# Identidade Digital

**Coordenador: Paulo Veríssimo ( FC/UL )**

**18 de Abril de 2007**

**Fundação Portuguesa das Comunicações**

apdsi
associação para a
Promoção e Desenvolvimento
da Sociedade da Informação

Patrocínio

ctt

Sun microsystems

# Estudo sobre a Identidade Digital

**Apresentado por:**
**Paulo Esteves Veríssimo (coordenador)**

**Relatores:**
**José Gomes Almeida**
**Pedro Antunes**
**Rogério Bravo**
**José Pina Miranda**
**Pedro Verdelho**
**André Zúquete**

# Introdução

- Não há um único cidadão, instituição, entidade, a quem ela não vá afectar quando a actividade da sociedade se deslocar para a esfera do ciberespaço.
- Não ter identidade digital será em grande medida como não ter bilhete de identidade nos dias de hoje.
- “Digitalização da sociedade” é caldeirão de pressões
  - sinal de modernidade via *gadgets*,
  - oportunidade de negócio via efeito de escala,
  - ditame abstractamente imposto por decreto,
  - último reduto contra o fantasma da insegurança.

# A Identidade social

- existe já uma noção bastante clara e arreigada na sociedade, acerca da *identidade social* e das formas clássicas da sua utilização e gestão.
- a organização ou indivíduo não quererão abdicar das mesmas ou vê-las deterioradas em seu prejuízo por mor da introdução de novas tecnologias
- quererão sim vê-las amplificadas, melhoradas e consolidadas em seu benefício.

# A Identidade Digital

- *Informação compilada, organizada e actualizada em sistemas informáticos, relativamente a pessoas físicas e jurídicas*.
- convergência do significado legal e social dessa informação com o significado técnico e informático da mesma.

# Assinatura digital

- cadeia de bits resultado da aplicação de uma função criptográfica a um texto arbitrário (o que é assinado),
- univocamente parametrizada por uma chave privada a que corresponde uma chave pública.
- deve existir a noção do próprio sujeito que assinou, como detentor do pseudónimo digital relacionado com o certificado da chave utilizada.
- chave privada (que é secreta) é utilizada pelo próprio e só por ele para assinar, chave pública é utilizada para verificar essa mesma assinatura.
- documento electrónico de identidade serve para acreditar electronicamente a identidade pessoal do titular e permite-lhe assinar electronicamente.

# Gestão da Identidade

- debate sobre a gestão da ID muito influenciado por:
  - documentos de identificação digitais (CdC, PEP) e pelas tecnologias de autenticação disponíveis pelos fornecedores
- em lugar de responder a um conjunto de problemas:
  - os anseios justificados dos cidadãos
  - as preocupações de segurança nacional
  - e a eficiência funcional do “todo” público (Admin. Pública)
- digitalização da sociedade introduz mudanças no equilíbrio dessa gestão, a não minimizar:
  - capacidades dos sistemas tecnológicos facilitam operações indevidas, roubo, chantagem
  - questões de protecção de privacidade e de segurança de activos agravam-se

# O problema (I)

- A questão da *identidade digital* (ID) pertence ao processo amiúde chamado da «sociedade da informação» e é multifacetada
- Alguns dos problemas que têm surgido no processo de “digitalização” da identidade derivam de percepções estreitas dessa realidade
- A ser assim, a visão ID nunca será bem sucedida

# A Identidade no quadro mundial actual

- existe correntemente uma atitude obsessiva em relação à segurança
  - enquadramentos legais e policiais que podem vir a ser detrimentosos do conceito moderno de sociedade democrática
- recolha, digitalização e arquivamento de dados biométricos (foto e impressões digitais)
  - dos cidadãos estrangeiros que entram em território dos EUA
- União Europeia titubeia neste campo
  - e manifesta uma notória falta de iniciativa e de estratégia.

# A Identidade no quadro mundial actual

- UE submete-se de forma quase incondicional a dinâmicas que contrariam princípios sociais europeus
  - silêncio à volta dos dados biométricos nas fronteiras dos EUA
  - não exercício do direito de reciprocidade
- compromete de forma muito grave a sua liderança tecnológica em algumas áreas de TIC:
  - biometria, comunicações móveis, segurança de infraestruturas críticas, preservação da privacidade
- a seguir à biometria transfronteiriça, veio o passaporte electrónico.
  - E... O cartão único de identificação? Os sistemas de voto electrónico?

# O problema (II)

- abordar a ID somente pela perspectiva tecnocrática, ou comercial, ou política, ou mesmo policial/securitária:
  - apenas como um sinal frívolo de modernidade via *gadgets*,
  - uma oportunidade de negócio via efeito de escala,
  - um ditame abstractamente imposto por decreto,
  - ou ainda o último reduto contra o fantasma da insegurança.

- lê-se e ouve-se amiúde, que «tudo se justifica para garantir a segurança face a ameaças» ou «tudo pela eficiência dos processos administrativos».
- ... acreditando que o cidadão tem uma atitude estática e passiva em relação às medidas impostas.
- No entanto e citando:
  - «... os cidadãos têm uma desconfiança crescente nos serviços e infra-estruturas de informação e comunicação ...» ou «... a experiência do cidadão comum é dominada pelo conhecimento público de falhas de computadores, grandes projectos de software mal sucedidos, programas maliciosos (vírus, *spam*, espiões)» [SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework]

- a não percepção destas dinâmicas pelas partes interessadas pode levar a situações de difícil retorno no que respeita deterioração da *confiança* na sociedade da informação. Citando de novo:
  - «... se uma sociedade baseada em TIC não for capaz de criar confiança nos serviços, isto é, confiança que se baseie em argumentos justificados e credíveis, então esses serviços, que serão de qualquer modo disponíveis devido à pressão do mercado: serão vistos com desconfiança pelos utilizadores; serão geridos por grupos restritos de “peritos”, aumentando a info-exclusão; poderão ser mal geridos, levando ao ciber-crime, e-fraude, ciber-terrorismo ou sabotagem...». [SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework]

# ID, uma questão de confiança

- a ID está a montante de vários outros processos críticos da sociedade da informação, como sejam:
  - votação electrónica; controlo de acessos incluindo passagem de fronteiras; digitalização de processos na administração pública e de saúde; comércio electrónico.
- por outro lado, ID é a ligação umbilical dos cidadãos e outros *stakeholders à* vertente digital da sociedade.
- na migração para a ID, existem vantagens, riscos e oportunidades não desprezáveis.
- a falência da confiança na ID,terá consequências dramáticas para a sociedade da informação

# Vertentes da via para a ID

- Mas um erro quase equivalente será achar, por contraponto e pela perspectiva fundamentalista, que:
  - os *gadgets* são supérfluos,
  - os lucros imorais,
  - as leis bloqueantes,
  - ou o rastreamento *bigbrotheriano*.
- Uma visão equilibrada assenta no que podemos denominar de *vertentes da via para a sociedade da informação*, e logo, para a identidade digital:
  - **Sociedade; Lei/Polícia/Tribunais; Segurança; Tecnologia**

# Vertentes da via para a ID: Societária

- porque tudo começa na projecção para o domínio cibernético de uma ontologia já existente nas sociedades, de modos mais ou menos formais
- é necessário pensar o que se quer realmente projectar: pessoas, papéis, pseudónimos,...
- é necessário equacionar e divulgar os ganhos e riscos sociais da migração para a ID, sendo que claramente deve haver um balanço positivo.

# Vertentes da via para a ID: Societária

- na vertente societária há um sem número de questões que merecem reflexão, p. ex.:
  - Novas tecnologias podem levantar dúvidas quanto à identidade dos indivíduos
  - Serviços criados por razões de conveniência podem reduzir a privacidade e segurança
  - Processos e sistemas destinados a identificar terroristas e outros criminosos podem levantar dúvida moral
  - Interoperabilidade de sistemas com origens diversas afectam o contrato social entre os cidadãos e o estado
  - Os períodos de adaptação dos sistemas às novas tecnologias abrem muitas possibilidades para a ocorrência de falhas não previstas
  - O síndroma *Big Brother*

# Vertentes da via para a ID: Societária

- n

*«Eu, Fulano, declaro que não me responsabilizo por qualquer dívida contraída ou a contrair, em compras electrónicas, pelo meu avatar na Internet que ficou fora de controlo.»*
*Ou*
*«Eu, Sicrano, declaro que a entidade digital que efectua transacções electrónicas personificando-me de modo “perfeito”, não sou eu!»*

# Vertentes da via para a ID: Jurídica, Policial e Judicial

- porque as leis existentes estão pensadas para uma ontologia ligada à identidade social
- realidade da ID facilmente pode tornar essas noções obsoletas (ex. pseudónimos), mais ricas (ex. avatares), ou mais complexas (ex. biometria)
- nada será mais nefasto do que as leis, métodos e meios de acção policial e judicial, não se adequarem à migração da actividade da sociedade para o domínio do virtual, digital, imaterial.

# Vertentes da via para a ID: Jurídica, Policial e Judicial

- porque a velocidade e perfeição com que atentados à noção de ID se vão processar vai afectar equilíbrios e noções existentes:
- do *timing* de acção/reacção entre criminoso e polícias;
- da produção (agora virtualizada) de prova e da consequente responsabilização;
- da relativa verosimilhança da identificação fraudulenta.

# Vertentes da via para a ID: Jurídica, Policial e Judicial

- po… os
  à…
  e…

*«Fulano foi responsabilizado por operações bancárias na Internet feitas por outrém, com uma mera cópia do seu nome de utilizador e palavra-de-passe: os Bancos obrigaram contratualmente o cliente, assumindo ser este um meio de identificação "perfeito" em termos legais e a Lei, no que respeita às transacções electrónicas, legitima essa cláusula por omissão.»*

# Vertentes da via para a ID: Jurídica, Policial e Judicial

- leis inadequadamente castradoras, e/ou  métodos de investigação musculados, poderão fazer mais dano à sociedade que aos criminosos.
- existe a possibilidade de ocorrência de crimes e fraudes informáticas em que se torne tecnicamente inexequível provar em tribunal de que lado está a razão.
- se actualmente a visão acerca do *furto de identidade* corresponde a um tipo de dano económico, o grau de ameaça que o tema representa é tanto mais distinto, quanto sério.

# Vertentes da via para a ID: Jurídica, Policial e Judicial

- leis inadequadamente castradoras, e/ou  métodos de investigação musculados, poderão fazer mais dano à sociedade que aos criminosos.
- existe a possibilidade de ocorrência de crimes e fraudes informáticas em que se torne tecnicamente inexequível provar em tribunal de que lado está a razão.
- se actualmente a visão acerca do *furto de identidade* corresponde a um tipo de dano económico, o grau de ameaça que o tema representa é tanto mais distinto, quanto sério.

# Vertentes da via para a ID: Jurídica, Policial e Judicial

- le… …e
  ir… …à

*«Descoberta vulnerabilidade em bilhetes de identidade digitais que possibilita o roubo de identidade quando o mesmo é utilizado em operações legítimas. Inúmeros casos de fraude, negados tanto pelos legítimos possuidores da identidade, como pelos arguidos, estão a entupir os tribunais. Peritos chamados a depor alegam que, devido ao tipo de vulnerabilidade em questão, as assinaturas falsas são indistinguíveis das verdadeiras.»*

…*ntidade*
… grau de
…s distinto,
quanto

# Vertentes da via para a ID: Segurança (informática)

- porque a representação informática da identidade coloca a noção de ID sob um número de riscos, no plano informático, devido a ataques aos sistemas:
  - a automatização e velocidade da fraude, a fidedignidade do roubo de identidade, a permeância da violação da privacidade
- é então indispensável definir e concretizar as propriedades necessárias para os sistemas que gerem a ID trabalharem correctamente:
  - confidencialidade, privacidade, autenticidade, não-repudiação, anonimidade, integridade, disponibilidade

# Vertentes da via para a ID: Segurança (informática)

- os sistemas e processos informáticos de suporte à ID têm de dar garantias de confiança às partes interessadas:
  - procedimentos auditáveis de verificação e teste;
  - o processo e o produto do desenvolvimento devem ser susceptíveis de certificação.

# Vertentes da via para a ID: Segurança (informática)

- os
  té

*«Credenciais digitais de 43 567 cidadãos, arquivadas no servidor de uma conhecida firma de comércio electrónico, foram esta madrugada roubadas por ciber-criminosos. Ao abrir do expediente, mais de 3 400 fraudes, em compras e transacções várias, haviam já sido automaticamente perpetradas, utilizando as credenciais roubadas através de serviços interactivos na Internet, atingindo um total superior a 6 milhões de euros.»*

# Vertentes da via para a ID: Tecnologia

- a tecnologia deve ser utilizada no sentido de fornecer meios de gerar/manter/verificar a ID, nem mais, nem menos.
- deve fazê-lo sem comprometer direitos de cidadania e equilíbrio funcional das sociedades democráticas.
- evitando que a disponibilidade de tecnologia faça inverter os objectivos e prioridades do sistema de ID.
- as empresas envolvidas no ciclo produtivo da ID devem lucrar, mas devem fazê-lo através do desenvolvimento e colocação em serviço de tecnologias que sirvam os propósitos da ID.

# Vertentes da via para a ID: Tecnologia

- os sistemas e processos da ID são críticos para a sociedade
  - o Estado deve definir, regulamentar e controlar parcialmente a introdução das tecnologias mais adequadas.
  - deve assegurar processos de certificação *auditáveis pela sociedade* que, com altíssima probabilidade, garantam o funcionamento do sistema de acordo com o especificado.
- deve-se ter um cuidado extremo com a mistura de credenciais de identificação na esfera digital:
  - o bilhete de identidade serve para nos identificar em instâncias diversas das de um cartão de clube

# Vertentes da via para a ID: Tecnologia

- O
s

*«Ex-empregado da empresa multinacional ACME, que fabrica, no estrangeiro, o cartão de identidade digital nacional do país XPTO, confessou, a partir de local desconhecido, existir uma back-door que permite perpetrar e-fraudes e aceder indiscriminadamentre aos dados do cartão. Sendo o cartão produzido com sistemas proprietários, cujo interior e funcionalidade eram em grande medida desconhecidos, as autoridades reportaram não ter sido possível descobrir atempadamente este problema.»*

# Panorama corrente

# Segurança e Tecnologia na realidade nacional

- Torna-se oportuno discutir as vertentes da segurança e da tecnologia em torno dos mais recentes símbolos da ID no nosso país:
- o Cartão de Cidadão (CC)
- o Passaporte Electrónico Português (PEP)

# Cartão de Cidadão (CC)

- terá um formato "smart card" e substituirá os actuais “bilhete de identidade”, “cartão do contribuinte”, “cartão de beneficiário da Segurança Social”, “cartão de eleitor” e “cartão de utente do Serviço Nacional de Saúde”.
- exibirá, na frente, a fotografia e os elementos de identificação civil e no verso, os números de identificação dos organismos mencionados
- terá um chip de contacto, com certificados digitais (para autenticação e assinatura electrónica), podendo ainda ter a mesma informação do cartão físico, completada por outros dados, designadamente a morada.

# Cartão de Cidadão (CC) - problemas

- cruzamento dos vários números leva virtualmente a “número único”
- alguma facilidade no acesso indiscriminado a dados por configuração ingénua (sem PIN ou com PIN igual para tudo), ou por endosso do cartão
- acesso excessivo a dados não necessários pelas autoridades, só porque existentes no cartão
- armazenamento de dados biométricos directos representa risco muito elevado de perda de identidade em caso de incidente

# Passaporte Electrónico Português (PEP)

- características de reconhecimento do titular
- nova geração de dispositivos como o reconhecimento facial
- *chip contactless (RFID)*, com a mesma informação impressa na página do titular organizada numa estrutura normalizada assinada digitalmente pelo País emissor
- estes dados são protegidos por um sistema de protecção simples (*Basic Access Control*, BAC)
- o PEP possui duas chaves resp. para cifra e controlo de integridade, derivadas de dados constantes do PEP, tanto em papel (MRZ) como no chip: o número do PEP, a data de nascimento e a data de expiração do PEP
- na segunda geração de PEPs o chip terá de obedecer aos requisitos de um novo Sistema de protecção reforçada (Extended Access Control, EAC)

# Passaporte Electr. Port. (PEP) - problemas

- autenticação é unilateral (não pode verificar-se se leitor é ou não legítimo)
- espaço de chaves, embora grande, permite alguma previsibilidade na procura das chaves
- permite que os dados constantes no *chip* sejam lidos remotamente sem autorização do dono, num raio de cerca de 10 metros
- acesso excessivo a dados não necessários pelas autoridades, só porque existentes no cartão
- armazenamento de dados biométricos directos representa risco muito elevado de perda de identidade em caso de incidente
- conteúdo de um *chip* de um PEP pode ser inteiramente duplicado para outro *chip* de outro PEP

# ANÁLISE
# E RECOMENDAÇÕES

# O furto de identidade acontece...

- *… The perception is growing, but mainly they think that only their neighbours can be the victim, well there are already a lot of people who have received some extra letters off the tax inspectors and that's hard to prove that you're not the person that did the work. These kinds of experiences are making the people aware that this is a serious problem – I think it's definitely not so common and understood by the people.'..*

[The Fight Against Identity Fraud]

# A biométrica não é a *chave*...

- *For instance biometrics is problematic for use for authentication as the "secret key" is not secret, revocable or unique – biometrics can be spoofed and victims of identity theft cannot get a new set of biometrics – using several spoofable biometrics can merely create more "fake security".*

  [SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework]

## ANÁLISE : Principais riscos

- Furto, falsificação ou perda de identidade
- Violação da privacidade e do controlo sobre os dados pessoais
- Síndroma do número único
- Velocidade e automatização das fraudes
- Fidedignidade das fraudes

## RECOMENDAÇÕES : Princípios fundamentais

- Projecção do social no digital
- Adequação do regime juridico-legal
- Compreensão e confiança no digital
- Subordinação do tecnológico ao social

## RECOMENDAÇÕES : Medidas específicas

- *Sociedade*
- Promover a educação das partes interessadas
- Promover uma cultura de exigência no cidadão
- Garantir a transparência, certificação e auditabilidade dos sistemas e processos
- Garantir a posse da sua ID (empowerment) pelas partes interessadas

## RECOMENDAÇÕES : Medidas específicas

- *Legislação*
- Promover urgentemente a modernização da lei do crime informático
- Promover a adequação das leis relacionadas com a identidade e identificação
- Garantir a responsabilização dos agentes públicos por incompetência/negligência

## RECOMENDAÇÕES : Medidas específicas

- *Polícias/Tribunais*
- Promover a formação da administração/polícias/ magistratura, nas questões da ID
- Criar meios tecnológicos que garantam a eficácia das polícias e dos tribunais em ID

## RECOMENDAÇÕES : Medidas específicas

- *Segurança*
- Definir as propriedades de segurança necessárias aos sistemas e processos da ID
- Definir os procedimentos conducentes à imposição de segurança (ex. certificação)
- Assegurar os direitos de privacidade das partes interessadas, na transição para a ID
- Promover uma cultura de segurança sustentada na Administração Pública

## RECOMENDAÇÕES : Medidas específicas

- *Tecnologia*
- Regulamentar e controlar as tecnologias mais adequadas ao objectivo da ID
- Regulamentar e controlar os procedimentos conducentes à imposição de segurança
- Garantir auditabilidade pela sociedade para obter a sua confiança no sistema

# Conclusões

- propriedades essenciais de um sistema de ID podem ser comprometidas por insuficiências em várias vertentes
- funcionar mais ou menos bem não é aceitável para sistemas e infra-estruturas críticas com os da ID
- parte substancial dos pontos recomendados é imperativa, sob pena de graves problemas na ID
- sucesso ou insucesso da ID influenciará outros processos críticos para a sociedade da informação:
  - votação electrónica; controlo de acessos e passagem de fronteiras; administração pública e saúde; e-comércio.

*Esperamos ter dado uma contribuição positiva para o sucesso deste processo*

***Muito Obrigado!***

***O Grupo de Estudo***