MODELOS ALTERNATIVOS PARA A UTILIZAÇÃO DE INFRA-ESTRUTURAS DE CHAVE PÚBLICA NO COMÉRCIO ELECTRÓNICO

*Carlos Serrão & José Cordeiro Gomes**

RESUMO

A actual Nova Economia, baseada essencialmente na Internet, depende em muito da validade e segurança da informação. O comércio em geral não poderia existir se não existisse um laço de confiança entre vendedores e compradores, e em particular no Comércio Electrónico este aspecto é de especial importância devido à inexistência do tradicional contacto físico entre ambos. De facto, a confiança é a fundação de todo o comércio. Apenas se as relações comerciais forem seguras contra intrusões, má utilização, sabotagem, utilização lesiva ou roubo se conseguem estabelecer relações de confiança. Apesar deste problema não depender somente de uma componente tecnológica não há dúvida de que esta representa um papel extremamente importante, que passa pela utilização de tecnologia criptográfica, garantindo princípios fundamentais: privacidade, autenticação, integridade e não repúdio. O modelo de confiança ubíquo que lhe está subjacente designa-se por PKI ou Infra-estrutura de Chave Pública.

Palavras-chave: PKI, Segurança, Confiança, Criptografia, E-Business, E--Commerce.

I. INTRODUÇÃO

O mercado do futuro irá ser global e electrónico, representando uma mudança profunda da forma de conduzir negócios. Esta mudança profunda, amplamente reconhecida, está já a iniciar-se, atingindo proporções significativas nos Estados Unidos e na Europa (Eng, 2000).

Este crescimento depende do número de empresas, organismos de administração e utilizadores particulares que adiram, mas é um fenómeno em expansão que conduz a uma utilização bastante alargada.

A visão que prevalece é a de que a economia irá organizar-se em torno de vastos sistemas de negócio electrónico, constituídos por redes de fornecedores, distribuidores e clientes, que utilizarão meios electrónicos como plataformas base para colaborarem e competirem no mercado.

A criação desta nova forma de organização, frequentemente designada por Nova Economia, reside na possibilidade das empresas e organizações em geral se reinventarem, aproveitando o seu conhecimento e as suas potencialidades internas para, com base nas possibilidades oferecidas pela tecnologia, se reposicionarem nas cadeias de valor, redefinirem os seus processos de negócio, aumentarem a produtividade e se globalizarem.

* Docentes do Instituto Superior de Ciências do Trabalho e da Empresa.

A ligação entre os diferentes participantes nos processos de negócio existe desde a criação do mercado, no entanto, o factor significativo de alteração que foi introduzido pela tecnologia actual dos computadores é o conjunto das características do novo tipo de relacionamento económico, que passou a ser directo, interactivo, activo a todo momento e omnipresente (Kaen, Ballance, Chan, Schrume: 1992).

A capacidade disponibilizada pelos computadores interligados em vários níveis de rede vai para além do mercado - permite transferir e partilhar informação e conhecimento, melhorar o processo de decisão, eliminar esforço duplicado, favorecer o trabalho em equipa mesmo remotamente, ligar estreitamente quem trabalha, em suma, repensar toda a organização da empresa e dos seus processos de negócio (Garfinkel, Spafford:1997). É este contexto mais alargado que terá um impacto profundo na estrutura das empresas e organizações e conduzirá realmente a uma Nova Economia.

Esta Nova Economia, baseada essencialmente na Internet, depende em muito da validade e da segurança da informação (Garfinkel, Spafford:1997). O comércio não poderá existir se não existir confiança entre o vendedor e comprador on-line. Números de cartões de crédito e outros dados sensíveis não podem ser transmitidos em claro sem qualquer mecanismo de protecção[1] (Commercents:2000).

Ao longo deste artigo irão ser focadas as principais tecnologias emergentes que permitem a utilização de mecanismos de confiança electrónicos, comparando-os com os seus equivalentes no mundo real. De seguida serão apresentadas as infra-estruturas de chave pública, assim como as vantagens que estas podem trazer para o Comércio e Negócio Electrónico. Por último são apresentados os principais modelos de confiança PKI, assim como a sua adequação para o estabelecimento de vários tipos de confiança na Nova Economia.

II. TECNOLOGIAS DE SEGURANÇA EMERGENTES

Três tecnologias de segurança têm vindo a marcar o panorama: os certificados digitais, a criptografia e as PKI (Eng,2000). Todas estas tecnologias estão relacionadas e não podem existir dissociadas umas das outras. Os certificados digitais dependem da criptografia de chave pública, uma vez que associam a identidade de uma entidade à sua correspondente chave pública através da inserção de uma assinatura digital produzida por uma autoridade de confiança (Autoridade de Certificação). A criptografia recorre às PKI como mecanismo eficaz para estabelecer a confiança entre as entidades que desejem trocar dados utilizando chaves criptográficas[2]. Por seu turno, as PKI dependem de certificados digitais e de criptografia para poderem operar em segurança e estabelecerem relações de confiança com outras PKI.

Estas tecnologias estão a ajudar as empresas a construírem e a reformularem os seus negócios para a *Web*, enquanto que asseguram que informação vital dos consumidores e da própria empresa é mantida confidencial. Os certificados digitais são importantes para diferentes tipos de negócio (Eng,2000). Ajudam os consumidores e os negócios a verificar a fonte da informação e na determinação da autenticidade de aplicações de *software* e outros produtos.

Sem a existência de certificados digitais, modelos de negócio baseados na distribuição de *software* através da Internet, estaria condenada ao fracasso e não teria amadurecido como tem vindo a fazê-lo ao longo dos últimos anos. Sem uma forma fácil de verificar a fonte de actualizações de produtos, correcções de *software* e actualizações de ferramentas antivírus, os clientes não poderiam de todo confiar na informação fornecida pelos negócios on-line.

A maturação deste tipo de tecnologias, ao longo dos últimos tempos, tem ajudado em muito o crescimento da Economia Internet. Os negócios têm tido reduções significativas

[1] A criptografia é um exemplo de um dos mecanismos mais utilizados como medida de protecção.
[2] As PKI certificam que as chaves criptográficas utilizadas na troca de dados pertencem efectivamente às entidades que as utilizam.

de custos através da utilização destas tecnologias, o que permite uma forma de troca viável e de confiança de produtos e de informação (Gerck,1998; Keen et al., 1998). Mais, estas tecnologias têm permitido o verdadeiro comércio baseado em Internet e a utilização da *Web* pelos negócios, o que sem a utilização de certificados digitais, criptografia e PKI seria de todo impensável (Stalling, 2000). Negócios baseados na *Web* espalhados por todo o mundo não teriam a possibilidade de funcionar, ou teriam o seu funcionamento extremamente restringido, se não tivessem a possibilidade de verificar informação, encriptá-la, partilhar as chaves de encriptação com os seus empregados, clientes e parceiros de negócio.

Cada vez mais se tem verificado uma adopção mais alargada dos certificados digitais, da criptografia e do PKI pelos negócios na Internet, uma vez que mais e mais empresas adoptam a tecnologia (Nash, Duane, Joseph, Brink, 2001), existindo igualmente uma crescente percepção por parte dos consumidores das suas vantagens.

Recentemente foi realizado um estudo pela CommerceNet (2000), em que eram identificadas as principais barreiras e inibidores do Comércio Electrónico de três perspectivas distintas: Comércio Electrónico B2B[3] em Grandes Empresas, em Pequenas e Médias Empresas e no Comércio Electrónico B2C[4].

De acordo com este estudo, a mais importante barreira ao crescimento do Comércio Electrónico continuam a ser as preocupações de segurança: Segurança e Encriptação, Confiança e Risco, Autenticação dos Utilizadores e Inexistência de Infra-estruturas de chave pública, Fraude e Risco de Perda de Informação e Questão Legais são alguns dos aspectos mais citados neste estudo (CommerceNet, 2000).

A confiança sempre representou um papel fundamental nos negócios. Como percursor fundamental do comércio a confiança está incorporada em todas as estruturas e processos de mercado (Gerck: 1992; Keen et al,1998). No entanto, o Comércio e Negócio Electrónico modificaram profundamente essas estruturas e processos, e o próprio conceito de confiança sofreu igualmente alterações.

A. UMA NOVA FORMA DE FAZER NEGÓCIOS

A chegada do Comércio e Negócio Electrónico impulsionou as empresas e a própria sociedade para uma nova era de negócios, em que os efeitos se fazem sentir. Indústrias inteiras estão a sofrer uma profunda "desintermediação" e reestruturação. As empresas estão a redefinir quem elas são e como virão a actuar nesta nova era (Baltimore Technologies, 2001). A concorrência força-as a reavaliar as relações fundamentais e os consumidores estão a ganhar cada vez mais importância no mercado. É a primeira vez que, alterações desta magnitude se vislumbram em tão curto período de tempo nesta era moderna dos negócios.

Estas alterações afectaram as estruturas sobre as quais os negócios têm vindo a conduzir toda a sua actividade nos mercados. Relações entre compradores e vendedores estão a ser redefinidas e novas regras de negociação evoluíram e novos modelos de negócio têm vindo a surgir. As regras de negócio implícitas sob as quais os negócios são conduzidos estão a ser colocadas de parte e novas regras estão a ser criadas (Gerck, 1998). Ao ritmo que as estruturas e processos de mercado tendem a evoluir rapidamente para o Comércio e Negócio Electrónico, os mecanismos de confiança existentes revelam-se profundamente ineficientes (Gerck, 1998). A ausência de um consenso universal na forma como a confiança é estabelecida no Comércio e Negócio Electrónico é um dos aspectos inibidores do mesmo.

Estruturas comerciais sempre incluíram elementos implícitos e explícitos que estabelecem um ambiente aceitável no qual as transacções de negócio podem ser efectuadas a um nível aceitável de risco: lei comercial, normas regulamentares, apertos de mão, entre outros (Norris, West, Gaughan, 2000). Todos estes elementos foram agregados em vários

[3] Business-to-Business
[4] Business-to-Consumer

modelos de confiança que permitiam que os vários negócios e mercados pudessem operar. No entanto, o aparecimento quer da Internet, quer do Comércio e Negócio Electrónico alteraram profundamente estes modelos de confiança previamente estabelecidos tornando-os perfeitamente inadequados para esta nova era dos mercados e negócios electrónicos.

Como consequência, a incerteza e um crescimento do risco ensombra o novo espaço de mercado: os legisladores hesitam no desenvolvimento de novas ferramentas legais que possam acompanhar a evolução natural dos mercados; os consumidores não possuem formas eficazes e simples de determinarem com quem estão a realizar negócios; os novos modelos de negócio electrónico tornam a aplicação de algumas das actuais normas, perfeitamente questionáveis. Os actuais modelos de confiança não se adequam ao meio e aos desafios colocados pelos mercados electrónicos dos nossos dias.

B. COMÉRCIO E NEGÓCIO ELECTRÓNICO

O Comércio e Negócio Electrónico pode ser analisado e avaliado de várias perspectivas, interligando vários actores principais em vários cenários: Consumidores, Empresas e Administração Pública (ver Figura 1). Entre estes actores, devem existir relações de confiança entre eles que podem ser estabelecidas utilizando os modelos mais apropriados para cada um deste tipo de relações, como teremos oportunidade de ver mais adiante.

De acordo com os mais recentes estudos realizados para a Europa Comunitária, o Comércio Electrónico representou em 1999 um volume de negócios de cerca de 17000 milhões de euros e previsões apontam para que em 2002 este valor possa ascender a cerca de 199000 milhões de euros[5].

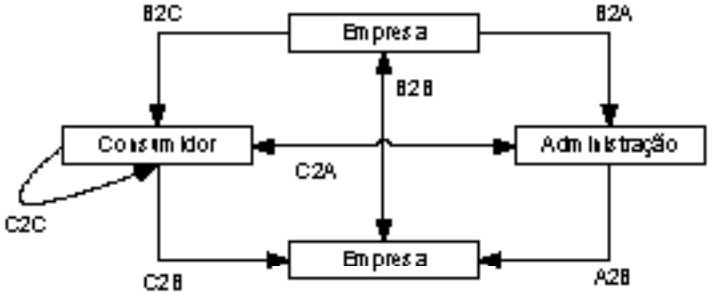

Figura 1 Relações de Comércio e Negócio Electrónico

Como pode ser facilmente constatado, por este e por outros estudos semelhantes, o volume de negócios e de transacções na rede é demasiadamente elevado para que as preocupações de segurança possam ser ignoradas.

Aspectos como a Privacidade, Autenticação, Integridade e Não Repúdio são importantes para a implementação e realização de Comércio e Negócio Electrónico e as Infra-estruturas de Chave Pública (PKI), o elemento principal que permite garantir este aspecto (Stallings, 2000).

III. AS INFRA-ESTRUTURAS DE CHAVE PÚBLICA

As Infra-estruturas de Chave Pública (PKI) são cada vez mais uma componente das arquitecturas de segurança das empresas (Addams, Lloyd: 1999). As PKI proporcionam um ponto de foco para muitos aspectos da gestão de segurança, assim como funcionam como impulsionadores da utilização de um crescente número de aplicações se segurança. Muitos

[5] Outros estudos apontam para outros valores, nomeadamente a nível mundial.

dos protocolos *standard* para correio electrónico seguro, acesso *Web*, Redes Privadas Virtuais (VPN) e sistemas de autenticação de utilizadores através de "*sign-on*" único fazem utilização de certificados de chave pública e como tal necessitam das PKI (Stallings: 2000).

Estas tecnologias PKI proporcionam importantes vantagens para as entidades que as utilizam, nomeadamente (Addams et al, 1999; Nash et al., 2001):

- Redução de custos administrativos;
- Redução do número de eventos "*sign-on*" requeridos pelos utilizadores finais;
- Redução da utilização de papel e melhoria da eficiência do fluxo de trabalho através de processos de negócio mais automáticos e seguros;
- Optimização da produtividade da força de trabalho;
- Reduzidos requisitos de treino para os utilizadores finais relacionados com os serviços de segurança.

As fundações do PKI são já conhecidas acerca de duas décadas com a invenção da criptografia de chave pública, no entanto a tecnologia PKI apenas teve o seu desenvolvimento comercial nos últimos anos, com a crescente procura comercial de serviços PKI nos últimos tempos por parte das empresas (Eng: 2000).

A segurança electrónica depende de processos e serviços que permitam a construção de uma solução segura para a distribuição de informação de negócio e serviço através da rede (Addams et al., 1999; Stallings, 2000). Estes serviços incluem:

- **Identificação**: processo de reconhecimento de um determinado indivíduo;
- **Autenticação**: processo através do qual se prova e verifica determinada informação;
- **Autorização**: processo de determinar o que uma entidade está autorizada a
- realizar;
- **Integridade**: processo de assegurar que a informação é inalterada;
- **Confidencialidade ou Privacidade**: processo de manutenção de informação secreta;
- **Não Repúdio**: processo que significa que não se pode negar a ter feito algo.

Todos estes serviços são utilizados de uma forma, ou de outra, no nosso dia a dia. O desafio consiste na reprodução de serviços semelhantes no mundo do Comércio e Negócio Electrónico. As técnicas que são utilizadas para criar os equivalentes electrónicos destes serviços são baseadas em criptografia (Stallings, 2000).

As PKI proporcionam ferramentas que permitem a disponibilização de serviços de segurança baseados em criptografia de chave assimétrica (ou criptografia de chave pública). Outras infra-estruturas que utilizam apenas criptografia simétrica têm vindo a ser sistematicamente utilizadas, como é por exemplo o caso do Kerberos (Stallings: 2000), mas têm tido pouco sucesso devido essencialmente a problemas de gestão, escalabilidade e ciclo de vida das chaves criptográficas. As soluções PKI permitem a criação de identidades e o estabelecimento da confiança a elas associada para processo de identificação e autenticação através da ligação entre a identidade de uma entidade e a sua correspondente chave pública, certificada por uma autoridade de confiança (CA). A gestão da encriptação de chave pública/ privada proporciona uma solução muito mais escalável que as suas congéneres anteriores.

IV. MODELOS DE CONFIANÇA

Os modelos de confiança baseados em PKI são importantes uma vez que permitem responder a questões tais como: em que certificados digitais é que uma entidade pode confiar? Como é que a confiança pode ser estabelecida e de que forma é que a confiança pode ser

controlada num determinado ambiente (Addams et al., 1999; Nash et al., 2001)?

Uma boa definição de confiança pode ser a seguinte: "*uma entidade A confia numa entidade B quando A assume que B irá ter um comportamento igual ao que A espera*" (Addams et al., 1999). A confiança é assim construída na base de suposições, expectativas e comportamentos, não podendo ser medida quantitativamente, pelo que existe sempre um risco associado com a mesma, o que implica que o estabelecimento de uma relação de confiança nem sempre pode ser um processo automático.

De seguida apresentam-se quatro dos tipos de modelos de confiança mais utilizados pelas PKI: Hierarquia de Autoridades de Certificação, Arquitectura Distribuída de Confiança, Modelo em Rede e Confiança Centrada no Utilizador (Addams et al., 1999; Nash et al., 2001).

A. HIERARQUIA DE AUTORIDADES DE CERTIFICAÇÃO

Este tipo de modelo pode ser representado como uma árvore invertida (raiz no topo e folhas na parte de baixo). A raiz desta árvore corresponde à Autoridade de Certificação (CA) raiz para o domínio inteiro da PKI. Abaixo desta CA podem existir zero ou mais CAs intermédias. As folhas desta árvore correspondem normalmente aos utilizadores finais[6] (Nash et al., 2001).

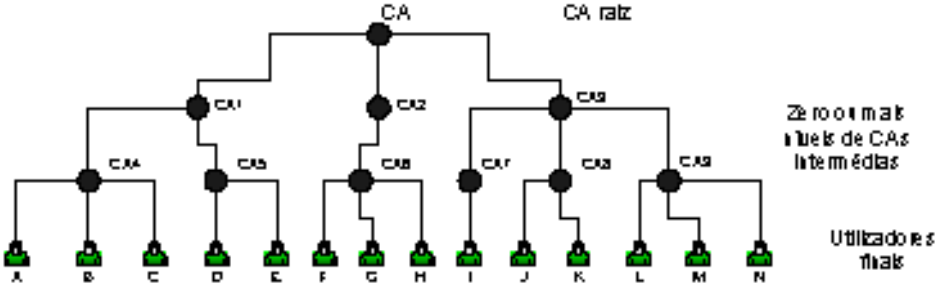

Figura 2 Hierarquia de Autoridades de Certificação

Neste modelo, todas as entidades na hierarquia confiam numa única CA de raiz. A hierarquia é estabelecida da seguinte forma:

1) A CA de raiz certifica zero ou mais CAs imediatamente abaixo dela;
2) Cada uma destas CAs certifica zero ou mais CAs imediatamente abaixo delas;
3) No final da hierarquia as CAs certificam utilizadores finais.

Como é que os utilizadores finais confiam uns nos outros? Por exemplo, como é que um utilizador 'A' confia no utilizador 'E' e vice-versa? O utilizador 'A' possui um certificado com o seguinte caminho de certificação (CA_4, CA_1, CA) e 'E' com (CA_5, CA_1, CA). Como no caminho de certificação de ambos existe uma CA em comum (CA_1) então ambos podem estabelecer confiança entre si. Em último caso esta procura poderia ascender até à CA raiz desta hierarquia.

Este modelo de confiança é o mais adequado para entidades com uma dimensão fixa (por exemplo, uma empresa) e menos adequado para ambientes mais vastos (por exemplo, a Internet). Um exemplo da aplicação deste modelo de confiança pode ocorrer por exemplo numa organização que esteja organizada por departamentos e secções. A organização possui uma CA de raiz que irá certificar cada uma das diversas CAs departamentais. Por sua vez, cada CA departamental pode ainda certificar várias CAs de secções da empresa, que por sua

[6] Por utilizadores finais, não se entenda apenas indivíduos (pessoas) como também entidades, software ou outros.

vez emitem certificados para os seus diversos colaboradores e aplicações. É, assim, possível estabelecer relações de confiança electrónica entre colaboradores de secções e departamentos diferentes da mesma organização, sem que estes tenham que se conhecer fisicamente.

B. ARQUITECTURA DISTRIBUÍDA DE CONFIANÇA

Ao contrário do anterior modelo de confiança, em que todas as entidades dependiam de uma única CA de raiz, neste modelo a confiança é partilhada e distribuída por várias CAs (Addams et al: 1999).

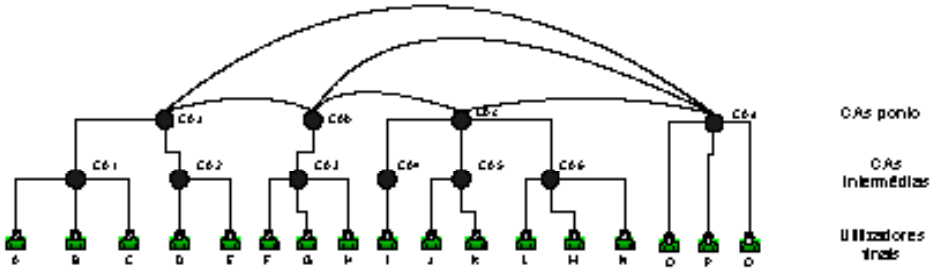

Figura 3 Hierarquia Distribuída de Confiança

O processo de interligação entre as diversas CAs ponto designa-se por certificação cruzada, em que ambas certificam a chave pública de cada uma delas. A certificação cruzada é um mecanismo extremamente útil para relacionar CAs que previamente não se encontravam de todo relacionadas.

Neste modelo podem ocorrer dois tipos distintos de certificação cruzada (Addams et al., 1999). No primeiro tipo, pode acontecer que todos os certificados das CAs de raiz são cruzados uns com os outros, dando origem a uma malha de certificações cruzadas (todos estão certificados de forma cruzada com todos). No segundo tipo cada CA de raiz efectua uma certificação cruzada com uma única CA central cuja função é a de facilitar a interligação entre as diversas CAs. Esta CA central pode ser interna ou externa às organizações e actua como uma "ponte" entre os sistemas PKI de organizações. A diferença entre esta configuração e a anterior é que cada CA apenas precisa de efectuar uma certificação cruzada com esta CA central.

Este modelo de confiança é, particularmente, adequado para o estabelecimento de relações electrónicas entre parceiros de negócio de diferentes organizações. Cada uma das organizações poderá ter um modelo de PKI organizado em hierarquia a funcionar internamente, mas quando ambas as organizações resolvem estabelecer relações de segurança electrónica entre si (por exemplo, clientes e fornecedores) torna-se necessário alterar o modelo de confiança. Assim, o modelo de confiança mais adequado para este caso é o de Hierarquia Distribuída de Confiança, pois através do cruzamento dos certificados das CAs raiz de cada uma das organizações irá permitir que utilizadores de uma organização possam confiar em outros utilizadores da outra organização, sem o prévio contacto físico entre ambos.

C. MODELO EM REDE

O modelo em rede deve o seu nome à *World Wide Web* e está dependente dos tradicionais *browser* de *Web* (Netscape Navigator e Microsoft Internet Explorer) (Nash et al., 2001).

Neste tipo particular de modelo, um determinado número de chaves públicas perten-

centes a CAs estão pré-instaladas nos *browsers*. Estas chaves definem o conjunto de CAs em que a utilização do *browser* inicialmente confia para funcionar como raiz para verificação dos certificados (Addams et al., 1999; Garfinlkel e Spafferd, 1997).

Embora este conjunto de chaves raiz possa ser alterado pelo utilizador, é reconhecido que poucos utilizadores dos *browsers* são suficientemente evoluídos para modificar estes aspectos de segurança do *browser*.

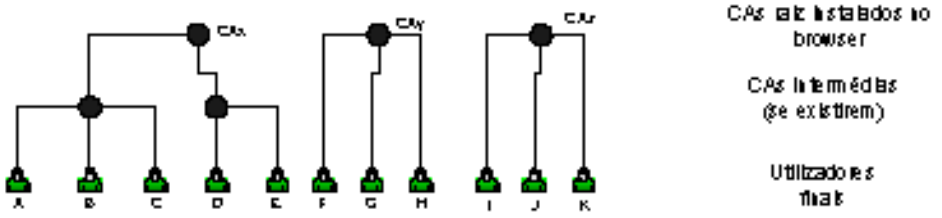

Figura 4 Modelo em Rede

O modelo em rede apresenta algumas vantagens em termos de conveniência e simplicidade. No entanto, existe um largo número de implicações de segurança com este modelo que devem ser tidos em consideração quando são tomadas decisões de implementação num determinado ambiente (Addams et al., 1999). Por exemplo, uma vez que os utilizadores de *browsers* confiam automaticamente num conjunto de chaves públicas pré-instaladas, a segurança poderá estar comprometida se uma destas CAs raiz for "má" o que levará o utilizador a confiar nela como se esta fosse "boa".

Outro dos potenciais problemas de segurança deste modelo é o de que não existe nenhuma forma fácil de revogar qualquer das chaves raiz embebidas no *browser*. Caso se descobrisse que uma das CAs era "má", ou que a correspondente chave privada havia sido comprometida, era quase impossível descontinuar a utilização dessa chave nos vários milhões de cópias dos *browsers* de *Web* espalhados pelo mundo.

Este é o modelo de confiança que está implementado no protocolo SSL/TLS[7] que é actualmente o que é mais utilizado na *World Wide Web* para segurar transacções electrónicas realizadas entre os *browsers* de *Web* e os servidores de *Web*. Este modelo permite que um utilizador de um *browser* de *Web* possa confiar num determinado servidor de *Web,* porque este possui um certificado instalado que foi emitido por uma CA cuja chave raiz está instalada no *browser* de *Web* do utilizador. Na prática, este é o actual mecanismo que faz com que eventuais compradores possam confiar em lojas electrónicas e na segurança da transmissão dos seus dados pessoais que podem incluir dados de pagamento.

Este modelo tem imenso sucesso, pois a sua utilização por parte do utilizador é totalmente transparente para este, e mesmo para quem deseja implementar lojas electrónicas os requisitos técnicos não são muito elevados.

Este tipo de modelo de confiança é mais utilizado para o Comércio Electrónico do tipo B2C, embora possam existir algumas variantes a este modelo.

D. CONFIANÇA CENTRADA NO UTILIZADOR

Neste modelo de confiança, cada utilizador é directa e totalmente responsável por decidir em que certificados confia e quais rejeita. Esta decisão pode ser influenciada por um número de factores, embora o conjunto inicial de chaves de confiança possa incluir as de amigos, familiares ou colegas que o utilizador conhece pessoalmente (Addams et al., 1999; Nash et al., 2001).

[7] Secure Sockets Layer/Transport Layer Security

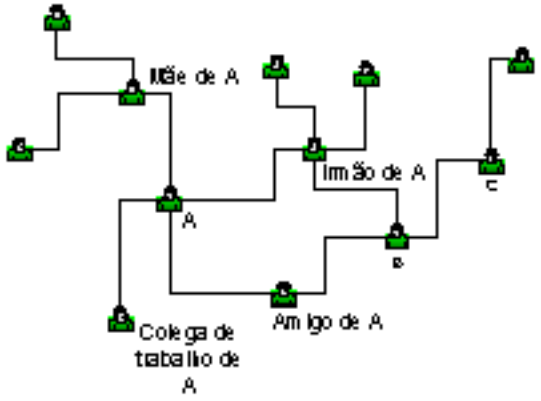

Figura 5 Modelo de Confiança Centrada no Utilizador

Por causa da dependência das acções e decisões dos utilizadores este modelo de confiança pode funcionar bem em comunidades científicas, mas é pouco realista para a comunidade em geral. Mais, este modelo é geralmente inapropriado para ambientes empresariais, financeiros ou governamentais uma vez que estes desejam exercer algum controlo sobre a confiança dos utilizadores. Estas políticas de confiança organizacional não podem de todo ser implementadas neste modelo de confiança.

O PGP ou Pretty Good Privacy (NetWork Associates: 2000), é uma ferramenta que se baseia neste modelo de confiança, e que foi criada por Phil Zimmermann para protecção dos dados pessoais.

Este modelo é adequado para ambientes em que os utilizadores já tenham estabelecido outro tipo de relação de confiança à priori, uma vez que são os utilizadores que decidem em quem confiam (numa organização pequena em que todos os utilizadores se conhecem pessoalmente). Apesar de ser igualmente fácil de estabelecer e de utilizar (embora menos transparente que o modelo anterior), não é muito adequado para utilização no Comércio e Negócio Electrónico.

A grande vantagem deste modelo, face ao anterior, reside no facto de que o mecanismo de estabelecimento de confiança não depende de entidades externas (como acontece no caso dos *browsers*), mas sim é deixado ao cuidado do próprio utilizador.

V. CONCLUSÕES

O Comércio e Negócio Electrónico é actualmente uma realidade que vem trazer importantes vantagens nas relações de confiança electrónicas que se estabelecem entre as várias entidades participantes: Consumidores, Empresas e Administração Pública. No entanto, e visto que neste meio electrónico sem existência de contacto físico entre os vários intervenientes é necessário estabelecer relações fortes de confiança, a resposta técnica adequada para este problema são as Infra-Estruturas de Chave Pública que são baseadas em criptografia assimétrica e em certificados digitais.

Os serviços baseados em infra-estruturas de PKI proporcionam a confiança electrónica necessárias, através de serviços e processos que incluem a Identificação, Autenticação, Autorização, Integridade, Privacidade, Confidencialidade e Não Repúdio. Estes serviços são proporcionados a pessoas e aplicações de uma forma totalmente transparente para os mesmos, o que vem reduzir significativamente os custos, normalmente, associados a implementações de outro tipo de soluções de segurança da informação.

Dos vários modelos de confiança mais comuns de PKI existentes, e que foram anali-

sados, verifica-se que nem todos são adequados para qualquer tipo de Comércio e Negócio Electrónico. De seguida, apresenta-se um quadro resumo que indica o tipo de modelo mais adequado para o estabelecimento de relações de confiança entre os diversos intervenientes no Negócio e Comércio Electrónico.

Tipo de Modelo	Tipo de CE e NE	Exemplo
Hierarquia de Autoridades de Certificação	B2B	Uma organização que deseje implementar uma estrutura PKI internamente: Raiz, Departamentos, Secções, Entidades Finais.
Arquitectura Distribuída de Confiança	A2B, B2A, B2B	Diferentes organizações que possuam estruturas PKI internamente e que desejem estabelecer relações de confiança entre si.
Modelo em Rede	B2C, C2B, C2A	SSL/TLS
Confiança Centrada no Utilizador	C2C	PGP

Tabela 1 Tipologia dos modelos de confiança PKI

Os modelos de confiança PKI apresentados permitem o estabelecimento de confiança entre as diversas entidades que detenham relações de Comércio ou Negócio Electrónico entre si, assim como o estabelecimento dos modelos mais adequados para o tipo de relação de confiança que se pretende estabelecer.

VI. BIBLIOGRAFIA

[1] Network Associates, (Set, 2000) "Introduction to Cryptography", *PGP 7.0*, Network Associates Inc.

[2] Addams, C., Lloyd, S., (1999) "Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations", Mac Millan Technicall Publishing.

[3] Baltimore Technologies, (2001)"Public Key Infrastructures - An Evaluation Guide", Baltimore Technologies Whitepaper.

[4] CommerceNet, (2000) "Barriers to Electronic Commerce - 2000 Study".

[5] Eng, T., (2000) "Certificate Authorities: The keys to E-Commerce?", PlanetIT, http://www.planetit.com.

[6] Garfinkel, S., Spafford, G., (1997) "*Web Security & Commerce: Risks, Technologies and Strategies*", O'Reilly & Associates, Inc.

[7] Gerck, E., (1998) "Towards a Real World Model of Trust: Reliance on Received Information", Meta Certificate Group, http://www.mcg.org.br.

[8] Keen, P., Ballance, C., Chan, S., Schrume, S., (2000) "*Electronic Commerce Relationships: Trust By Design*", Prentice Hall PTR.

[9] Nash, A., Duane, W., Joseph, C., Brink, D., (2001) "*PKI: Implementing and Managing E-Security*". Osborne McGrawHill.

[10] Norris, M., West, S., Gaughan, K., (2000) "*eBusiness Essentials: Technology and Network Requirements for the Electronic Marketplace*", John Wiley & Sons.

[11] Stallings, W., (2000) "*Networking Security Essentials: Applications and Standards*", Prentice Hall.

Contacto: carlos.serrao@iscte.pt; cordeiro.gomes@iscte.pt.