

Cartão Único do Cidadão

“O governo propõe-se criar um cartão único do cidadão para eliminar a burocracia e os actos inúteis, numa estratégia para a justiça, que passa também por um descongestionamento processual e uma melhoria da resposta judicial”.

Prevê-se que este documento, futuramente, reunirá informações de identificação civil, fiscal, de saúde e de eleitor, substituindo assim o Bilhete de Identidade convencional.

O B.I. em papel é a modalidade mais antiga de identificação e estabelece a relação entre dados biométricos (fotografia, local e data de nascimento,...) e institucionais (nome, número do B.I.,...). Este documento consiste numa identificação por atributos que determina a personalidade jurídica de uma pessoa. Assume a forma de um registo institucional e autenticado desses mesmos atributos num único cartão, numa base de dados, etc.

Consiste ainda na capacidade do identificador poder comparar o registo com atributos reais do identificado.

Portanto, existem dois agentes: um identificador e um agente amigo, que associa um atributo que determine a personalidade, por exemplo o número do B.I., com o atributo medido pelo agente identificador, exemplo: impressões digitais, etc.

O agente identificado não entra nesta relação de confiança pois não realiza nenhum acto de vontade.

O B.I. não é mais do que um registo de uma base de dados distribuída que transportamos no bolso, em contraposição a um registo centralizado. O identificado não tem posse sobre a informação, quer esteja no B.I., quer esteja num registo centralizado. O B.I. consiste portanto numa base de dados de bolso, seja um cartão de papel, seja um chip-card.

O problema que subsiste a este B.I. é que não passa de um registo de atributos que torna mais propensa a violação dos direitos do cidadão.

A outra forma de identificação seria a identificação por acto de vontade que tem por objectivo a garantia de direitos do identificado. Aqui, o identificado participa activamente, pelo que tem que ter qualquer forma de identificação exclusiva. A identificação por acto de vontade define-se num sincronismo de ocorrência de dois actos: um primeiro acto que é um segredo (chave privada) e um outro acto (chave pública) num único evento de identificação, assumindo a forma de protocolo login – password.

O identificado envia ao identificador os dois itens de informação: login (elemento de identificação pública – estabelece a nossa identidade perante o fornecedor de serviços/identificador) e password (o segredo, o código de acesso). O identificador recebe-os reconhecendo o acto através de um registo do segredo identificador (informação pública que permite isto). A aceitação da identificação verifica-se, se o que o identificador espera receber for realmente igual ao que recebe.

Este protocolo tem muitos problemas de segurança, pois esta informação viaja pelo canal público, que pode ser visto por agentes

maliciosos que se podem fazer passar pelo identificado, nomeadamente os sniffers.

Mesmo que este problema não exista, o identificador pode ser hostil, podendo assumir a personalidade do identificado.

A única maneira de saber que o identificador não será hostil, seria ter controlo sobre esse identificador, isto, só sendo possível em situações específicas como é o caso do telemóvel, em que se sabe que o teclado é um meio relativamente privado e confidencial. Todavia, nada nos garante que o fabricante do telemóvel não tenha instalado um “cavalo de tróia”.

Em todas as outras circunstâncias, é prudente assumir que um dos problemas mencionados ocorre.

Outra solução passaria pelo recurso à técnica criptográfica: desafio-resposta (que assegura a personalidade). Esta técnica consiste num mecanismo de identificação que pode usar canais abertos. Aqui, toda a informação que viaja de um lado para o outro é pública. O identificado manifesta num primeiro passo do protocolo uma intenção de identificação e o identificador responde com um desafio aleatório. Por sua vez, o identificado emite uma resposta apropriada ao desafio (que engloba o desenvolvimento com uma chave privada) que é confirmada pelo identificador.

Tanto o identificado como o identificador não são agentes naturais, mas programas de computador.

A resposta passaria por pegar nestas duas “falsas” soluções e constituir uma boa solução: identificação por representante ou proxy, e como exemplo a criação do cartão único do cidadão. Este também denominado por cartão comum do cidadão comportará as normas do B.I. Europeu, mas conterà mais informações, nomeadamente de identificação civil do contribuinte, do eleitor e do utente de saúde. Ele contribui deste modo para eliminar a burocracia e simplificar actos administrativos, sendo sinónimo de uma maior facilidade dos cidadãos na sua relação com a administração.

“Não existirá um número de identificação único (proibido pelo artigo 35º. da Constituição da República) nem o cartão conterà qualquer base de dados, pelo que estarão assegurados os Direitos, Liberdades e Garantias.

A ideia básica que preside ao cartão comum do cidadão é que ele aja como representante do identificado, num protocolo de desafio-resposta, e o identificador se apresente como o cartão, através do sistema login-password.

Existe um computador no cartão que serve como representante, e em relação a estes cartões detenho posse. O sistema login-password funciona no protocolo desafio-resposta. A única informação que precisa é a chave privada para identificação e a chave pública do protocolo desafio-resposta. É necessária capacidade computacional para entrar num protocolo destes e as técnicas criptográficas para proteger as duas chaves utilizadas.

Ao contrário do B.I. convencional, o cartão único do cidadão não necessita de nenhuns atributos pessoais, garantindo melhor a protecção dos direitos do cidadão.

Bibliografia:

- Aulas leccionadas pelo professor: José Manuel Valença
- Artigo do Jornal de Notícias, respeitante ao dia 26 de Abril de 2005
- Artigo do Diário de Coimbra, respeitante ao dia 29 de Abril de 2005
- Resolução do Conselho de Ministros, n.º. 77/01 de 05 de Julho

Autoria:

Andreia Sofia de Sousa Fernandes Leite, n.º 34884
Ângela Afonso Santos, n.º 34886
Vera Lúcia Gomes da Silva, n.º 34983