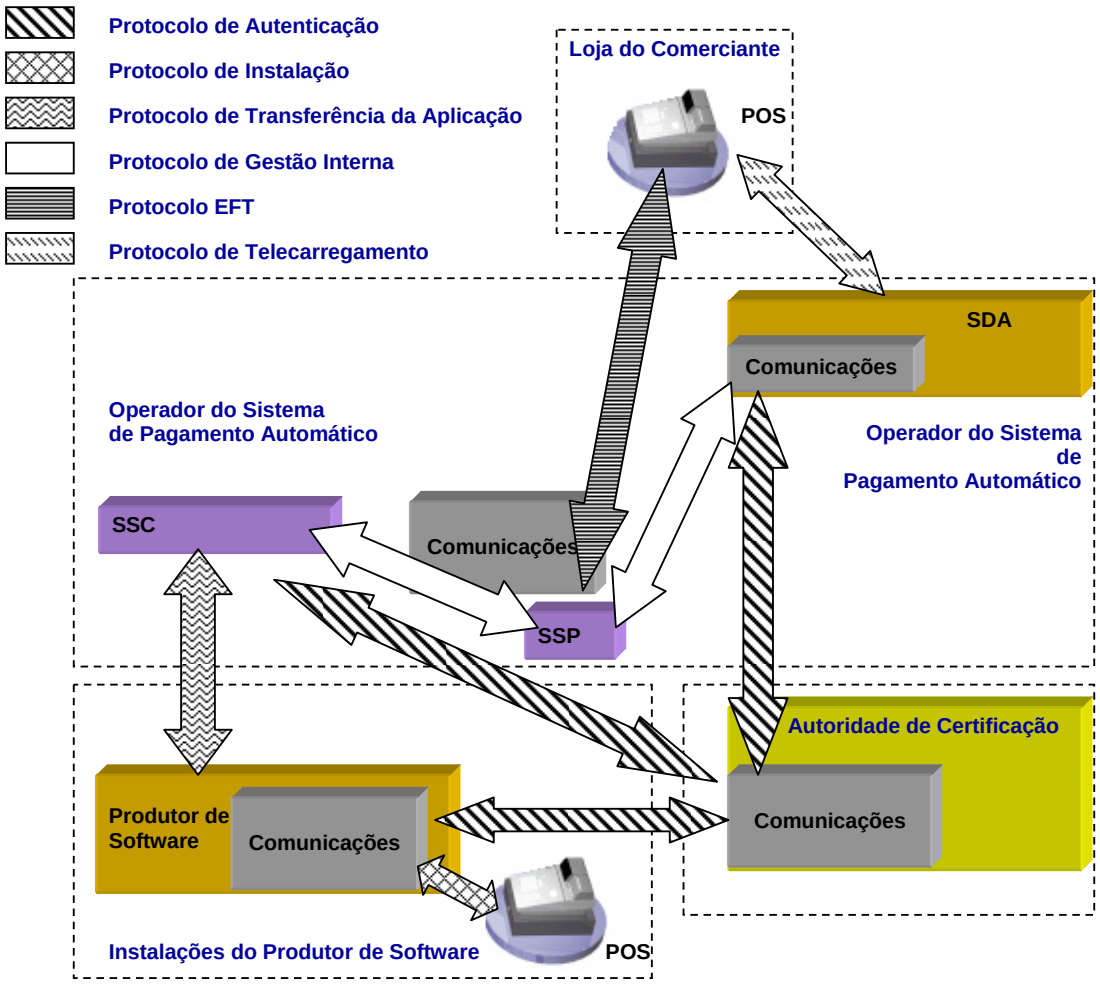


Figura 21 : Conjunto de protocolos do modelo adoptado.

- **Protocolo de Instalação** – Este protocolo define o processo de instalação do software de base, a geração e transferência das chaves e certificados necessários ao funcionamento do POS;

- **Protocolo de Transferência da Aplicação** – Este protocolo especifica a forma como uma nova aplicação EFT é enviada do Produtor de Software para o SSC;

- **Protocolo de Gestão Interna** – Uma vez decidido a actualização duma aplicação, é através deste protocolo que a aplicação é transferida do SSC para os diversos SDAs. Especifica também a forma como o SSP desencadeia o início do processo de actualização e a forma como devem ser disponibilizadas os elementos de segurança para que os SDAs possam autenticar os POS;

- **Protocolo EFT** – Com base no protocolo EFT existente são introduzidas alterações por forma a ser possível gerir e desencadear o processo de actualização de aplicações;

- **Protocolo de Transferência** – Este protocolo especifica como os POS e o SDAs se autenticam mutuamente e como as aplicações EFT são transferidas e actualizadas.

4.3.1 Protocolo de Autenticação

O protocolo de autenticação destina-se a criar a base de confiança que permite aos Produtores de Software, ao SSC e diversos SDA a construção de formas de autenticação.

O SSC, todos os Produtores de Software e todos os SDA devem efectuar as seguintes acções:

- Obter uma cópia segura da chave pública da CA;

- Gerar um par de chaves assimétricas;

- Guardar de forma segura as chaves geradas;

- Solicitar à CA a geração dum certificado para a sua chave pública.

4.3.1.1 Análise da Segurança do Protocolo

A chave pública da CA deve ser inserida e armazenada em segurança em cada um dos elementos. Caso haja a substituição da chave *KuCA* por uma chave falsa, *KuCAFalsa*, existem consequências para o funcionamento do sistema.

Admitamos que a chave *KuCA* é substituída pela chave *KuCAFalsa* pertencente a uma falsa CA. Vamos admitir também que nos elementos onde ocorreu essa substituição, a falsa CA também emitiu novos certificados para as suas chaves públicas assinados com a chave *KuCAFalsa*:

- **Chave de CA falsa nos Produtores de Software** – No Produtor de Software a autenticação realizada com o SSC falha porque o certificado que contem a chave pública do SSC não foi assinado pela chave *KrCAFalsa*. O Produtor de Software não consegue enviar novas aplicações para os POS;

- **Chave de CA falsa no SSC** – No SSC a autenticação dos Produtores de Software e dos SDAs vai falhar porque os certificados emitidos para as correspondentes chaves públicas não foram assinados pela chave *KrCAFalsa*. Como consequência o SSC fica impossibilitado de receber aplicações, nem consegue enviar aos SDAs aplicações para actualização;

- **Chave de CA falsa nos SDA** – No SDA a autenticação efectuada ao SSC e aos POS falha. Como consequência os SDAs não recebem aplicações para actualização nem transferem aplicações para os POS.

4.3.2 Protocolo de Instalação

Nas instalações do fabricante do POS é necessário carregar no terminal o software de base que permite a utilização do equipamento: o *Loader* e o Gestor de Aplicações. Nas mesmas instalações são carregadas em segurança as chaves:

- As chaves assimétricas *KrPOS* e *KuPOS* geradas pelo Produtor;

- Cópia da chave pública da CA, *KuCA*;

- O certificado da chave *KuProd* emitido pela CA;

- O certificado da chave *KuPOS* emitido pelo Produtor.

4.3.2.1 Análise da Segurança do Protocolo

Neste protocolo é importante que o software de base do POS seja carregado em segurança. Caso seja instalado outro software o POS poderá não funcionar como esperado.

À semelhança da norma EMV, é o Produtor do Software que gera e instala as chaves assimétricas do POS: *KrPOS* e *KuPOS*. Depois de geradas e instaladas, a chave *KrPOS* deve ser destruída. Estas acções devem ser feitas em segurança para evitar que alguém possa obter a *KrPOS* e assim fazer-se passar por esse POS.

A instalação da correcta chave da CA, *KuCA*, garante mais tarde que o POS possa validar os certificados emitidos por esta entidade. Se esta chave for trocada pela chave pública

duma CA falsa, o POS validará os certificados emitidos por essa entidade, ficando sobre o seu controlo.

A transferência do certificado da chave *KuProd* permite ao POS recuperar essa chave para poder verificar a assinatura das aplicações produzidas pelo Produtor de Software.

4.3.3 Protocolo de Transferência da Aplicação

O protocolo de transferência da aplicação estabelece a forma como as novas aplicações e os relatórios de certificação devem ser transferidos entre os Produtores de Software e o SSC.

- **Envio da Aplicação**: O Produtor do Software envia para o SSC a aplicação EFT assinada com a chave *KrProd*. O SSC obtém da CA o certificado do Produtor, valida o certificado com base na chave *KuCA* e recupera a chave *KuProd* para verificar a assinatura da aplicação. O SSC envia ao Produtor uma mensagem contendo: o resultado da recepção da aplicação assinada com a chave *KrSSC*. O Produtor obtém da CA o certificado do SSC valida a autenticidade do certificado com base na chave *KuCA* e recupera a chave *KuSSC* para verificar a assinatura da mensagem recebida;

- **Envio do Relatório da Certificação**: O SSC envia para o Produtor uma mensagem contendo o ficheiro do relatório assinado com a chave *KrSSC*. O Produtor obtém o certificado do SSC, valida a autenticidade do certificado com base na chave *KuCA* e recupera a chave *KuSSC* para verificar a assinatura do ficheiro. O Produtor envia ao SSC uma mensagem contendo: o resultado da recepção do relatório assinado com a chave *KrProd*. O SSC usa a chave *KuProd* para verificar a assinatura da mensagem recebida.

4.3.3.1 Análise da Segurança do Protocolo

Neste protocolo é interessante analisar com brevidade os impactos para o sistema dum adversário ganhar individualmente o controlo sobre: o Produtor do Software e o SSC.

- **Produtor de Software** – Suponhamos que um oponente detém: *KrProd* e *KuProd.* Neste caso o oponente consegue submeter para certificação uma

aplicação EFT sob o seu controlo. Os potenciais problemas de segurança resultantes desta aplicação deveriam ser detectados pelo processo de certificação;

- **SSC** – Se o SSC estiver sobre o controlo dum oponente que detém: *KrSSC* e *KuSSC*, pode receber uma aplicação para certificação ou negar o serviço ao Produtor. Em relação ao SSP pode indicar a existência de aplicações para actualização. Relativamente aos SDA pode enviar-lhes aplicações POS sob o seu controlo, no entanto como estas não estão assinadas pelo Produtor do Software, o POS rejeita-as. O maior estrago que este ataque pode produzir é a negação da recepções de aplicações para certificação ou desencadear o processo de actualização de aplicações em massa sem com isso causar outro efeito para além da degradação do serviço de pagamentos. Efeito esse que se for detectado pelo SSP pode ser minimizado na medida em que é ele que controla a ordem para a actualização das aplicações.

4.3.4 Protocolo de Gestão Interna

O Protocolo de Gestão Interna compreende todas as acções entre os diversos elementos do OSP que são necessárias à actualização das aplicações nos POS. Para maior simplificação, este protocolo é subdividido em dois outros, nomeadamente:

- **Transferência do Software para os SDA** – Este protocolo especifica a forma como o SSC deve transferir o software de actualização para os diversos SDA que estarão dedicados a efectuar a transferência da aplicação EFT;

- **Notificação de aplicações EFT disponíveis** – Este protocolo especifica a forma como o SSC deve notificar o SSP de quais os POS que devem ser actualizados.

4.3.4.1 Transferência do Software para os SDA

O SSC envia para cada um dos SDA um ficheiro assinado com a chave *KrSSC*, contendo:

- Modelo do POS compatível com o software;

- Software para actualização.

Cada SDA obtém o certificado emitido pela CA para o SSC e recupera a chave *KuSSC*. O SDA verifica a assinatura do ficheiro usando essa chave. Se a assinatura for verdadeira guarda o ficheiro associando-o ao modelo do POS.

4.3.4.2 Notificação de Aplicações Disponíveis

Sempre que existe uma aplicação certificada, o SSC regista numa base de dados a informação sobre: a versão da aplicação, o modelo dos terminais compatíveis e a assinatura do software (ver Tabela 1).

Registo de Aplicação Disponível
Modelo do POS compatível
Versão da Aplicação
Assinatura do Software assinado com *KrProd*

Tabela 1 : Registo de aplicação disponível na base de dados.

Sempre que o SSP processa um serviço solicitado por um POS consulta essa base de dados. Caso o POS seja compatível com alguma aplicação certificada e possua uma versão de aplicação diferente da que se encontra registada, o SSP ordena ao POS a realização do processo de actualização (ver Figura 22).

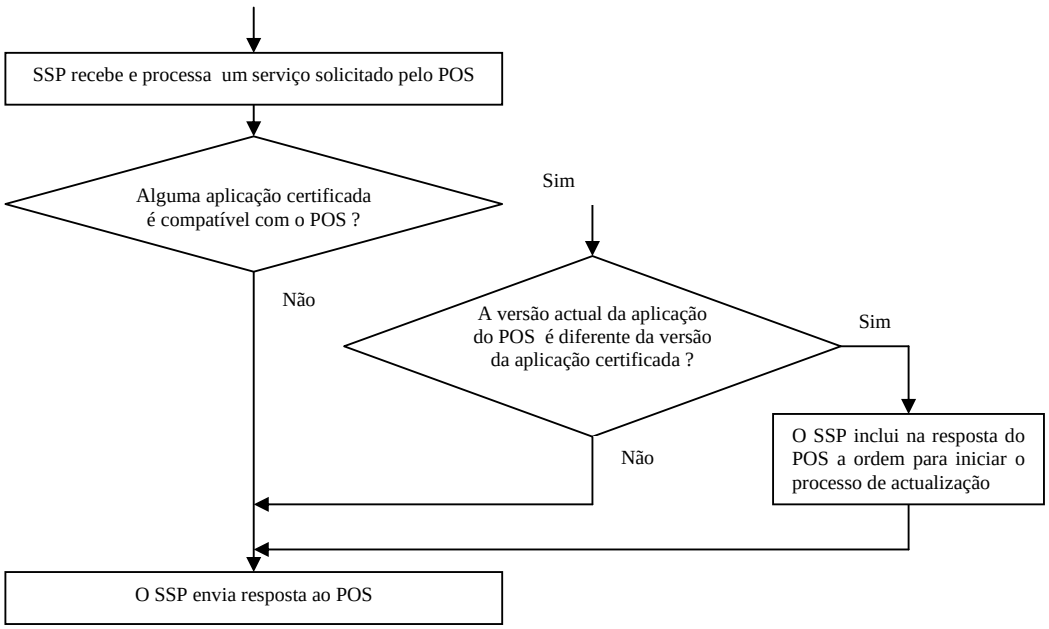


Figura 22 : Processo de decisão de início de processo de decisão.

4.3.4.3 Análise da Segurança do Protocolo

Neste protocolo estão envolvidas as três entidades do OSP: o SSC, os SDAs e o SSP. Já foi referido anteriormente os impactos causados pelo controlo por parte dum oponente sobre o SSC. Vamos analisar brevemente os impactos para o sistema se um adversário ganhar individualmente o controlo sobre: o SDA e o SSP.

- **SDA** – Suponhamos que um oponente detém: *KrSDA* e *KuSDA*. Neste caso o oponente consegue fazer com que um POS receba na integra uma aplicação POS. No entanto, como não se encontra assinada pela chave *KrProd*, o POS rejeita-a. Neste cenário ao controlar o SDA, o adversário também pode recusar todos os pedidos de transferência efectuados pelos POS;

- **SSP** – Está fora do âmbito deste trabalho analisar as consequências do controlo do SSP do ponto de vista das transacções relacionadas com os serviços de pagamento. Vamos limitar a analise às consequências para o sistema de actualização. Suponhamos que um oponente detém: *KrSSP* e *KuSSP*. Neste caso o oponente tem poder para iniciar ou adiar o processo de actualização.

4.3.5 Protocolo EFT

As modificações necessárias ao protocolo EFT, visam dotar o sistema de pagamentos dos mecanismos necessários para desencadear o processo de actualização. Esse mecanismo é integrado no protocolo EFT por intermédio de quatro novas transacções:

- **Transacção "Actualização de Chaves" -** usada para alterar chaves no POS;

- **Transacção "Versão de Chaves" -** usada para conhecer a versão de chaves no POS;

- **Transacção "Início de Actualização"** - usada para dar início ao processo de actualização;

- **Transacção "Fim de Actualização"** - usada para informar o fim do processo de actualização.

Seguidamente, far-se-á a descrição em pormenor do funcionamento e estrutura de cada uma dessas transacções.

4.3.5.1 Transacção "Actualização de Chaves"

O SSP é responsável por manter actualizadas as chaves no POS. A transacção "Actualização de Chaves" (ver Tabela 2) é o mecanismo que permite a alteração das chaves existentes no POS, uma vez que todas as chaves estão sujeitas ao mesmo ciclo de vida: planeamento, geração, distribuição, uso e revogação (planeada ou acelerada).

As chaves públicas utilizadas pelo POS: *KuProd* e *KuCA* são actualizadas enviando um certificado emitido pela CA.

As novas chaves do POS, *KrPOS* e *KuPOS* são enviadas cifradas pela chave *KuPOS* antiga e decifradas no POS com a chave *KrPOS* antiga.

Transacção de "Actualização de chaves"				
Campos da mensagem			**Pedido** (POS - SSP)	**Resposta** (SSP - POS)
MTI			AK01	AK11
Primary Bitmap (Bit Map 1)			M	M
Data Elements	**Bit Map**	**Posição**		
Versão da mensagem	1	1	01	01
Identificador do POS	1	2	M	M
Código de Processamento	1	3	M	M
Número de sequência	1	71	M	M
Próxima MTI a executar pelo POS	1	63		M
Versão de chaves	1	90	M	O
Certificado da Chave KuCA	1	100		O
Certificado da Chave KuProd	1	101		O
Certificado da Chave KuPOS	1	102		O
Chave KrPOS cifrada pela chave KuPOS antiga	1	110		O
Chave KuPOS cifrada pela chave KuPOS antiga	1	111		O
MAC	1	128	M	M

M – Elemento obrigatório na mensagem
O – Elemento opcional, só está presente se o campo código de processamento for diferente de zero.

Tabela 2 : Estrutura da transacção "Actualização de Chaves".

4.3.5.2 Transacção "Versão de Chaves"

A transacção "Versão de Chaves" (ver Tabela 3) é o mecanismo que permite ao SSP conhecer a versão das chaves existentes no POS para sincronização do processo de actualização de chaves. Esta transacção pode ser pedida pelo SSP após se efectuar a transacção "Actualização de Chaves" para determinar se o POS actualizou ou não as chaves.

Transacção de "Versão de Chaves"				
Campos da mensagem			**Pedido** (POS - SSP)	**Resposta** (SSP - POS)
MTI			VK01	VK11
Primary Bitmap (Bit Map 1)			M	M
Data Elements	**Bit Map**	**Posição**		
Versão da mensagem	1	1	01	01
Identificador do POS	1	2	M	M
Código de Processamento	1	3	M	M
Número de sequência	1	71	M	M
Próxima MTI a executar pelo POS	1	63		M
Versão de chaves	1	90	M	
MAC	1	128	M	M

M – Elemento obrigatório na mensagem

Tabela 3 : Estrutura da transacção "Versão de Chaves".

4.3.5.3 Transacção "Início de Actualização"

Esta transacção (ver Tabela 4) tem como objectivo preparar o POS para iniciar o processo de actualização. Na mensagem de resposta são recebidos os parâmetros necessários para a recepção da aplicação, nomeadamente: os dados de comunicação do SDA, a chave pública do SDA e o respectivo certificado emitido pela CA, e a Assinatura da aplicação efectuada pelo Produtor do Software. Esta transacção deve ser desencadeada pelo POS a pedido do SSP ou localmente no POS a pedido do técnico.

Transacção "Início de Actualização"				
Campos da mensagem			**Pedido** (POS - SSP)	**Resposta** (SSP - POS)
MTI			IA01	IA11
Primary Bitmap (Bit Map 1)			M	M
Data Elements	**Bit Map**	**Posição**		
Versão da mensagem	1	1	01	01
Identificador do POS	1	2	M	M
Código de Processamento	1	3	M	M
Número de sequência	1	71	M	M
Versão da aplicação corrente	1	5	M	
Próxima MTI a executar pelo POS	1	63		M
Versão da nova aplicação	1	6		O
Dados de comunicação do SDA	1	7		O
Certificado da Chave KuSDA	1	103		O
Certificado da Chave KuProd	1	101		O
Assinatura do novo software efectuada pela chave KrProd: EKrProd(Hash(software))	1	10		O
Mensagem para o utilizador	1	11		M
MAC	1	128	M	M

M – Elemento obrigatório na mensagem

O – Elemento opcional, só está presente se o campo código de processamento for diferente de zero.

Tabela 4 : Estrutura da transacção "Início de Actualização".

4.3.5.4 Transacção "Fim de Actualização"

A transacção de "Fim de Actualização" (ver Tabela 5) é utilizada pelo POS no final do processo de actualização. A recepção desta informação é essencial para que o SSP registe que o POS já possui (ou não) a nova versão da aplicação, evitando (ou forçando) em contactos futuros que o POS tiver com o SSP, a necessidade de iniciar o processo de actualização.

Transacção "Fim de Actualização"				
Campos da mensagem			**Pedido** (POS - SSP)	**Resposta** (SSP - POS)
MTI			FA01	FA11
Primary Bitmap (Bit Map 1)			M	M
Data Elements	**Bit Map**	**Posição**		
Versão da mensagem	1	1	01	01
Identificador do POS	1	2	M	M
Código de Processamento	1	3	M	M
Número de sequência	1	71	M	M
Versão da aplicação corrente	1	5	M	
Próxima MTI a executar pelo POS	1	63		M
Mensagem para o utilizador	1	11		M
MAC	1	128	M	M

M – Elemento obrigatório na mensagem

Tabela 5 : Estrutura da transacção "Fim de Actualização".

4.3.5.5 Diagrama de Mensagens

Para demonstrarmos a utilização das quatro transacções definidas anteriormente, vamos considerar os seguintes cenários:

- **Alteração de Chaves do POS** - O POS executa uma transacção (por exemplo a compra), durante o processamento do pedido o SSP determina que as chaves do POS necessitam de ser actualizadas. O SSP inclui na mensagem de resposta da transacção o código da transacção "Actualização de Chaves". O POS recebe a resposta ao serviço solicitado, efectua o respectivo processamento, e verifica a existência de um pedido de actualização de chaves enviado pelo SSP. O POS envia a mensagem de pedido desse serviço e em resposta recebe os certificados das chaves: *KuCA*, *KuProd*. Recebe também as novas chaves *KuPOS* e *KrPOS* cifradas pela chave *KrProd* (ver Figura 23).

- **Versão de Chaves do POS** - O SSP deve ter o cuidado de solicitar no fim da actualização de chaves a transacção "Versão de Chaves" para determinar a

correcta actualização das mesmas. Esta transacção pode também ser desencadeada sempre que o SSP achar necessário (ver Figura 23);

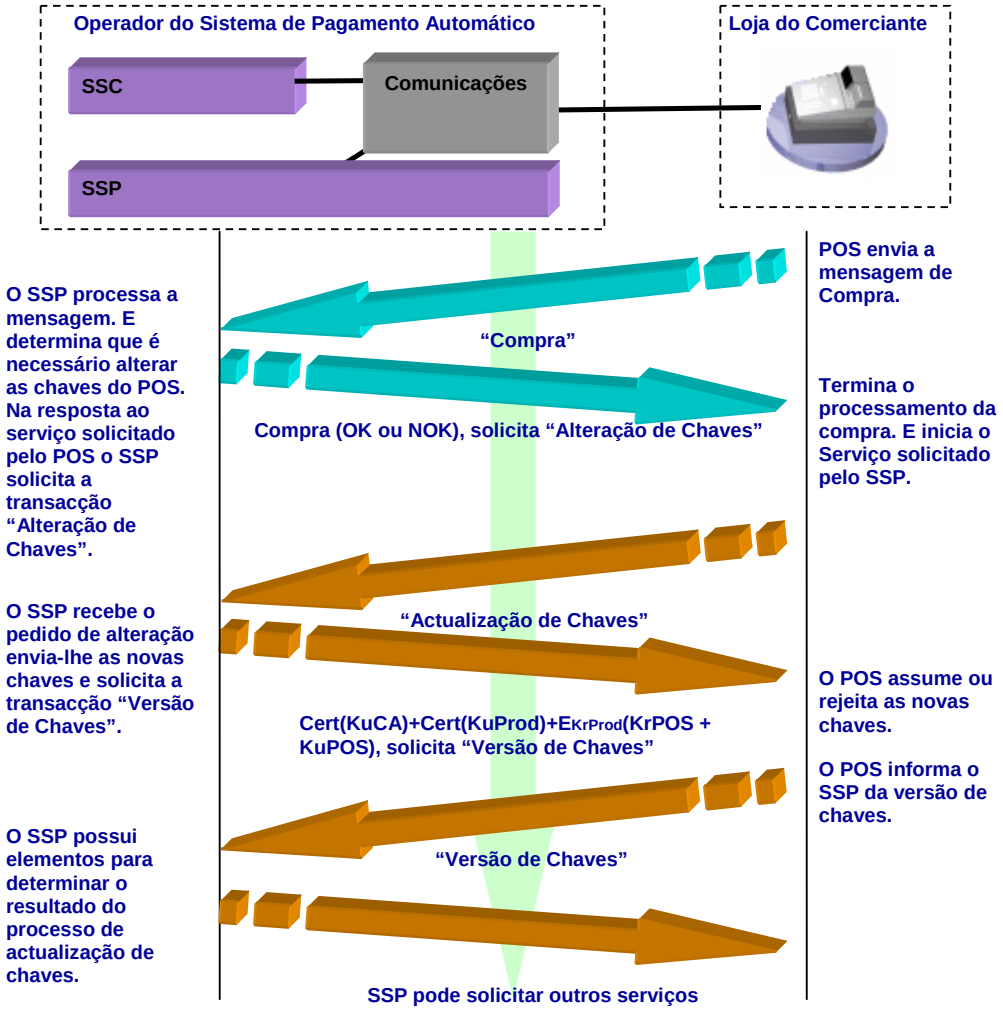


Figura 23 : Sequência de mensagens das transacções de Actualização de Chaves.

- **Início de Actualização** – O POS executa uma transacção e o SSP determina a necessidade de dar início ao processo de actualização. O POS recebe a resposta dessa transacção, efectua o respectivo processamento e verifica a existência dum pedido de actualização enviado pelo SSP. O POS envia a mensagem de pedido da transacção "Início de Actualização" ao SSP para obter os diversos parâmetros necessários para contactar o SDA. Depois de receber esses dados do SSP e uma vez determinada a melhor altura para realizar a operação de actualização o POS recebe a nova aplicação do SDA indicado pelo SSP (ver Figura 24);

- **Fim de Actualização** – Terminada a transferência da nova aplicação, com ou sem sucesso, o POS inicia uma transacção de "Fim de Actualização" para informar o SSP do resultado do processo, função desse resultado o SSP pode determinar acções futuras (ver Figura 24).

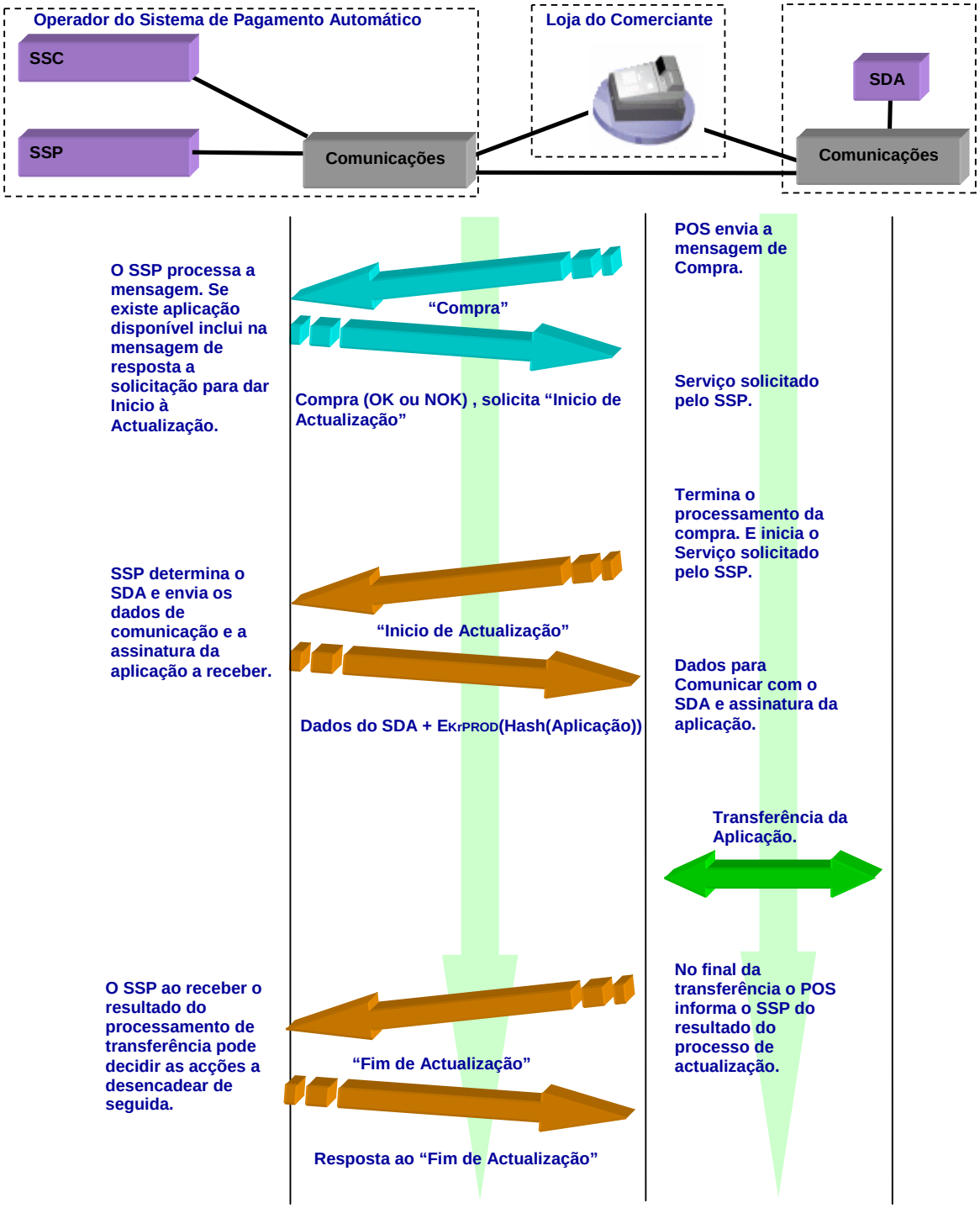


Figura 24 : Sequência de mensagens das transacções de Actualização.

4.3.5.6 Análise da Segurança do Protocolo

Uma vez que estas quatro novas transacções passam a fazer parte do protocolo EFT, utilizam a mesma infra-estrutura de segurança usada para as outras transacções que compõem o referido protocolo. Por essa razão não nos vamos adiantar ao modo como se protegem essas mensagens fazendo apenas referência de que a autenticidade e integridade destas transacções é garantida pelo MAC incluído em cada mensagem.

4.3.6 Protocolo de Transmissão

O protocolo de transmissão define o processo de transferência do software do SDA para o POS e é definido pela sequência das seguintes fases:

- Início da sessão de transmissão;
- Transferência do software;
- Fim da sessão de transmissão.

Em cada uma destas três fases existe a troca de mensagens entre o POS e o SDA. Nos pontos que se seguem vamos explicar o funcionamento detalhado de cada uma destas fases ao mesmo tempo que se justifica a estrutura de cada uma das transacções que as compõem.

4.3.6.1 Início da Sessão de Transmissão

Esta transacção inicia a sessão de transmissão do software. As mensagens trocadas têm como objectivos:

- Efectuar a autenticação mútua entre o POS e o SDA;
- Troca de dados que permitam a adaptação da transferência do software às características dos dispositivos.

O POS toma a iniciativa de contactar o SDA e envia na mensagem de pedido da transacção “Início da Sessão de Transmissão” a informação sobre as suas características de transporte e recepção de dados, de maneira a que o SDA possa adaptar o tamanho das mensagens que transportam a aplicação aos valores suportados pelo terminal. O envio do

formato do ficheiro como parâmetro desta mensagem permite a utilização de diversas formas de compressão de dados.

Na mensagem de resposta o POS recebe informação sobre o tamanho total da aplicação e o número de blocos a receber (ver Tabela 6).

Transacção "Início de Sessão de Transmissão"				
Campos da mensagem			**Pedido** (POS - SDA)	**Resposta** (SDA - POS)
MTI			IS01	IS11
Primary Bitmap (Bit Map 1)			M	M
Data Elements	**Bit Map**	**Posição**		
Versão da mensagem	1	1	01	01
Identificador do SDA	1	80	M	M
Identificador do POS	1	2	M	M
Número de sequência	1	71	M	M
Dimensão máxima do campo de dados	1	81	M	
Código de Processamento	1	3		M
Próxima MTI a executar pelo POS	1	63		M
Formato do ficheiro	1	82	M	O
Dimensão total da aplicação	1	83		O
Número de blocos de dados	1	84		O
Mensagem para o utilizador	1	11		M
Assinatura da mensagem com chave KrPOS: EKrPOS(Hash (Mensagem))	1	85	M	
Assinatura da mensagem com chave KrSDA: EKrSDA(Hash (Mensagem))	1	86		M

M – Elemento obrigatório na mensagem
O – Elemento opcional, só está presente se o campo código de processamento for diferente de zero.

Tabela 6 : Estrutura da transacção "Inicio de Sessão de Transmissão".

4.3.6.2 Transferência da Aplicação

A transferência da aplicação é efectuada com recurso a várias mensagens que mantêm o sincronismo do processo de transmissão e transportam os blocos de dados que formam a aplicação EFT.

Em cada transacção de "Transferência de Dados da Aplicação" o POS informa a identificação do bloco de dados pretendido com base no número total de blocos de dados a receber. Em caso de falha ou interrupção da transmissão, por intermédio deste parâmetro é possível voltar a sincronizar o processo de transferência no momento em que foi interrompido.

Na mensagem de resposta o SDA envia o bloco de dados pedido pelo POS. Enquanto o processo de transmissão não estiver terminado o SDA incluí nesta mensagem o código

desta transacção para que o POS repita o seu envio pedindo um novo bloco de dados (ver Tabela 7).

Transacção "Transferência de Dados da Aplicação"				
Campos da mensagem			**Pedido** (POS - SDA)	**Resposta** (SDA-POS)
MTI			TD01	TD11
Primary Bitmap (Bit Map 1)			M	M
Data Elements	**Bit Map**	**Posição**		
Versão da mensagem	1	1	01	01
Identificador do SDA	1	80	M	M
Identificador do POS	1	2	M	M
Número de sequência	1	71	M	M
Código de Processamento	1	3		M
Próxima MTI a executar pelo POS	1	63		M
Número do bloco de dados	1	90	M	O
Número do próximo bloco de dados	1	91		O
Dimensão dos Dados	1	92		O
Dados da aplicação	1	93		O
Mensagem para o utilizador	1	11		M
Assinatura da mensagem com chave KrPOS: EKrPOS(Hash (Mensagem))	1	85	M	
Assinatura da mensagem com chave KrSDA: EKrSDA(Hash (Mensagem))	1	86		M

M – Elemento obrigatório na mensagem
O – Elemento opcional, só está presente se o campo código de processamento for diferente de zero.

Tabela 7 : Estrutura da transacção "Transferência de Dados da Aplicação".

4.3.6.3 Fim de Sessão de Transmissão

O fim da sessão de transmissão pode ocorrer pelos seguintes motivos:

- **A sessão expirou** – Este cenário corresponde a uma situação anómala detectada pelo SDA em que o POS iniciou uma sessão de transmissão mas que não foi completada atempadamente. Os POS que se encontram nesta situação poderão receber nova ordem do SSP para iniciar o processou ou necessitar de intervenção técnica no local;

- **Sessão cancelada** – Tanto o SDA como o POS podem cancelar o processo de transmissão sempre que detectarem que não estão reunidas as condições para a sua continuação. Incluem-se neste cenário as seguintes situações: O SDA cancela as actualizações em curso por ter recebido uma aplicação mais recente do SSC, o POS detectou uma falha durante o processo, etc.;

- **A sessão terminou sem sucesso** – Este cenário corresponde à situação em que a aplicação foi totalmente transmitida para o POS mas ocorreu um erro na validação da aplicação recebida. Incluem-se nesta situação o caso em que ocorre uma falha na verificação da assinatura da aplicação;

- **A sessão terminou com sucesso** – Este cenário corresponde à situação em que a aplicação foi totalmente transmitida para o POS e que todas as validações aplicáveis à aplicação recebida foram efectuadas com sucesso.

O fim da sessão de transmissão com ou sem sucesso é assinalado pela transacção "Fim de Sessão de Transmissão" (ver Tabela 8). Nesta transacção o POS envia ao SDA o resultado da sessão de transferência. A confirmação dessa recepção é dada pela mensagem de resposta enviada pelo SDA. A integridade e autenticidade das mensagens é garantida pela assinatura do seu emissor.

Esta transacção é enviada no contexto da aplicação que iniciou o processo de actualização. A execução da nova aplicação dá-se num momento posterior ao envio desta transacção. Pode acontecer por exemplo que a aplicação foi correctamente transferida para o POS mas que ocorre um erro durante a sua execução. Esses acontecimentos são externos a este protocolo mas tratados no protocolo EFT (ver secção 4.3.5).

Transacção de "Fim de Sessão de Transmissão"				
Campos da mensagem			**Pedido** (POS – SDA)	**Resposta** (SDA-POS)
MTI			FS01	FS11
Primary Bitmap (Bit Map 1)			M	M
Data Elements	**Bit Map**	**Posição**		
Versão da mensagem	1	1	01	01
Identificador do SDA	1	80	M	M
Identificador do POS	1	2	M	M
Número de sequência	1	71	M	M
Código de Processamento	1	3		M
Próxima MTI a executar pelo POS	1	63		M
Mensagem para o utilizador	1	11		M
Assinatura da mensagem com chave KrPOS: EKrPOS(Hash (Mensagem))	1	85	M	
Assinatura da mensagem com chave KrSDA: EKrSDA(Hash (Mensagem))	1	86		M

M – Elemento obrigatório na mensagem

O – Elemento opcional, só está presente se o campo código de processamento for diferente de zero.

Tabela 8 : Estrutura da transacção "Fim de Sessão de Transmissão".

4.3.6.4 Sequência de Mensagens

A sequência de mensagens que compõem a execução deste protocolo estão ilustradas na Figura 25.

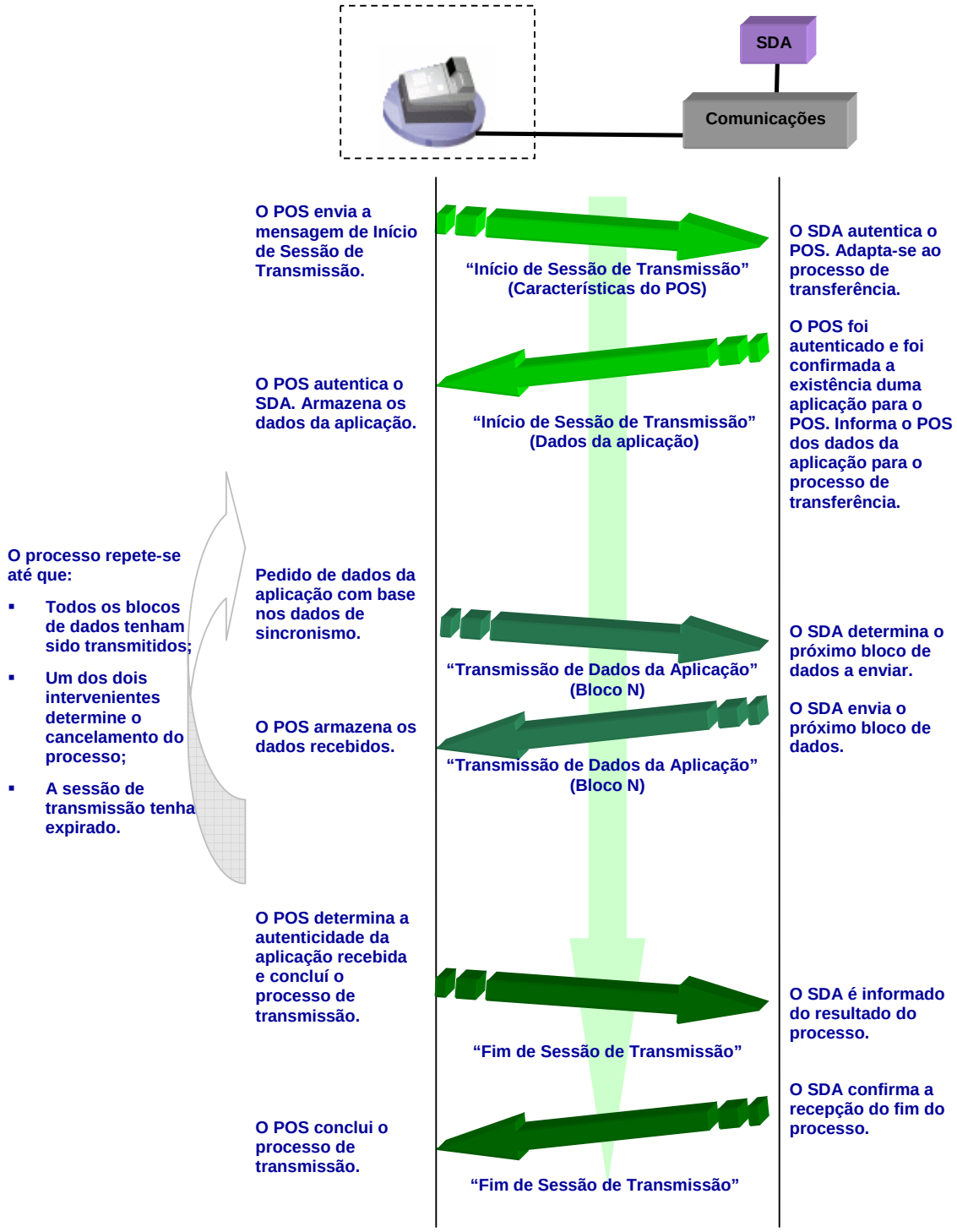


Figura 25 : Sequência de mensagens do protocolo de transmissão.

4.3.6.5 Análise da Segurança do Protocolo

A integridade e autenticidade das mensagens é garantida pela assinatura do seu emissor.

Ambos os intervenientes possuem a chave *KuCA* que lhes permite recuperar dos certificados por ela emitidos a chave pública do seu interlocutor e verificar a autenticidade das mensagens recebidas. O POS recebeu do SSP o certificado emitido pela CA para a chave *KuSDA*. Com base na chave *KuCA* recupera desse certificado a chave *KuSDA*. Com essa chave o POS valida a assinatura das mensagens enviadas pelo SDA. Paralelamente o SDA recupera do certificado do POS, obtido da CA, a chave *KuPOS*. Com base nessa chave pode assim autenticar as mensagens recebidas do POS.

A assinatura do software recebido do SDA foi previamente recebida pelo POS do SSP. Depois de transferido, o POS pode verificar essa assinatura e efectuar as seguintes validações:

- Autenticar a assinatura do software com base na chave *KuProd*;
- Verificar se essa assinatura é igual à transmitida pelo SSP.

Se estas duas acções forem concretizadas o POS pode realizar a substituição do software.

4.4 Sumário

Neste capítulo começou-se por descrever genericamente o conceito de infra-estrutura de chave pública, identificando-se os requisitos para a sua utilização, os componentes envolvidos, a definição da hierarquia e a forma de armazenamento segura das chaves. Baseado nessa infra-estrutura, e relacionando-se com as especificações EMV e "Transferência Segura de Ficheiros" descritas no Capítulo 2, apresentou-se o modelo adoptado, descrevendo a infra-estrutura de segurança e a sua arquitectura. Em seguida apresentaram-se em detalhe os protocolos envolvidos, fazendo-se sempre que justificável uma breve análise à segurança dos mesmos.

Capítulo 5 Realização e Análise de Resultados

O sistema de actualização envolve diferentes sistemas e organizações, aos quais não foi possível ter acesso em tempo para a elaboração deste trabalho.

No entanto, sem recorrer aos sistemas reais, foi desenvolvido um conjunto de aplicações que permitem simular o sistema de actualização. Foram implementados simuladores para cada um dos componentes envolvidos nesta solução, o que traz a vantagem de se poder efectuar a análise do sistema gastando um mínimo de recursos. Permite avaliar em concreto o modelo, os protocolos e o desempenho obtidos com a transferência das aplicações, bem como detectar eventuais falhas, problemas ou melhorias a realizar nos protocolos.

Neste capítulo descreve-se a implementação do simulador do sistema de actualização, os cenários de simulação e a análise dos resultados obtidos.

5.1 Modelo do Simulador

A impossibilidade de obter em tempo útil o acesso aos meios para efectuar a implementação da solução proposta foi a principal motivação para a criação duma simulação dum sistema de pagamentos que implementa a actualização de software para POS. Todos os componentes do sistema, nomeadamente, o POS, SSP, SDA, SSC, SProd e CA, são simulados numa rede de PCs através duma aplicação, SIMGEN, que faz a gestão da infra-estrutura de comunicações TCP/IP e permite realizar a monitorização das mensagens trocadas.

A aplicação de base, SIMGEN, é suficientemente genérica para ser reutilizada por todos os componentes, mas também bastante flexível para suprir as necessidades específicas de cada um deles. A sua flexibilidade advém do uso de DLLs que se registam na aplicação base e que definem o processamento específico.

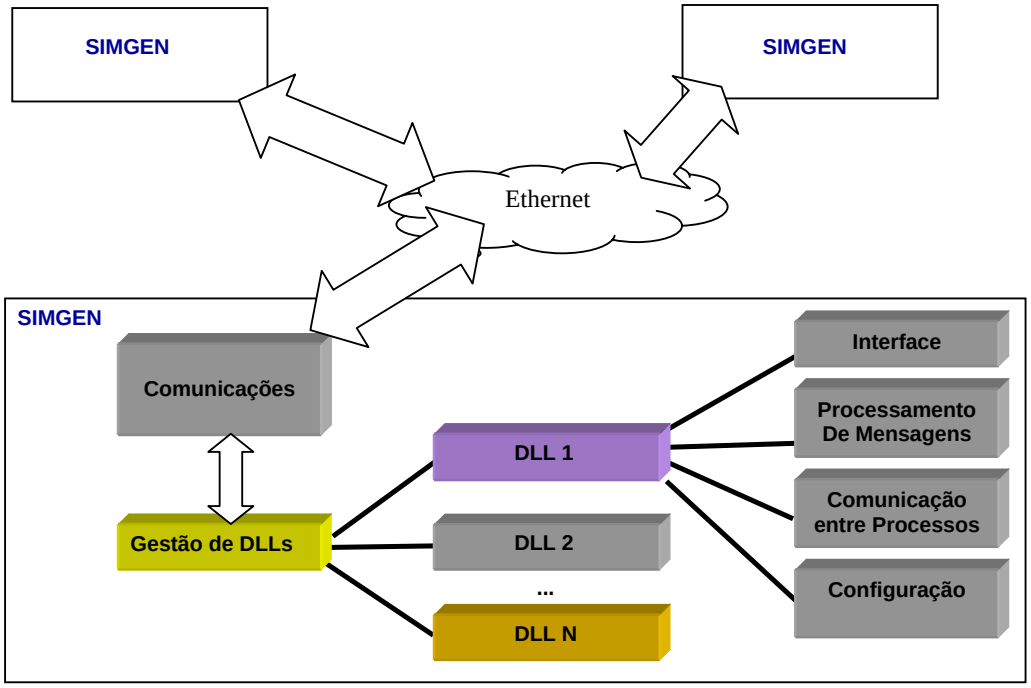


Figura 26 : Estrutura da SIMGEN

Descrevemos seguidamente duas das características de funcionamento que a fazem adaptar à construção de aplicações do tipo Servidor, Cliente ou ambos simultaneamente:

- Em primeiro lugar permite uma espera activa de mensagens sobre um porto TCP. Neste caso ao receber uma mensagem, esta aplicação pesquisa todas as DLLs registadas até determinar a que possui capacidade para efectuar o processamento da mensagem recebida.

- Em segundo lugar, para a implementação da parte cliente, esta aplicação disponibiliza às DLLs um conjunto de funções que lhes permitem abrir um canal de comunicações, tomar a iniciativa de enviar mensagens e esperar pela respectiva resposta.

Genericamente a SIMGEN possui na sua estrutura, um gestor de comunicações e um gestor de DLLs que permite a adição e remoção de DLLs (ver Figura 26).

Todas as DLLs compatíveis com esta aplicação devem possuir um conjunto de funções de interface que permite à SIMGEN reconhecer a sua compatibilidade e comunicar da mesma forma com todas elas.

Esse conjunto de funções disponibiliza:

- A apresentação duma interface humana adequada;
- O envio e recepção de mensagens;
- A comunicação entre DLLs;
- O armazenamento e restauração de diversos parâmetros de configuração.

O ficheiro de configuração assegura no momento de arranque da SIMGEN que todas as DLLs que formam um simulador são carregadas e também que todos os ficheiros de configuração pertencentes a cada uma das DLLs são lidos. Combinando diversas DLLs obtém-se a simulação dum componente específico do sistema. A Figura 27 mostra a organização das aplicações na simulação efectuada.

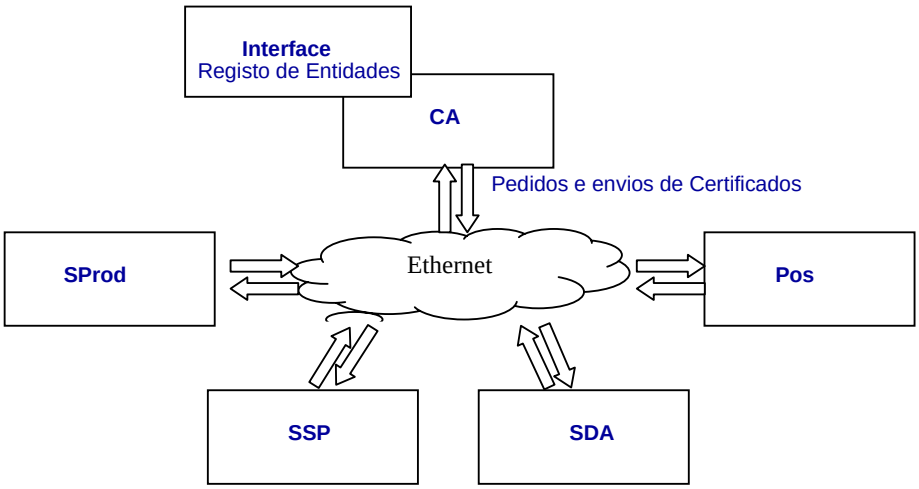


Figura 27 : Organização das aplicações de simulação

O código de simulação foi desenvolvido utilizado a ferramenta Borland C++ Builder [41] e as aplicações foram compiladas para o sistema operativo Windows. As rotinas de segurança utilizadas foram agrupadas por Wei Dai [42].

5.2 Simulação da CA

O modelo do sistema de actualização de software utiliza uma infra-estrutura de segurança de chave pública e depende da existência duma CA para fazer a gestão dos diversos certificados. Para efeitos de demonstração e avaliação de resultados optou-se por implementar uma CA construída com base na aplicação SIMGEN. Nesta CA, os pedidos

de emissão e revogação de certificados são efectuados através duma interface humana onde o utilizador regista:

- Data de início e fim de validade – O certificado é válido entre as duas datas que compõem este período;
- Titular – Identifica o titular do certificado;
- Chave Pública – A chave pública do titular do certificado.

Os pedidos de cópias de certificados e as respostas contendo o correspondente certificado são transmitidos via TCP/IP, ou seja, qualquer entidade pode enviar uma mensagem à CA fazendo o pedido de cópia do certificado, identificando o titular de cuja cópia do certificado pretende receber.

Transacção de "Pedido de Cópia de Certificado"		
Descrição dos campos da mensagem	**Pedido** (para a CA)	**Resposta Positiva** (da CA)
Código da mensagem	"CER001"	"CER101"
Versão da mensagem	M	M
Identificador do Titular do Certificado	M	
Código de resposta		M
Certificado de Chave Pública		M

M – Elemento obrigatório na mensagem

Tabela 9 : Estrutura da transacção "Pedido de Cópia de Certificado".

O certificado emitido pela implementação desta CA não segue o especificado no standard do certificado X.509 mas é composto por elementos semelhantes (ver Tabela 10).

Certificado de Chave Pública			
Descrição dos campos do certificado	**Conteúdo/Formato**	**Tipo de Dados**	**Dimensão**
Versão	"01"	N	2
Número de Série		N	10
Algoritmo	"00001"	N	5
Data de Início de Validade	"AAAA-MM-DD"	C	10
Data de Fim de Validade	"AAAA-MM-DD"	C	10
Titular		C	25
Chave Pública do Titular		H	320
Assinatura da CA – EKuCA(SHA(Versão || Número de Série || Algoritmo || Data de Início de Validade || Data de Fim de Validade || Titular || Chave Pública do Titular))		H	128

|| - Concatenação

N – Numérico, C – Caracter, H - Hexadecimal

Tabela 10 : Estrutura do certificado de chave pública usado na implementação da CA.

5.3 Simulação do Operador do Sistema de Pagamentos

No sistema de pagamentos adaptado à transferência de software para POS fazem parte do OSP o SSC, SSP, e os diversos SDAs. Cada um deles possui atribuições específicas, que dependem contudo de informação sobre os diversos elementos do sistema, tais como: identificação dos Produtores de Software, POS, software para actualização, identificação e dados de comunicação dos servidores.

Esta informação é essencial para que se possam efectuar tanto a validação dos interlocutores, como as decisões intrínsecas ao seu processamento enquanto elementos do sistema. A dependência dessa informação é resolvida com recurso a uma base de dados partilhada.

Base de Dados

Na base de dados do OSP, o modelo relacional escolhido permite guardar toda a informação essencial ao seu funcionamento. Este modelo é constituído pelas tabelas:

- Tabela de CAs;
- Tabela de SDAs;
- Tabela de Produtores de Software;
- Tabela de Software certificado;
- Tabela de POS;
- Tabela de Actualizações.

Na tabela de CAs cada registo guarda a seguinte informação:

- Identificador da CA;
- Dados de comunicação – Endereço e porto TCP/IP da CA;
- Chave pública da CA.

Na tabela de SDAs cada registo guarda a seguinte informação:

- Identificador do SDA;
- Dados de comunicação – Endereço e porto TCP/IP do SDA;

- O identificador da CA responsável por emitir o certificado de chave pública para o SDA.

Na tabela de Produtores de Software cada registo guarda a seguinte informação:

- Identificador do Produtor de Software;
- O identificador da CA responsável por emitir o certificado de chave pública para o SDA.

Na tabela de Software cada registo guarda a seguinte informação:

- Nome do ficheiro;
- Versão de Software;
- Identificador do Produtor de Software;
- Modelo do POS compatível;
- Assinatura de Ficheiro efectuada pelo Produtor de Software.

Na tabela de POS cada registo guarda a seguinte informação:

- Identificador do POS;
- Modelo do POS;
- Versão de Software;
- Chave simétrica para o cálculo do MAC;
- Número de sequência da transacção.

Na tabela de actualizações cada registo guarda a seguinte informação:

- Identificador da actualização;
- Nome do Ficheiro de actualização;
- Lista de SDAs para onde o ficheiro foi transferido;
- Estado da actualização – actualização activa ou inactiva.

Simulador do SSP

O simulador do SSP possui uma interface gráfica que permite a monitorização das mensagens trocadas com os POS. Implementa uma versão reduzida do protocolo EFT composto exclusivamente pelas transacções:

- Compra;
- Actualização de Chaves;
- Versão de Chaves;
- Início de Actualização;
- Fim de Actualização.

Sempre que o SSP recebe uma mensagem verifica se o tipo de transacção recebida corresponde a uma das transacções implementadas. Em caso afirmativo, efectua as validações necessárias a cada campo da mensagem, nomeadamente, formato, dimensão e conteúdo. Valida em particular os dados do POS: número de transação e MAC da mensagem.

Na transacção de Compra, caso todas as validações tenham sucesso, verifica na base de dados se existe alguma actualização de software para o POS, comparando os dados da tabela de actualizações com os da tabela de POSs. Em caso afirmativo desencadeia o processo de actualização.

Simulador do SSC

Esta aplicação possui uma interface gráfica que permite a manipulação dos dados da tabela de actualizações, bem como a inserção manual dos dados da actualização na base de dados do OSP, e ainda desencadear e cancelar os processos de actualização.

Simulador do SDA

Embora faça parte do OSP, em termos de arquitectura, os diversos SDA podem estar geograficamente distribuídos na área abrangida pelos serviços do OSP. Funcionam como um repositório de armazenamento dos ficheiros para actualização, recebendo do SSC o software de actualização para os POS.

Nesta implementação colocou-se disponível uma interface gráfica que permite fazer a configuração dos seus dados de comunicação, a configuração dos dados de comunicação da CA, a monitorização dos ficheiros para actualização, a visualização e modificação da informação referente aos POS autorizados pelo SSC a procederem à actualização.

5.4 Simulador do POS

Na implementação do POS ficou disponível uma interface que permite a definição de parâmetros genéricos relativos ao protocolo EFT, nomeadamente, os dados de comunicação do SSP e a chave assimétrica para o cálculo do MAC.

A chave pública e privada do POS são geradas pelo SProd e colocadas através dum ficheiro no POS em conjunto com o certificado da chave pública emitido pela CA.

No POS foi construída uma interface que permite a parametrização e monitorização do processo de transferência, através dela é possível definir os seguintes parâmetros de actualização:

- Velocidade do processo de transferência;
- Tamanho máximo do bloco de dados;
- Taxa de erros, i.e., percentagem de blocos errados durante a transmissão;
- Habilitar / não habilitar o calculo e verificação do MAC das mensagens;
- Habilitar / não habilitar a geração e verificação das assinaturas das mensagens.

A mesma interface também permite a monitorização de diversos dados do processo de transferência, nomeadamente:

- O identificador do SDA designado para transferir o ficheiro;
- A chave pública do SDA recebida do SSP;
- Os dados de comunicação do SDA designado para proceder à transferência;
- Tamanho total da aplicação;
- Assinatura da aplicação gerada pelo SProd;

- Número total de blocos necessários à transmissão total do ficheiro;
- Número do bloco em transmissão;
- Número de erros do processo de transmissão;
- Velocidade de transmissão.

5.5 Simulador do SProd

A aplicação que simula o SProd possui uma interface que permite a geração do seu par de chaves assimétricas (KrProd e KuProd), permite assinar o ficheiro contendo o software para o POS com a chave privada KrProd. É também através da mesma interface que são geradas as chaves privada e pública do POS (KrPOS e KuPOS) para posterior instalação nesse componente.

A ligação à CA, via TCP/IP, assegura que o SProd possa pedir a geração do certificado da chave pública KuPOS. Esse certificado é gravado num ficheiro e instalado no POS.

5.6 Arquitectura do Software do POS

Embora não tenha sido referido com a ênfase adequada por se tratar dum aspecto fora do âmbito deste trabalho, achámos que valeria a pena nesta altura tecer algumas considerações sobre a arquitectura do software nos POS quanto à maior ou menor dificuldade de implementação do processo de substituição de aplicações.

Em termos gerais uma aplicação pode ser compilada numa de duas formas: código objecto ou código interpretável. A primeira solução geralmente leva a aplicações de melhor desempenho porque toma em consideração as particularidades do sistema para a qual foi construída. Mas exactamente porque possui essa dependência não é portável. Mais, o código fonte tem que ser recompilado para cada sistema diferente onde vai correr.

Usando a aproximação da utilização de código interpretável, o código fonte é transformado em byte codes duma máquina virtual. Uma máquina virtual é um processador teórico, com características standard, que definem coisas como modos de endereçamento, registos e espaço de endereçamento. Uma vez feita a tradução, o código pode ser interpretado por um máquina virtual implementada especificamente para um determinado sistema.

Mesmo assim, em ambas as soluções, em algum nível, existe sempre dependência do sistema, quer se use código compilado quer código interpretado.

Um outro aspecto a ter em consideração é o processo de carregamento. Antes da execução do programa este tem que ser carregado em memória e existem essencialmente dois tipos de código quanto à sua localização em memória: *relocatable code* e *non relocatable code* [16][45]. No primeiro caso todas as instruções do processador são referentes a posições de memória relativas a um endereço de referência em vez de um endereço absoluto. Quando o programa é carregado em memória o endereço de referência é atribuído pelo sistema operativo. Em consequência é possível carregar código em quase qualquer posição da memória e suportar a execução simultânea de vários programas carregados em diferentes *offsets* de memória.

Uma desvantagem desta aproximação é que tipicamente necessita dum sistema operativo para carregar os programas e fazer a gestão dos programas em memória.

A utilização de código *non relocatable* pode ser usada sem necessidade de utilização dum sistema operativo, mas assim o programa estará localizado sempre no mesmo endereço base.

Tendo em consideração o que foi exposto anteriormente, é essencial uma correcta organização do software do POS para minimizar as dificuldades associadas à gestão das aplicações, carregamento e execução, e tirar todo o potencial da actualização de software minimizando onde possível o tempo de transmissão.

Existem vários cenários possíveis para a organização das aplicações dependendo das características físicas do terminal.

Tomemos em consideração dois exemplos extremos: uma arquitectura PC que corre um sistema operativo bem conhecido e uma arquitectura baseada num sistema embebido desenhado de raiz.

Na arquitectura PC, os programas podem ser compilados em código objecto ou interpretado. Existem bastantes construtores de aplicações e várias linguagens de programação disponíveis.

O código máquina resultante (seja código objecto ou interpretado) é tipicamente do tipo *relocatable* e o Sistema Operativo pode ser directamente evocado através de interfaces de programação *Application Program Interface* (API) para efectuar a gestão das aplicações.

A arquitectura do software deve ser organizada nos seguintes módulos e programas:

- Módulo que implementa o Protocolo de Instalação;
- Módulo que implementa o Protocolo de Transferência;
- Módulo que implementa o Protocolo EFT;
- Subrotinas comuns.

Sendo assim as actualizações podem ser efectuadas em separado, e quase se resume a uma tarefa de receber, verificar, substituir e apagar ficheiros.

Por outro lado os sistemas embebidos são desenhados para soluções particulares e que necessitam de implementações especiais. Neste tipo de sistemas o número de fabricantes de software é bastante restrito, existem poucas ferramentas de desenvolvimento disponíveis e quase nenhumas implementações de máquinas virtuais ou sistemas operativos. Consequentemente a solução mais simples para uma actualização de software consiste em gerar os programas em código *non relocatable* e substituir todas as linhas de código máquina pelas recebidas no ficheiro de actualização.

Nesta situação, as tarefas envolvidas são:

- Guardar a aplicação recebida em memória não volátil sem apagar a aplicação que se encontra em execução;
- Verificar a integridade da aplicação recebida;
- Copiar a aplicação recebida para o espaço de endereçamento da aplicação antiga ou apontar o endereço de reset do processador para a nova aplicação;
- Libertar o espaço de endereçamento desnecessário para futuras actualizações.

Esta solução pode conduzir a tempos de transmissão mais elevados porque a aplicação não se encontra dividida em módulos independentes tendo que ser transmitida como um todo. Uma melhor solução (mas também mais cara do ponto de vista económico) consiste

em construir um sistema operativo para o sistema embebido, dividir a aplicação EFT segundo a organização já referida anteriormente e utilizar código *relocatable*. Como os módulos podem ser actualizados em separado esta alternativa pode conduzir a uma redução efectiva dos tempos de transferência e actualização.

5.7 Simulação e Análise de Resultados

O ambiente de simulação é constituído por uma rede Ethernet a funcionar a 10MBits/s que liga dois PCs, PC1 e PC2. O PC1 foi equipado com um processador AMD Duron @ 1,4GHz com 128MBytes e o PC2 equipado com um processador Pentium Celeron @700MHz também com 128MBytes.

Nesta implementação foi usada para função de hash o SHA[8] e como algoritmo de cifra o RSA[9][10][15] com chaves de 1024 bytes.

5.7.1 Preparação da Simulação

A simulação começa pela distribuição dos diversos componentes do sistema pelos dois PCs (ver Figura 28). No PC1 ficaram instalados os simuladores do OSP, o SSP, o SSC e o SDA tendo-lhes sido atribuídos os portos 7000, 7001 e 7002. No PC2 ficaram instalados o SProd, a CA e o POS, respectivamente nos portos 7003, 7004 e 7005.

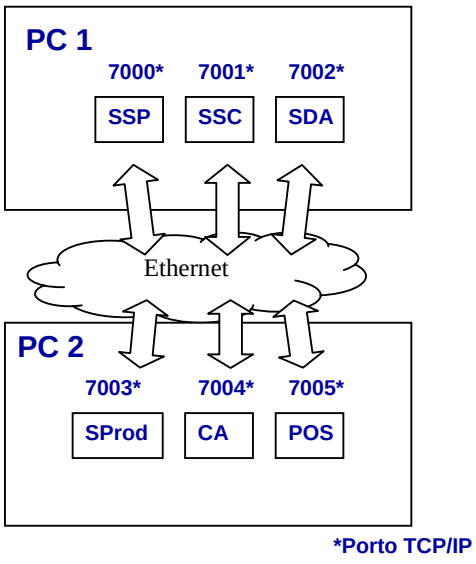


Figura 28 : Distribuição dos componentes por PC

A simulação prossegue com a execução do protocolo de autenticação. Em primeiro lugar obteve-se uma cópia do certificado da chave pública da CA (CERT_KuCA) para o SProd, SDA e SSC. Este certificado foi pedido através da interface da CA que em consequência gerou um ficheiro contendo o certificado. Depois, accionou-se para cada um dos componentes mencionados, o mecanismo de geração do par de chaves assimétricas, pública e privada. Através da mesma interface da CA, registaram-se os componentes na sua base de dados interna, tendo-lhes sido atribuídos respectivamente os identificadores SProd00001, SDA00001, SSC00001 e POS00001.

Segue-se a execução do protocolo de instalação. No SProd foi gerado o par de chaves assimétricas para o POS, respectivamente KuPOS e KrPOS. Através da interface do POS esta informação foi instalada neste componente em conjunto com uma cópia do certificado de chave pública do SProd (CERT_KuSProd) e uma cópia do certificado de chave pública da CA (CERT_KuCA).

Através da interface do SSP inseriram-se na base de dados do OSP os dados do novo POS: identificador, modelo, versão de software, e número de transacção. Em resultado dessa acção o SSP gerou a chave de MAC que foi inserida no POS.

A partir deste momento passa a ser possível realizar transacções EFT entre o POS e o SSP.

O protocolo de Transferência da Aplicação é desencadeado na interface do SProd indicando o ficheiro que contem a nova aplicação e fazendo-o gerar um ficheiro contendo a assinatura do código da aplicação. Estes dois ficheiros são inseridos no OSP através da interface do SSC caracterizando a versão do software e os modelos de POS a que se destinam.

Nesta implementação o SDA tem acesso ao ficheiro que contem a aplicação uma vez que tanto o SDA como o SSC estão na mesma máquina.

As medições efectuadas foram dirigidas em particular para as transacções de actualização de software e incluem todas as transacções executadas entre o POS e o SDA.

5.7.2 Cenários de Simulação

Pretendeu-se avaliar a influência no desempenho do protocolo de transferência quando de diversos factores, nomeadamente, o tamanho das aplicações a transferir, a velocidade de

transmissão, o tempo despendido na geração e verificação de assinaturas, a taxa de erros de comunicação durante a transmissão e o tamanho dos blocos de dados.

As condições iniciais, salvo indicação em contrário, são comuns a todas as simulações. Os ficheiros de transporte das aplicações possuem dimensões compreendidas entre 500Kbytes e 2Mbytes. Admitindo que o ficheiro de transporte pode conter uma aplicação em formato comprimido, a aplicação na realidade pode ser bastante superior a esta medida [43][44]. As velocidade de transferências nos ensaios efectuados variam entre 9,6Kbit/s e 10Mbit/s. Estas velocidades foram escolhidas em função da sua utilização. A velocidade de 9,6Kbit/s é utilizada na grande maioria dos terminais POS ligados ao SSP, correspondendo a uma ligação telefónica. A escolha da velocidade de 10MBit/s disponibiliza indicadores sobre o comportamento do protocolo à medida que se começam a utilizar novas tecnologias de transmissão. O tamanho do bloco de dados foi fixado em 2048bytes por ser um valor razoável para utilização com os actuais equipamentos POS.

Nas secções que se seguem são apresentadas, se existirem, as condições particulares da simulação, os resultados e a sua análise.

5.7.2.1 Influência da Geração e Verificação de Assinaturas

O desempenho do protocolo foi avaliado quanto à influência da realização da geração/verificação de assinaturas.

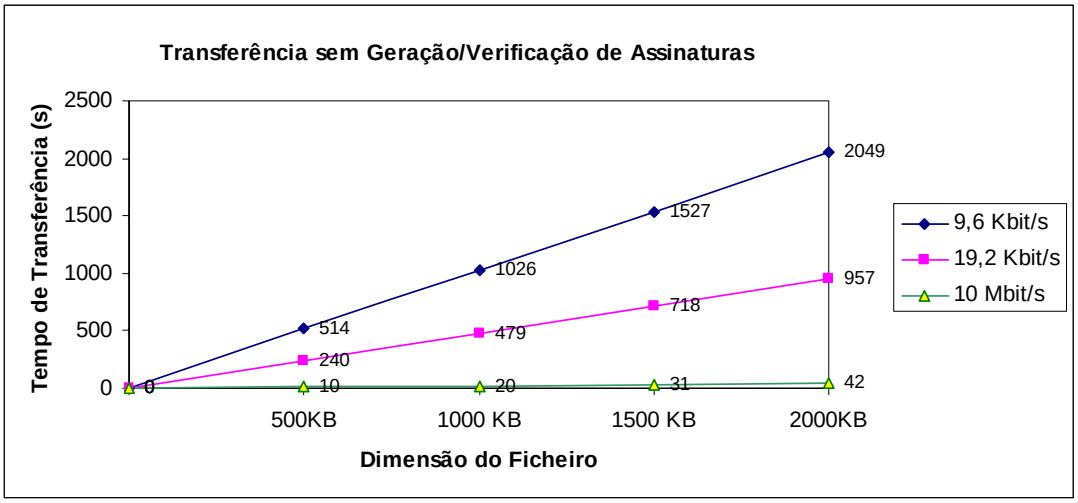


Figura 29 : Transferência sem Geração/Actualização de Assinaturas

Os resultados apresentados na Figura 29 correspondem ao desempenho do protocolo de transmissão não havendo geração ou verificação das assinaturas ou erros de comunicação.

A análise dos resultados apresentados permite-nos concluir resultados óbvios e comuns a este tipo de situações, mas que servem para validar o modelo. A baixas velocidades de transmissão existe uma proporcionalidade inversa entre a velocidade de transmissão e o tempo de transmissão. No entanto esse fenómeno desaparece quando a velocidade de transmissão aumenta, em particular a 10Mbit/s, devido ao tempo de processamento das mensagens que se aproxima do tempo de transmissão.

Existe um outro fenómeno da mesma natureza entre os tempos de transmissão e o tamanho do ficheiro transmitido uma vez fixada a velocidade. Assiste-se a uma proporcionalidade directa, ficheiros com o dobro do tamanho demoram cerca do dobro do tempo a serem transmitidos.

Ao introduzir-se a capacidade de geração e verificação de assinaturas durante o processo de transferência verifica-se uma degradação no desempenho do sistema, conforme se mostra na Figura 30.

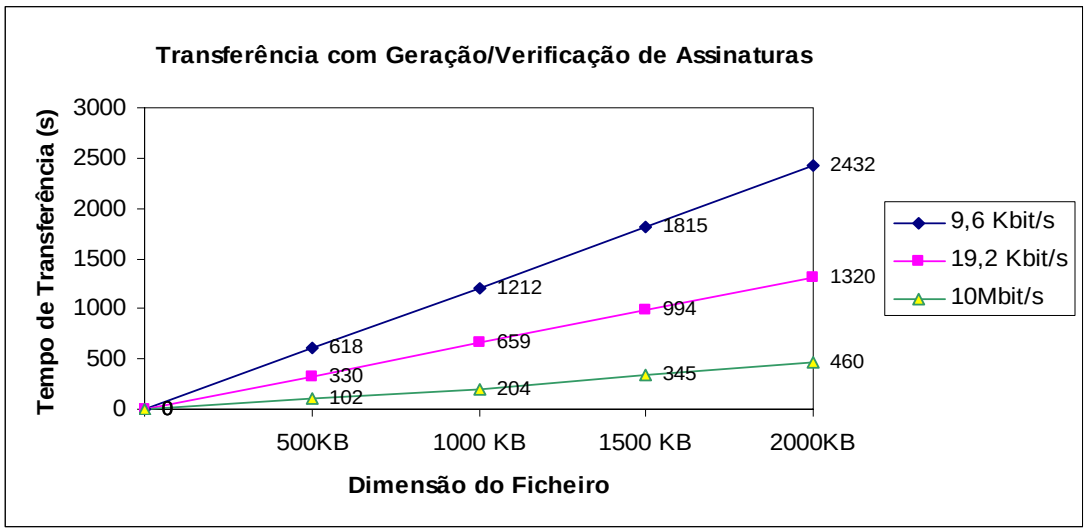


Figura 30 : Transferência com Geração/Verificação de Assinatura

O acréscimo do tempo de processamento e o correspondente aumento do tempo global de transmissão resulta do somatório do tempo despendido em cada mensagem para a geração e verificação das assinaturas de ambos os intervenientes no processo de transferência.

Uma vez que estamos perante o mesmo fenómeno perturbador é de esperar que haja uma diminuição de desempenho uniforme uma vez fixada a velocidade de transmissão e o tamanho do ficheiro transmitido.

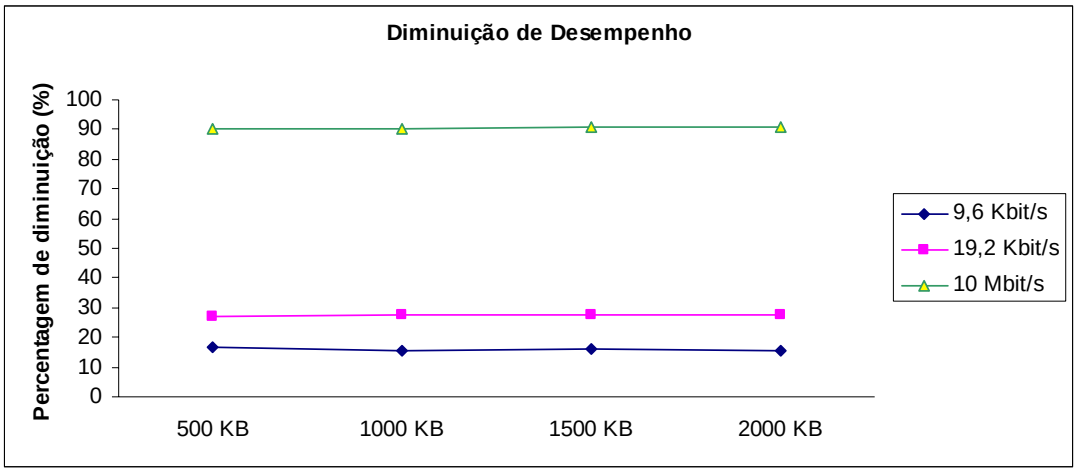


Figura 31 : Diminuição do Desempenho do Processo de Transferência

A Figura 31 confirma que a diminuição de desempenho se deve ao facto de se ter introduzido geração/verificação das assinaturas.

Considerando o pior caso nos resultados anteriormente obtidos, conclui-se que a uma velocidade de 9,6 Kbit/s a transmissão da aplicação demoraria cerca de 40 minutos a concluir.

Este valor é suficiente para constatar que:

- Durante o normal funcionamento do POS, haverá em muitos casos, períodos de inactividade desta ordem de grandeza. O custo de comunicações associado a este intervalo de tempo é suportável e muito mais reduzido do que uma intervenção técnica realizada com a presença humana;

- Durante esses 40 minutos é provável que existam diversas interrupções, por um lado devido possíveis a erros de transmissão, por outro à necessidade de realizar operações de cliente. Estes dois factores confirmam a necessidade do protocolo de transferência possuir mecanismos de recuperação que permitam construir o ficheiro aproveitando os blocos de dados já transferidos.

5.7.2.2 Influência do Tamanho do Bloco de Dados

Podemos pensar que o protolcolo de transferência é tanto mais eficiente quanto menor for a informação redundante transmitida. Ainda que necessária, essa informação está presente na totalidade do conteúdo das mensagens enviadas pelo POS ao SDA, e no cabeçalho das

mensagens enviadas do SSP para o POS. Podemos reduzir esta interferência diminuindo o número de transacções necessárias para a transmissão do ficheiro aumentando o tamanho do bloco de dados em cada transacção. No entanto, aumentando o bloco de dados estamos também a aumentar o tempo de processamento para a geração/verificação de assinaturas. Como a geração/verificação das assinaturas é efectuada sobre o Hash das mensagens, logo é independente do tamanho do bloco de dados. O acréscimo de tempo nesta situação deve-se ao processamento do cálculo do Hash da mensagem.

O desempenho do protocolo foi avaliado face a variações do tamanho do bloco de dados. Para todas as simulações deste cenário utilizou-se um ficheiro com 500Kbytes transferido sobre TCP/IP a uma velocidade de 10Mbit/s com geração/verificação de assinaturas. Em cada simulação o bloco de dados foi configurado para um múltiplo de 1024 bytes. A Figura 32 mostra os valores médios obtidos.

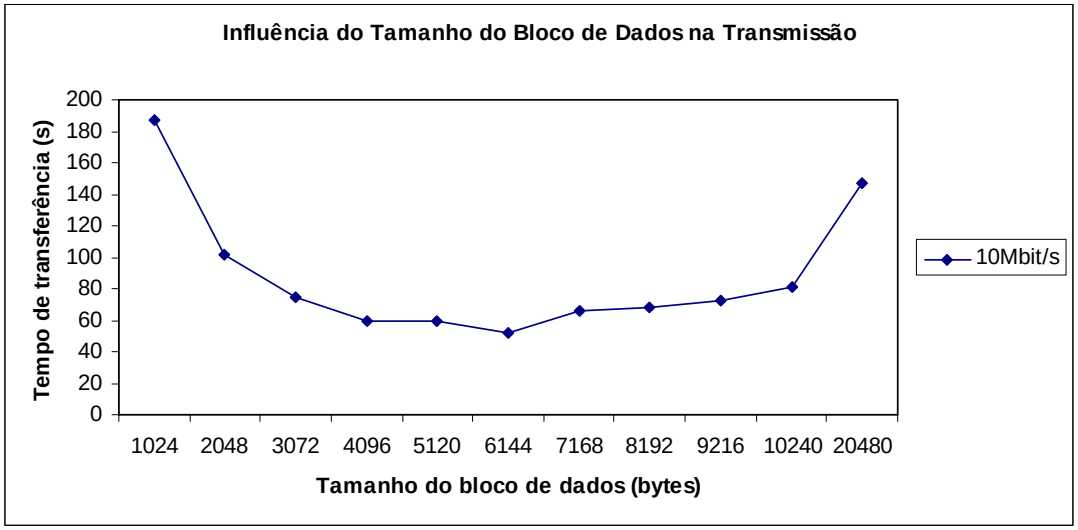


Figura 32 : Desempenho do Processo de Transferência função do Tamanho do Bloco de Dados

Até o bloco de dados atingir o tamanho de 6144 bytes assistiu-se a uma diminuição do tempo de transferência explicada pela diminuição do número de transacções. A partir desse valor, embora o tamanho do buffer fosse aumentando, verificou-se que o tempo de transmissão aumentava. A implementação do simulador fornece a interpretação deste fenómeno. Acontece que a partir desse valor, as transacções eram fragmentadas ao nível das camadas de comunicação aumentando em consequência o tempo de processamento das mesmas. Verifica-se nesta situação a existência dum valor óptimo para o tamanho do bloco de dados.

5.7.2.3 Influência dos Erros de Transmissão

Os erros de transmissão podem ser detectados pelo POS ou SSP sempre que ocorra um dos seguintes problemas:

- Impossibilidade de enviar uma mensagem;
- Tempo expirado durante a espera duma mensagem;
- Tamanho da mensagem recebida diferente do esperado;
- Erro na identificação da origem da mensagem;
- Alteração na ordem das mensagens;
- Assinatura da mensagem inválida;
- Formato ou intervalo de valores errado admitidos nos diversos campos da mensagem.

Essas validações podem falhar por um de dois tipos de interferência no canal de comunicação:

- Fenómenos de natureza física que se manifestaram durante a propagação da mensagem que são detectados ao nível físico dos dispositivos de comunicação;
- Fenómenos de natureza lógica, como por exemplo, erros de programação ou ataques de integridade perpetuados por adversários, que alteraram o conteúdo da mensagem sem com isso provocar erros detectados pelos dispositivos físicos de comunicação.

É interessante verificar como se comporta o protocolo na presença de erros de comunicação. Os resultados permitem verificar se na presença de determinada taxa de erros o sistema de actualização continua ou não a ser exequível. Embora de forma especulativa também se pode tentar estabelecer uma relação entre a taxa de erros e a origem dos mesmos.

Neste cenário de simulação as condições iniciais são as seguintes: o tamanho do bloco de dados foi fixado em 2048bytes, a velocidade de transmissão foi fixada em 10Mbit/s, o

tamanho do ficheiro de transporte da aplicação foi fixado em 500Kbytes e o sistema executa a geração e a verificação das assinaturas das mensagens.

Nos ensaios efectuados fez-se variar a percentagem de erros de transmissão admitindo que a probabilidade de ocorrência de um erro de transmissão numa transacção possui uma distribuição uniforme.

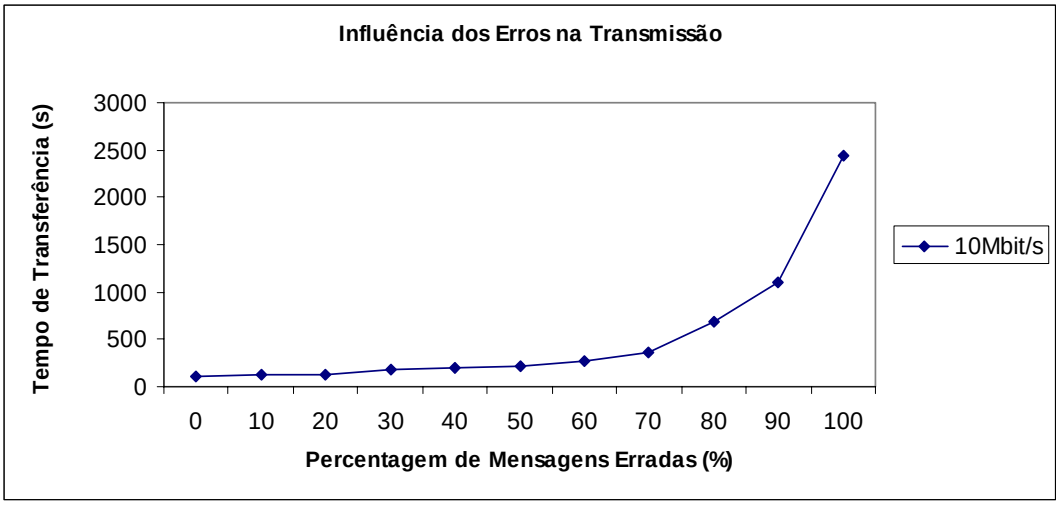


Figura 33 : Desempenho Médio do Processo de Transferência na presença de erros de transmissão

O tempo de transferência aumenta exponencialmente face aos erros de transmissão devido à repetição das transacções e à possibilidade de nas mesmas ocorrerem erros.

Os resultados obtidos são interessantes porque mostram que o desempenho do sistema é aceitável mesmo quando a probabilidade de ocorrência de erros é de 50%.

5.8 Conclusões

A implementação da solução, ainda que simulada, permite fazer a avaliação do desempenho do protocolo.

Constata-se que numa situação ideal de transmissão, sem erros e sem geração/verificação de assinaturas, utilizando a velocidade de transmissão típica de 9,6KBit/s os tempos de transmissão variam entre 514 e 2049 segundos para actualizações de aplicações usando ficheiros de transporte com dimensão entre 500Kbytes e 2MBytes.

Quando se procede à geração/verificação de assinaturas, no pior caso o tempo de transmissão ascende a cerca de 40 minutos. Se considerarmos que enquanto o POS está a proceder ao processo de actualização não permite a realização de transacções EFT

significa que com ficheiros de transmissão da ordem de 2Mbytes o serviço de pagamentos pode ficar indisponível por períodos dessa ordem de grandeza. É por isso importante que o POS disponha de mecanismos que permitam a interrupção do processo de transferência sempre que exista necessidade de executar operações de cliente. Por outro lado é um valor perfeitamente aceitável face aos períodos de inactividade comercial dos estabelecimentos onde existe certamente períodos de inactividade de ordem de grandeza superior durante o qual o processo de actualização pode decorrer sem prejuízo da interrupção do serviço de pagamentos. Em todo o caso o protocolo de actualização, tal como se encontra desenhado, suporta que um POS faça múltiplas interrupções durante o processo de actualização prosseguindo a actualização nos tempos de inactividade.

A evolução no tipo de infra-estrutura de comunicações diminui este problema uma vez que para velocidades de comunicação da ordem dos 10Mbit/s os tempos de transmissão podem ser desprezados face aos períodos de inactividade comercial dos estabelecimentos.

O tamanho do bloco de dados é um factor a ter em conta na implementação do POS. Embora teoricamente o tamanho do bloco seja inversamente porporcional ao tempo de transmissão, os valores obtidos demonstraram que para a implementação realizada existe um valor óptimo para o bloco de dados que não corresponde ao maior valor possível.

O protocolo mostra-se também exequível mesmo em condições de transmissão com erros. Concluiu-se que embora exista um porporcionalidade exponencial entre a taxa de erros e o tempo de transmissão, o sistema pode ser considerado linear, e portanto exequível mesmo quando a taxa de erros é de cerca de 50%.

Os diversos resultados obtidos também são importantes para dimensionar o sistema nas suas várias componentes, ajudando a analisar outras variáveis que influenciam o processo de actualização como um todo, como por exemplo, o número de SDAs necessários para um processo de actualização de grande escala, o número de transferências que podem decorrer em simultâneo e o processo de gestão de actualizações a implementar no SSP face às restrições anteriores;

5.9 Sumário

Este capítulo foi dedicado à descrição da implementação do simulador que foi desenvolvido para implementar o sistema de actualização de software. Descreveu-se o

funcionamento genérico da aplicação de base que permitiu a implementação dos diversos componentes do sistema.

Antes de se descrever o ambiente de simulação fizeram-se algumas considerações sobre a organização do software dos POS e o modo como esta pode influenciar a menor ou maior dificuldade de actualização.

Nas secções seguintes procedeu-se à descrição do ambiente e das condições de teste do protocolo que permitiram obter resultados para a sua avaliação. Fez-se a análise dos resultados obtidos em diversas situações distintas de transferência de aplicações permitiram determinar a viabilidade de implementação.

Capítulo 6 Conclusões e Trabalho Futuro

Com o trabalho desenvolvido nesta dissertação lançaram-se as bases para a implementação duma solução de actualização de aplicações para POS, num sistema de pagamentos que permite, conforme explicado, obter múltiplas vantagens na gestão das aplicações dos terminais de sistemas de pagamento, tanto em termos de segurança como de economia.

O trabalho futuro depende em parte da vontade política e da visão estratégica das organizações envolvidas nesta solução, uma vez que a decisão da sua implementação terá necessariamente que partir das entidades que gerem os sistemas de pagamentos.

Como continuação deste trabalho segue-se a simulação do processo de transferência utilizando vários POS reais. Nesta fase é extremamente importante a utilização de equipamentos com características distintas, nomeadamente, os equipamentos mais representativos em termos de mercado e utilização, os que oferecem melhores desempenhos técnicos e perspectivas de evolução versus os que oferecem os piores desempenhos. Isto implica naturalmente a implementação do software de base do POS.

Os resultados obtidos com essas experiência, permitem tirar conclusões mais precisas sobre o desempenho para esses casos concretos, conhecer as dificuldades de implementação e efectuar os ajustes necessários ao protocolo como um todo.

Depois de obtidos e analisados esses resultados, e tendo o consenso sobre a viabilidade da implementação do processo nos POSs, seguir-se-ia um estudo sobre o impacto deste protocolo no funcionamento do sistema de pagamentos. Esse estudo deveria abordar as alterações necessárias a efectuar na actual implementação do sistema de pagamentos, bem como a necessidade de encontrar soluções e recursos informáticos adequados para a implementação dos diversos servidores.

Embora a análise dos aspectos técnicos seja sem dúvida da maior importância, há também que incluir nesse estudo uma análise cuidada, económica e financeira, sobre a viabilidade do projecto.

Se os estudos concluírem que existem condições para avançar com a implementação da solução, então, dever-se-ia gradualmente substituir cada um dos componentes simulados pelos seus equivalentes reais, e analisar em cada iteração o desempenho do protocolo nessas condições, sempre tendo o cuidado de rever, em detalhe, quaisquer situações anómalas encontradas para atempadamente efectuar as correcções necessárias.

Estando todos os componentes do sistema na sua versão final, será altura de um teste de carga de forma a colocar a descoberto qualquer vulnerabilidade do sistema. Seria então altura de entrar em produção.

Conforme mencionado no início deste capítulo, a implementação deste processo depende do interesse e vontade política, bem como da estratégia das organizações. Quer isto dizer que a implementação deste sistema deverá trazer vantagens para todas as partes envolvidas. Poderá depender de consenso, ou ser imposta pelo operador do sistema de pagamentos.

Caso esta solução seja vantajosa apenas para os implementadores dos sistemas de POS e não haja colaboração do operador do sistema de pagamentos, pensamos que neste caso, parte da solução poderá ser utilizada, considerando para o efeito as devidas alterações. Também nesta situação há matéria de investigação para trabalho futuro.

Anexo 1 Segurança Informática

Neste anexo, faz-se uma breve introdução a conceitos relacionados com a segurança informática que são objecto de referência ao longo deste trabalho.

A.1.1Tipos de Algoritmos Criptográficos

Um algoritmo criptográfico é composto pelos procedimentos de cifra (*E – enciphering*) e decifra (*D – deciphering*), que muitas vezes são idênticos ou simplesmente possuem os mesmos passos mas executados por ordem diferente.

A chave de um algoritmo criptográfico é um parâmetro usado na transformação do texto em claro em texto cifrado e vice-versa. As chaves seleccionadas são constituídas por uma sequência de números ou caracteres.

Uma chave de cifra *Ke* (*enciphering Key*) é usada para tornar um texto em claro *X* num texto cifrado *Y*.

$$E_{Ke}(X)=Y \qquad \textbf{Equação 1-1}$$

Uma chave de decifra *Kd* (*deciphering Key*) é usada para decifrar o texto cifrado *Y* tornando-o em texto claro *X*.

$$D_{Kd}\left(E_{Ke}\left(X\right)\right)=D_{Kd}\left(Y\right)=X \qquad \textbf{Equação 1-2}$$

Se os algoritmos *E* e *D* são públicos então a segurança criptográfica depende apenas da protecção das chaves.

Nos sistemas informáticos utilizam-se dois tipos de algoritmos criptográficos:

- Algoritmos simétricos;
- Algoritmos assimétricos.

A.1.1.1 Algoritmos Simétricos

Num algoritmo simétrico, também chamado de chave secreta, é usada apenas uma chave (*Ks*), partilhada pelo o emissor e pelo receptor. Esta chave é usada tanto para cifrar como para decifrar, tendo assim de ser conhecida quer pelo emissor quer pelo receptor (ver Figura 34).

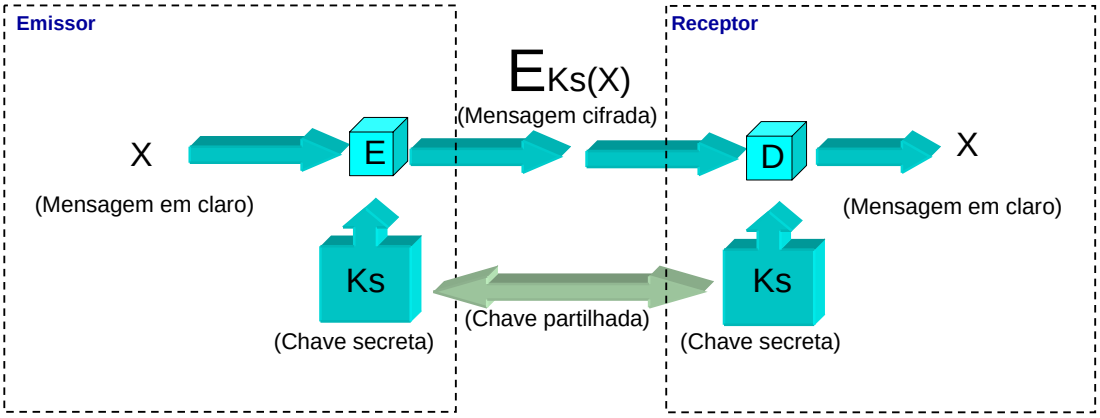


Figura 34 : Sistema de criptografia simétrica usado para garantir confidencialidade.

Ao longo dos anos foram definidos vários algoritmos de chave secreta, mas todos têm o mesmo propósito, a transformação reversível do texto cifrado em texto em claro. O texto cifrado é inútil para quem não tenha a chave secreta que o decifra.

Como tanto o emissor como o receptor partilham a mesma chave, a segurança deste tipo de criptografia depende da não revelação da chave secreta a pessoas ou sistemas não autorizados.

Alguns exemplos destes algoritmos são o DES, AES ou IDEA.

A.1.1.2 Algoritmos Assimétricos

Num algoritmo assimétrico, ou de chave pública, as chaves de cifra e de decifra são diferentes. Uma chave é tornada pública enquanto que a outra é mantida privada. Os comunicadores devem conseguir calcular um par de chaves de forma eficiente, de tal forma que conhecendo uma chave, seja computacionalmente difícil calcular a outra.

Se a chave *Ku* é tornada pública sem comprometer a segurança de *Kr*, que é mantida em segredo, então o algoritmo assimétrico pode ser usado para a comunicação de

dados segura. Neste caso, todos podem cifrar uma mensagem usando a chave pública do receptor mas só o receptor pode decifrar a mensagem com a chave privada que só ele conhece (ver Figura 35). O algoritmo de cifra assimétrica que tem sido mais usado é o RSA [9][10][15].

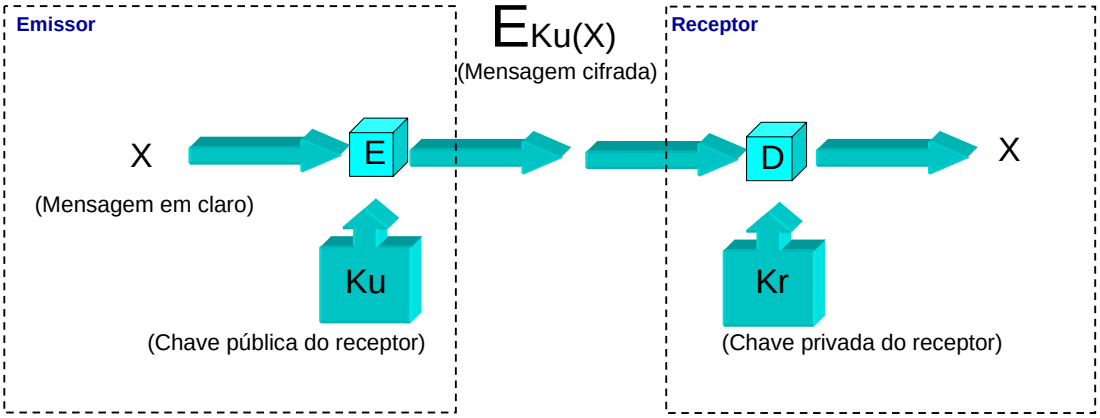


Figura 35 : Sistema de criptografia assimétrica usado para garantir confidencialidade.

A.1.1.3 Algoritmos de Hash

Os algoritmos de *hash* são também conhecidos por outras designações, como: algoritmos de compressão, algoritmos de contracção, *message digest* (resumo da mensagem), e *manipulation detection code* (MDC). Um algoritmo de *hash* recebe como entrada um texto de dimensão variável (pré-imagem) e converte-o num texto de dimensão fixa *h* (o valor de *hash*) normalmente mais pequeno.

$h=H(M)$, onde h é de dimensão m **Equação 1-3**

Muitos algoritmos conseguem transformar um texto com uma dimensão arbitrária num outro de dimensão fixa mas os algoritmos *one-way hash* possuem propriedades adicionais, nomeadamente:

- Dado *M* é fácil calcular $H(M) = h$, em que *h* tem tamanho fixo;
- Dado *h* é difícil determinar *X* tal que $H(X)=h$;
- Dado *M* é difícil determinar X tal que $H(M)=H(X)$;
- É difícil encontrar *M* e *X* tal que $H(M)=H(X)$.

Alguns exemplos desses algoritmos são: MD2 [34], MD4 [30], MD5 [31], SHA [11], RIPE-MD [32] , HAVAL [33].

A.1.2 Autenticação de mensagens

A autenticação de mensagens, quando estabelecida entre duas entidades que comunicam entre si, é o processo que permite a cada um dos comunicadores verificar que as mensagens recebidas são genuínas e que provêm de determinado interlocutor.

Tipicamente um comunicador age tanto como emissor como receptor embora seja possível agir apenas como emissor ou receptor.

A autenticação de mensagens permite ao receptor de uma mensagem determinar que:

- A mensagem foi enviada pelo alegado emissor;
- O conteúdo da mensagem não foi mudado de forma acidental ou intencional;
- A mensagem foi recebida pela mesma ordem em que foi enviada;
- A mensagem foi entregue ao receptor pretendido.

De outra forma, a autenticação de mensagens permite a um receptor validar as seguintes propriedades da mensagem:

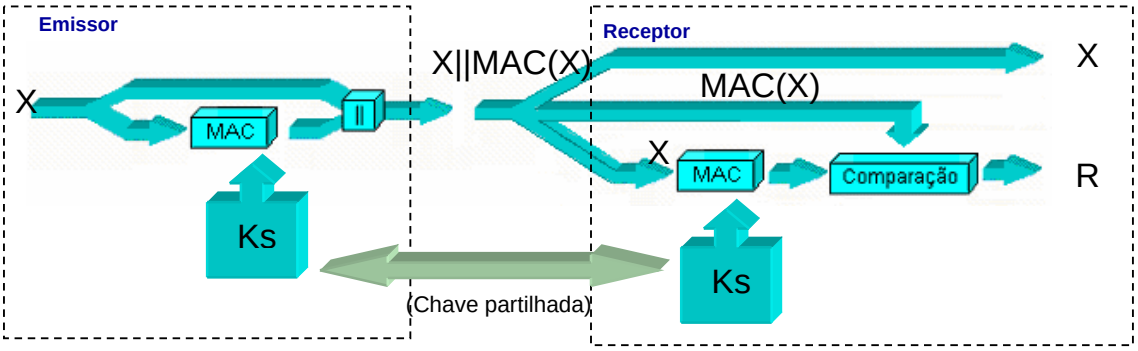
- Origem;
- Conteúdo;
- Ordem;
- Destino.

Embora a autenticação de mensagens permita ao receptor verificar que as mensagens são genuínas, nem sempre permite que as propriedades anteriores sejam provadas ou verificadas por uma terceira entidade. Se o emissor e o receptor partilharem a mesma informação secreta, o emissor pode mais tarde afirmar que o receptor forjou a mensagem.

Contudo uma aproximação que use assinaturas digitais permite ao receptor provar a uma terceira entidade que a mensagem é genuína e que pertence ao emissor que a enviou. Permite ainda que o emissor não possa repudiar que a mensagem não lhe pertence e que o receptor não forjou a mensagem ou a assinatura.

A.1.2.1 Message Authentication Codes (MAC)

Os algoritmos *Message Authentication Code* (MAC) são uma forma de autenticação de mensagens cujo principio de funcionamento usa criptografia simétrica. Estes algoritmos podem ser usados em situações onde é necessário autenticação de mensagens sem necessidade de privacidade. Possuem as mesmas propriedades que os algoritmos de *hash* mas dependem duma chave secreta. Somente alguém que possui a mesma chave usada na geração do MAC o pode verificar.



|| - Concatenacão
X -Mensagem
R - Resultado da comparação: Verdadeiro ou Falso

Figura 36 : Cálculo e verificação do MAC numa mensagem.

Por exemplo suponhamos que se pretende transferir entre um emissor e um receptor uma mensagem de forma a garantir a sua autenticidade (ver Figura 36):

1. O emissor calcula o MAC da mensagem usando a chave *Ks*;
2. O emissor envia a mensagem e o MAC para o receptor;
3. O receptor calcula o MAC da mensagem recebida usando a mesma chave *Ks*;
4. Se o MAC calculado for idêntico ao MAC recebido na mensagem então a mensagem é autentica.

Qualquer algoritmo de *hash* pode ser transformado num algoritmo de MAC se o valor de *hash* for cifrado com um algoritmo criptográfico simétrico. Qualquer MAC pode ser transformado num algoritmo *one way hash* tornando a chave de cifra pública.

A forma mais simples de gerar o MAC duma mensagem consiste em cifrá-la com a chave secreta. O texto cifrado é o MAC da mensagem.

$$MAC = E_{Ks}(X) \qquad \textbf{Equação 1-4}$$

Uma segunda forma ainda mais eficiente de gerar o MAC duma mensagem consiste em integrar no próprio algoritmo de *Hash* a chave secreta:

$$MAC = Hash(X, K_s) \qquad \textbf{Equação 1-5}$$

Como terceira alternativa o MAC pode ser calculado cifrando com a chave *Ks* o resultado da função de *Hash*:

$$MAC = E_{Ks}(Hash(X)) \qquad \textbf{Equação 1-6}$$

Como exemplos de algoritmos de MAC podemos destacar: *Message Authentication Algorithm* (MAA) [12], RIPE-MAC [32], IBC-Hash [32].

A.1.2.2 Assinatura Digital

A assinatura digital é um mecanismo que permite transpor para os sistemas e documentos informáticos as propriedades que a assinatura manuscrita possui:

- **Autenticidade** - A assinatura dum documento convence o receptor que o emissor o assinou deliberadamente;
- **Não forjamento** – A assinatura é a prova de que o assinante, e mais ninguém, deliberadamente o assinou;
- **Não reutilização** – A assinatura faz parte do documento, a qual não pode ser removida para ser colocada noutro documento;
- **Integridade do documento** – Depois do documento assinado o documento não pode ser alterado;

- **Não repudiação** – Depois dum documento assinado o assinante não pode mais tarde alegar que não o assinou porque só ele poderia produzir essa assinatura.

Foram desenvolvidos protocolos de assinatura tanto para o sistema de criptografia simétrica como para o sistema de criptografia assimétrica.

A.1.2.3 Assinatura Digital usando Criptografia Simétrica

No caso dos sistemas de criptografia simétrica os protocolos para assinatura envolvem três entidades: o emissor, o receptor e um árbitro. Tanto o emissor como o receptor confiam no árbitro e este partilha uma chave secreta com o emissor, *KsA*, e outra com o receptor *KsB*.

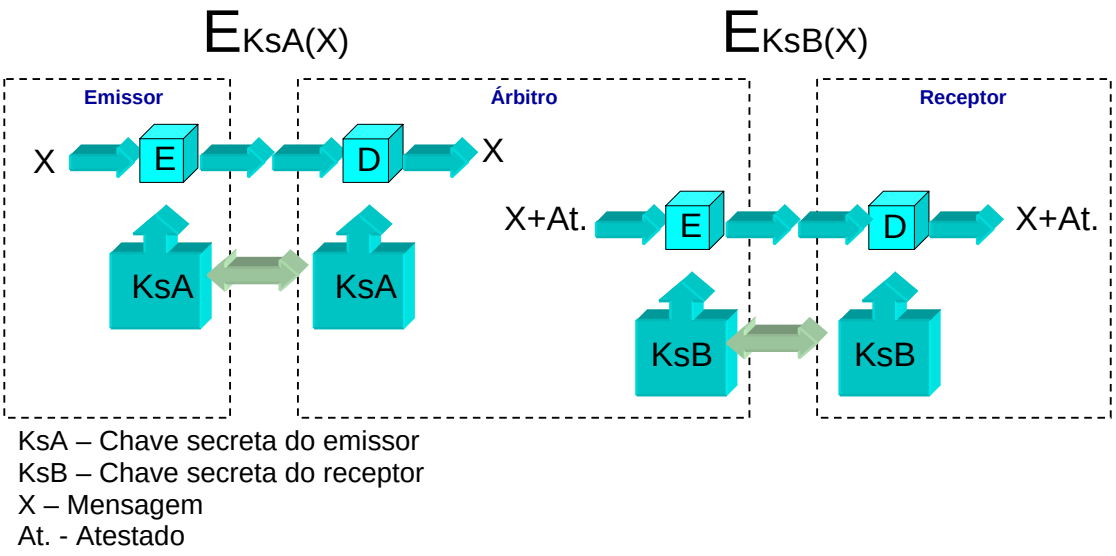


Figura 37 : Assinatura digital num sistema de criptografia simétrica.

Um exemplo de protocolo com árbitro funciona da seguinte forma (ver Figura 37):

1. Quando o emissor quer enviar um documento assinado para o receptor, cifra o documento usando a chave *KsA* e envia-a para o árbitro;

2. O árbitro decifra o documento com a chave *KsA*;

3. O árbitro gera um atestado e cifra o documento, juntamente com a informação de que recebeu a mensagem do emissor, usando a chave *KsB*;

4. O árbitro envia o conjunto assinado para o receptor.

5. O receptor recebe a mensagem e decifra-a com a chave *KsB*. Agora o receptor possui a mensagem enviada pelo emissor e a informação elaborada pelo árbitro que confirma a origem da mensagem.

A.1.2.4 Assinatura Digital com Criptografia Assimétrica

Existem algoritmos de criptografia assimétrica que podem ser usados para assinar mensagens.

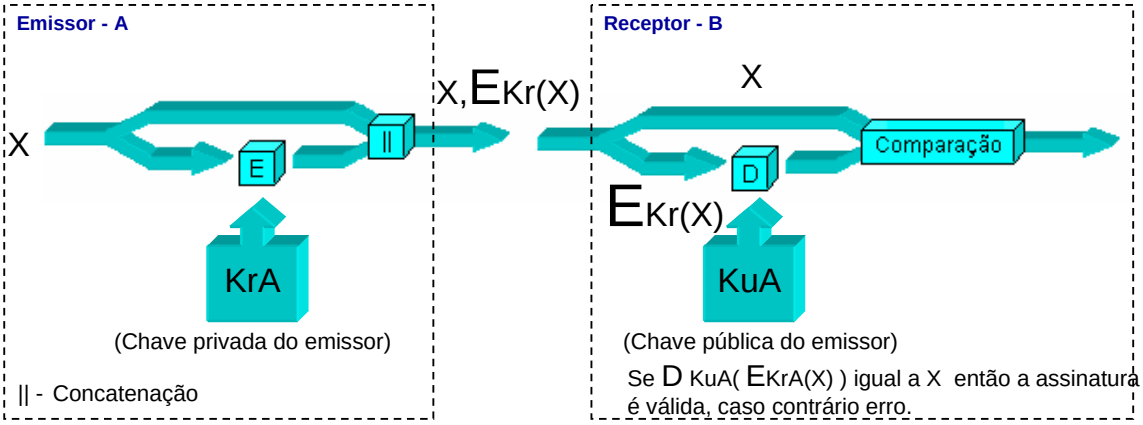


Figura 38 : Sistema de criptografia assimétrica para gerar e verificar uma assinatura digital.

Nesse caso, o protocolo funciona da seguinte forma (ver Figura 38):

1. O emissor cifra a mensagem com a sua chave privada;

2. Os dados são enviados para o receptor;

3. Os dados recebidos são decifrados usando a chave pública do emissor e por consequência prova a origem dos dados, pois só o emissor pôde cifrar os dados por deter a correspondente chave privada.

Inserindo alguma informação em todas as mensagens (tal como a identificação do emissor, identificação do receptor e o número de sequência da mensagem), as mensagens verificam a propriedade de não reutilização.

Contudo, porque os dados estão disponíveis a todos os que possuírem a chave pública de decifra do emissor, não existe privacidade. Se for o caso de que a cifra seguida de decifra e a decifra seguida de cifra, produz o texto em claro original, isto é:

$$D_{Ku}(E_{Kr}(X)) = E_{Kr}(D_{Ku}(X)) = X; \quad \text{para todo o X} \qquad \textbf{Equação 1-7}$$

então o algoritmo baseado em chave pública pode ser usado para ambos, comunicação privada e assinatura digital.

A mensagem é assinada pelo facto de ser cifrada usando a chave privada do emissor A, *KrA*, a privacidade é obtida por cifrar o resultado com a chave pública do receptor B, *KuB*, (ver Figura 39).

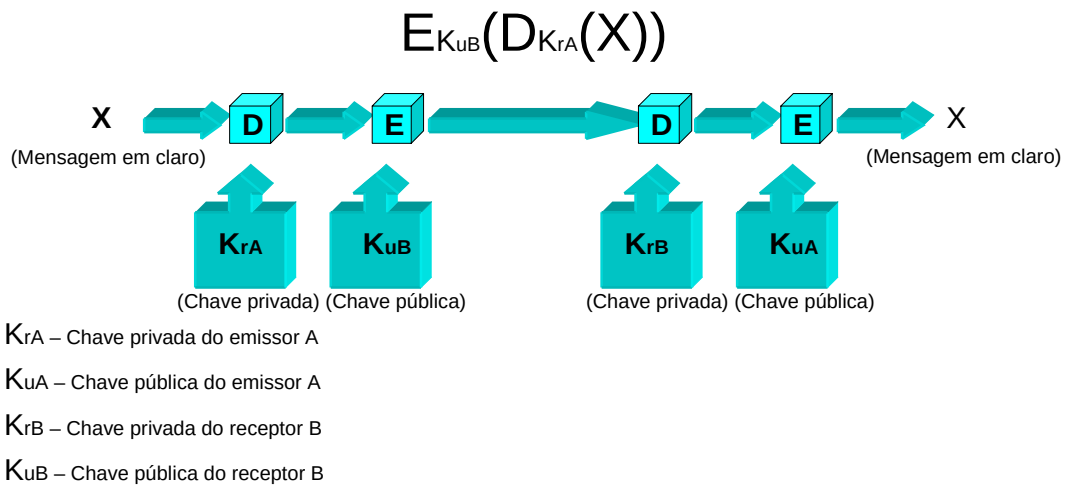
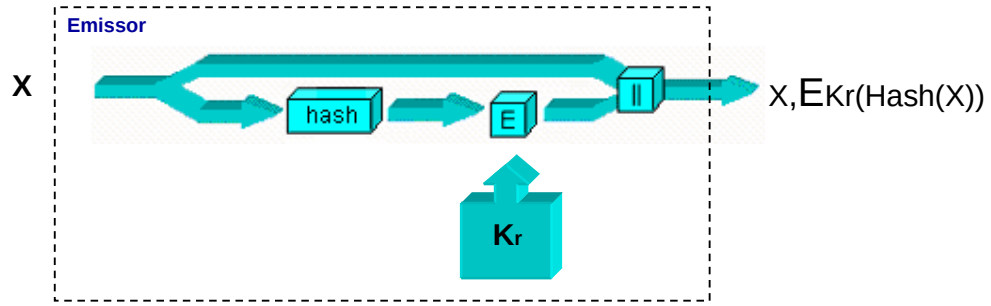


Figura 39 : Sistema criptográfico usado para garantir confidencialidade e assinatura digital.

Este protocolo em comparação com o protocolo de assinatura de criptografia simétrica possui a vantagem de dispensar a terceira entidade, o árbitro.

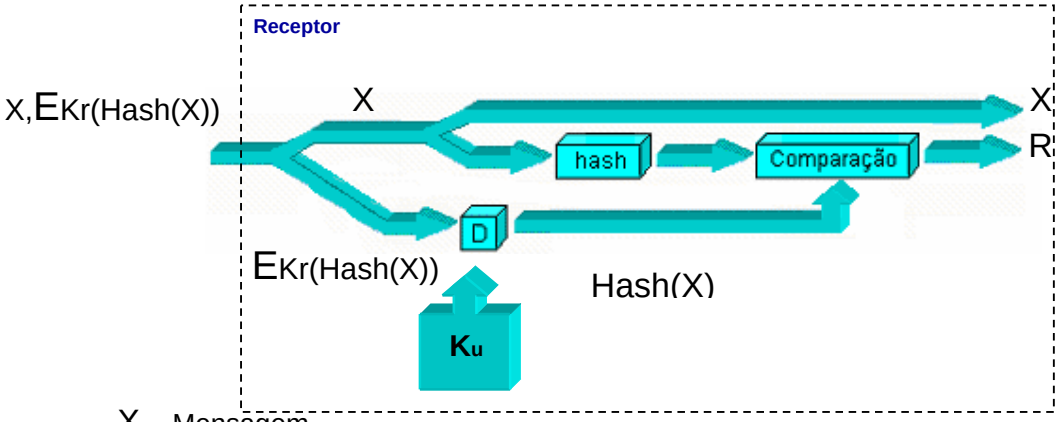
Nas implementações práticas, os algoritmos de chave pública são muitas vezes ineficientes para assinar documentos muito longos. Para poupar tempo, os protocolos de assinatura digital são muitas vezes implementados com funções de *hash*. Em vez de se assinar o documento todo, assina-se o *hash* do documento que é muitas vezes menor do que o tamanho do documento. Qualquer alteração na mensagem resulta numa alteração do resumo da mesma com alta probabilidade.



X – Mensagem

Kr – Chave privada do emissor

Figura 40 : Geração da assinatura com hash.



X – Mensagem

R – Resultado da comparação: Assinatura Verdadeira ou Falsa

Ku – Chave pública do emissor

Figura 41 : Verificação da assinatura com hash.

A Figura 40 e a Figura 41 ilustram a geração e verificação da assinatura digital usando um algoritmo de *hash*.

A.1.3 Infra-estrutura de Segurança

Num ambiente transaccional onde existe troca e distribuição de informação é necessário a existência duma cadeia de confiança para que este possa ser considerado seguro. É necessário que todos os intervenientes no processo possam ser autenticados entre si. Há também a necessidade de se garantir que se detecta qualquer alteração efectuada à informação ou às mensagens trocadas entre os diversos interlocutores.

Em termos práticos, uma infra-estrutura de segurança gere relações e estabelece um determinado nível de confiança numa rede de informação.

Todas as infra-estruturas operam, são administradas, geridas e desenhadas de acordo com um determinado modelo de negócio que define a política de segurança a elas associada. É importante frisar que uma infra-estrutura de segurança não se limita a uma tecnologia, software ou produto, mas estende-se pelas regras e ao modo com essa tecnologia, software ou produto é gerida, administrada e usada. Assim, as infra-estruturas de segurança são específicas em primeiro em lugar função do modo de operação do negócio e em segundo lugar em função da sua arquitectura técnica.

A.1.3.1 Gestão de Chaves e Certificados Digitais

Nos sistemas criptográficos tradicionais, a gestão de chaves era quase restrita ao estabelecimento e manutenção da partilha de chaves secretas. Com o aumento da utilização de esquemas de criptografia assimétrica a natureza da gestão de chaves mudou. Nos sistemas de criptografia assimétrica as chaves existem aos pares, a chave pública, que pode ser amplamente disseminada e a chave privada que deve ser mantida em segredo pelo seu proprietário. O problema relacionado com a gestão de chaves tem a haver como fazer a distribuição das chaves públicas de forma fiável a todas as entidades que delas necessitam. Mais especificamente, embora não seja necessário manter confidencialidade sobre as chaves públicas, para que essa chave seja útil ao seu utilizador tem que existir a certeza de que pertence realmente ao seu legitimo proprietário. Este problema tem sido resolvido com base na utilização de certificados digitais.

Os certificados digitais são usados para impedir tentativas de substituição duma chave por outra, permitindo a alguém usurpar a identidade. Um certificado digital é uma estrutura de dados que associa de forma fiável uma chave pública ao seu titular garantindo a sua autenticidade.

Os certificados digitais permitem a troca segura de chaves públicas em redes não seguras. Quando esta estrutura é assinada por alguém de confiança passa a ser fiável para alguém que use essa estrutura mesmo que não se conheça o proprietário dessa estrutura.

Entre os certificados digitais com maior divulgação encontram-se:

- **Certificado *"Privacy Enhanced Mail"* (PEM)**– Este certificado é o standard adoptado pelo *Internet Architecture Board* (IAB) para disponibilizar correio electrónico seguro através da Internet. Foi inicialmente desenhado pelo *Internet Research Task Force* (IRTF) *Privacy and Security Research Group* (PSRG), e depois entregue ao grupo de trabalho PEM do *Internet Engineering Task Force* (IETF). Os protocolos do PEM disponibilizam cifra, autenticação, integridade das mensagens e gestão de chaves. Os protocolos foram modificados e melhorados, e a versão final está descrita numa série de documentos RFC [23][24][25][26]. A infra-estrutura de gestão de chaves estabelece uma única raiz para todas as certificações na Internet. A *Internet Policy Registration Authority* (IPRA) estabelece a política global para o registo de utilizadores e organizações. Por baixo da raiz IPRA encontram-se as *Policy Certification Authorities* (PCAs), e cada uma das quais define e publica as suas políticas para o registo dos utilizadores e organizações. Cada PCA é certificada pela IPRA. Por baixo das PCAs, as *Certification Authority* (CA) certificam os utilizadores e entidades organizacionais subordinadas;

- **Certificado *"Message Security Protocol"* (MSP)** – Este certificado é o equivalente militar do certificado PEM. Foi desenvolvido pela NSA e é compatível com o standard X.400 para segurança no correio electrónico;

- **Certificado *"Pretty Good Privacy"* (PGP)** – O PGP é um programa originalmente desenvolvido por Philip Zimmermann [27] para transferência segura de *mail*. Na sua abordagem para a gestão das chaves, não existe CA. Em vez disso suporta uma teia de confiança. Todos os utilizadores geram e distribuem a sua chave pública. Cada utilizador assina a chave pública doutros utilizadores criando uma rede de utilizadores PGP. Cada utilizador possui uma colecção de chaves públicas assinadas num ficheiro designado por *Public Key Ring*. Cada utilizador em particular atribui um grau de confiança a cada chave desse ficheiro. Quanto mais alto for esse parâmetro mais merecedora de confiança é a chave;

- **Certificado X.509** – Este certificado faz parte duma recomendação da organização ISO e, tendo sido o certificado mais usado, é tratado com mais detalhe na secção que se segue.

A.1.3.1.1 Certificado X.509

O organização ISO recomendou a utilização de criptografia de chave pública para os esquemas de autenticação conhecido por standard X.509. Este conjunto de protocolos proporcionam autenticação através das diversas plataformas. Embora não seja especificado nenhum algoritmo criptográfico em particular, quer para segurança quer para autenticação, as especificações recomendam a utilização do RSA [9].

A parte considerada mais importante deste standard é a estrutura do certificado de chave pública. Cada utilizador possui um nome distinto atribuído pela autoridade de certificação. Um certificado contém esse nome e a chave pública do titular. Dos diversos campos que compõem essa estrutura fazem parte:

- **Versão** – Identifica o formato do certificado;
- **Número de série** – Identificador único para cada certificado da CA;
- **Algoritmo** – Indica os parâmetros e algoritmo de cifra usados;
- **Período de validade** – O certificado é válido entre as duas datas que compõem este período;
- **Titular** – Identifica o titular do certificado;
- **Chave Pública** – A chave pública do titular do certificado;
- **Informação da Chave pública** – Junto com a chave pública do titular incluem-se o algoritmo e os parâmetros necessários;
- **Assinatura da CA** – Este último campo é a assinatura da CA.

A.1.3.1.2 Protocolo de Autenticação

Quando um emissor *A* pretende comunicar com um receptor *B*, em primeiro lugar, o emissor *A* obtém o certificado do receptor *B* duma base de dados. Depois, o emissor *A*

verifica a autenticidade do certificado, ficando com a certeza de que a chave pública *KuB* desse certificado pertence a *B*. Desta forma, *A* pode enviar uma mensagem cifrada com a chave *KuB* que só *B* poderá decifrar. Paralelamente, se *A* assinar essa mensagem, *B* pode obter o certificado de *A* e verificar que a mensagem foi originária de *A*.

Bibliografia

[1] K. Bohle, M. Rader, U. Riehm, *"Electronic Payment Systems in European Countries, Country Synthesis Report"*, Istitut fur Technikfolgenabschatzung und Systemankyse, 1999

[2] American National Institute, *"Proposed American National Standard X4.16, Magnetic Stripe Encoding for Financial Transaction Cards"*, 1980

[3] F. Halsall, *"Data Communications, Computers, Networks and Open Systems"*, Addison-Wesley Third Edition, 1992

[4] Ç. K. Koç, D. Naccache, C. Paar, *"Cryptographic Hardware and Embedded Systems – CHES"*, Springer, 2001

[5] B. Schneier, *"Applied Cryptography"*, Wiley Second Edition, 1996

[6] U. Black, *"X.25 and Related Protocols"*, IEEE Computer Society Press, 1991

[7] RSA Laboratories, *"Frequently Asked Questions About Today's Cryptography"*, RSA Security Inc., 2000

[8] U.S Department of Commerce, *"FIPS PUB 180-1 Secure Hash Standard"*, 1995

[9] RSA Laboratories, *"PKCS#1: RSA Encryption Standard. Version 2.1"* , 2002

[10] RSA Laboratories, *"PKCS#7:Cryptographic Message Syntax Standard. Version 1.5"*, 1993

[11] National Institute of Standards and Technology, *"FIPS PUB 180-1 Secure Hash Standard"*, U.S. Government Printing Office, 1995

[12] International Standard, *"ISO/IEC 9797 Information technology - Security techniques - Message Authentication Codes (MACs)"*, 1999

[13] International Standard, *"ISO/IEC 9807 Banking and related financial services - Requirements for message authentication (retail)"*, 1991

[14] American National Standard, *"ANSI X9.8 American National Standard for Pin Management and Security"*, 1982

[15] American National Standard for Financial Services, *"ANSI X9.31 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)"*, 1998

[16] Intel, *"Intel Hexadecimal Object File, Format Specification Revision A"*, Intel Co, 1988

[17] International Standard, *"ISO 8583, Financial transaction card originated messages – Interchange message specification", 2003*

[18] International Standard, *"ISO 9564 Personal Identification Number (PIN) management and security - Part 1 and 2"*, 2002

[19] International Standard, *"ISO 8731 Approved algorithms for message authentication - Part 1: DEA"*, 1987

[20] International Standard, *"ISO 8731 Approved algorithms for message authentication - Part 2: Message authenticator algorithm"*, 1992

[21] International Standard, *"ISO 11568 Key management (retail) – Part 1, 2 and 3"*, 1994

[22] International Standard, *"ISO 15668 Banking Secure File Transfer (retail)"*, 1997

[23] J.Linn, *"Privacy Enhanced for Internet Electronic Mail: Part I – Message Encipherment and Authentication Procedures"*, RFC 1421, 1993

[24] S.T. Kent, *"Privacy Enhanced for Internet Electronic Mail: Part II – Certificate Based Key Management"*, RFC 1422, 1993

[25] D.Balenson, *"Privacy Enhanced for Internet Electronic Mail: Part III – Algoritms, Modes, and Identifiers"*, RFC 1423, 1993

[26] B.S. Kalinski, *"Privacy Enhanced for Internet Electronic Mail: Part IV - Key Certificates and Related Services"*, RFC 1424, 1993

[27] P.R. Zimmermann, *"PGP Official PGP User's Guide"*, Boston: MIT Press, 1995

[28] Dhir, Amit, *"Voice-Data Convergence – Voice Over IP"*, XILINX, 2001

[29] ETSI, *"GSM Technical Specification"*, European Telecommunication Standards Institute, 1995

[30] R.L. Rivest, *"The MD4 Message Digest Algorithm"*, RFC 1320, 1992

[31] R.L. Rivest, *"The MD5 Message Digest Algorithm"*, RFC 1321, 1992

[32] Research and Development in Advanced Communication Technologies in Europe, *"RIPE Integrity Primitives: Final Report of RACE Integrity Primitives Evaluation (R1040)"*, RACE, 1992

[33] Y. Zheng, J. Pieprzyk, J. Seberry, *"HAVAL-A One-Way Hashing Algorithm with Variable Length of Output, Advances in Crytology – AUSCRYPT '92 Proceeding"*, Springer-Verlag, 1993

[34] B.S. Kaliski, *"The MD2 Message Digest Algorithm"*, RFC 1319, 1992

[35] EMVCo, *"EMV2000 Integrated Circuit Card Specification for Payment Systems – Book 1 - Application Independent ICC to Terminal Interface Requirements"*, Version 4.0, 2000

[36] EMVCo, *"EMV2000 Integrated Circuit Card Specification for Payment Systems – Book 2 - Security and Key Management"*, Version 4.0, 2000

[37] EMVCo, *"EMV2000 Integrated Circuit Card Specification for Payment Systems – Book 3 – Application Specification"*, Version 4.0, 2000

[38] EMVCo, *"EMV2000 Integrated Circuit Card Specification for Payment Systems – Book 4 – Cardholder, Attendant, and Acquirer Interface Requirements"*, Version 4.0, 2000

[39] EMVCo, *"EMV Issuer Security Guidelines"*, Version 0.5, 2000

[40] ANSI X3.92, *"American National Standards for Data Encryption Algorithm (DEA)"*, American National Standards Institute, 1981

[41] http://www.borland.com

[42] http://www.eskimo.com/~weidai

[43] A. B. Carlson, *"Communication Systems"*, McGrawHill, 1986

[44] J. G. Proakis, *"Digital Communications"*, McGrawHill, 1989

[45] D. V. Hall, *"Microprocessors and Interfacing"*, McGrawHill, 1992

[46] M. J. Mendonça, N. F. Neves, *"Secure Updates on Point of Sale Devices, Proceedings of the First International Conference on E-Business and Telecommunication Networks"*, Volume 2, INSTICC, 2004

[47] M. J. Mendonça, N. F. Neves, *"Actualização Segura e Automática de Aplicações em Terminais de Venda"*, Actas da 7ª Conferência sobre Redes de Computadores, CRC, 2004

Glossário

AID *Application Identifier*

API *Application Program Interface*

ARL *Authority Revocation List*

ATM *Automated Teller Machine* – Caixa Automático

BIN *Bank Identification Number*

CA *Certification Authority* – Autoridade de Certificação

CRL *Certification Revocation List*

EFT *Electronic Founds Transfer* – Transferência electrónica de fundos

EMV Europay Master Card e Visa

IAB *Internet Architecture Board*

IETF *Internet Engineering Task Force*

IPRA *Internet Policy Registration Authority*

IRTF *Internet Research Task Force*

Ku Chave Pública

Kr Chave Privada

MSP *Message Security Protocol*

MTI *Message Type Identifier* – Identificador do Tipo de Mensagem

OSP Operador do Sistema de Pagamentos

PCA *Policy Certification Authority*

PED *Pin Entry Device*

PEM *Privacy Enhanced Mail*

PGP *Pretty Good Privacy*

PIN *Personal Identification Number*

PINBLOCK PIN Cifrado

PKI *Public Key Infrastructure* – Infra Estrutura de Chave Pública

PSRG *Privacy and Security Research Group*

PED *Pin Entry Device*

RA *Registration Authority*

SSP Servidor de Sistema de Pagamento

SDA Servidor de Descarga de Aplicações

SSC Servidor do Sistema de Certificação

SProd Servidor do Produtor de Aplicações