Universidade do Minho

Mestrado Sistemas Dados e Processamento Analítico

Segurança e Privacidade em Sistemas de Armazenamento e Transporte de Dados

Ano Lectivo de 2006/2007

Certificados Digitais

Sistema de Certificação Electrónica do Estado (SCEE)

Luís Miguel Sá Neiva Ferros

Junho, 2007

Data de Recepção	
Responsável	
Avaliação	
Observações	

Luís Miguel Ferros

Junho, 2007

Conteúdo

Índice de Figuras

Índice de Tabelas

1. Introdução

Nos dias de hoje, verificando-se um aumento crescente das transacções electrónicas para troca e distribuição de informação muitas vezes sensível, há que assegurar a existência de ambientes confiáveis para a realização dessas transacções de uma forma segura. Tal é possível através do recurso à criptografia. A criptografia (*kriptós* = escondido/oculto + *gráph* = grafia) já existe desde a era romana e define-se como a arte ou ciência de escrever em cifra ou em código uma mensagem, de forma a permitir que somente o destinatário a decifre e compreenda. As técnicas de criptografia oferecem seis tipos de serviços básicos, sem os quais não seria possível realizar transacções electrónicas de uma forma segura através da Internet. Estes predicados são nomeadamente: disponibilidade, integridade, controlo de acesso, autenticação da origem, não repúdio e privacidade.

Com a criptografia é possível transformar um texto original ou texto claro em texto cifrado, texto código ou simplesmente cifra, que tem a aparência de um texto ilegível. Para que seja possível ler esse texto é necessário desencriptar (ou descodificar) a mensagem.

Tradicionalmente um sistema criptográfico integra os seguintes elementos:

- 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 (não codificado) em criptograma (operação cifrar), ou pela transformação em texto claro (operação decifrar).

Basicamente existem dois tipos de criptografia nos sistemas computacionais: criptografia simétrica ou de chave privada e a assimétrica ou de chave pública.

Dado o tema do trabalho, neste documento vai-se incidir principalmente no contexto da criptografia assimétrica ou de chave pública.

Ao longo deste documento o objectivo principal será a análise do contexto e legislação inerentes à certificação digital no âmbito das entidades públicas. Numa primeira fase descreve-se de uma forma geral a teoria em torno da certificação digital, para leitores que não se estejam familiarizados nesta matéria. Numa segunda fase é feita a instanciação dessa teoria a um caso concreto e ainda imaturo: o Sistema de Certificação Electrónica do Estado, o qual foi criado pelo Decreto-Lei n.º 116-A/2006, de 16 de Junho de 2006 (ver anexo II), para assegurar a unidade, a integração e a eficácia dos sistemas de autenticação digital forte nas relações electrónicas de pessoas singulares e colectivas com o Estado e entre entidades públicas [1].

2. Certificação digital

2.1.1 Criptografia simétrica e assimétrica

Na **criptografia simétrica** ou de chave privada 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 [2].

A **criptografia assimétrica** ou de chave pública usa um par de chaves distintas em que, embora não se consiga obter uma chave a partir de outra, estas encontram-se matematicamente relacionadas, conseguindo uma decifrar aquilo que a outra cifrou. Esta característica vai permitir que uma das chaves seja publicada, 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. A grande vantagem deste sistema é permitir que qualquer pessoa possa enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como é feito no modelo simétrico. 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 cifra operam em conjunto [2].

2.1.2 Confidencialidade, Integridade e Assinatura digital

"*A Assinatura Digital é um processo de assinatura electrónica baseado em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo, e ao declaratário usar a chave pública para verificar se a assinatura foi criada mediante o uso da*

correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura." [in Decreto-Lei relativo à Assinatura Digital (n.º 290-D/99)]

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

- Personificação – Um elemento fazer-se passar por outro, perante terceiros, numa troca de informação;
- Alteração de dados – Modificação de alguns ou de todos os dados transmitidos numa sessão.

Desta forma, a assinatura digital de um documento garante:

- A autenticação da identidade da entidade que assinou o documento (o emissor do documento);
- A não alteração (acidental ou maliciosa) do documento durante a sua transmissão, i.e., protege a integridade do documento;
- O não repúdio do documento por parte do emissor, i.e., o emissor não pode reclamar que não foi ele que assinou o documento.

Tecnologicamente, a assinatura digital é criada e verificada criptograficamente. No caso da criptografia assimétrica, utilizam-se as duas chaves, a privada e a pública. A chave privada serve para criar uma assinatura digital, ou seja, é utilizada pelo emissor da mensagem quando este a assina, e a segunda será utilizada pelo receptor da mensagem para verificar 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 de forma a forjar essa mesma assinatura. O facto do emissor da mensagem assinar esta com a sua chave privada, permite a autenticação, pois mais ninguém, além dele, poderia ter utilizado aquela chave.

Para criar uma assinatura digital é necessário primeiro que o emissor da mensagem gere uma versão da mensagem (versão reduzida, 160 bits por exemplo), conhecida por código *Hash* ou código da mensagem. Este código, gerado por algoritmos públicos (SHA-1, MD5, etc.), é único para o texto original. Basta alterar ligeiramente o texto original para que o código então gerado seja completamente diferente.
Posteriormente, o emissor cria a assinatura digital ao assinar (cifrar) o código *Hash* da mensagem com a sua chave privada.

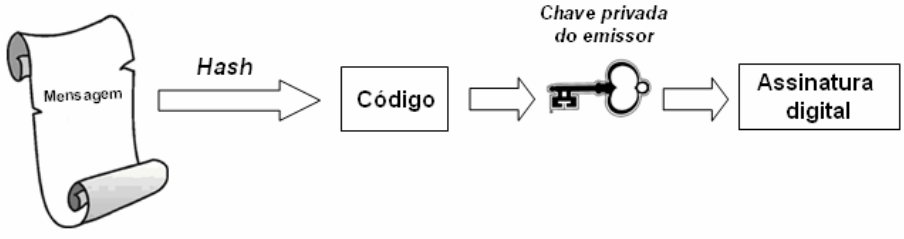

Figura 1 – Processo de criação de uma assinatura digital (baseado em [3])

Confidencialidade

A cifragem de um documento garante que só o destinatário do documento o consegue ler na sua forma original, sendo incompreensível para terceiros que o consigam interceptar.

Com o sistema de chave pública, tanto o remetente como o destinatário podem, de uma forma segura, trocar informação privada numa transacção electrónica. Para isso, para proteger a informação a enviar, o remetente utiliza a chave pública do destinatário para cifrar os dados. Quando o destinatário recebe os dados, pode decifrar essa informação com a sua chave privada, e assim obter acesso à informação original em formato legível. Enquanto o destinatário mantiver a sua chave privada segura a informação que é transaccionada muito dificilmente será acessível a outros.

Desta forma, com o objectivo de mais ninguém ter acesso ao conteúdo da mensagem, a não ser o correcto receptor, isto é, para garantir a confidencialidade na transmissão de informação, o emissor da mensagem adiciona a assinatura digital criada à mensagem original, que cifra, por sua vez, com a chave pública do receptor. É criada assim uma mensagem electrónica confidencial e assinada digitalmente.

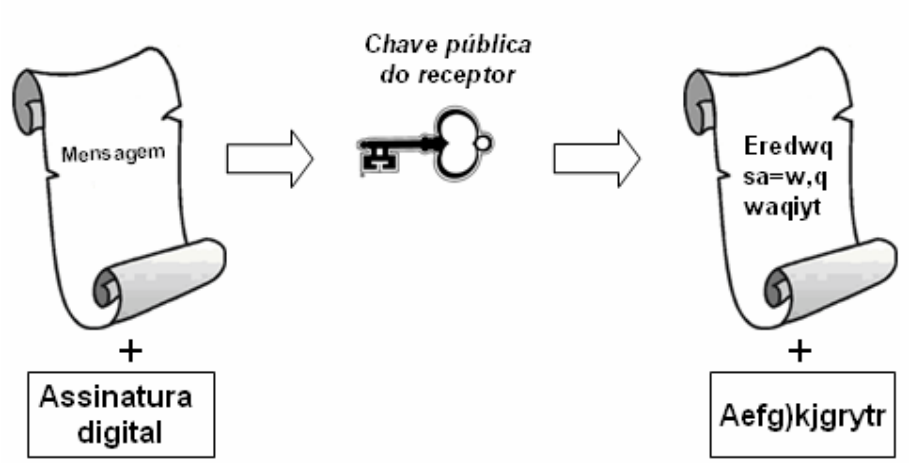

Figura 2 – Processo de cifragem das mensagens assinadas digitalmente (baseado em [3])

Processo de validação das mensagens assinadas digitalmente

Após a recepção da mensagem, caso a mensagem esteja cifrada, o receptor acede ao texto utilizando a sua chave privada. A fim de obter a assinatura digital original em formato legível, o receptor decifra o código *Hash* recebido com a chave pública do emissor (Valor A). Para verificar a exactidão da assinatura digital e a integridade da informação, o receptor gera um código *Hash* com a mensagem original que recebeu (Valor B), e compara este código com o que obteve da decifragem da assinatura digital recebida (Valor A). Se o receptor validar positivamente a assinatura digital com a chave pública do emissor, temos a garantia de que a mensagem foi enviada pelo dono da chave privada e que, simultaneamente, não foi alterada no seu trajecto.

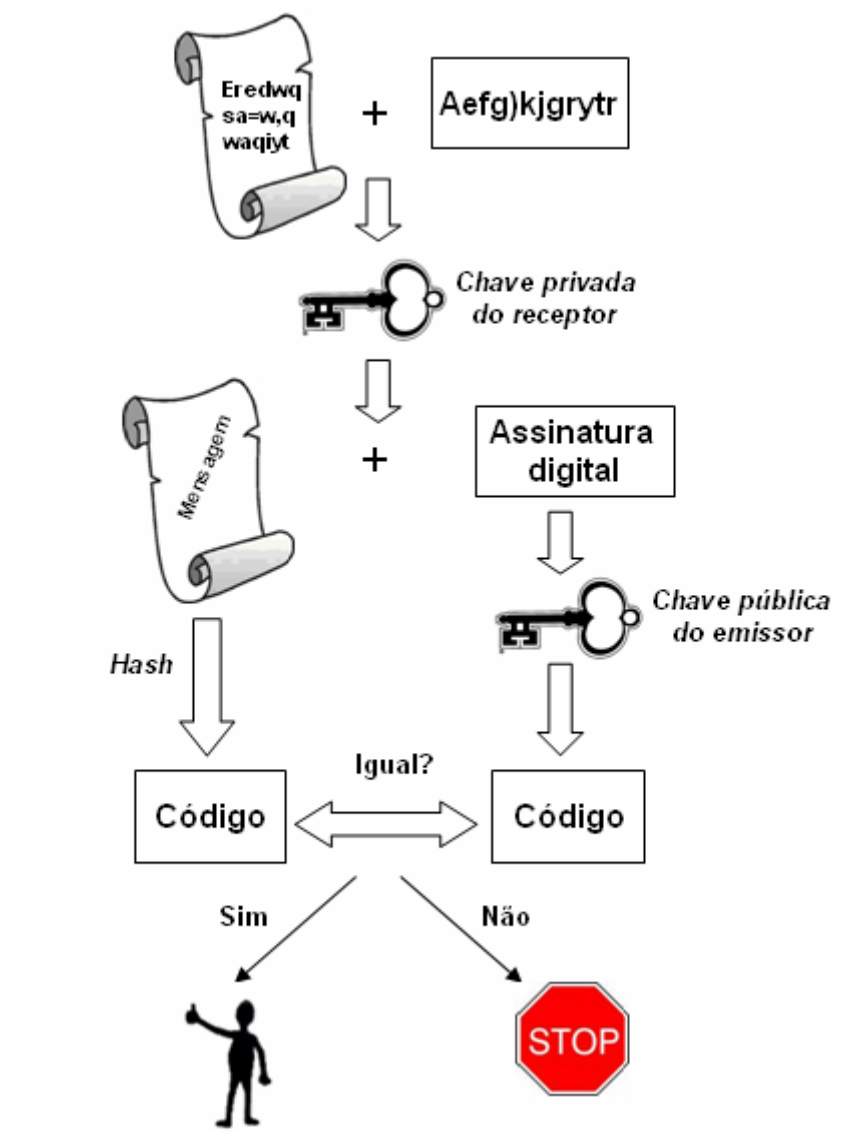

Figura 3 – Processo de validação das mensagens assinadas digitalmente (baseado em [3])

2.1.3 Certificado Digital

Aquando da 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 em 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.

Um certificado digital é um documento electrónico assinado digitalmente, emitido por uma terceira parte de confiança, denominada Entidade Certificadora ou Autoridades de Certificação (CA - *Certification Authority*). Usando metodologias, processos e critérios bem definidos e públicos, a CA regula a gestão dos certificados através da emissão, renovação e revogação dos mesmos, por aprovação individual.

Para criar um certificado digital, a Entidade Certificadora cria um código *Hash* com, entre outros dados, a informação da identidade do utilizador e a sua chave pública. A Entidade Certificadora "assina" esta informação ao utilizar a sua chave privada, criando um código *Hash* cifrado. Esta informação é incluída no certificado a emitir. Se a informação da identidade do utilizador, ou a chave pública contida no certificado digital, for alterada de qualquer forma, o certificado é detectado como inválido.

Para confirmar a integridade de um certificado digital, o receptor:

- Recria o código *Hash* usando o mesmo algoritmo e informação que a Entidade Certificadora utilizou na criação do *Hash* original para o certificado em questão (valor A).
- Decifra o *Hash* existente no Certificado Digital com a Chave Pública da Entidade Certificadora (valor B).
- Compara os dois valores obtidos (A e B) e se estes forem iguais o Certificado Digital apresenta-se como íntegro. Caso contrário, o Certificado Digital sofreu alterações e é inválido.

Para verificar a validade (fiabilidade) de um certificado, além da verificação da sua integridade há que determinar se:

- Uma CA fiável assinou o 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" (CA - *Certificate Policy*).

Embora um certificado tenha uma validade predefinida, poderão surgir situações dentro do prazo de validade que determinem a necessidade de cancelar o certificado. A isto chama-se revogação do certificado e pode ocorrer, por exemplo, nas seguintes situações:

- 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 do uso mal intencionado por parte do titular;
- Término das condições para o qual tinha sido emitido (ex.: 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.

Nestes casos é necessário 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) deve ser depois divulgado por toda a comunidade que eventualmente interaja com ele.

As Listas de Certificados Revogados (CRL – *Certificate Revocation Lists*) são um método de revogação definido pelo standard X.509 e que à semelhança dos certificados digitais baseados neste formato, são uma estrutura de dados que contêm a lista dos certificados revogados. Esta estrutura é assinada digitalmente pela CA que assinou esses certificados quando estes foram emitidos.

Formato do certificado	Versão 3
Nº de Série do certificado	123456789
Identificador do algoritmo de assinatura da EC	RSA com MD5
Endereço X.500 do emissor	C=PT, o=EC
Período de validade	start=01/08/96, expiry=01/08/98
Nome X.500 do utilizador	c=PT, o=organização, cn=João Silva, …
Chave pública do utilizador e método criptográfico utilizado	C.P.U. + RSA com MD5

Tabela 1 – Informação básica de um certificado digital X.509 v3 (não incluindo as extensões v3 standard) (baseado em [3])

2.1.4 Infra-estrutura de chave pública

A Infra-estrutura de Chave pública (PKI) tem como principal objectivo 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 [2]. Esta estrutura é composta por um conjunto de elementos, cada um com funções específicas que, interligados, permitem realizar o objectivo da PKI. São eles:

a) **Autoridades de Certificação (CA - Certification Authority) ou Entidade Certificadora**

Esta entidade é a base de confiança de toda a PKI. Toda a confiança na infra-estrutura depende da sua assinatura.

As funções básicas de uma Entidade Certificadora incluem:

- Aceitar solicitações de utilizadores (por exemplo: browsers, carteiras virtuais) e servidores de rede;
- Efectuar as verificações necessárias quanto ao conteúdo e veracidade das credenciais apresentadas nas solicitações;
- Gerar e emitir certificados digitais.

O processo de criação de certificados é um dos elementos que uma Entidade Certificadora tem que gerir, mas é absolutamente necessária a gestão completa de todo o ambiente de certificados para estabelecer e manter um ambiente de confiança com terceiros.

A possibilidade de uma Entidade Certificadora identificar certificados não confiáveis (por exemplo, certificados revogados) é tão importante e fundamental quanto o processo de emissão. No momento em que a Entidade Certificadora emite um certificado de chave pública, cria uma relação entre a chave pública de um indivíduo (portador da correspondente chave privada) e os dados relativos ao próprio indivíduo (por exemplo, a empresa em que trabalha ou dados do cartão de crédito pessoal).

No entanto, num determinado momento no futuro, e por diversas razões possíveis, a Entidade Certificadora poderá ter que proceder à revogação do certificado previamente emitido por este já não ser de confiança (ver acima exemplos que levam à revogação do certificado). Sem esta capacidade não é possível criar e manter um ambiente de confiança numa rede baseada em criptografia de chaves públicas.

Adicionalmente à criação de certificados confiáveis e à gestão eficaz de processos de revogações, outros aspectos importantes são:

- Geração segura de pares de chaves públicas e chaves simétricas;
- Salvaguarda e uso da componente privada de pares de chaves públicas da Entidade Certificadora num ambiente seguro;
- Actualização, no tempo, das chaves públicas dos utilizadores;
- Certificação cruzada com outras entidades certificadoras;
- Publicação de certificados digitais emitidos num local de acesso público (exemplo: Servidor LDAP ou OCSP);
- Serviço público, em tempo real, para verificação da validade de um certificado;
- Publicação de listas de certificados digitais revogados;

Um aspecto importante para uma Entidade Certificadora é a integridade e publicidade do seu certificado público. Este é utilizado por browsers e servidores de rede com o fim de verificarem a veracidade do conteúdo de certificados de outrém, sendo necessário que cada elemento numa troca de informação possua uma cópia fidedigna do certificado da Entidade Certificadora, e sendo crucial que a chave pública da Entidade Certificadora seja divulgada por um canal de confiança, e que possa ser verificada em qualquer altura por qualquer um dos elementos da cadeia.

A CA que se encontra no topo da hierarquia gera o seu próprio par de chaves;

b) **Autoridade de Registo (RA – *Registration Authority*)**

Providencia a 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 responsabilidade.

c) **Repositório de certificados (*Certificate Repository*)**

Repositório *on-line* robusto e escalável para o armazenamento dos certificados.

d) ***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 a essa infra-estrutura. 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.

e) **Declaração de Práticas de Certificação *(CPS - Certification Practice Statment)***

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 funciona, 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.

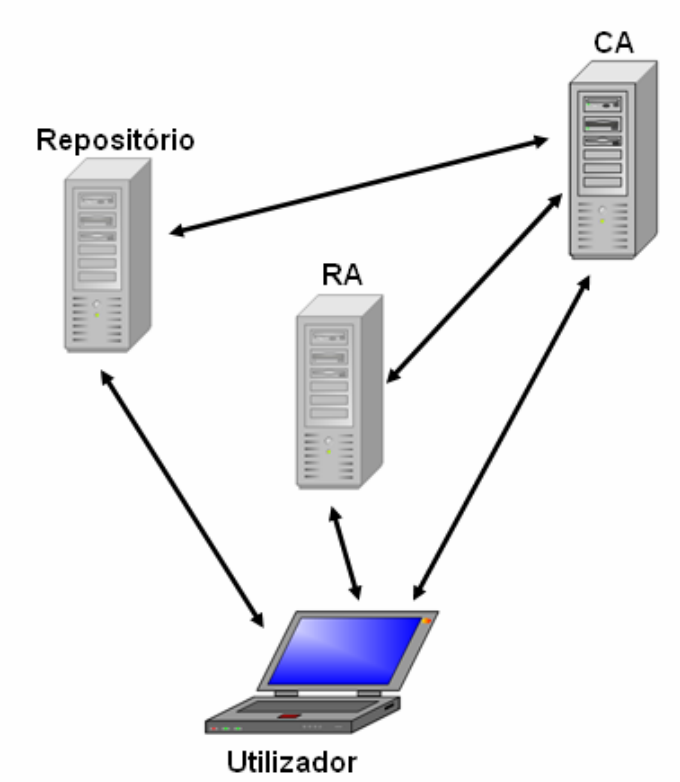

Figura 4 – Infra-estrutura de Chave Pública (baseado em [2])

3. Sistema de Certificação Electrónica do Estado (SCEE)

Decorrente da implementação em curso de vários programas públicos para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não governamentais e o Estado, com vista ao fortalecimento da sociedade de informação e do governo electrónico (*eGovernment*), foi aprovado através da Resolução do Conselho de Ministros n.º 171/2005 (ver anexo I) [4], publicada em Diário da República em 3 de Novembro de 2005 a criação do Sistema de Certificação Electrónica do Estado (SCEE) – Infra-estrutura de Chaves Públicas.
Esses programas envolvem, para certos fins específicos, mecanismos de autenticação digital forte de identidades e assinaturas electrónicas que podem ser concretizados mediante a utilização das denominadas infra-estruturas de chaves públicas [1].
Nesta resolução definiu-se que a arquitectura do SCEE constituirá uma hierarquia de confiança, que promoverá a segurança electrónica do Estado. Para o efeito a SCEE compreenderá um Conselho Gestor que dá parecer sobre a aprovação e integração de entidades certificadoras no SCEE pronunciando-se igualmente sobre práticas e políticas de certificação, uma Entidade Certificadora Electrónica Raiz, que constitui o primeiro nível da cadeia hierárquica de certificação, e as várias Entidades Certificadoras do Estado a esta subordinadas.

No ano de 2006, o Sistema de Certificação Electrónica do Estado (SCEE) foi criado pelo Decreto-Lei n.º 116-A/2006, de 16 de Junho de 2006 (ver anexo II) [5], para assegurar a unidade, a integração e a eficácia dos sistemas de autenticação digital forte nas relações electrónicas de pessoas singulares e colectivas com o Estado e entre entidades públicas.
A arquitectura do SCEE constitui, uma hierarquia de confiança que garante a segurança electrónica do Estado e a autenticação digital forte das transacções electrónicas entre os vários serviços e organismos da Administração Pública e entre o Estado e os cidadãos e as empresas.
O SCEE funciona independentemente de outras infra-estruturas de chaves públicas de natureza privada ou estrangeira, mas permitir a interoperabilidade com as infra-estruturas que satisfaçam os requisitos necessários de rigor de autenticação, através dos mecanismos técnicos adequados, e da compatibilidade em termos de políticas de certificação, nomeadamente no âmbito dos países da União Europeia.
A criação do SCEE foi efectuada, com as devidas adaptações, em conformidade com toda a legislação nacional e comunitária em vigor, nomeadamente a relativa às regras técnicas e de

segurança aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados qualificados.

Foi atribuído neste mesmo Decreto-Lei à Autoridade Nacional de Segurança, as funções de autoridade credenciadora, que até agora se encontravam atribuídas ao Instituto das Tecnologias da Informação da Justiça.

Assim, é criado o Sistema de Certificação Electrónica do Estado Português – Infra-Estrutura de Chaves Públicas, que opera para os organismos e funcionários da Administração Pública bem como para as pessoas singulares e colectivas no seu relacionamento com o Estado. A SCEE estabelece uma estrutura de confiança electrónica, de forma a que os serviços disponibilizados pelas entidades certificadoras que a compõem, proporcionem nomeadamente a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação [6].

3.1. Participantes na infra-estrutura de chaves públicas

Descrevem-se de seguida as entidades que participam na infra-estrutura de chaves públicas do Sistema de Certificação Electrónica do Estado segundo o decreto-lei n.º 116-A/2006.

3.1.1 Entidades Certificadoras (EC) do Estado

São entidades certificadoras do Estado as entidades públicas que exerçam funções de entidade certificadora nos termos do disposto no Decreto-Lei nº 290-D/99, de 2 de Agosto, na redacção introduzida pelo Decreto-Lei nº 62/2003, de 3 de Abril[1], e pelo presente decreto-lei e respectiva regulamentação, e que:

a) Estejam admitidas como entidades certificadoras, nos termos do nº 2 do artigo 5º;

b) Actuem em conformidade com as declarações de práticas de certificação e com a política de certificação e práticas aprovadas pelo Conselho Gestor do SCEE.

Consideram-se também entidades certificadoras do Estado quaisquer entidades que, independentemente da sua natureza, prestem funções de certificação para a realização de fins próprios da Administração Pública.

Só podem prestar serviços de certificação electrónica, no âmbito do SCEE, as entidades reconhecidas como entidades certificadoras do Estado.

[1] **Decreto-Lei nº 62/2003, de 3 de Abril** – Transpõe para a ordem jurídica interna a Directiva 1999/93/CE, de 13 de Dezembro, relativa a um quadro legal comunitário para as assinaturas electrónicas, alterando o Decreto-Lei nº 290-D/99, de 2 de Agosto. Republica, em anexo, o Decreto-Lei n.º 290-D/99, de 2 de Agosto, com as alterações introduzidas (DR n.º 79, I Série A, de 3 de Abril de 2003).

As entidades certificadoras não podem emitir certificados de nível diverso do imediatamente subsequente ao seu, excepto nos casos de acordos de certificação lateral ou cruzada promovidos e aprovados pelo Conselho Gestor do SCEE.

Os serviços de registo podem ser atribuídos a entidades, individuais ou colectivas, designadas como entidades de registo, nas quais as entidades certificadoras do Estado delegam a prestação de serviços de identificação e registo de utilizadores de certificados, bem como a gestão de pedidos de revogação de certificados, nos termos do disposto no nº 1 do artigo 4º do Decreto Regulamentar nº 25/2004, de 15 de Julho[2].

A hierarquia de confiança da Entidade de Certificação Electrónica do Estado (ECEE) compreende a Entidade Certificadora Raiz do Estado (ECRaizEstado), as Entidades Certificadoras do Estado (ECEstado) e Entidades Certificadoras Subordinadas (subECEstado).

As Entidades Certificadoras que compõem o SCEE são:

- ECEE como Entidade de Certificação de primeiro nível.
  A sua função é estabelecer a raiz da cadeia de confiança da infra-estrutura de chaves públicas (PKI). Esta EC não emite certificados para utilizadores finais, emitindo apenas certificados para assinar as Entidades Certificadoras do Estado. A "ECEE" assina-se a si própria.
- As EC são entidades que se encontram no nível imediatamente abaixo da EC Raiz, sendo a sua função principal providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação para os seus subscritores. O seu certificado é assinado pela EC Raiz.
- As subEC, são entidades que se encontram no nível imediatamente abaixo das EC, tendo como função a prestação de serviços de certificação para o utilizador final. O seu certificado é assinado pela respectiva EC.

As Entidades Certificadoras constituídas no âmbito da ECEE, deverão disponibilizar uma versão completa da sua Declaração de Práticas de Certificação (DPC).

Entidade Certificadora Raiz do Estado

A Entidade de Certificação Electrónica do Estado é a certificadora Raiz do Estado é a entidade certificadora de topo da cadeia de certificação da SCEE, executora das políticas de certificados e directrizes aprovadas pela Entidade Gestora de Políticas de Certificação. Compete a esta prestar os serviços de certificação às Entidades Certificadoras do Estado no nível hierárquico imediatamente inferior ao seu na cadeia de certificação em conformidade com as normas aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados digitais qualificados.

[2] **Decreto Regulamentar nº 25/2004, de 15 de Julho** – Estabelece as regras técnicas e de segurança aplicáveis às entidades certificadoras estabelecidas em Portugal, na emissão de certificados qualificados (DR n.º 165, I Série B, de 15 de Julho de 2004).

Compete à Entidade de Certificação Electrónica do Estado obter o certificado de credenciação referido no nº 2 do artigo 8º (Decreto-Lei n.º 116-A/2006).

A Entidade de Certificação Electrónica do Estado disponibiliza exclusivamente os seguintes serviços de certificação digital:

a) Processo de registo das entidades certificadoras;
b) Geração de certificados, incluindo certificados qualificados, e gestão do seu ciclo de vida;
c) Disseminação dos certificados, das políticas e das práticas de certificação;
d) Gestão de revogações de certificados;
e) Disponibilização do estado e da situação das revogações referidas na alínea anterior.

Compete, ainda, à Entidade de Certificação Electrónica do Estado:

f) Garantir o cumprimento e a implementação enquanto entidade certificadora de todas as regras e todos os procedimentos estabelecidos no documento de políticas de certificação e na declaração de práticas de certificação do SCEE; Implementar as políticas e práticas do Conselho Gestor do SCEE;
g) Gerir toda a infra-estrutura e os recursos que compõem e garantem o funcionamento da entidade certificadora raiz do Estado, nomeadamente o pessoal, os equipamentos e as instalações;
h) Gerir todas as actividades relacionadas com a gestão do ciclo de vida dos certificados por si emitidos para as entidades certificadoras de nível imediatamente inferior ao seu;
i) Garantir que o acesso às suas instalações principal e alternativa é efectuado apenas por pessoal devidamente autorizado e credenciado;
j) Gerir o recrutamento de pessoal tecnicamente habilitado para a realização das tarefas de gestão e operação da entidade certificadora raiz do Estado;
k) Comunicar imediatamente qualquer incidente, nomeadamente anomalias ou falhas de segurança, ao Conselho Gestor do SCEE.

A Entidade de Certificação Electrónica do Estado emite exclusivamente certificados para as entidades certificadoras do Estado subordinadas, não podendo emitir certificados destinados ao público.

A Entidade de Certificação Electrónica do Estado é dirigida, por inerência, pelo director do Centro de Gestão da Rede Informática do Governo (CEGER).

3.1.2 Entidades de Registo (ER)

São entidades que por via do estabelecimento de um acordo com uma Entidade Certificadora do Estado, estas delegam a prestação de serviços de identificação e registo de utilizadores, bem como a gestão de pedidos de revogação de certificados.

As Entidades de Registo desenvolvem a sua actividade de acordo com o estabelecido na DPC da respectiva EC e pela EGPC.

3.1.3 Titulares de Certificados

O subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados por uma ECEstado ou subECEstado.

No âmbito do SCEE são considerados como titulares, aqueles em que o nome está inscrito no campo *Subject* do certificado e utilizam o certificado e respectiva chave privada de acordo com o estabelecido nas diversas politicas de certificado, sendo consideradas as seguintes categorias titulares:

- Pessoa singular;
- Pessoa colectiva;
- Equipamentos tecnológicos.

Não são considerados titulares, as seguintes categorias:

- Entidade Certificadoras, independentemente do nível a que se encontram;
- Entidades de Registo;
- O pessoal das Entidades Certificadoras e Entidades de Registo cujos certificados tem como uso exclusivo a operação dos respectivos sistemas.

3.1.4 Partes Confiantes

As partes confiantes ou destinatários são pessoas singulares, entidades ou equipamentos que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação do nome do titular com a sua chave pública, ou seja que o certificado corresponde na realidade a quem diz pertencer.

Na prática, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado, podendo ser titular de certificados da comunidade SCEE ou não.

3.1.5 Outros participantes

Conselho Gestor do Sistema de Certificação Electrónico do Estado

Segundo o Decreto-Lei nº 116-A/2006, de 16 Junho (ver anexo II), o Conselho Gestor do Sistema de Certificação Electrónica do Estado é o órgão responsável pela gestão global e administração do SCEE.

Compete especialmente ao Conselho Gestor do SCEE:

a) Definir, de acordo com a lei e tendo em conta as normas ou especificações internacionalmente reconhecidas, a política de certificação e as práticas de certificação a observar pelas entidades certificadoras que integram o SCEE;
b) Garantir que as declarações de práticas de certificação das várias entidades certificadoras do Estado, bem como da entidade certificadora raiz do Estado, estão em conformidade com a política de certificação do SCEE;

c) Propor os critérios para aprovação das entidades certificadoras que pretendam integrar o SCEE;
d) Aferir a conformidade dos procedimentos seguidos pelas entidades certificadoras do Estado com as políticas e práticas aprovadas, sem prejuízo das competências legalmente cometidas à autoridade credenciadora;
e) Pronunciar-se pela exclusão do SCEE das entidades certificadoras do Estado em caso de não conformidade com as políticas e práticas aprovadas, comunicando tal facto à autoridade credenciadora;
f) Pronunciar-se sobre as melhores práticas internacionais no exercício das actividades de certificação electrónica e propor a sua aplicação;
g) Representar institucionalmente o SCEE.

Compete, ainda, ao Conselho Gestor do SCEE a promoção das actividades necessárias para o estabelecimento de acordos de interoperabilidade, com base em certificação cruzada, com outras infra-estruturas de chaves públicas, de natureza privada ou pública, nacionais ou internacionais, nomeadamente:

a) Dar indicações à entidade certificadora raiz do Estado para a atribuição e a revogação de certificados emitidos com base em certificação cruzada;
b) Definir os termos e condições para o início, a suspensão ou a finalização dos procedimentos de interoperabilidade com outras infra-estruturas de chaves públicas.

O Conselho Gestor do SCEE é presidido pelo Ministro da Presidência, com faculdade de delegação, e composto por representantes de cada uma das seguintes entidades, designados pelos competentes membros do Governo:

- Agência para a Sociedade do Conhecimento (UMIC);
- Centro de Gestão da Rede Informática do Governo (CEGER);
- Fundação para a Computação e Cálculo Científico Nacional (FCCN);
- Gabinete Nacional de Segurança (GNS);
- Instituto das Comunicações de Portugal (ICP – ANACOM);
- Instituto de Informática (II no MF);
- Instituto de Telecomunicações (IT);
- Instituto das Tecnologias da Informação na Justiça (ITIJ);
- Rede Nacional de Segurança (no MAI);
- Unidade Coordenadora para a Modernização Administrativa (UCMA).

Autoridade Credenciadora

O Decreto-Lei 116-A/2006, de 16 de Junho (ver Anexo II), procede à criação do Sistema de Certificação Electrónica do Estado – Infra-estrutura de Chaves Públicas e designa também a Autoridade Nacional de Segurança como autoridade credenciadora nacional, nos termos do artigo 3º do Decreto-Lei nº 217/97, de 20 de Agosto.

No âmbito da aplicação do artigo 1º deste Decreto-Lei , a Autoridade Nacional de Segurança é competente para emitir o certificado de credenciação das entidades certificadoras e exercer as

competências de credenciação previstas no Decreto-Lei nº 290-D/99, de 2 de Agosto, alterado pelo Decreto-Lei nº 62/2003, de 3 de Abril[3], e na redacção introduzida pelo presente decreto-lei.

Autoridade Nacional de Segurança é assistida no exercício das suas competências, pelo conselho técnico de credenciação.

De uma forma geral o papel da Autoridade Credenciadora, no domínio da SCEE, está relacionado com a disponibilização de serviços de auditoria/inspecção de conformidade, no sentido de aferir se os processos utilizados pelas EC nas suas actividades de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos neste documento e com o estabelecido na DPC da respectiva entidade.

Assim, consideram-se como principais atribuições as seguintes:

- A condução de auditorias;
- A gestão do controlo de qualidade de todo o processo de certificação;
- A fixação de procedimentos e documentação relativa às auditorias;
- Gestão dos relatórios de auditoria, nomeadamente, na elaboração e recepção (quando efectuados por pessoal externo);
- A fixação de planos de medidas correctivas aplicáveis às entidades certificadoras da SCEE;
- A fixação e acompanhamento de metas para indicadores de qualidade que deverá propor para aprovação do Conselho Gestor do SCEE no contexto de objectivos estratégicos previamente fixados pelo Conselho Gestor do SCEE;
- A gestão da bolsa de auditores;
- A apresentação à ECEE de proposta de registo e de rescisão de registo de entidades certificadoras na SCEE;
- A promoção da competência técnica dos auditores.

Autoridades de Validação

As Autoridades de Validação (AV), tem como função comprovar o estado dos certificados emitidos, através da utilização do protocolo *Online Certificate Status Protocol* (OCSP), de forma a determinar o estado actual do certificado a pedido de uma entidade sem necessidade de recorrer à verificação do estado através da consulta das LCR.

[3] **Decreto-Lei n.º 62/2003, de 3 de Abril –** Transpõe para a ordem jurídica interna a Directiva 1999/93/CE, de 13 de Dezembro, relativa a um quadro legal comunitário para as assinaturas electrónicas, alterando o Decreto-Lei nº 290-D/99, de 2 de Agosto. Republica, em anexo, o Decreto-Lei n.º 290-D/99, de 2 de Agosto, com as alterações introduzidas (DR n.º 79, I Série A, de 3 de Abril de 2003).

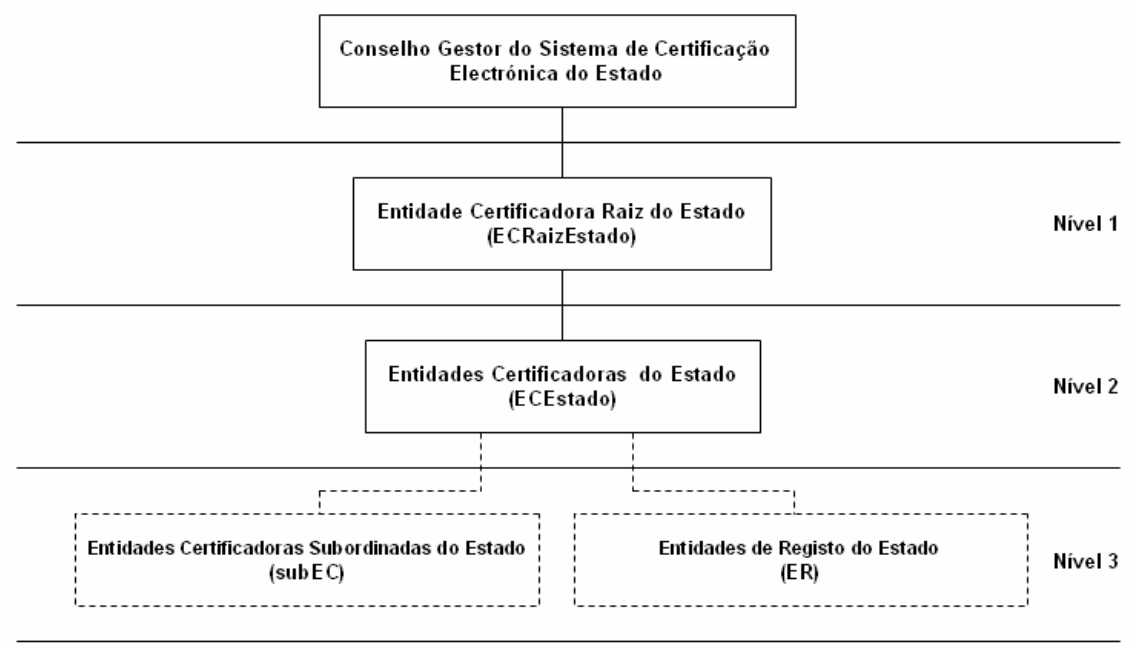

Figura 5 – Arquitectura funcional da ECEE (baseado em [1])

3.2. Utilização do Certificado

Os certificados emitidos no domínio do SCEE são utilizados, pelos diversos sistemas, aplicações, mecanismos e protocolos, com o objectivo de garantir os seguintes serviços de segurança:

a) Controlo de acessos;
b) Confidencialidade;
c) Integridade;
d) Autenticação;
e) Não repúdio.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a SCEE proporciona. Assim, os serviços de identificação e autenticação, integridade e não repúdio são obtidos mediante a utilização de assinaturas digitais. A confidencialidade é garantida através dos recursos a algoritmos de cifra, quando conjugados com mecanismos de estabelecimento e distribuição de chaves [6].

3.3. Identificação e Autenticação

Todos os titulares de certificados requerem um nome único (DN - *Distinguished Name*) de acordo com o standard X.500.

Os certificados atribuídos a cada entidade deverão conter no campo *Subject*, um DN, para utilização como identificador único de cada entidade, de acordo com o preconizado no RFC 3280, pelo que:

a) Para os certificados emitidos a pessoas, o atributo descreve a organização a que o titular do certificado pertence;
b) Nos certificados atribuídos a equipamentos, é inscrito o nome da organização responsável pela sua operação (patrocinador);
c) O DN deverá ser sempre preenchido.

O campo *Subject* deverá ser construído através dos seguintes atributos obrigatórios:

Atributo	Código	Regras para preenchimento
CountryName	C	Incluir o código “PT”
OrganizationName	O	Este campo corresponde, regra geral, ao Ministério (ou equivalente) do titular do certificado.
OrganizationUnitName	OU	Neste campo deverá constar informação relativa ao organismo (ou equivalente) a que o titular do certificado pertence.
CommonName	CN	É proibida a utilização de *nicknames*. Os equipamentos deverão ser identificados através do modelo e número de série. Se os equipamentos forem servidores, estes serão designados pelo FQDN (CN = “FQDN”.), sendo proibida a sua designação através do endereço IP. Nos certificados emitidos para pessoa colectiva, deverá ser incluído o nome da pessoa singular responsável pela sua utilização. Quando se trate de nomes reais, deverá corresponder com o nome que aparece identificado no documento de Identificação. Quando se trate de pseudónimos, o nome deverá ser antecedido da expressão “Pseudo:”.

Tabela 2 – Identificação e autenticação (baseado em [6])

4. Conclusão

Ao longo deste documento numa primeira fase descreveu-se as definições que estão em torno da área da certificação digital. Nesta fase tentou-se clarificar algumas das propriedades que um sistema de efectue transacções pela rede deve garantir, tais como segurança, autenticidade, integridade, etc.

Numa segunda fase, após descrição dos conceitos base, instanciou-se esta matéria com um sistema real, o Sistema de Certificação Electrónica do Estado, o qual foi criado pelo Decreto-Lei n.º 116-A/2006, de 16 de Junho de 2006 (ver anexo II), para assegurar a unidade, a integração e a eficácia dos sistemas de autenticação digital forte nas relações electrónicas de pessoas singulares e colectivas com o Estado e entre entidades públicas [1].

De uma forma geral foi estudado todo o contexto envolvente, pela análise da legislação nacional em vigor. No entanto apenas foram realçados os pontos mais relevantes, não se entrando de forma detalhada na descrição de toda a politica de certificados do SCEE.

A realização deste trabalho além de estar no âmbito da matéria e avaliação da cadeira de "Segurança e Privacidade em Sistemas de Armazenamento e Transporte de Dados" do mestrado em Sistemas de Dados e Processamento Analítico, também se revelou importante para a contextualização e análise da legislação inerente a esta matéria, a qual está a ser colocada em prática em projectos no qual me encontro envolvido. É aqui que se torna aliciante a passagem de uma teoria e legislação existente para a prática que ainda está numa fase embrionária ou inexistente no contexto das entidades públicas. O objectivo geral é disponibilizar aos utilizadores de uma determinada entidade pública documentos em formato digital certificados digitalmente, que garantam as mesmas propriedades que os documentos (certidões) disponibilizados pela forma tradicional. É certamente este o principal alvo a atingir e que deve ser assegurado pelo SCEE, o qual foi analisado ao longo deste documento.

Referências

1. SCEE. *Sistema de Certificação Electrónica do Estado*. [cited; Available from: http://www.scee.gov.pt/.

2. Anabela Moreira Bernardino, A.C., Eugénia Moreira Bernardino, Rafael Relvão, *Autenticação: Mestrado e Curso de Especialização em Sistemas de Informação Tecnologias para o Comércio Electrónico*. 2004, Universidade do Minho.

3. Multicert. *Multicert - Serviços de Certificação Electrónica S.A.* [cited; Available from: http://www.multicert.pt/.

4. República, D., *Resolução do Conselho de Ministros n.º 171/2005.* 2005.

5. República, D., *Decreto-Lei Nº116-A/2006 Criação SCEE.* 2006.

6. SCEE, *Política de Certificados do SCEE*. 2006.

Anexos

I. Resolução do Conselho de Ministros nº171/2005

6284 DIÁRIO DA REPÚBLICA — I SÉRIE-B N.º 211 — 3 de Novembro de 2005

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Resolução do Conselho de Ministros n.º 171/2005

Os programas públicos para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não governamentais e o Estado, com vista ao fortalecimento da sociedade da informação e do governo electrónico *(eGovernment)*, envolvem, para certos fins específicos, mecanismos de autenticação digital forte de identidades e assinaturas electrónicas que podem ser concretizados mediante a utilização das denominadas infra-estruturas de chaves públicas.

Exemplos de projectos programados ou em curso no âmbito da sociedade da informação e do governo electrónico são os relativos ao cartão do cidadão, ao passaporte electrónico português, à disponibilização de serviços da Administração Pública pela Internet que requeiram autenticação digital forte de identidades e assinaturas electrónicas e à desmaterialização dos processos intra e interorganismos do Estado que requeiram esse tipo de autenticação.

Assim, para assegurar a unidade dos sistemas de autenticação digital forte nas relações electrónicas de pessoas singulares e colectivas com o Estado e entre entidades públicas, é necessário estabelecer uma entidade de certificação electrónica do Estado.

Esta entidade deve funcionar independentemente de infra-estruturas de chaves públicas privadas ou estrangeiras, mas deve permitir a interoperabilidade com as infra-estruturas que satisfaçam os requisitos necessários de rigor de autenticação, através dos mecanismos técnicos adequados, nomeadamente no âmbito dos países da União Europeia (UE).

A análise de infra-estruturas de chaves públicas de outros Estados, a avaliação da necessidade de criação de um destes sistemas para o Estado Português e a proposta de recomendações para a sua constituição foram objecto de um estudo levado a cabo pela UMIC — Agência para a Sociedade do Conhecimento, I. P., em colaboração com a Fundação para a Computação Científica Nacional (FCCN), a Autoridade Nacional de Comunicações (ICP — ANACOM) e o Gabinete Nacional de Segurança (GNS).

O Governo decide, assim, criar e desencadear a colocação em funcionamento de uma Entidade de Certificação Electrónica do Estado — Infra-Estrutura de Chaves Públicas, que garanta a satisfação das necessidades da sociedade e do Estado nesta área, designando um grupo de trabalho para acompanhar o processo de instalação.

Assim:

Nos termos da alínea *g*) do artigo 199.º da Constituição, o Conselho de Ministros resolve:

1 — Aprovar a criação da Entidade de Certificação Electrónica do Estado — Infra-Estrutura de Chaves Públicas (ECEE), nas suas componentes legal, orgânica e operacional, encarregando o Secretário de Estado da Presidência do Conselho de Ministros de coordenar o respectivo processo de instalação.

2 — Determinar que o processo de instalação deve assegurar os seguintes objectivos:

a) Definição da estrutura de gestão e do modelo de organização das autoridades certificadoras a adoptar para a ECEE;
b) Elaboração dos projectos de diploma destinados a regular o funcionamento da ECEE, nomeadamente nas matérias respeitantes à definição das políticas de certificação, às práticas de certificação, à inspecção e à credenciação de entidades certificadoras;
c) Identificação das entidades e dos órgãos intervenientes no processo de implementação e de operação da ECEE;
d) Definição e preparação da localização física da autoridade certificadora de raiz, bem como de uma sua localização alternativa;
e) Aquisição de todos os bens, serviços e infra-estruturas necessários para a instalação e colocação em funcionamento da ECEE;
f) Compatibilização do quadro normativo regulador da ECEE com as recomendações técnicas internacionais e com os normativos aplicáveis às organizações internacionais de que Portugal faz parte, de modo a garantir a futura interoperabilidade com outras infra-estruturas de chaves públicas, através dos mecanismos técnicos apropriados;
g) Habilitação da ECEE para emitir certificados digitais que suportem autenticação forte de identidades, assinaturas electrónicas e integridade, privacidade e não repúdio de comunicações certificadas com as chaves fornecidas pela infra-estrutura;
h) Dotação da ECEE de mecanismos de compatibilidade transversal que garantam a necessária integração de funcionalidades para a sua utilização por serviços como comércio electrónico, correio electrónico pessoal e institucional, distribuição de publicações electrónicas que requeiram integridade de comunicações e ou autenticação forte de identidades, encriptação de mensagens, serviços Web, serviços de directório, configuração e manutenção de dispositivos de rede.

3 — Determinar que o processo de instalação é acompanhado por um grupo de trabalho, com funções de assessoria técnica, constituído por representantes das seguintes entidades:

a) Unidade de Coordenação da Modernização Administrativa (UCMA);
b) Agência para a Sociedade do Conhecimento, I. P (UMIC);
c) Autoridade Nacional de Comunicações (ICP — ANACOM);
d) Gabinete Nacional de Segurança (GNS);
e) Fundação para a Computação Científica Nacional (FCCN);
f) Instituto de Telecomunicações (IT);
g) Centro de Gestão da Rede Informática do Governo (CEGER);
h) Instituto das Tecnologias da Informação na Justiça (ITIJ);
i) Centro de Instalação da Rede Nacional de Segurança Interna.

4 — Estabelecer que os membros do grupo de trabalho são nomeados pela entidade a que pertencem, no prazo de 15 dias contados da data de publicação da presente resolução.

5 — Estabelecer que o grupo de trabalho referido nos números anteriores reporta ao Secretário de Estado da Presidência do Conselho de Ministros, o qual articula com os demais membros do Governo competentes em razão da matéria.

6 — Determinar que os membros do grupo de trabalho não auferem, pelas funções que desempenhem a esse título, qualquer vencimento, suplemento remuneratório ou senhas de presença, sem prejuízo do abono de ajudas de custo a que eventualmente tenham direito.

7 — Determinar que, no âmbito da sua actuação, pode o grupo de trabalho solicitar a cooperação dos serviços e organismos da administração directa e indirecta do Estado.

8 — Estabelecer que o mandato do grupo de trabalho tem a duração de 90 dias contados da data da publicação da presente resolução, que pode ser prorrogado até um prazo de 60 dias, por despacho do membro do Governo que o tutela.

9 — Determinar que os encargos orçamentais, de mero funcionamento, decorrentes da presente resolução sejam suportados por verbas do orçamento da Secretaria-Geral da Presidência do Conselho de Ministros, à qual compete ainda o apoio administrativo e logístico ao grupo de trabalho.

10 — Estabelecer que a presente resolução produz efeitos desde o dia seguinte ao da sua publicação.

Presidência do Conselho de Ministros, 6 de Outubro de 2005. — O Primeiro-Ministro, *José Sócrates Carvalho Pinto de Sousa.*

MINISTÉRIOS DO AMBIENTE, DO ORDENAMENTO DO TERRITÓRIO E DO DESENVOLVIMENTO REGIONAL E DA AGRICULTURA, DO DESENVOLVIMENTO RURAL E DAS PESCAS.

Portaria n.º 1136/2005

de 3 de Novembro

Pela Portaria n.º 657/2003, de 30 de Julho, alterada pela Portaria n.º 404/2004, de 22 de Abril, foi renovada até 25 de Junho de 2012 a zona de caça turística de Vasco Martins e outras, processo n.º 922-DGRF, englobando vários prédios rústicos sitos nos municípios de Beja e Mértola, com uma área de 1956 ha, e concessionada à Herdade da Cascalheira — Sociedade Agro-Pecuária, L.da

Vem agora a Caçadores de Demangas — Sociedade de Exploração de Caça e Turismo, L.da, requerer a transmissão da concessão da zona de caça atrás citada.

Assim:

Com fundamento no disposto no artigo 45.º e no n.º 1 do artigo 118.º do Decreto-Lei n.º 202/2004, de 18 de Agosto:

Manda o Governo, pelos Ministros do Ambiente, do Ordenamento do Território e do Desenvolvimento Regional e da Agricultura, do Desenvolvimento Rural e das Pescas, o seguinte:

Pela presente portaria, a zona de caça turística de Vasco Martins e outras, processo n.º 922-DGRF, situada nas freguesias de Quintos e Mértola, municípios de Beja e Mértola, é transferida para a Caçadores de Demangas — Sociedade de Exploração de Caça e Turismo, L.da, com o número de pessoa colectiva 505798913 e sede no Edifício Espaço Chiado, Rua da Misericórdia, 14, 6.º, 1249-038 Lisboa.

Pelo Ministro do Ambiente, do Ordenamento do Território e do Desenvolvimento Regional, *Humberto Delgado Ubach Chaves Rosa,* Secretário de Estado do Ambiente, em 14 de Outubro de 2005. — Pelo Ministro da Agricultura, do Desenvolvimento Rural e das Pescas, *Rui Nobre Gonçalves,* Secretário de Estado do Desenvolvimento Rural e das Florestas, em 19 de Setembro de 2005.

MINISTÉRIOS DA ECONOMIA E DA INOVAÇÃO E DA AGRICULTURA, DO DESENVOLVIMENTO RURAL E DAS PESCAS

Portaria n.º 1137/2005

de 3 de Novembro

Com fundamento no disposto no n.º 3 do artigo 164.º do Decreto-Lei n.º 202/2004, de 18 de Agosto, e na alínea *a*) do n.º 2 do artigo 36.º do Decreto-Lei n.º 227-B/2000, de 15 de Setembro, com as alterações introduzidas pelo Decreto-Lei n.º 338/2001, de 26 de Dezembro;

Ouvido o Conselho Cinegético Municipal de Gavião:

Manda o Governo, pelos Ministros da Economia e da Inovação e da Agricultura, do Desenvolvimento Rural e das Pescas, o seguinte:

1.º Pela presente portaria é concessionada, pelo período de seis anos, renovável automaticamente por um único e igual período, à BIOQUITO — Sociedade de Gestão Agrícola, L.da, com o número de pessoa colectiva 505140250 e sede na Quinta dos Garfos, 6040 Gavião, a zona de caça turística da Fonte dos Garfos (processo n.º 4093-DGRF), englobando vários prédios rústicos sitos na freguesia e município de Gavião, com a área de 945 ha, conforme planta anexa à presente portaria e que dela faz parte integrante.

2.º A Direcção-Geral do Turismo emitiu, ao abrigo do disposto no n.º 3 do artigo 34.º do Decreto-Lei n.º 227-B/2000, de 15 de Setembro, com as alterações introduzidas pelo Decreto-Lei n.º 338/2001, de 26 de Dezembro, parecer favorável condicionado à aprovação do projecto de arquitectura do pavilhão de caça, à conclusão da obra no prazo de 12 meses a contar da data de notificação da aprovação do projecto, à verificação da conformidade da obra com o projecto aprovado e ao enquadramento legal do alojamento previsto a médio prazo, caso venha a ser destinado à exploração turística.

3.º A zona de caça concessionada pela presente portaria produz efeitos relativamente a terceiros com a instalação da respectiva sinalização.

4.º A sinalização da zona de caça deve obedecer ao disposto no n.º 8.º da Portaria n.º 1391/2002, de 25 de Outubro, com a redacção que lhe foi conferida pela Portaria n.º 45/2004, de 14 de Janeiro.

Em 9 de Setembro de 2005.

Pelo Ministro da Economia e da Inovação, *Bernardo Luís Amador Trindade,* Secretário de Estado do Turismo. — Pelo Ministro da Agricultura, do Desenvolvimento Rural e das Pescas, *Rui Nobre Gonçalves,* Secretário de Estado do Desenvolvimento Rural e das Florestas.

II. Decreto-Lei nº 116-A/2006 de 16 Junho de 2006

4330-(4) DIÁRIO DA REPÚBLICA — I SÉRIE-A N.º 115 — 16 de Junho de 2006

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Decreto-Lei n.º 116-A/2006

de 16 de Junho

Decorrente da implementação em curso de vários programas públicos para a promoção das tecnologias de informação e comunicação e da introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não governamentais e o Estado, com vista ao fortalecimento da sociedade de informação e do governo electrónico *(e-government)*, foi aprovada, através da Resolução do Conselho de Ministros n.º 171/2005, de 3 de Novembro, a criação da Entidade de Certificação Electrónica do Estado — Infra-Estrutura de Chaves Públicas (ECEE-ICP).

Esses programas envolvem, para certos fins específicos, mecanismos de autenticação digital forte de identidades e assinaturas electrónicas que podem ser concretizados mediante a utilização das denominadas infra-estruturas de chaves públicas.

Assim, para assegurar a unidade, a integração e a eficácia dos sistemas de autenticação digital forte nas relações electrónicas de pessoas singulares e colectivas com o Estado e entre entidades públicas é necessário estabelecer um sistema de certificação electrónica do Estado (SCEE).

A arquitectura do SCEE constitui, assim, uma hierarquia de confiança que garante a segurança electrónica do Estado e a autenticação digital forte das transacções electrónicas entre os vários serviços e organismos da Administração Pública e entre o Estado e os cidadãos e as empresas.

O SCEE compreende o Conselho Gestor, que estabelece as políticas e práticas de certificação, e a Entidade de Certificação Electrónica do Estado, que aprova a integração de entidades certificadoras no SCEE e que, enquanto entidade certificadora raiz do Estado, constitui o primeiro nível da cadeia hierárquica de certificação relativamente às várias entidades certificadoras do Estado a esta subordinadas.

O SCEE funciona independentemente de outras infra-estruturas de chaves públicas de natureza privada ou estrangeira, mas deve permitir a interoperabilidade com as infra-estruturas que satisfaçam os requisitos necessários de rigor de autenticação, através dos mecanismos técnicos adequados, e da compatibilidade em termos de políticas de certificação, nomeadamente no âmbito dos países da União Europeia.

A criação do SCEE é efectuada, com as devidas adaptações, em conformidade com toda a legislação nacional e comunitária em vigor, nomeadamente a relativa às regras técnicas e de segurança aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados qualificados.

O presente decreto-lei comete ainda à Autoridade Nacional de Segurança as funções de autoridade credenciadora, que até agora se encontravam atribuídas ao Instituto das Tecnologias da Informação da Justiça.

A atribuição destas funções à Autoridade Nacional de Segurança justifica-se pela especial aptidão que esta entidade possui para actuar como autoridade credenciadora, bem como pelo facto de se encontrar integrada na Presidência do Conselho de Ministros e garantir forte hierarquia de segurança.

Assim:

Nos termos da alínea *a*) do n.º 1 do artigo 198.º da Constituição, o Governo decreta o seguinte:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objecto e âmbito

1 — É criado o Sistema de Certificação Electrónica do Estado — Infra-Estrutura de Chaves Públicas, adiante designado abreviadamente por SCEE, destinado a estabelecer uma estrutura de confiança electrónica, de forma que as entidades certificadoras que lhe estão subordinadas disponibilizem serviços que garantam:

a) A realização de transacções electrónicas seguras;
b) A autenticação forte;
c) Assinaturas electrónicas de transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade, não repúdio e confidencialidade.

2 — O SCEE opera para as entidades públicas e para os serviços e organismos da Administração Pública ou outras entidades que exerçam funções de certificação no cumprimento de fins públicos daquela.

Artigo 2.º

Estrutura e funcionamento do SCEE

1 — O SCEE compreende:

a) O Conselho Gestor do Sistema de Certificação Electrónica do Estado;
b) A Entidade de Certificação Electrónica do Estado;
c) As entidades certificadoras do Estado.

2 — O funcionamento do SCEE obedece às regras estabelecidas no presente decreto-lei.

CAPÍTULO II

Conselho Gestor do SCEE

Artigo 3.º

Composição e funcionamento

1 — O Conselho Gestor do SCEE é o órgão responsável pela gestão global e administração do SCEE.

2 — O Conselho Gestor do SCEE é presidido pelo Ministro da Presidência, com faculdade de delegação, e composto por representantes de cada uma das seguintes entidades, designados pelos competentes membros do Governo:

a) Agência para a Sociedade do Conhecimento, I. P. (UMIC);
b) Centro de Gestão da Rede Informática do Governo (CEGER);
c) Fundação para a Computação Científica Nacional (FCCN);
d) Gabinete Nacional de Segurança (GNS);

e) ICP — Autoridade Nacional de Comunicações (ICP — ANACOM);
f) Instituto de Informática (II);
g) Instituto de Telecomunicações (IT);
h) Instituto das Tecnologias de Informação na Justiça (ITIJ);
i) Rede Nacional de Segurança Interna;
j) Unidade de Coordenação da Modernização Administrativa (UCMA).

3 — Salvo indicação expressa em contrário no acto de designação, o membro do Governo indicado nos termos do número anterior pode delegar a presidência em qualquer membro do Conselho Gestor do SCEE.

4 — O Conselho Gestor do SCEE pode solicitar a colaboração de outras entidades públicas, bem como de entidades privadas ou de individualidades, para a análise de assuntos de natureza técnica especializada, no âmbito das competências que lhe são cometidas pelo presente decreto-lei.

5 — O Conselho Gestor do SCEE reúne, de forma ordinária, duas vezes por ano e, de forma extraordinária, por convocação do seu presidente.

6 — O apoio técnico, logístico e administrativo ao Conselho Gestor do SCEE bem como os encargos inerentes ao seu funcionamento são da responsabilidade da entidade à qual é cometida a função de operação da entidade certificadora raiz do Estado.

7 — Os membros do Conselho Gestor do SCEE não têm direito a auferir suplemento remuneratório pelo desempenho das suas funções, sem prejuízo da possibilidade do percebimento de abonos ou ajudas de custo, nos termos gerais.

Artigo 4.º

Competências

1 — Compete ao Conselho Gestor do SCEE:

a) Definir, de acordo com a lei e tendo em conta as normas ou especificações internacionalmente reconhecidas, a política de certificação e as práticas de certificação a observar pelas entidades certificadoras que integram o SCEE;
b) Garantir que as declarações de práticas de certificação das várias entidades certificadoras do Estado, bem como da entidade certificadora raiz do Estado, estão em conformidade com a política de certificação do SCEE;
c) Propor os critérios para aprovação das entidades certificadoras que pretendam integrar o SCEE;
d) Aferir a conformidade dos procedimentos seguidos pelas entidades certificadoras do Estado com as políticas e práticas aprovadas, sem prejuízo das competências legalmente cometidas à autoridade credenciadora;
e) Pronunciar-se pela exclusão do SCEE das entidades certificadoras do Estado em caso de não conformidade com as políticas e práticas aprovadas, comunicando tal facto à autoridade credenciadora;
f) Pronunciar-se sobre as melhores práticas internacionais no exercício das actividades de certificação electrónica e propor a sua aplicação;
g) Representar institucionalmente o SCEE.

2 — Compete, ainda, ao Conselho Gestor do SCEE a promoção das actividades necessárias para o estabelecimento de acordos de interoperabilidade, com base em certificação cruzada, com outras infra-estruturas de chaves públicas, de natureza privada ou pública, nacionais ou internacionais, nomeadamente:

a) Dar indicações à entidade certificadora raiz do Estado para a atribuição e a revogação de certificados emitidos com base em certificação cruzada;
b) Definir os termos e condições para o início, a suspensão ou a finalização dos procedimentos de interoperabilidade com outras infra-estruturas de chaves públicas.

CAPÍTULO III

Entidade de Certificação Electrónica do Estado

Artigo 5.º

Definição e competências

1 — A Entidade de Certificação Electrónica do Estado, enquanto entidade certificadora raiz do Estado, é o serviço certificador de topo da cadeia de certificação do SCEE que executa as políticas de certificados e directrizes aprovadas pelo Conselho Gestor do SCEE.

2 — Compete à Entidade de Certificação Electrónica do Estado admitir a integração das entidades certificadoras que obedeçam aos requisitos estabelecidos no presente decreto-lei, bem como prestar os serviços de certificação às entidades certificadoras, no nível hierárquico imediatamente inferior ao seu na cadeia de certificação, em conformidade com as normas aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados digitais qualificados.

3 — Para os efeitos previstos no número anterior, compete à Entidade de Certificação Electrónica do Estado obter o certificado de credenciação referido no n.º 2 do artigo 8.º

4 — A Entidade de Certificação Electrónica do Estado disponibiliza exclusivamente os seguintes serviços de certificação digital:

a) Processo de registo das entidades certificadoras;
b) Geração de certificados, incluindo certificados qualificados, e gestão do seu ciclo de vida;
c) Disseminação dos certificados, das políticas e das práticas de certificação;
d) Gestão de revogações de certificados;
e) Disponibilização do estado e da situação das revogações referidas na alínea anterior.

5 — Compete, ainda, à Entidade de Certificação Electrónica do Estado:

a) Garantir o cumprimento e a implementação enquanto entidade certificadora de todas as regras e todos os procedimentos estabelecidos no documento de políticas de certificação e na declaração de práticas de certificação do SCEE;
b) Implementar as políticas e práticas do Conselho Gestor do SCEE;

c) Gerir toda a infra-estrutura e os recursos que compõem e garantem o funcionamento da entidade certificadora raiz do Estado, nomeadamente o pessoal, os equipamentos e as instalações;
d) Gerir todas as actividades relacionadas com a gestão do ciclo de vida dos certificados por si emitidos para as entidades certificadoras de nível imediatamente inferior ao seu;
e) Garantir que o acesso às suas instalações principal e alternativa é efectuado apenas por pessoal devidamente autorizado e credenciado;
f) Gerir o recrutamento de pessoal tecnicamente habilitado para a realização das tarefas de gestão e operação da entidade certificadora raiz do Estado;
g) Comunicar imediatamente qualquer incidente, nomeadamente anomalias ou falhas de segurança, ao Conselho Gestor do SCEE.

6 — A Entidade de Certificação Electrónica do Estado emite exclusivamente certificados para as entidades certificadoras do Estado subordinadas, não podendo emitir certificados destinados ao público.

Artigo 6.º

Direcção e pessoal

1 — A Entidade de Certificação Electrónica do Estado é dirigida, por inerência, pelo director do Centro de Gestão da Rede Informática do Governo (CEGER).

2 — Desempenham funções na Entidade de Certificação Electrónica do Estado, sem prejuízo do exercício de funções no lugar de origem, os técnicos do CEGER com as seguintes categorias:

a) Um consultor de sistemas, incumbido da articulação entre a Entidade de Certificação Electrónica do Estado e o Conselho Gestor do SCEE e entre aquela e as entidades certificadoras do Estado;
b) Um administrador de sistemas, autorizado a instalar, configurar e manter o sistema, tendo acesso controlado a configurações relacionadas com a segurança;
c) Um operador de sistemas, responsável por operar diariamente os sistemas, autorizado a realizar cópias de segurança e reposição de informação;
d) Um administrador de segurança, responsável pela gestão e implementação das regras e práticas de segurança;
e) Um administrador de registo, responsável pela aprovação da emissão, pela suspensão e pela revogação de certificados;
f) Um auditor de sistemas, autorizado a monitorizar os arquivos de actividade dos sistemas.

3 — Nos termos da legislação em vigor, as funções de administrador de sistemas, de administrador de segurança e de auditor de sistemas devem ser desempenhadas por pessoas diferentes.

4 — Para os efeitos do disposto no n.º 2, o quadro de pessoal do CEGER pode ser alterado por portaria conjunta dos membros do Governo responsáveis pelas áreas das finanças e da Administração Pública e pelo CEGER.

CAPÍTULO IV

Entidades certificadoras do Estado

Artigo 7.º

Requisitos

1 — São entidades certificadoras do Estado as entidades públicas que exerçam funções de entidade certificadora nos termos do disposto no Decreto-Lei n.º 290-D/99, de 2 de Agosto, na redacção introduzida pelo Decreto-Lei n.º 62/2003, de 3 de Abril, e pelo presente decreto-lei e respectiva regulamentação, e que:

a) Estejam admitidas como entidades certificadoras, nos termos do n.º 2 do artigo 5.º;
b) Actuem em conformidade com as declarações de práticas de certificação e com a política de certificação e práticas aprovadas pelo Conselho Gestor do SCEE.

2 — Para os efeitos da aplicação do regime previsto do número anterior, consideram-se abrangidas quaisquer entidades que, independentemente da sua natureza, prestem funções de certificação para a realização de fins próprios da Administração Pública.

3 — Só podem prestar serviços de certificação electrónica, no âmbito do SCEE, as entidades reconhecidas como entidades certificadoras, nos termos dos números anteriores.

4 — As entidades certificadoras não podem emitir certificados de nível diverso do imediatamente subsequente ao seu, excepto nos casos de acordos de certificação lateral ou cruzada promovidos e aprovados pelo Conselho Gestor do SCEE.

5 — Os serviços de registo podem ser atribuídos a entidades, individuais ou colectivas, designadas como entidades de registo, nas quais as entidades certificadoras do Estado delegam a prestação de serviços de identificação e registo de utilizadores de certificados, bem como a gestão de pedidos de revogação de certificados, nos termos do disposto no n.º 1 do artigo 4.º do Decreto Regulamentar n.º 25/2004, de 15 de Julho.

CAPÍTULO V

Autoridade credenciadora nacional

Artigo 8.º

Autoridade credenciadora

1 — A autoridade credenciadora competente para a credenciação e a fiscalização das entidades certificadoras compreendidas no SCEE é a Autoridade Nacional de Segurança, nos termos do artigo 3.º do Decreto-Lei n.º 217/97, de 20 de Agosto.

2 — No âmbito da aplicação do artigo 1.º, a Autoridade Nacional de Segurança é competente para emitir o certificado de credenciação das entidades certifica-

doras e exercer as competências de credenciação previstas no Decreto-Lei n.º 290-D/99, de 2 de Agosto, alterado pelo Decreto-Lei n.º 62/2003, de 3 de Abril, e na redacção introduzida pelo presente decreto-lei.

3 — A Autoridade Nacional de Segurança é assistida, no exercício das suas competências, pelo conselho técnico de credenciação.

Artigo 9.º

Conselho técnico de credenciação

1 — O conselho técnico de credenciação é um órgão consultivo da autoridade credenciadora, competindo-lhe pronunciar-se sobre todas as questões que a autoridade credenciadora lhe submeta.

2 — O conselho técnico de credenciação pode, ainda, por sua iniciativa, emitir pareceres ou recomendações à autoridade credenciadora.

Artigo 10.º

Composição

O conselho técnico de credenciação é composto:

a) Pela Autoridade Nacional de Segurança, que preside;
b) Por duas personalidades designadas pelo Primeiro-Ministro;
c) Por uma personalidade designada pelo Ministro da Administração Interna;
d) Por uma personalidade designada pelo Ministro da Justiça;
e) Por uma personalidade designada pelo Ministro da Ciência, Tecnologia e Ensino Superior;
f) Por um representante do ICP — ANACOM.

Artigo 11.º

Reuniões

O conselho técnico de credenciação reúne ordinariamente de seis em seis meses e extraordinariamente por iniciativa do seu presidente.

Artigo 12.º

Apoio logístico

O Gabinete Nacional de Segurança assegura o apoio logístico e administrativo ao conselho técnico de credenciação, suportando também os encargos inerentes ao seu funcionamento.

Artigo 13.º

Colaboração com outras entidades

A autoridade credenciadora pode, no exercício das competências que lhe estão cometidas pelo presente decreto-lei, solicitar a outras entidades públicas ou privadas toda a colaboração que julgar necessária.

CAPÍTULO VI

Disposições finais e transitórias

Artigo 14.º

Instalação e equipamento da Entidade de Certificação Electrónica do Estado

Para além do previsto no presente decreto-lei, os demais aspectos regulamentares relacionados com a instalação e o equipamento da Entidade de Certificação Electrónica do Estado são regulados por despacho do membro do Governo responsável pelo CEGER.

Artigo 15.º

Disposição transitória

No ano de 2006, a Secretaria-Geral da Presidência do Conselho de Ministros transfere para o Gabinete Nacional de Segurança os montantes necessários para o cumprimento do disposto no artigo 12.º do presente decreto-lei.

Artigo 16.º

Alteração ao Decreto-Lei n.º 290-D/99, de 2 de Agosto

O artigo 9.º do Decreto-Lei n.º 290-D/99, com a redacção que lhe foi dada pelo Decreto-Lei n.º 62/2003, de 3 de Abril, passa a ter a seguinte redacção:

«Artigo 9.º

[...]

1 — .....

2 — Sem prejuízo do disposto no número anterior, as entidades certificadoras que emitam certificados qualificados devem proceder ao seu registo junto da autoridade credenciadora, nos termos a fixar por portaria do membro do Governo responsável pela autoridade credenciadora.

3 — A credenciação e o registo estão sujeitos ao pagamento de taxas em função dos custos associados às tarefas administrativas, técnicas, operacionais e de fiscalização correspondentes, nos termos a fixar por despacho conjunto do membro do Governo responsável pela autoridade credenciadora e do Ministro das Finanças, que constituem receita da autoridade credenciadora.»

Artigo 17.º

Aditamento ao Decreto-Lei n.º 290-D/99, de 2 de Agosto

É aditado ao Decreto-Lei n.º 290-D/99, com a redacção que lhe foi dada pelo Decreto-Lei n.º 62/2003, de 3 de Abril, o artigo 40.º-A, com a seguinte redacção:

«Artigo 40.º-A

Credenciação de entidades certificadoras públicas

1 — As disposições constantes dos capítulos III e IV só são aplicáveis à actividade das entidades certificadoras públicas na estrita medida da sua adequação à natureza e às atribuições de tais entidades.

2 — Compete à autoridade credenciadora estabelecer os critérios de adequação da aplicação do disposto no número anterior, para efeitos da emissão de certificados de credenciação a entidades certificadoras públicas a quem tal atribuição esteja legalmente cometida.

3 — Os certificados de credenciação podem ser emitidos, a título provisório, por períodos anuais renováveis até um máximo de três anos, sempre que a autoridade credenciadora considere necessário determinar procedimentos de melhor cumprimento dos requisitos técnicos aplicáveis.»

Artigo 18.º

Norma revogatória

São revogados:

a) O Decreto-Lei n.º 234/2000, de 25 de Setembro;
b) A alínea *i*) do artigo 18.º do Decreto-Lei n.º 146/2000, de 18 de Julho;
c) A alínea *j*) do artigo 5.º do Decreto-Lei n.º 103/2001, de 29 de Março.

Visto e aprovado em Conselho de Ministros de 4 de Maio de 2006. — *José Sócrates Carvalho Pinto de Sousa — António Luís Santos Costa — Fernando Teixeira dos Santos — Manuel Pedro Cunha da Silva Pereira — Alberto Bernardes Costa — Mário Lino Soares Correia — José Mariano Rebelo Pires Gago.*

Promulgado em 8 de Junho de 2006.

Publique-se.

O Presidente da República, ANÍBAL CAVACO SILVA.

Referendado em 12 de Junho de 2006.

O Primeiro-Ministro, *José Sócrates Carvalho Pinto de Sousa.*

Decreto-Lei n.º 116-B/2006

de 16 de Junho

O Centro de Gestão da Rede Informática do Governo (CEGER) foi criado em 1989 pelo Decreto-Lei n.º 429/89, de 15 de Dezembro, tendo, posteriormente, sido objecto de uma alteração do seu enquadramento jurídico através do Decreto-Lei n.º 184/98, de 6 de Julho.

Esta reestruturação visou conferir ao CEGER uma maior amplitude de actuação, que abrange, actualmente, não só a gestão da rede informática do Governo, mas também a gestão das tecnologias de informação e de comunicações de todos os gabinetes governamentais.

Pretende-se, agora, que o CEGER desempenhe ainda as funções de entidade certificadora do Governo, no âmbito do Sistema de Certificação Electrónica do Estado — Infra-Estrutura de Chaves Públicas, criado pelo Decreto-Lei n.º 116-A/2006, de 16 de Junho.

Torna-se, por isso, indispensável adaptar a Lei Orgânica do CEGER, designadamente para especificar as novas atribuições da segurança electrónica do Estado emergentes da evolução tecnológica da Internet e dos projectos e serviços em implementação no domínio do governo electrónico *(e-government)*.

Aproveita-se, ainda, para eliminar os artigos 9.º e 16.º, declarados inconstitucionais com força obrigatória geral pelo Tribunal Constitucional, através do Acórdão n.º 208/2002, de 21 de Maio, publicado no *Diário da República,* 1.ª série-A, de 8 de Julho de 2002.

Assim:

Nos termos da alínea *a*) do n.º 1 do artigo 198.º da Constituição, o Governo decreta o seguinte:

Artigo 1.º

Alteração ao Decreto-Lei n.º 184/98, de 6 de Julho

Os artigos 1.º, 2.º, 3.º e 7.º do Decreto-Lei n.º 184/98, de 6 de Julho, passam a ter a seguinte redacção:

«Artigo 1.º

[...]

1 — .....

2 — O CEGER exerce ainda as funções de entidade certificadora, no âmbito do Sistema de Certificação Electrónica do Estado — Infra-Estrutura de Chaves Públicas (SCEE).

3 — O CEGER, enquanto entidade certificadora no âmbito do procedimento legislativo, exerce tais funções com autonomia em relação a todas as demais atribuições, nos termos do n.º 2 do artigo seguinte.

4 — *(Anterior n.º 2.)*

Artigo 2.º

[...]

1 — São atribuições do CEGER:

a) Prestar apoio de consultoria aos membros do Governo e seus gabinetes, bem como a outros organismos, em matérias de tecnologias de informação, de comunicações, de sistemas de informação e de segurança electrónica;
b) Actuar como entidade certificadora do Governo, no âmbito do SCEE;
c) Actuar como entidade certificadora de outros serviços, organismos e entidades públicas, nos casos em que essas funções lhe sejam especialmente cometidas por lei ou convenção;
d) Assegurar as demais funções que lhe sejam cometidas no âmbito do SCEE;
e) *[Anterior alínea b).]*
f) *[Anterior alínea c).]*
g) *[Anterior alínea d).]*
h) Assegurar a concepção, desenvolvimento, implantação e exploração de sistemas de informação de utilização comum para os gabinetes dos membros do Governo, nomeadamente novos serviços adaptados ao governo electrónico *(e-government)* e Internet e sistemas avançados de apoio à decisão do Governo;
i) *[Anterior alínea f).]*
j) Coordenar o apoio aos utilizadores, incluindo às entidades e serviços integrados na Presidência do Conselho de Ministros, e gerir o parque de equipamentos e *software* sob a sua responsabilidade;
l) Assegurar serviços de gestão e de apoio técnico orientados para a utilização de redes globais externas, nomeadamente das infra-estruturas electrónicas comuns ao Governo e a serviços e organismos públicos, decorrentes da evolução tecnológica da Internet;
m) Assegurar serviços de certificação temporal que permitam a validação cronológica de transacções e documentos electrónicos;
n) *[Anterior alínea i).]*
o) *[Anterior alínea j).]*