INFRA-ESTRUTURA DE CHAVE PÚBLICA DO MINISTÉRIO DA JUSTIÇA

Claudia Isabel P. M. Carvalho

DI-FCUL TR–03–27

Setembro 2003

Departamento de Informática
Faculdade de Ciências da Universidade de Lisboa
Campo Grande, 1700 Lisboa
Portugal

Technical reports are available at http://www.di.fc.ul.pt/tech-reports. The files are stored in PDF, with the report number as filename. Alternatively, reports are available by post from the above address

INFRA-ESTRUTURA DE CHAVE PÚBLICA DO MINISTÉRIO DA JUSTIÇA

Claudia Isabel Polainas Mateus Carvalho

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:

André Ventura da Cruz Marnôto Zúquete

Luis Manuel Carriço

Dezembro de 2002

Resumo

Ao longo dos últimos anos, as infra-estruturas de chave pública ("*Public Key Infrastructure*" (PKI)) têm merecido um interesse crescente à medida que as organizações e utilizadores se vão apercebendo das debilidades que os sistemas informáticos apresentam em termos de segurança. De uma forma sintética, esta tecnologia permite a emissão e distribuição de certificados digitais, elementos que suportam, por exemplo, a existência da figura da assinatura digital, e a construção de mecanismos de autenticação e de protocolos de comunicação segura. No seu conjunto, a infra-estrutura mais os serviços derivados, asseguram que as transacções electrónicas observam propriedades como a integridade, a confidencialidade, o não repúdio e a autenticidade.

Embora os fundamentos teóricos da criptografia assimétrica (ou de chave pública) tenham mais de vinte anos, o uso da tecnologia PKI é muito recente e em parte bastante desconhecido. Esta tese pretende demonstrar através do estudo de um cenário específico, o Ministério da Justiça, como é que uma PKI pode ser desenvolvida e integrada numa estrutura informática existente. O Ministério da Justiça é composto por um número elevado de organismos, incluindo a Polícia Judiciária, os Serviços Prisionais, e os Tribunais, que lidam com aspectos do foro legal, e que resultam na troca de informação sensível entre eles e com os Cidadãos. Torna-se assim imperativo que o manuseamento desta informação seja efectuado de uma forma segura, caso contrário, poderão surgir situações em que investigações são comprometidas ou em que decisões judiciais são alteradas enquanto em trânsito entre organismos.

Esta tese descreve os diversos aspectos que se encontram relacionados com o desenvolvimento da PKI do Ministério da Justiça. Em particular, faz um levantamento das necessidades existentes, discute as várias opções que se podem tomar em relação aos elementos que poderão integrar a infra-estrutura, e por fim apresenta uma implementação. Um protótipo da infra-estrutura encontra-se neste momento em fase de teste, tendo já sido utilizado em algumas ocasiões, nomeadamente, durante as eleições presidenciais de 2001 e as eleições legislativas de 2002.

PALAVRAS-CHAVE: segurança, infra-estrutura de chave pública (PKI), certificados digitais, assinatura digital, criptografia assimétrica.

Abstract

During the last years, Public Key Infrastructures (PKI) have deserved an increasing interest by the organizations and users as they realise that computer systems can suffer from security related problems. This technology allows the creation and dissemination of digital certificates, which are essential to support digital signature algorithms, and the construction of authentication mechanisms and secure communication protocols. Together, this infrastructure plus its derived services, ensure that electronic transactions have properties such as integrity, confidentiality, non-repudiation and authenticity.

Even though the theoretical foundations of asymmetric (or public key) cryptography have more than twenty years, the use PKI technology is reasonably new and many aspects of its implementation are still unknown to most people. This thesis demonstrates through a case study, the Ministry of Justice, how a PKI can be developed and integrated into an existing computational system. The Ministry of Justice has jurisdiction over a large number of organizations, including the Police, Courts, and Prisons, which have to deal and exchange sensitive information. Therefore, it is of great importance that this information is handled in a secure way, otherwise, in some cases police investigations might be compromised or judicial decisions might be tampered with while being sent from one organization to another.

This thesis describes all aspects involved in the development of the PKI of the Ministry of Justice. It begins by presenting the existing needs in terms of security, then it discusses several options available in what concerns the components of the infrastructure, and finally, it describes the current implementation. At the present time, the prototype of the infrastructure is still in the test phase, however, it has already been used in some occasions, for example, during the Presidential elections of 2001 and the Legislative elections of 2002.

KEY-WORDS: security, public key infrastructure (PKI), digital certificates, digital signature, asymmetric cryptography.

Agradecimentos

Quero agradecer ao meu Orientador, o Professor Nuno Ferreira Neves, toda a paciência e perseverança com que me acompanhou e todo o empenho e profissionalismo que demonstrou na orientação da minha dissertação. Nunca deixou de me apoiar e soube sempre como conduzir o meu trabalho de forma a este conseguir transparecer de uma forma clara e tecnicamente correcta, todas as fases, opções e dificuldades pelas quais o projecto desenvolvido no Instituto das Tecnologias de Informação na Justiça (ITIJ), passou.

A segunda pessoa a quem quero agradecer é ao Fernando, o meu namorado. Não se cansou de me estabelecer metas a atingir e não me deixava largar a tese, enquanto não as cumprisse. Por todos os sacrifícios que fez por mim, especialmente este ano, que abdicou das suas férias e de muitos passeios para estar por perto a apoiar-me, o meu muito obrigada.

De seguida quero agradecer ao Eng. Carlos Gonçalves, Vogal do Conselho Directivo do ITIJ, o ter-me sugerido e proporcionado um tema para dissertação de uma tese. Demonstrou-se uma mais-valia para a minha dissertação o facto de poder verificar e testar na prática aquilo que me era apresentado na teoria.

Por último, mas não com menos importância, agradeço aos amigos que eu conheci no ITIJ, a coragem que me deram quando me sentiam a vacilar. Um especial agradecimento à Marta Jacinto pelas dicas e opiniões que me ia dando à medida que também ela ia avançando na sua dissertação, uns passitos mais à frente, sabendo advertir-me do que me aguardaria em cada fase.

Índice Geral

Índice de Figuras

Capítulo 1

Introdução

"O sistema de Justiça deve ser o sustentáculo dos direitos de cidadania e não um obstáculo ao exercício desses direitos.
Sem celeridade, eficácia, agilidade e efectividade não pode haver uma Justiça verdadeira: uma Justiça tardia nunca é Justiça."

(*in Programa do XV Governo Constitucional para a área da Justiça*)

O Ministério da Justiça (MJ) é composto por um complexo conjunto de organismos, que inclui Conservatórias, Notários, Tribunais, Polícia Judiciária, Instituto de Reinserção Social, Direcção Geral dos Serviços Prisionais e Centro de Estudos Judiciários. Estes, têm normas e funções distintas que por vezes se interligam em casos processuais, requerendo uma resposta rápida de todos os organismos envolvidos, sob pena de causar atrasos na recolha dos dados necessários a uma situação específica.

Começam, desde logo, as dificuldades na recolha dos dados em arquivos de grandes dimensões, de anos, por vezes sem uma coerência lógica no arquivo das pastas, lutando com a falta de espaço e com as condições desse mesmo espaço.

A burocracia também entra em acção: para requerer determinado documento é necessário preencher mais dois ou três, aumentando cada vez mais o número de papel em arquivo. E com a agravante de, em todo este manuseamento de papeis, poder haver uma falha humana: um documento arrumado numa pasta incorrecta, dificultando ou impossibilitando a sua procura mais tarde, um número de processo incorrectamente preenchido, separando esse documento dos restantes a si ligados, etc..

Pode-se imaginar o que acontece se estas situações surgirem quando se pretender interligar informações dos vários organismos.

Por algum motivo existem processos a arrastarem-se há anos.

Com o aparecimento da informática, cedo se verificou que esta poderia solucionar muitos dos problemas existentes nos organismos do MJ. Assim, em 1972 com o decreto-lei nº 523/72 de 19 de Dezembro, foi criado o Centro de Informática do MJ com funções de concepção, estudo e tratamento informático das matérias atribuídas aos vários departamentos centrais dependentes do Ministério. Demonstrou promover uma grande expansão e desenvolvimento a nível interno, mas, com as inúmeras áreas que estavam a nascer, depressa se tornou necessário ajustar a sua estrutura orgânica, destacando-se a necessidade de aumento de equipamento e pessoal especializado. Impunha-se assim a caracterização legal do Centro de Informática a nível de Direcção-Geral. Tal veio a acontecer em 1983 em que, com o decreto-lei nº 111/83 de 21 de Março, foi criada a Direcção Geral dos Serviços Informáticos (DGSI), para ser "[...] um serviço de concepção e apoio técnico que tem por fim promover o estudo e o tratamento automático da informação correspondente às atribuições do MJ e prestar a cooperação necessária à sua utilização." (artigo 1º do referido D.L.). Foram-lhe atribuídas como funções, colocar as tecnologias da informação ao serviço da justiça, automatizando muitas das tarefas realizadas nos vários organismos, procedendo à elaboração e manutenção de bases de dados, que vieram a facilitar o manuseamento dos dados e aumentaram a sua fiabilidade (recorde-se a importante base de dados de identificação civil - Bilhetes de Identidade), automatizando a contagem dos votos das eleições, desenvolvendo e adaptando suportes lógicos às necessidades da Administração Pública, entre outras.

Mais tarde, com o decreto-lei nº 146/2000, de 18 de Julho, foi aprovada a Lei Orgânica do MJ onde se procedeu à regulamentação dos termos de organização e funcionamento do Instituto das Tecnologias de Informação na Justiça (ITIJ). Esta entidade apresentou-se como sendo uma reformulação orgânica e funcional da acima referida DGSI, a quem foram atribuídas competências de estudo, concepção e emissão de normas técnicas e, entre outras, a gestão integrada da rede de informação e comunicações da justiça, garantindo a sua segurança e operacionalidade.

Com o aparecimento da Internet, abriram-se as portas para a ligação em rede de todo o MJ, permitindo a interligação de todos os serviços, o acesso directo às várias bases de dados e a eliminação do isolamento em que se encontravam os vários organismos, tornando-os parte de um todo.

O Governo, consciente da ineficácia do sistema de justiça em responder ao crescimento exponencial das solicitações da sociedade, sistema este que se encontra preso a regras,

procedimentos e estruturas pouco flexíveis que provocam uma acumulação de dificuldades e atrasos, encontra-se a proceder a uma reforma. Definiu, para tal, uma política de modernização da Justiça, com o objectivo de torná-la mais acessível aos cidadãos, mais adequada às necessidades das empresas, mais célere e eficaz.

Pretende fazer muitas alterações a nível sectorial, institucional e processual, mas uma das mais importantes e que importa referir nesta dissertação, é a de pretender apostar na informatização como forma de obtenção de ganhos de produtividade.

Poder-se-ão referir como objectivos nesta área, os seguintes itens [1]:

- Informatização dos tribunais, conservatórias e cartórios notariais e ligação dos primeiros à rede - Presentemente está-se a terminar a ligação dos tribunais aos vários nós da rede, faltando depois instalar os vários serviços básicos de rede, como Internet, Correio Electrónico, Nomes de Domínios, Serviços WWW e Intranet nos vários postos de trabalho. As conservatórias e cartórios ainda se encontram na fase de ligação à rede [2];

- Informatização do sector dos registos e início do processo de microfilmagem dos registos ainda existentes em livros - Denota-se uma tentativa de eliminação dos arquivos em papel, passando tudo para suporte electrónico;

- Aproveitamento das possibilidades oferecidas pela Internet, adoptando medidas que facilitem o acesso dos cidadãos a informação actualizada dos principais actos legislativos em vigor - Existe o "*site*" do MJ (http://www.mj.gov.pt) que permite ao cidadão, para além do acesso à informação dispersa pelos vários Organismos do Ministério, expressar as suas opiniões e dúvidas relativamente a vários assuntos, originando uma interacção entre a Instituição e o Cidadão, e obter serviços on-line, como emissão de Certificados de Registo Criminal, Civil, Comercial, Predial ou Admissibilidade de Firma, que anteriormente o forçavam a deslocar-se aos serviços do Ministério;

- Utilização da Intranet para acesso às bases de dados de jurisprudência dos Tribunais Superiores e pareceres da Procuradoria Geral da República, acesso às bases de dados centrais do Ministério e à Rede Judiciária Europeia para emissão das cartas rogatórias;

- Qualificação e formação contínua dos funcionários na área das novas tecnologias e redefinição das exigências mínimas para preenchimento de lugares abertos nos quadros dos tribunais - Esta medida apresenta-se crucial para um bom aproveitamento dos benefícios que advêm do processo de informatização que todos os serviços estão a sofrer. Não basta apenas construir uma rede e colocar os computadores nos locais de trabalho. Há que dar formação aos funcionários e exigir que os entretanto admitidos tenham conhecimentos mínimos, a nível de utilizador.

Assim, entraram em vigor em 1 de Janeiro de 2001, um conjunto de medidas simplificadoras do processo civil e do processo penal, com o intuito de consagrar o direito a uma justiça acessível aos cidadãos e exercida em tempo útil.

Para este trabalho em concreto, importa focar, de entre outras, a possibilidade de, desde Janeiro de 2001 e com obrigatoriedade a partir de Janeiro de 2003, se apresentarem peças processuais como articulados, alegações, requerimentos e respostas a estes, por telecópia, disquete, correio electrónico ou outro suporte digital, expressamente referido no nº 4 do artigo 143º, no artigo 150º e no nº 6 do artigo 152º, do Código do Processo Civil [3].

Com a introdução do correio electrónico para transmissão dos articulados, alegações e demais documentos legais, obtém-se uma grande comodidade, economia e, sobretudo, uma notável celeridade na prática de actos processuais, por não haver sujeição aos horários das secretarias ou dos serviços postais. Dado o teor dos documentos a enviar por correio, é essencial a utilização de uma tecnologia que permita proteger esses dados e quem os enviou pois há o receio de essa informação ser visualizada ou mesmo alterada de forma maliciosa quando em trânsito pela rede. Urge encontrar uma tecnologia que permita eliminar este desconforto.

É pois, no âmbito da segurança das comunicações, especialmente as de carácter sensível, na rede do MJ, que surge a necessidade de implementação de uma estrutura que permita o envio de correio electrónico de uma forma segura em que se possa comprovar, com toda a certeza, que determinada mensagem enviada, não foi alterada aquando da transmissão (integridade), nem foi lida por ninguém (confidencialidade) e que de facto foi enviada por quem disse tê-la enviado (autenticidade). De notar a importância deste projecto para a elaboração e troca electrónica de peças processuais entre magistrados e entre magistrados e advogados.

Para obtenção daquelas propriedades, há que recorrer a uma tecnologia que permita esconder de terceiros o conteúdo das mensagens e impedir a alteração das mesmas. Tal é conseguido através da utilização da criptografia combinada com um método de chaves de cifra/decifra assimétricas como se abordará adiante no Capítulo 2.

Com a implementação de uma Infra-estrutura de Chaves Públicas ("*Public Key Infrastructure*" (PKI)), fornece-se uma infra-estrutura básica para a gestão de chaves assimétricas que poderão vir a ser utilizadas de inúmeras formas, quer por aplicações quer por serviços, utilizando protocolos como o "*Secure Multipropose Internet Mail Extensions*" (S/MIME) para correio seguro, o "*Secure Electronic Transaction*" (SET) para transacções seguras e o "*Secure Sockets Layer/Transport Layer Security*" (SSL/TLS) para comunicações seguras.

Assim, para além da possibilidade de se enviar mensagens de correio electrónico ("*e-mails*") assinados e/ou cifrados, principal necessidade do Ministério, a criptografia assimétrica com o apoio desta infra-estrutura, permitirá identificar o titular da chave privada para efeitos de acesso a máquinas e serviços, bem como a locais físicos, de uma forma fiável.

Com esta infra-estrutura montada no ITIJ, o MJ ficará dotado de uma Entidade Certificadora própria para emissão dos seus certificados digitais. Além disso, este empreendimento demonstra-se importante para uma compreensão *in situ*, daquilo que o ITIJ, como Entidade Credenciadora Nacional (atribuição estipulada para este Instituto pela alínea i) do artigo 18 do já referido decreto-lei 146/2000 de 18 de Julho), deverá definir como regras de segurança física e lógica, políticas de acessos e de salvaguardas ("*backups*") e características dos componentes da infra-estrutura.

1.1 Enquadramento

Uma vez que a infra-estrutura tem como objectivo criar segurança nas comunicações, este seria um serviço a desenvolver no departamento do ITIJ afecto à área de redes e comunicações (Departamento de Infra-estruturas Redes e Comunicações[1]). Tal, justifica-se com o facto de a PKI ir recair numa estrutura de rede já montada ("*firewalls*", rede interna/rede externa, acessos/permissões a máquinas/serviços), requerendo ser gerida por alguém da área com capacidades para ajustar a estrutura a realizar à realidade existente e efectuar nesta as alterações que se determinem necessárias.

Foi assim que este projecto me foi atribuído, na qualidade de elemento integrante daquele Departamento. Este projecto seria desenvolvido no ITIJ, realizando-se, numa fase inicial, um piloto com os funcionários do ITIJ, sendo posteriormente estendido a todos os organismos do MJ.

Determinou-se que o ITIJ não possuía conhecimentos suficientes que lhe permitissem desenvolver ele próprio esta infra-estrutura, tendo-se de imediato decidido adjudicar este serviço a uma empresa que apresentasse competências para tal.

Seria então função do elemento do ITIJ afecto a este projecto, ou seja eu, antes de mais, realizar uma proposta para apresentar às empresas concorrentes as características que se pretendia que a PKI do Ministério possuísse. Tal, requereria um estudo intensivo de todas as opções existentes ao nível tecnológico e de mercado e um conhecimento profundo da realidade existente no ITIJ e dos objectivos que este pretendia atingir ao desenvolver tal estrutura, por forma a decidir pelas opções correctas, ou seja, as que cumpririam os objectivos.

A segunda tarefa que se avizinhava, seria a leitura das propostas apresentadas por empresas convidadas pelo ITIJ (não foi aberto concurso público). Os factores de apreciação seriam o cumprimento dos requisitos exigidos, sendo o preço o factor de desempate.

---

[1] Unidade funcional de natureza operacional criada pelo decreto-lei nº 103/2001 de 29 de Março que aprovou os Estatutos do ITIJ.

Seleccionada a empresa, as tarefas passariam a ser de gestão e orientação do projecto, realização de dados de teste, verificação do cumprimento de todos os requisitos e elo de ligação entre o ITIJ e a empresa, pedindo a execução de tarefas afectas a outros departamentos, que se apresentassem essenciais para o bom desempenho da PKI.

Também seria da minha responsabilidade, o desenvolvimento das tecnologias que tirassem partido desta infra-estrutura, bem como o esclarecimento do seu funcionamento e utilização.

Competir-me-ia, também, prestar esclarecimentos a dúvidas que surgissem tanto aos funcionários do MJ que viessem a receber documentos assinados digitalmente, como aos advogados que necessitassem de obter os certificados digitais para envio de documentos assinados, bem como apresentar esta tecnologia aos responsáveis pelo desenvolvimento de aplicações, referindo a qualidade que esta possui de permitir acessos seguros àquelas e trocas seguras de informação sensível com outros servidores. Sendo esta uma tecnologia que irá revolucionar as transacções electrónicas, actualmente consideradas inseguras, há uma grande necessidade de a dar a conhecer por forma a diluir os entraves que actualmente se colocam na utilização destas para dados mais sensíveis.

Pretendia também tirar o máximo partido das propriedades de autenticidade, integridade e não repúdio obtidas com os certificados digitais emitidos pela Entidade Certificadora entretanto criada, apoiando o desenvolvimento de serviços que requeressem este tipo de fiabilidade: acesso seguro a servidores Web, a aplicações, "*login*" a máquinas, registo de entradas e controlo de acessos.

Assim, defini, numa primeira fase, que esta infra-estrutura teria como prioridade a troca de correio electrónico seguro entre os magistrados, necessidade há muito sentida por estes, aquando do envio de peças processuais. Seguidamente, estender-se-ia à própria identificação dos funcionários, conseguida com a colocação dos certificados digitais em cartões inteligentes (smart cards) que funcionariam como cartões de identificação. Esta funcionalidade abrangeria o controlo de acessos quer a serviços, quer a locais e o registo de entradas e saídas. Paralelamente, proteger-se-iam documentos e far-se-ia a protecção do próprio posto de trabalho (PC).

Assim que esta infra-estrutura se apresente estável, partir-se-á para o desenvolvimento do serviço de estampilha temporal, serviço este considerado crucial para uma boa garantia da propriedade de não repúdio.

Esta dissertação abordará a parte do desenvolvimento da PKI e as primeiras funcionalidades desenvolvidas e actualmente em funcionamento no ITIJ. As restantes ainda não foram desenvolvidas.

Assim, a dissertação referir-se-á ao serviço de envio de correio electrónico assinado e/ou cifrado, à protecção do posto de trabalho, à assinatura e/ou cifra de ficheiros e ao acesso seguro a serviços Web.

A título informativo, poderei referir que, para assegurar a integridade dos votos transmitidos aquando da contagem dos escrutínios eleitorais e a própria autenticação dos introdutores daqueles, quando das Presidenciais 2001 e das Autárquicas 2002, utilizou-se esta infra-estrutura, para estabelecimento de uma SSL. Também já se estão a fazer os acessos às aplicações por SSL, enumerando, por exemplo, o projecto Atlas, já em funcionamento, em que os elementos dos vários países pertencentes à Rede Judiciária Europeia responsáveis pela actualização das Bases de Dados, acedem, por "*HyperText Transfer Protocol Secure*" (HTTPS), ao servidor Web onde se encontram as páginas "*HyperText Markup Language*" (HTML) da aplicação. Para além do servidor possuir um certificado digital que lhe permite autenticar-se perante aqueles utilizadores, estes também têm um certificado digital que lhes permitirá autenticarem-se perante o servidor garantindo o não repúdio das acções que realizem nas bases de dados.

Actualmente terminaram os testes com o piloto montado no ITIJ e vai-se proceder ao início da produção dos certificados para todo o Ministério, em paralelo com a elaboração da proposta para desenvolvimento da "*Time Stamp Authority*" (TSA). Tais tarefas já não serão contempladas nesta dissertação.

1.2 Contribuição

Pretende-se com esta dissertação, apresentar um cenário específico em que se utiliza uma PKI. Apresentar-se-ão:

- As justificações para a necessidade de desenvolvimento de uma infra-estrutura desta envergadura;
- Os resultados que se pretendem obter com ela;

- A necessidade de adaptação da estrutura à realidade existente, que muitas vezes implica ter de contornar problemas inicialmente não imaginados por se julgarem as normas standard para todos os ambientes;
- Apresentar os vários tipos de opções que se podem tomar na escolha dos vários elementos integrantes da infra-estrutura;
- O porquê das decisões tomadas no caso específico do ITIJ.

A intenção desta tese é servir de guia para as várias fases existentes no desenvolvimento desta infra-estrutura: levantamento das necessidades que se pretendem satisfazer; opções a tomar de acordo com a satisfação dessas necessidades, estudo da viabilidade de ser uma estrutura desenvolvida pelo próprio adquirente, ou se é preferível adjudicar esse serviço a uma empresa; se há interesse em ser-se uma Autoridade de Certificação ("*Certification Authority"* (CA)) Raiz ou se a CA se deve colocar numa hierarquia já existente, poupando alguns inconvenientes de não reconhecimento da estrutura a nível dos "*browsers*".

Dever-se-á, também, efectuar uma análise de quem, na organização, tem necessidade de ser detentor de um certificado digital, havendo sempre o factor financeiro a ter em consideração. Esta é uma infra-estrutura cara que deverá ser bem gerida. Há que determinar como deverá ser efectuado o pedido de emissão de certificado: se pelo titular, se pela organização, se de forma presencial, ou confrontando os dados com alguma base de dados; se a emissão irá ser realizada apenas para o grupo restrito da organização, se será também para os seus afiliados, ou se para toda a gente que o pretenda; se será um serviço oneroso ou gratuito.

Há que avaliar todas as opções que se apresentam para definir a estrutura mais adequada a determinada realidade.

Apresentando este cenário, espera-se que sirva de exemplo e de impulsionador ao desenvolvimento de outras infra-estruturas nacionais, *qui sa*, noutros Ministérios.

Finalmente, de uma maneira geral, pretende-se com esta tese desmistificar esta tecnologia tornando-a fiável por forma a eliminar actuais receios que sufocam o desenvolvimento de áreas que vivem das transacções electrónicas.

1.3 Estrutura da Tese

O resto desta tese encontra-se estruturada da seguinte forma:

No segundo capítulo, são apresentados os vários componentes que integram uma PKI, bem como são abordadas as várias funcionalidades e utilizações de uma infra-estrutura destas, mais particularmente aquilo que é por ela gerado e administrado – os certificados digitais.

No capítulo três, faz-se uma resenha breve do principal em relação à legislação sobre esta matéria tanto em Portugal como na Comunidade Europeia (CE), referindo a tentativa de consolidar e tornar coerentes as regras a seguir a nível da CE, por forma a atingir um consenso e a permitir que as infra-estruturas geradas nesse espaço possam ser compatíveis e reconhecidas entre si. É também neste capítulo que é apresentada a realidade existente ao nível das estruturas que interagirão com a PKI e os objectivos a atingir com o desenvolvimento desta. É proposta uma arquitectura para o MJ justificando as principais opções face ao pretendido e ao já existente.

No quarto capítulo é apresentado o modelo adoptado e inerente personalização, para sua adaptação às especificidades do MJ. Explica-se como se concretizou a tarefa, descrevendo pormenorizadamente o ciclo de funcionamento da infra-estrutura.

No capítulo cinco refere-se a necessidade de execução de determinados serviços adicionais, bem como os problemas que foram surgindo à medida que se avançava no projecto, muitos deles relacionados com incompatibilidades encontradas em componentes que se consideravam standard. São referidas possíveis optimizações que esta poderá sofrer por forma a melhorar o seu desempenho. Descrevem-se, ainda, as aplicações em que esta tecnologia já foi empregue.

Por fim, no sexto capítulo, é analisado o desempenho da infra-estrutura criada, apreciando os resultados obtidos. É também apresentado o prosseguimento futuro deste projecto.

Capítulo 2

Infra-estrutura de Chave Pública

Antes de se fazer uma referência à estrutura desenvolvida no ITIJ, é conveniente fazer uma abordagem, ainda que sucinta, de conceitos e elementos que irão ser referidos ao longo desta dissertação.

A infra-estrutura que se irá utilizar é complexa envolvendo uma série de protocolos e interagindo com muitas áreas a que convém fazer referência. Far-se-á uma abordagem aos vários tipos de criptografia e qual o motivo da sua utilização, terminando na referência àquela que se utiliza numa PKI e porquê. Também se apresentará a figura da assinatura digital, como poderá ser obtida e para quê. Por fim, descrever-se-ão os vários tipos de elementos que compõem uma PKI, bem como os serviços que se disponibilizarão com ela e as tarefas que se executarão. Apresentar-se-ão várias formas de realizar determinada acção para, nos capítulos seguintes, se poder justificar o porquê de determinadas opções.

2.1 Tipos de Criptografia

Com o aumento crescente das transações electrónicas para troca e distribuição de informação muitas vezes sensível, há que assegurar a existência de ambientes confiáveis para a realização dessas transações de uma forma segura. Tal é possível através do recurso à criptografia.

A criptografia já existe desde a era romana e define-se como a arte ou ciência de escrever de forma escondida, garantindo a privacidade da informação. Tradicionalmente, um sistema criptográfico integra os seguintes elementos (ver Figura 2.1) [4]:

- Algoritmo - Fórmula orientadora para a transformação dos dados;
- Criptograma - Texto que sofreu a transformação imposta pelo algoritmo definido;

– Chave - Parâmetro definido pelo algoritmo, responsável pela transformação do texto em claro[2] em criptograma (operação cifrar), ou pela transformação do criptograma em texto em claro (operação decifrar).

Figura 2.1: Cifrar/decifrar de um texto

Hoje em dia empregam-se dois tipos de criptografia nos sistemas computacionais. São elas a criptografia simétrica e a assimétrica. As principais características de ambas são:

– Criptografia simétrica – Existe apenas uma chave secreta que é partilhada pelo emissor e pelo receptor da mensagem, ou seja, a chave que cifra é a mesma que decifra. Tal, requer que a chave seja só do conhecimento daqueles interlocutores e que não se repita para pares de interlocutores diferentes. Esta forma de criptografia tem como principal vantagem a rapidez no cálculo das operações de cifra/decifra. No entanto, tem como desvantagem o facto de requerer $n*(n-1)/2$ chaves para n interlocutores e o problema do modo como as chaves devem ser distribuídas pelos vários intervenientes sem que se quebre o seu secretismo;

– Criptografia assimétrica – Este tipo de cifra usa um par de chaves distintas em que, embora não se consiga obter uma chave a partir da outra, estas encontram-se matematicamente relacionadas, conseguindo uma decifrar aquilo que a outra cifrou. Esta característica vai permitir que uma das chaves seja publicitada, a chave pública, pelo que só serão necessárias n chaves para n interlocutores, uma vantagem em relação à criptografia simétrica. O factor de sucesso deste tipo de cifra é manter-se a chave privada protegida e só do conhecimento do seu titular. Preenchendo este requisito, é possível obter a autenticação de conteúdos e de autoria, como se explicará na secção 2.3. Uma desvantagem que este tipo de cifra apresenta em relação à simétrica, resume-se ao facto de o seu desempenho ser mais lento, por utilizar um processo algorítmico mais complexo. Por este motivo muitas vezes estes dois tipos de

[2] Texto no seu estado natural, não codificado.

cifra operam em conjunto, como adiante se referirá, para tirar partido das vantagens de ambas.

2.2 Cifrar e Decifrar Dados

A cifra de dados é uma medida de segurança contra a visualização de dados confidenciais ("*Eavesdropping*"), que consiste na monitorização, sem alteração, de uma sessão de troca de informação por forma a obter dados confidenciais.

Para se obter a propriedade da *confidencialidade*, há que cifrar a mensagem com a chave pública do ou dos receptores pretendidos, de forma a que só estes, com as respectivas chaves privadas, tenham a capacidade de a decifrar. Uma forma de evitar a lentidão provocada pela cifra e decifra com chaves assimétricas de toda a mensagem, consiste na utilização de um método híbrido de criptografia. Através deste método, apenas se cifra com a chave assimétrica uma chave simétrica, criada naquele momento, designada de chave de sessão com a qual se cifra então a mensagem (ver Figuras 2.2 e 2.3). Como a criptografia com chave simétrica é mais rápida, reduz-se consideravelmente o tempo despendido a cifrar/decifrar as mensagens. Em situações em que se pretenda enviar uma mensagem confidencial para mais do que um receptor, aquela é só cifrada uma vez com a chave de sessão gerada. Esta é depois cifrada para cada um dos receptores com a chave pública apropriada, anexando cada uma destas chaves de sessão cifradas à mensagem.

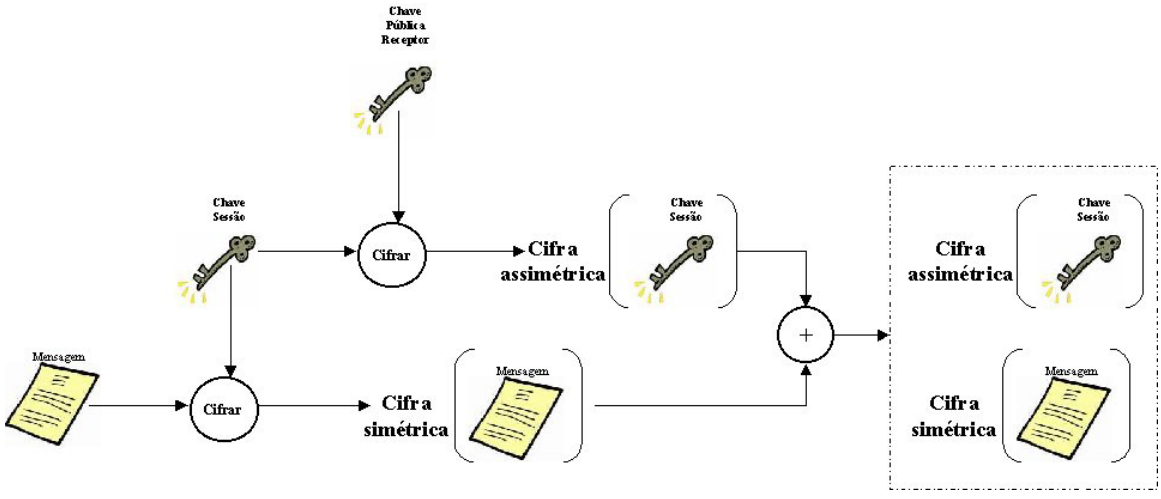

Figura 2.2: Uso de criptografia híbrida para cifrar uma mensagem

- O emissor gera uma Chave de Sessão (simétrica), com a qual cifrará a Mensagem;
- De forma a garantir a *confidencialidade* da Mensagem, cifrará, com a Chave Pública do receptor, essa Chave de Sessão;
- Enviará ao receptor estas duas cifras.

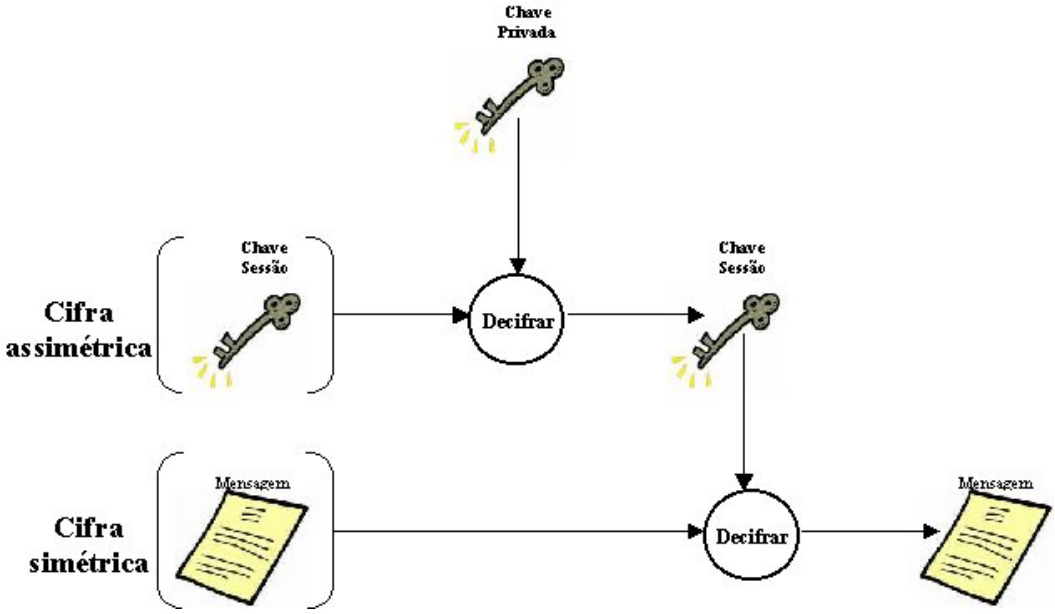

Figura 2.3: Uso de criptografia híbrida para decifrar uma mensagem

- O receptor deverá utilizar a sua Chave Privada, para decifrar a Chave de Sessão;
- Com a Chave de Sessão assim obtida, poder-se-á decifrar a Mensagem.

2.3 Assinatura Digital

A assinatura digital é o elemento responsável pela obtenção de determinadas propriedades que vêm permitir um aumento da segurança em transações consideradas inseguras. Tais propriedades permitem que a assinatura digital, surja como medida de segurança contra fraudes electrónicas como [5, 6]:

- Personificação ("*Masquerading*") – Um elemento fazer-se passar por outro, perante terceiros, aquando uma troca de informação;
- Alteração de dados ("*Data Tampering*") – Modificação de alguns ou de todos os dados transmitidos numa sessão.

Essas propriedades designam-se de *autenticidade* e *integridade*, respectivamente. A assinatura digital possui ainda as seguintes propriedades [7, 8]:

- Não forjamento – Quem assinou, fê-lo deliberadamente;
- Não reutilização – A assinatura não é reutilizável noutro documento;
- Não repúdio – Comprova o envio da mensagem, por forma a proteger o receptor da negação de envio daquela por parte do emissor, assim como protege o emissor de possíveis negações de recebimento desta por parte do receptor. Tais protecções são conseguidas, respectivamente, através da prova de envio e da prova de entrega. A primeira é obtida através da elaboração de um resumo ("*message digest*"), da concatenação da mensagem com, por exemplo, a hora de envio daquela, que depois é assinado. Tal fará prova de que a mensagem foi enviada. A segunda, corresponde ao pedido de aviso de recepção. Pode ser implementado numa mensagem de correio electrónico, pedindo ao receptor que assine um resumo da concatenação da mensagem com a hora de entrega daquela. Tal, como se pode verificar, requer a cooperação do receptor, pois este poderá negar-se a assinar o recibo [9].

Tecnologicamente, a assinatura digital é criada e verificada criptograficamente. No caso da criptografia assimétrica, utilizam-se as duas chaves, a privada e a pública, da seguinte forma: A primeira serve para criar uma assinatura digital, ou seja, é utilizada pelo emissor da mensagem quando este a assina, e a segunda será utilizada pelo ou pelos receptores da mensagem para verificarem a validade dessa assinatura digital. Embora várias pessoas conheçam a chave pública de determinado assinante e a utilizem para verificar a sua assinatura, não conseguem descobrir a sua chave privada por forma a forjar essa mesma assinatura. O facto de o emissor da mensagem assinar esta com a sua chave privada, permite a existência da já referida propriedade da *autenticidade*, pois mais ninguém, além dele, poderia ter utilizado aquela chave.

Mais especificamente, a assinatura digital é o resultado da cifra, efectuada com a chave privada, de uma representação digital sob a forma de um valor ("*hash value*") com um tamanho fixo. Este, é obtido através de um processo algorítmico designado de função de resumo ("*hash function*"), a partir da mensagem a assinar. Qualquer alteração feita na mensagem, produz um resumo diferente. Não é, também, possível obter a mensagem através do resumo (ver Figura 2.4). Quando o receptor recebe a mensagem, cria também ele um resumo dessa mensagem. Decifra com a chave pública do emissor o resumo enviado e compara ambos. Se forem iguais, significa que o conteúdo da mensagem não

foi alterado, verificando-se as propriedades da *integridade* e da *autenticidade* (ver Figura 2.5) [10, 11, 12, 13].

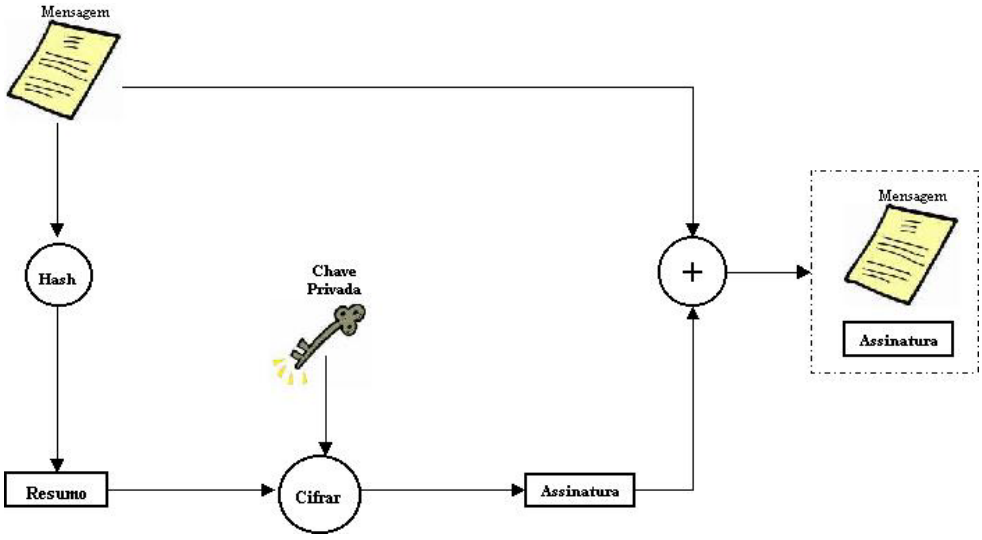

Figura 2.4: Assinatura de um documento

- A mensagem passa por um processo algorítmico designado de função de resumo ("*Hash*"), produzindo uma síntese (Resumo) daquela;
- Esse Resumo é cifrado com a Chave Privada do emissor, sendo o resultado designado de Assinatura;
- Essa Assinatura será enviada ao receptor, juntamente com a Mensagem.

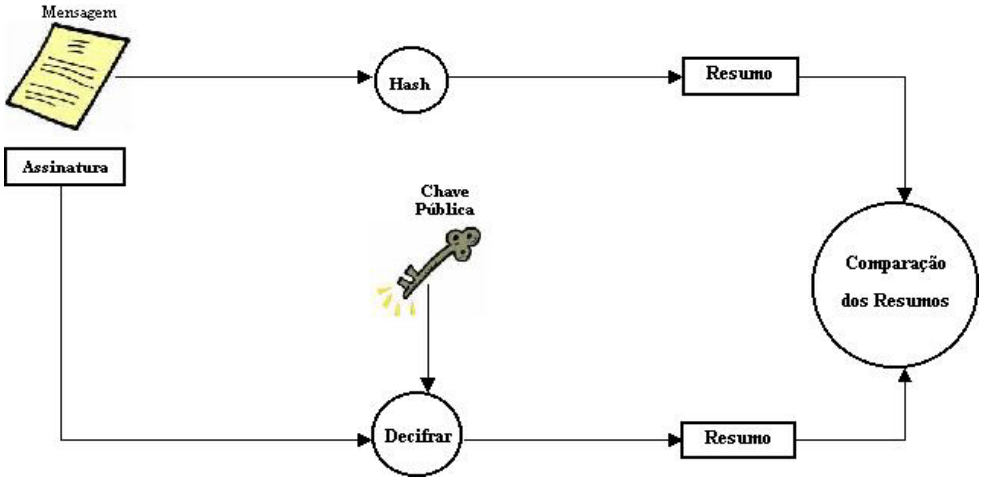

Figura 2.5: Verificação de uma assinatura

- A Mensagem e a Assinatura são recebidas pelo receptor;

- Este, à semelhança do que fizera o emissor, vai passar a Mensagem pelo mesmo processo algorítmico ("*Hash*") produzindo, também ele, uma síntese (Resumo) daquela;
- Com a Chave Pública do emissor que, como o próprio nome indica é do conhecimento público, irá decifrar a Assinatura, obtendo o Resumo da mensagem enviada pelo emissor;
- Irá então proceder à comparação de ambas as sínteses, que, a serem iguais, comprovarão a *integridade* e a *autenticidade* da mensagem.

2.4 Certificados Digitais

Aquando a utilização das operações de criptografia assimétrica, um dos interlocutores necessita de obter, de uma forma segura, a chave pública do outro interlocutor. Significa isto, que é necessária uma maneira que possa assegurar a integridade da chave pública que se está a adquirir, bem como garantir a ligação desta ao titular requerido. Tal método, no entanto, deve manter a escalabilidade, que este género de criptografia oferece, ou seja, permitir o acesso à mesma chave pública, tanto por entidades conhecidas, como desconhecidas do seu titular. Fica assim, à partida, eliminada a hipótese de entrega em mão ou por disquete da chave pública, por ausência de escalabilidade.

É introduzido assim o conceito de certificado digital que se define como sendo uma estrutura de dados que tem como principal objectivo associar, de forma fiável, a chave pública ao seu titular e garantir a autenticidade daquela, permitindo a troca segura de chaves públicas em redes não seguras [14].

Actualmente, sempre que se faz referência a certificados digitais, é do certificado de chave pública X.509 que se está a falar, pois é o que está a ser usado pela maioria das aplicações baseadas em criptografia assimétrica. Há, no entanto, outros tipos de certificados digitais, que também têm tido alguma divulgação:

- Certificado "*Simple Public Key Infrastructure*" (SPKI) – Um grupo IETF diferente daquele que pegou na estrutura X.509 e a adaptou à Internet, baseou-se na estrutura PKI e tentou torná-la mais simples e perceptível para a Internet. Por conseguinte, o certificado gerado por esta infra-estrutura, seria também mais fácil de utilizar. No

entanto, após a sua conclusão, não houve grande procura no mercado pelo que os vendedores optaram por não investir nele;

- Certificado "*Pretty Good* Privacy" (PGP) – Baseado no conceito de que as relações de confiança são feitas entre os indivíduos, eliminando a existência de uma terceira parte confiante. Tal estrutura não interessa aos sistemas corporativos nos quais se pretende que as decisões de estabelecimentos de confiança sejam efectuadas ao nível das organizações.

Um certificado X.509 é utilizado num grande conjunto de aplicações como o S/MIME, IPsec, SSL/TLS e SET. É emitido por uma CA que o assina digitalmente com a sua chave privada, por forma a garantir a integridade e autenticidade dos seus dados. Como em qualquer assinatura digital, qualquer um pode verificar se o certificado foi assinado pela CA, bastando para isso conhecer a chave pública dessa CA.

Para verificar a validade (fiabilidade) de um certificado, há que determinar se:
- Uma CA fiável assinou o certificado;
- A integridade do certificado está a salvo, ou seja, a assinatura digital incluída no certificado decifrada pela chave pública da CA, corresponde ao valor calculado pelo resumo do próprio certificado;
- O certificado encontra-se dentro do período de validade;
- O certificado não foi revogado;
- O certificado está a ser utilizado de acordo com as políticas estabelecidas pelo documento "Políticas de Certificado" ("*Certificate Policy*" (CP)).

A própria CA possui um certificado digital cuja chave pública é utilizada para verificar a assinatura da CA [15].

2.4.1 O Standard X.509

O standard X.509 faz parte de um conjunto de recomendações X.500, que definem um serviço de directório. Foram definidas, até ao momento, três versões para este tipo de certificado digital:

- Em 1988 surgiu o X.509 v1, versão genérica, que apresentava alguma inflexibilidade, uma vez que não era possível adicionar-lhe novos atributos;

- Seguidamente apareceu a X.509 v2 que introduziu o conceito de identificadores únicos para o titular e para o emissor, por forma a lidar com a possibilidade de reutilização dos nomes daqueles ao longo do tempo. A maioria dos documentos de perfis de certificados recomenda fortemente que os nomes não devem ser reutilizados. Por isso, a versão 2 não foi muito utilizada;

- X.509 v3 é a versão mais recente (1996) suportando a noção de extensões, onde qualquer um pode definir uma e incluí-la.

O formato de um certificado X.509 v3 apresenta um conjunto de dados associados ao titular do certificado e à CA que o emitiu. De referir que todos estes dados se encontram codificados utilizando dois standards relacionados, designados de "*Abstract Syntax Notation 1*/*Distinguished Encoding Rules*" (ASN.1/DER) que, de acordo com a Recomendação X.208, entretanto substituída pelas Recomendações X.680 a 683, é um sistema de codificação de valores. Os dados são os seguintes [16]:

- Versão do certificado – Identifica a versão do certificado X.509, actualmente a v3, que permite a utilização de extensões;

- Número de série – Identificador único do certificado emitido pela correspondente CA. Esta informação é usada em várias situações, como por exemplo, quando um certificado é revogado, o seu número de série é colocado na Lista de Certificados Revogados ("*Certificate Revocation List*" (CRL)), que é uma lista gerada e gerida pela CA, e que se encontra disponível a todos os utilizadores para verificação da validade de qualquer certificado (*vide* secção 2.4.2.1);

- Algoritmo de assinatura – Identificação dos algoritmos utilizados pela CA para a assinatura do certificado, que podem ser, por exemplo, o SHA-1 para resumir e o RSA para cifrar;

- Nome do emissor – A identificação da CA que emitiu e assinou o certificado. Usar este certificado, implica confiar na entidade que o assinou. De referir que, no caso do certificado da CA de raiz ("*root certificate*"), o emissor assina o seu próprio certificado. Este nome utiliza o standard X.500 [17] esperando-se, por isso, que seja único em toda a Internet. Será o Nome Distinto ("*Distinguished Name*" (DN)) da entidade. Exemplo: CN=ITIJ-CA, OU=ITIJ, O=MJ, C=PT (As siglas referem-se ao

"*Common Name*", "*Organization Unit*", "*Organization*" e "*Country*", respectivamente);

- Período de validade do certificado – A validade de um certificado é o intervalo de tempo durante o qual a CA garante que mantém a informação sobre o estado do certificado. Este período tanto poderá ser uns segundos, como um século. A escolha do período dependerá de factores como a robustez (tamanho) da chave privada, ou o valor que se está disposto a despender por um certificado. Uma vez que os certificados têm um prazo de validade, é possível que este expire, tornando-os inválidos. Se, por exemplo, um utilizador tentar aceder a um servidor seguro utilizando um certificado expirado, o software de autenticação do servidor rejeitará, automaticamente, o seu pedido de acesso. Para evitar esta situação, é possível o utilizador renovar o seu certificado antes que este expire;

- Identificação do titular – O nome da entidade cuja chave pública o certificado identifica. À semelhança do nome do Emissor, este nome também utiliza a estrutura do standard X.500;

- Chave pública – Chave pública do titular do certificado e apresentação do algoritmo com o qual ela é utilizada;

- Extensões – Várias extensões ao certificado que permitem, entre outras coisas, a indicação das limitações à responsabilidade da CA que tenham sido acordadas entre as partes.

  Algumas extensões vulgarmente utilizadas são a "*Key Usage*", que limita o uso das chaves para determinados propósitos como "*signing-only*" e a "*Subject Alternative Name*", que permite que outras identificações, como o nome do DNS, o endereço de correio electrónico, ou o endereço IP, possam ser associadas à chave pública daquele certificado. As extensões podem ser marcadas como críticas para indicar que deverão ser verificadas e exigidas. Por exemplo, se um certificado tem a extensão "*Key Usage*" marcada como crítica e definida como "*KeyCertSign*", e se esse certificado for apresentado durante uma comunicação SSL, então deverá haver uma rejeição, uma vez que essa extensão indica que a chave privada associada deverá ser utilizada apenas para assinar certificados.

  Observando a Figura 2.6, uma apresentação gráfica via "*browser*" de um certificado digital, detectam-se sete extensões, duas das quais consideradas críticas. Olhando para

o conteúdo da extensão crítica "Utilização de chaves" ("*Key Usage*"), verifica-se que a chave privada será utilizada apenas com o propósito de assinar.

Os dados acima descritos, são resumidos pela função de resumo apresentada no "Algoritmo de assinatura", sendo a síntese obtida assinada com a chave privada da CA que gerou o certificado, utilizando o algoritmo de assinatura também apresentado nesse campo. A assinatura produzida é codificada em ASN.1 numa "*string*" de bits e colocada num campo do certificado designado de "Assinatura". Ao gerar esta assinatura, a CA está a certificar a integridade da informação apresentada nos dados, bem como a ligação entre a chave pública e o titular do certificado.

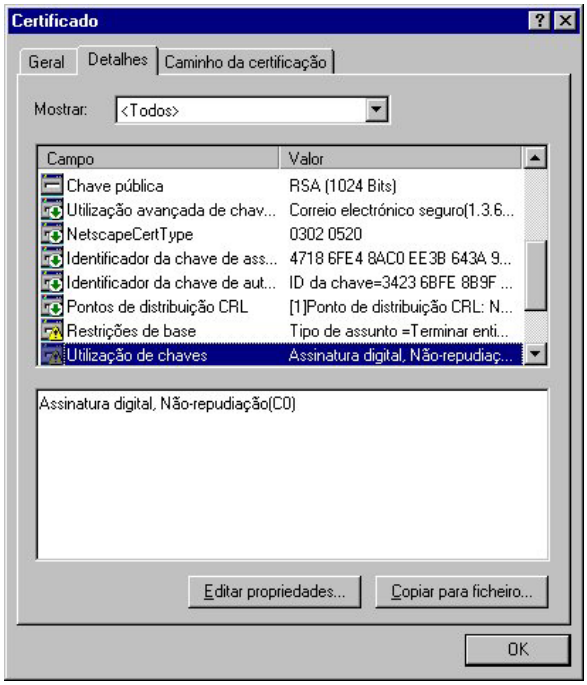

Figura 2.6: Campos de um certificado

2.4.2 Revogação de um Certificado

Embora um certificado digital tenha uma validade pré-definida, poderão surgir situações dentro do prazo de validade que determinem a necessidade de cancelar o certificado. Enumerando alguns exemplos:

- Alteração dos dados identificativos do titular apresentados no certificado;
- Perda ou furto do dispositivo que guarda o certificado;
- Obtenção por terceiros do código de segurança que o protege;

- Divulgação ou suspeita de divulgação da chave privada;
- Conhecimento de uso mal intencionado por parte do titular;
- Término das condições para o qual tinha sido emitido (*e.g.* fim de contrato ou quebra de ligação com o organismo ou serviço que requeria o uso do certificado para determinados propósitos);
- A segurança da CA foi comprometida.

Nesses casos há que accionar um mecanismo fiável e eficiente de revogação desse certificado, quer pelo titular, quer pela CA quando detecte anomalias na utilização daquele.

O novo estado do certificado (Revogado) deverá ser divulgado por toda a comunidade que eventualmente interaja com ele. Surgem então duas formas escaláveis de o fazer: as CRL's e o Protocolo de Estado do Certificado em Modo On-line ("*On-line Certificate Status Protocol*" (OCSP)).

Há que ter em conta que haverá sempre um período de tempo entre o pedido de revogação do certificado e a divulgação do estado deste a toda a comunidade. O período máximo de tempo permitido entre uma acção e outra deverá ser analisado caso a caso pois se para determinadas aplicações o atraso de umas horas não causa transtorno, para outras a publicitação do estado actual deveria ser quase imediata.

2.4.2.1 Listas de Certificados Revogados

As Listas de Certificados Revogados ("*Certificate Revocation Lists*" (CRL's)) são um método de revogação definido pelo standard X.509 [16] e que à semelhança dos certificados digitais baseados neste formato, são uma estrutura de dados que contém a lista dos certificados revogados. Esta estrutura é assinada digitalmente pela CA que assinou esses certificados quando estes foram emitidos. Tal como sucede com os certificados, a sua autenticidade e integridade são confirmadas pela assinatura ligada a essa CRL. Encontrando-se desta forma auto-protegida ("*self-protected*"), é um mecanismo de publicação periódica que poderá ser colocado à disposição num repositório, via comunicações inseguras ou sistemas de servidores não fiáveis. É esta a grande vantagem das CRL's relativamente ao mecanismo de verificação on-line do estado do certificado, o OCSP, adiante referido na secção 2.4.2.2.

Como limitação deste método de revogação, pode-se enumerar o facto de a granularidade do tempo da revogação estar limitada ao período de emissão da CRL. Por exemplo, se um pedido de revogação for efectuado neste preciso momento, tal revogação não será notificada aos utilizadores do sistema de certificação até à próxima actualização da CRL. Esta limitação, no entanto, poderá ser colmatada com a utilização de Delta CRL's [18]. Estas serão automaticamente emitidas sempre que houver uma nova revogação e publicadas sem que seja necessário mexer na estrutura da CRL principal. Esta terá um apontador que indicará o local onde se encontra a Delta CRL. Quando a validade da CRL principal expirar, actualizar-se-á a sua informação com a adição das novas revogações apresentadas na última Delta CRL emitida, que incrementou todas as revogações até aí efectuadas. De seguida, esta Delta CRL será eliminada, iniciando-se um novo ciclo.

Cada certificado revogado é identificado na CRL pelo seu número de série (ver Figura 2.7), para impedir que a estrutura se torne muito pesada rapidamente.

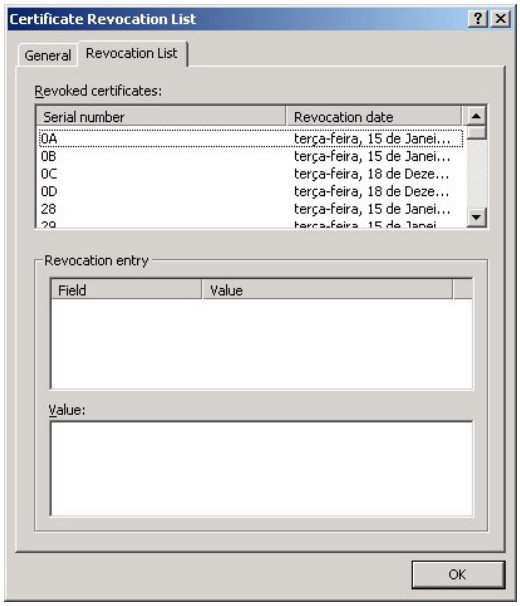

Figura 2.7: Visualização dos números de série na Lista de Certificados Revogados

No acto de verificação de, *e.g.* uma assinatura digital, o receptor não só verifica a assinatura desse certificado e a sua validade, como adquire a última CRL emitida, por forma a verificar se o número de série daquele certificado se encontra na lista, indicando a sua revogação. O receptor poderá saber a localização da CRL, através de uma das extensões do certificado recebido, designada de "Pontos de distribuição CRL" ("*CRL*

distribution points"), que apresenta a "*Uniform Resource Locator*" (URL) de acesso à CRL pretendida.

Presentemente, encontram-se definidas duas versões de CRL's em formato X.509:

- CRL X.509 v1 – Foi definida nas especificações originais do X.509 em 1988, apresentando uma série de falhas:
  - Ausência de escalabilidade – O tamanho da lista tinha tendência a aumentar para limites não razoáveis;
  - Limitações funcionais – Incapacidade de adicionar características específicas quando tal se apresentasse necessário;
  - Vulnerável a ataques de substituição – Permitia a substituição maliciosa de uma CRL por outra.

- CRL X.509 v2 – Veio resolver os problemas apresentados pela versão anterior introduzindo, tal como os certificados X.509 v3, a noção de extensões.

À semelhança do que foi referido no formato do certificado, o formato de uma CRL X.509 v2 apresenta um conjunto de dados que se encontram codificados utilizando os standards ASN.1/DER [16]:

- Versão da CRL – Identifica a versão da CRL X.509, actualmente a v2, que permite a utilização de extensões;

- Algoritmo de assinatura – Identificação dos algoritmos utilizados pela CA para a assinatura da CRL;

- Nome do emissor – A identificação da CA que emitiu e assinou a CRL. Este nome utiliza o standard X.500, tal como o nome do emissor do certificado digital;

- Data da última actualização da CRL – Apresenta a data em que a CRL foi emitida;

- Data da próxima actualização da CRL – Indica a data em que a próxima CRL será emitida;

- Certificados revogados – Lista os certificados que se encontram revogados. Apresenta como parâmetros o número de série do certificado revogado, a data da sua revogação e eventuais extensões que se considerem necessárias, como o motivo da revogação (ver Figura 2.8);

– Extensões – Várias extensões à CRL que permitem a adição de atributos às CRL's, a definição de extensões privadas para determinada comunidade de utilizadores. Tal como as extensões do certificado, podem ser consideradas críticas ou não. É na extensão "*Delta CRL indicator*" que é colocado o apontador para as Delta CRL's emitidas, sendo uma extensão crítica.

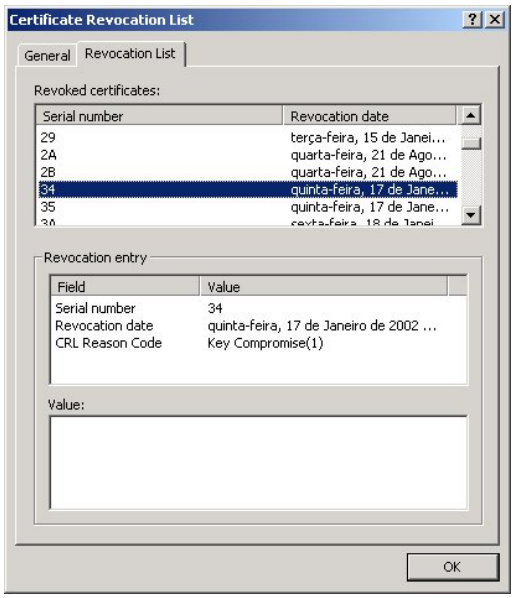

Figura 2.8: Parâmetros de um certificado revogado

Tal como foi referido nos certificados digitais, os dados acima descritos, são resumidos pela função de resumo apresentada no "Algoritmo de assinatura", sendo a síntese obtida assinada, utilizando o algoritmo de assinatura também apresentado nesse campo. A assinatura produzida é codificada em ASN.1 numa "*string*" de bits e colocada num campo do certificado designado de "Assinatura". Ao gerar esta assinatura, a CA está a certificar a integridade da informação apresentada nos dados da CRL.

Esta estrutura adquire o nome de Lista de Certificados de CA's Revogados ("*Authority Revocation List*" (ARL)), quando a sua lista apresenta a revogação de certificados pertencentes a sub CA's (*vide* definição de sub CA na secção 2.5.1.1). Em consequência da revogação destes certificados, todos os certificados emitidos por essas sub CA's, ficam inválidos.

2.4.2.2 Protocolo de Estado do Certificado em Modo On-Line

O Protocolo de Estado do Certificado em modo On-line ("*On-line Certificate Status Protocol*" (OCSP)), é uma alternativa às CRL's. Tal método permite a redução da latência entre o aviso de pedido de revogação e o conhecimento desta pela comunidade utilizadora de certificados digitais. Contudo, há que ter em conta que este método impõe requisitos de segurança considerados desnecessários nas CRL's: deverá haver uma validação do servidor responsável pelo serviço de verificação do estado dos certificados.

O processo de utilização deste protocolo é o seguinte [19]:

- O utilizador que tenciona saber o estado de determinado certificado, envia esse pedido a um servidor de OCSP ("*OCSP responder*"), suspendendo a aceitação do certificado até que aquele lhe envie uma resposta. O pedido apresenta o seguinte formato:
  - Versão do protocolo OCSP;
  - Serviço pedido;
  - Apresentação do identificador do certificado ou da lista de identificadores de certificados dos quais se pretende saber o estado;
  - Extensões opcionais que poderão ser processadas pelo "*OCSP responder*".

- Após a recepção do recibo, o "*OCSP responder*" verifica se este contém toda a informação necessária para uma correcta pesquisa do estado do certificado. Caso tal não se verifique, devolverá uma mensagem de erro ao utilizador;

- O "*OCSP responder*" enviará a resposta numa estrutura com os seguintes dados:
  - Versão da sintaxe da resposta;
  - Nome do "*OCSP responder*";
  - Apresentação do estado de cada um dos certificados enviados no pedido;
  - Extensões opcionais;
  - Algoritmo de assinatura;
  - Assinatura efectuada sobre o "*hash*" da resposta.

  Como estado do certificado poder-se-á definir um de três estados: "Bom", "Revogado" ou "Desconhecido". De referir que o facto de o certificado se apresentar com o estado "Bom", confirma apenas que ele não se encontra revogado, ou seja, não garante, por exemplo, que o certificado está dentro da validade, ou que foi emitido por

uma CA fiável. Caso esteja revogado ou suspenso[3] apresentará o estado "Revogado" e caso não seja conhecido pelo "*OCSP* r*esponder*", apresentará o estado "Desconhecido".

Em relação à assinatura que garante a integridade dos dados contidos na resposta, não tem forçosamente de ser efectuada pela chave privada que assinou anteriormente esses certificados. A CA que emitiu aqueles certificados delega no "*OCSP Responder*" autoridade para assinar, ao emitir-lhe um certificado apenas para esse propósito.

Este protocolo apresenta, no entanto, algumas limitações:

- Uma vez que tem de haver comunicação com o servidor "*OCSP* r*esponder*", este está vulnerável ao ataque de negação de serviço ("*Denial of service*"), por excesso de pedidos efectuados ao mesmo tempo;

- O facto de as respostas aos vários pedidos efectuados terem de ser assinadas no momento, vai atrasar o processo de resposta;

- Os pedidos não são direccionados para um "*OCSP responder*" específico pelo que um atacante poderá repetir esse pedido por vários "*OCSP responders*".

2.5 A Infra-estrutura de Chave Pública

Uma estrutura, seja ela desenhada para o que for, tem sempre como fundamento definir uma arquitectura que permita reunir um conjunto de elementos, orientá-los pelas mesmas regras e colocá-los a interagir para um objectivo comum.

A Infra-estrutura de Chave Pública (PKI) não foge a esta regra. A razão da sua existência, é desenvolver um ambiente seguro, cujos serviços apresentados sejam baseados em técnicas e conceitos relativos ao uso de criptografia assimétrica. Reúne um conjunto de hardware, software, políticas e procedimentos para alcançar um propósito: a emissão de pares de chaves e distribuição dos correspondentes certificados digitais [18].

[3] Revogação temporária que a qualquer momento pode terminar, voltando o certificado a estar válido

2.5.1 Componentes e Serviços

Esta estrutura é composta por um conjunto de elementos, cada um com funções específicas que, interligados, permitem realizar o objectivo da PKI. São eles [20]:

- Autoridade de Certificação ("*Certification Authority*" (CA)) – É a base de confiança de toda a PKI. Toda a confiança na infra-estrutura depende da sua assinatura.
  A sua função é gerar ou fornecer os meios técnicos para a geração dos pares de chaves e emitir certificados digitais. Tem como tarefas, a recepção de pedidos de certificação e de revogação feitos pela Autoridade de Registo e o retorno de certificados e de listas de certificados revogados, respectivamente. Para garantir a integridade de toda a estrutura, assina os certificados emitidos quer para utilizadores, quer para eventuais sub CA's. Caso haja certificação cruzada (*vide* secção 2.5.1.2), assina também os certificados de outras CA's. Assina e publica num repositório público, toda a informação de revogação sob a forma de CRL's e ARL's. Assina e arquiva na sua base de dados, todos os dados e históricos ("*logs*") originados. De referir que a root CA, ou seja, a CA que se encontra no topo da hierarquia, gera o seu próprio par de chaves;

- Autoridade de Registo ("*Registration Authority*" (RA)) – Providencia o interface entre o utilizador e a CA. Responsável pela recepção dos pedidos de emissão de certificados digitais e verificação da autenticidade dos requerentes. Este elemento é facultativo pois os seus serviços podem ser realizados pela CA. Esta divisão de tarefas tem como objectivo reportar um serviço que requer bastante responsabilidade para outra entidade, de forma a aliviar a carga funcional da CA e repartir responsabilidades [21];

- Repositório de certificados ("*Certificate Repository*") – Repositório on-line robusto e escalável[4] para o armazenamento dos certificados;

- Software do cliente – Para que a infra-estrutura resulte, o software do cliente deverá estar preparado para reconhecer, originar e reagir a todos os eventos inerentes àquela. Deverá requerer os serviços de certificação e de revogação, deverá compreender os historiais das chaves ("*key histories*") e saber quando requerer uma actualização ou uma recuperação de chaves, etc.;

[4] Versátil o suficiente para suportar o aumento gradual dos certificados sem nenhum impedimento técnico.

- Declaração de Práticas de Certificação ("*Certification Practice Statement*" (CPS)) – Documento detalhado contendo os procedimentos operacionais que satisfazem as regras definidas pela Política de Segurança da PKI. Normalmente inclui as definições de como a CA foi construída e opera, como os certificados são aceites, emitidos e revogados, como as chaves são geradas, registadas e certificadas, onde irão ser guardadas e como serão disponibilizadas aos utilizadores. O rigor deste documento é bastante importante para o fortalecimento da base de confiança das partes confiantes na infra-estrutura desenvolvida (uma descrição mais pormenorizada é apresentada na secção 2.5.1.3).

Existe uma série de serviços que uma PKI deve manter para que os seus objectivos sejam satisfeitos de forma eficaz, a saber, a garantia da fiabilidade dos certificados e das chaves por ele geridas. São eles:

- Recuperação e cópias de segurança de chaves ("*Key backup and Recovery*") – Assegura a recuperação de chaves privadas perdidas devido a esquecimento da palavra passe ou destruição do disco ou do smart card onde se encontrava guardada. As chaves privadas a guardar deverão ser as de cifra e não as de assinatura, para garantir a propriedade do não repúdio. Como já foi apresentado na secção 2.3, esta propriedade refere-se à impossibilidade de o emissor de determinada mensagem assinada poder negar mais tarde o seu envio. Significa isto que nem a própria CA deve ter acesso à chave privada de assinatura dos titulares, guardando por isso, apenas a chave privada de cifra. A recuperação desta última é considerada crucial uma vez que os dados cifrados pela respectiva chave pública, ficariam irremediavelmente por decifrar, podendo ter consequências graves. Relativamente aos dados assinados pela chave privada perdida tal necessidade já não se verifica, uma vez que, como já foi explicado na secção 2.3, se usa a chave pública para se verificar a assinatura;

- Actualização automática das chaves ("*Automatic Key Update*") – Um certificado deve ter um prazo de validade e ser automaticamente substituído por outro antes do prazo expirar. Idealmente, não haverá qualquer intervenção por parte do utilizador. Sempre que o certificado está para ser utilizado, é verificado o seu prazo de validade. Quando a data de expiração está próxima, ocorre uma operação de renovação e um novo certificado é gerado. Então o novo certificado é utilizado em lugar do outro e o pedido de transacção continua normalmente;

- Gestão do historial da chave ("*Key History Management*") – No decurso do tempo, um utilizador vai coleccionando várias chaves "antigas". A esta colecção de certificados e correspondentes chaves públicas, dá-se o nome de Historial da Chave ("*Key History*" ou "*Key and Certificate History*"). É importante manter este historial pois os dados que um utilizador cifrou há cinco anos, não podem ser decifrados com a sua chave pública actual. A manutenção do historial das chaves também deve ser automática;

- Certificação cruzada ("*Cross-Certification*") – Na impossibilidade de existência de uma PKI global, há a necessidade de estabelecer relações de confiança entre PKI's, por forma a obter um reconhecimento automático dos certificados emitidos pelas CA's integradas em determinada relação de confiança (*vide* secção 2.5.1.2);

- Suporte ao não repúdio – Por forma a impedir que o detentor de um certificado digital possa mais tarde negar ter assinado digitalmente documentos, alegando ter sido esta acção efectuada por terceiros, a PKI terá que providenciar os mecanismos que impeçam tal repúdio, tais como garantir que ela própria não retém as chaves privadas de assinatura dos detentores dos certificados, autenticar a origem dos dados e atestar de forma fidedigna o dia e a hora em que o documento foi assinado;

- Estampilha temporal ("*Time Stamping*") – Este é um dos elementos críticos ao suporte ao não repúdio, para além de outras utilidades secundárias. É fundamental obter uma estampilha temporal fidedigna, ou seja, fornecida por uma fonte de tempo autorizada em quem os utilizadores da PKI confiem. Esta fonte de tempo autorizada será, no fundo, um servidor de estampilhas temporais cujo certificado digital é verificado pelos utilizadores da PKI e cujas estampilhas temporais emitidas e anexadas aos documentos, são consideradas autênticas e íntegras. De referir que esta estampilha poderá não ser uma representação do tempo real mas sim um número sequencial demonstrando que o documento foi apresentado à autoridade antes do documento *x* e depois do documento *y*.

2.5.1.1 Hierarquia de Autoridades de Certificação

Uma PKI, assenta em hierarquias de confiança. Ao contrário do PGP, em que cada pessoa estabelece relações de confiança com conhecidos seus e posteriormente com conhecidos de conhecidos seus, uma PKI é mais institucional. Há uma terceira parte de confiança,

que permite criar um triângulo fiável com dois elementos que não se conhecem. A partir do momento em que se confia numa CA (terceira parte de confiança), confiam-se em todos os certificados emitidos por aquela.

Numa hierarquia de CA's, no topo encontra-se a root CA (CA raiz), assim designada por agir como raiz de confiança para todos os elementos que se encontram abaixo daquela. Nos nós intermédios, que podem ser de 0 a *n*, encontram-se CA's intermédias designadas de sub CA's (CA's subordinadas). O último nível de nós corresponde aos utilizadores finais (ver Figura 2.9). A raiz duma hierarquia não indica apenas o início desta, indicando também o ponto inicial de uma cadeia de confiança. Cada um dos nós intermédios, terá de possuir uma cópia da chave pública da root CA. Independentemente de os certificados dos utilizadores finais serem emitidos por uma CA intermédia, o seu ponto de confiança será sempre a root CA. Partindo do pressuposto de que o utilizador A obtém de uma forma segura o certificado da root CA da cadeia de confiança do utilizador B cujo certificado aquele pretende verificar, consegue, através desse certificado, verificar o certificado de uma eventual sub CA, cujo certificado verificará o certificado desse utilizador. Tomando como exemplo a Figura 2.9, para verificar o certificado do utilizador final, há que "descer" na hierarquia de certificação desde a root CA até àquele. Bastará para tal, obter o certificado raiz que a hierarquia de confiança se formará.

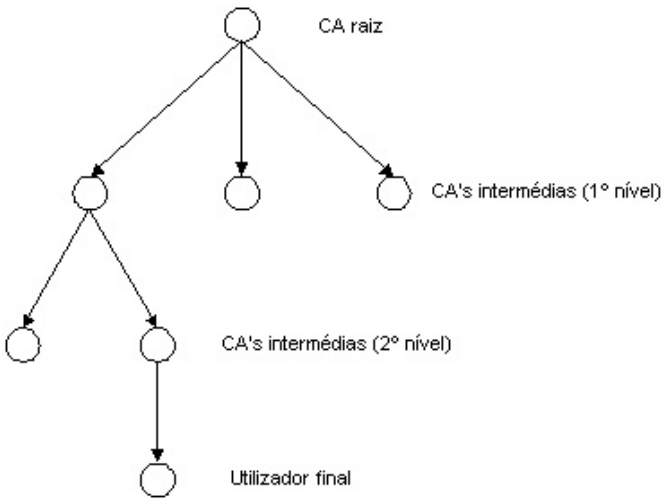

Figura 2.9: Hieraquia de confiança

Há, pois, que accionar os mecanismos necessários para demonstrar a confiança existente em determinada CA. Existem vários modelos de confiança instituídos, sendo o modelo Web o mais divulgado.

Neste modelo, um conjunto de certificados digitais de CA's consideradas fiáveis pelo "*browser*", são pré-instalados neste (ver Figura 2.10). Tal modelo torna-se bastante vantajoso em termos de comodidade para o utilizador que utiliza, de forma transparente, os certificados emitidos pelas CA's que lá se encontrarem.

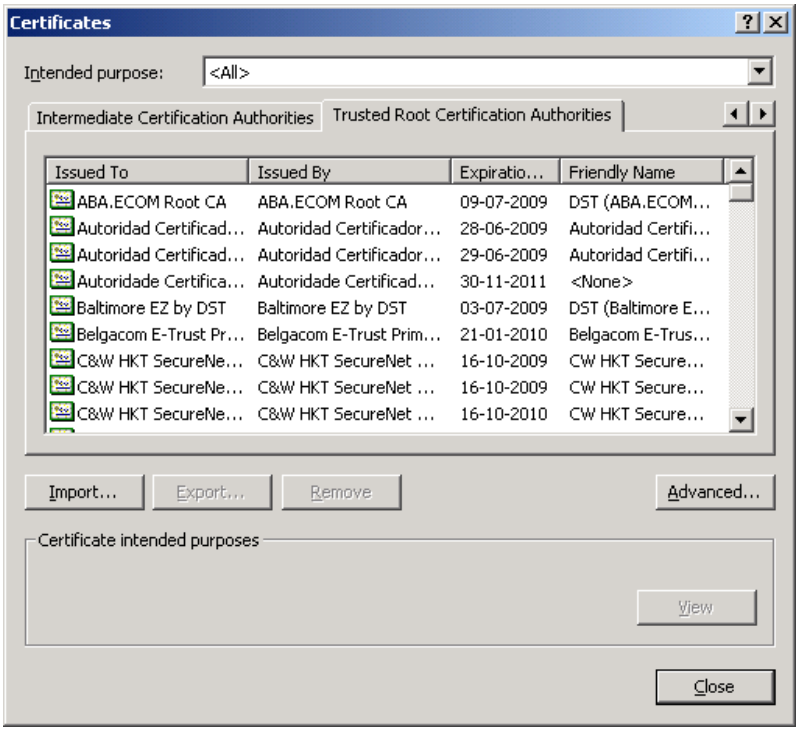

Figura 2.10: CA's presentes no "*browser*"

Mas, como se compreenderá, não estão lá todas as CA's existentes, até porque tornaria o "*browser*" pesadíssimo. As possibilidades que surgem a essas CA's serão então colocarem-se debaixo de uma hierarquia já existente e reconhecida, ou seja, tornarem-se uma sub CA de determinada CA existente no "*browser*", ou então permitirem a descarga do seu certificado, à comunidade de utilizadores da sua PKI (ver Figuras 2.11 e 2.12).

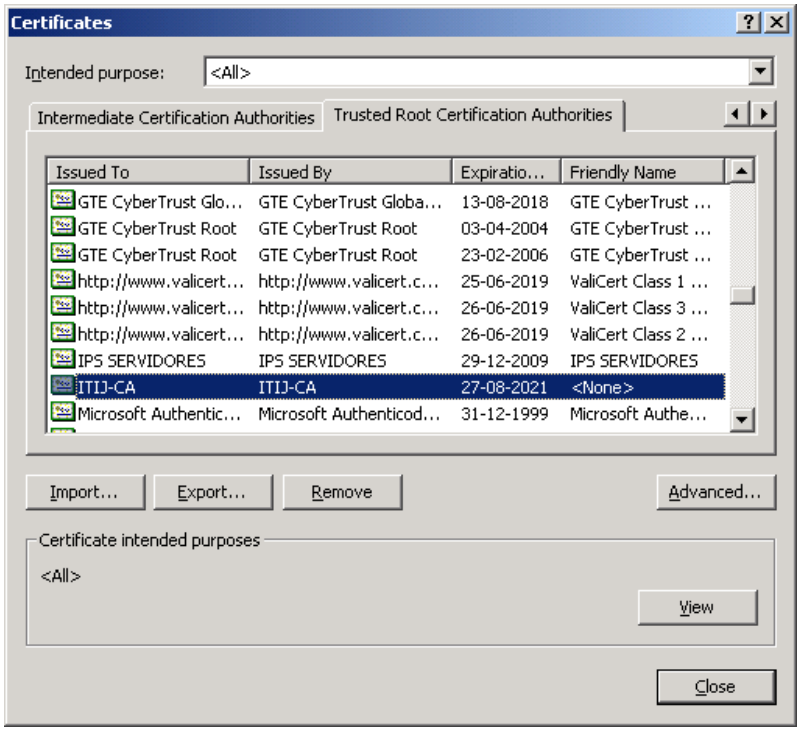

Figura 2.11: Certificado da root CA do ITIJ no "*browser*" após realização da descarga

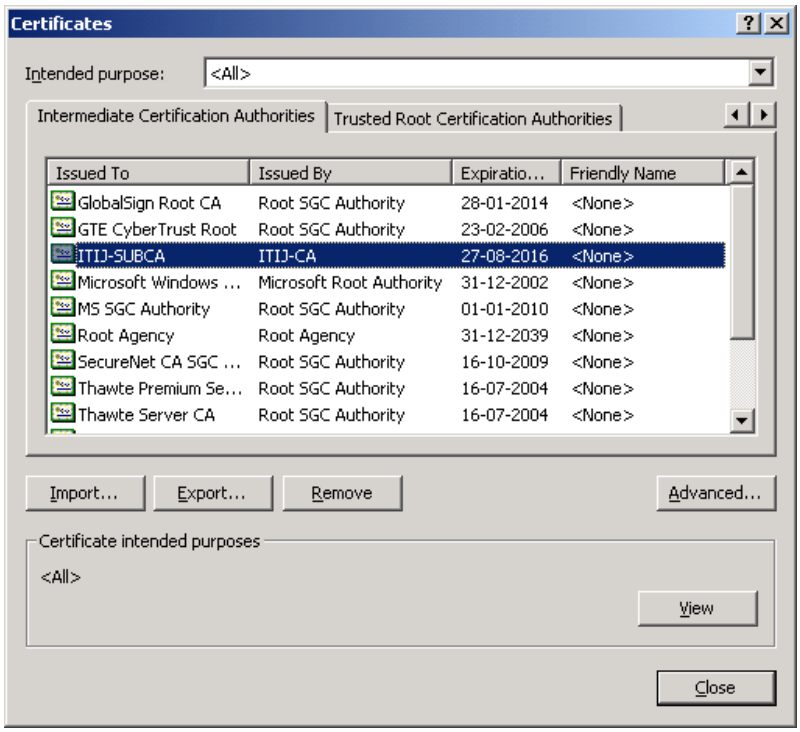

Figura 2.12: Certificado da sub CA do ITIJ no "*browser*" após realização da descarga

Tal descarga, geralmente é apresentada numa página da Internet referente a essa CA, normalmente criada para apresentar informações relativas a essa estrutura, tais como o CPS e o CP, os certificados com as chaves públicas disponibilizados para a Internet,

pedido de emissão/renovação/revogação de certificados, visualização de CRL's, ou seja, todos os procedimentos relacionados com essa PKI.

Há no entanto a referir, que o modelo Web apresenta algumas desvantagens. O facto de o "*browser*" já trazer incorporado um conjunto de root CA's, faz com que o software do utilizador aceite automaticamente aquelas CA's como fidedignas, independentemente de o utilizador confiar nelas ou sequer conhecê-las. Também apresenta vulnerabilidades relativamente a CA's que possam ser incorporadas via Internet de forma mal intencionada.

2.5.1.2 Certificação Cruzada

Embora existam diferentes PKI's a prestar serviços a diferentes comunidades de utilizadores, por vezes elas precisam de se interligar. Por exemplo um utilizador da PKI_1 necessita de confiar num certificado de outro utilizador, que foi emitido por uma CA pertencente a uma PKI_2. A melhor forma de o fazer será estabelecer um voto de confiança ao nível mais superior das hierarquias, ou seja, ao nível das CA's de raiz. A partir do momento em que uma CA de raiz refira que confia noutra CA de raiz, toda a sua estrutura confiará automaticamente naquela CA. É estabelecido um caminho de confiança ("*chain of trust*") entre ambas.

Surge assim o conceito de certificação cruzada para lidar, precisamente, com a necessidade de criar relações de confiança entre CA's pertencentes a diferentes PKI's. Duas CA's trocam informação para estabelecer uma certificação cruzada, emitindo um certificado cruzado ("*cross-certificate*"). Um certificado cruzado é um certificado emitido por uma CA para outra CA, que contém a chave pública correspondente à chave privada utilizada para assinar os certificados da sua PKI [16]. De referir que uma certificação cruzada não é forçosamente recíproca: O facto de a CA_1 certificar, ou seja, assinar a chave pública da CA_2, não significa que esta tenha de certificar a primeira. Caso haja uma certificação bilateral, significa que irão existir dois certificados cruzados [22]. O par de certificados formado, será armazenado nos repositórios públicos (*vide* definição na secção 2.5.3) de ambas as CA's.

Verifica-se a vantagem que uma certificação cruzada proporciona: o $titular_1$ cujo certificado foi emitido pela CA_1, consegue automaticamente verificar o certificado do $titular_2$, emitido pela CA_2. Tal situação deve-se ao facto de ele ser detentor da chave

pública da CA_1 cuja chave privada associada assinou um certificado com a chave pública da CA_2, estabelecendo o caminho de confiança até ao certificado do $titular_2$.

2.5.1.3 Declaração de Práticas de Certificação e Políticas de Certificado

De acordo com o RFC 2527, uma Declaração de Práticas de Certificação ("*Certification Practice Statement*" (CPS)) é um documento que apresenta um conjunto de regras que uma CA segue ao emitir certificados. Uma Política de Certificado ("*Certificate Policy*" (CP)) é um conjunto de regras que indicam a aplicabilidade de um certificado para uma determinada comunidade com requisitos de segurança comuns. Pode servir para ajudar um utilizador a decidir quando é que um certificado é fidedigno o suficiente para ser usado em determinada aplicação [23].

As políticas sob as quais os certificados são emitidos, determinam o grau de confiança que as outras partes terão nos certificados gerados por aquela CA. Estas políticas normalmente encontram-se publicadas na CPS. Esta, tipicamente, apresenta as políticas para obtenção de vários níveis de certificados e o processo de registo que o utilizador deve realizar por forma a obter um [24].

A CPS tem informação mais detalhada que a CP, tal como:

- A Política de Segurança que apresenta os princípios de segurança que regem a PKI;
- O guia de requisitos de segurança e auditoria que descreve detalhadamente os requisitos de pessoal, físicos, lógicos, de telecomunicações e de segurança e gestão das chaves;
- O guia de requisitos legais que regem a emissão de certificados digitais e os propósitos das assinaturas digitais no país de origem da CA.

Em suma, enquanto que a CP define os requisitos, a CPS explica como é que a PKI aplica os procedimentos para cumprir esses requisitos.

Ambas são disponibilizadas ao público através de uma extensão do certificado, designada de "*Certificate Policies*" [16]. Esta extensão contém uma sequência de uma ou várias políticas correspondendo cada uma delas a um identificador ("*Object IDentifier"* (OID)) [25, 26] e a qualificadores opcionais (ver Figura 2.13). O propósito desta extensão é apresentar uma forma de a CA identificar sob que política aquele certificado foi emitido.

Estas políticas são aquelas sob as quais o certificado foi emitido e apresentam os propósitos para os quais deverá ser utilizado.

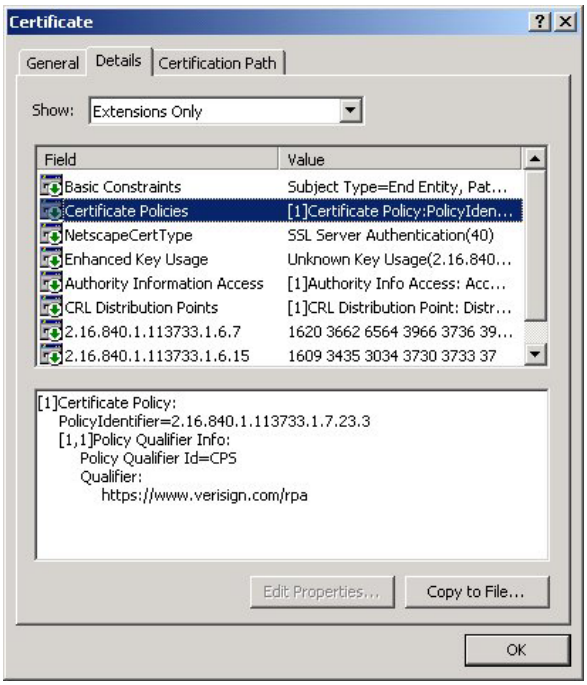

Figura 2.13: Localização dos documentos CPS e CP

De acordo com o RFC 2459, há dois tipos de qualificadores: um deles é um apontador em formato de "*Uniform Resource Identifier*" (URI) para o CPS e o outro é uma informação para o utilizador ("*User Notice*"), que serve para ser visualizado por uma parte confiante[5] quando o certificado é utilizado (ver Figuras 2.14 e 2.15).

[5] Utilizador passivo (receptor) de uma PKI

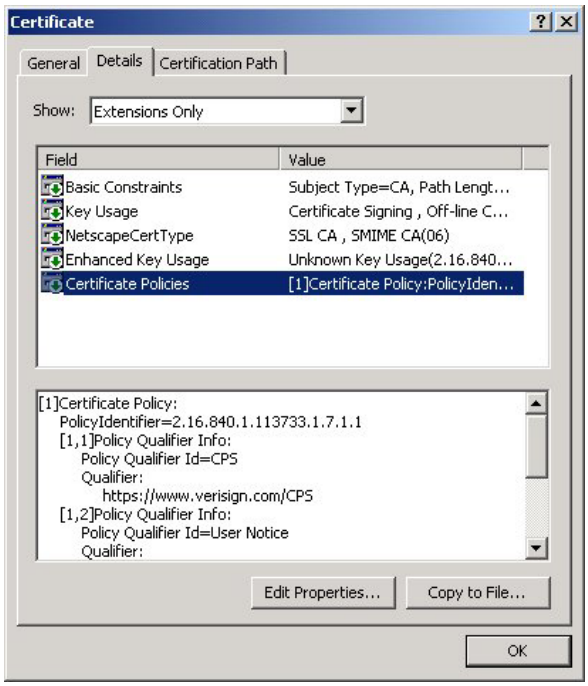

Figura 2.14: Visualização dos dois qualificadores

```
[1]Certificate Policy:
    PolicyIdentifier=2.16.840.1.113733.1.7.1.1
    [1,1]Policy Qualifier Info:
        Policy Qualifier Id=CPS
        Qualifier:
            https://www.verisign.com/CPS
    [1,2]Policy Qualifier Info:
        Policy Qualifier Id=User Notice
        Qualifier:
            Notice Reference:
                Organization=VeriSign, Inc.
                Notice Number=1
            Notice Text=VeriSign's Certification Practice Statement,
www.verisign.com/CPS, governs this certificate & is incorporated by
reference herein. SOME WARRANTIES DISCLAIMED & LIABILITY
LTD. (c)1997 VeriSign
```

Figura 2.15: Pormenor do conteúdo de uma CP com dois qualificadores

2.5.2 Armazenamento Seguro de Chaves

Relembrando o que foi abordado nos vários itens deste capítulo, conclui-se que o elemento sensível desta infra-estrutura, é a chave privada, devendo por isso ser protegida da melhor forma possível. Quer ela seja de um utilizador comum, quer seja de uma CA, está sempre exposta ao mesmo perigo, embora na segunda situação, com maiores implicações que na primeira. Se forem descobertas por terceiros, eliminam a propriedade

da autenticidade que esta garantia. No caso da chave privada da CA, a situação é gravíssima pois destruirá toda a hierarquia de segurança nela suspensa.

Assim, para além de sensibilizar os titulares das chaves para as precauções que devem tomar, utilizam-se dispositivos de armazenamento considerados robustos, numa tentativa de eliminar ao máximo ataques bem sucedidos.

Apresentam-se três dispositivos de armazenamento de chaves considerados seguros. A hipótese de gravação da chave em disquete ou em disco é descartada, pois nestes suportes aquela pode-se eliminar ou copiar facilmente, uma vez que são suportes de fácil acesso.

2.5.2.1 Smart Card

Os smart cards são normalmente de um dos seguintes tipos [27, 28, 29]:

- Cartões de memória ("*Memory cards*") – Limitam-se a armazenar informação, não tendo capacidade de reagir contra intrusões nem capacidade de processamento para suportar algoritmos de segurança;

- Cartões com microprocessador ("*Microprocessor cards*") – Têm as características de um computador simples. Uma vantagem em relação aos anteriores é que normalmente são mais robustos, dificultando a cópia da informação lá armazenada. Contêm um componente electrónico, um "*chip*" (ver Figura 2.16), que é um microprocessador "*Self Programmable One Microcalculator*" (SPOM) que integra os elementos que constituem um microprocessador:
  - Unidade de processamento;
  - Memórias: RAM, ROM, EEPROM que contêm a informação do detentor do cartão e as aplicações aí desenvolvidas;
  - Mecanismos anti-intrusão;
  - Interface standard de input-output.

  Relativamente à segurança, tem como principais características a resistência à alteração, o "*chip*" não ser lido através de meios físicos directos, a capacidade de detecção de ataques por raios ultravioleta ou voltagem diferente.

  Tem capacidade para gerar a chave privada dentro do cartão sendo guardada num ficheiro secreto. Como "*input*" são-lhe fornecidos parâmetros, alguns deles públicos e

consequentemente gerados fora do cartão, tendo sido anteriormente utilizados na criação da chave pública. A chave pública foi gerada fora do cartão sendo juntamente com o certificado associado, guardada naquele.

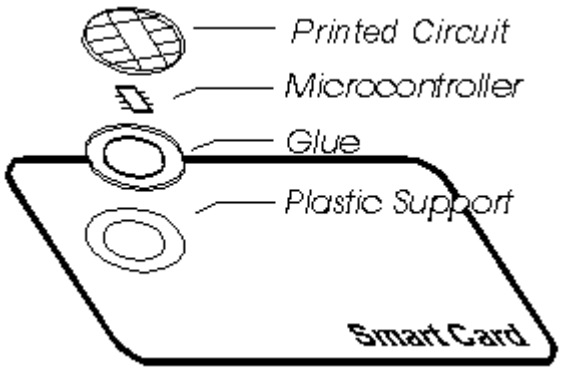

Figura 2.16: Estrutura física de um smart card

O smart card apresenta como vantagem o facto de permitir apresentar os dados do seu titular impressos na sua superfície, funcionando como um cartão de identificação. Como desvantagem apresenta o custo, uma vez que requer a aquisição do cartão e do respectivo leitor.

2.5.2.2 USB Token

O "*token*" de segurança ou de autenticação é um pequeno dispositivo de hardware que se pode apresentar sob a forma de cartões magnéticos, smart cards, cartões sem contacto que usam o rádio para transmitir os dados e dispositivos USB ("*USB Tokens*") [30].

O "*USB Token*", possui as mesmas características lógicas e de segurança que um smart card (o seu conteúdo é protegido por PIN, guarda o par de chaves assimétricas, executa funções criptográficas, gera a chave privada, etc.), diferindo deste ao nível físico. Como o próprio nome indica, é ligado à porta "*Universal Serial Bus*" (USB) do computador, não necessitando de leitor (ver Figuras 2.17 e 2.18). Esta particularidade pode ser considerada uma vantagem em relação ao smart card.

Figura 2.17: USB Token

Figura 2.18: Token ligado à porta USB

2.5.2.3 Hardware Security Module

O Módulo de Segurança em Hardware ("*Hardware Security Module*" (HSM)) é um dispositivo resistente a alterações, utilizado em sistemas criptográficos como um método que assegura a segurança de uma variedade de operações. Normalmente é o dispositivo utilizado para armazenamento da chave privada da CA, desempenhando as seguintes funções, para além da já referida [31, 32, 33]:

- Assinatura de certificados;
- Geração de números aleatórios;
- Geração de chaves;
- Geração das chaves da CA dentro do módulo.

Tem como características:

- O hardware é menos susceptível a falhas, corrupções e vírus;
- Operações criptográficas de grande rapidez;
- Armazenamento seguro – As chaves e material criptográfico são armazenadas de forma segura no módulo;
- Salvaguarda ("*Backup*") segura – As chaves podem de forma segura ser recuperadas para smart cards ou para outro módulo;
- À prova de alterações – O material considerado sensível é destruído caso o conteúdo do módulo seja alterado;
- Criptografia dentro do módulo – Todas as funções criptográficas que envolvem a protecção das chaves são desempenhadas sobre o módulo;

– Por meio de selos holográficos detecta qualquer tentativa de intrusão física;

O código de acesso ao seu conteúdo é feito através da combinação de fragmentos de uma chave simétrica (3DES) guardados em vários smart cards distribuídos aos operadores da CA e por isso denominados de "Cartões de operador". Por uma questão de segurança, pois os smart cards podem perder-se ou estragar-se, a quantidade de fragmentos necessários ("*split keys*") para a recriação de uma chave, deve ser inferior à quantidade de fragmentos existente. Um conjunto de fragmentos de chave ("*split keys*") quando combinados entre si, permitem a recriação de várias chaves válidas.

2.5.3 Disseminação de Certificados e da Informação de Revogação de Certificados

Existem várias formas de distribuir os certificados e a informação de revogação destes, normalmente sob a estrutura de CRL's, pela comunidade de utilizadores. Como exemplo, surge o repositório, a entrega em mão de uma disquete ou de outro tipo de suporte e o anexo ("*attachment*") a uma mensagem de correio electrónico. As duas últimas, são denominadas formas de disseminação privada, uma vez que não são fornecidas a toda a comunidade, apresentando algumas desvantagens como, não haver a certeza de toda a comunidade partilhar a mesma informação actualizada, a informação não ser enviada por uma terceira parte de confiança e não ser escalável.

Devido a estas desvantagens, o método mais comum de distribuição de certificados e CRL's é a publicação, em que estes são colocados num local facilmente acessível, do conhecimento geral e disponível ao público. O normal é colocar a informação num repositório, que é um termo genérico para referir qualquer base de dados logicamente centralizada, capaz de armazenar informação e disseminá-la quando tal for requerido. Assim, a informação não precisa de ser distribuída individualmente.

Alguns exemplos de repositório são:

– Servidores de "*Lightweight Directory Access Protocol*" (LDAP);
– Agentes de Sistema de Directório X.500 ("*Directory System Agents*" (DSA's));
– "OCSP *responders*" – De referir que este tipo de repositório serve apenas para a informação do estado do certificado (revogado ou não);
– "*Domain Name System*" (DNS) [34];

- Servidores Web em que os certificados e as CRL's podem ser obtidos via HTTP [35];
- "*File Transfer Protocol*" (FTP) [35];
- Bases de Dados corporativas em que estão bem definidas as práticas de gestão de acesso à informação.

Na prática, o tipo de repositórios mais comuns são servidores remotos baseados no LDAP (protocolo standard utilizado para aceder a serviços de directório) e nas recomendações X.500 [36].

A localização de um repositório pode ser comunicada numa página HTML criada para o efeito. Essa página entre outras informações consideradas relevantes para a PKI, poderá apresentar a localização do repositório.

É bastante prática e vantajosa a utilização de um repositório, na medida em que a maioria das organizações têm, de antemão, um sistema de repositório desenvolvido, sendo apenas necessário proceder à integração da informação adicional relacionada com a PKI, na infra-estrutura de repositório já existente. Ao contrário da disseminação privada, em que uma pessoa só trocaria certificados com quem conhecesse, este método permite estabelecer comunicações com toda a gente. Providencia também, uma localização central onde a informação se encontra armazenada, reduzindo bastante a quantidade de certificados e CRL's a guardar. Para além disso, este repositório não precisa de ser seguro, uma vez que, tanto os certificados como as CRL's, são auto-protegidas, havendo uma garantia da sua integridade. Deverá, contudo, haver um controlo de acessos ao repositório para impedir a substituição maliciosa daqueles.

2.6 Entidade Certificadora *vs* Entidade Credenciadora

Embora as designações destas entidades pareçam semelhantes, as suas funções são distintas. A Entidade Certificadora ou Autoridade de Certificação, tem como função emitir certificados digitais, como já foi mencionado.

A Entidade Credenciadora tem uma actividade fiscalizadora. Os seus alvos são as entidades do país que exercem funções de Entidade Certificadora e que pretendem emitir certificados digitais que possuam valor probatório, ou seja, legalmente tenham o mesmo

valor que uma assinatura autógrafa. Estes certificados designam-se de certificados qualificados. Define um conjunto de requisitos pelos quais essas Entidades Certificadoras se devem reger. Possui um conjunto de auditores cuja tarefa é verificarem se a entidade que se está a submeter à auditoria, está em conformidade com os requisitos, *i.e.*, apresenta as condições de segurança física, lógica e humana exigidas.

Estando em conformidade com os requisitos exigidos, as Entidade Certificadoras recebem um atestado da Entidade Credenciadora a garantir que apresentam as condições necessárias para emitir certificados digitais qualificados.

Capítulo 3

Arquitectura para o Ministério da Justiça

Neste capítulo, numa primeira abordagem, far-se-á referência aos pressupostos legais elaborados, tanto no País como na Comunidade Europeia, com o objectivo de legislar sobre matérias tão sensíveis como comércio electrónico, factura electrónica e assinatura digital. Tais matérias careciam de regulamentação uma vez que vieram revolucionar a tradicional forma de estabelecimento de contractos e o valor probatório imposto a uma assinatura. Apresenta-se crucial esta abordagem, uma vez que foi baseado nestes pressupostos legais que o MJ se orientou para tomar a decisão de utilizar a assinatura digital nas suas transacções electrónicas. Inclusivamente, algumas das disposições legais que se irão apresentar, foram redigidas precisamente para legislar a actividade que o ITIJ virá a desempenhar nesta área – a actividade exercida como Entidade Credenciadora.

Dá-se a conhecer a realidade que existia no MJ ao nível das tecnologias da informação, no momento em que foi iniciado este trabalho, concluindo-se que esta não possuía os requisitos suficientes para apelar às necessidades de segurança que surgiam nas transmissões electrónicas. Apresentar-se-ão os componentes que já existiam no MJ e que irão interagir com a infra-estrutura a montar e a adaptação destas àquela ou, eventualmente, o inverso.

Serão também apresentados os objectivos que se pretendem atingir no MJ com a elaboração da PKI. É apresentada uma proposta de PKI apresentando argumentos que fundamentam os requisitos definidos e as opções tomadas.

3.1 Enquadramento Jurídico

A entrada em vigor da *Resolução do Conselho de Ministros nº 60/98, de 6 de Maio*, determinou a existência de um endereço de correio electrónico nos serviços e organismos integrados na administração directa ou indirecta do Estado e regulou o valor a atribuir aos documentos circulados por via electrónica. Com tal Resolução, verificou-se uma tentativa de desburocratizar as relações entre o Estado e os Cidadãos, aproveitando os instrumentos disponibilizados pelas novas tecnologias de informação. Esta Resolução, encontrou formulação legislativa nos artigos 25º e 26º do *Decreto-lei nº 135/99, de 22 de Abril*, que adoptou diversas medidas de modernização administrativa.

Assumiram assim uma grande importância, as formas de comunicação por via electrónica, como meio de facilitação do "diálogo" entre cidadãos e Estado e como factor que potenciava a eficácia do aparelho administrativo. Tal, levou a que fosse disponibilizado um correio electrónico nos vários serviços públicos, paralelamente às formas tradicionais baseadas na presença física, no correio, telefax ou telefone. Aquela Resolução apresentou a necessidade de se poder conferir aos documentos transmitidos via electrónica, o mesmo valor de que beneficiavam os documentos que circulavam em suporte de papel, assegurando o mesmo tratamento. À data da sua entrada em vigor, exceptuavam-se os eventos que exigissem a assinatura ou a autenticação dos documentos electrónicos, até que se adaptasse um diploma que regulasse tal matéria.

O *Decreto-lei nº 290-D/99, de 2 de Agosto*, foi então esse diploma. Nele foi apresentada a assinatura electrónica como meio de obtenção da desejada autenticação dos documentos electrónicos. Tecnologicamente, a actual forma de assinatura electrónica que possui as propriedades de uma assinatura autógrafa, é a assinatura digital, ressalvando o documento outras formas de assinatura tecnologicamente evoluídas, que entretanto possam surgir.

O referido diploma, juntamente com a referida Resolução e com os diplomas sobre a Factura Electrónica (*Decreto-lei nº 375/99, de 18 de Setembro*) e sobre a classificação da informação pública, deu cumprimento ao estabelecido no "Livro Verde para a Sociedade da Informação" [37]. Este livro identificou também a necessidade de se viabilizar e dinamizar o comércio electrónico, como forma de protecção da competitividade das PME's portuguesas. Assim, apresentou o comércio electrónico como sendo uma das vias

a seguir para atingir aquele objectivo, criando, para tal, a "Iniciativa Nacional para o Comércio Electrónico" cujos objectivos foram descritos na *Resolução do Conselho de Ministros nº 115/98, de 1 de Setembro*, sendo um deles a promoção da adopção pela Administração Pública das práticas do comércio electrónico. Este documento também referiu a necessidade do estabelecimento de um regime jurídico aplicável aos documentos electrónicos e assinatura digital, bem como à factura electrónica.

Mas, para conferir à assinatura digital a fiabilidade exigida por todos estes pressupostos legais, havia que criar uma entidade cuja função fosse assegurar os elevados níveis de segurança do sistema, indispensáveis à existência da desejada confiança no que toca às assinaturas de documentos electrónicos.

Assim, o acima mencionado DL 290-D/99, além de regular o reconhecimento e o valor jurídico dos documentos electrónicos e das assinaturas digitais, confiou também o controle da actividade de certificação de assinaturas a uma entidade a designar. Não abordou detalhadamente os pressupostos tecnológicos e operacionais desta actividade, sob pena de se tornar um obstáculo à evolução da técnica e da actividade empresarial de certificação, constando apenas do regulamento, os princípios técnicos a observar nessa actividade. A entidade credenciadora deveria exercer uma função de controle e regulação satisfatória, do ponto de vista ético e que fosse suficientemente flexível, do ponto de vista técnico. Referiu, também, que a actividade de certificação pelas denominadas Autoridades de Certificação, não estava sujeita a autorização administrativa prévia [11].

Foi também elaborado, sob a égide da Equipa de Missão para a Sociedade da Informação, o "Documento Orientador da Iniciativa Nacional para o Comércio Electrónico" *(Resolução do Conselho de Ministros nº 94/99, de 25 de Agosto*). Este Documento, tem como objectivo criar condições para que o desenvolvimento do comércio electrónico seja uma realidade em Portugal contribuindo, dessa forma, para que a competitividade das empresas seja salvaguardada face à concorrência à escala mundial. Refere, para tal, que deve ser assegurado o reconhecimento jurídico, tanto da factura electrónica como da assinatura electrónica e do valor probatório do documento em formato electrónico ao qual lhe tenha sido aposto uma assinatura digital. Esta deverá ser certificada por uma entidade credenciada por uma autoridade pública a designar. Esta Resolução promoveu a elaboração de ante-projectos de diplomas legais, referentes ao regime jurídico dos documentos electrónicos e assinaturas digitais (os já mencionados Decretos-lei 290-D/99 e 375/99).

A autoridade pública, designada de Entidade Credenciadora Nacional, foi definida como sendo o ITIJ, na Lei Orgânica do MJ, aprovada pelo *Decreto-lei nº146/2000, de 18 de Julho*. Posteriormente, na sequência do nascimento desta entidade, foi criado pelo *Decreto-lei nº 234/2000, de 25 de Setembro*, o Conselho Técnico de Credenciação, como estrutura de apoio ao ITIJ no exercício das funções de Entidade Credenciadora.

Relativamente a um quadro geral comunitário para as assinaturas electrónicas, foi redigida a *Directiva 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro*. Chama-se a atenção para o facto de a legislação portuguesa sobre a matéria, ser anterior a este documento, tendo sido tidas em conta, no entanto, as versões preparatórias da Directiva na elaboração do DL português (DL nº 290-D/99), pelo que se antecipa a consagração no direito interno nacional da generalidade das soluções da referida Directiva.

Posteriormente, foi aprovado o "Plano de Acção da Iniciativa Internet" pela *Resolução do Conselho de Ministros nº 110/2000, de 22 de Agosto*, apresentando um conjunto de objectivos a alcançar no que concerne ao uso da Internet pela Administração Pública e pelos cidadãos ao interagirem com esta. Destaca-se, de entre eles, a generalização do comércio electrónico em toda a Administração e a reforma da Central de Compras do Estado para a dinamização da aquisição de bens e serviços via electrónica.

Entretanto, ao nível da Comunidade Europeia, o "Plano de Acção eEurope 2002", adoptado durante a presidência portuguesa do Conselho de Ministros da União Europeia, chama a atenção para as vantagens das práticas do comércio electrónico no seio das Administrações Públicas e aponta a necessidade para o seu desenvolvimento.

A *Resolução do Conselho de Ministros nº 143/2000, de 27 de Setembro*, veio reforçar a necessidade de desenvolvimento do comércio electrónico, definindo um conjunto de medidas para a prática da aquisição de bens e serviços por via electrónica pela Administração Pública.

3.1.1 Enquadramento Jurídico Específico do Ministério da Justiça

Dentro daquela sequência de raciocínio, surgiu o *Decreto-lei nº 183/2000, de 10 de Agosto*, que procedeu à alteração do *artigo 150º do Código de Processo Civil*, de modo a

prever a possibilidade de apresentação em tribunal das peças processuais em suporte digital e o seu envio por correio electrónico. Esta apresentação em suporte digital, será obrigatória a partir de 1 de Janeiro de 2003, sendo facultativa desde a data de entrada em vigor deste diploma, até lá.

A *Portaria nº 1178-E/2000, de 15 de Dezembro*, veio regulamentar os aspectos técnicos desta inovação, apresentando, assim, a obrigatoriedade da aposição de uma assinatura digital quando os actos processuais forem praticados por correio electrónico. Posteriormente, esta Portaria é alterada pela *Portaria 8-A/2001 de 3 de Janeiro*, que veio retirar a obrigatoriedade de o certificado digital ser emitido por uma autoridade de certificação credenciada, uma vez que esta entidade ainda não se encontra no exercício de funções.

De referir que actualmente há um rascunho de um decreto-regulamentar redigido pelo ITIJ, que irá regular o DL 290-D/99, para estabelecer as regras técnicas e de segurança aplicáveis às CA's, estabelecidas em Portugal, na emissão de certificados qualificados.

3.2 Objectivos a Atingir

Foi envolvido neste ambiente de modernização tecnológica e de definição de regras a seguir para se atingir esse objectivo que se fazia sentir na Administração Pública, que o ITIJ se propôs a exercer as funções de CA, desenvolvendo uma PKI.

Há muito que se fazia sentir a necessidade de permitir que as trocas de informação electrónica fossem efectuadas de uma forma que inspirasse confiança, ou seja, que não houvesse o receio da informação ser visualizada ou mesmo alterada. Esta insegurança impedia a utilização deste meio de comunicação em situações que requeressem confidencialidade da informação ou prova da inalterabilidade dos dados enviados. Situações como contratos, processos de contencioso, etc., em que era necessário este tipo de garantias, ficavam à partida eliminadas.

Os Magistrados pretendiam utilizar o correio electrónico como meio rápido e prático de trocar pareceres com os seus colegas, mas, sendo a informação sensível, receavam que ela fosse interceptada ou adulterada, alterando o seu teor. Neste tipo de situações, persistiam

em utilizar o suporte de papel assinado e enviado em envelope selado, para garantir aquelas premissas.

Esta era a principal necessidade (utilização do correio electrónico de forma segura) que se pretendia satisfazer com o desenvolvimento da PKI.

Em segundo plano e aproveitando as várias funcionalidades de um certificado digital, pretendia-se eliminar o arquivo em papel, passando a assinar digitalmente os documentos gerados em suporte electrónico e armazená-los dessa forma.

Também se pretendia começar a aceder aos servidores remotos de uma forma mais segura que a actual: impedir que o actual "*login*" e palavra passe utilizados no acesso fossem transmitidos em claro garantindo que a comunicação pudesse ser cifrada. Pensou-se logo na enorme vantagem que se obteria na introdução dos votos nas legislativas pelos Governos Civis do País, cuja autenticação seria efectuada de forma segura e cujos dados seriam enviados cifrados para o servidor sitiado no ITIJ.

O condicionamento dos acessos físicos dos funcionários a determinados locais, também foi uma funcionalidade de imediato ponderada.

Em 2000, com a entrada em vigor do já referido DL 183/2000, os Tribunais viram-se forçados a receber o correio electrónico assinado digitalmente, confirmando a necessidade da familiarização com esta infra-estrutura para posterior apoio e formação aos funcionários daqueles organismos.

Não foi só aos Magistrados que estas seguranças interessaram. A Polícia Judiciária, ao ter conhecimento da possibilidade da informação poder ser transmitida cifrada, também ficou interessada nesta aplicação.

A intenção do ITIJ foi, de antemão, desenvolver uma PKI que lhe permitisse emitir certificados digitais para todo o Ministério, em lugar de obtê-los a uma CA já existente no mercado. Em termos de estratégia governamental, determinou-se que seria a opção mais viável, não descurando também o facto de ser sua intenção propor-se a Entidade Credenciadora Nacional, função essa que requereria um profundo conhecimento da infra-estrutura de chave pública. Havia, pois, uma grande mais-valia se se tivesse, entretanto, desenvolvido uma.

3.3 Sistema Informático Existente

Quando foram detectadas as necessidades acima referidas, foi feita uma análise à estrutura que na altura estava desenvolvida, depressa se concluindo que esta se encontrava incapacitada para satisfazer aquelas.

Com efeito, a estrutura disponível no ITIJ ao nível de redes e servidores não permitia, por si só, dar resposta às necessidades de segurança apresentadas. Estas não se solucionavam com regras colocadas na "*firewall*" ou opções definidas no gestor de correio ou no "*browser*". Estas necessidades requeriam a integração de uma infra-estrutura com características específicas, na já existente. Como já foi referido, esta infra-estrutura é a PKI. Ela necessita de interagir com vários elementos externos que virão a tornar-se sua parte integrante. São o caso do directório público, do gestor de correio e do "*browser*" utilizados. Assim, a montagem desta infra-estrutura, deve ter em conta a configuração daqueles componentes para se adaptar a eles ou, eventualmente, se possível, adaptá-los a si.

Na Figura 3.1, encontram-se representados os elementos da rede do MJ que estão directamente relacionados com a realização da PKI e que existiam à data do início deste trabalho:

- Na Zona Desmilitarizada (DMZ), estava o servidor Web bem como o "*dispatcher*", conector dos restantes servidores de directório X.500 pertencentes aos restantes sub-domínios do domínio MJ, que permite a distribuição do tráfego pelas várias redes locais;
- Protegida pela "*firewall*" interna, encontrava-se a rede interna onde estava o directório X.500 do sub-domínio ITIJ.

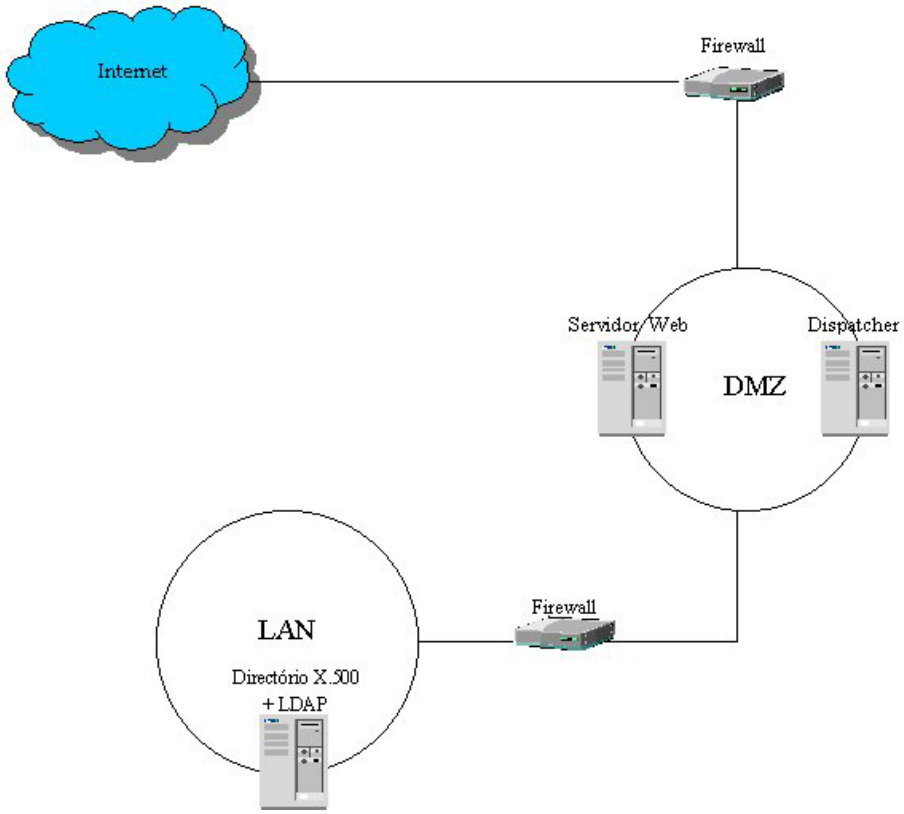

Figura 3.1: Estrutura existente no início do trabalho

A plataforma utilizada em todo o MJ é a Microsoft e os serviços acima referidos não são excepção à regra, utilizando, portanto, Microsoft® Exchange 5.5 Server como directório público, o Microsoft® Outlook® 98 ou 2000 como gestor de correio e o Microsoft® Internet Explorer como "*browser*".

Tendo em consideração a estrutura existente e as aplicações mais usadas, pode então definir-se os seguintes aspectos da PKI:

- O sistema de armazenamento de certificados deverá ser o directório X.500 com acesso via LDAP, de acordo com o referido na secção 2.5.3;
- O gestor de correio deverá reconhecer o protocolo S/MIME (adição de extensões de segurança ao formato de mensagem de correio electrónico MIME) para permitir a troca de correio seguro;
- O "*browser*" deve permitir a utilização de SSL/TLS e SET para comunicações e transacções seguras.

3.3.1 O Directório Exchange

O Microsoft® Exchange 5.5 Server é uma plataforma de correio electrónico que permite a criação, armazenamento, troca e gestão de texto, imagens e voz, através de comunicações em rede [38, 39]. Esta plataforma tem como principais características, uma capacidade de armazenamento ilimitada, uma fiabilidade elevada e possibilita comunicações seguras ao suportar os standards SSL, "*Simple Authentication and Security* Layer" (SASL), S/MIME e assinaturas digitais. Este servidor permite também a interacção com os standards da Internet SMTP, "*Post Office Protocol 3*" (POP3), "*Internet Mail Access Protocol 4*" (IMAP4), LDAP v3 (protocolo de acesso a directórios) e "*Network News Transfer Protocol*" (NNTP), facilitando a conexão e partilha de informação com outros clientes e servidores.

Integrado no Sistema Operativo Microsoft® Windows® NT server 4.0, o Microsoft® Exchange 5.5 Server foi desenhado para corresponder a todas as necessidades existentes na troca de mensagens. Juntamente com o software cliente Microsoft® Outlook® 98 ou 2000, o Exchange permite uma infra-estrutura de troca de mensagens fiável, escalável e de fácil gestão, com um repositório de endereços potente.

A utilização de standards é vital para que determinada tecnologia possa ser reconhecida por outras. Caso não tenha isso em consideração, arrisca-se a estar a isolar-se do mundo. O Exchange usa, então, quatro standards para serviço de mensagens: X.400, X.500, SMTP e MAPI.

3.3.2 Gestor de Correio Outlook

O Microsoft Outlook é um gestor de correio electrónico, para além de ter outras funcionalidades como um calendário com programação de tarefas e informação pessoal como Contactos e Tarefas, ajudando a organizar, procurar e visualizar toda esta informação, numa só aplicação [40].

Em conjunto com o Microsoft Exchange Server, desempenha funcionalidades avançadas como replicação e sincronização das pastas de correio electrónico, contactos, calendário e pastas públicas, incluindo páginas Web associadas e informação pessoal.

O Outlook 2000, actualmente o mais utilizado no MJ, está preparado para suportar standards da Internet como SMTP e POP3; IMAP4; "*Dynamic*" HTML; NNTP, bem como S/MIME e LDAP, os que interessam directamente ao PKI.

Com o S/MIME, os utilizadores podem enviar e receber mensagens assinadas e/ou cifradas. A gestão das chaves públicas e respectivos certificados é partilhada com o Internet Explorer.

O LDAP permite um grande desempenho no acesso ao directório público na procura e verificação de contas de correio electrónico. Importando referir, no entanto, que o Outlook não permite a visualização no "Livro de Endereços Públicos" dos certificados com as chaves públicas correspondentes às contas de correio electrónico aí apresentadas.

Há uma outra fraqueza a referir se compararmos o Outlook com o Outlook Express: não pesquisa as CRL's de forma on-line, situação que se tornaria mais confortável na pesquisa de certificados revogados.

3.3.3 "*Browser*" Internet Explorer

O Internet Explorer é a plataforma que permite a navegação na Internet com um conjunto de capacidades que inclui a reprodução de multimédia e redimensionamento automático de imagens para utilizadores finais. Permite a utilização de standards como SSL/TLS que utilizam certificados digitais para o estabelecimento de canais seguros [41].

Possui de raiz, entre outras coisas, uma lista de certificados de "*root*" CA's mundialmente reconhecidas como tal para prevenir os utilizadores da instalação de software não recomendado.

3.4 Proposta de Modelo para a PKI

Feita a análise das necessidades existentes e dada a complexidade de algumas delas, decidiu-se atribuir-lhes uma ordem de prioridades para se proceder à sua concretização. Assim, determinou-se que numa primeira fase ir-se-ia preparar a PKI para permitir enviar

correio assinado/cifrado, bem como assinar/cifrar documentos. Seguidamente, criar-se-ia uma política de certificados que permitisse também utilizar o SSL. Mais tarde, quando esta fase estivesse terminada, integrar-se-ia na estrutura uma TSA com o intuito de reforçar a propriedade de não repúdio (ver desenvolvimento em Capítulo 6). Posteriormente, utilizar-se-ia esta infra-estrutura para acessos a locais físicos, e cartão de ponto, eventualmente combinados com técnicas de biometria.

Esboçou-se então a estrutura que se considerou ideal para dar resposta às necessidades do MJ.

3.4.1 Arquitectura da PKI

Assim, face a esta ordem de prioridades e ao objectivo pretendido (emissão de certificados digitais para todo o MJ), foi definida uma PKI com os seguintes elementos:

- Uma root CA;
- Uma sub CA;
- Uma RA;
- Um sistema de directório público com acesso LDAP;
- Uma impressora de smart cards.

Optou-se por utilizar uma sub CA pela razão de mais tarde poder-se sentir a necessidade de descentralizar o serviço de emissão de certificados, distribuindo geograficamente sub CA's, com as respectivas RA's a si conectadas. Tal necessidade poderá surgir quando a infra-estrutura estiver montada e a produção de certificados, bem como os restantes serviços a ela associados, se encontrarem em velocidade de cruzeiro. Assim sendo, preparou-se de imediato a PKI para esse fim, definindo-se uma root CA que se encarregará da emissão de certificados para as CA's suas subordinadas e da revogação das suas chaves públicas emitindo, por conseguinte, ARL's (ver secção 2.4.2.1).

Existindo uma sub CA responsável por todo o ciclo de certificação, a root CA pode perfeitamente estar off-line e colocada num local físico seguro, aumentando a segurança do topo da hierarquia da PKI. Tal decisão é considerada bastante sensata dado que caso esta seja comprometida, porá em causa toda a estrutura, obrigando a que toda a PKI seja refeita. Estando off-line não haverá o perigo de um "*hacker*" conseguir aceder-lhe através da rede, obtendo o seu certificado e corrompendo-o ou mesmo substituindo-o por outro da

sua autoria permitindo-lhe validar uma estrutura criada por si. Estando inclusivamente colocada num local seguro de acesso condicionado aos operadores da CA, assegurar-se-á a sua segurança a nível interno também.

Optou-se também por associar uma RA por sub CA para registar os utentes, descentralizando o serviço da sub CA. Assim, esta não tem de se preocupar com a parte administrativa da actividade, dedicando-se somente à parte técnica. É uma forma de reduzir custos operacionais e aumentar a escalabilidade.

Presentemente é esta a estrutura que se pretende executar, uma RA por sub CA, distribuídas geograficamente por pontos estratégicos do país. Não está, no entanto, posta de parte a opção de ter várias RA's ligadas a uma sub CA. Aquelas encontram-se distribuídas geograficamente, sendo o processo de certificação efectuado remotamente por uma sub CA centralizada.

A impressora de smart cards vai estar ligada à sub CA. Além de imprimir a face do cartão, vai desencadear o processo de geração das chaves privadas no "*chip*" do cartão. A explicação para a opção do smart card como dispositivo de armazenamento das chaves privadas é apresentada na secção 3.4.3.

Tendo em consideração a estrutura existente no ITIJ apresentada na Figura 3.1, determinou-se que os novos elementos a integrar, deveriam ser dispostos de acordo com a estrutura representada na Figura 3.2.

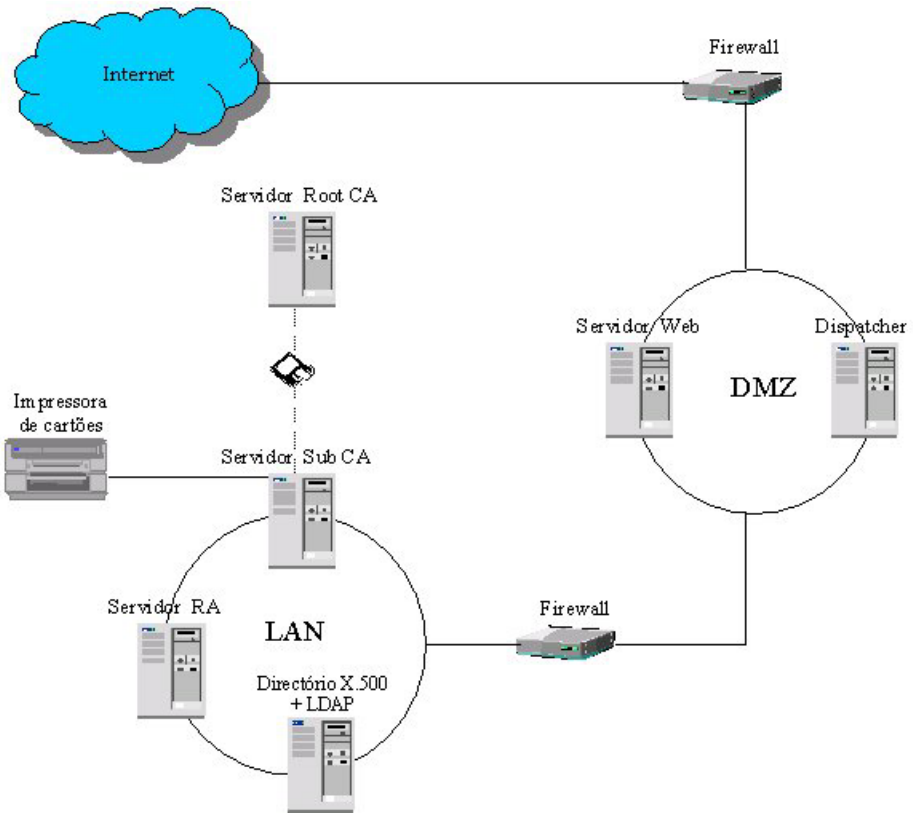

Figura 3.2: Arquitectura da PKI

A escolha da disposição apresentada na figura, deve-se às seguintes razões:

- A root CA encontra-se nas instalações do ITIJ e está desligada da rede pelas razões indicadas atrás;

- Os servidores sub CA e RA ficam colocados na rede interna do ITIJ protegidos pela "*firewall*" interna, para aumentar a sua protecção contra ataques externos. É aí também que já se encontra o servidor do directório X.500 do sub-domínio ITIJ, onde já se encontram publicadas as contas dos utilizadores da rede do MJ;

- Os certificados digitais são publicados no Directório X.500 no respectivo sub-domínio a que pertencem os seus titulares. Assim, caso não pertençam ao sub-domínio ITIJ, serão enviados para o "*dispatcher*", encarregando-se este de os distribuir pelos sub-domínios correspondentes. Relativamente às CRL's, elas são publicadas numa página da Intranet. Nessa página também se encontram acessíveis para descarga os certificados da root CA e da sub CA;

– Para que aqueles certificados e CRL's fiquem acessíveis na Internet, é colocada uma cópia deles no servidor Web localizado na DMZ. Também são armazenados nesse servidor os certificados da root CA e da sub CA.

3.4.2 Armazenamento dos Certificados de Raiz

Há um pormenor que se poderá tornar incómodo para utilizadores menos experientes nesta área da certificação digital. Como se decidiu que a CA não seria colocada em nenhuma hierarquia de CA's já existente e reconhecida pelos "*browsers*", tal requererá a necessidade de os receptores procederem à descarga, uma única vez, dos certificados da root CA e da sub CA, de forma a estabelecer-se a correcta hierarquia até ao certificado do utilizador (ver Figura 3.3), havendo um reconhecimento automático da validade da assinatura digital. Caso tal acção não seja efectuada, arriscam-se a receber uma mensagem avisando que a CA que emitiu aquele certificado não é fidedigna (ver Figuras 3.4 e 3.5).

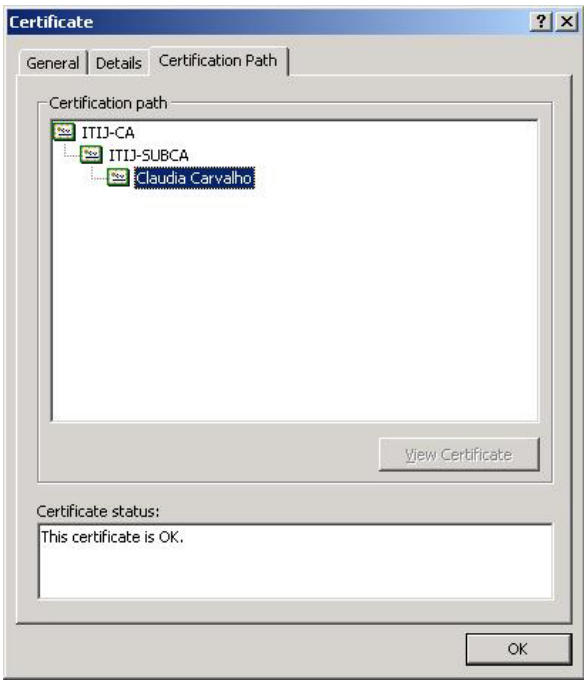

Figura 3.3: Cadeia válida de certificação

Apenas os utilizadores do MJ têm acesso à página de pedido de emissão/renovação de certificados, aos certificados reais da root CA e da sub CA e às CRL's reais. A Internet

tem acesso a uma réplica, colocada via FTP no servidor Web, das CRL's para verificação do estado dos certificados, e dos certificados da root CA e da sub CA para reconhecimento da hierarquia de certificação. Para tentar proteger os certificados da sub CA e da root CA aí colocados, definiu-se como única porta aberta a 80 (HTTP) e o sistema de directórios no qual as páginas web se encontram, estão protegidos contra a escrita, tendo o atributo de "*read-only*". Não obstante todas estas medidas de segurança, decidiu-se mensalmente ir à própria root CA exportar uma cópia do seu certificado e colocá-la, tanto na RA como na página Web.

Mais tarde, quando a linha de produção estiver terminada e em acção, tenciona-se pôr a hipótese da utilização de certificação cruzada (*vide* 2.5.1.2) com outras CA's em que o ITIJ venha a confiar.

Figura 3.4: Inexistência de cadeia de certificação

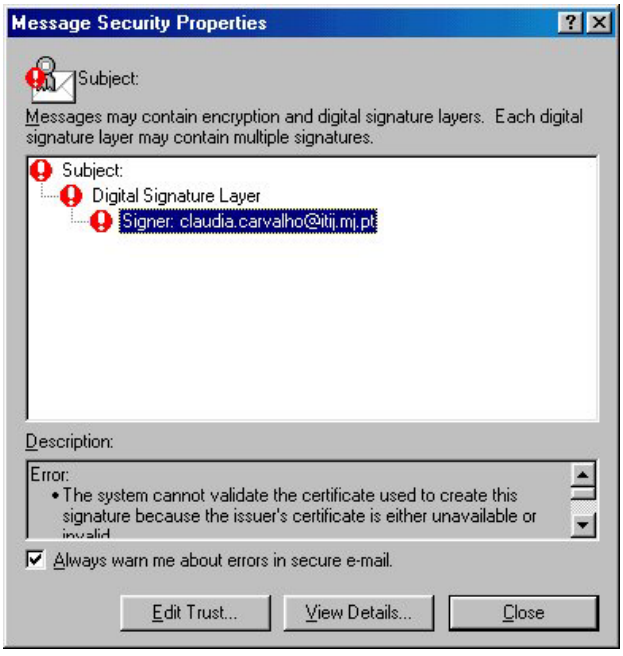

Figura 3.5: Detalhe do erro de inexistência de cadeia de certificação

3.4.3 Armazenamento das Chaves Privadas

Tal como foi discutido no Capítulo 2, existem diversas possibilidades para colocação da chave privada e do certificado pessoal, entre elas o "*USB token*" e o smart card. A opção de colocação da chave privada no disco rígido foi logo eliminada por falta de segurança, pois, já não falando da possibilidade de ataques externos à máquina, numa estrutura como a do MJ que está em rede, todos os utilizadores podem entrar em todas as máquinas desde que estas pertençam ao seu domínio. Desta forma conseguem aceder a todo o conteúdo do disco, embora estando num perfil diferente do dono da máquina. O disco também é susceptível de ser infectado com vírus e é bastante propenso a avarias com eventuais perdas de informação, havendo no MJ apenas política de "*backups*" para servidores.

Verificando-se que presentemente no MJ ainda existem máquinas sem porta USB e antevendo a utilização dos certificados para inúmeras situações, nomeadamente controlo de acessos, optou-se pelo smart card que poderia também funcionar como cartão de identificação do MJ. Num smart card o acesso às chaves privadas encontra-se condicionado pela introdução de um PIN que, a ser introduzido incorrectamente três vezes seguidas, bloqueia o cartão.

Alguns algoritmos de cifra assimétrica, nomeadamente o RSA, permitem que o mesmo par de chaves possa ser usado quer para assinar, como para cifrar. Mas para garantir o não repúdio de uma mensagem assinada, a CA não poderá fazer "*backup*" da chave privada. Caso contrário, em caso de litígio, o titular da chave poderia alegar que alguém com acesso à CA tinha utilizado a sua chave para assinar determinada mensagem fazendo-se passar por ele. Mas esta regra imposta à CA, impedirá garantir a decifra dos documentos ou mensagens cifrados. Esta decifra, como já foi referido, faz-se com a chave privada e caso esta seja perdida pelo seu titular, não haverá hipótese de a recuperar ficando os documentos cifrados irremediavelmente perdidos.

Para eliminar este dilema, optou-se por adoptar o modelo designado de "*Dual-Key Pair*", ou seja, decidiu-se atribuir dois pares de chaves a cada utilizador, um para assinar e outro para cifrar, por forma a poder-se guardar a chave privada de cifra. A chave privada de assinatura encontra-se na posse do seu titular guardada no smart card e a de cifra tanto se encontra na posse do seu titular, como é guardada uma cópia daquela nas bases de dados da CA. Adoptando este modelo, pode-se garantir com toda a certeza que, apenas quem esteve na posse do cartão e conhecia o PIN, poderia ter assinado determinado documento.

O titular do cartão não é desresponsabilizado pelos actos efectuados, pois deve manter o PIN secreto e em caso de extravio do cartão, deve pedir de imediato a revogação do certificado.

3.4.4 Publicação dos Certificados Digitais

A publicação das chaves públicas e respectivos certificados, será efectuada via LDAP utilizando a estrutura "*Exchange*" já existente no MJ. Esta é a solução mais viável, uma vez que toda a estrutura de directório X.500 já está montada, bastando pesquisar no LDAP o utilizador em questão e gravar no atributo correcto o seu certificado digital com a correspondente chave pública.

Os certificados e respectivas chaves públicas são publicados no servidor "*Exchange*" do sub-domínio onde estão localizadas as respectivas contas dos seus titulares, havendo depois uma replicação para os servidores "*Exchange*" dos restantes sub-domínios do MJ [42]. Assim, todos os funcionários têm acesso à mesma informação. É claro que a replicação não é instantânea, havendo um período de tempo em que determinado certificado já está replicado nuns servidores e não noutros. Tal demora na replicação não se apresenta preocupante aquando o envio de uma mensagem assinada, uma vez que esta leva apenso o certificado e correspondente chave pública do seu emissor. Naquele momento, para aquela mensagem, o receptor fica detentor da chave pública que lhe irá permitir verificar a assinatura da mensagem. Apenas se sentirá necessidade de aceder ao certificado e à chave pública de determinado utilizador, caso se pretenda enviar-lhe uma mensagem cifrada.

Como alternativa à obtenção da chave pública no directório público, pode-se armazenar localmente os certificados que chegaram juntamente com as mensagens assinadas. Esse receptor ficará na posse da chave pública daquele emissor, podendo fazer uso dela quando pretender enviar-lhe mensagens cifradas.

Há apenas a referir que eventuais alterações ao certificado (sua actualização/renovação), irão transparecer automaticamente no directório, situação que não acontecerá com aquele guardado no PC.

3.4.5 Pedido de Emissão do Certificado Digital

Em relação ao pedido de emissão de certificados, determinou-se que não seria necessária a apresentação presencial do titular. Tal justifica-se com o facto de os dados pessoais do requerente poderem ser facilmente confirmados por acesso à Base de Dados do Arquivo de Identificação Civil, na posse do ITIJ. O endereço de correio electrónico apresentado, poderá ser confrontado com o existente no directório público e ao qual todo o Ministério tem acesso. Acedendo à Base de Dados das Remunerações, poder-se-á confirmar o cargo do titular, bem como o organismo a que pertence.

O pedido de emissão do certificado será realizado pelo futuro titular, via web ou correio electrónico, através do preenchimento de um formulário com os dados identificativos do requerente, sujeitos a posterior verificação por parte da RA. Desta forma é definido o seu Nome Distinto garantindo a unicidade do certificado.

O pedido via correio electrónico foi idealizado por se pensar na hipótese de surgir a necessidade de pedir um certificado não tendo, naquele momento acesso à Intranet do MJ. A intenção não é o requerente colocar os seus dados no corpo da mensagem, mas sim preencher um formulário com uma configuração idêntica à do formulário apresentado via Web, enviado pela RA após solicitação do seu envio por parte do requerente e que quando recebido por aquela, os procedimentos a executar sejam idênticos aos da forma web.

Para uma identificação inequívoca do requerente, definiu-se que o formulário conteria os seguintes dados:

- Nome do titular;
- Nome do titular para impressão no cartão;
- Número de bilhete de identidade para identificação única do titular e posterior acesso à base de dados do Arquivo de Identificação Civil para confirmação dos dados introduzidos;
- Número de contribuinte por ser a chave de acesso da base de dados de remunerações do MJ elaborada e em poder do ITIJ;
- Organismo e departamento onde trabalha;

- Categoria profissional;
- Correio electrónico pessoal;
- Endereço da residência para posterior envio do PIN para aumento da segurança;
- Fotografia para impressão na face do smart card – Este campo é de preenchimento facultativo, pois sabe-se que nem todos os serviços dispõem de digitalizador de imagens ("s*canner*"), sendo enviada uma fotografia tipo passe aos Operadores de RA, procedendo eles à sua digitalização.

Determinou-se que a criação dos pares de chaves seria realizada pela própria sub CA em lugar de estas serem geradas no lado do cliente e posteriormente a chave pública ser enviada à CA para associação de um certificado. Tal opção deveu-se ao facto de a maior percentagem da população alvo da PKI do MJ, serem magistrados que pretendem tecnologias eficazes, que resolvam os seus problemas, mas que sejam o mais práticas possíveis e estejam prontas a entrar em funcionamento. Como a maioria dos técnicos de informática encontram-se concentrados no ITIJ havendo poucos espalhados pelos vários Organismos, tal tarefa, não sendo realizada pelo próprio utilizador, iria requerer um grande dispêndio de horas/homem àqueles técnicos, que de antemão, encontram-se adjudicados a muitos outros serviços. Também o facto de o MJ ter uma grande multiplicidade de versões de sistemas operativos e de máquinas, requereria que o software a instalar nos utilizadores se encontrasse preparado para tão grande diversidade. Concluiu-se que centralizando a criação dos pares de chaves num só ponto estabilizaria muito mais rapidamente a aplicação.

Assim, determinou-se que a melhor opção seria, de facto, transferir todas as tarefas para a CA, ficando apenas do lado do cliente aquelas que de todo não pudessem ser realizadas naquela.

Uma das questões que se poderia levantar com este procedimento seria a existência de idoneidade, sobretudo da equipa da RA, por ser ela quem valida os dados dos pedidos de emissão de certificados, e recearem-se tentativas de falsificação dos certificados e personificação de titulares. Tal situação no entanto foi salvaguardada pois, aquando do envio da mensagem assinada, há uma comparação entre o endereço de correio electrónico apresentado no certificado e aquele pelo qual se está a enviar a mensagem. Por outro lado, quem cria as contas dos utilizadores será uma equipa diferente daquela que irá emitir os

certificados, dificultando ou mesmo eliminando alguma tentativa de fraude. O próprio "*Exchange*" impede a criação de uma conta com um endereço de correio já existente. Caso se crie uma falsa conta de utilizador com um falso endereço para um utilizador já existente, tal será descoberto mais tarde por confrontação com o verdadeiro DN. Também há que referir que todas as acções desempenhadas pelo Administrador de RA serão assinadas impedindo posterior repúdio.

Capítulo 4

Pormenores de Concretização da Arquitectura

Feito o levantamento das necessidades e o estudo conceptual da estrutura, estavam reunidas as condições para se dar início aos trabalhos de desenvolvimento da PKI.

Primeiramente, havia que esquematizar numa proposta os requisitos definidos para a PKI do MJ. Posteriormente, face a análise efectuada às várias propostas apresentadas, escolher aquela que mais se adequasse às exigências estabelecidas. Finalmente iniciar o desenvolvimento do projecto com a solução escolhida.

Neste capítulo começar-se-á por apresentar os requisitos que se definiram e se apresentaram às empresas, para o caso específico do MJ. Depois apresentar-se-á a solução escolhida, justificando a decisão. Far-se-á uma descrição sumária dos elementos que compõem a estrutura adquirida e como eles se relacionam entre si.

Também se irão referir algumas alterações ao modelo inicialmente definido, por se verificarem algumas irregularidades que também aqui se apresentarão.

4.1 Modelo Adoptado

Feito o estudo do que se pretendia obter com o desenvolvimento de uma PKI e definidas as características desejadas para ela, chegou o momento de escolher no mercado aquela que correspondesse aos requisitos definidos, a saber:

1. Root CA off-line;
2. Uma sub CA mas com a estrutura preparada para posteriormente poderem haver mais;
3. Uma RA;

4. Uma impressora de cartões que permita a impressão a cores de uma fotografia e a gravação das chaves e certificados no "*chip*";

5. Ser uma estrutura escalável – A escalabilidade é uma característica importante pois, à medida que a PKI aumenta, é essencial que o seu sistema se possa expandir, por forma a acompanhar esse crescimento. Numa primeira fase, a PKI pode suportar apenas uma aplicação, devendo, contudo, estar preparada para suportar um número crescente de aplicações. Deve ser possível adicionar mais sub CA's e respectivas RA's. Também deve suportar o crescente número de certificados emitidos bem como, eventualmente, uma variedade de tipos de certificados e de mecanismos de registo;

6. Pedido de emissão do certificado efectuado em formulário via web ou correio electrónico cujos dados sejam automaticamente colocados na cadeia de procedimentos da RA para validação dos dados por parte do Operador da RA;

7. Haver uma distinção entre as figuras Administrador de CA, Administrador de RA, Operadores de CA e Operadores de RA para, em caso de fraude, ser possível o posterior apuramento de responsabilidades;

8. Instalação do software cliente pelo próprio utilizador, ou seja, efectuada a partir de um "*kit*" composto por um CD com o software de instalação preparado para várias plataformas (Windows 95, 98, NT e 2000), manual de instalação e leitor de smart card adequado a PC ou a Portátil;

9. Publicação dos certificados no directório público do MJ através de LDAP;

10. Utilização de CRL's para verificação do estado dos certificados (válido/revogado);

11. Assinatura/cifra de documentos e de mensagens de correio electrónico e estabelecimento de canais seguros através de SSL [43];

12. Emissão de certificados para servidores Web;

13. Emissão de dois pares de chaves por titular, um para assinar e outro para cifrar;

14. Elaboração de um serviço que permita a replicação parcial do directório público, disponibilizando os certificados e respectivas chaves públicas na Internet;

15. Utilização de smart cards para armazenamento seguro da chave privada dos titulares;

16. Elaboração dos documentos CP e CPS.

Estes requisitos foram apresentados a empresas convidadas pelo ITIJ, para elaboração de uma proposta baseada naqueles e que desse resposta aos serviços pretendidos. As Empresas concorrentes apresentaram soluções de PKI da Baltimore, da Microsoft e da Safelayer.

Feito o estudo das várias propostas, houve uma delas que se destacou das restantes pelo facto de apresentar uma estrutura bem delineada com todos os elementos acima referidos. Essa proposta foi a da KeyOne da Safelayer [44, 45].

4.2 Concretização da PKI

O sistema KeyOne foi desenhado para gerar e gerir certificados digitais que reconhecem protocolos e standards, tais como SSL, X.509, S/MIME e PKCS. A arquitectura é flexível e escalável e permite o desenvolvimento de diferentes módulos de certificação providenciando os meios para:

- Assinar digitalmente código de programa;
- Assinar digitalmente mensagens de correio electrónico;
- Cifrar informação;
- Garantir a identidade do servidor e do utilizador.

A CA pode ser configurada para funcionar com dois modos distintos de operação: o off-line e o on-line. Há que referir que o modo off-line não significa obrigatoriamente estar a operar com a CA desligada da rede. Significa sim que há uma divisão distinta entre os serviços realizados por aquela e pela RA, requerendo a intervenção dos operadores aquando a transferência de dados de um servidor para outro.

A cada um destes modos, corresponde um módulo com componentes distintos. No modo off-line, os componentes da CA e da RA são completamente separados e a comunicação entre eles é feita através de ficheiros batch que são colocados numa disquete, por exemplo, fazendo-se desta forma a transacção da CA para a RA e vice-versa. Tal possibilita o desenvolvimento de uma PKI onde a CA se encontra isolada e opera sem estar conectada a uma rede, aumentando a segurança, como já foi referido anteriormente.

No modo on-line comunicam entre eles não necessitando da intervenção de um administrador. Tal pode tornar-se mais conveniente, embora requeira que a CA e a RA tenham de comunicar directamente através de uma rede, que potencialmente pode vir a ser atacada.

Ponderadas as diferenças dos dois modos de operação, o ITIJ acabou por optar por uma CA a funcionar em modo off-line. A PKI ficou então com os seguintes componentes:

- KeyOne CA;
- KeyOne RA;
- Private Secure Store;
- KeyOne WEB (componente da RA);
- Scryptor;
- KeyOne Toolkits;
- KeyOne Desktop.

KeyOne CA

Este elemento corresponde à CA e o acesso aos seus serviços é feito em modo off-line através da troca de ficheiros batch de input e de output. Esta troca de ficheiros pode ser efectuada através de um conjunto diverso de métodos, nomeadamente uma directoria partilhada, sessões TCP, correio electrónico e disquetes.

O processo efectua-se da seguinte forma: A CA recebe um ficheiro batch contendo um conjunto (lote) de pedidos de certificação ou de revogação. Uma vez aceites, os lotes são processados, sendo gerados os certificados X.509 e as chaves em formato PKCS#12 (formato portátil para guardar a chave privada), se tal formato for definido. É então enviado um ficheiro batch à RA que permitirá a esta publicar os certificados emitidos. A KeyOne CA tem sempre um "*Private Secure* Store" (PSS) (*vide* explicação mais abaixo) associado, para guardar os certificados, as chaves privadas e as CRL's. Opcionalmente, tem um dispositivo PKCS#11 (dispositivo criptográfico, por exemplo, o smart card, o USB Token ou o HSM, definido por uma tecnologia de interface de programação, designada de Cryptoki) associado a si, de modo a guardar neste as suas chaves privadas em vez de estas serem guardadas no PSS [46].

É conveniente frisar que é adquirido um componente KeyOne CA por cada CA existente na PKI. Assim, no caso do ITIJ serão necessários dois KeyOne CA.

KeyOne RA

Este elemento corresponde à RA. Tem como funções:

- Receber e guardar os pedidos de certificação e revogação;
- Aprovar ou negar esses pedidos;
- Elaborar ficheiros batch com aqueles para envio à CA para serem processados por esta;
- Receber os ficheiros batch processados pela CA;
- Publicar os certificados e as CRL's emitidas.

Private Secure Store

A sua principal função é providenciar uma área segura para se armazenarem os certificados, as CRL's e a informação considerada sensível, tal como as chaves privadas. Guarda também o historial das chaves permitindo que se decifre a informação cifrada com chaves expiradas. O PSS pode ser guardado em disco, em smart card, ou em HSM, sendo todo o seu conteúdo assinado e cifrado.

KeyOne Web

É o módulo de conexão responsável pela construção de páginas HTML que permitem o acesso aos serviços oferecidos pela KeyOne RA através de uma "*Common Gateway Interface*" (CGI). Estas páginas permitem ao utilizador final fazer os seus pedidos de certificação, visualizar as CRL's, CPS e CP's e descarregar o certificado da CA, para estabelecimento da hierarquia.

Scryptor

É uma linguagem interpretada que permite fornecer capacidades criptográficas, acessos a bases de dados SQL, conexão HTTP, SMTP e LDAP, acesso ao "*registry*" do Windows NT/2000 e aos ficheiros de sistema. Esta linguagem é a responsável por toda a flexibilidade e capacidades desta PKI, permitindo, inclusive, personalizações daquela de acordo com as exigências do seu adquirente. É utilizada na personalização dos vários módulos da aplicação KeyOne.

KeyOne Toolkits

Cada uma das ferramentas apresenta meios para os programadores integrarem funcionalidades PKI tanto na aplicação cliente como na servidor.

KeyOne Desktop

É uma aplicação do lado do cliente que é integrada com o explorador do Windows permitindo cifrar, decifrar, assinar e verificar a assinatura de ficheiros.

4.2.1.1 Personalização dos Módulos

Os vários elementos que integram a PKI da KeyOne permitem diversas formas de configuração, sendo assim necessário escolher as opções que melhor se adaptavam às necessidades da PKI do MJ. Umas já vinham pré-definidas pela empresa fornecedora, outras foram efectuadas pelo ITIJ.

Relativamente ao modo de funcionamento das CA's optou-se pelo modo off-line, como já foi referido. A root CA encontra-se desligada da rede, sendo a comunicação efectuada através de disquetes. Relativamente à sub CA, troca ficheiros batch via uma directoria partilhada com a RA. Embora ambas as máquinas (sub CA e RA) estejam ligadas em rede, definiu-se a arquitectura off-line, pois pretendia-se fazer uma separação integral das tarefas das duas equipas.

Os certificados digitais que contêm as chaves públicas emitidas, são publicados internamente via LDAP no Exchange e externamente via Web.

As chaves privadas de assinatura dos utilizadores não estão a ser guardadas no PSS, para garantir a propriedade do não repúdio. Estão unicamente a ser guardadas num dispositivo PKCS#11**,** que no caso do ITIJ é o smart card (ver Figura 4.1). Este smart card encontra-se em poder do titular do certificado digital.

Definiu-se que em relação às chaves privadas de cifra seria gerado o formato PKCS#12, para que a CA tivesse capacidade para disponibilizar a chave privada de cifra, através de uma disquete, por exemplo, em caso de solicitação desta por parte do seu titular. A chave privada de cifra tanto se encontra guardada no smart card do seu titular, como no PSS.

Figura 4.1: Aparência do smart card personalizado do ITIJ

Os leitores de smart card escolhidos tanto para PC's como para portáteis, encontram-se representados nas Figuras 4.2 e 4.3, respectivamente. O leitor a utilizar em PC's (ver Figuras 4.2 e 4.4) liga o seu cabo de transmissão de dados a uma porta série RS232 e liga o cabo de energia à porta PS2 do rato ou do teclado. No caso dos portáteis, por uma questão de comodidade, optou-se por leitores que se inserem na porta PCMCIA (ver Figuras 4.3 e 4.4).

Figura 4.2: Leitor para PC

Figura 4.3: Leitor para portátil

Figura 4.4: Leitor para PC's e leitor para portáteis

A chave privada da root CA está guardada num HSM (ver Figura 4.5), adquirido à nCipher designado de nShield [31], sendo o acesso a este efectuado através de uma chave dividida ("*split key*"), em que se utilizam duas partes de um grupo de quatro. As várias partes da chave encontram-se guardadas em smart cards com PIN designados de *Cartões de Operador* ("*Operator Cards*"), sendo distribuídos pelos operadores da CA [47]. Teoricamente, terão de estar presentes dois deles para que se possa aceder à CA. De igual forma a chave privada da sub CA está guardada num HSM, verificando-se os mesmos procedimentos acima referidos. Foram, pois, adquiridos dois HSM's.

O PSS está a ser guardado de forma cifrada no disco, embora o seu acesso esteja a ser feito com a protecção do HSM onde se obtém a sua chave de decifra. Existem dois PSS's, um por cada CA.

Figura 4.5: HSM interno com ligação à porta SCSI

Embora a Safelayer possua a aplicação KeyOne Desktop, tal não fazia parte do pacote apresentado pela Empresa fornecedora da PKI, tendo sido apresentada em sua substituição, a aplicação SmartSignature da Bull. Esta desempenha as mesmas funções, ou seja, assina e cifra documentos, bem como verifica a assinatura de documentos assinados e decifra documentos cifrados. Permite também o designado "Apagar seguro" em que o documento apagado através desta aplicação não poderá ser posteriormente recuperado.

O SmartWin foi uma aplicação adicional que foi incluída no pacote tendo como função substituir o "*login*" do Sistema Operativo pelo do PIN do smart card. Tal requer a presença deste no leitor de smart cards e o conhecimento do código do PIN, o que representa um reforço da protecção do conteúdo da máquina.

4.2.1.2 Processo de Emissão do Certificado

O processo de emissão de um certificado é iniciado através do pedido de emissão deste por parte do requerente, funcionário do MJ. Este preenche um formulário com os seus dados pessoais através de uma página Web desenvolvida pelo módulo KeyOne Web (ver Figura 4.6).

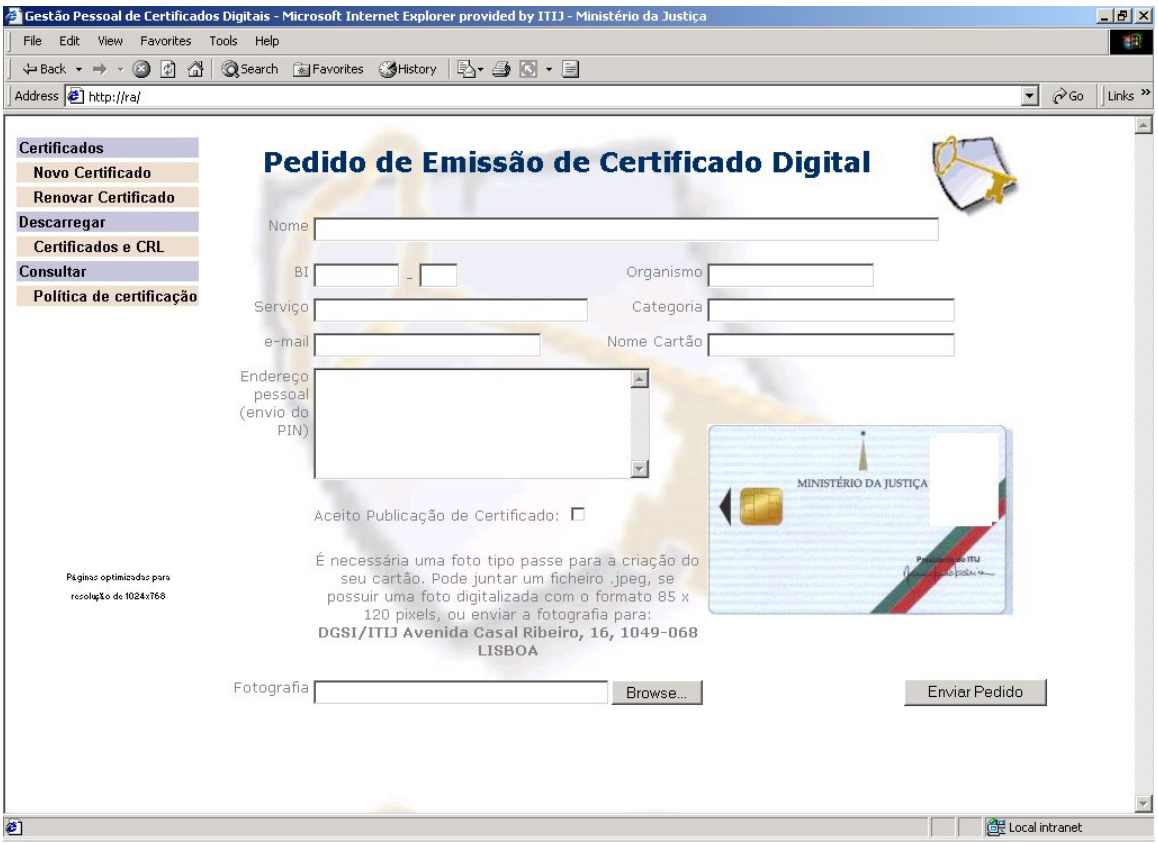

Figura 4.6: Formulário de pedido de emissão de um certificado

Como se pode verificar, houve uma ligeira alteração nos campos constituintes do formulário, relativamente ao que originalmente se havia definido (ver secção 3.4.5). Tal deveu-se ao seguinte: Devido ao problema do cruzamento da informação, o número de contribuinte (NIF) e o número de bilhete de identidade, não poderão pertencer à mesma Base de Dados, pois permitem a interligação de dados judiciais com dados fiscais, proibida pelo Registo Nacional de Protecção de Dados (RNPD). Assim, eliminou-se o campo NIF e já não haverá comparações com os dados da Base de Dados das remunerações.

O número de bilhete de identidade encontra-se no formulário para que haja um campo numérico único que permita servir de chave de acesso a bases de dados auxiliares, mas foi posta de parte a ideia de aceder ao Arquivo Civil pois, embora este seja gerido pelo ITIJ, é propriedade da DGRN. Também de acordo com a Jurista do ITIJ, o RNPD não permite a interligação de Bases de Dados cujos dados sejam pessoais.

Devido ao facto de neste formulário surgir o campo Endereço pessoal, há que informar o RNPD de tal situação, referindo o porquê da existência daquela Base de Dados e havendo um compromisso de que tal Base de Dados não será utilizada para outros fins que não os referidos.

A página com o formulário, só é acessível dentro da rede pelo que, caso se pretenda solicitar a emissão de um certificado digital estando-se fora desta, poder-se-á fazê-lo via correio electrónico requerendo esse formulário. Este, quando da recepção por parte do gestor de correio da RA, será de igual forma colocado em lista para processamento pela KeyOne RA. Os campos são todos obrigatórios excepto o da fotografia digitalizada com o tamanho solicitado, para posterior impressão no smart card. Se não se preencher este campo, ter-se-á de enviar à RA, uma fotografia tipo passe, para que esta proceda então à conclusão do preenchimento do formulário.

O processo de um pedido faz-se de acordo com o diagrama da Figura 4.7. Os pedidos são descarregados ficando no estado *Pendentes*, caso o campo *Fotografia* se encontre preenchido. Senão, encontrar-se-ão numa fase anterior a aguardar a colocação daquela pelo operador de RA. Será no estado *Pendentes* que os dados serão conferidos e verificada a identidade do requerente. Validada a identificação daquele, é remetido o pedido de emissão à sub CA. A RA poderá, caso detecte alguma irregularidade, negar o pedido, justificando o motivo, ficando o evento registado no histórico no estado *Negado*. Poderá, também, proceder à correcção dos campos preenchidos, quando detectar ligeiras incorrecções que não põem em causa a identidade do requerente.

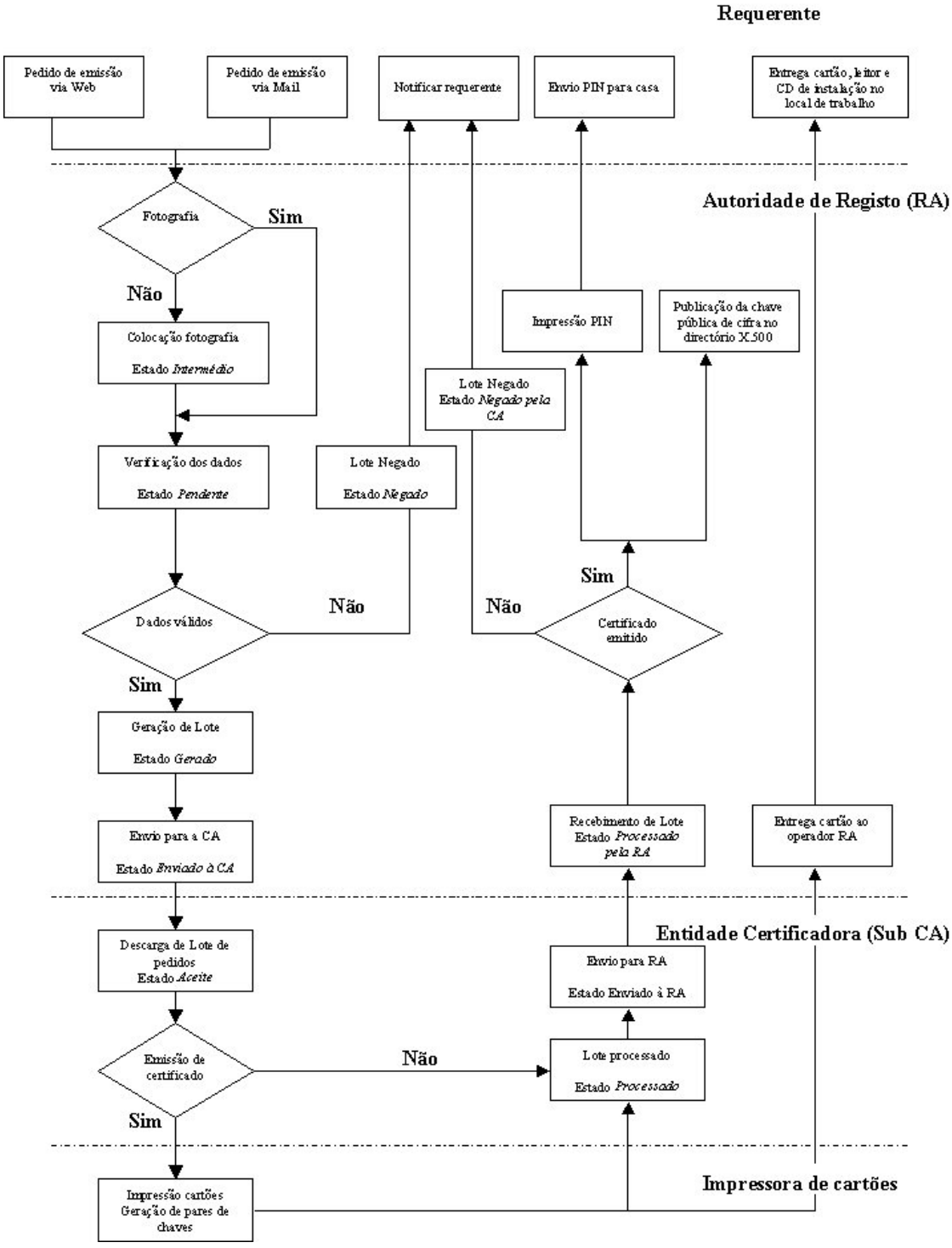

Figura 4.7: Ciclo de emissão de um certificado

Observando o mesmo diagrama, podem-se seguir os passos do ciclo de emissão de um certificado.

Se for aprovado, irá, juntamente com outros entretanto aprovados, formar um lote que se apresentará no estado *Gerado*. Posteriormente, será enviado à KeyOne CA (sub CA),

passando para o estado *Enviado à CA*. Cada lote poderá conter *Pedidos de certificação* ou *Pedidos de revogação*. Não há mistura num só lote destes dois tipos de pedidos.

A sub CA faz a descarga dos lotes, ficando estes no estado *Aceite* e, ou emite-os, ou nega-os, caso detecte alguma anomalia que impeça a sua emissão, ficando estes em ambos os casos no estado *Processado*. Embora no último caso não haja formalização da emissão do certificado, o pedido é reenviado à RA, ficando guardado no histórico no estado *Negado pela CA*. Caso processe um lote de *Pedidos de revogação*, a sub CA gera automaticamente uma CRL com a adição destas novas revogações.

Se processar um lote de *Pedidos de certificação*, estabelece uma conexão com o módulo criptográfico que se encontra ligado à impressora de cartões e que é o responsável pelo envio dos dados dos certificados digitais.

Após a gravação dos certificados, geração dos pares de chaves no "*chip*" e impressão da face do cartão, procede-se ao reenvio do lote à RA, ficando o lote no estado *Enviado à RA*. Uma vez recebido o lote pela RA, esta fará a impressão dos PIN's correspondentes àqueles pedidos e procederá à publicação dos certificados, via LDAP, no Exchange. Encarrega-se de expedir os primeiros para o local de trabalho, juntamente com o leitor de cartões apropriado e o correspondente software de instalação. O software inclui também o SmartWin e o SmartSignature. O PIN do cartão é enviado para casa do requerente por forma a garantir segurança e confidencialidade na recepção deste.

O smart card está preparado para bloquear ao fim de três tentativas erradas de introdução do pin, tendo de se solicitar nova emissão de cartão com novos certificados e novos pares de chaves, procedendo-se à revogação dos certificados pertencentes ao cartão bloqueado. De referir, também, que o único PIN que a RA retém é o inicial. Caso o utilizador decida alterá-lo, não há hipótese daquela saber qual é.

Ficará concluído o processo, com o lote no seu estado final de *Processado pela RA*.

Caso o lote seja de pedidos de revogação, o processo deste é em tudo idêntico ao do lote de pedidos de certificados, à excepção de, em lugar de emitir certificados, emite CRL's.

De referir que há um caso particular da revogação que é a suspensão, ou seja, o operador da RA poderá optar por suspender temporariamente um certificado em lugar de revogá-lo definitivamente. Ao contrário da revogação que é um estado irreversível, a suspensão poderá tornar novamente ao estado válido. Enquanto considerado no estado de suspensão,

esse certificado será tratado como revogado e como tal será colocado numa CRL. Posteriormente se voltar ao estado válido, será retirado de lá.

Em todo este processo não há uma interacção da root CA. Esta encontra-se sempre desligada, sendo apenas utilizada para emitir uma nova ARL quando a anterior expira. Quando se decidir criar mais sub CA's, ela também se encontrará operacional para gerar-lhes os pares de chaves e emitir-lhes os certificados. Fora estas tarefas, nunca é utilizada.

Importa referir que, nesta fase de concretização da arquitectura, se decidiu introduzir alterações à política inicialmente definida de os certificados digitais serem para todos os funcionários do MJ. Verificando-se que nesta primeira fase ir-se-iam apenas disponibilizar os serviços de assinatura/cifra de correio electrónico/documentos, considerados importantes apenas para os funcionários que lidam com informação sensível, foi determinado que o pedido de emissão de um certificado digital deverá ser previamente autorizado pelo organismo empregador, pelo que o Operador da RA deverá reter o pedido de emissão, até que lhe seja enviado por aquele organismo um ofício.

4.2.1.3 Interligações entre Módulos

Nesta secção apresenta-se de uma forma mais profunda, a interligação existente entre o servidor da sub CA e a impressora de cartões. Determinou-se importante detalhar esta ligação, uma vez que apresenta um conjunto de elementos complexos com funções determinantes para o bom funcionamento e a segurança da fase principal desta PKI: a emissão de certificados. Na Figura 4.8 encontra-se representada a ligação existente entre a sub CA e a impressora de cartões.

A impressora que se adquiriu foi a ImageCard Select2 da Datacard, que possui um módulo que pode ser utilizado por uma aplicação de smart cards exterior a si, e que permitirá àquela aplicação inicializar e programar o "*chip*" do cartão (personalização do cartão). Tem uma porta paralela ECP à qual liga o seu cabo de interface, que por sua vez se liga à porta paralela do servidor sub CA e pelo qual irão ser transmitidos os dados para impressão da face do cartão. Para além dessa porta, tem também uma porta série, em que liga um cabo série DB9 blindado, que se irá ligar à porta série do servidor sub CA que contém os dados a inserir no "*chip*" do cartão [48].

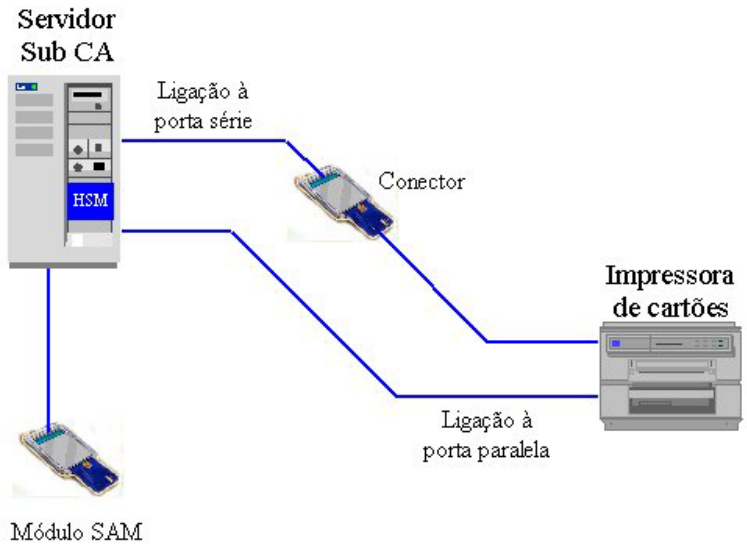

Figura 4.8: Relação sub CA/Impressora de cartões

A aplicação da Safelayer requer que a ligação à porta série do servidor sub CA se faça via um leitor de smart cards ligando-se, por isso, o cabo série da impressora a um conector (Bull DatacardConector), entretanto inserido nesse leitor. Esse conector simulará um smart card. Tal ligação deve-se ao seguinte: A KeyOne CA foi concebida para, ou gerar ela própria os pares de chaves e colocá-los numa PKCS#12 juntamente com o certificado associado, ou os pares de chaves serem gerados no lado do cliente, ou seja, no próprio smart card, sendo a chave pública certificada pela CA que entretanto enviará o respectivo certificado.

No caso da PKI do MJ, há uma mistura destas duas situações. O par de chaves de cifra é gerado pela sub CA que as guarda em formato PKCS#12 e o par de chaves de assinatura é gerado no lado do cliente (simulado, neste caso) certificando ela a chave pública e enviando o certificado associado. Desta forma garante-se o não repúdio (nem a própria sub CA possui a chave privada dos utilizadores) e permite-se a decifra de documentos cifrados com chaves entretanto expiradas.

O papel do conector colocado no leitor de smart cards será então fazer-se passar por um cliente, simulando um smart card para onde a sub CA envia os dados, enviando-os aquele para a impressora que tratará de processá-los.

O "*driver*" da impressora, entretanto instalado no servidor sub CA, recebe informação digital da aplicação de criação de cartões e processa os dados a enviar à impressora.

Quando a impressora recebe os dados, imprime o cartão. O "*driver*" segue todo o processo de impressão do cartão e assim que esta finaliza e a impressora se apresenta livre, envia-lhe mais dados para impressão de um novo cartão.

O módulo "*Security Access Module*" (SAM) pertencente ao kit Crypto Builder da Bull [28], conectado à outra porta série da sub CA por um leitor de smart cards, tem como objectivo actuar como uma protecção contra fraudes e é um mecanismo de controle para a aplicação de smart card [49]. O "*chip*" que se encontra embutido no SAM contém informação proprietária sobre esta solução particular de smart cards, que controlará o acto de envio da informação digital para a impressora e confirmará se o cartão inserido na impressora é do modelo que a aplicação espera que seja, neste caso o cartão TBC80 da Bull [27, 50].

A Figura 4.8 apresenta também o HSM colocado no lugar de uma unidade de CD's da sub CA, sendo ligado a uma porta SCSI interna.

Capítulo 5

Avaliação da Arquitectura Corrente

"*Na teoria, não há diferença entre a teoria e a prática. Na prática, há.*"

(Yogi Berra)

Embora ainda não estejam desenvolvidas todas as especificações requeridas para a PKI do MJ, esta já se encontra numa fase em que se poderá fazer uma avaliação dos resultados obtidos, das suas limitações e inclusive das dificuldades encontradas que inicialmente não tinham sido previstas.

Tal como já foi referido, mal a estrutura se apresentou em condições de produzir certificados, foi logo colocada à prova no estabelecimento de uma SSL aquando das eleições presidenciais de 2001 e das eleições legislativas de 2002, tendo sido um sucesso. Uma vez que os certificados dos utilizadores foram emitidos para aquele propósito, tendo-se inclusivamente reduzido o seu prazo de validade para um mês, não havia problema de situações como a *recuperação e cópia de segurança de chaves* e o *historial da chave* ainda não estarem testadas, bem como as chaves públicas ainda não estarem a ser publicadas no directório público. Havia que aproveitar a oportunidade para justificar a utilidade da PKI e foi o que se fez.

Também em 2001 surgiu nova oportunidade de aproveitar as grandes potencialidades da PKI e, como mais uma vez era apenas para estabelecimento de um canal seguro, não causava transtorno as chaves públicas continuarem a não estar publicadas no directório público, até porque, no caso em questão, os certificados foram emitidos para utilizadores não pertencentes ao Domínio MJ, não podendo de qualquer das formas serem publicadas no Directório. A oportunidade em questão, foi a utilização do SSL na aplicação Atlas desenvolvida pelo ITIJ para a Rede Judiciária Europeia (RJE) para manutenção da informação jurídica disponibilizada pelos vários países da comunidade europeia, no âmbito da cooperação judicial.

5.1 Aplicação dos Certificados nas Eleições

Em Dezembro de 2001, o ITIJ encontrava-se a preparar e a adaptar a sua aplicação para recebimento das contagens dos votos pelos vários Governos Civis, com apresentação em tempo real dos dados relativos ao escrutínio dos resultados das eleições. Nessa mesma altura, a PKI estava apta a emitir certificados, quer para utilizadores (smart cards), quer para servidores.

Assim, foi colocada a hipótese de se realizar a autenticação dos introdutores dos dados do escrutínio não por "*login*" e palavra passe, mas através de certificado digital, guardado em smart card personalizado para cada um dos introdutores. Do lado do servidor também foi colocado um certificado estabelecendo-se um canal seguro por SSL.

A tarefa da contagem dos votos das eleições sempre pertenceu ao ITIJ. Quando surgiram as comunicações em rede, utilizou-se a nuvem X.25 da Telepac sendo os dados transmitidos em claro. Recentemente, substituiu-se o X.25 pelo framerelay, mas os dados continuavam a ser enviados em claro. O único ponto a favor da segurança destes devia-se ao facto de se estar a transmitir directamente para a operadora pelo que os pacotes enviados pelos Governos Civis misturavam-se com os restantes, sendo a tarefa de um eventual "*hacker*" de juntar a sequência de envio destes, praticamente impossível.

Com o estabelecimento de canais seguros por SSL, os dados transmitidos passariam a estar cifrados, melhorando substancialmente a segurança e a confidencialidade destas transmissões.

Esta experiência foi realizada em dois Governos Civis. Os restantes acederam normalmente por HTTP através de "*login*" e palavra passe.

A experiência correu bem, tendo sido repetida nas Legislativas, embora com algumas variantes. Não se emitiram certificados para os introdutores, devido a ter-se verificado, aquando da experiência das Presidenciais 2001, que subsistiam PC's obsoletos nalguns Governos Civis que inviabilizariam a instalação da aplicação cliente para utilização dos certificados. Assim, determinou-se que apenas o servidor teria um certificado para criação de um canal seguro SSL, autenticando-se os Governos Civis por "*login*" e palavra passe. Desta vez, a experiência abrangeu todo o país.

5.2 Aplicação dos Certificados no Programa Atlas

O Atlas foi uma aplicação que nasceu em 2000, ano em que se encontrava Portugal na presidência do Parlamento Europeu. Assim, numa cimeira realizada em Portugal, em Sesimbra, em que se reuniram os membros da Rede Judiciária Europeia (RJE), Portugal propôs-se a desenvolver uma aplicação que permitisse unir, num único "*site*", a informação judicial referente aos vários países da RJE.

O Atlas apresenta as famosas "*Fiches Belges*" que são o resultado de um questionário enviado aos Estados Membros. As respostas foram lidas entre Janeiro e Abril de 1999 e as modificações e desenvolvimentos sugeridas aos Estados Membros. As "Fiches" foram actualizadas de acordo com aquelas sugestões. A informação contida nas "*Fiches Belges*" apenas têm valor indicativo, não adicionando valor judicial no contexto de um procedimento legal.

O Atlas apresenta também os Pontos de Contacto de cada país para resolução de problemas, bem como as entidades competentes ao nível regional em cada país. Os dados de cada país são actualizados apenas pelos Pontos de Contacto desse país. Um Ponto de Contacto é, como o próprio nome indica, a pessoa responsável por responder pelo seu país no que concerne a questões judiciais colocadas a esse país, bem como manter as bases de dados actualizadas. Este só tem acesso aos dados do seu país e a mais nenhum.

Um ano depois, em Setembro de 2001, na cimeira realizada em Tavira com o mesmo grupo de trabalho, o Atlas é-lhes apresentado com o adicional de segurança do SSL. Este será utilizado pelos Pontos de Contacto, para procederem a alterações nas bases de dados do seu país.

A utilização desta tecnologia tem o seguinte fundamento: as bases de dados que os Pontos de Contacto actualizam, contém informação sensível, havendo por isso o interesse em poder-se confirmar que os dados estão a ser recebidos pelo servidor correcto. Também é conveniente que a identidade do Ponto de Contacto possa ser verificada e que se possa assegurar que só ele possui as credenciais necessárias para aceder à base de dados do seu país. A integridade dos dados em trânsito também é salvaguardada. Emitiram-se então certificados, um para cada Ponto de Contacto e um para o servidor que contém a aplicação Atlas. Os certificados dos Pontos de Contacto foram guardados em smart card.

O processo de pedido de emissão de certificados para os Pontos de Contacto, foi efectuado pela RA a partir de ofícios enviados pelo Gabinete para as Relações Internacionais, Europeias e de Cooperação (GRIEC) contendo os dados pessoais daqueles. Tal acção, deveu-se ao facto de aqueles não pertencerem à rede interna do MJ, não podendo, por isso, aceder ao formulário desenvolvido para o efeito.

Presentemente, a emissão destes certificados é uma excepção à regra de emissão de certificados unicamente para o MJ. Estes certificados servem somente para SSL, pois apenas contêm o certificado de cifra. Tal deveu-se ao seguinte: mantendo-se a política de dois certificados por titular (um para assinar outro para cifrar), ambos seriam visualizados no "*browser*" no acto de selecção do certificado para acesso à aplicação, o que se tornaria confuso para o seu utilizador, uma vez que só um deles, o de cifra, é que permitiria o acesso, dando o outro erro.

Em 2002, já houve segundo encontro para apresentação de mais funcionalidades do Atlas, permanecendo o SSL a funcionar correctamente.

5.3 Apreciação do Resultado Obtido

Presentemente, ainda se encontram em fase de conclusão alguns dos serviços apresentados na proposta.

Praticamente três meses depois do início dos trabalhos em Setembro de 2000, já a impressora estava a imprimir cartões com a apresentação exterior definida e contendo no seu "*chip*" os certificados juntamente com os pares de chaves. Mas, uma PKI não se restringe apenas à emissão de certificados. Há toda uma envolvente de políticas e de segurança que devem ser tomadas em conta para que tudo resulte. Por exemplo:

- As CRL's e ARL's devem estar publicadas para que se possa verificar a validade dos certificados que se estão a utilizar no momento;

- As CP's devem estar muito bem definidas e ao alcance das partes confiantes de forma a que estas possam verificar se determinado certificado está a ser utilizado para o propósito que foi criado;

- A CPS deve estar publicada numa URL indicada numa extensão do certificado para que as partes confiantes possam conhecer os procedimentos e políticas de segurança seguidas pela CA na emissão dos seus certificados, por forma a determinarem se devem ou não confiar naqueles certificados. As várias partes implicadas no processo de certificação também devem conhecer os direitos e deveres que lhes assistem;

- Os procedimentos de *recuperação e cópias de segurança de chaves* e de *historial da chave* devem estar muito bem definidos para posterior recuperação de dados cifrados e verificação de assinaturas efectuadas com chaves entretanto expiradas;

- Os certificados das Root CA e Sub CA deverão estar disponibilizados para descarga, para validação da hierarquia;

- As chaves públicas devem estar publicadas no directório público.

Em relação à CRL e aos certificados das CA's, também desde praticamente o início do projecto que se encontram disponíveis para descarga.

Relativamente aos documentos, considerados vitais para o estabelecimento de confiança na estrutura, apenas agora estão a ser elaborados.

Os certificados já estiveram a ser publicados no directório público, quando este era o Exchange 5.5. Mas, há pouco tempo, houve uma migração para Exchange 2000 com utilização de ActiveDirectory, migração esta que ainda não se encontra estabilizada. Esta migração veio provocar alterações na estrutura de nomes do X.500, requerendo uma restruturação da forma de pesquisa destes por parte da PKI. Presentemente, esta tarefa encontra-se involuntariamente suspensa até término da migração do Exchange.

O software de instalação do software do cliente para leitores para PC's (ver Figura 4.2) está desenvolvido e em utilização. De momento está-se a desenvolver outro software de instalação preparado para o Windows XP, que entretanto começou a ser bastante utilizado no MJ. Relativamente ao software de instalação para leitores para portáteis (ver Figura 4.3), ainda está a ser desenvolvido, pois está a haver dificuldade em prepará-lo para o Windows 98, sistema operativo muito comum nos portáteis do MJ.

Os certificados e respectivas chaves públicas já se encontram publicados na Internet. Devido à actual instabilidade existente no Exchange, não se pôde proceder à réplica parcial deste, designada de "*border repository*", utilizando o "*Directory System Protocol*"

(DSP), como teoricamente foi sugerido [18]. Utilizou-se antes uma forma menos funcional, mas a única possível no momento. Aproveitando as bases de dados existentes na RA em que estão guardados todos os certificados emitidos, elaborou-se uma nova tabela com os certificados cujos titulares permitiram a sua publicação na Internet, aquando o preenchimento do formulário do pedido de emissão (ver Figura 4.6). Esta entretanto é descarregada via FTP no Web Server. Tal tarefa apresenta-se bastante penosa para o operador de RA, para além de não dar garantias de apresentar a realidade mais actual, sendo imediatamente corrigida assim que o Exchange estabilizar.

5.4 Limitações da Concretização Actual

À medida que se ia adaptando a estrutura às necessidades do MJ, detectaram-se limitações na aplicação adquirida, inicialmente dadas como possíveis de concretizar:

- Não há vários níveis de acesso para os administradores da CA. Todos poderão executar as mesmas tarefas pelo que não se podem apurar responsabilidades de actos realizados;

- Esta PKI não apresenta um arquivo de chaves, permitindo apenas a gravação da chave de cifra e palavras passe fora do disco, para elaboração de um arquivo normal.

- O historial das chaves não se encontra no lado do cliente. O cartão não acumula as chaves públicas do utilizador pelo que sempre que este deseje decifrar algo cifrado com uma chave já expirada, não poderá fazê-lo de forma transparente, tendo de solicitar a intervenção da RA. Mesmo na PKI, não há um historial das chaves automático. A versão 2.1 da Safelayer KeyOne, não possui nem esta funcionalidade nem tem um sistema integrado de *recuperação e cópias de segurança de chaves*, havendo apenas um sistema de arquivo rudimentar que utiliza as capacidades de "*callback*", que funciona relativamente bem, embora não sendo muito prático;

- Os históricos são muito rudimentares e não se podem imprimir ou exportar para serem processados por outras aplicações.

De todas estas limitações da própria aplicação, as que se afiguram mais graves são a ausência de um historial das chaves automático e de um sistema de *recuperação e cópias*

de segurança de chaves integrado. Poderão ser obtidas através de desenvolvimento de "*scritps*" em Scryptor, mas uma vez que eles já estão integrados na "*release*" seguinte, vai-se aguardar por esta.

O modelo off-line da KeyOne, poder-se-á revelar pouco prático quando houver pedidos de revogação em que, de acordo com a política definida na CPS, em horário laboral, deverão ser efectuados, no máximo, em 4 horas. Este problema terá de ser torneado com uma excelente comunicação entre ambas as equipas.

O facto de o processo ser efectuado com lotes de "Pedidos de certificação" não se torna prático quando, porventura, surge uma falha na emissão de um dos certificados. Tal situação invalida todo o lote tendo de se realizar o ciclo desde o início, requerendo novamente os pedidos de certificação, pois a RA não tem hipótese de repetir a descarga daquele lote para a CA. A solução encontrada para colmatar esta situação, foi reduzir o número de pedidos de certificação por lote. Pelo menos assim, havendo uma falha num deles, não serão tantos os pedidos sacrificados. A não ser que a Safelayer reveja toda a estrutura em que recai a KeyOne, os lotes hão-de continuar a existir, mantendo-se a solução definida pelo ITIJ.

Detectou-se, também, uma falha gravíssima na aplicação SmartSignature responsável pela assinatura/cifra de ficheiros: Sempre que se pretende decifrar um ficheiro, a aplicação procura a chave de decifra no cartão que se encontra no leitor, não permitindo a pesquisa da chave noutros dispositivos. Esta falha far-se-á sentir especialmente quando o utilizador decidir decifrar documentos cifrados por chaves que já expiraram e consequentemente não se encontram no cartão pois este não mantém o historial daquelas. Este problema já foi colocado à empresa fornecedora que decidiu substituir este produto pelo KeyOne Desktop (*vide* secção 4.2).

Algumas opções tomadas pelo ITIJ também já se revelaram infrutíferas:

- Devido ao facto de se ter optado pela utilização de CRL's em lugar do OCSP por serem uma estrutura auto-protegida, surge o problema de estas não serem verificadas on-line pelo Microsoft Outlook. A detecção de revogação de um determinado certificado, não é efectuada de forma transparente, temendo-se que as partes confiantes simplesmente não verifiquem a validade dos certificados. Esta é uma limitação do próprio Outlook, já que, em testes realizados no Outlook Express, tal não

acontecia. Tal problema requererá o desenvolvimento de um "*plug in*" que permita tornear esta situação;

- O facto de a utilização da aplicação SmartWin exigir a presença do cartão aquando o "*login*" da máquina, constitui um factor de segurança mas também um factor de desconforto para o utilizador, já que este se vê impossibilitado de aceder à sua máquina caso se tenha esquecido do seu cartão. Tomou-se então a decisão de fazer um novo software de instalação com a opção de instalação ou não da aplicação SmartWin e advertindo o utilizador para as precauções a tomar, caso opte pela instalação desta;

- Também para garantir a todo o custo o não repúdio, não há hipótese de seguimento do rasto de substituições do PIN. Se porventura houver esquecimento daquele por parte do utilizador, não haverá resolução do problema. Deveria haver a possibilidade de se fazer um "*reset*" à memória do "*chip*" que detém o PIN e preenchê-la de novo com o PIN inicial.

Todas estas limitações apresentadas não são impeditivo para um bom sucesso da PKI, pois a parte algorítmica já deu mostras de estar a funcionar correctamente. O que de facto se tem revelado um ponto contra, é o tempo que a aplicação tem demorado a ser desenvolvida. À medida que o tempo passa, denota-se que a aplicação vai gradualmente caindo no esquecimento e todas as expectativas de utilização que tinham sido criadas, vão sendo abandonadas.

5.5 Optimizações Possíveis

Já foram consideradas várias optimizações a pôr em prática para um melhoramento da PKI.

Tendo-se tido conhecimento de como algumas empresas concorrentes tornearam problemas idênticos aos encontrados nesta infra-estrutura, foram sugeridos alguns desenvolvimentos extra:

- Sugeriu-se o desenvolvimento de um "*plug in*" que permitisse ao Outlook detectar automaticamente, quando da recepção de uma mensagem assinada, se o certificado que a assinou se encontrava revogado e avisar de imediato o receptor dessa

mensagem. Ou então, caso se demonstrasse mais fácil ao nível da programação, impedir que o titular de um certificado revogado pudesse mandar uma mensagem assinada por este;

- Em lugar da nota de rodapé colocada numa mensagem de correio electrónico assinado (ver Figura 5.1) dirigida aos receptores desta pedindo para que eles procedam à descarga dos certificados da Root CA e da Sub CA por forma a estabelecerem a hierarquia de confiança, estes deveriam era ser enviados juntamente com a mensagem de correio electrónico, tal como já se faz com o certificado do utilizador. Esta optimização revelar-se-ia uma mais-valia dado que em testes já efectuados, se verificou que a primeira reacção do receptor ao ler o aviso de que aquele certificado não é válido, é dizer que os certificados do ITIJ não funcionam correctamente e poucos são aqueles que lêem a nota de rodapé e seguem as instruções propostas;

- Outra optimização que chegou a ser posta em prática mas que de momento não funciona devido à passagem para o Exchange 2000, foi a execução de um "*plug in*" que permitiu criar uma pasta pública onde se encontravam os utilizadores possuidores de chave pública. Assim, quem pretendesse cifrar uma mensagem para um desses utilizadores, dirigia-se àquela pasta pública (ver Figura 5.2). Como já foi mencionado anteriormente, embora utilizando protocolos standard, houve grandes dificuldades no reconhecimento destes pelos produtos Microsoft. O Microsoft Outlook revelou não importar das contas do Exchange para o seu Livro de Endereços, a chave pública destes, para, de uma forma transparente, ser-se possível enviar-lhes mensagens cifradas. Em testes realizados com o Outlook Express, este revelou-se preparado para esta situação. Mas, estava fora de questão todo o MJ passar a utilizar o Outlook Express, até porque este não tem todas as potencialidades do outro como o calendário com tarefas agendadas, tão utilizado para marcação de reuniões. Entretanto, verificou-se que o Outlook XP já permite a integração da chave pública no livro de endereços mediante uma pequena tarefa a realizar pelo próprio titular daquela que consiste na autorização da sua publicação no Livro de Endereços. Presentemente, está-se a colocar a hipótese de desistir da modificação do "*plug in*" para os restantes Outlooks que não o XP, uma vez que a tendência será começar a migrar todas as máquinas para este.

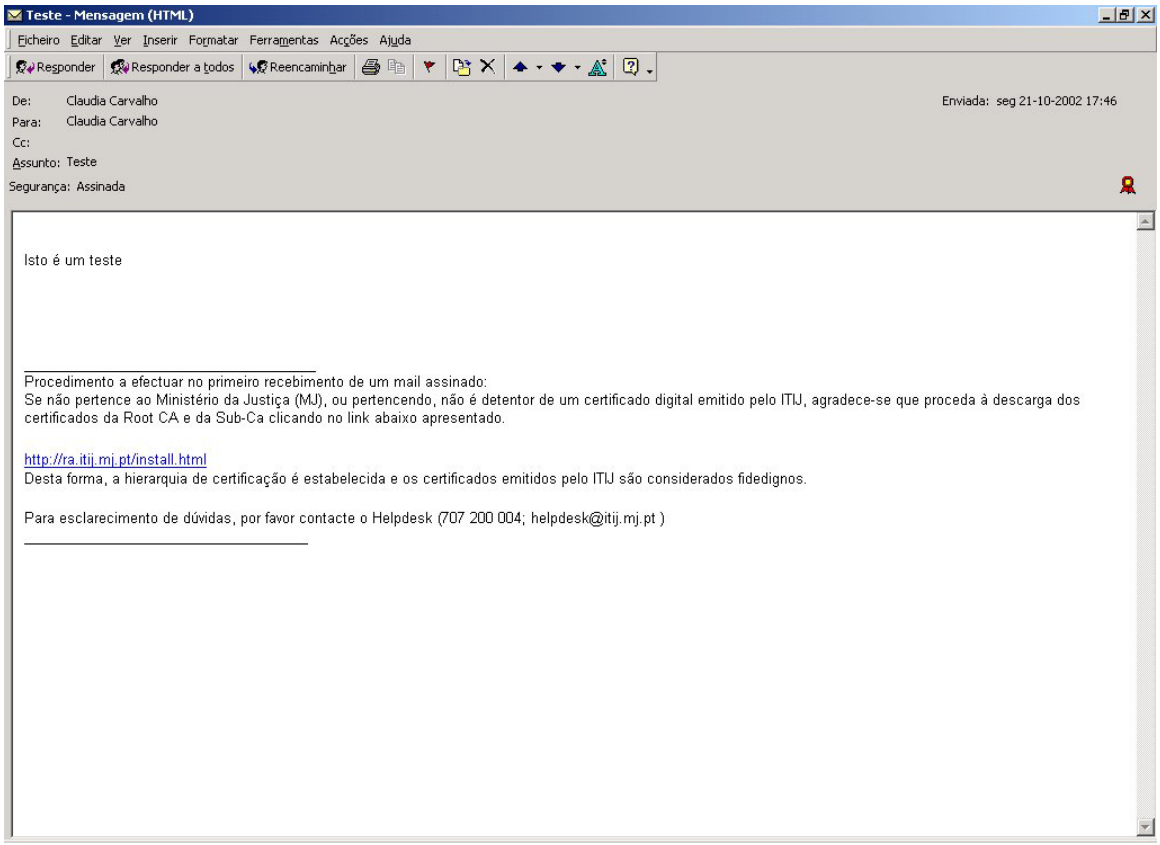

Figura 5.1: Aposição de rodapé em mensagens assinadas

Figura 5.2: Pasta pública com lista de Utilizadores Certificados

No que concerne ao modelo off-line da KeyOne CA utilizado no ITIJ, este não está a trazer nenhum benefício ao nível da segurança relativamente à sub CA, uma vez que esta se encontra conectada à rede interna, estando exposta a ataques internos. O que se

pretende efectuar é desligá-la da rede, uma vez que apenas a RA é que tem necessidade de interagir com a Intranet. Assim, ir-se-á colocar mais uma placa Ethernet na RA, ligando a esta a sub CA através de um cabo cruzado. Desta forma, a sub CA já não estará visível na Intranet e apenas conseguirá ser acedida através da RA por quem conheça o seu "*login*". Estando a directoria partilhada, para transferência de lotes de uma máquina para a outra, criada na RA, a CA limitar-se-á a "mapear" essa directoria para carregar o lote com os pedidos e posteriormente descarregar para lá o lote com as emissões efectuadas.

Capítulo 6

Conclusões e Trabalho Futuro

Ao longo dos dois anos que esta PKI demorou a ser desenvolvida, verificou-se que as aplicações que têm de interagir com certificados digitais, têm-se gradualmente preparado para uma cada vez melhor interacção com aqueles. Esta alusão é feita à plataforma Microsoft, uma vez que é esta que é comummente utilizada em todo o MJ: O Outlook XP ao contrário do detectado nos anteriores Outlooks, faz uma verificação on-line das CRL's, detectando, sem a intervenção do utilizador, o estado do certificado recebido em determinada mensagem assinada. Também permite fazer um pedido de recibos de leitura assinados. Apresenta também outro serviço que elimina a desvantagem detectada nos anteriores Outlooks, que é a de permitir que o próprio titular publique a sua chave pública no directório público, ficando esta automaticamente acessível a todos os utilizadores desta infra-estrutura, dentro do MJ. Também se detectou uma evolução no "*browser*", o Internet Explorer em que presentemente, as suas versões permitem encriptação segura a 128 bits, recomendada pelas PKI's.

Relativamente aos projectos desenvolvidos no seio da PKI do MJ, a aplicação Atlas encontra-se a funcionar correctamente e sem percalços, sentindo-se os utilizadores confortáveis com a sua utilização. As eleições, continuarão a efectuar-se com o apoio do SSL. O projecto piloto efectuado no ITIJ para teste do S/MIME, do SmartWin e do SmartSignature, também funcionou correctamente após se ter conseguido preparar o software de instalação para os três sistemas operativos mencionados na proposta. Tal projecto piloto ficou confinado ao ITIJ, devido ao facto da migração do Exchange para 2000 ter impedido a correcta publicação dos certificados digitais dos restantes organismos do MJ. Dado que ainda não está prevista a finalização desta migração, decidiu-se tornear este problema, para não atrasar mais a entrada em produção, que se tenciona iniciar em Janeiro de 2003. Uma vez que já foi desenvolvido o serviço de publicação dos certificados digitais na Internet, poder-se-á descarregar por aí a chave pública do receptor pretendido para envio da mensagem cifrada.

Assim, o próximo passo será efectuar acções de sensibilização nos vários organismos, para compreensão da estrutura e suas funcionalidades. Tal tarefa não se pode atrasar mais, uma vez que está a ser definido para 2003 (há pouco tempo adiado de Janeiro para Setembro), a recepção das peças processuais via correio electrónico com assinatura digital.

À parte todos os atrasos adjacentes a um projecto com uma tecnologia muito recente, este apresenta boas hipóteses para ser bem sucedido e funcional, especialmente nos Tribunais, entidades que trabalharão mais directamente com a figura da assinatura digital, na sua permanente interacção com os Advogados.

6.1 Trabalho Futuro

O próximo trabalho a desenvolver será o serviço de estampilha temporal. Este serviço está-se a demonstrar vital para um bom serviço de não repúdio das mensagens.

Estão a surgir conflitos entre Tribunais e Advogados relativamente às datas de envio e de recepção das peças processuais enviadas por estes últimos aos primeiros.

Em situações como estas em que a data de entrega de um documento é regulamentada por prazos, a hora apresentada nas mensagens de correio electrónico, deverá ser a real, não havendo a hipótese de ser manipulada pelo seu emissor.

O próximo projecto será então obter a hora legal (em Portugal esta será dada pelo Observatório Astronómico de Lisboa), apondo-lhe um certificado fidedigno comprovando que a hora aposta naquela mensagem foi obtida naquela entidade.

Bibliografia

[1] Ministério da Justiça - Serviços do Ministério, *Programa do Governo para a área da Justiça - Programa do XV Governo Constitucional*. 2000. (http://www.mj.gov.pt/index.php?article=1489&visual=2&id=19)

[2] Ministério da Justiça, *Rede de comunicações do Ministério da Justiça*. 2002. (http://www.itij.mj.pt)

[3] Ministério da Justiça, *Processo Simples Justiça Segura – Breve Guião*. Link – ICS, 1999.

[4] A. Zúquete, *Especialização em Segurança Informática.* CEPEI – Protocolos e Mecanismos de Segurança. 2002.

[5] Baltimore Technologies Limited, *MailSecure™ Overview – A Baltimore White Paper*. 1999.

[6] Certipor, *O que é uma Entidade Certificadora?*. 2000. (http://www.certipor.com/documentacao/art00001.html)

[7] P. Veríssimo, *Segurança em rede informáticas - Acetatos teóricos*. FCUL, 1996-1998.

[8] B. Schneier, *Applied Cryptography – second edition*. John Wiley & Sons, Inc., 1996.

[9] C. Kaufman, R. Perlman, M. Speciner, *Network Security Private Communication in a public world*. Prentice Hall, Maio de 1995.

[10] A. S. Tanembaum, *Redes de Computadores.* Editora Campus, 1997.

[11] M. L. Rocha, M. F. Rodrigues, M. A. Andrade, M. P. Correia, H. Carreiro, *As Leis do Comércio Electrónico*. Edições Centro Atlântico, Março de 2000.

[12] American Bar Association Section of Science and Technology Information Security, *Digital Signature Guidelines Tutorial American Bar Association*. 1996. (http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html)

[13] M. Duarte, S. Fonte, *Como produzir uma Assinatura Electrónica?*. Janeiro de 2002. (http://mcduarte.planetaclix.pt/assinaturadigital.html)

[14] Microsoft Corporation, *Overview of Certificates and Authentication*. 1997.

[15] GlobalSign – Trust on the Net, *About Digital Certificates.* 2000/2001. (http://support.globalsign.net/en/general/faqct_body.htm)

[16] R. Housley, W. Ford, W. Polk e D. Solo, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 2459, Janeiro de 1999.

[17] J. W. Hong, *The X.500 Directory: Overview of Concepts, Models and Services*. 2000. (http://dpnm.postech.ac.kr/~jwkhong/x500_dir.html)

[18] C. Adams, S. Lloyd, *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations.* Macmillan Technical Publishing, Novembro de 1999.

[19] M. Myers, R. Ankney, A. Malpani, S. Galperin, e C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, RFC 2560, Junho de 1999.

[20] Baltimore Technologies Limited, *An Introductory Guide to PKI*. 2000.

[21] J. Jacob, A. Asay, A. Brett-Holt, D. Faber, N. Hickson, M. Mahony, P. Waller, *Digital Signature Guidelines*. Judicial Studies Board, Julho de 2000.

[22] Baltimore Technologies plc., *Why use security?*. 2000.

[23] S. Chokhani, W. Ford, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, RFC 2527, Março de 1999.

[24] Globalsign, NV/SA, *GlobalSign Certification Practice Statement – version 3.0*. Janeiro de 1999. (http://www.microsoft.com/technet/prodtechnol/ad/windows2000/evaluate/05w2kadb.asp?frame=true)

[25] Microsoft Corporation, *Object Identifiers – Active Directory Schema*. 2001. (http://www.microsoft.com/windows2000/techinfo/reskit/en/distrib/dsbe_ext_srww.htm)

[26] H. T. Alvestrand, *OID assignments from the top node*. Alvestrand Data, Fevereiro de 1997. (http://www.alvestrand.no/objectid/top.html)

[27] Bull Ellectronics Angers, S.A., *Smart Cards User Guide Crypto Safe - 43 A2 76TK Rev00*. Outubro de 1999.

[28] Bull Ellectronics Angers, S.A., *Smart Cards User Guide Crypto Builder - 43 A2 85TK Rev01*. Novembro de 1999.

[29] R. Poynder, *The Smart Card Club*. Março de 2001. (http://www.smartex.com)

[30] M. Fratto, *Security Tokens*. Network Computing, Agosto de 2001. (http://www.networkcomputing.com/1217/1217buyers2.html)

[31] nCipher Corporation Limited, *nForce & nShield User Guide Window v3.2.31*. Agosto de 2000.

[32] CRENA – Corporation for Research & Educational Networking, *CREN Strategic and Practical FAQ – Hardware Security Modules – What to Look For*. Novembro de 2001.

[33] Baltimore Technologies plc., *Unicert Product Overview*. 1999. (http://www.Baltimore.com)

[34] D. E. Eastlake, O. Gudmundsson, *Storing Certificates in the Domain Name System (DNS)*, RFC 2538, Março de 1999.

[35] R. Housley, P. Hoffman, *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*, RFC 2585, Maio de 1999.

[36] Microsoft Corporation, *Active Directory Service Interfaces – The Easy Way to Access and Manage LDAP-Based Directories (Windows NT 4.0)*. Fevereiro de 1997. (http://www.microsoft.com/TechNet/prodtechnol/winntas/maintain/featusability/adsildap.asp?frame=true)

[37] Missão para a Sociedade da Informação – Ministério da Ciência e da Tecnologia, *Livro Verde para a Sociedade da Informação em Portugal*. 1997.

[38] MSDN Library – Technical Articles, *Microsoft Exchange Server: Using Industry Standards for Greater Compatibility*. 2000. (http://msdn.microsoft.com/library/en-us/dnexch55/html_stan10.asp?frame=true)

[39] Microsoft Corporation, *Exchange Server 5.5 Datasheet*. Dezembro de 1999. (http://www.microsoft.com/Exchange/evaluation/previous/datasheet.asp)

[40] Microsoft, *Microsoft® Outlook™ 2000 - Product Enhancements Guide*. Outubro de 1998.

[41] Microsoft Corp., *White Paper: Advantages of Using Microsoft® Internet Explorer 5 in Your Business*. Março de 1999.

[42] W. R. Stanek, *Microsoft Windows 2000 Administrator's Pocket Consultant*. 1999.

[43] Netscape Communications Corporation, *Secure Sockets Layer*.1999. (http://developer.netscape.com/tech/security/ssl/protocol.html)

[44] NSS, *Safelayer KeyOne 2.1- Product Testing.* 2000. (http://www.nss.co.uk/PKI/safelayer/safelayer.htm)

[45] Safelayer, *General KeyOne Architecture*. Julho de 2002. (http://www.safelayer.com)

[46] Safelayer Secure Communications, S.A., *General KeyOne Architecture.* Julho de 2002. (http://www.safelayer.com)

[47] nCipher, *nShield™ Hardware Security Module (HSM) - Cryptographic security platform with advanced key management*, 2002. (http://www.ncipher.com/nshield/)

[48] Datacard, *User's Guide for Express™ and Select™ Class Printers*, Junho de 2000.

[49] Verifone, *Security Access Module White Paper – Smart Card Security Access Modules in VeriFone Omni 3350 Countertop and Omni 3600 Portable Terminals*. 2001.

[50] Bull, *What is a smart card?*. 2000. (http://www.cp8.bull.net/sct/uk/world/index.html)

Legislação:

Decreto-Lei nº 111/83 de 21 de Fevereiro, *Lei Orgânica do Ministério da Justiça*

Resolução do Conselho de Ministros nº 60/98, de 6 de Maio – Determina a existência de um endereço de correio electrónico nos serviços e organismos integrados na administração directa ou indirecta do Estado e regula o valor a atribuir aos documentos circulados por via electrónica

Resolução do Conselho de Ministros nº 115/98, de 1 de Setembro – Iniciativa Nacional para o Comércio Electrónico

DL nº 135/99, de 22 de Abril – Define os princípios gerais a que devem obedecer os serviços e organismos da Administração Pública na sua actuação face ao cidadão, bem como reúne de uma forma sistematizada as normas vigentes no contexto da modernização administrativa

DL nº 290-D/99, de 2 de Agosto – Aprova o regime jurídico dos documentos electrónicos e da assinatura digital

Resolução do Conselho de Ministros nº 94/99, de 25 de Agosto – Documento Orientador da Iniciativa Nacional para o Comércio Electrónico

DL nº 375/99, de 18 de Setembro – Estabelece a equiparação entre a factura emitida em suporte papel e a factura electrónica

Directiva 1999/93/Ce do Parlamento Europeu e do Conselho, de 13 de Dezembro – Quadro legal comunitário para as assinaturas electrónicas

Lei Orgânica do Ministério da Justiça, aprovada pelo Decreto-Lei nº146/2000, de 18 de Julho – Atribui ao ITIJ a função de Entidade Credenciadora

Resolução do Conselho de Ministros nº 110/2000, de 22 de Agosto – Plano de Acção da Iniciativa Internet

DL nº 234/2000, de 25 de Setembro – Cria o Conselho Técnico de Credenciação como estrutura de apoio ao ITIJ no exercício das funções de autoridade credenciadora de entidades certificadoras de assinaturas digitais

Resolução do Conselho de Ministros nº 143/2000, de 27 de Setembro – Define medidas dirigidas à generalização da prática de aquisição de bens e serviços por via electrónica pela administração pública

Glossário

Algoritmo

Sequência de instruções para efectuar determinado processo passo a passo.

Browser

Programa que permite navegar na Internet

DER

Distinguished Encoding Rules – Baseado em BER (Basic Encoding Rules), é utilizado como base para os standards ASN.1 e o X.509. Foi estandardizado pela ITU (International Telecommunication Union), como forma de apresentação dos campos de um certificado.

Dispatcher

Máquina que se encontra na DMZ e que tem como função receber as mensagens de correio electrónico destinadas aos utilizadores internos, canalizando-as para as respectivas contas de correio, protegendo-as assim de ataques externos. Interliga, também, os vários Exchange do domínio, promovendo a replicação da estrutura X.500 daquele.

LDAP

Lightweight Directory Access Protocol – Como protocolo de acesso ao directório standard OSI, o directório X.500, definiu-se o DAP ("*Directory Access Protocol*"). Sendo um protocolo OSI, tornava-se mais complicado que os assentes no modelo TCP/IP, requerendo mais linhas de código e máquinas mais potentes. Apresentava-se também difícil de correr em clientes PC e Macintosh®, em que a funcionalidade TCP/IP já vem com a máquina. Assim, em 1993, na Universidade de Michigan, foi desenhado e desenvolvido um protocolo que trabalhasse sobre TCP/IP e que fosse pequeno o suficiente para correr em clientes com Sistema Operativo Windows® ou um Macintosh®. Deu-se-lhe o nome de LDAP que actualmente já se encontra na terceira versão.

OCSP

On-line Certificate Status Protocol – Protocolo que desempenha as funções da CRL, eliminando ainda certas limitações daquela, tal como a verificação off-line da revogação do certificado.

PKCS

Public-Key Cryptography Standards – Conjunto de normas standard para criptografia de chave pública desenvolvido pelos Laboratórios RSA. É compatível com o standard X.509. Os standard publicados são: PKCS #1, #3, #5, #7, #8, #9, #10 #11, #12, e #15; PKCS #13 e #14.

- PKCS #7 define uma sintaxe geral para as mensagens que incluem criptografia como Assinaturas Digitais e Cifra;
- PKCS #10 descreve uma sintaxe para pedidos de certificação digital;
- PKCS #11 define uma tecnologia de interface de programação, designada de Cryptoki para dispositivos criptográficos tais como smart cards e cartões PCMCIA;
- PKCS #12 especifica um formato portátil para guardar e transportar chaves privadas, certificados, etc..

RFC

Request For Comments – Documentos que definem normas e protocolos para a internet onde se fazem discussões de nível técnico para a definição de novos protocolos.

SAM

Security Access Module – Micromódulo não maior que um chip de smart card, daí ser normalmente guardado num cartão idêntico ao smart card, designando-se de "*full-sized*" SAM. Tem como função proteger e garantir a integridade dos smart cards que estão a ser utilizados por uma aplicação.

S-HTTP

Secure Hypertext Transfer Protocol – Extensão do HTTP. HTTP é o protocolo que forma a base da World Wide Web permitindo a troca de documentos multimedia naquela. O S-HTTP foi desenhado para providenciar confidencialidade, autenticidade, integridade e não repúdio, enquanto suporta mecanismos de gestão de chaves múltiplas e algoritmos criptográficos através de uma negociação opcional de ambas as partes envolvidas na transacção.

S/MIME

Secure Multipropose Internet Mail Extensions – Standard para envio de correio electrónico seguro. O protocolo MIME define como uma mensagem electrónica é organizada e suportada pela maioria das aplicações de correio electrónico. O S/MIME constrói segurança sobre aquele protocolo ao permitir informação cifrada e a inclusão de um certificado digital como componentes da mensagem.

SSL

Secure Sockets Layer – Protocolo não proprietário desenvolvido pela Netscape que providencia segurança em comunicações consideradas sensíveis. É aceite como um standard Web para comunicações cliente-servidor autenticadas e cifradas, sendo tipicamente utilizado entre "*browsers*" e servidores. Permite confidencialidade, autenticidade e integridade sob a forma de conexões cifradas, autenticação de servidores e clientes e integridade das mensagens. Necessita de utilizar certificados digitais.

Como é que o SSL funciona?

- O cliente e o servidor trocam informação segura. É o designado "*handshaking*";
- O cliente apresenta a identificação da sessão, os algoritmos de encriptação e os métodos de compressão por ele suportados;
- O servidor faz a sua selecção usando esta informação. Se tal for requerido, ambos trocam certificados;
- O servidor define uma chave de sessão apropriada para o algoritmo de cifra, na fase do "*handshaking*".

Servidor e cliente poderão a partir deste momento comunicar de forma segura.

TLS

Transport Layer Security – Baseado em SSL. Parte integrante dos browsers de clientes e de servidores

TCP

Transmission Control Protocol – Protocolo ao nível de transporte (nível 4 do modelo OSI) utilizado na Internet. Estabelece uma ligação lógica entre duas máquinas e garante a entrega das mensagens.

X.500

É o standard ISO para os serviços de nome e de directório