Segurança Informática

José Manuel E. Valença *

30 de Maio de 2005

*Professor Catedrático do Departamento de Informática da Universidade do Minho

Conteúdo

1. Sociedade da Informação.
2. Segurança: o que é?
3. Um pouco de Teoria dos Sistemas.
4. Técnicas de segurança.
   (a) Cifras e Assinaturas Digitais
   (b) Identificação Digital
   (c) Códigos de autenticação e estampilhas temporais
   (d) Certificados de chave pública.
5. Segurança nas aplicações informáticas.
   (a) Documentos & Comunicações
   (b) Identificação & Protecção de Dados Pessoais
   (c) Voto Electrónico
   (d) *Electronic Cash*

Sociedade da Informação

Existe um sistema social que é originário e motivado pelas **Tecnologias da Informação** (TI's) e que, à falta de melhor nome, designamos por **Sociedade da Informação**.

Este curso pretende apresentar o ponto de vista do **agente activo** neste sistema: alguém com capacidade de capaz de influenciar o seu enquadramento nesta realidade (assim como o dos seus concidadãos) quer através de um domínio das tecnologias mas também, e principalmente, dum posicionamento moral sobre o alcance social dessas tecnologias.

Como realidade social a dita "Sociedade de Informação" determina contextos sociais e relações entre contextos a que genericamente chamamos **Sistemas de Informação**.

Quais são os Sistemas de Informação e como eles afectam o nosso quotidiano resulta de uma evolução que, em minha opinião, é essencialmente não-determinista e, por isso, na maior parte dos casos está longe da capacidade determinante de qualquer decisão política.

Penso que a Sociedade da Informação evolui metabólicamente condicionado por vários tipos de **forças** ou **tendências ecológicas**[1] que lhe são específicas e que podem (por simplicidade) ser agrupadas em três dimensões, designadas por **ubiquidade**, **mobilidade** e **hostilidade**, e que veremos em seguida.

[1] *Ecologia* e *Economia* têm raiz comum no vocábulo grego **oîkos** que significa "casa"; têm sufixos diferentes: **logos** (linguagem, discurso) e **nomos** (norma, direcção, ordem); etimologicamente significam, respectivamente, "a linguagem da casa" e "a norma da casa". Faz todo sentido falar de Ecologia da Informação (**infoecologia**) como falar de Economia da Informação (**infoeconomia**); a primeira será o estudo das relações dos agentes humanos ou artificiais entre si e entre o contexto (meio, ambiente, casa) informativo onde residem; a segunda será o estudo dos recursos, e dos fenómenos que geram e consomem tais recursos, necessários à evolução e sobrevivência do contexto informativo.

Ubiquidade

Existe uma tendência para introduzir tecnologias da informação em todas as facetas da actividade humana. Desde a esfera meramente pessoal até ao nível relações entre os cidadãos e os estados ou entre estados, surgem tecnologias de comunicação ou de automação que propõem novas formas para os ciclos de actividade existentes ou sugerem mesmo novos ciclos de actividade.

Exemplo 1: Os processos de decisão na **administração pública** são exemplos paradigmáticos de ciclos de actividade onde as tecnologias da comunicação e da automação se tornam indispensáveis. Cada vez são mais exigentes os requisitos que são colocados nos serviços públicos e cada vez existem menos argumentos que justifiquem os custos administrativos que lhe estão inerentes. Por isso se acha indispensável redefinir estes ciclos de actividade à luz de novas soluções tecnológicas sem que tal ponha em causa direitos fundamentais dos cidadãos.

Exemplo 2: A **informática pessoal** veio trazer uma profunda alteração na perspectiva social das TI's aproximando-as do cidadão comum; por uma lado, no trabalho, permitindo-lhe adaptar os seus ciclos de actividade local às suas próprias especificações; por outro, e principalmente, permitindo estender às actividades de lazer uma capacidade de decisão que, sem o recurso a essas tecnologias, seria impensável. De facto é a informática pessoal, na sua componente de lazer, o principal motor económico das TI's actuais.

Exemplo 3: A **segurança** (ambiental, militar, económica) das sociedades e dos estados está intrinsecamente ligada às TI's que intervêm directamente nas componentes de monitorização, recolha e análise da informação, tomada de decisão e resposta. Não é exagero afirmar que a segurança de um estado de direito moderno seria impossível de garantir sem um envolvimento profundo das TI's.

A justificação subjacente à expansão das tecnologias da informação baseia-se, essencialmente, naquilo que podemos designar pelo **argumento da eficácia**:

*As TI permitem fazer de forma mais **eficaz** (barata, rápida, auto-suficiente, ...) uma actividade que não está adequada ao seu **contexto** (económico, social,...).*

Este argumento é usado frequentemente quando se manifesta o alargamento do contexto social de um determinado ciclo de actividades e, por isso, uma das medidas de ubiquidade de um sistema de informação assenta precisamente na noção de *impacto social* desse sistema.

Exemplo 4: Na **prestação de serviços de saúde**, quando o impacto de um determinado serviço deixou de ser apenas local a uma comunidade restrita mas passou a cobrir comunidades muito maiores e, principalmente, quando passou a estar associada a toda a comunidade onde o doente se insere, nessa altura as tecnologias da informação tornaram-se indispensáveis.

É importante frisar que, sendo o argumento da eficácia frequentemente atenuado com afirmações do tipo

. . . as TI's não passam de uma "ferramenta" e, essencialmente, nada mudam . . .

de facto não é assim; as TI's vão muito além das ferramentas e introduzem alterações profundas de paradigma com fortes impactos sociais e económicos nos contextos onde se inserem.

Uma outra característica desta ubiquidade está no seu carácter trans-fronteiriço. As fronteiras entre áreas de actividade, entre classes, sociedades, sistemas políticos e mesmo estados, são esbatidas, senão ultrapassadas, pelas TI's. As tecnologias da informação determinam uma nova **geografia social** que, sendo frequentemente surge confundida com a palavra "globalização", tem em minha opinião, implicações bastante mais profundas.

Exemplo 5: É frequente destacar o papel da Internet em transpor as barreiras criadas pelas sociedades fechadas com regimes políticos ditatoriais. Sendo a principal defesa desses regimes o fechar das fronteiras (territoriais, culturais) impossibilitando o discurso crítico e a avaliação pelos seus próprios cidadãos e pela comunidade internacional, é normalmente através da Internet que algumas dessas barreiras podem ser ultrapassadas.

Indo além das fronteiras tradicionais, a geografia da informação introduz novos discriminadores que, essencialmente, são de natureza cultural.

É tradicional destacar a grande barreira colocada entre os que têm acesso natural às TI's e os que não o têm ("info-excluídos"); na perspectiva de um eventual "info-mapa" esta barreira faz o papel daquela que, nos mapas medievais, separava o mundo conhecido do mundo mitológico.

Mas dentro do "mundo conhecido" muitas outras fronteiras surgem; algumas têm carácter tecnológico (entre sistemas operativos, entre comunidades tecnológicas), outras assentam no grau conhecimento. Estas barreiras são, como todas as fronteiras, ultrapassáveis; no entanto servem para definir uma geografia de comunidades com visões distintas sobre o papel da sociedade da informação.

Exemplo 6: Não são displicentes as barreiras criadas entre sistemas operativos (*Windows*, *McOS*, *Linux*), com reflexos directos na dicotomia *softwre livre*/*software comercial*.

Exemplo 7: Cultura e conhecimento determinam a forma como a **agente activo** interage com a Sociedade da Informação e determinam. A componente de lazer (jogos de computador, música, vídeo,. . .) é, juntamnte com a componente de comunicação rápida, característica de de um grupo etário mais jovem; normalmente estas pessoas

envolvem-se fortemente nos próprios sistemas e o grau de interacção é razoavelmente elevado.

Já a interacção com os sistemas instituicionais (administração pública, banca, comércio electrónico) é típica de um grupo etário mais velho que que, ao contrário do primeiro, tem uma atitude muito mais passiva em relação a esses sistemas. Só uma minoria é suficientemente informada e politicamente activa para poder influenciar decisivamente os sistemas de informação que condicionam o nosso quotidiano.

As fronteiras mais importantes, porém, são as que assentam na capacidade de controlo sobre os sistemas de informação; são barreiras muito mais difíceis de ultrapassar e são aquelas que são mais relevantes a este nosso curso.

Exemplo 8: **Questões:**

1. Que controlo pode exercer o cidadão comum sobre os seus dados pessoais que constam dos sistemas de informação da administração pública?
2. O sistema fincanceiro assenta exclusivamente em informação; que controlo exerce o cidadão sobre os recursos financeiros que lhe são relevantes?
3. Identificação: o que significa? Como pode o cidadão controloar a confidencialidade e provacidade das interacções com sistemas de informação?

Mobilidade

A tendência da MOBILIDADE está associada ao aproveitamento limite de recursos computacionais escassos e fisicamente condicionados. De certa forma a mobilidade pode caracterizar a crescente capacidade dos SI's de se isolarem dos seus suportes físicos e evoluírem para "informação pura".

Exemplo 9: É possível avaliar a mobilidade dos sistemas de informação seriando-os tendo em atenção as características computacionais do seus suportes de informação principais; nomeadamente, pode-se propor uma classificação dos sitemas de informação em *níveis de mobilidade* como se indica em seguida:

- Mobilidade mínima (recursos computacionais máximos) é o que cobre os tradicionais *mainframes* conjuntamente com servidores de rede, infraestruras de comunicação etc.
- Portabilidade: computadores portáteis e os sistemas da domótica (TV *set top box*,. . .).
- Dispositivos pessoais: os sistemas de computação e comunicação "de bolso"; e.e. PDA's e telefones celulares.
- Tokens de identificação criptográfica: *smart cards*, *ibuttoms*, *itokens*, etc.
- Mobilidade máxima (recursos computacionais mínimos): os materiais inteligentes; i.e., materiais com capacidade de computação própria o que inclui, por exemplo, têxteis inteligentes e nano-computadores.

Mobilidade está também relacionada com a noção que (em inglês) se designa por *pervasiveness*

que denota a tendência das tecnologias de informação em se "diluirem" em todo o contexto sócio/tecnológico onde se inserem.

Exemplo 10: Tradicionalmente, quando um sistema de informação se insere num contexto tecnológico bem determinado (numa linha de produção de uma fábrica, num hospital,. . .), as tecnologias de informação estão bem localizadas no tempo e no espaço; sabe-se distinguir os eventos onde intervêm os computadores dos eventos e onde esses computadores não intervêm; sabe-se onde estão os computadores e o que é um computador e o que não é um computador.

Pervasiveness é a tendência que procura eliminar estas distinções; as TI's não estão concentradas no tempo e no espaço mas estão distribuídas por todo o tempo e todo o espaço. Num sistema de informação onde esta tendência seja prevalecente, qualquer peça de tecnologia tem capacidade computacional própria e, o que é mais importante, integra essa capacidade computacional com a das restantes componentes do sistema.

Mesmo que a capacidade computacional individual de cada uma das componente tecnológicas seja diminuta e muito inferior à de um computador tradicional, a integração de todos esses pequenos recursos computacionais pode-se resultar num sistema computacional extremamente poderoso.

Hostilidade

Tradicionalmente os sistemas de informação são apresentados como entidades benigas que, perante um utilizador, têm como objectivo melhorar a eficácia de serviços e de processos ou satisfazer necessidades de lazer ou mesmo necessidades vitais indispensáveis à sua sobrevivência.

Porém esta não é uma visão realista da realidade dos sistemas de informação. A tendências **hostilidade** traduz a realidade essencial e parte do princípio que em qualquer sociedade (e a da informação não é excepção) as relações entre agentes têm formas *benignas* mas também assumem formas de *competição* e de *conflicto*, em vários graus que, em último caso, pode incluir a própria guerra.

Exemplo 11: Em termos de tendência para a hostiliadde como se poderão classificar sistemas de informação como

. . . um sistema de gestão hospitalar,

. . . um sistema de vendas (comércio electrónico),

. . . um jogo de computador (jogo de guerra) com vários participantes,

A tendência para a hostilidade tem como consequência torna indispensável identificar os **direitos da sociedade da informação** e os mecanismos que permitem garantir esses direitos.

A hostilidade dos SI's levanta algumas questões essenciais:

1. Faz sentido falar de direitos específicos da Sociedade da Informação ou basta transpor para o novo contexto os direitos actuais?
2. Nesse caso, será necessário redefinir ou "re-especificar" direitos ?
3. Na SI bastam os mecanismos usuais de garantia de direitos (tribunais) ou são necessárias soluções alternativas; que soluções tecnológicas podem dar essas garantias?

A discussão destes pontos constitui o núcleo da àrea que intitulamos por **Segurança Informática** e que vai ser a componente principal deste nosso curso.

Segurança: o que é?

Na Sociedade da Informação a questão da garantia de direitos coloca-se quando a hostilidade é uma tendência prevalecente; o entendimento que se tenha desta hostilidade condiciona a perspectiva que se vai ter da *segurança*. São possíveis dois pontos de vista:

Perspectiva determinística: *a hostilidade é excepcional e indesejável;*
a segurança é um atributo próprio de cada sistema de informação;
quando se introduz tecnologia como forma de garantir segurança (*criptografia*) essa solução é parte integrante do sistema de informação e cumpre-lhe isolar o sistema de eventuais violações á sua funcionalidade e integridade.

Perspectiva caótica: *a hostilidade é prevalecente, natural e real;*
a sociedade de informação é um eco-sistema com um desenvolvimento metabólico que resulta da interacção de vários agentes (institucionais ou não) em constante competição e, eventualmente, conflito; a segurança é a garantia dos direitos pessoais de cada agente;
a tecnologia é "pessoal e democrática": i.e. age ao nível das relações individuais dos agentes.

Pode-se dizer que, sob a perspectiva determinística, a segurança é *orientada ao sistema*; assume que existe uma fronteira nítida entre sistema e ambiente e assume que existe uma caracterização funcional tanto do sistema como do ambiente; o papel da segurança é a preservação dessa funcionalidade.

Esta abordagem conduz naturalmente á conclusão que sistemas fechados são eminentemente mais seguros que sistemas abertos.

Na perspectiva caótica a segurança é *orientada ao direito*; nela a fronteira entre sistema e ambiente é fluída e, por isso, faz apenas sentido falar de agentes, das suas relações e dos direitos que pretendem preservar.

Nesta abordagem a própria noção de sistema tem de ser revista e um sistema de informação pode não ser mais do que uma abstracção conveniente para descrever um determinado arranjo de relações inter-agentes.

Neste ponto de vista (algo extremo) os sistemas fechados nem sequer fazem sentido e, por isso, nem se devia colocar a questão da sua segurança.

Exemplo 12: Um sistema de *home banking* que adopte exclusivamente uma perspectiva determinística da segurança preocupa-se em que nenhum utilizador viole a integridade do sistema e, dessa forma, a sua funcionalidade. De facto a integridade acaba por ser mais importante que a funcionalidade já que interrupção do serviço pode ser inconveniente mas quase nunca é crítica. Uma perspectiva caótica teria tendência a privilegiar o equilíbrio de direitos entre o banco e os seus utentes assumindo que existem "interesses justos" de um lado e de outro que podem entrar em conflito.

Exemplo 13: A identificação dos utentes num sistema de saúde é uma outra situação onde as duas perspectivas da segurança entram em evidente conflito. É óbvio que a preservação da funcionalidade ou integridade está longe de ser suficiente para garantir os direitos de privacidade e confidencialidade dos dados clínicos que são essenciais aos utentes já que, neste sistema, a hostilidade essencial é interna ao sistema e raramente pode ser apontada a factores externos.

Exemplo 14: Considere-se um escritório de advogados que usa intensivamente o correio electrónico não só para estabelecer relações de cooperação entre colaboradores mas também para comunicar com outros agentes jurídicos (outros escritórios, tribunais, conservatórias, etc.). Uma perspectiva determinística da segurança tende a concentrar-se na preservação da funcionalidade e integridade do sistema de informação do escritório. A perspectiva caótica tem a atenção os direitos que regulam as relações de confiança entre os vários agentes intervenientes.

Contextos de Segurança

Assumindo uma abordagem de segurança orientada aos direitos faz sentido questionar em que planos se entendem e se interpretam esses direitos. Como exemplo tomemos de novo um sistema de informação hospitalar associado aos direitos dos seus utentes.

A justificação, numa "sociedada bem-ordenada", de princípios de respeito pela privacidade e confidencialidade dos dados clínicos cai dentro do **contexto ético** da segurança.

As normas legais que balizam os direitos de privacidade e confidencialidade e as instituições judiciais que lhe estão associadas determinam o **contexto jurídico** da segurança.

A implementação dos procedimentos que garantem os direitos, a gestão dos recursos necessários e a aceitação social destes mecanismos definem o **contexto económico/cultural** da segurança.

A caracterização precisa desses direitos em termos de comunicação, consenso ou automação de sistems de informação geram o **contexto tecnológico** da segurança.

Contexto Ético

Na perspectiva do "agente activo" da Sociedade da Informação é particularmente oportuno discutir os princípios morais essenciais que devem orientar o seu comportamento; isto porque, dada a ausência de uma tradição ética neste domínio, não existe um consenso suficientemente alargado sobre quais são esses princípios nem como se justificam.

Alguns princípios abstractos, como a privacidade dos dados pessoais, são suficientemente consensuais; já outros, como a titularidade ou a propriedade de items de informação, estão longe de obter tal consenso.

Mesmo que seja possível acordar sobre princípios morais abstractos, ainda assim, dada uma situação concreta e no âmbito de um sistema de informação específico, coloca-se sempre a questão de saber quais os princípios éticos que devem reger essa situação, como se justificam socialmente esses princípios e como devem ser apresentados de modo a ser possível chegar ao "equilíbrio social" que está sempre inerente ao conceito liberal de justiça.

Partindo do princípio que está definido um contexto básico de justiça (**sociedade bem-ordenada**) que podemos caracterizar por

- um consenso e um respeito dos **direitos básicos** (liberdade de pensamento, liberdade de associação, integridade pessoal, liberdade de escolha),
- a garantia de um **mínimo social** (de recursos e bens), sem o qual os direitos básicos se tornam meramente formais sem possibilidade de serem efectivos para as camadas da população economicamente abaixo desse limiar,
- uma vontade maioritária genuinamente expressa para a obtenção de um **equilíbrio social** onde "todos os que tomam parte em decisões justas têm consciência do seu sentido de justiça e nos seus actos suportam essas decisões",

então, e só então, é possível conjecturar alguma abordagem que permita resolver o nosso problema fundamental face a uma situação concreta

quais os princípios éticos relevantes, como se justificam e como se apresentam

O pensamento do liberalismo político apresenta uma primeira justificação para princípios éticos que reside na ideia do **equilíbrio reflexivo**:

> *O agente, perante uma situação concreta, supondo que está devidamente informado dos factos, que não está sujeito a conflitos de interesses ou pressões e procede com reflexão, estabelece um conjunto de juízos (e respectivas justificações) que lhe parecem correctos nessa situação; em seguida procura formular princípios abstractos que suportem esses juízos; existindo, como é natural, discrepâncias entre a concretização dos princípios e os juízos iniciais, procura adaptar iterativamente uns e outros de forma a atingir um eventual equilíbrio.*

Obviamente que, sob o ponto de vista da concepção da justiça, isto é insuficiente; se a função primordial da concepção da justiça é a de servir como uma referência pública e justa para resolução de conflitos entre agentes e instituições, então a noção de a associação de "juízo" com "interesse justo" é crucial.

A noção de **posição original**, contempla todos os agentes com "interesses justos" relevantes à situação concreta aceites como legítimos por todos (no sentido em que cada se pode ver na posição de titular desse interesse); a noção de "interesse justo" não pode permitir que juízos

derivados da posição original beneficiem indivíduos ou grupos de indivíduos pela sua posição no contexto social ou pela sua concepção própria de "bondade" das decisões.

Uma última ideia conducente à justificação dos princípios éticos é a **racionabilidade pública**.

Pode-se argumentar que os princípios do equilíbrio reflexivo e da posição original podem conduzir a situações onde, com o evoluir do tempo, possam ocorrer diferentes concepções para princípios éticos essenciais, concepções essas obtidas de forma completamente racional; o liberalismo político procura compatibilizar a existência de tais concepções com a noção de equilíbrio social inerente a uma sociedade bem-ordenada.

A ideia de "consenso público" resulta desta compatibilização; por um lado este consenso deve ser permitir um sentido público de justiça que ultrapasse a diversidade dessas concepções; por outro lado todas as questões essenciais devem ser resolvidas recorrendo a mecanismos políticos em que todos (independentemente das suas concepções particulares para os princípios básicos) se possam rever e tenham interesse em preservar; em terceiro lugar permitindo que a concepção da justiça sirva, como já foi referido, de referência pública à luz da qual sejam resolvidos conflitos e justificados os juízos.

Exemplo 15: A **privacidade dos dados clínicos** é um princípio ético amplamente suportado pela legislação (desde a Constituição da República até à Lei de Protecção de Dados Pessoais); é também um princípio que tem suporte consensual da opinião pública. Por isso deve ser fácil justificá-lo.
Como?

Exemplo 16: A **preservação da propriedade intelectual** de obras artísticas audio-visuais distribuídas da Web, é um princípio ético mais difícil de justificar.
É interessante um exercício em que se usa esta metodologia de justificação para construir opiniões a favor e contra este princípio.

Exemplo 17: De que forma se justifica uma política universal de **identificação obrigatória dos cidadãos** ?. Que "interesses justos" estão em causa? É possível construir justificações coerentes contra e a favor dessa identificação? E se a identificação fosse facultativa?

Exemplo 18: Um aspecto expressamente definido na Constituição da República (nº 5 do Art. 35º) é proibição da **atribuição de um número de identificação único** aos cidadãos. Como se justifica eticamente essa proibição num contexto administrativo onde abundam números identificadores do cidadão (BI, Segurança Social, Contribuinte, etc.).

Contexto Jurídico

Os mecanismos legais e judiciais cobrem uma parte relativamente restrita das relações que constituem o núcleo essencial da Sociedade da Informação. De certa forma o contexto jurídico existente assenta num modelo que tem dificuldades em se adaptar à dimensão e ao nível de complexidade destas relações; isto conjuga-se com o facto de as instituições judiciais (nomeadamente os tribunais) ainda têm dificuldades em lidar com este tipo de relações sociais.

No entanto algumas áreas fundamentais a este curso estão já cobertas por um suporte legislativo razoável que, para além da Constituição da República (no seu artigo 35º), deriva essencialmente de transcrições da legislação comunitária.

Sendo essencial integrar cada situação concreta no seu contexto jurídico não é, no entanto, este o objectivo primário deste curso e portanto as referências serão necessariamente breves.

Contexto Económico/Cultural

A gestão dos aspectos culturais da segurança é frequentemente descurada; nomeadamente na forma como as pessoas têm consciência dos seus direitos e gerem os mecanismos de segurança que lhes garantem esses direitos.

Exemplo 19:

Veja-se a forma displicente com que muitos de nós gerimos as palavras chave e códigos de acesso a um grande número de sistemas de informação de que dependemos.

De alguma forma este próprio curso pretende ser uma acção com objectivos de colmatar essa deficiência.

A componente económica é muito mais evidente já que quase toda a actividade económica numa sociedade industrializada está dependente de sistemas de informação seguros. Este é um aspecto que cai um pouco fora dos objectivos do curso mas que procuraremos referir sempre que as situações estudadas assim o motivarem.

Contexto Tecnológico

A caracterização de um sistema de informação através de relações internas (estabelecidas entre os agentes constituem o sistema) e externas (estabelecidas com outros sistemas de informação) implica uma definição clara dos direitos associados a tais relações.

Normalmente estes direitos referem-se ao grau de partilha de conhecimento entre os vários agentes e ao grau de confiança que cada agente associa a tal conhecimento. A tecnologia fornece algumas garantias para que tais direitos não sejam violados.

O contexto tecnológico para a segurança de um determinado sistema de informação, determina quais são os agentes que nele têm "interesses legítimos" e os que não têm (os "intrusos"). Define depois as relações de conhecimento e confiança entre esses agentes e caracteriza os direitos relevantes.

Face a essa descrição escolhe a tecnologia adequada à preservação de tais direitos.

Exemplo 20: De novo o escritório de advogados referido no exemplo **??**.
Se vários advogados contribuem com peças processuais para um mesmo processo têm de existir meios que garantam a confiança entre os advogados em relação à **autenticidade** de tais elementos. Por outro lado a **confidencialidade** é crítica: nem todos os advogados necessitam ou devem ter conhecimento sobre todas as peças no processo. A política de **autorizações** (quem faz o quê e quando) é também crítica; nomeadamente a **prova do cumprimentos de prazos** é essencial tanto sob o ponto de vista interno como sob o ponto de vista externo (existem deveres de informação atempada em relação a vários agentes externos e existem os prazos judiciais). Finalmente nada destas questões pode ser resolvida sem uma forma expedita de **identificação** dos agentes (internos e externos).
Este conjunto de relações e direitos determina o contexto tecnológico deste sistema; é este contexto que vai determinar as tecnologias usadas para garantir tais direitos.

Exemplo 21: Considere-se um tipo de situação que ainda não foi referia: o **voto electrónico**.
É necessário garantir a **unicidade** do voto (cada votante só vota uma vez) e a sua **autenticidade** (só vota quem tem o direito de voto). É preciso garantir também o **anonimato** do voto quer no acto de votação quer no processo de contagem. O votante também quer ter garantias de que o seu voto é **bem contado** (é contado e é atribuído ao sítio certo). Finalmente o escrutinador deve ter capacidade de provar perante terceiros (a CNE, um juíz, etc.) que procedeu correctamente sem que para isso necessite de violar o anonimato do voto.
O processo de votação electrónica é, assim, um dos mais exigentes em termos de tecnologia de segurança.

Um pouco de Teoria dos Sistemas

Numa perspectiva informal, **sistema** é qualquer conjunto de **agentes** cujo **comportamento**, ao longo do tempo, é condicionado pelo comportamento dos restantes.

O condicionalismo mútuo de comportamentos estabelece-se através de **relações** entre os vários agentes; nos sistemas de informação estas relações assentam em tecnologias específicas (obviamente, as tecnologias da informação) que "colam" as suas várias componentes. A natureza de cada sistema de informação é condicionada pela forma como essa "cola" funciona.

Sobre essa caracterização (agentes, relações, comportamentos, etc.) coloca-mos o nível da segurança, cujo contexto tecnológico define, como vimos, direitos e tecnologias que garantem esses direitos.

Nomeadamente, quais são os objectivos dessa "cola"? De que forma os agentes condicionam mutuamente os respectivos comportamentos?

Genericamente, ao nível do sistema (ignorando a segurança), nos sistemas de informação é possível identificar várias classes de objectivos para as tecnologias de informação, objectivos esses que se podem classificar nas seguintes classes:

comunicação onde as tecnologias potenciam a partilha de conhecimento entre os agentes de um sistema.

consenso onde as tecnologias procuram definir uma base coerente de conhecimento partilhado por vários agentes.

automação onde as tecnologias potenciam o controlo dos comportamentos de agentes específicos dentro do sistema.

Exemplo 22:

Tomando como base o escritório de advogados dos exemplos **??** e **??** e inserindo-o num sistema mais vasto que inclua tribunais, conservatórias, outros escritórios, etc., será interessante tentar identificar os objectivos das várias tecnologias de informação à luz de uma caracterização de sistema.

A descrição de um sistema recorre a algumas palavras que temos vindo a usar (ou que usaremos em breve) e que convém clarificar; temos

- entidades essenciais como **agente**, **conhecimento**, **evento** e **comportamento**.
- atributos como **item** e **acto**,
- relações entre *agentes*/*eventos* e *conhecimento* como **partilha**, **controlo** e **confiança**,
- relações entre *agentes*/*eventos* e *comportamentos* como **causalidade**, **incompatibilidade** e **cooperação**.
- entidades de 2^{o} nível como o **conhecimento introspectivo**: conhecimento sobre o conhecimento.

Muitas são as interpretações possíveis para estes conceitos e está fora do contexto deste curso tentar formalizar qualquer delas. De qualquer forma é conveniente ter uma perspectiva geral do seu papel pela importância que têm na conceptualização dos direitos que associamos a um qualquer sistema de informação com relevância jurídica.

Agentes & Eventos

Agentes e **Eventos** designam as entidades fundamentais de qualquer sistema dinâmico: um sistema que evolui com o tempo.

Agentes podem ser entes com personalidade jurídica ou agentes artificiais; nesse caso são normalmente processos informáticos que automatizam determinados procedimentos.

Eventos representam "marcas temporais" significativas na caracterização global do sistema; os eventos não são atributos de nenhum agente em particular mas são vistos como componentes do comportamento do sistema como um todo.

Por questões de simplicidade conceptual vamos supor que o reportório de agentes e eventos que compõem um sistema é estático (não evolui com o tempo); deste modo existe uma fronteira bem definida entre o sistema e "aquilo que não é o sistema".

Essa entidade extra-sistema, mas com quem o sistema interage, designa-se por **ambiente**.

Exemplo 23: Recuperemos o exemplo do escritório de advogados (exs. **??** e **??**). Que agentes e eventos podemos associar a este sistema? Sem tentar ser exaustivo pode-se enumerar:

Agentes

Cada um dos advogados, com o seu conhecimento e com os actos a que está habilitado é um agente. Se o escritório possuir uma qualquer forma de automatização de procedimentos (ao nível das comunicações e ao nível do arquivo e recuperação de informação) então cada procedimento automático é definido por um ou vários agentes artificiais.

Eventos

Cada julgamento é claramente um evento; a apresentação de uma acção ou de uma alegação são também eventos; entrevistar uma testemunha, reunir com um cliente, enviar uma nota de honorários, etc., são tudo exemplos de eventos que vão determinar a dinâmica deste sistema.

O **ambiente** é, neste caso, formado por todos os restantes sistemas com que o escritório interage. Estes sistemas serão necessariamente os tribunais, outros escritórios de advogados, conservatórias e outros organismos do estado, e ainda, principalmente, os seus clientes institucionais ou particulares.

Nomeadamente para clientes institucionais é natural que eles próprios estejam associados a sistemas de informação complexos (com contabilidade, unidade jurídica, etc.) com que o escritório tem de interagir. Nesse caso as relações já não se estabelecem ao nível global dos sistemas mas com agentes específicos dentro desses sistemas.

Agentes e eventos são caracterizados pelos *atributos* que lhes estão associados e pelas *relações* que são estabelecidas entre as entidades fundamentais através desses atributos.

Os atributos que caracterizam a individualidade de um agente são os *items* do conhecimento que poderá (eventualmente) obter, e os *actos* a que está habilitado.

Exemplo 24: Saber que um agente pode conhecer uma chave de acesso é um atributo (item) de um agente mas não é conhecimento; só passa a ser conhecimento quando o agente sabe qual é o valor exacto dessa chave; na nosa terminologia diz-se que o agente "partlha" esse conhecimento. Assim, uma forma particular de conhecimento, está na associação de um valor concreto a um item.

Do mesmo modo saber que um advogado está habilitado para entrevistar uma testemunha é um acto (um atributo do agente) mas ainda não é comportamento. Só passa a ser comportamento quando se concretiza num evento e sabe-se que o acto ocorreu com uma testemunha bem determinada, numa data e hora bem determinadas, etc. Isto indica que uma forma particular de evento é uma ocorrência específica de um determinado acto.

Atributos representam a "visão estática" do sistema; a própria enumeração dos agentes e dos eventos não chega para caracterizar a sua dinâmica. Para isso precisamos de mais informação que nos é trazida pelas duas outras noções essenciais.

Conhecimento & Comportamento

A cada item de informação, atributo de um qualquer agente, pode estar associado um valor desconhecido ou então um valor concreto. Este arranjo de associações de valores conhecidos ou desconhecidos a items é um **estado de conhecimento** ou, simplesmente, **conhecimento**.

Um agente, que tenha um determinado item como atributo, pode ou não **partilhar** esse conhecimento; o arranjo de valores que o agente partilha num determinado instante do tempo é a sua **visão local** do conhecimento. Um **segredo** desse agente é um item que apenas ele partilha; se o conhece ou não depende apenas do estado do conhecimento nesse instante.

Dentro de todos os eventos possíveis de um sistema, um determinado instante do tempo só são possíveis um determinado arranjo de eventos. A um tal arranjo chamamos o **comportamento** do sistema nesse instante.

A ocorrência de um evento altera os valores (ou o grau de conhecimento) associados a determinados items do conhecimento. Este facto exprime a relação de **controlo** entre eventos e conhecimento.

Exemplo 25:

De novo o exemplo **??**. O estado do conhecimento deste escritório, num determinado instante, contém a informação global que os vários agentes (advogados) podem ou não partilhar.

Nomeadamente, o conteúdo de todos os processos associados ao escritório faz parte desse estado de conhecimento; obviamente que esse conhecimento vai variando com o tempo. Selectivamente, cada um dos advogados tem acesso ao todo ou a parte de cada um dos processos; isso é determinado pelos items que ele partilha e constitui a sua visão local do estado de conhecimento.

A cada advogado estão associados actos a que está habilitado; as diferentes possibilidades de ocorrências de actos possíveis num determinado instante determina o comportamento do sistema nesse instante.

Cada ocorrência de um acto é um evento que vai influenciar os futuros valores de certos items do sistema. Por exemplo, em abstracto, o inquérito a uma testemunha é um acto; mas uma ocorrência concreta desse inquérito é já um evento; obviamente que esse evento vai determinar o estado de conhecimento futuro de um ou mais advogados.

Existem eventos, como por exemplo um julgamento, que não podem ser vistos como simples ocorrências de actos de agentes do sistema; no entanto a forma como esses eventos afectam o estado de conhecimento do sistema é feita através de ocorrências de tais actos. Por exemplo o julgamento só afecta o estado do conhecimento do escritório se houver algum advogado que leia a sentença; e isso já é uma ocorrência de um acto próprio do sistema.

Os eventos possíveis num determinado instante (i.e. o comportamento do sistema nesse instante) vão depender do estado de conhecimento mas também, crucialmente, no grau de **confiança** que cada evento deposita nesse conhecimento.

Nomeadamente um agente, que tem associado um acto, pode fazer com que esse acto ocorra (ou não) em função do grau de confiança que tem no conhecimento que partilha.

Outra relação importante, agora entre eventos, é a da **incompatibilidade**; isto acontece, por exemplo, quando a ocorrência de um acto impede completamente a ocorrência de outro acto; ou, por exemplo, quando a ocorrência de uma acto altera o estado de conhecimento de uma forma que é incoerente com a eventual alteração do conhecimento provocada pela ocorrência de outro acto.

A outra relação fundamental entre eventos é a relação de **precedência** ou **causalidade**; mais uma vez, é vulgar que um acto não possa ocorrer sem que um outro acto acorra: o segundo precede o primeiro.

O conjunto de eventos que precedem um evento **A** e que não são mutuamente incompatíveis designa-se por **configuração** de **A**.

Incompatibilidade e precedência são relações fundamentais (não podem ser expressas à custa de outros conceitos). Porém estão relacionada através da *Lei dos Precedentes Incompatíveis*

> Se o evento **A** precede o evento **B** e é incompatível com o evento **C**, então também **B** é incompatível com **C**.

Podemos ter, finalmente, uma ideia mais precisa do que é comportamento

> Um conjunto de eventos forma um comportamento quando cada um tem suficiente confiança no estado de conhecimento, não são mutuamente incompatíveis e nenhum precede outro.

Num determinado estado de conhecimento, são possíveis vários comportamentos: cada conjunto de eventos que satisfaça estas condições define um comportamento.

Comportamentos diferentes podem ser **incompatíveis** caso contenham eventos incompatíveis; ou um pode **causar** outro desde que o primeiro contenha as configurações de todos os eventos no segundo; etc. . .

A **cooperação** é uma associação entre dois ou mais eventos, interpretada como um evento único, que produz, no mínimo, os efeitos individuais dos cooperantes.

Exemplo 26: Na continuação do exemplo **??** vamos procurar reconhecer as relações fundamentais que determinam o comportamento deste escritório de advogados.

Como consequência do evento *"inquérito à testemunha X"* o estado de conhecimento foi alterado; isto não significa que o agente *"advogado Y"* tenha confiança nesse novo conhecimento; se o agente tiver como atributo o acto *"processar"*, uma ocorrência particular desse acto pode depender dessa confiança.

Por outro lado parece ser claro que exista uma precedência entre os eventos *"inquérito à testemunha X"* e *"acção contra X por falsas declarações"*: o segundo é precedido pelo primeiro. Outros eventos podem ter precedência sobre *"acção contra X . . . "*; o conjunto de tais eventos constitui a configuração do evento em questão.

Incompatibilidade de eventos num escritório de advogados é frequente; por exemplo, o evento *"acção contra X. . . "* deve ser incompatível com o evento *"facturar o cliente X. . . "*!

Um comportamento, para este estado de conhecimento, pode conter o comportamento *"acção contra X"*; porém este mesmo comportamento não pode conter o evento *"inquérito à testemunha X. . . "* por preceder o primeiro; também não pode conter o evento *"facturar o cliente X. . . "* por incompatibilidade de eventos.

Exemplo 27: Considere-se de novo o exemplo do voto electrónico (exemplo **??**).

A um primeiro nível de análise os agentes essenciais são o **votante**, a **urna** e o **escrutinador**. Temos depois outros agentes que refinam o comportamento deste três: a **mesa de voto**, por exemplo, é uma componente do agente *urna*.

Actos que são atributos do *votante* são, por exemplo, **gerar voto** e **votar**; outros actos ligadas à confirmação e prova de voto podem ser definidos. O item de conhecimento essencial é o **voto**; no entanto a confirmação e prova de voto assim como as garantias de anonimato e autenticidade do voto vão exigir, naturalmente, outros items; sem entrar em detalhes são necessários, no mínimo, dois segredos adicionais: a *chave privada* e o *identificador de confirmação*. Actos atributos da urna serão, *autenticar votante* e *receber voto*; actos do escrutinador serão *contar votos* e *provar correcção do escrutínio*, etc..

Eventos podem resultar da **cooperação** de ocorrências de actos diferentes; p.ex. *"votante X vota"* conjuga-se com *"recepção do voto de X"* (derivados de actos distintos) para gerar um único evento *"X votou"*.

Precedência: os eventos *"X define o seu voto"* (ocorrência de um acto de votante) e *"autenticação do votante X"* (ocorrência de um acto do agente urna) precedem ambos o evento *"X votou"*.

Confiança: a autenticação de um eventual votante provoca alterações no conhecimento; o grau de confiança que a urna tem nesse conhecimento permite ou não que ocorra o acto de receber o voto respectivo.

Incompatibilidade: duas ocorrências distintas de recepção de voto para o mesmo votante são eventos incompatíveis.

Técnicas de Segurança

Sobre a definição de agentes e suas relações, que constituem um sistema, faz parte do nosso programa especificar os direitos que caracterizam essas relações e propor tecnologias que contribuam para a garantia desses direitos.

Antes porém é preciso inventariar as técnicas que estão ao nosso dispor e compreender as suas finalidades e limitações.

Essencialmente todas as técnicas relevantes à segurança dirigem-se ou à **confidencialidade** ou então à **autenticidade** da informação; de facto qualquer técnica criptográfica é essencialmente um mecanismo para gerir **segredos** e/ou **confiança** em condições adversas.

Como vimos antes, agentes agem em função da confiança que depositam sobre o conhecimento; nomeadamente agentes usam técnicas criptográficas em função do grau de confiança que têm no conhecimento dessas técnicas.

Mas, *o que é "confiança"*?

Confiança

A relação de confiança de um agente em relação a um outro agente (**A** *confia em* **B**) resulta da *convicção* que **A** tem de que qualquer ocorrência possível dos actos de **B** nunca será hostil ao comportamento de **A**; i.e., não viola direitos de **A**.

Similarmente, um agente confia num item de conhecimento quando confia no **autor** desse item.

Isto leva-nos a pensar que a relação de"confiança" estabelecida por um determinado agente resulta da conjunção de várias noções; por exemplo,

- **crenças**: visões do conhecimento sobre os quais o agente deposita confiança absoluta; a crença pode ser **bem fundada** ou não ("*well-founded*" ou "*ill-founded*") dependendo da sua inserção no estado de conhecimento global do sistema.
- **provas**: processo cognitivo que permite estabelecer uma relação de confiança a partir de crenças; tipicamente uma prova é, ela própria, resultado de outras crenças;
- **agentes amigos** ("*trusted agents*"): agentes cujos actos nunca originam violação dos direitos do agente em questão; a convicção de que um determinado agente cai dentro desta classe é uma forma particular de crença.

Exemplo 28:
Considere-se o sistema simples que contém um agente de trânsito **A** e o evento **e** $\equiv$ "*o automobilista* $\boldsymbol{X}$ *conduzia um automóvel às ?? horas do dia ??*".

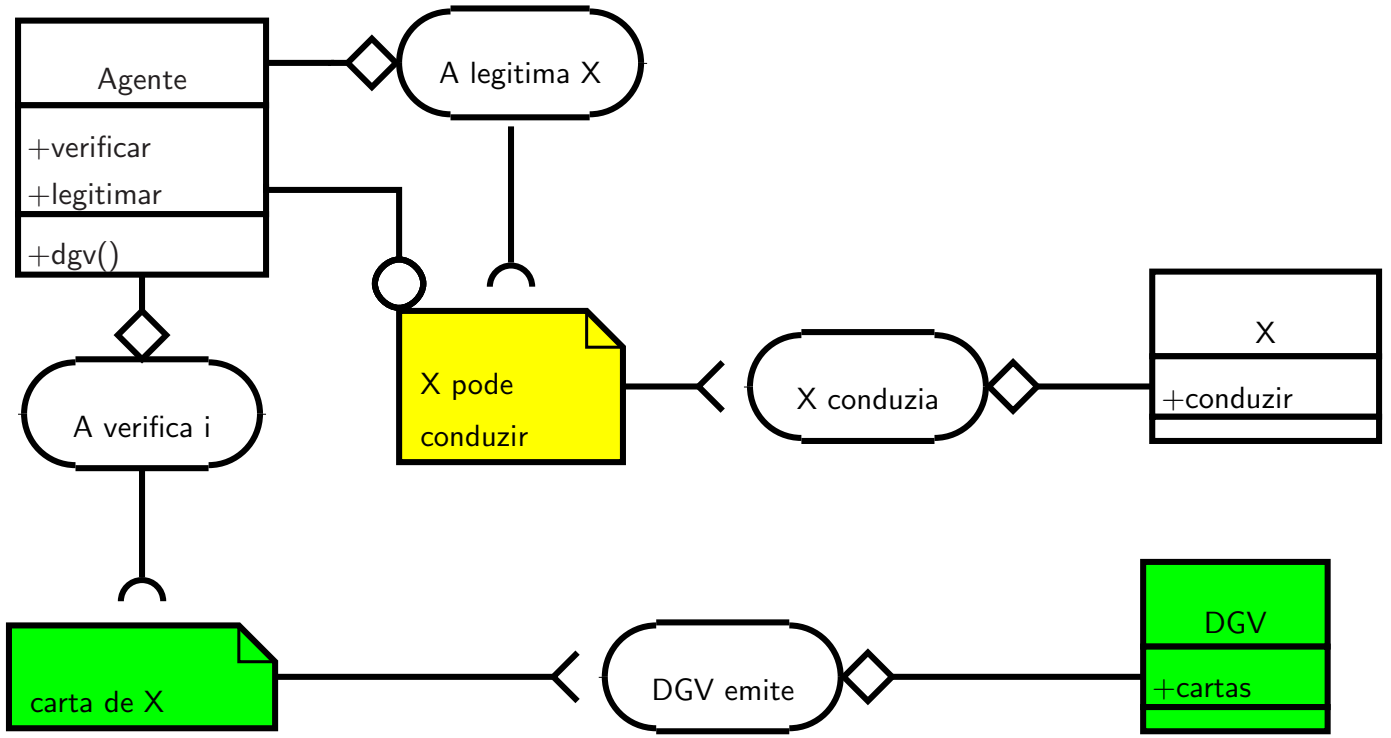
Vários outras componentes vão ocorrer neste sistema mas estas duas são as essenciais. Por exemplo, como consequência de **e** resulta o item de conhecimento **i** $\equiv$ "*o automobilista* $\boldsymbol{X}$ *está habilitado a conduzir automóveis*". Que relação de confiança se estabelece entre **A** e **i**?

Essa relação é estabelecida por um outro item de informação: a carta de condução de **X**; esse item resulta do evento "*emissão* de carta" que, por seu turno, é uma ocorrência de um acto de um outro agente: a **DGV**.

A tem como **crença** que **DGV** é um **agente amigo** e por isso acredita que todos os eventos que são ocorrência dos seus actos produzem items que são de confiança; essa crença torna possível o evento "$\boldsymbol{A}$ *verifica* $\boldsymbol{i}$" que conduz à relação de confiança entre **A** e **i**. Todo este mecanismo constitui a **prova** que justifica essa relação de confiança.

O seguinte diagrama representa os agentes com os seus actos, os eventos e os items de informação; estão também representadas as relações de ocorrência, controlo e confiança; dessas últimas distinguem-se as relações de crença entre agentes e items e as relações de confiança que possibilitam eventos.

Neste diagrama todo o conhecimento é considerado público; por isso não é necessário explicitar a relação de partilha. Nos agentes representamos apenas os seus actos e as suas crenças não sendo necessário representar os seus segredos.


Agente
+verificar
+legitimar
+dgv()
A legitima X
A verifica i
X pode
conduzir
X conduzia
X
+conduzir
carta de X
DGV emite
DGV
+cartas

No caso particular da relação de confiança entre um agente e uma técnica criptográfica (e que motiva o agente para usar essa técnica) é possível defini-la por uma de duas crenças:

Confiança por Obscurantismo (ou *confiança nos sistemas fechados*): o conhecimento sobre a técnica criptográfica é restrito a **agentes amigos**; a confiança é consequência da convicção que a técnica só é conhecida por agentes que nunca irão agir de forma hostil.

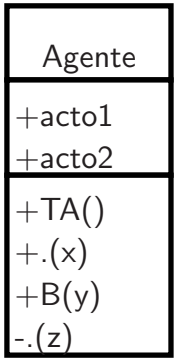
Confiança por Escrutínio Público (ou *confiança nos sistemas abertos*): o conhecimento sobre a técnica criptográfica é público e existem incentivos à publicação de tal conhecimento; a confiança é consequência da convicção de que quaisquer actos que conduzam a eventos hostis têm grande probabilidade de estar, à partida, identificados uma vez que a comunidade que tem interesse em os tornar públicos é grande.

A primeira conduz, tipicamente, a técnicas criptográficas mais simples; no entanto não é, normalmente, uma crença bem-fundada por uma razão também simples: na eventualidade de um agente hostil, por qualquer forma, ter tido acesso à técnica então tem todo o interesse em não tornar esse conhecimento público; o que torna muito difícil detectar essa falha.

Por isso existe uma tendência crescente para basear a confiança nas técnicas criptográficas sujeitas ao escrutínio público e assentar a segurança nos segredos e na confiança sobre a capacidade de manter esses segredos.

Desta forma quando de diz que um determinado item de informação x é um **segredo** de um agente **A**, automaticamente acrescenta-mos a **crença** de que esse agente é o único que partilha o conhecimento de x; como habitualmente essa crença pode ou não ser bem-fundada. Assim não existe uma fronteira nítida entre o que são segredos e o que são crenças.

Num diagrama um agente é representado pelo seu nome, pelos seus actos e pelas suas crenças. A associação dos atributos aos agentes pode ser pública ou privada; a distinção é expressa pelos sinais $+$ ou $-$ antes do atributo.



Neste exemplo, $TA()$ indica que o agente **TA** é um "*trusted agent*". $B(y)$ é a crença de que **B** é o único agente que conhece o item y.

O ponto $\cdot$ representa o próprio agente; assim $\cdot(x)$ é a crença de que o próprio é o único que conhece o item x. Já a crença $-.(z)$ tem a haver com conhecimento introspectivo; não só indica a crença de que o próprio é único que conhece o item z mas também indica que esse conhecimento sobre o conhecimento é confidencial.

Cifras

Cifras são técnicas criptográficas que lidam com a confidencialidade da informação; i.e., a crença de que o conhecimento de um determinado item de informação é partilhado por um conjunto restrito e pré-determinado de agentes. O uso típico de uma cifra está representado no diagrama seguinte.

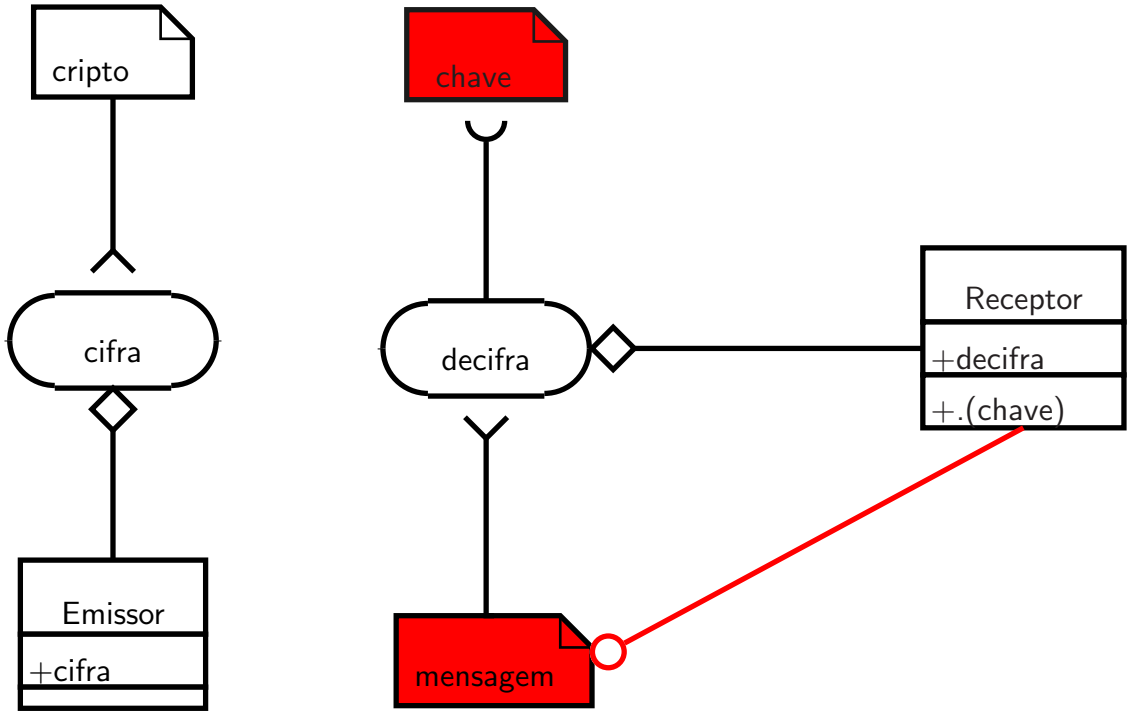
Envolve dois agentes: o **Emissor**, que está habilitado a **cifrar** textos, e o **Receptor**, que está habilitado a **decifrar**[2] mensagens.

Como resultado do evento "cifrar" é produzido um **criptograma**; neste sistema o criptograma é considerado público e por isso pode ser usado em qualquer evento que saiba fazer uso dessa informação.

Para decifrar o receptor tem acesso exclusivo a um segredo: a **chave**; o evento "decifrar" requer o conhecimento da chave (representado por uma relação de confiança nessa informação) e produz uma **mensagem**.

[2] Mas nunca *"encriptar"* e *"desencriptar"* dado que ninguém está habilitado a actos que não existem na língua portuguesa.

Uma relação de confiança é estabelecida em consequência representando a crença que o receptor é o único agente que conhece a mensagem.



Nota: Representamos a vermelho os items de conhecimento cuja partilha é restrita; a relação de confiança a vermelho denota a consequência de um acesso restrito a informação.

O facto de o criptograma ser público implica que ele está disponível a qualquer agente hostil (atacante) que, de forma ilegítima, tente daí recuperar a mensagem.

Pode parecer estranho não prestar-mos atenção ao modo como o criptograma é produzido; poderia parecer que se devia impor algo da forma:

> *"o criptograma exige o conhecimento prévio de um texto que vai coincidir com a mensagem decifrada".*

De facto uma condição deste tipo tem a haver com a **correcção** da cifra mas pouco tem a haver com segurança. Como nestes sistemas é a segurança (e não a correcção) a nossa preocupação principal não sentimos grande necessidade de especificar esta condição.

Uma cifra correcta diz-se **simétrica** que o evento de cifrar exige que também o emissor conheça a chave usada pelo evento decifrar.

Uma cifra correcta diz-se **assimétrica** se o evento de cifrar apenas exige o conhecimento do texto que vai coincidir com a mensagem.

Exemplo 29: De entre todas as técnicas criptográficas as cifras são as mais antigas e têm uma longa folha de serviços quer no campo de guerra como no campo diplomático. Já os exércitos de César usavam cifras e existem exemplos de máquinas de cifrar, por exemplo, nas civilizações chinesa e azteca.

A época mítica das cifras e dos ataques às cifras é certamente a 2ª Grande Guerra Mundial; os ataques à máquina Enigma constitui fonte de exemplos paradigmáticos nos processos de gestão segura da informação.

No entanto nada do que foi feito até aquela altura estava preparado para as consequências da introdução dos computadores; de facto uma cifra considerada extremamente segura na 2ª GG, e da qual dependia a sobrevivência de nações, é hoje uma "brincadeira" para qualquer criptógrafo principiante munido de um computador portátil.

As cifras modernas têm de ser capazes de resistir a atacantes dispondo de um poder computacional praticamente ilimitado (muitas vezes, instituições muito poderosas com muito tempo e muito dinheiro); simultaneamente têm de se limitar, elas próprias, a recursos computacionais muito reduzidos (um telemóvel, uma máquina ATM - vulgo "Multibanco", um computador portátil, etc.).

Por isso requerem um profundo estudo das suas propriedades matemáticas e é uma ilusão pensar que um simples "amador" pode produzir algo que resista a este tipo de restrições sem esse estudo e sem a experiência combinada de uma vasta comunidade de criptógrafos.

Dois nomes a destacar em termos de cifras: o AES é o novo standard para a cifra que protege o sistema financeiro mundial; o KASUMI é a cifra que acompanha o standard das comunicações móveis de 3ª geração (vulgo, UMTS).

Assinaturas Digitais

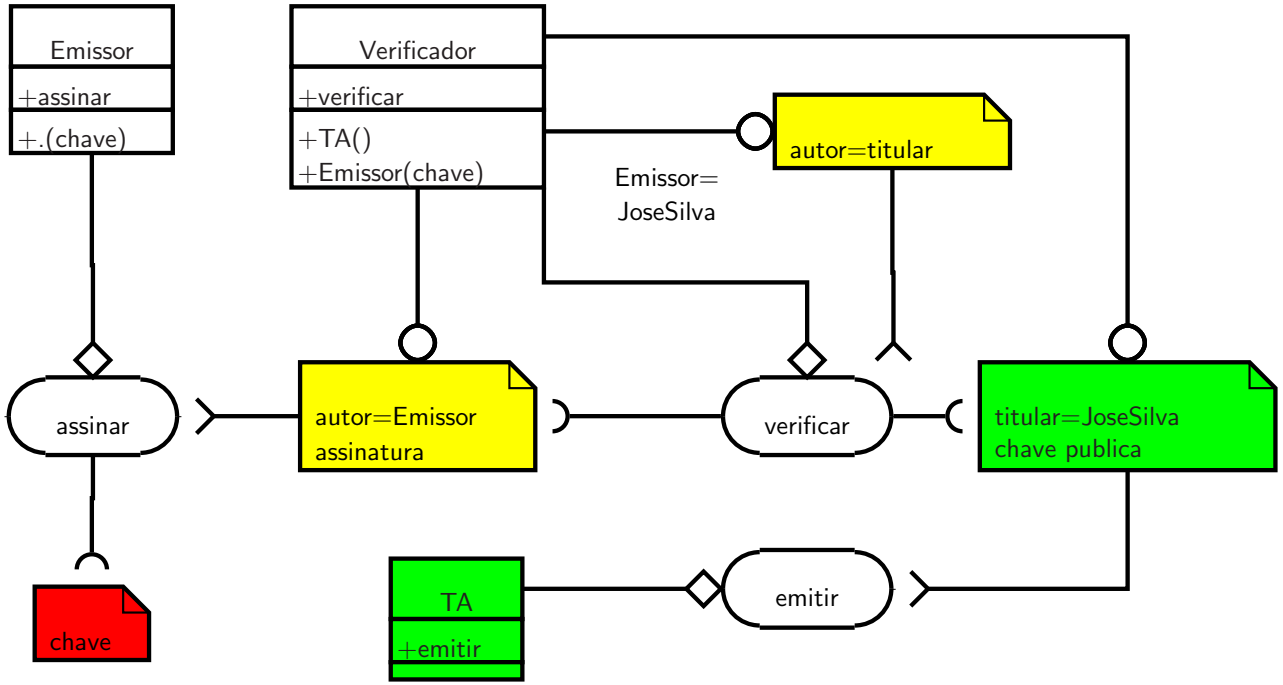
Assinaturas digitais são técnicas criptográficas que se destinam a autenticar items de informação.

O resultado final de um mecanismo de assinatura/verificação é o estabelecimento de uma relação de confiança entre um agente, designado por **Verificador**, e um item de informação que lhe permite concluir propriedades do autor do documento; nomeadamente que o autor tem um determinado nome. A fonte de confiança reside na existência de um terceiro agente: **TA** ("trusted agent").

O diagrama seguinte representa uma situação paradigmática do uso de assinaturas digitais e da prova que justifica a relação de confiança em relação à **autoria** da assinatura.

Normalmente esta relação não é suficiente para garantir a autenticidade de um documento; pelo menos é necessário garantir, ainda, que o documento assinado e o documento verificado são o mesmo; i.e., é necessário ter confiança na sua **integridade**.

O diagrama da página **??** representa essa relação de confiança.



AUTORIA

Notas:
Com a cor verde representamos os "agentes amigos" e a informação pública que, por ter os agentes amigos como autor, é da confiança de todos os agentes que acreditam que esse agente é de confiança.
Com a cor amarela representamos os items que contêm asserções cuja validade deriva da ocorrência do evento que lhes deu origem.

O *Emissor* tem acesso a um segredo: a **chave**; daí a existência da crença `+.(chave)` nesse agente. Com esse segredo é produzida um item de conhecimento designado por **assinatura** e, adicionalmente, informação que representa a asserção *"o autor (da assinatura) é o Emissor"*.

É o segredo *chave* que identifica o *Emissor*; para o *Verificador* esta é a única informação relevante: o *Verificador* acredita que este agente é o único que conhece esse segredo e daí, nas suas crenças, incluir `+Emissor(chave)`.

O *Verificador* tem confiança em tudo que o agente `TA` emite (daí a crença `+TA()`); por isso tem confiança no item **certificado**. Este item representa a asserção *"o titular (do certificado) chama-se José Silva"* e ainda contém a informação que permite verificar a assinatura.

Esse conhecimento adicional é o item de informação público criptograficamente ligado à `chave` que construiu a assinatura; por isso é também uma chave; designa-se por **chave pública**.

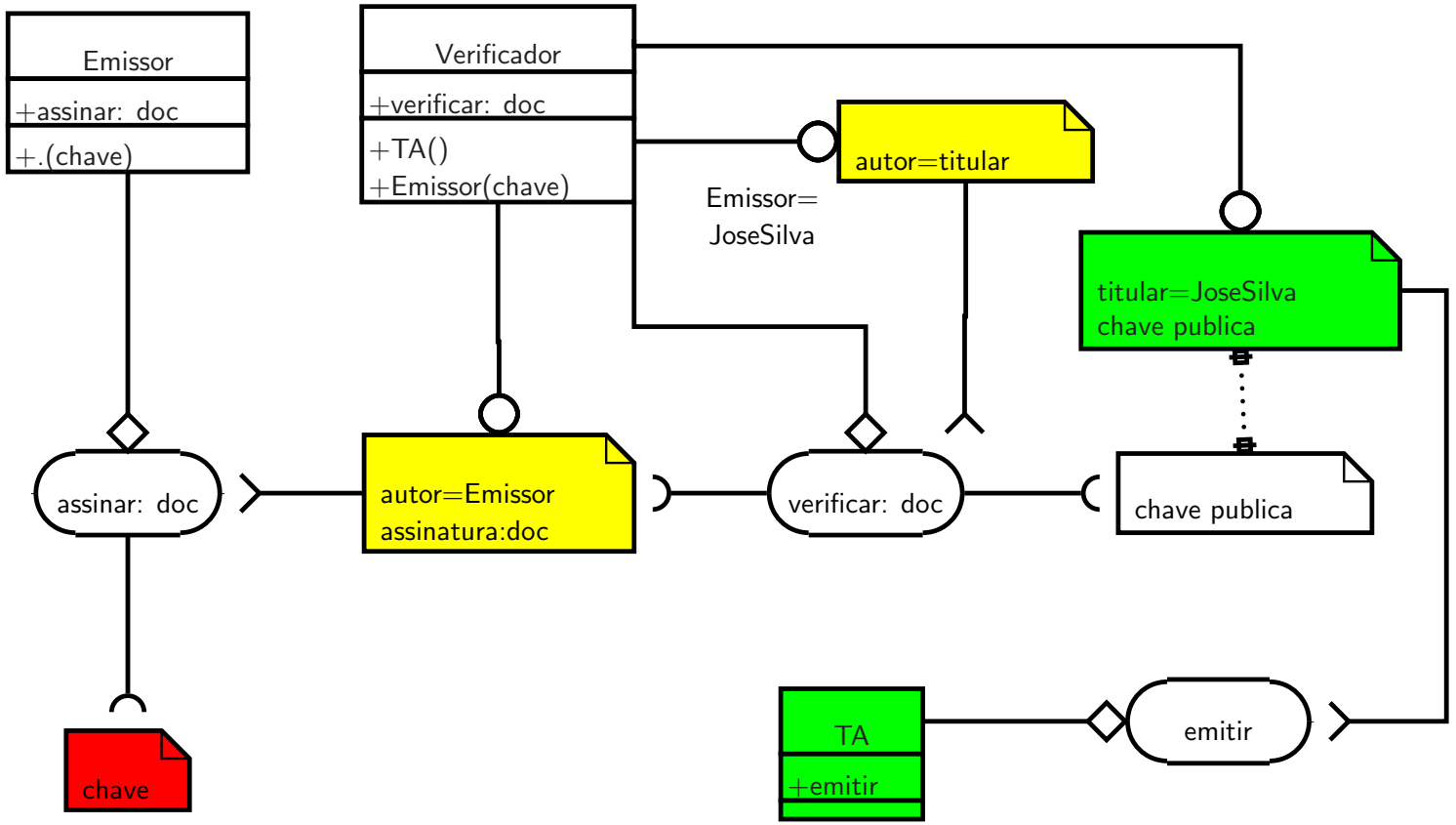
Através do evento de **verificar** é gerado um item de informação final que representa a asserção *"o autor (da assinatura) é o titular (do certificado)"*. O diagrama constitui a **prova** que faz com que o *Verificador* acredite nestes três items de informação; como inferência dedutiva dessas três crenças, ele conclui (e passa a acreditar em) a asserção *"o Emissor chama-se José Silva"*.

Notas

Assinaturas digitais são, em comparação com as cifras, técnicas criptográficas relativamente recentes; isto deriva essencialmente de só recentemente terem sido descobertas as técnicas matemáticas e computacionais que permitem garantir a relação entre a chave e o certificado mantendo público este último e, ao mesmo tempo, garantindo que a chave é um segredo do Emissor.
Estas técnicas constituem deram origem a uma área fundamental da Criptografia chamada **Criptografia de Chave Pública** ("*Public Key Cryptography*" ou PKC, em inglês);

As aplicações de rede usuais ("*browsers*", "*mailers*", etc.) usam implementações de *standards* de criptografia de chave pública; esses *standards* são designados por PKCS# (de "public key cryptography standard"); por exemplo, o PKCS11 é o standard que determina os mecanismos de assinatura digital nestas aplicações, o PKCS7 é o standard para o formato das assinaturas que são incluídas nas mensagens do correio electrónico, o PKCS12 é o formato para transportar chaves de forma segura entre aplicações, etc.

Sem entrar em pormenores convém referir dois nomes de mecanismos de assinatura digital usados frequentemente nas aplicações de rede e na utilização corrente destas técnicas criptográficas.
O **RSA** é o standard de facto de assinaturas digitais para as aplicações correntes de rede: faz parte do PKCS11, é usada em "*chip-cards*" no sistema financeiro e nos mecanismos de autenticação segura mais frequentes.
O **DSA** é o standard oficial de assinatura digital aprovado pelo governo federal nos USA; é usado essencialmente nas aplicações mais exigentes, na diplomacia e, cada vez mais, nas aplicações jurídicas.



INTEGRIDADE

A representação da integridade requer uma qualificação mais detalhada dos actos e dos eventos; é preciso especificar o documento a que estes actos e eventos dizem respeito.

Por isso os actos `assinar` e `verificar` são qualificados com o documento específico a que se referem; os eventos que são instância desses actos são também qualificados com o mesmo documento e os items que daí resultam são igualmente qualificados.

Daqui resulta que o evento `verificar` e o item `assinatura` são ambos qualificados com um documento; o evento só é possível se o qualificador `:doc` for o mesmo em ambos os casos.

Um outro aspecto de notação diz respeito *chave pública*. Não é necessário que a chave pública tenha sido criada com o certificado; basta que o certificado confirme que a chave pública está associado ao titular e que a confiança no certificado pode ser transferida para a chave pública.

No diagrama indicamos essa *transferência de confiança* de um item (o certificado) para outro (a chave pública) com uma nova forma de relação.

Uma terceira componente da noção de *autenticidade* é a capacidade ou incapacidade de **repúdio de autoria** por parte do *Emissor*, de um documento que o *Verificador* afirma autêntico.

Esse repúdio só faz sentido se for feito perante um terceiro agente: o *Juiz*. O *Emissor* sustenta a não-autenticidade do documento enquanto que o *Verificador* sustenta a sua autenticidade. Agora já não se trata de estabelecer uma relação de confiança entre o *Verificador* e o documento mas sim da relação de confiança do *Juiz* perante documentos apresentados pelo *Verificador*.

Duas situações podem ocorrer:

- O *Emissor* é o autor do documento: **repúdio fraudulento da mensagem legítima**.
- O *Emissor* não é autor do documento: **repúdio legítimo de mensagem fraudulenta**.

Põe-se a questão de saber que tecnologia permite ao *Juiz* tomar a decisão correcta.

As assinaturas digitais garantem a impossibilidade do 1º evento: o *Juiz* pode comportar-se como o *Verificador* desde que tenha as mesmas crenças (confiança no `TA` e confiança no facto de que a `chave` usada para assinar a mensagem é segredo exclusivo do `Emissor`).

Identificação Digital

Com a massificação dos sistemas de informação que prestam serviços a um enorme conjunto de utilizadores a noção de **personalidade** na sociedade da informação tornou-se crítica; várias questões se colocam:

- quem são os utentes do serviço; como se identificam; para quê; quais são os seus direitos;. . .
- quem são os agentes decisores do serviço; como se identificam; como podem ser responsabilizados (*accountable*) pelos seus actos; . . .
- quem são os eventuais intrusos[3] ; como se classificam; que perigos colocam;. . .
- . . .

A **identificação digital** é portanto um dos problemas centrais da sociedade de informação e é aquela sobre a qual a opinião pública coloca maiores exigências de segurança.

[3] Não existe qualquer razão que impeça um utente ou um decisor de ser, simultaneamente, um intruso (aliás esta é a situação mais frequente). Do mesmo modo que um utente pode também ser um decisor. A diferença está na partilha dos segredos fundamentais do sistema: normalmente o utente não partilha esses segredos enquanto que o decisor tem acesso aos segredos.

É importante distinguir duas situações:

Identificação digital pura

Neste tipo de situação não existe outra forma de personalidade que não assuma a forma de informação. Um agente só pode ser identificado pelo conhecimento que apenas ele partilha: os seus **segredos**. Mesmo o comportamento do agente é determinado pelos seus segredos. Nesta situação, **personalidade** é equivalente a **conjunto de segredos**.

Identificação electrónica

Quando a **personalidade jurídica** é verificada recorrendo a meios electrónicos. A personalidade aqui é jurídica e tanto pode ser aplicada a pessoas singulares como colectivas.

No caso da **identificação electrónica da pesssoa colectiva** ela é constituída, no mínimo, por dois actos de identificação: a identificação individual do representante e a autenticação de um documento atestando essa representatividade; isso envolve, normalmente, uma identificação do 1^{o} tipo.

Para a **identificação electrónica individual** temos também de distinguir duas situações que produzem consequências radicalmente opostas na abordagem geral ao problema da identificação.

Identificação por atributos

O objectivo do processo de identificação é a garantia de direitos do *Identificador* ou quem ele representa. A segurança identifica-se com a incapacidade pelo *Identificado* de **repúdio da personalidade**.

Identificação por acto de vontade

O objectivo do processo de identificação é a garantia de direitos do *Identificado*: ele prova, perante o identificador, que é titular de direitos.

A segurança reside na garantia que o *Identicado* tem de que nenhum outro agente tem capacidade de reclamar esses direitos; a segurança identifica-se com a incapacidade por qualquer outro agente (incluindo o *Identificador*) da **assunção de personalidade alheia**.

Dado que a personalidade jurídica individual é determinada por um conjuntos de atributos (sociais, físicos ou institucionais) a primeira forma de identificação assume a forma de um **registo** institucional e autenticado desses atributos (num cartão, numa base de dados[4], etc.) e na capacidade do *Identificador* **poder comparar** o registo com atributos reais do *Identificado*.

Neste caso é ónus do *Identificado* provar (ou repudiar) a associação entre a sua personalidade jurídica e os direitos do *Identificador*.

Já a segunda forma de identificação reside na vontade do *Identificado* em provar que é titular de direitos. A forma de identificação implica o reconhecimento, por parte do Identificador, da **autoria de um evento** que demonstre essa manifestação de vontade. Normalmente o evento só pode ser reconhecido através da crença que o *Identificado* é o único detentor de segredos; portanto o processo acaba por se basear também numa identificação do 1º tipo.

Aqui é o *Identificador* (para garantir direitos próprios) que deve estabelecer a associação entre uma determinada personalidade jurídica (a do *Identificado*) e o respectivo conjunto de direitos; essa associação é irrelevante ao *Identificado*.

[4] Note-se as propostas recentes para criação de uma base de dados nacional de informação genética.

Exemplo 30:
Uma variedade muito grande de atributos contribui para a determinação ou caracterização da personalidade jurídica de uma pessoa.

Alguns atributos estão associadas a características geométricas ou biológicas do corpo humano: desde as tradicionais expressão facial e impressão digital, às mais "futuristas" imagens de retina, grupo sanguíneo ou assinatura do ADN; genericamente todos se podem classificar como **atributos biométricos** ou, simplesmente, **físicos**.

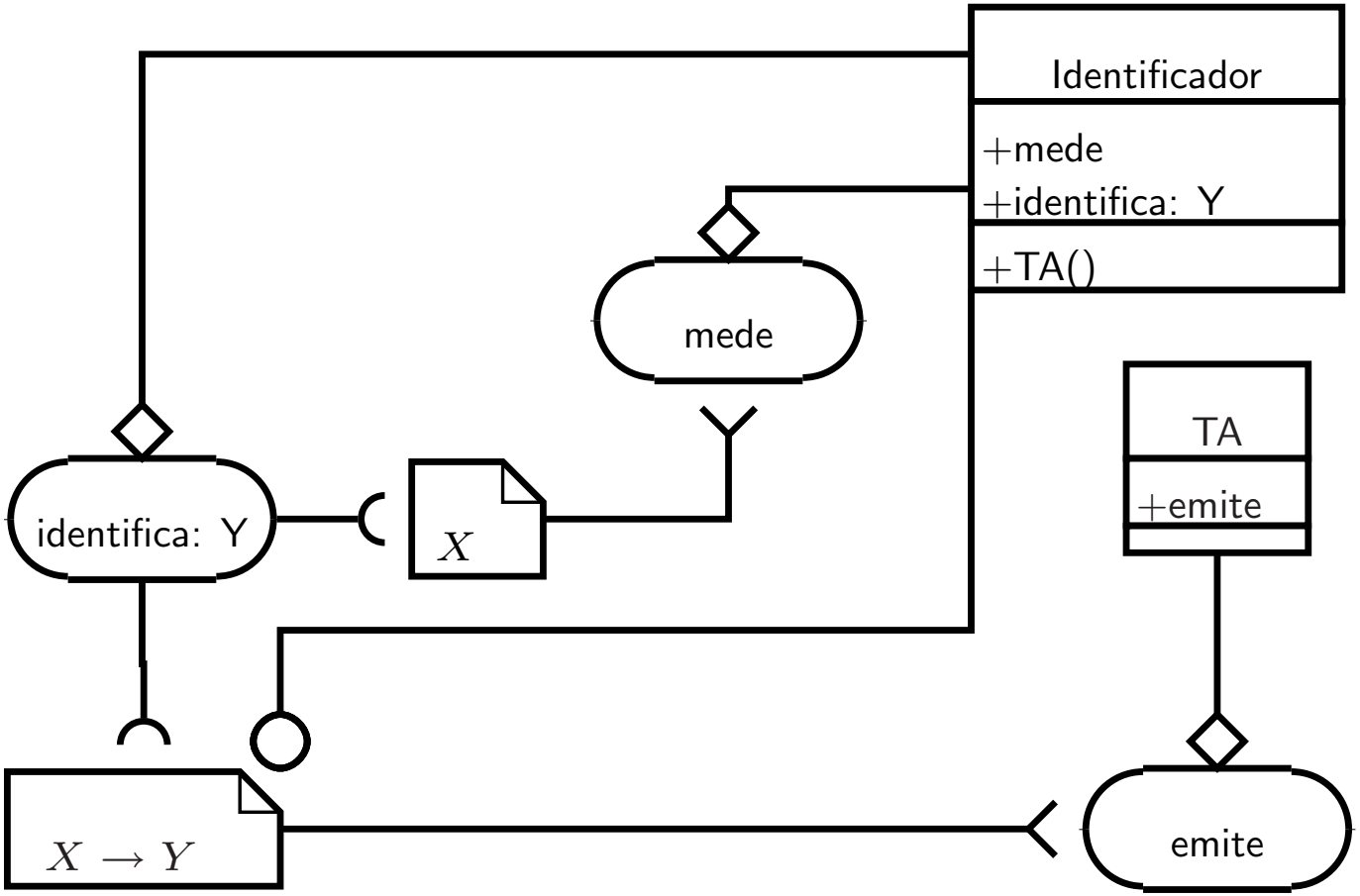
Outros atributos derivam da inserção social da aquisição da personalidade jurídica que, como sabemos, advém do nascimento; nesta categoria surgem **atributos sociais** como o local e a data/hora de nascimento.

Atributos nestas duas primeiras classes podem-se classificar como **atributos naturais** uma vez que os seus valores não dependem de um acto de vontade específico a qualquer agente[5].

Ao invés, temos os **atributos institucionais** cujo valor depende da vontade de terceiros. O mais óbvio destes atributos é o nome da pessoa; porém muitos outros surgem e destes se destacam os vários identificadores que determinam relações jurídicas com vários entidades no estado: número do BI, número do contribuinte, da segurança social, da saúde, etc.

[5] Uma questão interessante, dados os restantes avanços da "tecnologia da procriação", será a de saber se a identificação dos "pais" pode ser considerado um atributo natural.

Identificação por Atributos



O diagrama anterior representa as relações de confiança que caracterizam uma identificação por atributos. Nele estão representados os dois únicos agentes envolvidos nestas relações: o *Identificador* e um "agente amigo" `TA`[6]. Este último autentica um registo (através de um evento `emite`) onde se estabelece uma **associação** entre dois atributos:

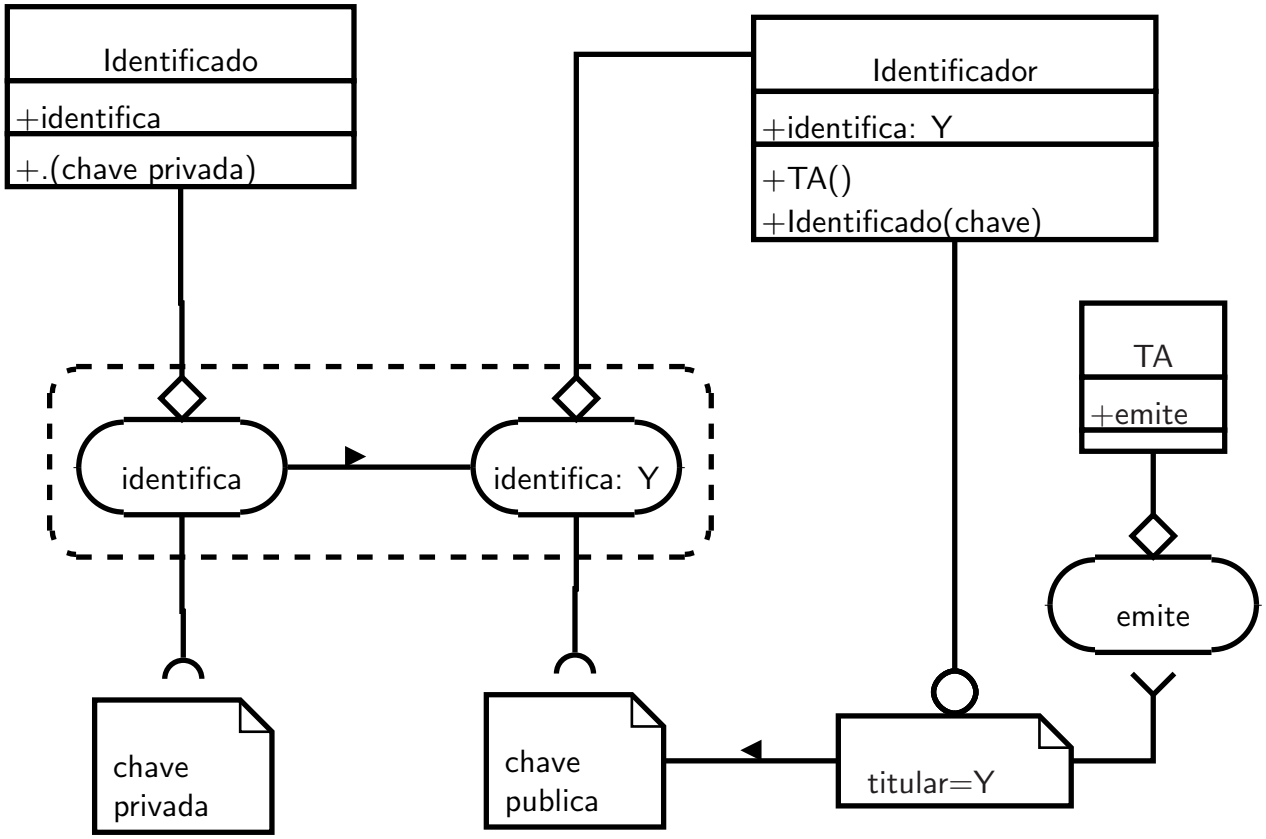
- Um atributo (no diagrama representado por Y) que determina a personalidade; exemplos, o nome, o número do BI ou do passaporte, etc.
- Um atributo (no diagrama representado por X) que pode ser medido pelo agente *Identificador*; exemplos, a feições (registadas em fotografia), as impressões digitais, etc.

As crenças do *Identificador* assentam exclusivamente no `TA`; os seus actos representam a capacidade de medir o atributo X e identificar um agente qualificado pelo atributo Y.

Assim o *Identificador* tem confiança no registo que estabelece a relação $X \rightarrow Y$ interpretada como "X é suficiente para determinar Y". O evento `identifica: Y` necessita de ter confiança não só neste registo mas também na medição do valor X. A possibilidade do evento `identifica: Y` é a prova pretendida.

[6] Note-se que o agente *Identificado* não é relevante para este diagrama de confiança pois não se lhe reconhece nem actos nem crenças.

Identificação por Acto de Vontade



Nesta situação o agente *Identificado* intervém activamente; ele detém um segredo (a `chave privada`) e está habilitado a um acto (`identifica`) que o permite participar num evento de identificação. O *Identificador*, para além de ter confiança no `TA` e nos certificados de chave pública que ele emite, acredita que o *Identificado* é o único agente que controla o item `chave`.

Neste diagrama temos pela primeira vez um evento que é ocorrência conjunta de dois actos, um de cada uma destes agentes[7].

Este evento necessita de confiança em dois items (a chave privada e a chave pública) e essa confiança é resultado nas crenças que os dois agentes têm nessas chaves; assim o evento tem duas "facetas" consoante é visto pelo agente *Identificado* (como ocorrência de um dos seus actos) ou pelo agente *Identificador*. A primeita faceta *controla* a segunda porque é ela que se baseia na confiança da chave privada: por isso o *Identificador* necessita da crença `Identicado(chave)`.

Outra forma de controlo é a que se estabelece entre o certificado (que identifica o titular) e a chave pública; esta é parte integrante do certificado e está, por ele, associada ao titular.

[7] Na linguagem da Teoria dos Sistemas diz-se que o evento resulta do **sincronismo** de ocorrências dos dois actos.

Tecnologia de Identificação por Atributos

A tecnologia para a identificação por atributos é essencialmente simples: a componente principal é o **registo autenticado** da associação entre o atributo (ou atributos) que podem ser medidos pelo agente identificador e os atributos institucionais que determinam a personalidade jurídica.

O registo pode ter um suporte físico num cartão convencional ou, na sua forma electrónica, num qualquer dispositivo apropriado (um *chip-card*, por exemplo). Pode também ser uma simples base de dados institucional.

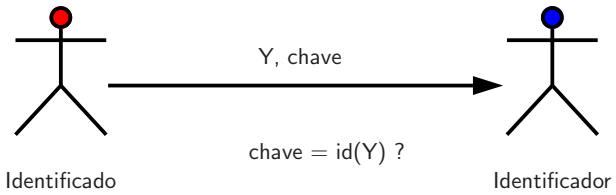
Existe depois tecnologia periférica como a usada na medição dos atributos e nas garantias de autenticidade do registo.

Aqui não se coloca a questão da **posse** do registo pelo identificado; quer o registo seja um cartão que o identificado transporta quer assuma a forma de uma base de dados centralizada, o registo pertence sempre à instituição que o emite ou controla.

Tecologia para Identificação por Acto de Vontade

A tecnologia usada tem de garantir o sincronismo de duas ocorrências de actos transformando-as num evento único de identificação.

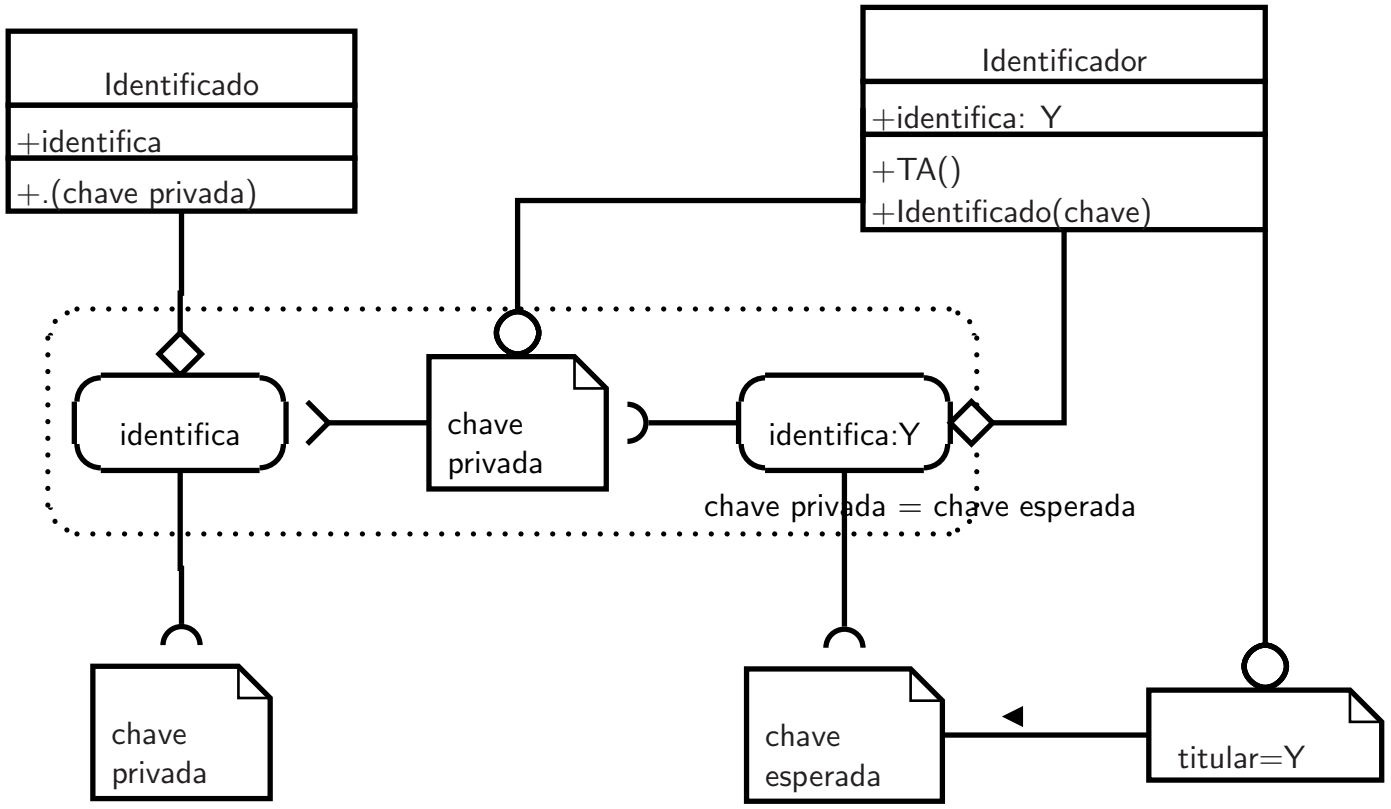
A forma mais comum da ocorrência de um acto de vontade é a **revelação controlada de um segredo** que assume a forma do chamado protocolo **login-password**.



- O *Identificado* envia ao *Identificador* um item que determina a sua personalidade perante este (o **login**) e um segredo (**password**),
- O *Identificador* tem um registo do segredo identificador de cada agente com que interage (representado na função **id**) e compara o valor esperado de Y com o valor recebido. Aceita a identificação se os dois valores coincidem.

O diagrama seguinte representa as relações de confiança neste caso. O evento `identifica: Y` só é possível quando a chave esperada coincide com a chave privada recebida.

Isto significa que o registo reconhecido pelo identificador contém conhecimento sobre a chave privada, e esse conhecimento deveria ser um segredo do identificado.



Sob o ponto de vista da segurança do identificado, este protocolo tem vários problemas:

(i) Se a comunicação usar um canal público, a chave deixa de ser um segredo do agente identificado: qualquer agente com acesso ao canal pode assumir a sua personalidade.

(ii) Se o *Identificador* for um agente eventualmente hostil ao *Identificado*, pode usar o segredo para assumir a personalidade do *Identificado* perante terceiros.

O uso do protocolo *login-password* só é recomendado quando existe a certeza absoluta que nenhuma destas situações ocorre: quando a comunicação é feita sobre canal confidencial e quando o identificador é um "agente amigo".

Exemplo 31: Quando o agente identificador é virtual e assume a forma de um processador pessoal (*chipcard*, tele-móvel, agenda electrónica, etc.) então a comunicação entre o dispositivo e quem tem a sua posse legitima pode ser vista como uma situação ideal para o uso do protocolo *login-password*: a comunicação faz-se por um canal razoavelmente confidencial (por teclado, por reconhecimento de voz,. . .) e o identificador é um agente não hostil.

Mesmo neste caso é possível violar estas condições de segurança; por exemplo a radiação electromagnética do teclado de um tele-móvel pode ser detectada à distância. Mesmo o tele-móvel pode ter um "cavalo de Troia" instalado que faça, por iniciativa própria, uma chamada enviando segredos para um destino pré-estabelecido.

A alternativa ao mecanismo *login-password* é um **protocolo desafio-resposta**.

O identificado envia uma **intensão** de identificação; o identificador responde com um **desafio** aleatório e o identificado gera uma **resposta** apropriada ao desafio que é verificada pelo identificador.

Todos estes três items são públicos e não revelam qualquer informação privada de nenhum dos agentes; a resposta correcta só pode ser determinada conhecendo a chave privada; a verificação exige o conhecimento da chave pública.

Como a informação que passa pelo canal não revela quaisquer segredos, um agente com acesso ao canal não obtém informação que o permita assumir a identidade do identificado. Como o identificador só tem acesso à chave pública e nunca conhece a chave privada também não pode assumir a identidade do identificado.

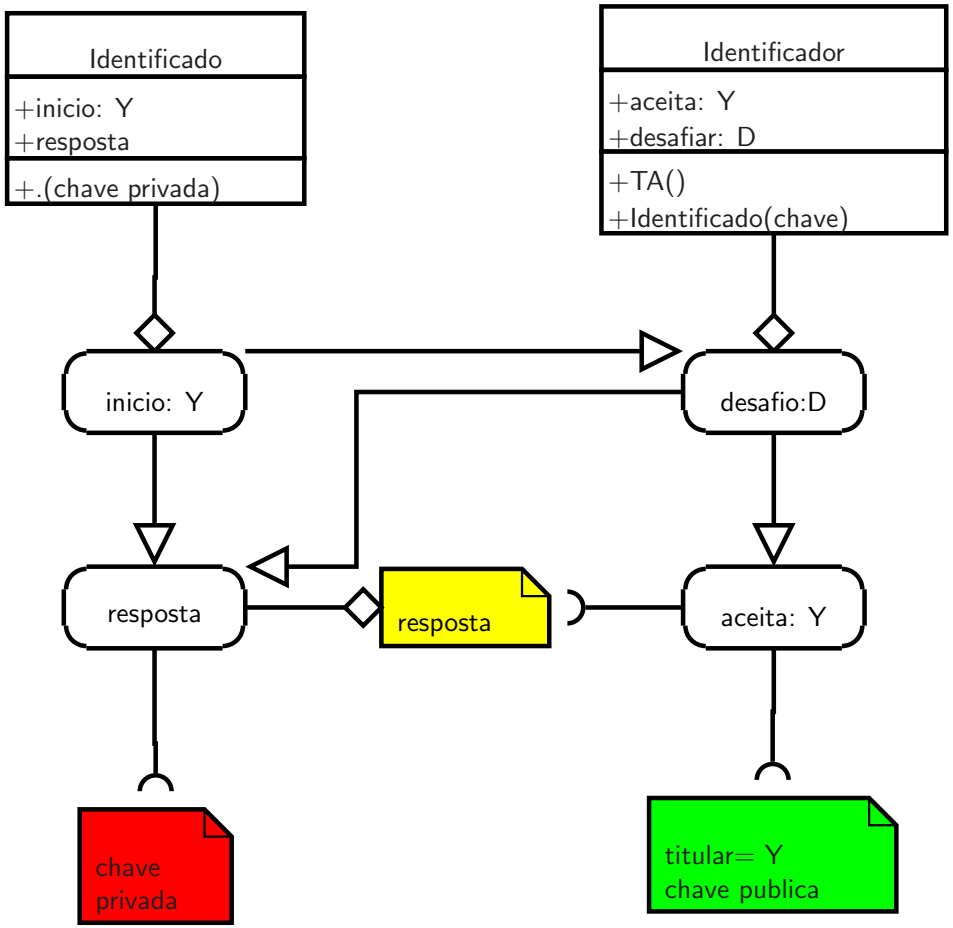
Portanto este sistema é robusto não só em relação ao uso de canais públicos como em relação à existência de identificadores hostis.

O seguinte diagrama representa as relações de confiança e precedência no protocolo desafio-resposta. Por simplicidade não representamos explicitamente o agente TA (que emite os certificados) e os seus eventos e relações.

Os eventos **identifica** no diagrama da página **??**, aparecem aqui decompostos em dois eventos para cada agente; **inicio** e **resposta** do lado do *Identificado* e **desafio** e **aceita** do lado do *Identificador*.

O ponto essencial deste diagrama é a representação da relação de precedência entre os eventos, representada pela seta $-\triangleright$. O fluxo de informação do protocolo é consequência dessa precedência:

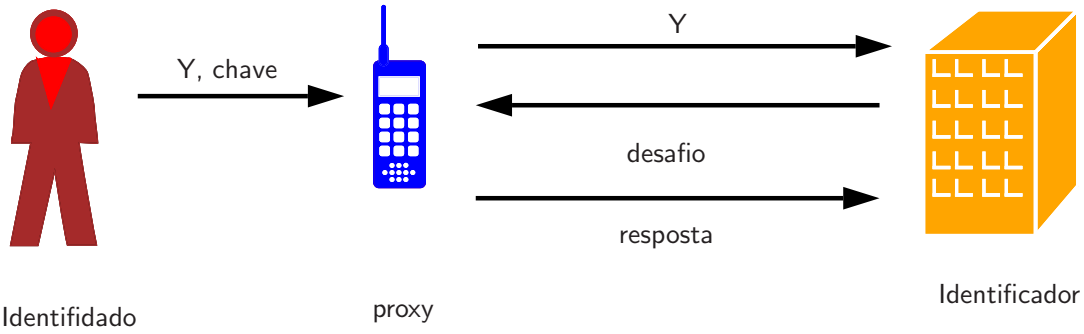
- o evento **inico:Y** precede **desafio:D** que, por seu lado, precede **resposta**.
- o *Identificador* confia na resposta porque é um item que depende do conhecimento da chave privada que este agente crê ser segredo do *Idenificado*.
- o evento **resposta** precede **aceita:Y** porque cria a informação que este último necessita acreditar.


Identificado
+inicio: Y
+resposta
+.(chave privada)
Identificador
+aceita: Y
+desafiar: D
+TA()
+Identificado(chave)
inicio: Y
desafio:D
resposta
resposta
aceita: Y
chave
privada
titular= Y
chave publica

Dado que um protocolo desafio-resposta é computacionalmente mais complexo que o *login-passowrd* é usual que ele seja realizado por agentes virtuais sob controlo do identificado e do identificador.

Isto implica um processo de identificação em duas fases envolvendo um dispositivo que age em nome do identificado[8].

Numa primeira fase o identificado usa um mecanismo simples *login-password* para de identificar perante o seu representante (que aqui age como identificador). Na segunda fase o representante age como agente identificado num protocolo desafio-resposta perante o identificador original.



[8] Normalmente designado como **representante** ou **proxy** do identificado.

A forma mais comum de um *proxy* de identificação é um cartão *chip-card* com capacidade criptográfica.

Um tal cartão precisa apenas:

1. Para implementar o protocolo desafio-resposta, funcionando como agente identificado, necessita de armazenar (de forma segura) a chave privada e ter capacidade computacional para implementar as operações matemáticas necessárias à geração da intensão e ao cálculo da resposta.
2. Para implementar o protocolo *login-password*, em que funciona como identificador, necessita de armazenar a *password* que, uma vez reconhecida, controla a gestão do protocolo anterior.
3. Para proteger ambas as chaves privadas necessita da capacidade computacional para implementar um sistema de cifra eficiente.

É importante referir que, para além destes items de informação que estão só ligados às operações criptográficas, mais nenhuma informação é necessária. Nomeadamente não são necessários nenhuns atributos pessoais.

Funções e Códigos de Hash

As **funções de hash** são técnicas simples e eficientes que complementam outras técnicas criptopgraficas mais complexas (nomeadamente as assinaturas digitais); destinam-se a gerar "impressões digitais" de um um texto, uma imagem ou qualquer outro item de informação.

A partir desse texto é construído um pequeno código (chamado **código de hash** ou **impressão digital**) tendo em vista vários objectivos:

1. O código é **muito menor** que o texto inicial: o código de "hash" tem sempre um tamanho fixo (16 ou 20 bytes) enquanto que o texto não tem limites no tamanho.
2. O código **representa inequivocamente** o texto, no sentido em que qualquer alteração no texto (por muito pequena que seja) reflecte-se numa alteração do código.
3. O código **autentica** o texto no seguinte sentido: conhecido o código e sendo o texto desconhecido não é possível gerar um texto que tenha esse código; se por acaso o texto for também conhecido não é possível construir um segundo texto, diferente do primeiro, que tenha o mesmo código; finalmente nunca é possível construir dois textos diferentes que tenham o mesmo código.

Funções e códigos de *hash* são usados intensamente com outras técnicas; por exemplo, as assinaturas digitais nunca usam directamente o documento que pretendem assinar mas sim um *hash* desse documento. Dada a simplicidade das técnias de *hash* as suas aplicações são inúmeras e, quase sempre, estão na linha da frente de qualquer sistema de informação seguro.

É frequente, quando se publica um documento, dar garantias da sua integridade publicando também (e de forma autenticada) um código *hash* do mesmo documento. Quem tiver acesso ao documento pode usar um programa informático apropriado (disponível na Web) para calcular o código do documento e comparar o valor calculado com o valor publicado.

É também frequente "misturar" o documento com uma chave privada antes de calcular o *hash* publicado; para poder verificar a integridade o utilizador precisa efectuar as mesmas operações e, para isso, precisa de conhecer a chave privada. Um código gerado desta forma designa-se por **MAC** (abreviatura de *Message Authentication Code*).

Esta técnica é usada para autenticar cada um dos blocos de informação ("mensagens") que são trocados quando se faz o acesso a um *site* seguro e para autenticar os endereços *ethernet* das máquinas que estão autorizadas a aceder a um determinado serviço de rede.

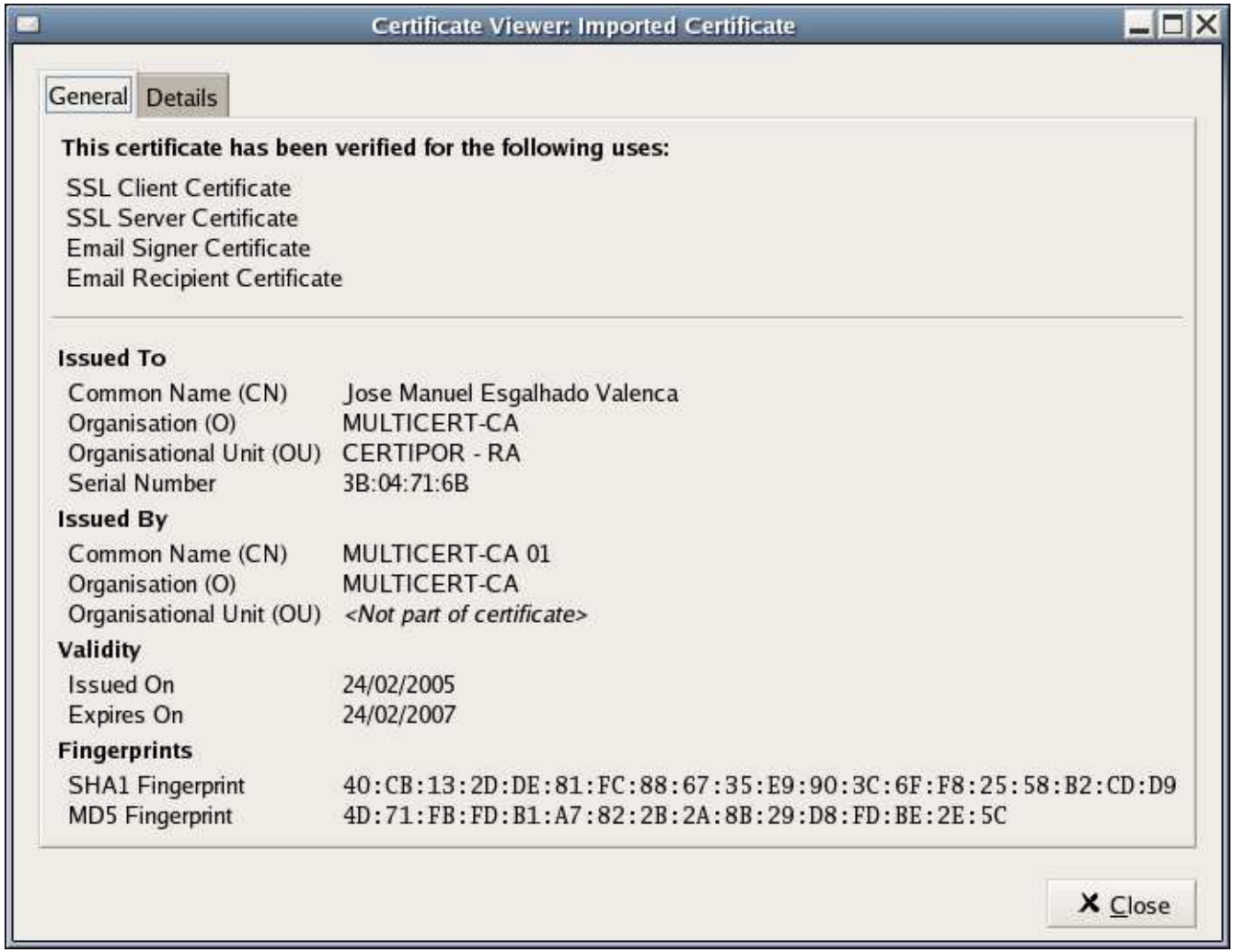
Correntemente as aplicações de rede usuais usam duas funções de "hash": o **MD5** (códigos de 16 bytes) e o **SHA-1** (códigos de 20 bytes).

Na figura da página **??** apresenta-se um certificado de chave pública usado numa aplicação de correio electrónico; uma das componente desse certificados são os dois códigos de *hash* em MD5 e SHA-1. Um utilizador autentica o certificado calculando os seus códigos de *hash* (usando programas informáticos publicamente disponíveis) e comparando os valores obtidos com os valores que constam do certificado.

Nota

Os 16 bytes do código MD5 e os 20 bytes do código SHA-1 aparecem representados numa notação designada por **representação hexadecimal**. Recordemos que **byte** é uma unidade de informação que corresponde a 8 **bits**.
A representação hexadecimal escreve cada byte usando dois dígitos em que cada um representa um número compreendido entre 0 e 15; os digitos usados são os usuais algarismos `0..9` e ainda as letras `A..F` que denotam os números $10..15$.
Por exemplo, o byte escrito como `7C` contém nos 4 primeiros bits o número 7 (correspondente à representação 0111) e nos últimos 4 bits o número 12 (correspondente à representação 1100); assim, é formado pela sequência 01111100.

Neste exemplo é evidente a forma como os códigos de *hash* preservam a confidencialidade sobre o documento; conhecido o código mas não conhecido o documento é possível verificar a sua autenticidade sem ter acesso ao conteúdo.


Certificate Viewer: Imported Certificate
General
Details
This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate
Email Signer Certificate
Email Recipient Certificate
Issued To
Common Name (CN) Jose Manuel Esgalhado Valenca
Organisation (O) MULTICERT-CA
Organisational Unit (OU) CERTIPOR - RA
Serial Number 3B:04:71:6B
Issued By
Common Name (CN) MULTICERT-CA 01
Organisation (O) MULTICERT-CA
Organisational Unit (OU) <Not part of certificate>
Validity
Issued On 24/02/2005
Expires On 24/02/2007
Fingerprints
SHA1 Fingerprint 40:CB:13:2D:DE:81:FC:88:67:35:E9:90:3C:6F:F8:25:58:B2:CD:D9
MD5 Fingerprint 4D:71:FB:FD:B1:A7:82:2B:2A:8B:29:D8:FD:BE:2E:5C
Close

Certificados de Chave Pública

Vimos, nas situações que envolviam cifras, assinaturas ou protocolos de identificação, como os certificados de chave pública (CCP) desempenhavam um papel fundamental nas provas de confiança que daí advinham: os certificados são o veículo essencial através do qual se transfere confiança de uma "fonte de confiança" (o agente **TA**) para a prova.

Essencialmente um CCP é um **registo autenticado** da associação entre um **titular** e uma **chave pública**. A ideia é simples mas a concretização é bastante complexa; tomando como referência o espécimen apresentado na página **??**, temos

titular (na terminologia PKI, o *"subject"*)
: O titular é determinado por um nome inequívoco (a terminologia PKI chama a estes nomes *"distinguishing name"* – ou DN) que e é formado por várias componentes: no mínimo é obrigatório um *"common name"* (CN) mas podem existir outras componentes como *"organisation"* ou *"organisational unit"* ou ainda *"e-mail address"*.

emissor (na terminologia PKI, o *"issuer"*)
: Quem emite o certificado igualmente identificado por um *DN*.

chave pública (não visível nesta imagem)

É o objecto do certificado e aparece, normalmente, representada como um grande número (¿ 128 bytes) representado em notação hexadecimal.

apólice (*policy*, na terminologia PKI)

As condições de utilização do certificado e o seu prazo de validade.

autenticação (não visível na imagem)

A informação que permite verificar publicamente que o certificado é integro, que o seu autor é o emissor e que ele não pode repudiar essa autoria; consiste nos já referidos códigos de *hash* e na assinatura digital, pelo emissor, do certificado.

Um CCP é um documento electrónico que tem analogias com uma apólice de seguros. Nomeadamente existe **responsabilidade civil** inerente à emissão de um certificado: **o emissor responde por danos causados por eventuais falsas declarações que nele constem**.

Nomeadamente, se a chave pública no certificado for falsa (não corresponder à chave pública correcta do titular), então quem tenha acesso à chave privada correspondente pode assumir a personalidade do titular e provocar-lhe imensos danos.

Por isso,

- o emissor tem necessidade de limitar a sua responsabilidade civil através dos limites que impõe ao uso do certificado; daí a componente *"policy"*,
- o verificador tem necessidade de garantir o não-repúdio do certificado pelo emissor; daí a necessidadede técnicas de autenticação, como os códigos de *hash* e a assinatura digital.
- o verificado, na eventualidade de ser lesado pelo uso de um certificado, tem de ter garantias que o emissor tem capacidade de reparar os danos[9]; daí o facto de o emissor ter de ser, ele próprio, certificado e a actividade de emissão de certificados ser devidamente regulamentada.

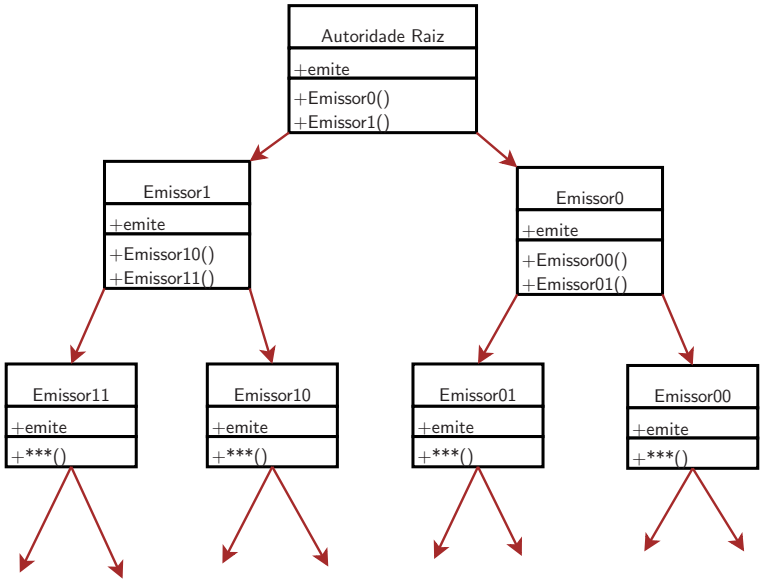
O facto de a autenticidade do certificado assentar (essencialmente) na assinatura digital produzida pelo emissor, exige um processo de verificação que depende da autenticidade da chave pública do próprio emissor; isto significa que tem de existir também um certificado que assegura a titularidade dessa chave pública.

Esse segundo certificado tem também um emissor e uma assinatura digital produzida por esse

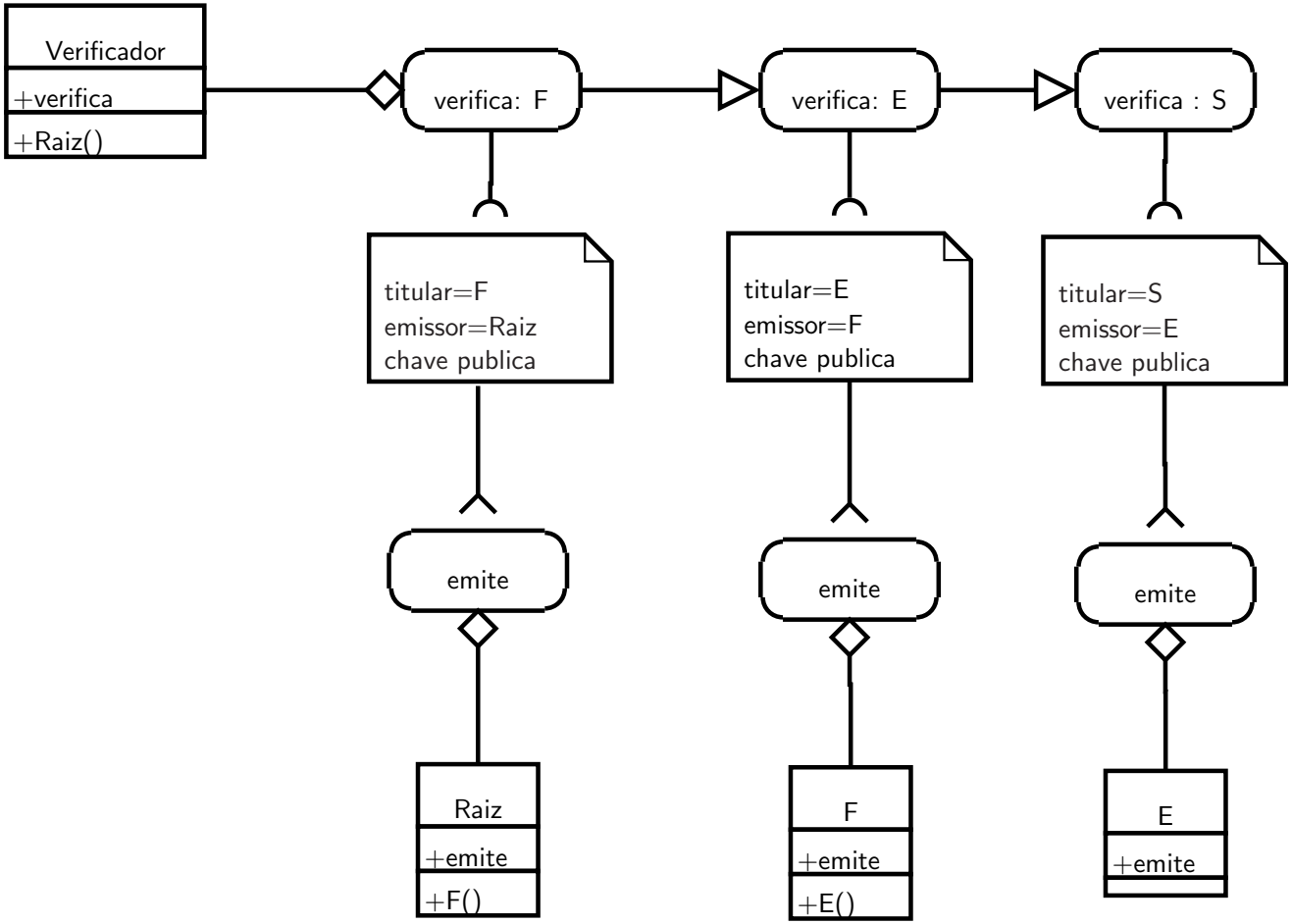
[9] A legislação portuguesa exige que uma entidade, para poder emitir certificados, tem de depositar uma garantia bancária de não menos de 250 000€.

emissor e que deve ser verificada. Essa verificação exige um novo certificado e o processo repete-se.

Desta forma os diversos emissores agrupam-se numa hierarquia em que os emissores numa posição mais elevada vão certificando as chaves públicas dos certificados mais abaixo. Os certificados no topo da hierarquia chamam-se **certificados raiz** e não são autenticados por nenhuma outra autoridade que não os próprios.
A confiança nesses emissores raiz têm de advir de outros mecanismos. Nomeadamente das entidades reguladoras, do enquadramento jurídico e do facto de serem de tal forma públicos que qualquer fraude é facilmente detectada.



A sequência de certificados desde a raiz até ao que está a ser verificado chama-se **cadeia de confiança**. O diagrama seguinte ilustra uma cadeia com 3 certificados e os eventos inerentes.


Verificador
+verifica
+Raiz()
verifica: F
verifica: E
verifica : S
titular=F
emissor=Raiz
chave publica
titular=E
emissor=F
chave publica
titular=S
emissor=E
chave publica
emite
emite
emite
Raiz
+emite
+F()
F
+emite
+E()
E
+emite

Assinatura Digital Cega

Frequentemente, em aplicações de voto electrónico (*eVote*) ou dinheiro electrónico (*eChash*), é necessário assinar um documento desconhecendo tanto o seu conteúdo como o seu autor. Este tipo de assinaturas digitais chamam-se **assinaturas cegas** e a sua utilização típica é:

- O autor **A** gera uma mensagem **m** e esconde-a (usando um sistema apropriado de cifra) num criptograma **m'**; em seguida apresenta este criptograma a um signatário **S**.
- O signatário calcula uma assinatura digital **s'** para este criptograma e continua numa de duas formas possíveis:
  - ▷ **S** devolve **s'** a **A** e, a partir deste valor, o agente **A** é capaz de calcular a assinatura **s** para a mensagem original **m**.
  - ▷ **S** entrega **s'** a um agente verificador **V** que tem informação suficiente para recuperar **m** e **s** deste item.
- Em qualquer das continuações quem conhecer **s** e **m** pode verificar que a primeira é a assinatura correcta de **S** para **m** mas não consegue (a menos que **A** o queira) identificar o autor.

Exemplo 32:
Num sistema de votação electrónica o **Votante**, depois de se autenticar perante a **Mesa**, apresenta o seu voto cifrado de modo que a mesa não tenha possibilidade de conhecer o seu conteúdo.

A mesa produz uma assinatura cega sobre o voto cifrado e entrega o resultado ao **Escrutinador**. Este é capaz de recuperar o voto original e a assinatura da mesa sobre esse voto. Assim pode verificar que este voto é produzido por um votante autenticado pela mesa mas não tem possibilidade de saber quem é esse votante.

Exemplo 33: O objectivo é a emissão de pagamentos electrónicos anónimos (normalmente designados por *eCash*); uma versão insegura de um protocolo de *eChash* seria:

O **Cliente** emite 100 pedidos de 100 euros cada um equipado com um número de série aleatório cifra-os e entrega-os ao **Banco**. O **Banco** escolhe um pedido aleatório e ordena ao **Cliente** que abre todos os restantes e mostre que todos têm o mesmo valor. Sobre o pedido restante o banco produz uma assinatura cega e retira o valor de 100 euros da conta do cliente.

Dessa assinatura o cliente extrai o pedido assinado que funciona como dinheiro que pode ser entregue a um outro agente **X** (como forma de pagamento, por exemplo). **X** verifica a assinatura do banco sobre o pedido e aceita o pagamento; **X** entrega o pedido assinado ao banco que verifica a sua própria assinatura, verifica a unicidade do número de série e credita a conta de **X**. No final o banco não conhece a proveniência do dinheiro.

Estampilhas Temporais

Frequentemente necessário obter uma prova documental de que determinado evento ocorreu numa data e numa hora específica. Tipicamente quando se realiza uma comunicação electrónica importante, o emissor pretende obter um recibo (emitido por uma autoridade apropriada) de que a mensagem foi enviada num instante temporal bem determinado.

Exemplo 34:

A submissão de peças processuais a tribunal é um exemplo de comunicação importante onde o emissor pretende ter uma prova de que cumpriu os prazos legais.

As **estampilhas temporais** são uma tal prova; essencialmente são documentos electrónicos análogos a certificados de chave pública que estabelecem uma associação entre a o evento de emissão de um documento (incluindo o seu conteúdo) e um instante de tempo fornecido por uma relógio de alta precisão.

MDDE (*"Marca Do Dia Electrónica"*) é o nome comercial de um serviço de estampilhas temporais disponível em Portugal tendo em vista, principalmente, a comunidade dos juristas.

Essencialmente uma estampilha temporal é um documento electrónico autenticado que contém:

Autoridade
a identificação do emissor da estampilha; tal como nos certificados de chave pública, o emissor responde por danos causados por falsas declarações neste documento,

Documento
o representante do conteúdo do documento, normalmente sob a forma de um ou mais códigos de *hash*, que servem, inclusive, para garantir a sua integridade,

Evento
identificação da mensagem através de meta-informação sobre o documento (identificação, tamanho, identificação de documentos anexos, etc.) e de informação sobre o evento de transporte da informação (via *eMail* ou outro protocolo análogo),

Tempo
a marca temporal gerada por um relógio de alta precisão; normalmente o relógio está sincronizado com relógios de precisão astronómica (relógios atómicos e similares),

Autenticação a assinatura digital do emissor sobre a restante informação, garantindo a sua integridade e o não repúdio,

Esteganografia

A **Esteganografia** define um conjunto de técnicas de segurança que são conceptualmente diferentes das técnicas criptográficas. Enquanto a Criptografia lida com segredos e confiança mas assume que a existência da informação crítica é publicamente conhecida (um atacante pode não conhecer o conteúdo de uma mensagem mas sabe que ela existe) a Esteganografia oculta a própria existência da mensagem.

As técnicas esteganográficas ocultam uma **mensagem útil** m num **disfarce** ("cover" em inglês) C produzindo uma modificação C^* de tal forma que:

- Sem se conhecer o processo de geração de C^* é computacionalmente intratável decidir se este conteúdo resulta de uma alteração de um qualquer disfarce ou se é um conteúdo "limpo" (sem inclusão de mensagens)
- Conhecido o processo de geração de C^* é possível recuperar m e C de C^*

A alteração C^* é obtida de C acrescentando-lhe informação que se costuma designar por **marca de água electrónica**.

Exemplo 35:
Algumas das mais importantes aplicações da esteganografia estão na inclusão de marcas de água electrónica em conteúdos de forma a garantir direitos de autor sobre os mesmos.

É possível acrescentar estas marcas de água em faixas de música gravada, imagens digitalizadas, vídeos, etc. Essas marcas de água não são detectáveis por qualquer utilizador dessa informação (legítimo ou não) mas o autor, ou um seu representante, pode detectar que as marcas existem; principalmente, pode fazer prova de que elas existem e assim processar judicialmente um eventual uso ilegítimo da mesma.

É também possível usar marcas de água para identificar diferentes cópias de um mesmo documento; desta forma se um documento, supostamente confidencial, passa a ser do conhecimento público de forma ilegítima, é possível detectar qual a cópia que foi responsável por essa fuga de informação.

Outro tipo de aplicação (mais tradicional) envolve o uso da esteganografia para ocultar a existência de mensagens. Por exemplo é possível usar imagens para ocultar pequenas mensagens textuais.

Das Situações aos Contextos, aos Sistemas, às Tecnicas e, finalmente, às Aplicações na Sociedade da Informação

Pretendi apresentar algumas ferramentas que podem permitir a um jurista posicionar-se face a uma situação concreta onde as tecnologias da informação interagem com os direitos dos cidadãos; nestas circunstâncias acho que o jurista deve

- começar por analisar e identificar a situação de direito independentemente das TI's,
- identificar claramente o contexto ético inerente à introdução das TI's: que direitos, que interesses legítimos, que racionalidade pública,
- em termos tecnológicos, identificar os agentes, os seus graus de confiança, os actos a que estão habilitados e os eventos mais relevantes,

Com este trabalho prévio o jurista pode, finalmente, ter uma opinião informada sobre a tecnologia apropriada à situação em causa: que técnicas de segurança devem ser usadas e, finalmente, quais as **aplicações informáticas** que suportam essas técnicas.

Correio Electrónico

A submissão de peças processuais por via informática, que resultou das alterações ao Art. 150º do Código do Processo Civil[10], põe em destaque a relevância social e jurídica da noção de "valor probatório dos documentos electrónicos" que o DL 290-D/99 veio trazer ao ordenamento jurídico nacional: pela primeira vez uma actividade social essencial, envolvendo uma comunidade significativa de agentes socialmente determinantes, assenta exclusivamente nas tecnologias da informação e, nomedamente, num tipo de aplicação informática específico: o **correio electrónico**.

A relevância do correio electrónico nos eventos jurídicos levanta imediatamente a questão da confiança que os diversos agentes têm nos documentos assim transmitidos e nas consequências jurídicas desses documentos.

Genericamente (ver pag. **??**) a confiança vai resulta das **crenças** que cada agente tem sobre o comportamento dos restantes agentes do sistema, naturais ou artificiais. Num sistema judicial, assente no correio electrónico, estas crenças colocam-se a vários níveis:

[10] Ver http://www.oa.pt/genericos/detalheArtigo.asp?idc=68&ida=22593.

I Ao nível dos **conteúdos** das mensagens, exige-se garantias quanto à **confidencialidade** e **autenticidade** do conhecimento.

Estas questões já foram, em parte, analisadas neste curso e vimos a relevância de técnicas como as cifras, assinaturas digitais e certificados, para este tipo de garantias.

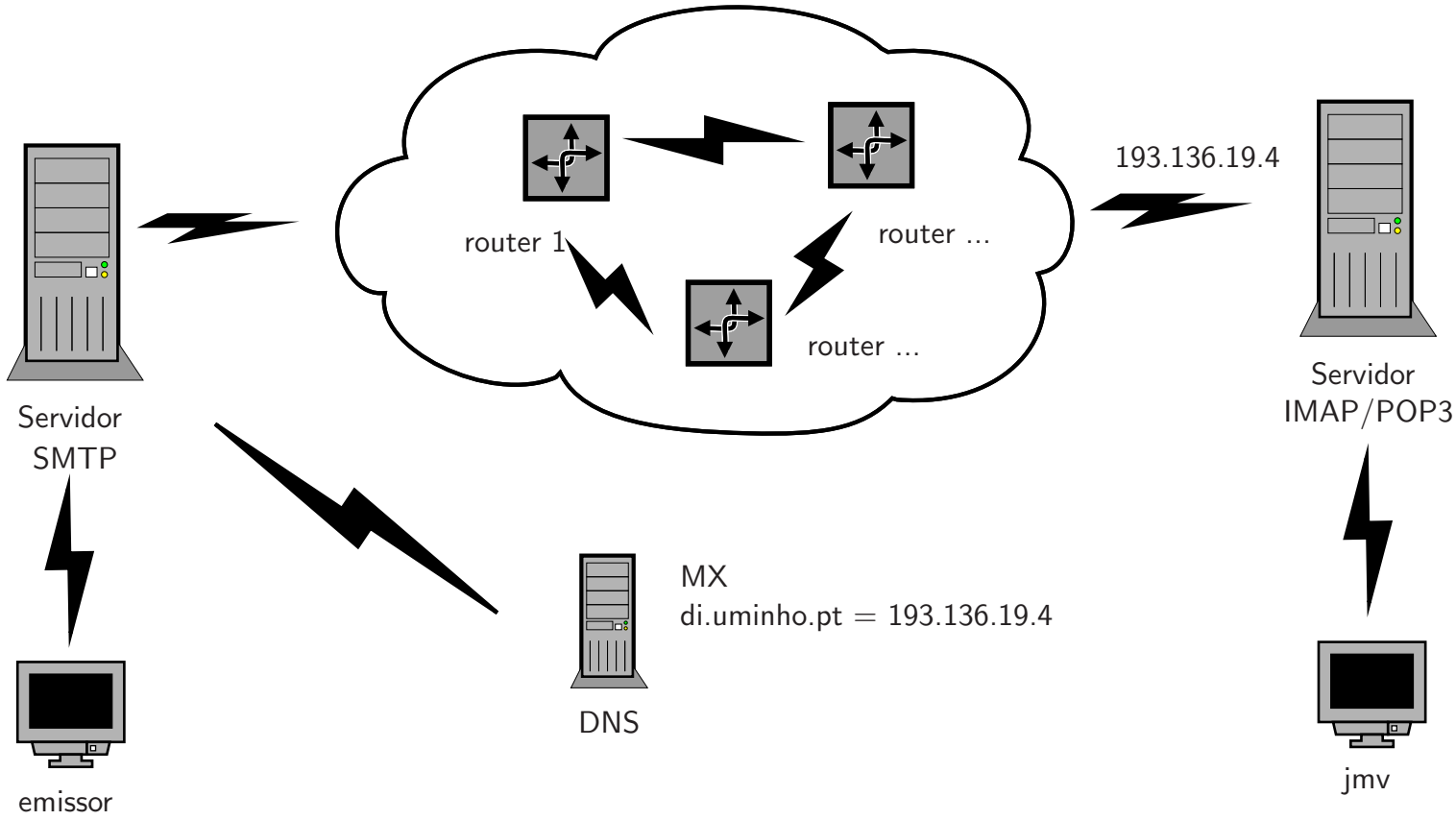
II Ao nível da **eficácia** das mensagens, exige-se garantias quanto à ocorrência do próprio **evento** de comunicação.

Nomeadamente o emissor requer provas de que o evento de comunicação se realizou dentro de um determinado prazo temporal e de que o receptor teve, dentro desse prazo, acesso ao conteúdo legítimo da mensagem. As estampilhas temporais permitem dar algumas destas garantias mas não todas.

III Ao nível da **fiabilidade da infraestrutura informática** que garante a ocorrência do evento de comunicação e a autenticidade desse evento.

Este último tipo de questões de segurança deriva da eventual existência de bloqueios ao próprio serviço de correio electrónico; as garantias aqui colocam-se em relação à **disponibilidade do serviço** que pode ser ameaçada, por exemplo, através de *virus* ou *"worms"* informáticos.

Em termos da infraestrutura informática para o correio electrónico convém ter uma ideia como funciona e quais são as suas principais fragilidades.



Suponhamos que o `emissor` pretende enviar uma mensagem para `jmv@di.uminho.pt`; desencadeia a seguinte sequência de eventos:

1. O `emissor`, depois de preparar a mensagem, entra em contacto com um servidor que vai diligenciar a sua entrega usando um protocolo chamado *Simple Mail Transfer Protocol* (SMTP). Normalmente o servidor exige alguma autenticação e só aceita possíveis clientes devidamente certificados.
2. O servidor SMTP divide o endereço em duas partes: o **nome** (`jmv`) e o **domínio** (`di.uminho.pt`). A segunda parte identifica um conjunto de recursos (máquinas e utilizadores) agrupados debaixo desse nome; nomeadamente esse domínio tem uma ou mais máquinas ("hosts" na terminologia da internet) que têm por missão receber o correio electrónico. No entanto o servidor SMTP não sabe quais são essas máquinas nem sabe como encaminhar as mensagens para as fazer lá chegar.
3. Na *internet* os diferentes hospedeiros são identificados por um número designado *código* IP; a informação sobre qual é a máquina destinada a receber o correio electrónico para um determinado domínio é fornecida por um servidor DNS (*Domain Name Server*). Estas são máquinas que têm um papel crucial na internet já que fornecem a toda a rede informação

de gestão essencial; nomeadamente contêm registos, chamados **MX** (*Mail Exchange*), que associam a cada domínio os hospedeiros de *email*. Neste caso particular, ao domínio `di.uminho.pt` está associado ao hospedeiro `193.136.19.4`.

4. Conhecido o código IP, o servidor SMTP pode tentar descobrir o caminho até esse endereço através da internet; para isso recorre a dispositivos especiais chamados **encaminhadores** (*"routers"*, na terminologia IP) que contêm registos dos melhores caminhos entre dois pontos. Estes registos, chamados **tabelas de encaminhamento**, permite aos diversos encaminhadores transportar a mensagem de rede para rede (daí o nome *inter*net) até ao destino final.
5. Quando a mensagem chega ao servidor de *mail* do domínio `di.uminho.pt` fica a aguardar até que o utilizador de nome `jmv` a vá aí buscar.

   O utilizador usa um de dois protocolos para aceder à mensagem: o POP3 (*"Post Office Protocol, version 3*) ou o IMAP (*"Internet Message Access Protocol"*). O servidor (POP3 ou IMAP) só permite o acesso se o utilizador se autenticar; istode forma a garantir que o correio não é entregue ao destinatário errado.

   Igualmente é prudente que o utilizador se crtifique da autenticidade do servidor dado que a autenticidade da mensagem depende, de certa forma, da confiança que o utilizador deposita na infraestrutura.

Pondo de parte as questões de autenticidade dos conteúdos e dos eventos, e focando apenas as questões de fiabilidade da infraestrutura, são aparentes (mesmo neste modelo simplificado) diversas fragilidades:

(i) Os servidores DNS são uma fragilidade óbvia: em primeiro lugar porque um número excessivo de pedidos pode bloquear o serviço (se existirem várias réplicas de servidores DNS isto pode não ser muito importante).

Em segundo lugar - e isto é crucial - porque os registos MX não são, normalmente, autenticados; isto significa que é possível inserir na rede um *falso* DNS que associe uma máquina hostil em substituição do legítimo servidor de mail do domínio. Esta máquina hostil fica, assim, com capacidade para "sugar" todo o tráfico que se dirija a esse domínio.

(ii) Os *routers* são pontos de ataque onde as consequências são ainda mais devastadoras: se deixarem de operar, fica bloqueado não só o correio electrónico como qualquer outro serviço.

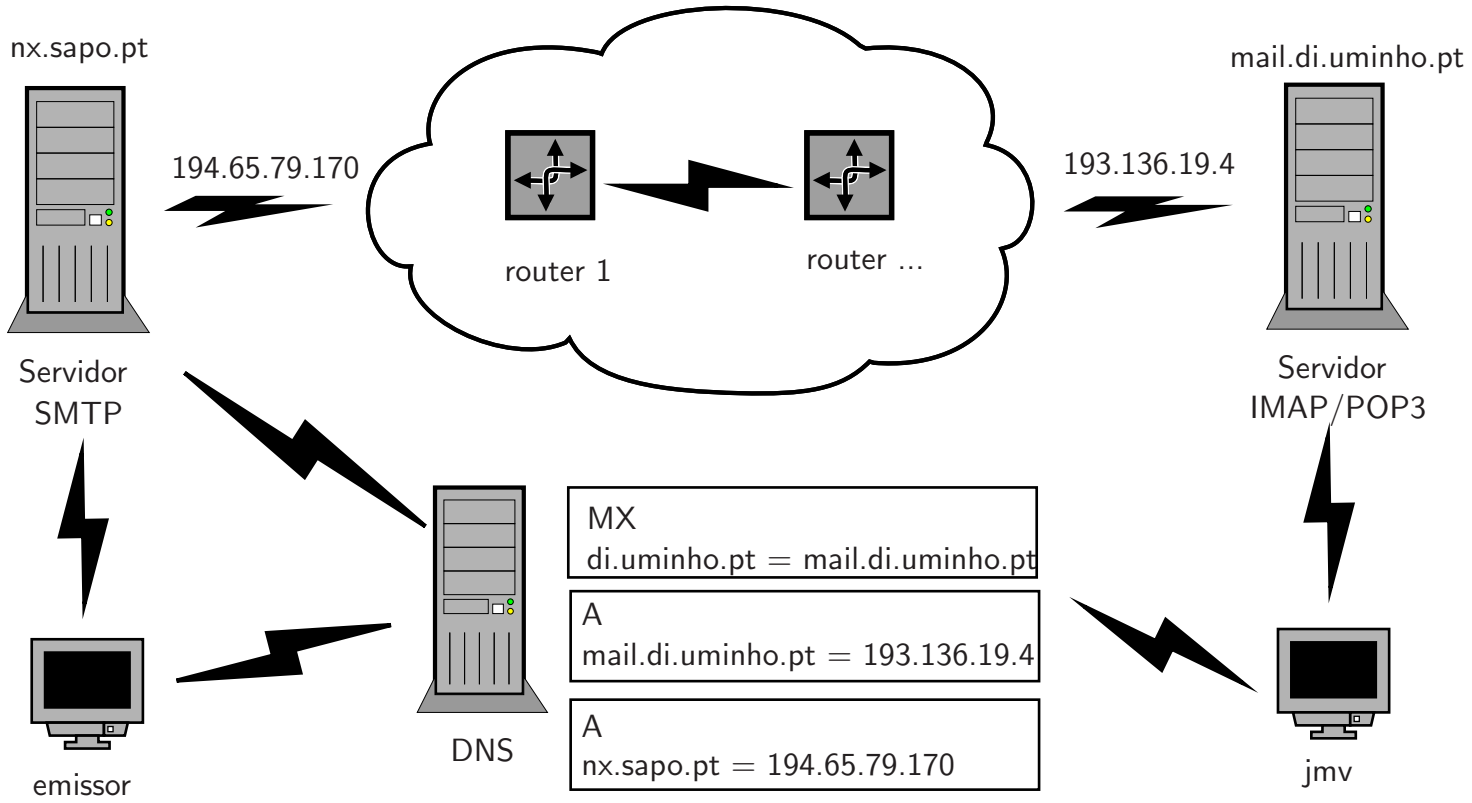
É difícil bloquear um router através de um número excessivo de pedidos já que estas máquinas operam só nas redes a que estão directamente ligados. No entanto as tabelas de encaminhamento sofrem das mesmas fragilidades que os registos MX; um falso router, com uma falsa tabela, pode encaminhar o tráfego para um "beco sem saída".

As fragilidades que resultam da falta de autenticação da informação fornecida pelos *routers* e pelo serviço DNS são ainda mais aparentes se substituirmos o diagrama da página **??** por um modelo mais realista de uma ligação por correio electrónico.

Note-se que o emissor e o utilizador têm de contactar os servidores respectivos (SMTP e IMAP/POP3) através da internet; os dois servidores são identificados por códigos IP e, no entanto, emissor e utilizador apenas conhecem as máquinas através de um nome-endereço construído de forma análoga a um endereço *email*. Neste exemplo `nx.sapo.pt` e `mail.di.uminho.pt` são, respectivamente, os nomes do servidor SMTP e do servidor de *email*.

A conversão destes nomes em códigos IP, que os routers têm capacidade de entender, é feita por uma outra forma de registo gerido pelos servidores DNS. Estes registos, designados por **A** ("address") fornecem a informação IP que permite aos clientes aceder, através da internet, ao servidor respectivo; obviamente que estes registos são, igualmente, pontos de ataque potencial: registos falsos associam nomes legítimos a máquinas falsas que "sugam" o tráfico.

A fiabilidade da infraestrutura depende crucialmente da autenticação da informação de gestão de rede, nomeadamente as tabelas de encaminhamento dos "routers" e os registos DNS.


nx.sapo.pt
194.65.79.170
router 1
router ...
193.136.19.4
mail.di.uminho.pt
Servidor
SMTP
Servidor
IMAP/POP3
MX
di.uminho.pt = mail.di.uminho.pt
A
mail.di.uminho.pt = 193.136.19.4
A
nx.sapo.pt = 194.65.79.170
DNS
emissor
jmv

Passaportes Electrónicos

A abordagem "*identificação por atributos*" está institucionalizada em todas as áreas onde os direitos de uma colectividade (representada pelo agente identificador) prevalecem sobre os direitos do indivíduo identificado.

A situação paradigmática está no controlo das fronteiras: em Dezembro de 2004, o Parlamento Europeu aprovou a regulamentação dos novos passaportes[11] que incluem representação electrónica de dados biométricos. Os novos passaportes devem poder ser lidos electronicamente e devem incluir a representação electrónica de imagens faciais (dentro de 18 meses) e impressões digitais (dentro de 3 anos); imagens da iris ocular poderão ainda ser acrescentadas.

Esta directiva segue essencialmente as normas **ICAO** (*International Civil Aviation Organization*)[12] fortemente inspiradas pelas recomendações dos Departamentos da Justiça e da Segurança Interior dos Estados Unidos [13] para passaportes que sejam legíveis electronicamente.

[11] Ver http://www.euractiv.com/Article?tcmuri=tcm:29-132063-16&type=LinksDossier.

[12] Ver http://www.icao.int/mrtd/biometrics/recommendation.cfm.

[13] Retirado de http://www.dhs.gov/dhspublic/: "May 12, 2005 - The Department of Homeland Security reminds all Visa Waiver

O tipo de dispositivo usado é a de um cartão plástico, inserido no passaporte, onde está embebida uma antena e um *"chip"*; por indução magnética a antena captura energia e o sinal de comunicação entre o *"chip"* e um leitor externo.

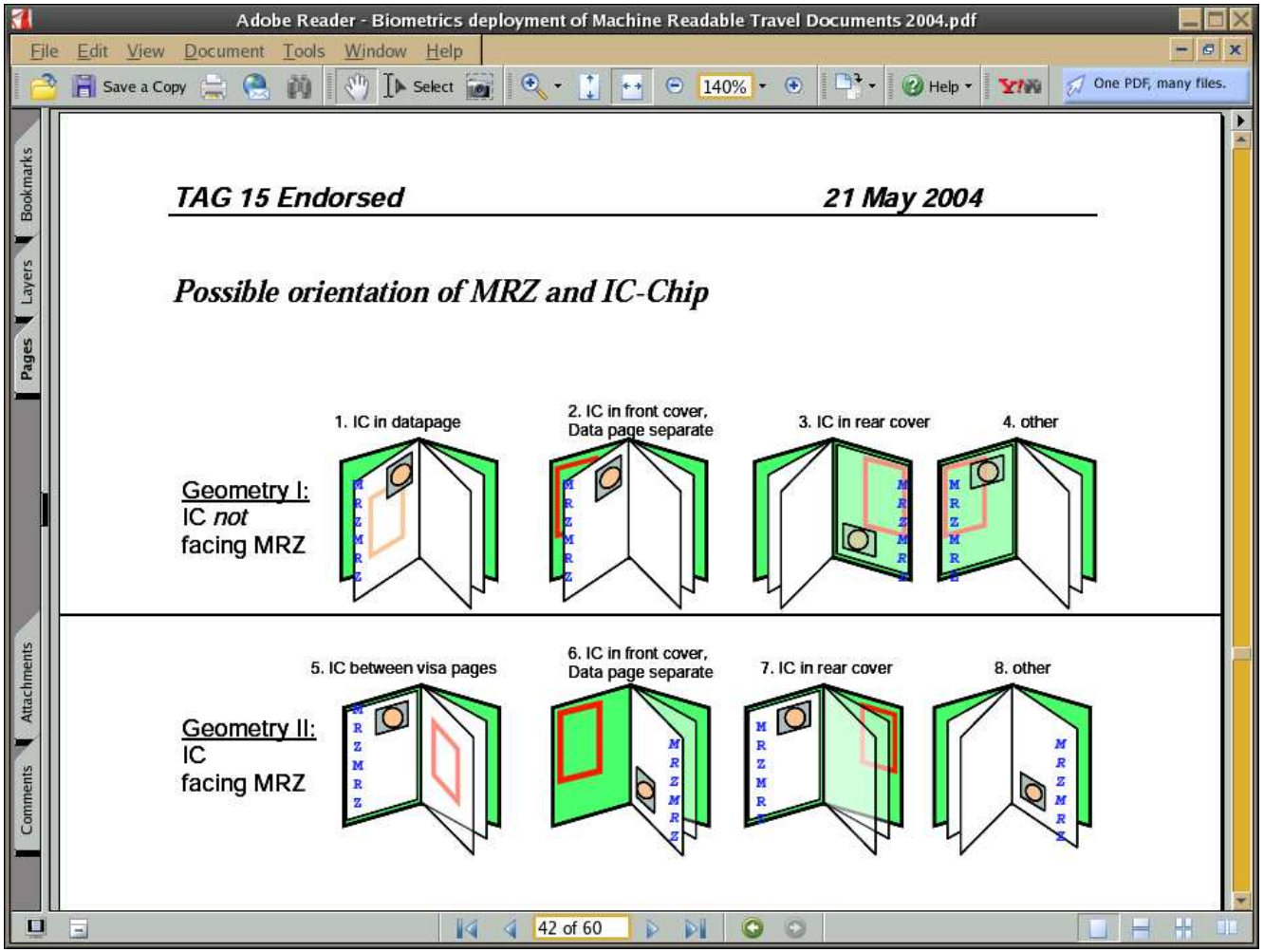
O processo de verificação de identidade envolve a comparação do atributo medido (expressão facial ou impressão digital) com a representação pictórica no passaporte e com a representação electrónica no *"chip"*.

Adicionalmente pressupõe a existência de uma base de dados biométricos e a comparação da informação recolhida no passaporte com essa base de dados.

Essencialmente este tipo de tecnologia tem dois tipos de objectivos:

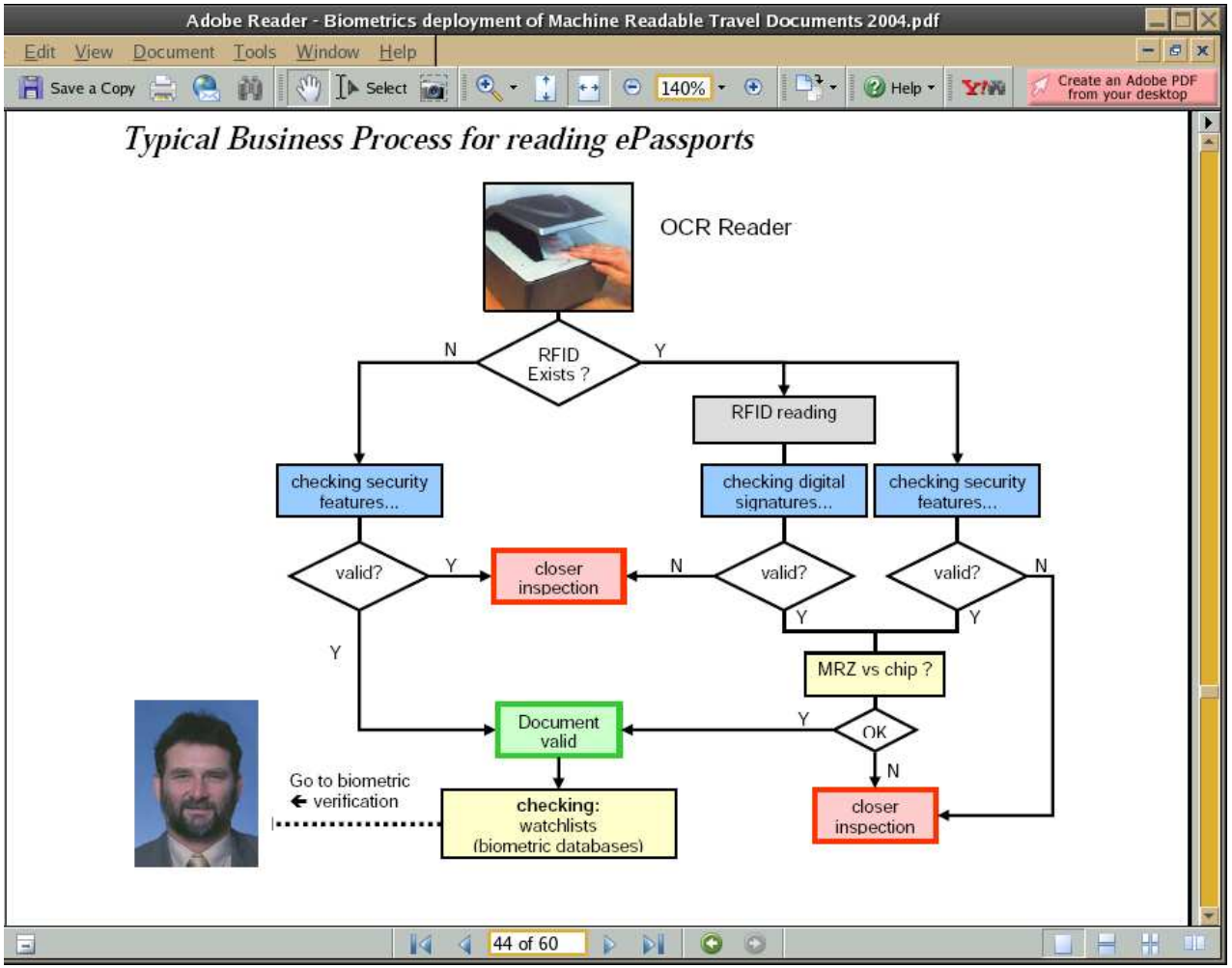
- eficácia no processo de recolha da informação e comparação com a base de dados central
- garantias quanto à autenticidade da informação recolhida, evitando fraudes na emissão dos passaportes

Country travelers that as of June 26, 2005, they must have a machine-readable passport to enter the United States without a visa. Machine-readable passports have a sequence of lines that can be swiped to confirm the passport holder's identity quickly and to obtain other information about the holder typically found on a passpor's inside cover".



14

[14] ICAO TAG MRTD/NTWG - *Biometrics Deployment of Machine Readable Travel Documents*


Adobe Reader - Biometrics deployment of Machine Readable Travel Documents 2004.pdf
Edit View Document Tools Window Help
Save a Copy
Select
140%
Help
Create an Adobe PDF from your desktop
Typical Business Process for reading ePassports
OCR Reader
RFID Exists ?
N
Y
RFID reading
checking security features...
checking digital signatures...
checking security features...
valid?
Y
closer inspection
N
valid?
valid?
N
Y
Y
Y
MRZ vs chip ?
Document valid
Y
OK
N
Go to biometric verification
checking: watchlists (biometric databases)
closer inspection
44 of 60

Bilhete de Identidade Electrónico

A existência de um bilhete de identidade cívica electrónico, numa abordagem "identificação por acto de vontade", presupõe que o cidadão assume, por vontade própria, uma determinada **personalidade digital** que lhe permite provar a titularidade de determinadas **situações de direito**.

Programa do XVII Governo Constitucional

"Criar um cartão único, o Cartão do Cidadão, reunindo as informações de identificação civil, do contribuinte, do utente de saúde, do eleitor e todas as demais que possam ser associadas nos termos constitucionais"

Projecto de Lei 112/IX

"ARTIGO 3º (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.
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.
..."

1º Paradigma

Cartão multifunção agindo como **depósito**[15] de dados pessoais (*"base de dados de bolso"*) que representam electronicamente **atributos** dentro de todos ou alguns dos seguintes grupos:

- **atributos institucionais**, específicos a cada serviço[16], identificadores do utente.
- **atributos naturais** identificadores da personalidade jurídica do cidadão
- **atributos biométricos** identificadores da personalidade física do cidadão

[15] *autenticado ou não, eventualmente com acesso controlado usando cifras apropriadas.*

[16] *um grupo por serviço: Identificação Civil, Finanças, Saúde, Segurança Social.*

. . . abordagem não recomendável, porque é . . .

- **inflexível** já que está orientado de raiz a um conjunto limitado de aplicações e serviços,
- **ambígua** quanto às limitações de responsabilidade associadas a cada um dos sistemas de informação com que interage,
- **insegura** uma vez que cria a possibilidade de violações à privacidade do cidadão através do cruzamento não controlado de dados dos vários sistemas,
- **ineficaz** já que recorre a soluções tecnológicas específicas com maiores custos e tempos de desenvolvimento mais longos.

. . . mas, principalmente, porque . . .

contraria as recomendações que estão a surgir de vários organismos ligados ou patrocinados pela CE que têm, por objectivo, a normalização e compatibilização dos vários sistemas de identificação electrónica na Europa

Setting an agenda for the future:

. . .

· *Coordination work is needed to find common answers to questions such as electronic identification. A number of initiatives are exploring this and the European Commission will look at how to bring them together. Collaboration with standardisation bodies will also be heightened, with a view to preparing practical recommendations during the first half of 2006.*

17

[17] The Interoperable Delivery of pan-European eGovernment Services to public Administrations, Businesses and Citizens (IDABC) . . . Brussels on 17-18 February 2005.

Iniciativas na UE [18]

eEurope

A iniciativa política resultante do Conselho Europeu da Feira (Junho/2000).

Estabeleceu os objectivos *eEurope2002* que previa *"secure networks and smart cards"* e uma das acções implementadas foi o estabelecimento da *"eEurope Smart Card Charter"*.

Estes objectivos são continuados na iniciativa *eEurope2005* estabelecida no Conselho Europeu de Sevilha (Junho/2002). Refere

"The development of secure and seamless access to e-Government services depends on deployment and the effective use of electronic authentication means".

Um dos focos de actividade intitula-se "Secure e-Government and Identity Management".

EESSI & CEN TC 224

Comissão de normalização para a Sociedade da Informação (EESSI) e comissão técnica de acompanhamento das tecnologias relacionadas como *smart cards* (CEN TC 224).

No âmbito desta última existe um grupo de trabalho (WG 15) para cartões de cidadania, estabelecido em 2003; reuniu pela primeira vez no início de 2004 e deve produzir recomendações durante 2005.

[18] Em "Survey on EU's Electronic-ID Solutions" A-SIT Report, Aug. 2004

Grupo de Porvoo

Consórcio de autoridades públicas ligadas à identificação electrónica criado no seguimento do *Smart Card Charter Trailblazer TB1*.

Responsável pelo documento *Electronic Identity White Paper* anexo a esta comunicação. Proponente das norma OSCIE (*Open Smart-Card Infrastructure for Europe*) resultante do eESC (*eEurope Smart-card Charter*). Responsável por "surveys" periódicos sobre o estado dos diversos projectos de eID na Europa.

EUCLID (European initiative for a Citizen digital ID solution)

Projecto do 5FP para suportar as actividades do "eEurope Smart Card Charter Trailblazer 1 (TB1) Public Identity" e do Grupo de Porvoo.

PRIME (Privacy and Identity Management for Europe)

Projecto 6FP com objectivos nas tecnologias de gestão de identidade.

eEpoch

Projecto do 5FP para demonstrar a interoperabilidade de soluções de identificação electrónica baseadas em *smart cards* em 6 projectos piloto

2º Paradigma

O cartão é um **token criptográfico**, contendo só chaves privadas e respectivos certificados de chave pública, e está equipado com funcionalidade criptográfica que permite:

- gerir de forma segura a posse das chaves privadas; isto implica
  - ▷ garantias de confidencialidade para as chaves privadas
  - ▷ garantia de posse efectiva do dispositivo criptográfico (protecção do cartão com PIN's ou autenticação biométrica)
- gerar as chaves privadas, gerar assinaturas digitais e participar em protocolos de identificação seguros,

. . . este cartão permite ao cidadão . . .

- produzir identificação electrónica e autenticação de actos perante serviços públicos ou privados, através de um acto de vontade exclusivo,
- construir assinaturas digitais qualificadas sobre documentos electrónicos,
- opcionalmente, cifrar documentos electrónicos,
- opcionalmente, gerir certificados de atributos.

Cartão/PKI e os Serviços

Na identificação "por acto de vontade", o cidadão identifica-se (e nunca "é identificado") fazendo prova que é titular de direitos.

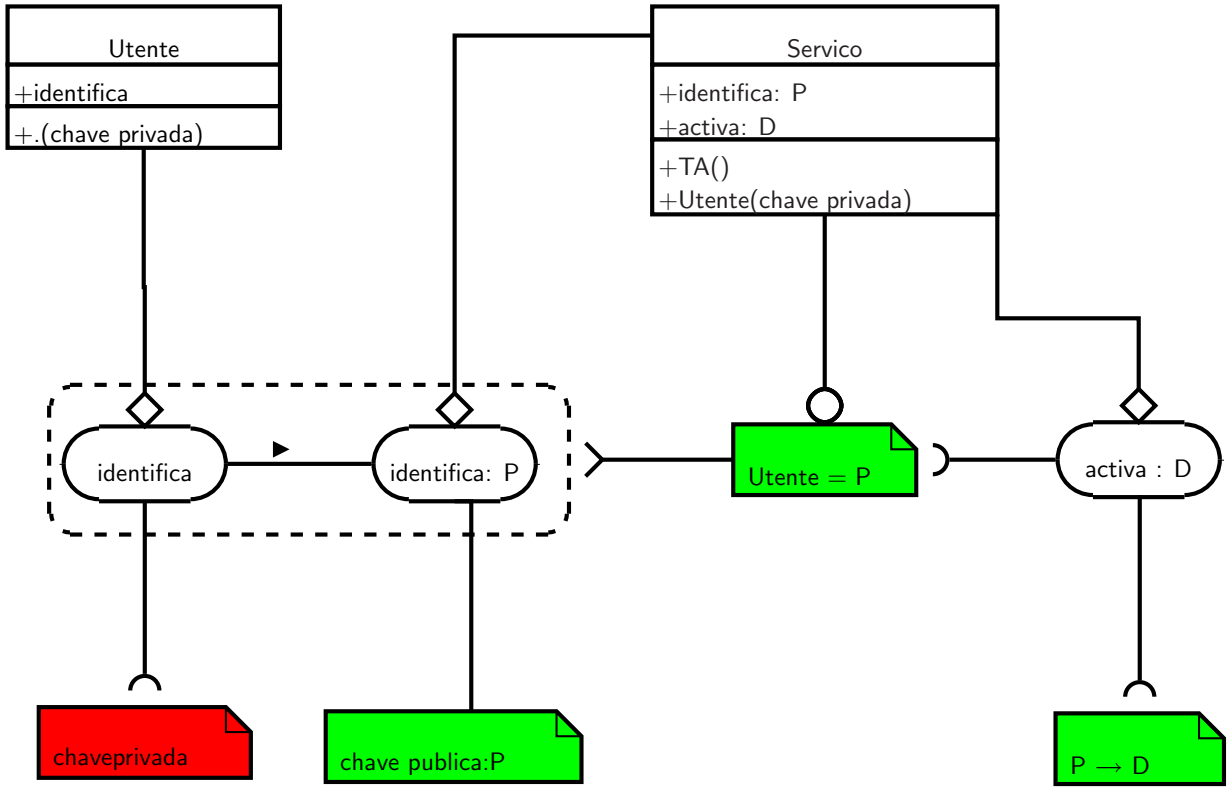
Cada interacção onde o cidadão intervêm resulta da cooperação entre o agente **utente** e o agente **serviço** de acordo com o seguinte protocolo:

1. O **utente** faz prova que é titular de uma determinada **personalidade digital**[19] P mostrando que controla a chave privada respectiva,
2. O **serviço**, confiando na autenticidade da chave pública[20], reconhece que está em presença da personalidade P e disponibiliza-se para activar os **direitos** D que lhe estão associados.

A figura seguinte é um diagrama de confiança que representa este protocolo. Estão representados os dois agentes, os eventos e, a verde, os items de informação em que o serviço confia.

[19] Representada, normalmente, por uma chave pública

[20] Recorrendo a um certificado de chave pública apropriado.


Utente
+identifica
+.(chave privada)
Servico
+identifica: P
+activa: D
+TA()
+Utente(chave privada)
identifica
identifica: P
Utente = P
activa : D
chaveprivada
chave publica:P
P → D
Certificado
Registo

Para saber quais são os direitos D associados à personalidade P é necessário que exista um **registo autenticado** da associação $P \longrightarrow D$.

O serviço que activa o direito D tem de conhecer este registo e tem de ter garantias da sua autenticidade e, por vezes, da sua confidencialidade.

A confiança no registo $P \longrightarrow D$ ou na chave pública resulta de **provas de autenticidade** dos items e do **reconhecimento** das autoridades que os emitem.

As provas de autenticidade assumem, normalmente, a forma de **certificados**[21] emitidos por **autoridades de certificação** apropriadas.

O reconhecimento resulta das hierarquias de confiança associadas ao sistema de Autoridades de Certificação inerentes à "Public Key Infrastruture".

[21] Para a chave pública é sempre assim; porém para o registo $P \longrightarrow D$ a autenticidade pode resultar de outro tipo de confiança. Para as chave pública os certificados são, obviamente, **certificados de chave pública** enquanto que para os registos serão **certificados de atributos**.

O que são registos?[22]

Sob o ponto de vista do serviço é indispensável implementar os registos $P \longrightarrow D$ e integrá-los nos sistemas de informação existentes. Para isso tem de definir:

Personalidade P: é o item de informação que contém a chave pública mas pode conter, também, outro tipo de informação relevante (limitações à personalidade, períodos de validade, etc.).

É essencial que P seja **não invertível/impessoal**; isto é, o seu conhecimento não deve permitir determinar a personalidade jurídica do utente. [23]

Direitos D: é um item de informação que pode, simplesmente, ser um identificador de utente do serviço (número de contribuinte, da segurança social, etc.)[24].

[22] É importante ter em conta que estes registos são específicos de um determinado serviço e, por isso, cada serviço pode exercer um grau de controlo elevado sobre a sua estrutura sem afectar a funcionalidade dos restantes serviços.

[23] Dado que os certificados de chave pública são públicos é possível (com recurso computacionais apropriados) construir historiais da sua utilização e assim violar, eventualmente, a privacidade do seu titular. Por isso é indispensável que a informação neles contida seja não invertível. Os registos $P \longrightarrow D$ podem ou não ser públicos; caso o sejam deve existir o mesmo tipo de cuidados: aqui a construção de historiais é ainda mais grave.

[24] Dado que não é possível garantir a não invertibilidade destes identificadores, é essencial que um registo com este tipo de definição de

Noutras situações pode ser informação mais estruturada; por exemplo, *scripts* que especifiquem uma determinada sequência de actos realizados em benefício do utente.

Qualquer que seja a forma de descrição dos direitos, caso os registos sejam públicos, é essencial garantir a sua não invertibilidade.

direitos seja confidencial e sejam colocadas todas as garantias respeitantes ao eventual cruzamento de dados.

Registos: geração e emissão

A geração do registo escolhe os direitos D que devem ser associados a uma determinada personalidade digital P.

Frequentemente isso implica conhecer a personalidade jurídica que está associada a P mesmo que tal não faça parte do registo.

O Serviço tem de confiar no registo e na autoridade que o emite (o **Emissor**). Frequentemente o próprio Serviço (ou um departamento específico dentro do Serviço) funciona como Emissor para os seus registos.

No entanto pode acontecer que o Serviço delegue essa responsabilidade num outro agente em quem confia e os registos assim emitidos podem ser suficientemente genéricos para poderem ser usados por vários serviços ou departamentos dentro de um mesmo Serviço.

A geração do registo segue o seguinte protocolo:

1. O **Emissor** recolhe do Utente a sua personalidade digital P e obtém provas de que o utente tem a posse da chave privada respectiva[25].
2. O **Emissor** obtém a personalidade jurídica do Utente e por ela determina quais os direitos D a associar a P. [26]
3. O **Emissor** constrói o registo $P \longrightarrow D$, autentica-o[27] e fornece-o ao Serviço apropriado.

[25] Correndo um protocolo de identificação, por exemplo.

[26] A informação recolhida neste passo de protocolo deve ser a indispensável para ser possível determinar os direitos; pode ocorrer, em serviços não críticos, que o conhecimento assim obtido seja mínimo. De qualquer forma esta informação é fornecida voluntariamente e, portanto, está ao abrigo da legislação sobre protecção de dados pessoais.

[27] Assinando-o digitalmente, por exemplo; podem, ainda, ser usados outros mecanismo de autenticação, nomeadamente quando os registos são emitidos pelo próprio serviço que os vai usar.

Gestão e Confidencialidade dos Registos

O serviço tem de aceder ao registo $P \longrightarrow D$ sempre que o Utente, com a personalidade digital P, solicita um serviço.

Onde reside essa informação e qual o grau de confidencialidade que lhe está associada é algo a definir já que isso determina o nível de protecção contra o acesso indevido a dados pessoais[28] e cruzamento de dados.

Por isso o controlo do acesso aos registos é crucial ao funcionamento correcto do Serviço (garantido a privacidade do Utente) e deve ser colocada ao abrigo da Lei de Protecção de Dados Pessoais.

Algumas possibilidades:

- O registo não contém dados pessoais, é público e emitido por uma autoridade independente

[28] Apesar de os registos não conterem, normalmente, dados pessoais, o acesso indevido a esses registos permite construir historiais de utilização associados a personalidades digitais específicas. Caso a definição dos direitos D permita reconstruir a personalidade jurídica (seja "pessoal") então a situação ainda é mais grave porque os registos, caso fossem públicos, permitiriam reconstruir dados pessoais.

dos serviços e reconhecida por estes. Aqui ele pode ser armazenado no próprio cartão e fornecido a cada Serviço no acto de identificação.

- P é uma chave pública, D é um identificador específico do serviço e o registo é emitido pelo próprio serviço. Neste caso o serviço limita-se a manter uma tabela com estas associações que ele próprio autentica e garante a confidencialidade[29].
- O registo permite a reconstrução de dados pessoais ou historiais de utilização mas é emitido por uma autoridade externa ao Serviço. Neste caso, para além de ser exigida uma autenticação digital, o Emissor deve cifrar os registos com a chave pública de cada Serviço que está autorizado a conhecer o seu conteúdo.

[29] Na terminologia do Projecto de Lei 112/IX estas tabelas eram designadas por "depósitos de chaves"; esta forma de registo era a única aí prevista.

Latência da Personalidade Digital e Número Único(?)

Por **latência** da personalidade digital entende-se o grau com que essa personalidade se mantém ao longo do tempo mesmo quando, por degradação de equipamentos ou "software", se torna necessários substituir os seus suportes tecnológicos[30].

Cada certificado de chave pública contém uma forma de identificação do seu titular. Em actos de identificação, essa informação pode ser um simples pseudónimo, não invertível e sem qualquer latência; isso em nada afecta os mecanismos de identificação ou de geração e manuseamento de registos que indicamos.

O certificado de chave pública usado na identificação digital, por si só, não necessita de conter qualquer tipo de informação que permita reconstruir a personalidade jurídica do seu titular.

Já no uso de assinaturas digitais, em actos que exigem o "não repudio", isto não é assim. Uma

[30] Por exemplo, um *smart-card* tem um tempo de vida útil de cerca de 3 anos; como as chaves privadas são geradas dentro do cartão e nunca de lá saem, a emissão de um cartão de substituição implica sempre a geração de novas chaves privadas e novas chaves públicas o que tem efeitos na latência da personalidade digital.

assinatura digital deve ser publicamente verificável e o seu reconhecimento implica a identificação da personalidade jurídica de quem a produziu.

Isto implica que o certificado de chave pública usado nas assinaturas digitais tem de conter informação que permita reconstruir a personalidade jurídica relevante ao contexto onde a assinatura está a ser usada[31].

Daqui resulta que a identificação do titular de um certificado de chave pública usado em assinaturas digitais, deve ter elevada latência e ser essencialmente invertível (ou "pessoal").

É devido a esta distinção que o Cartão do Cidadão necessita, no mínimo, de dois certificados (e as respectivas chaves privadas): um usado em identificação digital e outro usado em assinaturas digitais.

Se o identificador de elevada latência pode ou não ser considerado um "número único" que viole o disposto no nº 5 do Art. 35º da CRP, é algo que depende da interpretação jurídica[32].

[31] Pode ser um simples endereço de "e-mail" se o contexto não exigir mais.

[32] Em último caso, tanto uma representação digital do nome de um cidadão como um qualquer dado biométrico podem ser considerados "números" únicos.

Outra questão deriva da latência, que é necessário garantir nos registos dos vários serviços, quando existe alteração da chave pública de um Utente.

O problema, aparentemente complexo, tem uma solução simples:

- a Autoridade de Certificação (AC) que emite os certificados de chave pública (e que conhece a personalidade jurídica associada a cada chave pública) emite **certificados de substituição** que essencialmente estabelecem uma associação $K \longrightarrow K'$ entre a chave pública antiga K e a nova chave pública K'.
- cada Emissor de registos consulta regularmente a AC, recolhe os eventuais certificados de substituição e actualiza automaticamente os seus registos.

  Note-se que o conhecimento que o Emissor detém sobre a personalidade jurídica do Utente não sofre qualquer alteração.

A favor das "base de dados de bolso"

Como substituto directo dos actuais meios identificadores, um cartão assente no paradigma "base de dados de bolso"[33] apresenta, como vantagem aparente, uma integração mais simples com as aplicações.

No entanto, analisando as várias variantes de integração dos processos de identificação/processamento, vê-se que, mesmo neste modelo restrito, a eventual vantagem não se concretiza.

[33] Restringida a sua funcionalidade a um conjunto muito limitado de serviços e ignorando as dificuldades em termos de segurança, privacidade de dados pessoais e interoperabilidade com outros sistema europeus.

Questão:
Existem vantagens funcionais para o armazenamento directo de dados pessoais num cartão?

	ID visual	e-ID on-line	e-ID off-line
proc. deferido	Não	Não	Não
proc. imediato	Não	Não	Sim

Vantagens económicas do cartão PKI

- A flexibilidade encoraja um grande número de serviços integrados na "comunidade do cartão"[34]
- A interoperabilidade de cartões europeus encoraja a questão de escala e faz reduzir os custos.
- Torna viável um "mercado de serviços".[35]
- . . .

[34] Na Finlândia, em 2003, eram mais de 50 serviços públicos e alguns privados, com variadas ofertas de serviços, que estavam integraddos com o cartão.

[35] A emissão de um registo pode ser feita por uma instituição distinta de quem presta o serviço; um registo é um "token de serviço" (funcionalmente análogo aos do "electronic cash") que pode, posteriormente, ser consumido por diferentes concorrentes a prestar o serviço.

Postscriptum

Em países onde existem projectos de identificação electrónica dos cidadãos baseados em atributos (nomeadamente, atributos biométricos), e em que a representação no cartão desses atributos é replicada numa base de dados central (p.ex. Reino Unido e França) tem-se vindo a observar uma forte reacção da opinião pública contra a existência de tal base de dados.

Nesses países observou-se, na opinião pública, um inicial entusiasmo mitigado quando o projecto foi apresentado em termos de funcionalidade e que esse entusiasmo se converteu rapidamente em criticismo quando questões como esta foram tornadas públicas.

A identificação assente numa PKI não requer tal base de dados e é importante passar esta mensagem para a opinião pública. Parece-metambém importante que no projecto do CC não surjam aspectos deste tipo que criem situações de hostilidade pública que, a meio do projecto, o tornem inviável. Para isso parece-me essencial focar, dedesde o nío, no facto de o CC ter por objectivo garantir direitos na Sociedade da Informação.