



ASSEMBLEIA DA REPÚBLICA

PROJECTO DE LEI N.º 112/IX

ADOPTA MEDIDAS LEGAIS TENDENTES A INSTITUIR E VIABILIZAR O CARTÃO DO CIDADÃO

1 — Através da Resolução n.º 77/2001, de 5 de Julho, o Conselho de Ministros desencadeou o processo de criação de um «cartão do cidadão», capaz de identificar o respectivo titular perante diversos serviços públicos, tirando pleno partido da proliferação das redes electrónicas e das demais inovações tecnológicas próprias da era digital.

Com esta medida de modernização e racionalização permitir-se-á mais eficácia da Administração, menos incómodos para os cidadãos e uma notável simplificação de procedimentos. Desde logo, o Estado poderá poupar milhões de contos eliminando a actual multiplicidade de formas de produção e emissão de cartões de serviços públicos tão importantes, como os de identificação civil, fiscal, segurança social e eleitoral.

Face a estudos preliminares elaborados pelo Ministério da Justiça e a debates realizados em reunião de Secretários de Estado, foi entendido que, em vez de uma mera versão revista do tradicional bilhete de identidade, com funções limitadas e da responsabilidade de um só departamento ministerial, Portugal deveria passar a dispor, a partir de Janeiro de 2003, de um novo tipo de cartão multiusos, susceptível de funcionar, por um lado, como chave de acesso a informação arquivada nas bases de dados públicas responsáveis pela identificação civil, eleitoral, fiscal e de segurança social



ASSEMBLEIA DA REPÚBLICA

e, por outro, como um meio de acesso a serviços electrónicos oferecidos aos titulares.

Filiada em preocupações de simplificação, desburocratização e inovação, a iniciativa merece, no quadro político decorrente das eleições de 17 de Março, o mesmo juízo de valor positivo que lhe foi conferido no ciclo anterior.

O projecto insere-se plenamente na linha de reflexão europeia impulsionada pelo Conselho da Feira (Junho de 2000) sobre o processo de criação de um documento de identificação digital previsto no Plano de Acção eEurope 2002, tendo em vista estimular o uso de serviços electrónicos, públicos e privados, por um cada vez maior número de cidadãos europeus. Sendo natural que todos os estudos produzidos se encontrem em apreciação e releitura por parte dos responsáveis governamentais em funções, reveste-se de grande importância que o processo não perca velocidade e seja mesmo acelerada a criação de condições institucionais e legais para as próximas fases de implementação.

O Parlamento tem, sob esse ponto de vista, um papel central, uma vez que lhe cabe criar a credencial legal que permitirá à Comissão Nacional de Protecção de Dados velar para que o complexo processo de tratamento de dados necessário decorra em condições constitucionalmente adequadas.

O tema foi equacionado pelo grupo de trabalho constituído para recolher a informação relevante e articular os departamentos interessados, sob coordenação do Secretário de Estado dos Assuntos Parlamentares, mas, dada a aproximação do acto eleitoral, foi entendido não produzir articulados.



ASSEMBLEIA DA REPÚBLICA

O caso português é já, todavia, correntemente mencionado internacionalmente como uma expressão da tendência emergente de emissão de «e-cards», ao lado de países como a Finlândia, Áustria, Bélgica, Irlanda, Itália, Holanda, Espanha e Suécia

(www.sahkoinenhenkilokortti.fi/download/scc/haikko/van_Arkel.ppt#1)

2 — O presente projecto de lei acolhe as conclusões do estudo de viabilidade realizado por peritos da Universidade do Minho, sob a coordenação do Prof. Doutor José Manuel E. Valença, com mediação da Agência para a Inovação, através do qual foi possível:

— Densificar os parâmetros relevantes para a definição conceptual do cartão;

— Preparar uma descrição pormenorizada das especificidades físicas, logísticas e electrónicas do projecto;

— Estudar os procedimentos a adoptar para recolha da informação necessária para preencher os campos a incluir no cartão;

— Inventariar as dificuldades organizativas decorrentes de rotinas e regras vigentes em cada um dos sistemas de identificação actualmente não articulados;

— Considerar as questões legais a dirimir para dar cumprimento às normas constitucionais atinentes à protecção da privacidade e à segurança dos dados pessoais;

— Propor um processo de emissão, definindo as implicações de uma eventual opção de centralização da produção;

— Definir a estrutura e procedimentos de certificação digital;



ASSEMBLEIA DA REPÚBLICA

— Avaliar os custos da instituição dos novos sistemas, ponderando as poupanças geradas e as despesas a realizar nas diversas fases do projecto;

— Preconizar formas de articulação do projecto do «cartão do cidadão» com a dinâmica de reforma da Administração Pública, por forma a multiplicar aplicações e serviços electrónicos capazes de tirar partido da nova «chave de acesso» a atribuir aos cidadãos.

3 — O modelo desenhado afigura-se recomendável e digno de consagração sob forma de lei, sem vazar para o articulado toda a malha de especificações técnicas e deixando ao Governo todo o espaço necessário para levar a cabo a difícil tarefa de organizar no plano regulamentar e administrativo o processo de transição que conduza às primeiras emissões.

São assumidos como bons os seguintes pressupostos orientadores:

a) Em matéria de cartão do cidadão, Portugal deve adoptar uma solução *light*, similar à que está a ser implementada pela Finlândia. O cartão deve ter um *chip* totalmente desprovido de informação de conteúdo, dotado somente dos mecanismos necessários para garantir a identificação *on-line* de forma segura. Podendo funcionar como BI presencial, facilmente legível a olho nu, o cartão terá, pelas suas características digitais, melhores defesas contra a falsificação. Pode constituir ainda um meio de identificação digital *on-line* com o Estado e os diferentes serviços da Administração.

Esta solução:



ASSEMBLEIA DA REPÚBLICA

— Aumenta a segurança para o cidadão, inviabilizando acessos ilegítimos a dados pessoais;

— É a mais adequada em plena era da Internet, em que os conteúdos já estão ou deverão estar a breve trecho acessíveis na rede, não sendo necessário serem transportados dentro do cartão;

— É, por isso, também a solução mais económica dado que os *chips* necessários têm custo mais baixo do que no caso de serem dotados de elevada capacidade de memória para transportarem conteúdos dos diversos serviços da Administração;

— É a mais flexível em dois sentidos: nos *timings* de implementação dos serviços a que dá acesso (estes serão acessíveis à medida em que estiverem disponíveis, permitindo ainda a adesão progressiva de novos departamentos da Administração, sem que tal implique a substituição do cartão); na susceptibilidade de ajustamentos (sendo a opção mais barata, criará menos entraves à substituição no futuro por novas versões mais avançadas, que entretanto se revelem viáveis);

b) A emissão de um BI electrónico deve possibilitar a identificação *online* não só nas relações com a Administração Pública mas eventualmente com entidades privadas que o desejem.

A disponibilidade das chaves públicas possibilitará aos diversos serviços públicos e privados que o pretendam o acesso às informações e serviços disponibilizados, na Net, de forma mais segura, substituindo a identificação por sistema *login e password*;

c) Na identificação *off-line*, o BI deverá ter na parte de trás do cartão apostos os números específicos dos diferentes serviços para que os utentes



ASSEMBLEIA DA REPÚBLICA

não tenham de transportar consigo todos os cartões sectoriais com, os respectivos números, ou não tenham que os conhecer de cor.

Na identificação presencial com os serviços a identificação *on-line* poderá ser também utilizada, na medida em que os serviços estejam equipados com leitores de cartão com *smart-card*, que são facilmente generalizáveis pelo seu baixo preço;

d) Como a utilização do BI electrónico como cartão do cidadão, na sua relação com os diferentes serviços da Administração, dependerá do grau de informatização dos serviços e sua disponibilização na Net, o grau de utilidade para os cidadãos da disponibilidade do BI electrónico dependerá, em última análise, do ritmo a que estes serviços estejam disponíveis na Net, o que salienta a importância de definir estratégias de produção de aplicações que tirem partido da existência do novo tipo de chave de acesso;

e) A introdução do BI electrónico terá um grande impacto na melhoria das relações dos cidadãos com o Estado. A disponibilidade do cartão possibilitará um instrumento importante na identificação das relações *on-line* entre serviços públicos, passo importante para a implementação do princípio do «guichet único», podendo acabar-se com as certidões emitidas pela Administração para utilização por outros serviços públicos;

f) A criação do cartão do cidadão também poderá ser uma oportunidade para estimular o desenvolvimento de sectores tecnologicamente avançados, quer dos sistemas necessários ao seu



ASSEMBLEIA DA REPÚBLICA

lançamento e funcionamento quer no desenvolvimento das inúmeras aplicações em *software* a que abre caminho;

g) O projecto implica a existência de autoridades de identificação, certificação e emissão, garantes da legalidade do processo implementação do cartão;

h) Para o sucesso do cartão do cidadão é indispensável realizar uma fase piloto, com grupos de utilizadores, recomendando-se que sejam incluídos destacadamente os cidadãos funcionários públicos. Outros grupos piloto deverão ser definidos, por exemplo de natureza geográfica, para avançar com pilotos de utilização específicos, como, por exemplo, a realização de eleições por voto electrónico em algumas áreas de voto, ou experiências de Administração Pública *on-line* em regiões do interior, ou ainda com grupos de emigrantes.

Nestes termos, os Deputados abaixo assinados apresentam o seguinte projecto de lei:

Artigo 1.º

(Objecto)

A presente lei estabelece o enquadramento geral do processo de emissão e generalização do uso de um cartão do cidadão na República portuguesa.

Artigo 2.º

(Cartão do cidadão)



ASSEMBLEIA DA REPÚBLICA

1 — As entidades da Administração Pública responsáveis pela recolha, tratamento e conservação dos dados pessoais individualizadores de cada cidadão com o fim de estabelecer a sua identidade civil, fiscal e eleitoral, bem como perante o Serviço Nacional de Saúde e a segurança social, estabelecerão programas de acção tendentes à emissão a partir de Janeiro de 2003 de um cartão do cidadão, generalizando progressivamente o seu uso.

2 — O elenco das entidades participantes no projecto é gradualmente ampliado pelo Governo, por forma a gerar crescentes economias de custos, eliminar duplicações, racionalizar a organização da Administração Pública e impulsionar processos de relacionamento electrónico entre os cidadãos e as instituições públicas e privadas próprios da sociedade de informação.

3 — A selecção dos serviços e respectiva reorganização tem em conta as directrizes e recomendações constantes do Anexo 1.

Artigo 3.º

(Definição)

1 — O cartão do cidadão constitui um documento autêntico de identificação múltipla, que permite ao titular provar a sua identidade perante terceiros e autenticar documentos electrónicos.

2 — O cartão do cidadão contém a foto da pessoa sua titular e tem impressos, de forma bem legível, elementos de identificação perante os diferentes serviços sectoriais a que faculta acesso.



ASSEMBLEIA DA REPÚBLICA

3 — O cartão do cidadão funciona como certificado electrónico de cidadania, facultando mecanismos seguros que perante serviços informatizados fazem prova da sua qualidade de titular de direitos.

4 — Os procedimentos tendentes à emissão do cartão do cidadão assentam cooperação interdepartamental, sem concentração ou centralização orgânica dos sistemas informáticos das entidades participantes no projecto.

Artigo 4.º

(Princípios aplicáveis)

A identificação assegurada pelo cartão do cidadão observa o princípio da legalidade e, bem assim, os princípios da autenticidade, veracidade, univocidade e segurança dos dados pessoais em causa.

Artigo 5.º

(Regras para elaboração)

A elaboração do cartão do cidadão obedece aos seguintes princípios e regras essenciais:

a) O uso de técnicas criptográficas de chave pública para identificação do titular do cartão e autenticação dos seus documentos electrónicos;



ASSEMBLEIA DA REPÚBLICA

b) A inserção do mínimo de conteúdo informativo no cartão, circunscrito ao estritamente indispensável ao uso das apropriadas técnicas criptográficas;

c) Independência em relação às aplicações clientes, que correrão nos sistemas informáticos das entidades da Administração Pública que sejam parceiras do projecto;

d) A salvaguarda de que os registos específicos de cada base de dados serão inacessíveis a terceiros não autorizados;

e) A defesa dos direitos de acesso a informação pessoal constante nas diversas bases de dados;

f) O sistema de produção e os procedimentos de carregamento e gestão devem assentar em *standards* protocolos e programas abertos e de uso comum;

g) O projecto assegurará compatibilidade adequada com as recomendações das iniciativas comunitárias neste domínio, designadamente a *Smart Card Charter* e o projecto *Public Identity*.

Artigo 6.º

(Limitação do conteúdo informativo)

1 — Em obediência ao princípio da limitação do conteúdo informático aos itens de informação indispensáveis à concretização dos seus objectivos, o cartão do cidadão contém apenas:



ASSEMBLEIA DA REPÚBLICA

- a) Um *token* criptográfico, formado por um certificado de chave pública e a respectiva chave privada cifrada, titulado pelo titular do cartão, destinado aos protocolos de identificação e acordo de chaves;
- b) Um segundo *token* criptográfico, idêntico ao primeiro e com o mesmo titular, mas destinado à autenticação de documentos via assinaturas digitais;
- c) Um certificado de chave pública titulado pela autoridade de certificação que emitiu os dois certificados anteriores.

2 — O conteúdo do cartão e o processo da sua emissão são progressivamente adaptados por forma a acolher as directrizes e recomendações relativas à identificação electrónica de âmbito europeu e as conclusões dos estudos sobre a simplificação administrativa dos sistemas de identificação nacionais.

Artigo 7.º

(Determinação da identidade)

A determinação da identidade dos cidadãos obedece às seguintes regras:

- a) A identidade do titular de qualquer certificado é determinada, no próprio documento, por uma denominação inconfundível (*distinguished name, DN*), representação unívoca não invertível de atributos naturais decorrentes de informação pública não volátil, associada ao cidadão pelo



ASSEMBLEIA DA REPÚBLICA

nascimento, e que o possa identificar, como seja o nome original, a data e local de nascimento e a paternidade;

b) Os atributos naturais não são recuperáveis a partir do conhecimento da denominação inconfundível;

c) Cada sistema de informação que interage com o cartão do cidadão deve definir um registo do certificados que aceita, genericamente designado por «depósito de chaves públicas» onde define quais os recursos e funcionalidades que estão associados ao titular de cada um dos certificados;

d) Os depósitos de chaves públicas constituem bases de dados pessoais, para os efeitos da Lei n.º 67/98, de 26 de Outubro;

e) Cada sistema tem um mecanismo próprio para referenciar os seus utilizadores, designadamente o seu próprio código identificador e os seus próprios atributos, tornando desnecessária qualquer forma universal de referenciar electronicamente o cidadão;

f) O protocolo de identificação fornece ao agente identificador o certificado do titular do cartão em termos tais que esse agente, através do seu depósito de chaves públicas, saiba como referenciar internamente esse utilizador e quais os recursos a que ele pode aceder e de que forma o pode fazer.

Artigo 8.º

(Garantia da protecção de dados)



ASSEMBLEIA DA REPÚBLICA

1 — Os procedimentos a adoptar para a elaboração do cartão do cidadão asseguram a completa protecção nos dados pessoais incluídos em cada um dos sistemas e não devem permitir qualquer cruzamento de dados.

2 — São aplicáveis para o efeito as regras técnicas publicadas em anexo (Anexo 2), que, sem prejuízo do disposto no artigo seguinte, vale para todos os efeitos como autorização especial para os tratamentos de dados necessários.

Artigo 9.º

(Comissão Nacional de Protecção de Dados)

A Comissão Nacional de Protecção de Dados acompanha a execução dos procedimentos a adoptar para a elaboração do cartão do cidadão, exercendo as suas competências de fiscalização e emitindo parecer sobre a legislação regulamentar da presente lei.

Artigo 10.º

(Institucionalização de autoridades)

1 — Com vista a assegurar a autenticidade do cartão do cidadão e a força probatória dos actos que lhe estão associados serão adoptadas medidas adequadas com vista à institucionalização de autoridades com três tipos de funções:



ASSEMBLEIA DA REPÚBLICA

a) A garantia de identidade do titular do cartão e o reconhecimento dos seus direitos de cidadania (autoridade de identificação ou autoridade de registo);

b) A geração dos conteúdos criptográficos associados ao titular e a segurança desses conteúdos (autoridade de certificação);

c) A emissão do cartão e as garantias da posse efectiva do cartão pelo seu titular (autoridade de emissão).

2 — São aplicáveis para o efeito as regras técnicas publicadas em anexo à presente lei (Anexo II).

Artigo 11.º

(Experiências-piloto)

Será realizada uma fase piloto com grupos de utilizadores, designadamente com os funcionários públicos, e feitos testes de utilização específicos, nomeadamente a realização de eleições por voto electrónico em algumas áreas de voto, experiências de Administração Pública *on-line* em regiões do interior e novas formas de interacção com os portugueses residentes no estrangeiro.

Artigo 12.º

(Regulamentação)



ASSEMBLEIA DA REPÚBLICA

O Governo aprovará a legislação necessária à regulamentação da presente lei e adoptará as demais providências necessárias à criação atempada do cartão do cidadão.

Palácio de São Bento, 11 de Julho de 2002. Os Deputados do PS:
António Costa — Eduardo Ferro Rodrigues — José Magalhães — Eduardo Cabrita — Guilherme d'Oliveira Martins — Ascenso Simões.

Anexo I

Conceito estratégico para delimitação dos serviços susceptíveis de utilizar o cartão do cidadão

O cartão do cidadão deve ser instituído como parte de um conjunto de iniciativas tendentes a dinamizar o uso das tecnologias da informação para melhorar a interacção do cidadão com a Administração Pública, de acordo com o conceito estratégico seguidamente definido.

1 - Estratégia a adoptar:

O cartão do cidadão deve capitalizar no esforço feito nas restantes iniciativas da Administração Pública; não deve provocar rupturas nos serviços que já estão disponíveis em redes públicas nem um esforço de adaptação que seja incomportável por esses serviços.

Dado que existem custos de adaptação e aprendizagem para o cidadão (que não devem ser ignorados), o cartão do cidadão será realmente adoptado só se o cidadão puder reconhecer vantagens imediatas; exige-se



ASSEMBLEIA DA REPÚBLICA

não só maior comodidade, maior controlo e melhores garantias (reconhecíveis) no acesso a serviços existentes mas, principalmente, novos serviços.

Para encorajar novos serviços (e trazer a iniciativa privada para o projecto) os custos de desenvolvimento têm de ser muito baixos; se assim for, não só as «grandes aplicações» (saúde, fiscalidade, segurança social, etc.) usam o cartão do cidadão mas também as «pequenas aplicações» (com pequenas funcionalidades e interessando, eventualmente, a comunidades restritas) podem ser atraídas, em número significativo, para o projecto.

Uma outra faceta importante é a oportunidade do projecto. Para que o cartão seja aceite não deve existir um intervalo de tempo excessivo entre o seu anúncio e o aparecimento de aplicações que façam uso efectivo das suas funcionalidades. Daí ser essencial que o tempo de desenvolvimento das aplicações seja curto.

Compatibilidade com aplicações de rede existentes aliada a baixos custos de desenvolvimento e oportunidade implicam, necessariamente:

(i) O uso de formatos *standard* para os conteúdos de informação e para os seus contentores; só por si isto é razão suficiente para não se adoptar formatos de dados em cartão ou aplicações de segurança proprietários; os mecanismos de *software* para acesso aos cartões (desde os *drivers* dos leitores até ao acesso a conteúdos pelas aplicações cliente) têm de estar já desenvolvidos e disponíveis.

(ii) A estrutura básica das aplicações cliente tem de ser universal e estar já desenvolvida e disponível; não é possível desenvolver interfaces



ASSEMBLEIA DA REPÚBLICA

específicas para as aplicações cliente; é essencial usar-se ferramentas *standard* de interação: *browsers*, correio electrónico, etc.

(iii) As aplicações de servidor têm de ser «intocáveis»; os mecanismos de reconhecimento da identificação e de reconhecimento da autenticação têm de ser externos à aplicação servidor; as aplicações que garantem a segurança desses actos têm de ser *standard* e já desenvolvidas.

A integração do cartão do cidadão num serviço deve, tanto quanto seja possível, resumir-se a um esforço de configuração de ferramentas existentes, reduzindo o esforço de codificação ao mínimo.

2 - Integração nas aplicações cliente:

Dado que o cartão do cidadão assenta em soluções PKI padrão, as aplicações cliente podem resumir-se a *browsers* (ou, eventualmente, clientes de correio electrónico) configurados para o protocolo de transporte https e suportando as funcionalidades do protocolo SSL.

Os cartões devem usar o perfil *electronic identification profile* do PICCS#15. Este perfil é suportado pelas aplicações cliente atrás referidas desde que seja instalado o *driver* apropriado para o leitor de cartões usados. Estes *drivers* devem estar publicamente acessíveis.

3 - Registo de certificados:

O acto essencial para que um cidadão, titular de um cartão com certificados, seja reconhecido por um sistema de informação é o seu registo junto a esses sistemas.



ASSEMBLEIA DA REPÚBLICA

O objectivo do registo é a definição de uma correspondência entre a informação pública que o identifica (os seus certificados de chave pública) e a identificação como utilizador do sistema.

Cada sistema de informação pode usar formas diversas de identificar um seu utilizador; pode usar identificadores (número do contribuinte, número de bilhete de identidade, número de sócio de um clube desportivo, etc) ou usar um conjunto de atributos que sejam relevantes ao sistema. O sistema de informação pode também definir autorizações distintas (associações entre recursos e acções possíveis sobre esses recursos) consoante o utilizador e o certificado que o identifica.

O resultado do registo é a construção de uma «tabela» que associa certificados a identificadores (ou algo equivalente) e a autorizações. Esta tabela é genericamente designada por depósito de chaves (públicas) ou *key store*.

Dado que o processo de registo é um processo de reconhecimento de identidade próprio de cada sistema de informação, a forma como é efectuado vai depender do serviço e do grau de autoridade que reconhece ao cartão do cidadão. Algumas possibilidades:

(i) Para os serviços nucleares (justiça, saúde, finanças e segurança social) o registo pode ser feito automaticamente logo na emissão do cartão do cidadão. Para aqueles serviços que contribuíram com um identificador id para o passo 2, a autoridade de identidade pode usar esse identificador para proceder, em nome do cidadão, ao seu registo no serviço.



ASSEMBLEIA DA REPÚBLICA

(ii) Para serviços que já tenham um processo de identificação de rede (usando outros certificados ou sistemas *login-password*) onde o utilizador esteja reconhecido, pode-se fazer o registo *on-line* através de uma identificação com o sistema instalado e solicitando ao utilizador que forneça os seus novos certificados.

(iii) Para sistemas que ponham grande ênfase na identificação dos seus utilizadores, o registo pode ter de ser feito presencialmente. Isto significa que o cidadão tem de se apresentar com o cartão nesse serviço e fornecer-lhe evidência de que é realmente o titular do cartão.

iv) Para sistemas onde a autenticidade de identidade não seja uma questão crítica, o registo pode ser feito *on-line* fornecendo-se os certificados e, eventualmente, dados «identificadores» complementares.

É importante assegurar que a identificação e o registo apenas forneçam certificados (que são informação pública) ao sistema de informação; toda a informação associada a um utilizador deve ser interna ao sistema que define os atributos necessários e a forma como recolhe essa informação. Deste modo, a privacidade do utilizador (e a protecção dos seus dados pessoais) é uma questão interna a cada sistema e o acto de registo não introduz qualquer capacidade de violação desse direito.

4 - Integração nos serviços:

Um sistema de informação típico é constituído por várias aplicações que interagem com uma base de dados comum. Tem utilizadores individualizados através de um ou mais identificadores e tem um



ASSEMBLEIA DA REPÚBLICA

mecanismo de autorizações através do qual pode controlar que utilizadores acedem a que recursos e em que condições.

À IN/CASA DA MOEDA

(A figura segue apenas em suporte de papel)

Figura 4.1 - Integração de segurança e o CCC em aplicações de rede.

Num tal sistema a integração do cartão do cidadão, e genericamente dos mecanismos de segurança PKI, está representado na figura supra. Essencialmente, é necessário:

— Instalar um servidor de rede com capacidade de responder a pedidos https e configurá-lo para poder identificar certificados emitidos pela autoridade de certificação do cartão do cidadão;

— Criar e manter uma *key store* - este é o objectivo dos procedimentos de registo de certificados descritos anteriormente. A *key store* estabelece uma correspondência entre certificados reconhecidos, utilizadores do sistema e suas autorizações.

Anexo II

Conceito estratégico dos procedimentos para identificação, certificação e emissão do cartão do cidadão



ASSEMBLEIA DA REPÚBLICA

1 — Para efeitos do cumprimento das normas relativas à protecção de dados pessoais, nomeadamente no que diz respeito às garantias quanto ao cruzamento de dados informáticos, deve estabelecer-se uma distinção quanto ao tipo de acesso à representação informática nos vários itens de informação manuseados no cartão do cidadão.

Assim, deve considerar-se informação pública os certificados e os atributos naturais; será considerada informação confidencial os diversos identificadores (incluindo o do BI), a informação especificado BI e a informação de gestão.

No ciclo primordial de identificação-certificação-emissão do cartão do cidadão, o funcionamento global das várias autoridades e a sua interacção com o cidadão e com os serviços da administração pública obedece aos procedimentos representados na figura seguinte:

À IN/CASA DA MOEDA

(A figura segue apenas em suporte de papel)

O passo 2 é, conceptualmente, o procedimento essencial em todo este mecanismo; é neste passo que existe um efectivo reconhecimento da identidade do cidadão e os passos seguintes apenas constróem os mecanismos tecnológicos que garantem esse reconhecimento. Como acto essencialmente jurídico, mesmo recorrendo à tecnologia, o passo 2 não é automatizável.



ASSEMBLEIA DA REPÚBLICA

No entanto, os passos seguintes são, em grande medida, automatizáveis:

— A construção de certificados pela autoridade de certificação é feita num mecanismo completamente fechado e que pode ser certificado quando à segurança física, segurança informática e protecção de dados pessoais;

— A mesma estratégia de fecho+certificação pode ser usado pela autoridade de emissão; eventualmente a única tarefa que pode sair desse automatismo é a personalização dos cartões;

— A actividade final da autoridade de identificação (registo dos certificados nos serviços e nas suas próprias bases de dados) é também automatizável.

2 — Para além do procedimento inicial de identificação-certificação-emissão do cartão do cidadão são necessários outros procedimentos que garantam o seu regular uso pelos cidadãos e pelos serviços e encorajem a sua integração na sociedade da informação, nomeadamente as autoridades de emissão e certificação têm um papel essencial na gestão e manutenção do cartão do cidadão.

A autoridade de emissão deve gerir:

(i) Os centros de distribuição de certificados e os respectivos procedimentos;

(ii) Os mecanismos que permitam ao cidadão renunciar a posse do cartão (em casos de furto, transvio, etc.) ou actualizar a sua posse após terminar seu prazo de validade;



ASSEMBLEIA DA REPÚBLICA

(iii) Os *help desks* e os mecanismos de suporte técnico aos cidadãos (fornecendo, por exemplo, versões actualizadas de software *cliente*).

A autoridade de certificação deve:

(i) Suportar tecnicamente a AE nos seus procedimentos de revogação de certificados;

(ii) Gerir os mecanismos que permitem às aplicações, que aceitam os cartões, verificar a sua validade. Aqui se incluem a gestão de CRL (*certificate revocation lists*) ou a de outros protocolos de rede com funções análogas, como, por exemplo, o OCSP (*on-line certificate status protocol*);

(iii) Suportar os serviços e eventuais administradores de sistemas de informação fornecendo-lhes informação técnica e *software*" que permita o desenvolvimento de novas aplicações do cartão do cidadão.