

# Arquitectura de Autenticação Baseada em Certificados para a Rede Telemática da Saúde (RTS)

Hélder Gomes<sup>1</sup>, André Zúquete<sup>2</sup>,  
João P. Silva Cunha<sup>3</sup>

<sup>1</sup> Escola Superior de Tecnologia e Gestão de Águeda - Universidade de Aveiro,  
Zona Industrial da Alagoa  
3754-909 Águeda, Portugal  
helder.gomes@estga.ua.pt

<sup>2</sup> IEETA / Universidade de Aveiro  
Campus Universitário de Santiago  
3810-193 Aveiro, Portugal  
avz@det.ua.pt

<sup>3</sup> Dep. Electrónica, Telecomunicações e Informática / IEETA / Universidade de Aveiro  
Campus Universitário de Santiago  
3810-193 Aveiro, Portugal  
jcunha@det.ua.pt

## Resumo

Neste documento apresenta-se uma arquitectura para identificar e autenticar profissionais de saúde num sistema de gestão de informação médica (Rede Telemática da Saúde – RTS). A arquitectura proposta, baseada em criptografia assimétrica e certificados digitais de chave pública, é independente dos mecanismos de identificação e autenticação dos profissionais nos restantes sistemas das suas instituições de origem. É também flexível e escalável, sendo capaz de suportar futuras adesões à RTS de forma simples e sem degradação de serviço.

## 1 Introdução

A segurança da informação é um dos aspectos fundamentais na sociedade de hoje. Isto é verdade para todas as áreas de actividade. No entanto, a área da saúde, dado o carácter privado e confidencial da informação clínica, é uma das áreas onde a segurança é particularmente importante.

A Rede Telemática da Saúde (RTS<sup>1</sup>) é um sistema que se aplica à área da saúde [1]. A segurança tinha que ser uma das suas principais vertentes, tendo sido considerada de raiz para uma melhor integração com as funcionalidades disponibilizadas [2,3].

A arquitectura proposta visa disponibilizar serviços de autenticação à RTS. Baseia-se em criptografia de chaves assimétricas e certificados digitais de chave pública, tecnologia actualmente disponível nos mais populares navegadores (*browsers*) e servidores *Web*. As principais características da arquitectura são a utilização de certificados digitais com intervalos de validade de curta duração, cadeias de certificação curtas e flexíveis e utilização de *smart cards* para armazenamento de certificados de confiança e armazenamento e uso das chaves privadas.

Este documento está organizado da seguinte forma: primeiro é feita uma muito breve apresentação da RTS (§2) e da sua arquitectura (§3). Depois são apresentados os requisitos para autenticação (§4), seguidos da apresentação da arquitectura proposta (§5). Por fim apresentam-se as conclusões (§6).

---

<sup>1</sup> <http://www.rtsaude.org>

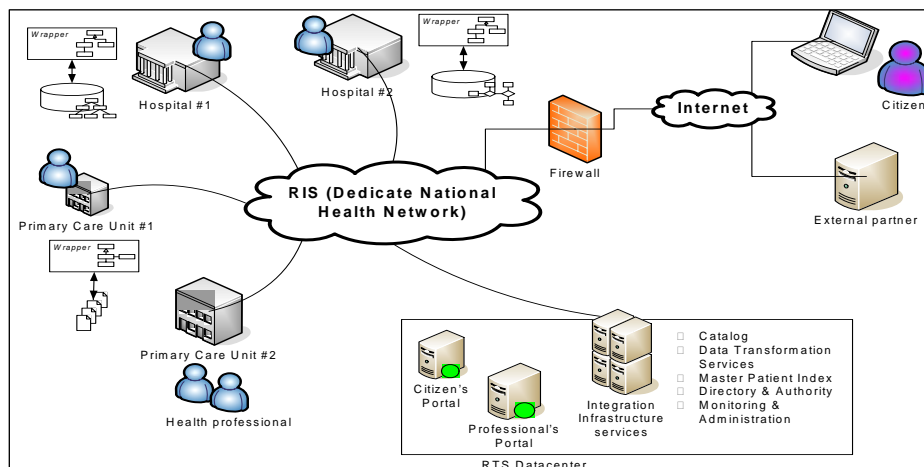


Figura 1: Arquitectura da RTS. Adaptado de [1]

## 2 Rede Telemática da Saúde

A Rede Telemática da Saúde (RTS) é um projecto que está a ser desenvolvido pela Universidade de Aveiro, com o apoio do programa Aveiro Digital, no qual participam o Hospital Infante D. Pedro de Aveiro (HIP), líder do consórcio, o Hospital Distrital de Águeda, a Sub-Região de Saúde de Aveiro, entre outros. Tem como grande objectivo potenciar a integração e a partilha da informação clínica disponível a nível regional [1]. O principal resultado dessa integração é o designado Processo Clínico Electrónico Regional, que agrega a informação clínica do utente, que pode estar dispersa por várias instituições, e potencia um importante conjunto de mais-valias, desde oferecer ao médico uma imagem mais completa do “perfil” do seu paciente, até evitar a duplicação da realização de meios complementares de diagnóstico. Pretende ainda melhorar a acessibilidade do utente aos serviços de saúde, permitindo a gestão da sua agenda de saúde, o que inclui a possibilidade de interagir com o seu médico assistente, de pedir de marcação de consultas, pedir renovação de receituário, entre outras [2,3].

## 3 Arquitectura da RTS

A Figura 1 apresenta um diagrama da arquitectura da RTS, onde podemos ver instituições de saúde (Hospitais e Unidades de Cuidados Primários), utentes e outras entidades externas, o *RTS Data Center* e a rede de comunicações, (RIS – Rede de Informação da Saúde), que interliga as várias instituições de saúde e sobre a qual se efectuará toda a comunicação RTS [1].

Várias entidades comunicam nesta arquitectura. Todas essas comunicações, seja entre entidades na mesma instituição, seja entre entidades em instituições diferentes, têm de ser seguras e sempre precedidas de autenticação mútua. Podemos considerar dois tipos de entidades a autenticar: (i) humanos, ou as máquinas que os representam, que vamos designar por Utilizadores, e (ii) os portais e restantes máquinas que implementam os serviços disponibilizados pelo RTS, que vamos designar por Serviços/Servidores (ver Figura 2).

Foram identificados os seguintes tipos de utilizadores: (i) Profissional (médico, médico chefe de serviço, enfermeiro, enfermeiro chefe de serviço e administrativo), (ii) Utente e (iii) Anónimo. As entidades externas não foram ainda consideradas nesta fase do projecto.

Cada um destes tipos de utilizador terá associado um conjunto de permissões para aceder à informação clínica. A informação acedida por cada um dos tipos de utilizador tem graus diferentes de sensibilidade, sendo a mais sensível a que é acedida por médicos, seguida, por ordem decrescente, da que é acedida pelos enfermeiros, administrativos, utentes e, por último, pelos anónimos. Naturalmente, quanto mais sensível for a informa-

ção, mais cuidados devem ser tomados para controlar o seu acesso, ou seja, existem necessidades de autenticação diferentes consoante o tipo de utilizador [2].

De um ponto de vista de implementação, uma característica da RTS é que é uma *Web Application*, ou seja, disponibiliza os seus serviços aos utilizadores através de uma interface *Web*, acessível através de qualquer navegador, e a comunicação entre os seus servidores é realizada através de *Web Services* [1].

#### 4 Requisitos de Autenticação

Um requisito de autenticação é que ela seja forte, ou seja, não deve ser fácil a uma entidade fazer-se passar por outra (personificação), principalmente quando a sensibilidade da informação passível de ser acedida pela entidade a autenticar é elevada. Deverá ainda poder adaptar-se a diferentes graus de sensibilidade, uma vez que nem todas as entidades acedem a informação sensível.

A solução de autenticação tem de suportar um ambiente heterogéneo em termos de tecnologias usadas. Uma vez que na RTS intervêm várias instituições, além dos utilizadores que podem aceder do exterior (Internet), impor requisitos em termos de tecnologias a usar, nomeadamente sistemas operativos, é contraproducente. Terá ainda que fazer a autenticação de servidores e serviços, além da autenticação de utilizadores.

Devido à participação de várias instituições, não existe um registo centralizado dos utilizadores, pelo que a solução terá que ser capaz de lidar com essa distribuição. Terá mesmo de ser capaz de fazer a autenticação de uma entidade, ainda que não haja, pontualmente, comunicação com a sua instituição de origem.

Em geral, a autenticação não deve ser um obstáculo à utilização do sistema; deve ocorrer de forma o mais transparente possível, mas sempre cumprindo a sua função. Assim, uma característica de interesse para a RTS é potenciar a mobilidade dos Profissionais, principalmente médicos e enfermeiros. A deslocação de um médico dentro da sua instituição, ou mesmo a uma outra instituição participante, não deverá ser impeditiva do seu acesso aos serviços da RTS. Significa isto que deverá ser possível autenticar Profissionais de uma instituição participante a partir de outra instituição participante, mesmo que, pontualmente, não exista comunicação com a sua instituição de origem.

A auditoria é algo de fundamental em sistemas de segurança. Daí ser imperativo o registo de todas as operações que envolvam autenticação.

Por fim, deve ser flexível e escalável, permitindo uma fácil integração de outras instituições que venham a aderir à RTS, bem como o aumento significativo de utilizadores nas instituições actuais, sem degradação relevante de desempenho.

#### 5 Arquitectura de Autenticação

Face aos requisitos de autenticação atrás indicados, a solução que nos pareceu mais adequada foi a autenticação através de pares de chaves assimétricas e certificados digitais das chaves públicas. Trata-se de uma tecnologia já bastante vulgarizada, baseada em criptografia de chaves assimétricas, sendo suportada pelos navegadores e servidores *Web* mais populares.

Para a gestão e suporte dos certificados será necessária uma infra-estrutura de chave pública, vulgarmente designada pela sigla PKI (*Public Key Infrastructure*) [4]. Uma PKI é um sistema composto de certificados digitais, entidades de certificação (CA – *Certification Authorities*), repositórios de certificados, listas de certifi-

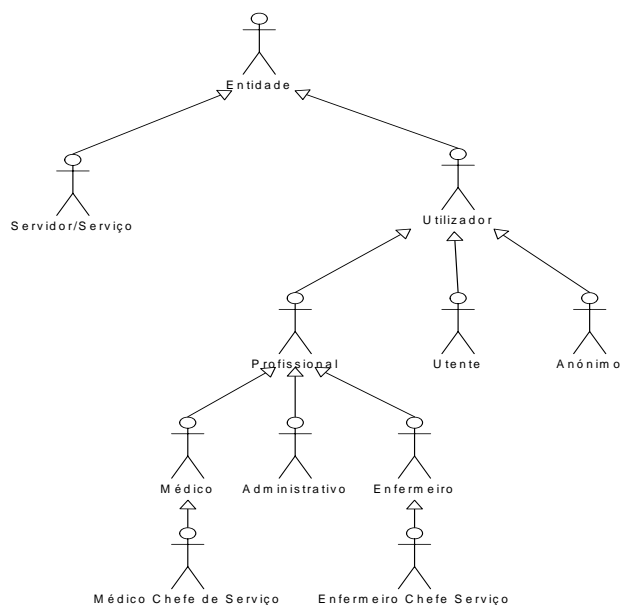


Figura 2: Tipos de Entidades

cados revogados (CRL – *Certificate Revocation List*), documentos públicos onde se declaram o modo como a CA e os certificados são geridos, graus de confiança, responsabilidades legais, etc.

Para a RTS propõe-se uma PKI simplificada baseada numa arquitectura inicialmente proposta para resolver o problema da autenticação de utilizadores em conjuntos de instituições de universitárias [5,6]. Esta arquitectura baseia-se em (i) certificados digitais com períodos de validade de curta duração e (ii) certificação cruzada entre instituições para a criação de cadeias de validação.

Para tornar a solução mais robusta recorre-se a *smart cards* para o armazenamento e protecção de chaves privadas e certificados raiz confiáveis. A sua adopção foi fundamentalmente concebida para a autenticação de Profissionais, e não necessariamente dos Utentes. A autenticação destes últimos, dada a menor sensibilidade da informação por eles acedida, será feita através do habitual nome de acesso (*login*) e senha (*password*).

## 5.1 Porquê certificados?

Como é referido em [1], a RTS é uma aplicação que disponibiliza os seus serviços aos utilizadores através de Portais com interface web (servidores web). Para que o Portal possa fornecer os serviços adequados ao profissional, necessita de fazer a sua autenticação e determinar qual a sua instituição de origem e qual a sua função. Os mecanismos disponíveis para a identificação e autenticação do profissional, utilizando um navegador (*browser*), em servidores web são (i) nome e senha (*login* e *password*) ou (ii) certificados digitais.

A utilização de nome e senha é o método de autenticação de utilizadores mais vulgar nas Instituições de Saúde [7]. É no entanto conhecida a dificuldade dos humanos em lidar com este tipo de autenticação, que se manifesta em *passwords* “fáceis”, anotadas em papel, repetidas, etc. Em [7] são indicadas algumas destas situações de fragilidade detectadas em Instituições de Saúde, e sugere-se a sensibilização dos utilizadores e a definição de políticas de *passwords* para tentar limitar esta dificuldade e melhorar a segurança. No entanto, estas medidas não resolvem totalmente a insegurança associada a este método. Além disso, para o portal obter a restante informação do utilizador que necessita, teria de (i) ter um serviço de directoria com a informação de todos os utilizadores RTS ou (ii) ir obter a informação à instituição de origem do utilizador.

Na primeira situação estaria claramente a replicar a informação de directoria de todas as instituições participantes na RTS. Na segunda implicaria que a RTS tivesse acesso *online* à informação de directoria nas várias Instituições de Saúde, o que teria imediato impacto em termos de atrasos no início da disponibilização do serviço. A utilização de *kerberos* [8] ou LDAP [9] poderiam implementar a validação remota.

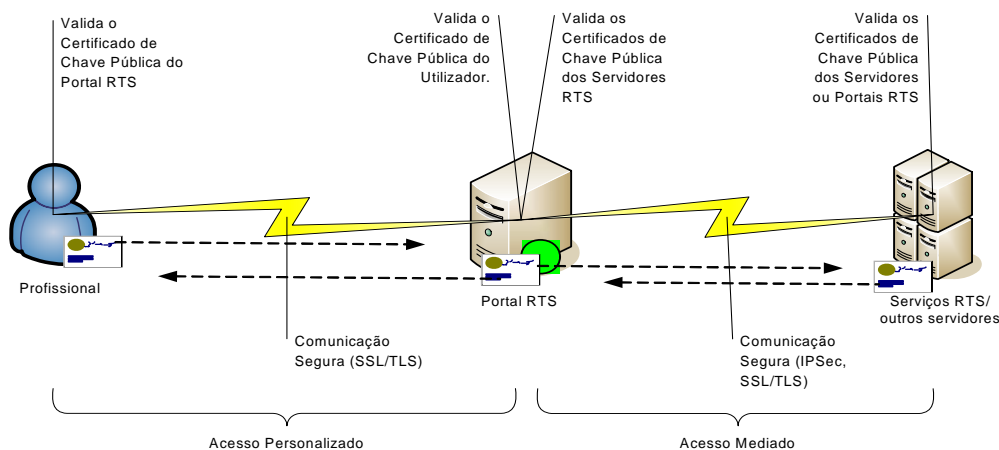
A utilização de certificados para a autenticação dos utilizadores permite que a sua validação seja feita localmente sem necessidade de acesso a informação remota. Para isso, basta que o certificado além de possuir a identificação do seu proprietário possua também informação acerca da sua instituição de origem e da sua função, e que tenha um período de validade tal que permita prescindir da verificação da sua revogação. Desta forma, se cada instituição emitir os certificados para os seus profissionais, para efectuar a validação não são necessários nem o repositório com a identificação de todos os utilizadores da RTS nem a comunicação *online* com o serviço de directoria da IS.

Se, adicionalmente, a chave privada e o correspondente certificado digital forem armazenados num *smart card* protegido com um código de acesso, reforça-se ainda mais a segurança da autenticação, uma vez que introduz um novo factor de autenticação: a posse do *smart card*. Ou seja, para o Profissional se identificar tem que possuir o seu *smart card* e indicar o seu código de acesso, o que é considerado uma solução de autenticação forte.

## 5.2 Modelo de Comunicação

A Figura 3 apresenta o modelo de comunicação e autenticação na RTS. Pressupõe-se que cada uma das entidades comunicantes obteve previamente um par de chaves assimétricas e respectivo certificado digital de chave pública emitido pela instituição a que pertence.

Como se pode verificar, a comunicação entre o Profissional e o Portal da RTS é uma comunicação personalizada, no sentido em que o profissional se autentica, enviando o seu certificado ao Portal. Este, depois de validar o certificado, e em função de informação contida no certificado, determina e aplica as autorizações adequadas para o tipo de Profissional.



**Figura 3: Modelo de comunicação e autenticação**

A comunicação entre o Portal e outros serviços, ou servidores, é mediada, no sentido em que o Profissional que requisitou a informação não se autentica neste troço. O Portal é o responsável pelo pedido e por garantir que não fornece ao Profissional mais informação do que aquela a que ele pode aceder. No entanto, continua a haver autenticação das entidades (Serviços/Servidores) envolvidas na comunicação e o estabelecimento do canal seguro de comunicação para garantir que a informação não é acedida por entidades não credenciadas para o acesso. De notar que, para obter a informação pretendida, pode ser necessário recorrer a vários serviços em cadeia, sendo contudo aplicado sempre o modelo de autenticação entre servidores.

A identificação subjacente à autenticação é feita através da troca de certificados entre as entidades. Cada uma delas terá que validar o certificado da outra e apenas prosseguir na comunicação se os certificados de ambas forem válidos, ou seja, foram emitidos por entidades de confiança e estão dentro do intervalo de validade. No caso do Portal, terá ainda que garantir que o certificado do utilizador corresponde a um tipo de utilizador válido. Após esta autenticação deve ser estabelecido um canal de comunicação seguro por onde fluirá toda a comunicação posterior.

No caso da comunicação entre Utente e Portal, em que o Utente não possui certificado, o modelo é semelhante, com a diferença de que não há envio do certificado do Utente para o Portal. No entanto, o Utente recebe o certificado do Portal e deve proceder à sua validação para estabelecer o canal seguro e prosseguir na comunicação. Depois de estabelecido o canal seguro, o Portal pede ao Utente para se identificar e autenticar através de um ecrã para introdução do respectivo nome de acesso e senha.

A tecnologia a usar na comunicação entre um profissional e o Portal RTS será tipicamente HTTP sobre SSL/TLS (HTTPS) [8] e entre Portal RTS e os Servidores institucionais será HTTPS ou IPSec [11].

### 5.3 Requisitos dos Certificados

Cada entidade, Profissional ou Serviço/Servidor, terá um par de chaves assimétricas e um certificado digital de chave pública, emitido pela sua instituição de origem, que lhe permitirá ser autenticada na RTS.

O certificado de um Profissional deve conter claramente identificado o seu possuidor (para quem ele foi emitido), a sua instituição de origem (que emitiu o certificado), o tipo de Profissional (médico, enfermeiro, etc.). É através deste conjunto de informação que o Portal RTS infere as permissões associadas ao Profissional. Desta forma, ao utilizar o certificado de identificação para transportar toda a informação necessária para inferir a autorização do Profissional, simplifica-se significativamente o sistema de autorização.

#### 5.3.1 Tipos de Certificados de Profissionais

Os certificados a utilizar obedecem ao formato X.509 versão 3 para utilização na Internet [12]. Como, para além da identificação da entidade e da instituição emissora, é necessário que o certificado contenha a informação sobre o tipo de utilizador, haverá necessidade de utilizar as extensões previstas na versão 3 do formato

X.509. Assim, será utilizada a extensão EKU (*Extended Key Usage*), para a qual será necessário definir OIDs (*Object Identifiers*) para cada um dos tipos de Profissional identificados na Arquitectura da RTS. Os OIDs são identificadores universais e são geridos pela IANA<sup>2</sup>, onde se pode fazer a sua reserva de forma gratuita.

### 5.3.2 Armazenamento dos Certificados e Chaves Privadas

As técnicas de autenticação são baseadas (i) naquilo que se sabe, (ii) naquilo que se possui, (iii) naquilo que se é ou (iv) em combinações das três anteriores.

O método mais comum de autenticação de pessoas, através de nome e senha, é um exemplo de uma autenticação baseada apenas num factor: algo que se sabe. É considerado um método de autenticação fraco porque, além de depender apenas de um factor, é conhecida a dificuldade dos seres humanos em lidar com senhas robustas (por exemplo, resistentes a ataques de descoberta com dicionários).

Um exemplo de autenticação mais forte, baseado em dois factores, é o que acontece nos terminais ATM da rede Multibanco ou nos telemóveis GSM [13]. A pessoa, para se autenticar, tem de conhecer um segredo, o PIN, e tem de estar na posse de um cartão (Multibanco ou SIM), ou seja, a autenticação é efectuada com base em algo que se sabe e em algo que se possui. Obviamente, a robustez da autenticação está associada ao número de factores de autenticação: quanto maior o número de factores, maior a robustez. Tipicamente, quando se exige uma maior segurança na autenticação utilizam-se sistemas baseados em dois factores, apesar de já existirem sistemas baseados em três.

A utilização de *smart cards* para o armazenamento das chaves privadas e respectivos certificados de chave pública permitem autenticação baseada em dois factores, uma vez que para se autenticar o utilizador tem de estar na posse do cartão e ter conhecimento do código de activação do mesmo, um PIN.

Uma outra vantagem dos *smart cards* é possuírem no seu interior um processador criptográfico que permite a geração e utilização do par de chaves no seu interior, impedindo que a chave privada saia para o exterior. Desta forma, garante-se a exclusividade das chaves privadas no *smart card*, o que permite a sua utilização para produzir assinaturas digitais. Esta característica é ainda fundamental para o aumento do grau de segurança global desta arquitectura, uma vez que elimina os riscos de comprometimento da chave privada nas máquinas dos utilizadores devidos a vírus, *spywares*, etc.

Os *smart cards* têm como desvantagem o aumento do custo de implementação do sistema, uma vez que é necessário dotar os computadores utilizados pelos Profissionais de leitores de *smart cards*. Uma hipótese alternativa é fornecer os *smart cards* em *dongles* com interface USB, o que evita a aquisição dos leitores mas acarreta um maior custo por unidade.



**Figura 4: Exemplo de smart card e leitor USB dongle (OMNIKEY CardMan)**

Na escolha dos *smart cards*, deve-se ter em conta o aspecto da mobilidade entre instituições de saúde. O problema está na disponibilidade dos *drivers* e *software* para os ler nas máquinas usadas pelos Profissionais. Como instituições diferentes podem adquirir *smart cards* de diferentes fabricantes, há sempre o risco de o Profissional de uma instituição não conseguir utilizar o seu *smart card* noutra instituição. Versões mais recentes do Windows já trazem instalado software para lidar com *smart cards* de alguns dos maiores fabricantes (v.g., Schlumberger, Gemplus e Infineon [14]).

---

<sup>2</sup> <http://www.iana.org>

A utilização de *smart cards* poderá ainda potenciar medidas extra de segurança não directamente relacionadas com a autenticação RTS, nomeadamente a realização de *login* através da introdução do *smart card* e o bloquear ou desligar de sessão do sistema operativo com o remover do *smart card*.

### 5.3.3 Tempo de Vida dos Certificados

Um dos aspectos fundamentais numa PKI é a gestão das listas de certificados revogados (CRL) [4]. Estas identificam todos os certificados que por alguma razão foram revogados e são publicadas com uma periodicidade previamente anunciada. Devido ao seu carácter periódico, têm uma janela de risco que é no máximo igual ao tempo que medeia entre duas publicações sucessivas. Este intervalo pode, nalgumas implantações, ter a duração de dias. Tem ainda associado o custo da sua gestão, desde a recepção da informação de comprometimento do certificado até à infra-estrutura para a sua disponibilização.

Para simplificar a gestão da PKI a utilizar na RTS, optou-se pela utilização de certificados com intervalos de validade de curta duração para a autenticação dos Profissionais e desta forma prescindir da utilização de CRLs, ou outros mecanismos, para lidar com a revogação dos certificados dos profissionais, tal como em [5]. A sua curta duração deve resultar de uma ponderação sobre o risco associado ao seu tempo de vida, e certamente será objecto de afinação em resultado da experiência acumulada após a entrada em funcionamento do sistema. A janela de risco do certificado é no máximo igual ao seu intervalo de validade, ou seja, é o máximo intervalo de tempo em que o certificado pode ser usado de forma mal intencionada, em caso de transvício. No entanto, é necessário não esquecer que o certificado, e respectiva chave privada, estão armazenados dentro de um dispositivo criptográfico (*smart card*) que bloqueia após um certo número de tentativas falhadas, o que dificulta ainda mais a sua utilização mal intencionada.

Quais são, então, as vantagens dos certificados de curta duração?

Por um lado, é mais simples fazer com que os Profissionais se autenticem frequentemente e obtenham um par de chaves e respectivo certificado, do que gerir a lista de certificados revogados.

Uma outra vertente tem a ver com a utilização do certificado para a RTS inferir sobre a autorização. Uma das dificuldades na utilização de certificados de autenticação para transporte de informação de autorização reside na sincronização da informação de permissão no certificado com o nível de permissões que o utilizador efectivamente possui quando o usa. Por exemplo, em certificados com intervalos de validade de um ano, uma alteração nas permissões implica a revogação do certificado e a obtenção de um novo. Com a utilização de certificados de curta duração, este pode ser escolhido de forma a poder ter um grau de sincronização adequado. Para os tipos de utilizadores identificados esta questão coloca-se apenas em relação ao ser ou não chefe de serviço.

Para os certificados emitidos para Serviços/Servidores não são aconselháveis intervalos de validade curtos. Isto porque, como estão em ambiente controlado, o risco de comprometimento é muito menor. Além disso, em caso de dificuldade na renovação dos certificados, haveria o risco de estes expirarem e os servidores ficarem inacessíveis até ao refrescamento das chaves e certificados. Isto implica que para este tipo de certificados seja necessário gerir uma CRL.

### 5.3.4 Emissão e Renovação de Certificados e Chaves

Os profissionais irão utilizar um *smart card* para o armazenamento das suas chaves privadas e respectivos certificados de chave pública. A entrega do *smart card*, com as chaves e certificados iniciais, deve ser presencial, ou seja, deverá ser entregue em mão após a validação da identidade do profissional.

Posteriores refrescamentos de chaves e certificados devem ser feitos da forma mais automática e transparente possível para o profissional, ainda que segura. Esta renovação pode ser efectuada, por exemplo, (i) utilizando as credenciais prestes a expirar para assinar o pedido de renovação ou (ii) através de um sítio na *Web* que exija identificação segura do utilizador sem para o efeito usar as credenciais, já inválidas, contidas no *smart card*.

Para garantir o refrescamento de chaves e certificados dos Profissionais com mobilidade inter-instituições, é necessário que estes tenham acesso à CA da sua instituição a partir da instituição onde se encontram.

Quanto aos certificados dos Serviços /Servidores, apesar terem intervalos de validade maiores, podem ser objecto da mesma política de emissão e renovação de chaves e certificados.

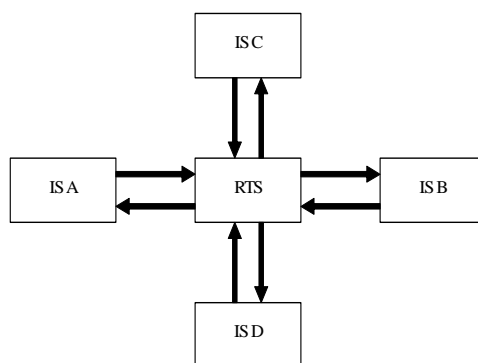


Figura 5: Modelo de confiança para a RTS

#### 5.4 Modelo de confiança

O modelo de confiança proposto para a RTS é apresentado na Figura 5. Neste modelo, cada uma das Instituições de Saúde (IS) participantes na RTS é a responsável pela emissão e gestão dos certificados para as suas entidades. É desta forma que se determina a instituição de origem da entidade possuidora de um certificado.

Para o estabelecimento de confiança mútua entre cada uma das IS e a RTS, e possibilitar que os certificados emitidos por cada uma das IS sejam válidos na RTS, e vice-versa, constitui-se uma estrela de certificações cruzadas na qual a RTS ocupa a posição central e as extremidades são ocupadas pelas Instituições de Saúde (IS) participantes na RTS. A certificação cruzada é feita individualmente com cada IS e consiste na emissão de um certificado pela RTS para a IS e na emissão de um certificado pela IS para a RTS.

De notar que o papel da RTS não é funcionar como uma ponte de confiança (*bridge*) entre as várias IS. Apenas pretende estabelecer uma relação de confiança com cada uma delas individualmente. Além disso, não é necessária a existência de laços de confiança entre as várias IS. No entanto, ela poderá eventualmente existir por outras razões alheias à RTS.

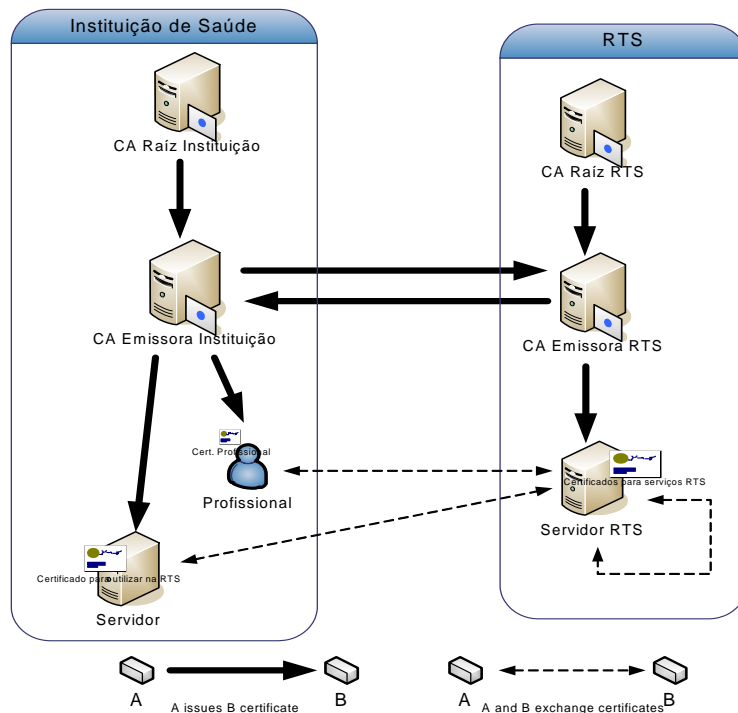
Cada IS é responsável pela emissão dos certificados para as suas entidades (Profissionais e Serviços/Servidores). Caso alguma IS já possua uma PKI em funcionamento preconiza-se a sua reutilização para a emissão dos certificados para a RTS, desde que estes estejam de acordo com os requisitos enunciados em 5.3 e que a emissão de certificados seja feita pelos serviços de pessoal da IS após identificação presencial do profissional. Para as restantes IS, sugere-se a implementação de uma hierarquia de CAs com pelo menos dois níveis, tal como se mostra na Figura 6. Notar que a implementação da hierarquia de CAs não interfere com os mecanismos de autenticação dos restantes sistemas da IS, que podem continuar a ser utilizados sem alterações. O mesmo modelo é proposto para a CA da RTS.

Por uma questão de simplicidade de representação, na Figura 6 apenas se encontram a hierarquia de CA da RTS e de uma Instituição de Saúde (IS), ambas de acordo com o modelo proposto. Para estender o modelo para suportar várias IS, basta criar réplicas da CA da IS, uma por cada nova IS.

No primeiro nível da hierarquia da IS encontra-se a CA raiz, ou de topo, que é a raiz de confiança para os certificados da IS. Possui um certificado auto-assinado e apenas emite certificados para as entidades certificadoras do nível seguinte. Por medida de segurança, na máquina da CA raiz apenas devem estar instalados os serviços estritamente necessários ao seu funcionamento. Depois de emitir os certificados para as CA do nível seguinte, deve ser desligada (*power off*) e mantida em local seguro para evitar ao máximo o risco de comprometimento da sua chave privada.

Debaixo da CA raiz, e com certificados por ela emitidos, encontram-se as CA Emissoras, responsáveis pela implantação das políticas de certificados e pela emissão de certificados (ver Figura 6) para as suas entidades, e que devem estar sempre activas (*power on*) e contactáveis.

Caso IS tenha necessidade de emitir certificados para qualquer outro fim, e sujeitos a uma política diferente, então, debaixo da sua CA raiz poderá possuir outras CA, eventualmente com mais de 2 níveis. Para a RTS não se vislumbra a necessidade de uma hierarquia de CAs com mais de dois níveis.



**Figura 6: Arquitectura interna das CA**

A certificação cruzada para o estabelecimento de confiança entre a RTS e a IS é feita entre as CA Emissoras da RTS e da IS, que assinam os certificados uma da outra: a CA Emissora da RTS emite um certificado para a CA Emissora da IS, e fica com uma cópia, e a CA Emissora da IS emite um certificado para a CA Emissora da RTS e fica com uma cópia. Desta forma, possibilita-se que uma entidade ao validar um certificado alheio utilize sempre como âncora de confiança o certificado de raiz da sua instituição de origem (RTS ou IS).

A razão para efectuar a certificação cruzada a nível das CA Emissoras e não das CA raiz é (i) limitar o âmbito da confiança entre as entidades, que se pretende apenas para os certificados a usar na RTS, e (ii) limitar danos em caso de quebra de confiança na outra instituição, uma vez que a publicação da CRL da CA Emissora é mais frequente que a da CA raiz, que está *offline*.

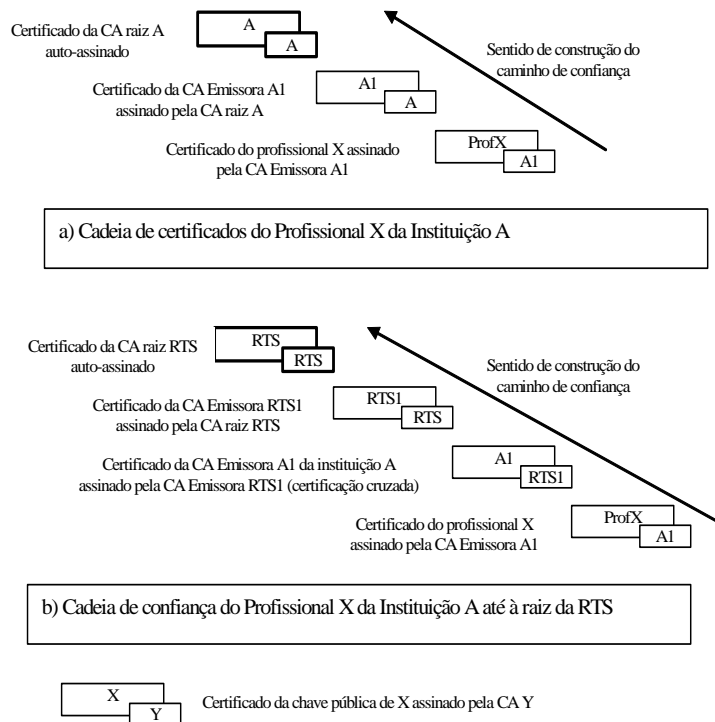
A escalabilidade em termos da adesão de novas IS à RTS implica mais extremidades na estrela de confiança, uma por cada IS, ou seja, a implementação uma hierarquia de CAs com certificação cruzada com a RTS, nos moldes atrás indicados.

## 5.5 Validação dos Certificados

Quando se inicia uma interacção na RTS, as entidades devem-se autenticar através da troca dos respectivos certificados digitais e de assinaturas digitais realizadas com a correspondente chave privada. Significa isto que cada uma delas deve validar o certificado e a assinatura da outra e prosseguir a comunicação apenas quando conclui que a outra parte é de confiança.

Uma entidade deve fazer as validações de certificados tendo como única âncora, ou raiz, de confiança o certificado de raiz da sua própria instituição. Para isso vai tentar construir o caminho ou cadeia de confiança que liga a entidade emissora do certificado a validar até ao certificado da raiz da sua instituição. A validação do certificado recebido implica a validação de todos os certificados da cadeia de confiança construída.

Na Figura 7 mostra-se um exemplo de validação de um certificado e respectiva cadeia de confiança. Nele, para validar o certificado de um Profissional de uma Instituição de Saúde A, o Portal RTS vai tentar construir o caminho de confiança desde a CA emissora do certificado do Profissional até ao certificado raiz da RTS, o único em que confia. No entanto, como se pode ver na Figura 7-a), o caminho de confiança do certificado do Profissional termina no certificado raiz da sua instituição de origem (IS A), na qual o Portal da RTS não confia,



**Figura 7: Construção de cadeia de confiança**

o que o impede de considerar o certificado válido.

A certificação cruzada intervém na construção de uma cadeia de certificação válida que termine no certificado de raiz da RTS. Como se pode ver na Figura 7-b), devido à certificação cruzada existe um certificado assinado pela CA Emissora da RTS (RTS1) a atestar a confiança na CA Emissora da IS A (A1) e, deste modo, a proporcionar um caminho de confiança até ao certificado raiz da RTS.

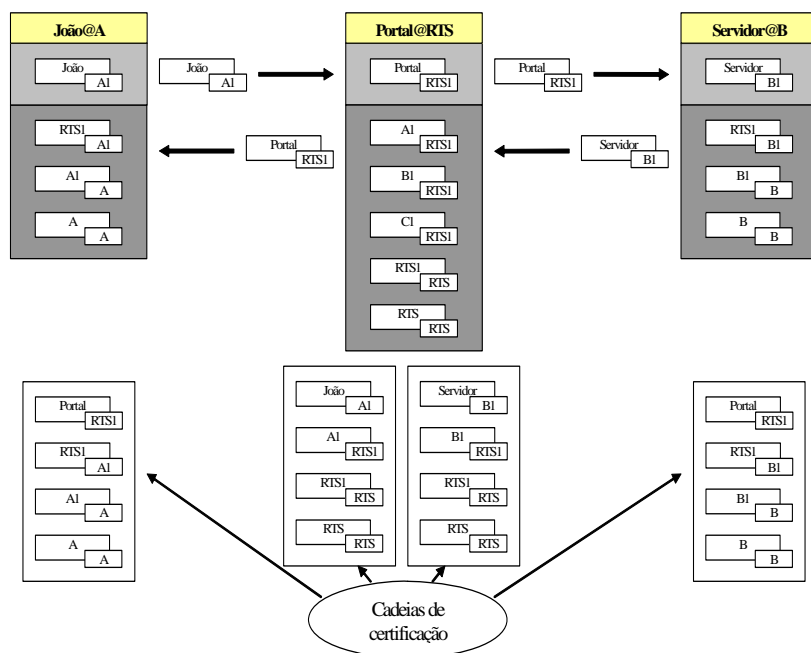
Para a validação do certificado do Portal da RTS pelo Profissional da IS acontece um processo semelhante, só que o certificado a validar é emitido pela CA Emissora da RTS e a âncora de confiança do Profissional é o certificado de raiz da sua instituição, Instituição A.

O problema com as certificações cruzadas é a dificuldade em obter de forma automática esses certificados. Assim é recomendável que todas as entidades que participam nas interações RTS estejam na posse dos certificados necessários para a construção das cadeias de confiança dos certificados das IS com as quais interagem. Isto implica que um Profissional terá que transportar no seu *smart card* o seu certificado, os certificados da sua cadeia hierárquica, no caso presente dois (CA Emissora e CA raiz), e o certificado da certificação cruzada em que a CA Emissora da sua IS assina a chave pública da CA Emissora da RTS.

No caso dos Portais e restantes servidores da RTS que necessitem de validar certificados emitidos pelas IS, têm de possuir todos os certificados cruzados emitidos pela RTS para as várias IS, além dos certificados da cadeia hierárquica da RTS.

A Figura 8 mostra um exemplo de uma possível interação da RTS. Na interação participam (i) o Profissional João, que pertence à Instituição de Saúde A, (ii) um Portal da RTS e (iii) um Servidor da Instituição de Saúde B. O Profissional João vai fazer um pedido ao Portal sobre dados que se encontram num Servidor da Instituição B. A figura mostra os certificados que têm que estar na posse de cada entidade, bem como as cadeias de certificação que cada entidade constrói para validar os certificados recebidos dos seus interlocutores. (Nota: O certificado C1 emitido pela CA RTS1 que está na posse do Portal não participa na transação e ilustra apenas que o Portal tem de estar na posse de cópias dos certificados cruzados com todas as instituições participantes na RTS).

A vantagem desta solução é que o Profissional tem de transportar um número reduzido de certificados, o que é relevante porque os *smart card* têm um espaço reduzido de memória, cabendo aos servidores ter de estar na posse de um número possivelmente grande de certificados (todos os certificados cruzados emitidos pela



**Figura 8: Exemplo de possível interação RTS. O profissional João da Instituição A faz um pedido ao portal da RTS para obter dados num servidor da Instituição C**

RTS). Notar que quanto maior for a profundidade da hierarquia de CAs das IS maior será o número de certificados que um Profissional dessa IS tem de transportar no seu *smart card*.

## 6 Conclusão

Neste documento descrevemos a proposta de uma arquitectura para a autenticação na RTS baseada em criptografia assimétrica e certificados de chave pública. Esta arquitectura satisfaz todos os requisitos apresentados:

- Autenticação forte dos profissionais através da utilização de chaves privadas armazenados em *smart cards* activados por um código e certificados digitais de chave pública.
- Comunicação segura entre as entidades (confidencialidade).
- Mobilidade dos profissionais ao possibilitar a sua autenticação na IS de origem e nas restantes IS participantes na RTS, com iguais procedimentos.
- Capacidade de operação numa grande variedade de sistemas operativos e aplicações por utilizar tecnologia bastante vulgarizada.
- Solução escalável onde facilmente se acomodam mais instituições de saúde e mais utilizadores.

A arquitectura caracteriza-se pelos seguintes aspectos fundamentais:

- Cada Instituição de Saúde emite os certificados digitais para os seus Profissionais
- Utilização de certificados digitais com intervalos de validade curtos.
- Utilização de *smart cards* pelos Profissionais para o armazenamento das suas chaves privadas e dos seus certificados de confiança.
- Recurso à certificação cruzada entre a RTS e as várias IS para a criação de uma plataforma de confiança.

As principais vantagens da arquitectura são:

- Modelo uniforme de autenticação de profissionais na RTS que é independente dos mecanismos e políticas de autenticação de profissionais nas IS.

- Autenticação forte baseada em dois factores: *smart card* e PIN.
- Elevado grau de segurança das chaves privadas e certificados de confiança.
- Utilização por parte das entidades de uma única raiz de confiança, a da sua instituição de origem.
- Necessidade de transporte de poucos certificados de confiança por parte dos profissionais para validarem os certificados da RTS.
- Certificados dos profissionais com informação de identificação e de informação para se inferir a respectiva autorização.
- Garantia de actualidade da informação para inferir a autorização nos certificados dos profissionais.
- Prescindir da gestão de CRLs para os certificados dos profissionais.

Esta arquitectura está neste momento a ser implementada num protótipo da RTS que irá interactivar com a IS HIP (Hospital Infante D. Pedro, Aveiro). A CA está a ser implementada utilizando os Certificate Services do Windows Server 2003 Enterprise Edition, acedendo aos serviços do Active Directory para a validação dos profissionais para efeitos de emissão de certificados. Os servidores RTS estão a ser implementados em Red-Hat Linux, com o servidor de aplicações Tomcat.

## 7 Agradecimentos

Os autores agradecem a colaboração e apoio prestado por toda a equipa de desenvolvimento da RTS, que foi fundamental para a realização deste trabalho.

## 8 Referências

1. João P. S. Cunha, Isabel Cruz, Ilídio Oliveira, António S. Pereira, César T. Costa, Ana M. Oliveira, and Amândio Pereira. The RTS Project: Promoting secure and effective clinical telematic communication within the Aveiro region. In eHealth 2006 High Level Conference, Malaga, Spain, May 2006.
2. Carlos Costa, Ilídio Oliveira, Isabel Cruz, Jacek Kustra, João P. Cunha, Jorge Moura, and Licínio Mano. Relatório de planeamento estratégico de sistemas de informação, November 2005. <http://www.rtsaude.org>.
3. Isabel Cruz, João P. Cunha, Licínio Mano, Daniel Polónia, Ilídio Oliveira, and Pedro Soares. Relatório de análise de processos e fluxos de informação, April 2005. <http://www.rtsaude.org>.
4. PKIX Working Group. Public-Key Infrastructure (X.509) (pkix). <http://www.ietf.org/html.charters/pkix-charter.html>.
5. Carlos Ribeiro, Fernando Silva, and André Zúquete. A Roaming Authentication Solution for Wifi using IPSec VPNs with client certificates. In TERENA Networking Conference 2004, Rhodes, Greece, June 2004.
6. André Zúquete and Carlos Ribeiro. A flexible, large-scale authentication policy for WLAN roaming users using IPSec and public key certification. In 7ª Conferência sobre Redes de Computadores, CRC2004, Leiria, Portugal, October 2004.
7. Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais, Relator – Amadeu Guerra, Comissão Nacional de Protecção de Dados, 2004, [http://www.cnpd.pt/bin/relatórios/outros/Relatorio\\_final.pdf](http://www.cnpd.pt/bin/relatórios/outros/Relatorio_final.pdf)
8. J. Kohl, C. Neuman. The Kerberos Network Authentication Service (V5). RFC 1510, IETF, September 1993.
9. J. Hodges, R. Morgan. Lightweight Directory Access Protocol (V3): Technical Specification. RFC 3377, IETF, September 2002.
10. E. Rescorla. HTTP Over TLS. RFC 2818, IETF, May 2000.

11. R. Thayer, N. Doraswamy, and R. Glenn. IP Security Document Roadmap. RFC 2411, IETF, November 1998.
12. R. Housley, W. Polk, W. Ford, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, IETF, April 2002.
13. GSM Technical Specification GSM 03.20 (ETS 300 534): "Digital cellular telecommunication system (Phase 2); Security related network functions". Technical report, European Telecommunications Standards Institute, August 1997.
14. Microsoft TechNet. How certificates work. <http://technet.microsoft.com>.