Universidade de Aveiro
2007
Departamento de Electrónica, Telecomunicações e Informática

Helder José Rodrigues Gomes

Autenticação em Sistemas Telemáticos Biomédicos

DOCUMENTO PROVISÓRIO

Universidade de Aveiro Departamento de Electrónica Telecomunicações e Informática
2007

Helder José Rodrigues Gomes

Autenticação em Sistemas Telemáticos Biomédicos

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica do Professor Doutor André Zúquete, Professor Auxiliar no Departamento de Electrónica Telecomunicações e Informática da Universidade de Aveiro e do Professor Doutor João Paulo Cunha, Professor Associado no Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

Para a Li e Mariana.

o júri

presidente

Dr. António Manuel Melo de Sousa Pereira
professor catedrático da Universidade de Aveiro

Dr. João Paulo Trigueiros da Silva Cunha
professor associado da Universidade de Aveiro

Dr. Carlos Nuno da Cruz Ribeiro
professor auxiliar do Instituto Superior Técnico da Universidade Técnica de Lisboa

Dr. André Ventura da Cruz Marnôto Zúquete
professor auxiliar da Universidade de Aveiro

agradecimentos

A realização do trabalho não seria possível sem a colaboração de várias pessoas a que quero agora agradecer.

Desde logo aos orientadores André Zúquete e João Paulo Cunha, pelo apoio, colaboração e incentivo.

A toda a equipa da RTS, dos quais destaco Isabel Cruz, Ilídio Oliveira, Martin Stein, Jacek Kustra, Licínio Mano e Jorge Moura, pela colaboração e disponibilização de informação.

Á Escola Superior de Tecnologia e Gestão de Águeda, dos quais destaco o seu director, o Prof. Estima de Oliveira, e o pessoal dos grupos de Informática e Electrotecnia, pela ajuda concedida para a concretização deste trabalho.

A toda a minha família, principalmente à Li e à Mariana, pelo constante apoio, apesar de todo o tempo e atenção que foram desviadas para este trabalho.

A todos,

Muito Obrigado!

palavras-chave

Autenticação, Segurança, Infra-Estrutura de Chave Públlica, X.509, Smart Card, eSaúde.

resumo

Neste documento apresenta-se uma arquitectura para identificar e autenticar profissionais de saúde num sistema telemático de informação médica (Rede Telemática da Saúde - RTS). A arquitectura proposta é independente dos mecanismos de identificação e autenticação dos profissionais nos restantes sistemas das suas instituições de origem e potencia a mobilidade dos profissionais de saúde inter e intra instituições. Baseia-se numa Infra-Estrutura de Chave Pública (PKI) simplificada, em certificados de chave publica de curta duração, na utilização de *smart cards* para o armazenamento das credenciais dos profissionais e em certificação cruzada para o estabelecimento de relações de confiança entre as IS e a RTS. É, também, flexível e escalável, sendo capaz de suportar futuras adesões à RTS de forma simples e sem degradação de serviço.

keywords Authentication, Security, Public Key Infrastructure, X.509, Smart Card, eHealth.

abstract This document presents an architecture to identify and authenticate health professionals accessing a Telematic Health Information System (RTS – Rede Telemática da Saúde). The proposed architecture, is independent of other identification and authentication systems in health professionals home organizations, and promotes health professionals mobility inter and intra health organizations. It is based in a simplified Public Key Infrastructure, with short-lived public key certificates, the use of personal smart cards to store health professional credentials and in the cross-certification to establish trust relations between RTS and health organizations. The architecture is also flexible and scalable, supporting the future RTS adherence of more health organizations, smoothly and without quality of service degradation.

Índice Geral

Índice de Figuras

1 Introdução

Nos nossos dias verifica-se uma crescente tendência para a utilização de tecnologias de informação nas mais variadas áreas de actividade. A área da saúde não podia ficar alheia a esse processo, e cedo começaram a aparecer aplicações informáticas biomédicas. Como aplicações biomédicas entendem-se aplicações para utilização na área da Biologia e da Medicina. Estas aplicações começaram por ser isoladas e específicas (destinadas apenas a resolver um problema muito concreto).

A evolução das redes de comunicações e a sua integração com os sistemas informáticos forma dando origem aos sistemas telemáticos, em que os serviços informáticos começaram a ser fornecidos à distância através de redes de comunicação podendo, desta forma, ser utilizados por um universo cada vez maior de utilizadores. Com esta evolução, também as aplicações biomédicas deixaram de ser aplicações isoladas, começando gradualmente a fornecer os seus serviços a toda uma instituição de saúde, sendo hoje obrigatoriamente aplicações integradas e geridas no contexto de uma política global da instituição de saúde.

Com a Rede Telemática da Saúde[1] (RTS) é dado um novo passo em frente, uma vez que o seu objectivo é a integração telemática das Instituições de Saúde a nível de toda uma região [1].

Esta integração implica uma visão agregadora da informação médica nas instituições de saúde aderentes e a sua partilha entre todas elas. O carácter confidencial da informação médica, legalmente protegida, faz com que a segurança informática seja um factor fundamental no desenho do sistema. Desse campo vasto que é a segurança informática, que envolve várias vertentes como a segurança das redes, das aplicações, etc., a autenticação é o aspecto abordado neste trabalho.

A autenticação é entendida como o processo pelo qual numa comunicação se faz prova de que a entidade interlocutora é quem de facto reivindica ser. Por entidades não se entendem obrigatoriamente pessoas, podendo ser máquinas ou serviços.

Por si só, a autenticação apenas valida a identidade de uma entidade. O seu resultado é que vai permitir, ou não, o desencadear de uma operação seguinte. Por exemplo, apenas sabendo quem pretende aceder a um determinado serviço ou elemento de informação se pode determinar se esse acesso é, ou não, autorizado e, em caso afirmativo, estabelecer o correcto nível de acesso. Isto não significa que a autenticação seja de pouca importância, pelo contrário, não existem sistemas seguros sem uma autenticação forte. No entanto, ela é apenas um fundamental primeiro passo para um sistema seguro e não um fim em si mesmo. Quanto mais forte a autenticação, mais garantias existem de que apenas as entidades autorizadas acedem ao sistema e mais confiança existe na confidencialidade e correcção da informação.

Tipicamente a autenticação é feita com recurso a um nome (*login*) e uma senha (*password*). São, no entanto, sobejamente conhecidos os problemas desta solução: vírus, *phishing*, *shoulder surfing*, etc. Com a informatização da informação médica, maiores são os riscos que se colocam para a sua confidencialidade.

[1] http://www.rtsaude.org

Assim preconiza-se a utilização de mecanismos de autenticação mais seguros, de fácil utilização e que em simultâneo potenciem a mobilidade entre instituições de saúde.

É nesse contexto particular da segurança informática que se insere este trabalho: estudo dos mecanismos de autenticação existentes em sistemas telemáticos e a sua aplicação a sistemas telemáticos biomédicos através do caso prático da RTS.

1.1. Objectivo

Neste trabalho define-se uma arquitectura para a autenticação da identidade das entidades envolvidas em interacções electrónicas no âmbito da Rede Telemática da Saúde.

Com base nos requisitos da RTS e na experiência anterior do grupo de trabalho na implementação de sistemas de informação clínica e em sistemas de segurança foi definido um conjunto de objectivos base a alcançar.

Um primeiro objectivo a atingir é a autenticação forte dos Profissionais no acesso aos serviços da RTS. Este objectivo deriva directamente dos requisitos da RTS e deve-se à já referida fragilidade do mecanismo de autenticação por nome e senha. Este objectivo leva à necessidade da utilização de *tokens* de segurança que possam transportar de forma segura as credenciais dos Profissionais, disponibilizando uma autenticação baseada em dois factores: (i) a posse do *token* e (ii) o conhecimento de um segredo que permita a sua utilização. A possibilidade de extensão deste objectivo à autenticação dos utentes no acesso à sua informação pessoal deverá ser considerada.

O segundo objectivo tem a ver com a mobilidade dos Profissionais. A arquitectura a implementar não deve ser um obstáculo à sua mobilidade, tanto dentro da sua Instituição de Saúde (IS) como entre diferentes IS.

O terceiro objectivo é que a RTS seja independente dos mecanismos de gestão de pessoal das IS participantes. Cada IS é uma instituição independente com os seus recursos, o seu Departamento de Pessoal e o seu serviço de directoria com a informação para a gestão dos seus recursos informáticos. A existência deste serviço é independente da existência da RTS, uma vez que é necessário para a gestão dos restantes sistemas informáticos da IS. Faz portanto sentido a sua reutilização ficando cada IS com a responsabilidade de fazer a gestão do acesso dos seus Profissionais à RTS.

O quarto objectivo é fornecer à RTS de forma confiável a informação do perfil do Profissional na IS a que está vinculado. Esta informação é importante porque determina qual a política de autorização a aplicar para o controlo dos acessos do Profissional à informação.

O quinto objectivo é minimizar a comunicação com a IS para a autenticação do profissional e a obtenção e validação do seu perfil. Isto implica que devem ser evitados serviços *online* para a obtenção e autenticação da identificação e perfis dos Profissionais, o que significa que as suas credenciais devem conter toda a informação necessária para que não seja necessário contactar a sua IS para a obtenção de informação adicional.

O sexto objectivo é a compatibilidade entre navegadores da Internet. Para evitar o requisito de utilizar um navegador específico para aceder à RTS, não é permitida a execução de código activo (ActiveX e Java Applets) no cliente. Isto significa que o mecanismo de autenticação utilizando os dois factores de autenticação já tem que ser uma das funcionalidades de base suportadas pelos navegadores.

Por fim, é um objectivo evitar o desenvolvimento de código. Sempre que possível deve ser dada preferência à utilização de tecnologia disponível, depois de devidamente configurada.

1.2. Contribuições

As principais contribuições deste trabalho foram: (i) a definição de uma Infra-estrutura de Chave Pública (PKI) para suporte à autenticação na RTS, que no futuro poderá vir a ser estendida para suportar outros serviços que eventualmente venham a ser necessários na RTS; (ii) Estudo de três dispositivos de tecnologia *smart card* para averiguar da sua adequação à arquitectura proposta e dos pontos importantes a considerar para a sua aquisição; (iii) Estudo dos serviços PKI do Windows com a implementação do protótipo utilizando esta tecnologia.

Foi implementado um protótipo da solução de autenticação proposta para averiguar da sua exequibilidade. Por falta de agenda, não se chegou a implementar a solução em ambiente de produção, ou seja nas Instituições de saúde onde os profissionais desempenham as suas funções. Será esta uma das tarefas seguintes.

No decurso deste trabalho foi publicado um artigo na 2ª Conferência Nacional sobre segurança Informática nas Organizações (SINO'2006) com o título "Arquitectura de Autenticação Baseada em Certificados para a Rede Telemática da Saúde (RTS)" [2].

Recentemente foi um outro artigo aceite para publicação no *2nd International Symposium on Information Security* (IS'07) com o título "*Authentication Architecture for e-Health Professionals*" [3].

1.3. Organização do texto

O resto do documento está estruturado da seguinte forma: No capítulo 2 é feita uma breve apresentação da RTS identificando os requisitos e pontos importantes para a autenticação. No capítulo 3 é dada uma panorâmica sobre conceitos de autenticação e de criptografia e sobre tecnologias e dispositivos de suporte à autenticação, com uma ênfase especial na Infra-estrutura de Chave Pública (PKI). No capítulo 4 é feita uma análise a trabalhos relacionados com este, como sendo as experiências da Grécia, HYGEIAnet, e Dinamarca, MEDCOM e Sundhed.dk. Analisa-se também a arquitectura de autenticação para redes sem fios em ambiente universitário, que serviu de base para a arquitectura proposta, e por fim analisa-se o Cartão do Cidadão dado o interesse na sua utilização para a autenticação dos utentes para a consulta da sua informação clínica. No capítulo 5 é feita a apresentação da arquitectura de autenticação proposta e no capítulo 6 a implementação do protótipo para prova do conceito. Finalmente no capítulo 7 é feita uma avaliação dos resultados obtidos e no capítulo 8 as conclusões e trabalho futuro.

2 Rede Telemática da Saúde

A Rede Telemática da Saúde (RTS) é um projecto desenvolvido pela Universidade de Aveiro, com o apoio do programa Aveiro Digital, financiado pelos Fundos FEDER/FSE da EU, através do POSI, 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.

Pretende promover, através duma plataforma informática distribuída e acessível por tecnologia web, o acesso electrónico seguro à informação clínica residente nas várias instituições de saúde a todos os profissionais credenciados, assim como permitir aos utentes a gestão de assuntos relacionados com a sua saúde [1, 4]. Ou seja, a RTS visa potenciar a integração e a partilha da informação clínica disponível a nível regional, de modo a agilizar a interacção entre as várias equipas de saúde e criar sinergias para uma melhor prestação dos cuidados de saúde.

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 de saúde, e potencia um importante conjunto de mais-valias, desde oferecer ao médico um mais completo “perfil” clínico do seu paciente, até evitar a duplicação da realização de meios complementares de diagnóstico. Outro resultado é a melhoraria da interacção do utente com os serviços de saúde, permitindo ao utente a gestão da sua agenda de saúde, que inclui a possibilidade de interacção com o seu médico assistente, de pedir marcação de consultas, pedir renovação de receituário, entre outras [5, 6]. A RTS oferece ainda mecanismos de comunicação electrónica entre profissionais e entre estes e os utentes assim como a agilização de diversas requisições de serviços, como as consultas de especialidades ou a renovação do receituário sem necessidade de deslocação do cidadão ao Centro de Saúde.

A RTS suporta a interacção com dois grandes grupos de utilizadores: (i) os profissionais de saúde e (ii) os utentes dos serviços de saúde. Esta interacção é baseada em portais dedicados a estes grupos de utilizadores: (i) o Portal do Profissional e (ii) o Portal do Utente [1].

No Portal do Profissional a ênfase é colocada na colaboração e no acesso integrado à informação clínica dos utentes dispersa pelas várias instituições de saúde.

O Portal do Utente serve, por um lado, como veículo de divulgação de conteúdos de informação médica de acesso público e, por outro lado, para que os utentes registados possam fazer uma gestão personalizada da sua agenda/plano de saúde.

É importante referir que a RTS não se pretende substituir aos sistemas de informação que suportam a actividade médica nas instituições de saúde, como por exemplo o SINUS, SONHO, etc. [1]. Estes sistemas continuam a funcionar e são os produtores exclusivos da informação médica. O papel da RTS não é produzir informação médica mas sim actuar como plataforma de comunicação e partilha dessa informação de uma forma integrada entre as várias instituições de saúde participantes [6].

2.1. Serviços Disponibilizados

Como já foi referido, a RTS disponibiliza através dos seus portais um conjunto de serviços aos seus utilizadores. Esses serviços encontram-se indicados na seguinte tabela [6]:

Serviços orientados às Instituições de Saúde / Profissionais		Identificação coerente dos utentes. Sistema seguro de autorizações de certificações electrónicas. Acesso ao resumo clínico do doente (características de saúde). Acesso aos resumos de episódios de prestação de cuidados (resumos de Admissão, de Alta e de Transferência; resultados de exames; resumo de terapêutica). Resumos (vista) por especialidade clínica e integração de protocolos existentes. Marcação remota de recursos entre parceiros. Suporte à interacção Profissional-Profissional, incluindo a troca de documentos digitais e de notas clínicas.
Serviços orientados para o utente	Serviços de acesso livre (público).	Notícias e anúncios de eventos. Conteúdos de educação para a saúde e prevenção. Glossários clínicos. Conteúdos interactivos: saudómetros, sondagens de opinião, etc. "Páginas amarelas" dos prestadores da RTS.
	Serviços de acesso restrito	Gestão da Minha Saúde: agenda de saúde, monitorização de plano terapêutico, preenchimento/consulta de boletins. Minha Saúde em Rede: pedido de aconselhamento clínico, interacção médica com o seu médico assistente, pedido de marcações, pedidos de renovação de receituário, gestão da conta corrente do utente. Gestão de dados pessoais de identificação.

Tabela 1: Serviços da RTS disponibilizados aos seus utilizadores.

Mais uma vez, convém realçar que os serviços fornecidos pelos portais não produzem directamente informação médica: ou visualizam informação existente ou geram mensagens a solicitar um serviço. O processamento das mensagens e a correspondente produção de informação médica será sempre efectuado pela aplicação apropriada e não pela RTS. Por exemplo, o caso da marcação remota de recursos gera uma mensagem para o serviço pretendido e, nesse serviço, após a recepção da mensagem e utilizando a aplicação apropriada, será verificada a possibilidade de efectuar tal marcação. Após o processamento será gerada uma mensagem de resposta indicando o sucesso ou não.

Além dos portais, que fornecem os serviços aos utilizadores, a RTS necessita de um conjunto de serviços de infra-estrutura que integrem os sistemas existentes nas várias IS e forneçam os serviços telemáticos necessários aos portais [1, 5]. Esses serviços de infra-estrutura, que são implementados no designado *RTS Data Center*, encontram-se listados na seguinte tabela:

Catálogo	Registo das fontes de dados acessíveis na rede. Registo dos objectos de dados fornecidos por cada fonte.
Serviços de Transformação de Dados	Conjunto de serviços de mediação para coordenar o acesso e unificação de dados distribuídos, disponíveis em várias fontes de dados. Funções de conversão de dados.
Serviços de Directoria e Autorização	Definição e armazenamento de políticas de acesso aos serviços e dados. Emissão de autorizações mediante os contextos de utilização e credenciais dos utilizadores.
Índice Mestre de Pacientes (*Master Patient Index*)	Tabela mestra com a identificação dos pacientes na região para resolver os problemas associados à utilização de diferentes códigos de identificação de pacientes em cada IS
Monitorização e Administração	Acompanhamento da qualidade de serviços da RTS e operações em curso. Estatísticas de utilização. Acções de supervisão e configuração da rede (controlo de utilizadores, configuração, etc.).

Tabela 2: Síntese dos serviços de infra-estrutura da RTS.

2.2. Arquitectura

A Figura 1 apresenta a arquitectura da RTS [1], onde podemos ver Instituições de Saúde (IS) – Hospitais e Unidades de Cuidados Primários – com os respectivos Profissionais, Utentes e outras Entidades Externas e o *RTS Data Center* – serviços de infra-estrutura da RTS.

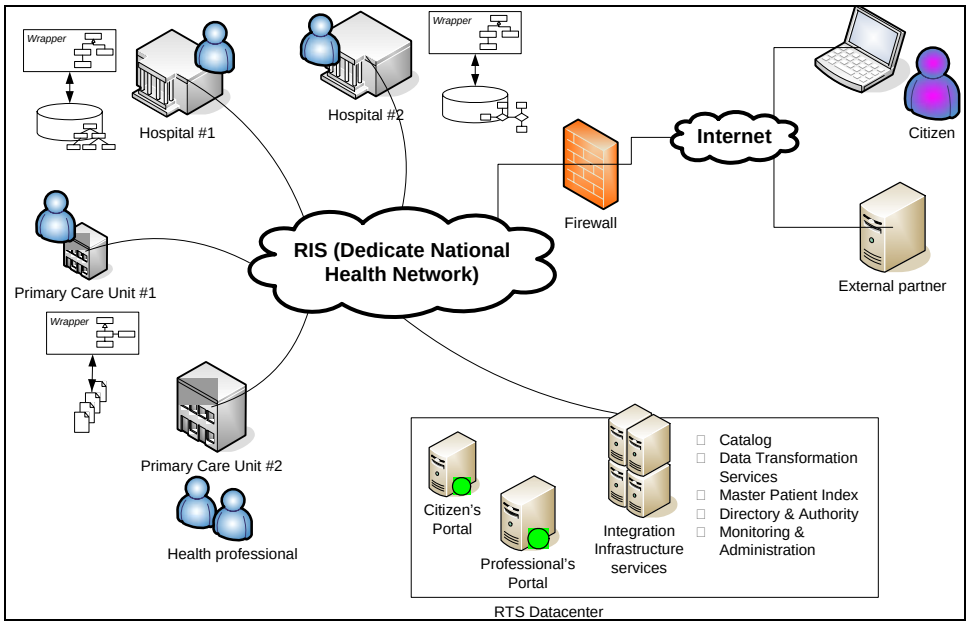


Figura 1: Arquitectura da RTS [1]

A Comunicação entre as várias IS é garantida pela RIS (Rede Informática da Saúde), que é uma rede privada nacional dedicada a fornecer serviços de comunicação segura entre as várias IS do país, sendo gerida pelo IGIF (Instituto de Gestão Informática e Financeira da Saúde) do Ministério da Saúde.

A informação médica é exclusivamente produzida e armazenada nas IS. De forma a permitir a partilha e integração da informação médica, cada IS irá ter um agente de integração, desigado por *Wraper*, que fará a interligação entre os sistemas de informação da respectiva IS e o *RTS Data Center*.

Todo o desenvolvimento de *software* da RTS foi baseado em ferramentas *Open Source*, tais como Linux, Apache ou PostgreSQL. O objectivo da utilização de ferramentas *Open Source* é não onerar os custos de licenças para o futuro.

Do ponto de vista técnico, os Portais são aplicações Web, vistas pelos utilizadores como servidores HTTP aos quais acedem através de um navegador da Internet (*browser*) comum (Internet Explorer, Mozilla Firefox, Nestcape Navigator, …). É um requisito a não utilização de código activo nos browsers (*Applets Java* ou controlos *ActiveX*) para evitar problemas de compatibilidades com browsers.

Quanto à comunicação interna, entre Portais e *Wrapers*, ela é baseada em serviços Web (*Web Services*), utilizando-se objectos SOAP.

Na figura está também prevista a interligação da RTS a serviços externos, tais como farmácias, laboratórios, etc. No entanto, esta não é uma funcionalidade a disponibilizar no imediato [1].

No momento actual, a RTS está em funcionamento pleno desde o Outubro de 2006, embora sem as funcionalidades de autenticação aqui propostas. Em Abril de 2007, integrava dois Hospitais e seis Unidades de Saúde, tendo sido gerados aproximadamente 11 milhões de episódios a partir de um universo de aproximadamente 350 000 cidadãos [4].

Entre os planos para o futuro estão a integração de mais instituições de saúde como sendo os Hospitais da Universidade de Coimbra (HUC) e o Hospital de S. Sebastião (HSS) da cidade de S. Maria da Feira; (ii) a criação de uma associação sem fins lucrativos para a manutenção e divulgação da RTS e (ii) a inclusão de mais funcionalidades como por exemplo o reforço da segurança dos acessos como proposto neste trabalho [4].

2.3. Modelo de Acesso à Informação

É importante discutir qual o modelo de funcionamento dos portais em termos de como é feito o acesso à informação pretendida. Dois modelos de funcionamento são possíveis:

- Um modelo tipo serviço de apontadores, em que o portal reencaminha o utilizador para o local com a informação pedida (modelo SAPO), ou seja, o utilizador acede directamente à fonte da informação pretendida; o portal apenas funciona como localizador (*broker*) da informação pretendida.
- Um modelo de acesso intermediado, em que é a RTS que vai buscar a informação pretendida pelo utilizador e faz a sua apresentação; o utilizador não acede directamente à fonte da informação pretendida.

A vantagem do modelo de apontadores é o acesso directo do utilizador à fonte da informação pretendida, sem a sobrecarga e o atraso da mediação. No entanto, actualmente as aplicações que gerem a infor-

mação médica não estão acessíveis a utilizadores de outras instituições, e nem todas elas dispõem de mecanismos de autenticação e de controlo de acessos eficazes.

Um dos objectivos da RTS é a uniformização das interfaces, com vista a facilitar a interacção com os utilizadores. Neste momento, tal apenas é possível se for a RTS a responsável por essa interface, uma vez que não é possível a alteração de todas as aplicações actuais, usadas pelas diversas IS, para se adaptarem às regras de interface da RTS.

Por estas razões, o modelo de acesso à informação a implementar pela RTS é o do acesso mediado. No entanto, com o surgimento nas IS de aplicações compatíveis com a RTS (RTS *compliant*), a tendência será a crescente adopção do modelo de acesso através de apontadores. No momento actual (Abril 2007) existe já uma aplicação, integrada com a RTS, que permite o acesso do profissional a relatórios de radiologia utilizando directamente os serviços da instituição de saúde possuidora do relatório.

2.3.1. Modelo de acesso intermediado

O modelo de acesso intermediado implementado na RTS está esquematizado na Figura 2.

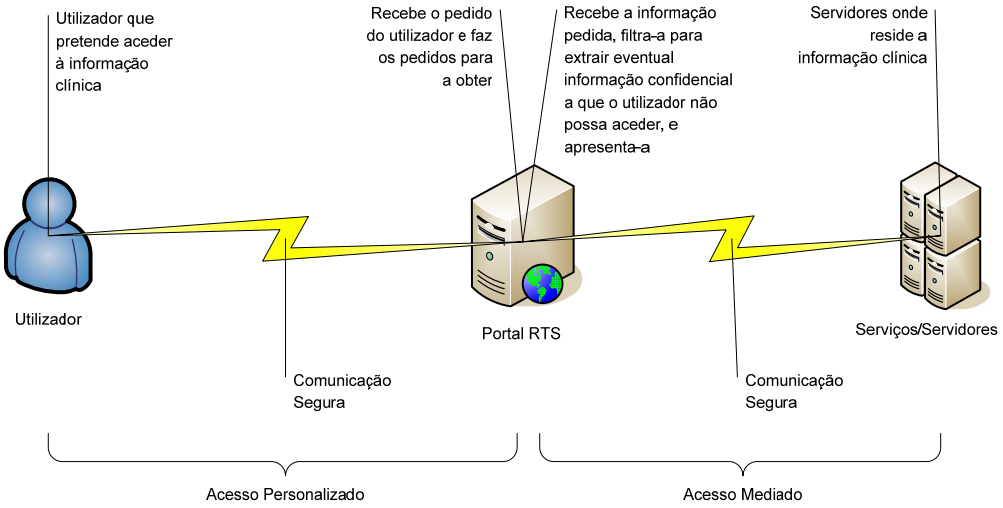


Figura 2:Modelo de comunicação intermediada na RTS

Para o estabelecimento do diálogo do utilizador com o Portal, este último necessita da identificação do utilizador para poder determinar o seu perfil de autorização, ou seja, a que informação/serviços é que pode aceder. Fragilidades na identificação do utilizador podem eventualmente permitir a personificação e consequente acesso não autorizado a informação protegida. Em simultâneo, dado o carácter confidencial e crítico da informação médica, o utilizador necessita de ter confiança de que o portal a que está a aceder é de facto um portal da RTS. Ainda devido ao carácter confidencial da informação médica, é necessário garantir que a comunicação entre o utilizador e o portal se efectua de forma segura, ou seja, que não é compreensível ou alterável durante o trajecto.

Para obter a informação pretendida pelo utilizador, o Portal vai aceder a um ou mais Serviços/Servidores que, por sua vez, podem aceder a outros. Apesar de aqui não haver a identificação e autentica-

ção do utilizador que pretende a informação, os serviços/servidores, da RTS e das diversas IS, devem autenticar-se entre si para garantir que não há acessos não autorizados e evitar fugas de informação. Eventualmente o serviço fonte da informação na IS poderá pedir ao portal da RTS evidências da identidade do utilizador. É ainda necessário que a comunicação se efectue através de um canal seguro para evitar, uma vez mais, que a informação trocada seja compreensível ou alterável durante o trajecto.

2.4. Entidades

Como foi referido na secção 2.3 – Modelo de Acesso à Informação, existe a necessidade de autenticar utilizadores, portais, serviços e servidores.

Para além disso, na hierarquia de classificação de utilizadores da RTS, apresentada na Figura 3, podem ser identificados dois grandes tipos de utilizadores: (i) os Profissionais – utilizadores que no âmbito das suas funções profissionais na IS acedem aos serviços da RTS, e (ii) os Utentes – utilizadores/consumidores dos serviços de saúde disponibilizados pelas IS. Estes utilizadores são genéricos e de alto nível, sendo necessário mais algum detalhe na sua caracterização. Assim, existem diversos tipos de profissionais a que correspondem diversas funcionalidades no acesso à RTS em termos dos serviços e informação a aceder. São eles: (i) Médico, (ii) Médico Chefe de Serviço, (iii) Administrativo, (iv) Enfermeiro e (v) Enfermeiro Chefe. Existe também um utilizador Anónimo que acede ao Portal do Utente para consulta de informação livre.

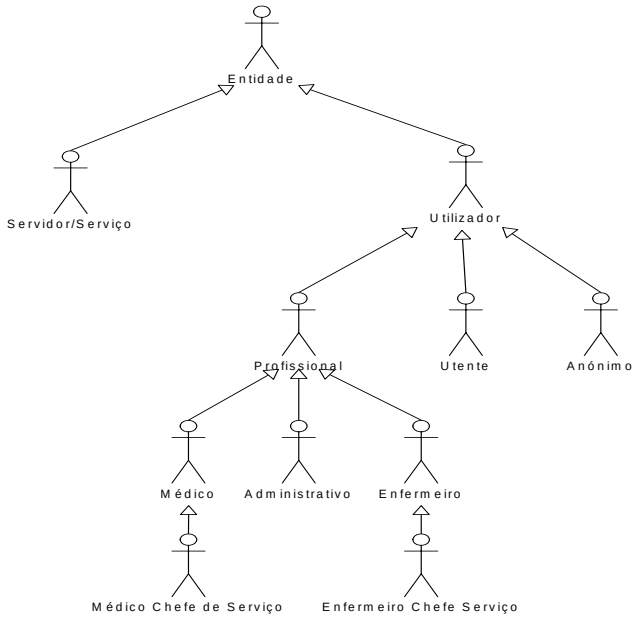


Figura 3: Entidades que comunicam na RTS

Estes tipos de utilizadores e os vários serviços/servidores, nos quais se incluem os portais, constituem as entidades que comunicam no âmbito da RTS e que devem ser sujeitas a autenticação.

2.5. Requisitos para a Autenticação

Como vimos na secção anterior, há dois grandes grupos de utilizadores que acedem à RTS: os profissionais e os utentes. O acesso destes utilizadores à RTS é efectuado através de portais, havendo um Portal dedicado a cada um destes tipos de utilizadores: o Portal dos Profissionais e o Portal dos Utentes. Estes portais disponibilizam um acesso Web, não sendo permitida a execução de código activo (Java A*pplets* ou *ActiveX*) nos *browsers*. Além disso, a comunicação com ambos os portais deve ser segura de modo a garantir a confidencialidade dos dados enquanto em trânsito.

O grau de sensibilidade da informação a que cada um dos grandes grupos de utilizadores acede é diferente, pelo que a sua autenticação no acesso aos portais poderá ter características diferentes.

O acesso dos profissionais é o mais crítico, dado o maior grau de confidencialidade da informação a que acedem. De acordo com o Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais [7], nas Instituições de Saúde a autenticação de utilizadores é normalmente efectuada através de nome (*login*/*username*) e senha (*password*). A quase totalidade das aplicações informáticas nas IS nacionais utiliza este mecanismo de autenticação. Contudo, este é um mecanismo de autenticação frágil, havendo no referido relatório exemplos de práticas de manuseamento de senhas à margem de todas as regras de segurança. Como solução para este problema preconiza-se, no referido relatório, (i) a educação dos utilizadores para os problemas associados às senhas, (ii) a definição clara de políticas de gestão de senhas e (iii) a introdução progressiva de mecanismos de autenticação mais fortes.

As políticas de gestão de senhas definem regras, mais ou menos rígidas, a que todos os utilizadores devem obedecer na definição e manutenção de senhas. Estas políticas, se bem aplicadas e acompanhadas da educação e sensibilização dos utilizadores, melhoram a eficácia deste mecanismo, mas não resolvem completamente os seus problemas de segurança. É, portanto, necessário um mecanismo de autenticação reconhecidamente mais forte, do que o tradicional nome e senha, para o acesso dos profissionais ao Portal dos Profissionais.

Uma característica de interesse para a RTS é potenciar a mobilidade dos Profissionais, principalmente médicos e enfermeiros, dentro e fora das IS a que estão vinculados. Essa mobilidade não deve ser impeditiva do acesso aos serviços da RTS. Portanto, um Profissional deverá poder autenticar-se e aceder à RTS a partir de qualquer IS participante. Isto implica que a autenticação na RTS seja de certa forma independente das soluções de autenticação em vigor dentro de cada IS e coerente em toda a RTS.

Quanto à autenticação dos utentes no acesso ao respectivo portal, por razões económicas e pela menor sensibilidade da informação acedida, poderá ser efectuada através de nome e senha. A obtenção de credenciais de acesso dos utentes será feita através de um registo prévio em que o utente autoriza a disponibilização *on-line* da sua informação clínica. Contudo, a solução a adoptar não deve fechar portas a um eventual uso futuro do cartão do utente, o qual poderá disponibilizar capacidades mais robustas de identificação do seu dono.

Além da comunicação entre utilizadores e Portais, também existe a comunicação entre Portais e Servidores ou Serviços. Esta comunicação também deve ser precedida de autenticação e deve também ser segura, de modo a garantir a confidencialidade da informação trocada.

Como na RTS não se produz informação clínica, a autenticação de informação não é neste momento um requisito.

Em geral, a autenticação não deve ser um obstáculo à utilização do sistema: deve ocorrer da forma mais facilitada possível, mas sempre cumprindo exigentemente a sua função. Deve também ser flexível e escalável, permitindo a fácil integração de outras instituições que adiram à RTS, bem como eventuais aumentos significativos de utilizadores nas IS actuais, sem comprometer o seu desempenho.

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

2.6. Requisitos para a Autorização

Em qualquer sistema é de extrema importância saber a que informação e/ou serviços pode um determinado utilizador aceder: raros são os sistemas em que todas a informação e serviços são livres. Normalmente existem áreas de acesso restrito para as quais é necessário controlar os acessos. Nestes casos, depois de autenticado o utilizador, é necessário verificar se ele tem, ou não, autorização para aceder da forma que pretende a um determinado objecto (serviço/informação).

A autenticação está intimamente ligada à autorização. É a autenticação que fornece à autorização a identificação da entidade que pretende aceder ao objecto sujeito a politicas de autorização. É pois necessário abordar um pouco este tema em relação à RTS.

A informação médica é considerada informação sensível, havendo inclusive legislação que regula a sua posse, acesso e manuseamento. De acordo com a legislação portuguesa, a propriedade da informação médica é do utente e as unidades do sistema de saúde as suas depositárias. Apenas o médico escolhido pelo utente para lhe prestar cuidados de saúde pode aceder ao seu processo clínico. O acesso por parte de outros profissionais de saúde apenas pode acontecer sob a supervisão, do médico designado pelo utente [8].

O modelo de autorização dos Profissionais das IS na RTS é baseado na função (perfil) que o Profissional desempenha na sua IS, sendo possível que um mesmo profissional desempenhe mais do que uma função. A determinação da correcta politica de autorização a aplicar pela RTS aos acessos dos profissionais baseia-se nos seguintes elementos de identificação: (i) o nome do Profissional, (ii) a IS a que está vinculado e (iii) o seu perfil na IS a que está vinculado. Dadas estas três informações, a RTS está em condições de saber qual a política de autorização a aplicar ao Profissional.

Nesta fase, o processo de gestão de autorização da RTS é essencialmente baseado na responsabilização dos profissionais. O controlo do acesso à informação é baseado apenas no perfil do Profissional, sendo a identificação do Profissional, e da IS a que está vinculado, utilizados para a criação relatórios detalhados de monitorização dos acessos. Estes relatórios têm como objectivo promover um auto controlo do Profissional no acesso à informação, permitindo a sua responsabilização na eventualidade de um acesso abusivo.

3 Tecnologias de Autenticação

O presente trabalho é sobre autenticação em sistemas telemáticos biomédicos. O que é então a autenticação?

Segundo a Wikipedia, autenticação é o "acto de estabelecer ou confirmar algo (ou alguém) como autêntico" ou, quando aplicado a segurança informática, "o processo de verificação da identidade digital do originador de uma comunicação" [9]. De acordo com o Grande Dicionário da Língua Portuguesa, autêntico significa "verdadeiro, certo, exacto, fidedigno" ou ainda "que é do autor a quem se atribui" [10]. Portanto, autenticação é o processo de garantir a veracidade da identidade das partes numa comunicação.

Desde os tempos remotos que a autenticação é utilizadas nas comunicações. Um exemplo, é a utilização do selo real para selar documentos: garantia que, independente do mensageiro, o documento tinha sido originado pelo rei [11]. Esta função era cumprida pelo facto de o selo ser único, ser reconhecido pela generalidade das pessoas e ser da posse exclusiva do rei. O selo poderia também cumprir outras funções, como garantir a integridade e confidencialidade da comunicação (a leitura ou alteração do documento obrigavam a destruição do selo) e garantir a autoria ou o não-repúdio (o selo é único e de posse exclusiva, pelo que apenas o rei poderia ter selado o documento).

A autenticação não se aplica apenas para garantir a autenticidade de informação, como no exemplo anterior. Utiliza-se, também, para garantir a autenticidade das identidades em interacções que dependam da identidade de quem nelas participa. Um exemplo é quando somos interpelados acerca da nossa identidade por um comerciante quando da apresentação de um cartão de crédito para efectuar um pagamento. Não é suficiente dizer quem somos, é necessário fazer prova de quem somos. É essa a função do BI. Foi emitido por uma entidade terceira de confiança, o Arquivo de Identificação, após a apresentação pessoal e a validação de um conjunto de documentos comprovativos da identidade. Como o comerciante confia no Arquivo de Identificação, e o BI tem elementos que permitem verificar a sua autenticidade e elementos que permitem reconhecer o sujeito para quem ele foi emitido, então, após a validação da identidade, o comerciante autoriza o pagamento através de cartão de crédito.

As duas formas de autenticação (informação e identidade) continuam a ser fundamentais na segurança de qualquer sistema de informação.

Como se pode ver dos dois exemplos acima, a autenticação consiste em dois passos: a apresentação da prova ou característica diferenciadora, o factor de autenticação, (o selo no documento e o BI) e a verificação da sua autenticidade (reconhecimento do selo e verificação da validade do BI e correspondência da fotografia e assinatura).

3.1. Autenticação versus Autorização

Apesar de muitas vezes confundidas, a autorização e a autenticação são processos distintos e visam objectivos distintos, contudo complementares.

A autorização é o processo que visa controlar os acessos a um determinado objecto. Apenas as entidades autorizadas lhe devem aceder. Para isso é, no entanto, necessária a resposta a uma questão prévia: quem é a entidade que pretende aceder ao objecto? É aqui que a autenticação desempenha o seu papel: garantir a identidade de quem pretende efectuar o acesso.

Assim, a autenticação precede a autorização e destina-se a fornecer-lhe a identidade de quem pretende efectuar o acesso.

3.2. Tipos de autenticação em transacções electrónica

3.2.1. Autenticação de identidade

A autenticação de identidade ocorre numa comunicação electrónica entre duas entidades quando pelo menos uma delas pretende ter a garantia da autenticidade da identidade do seu interlocutor. Para o efeito, é necessário que a entidade a ser autenticada envie as suas credenciais para que o seu interlocutor as possa validar e desta forma confiar na veracidade da sua identidade.

Exemplos de autenticação de identidade ocorrem, por exemplo, quando um utilizador inicia a sua sessão num computador, quando utiliza um modem para se ligar à rede de um ISP em que necessita de fornecer o seu nome e senha de acesso, quando acede a uma caixa Multibanco e introduz o seu cartão e o correspondente PIN.

Dependendo do sistema, a entidade que necessita de autenticação tanto pode ser uma pessoa, como uma máquina como um serviço.

A necessidade de autenticação tanto pode ser de apenas um dos interlocutores, autenticação do cliente ou autenticação do servidor, ou de ambos, autenticação mútua.

Como exemplo de autenticação mútua, temos uma sessão de banca electrónica (*home banking*) através da Internet, em que não é difícil perceber a relevância da autenticação mútua de ambas as entidades para evitar fraudes: o utilizador quer ter a certeza de que está de facto a comunicar com o seu banco, e o banco necessita de ter a certeza da identidade do cliente que está a conduzir a sessão.

Este tipo de autenticação é o indicado para a RTS. Dado o reconhecido grau de sensibilidade da informação clínica, é necessário um controlar o seu acesso de modo a que apenas entidades autenticadas e autorizadas lhe possam aceder.

No acesso ao Portal dos Profissionais é necessário que o Portal identifique o Profissional que pretende aceder à informação para poder controlar os acessos. Por outro lado, para que o Profissional tenha confiança na informação que vai aceder necessita da garantia de que o Portal é de facto o Portal dos Profissionais.

No caso da comunicação entre Portais e Servidores ou Serviços é também necessária a autenticação mútua para garantir que apenas máquinas e serviços idóneos acedem à informação.

3.2.2. Autenticação de mensagens

Enquanto que a autenticação de cliente e a autenticação mútua visam garantir que quem está a comunicar são de facto quem dizem ser, a autenticação de mensagens ou documentos visa proteger a integridade e determinar a autoria da mensagem. Depois de autenticada a mensagem, o receptor tem a garantia de que a mensagem foi produzida por uma entidade legítima e que não foi alterada enquanto em trânsito.

Devido ao facto de na RTS não ocorrer a produção de informação clínica, este tipo de autenticação não é um requisito. Poderia ser considerado para a autenticação de mensagens trocadas entre profissionais no contexto do Portal dos Profissionais, no entanto, o requisito da não existência de código activo nos *browsers* impede essa consideração.

3.3. Factores de autenticação

A prova ou característica diferenciadora, o factor de autenticação, pode tomar várias formas, que normalmente se classificam em [12]:

- Algo que se sabe: um segredo que a pessoa conhece, como por exemplo uma senha;
- Algo que se possui: um objecto que a pessoa tenha na sua posse, como por exemplo um cartão;
- Algo que se é: uma característica particular do corpo, como por exemplo a impressão digital ou o padrão da íris.

3.3.1. Algo que se sabe

Nesta autenticação, a pessoa a autenticar tem de ter conhecimento de um segredo. O exemplo típico de autenticação baseada num segredo é a autenticação baseada em nome (l*ogin*) e senha (*password*). É o mecanismo de autenticação mais vulgar nos sistemas de informação actuais. Cada utilizador é identificado através de um nome e tem na sua posse (sabe) uma senha a qual, tipicamente, é pessoal. O utilizador autentica-se indicando o seu nome e fornecendo a correspondente senha.

A grande vantagem da autenticação baseada no segredo é o facto de ser económica e fácil de implementar. Tem, no entanto, muitas vulnerabilidades, sendo conhecidos vários tipos de ataque, como por exemplo: ataques de dicionário, força bruta, *shoulder snifing*, engenharia social, *phishing*, etc. Muitos destes ataques têm sucesso não apenas por questões técnicas, mas sim pela dificuldade das pessoas em lidar com senhas [12, 13].

3.3.2. Algo que se têm

Nesta autenticação, a pessoa a autenticar tem de estar na posse de uma característica ou objecto diferenciador (único). Em computadores essa característica pode ser simplesmente um ficheiro. Frequentemente a característica diferenciadora é armazenada num dispositivo portátil, como por exemplo um *token*, um cartão

magnético, um *smart card*, ou num dispositivo fixo, como por exemplo um dispositivo HSM (*Hardware Security Module*).

Esta autenticação é mais segura que a autenticação baseada no segredo, uma vez que implica a posse de um objecto com uma característica que é única. Além disso, é mais fácil a detecção do seu comprometimento, ou roubo. Tem, no entanto, as desvantagens de ser cara e de haver o risco de perda ou falha do objecto diferenciador.

3.3.3. Algo que se é

Esta autenticação baseia-se em características físicas ou comportamentais exclusivas da pessoa a autenticar. A característica, designada biométrica, é medida no momento da autenticação e comparada com uma medida de referência efectuada anteriormente. Exemplos de características físicas vulgarmente utilizadas são a voz, impressões digitais e a íris.

A vantagem desta autenticação é que é de simples utilização pela pessoa a autenticar, estando a característica diferenciadora obviamente na posse da pessoa a autenticar. Tem a desvantagem de ser muito cara, de gerar rejeições em casos de ferimentos ou de alterações fisiológicas, de ter taxas de erro difíceis de ajustar para populações numerosas e de colocar problemas de correcção quando usada remotamente.

3.3.4. Autenticação forte

Quanto mais características diferenciadoras se utilizarem, mais forte a autenticação. As desvantagens de um factor de autenticação podem ser contrabalançadas pelas vantagens de outro. Deve, no entanto, haver um balanceamento entre a usabilidade, a protecção conseguida e a necessidade de autenticação forte. À partida, não faz grande sentido ter grandes medidas de segurança para proteger, por exemplo, um colar de contas de vidro (a menos que se pretenda fazer *bluff*).

A autenticação forte mais comum baseia-se em dois factores, normalmente, algo que se possui e algo que se sabe. Um exemplo simples é o Cartão Multibanco, onde a autenticação, além de depender da posse do cartão, depende também do conhecimento de um segredo: o PIN. Em sistemas de elevada grau de segurança podem utilizar-se três factores.

3.3.5. Autenticação remota

A autenticação remota acrescenta dificuldades extra à utilização dos factores de autenticação atrás mencionados. Qualquer que seja o factor de autenticação utilizado, o que de facto é produzido no momento da autenticação é um conjunto de bits que depois é enviado para a autenticar pela entidade remota. Como as entidades estão distantes entre si, não há forma de saber, por exemplo, se um registo biométrico foi gerado pela presença efectiva da pessoa, ou se está a ser replicado. Da mesma forma, não há forma de saber se a senha foi introduzida pela pessoa correcta. Por esta razão, qualquer que seja o factor de autenticação, é fundamental que a característica diferenciadora seja mantida em segredo.

3.4. Técnicas Criptográficas

A autenticação em transacções electrónicas baseia-se em técnicas criptográficas. Estas técnicas utilizam a criptografia para a protecção de segredos.

A Criptografia é a arte, ou ciência, de codificar uma mensagem de forma que apenas o seu destinatário a possa descodificar e compreender. Na sua forma mais básica é composta por duas operações: (i) a operação de cifra em que, utilizando uma chave, o emissor converte a mensagem em claro num criptograma (sequência de caracteres sem sentido aparente), e (ii) pela operação de decifra em que qualquer pessoa que conheça a chave de decifra transforma o criptograma de volta para a mensagem em claro.

Nos últimos anos as técnicas de criptografia evoluíram bastante com a utilização de computadores para a realização das operações criptográficas. Dependendo do tipo de chave, os tipos de cifra podem ser classificados como simétricos, assimétricos e híbridos [14].

A utilização de técnicas criptográficas permite a implementação de serviços tais como a autenticação, confidencialidade, integridade, entre outros.

3.4.1. Criptografia Simétrica

A criptografia simétrica é o mais antigo dos tipos de cifra. Baseia-se em algoritmos criptográficos simétricos, isto é, que utilizam a mesma chave para ambas as operações de cifra e decifra. Exemplos de algoritmos criptográficos simétricos frequentes são: o DES (*Data Encription Standard*), AES (*Advanced Encryption Standard*) e o IDEA (*International Data Encryption Algorithm*).

A principal vantagem dos algoritmos de chave simétrica é a sua eficiência, ou seja, são normalmente rápidos na sua execução. As suas principais desvantagens são a dificuldade da gestão das chaves, devido ao elevado número de chaves necessárias (num universo de N interlocutores, com uma chave secreta partilhada por cada par de interlocutores, são necessárias N(N-1)/2 chaves diferentes), e a distribuição segura de chaves pelos vários interlocutores (como fazer chegar de forma segura ao meu interlocutor a chave que nos irá permitir comunicar de forma segura?).

3.4.2. Criptografia Assimétrica

A criptografia assimétrica baseia-se em algoritmos de cifra que utilizam pares de chaves, uma chave para a cifra e outra diferente para a decifra. Estas chaves, apesar de diferentes, estão matematicamente relacionadas entre si, de tal forma que o que uma cifra apenas a outra consegue decifrar, e vice-versa. No entanto, a partir do conhecimento de uma das chaves não é possível obter a outra. O exemplo de algoritmo de cifra assimétrica mais conhecido é o RSA, cujo nome deriva dos nomes dos seus autores: *Rivest*, *Shamir* e *Adleman*.

Neste tipo de cifra, uma das chaves (chave privada) é mantida em segredo pelo seu dono, enquanto que a outra (chave pública) é publicitada o mais possível. Para se enviar uma mensagem confidencial para um interlocutor, cifra-se a mensagem com a sua chave pública, garantindo assim que apenas ele, com a sua

chave privada, é capaz de decifrar a mensagem. Da mesma forma, garante-se que uma entidade produziu uma mensagem se esta for decifrada utilizando a chave pública dessa entidade: apenas essa entidade poderia ter cifrado a mensagem porque apenas ela conhece a sua chave privada.

A grande vantagem desta cifra é a sua escalabilidade devida à redução do número de chaves necessárias para permitir comunicações confidenciais: num universo de N interlocutores são necessários N pares de chaves para permitir a comunicação confidencial entre qualquer par de interlocutores. Além disso, a distribuição de chaves fica facilitada dado o carácter público de uma delas.

A desvantagem é a sua pouca eficiência devido à complexidade das operações matemáticas em que se baseia. Além disso, é fundamental garantir a confidencialidade das chaves privadas e a distribuição fidedigna das chaves públicas.

3.4.3. Criptografia Híbrida

A criptografia híbrida surge da combinação das tecnologias de criptografia simétrica com a tecnologia assimétrica de forma a aproveitar as vantagens de ambas para obter comunicação segura – confidencialidade. Assim, utiliza criptografia simétrica, mais eficiente, para cifrar a mensagem a enviar e utiliza a criptografia assimétrica, menos eficiente, para cifrar a chave utilizada na cifra da mensagem, enviando ambas (mensagem e chave cifradas) ao destinatário. O destinatário, para obter a mensagem original, necessita (i) de utilizar a sua chave privada para obter a chave simétrica utilizada na cifra da mensagem e (ii) decifrar a mensagem utilizando a chave simétrica anteriormente obtida.

3.4.4. Funções síntese

As funções de síntese (*digest*) não são funções de cifra, mas sim funções de dispersão (*hash*) que permitem comprimir um bloco de dados inicial (supostamente grande) num bloco de resumo menor e de dimensão fixa, de tal forma que seja computacionalmente impossível (i) obter o bloco de dados inicial a partir do bloco de resumo – resistência à descoberta de um texto original, (ii) obter um segundo bloco de dados que dê origem ao mesmo bloco de resumo – resistência à descoberta de um segundo texto original e (iii) descobrir dois blocos de dados que produzam um mesmo bloco de resumo – resistência à colisão. Exemplos de funções de síntese são o MD5 e o SHA-1.

3.4.5. Assinatura digital

A assinatura digital é o equivalente à assinatura manual, aplicada a um documento sob a forma digital. Destina-se, tal como a sua equivalente manual, a assinar mensagens e documentos, garantindo entre outras propriedades a integridade, a autenticidade e o não-repúdio. A assinatura digital apenas é válida para a mensagem que assina e deve-a acompanhar sempre.

O princípio básico de funcionamento da assinatura digital utiliza criptografia assimétrica e funções de síntese. O autor da mensagem cifra-a com a sua chave privada. Desta forma, não a está a tornar confidencial porque toda a gente a pode decifrar utilizando a sua chave pública. O receptor, ao decifrar a mensagem

com a chave pública do autor, fica com a garantia de que foi o autor da mensagem quem efectivamente a produziu, uma vez que apenas este a poderia ter cifrado por a chave privada ser da sua exclusiva posse.

Na prática, por razões de eficiência, a assinatura digital não é feita exactamente desta forma. A assinatura digital consiste na cifra, com a chave privada do autor, do resultado de uma função de síntese aplicada à mensagem original. Esta assinatura é junta à mensagem original e enviada para o destinatário. O destinatário separa a mensagem da assinatura digital, decifra a assinatura digital com a chave pública do autor, para obter o resultado da função de síntese produzida pelo autor, e compara-a com o resultado da mesma função de síntese que ele aplica à mensagem recebida. Se forem iguais, o destinatário pode tirar as seguintes conclusões:

- Autenticação: A mensagem foi produzida pelo autor porque apenas ele a poderia ter assinado;
- Integridade: O documento é íntegro porque de outra forma os resultados das funções de síntese seriam diferentes.
- Não repúdio: o autor não pode alegar que não produziu a mensagem porque apenas ele a poderia ter assinado.

Como pode ser verificado da descrição do processo da assinatura digital, não pode haver reutilização de assinaturas de umas mensagens para outras, devido aos diferentes resultados produzidos pela função de síntese quando aplicada a diferentes mensagens.

3.5. Modelos de Autenticação

As arquitecturas de autenticação utilizadas em sistemas informáticos tipicamente enquadram-se nos seguintes modelos: Local, Directa, Indirecta e *Off-line* [12].

3.5.1. Modelo de autenticação local

O modelo Local refere-se a máquinas isoladas que possuem toda a informação necessária para efectuar a autenticação dos seus utilizadores.

3.5.2. Modelo de autenticação directa

No modelo de autenticação directa pretende-se autenticar um cliente remoto para o acesso a um determinado serviço. O serviço de autenticação, a informação para proceder à autenticação, e o serviço pretendido, residem todos na mesma máquina. Exemplos deste modelo são servidores de rede antigos, como o Microsoft LAN Manager e Novel Netware. Claramente este modelo não tem aplicação no caso da RTS em que a informação clínica e os serviços que a disponibilizam estão espalhados pelas várias Instituições de Saúde participantes.

3.5.3. Modelo de autenticação indirecta

No modelo de autenticação indirecta, o serviço de autenticação reside num servidor específico para essa função e os serviços a que o cliente pode aceder encontram-se em vários outros servidores. Os clientes são autenticados indirectamente contactando o servidor de autenticação quando pretendem aceder a um qualquer serviço. Toda esta comunicação entre as três entidades envolvidas na autenticação necessita de um protocolo. Exemplos de protocolos de autenticação indirecta são o RADIUS [15], o DIAMETER [16], 802.1X [17] e o Kerberos [18].

Como existe troca de mensagens com o servidor de autenticação, é necessária a utilização de criptografia para garantir a sua autenticidade.

Um ponto importante a considerar na utilização de autenticação indirecta é a necessidade de ter o servidor de autenticação permanentemente em funcionamento. Não é possível a autenticação dos clientes, e o correspondente acesso aos serviços pretendidos, se o servidor de autenticação não estiver contactável.

A Figura 4 ilustra o princípio de funcionamento deste tipo de autenticação, apesar de se referir mais concretamente ao protocolo 802.1X suportado por um servidor de autenticação RADIUS. Para aceder aos recursos da rede o cliente (*supplicant*) tem que primeiro ser autenticado. Para isso, envia as suas credenciais ao *Authenticator*, que por sua vez as envia ao *Authenticator Server* para serem validadas. Dependendo da resposta do *Authentication Server* o *Authenticator* permite ou não o acesso aos recursos da rede.

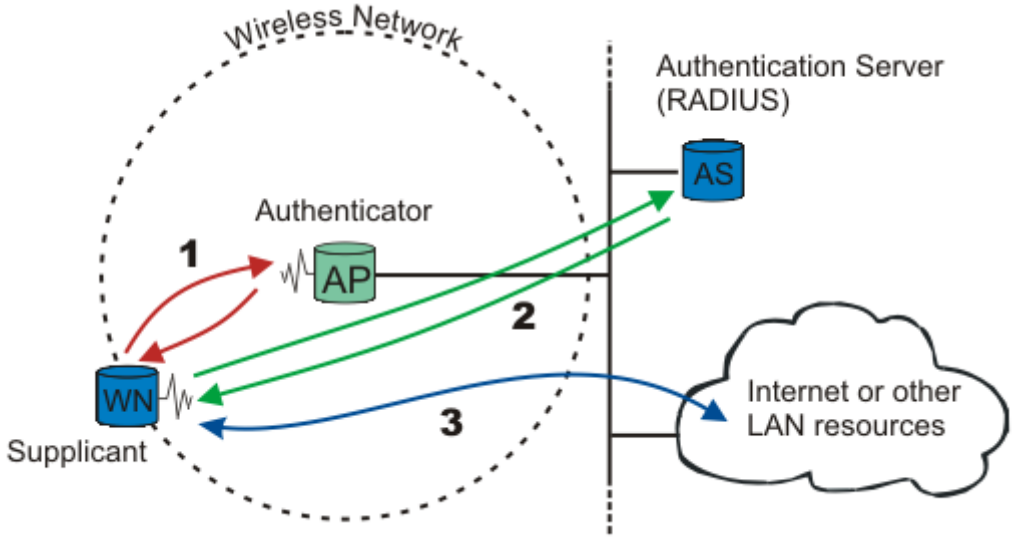


Figura 4: Exemplo de autenticação indirecta 802.1X.

A aplicação deste modelo de autenticação indirecta ao caso específico da RTS acarreta uma série de dificuldades. Estas dificuldades surgem devido à inexistência de um serviço centralizado com a informação de autenticação dos profissionais. Assim, ou seria necessário replicar as informações de autenticação de cada IS num único serviço de autenticação gerido pela RTS, ou o Portal teria que aceder ao serviço de autenticação da respectiva IS. Esta última opção é complicada porque como as IS são independentes entre si, podem

ter mecanismos de autenticação internos diferentes, o que implicaria que o Portal dos Profissionais fosse capaz de dialogar com todos eles.

3.5.3.1 RADIUS e DIAMETER

O protocolo de autenticação RADIUS (*Remote Authentication Dial-In User Service*) é um protocolo de autenticação, autorização e facturação (AAA – *Authentication, Authorization and Accounting*), para controlar o acesso a recursos de rede e fornecer informação para sistemas de facturação [15]. Foi inicialmente desenvolvido como um sistema para a identificação e autenticação de utilizadores em acessos através de bancos de modems. O RADIUS é frequentemente utilizado no padrão de autenticação 802.1X [17] actualmente usado para autenticação em redes sem fios.

É um protocolo cliente-servidor, envolvendo três tipo de elementos: o cliente que pretende o acesso ao recurso de rede, o NAS (*Network Access Server*) e o servidor RADIUS. O cliente requisita recursos de rede ao NAS, e envia-lhe as suas credenciais. Este por sua vez envia-as ao servidor RADIUS que verifica se elas são válidas. Se forem válidas, o NAS decide o nível de autorização apropriado e dá o correspondente acesso. A autenticação do cliente é geralmente feita com recurso a protocolos como o CHAP [19] ou EAP [20].

Em termos de segurança, a comunicação é segura entre o NAS e o servidor RADIUS, através de um segredo partilhado entre os dois. Além disso, o servidor RADIUS apenas dialoga com os NAS para os quais tenha sido configurado.

Este protocolo sofreu uma actualização para o DIAMETER [16], sendo no entanto ainda bastante frequente. As diferenças principais entre os dois estão ao nível do protocolo de transporte utilizado (UDP no RADIUS e TCP no DIAMETER), no uso de segurança ao nível da camada de transporte (IPSec ou TLS) e nas capacidades de suporte de *roaming*.

3.5.3.2 Kerberos

O Kerberos é um protocolo de autenticação criado pelo MIT (*Massachusetts Institute of Thecnology*) em meados dos anos 80, para fornecer um serviço de autenticação forte e centralizado em sistemas heterogéneos e distribuídos. Sofreu várias evoluções sendo a sua última versão a V5 definida no RFC 4120 do grupo de trabalho Kerberos da IETF [18].

O seu funcionamento baseia-se em criptografia simétrica e numa entidade de confiança (*Trusted Third Party*), o KDC (*Key Distribution Center*), que é composto por dois serviços independentes: o AS (*Authentication Server*) e o TGS (*Ticket Granting Server*). Todas as entidades na rede (clientes e servidores, *principals* no jargão do Kerberos) têm se registar no AS de forma a obter uma chave secreta partilhada unicamente pelo KDC e pela entidade. O AS mantém uma base de dados com todas as entidades registadas e respectivas chaves secretas. O conhecimento da chave secreta serve como prova da identidade de uma entidade.

Quando uma entidade cliente (*principal*) pretende aceder a um servidor (outro *principal*), ela começa por fazer um pedido ao TGS de “credenciais” para aceder ao servidor. Este responde com essas “credenciais”

cifradas com a chave do cliente, o que garante que apenas este as pode utilizar. As "credenciais" consistem num "bilhete" (*ticket*) para o servidor e uma chave temporária de sessão. O cliente envia ao servidor o bilhete recebido, que contém a identidade do cliente e a chave de sessão cifradas com a chave do servidor, para garantir que apenas este as pode utilizar. A partir deste momento, a entidade e o servidor estão ambas na posse da chave de sessão. O cliente confia que o servidor é autêntico, porque apenas ele poderia decifrar o bilhete para obter a chave de sessão, e o servidor confia que o cliente é autêntico porque apenas o KDC poderia ter cifrado o bilhete com a sua chave secreta (do servidor) após a verificação da identidade do cliente através da utilização da sua chave secreta (do cliente). A partir deste momento a chave de sessão pode ser utilizada para cifrar a comunicação entre o cliente e o servidor ou para cifrar sub-chaves de sessão, essas sim utilizadas para cifrar a comunicação.

Para evitar ataques através da repetição do envio de bilhetes, estes têm um período de validade, o que implica que contenham informação temporal e que o relógio de todas as entidades na rede esteja sincronizado.

O protocolo Kerberos permite a autenticação entre diferentes domínios de segurança (*realms*) , cada um deles com o seu AS e TGS. Para isso poder acontecer é necessário que se estabeleçam chaves inter-*realms*, ou seja, que o TGS de um *realm* se registe como uma entidade no outro *realm*. Assim, um cliente de um *realm* pode autenticar-se para um servidor noutro *realm*. Esta comunicação *cross-realm* tem contudo algumas fragilidades ao nível da segurança, robustez e performance. Os seguintes *Internet drafts* referem alguns desses problemas e propostas de solução [21-23].

Para utilizarem a autenticação fornecida pelo Kerberos, as aplicações têm que ser "kerberizadas", isto é, tem que suportar este protocolo de autenticação. O Windows 2000 e versões posteriores, Solaris e Linux são exemplos de Sistemas Operativos que suportam o *Kerberos*. No entanto, navegadores (*browsers*) e outras aplicações para funcionar na Internet não estão "kerberizadas".

Devido à reconhecida vantagem da tecnologia de chave pública, sob a forma de certificados X.509, na autenticação da origem de dados e no secretismo das chaves, foram definidas extensões ao *kerberos* para permitir a sua incorporação. Uma delas é a PKINIT, definida pela IETF na RFC 4556, que permite a utilização de chaves assimétricas na autenticação do cliente com o AS [24].

3.5.4. Autenticação "Off-Line"

Na autenticação *Off-Line* não se está dependente de um servidor de autenticação externo e remoto. A autenticação é efectuada pelas partes que pretendem efectuar uma transacção: o cliente autentica o serviço e o serviço autentica o cliente.

Para a autenticação *off-line* é necessária uma infra-estrutura de chave pública. Resumidamente, a autenticação é efectuada utilizando um reduzido número de chaves públicas preestabelecidas. Estas chaves públicas pertencem a entidades certificadoras (CA - *Certification Authority*) que emitem certificados de chave pública para os clientes e serviços, contendo a informação para realizar a autenticação.

Para um cliente autenticar um serviço, deve proceder da seguinte forma: (i) obter o certificado de chave pública do serviço e autenticá-lo utilizando a chave pré-estabelecida da CA que o emitiu; (ii) verificar se o serviço é de facto o possuidor da chave privada correspondente à chave pública do certificado do serviço autenticado. Esta verificação é inerente a um protocolo de comunicação segura, como por exemplo o SSL (*Secure Sockets Layer*) [25]. A autenticação em protocolos de comunicação será analisada na secção 3.9.

A vantagem desta solução é que não requer a comunicação com nenhum servidor de autenticação para efectuar a autenticação. Para efectuar a autenticação uma entidade apenas necessita do certificado pré-estabelecido (da CA) correcto, e pode guardá-lo, não havendo necessidade de comunicar com a CA. Esta (CA) funciona como um servidor de autenticação que mantém o registo das entidades para quem emitiu certificados e, depois de emitir os certificados para as suas entidades, deixa de ser necessária no processo de autenticação, podendo ser mantida desligada.

A desvantagem desta solução é que, por a autenticação ocorrer *off-line*, não é fácil remover entidades [12]. Este assunto será abordado na secção 3.6.5.6.

Este modelo de autenticação parece o mais adequado para a RTS porque não é necessário contactar nenhum servidor de autenticação *on-line*. Com já foi referido, a informação de autenticação pertence às IS que, por serem independentes entre si, podem ter mecanismos de autenticação diferentes. Com a autenticação *off-line* isso deixa de ser problema: apenas é necessário que cada entidade que comunica na RTS possua a sua chave privada, e o correspondente certificado de chave pública, e a chave pública (certificado) da sua CA.

Além de permitir a autenticação *off-line*, uma outra grande vantagem da criptografia de chave pública é o facto de ser suportada nativamente por muitas aplicações da Internet, tais como os *browsers*, os servidores Web, clientes e-mail, etc. Porém, a utilização de chaves assimétricas e certificados de chave pública normalmente obriga ao uso de Infra-estruturas de Chave Pública. Estas são descritas na secção seguinte.

3.6. Infra-estrutura de Chave Pública

Um dos problemas associados à criptografia de chave assimétrica é a garantia da fidedignidade das chaves públicas. Quando se pretende utilizar a chave pública de uma entidade, por exemplo para enviar uma mensagem, coloca-se a seguinte questão: como confiar que uma dada chave pública é de facto do interlocutor pretendido e não de outrem? A Infra-estrutura de Chave Pública (*Public Key Infrastructure* – PKI) surge para resolver este problema [26].

Para isso utiliza certificados digitais de chave pública, vulgarmente designados simplesmente certificados. Um certificado digital é um documento, assinado por uma entidade idónea (*Trusted Third Party* - TTP) – a Entidade de Certificação (*Certification Authority* – CA), que tem como função atestar que uma entidade, ou sujeito, (pessoa ou não) é o dono legítimo da chave pública contida no certificado. Pressupõe-se aqui uma relação de confiança: quem recebe o certificado confia na entidade que o emitiu e nos processos por ela utilizados para a verificação da identidade do sujeito e para a comprovação da posse da correspondente chave privada.

O funcionamento de uma PKI baseia-se na transitividade da confiança: se a entidade A confia na entidade B e a entidade B confia no valor C, então a entidade A também confia no valor C. Ou seja, quando se confia numa CA confia-se em todos os certificados por ela emitidos. É esta propriedade que vai permitir que uma entidade possa validar os certificados de outras entidades.

Uma PKI é uma infra-estrutura constituída por hardware, software, políticas e procedimentos necessários para gerir, criar, armazenar e distribuir chaves e certificados digitais [27]. É constituída pelos seguintes componentes: Entidades de Certificação, Entidades de Registo (*Registration Authorities* – RA), Clientes, Certificados Digitais e Repositórios.

Nas secções seguintes apresentam-se os aspectos mais relevantes de uma PKI.

Uma nota: o estabelecimento de uma PKI é algo de complexo que não envolve apenas questões técnicas. De facto, muito do esforço despendido na implementação de uma PKI está relacionado com aspectos legais.

3.6.1. Entidades Certificadoras

A entidade certificadora (*Certification Authority* – CA) é a entidade de confiança (*Trusted Thrid-Party*) que, através da emissão de um certificado digital, garante a veracidade de uma identidade digital e da sua efectiva posse da chave privada correspondente à chave pública contida no certificado. A CA legitima o certificado assinando-o com a sua chave privada.

Antes de emitir o certificado digital, a CA deve verificar um conjunto de procedimentos destinados a verificar a validade do pedido e a identidade do requerente. Este conjunto de procedimentos depende da política de emissão de certificados definida para a CA. Estas políticas, procedimentos e responsabilidades da CA, devem ser expressas em documentos públicos - *Certificate Policy* e *Certificate Pratice Statement* (CPS) [28].

Uma vez que a CA assina os certificados que emite com a sua chave privada, a protecção desta é crítica. O comprometimento da chave privada de uma CA implica o comprometimento de todos os certificados por ela emitidos. Por este motivo devem ser tomadas medidas de precaução no sentido de proteger a chave privada, tais como: implementação de restrições de acesso à CA, armazenamento da chave privada em dispositivo de segurança, etc.

Outras funções da CA são a revogação dos certificados e a emissão de Listas de Certificados Revogados (*Certificate Revocation Lists* – CRL). A revogação de certificados ocorre quando por algum motivo um certificado deixa de estar válido antes de terminar o seu prazo de validade. De acordo com a sua política de certificação, a CA é responsável por periodicamente publicar uma lista com todos os certificados revogados (CRL) para que quem valida os seus certificados possa verificar se ele foi ou não revogado. Estes assuntos são abordados mais detalhadamente na secção 3.6.5 sobre o ciclo de vida dos certificados.

3.6.2. Entidade de Registo

A Entidade de Registo (*Registration Authority* - RA) é responsável pela interface entre os clientes e a CA. Destina-se a aliviar as tarefas da CA, principalmente nas situações em que a CA lida com muitos pedi-

dos de certificados. Entre as suas funções está a validação dos pedidos de certificados e, depois de emitidos, a entrega ao respectivo cliente.

A RA é particularmente útil em PKIs que servem regiões geograficamente vastas, recebendo e validando as requisições de certificados antes de as enviar para a CA. Algumas PKIs dispensam a RA (por exemplo PKIs de pequena dimensão), sendo a sua funcionalidade garantida pela CA.

3.6.3. Clientes da PKI

Os clientes da PKI são as entidades que requerem certificados digitais à CA ou RA. A requisição do certificado é feita depois de gerado o par de chaves e deve decorrer sobre um canal seguro. Dependendo da política de certificação da PKI, o par de chaves pode ser gerado no cliente ou na CA.

O cliente fica com a responsabilidade de garantir a segurança da sua chave privada. A sua perda pode, por exemplo, impedir a decifra de eventuais documentos cifrados com a sua chave pública, e o seu comprometimento pode, por exemplo, permitir que terceiros não autorizados possam decifrar esses documentos.

O certificado e a chave privada serão depois usados pelo cliente nas operações para as quais o certificado é emitido. Entre operações mais vulgares estão a comprovação de identidade do cliente a um computador remoto e a protecção de mensagens de correio electrónico.

3.6.4. Certificados Digitais de Chave Pública

Como já foi referido, um certificado digital é um documento, assinado por uma entidade idónea, que tem como função atestar que uma entidade (pessoa ou não) é dona legítima da chave pública contida no certificado. Estabelece uma relação de identidade digital fiável entre uma chave pública e um sujeito.

Os certificados digitais são definidos pelo standard ITU-T X.509 [29], no âmbito da definição do serviço de directoria X.500 [30], que está actualmente na versão 3. Esta definição é abrangente, tendo a IETF através do seu grupo de trabalho PKIX [2] definido o perfil de certificados X.509 para a utilização na Internet no RFC 3280 [31].

Um certificado de chave pública é um conjunto de informação que identifica uma entidade, incluindo a sua chave pública, assinado por uma entidade de confiança (CA) após ter verificado a identidade da entidade e confirmado a posse da correspondente chave privada. Podem/devem ser distribuídos livremente, uma vez que por estarem assinados não podem ser alterados ou forjados.

Os vários campos de informação que constam num certificado são apresentados na Figura 5.

[2] PKIX Working Group. Public-Key Infrastructure (X.509) (pkix). http://www.ietf.org/html.charters/pkix-charter.html

Versão
Número de série
Identificador do algoritmo de assinatura
Nome do Emissor (*Issuer*)
Período de Validade: Data e Hora do inicio e do fim
Nome do Sujeito (*Subject*)
Informação da chave pública do sujeito: Identificador do algoritmo e chave pública
Identificador único de Emissor (Opcional)
Identificador único do Sujeito (Opcional)
Extensões (Opcional): Tipo – Crítico / não crítico – Valor
Assinatura: Identificador do algoritmo e valor da assinatura

Figura 5: Campos de informação de um certificado X.509.

Dentro do conjunto dos campos interessa referir os seguintes:

Nome do Emissor (*Issuer*): Nome único X.500, *Distinguished Name* (DN), da CA que assinou e emitiu o certificado. Os DN são especificados através de um conjunto de atributos, dos quais se referem *country* (C), *Organization* (O), *Organizational Unit* (OU).

Período de Validade: Data de início e data de fim do período de validade do certificado.

Nome do Sujeito (*Subject*): identifica a entidade associada com a chave pública armazenada no campo chave pública do sujeito. Deve ser um nome único dentro da CA que emite o certificado e deve ter o mesmo formato *Distinguished Name* que o presente no campo Emissor.

Informação da chave pública do sujeito: Chave pública e identificação dos algoritmos em que a chave pode ser utilizada.

Assinatura: Identificação do algoritmo utilizado para produzir a assinatura e o valor da assinatura digital do certificado, produzida pela CA Emissora, utilizando todos os restantes campos do certificado.

Extensões: O campo extensões permite a definição de atributos adicionais para o utilizador, para a chave pública ou para a gestão dos certificados. Permite também a definição de extensões com informação privada, por exemplo extensões que apenas fazem sentido no contexto de uma aplicação ou de uma empresa.

As extensões podem ser definidas como críticas ou não críticas. No processo de validação de um certificado, a presença de uma extensão desconhecida definida como crítica deve resultar na rejeição do certificado. Uma extensão não crítica pode ser ignorada se não for reconhecida.

As extensões são identificadas através de OIDs (*Object Identifiers*) em formato ASN.1 (*Abstract Syntax Notation*). Não pode haver mais do que uma extensão com o mesmo nome. O grupo de trabalho PKIX definiu várias extensões. As mais relevantes são:

Authority Key Identifier: Identificador da chave pública correspondente à chave privada utilizada para assinar o certificado.

Subject Key Identifier: Identificador para a chave pública no certificado. Útil para a construção de cadeias de validação.

Key Usage: Define quais as utilizações para a chave no certificado: cifra, assinatura, etc.

Certificate Policies: Identifica as políticas da CA que foram observadas para a emissão do certificado.

Basic Constraints: Indica se o certificado é um certificado de CA ou de cliente. Se for de CA pode definir restrições ao comprimento da cadeia de validação. Apenas se utiliza em certificados de CA.

Name Constraints: Define o espaço de nomes para os quais uma CA pode emitir certificados. Válido apenas para CA.

Policy Constraints: Coloca restrições na construção as cadeias de validação para obrigar a que todos os certificados tenham uma determinada política.

Extended Key Usage: Indica uma ou mais finalidades para as quais o certificado pode ser utilizado, para além das indicadas na extensão *Key Usage*. Esta extensão normalmente só se aplica a utilizadores finais, e pode ser crítica ou não-crítica.

CRL Distribution Points: Indica como é que se obtém a CRL Esta extensão deve ser não-crítica, mas recomenda-se a sua utilização.

Freshest CRL: Indica como obter o delta-CRL. Esta extensão deve ser não-crítica.

Authority Information Access: Indica como aceder a informação e serviços do emissor do certificado no qual a extensão aparece. Tipicamente utiliza-se para indicar a localização dos certificados de chave pública da CA que emitiu o certificado. Esta extensão deve ser não-crítica.

3.6.5. Ciclo de Vida dos Certificados

Os certificados têm um ciclo de vida com várias fases e que começa com o pedido de emissão do certificado. Estas fases são detalhadas nas secções seguintes.

3.6.5.1 Pedido de emissão de certificado

O sujeito requerente (cliente) fornece os seus dados pessoais e, após a validação desses dados, que pode ser presencial ou não dependendo da política da CA, é gerado um par de chaves e o pedido segue para a CA. O pedido pode ser efectuado numa RA ou numa CA dependendo da arquitectura da CA.

3.6.5.2 Emissão do certificado

Depois de recebido o pedido do certificado na CA, os dados são analisados, podendo ou não haver inclusão de mais dados, sendo então dada autorização para a emissão. A entrega do certificado pode ser das mais variadas formas como, por exemplo, e-mail, em *smart card*, etc.

3.6.5.3 Validação do certificado

Os certificados devem ser validados sempre que, no contexto de uma qualquer operação, uma entidade o apresente para a sua autenticação. A validação do certificado é feita através da validação da assinatura da sua entidade emissora. Se quem recebe o certificado conseguir validar a assinatura da entidade que o emitiu, e o certificado estiver dentro do seu período de validade, então pode concluir que ele é válido.

Para a validação de um certificado é necessário construir uma cadeia de certificados que una o certificado a validar a um certificado de confiança de quem valida. A cadeia começa pelo certificado a validar, seguindo-se o certificado da sua entidade emissora, e assim sucessivamente até atingir um certificado da confiança de quem valida.

A operação de validação começará então pelo certificado de confiança, utilizando a sua chave pública para validar a assinatura do certificado seguinte na cadeia, e assim sucessivamente até chegar ao certificado que se pretende validar. O certificado apenas é considerado válido se as assinaturas de todos os certificados na cadeia foram validadas. Este assunto será abordado novamente na secção 3.6.6 referente aos modelos de confiança.

3.6.5.4 Renovação de certificados

O processo de renovação de certificado é semelhante ao processo de pedido e emissão. Por o sujeito já ser conhecido, normalmente a quantidade de dados fornecida é menor e o processo de validação não é tão complexo. Em certos sistemas esta renovação é feita automaticamente, com o pedido de renovação a ser assinado com o certificado prestes a ser renovado.

3.6.5.5 Arquivo

Os certificados emitidos são depois colocados em arquivo, tipicamente um serviço de directoria, com os seguintes objectivos: por um lado, sendo o arquivo público, para publicitar os certificados e permitir a sua obtenção por quem deles necessita; por outro, para efeito de arquivo porque os certificados continuam a ser necessários para verificar actos praticados com a correspondente chave privada, mesmo depois de expirado o seu prazo de validade.

O arquivo também se pode aplicar a chaves privadas, não sendo obviamente público, nos casos em que o par de chaves seja gerado pela CA e ela mantenha uma cópia da chave privada (recomendável em chaves privadas utilizadas na decifra de documentos).

3.6.5.6 Revogação de Certificados

Todos os certificados contêm a indicação do seu período de validade, ou seja, o período dentro do qual podem ser utilizados. No entanto, ocorrem situações em que o certificado deixa de ser válido, sem que o seu período de validade tenha expirado. Estas situações podem ocorrer pelas mais diversas situações, como por exemplo: quebras de vínculo contratual, perda, comprometimento, etc. Estas situações exigem um meca-

nismo para divulgar a informação de revogação e impedir que esses certificados sejam aceites e considerados válidos.

O método mais simples para publicitar a revogação dos certificados é através das Listas de Certificados Revogados (*Certificate Revogation List* – CRL), que consiste na disponibilização periódica de uma lista datada e assinada pela CA com todos os certificados por ela emitidos e que foram revogados. Esta lista deve ser consultada por todas as entidades que pretendam validar um certificado.

A desvantagem deste método é a dimensão que a CRL pode atingir que dificulta o seu processamento. Para ultrapassar esta dificuldade utilizam-se CRL incrementais, Delta-CRL, que apenas publicam as alterações em relação à CRL anterior. No entanto, não prescinde da publicação periódica da CRL completa, *base* CRL.

Outra desvantagem é o que pelo facto da sua publicação ser periódica, haver um atraso entre o instante em que o certificado é considerado revogado e o instante da publicação da CRL. No máximo este atraso é igual ao período de publicação.

Outro método de publicação de certificados revogados é o OCSP – *Online Certificate Status Protocol*, que pretende ultrapassar algumas limitações da CRL, através de respostas imediatas e actualizadas a questões acerca do estado de um certificado. Este serviço é tipicamente disponibilizado sobre HTTP. Tem algumas limitações como sendo a validação ser efectuada certificado a certificado e validar apenas o certificado e não a sua cadeia de certificação. Caso o OCSP se baseie na publicação da CRL ou delta-CRL, não resolve o problema do atraso entre a revogação e a sua publicitação.

Esta é uma área ainda em discussão, estando o grupo de trabalho da PKIX a trabalhar num novo protocolo, SCVP – *Server-based Certificate Validation Protocol*, que neste momento se encontra sob a forma de *Internet-Draft*, estando prevista a sua passagem a *Proposed Standard* RFC em Abril de 2007.

Em casos específicos de certificados de curta duração pode-se prescindir da utilização de mecanismos de revogação dos certificados. Exemplos típicos incluem certificados para transacções financeiras de valores extremamente elevados em que os certificados são emitidos com intervalos de validade de horas [26].

3.6.6. Modelos de Confiança

A necessidade de modelos de confiança surge pela necessidade de existir múltiplas CA. Por vários motivos, desde operacionalidade a questões de confiança, não faz sentido haver apenas uma única CA a emitir certificados a nível mundial. Mesmo em ambientes mais limitados, como numa empresa pode fazer sentido ter mais do que uma CA: por exemplo, para limitar riscos em caso de comprometimento de chaves, por questões geográficas, para balanceamento de carga caso haja muitos utilizadores com certificados, por diferentes departamentos terem políticas de certificados diferentes, etc.

Havendo múltiplas CA, colocam-se questões do género: como estabelecer relações de confiança entre CA para que os certificados emitidos por uma CA possam ser aceites pela outra? Como é que uma entidade sabe quais os certificados em que pode confiar? Como controlar a confiança nas relações entre CA?

3.6.6.1 Modelo de CA única

Este é o modelo mais básico de arquitectura. Há apenas uma única CA que emite e distribui todos os certificados pelas entidades cliente. Todas estas confiam na CA e todas elas utilizam apenas certificados por ela emitidos. Há um único ponto de confiança comum entre todas as entidades, a CA: é a âncora, ou raiz, de confiança.

A confiança na CA nasce da confiança na segurança da chave privada da CA, uma vez que é ela que assina todos os certificados emitidos. A verificação da validade dos certificados faz-se utilizando a chave pública da CA para validar a sua assinatura no certificado.

O comprometimento da chave privada da CA implica que todos os certificados por ela emitidos fiquem também comprometidos.

Este modelo é muito limitado e não é escalável, aplicando-se apenas em situações sem grandes requisitos de segurança e de número muito reduzido de certificados.

3.6.6.2 Modelo hierárquico

O modelo hierárquico de confiança consiste numa árvore de CA, no topo da qual está a CA raiz, que actua como raiz, ou âncora, de confiança para todas as entidades no seu domínio (na sua árvore). A Figura 6 ilustra este modelo de confiança.

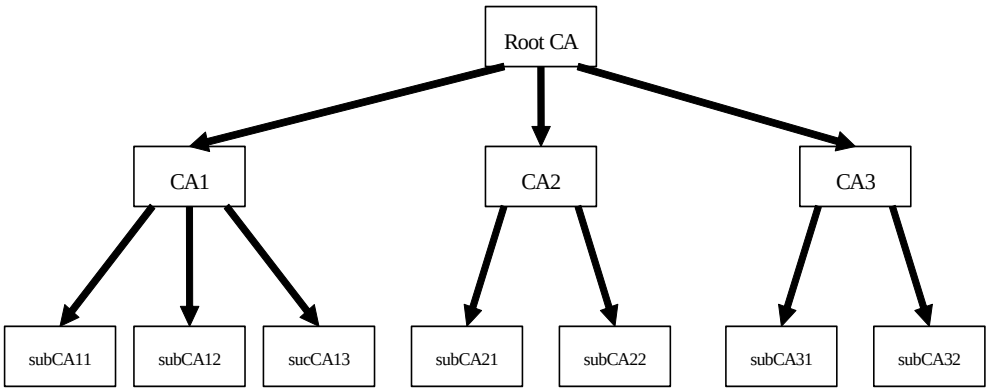


Figura 6: Modelo de confiança hierárquico

Neste modelo existe uma clara relação superior – subordinado entre CA de níveis diferentes. A CA raiz assina os certificados das CA no segundo nível, estas assinam os certificados das CA no 3º nível, e assim sucessivamente. Cada CA tem apenas uma CA superior, que assina o seu certificado. A excepção é a CA raiz que não tem nenhuma CA superior e assina ela própria o seu certificado: é a âncora de confiança de toda a hierarquia.

Todas as CA que não são raiz designam-se por CA subordinadas e podem ser CA emissoras ou CA intermédias. As CA emissoras emitem certificados para os clientes da PKI. As CA intermédias, além dos certificados dos clientes, emitem também certificados para CA subordinadas (as boas regras recomendam que emitam apenas para CA subordinadas, funcionando como um nível de segurança adicional).

O número de níveis nesta hierarquia não é obrigatoriamente de 3 como ilustrado na figura, podendo ter uma maior, ou menor, profundidade. No entanto, quanto maior a profundidade, maior a dificuldade na gestão da PKI.

Para validar um certificado, é necessário estabelecer um caminho de certificação entre esse certificado e a âncora de confiança. O caminho de certificação é único e composto pelo certificado a validar, a âncora de confiança e por todos os certificados das CA intermédias entre eles. A validação do certificado implica a validação de todos os certificados no caminho de certificação, partindo da âncora de confiança. Todos os certificados têm que ser válidos.

3.6.6.3 Modelo distribuído

No modelo de confiança distribuído (*distributed*), também designado em malha (*mesh*) e *peer-to-peer*, não há relações de subordinação entre CA. Todas estão ao mesmo nível (*peers*), estabelecendo entre si relações de confiança (normalmente bidireccionais mas também podem ser unidireccionais) conforme as suas necessidades. Como neste modelo não há uma CA central, implica que não haja uma âncora de confiança única para toda a PKI, como acontecia no modelo hierárquico. Cada CA funciona como âncora de confiança para as suas entidades cliente. A Figura 7 contém um exemplo de uma PKI de modelo distribuído.

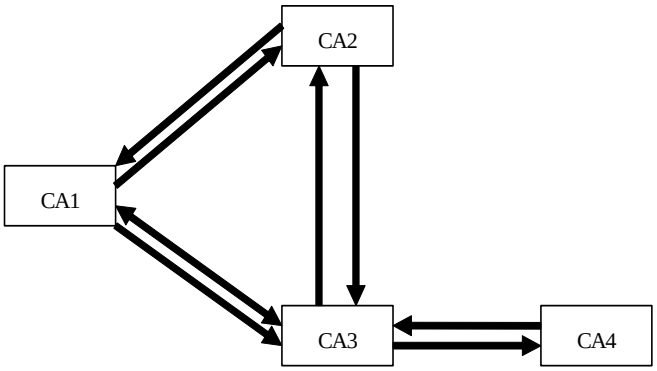


Figura 7: Modelo de confiança distribuído

As relações de confiança podem ser estabelecidas com recurso a certificação cruzada (*cross-certification*) ou a listas de certificados de confiança (*certificate trust lists*).

Certificação cruzada consiste na emissão de um certificado por uma CA para outra CA. Com a emissão deste certificado, a CA que o recebe fica de facto como uma CA dependente da que o emitiu. O certificado cruzado permite o estabelecimento de um caminho de certificação que permite que os certificados emitidos pela CA que recebeu o certificado cruzado possam ser validados pelas entidades clientes da CA que o emitiu.

A certificação cruzada é sempre unidireccional. Para o estabelecimento de um relacionamento bidireccional é necessário que ambas as CA emitam certificados cruzados, uma para a outra. Para a validação de certificados, as entidades de cada uma das CA continuam a confiar apenas na âncora de confiança da respectiva CA.

Uma lista de certificados de confiança é uma lista assinada de certificados raiz que um administrador considera de confiança para determinados propósitos. Além da sua âncora de confiança, as entidades da CA passam a confiar, também, nos certificados raiz das CA que constam na lista de certificados de confiança, podendo utilizá-las na validação de certificados.

A construção de caminhos de certificação é agora complexa, uma vez que pode haver vários caminhos entre quaisquer duas CA. Um dos problemas neste modelo é localizar os certificados cruzados que estabelecem as relações de confiança, para a construção dos caminhos de certificação.

Um outro problema associado a este modelo é o número de relações de confiança uma CA possa estabelecer, que pode tornar-se elevado e de difícil gestão. Ou seja, pouco escalável.

3.6.6.4 Modelo híbrido

Cada uma das CA participantes na rede de relações de confiança do modelo distribuído é a âncora de confiança para as suas entidades. Podem, então ser CA raiz de hierarquias de CA (modelo hierárquico) que estabeleceram relacionamentos de confiança entre si com vista ao reconhecimento mútuo dos seus certificados. Desta forma-se constitui-se um designado modelo híbrido. Esta arquitectura híbrida resulta tipicamente da interligação de PKIs independentes e já existentes.

O modelo híbrido resulta tipicamente da interligação de CA de PKIs que de outra forma permaneceriam separadas. Várias alternativas existem para a interligação, sendo as mais vulgares: (i) listas de certificados de confiança, (ii) certificação cruzada *peer-to-peer* e (iii) através de uma CA ponte (*bridge CA*) [32]. Os dois primeiros mecanismos já foram abordados no modelo distribuído, uma vez que também lá são utilizados no estabelecimento de relacionamentos entre as CA.

No modelo ponte (*bridge*), também designado *hub-and-spoke*, é constituída uma CA, a *bridge* CA, com o papel específico de facilitar a interligação entre PKIs. A interligação entre as CA é efectuada através da certificação cruzada entre a *bridge* CA e as CA raiz que se pretendem interligar. O papel da *bridge* CA não é ser a âncora de confiança, mas apenas de facilitar a integração das várias CA. Cada uma das PKIs individuais continua com a sua âncora de confiança inalterada.

A Figura 8 apresenta um diagrama com uma *bridge* CA a interligar as CA raiz de três PKIs de modelo hierárquico.

É importante referir que no modelo híbrido, o estabelecimento dos relacionamentos não é obrigatoriamente efectuado através das CA raíz, podendo ser efectuado por CA em qualquer nível na hierarquia de acordo com as necessidades das organizações.

A grande vantagem do modelo *bridge* é uma potencial maior escalabilidade, face ao modelo *peer-to-peer*, dado o menor número de ligações que são necessárias para interligar um mesmo número de CA.

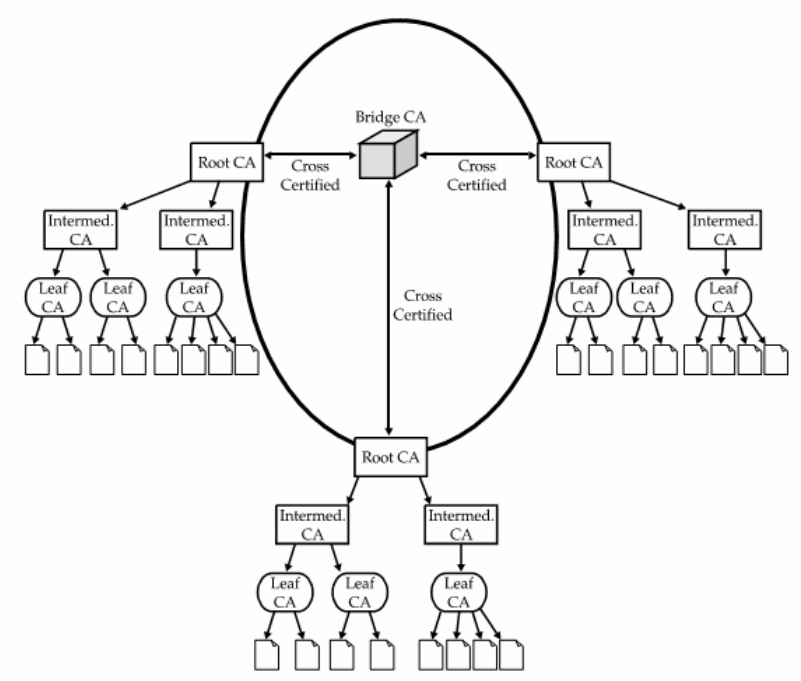


Figura 8: Bridge CA interligando três PKIs de modelo hierárquico.

3.6.6.5 Controlo da confiança na certificação cruzada

Como se viu o mecanismo de certificação cruzada permite a extensão de confiança entre CA que doutra forma seriam independentes. No entanto, esta extensão de confiança se não for controlada pode ter efeitos não desejados. Por exemplo, devido à transitividade da confiança, se A confia em B e B confia em C, então A confia em C. Colocando isto em termos de organizações, se a organização A confia nos certificados da organização B, e B confia nos certificados da organização C, então A confiaria nos certificados emitidos pela organização C. Este efeito pode nem sempre ser pretendido, por exemplo se a organização A for rival da organização C. Para impedir este efeito existem os mecanismos de controlo da confiança.

O controlo da confiança é efectuado através de extensões standard dos certificados, nomeadamente: (i) restrições de nome (*name constraints*), (ii) restrições de política (*policy constraints*) e (iii) restrições de comprimento de caminho (*path-length constraints*) [32].

As restrições de nome permitem que a confiança se aplique apenas a um restrito espaço de nomes da outra organização, como por exemplo, uma pessoa específica, uma secção, um departamento, etc.

As restrições de política permitem restringir certificados com base nas políticas de emissão. Por exemplo, aceitar apenas os certificados da outra organização que tenham sido emitidos após validação presencial do cliente.

As restrições de comprimento de caminho permitem limitar a transitividade da confiança exemplificada no início desta secção. Permite especificar o número máximo de certificações cruzadas que podem existir num caminho de certificação. Por exemplo, tomando como base o exemplo anterior, permite especificar

que A reconhece os certificados de B como válidos, mas rejeitar todos os certificados de outras organizações com quem B tenha relações de confiança.

3.6.7. Serviços baseados em PKI

A PKI é fundamental como suporte de confiança para pares de chaves assimétricos e certificados de chave pública utilizados em vários serviços, tais como: Assinatura digital, autenticação de cliente, cifra de documentos, etc.

A indicação de qual, ou quais, os serviços em que o certificado pode ser utilizado é colocada nas extensões *Key Usage* e *Extended Key Usage*.

3.7. Infra-estrutura de Gestão de Privilégios

Uma Infra-estrutura de Gestão de Privilégios (*Privilege Management Infrastrucure* – PMI) é o equivalente à PKI para a gestão de autorizações ou permissões de acesso a objectos. Tal como a PKI, baseia-se na 4ª edição da recomendação X.509 da ITU-T [29]. A IETF no RFC 3281 [33] define um perfil de certificados de autorização *(Authority Cerificates* – AC) para utilização na Internet.

Os certificados de autorização são muito semelhantes aos certificados de identificação (PKC) utilizados na PKI sendo a principal diferença entre eles a não inclusão no AC de nenhuma chave pública.

É frequente a confusão entre os certificados de identificação e de autorização. Uma analogia apresentada no RFC 3281 é considerar o PKC como um passaporte que identifica o indivíduo, que tipicamente tem um prazo de validade alargado e que não deve ser de fácil obtenção. Por sua vez o AC pode ser comparado a um visto, que é emitido por uma outra autoridade, tipicamente tem uma duração curta, e necessita da apresentação do passaporte para a sua obtenção.

Apesar de a informação de autorização poder ser veiculada num PKC, utilizando as extensões, tal não é recomendado pelas seguintes razões: (i) porque a informação de identificação tipicamente não tem o mesmo tempo de vida do que a informação de autorização e (ii) quem emite o certificado de identificação pode não ter acesso à informação de autorização. Normalmente a informação de autorização tem um tempo de vida inferior à informação de identificação, pelo que a incorporação da informação de autorização no PKC dá origem a certificados com um tempo de vida curto.

A utilização dos AC não prescinde a utilização de PKC, pelo que deve existir uma ligação entre o certificado de autorização e o correspondente certificado de identificação para quem a autorização se destina.

Os certificados de autorização são emitidos por uma *Attribute Authority* (AA), que é o equivalente numa PMI de uma CA numa PKI.

A distribuição dos certificados pode ser feita de dois modos: (i) *push* em que o cliente envia o seu AC para o servidor que necessita de decidir a autorização e (ii) *pull* em que o cliente apenas se autentica sendo da responsabilidade do servidor ir obter as AC correspondentes a um repositório de ACs. A vantagem do modo *push* é libertar o servidor do trabalho de pesquisa das AC e por isso ser mais eficaz, no entanto tem a

desvantagem de necessitar de um cliente adaptado para lidar com os AC. O modo *pull* é precisamente o inverso, sendo de destacar a vantagem de o cliente não necessitar de nenhuma adaptação específica para funcionar numa PMI.

3.8. Dispositivos de autenticação

Os dispositivos de autenticação implementam a autenticação dos utilizadores através dos factores de autenticação já discutidos. Normalmente utilizam mais do que um factor de autenticação. Em seguida faz-se uma análise a três tipos de dispositivos de autenticação mais comuns: *One-Time Passwords*, *Smart Cards* e dispositivos biométricos.

3.8.1. One-Time-Passwords

Um dispositivo de *One Time Password* (OTP) funciona como uma "calculadora", normalmente protegida com um PIN, que, durante uma ligação, fornece ao utilizador uma senha (*password*) com uma duração limitada. As senhas apenas são válidas durante um período limitado de tempo, e apenas podem ser utilizadas uma vez, pelo que o comprometimento de uma senha não é crítico. Além disso, conhecendo uma senha não é possível determinar qual irá ser a senha seguinte.

Em termos do princípio de funcionamento para gerar a senha, existem basicamente três tipos de OTP. Todos se baseiam em algoritmos matemáticos podendo além disso basear-se na senha anterior, num contador ou no relógio que tem que estar sincronizado com o do servidor de autenticação.

Para a RTS contudo não são um dispositivo interessante. Além do seu custo, o modelo de autenticação a que se aplicam é o de Autenticação Indirecta, o que como já analisámos não é o ideal para a RTS.

A Figura 9 mostra um dispositivo de *One-Time Password*,um SecurID, produzido pela RSA[3].

Figura 9: Dispositivo *One-Time Password*: SecurID da RSA

[3] http://www.rsa.com

3.8.2. Smart cards

Um *smart card* é um cartão de plástico, com as dimensões de um cartão de crédito, que com um microprocessador e memória embebidos no seu interior. Possui capacidade de armazenamento seguro de dados, e um módulo criptográfico no seu interior. Isto torna-o o dispositivo ideal para ser utilizado em conjunto com uma PKI no modelo de autenticação *off-line*, contribuindo para a segurança das chaves privadas e, portanto, para o aumento global da confiança. É além disso importante como potenciador da mobilidade dos seus utilizadores.

O aumento da segurança promovido pelo *smart card* é devido às seguintes características:

Possuir no seu interior um processador criptográfico capaz de gerar pares de chaves assimétricas e impedir a exportação para o exterior da respectiva chave privada. Desta forma, garante-se a exclusividade da chave privada o que é fundamental para aplicações como a assinatura digital em que não pode haver a menor suspeita de que a chave privada não seja totalmente secreta. Reduz também os riscos do comprometimento da chave privada através de vírus, *spyware* e outro software mal intencionado.

Obrigar a introdução de um código de segurança, um PIN, para que possa ser utilizado. Este código deve ser do conhecimento exclusivo do possuidor do *smart card*, tendo este possibilidade de o alterar sempre que o considere conveniente. Desta forma permite a autenticação baseada em dois factores: (i) a posse do cartão e (i) o conhecimento do respectivo PIN.

Dependendo da sua capacidade de memória, o *smart card* pode ter capacidade para o transporte de várias chaves privadas e de vários certificados digitais de chave pública. Isto permite, o transporte de certificados de confiança, além do transporte dos certificados digitais das chaves públicas correspondentes às suas chaves privadas. Esta característica é importante porque garante que a protecção e a integridade dos seus certificados de confiança, utilizados na validação de cadeias de certificação.

Como a chave privada nunca sai para o exterior e o cartão é portátil, potencia a mobilidade do seu possuidor ao permitir a utilização das suas credenciais nos vários computadores a que tenha de aceder.

Possuir protecções contra a violação física, que fazem com que o seu conteúdo seja destruído quando se tenta remover o invólucro de protecção física do *smart card*,

Possuir protecções contra tentativas de adivinhar o PIN, bloqueando ao fim de um número reduzido de introduções inválidas consecutivas, tipicamente três.

Têm como desvantagem o aumento do custo de implementação do sistema, uma vez que é necessário dotar os computadores em que são usados 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 10: Exemplo de *smart card* e leitor USB *dongle* (OMNIKEY CardMan)

Na escolha dos *smart cards*, deve-se ter em conta o aspecto da mobilidade dos utilizadores. O problema está na disponibilidade dos *drivers* e *software* para os ler nas máquinas em que é suposto serem utilizados. Como existem *smart cards* de diferentes fabricantes, há sempre o risco de o utilizador 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) [34]. Além disso, a maioria dos leitores mais recentes reconhecem *smart cards* de diversos fabricantes.

Outro problema associado aos *smart cards* é que a sua perda, ou esquecimento, impossibilitam o seu proprietário de realizar as operações para as quais ele era necessário. Recordar que não existem cópias das chaves privadas que residem no interior do *smart card* e, portanto, não é possível o fornecimento de uma segunda via com a mesma informação criptográfica.

3.8.3. Dispositivos biométricos

Os dispositivos biométricos são dispositivos que se baseiam na leitura de características físicas das pessoas, tais como a impressão digital, a íris ou voz, para verificar a sua identidade. Estas características são únicas em cada pessoa e não podem ser perdidas, roubadas ou esquecidas, o que se torna numa grande vantagem para estes dispositivos porque são os únicos que conseguem reconhecer de facto uma pessoa.

A validação da característica biométrica tem que ser sempre feita localmente. Caso contrário, pode ser capturada e utilizada em ataques por repetição da característica. Por isso, o único ambiente onde a biometria é utilizada, sem recurso a técnicas adicionais, é no controlo de acesso físico de pessoas a áreas reservadas onde o leitor e o dispositivo autenticador estão ligados fisicamente e em local supervisionado [35].

Para a utilização em autenticação remota, a tecnologia biométrica tem que ser combinada com técnicas criptográficas. Existem vários fabricantes que disponibilizam dispositivos *smart card*, protegidos por uma característica biométrica em substituição do PIN (2 factores de autenticação) ou em conjunto com o PIN (3 factores de autenticação). Cartões deste género normalmente aplicam-se em aplicações em que a segurança é crítica.

A Figura 11 ilustra a utilização de um cartão *smart card* com capacidades biométricas, e a Figura 12 mostra um destes cartões da FIDELICA Microsystems[4].

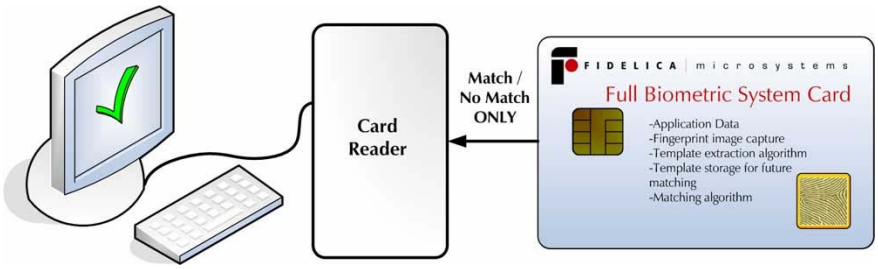


Figura 11: Ilustração da utilização de um cartão *smart card* com capacidades biométricas

Figura 12: Cartão *Smart Card* com capacidades biométricas da Fidelica Microsystems

A desvantagem deste tipo de sistemas é o seu custo. Em caso de alteração da característica física, por exemplo por um ferimento, não permitem a autenticação do seu possuidor.

3.9. Autenticação em protocolos para comunicação segura

A tecnologia PKI pode ser utilizada para fornecer serviços de autenticação em protocolos de comunicação segura. Os protocolos seguros mais comuns utilizados em comunicações através da Internet são o SSL/TLS e o IPSec.

3.9.1. Secure Sockets Layer / Transport Layer Security (SSL/TLS)

O SSL/TLS é um protocolo de comunicação segura que teve a sua origem na Netscape, fabricante de um dos *browsers* pioneiros na história da Internet, para a transmissão de informação de forma segura. O TLS é uma evolução do SSL, tendo a mudança de nome ocorrido com a sua adopção como recomendação IETF, com o RFC 2246 [36]. A versão actual é a 1.1, e encontra-se especificada no RFC 4346 [25]. As diferenças entre as duas versões não são grandes, mas são suficientes para não serem inter operáveis. No entanto, o TLS é capaz de dialogar com o SSL v3.0. A sua utilização mais frequentemente é na segurança do protocolo HTTP, que está definida no RFC 2812 [37].

[4] http://www.fidelica.com

Em termos da pilha protocolar, este protocolo constitui-se como mais uma camada protocolar localizada entre a camada de transporte e a camada de aplicação, como se mostra na Figura 13, fornecendo segurança na comunicação entre dois interlocutores e permitindo a sua autenticação.

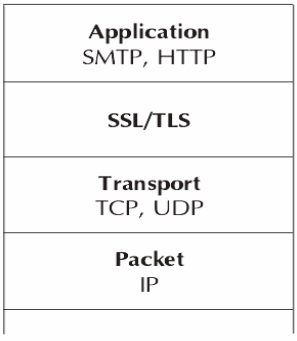


Figura 13: Localização do SSL/TLS na pilha protocolar TCP

As vantagens de implementar o SSL/TLS como uma nova camada protocolar é que exige alterações mínimas às camadas adjacentes e permite-lhe fornecer os seus serviços a vários protocolos de aplicação.

Este protocolo tornou-se o standard de-facto em termos de comunicação segura na Internet, podendo ser utilizado por várias protocolos de aplicação, tais como o HTTP e FTP, sendo suportado pela grande maioria dos *browsers* e servidores Web.

O protocolo caracteriza-se por ter uma fase inicial de negociação em que ocorre a autenticação dos interlocutores e a negociação de chaves para a segurança da comunicação durante o resto da sessão. Pode ser utilizado sem autenticação dos interlocutores, com autenticação apenas do servidor, ou com autenticação mútua do servidor e do cliente. Nos *browsers* são normalmente utilizadas as duas últimas formas de autenticação.

Do ponto de vista da sua utilização na RTS, este protocolo é interessante porque permite ter comunicação segura entre os utilizadores e os portais, bem como a autenticação mútua das entidades. Baseia-se em serviços PKI (certificados de chave pública) para efectuar a autenticação dos interlocutores e para negociar de forma segura os parâmetros da restante ligação, nomeadamente o tipo de cifra simétrica a utilizar (comprimento da chave, algoritmo, etc.).

O SSL também tem as suas desvantagens. Uma delas não é importante no contexto da RTS que é o não suportar comunicação sobre UDP. A outra, que é importante para a RTS, é que o SSL não garante o não repúdio da comunicação, ou seja, não impede que uma das partes possa negar que participou na transacção.

Um outro aspecto que convém realçar é que por muito boa que seja a segurança na comunicação, ela cai por terra se o computador não for seguro. Ou seja, nenhum protocolo protege a informação antes dela ser enviada, nem depois dela ser recebida.

3.9.2. Internet Protocol Security (IPsec)

O *Internet Protocol Security* (IPsec) [38] é um conjunto de protocolos, definidos pela Internet Engineering Task Force (IETF), que fornece serviços de segurança à camada IP da pilha protocolar TCP/IP. Estes serviços são fornecidos como uma extensão de segurança à camada IP, compatível com a norma IPv4 e obrigatória na norma IPv6. Desta forma, o IPSec pode ser usado onde normalmente se usaria o IP, como se ilustra na Figura 14, o que significa que é utilizado de forma transparente para as aplicações.

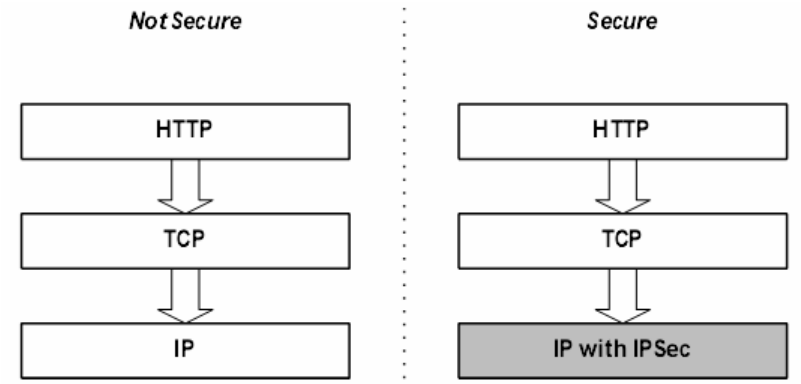


Figura 14: Integração do IPsec na pilha protocolar do TCP/IP.

Os serviços de segurança disponibilizados pelo IPSec são: confidencialidade, autenticidade, integridade de dados e protecção contra repetições. Estes serviços são implementados tendo como base dois protocolos: o *Authentication Header* (AH) [39] e o *Encapsulating Security Payload* (ESP) [40]. Ambos os protocolos funcionam adicionando informação ao cabeçalho dos datagramas IP e ambos funcionam com diversos algoritmos criptográficos.

O IPSec utiliza uma *Security Association* (SA) [38] para definir uma ligação segura entre a origem e o destino. Um SA é unidireccional. Para implementar comunicação segura bidireccional devem ser criadas duas SA, uma em cada sentido. Ambos os protocolos, AH e ESP, podem ser usados numa SA, isoladamente ou em simultâneo.

A comunicação com o IPSec pode ser efectuada de dois modos: modo de transporte e modo túnel. Em modo transporte o AH ou ESP alteram o datagrama IP original; em modo transporte o datagrama IP original é encapsulado nos dados de outro datagrama IP e é este último que é alterado pelo AH ou ESP.

O IPSec utiliza o protocolo IKE [41] para a autenticação mútua entre interlocutores e para o estabelecimento e manutenção das SA entre os mesmos. A autenticação pode ser efectuada de 3 modos: (i) com recurso a chaves secretas partilhadas, a (ii) pares de chaves assimétricas com chaves públicas pré-distribuídas ou a (iii) pares de chaves assimétricas com certificados X.509 de chaves públicas. Pensando em termos de utilização na RTS, a utilização de chaves partilhadas é uma solução pouco escalável devido ao grande número de chaves que são necessárias para identificar de forma única cada par de interlocutores. A utilização de chaves públicas pré-distribuídas é mais escalável mas pode obrigar a ter mais do que uma chave pública por instituição (para servidores diferentes). A utilização de certificados têm a vantagem de ser escalável, bastan-

do que exista uma cadeia de certificação que permita validar os certificados apresentados mutuamente pela RTS e pelas IS.

4 Trabalhos Relacionados

Neste capítulo são analisados trabalhos relacionados com o presente. Primeiro são analisados dois sistemas de informação médica, um regional (HYGEIAnet) e outro nacional (dinamarquês), que incorporam mecanismos de autenticação fortes. Em relação a estes trabalhos houve bastante dificuldade em obter informação específica sobre o modo como é efectuada a autenticação, nomeadamente sobre aspectos relacionados com as suas PKIs.

Analisa-se também uma arquitectura de autenticação proposta para permitir uma autenticação transparente no *roaming* de estudantes universitários no acesso às redes sem fios das várias universidades. Esta arquitectura serviu de base para a arquitectura simplificada proposta para a RTS.

Finalmente analisa-se a arquitectura de suporte ao Cartão do Cidadão recentemente introduzido em Portugal. A razão para a sua análise é o facto de este poder ser um veículo privilegiado para permitir a autenticação forte dos utentes no acesso à RTS.

4.1. HYGEIAnet

A HYGEIAnet é uma Rede Regional de Informação de Saúde (RHIN – *Regional Health Information Network*) desenvolvida pelo *Institute of Computer Science* (ICS) da *Foundation for Research and Technology – Hellas* (FORTH), da Grécia, e tem como objectivo o fornecimento de um ambiente integrado para os serviços de saúde na ilha de Creta [42], envolvendo tanto profissionais de saúde como pacientes [42, 43]. Nesta rede participam vários hospitais, unidades de saúde primária, como se pode observar na Figura 15 [44].

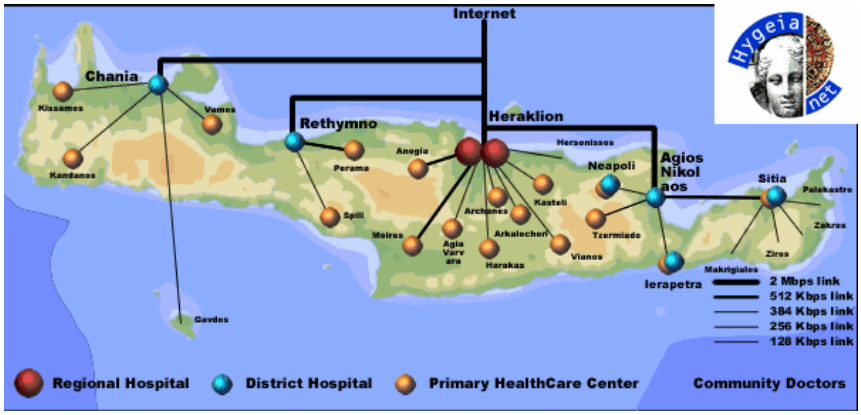


Figura 15: Mapa da rede de comunicações de suporte à HYGEIAnet

Tal como a RTS, pretende desenvolver sistemas de informação que facilitem a comunicação e colaboração entre profissionais de saúde das várias Instituições de Saúde e pacientes. O IEHR (*Integrated Electronic Heath Record*), equivalente ao Processo Clínico Electrónico Regional da RTS, é também um elemento fundamental na sua estratégia para a partilha da informação clínica. É através do IEHR que agregam a informação clínica do paciente, composta por episódios que podem estar dispersos por várias IS.

Em termos de implementação, a sua estratégia de comunicação entre IS baseia-se em *Web Services*, o que permite a virtualização das aplicações *legacy* internas (*wrappers* na arquitectura RTS) e também a partilha de informação através de documentos em formato XML (*Extensible Markup Language*) [45]. Uma das vantagens da utilização de documentos XML é a sua fragmentação: cada um destes fragmentos pode ter origens distintas, bem como assinaturas digitais independentes.

Do ponto de vista da autenticação dos utilizadores, ela é gerida de uma forma centralizada. Todas as aplicações e serviços têm que ser registados num serviço de autenticação para receberem a sua identificação, que é única, e o seu certificado para autenticação.

Os utilizadores também fazem o seu registo nesse mesmo serviço, após o que recebem o seu nome único (*username*), senha e certificado digital. O certificado digital, que pode ser armazenado num *smart card*, é utilizado para autenticação dos utilizadores, e para a assinatura digital para garantir a validade, a integridade e o não-repúdio da informação clínica.

A emissão e gestão dos certificados são efectuadas por uma PKI regional. Toda a RHIN é um só domínio de confiança, o que significa que os certificados são aceites em toda a RHIN. No entanto, não foi possível obter informação detalhada acerca da constituição desta PKI, nomeadamente, de quantas CA, da localização das CA e da informação contida nos certificados.

Quanto à autorização, ela é baseada no modelo de controlo de acessos baseado em papéis (RBAC – *Role-Based Access Control*). Para o efeito, são definidos perfis globais baseados nas funções que os utilizadores desempenham nas organizações de saúde. No entanto, o controlo dos acessos é efectuado localmente por cada aplicação.

Para a responsabilização dos utilizadores e detecção de eventuais quebras de confidencialidade, é colocado um grande enfoque na auditabilidade do sistema. São gerados relatórios exaustivos com a informação de todos os acessos de forma a permitir a reconstrução de todas as operações realizadas por todos os intervenientes. Estes relatórios são também utilizados para o controlo da utilização do sistema e detecção e identificação de intrusos.

4.2. A experiência Dinamarquesa

A MedCom é uma rede nacional de dados e informação de saúde que permite a comunicação segura entre os vários actores da saúde na Dinamarca. Está a funcionar desde 1994 e interliga mais de 2000 hospitais, farmácias, médicos de clínica geral e médicos de especialidade. Além destes, disponibiliza também acesso a pacientes e cidadãos [46].

Esta rede começou por ser uma VAN (*Value Added Network* – Rede Privada de Valor Acrescentado), rede de comunicação EDI, em que as mensagens eram trocadas em formato EDIFACT [47]. Em 2004 iniciou-se o processo de migração para a Internet do transporte das mensagens EDIFACT e a sua extensão de forma a incluir a telemedicina, sítios de informação na WEB e acesso baseado em XML ou EDIFACT a sistemas em hospitais e laboratórios. Actualmente permite o fluxo de informação rápido sob a forma de troca de

dados EDIFACT ou mensagens baseadas em XML entre os sistemas informáticos das instituições de saúde participantes.

Em termos de arquitectura, a rede da MedCom consiste num *Hub* central que interliga as várias redes seguras de saúde formando uma grande rede nacional. Esta rede está implementada sobre a Internet, sendo a segurança garantida em três níveis [48, 49]:

Para garantir a segurança na transmissão, todas as ligações com o *Hub* central são estabelecidas através de túneis VPN (*Virtual Private Network*), como se pode ver na Figura 16. A utilização de túneis VPN permite a reutilização das ligações à Internet que todas as organizações possuem.

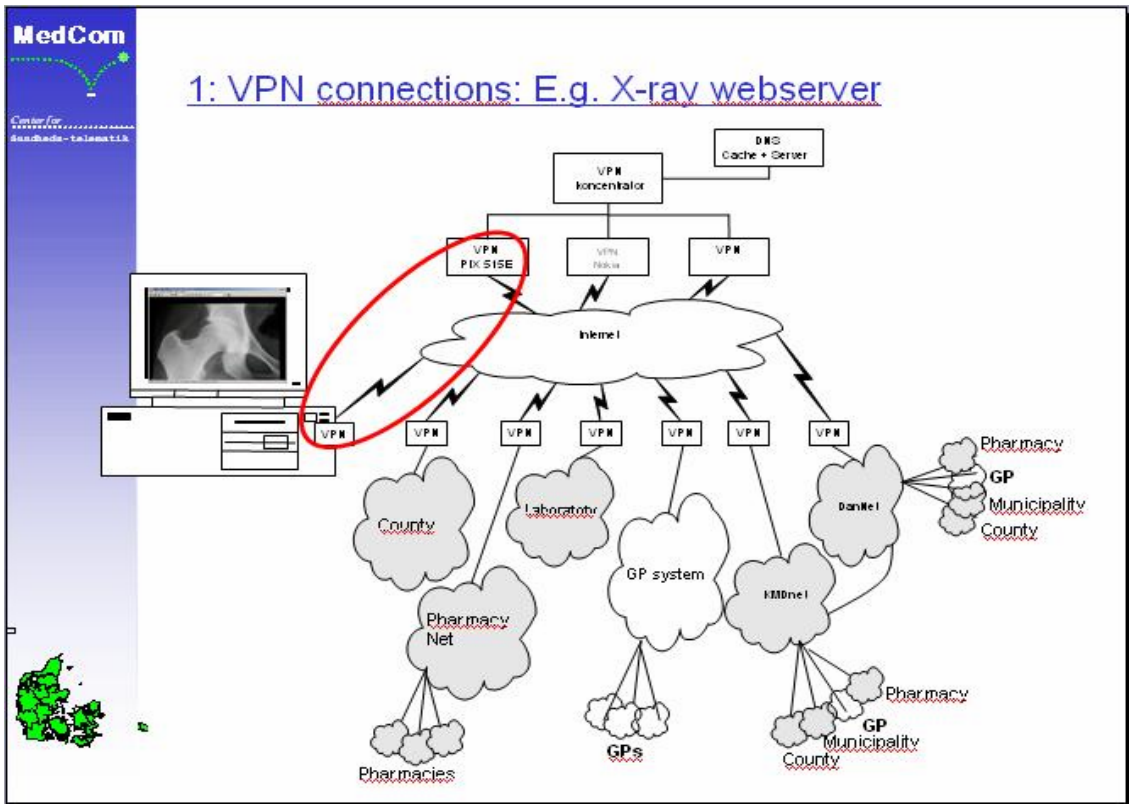


Figura 16: VPNs através da Internet ligando as várias redes da saúde ao *hub* central da MedCom

Um sistema de acordos electrónico que controla os fluxos de entrada e saída de dados de cada uma das redes para a ligação central. Quando duas entidades pretendem comunicar através do nó central, estabelecem uma ligação entre si no sistema de acordos. A identificação do utilizador é feita localmente através da sua identificação e *password*, ou do seu certificado. A Figura 17 mostra um exemplo de ligação entre duas entidades.

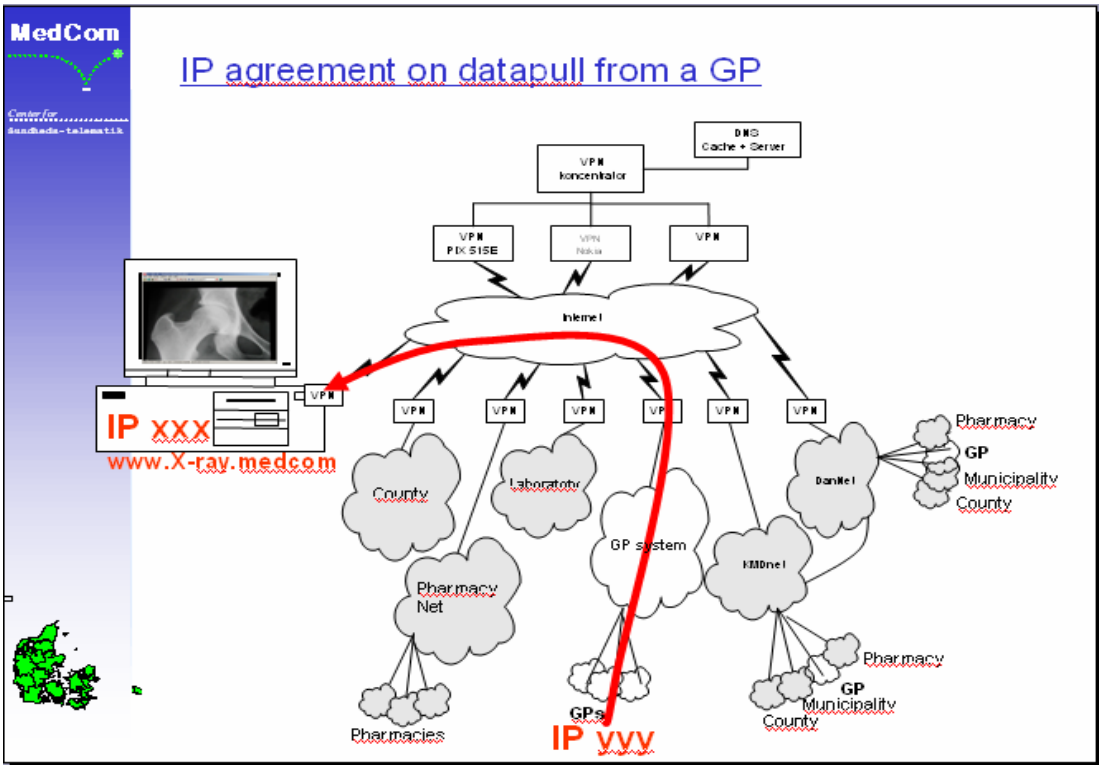


Figura 17: Exemplo de comunicação entre duas redes. Toda a comunicação entre redes passa obrigatoriamente pelo *hub* central e está sujeita a um sistema de acordos entre redes.

Em Dezembro de 2003 entrou em funcionamento o Portal da Saúde (www.sundhed.dk), que transporta todo o serviço de saúde dinamarquês na Internet, permitindo uma melhor comunicação entre os utentes e os profissionais de saúde. Este portal, tem como suporte a rede de dados da MedCom, sem a qual não seria possível ser implementado, e utiliza os standards de mensagens definidos também pela MedCom, como por exemplo o processo clínico electrónico. A arquitectura global da infra-estrutura de suporte ao portal apresenta-se na Figura 18 [50].

A autenticação dos utentes é efectuada com base em certificados, designados OCES (*Offentlige Certificakater til Elektronisk Service*), emitidos pela PKI do governo, e que podem ser utilizados em vários serviços públicos dinamarqueses. Para obter uma solução de autenticação forte, em conjunto com o certificado, é necessária a utilização de um identificador do utilizador e de uma *password* [51].

Quanto aos profissionais, além da sua *password* pessoal, dependendo da sua função podem ter vários certificados [52]:

- Certificado de assinatura digital administrativa da região, hospital ou médico;
- Certificado de assinatura digital de profissional de saúde com a identificação pessoal do profissional
- Certificado digital de autorização para tratamento de pacientes emitido pela *National Board of Health*.

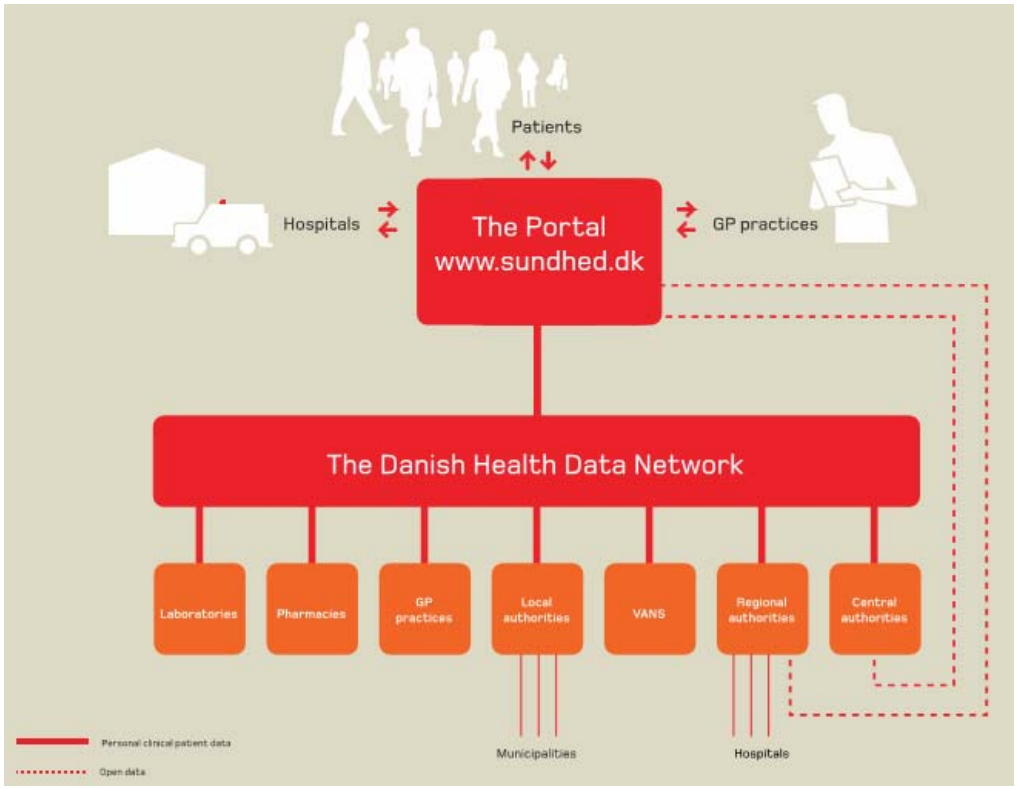


Figura 18: Infra-estrutura global de suporte ao Portal da saúde Dinamarquês.

4.3. Arquitectura de Autenticação para Redes sem Fios

A arquitectura de autenticação para redes sem fios aqui descrita foi implementada no Instituto Superior Técnico em Lisboa, no âmbito do programa e-U. Baseia-se em VPNs IPSec e permite a autenticação dos utilizadores, a confidencialidade na comunicação sem fios e o *roaming* automático entre instituições. Utiliza criptografia assimétrica e certificados de chave pública para a autenticação dos utilizadores (*suplicant*) e para o estabelecimento de um canal seguro IPSec para subsequente comunicação. As vantagens desta arquitectura são o não necessitar de uma infra-estrutura de *roaming* e utilizar uma PKI simplificada [53, 54].

A Figura 19 apresenta a arquitectura global da solução. Esta é composta por três segmentos separados por *gateways*/*firewalls*: (i) a Wifi VLAN à qual todos os AP (*Access Points*) estão ligados; (ii) a rede interna da instituição; e (iii) a Internet.

Para o acesso à rede interna ou à Internet, os utilizadores móveis "*laptop computers*" estabelecem uma VPN IPSec com o "*VPN Gateway & Firewall*". Desta forma, é garantida a confidencialidade da comunicação entre o utilizador e o *gateway*. O tráfego das ligações VPN é reencaminhado pelo *gateway* para o seu destino, rede interna ou Internet. O tráfego dos utilizadores sem ligação VPN é bloqueado no *gateway*, ficando assim impedidos de aceder aos recursos de rede da instituição e à Internet. Para permitir a obtenção de credenciais para o estabelecimento da VPN, o tráfego HTTP não autenticado é redireccionado para um servi-

dor seguro onde o utilizador, após autenticação (com outras credenciais obviamente), as poderá obter, caso tenha permissões para tal.

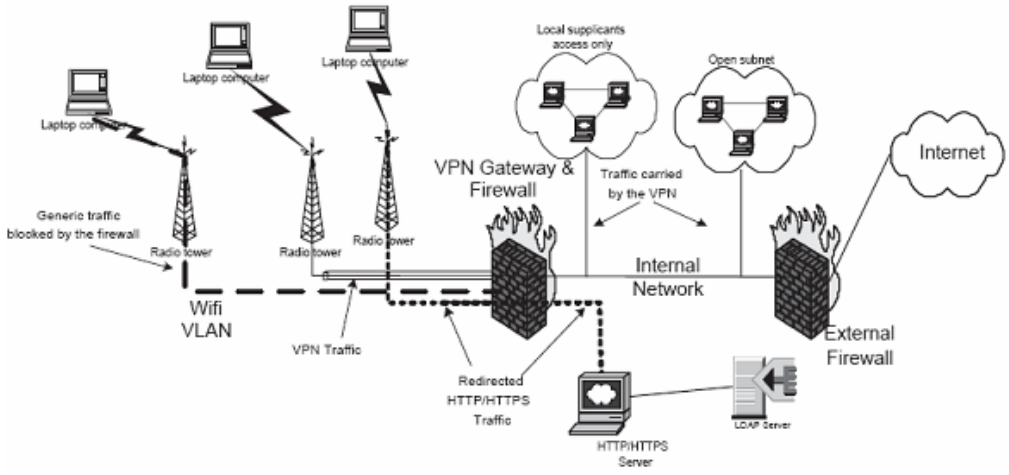


Figura 19: Arquitectura global da solução [53].

Para o estabelecimento da VPN IPSec é necessário a prévia autenticação do utilizador e do *gateway*. Esta autenticação é efectuada através da troca de certificados digitais de chave pública emitidos pelas suas instituições que actuam como entidades certificadoras de raiz. Caso ambos, *gateway* e utilizador, pertençam à mesma instituição, os seus certificados podem ser verificados pelo mesmo certificado de raiz que ambos possuem. Caso o utilizador seja de uma outra instituição, tanto o *gateway* como o utilizador necessitam de construir cadeias de certificação que terminem num certificado de raiz em que confiem.

Para permitir a simplificação da PKI utilizada nesta solução, os certificados obedecem a algumas restrições: não podem ser utilizados para assinatura digital e devem ser de curta duração. A curta duração permite prescindir da utilização de CRLs para publicitar certificados revogados, e a não utilização dos certificados para assinatura permite a geração da chave privada e do correspondente certificado no servidor de certificados da instituição. A razão para estas simplificações, é permitir uma fácil implementação da solução, com grande probabilidade de ser com a reutilização de equipamento existente na instituição.

Um utilizador em *roaming* apenas conseguirá estabelecer uma VPN com o gateway da instituição local após provar que pertence a uma instituição reconhecida. Esta prova é efectuada através da utilização do seu par de chaves assimétricas e da apresentação do seu certificado de chave pública emitido pela sua instituição de origem. Para garantir que o utilizador apenas estabelece VPNs com *gateways* de instituições reconhecidas pela sua instituição de origem, o *gateway* também se autentica utilizando do seu par de chaves assimétricas e apresentando o seu certificado de chave pública emitido pela instituição local.

O aspecto principal nesta solução é que cada instituição constitui-se com entidade certificadora de raiz, possui um certificado auto assinado, o certificado de raiz, e utiliza a sua chave privada para assinar os certificados dos seus utilizadores e *gateways*. Tanto os utilizadores como os *gateways* apenas confiam nos certificados de raiz das suas instituições, o seu certificado raiz de confiança. As cadeias de certificados ape-

nas são válidas se terminarem num certificado de raiz de confiança. Assim, a autenticação dos utilizadores locais é fácil, uma vez que tanto estes como o *gateway* confiam na mesma raiz.

O *roaming* entre as instituições acontecerá naturalmente, desde que o *gateway* consiga validar os certificados, emitidos pelas outras instituições, que lhe são apresentados pelos utilizadores externos. Para permitir a construção de cadeias de certificados para a validação dos certificados de diferentes instituições, estas podem estabelecer entre si acordos bilaterais, através de certificação cruzada, ou hierárquicos baseados numa entidade terceira de confiança.

A Figura 20 apresenta o modelo geral para a gestão dos certificados nesta solução, que inclui um exemplo de acordo bilateral (entre as instituições A e B) e um exemplo de acordo através de uma entidade terceira de confiança (entre as instituições A e C). Para a construção das cadeias de certificados para a validação de certificados entre instituições, é necessário que os utilizadores e os *gateways* tenham acesso aos certificados resultantes dos acordos estabelecidos entre as instituições. Para facilitar a gestão da distribuição destes certificados, cada instituição possuirá um servidor para a sua distribuição e, após a sua obtenção, serão mantidos em *cache* tanto pelos utilizadores como pelo *gateway*.

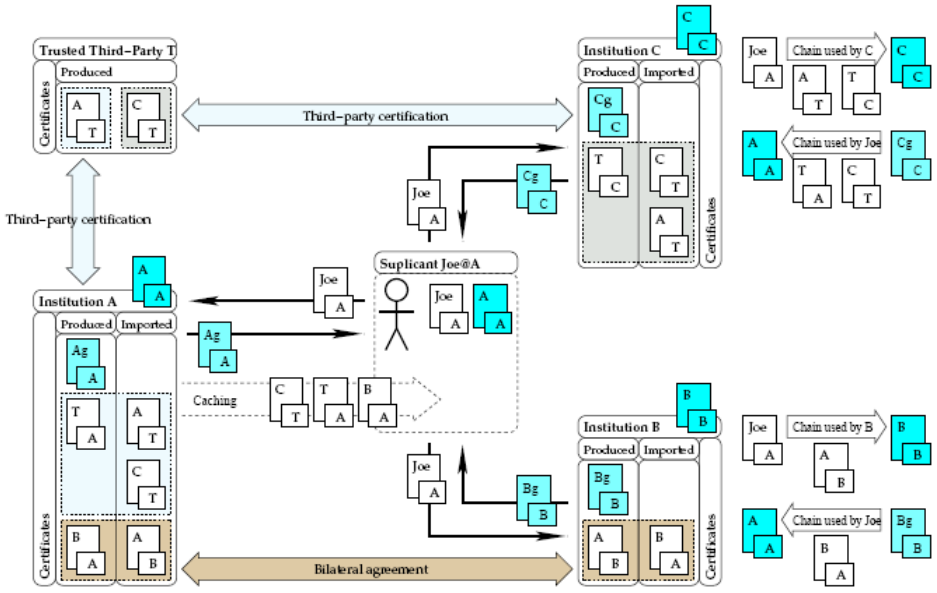


Figura 20: Gestão dos certificados para a autenticação das entidades no estabelecimento das ligações VPN IPSec [54].

Esta arquitectura serviu de inspiração para a arquitectura proposta neste documento. A sua grande vantagem é permitir a autenticação *offline* segura, independente da autenticação no interior de cada instituição, e o *roaming* automático dos utilizadores, utilizando tecnologias de comunicação e autenticação seguras bastante divulgadas e suportadas numa infra-estrutura de gestão de certificados de chave pública simplificada.

4.4. O cartão do cidadão

O Cartão do Cidadão (CC), que se pode observar na Figura 21, é o novo documento de identificação civil de Portugal e que vem substituir os principais cartões de identificação do cidadão perante a Administração Pública: Bilhete de Identidade, Cartão de Segurança Social, Cartão do Contribuinte e Cartão do Serviço Nacional de Saúde. Brevemente prevê-se que possa também substituir o cartão eleitoral [55, 56].

Figura 21: Exemplo de Cartão do Cidadão

Devido à sua vertente electrónica permite, através da utilização de certificados, a autenticação electrónica do seu titular, bem como a assinatura electrónica qualificada de documentos, com igual valor legal em canais não presenciais. Por exemplo, autenticação electrónica pela Internet do cidadão perante a Administração e a geração de assinaturas digitais qualificadas [57] com o mesmo valor legal da assinatura manuscrita.

O cartão do cidadão será baseado num *smart-card* que contém (i) informação em formato gráfico impressa na sua superfície e (ii) dois certificados digitais, e correspondentes chaves privadas, armazenados num chip embebido no cartão: o certificado de autenticação, que permite a autenticação do cidadão em sítios web seguros, e o certificado de assinatura digital, que permite assinar documentos e ficheiros, assegurando a sua integridade e comprovando a identidade do autor.

A utilização do cartão do cidadão é protegida por três códigos PIN (o que permite uma autenticação forte na sua utilização): (i) um PIN de assinatura que será solicitado quando o cidadão pretender assinar digitalmente um documento ou mensagem; (ii) um PIN de Autenticação que será solicitado para autenticação num sítio web ou outra aplicação; e (iii) um PIN de Morada que será solicitado para aceder à morada no cartão.

Para a utilização segura do cartão do cidadão é necessário garantir tanto a identidade do cidadão como a identidade da infra-estrutura técnica. Para isso foi implementada uma PKI de modelo hierárquica, a Infra-estrutura de Chave Pública Nacional (ICP Nacional), no topo da qual está a Entidade de Certificação Electrónica do Estado (ECEE) e que emite os certificados para as restantes Entidades Certificadoras (EC) do domínio do estado, entre as quais se encontra a EC do Cartão do Cidadão (ECCC), tal como ilustrado na Figura 22.

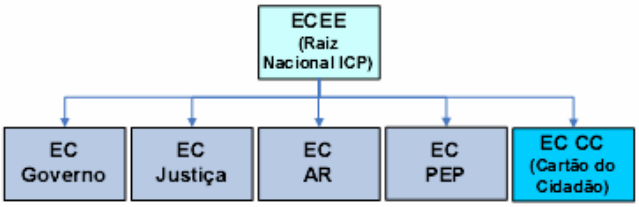


Figura 22: Infra-estrutura de Chave Pública Nacional (ICP Nacional)

A Infra-estrutura de Chave Pública do Cartão do Cidadão (ICP do Cartão do Cidadão) é uma infra-estrutura subordinada da ECEE, tal como se mostra na Figura 23. Nesta, a ECCC emite os certificados para as EC relacionadas com a segurança do CC (ECCCaut e ECCCass), para a EC de suporte aos serviços do CC (ECCCservi) e para o serviço de Entidade de Certificação de Documentos (ECD) que assina os conteúdos dos CC.

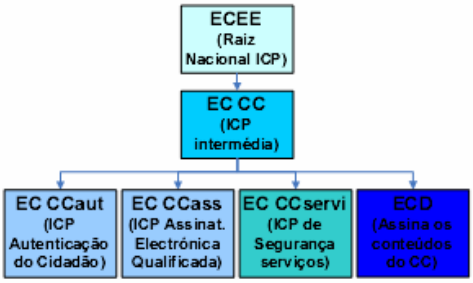


Figura 23: Infra-estrutura do Cartão do Cidadão (ICP do Cartão do Cidadão)

A entidade de certificação de autenticação do cidadão emite os certificados de autenticação dos cidadãos. A entidade de certificação de assinatura electrónica do cidadão emite os certificados qualificados [57] dos cidadãos. A entidade de certificação de suporte aos serviços emite certificados digitais para os sistemas/serviços de ciclo de vida e uso do Cartão do Cidadão associados a este, ou a pessoas e equipamentos destes serviços. A Entidade de Certificação de Documentos, não emitindo certificados, assina os conteúdos electrónicos do cartão, assegurando a sua integridade e autenticidade.

A informação de cancelamento de cartões é publicada numa CRL emitida regularmente, e disponibilizada num serviço de Directoria, e ainda divulgada num Serviço de Validação como o OCSP. Devido ao facto de a lista ser emitida periodicamente nem sempre está actualizada. No entanto, o Serviço de Validação está sempre actualizado e pode ser consultado para saber sobre o estado de validade de um determinado Cartão do Cidadão.

5 Arquitectura de autenticação para a RTS

Neste capítulo propõe-se uma arquitectura para a autenticação das entidades envolvidas em interacções na RTS. Dentro destas, o enfoque principal é colocado na autenticação dos Profissionais das IS, uma vez que são estes os principais utilizadores do sistema e aqueles que acedem a informação com o maior grau de sensibilidade. No entanto, a autenticação dos utentes e a autenticação de serviços e/ou servidores também é considerada. Como regra, a autenticação deverá ser mútua, no entanto poderá haver excepções, como, por exemplo, o acesso de utente anónimos a informação genérica.

A arquitectura proposta baseia-se na utilização de chaves assimétricas e certificados digitais de chave pública enquadrados numa infra-estrutura de chave pública (*Public Key Infrastructure*, PKI) de modelo híbrido, onde cada Instituição de Saúde (IS) é responsável pela emissão e gestão dos certificados digitais para as suas entidades – serviços/servidores e Profissionais. Para isso, a RTS, e cada uma das IS, constitui a sua própria PKI. Entre as PKI das várias IS e a PKI da RTS são estabelecidas relações de confiança, baseadas em certificação cruzada. Estas, permitem o reconhecimento mútuo dos certificados emitidos por cada delas e, desta forma, possibilitam a autenticação segura das entidades que interagem para aceder/disponibilizar a informação médica partilhada.

Para o transporte e armazenamento seguro das credenciais de autenticação dos Profissionais são utilizados *smart cards*. Estes cartões permitem um nível de autenticação forte, baseado em dois factores de autenticação (posse e senha), bem como um elevado nível de protecção física dos dados guardados no seu interior. Têm ainda a vantagem da mobilidade, uma vez que podem ser facilmente transportados pelo seu possuidor.

As credenciais de autenticação dos Profissionais são constituídas por dois certificados de chave pública e correspondentes chaves privadas: (i) um certificado para o acesso à RTS (certificado RTS) e (ii) um certificado para autenticação do Profissional na renovação do seu certificado RTS (certificado IS). O certificado RTS do Profissional cumpre uma dupla função: (i) autenticação do profissional no acesso à RTS e (ii) indicação do seu perfil (*role*) na IS a que está vinculado. Pelo facto de as alterações de perfil poderem, eventualmente, ser algo dinâmicas, preconiza-se um tempo de vida curto para estes certificados RTS. O tempo de vida curto permite ainda a implementação de uma PKI simplificada ao permitir dispensar a manutenção e consulta de CRLs na autenticação para o acesso à RTS, tal como na arquitectura de autenticação apresentada em [53, 54].

No modelo de confiança utilizado, cada entidade tem como âncora de confiança exclusivamente a entidade certificadora de raiz da instituição a que está vinculada. Além disso, como os caminhos de certificação são curtos, o número de certificados de confiança que cada entidade necessita de ter na sua posse, para validar os certificados que lhe são apresentados, é reduzido, o que é uma vantagem dado o pouco espaço de memória nos *smart cards*.

5.1. Porquê uma PKI?

Para a autenticação da identidade das entidades envolvidas numa comunicação remota, poderiam ser utilizadas várias tecnologias, como por exemplo Kerberos e PKI. No entanto, a PKI oferece as seguintes vantagens

- Permite uma autenticação *off-line* e é uma solução mais escalável.
- É a tecnologia utilizada na segurança em comunicações electrónicas na Internet envolvendo comércio electrónico e *home banking*.
- É também uma tecnologia considerada apropriada para lidar com os riscos de segurança em aplicações no âmbito da saúde (*eHealth*) [58].

Uma outra razão para a não utilização da tecnologia Kerberos prende-se com a sua necessidade de aplicações "kerberizadas", ou seja, que estejam preparadas para utilizar este protocolo. Os *browsers* não estão, mas em compensação estão preparados para lidar com tecnologia PKI.

Com a actual vulgarização da utilização de computadores portáteis faz sentido considerar a possibilidade de o Profissional poder aceder ao Portal da RTS a partir do seu portátil ou PDA. O acesso à RTS, ou de modo geral à Internet, só pode ser efectuado se existir conectividade, ou seja, depois de uma prévia ligação a uma rede de acesso, que poderá ser a rede hospitalar (RIS) ou a rede de um qualquer ISP (*Internet Service Provider)*. É neste processo de acesso de um equipamento a uma rede que tipicamente se utilizam as tecnologias AAA, como RADIUS [15] e DIAMETER [16]. A RTS é completamente alheia ao modo como é efectuada a ligação à rede de acesso, e à eventual autenticação que aí ocorra. No entanto, a tecnologia PKI pode também ser utilizada para a autenticação dos profissionais no acesso às redes da sua IS, por exemplo, utilizando 802.1X [17], criando, assim, um potencial de reutilização da arquitectura aqui proposta.

5.1.1. Serviços suportados

A PKI para a RTS tem como requisito o suporte dos serviços de autenticação de entidades em comunicações remotas e a confidencialidade dessas comunicações. O suporte a serviços de cifra de documentos, de assinatura digital de documentos ou mensagens e de marca temporal não é de momento um requisito. No entanto, a qualquer momento a PKI pode vir a ser estendida para incluir o suporte a esses serviços.

Os serviços de cifra e assinatura de documentos não são suportados pelo simples facto de que não é a RTS que controla os processos de criação e armazenamento da informação clínica. Para isso são utilizadas as aplicações específicas de processamento da informação médica existentes nas IS: a RTS apenas se constitui como plataforma para a partilha e apresentação dessa informação. Portanto, ao realizar essas funções a RTS estaria a interferir com esses processos, o que não se pretende.

Quanto à realização de assinatura digital de comunicações no âmbito da RTS, tal já poderia ser considerado. No entanto, o requisito da não utilização de código activo nos *browsers* (*Applet Java* ou *ActiveX*) para o acesso à RTS impede a realização da operação de assinatura digital pelo cliente, porque tal envolve processamento. Se o requisito for alterado, esta operação poderá vir ser realizada. Nesse caso, devido à curta

duração dos certificados de autenticação na RTS, é recomendável a utilização de um outro certificado para a operação de assinatura digital de mensagens.

Quanto ao serviço de marca temporal, as razões para o seu não suporte são as apresentadas para justificar o não suporte dos outros serviços. Mesmo que se venha a justificar a inclusão de uma marca temporal em documentos ou mensagens, devido ao elevado custo dos relógios de precisão e da infra-estrutura necessária para a implementar, deverá ser analisada a possibilidade de aquisição do serviço a um fornecedor externo, por exemplo, os CTT (v.g., Marca Do Dia Electrónica, MDDE[5]).

5.2. Modelo de comunicação segura

O modelo de comunicação da RTS é o modelo de comunicação via Internet, tal como apresentado na Figura 24. Os utilizadores, com o seu navegador (*browser*), acedem remotamente ao portal HTTP (Servidor Web) da RTS que, para satisfazer os pedidos do utilizador, acede a serviços remotos da RTS utilizando *Web Services*. Para prevenir o acesso não autorizado, todas estas comunicações têm que ser precedidas da autenticação mútua das entidades participantes, e para prevenir o acesso não autorizado e a alteração da informação em trânsito, a comunicação deve ocorrer apenas através de canais seguros.

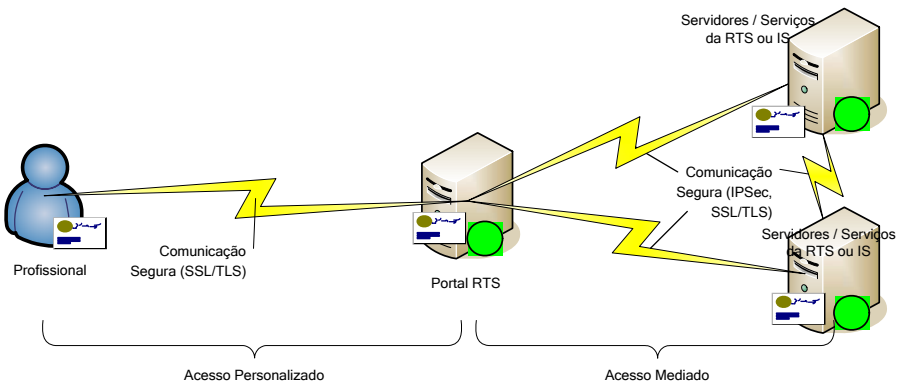


Figura 24: Modelo de comunicação segura na RTS

As tecnologias de comunicação segura que se preconizam são SSL/TLS para a comunicação entre Profissional e Portal, e SSL/TLS ou IPSec entre o Portal e os Serviços e Servidores a que ele acede. A autenticação mútua das entidades ocorre no contexto dos referidos protocolos de comunicação. Por exemplo, a autenticação do Profissional no acesso ao Portal, e a correspondente autenticação do Portal pelo Profissional, ocorrem no contexto da autenticação de cliente e de servidor no protocolo SSL.

[5] https://sce.ctt.pt/mdde/index.html

Para que as entidades participantes nas comunicações RTS se possam autenticar necessitam de estar na posse de um certificado digital e da correspondente chave privada. A PKI é a infra-estrutura de suporte da confiança nos certificados das várias entidades.

Como os serviços Web suportam o protocolo SSL, há vantagens em utilizar este protocolo na comunicação entre o Portal da RTS e os servidores/serviços da RTS e das IS. Com o SSL apenas a comunicação entre serviços é cifrada, ao contrário do que acontece com o protocolo IPsec em que toda a comunicação entre as duas máquinas é cifrada. Esta diferença tem um óbvio impacto na performance do sistema.

Um outro aspecto a mencionar é que a existência de segurança na comunicação entre os serviços, ao nível transporte, não deve invalidar a implementação de segurança ao nível dos protocolos de aplicação. Por exemplo, as normas de segurança WS-Security [59] e SAML [60] aplicam-se a mensagens SOAP [61], o formato comum das mensagens em serviços Web, para fornecer serviços de segurança ao nível da aplicação, entre os quais se inclui a autenticação.

5.3. Requisitos da Autorização

Na apresentação da RTS foi referido que, do ponto de vista do controlo de autorizações, a RTS funciona como um sistema baseado no perfil (*role*) do Profissional (RBAC). Assim, para que o Portal possa determinar a política de autorização a aplicar a um Profissional, necessita (i) do nome do profissional, (ii) do nome da IS a que está vinculado e (iii) o seu perfil na IS.

O nome do Profissional e o nome da instituição a que está veiculado fazem naturalmente parte da identificação do sujeito contida no seu certificado digital de chave pública emitido pela sua IS. O perfil do Profissional claramente não é informação de identificação, mas sim informação exclusivamente de autorização. O RFC 3281 recomenda que nestas situações se utilize uma PMI para a gestão de autorização, em paralelo com uma PKI para gerir a autenticação [33].

Nesta fase de desenvolvimento da RTS, o controlo do acesso à informação é baseado apenas no perfil do Profissional, sendo a identificação do Profissional e da IS a que está vinculado utilizados para a criação relatórios detalhados para monitorização dos acessos efectuados. Assim, a implementação de uma PMI seria exagerada. No entanto, como o Portal dos Profissionais necessita da informação do perfil do profissional, decidiu-se pela sua inclusão nos certificados digitais para a autenticação dos Profissionais no acesso à RTS.

A inclusão do perfil do Profissional na informação do certificado de identificação do Profissional para acesso à RTS implica que as CA emissoras destes certificados tenham acesso a essa informação, que tipicamente reside um serviço de directoria da IS. Implica também que os certificados dos Profissionais tenham tempos de vida curtos porque, ao contrário do que acontece com a informação de identificação da pessoa, que tende a ser constante, o perfil do Profissional na IS pode ser bastante dinâmico. Esta característica pode ser utilizada para uma simplificação da PKI.

5.4. Certificados digitais de autenticação

O formato dos certificados digitais a utilizar para a autenticação das entidades nos acessos à RTS obedece ao perfil de certificados X.509 para utilização na Internet, recomendado pelo IETF no RFC 3280 [31].

5.4.1. Entidades com certificados

Como já foi referido, os certificados digitais de chave pública da RTS têm como função autenticar as entidades que comunicam no âmbito da RTS. Estas entidades podem ser de dois tipos, Utilizadores e Servidores/Serviços, e impõem requisitos diferentes quanto à informação contida no certificado e ao seu tempo de vida.

Nesta fase, os Utentes não irão possuir nenhum *smart card.* A sua autenticação não será efectuada através de certificados, mas sim através de nome e senha. A razão para tal deve-se ao elevado custo que representaria dotar todos os Utentes de *smart cards* para o armazenamento dos seus certificados e chaves privadas. O armazenamento das chaves privadas num outro suporte menos seguro seria um risco para a confidencialidade da informação clínica do Utente.

A disponibilização do Cartão do Cidadão, actualmente em curso, pode vir a utilizada pela RTS para a autenticação do utente. Esta possibilidade é discutida na secção 5.9.

5.4.2. Tipos de certificados para autenticação na RTS

Os dois tipos de entidades que comunicam na RTS impõem requisitos diferentes quanto aos certificados de autenticação no âmbito da RTS: os certificados para os serviços/servidores destinam-se exclusivamente à sua autenticação; os certificados para os Profissionais têm de cumprir um segundo objectivo, que é o de fornecer ao Portal a informação do perfil do Profissional.

Portanto, irá haver dois tipos de certificados para a autenticação no acesso à RTS, um para cada tipo de entidade: (i) certificados de autenticação dos Profissionais (designados **certificados RTS**) e (ii) certificados de autenticação dos serviços e servidores (designados **certificados de Serviços**). Os certificados RTS diferenciam-se dos certificados de Serviços por (i) conterem a informação do perfil do Profissional na IS a que está vinculado e por (ii) terem tempos de vida curtos.

Os certificados RTS, porque têm um tempo de vida curto, precisam de ser renovados frequentemente. Por uma questão de comodidade essa renovação deverá ser realizada à distância pelos Profissionais, i.e., sem terem para o efeito de se deslocarem fisicamente a uma determinado serviço da RTS ou da sua (ou de outra) IS. Consequentemente, a autenticação dos Profissionais na renovação dos seus certificados RTS é crítica; um método de autenticação fraco no acesso à renovação de certificados RTS comprometeria a autenticação forte no acesso à RTS. Por este motivo, é necessário que os profissionais possuam um outro certificado, e correspondente chave privada. Como se preconiza que a gestão dos certificados para o acesso à RTS seja

feito pela IS a que o Profissional está vinculado, este certificado será designado por **certificado IS**, ou **certificado de Profissional da IS**. Para este certificado preconiza-se um tempo de vida "normal", 1 ou 2 anos.

Finalmente, para além dos certificados de autenticação haverá certificados cruzados para o estabelecimento de relações de confiança entre a RTS e as IS.

5.4.3. Formato dos certificados

Todos os certificados utilizados na RTS estão de acordo com o perfil de certificados para a utilização na Internet definido no RFC 3280. Os seguintes campos são fundamentais para a utilização na RTS:

Sujeito (*Subject*): Este campo contém a o nome da entidade para quem o certificado foi emitido e da IS a que está vinculado. A informação neste campo é especificada utilizando etiquetas (*tags*), devendo utilizar-se a *etiqueta* "CN" para o nome do Profissional e a etiqueta "O" ou "DN" para a identificação da IS. As etiquetas L e C poderão também ser utilizadas. Por exemplo, "CN = Helder Gomes", "O = HIP", L="Aveiro" e C="PT".

Emissor (Issuer): Este campo contém a identificação da CA que emitiu o certificado.

Validade: Este campo especifica o intervalo de validade do certificado, sendo composto pela data de início e pela data de fim. O certificado só é válido se a data actual se encontrar dentro do intervalo especificado.

Extensão EKU (*Extended ou Enhanced Key Usage*): Este campo é utilizado para indicar a finalidade do certificado. Nos certificados RTS deve conter os OID (*Object Identifiers*) de Autenticação de Cliente (1.3.6.1.5.5.7.3.2) e de identificação do perfil do Profissional na IS a que está vinculado. Para estes últimos, é necessário que a RTS faça a reserva de OIDs para os vários perfis de Profissionais, a qual pode ser feita gratuitamente na IANA (http://www.iana.org). Nos certificados de Serviços deve conter os OIDs referentes à Autenticação de Cliente (1.3.6.1.5.5.7.3.2) e Autenticação de Servidor (1.3.6.1.5.5.7.3.1). A necessidade destes dois OIDs advém do facto de os serviços poderem desempenhar os dois papéis.

***CRL Distribution Point* (CDP):** Este campo deve conter o endereço electrónico do local onde a CA que o emitiu publica as suas CRL. Este campo é fundamental para os certificados de Serviços. Para os certificados RTS, que são de curta duração, não é necessário.

5.5. Smart Cards para a autenticação dos Profissionais

O funcionamento de uma PKI baseia-se em dois pressupostos fundamentais: (i) a existência de uma entidade terceira de confiança que atesta, de forma verificável, que a chave pública contida no certificado pertence à entidade (sujeito) identificada no certificado e (ii) que se confia que a chave privada correspondente a essa chave pública está unicamente na posse da entidade para quem o certificado foi emitido. A privacidade (segredo) da chave privada é extremamente importante. É através da utilização da chave privada que se prova possuir a identidade do correspondente certificado. Como os certificados são públicos, a posse e utilização exclusiva da chave privada tornam-se críticos para a autenticação da identidade.

Como antes se viu, cada Profissional terá um certificado digital (certificado RTS) de uma chave pública, e a correspondente chave privada, que irá utilizar para se autenticar no acesso aos serviços da RTS. Para garantir a segurança (segredo) da chave privada do Profissional, foi decidida a utilização de *smart cards* com processador criptográfico.

Estes *smart cards* efectuam todo o processamento associado à utilização da chave privada, incluindo a geração do par de chaves assimétricas, e impedem a sua saída para o exterior. Além disso, os *smart cards* em geral têm mecanismos de protecção que, em casos de tentativa de uso ilícito (sem o PIN correcto, ver abaixo) bloqueiam o acesso ao *smart card* ou, em casos de violação física, limpam o conteúdo da memória impedindo o acesso às eventuais chaves no seu interior.

Outra característica dos *smart cards* é a possibilidade de definir um PIN de protecção para a sua utilização. Com esta característica implementa-se um sistema de autenticação forte baseado em dois factores: (i) a posse do *smart card* e (ii) o conhecimento do PIN.

Como não é requisito que o *smart card* contenha outros elementos de identificação do seu dono, como por exemplo uma fotografia, ele pode ser disponibilizado sob a forma de um *token* USB. Estes *tokens* ligam directamente a uma porta USB, actualmente vulgaríssimas em qualquer computador, não necessitando de qualquer *hardware* (leitor) adicional. É, contudo, necessário que todas as estações de trabalho com acesso à RTS tenham instalado o software para a leitura do cartão seleccionado, que eventualmente poderá vir de raiz com o sistema operativo. Desta forma, para aceder à RTS, o Profissional autentica-se utilizando o seu certificado (certificado RTS), e a correspondente chave privada, guardados no interior do seu *token*, a partir de qualquer máquina, desde que esta possua o software para aceder ao *smart card*.

A utilização de *smart cards* poderá ainda potenciar medidas extra de segurança não directamente relacionadas com a autenticação RTS, nomeadamente (i) a realização de *login* através da introdução do *smart card* e (ii) o bloquear ou desligar de sessão no sistema operativo com o remover do *smart card* [62].

5.6. Gestão dos certificados

As IS são instituições autónomas entre si, cada uma delas com a sua gestão de recursos informáticos e humanos. Esta gestão de recursos é independente da RTS, no sentido que ela é necessária quer a IS pertença à RTS ou não. Faz sentido, então, a RTS reaproveitar essa gestão de recursos das IS e serem as próprias IS a gerirem os acessos à RTS e portanto a gerir a emissão de certificados RTS para os seus Profissionais.

Apesar de cada IS gerir a emissão dos certificados RTS para os seus profissionais, deve haver uma política de certificados global a toda a RTS, a que todas as IS devem estar sujeitas, uma vez que não faz sentido ter critérios de emissão diferenciados em cada IS.

5.6.1. Emissão/renovação de certificados RTS

O curto tempo de vida dos certificados RTS implica renovações muito frequentes, o que faz com que o processo de renovação seja crítico para a sua utilização eficaz. O processo de renovação deverá ser flexível,

rápido e o mais transparente possível. Para os restantes certificados a renovação não é tão crítica, uma vez que ocorre a intervalos de tempo longos.

O pedido de renovação dos certificados RTS deve ser feito *online* e a sua emissão imediata. Como o tempo de vida preconizado para estes certificados é curto, não faz sentido o Profissional ter que se deslocar a um qualquer serviço para obter a sua renovação, ou estar à espera da aprovação da renovação por de um gestor do serviço de emissão de certificados.

Um método de renovação de certificados é através da utilização de um servidor Web com comunicação segura SSL. O cliente acede a uma página Web onde faz o pedido do certificado, fornecendo toda a informação que lhe é pedida. O servidor reencaminha o pedido para a CA Emissora e esta procede à emissão do certificado, que é então instalado no cliente. Mais uma vez, devido á curta duração dos certificados RTS, apenas faz sentido a sua emissão ser imediata e automática.

A grande questão com este método de renovação é a exigência de uma atitude activa do Profissional para iniciar este processo acedendo à página Web do servidor de renovação de certificados. Métodos de renovação mais amigáveis e automáticos poderão ser utilizados, caso estejam disponíveis. No entanto, o método apresentado deve ser disponibilizado porque, dependendo da disponibilidade de acesso ao servidor, permite ao Profissional a renovação do seu certificado RTS virtualmente a partir de qualquer máquina.

Um ponto que merece consideração é a questão da autenticação para controlo de acesso ao servidor de renovação. Não faz sentido ter um mecanismo de autenticação fraco para proteger o acesso a credenciais para um mecanismo de autenticação forte (certificados RTS). Isto implica que o mecanismo de autenticação para a renovação dos certificados RTS deva ser pelo menos tão forte quanto o mecanismo de autenticação na RTS. Por este motivo, o Profissional terá um segundo certificado, e correspondente chave privada, armazenados no seu *smart card*: o certificado IS. Este certificado terá um tempo de vida “normal” e possuirá no campo EKU um OID específico para a renovação de certificados RTS.

Este certificado IS, apesar de ser emitido em nome do Profissional, não pode ser por ele renovado. Uma vez que é com este certificado que se controla o acesso aos certificados RTS, a sua emissão é rodeada de maiores medidas de segurança. Assim, este certificado é emitido em nome do Profissional e instalado no seu *smart card* apenas no acto de iniciação do *smart card* por um técnico responsável pela iniciação de *smart cards* (*smart card enroller*). Posteriores renovações deste certificado pelo Profissional não são permitidas. Quando o certificado expirar, o *smart card* deve ser devolvido para que se proceda a uma nova iniciação por um técnico autorizado.

5.6.2. Iniciação do smart card dos Profissionais

Para um Profissional se autenticar no acesso à RTS, tem de estar na posse de um *smart card* contendo o seu certificado RTS e correspondente chave privada. E, para o obter, terá que possuir um certificado IS e a correspondente chave privada, os quais deverão ser colocados no *smart card* a quando da sua iniciação. A questão que se pretende discutir é onde deve ser feita a iniciação e distribuição do *smart card* do Profissional

com as suas credenciais para a obtenção de certificados RTS: (i) por um serviço central de emissão da RTS ou (ii) localmente em cada IS.

Antes da entrega do *smart card* ao Profissional ocorre o respectivo processo de registo e identificação. Este processo deve ocorrer de acordo com as regras que venham a ser definidas para o registo de Profissionais na RTS. Como os Profissionais exercem a sua actividade nas IS, os respectivos serviços de pessoal são a entidade melhor colocada para fazer o registo e a verificação da identidade de cada Profissional para a posterior entrega do *smart card* correctamente iniciado com o certificados IS e correspondente chave privada do Profissional. Portanto, faz sentido que o processo de registo seja local às IS, reutilizando os seus serviços.

Quanto ao local onde deve ser feita a iniciação do *smart card* com o certificado IS correspondente chave privada, faz também sentido que seja feito na própria IS a que o profissional está vinculado. A vantagem de serem realizadas na própria IS é acima de tudo prática. Se o profissional ficar impossibilitado de utilizar o seu *smart card*, porque o perdeu, ou danificou, ou qualquer outra razão, fica também impedido de aceder à RTS, e como tal o exercício das suas funções pode ficar comprometido. Dependendo do perfil do profissional na IS, pode eventualmente ser imperativa a reposição urgente de um novo *smart card* com novas credenciais para o profissional. Se a iniciação do *smart card* for feita localmente, na própria IS, rapidamente se inicia um novo *smart card*, com novo certificado IS e correspondente chave privada, de modo a que o Profissional possa obter um novo certificado RTS e retomar o exercício pleno das suas funções [63]. Desta forma, a falta de credenciais pode ser facilmente ultrapassada, evitando assim que a RTS possa ser acusada de limitar o exercício da actividade dos Profissionais (mesmo que, como na situação exemplificada, as responsabilidades do impedimento lhe sejam alheias). Se a iniciação do *smart card* for efectuada no exterior da IS, o tempo necessário para a iniciação e entrega de novo *smart card* será, com certeza, mais demorado, ficando o profissional limitado no exercício das suas funções durante esse intervalo de tempo.

As vantagens da gestão centralizada dos *smart cards* seriam (i) um maior controlo na gestão dos *smart cards*, uma vez que a sua iniciação ocorreria apenas num local, e (ii) um menor custo por evitar a replicação por cada IS do serviço de iniciação de *smart cards*. No entanto, como a rapidez do processo de iniciação de *smart cards* pode ser crítica em situações de emergência, optou-se pela iniciação local em cada IS.

A iniciação local dos certificados vai também em linha com o terceiro objectivo deste trabalho que é a independência da RTS da gestão dos profissionais nas suas IS, sendo estas a gerir o acesso dos seus Profissionais à RTS. Contudo, é necessário que os critérios para a identificação dos profissionais e entrega do *smart card* sejam homogéneos dentro de toda a RTS, o que implica a definição de uma política de certificação comum a ser seguida por todas as IS aderentes à RTS.

5.7. Simplificação da PKI

Se os certificados tiverem um tempo de vida suficientemente curto de forma que o risco associado a esse tempo de vida seja considerado reduzido, pode-se prescindir da utilização de CRL ou de outros mecanismos de publicitação de certificados revogados. A definição do tempo de vida deverá ser algo a afinar com a prática, mas não deverá passar de um ou dois dias. Notar que, como os certificados dos profissionais e cor-

respondentes chaves privadas são armazenados em *smart cards* protegidos por um PIN e como mecanismos de protecção contra falsificação e violação, o risco do seu comprometimento torna-se reduzido.

5.7.1. Revogação de certificados RTS

Os certificados RTS contêm, para alem da informação de identificação, a indicação de perfil do Profissional na IS a que está vinculado. A informação do perfil está sujeita a variações, por vezes frequentes, enquanto que a informação de identificação tende a ser estática. Por esta razão, os certificados RTS têm um tempo de vida curto.

O facto de um certificado ter um tempo de vida curto faz com que a sua janela de risco diminua. A janela de risco do certificado é o máximo intervalo de tempo em que o certificado pode ser usado de forma ilícita, ou seja, sem ser pelo seu dono. A janela de risco é limitada (i) pelo intervalo de validade do certificado ou (ii) pelo intervalo entre publicações da CRL da CA que emitiu o certificado.

A gestão de CRLs tem algumas limitações conhecidas, nomeadamente a sobrecarga que provoca nas comunicações e o facto de pela sua periodicidade não fornecer uma garantia absoluta da validade de um certificado [64]. A utilização de delta-CRLs também não resolve os problemas das CRLs. Por outro lado a utilização de mecanismos de teste de revogação *online* como o OCSP, vai contra o quinto objectivo deste trabalho, que é minimizar as comunicações da RTS com as IS para a autenticação dos Profissionais.

Como a emissão da CRL é periódica, a janela de risco dos certificados imposta pela CRL é, no máximo, igual ao intervalo entre publicações da CRL, como se pode ver na Figura 25. Quanto mais apertado o intervalo, menor a janela de risco, mas maior o custo de gestão das CRLs. Em sistemas de elevado risco o intervalo entre publicações pode ser de horas (por exemplo quando envolve certificados para utilizar em transacções financeiras de elevados montantes), enquanto que em sistemas de mais baixo risco pode ser de dias, semanas ou até meses.

Se o tempo de vida do certificado for bem mais curto do que o intervalo entre publicações de CRLs, a janela de risco fica limitada essencialmente pelo intervalo de validade do certificado. Assim, podemos pensar em simplificar a PKI, dispensando o mecanismo de revogação de certificados. Considerando que os certificados RTS, e respectivas chaves privadas, são armazenados dentro de dispositivos criptográficos (*smart card*), protegidos por um PIN e por um bloqueio após um certo número de tentativas falhadas de uso do PIN, o risco associado à não existência de mecanismos de revogação de certificados pode ser aceitável dependendo do tempo de vida definido para esses certificados.

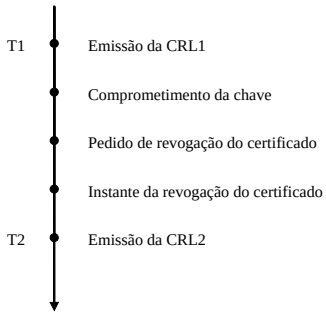


Figura 25: Sequencia temporal de revogação de um certificado

Assim, para simplificar a gestão da PKI decidiu-se definir um tempo de vida reduzido para os certificados RTS e prescindir da utilização de mecanismos de revogação para a sua autenticação. A definição do tempo de vida deve resultar de uma ponderação sobre o risco associado a ele associado, e certamente será objecto de afinação em resultado da experiência acumulada após a entrada em funcionamento do sistema.

Esta simplificação, que poderá racionalizar os custos da PKI, não implicando um aumento de risco significativo, está em linha com a arquitectura de autenticação proposta em [53, 54] e com o objectivo de minimizar a comunicação para a autenticação dos Profissionais.

Para o suporte aos restantes certificados, continua a ser necessária a publicação de CRLs. No entanto, por estes certificados não necessitarem de CRLs com periodicidades curtas e por o seu número ser reduzido, o custo da sua gestão é muito menor.

5.7.2. Armazenamento de chaves e armazenamento e publicação de certificados

Uma outra simplificação advém do facto de os certificados RTS serem apenas utilizados para a autenticação de identidades. Por esse facto, não é necessário manter um serviço para o armazenamento das chaves e dos certificados emitidos.

O armazenamento de chaves é imperativo para o suporte à operação de decifra. A perda de uma chave privada impede a recuperação da informação cifrada com a correspondente chave pública. Porém, o serviço de cifra de dados não é necessário para a RTS, logo não é necessário o armazenamento de chaves.

A necessidade do certificado de outra entidade ocorre quando se pretende utilizar a sua chave pública para iniciar uma comunicação, tipicamente para cifrar uma mensagem para ela. Na RTS não há essa necessidade. Na autenticação de identidades, é a própria entidade que apresenta o seu certificado para ser validado e usado pelo interlocutor. Logo, como todos os certificados emitidos no âmbito da RTS são para autenticação de identidades, não é necessário ter um serviço para o seu armazenamento e publicação.

5.8. Modelo de Confiança da PKI

Na escolha do modelo de confiança para a RTS foram consideradas as seguintes hipóteses:

- Uma PKI de modelo hierárquico com a raiz de confiança na PKI da RTS;
- Um modelo híbrido em que a RTS e cada uma das IS têm sua própria PKI.

A representação gráfica destes modelos é apresentada na Figura 26.

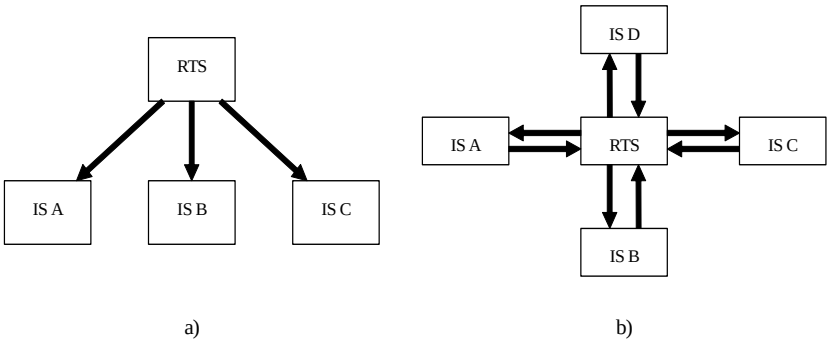


Figura 26: a) Modelo hierárquico, com âncora de confiança única; b) Modelo híbrido, com uma PKI em cada IS que estabelecem relações de confiança com a PKI da RTS

Em ambos os modelos, de acordo com a discussão na secção 5.6, a gestão dos *smart cards* e a emissão e gestão dos certificados de autenticação RTS deve ser feita localmente nas IS.

No modelo hierárquico, o certificado de raiz da RTS é a única raiz de confiança para todas as entidades que participam na RTS. No modelo híbrido, a PKI da RTS está ao mesmo nível das PKI das IS, cada uma com a sua raiz de confiança.

O modelo de hierárquico é o mais simples e, talvez, o mais económico, uma vez que apenas há necessidade de manter uma única raiz de confiança. No entanto, não espelha a autonomia que as várias IS possuem e limita-as em termos de futura adaptação da tecnologia PKI a outros serviços, uma vez que não são elas a gerir a PKI.

Na realidade, as IS são parceiras, cada uma com o seu modelo organizacional e com a sua gestão de recursos, podendo participar, ou não, na RTS. As que participam estabelecem acordos bilaterais de confiança com a RTS. O modelo híbrido espelha melhor esta realidade.

Preconiza-se então um modelo de confiança híbrido, em que cada IS constitua a sua própria PKI para a emissão e gestão de certificados para os seus Profissionais. A ideia por detrás destas PKI de cada IS é potenciar a sua reutilização para outros serviços dentro das IS, e desta forma promover a segurança global dos sistemas de informação nas IS. Caso alguma das IS já possua uma PKI implementada ela deve ser adaptada para a utilização na RTS.

Como a RTS não pretende ser uma rede nacional, mas apenas de âmbito regional, é razoável supor que o número das IS participantes nunca irá ser elevado. Como tal, para o estabelecimento dos relacionamen-

tos de confiança não se afigura necessária uma ponte (*bridge*), sendo estes estabelecidos directamente entre a RTS e cada uma das IS.

Este modelo híbrido de confiança aplica-se a ambos os modelos de acesso à informação que se referiram para a RTS. No modelo de acesso intermediado as IS não acedem directamente a informação noutras IS, sendo a RTS a responsável pela obtenção da informação pretendida. Assim, cada uma das IS apenas necessita de estabelecer relações de confiança com a RTS, não sendo necessária a extensão da confiança às restantes IS, nem o estabelecimento de relações de confiança directamente entre as IS. No modelo de acesso por apontadores, em que cada profissional acede directamente à informação no local (IS) onde ela reside, a confiança delegada na RTS por cada uma das IS pode ser estendida às restantes, evitando-se desta forma o estabelecimento de relações de confiança directa entre as IS ou a necessidade de uma *bridge* – a RTS acaba por fazer esse papel.

5.8.1. PKI das Instituições de Saúde

Cada IS deve implementar uma PKI para a gestão dos certificados de autenticação das entidades a si vinculadas. É da sua responsabilidade a escolha do modelo de confiança interno da sua PKI (hierárquico, rede ou híbrido). Do ponto de vista da RTS o importante é que no estabelecimento da relação de confiança a IS se comprometa com as políticas de certificação definidas pela RTS.

No momento actual nenhuma das IS que participa na RTS possui uma PKI implementada. Assim, achou-se conveniente fazer uma proposta para uma PKI da IS. O modelo proposto é o modelo hierárquico com dois níveis de CA que se apresenta na Figura 27. Esta hierarquia pode eventualmente ser reaproveitada para outras aplicações distintas da RTS. Salienta-se ainda que a implementação da PKI não interfere com outros eventuais mecanismos de autenticação que a instituição tenha em funcionamento para outros serviços.

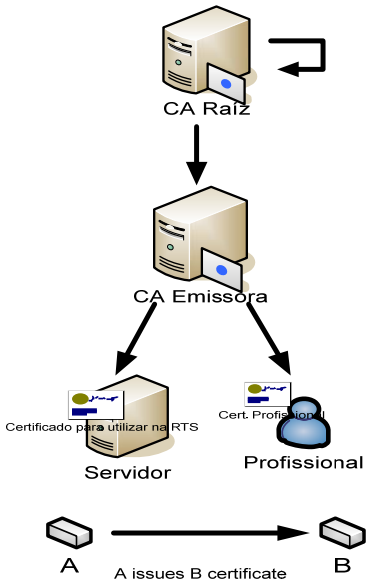


Figura 27: Modelo hierárquico de CA recomendado para as instituições

No topo da hierarquia está a CA raiz da IS que apenas emite certificados para as CA Emissoras. O seu certificado, emitido por si para si própria, é a raiz de confiança para o resto das entidades da IS. Para garantir a sua segurança, não deve estar ligada a qualquer rede, e deve permanecer desligada (*power off)* e ser ligada apenas quando é necessário emitir algum certificado. A sua chave privada deverá ser guardada num dispositivo criptográfico de segurança.

No segundo nível encontra-se a CA Emissora, que recebeu o seu certificado da CA Raiz, e é responsável pela emissão dos certificados de autenticação para serem utilizados na RTS – certificados IS, certificados RTS e certificados cruzados para o Portal da RTS.

5.8.2. Raiz de confiança das PKIs das IS

Na questão da escolha da raiz de confiança para sua PKI, as IS confrontam-se com duas possibilidades: (i) utilizarem os serviços de uma CA raiz externa, ou (ii) utilizarem uma CA raiz interna.

A utilização dos serviços de uma CA raiz externa normalmente coloca-se quando se pretende que os certificados emitidos sejam aceites (confiáveis) por uma grande audiência externa à organização. Por exemplo, em certificados para servidores que forneçam serviços na Web a uma audiência vasta.

As CA comerciais têm, normalmente, uma grande visibilidade externa que vem da inclusão dos seus certificados de raiz nos pacotes de software de grande divulgação e com suporte a PKI. Por exemplo o Windows XP traz consigo cerca de 200 certificados de raiz de entidades certificadoras comerciais. A desvantagem desta solução, além do custo, é a imposição de regras rígidas na gestão dos certificados, que podem, por exemplo, impedir a inclusão de informação proprietária no certificado, como seria o caso do papel do profissional.

A utilização de uma CA raiz interna tem a desvantagem da visibilidade externa, mas tem as vantagens da flexibilidade de gestão e de um menor custo.

Para as IS, a solução ideal para a raiz de confiança seria uma solução mista entre as duas anteriores. Tipicamente, as entidades que interagem com as IS são entidades que têm algum tipo de vínculo com o Ministério da Saúde. Assim, tal como sugerido em [65], a implementação de uma PKI pelo Ministério da Saúde, que certificaria as CA das IS, forneceria o contexto ideal para a utilização e validação dos certificados em aplicações da saúde. Neste contexto, a verificação de uma assinatura digital produzida por um médico de uma IS, por outro profissional noutra IS não ficaria dependente de acordos de confiança entre as respectivas IS, uma vez que haveria uma raiz de confiança comum: a raiz do Ministério da Saúde. Esta PKI da saúde poderia inclusivamente ficar sob o âmbito da Hierarquia de Infra-estrutura de Chaves Públicas Nacional – Entidade de Certificação Electrónica do Estado (ECEE) – desenvolvida no contexto do Cartão do Cidadão, o que permitiria um âmbito verdadeiramente nacional, e não apenas restrito ao domínio da saúde, aos certificados das IS.

Como neste momento não existe nenhuma PKI nacional da Saúde, e como não parece necessária a adopção de uma raiz externa, considera-se que as IS implementam o modelo de PKI de raiz interna proposto. Assim, cada IS contém uma CA raiz que funciona como âncora de confiança para os seus certificados.

5.8.3. Estabelecimento das relações de confiança

Como já foi referido, o modelo de confiança escolhido para a RTS é um modelo em que a RTS e cada uma das IS possuem a sua própria PKI e, cada uma das IS estabelece relacionamentos de confiança *peer-to-peer* com a RTS. Estes relacionamentos são estabelecidos com base em certificados cruzados. A questão agora é determinar quais as CA de cada uma das PKIs que devem emitir/receber os certificados cruzados.

Por razões de segurança, as CA raiz devem permanecer desligadas (*power off*), sendo ligadas apenas quando necessário, o que acontece raramente porque apenas emitem certificados para as CA Emissoras no segundo nível. Por este motivo, o intervalo entre publicações das suas CRLs é longo, tipicamente na casa dos meses, pelo que a certificação cruzada não deve ser efectuada a este nível [62].

Se o relacionamento for efectuado ao nível das CA do segundo nível, como o intervalo entre publicações das CRL é muito mais curto do que o das CA raiz, a propagação da informação de revogação dos certificados cruzados fica mais facilitada.

A Figura 28 ilustra o estabelecimento das certificações cruzadas entre uma IS e a RTS.

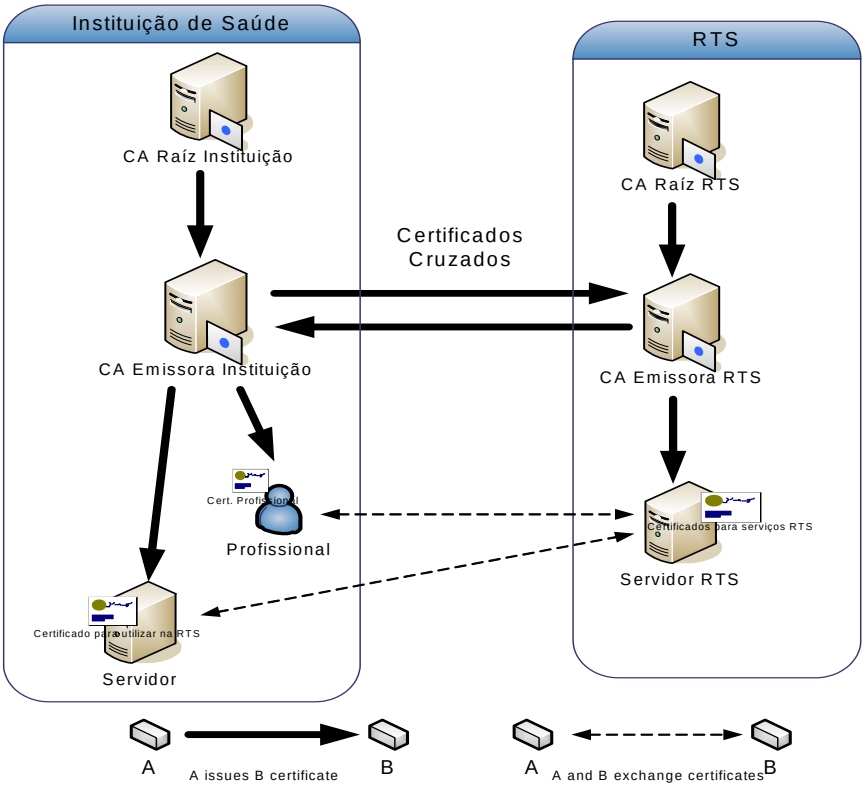


Figura 28: Utilização de certificados cruzados para o estabelecimento de relacionamento de confiança entre IS e RTS.

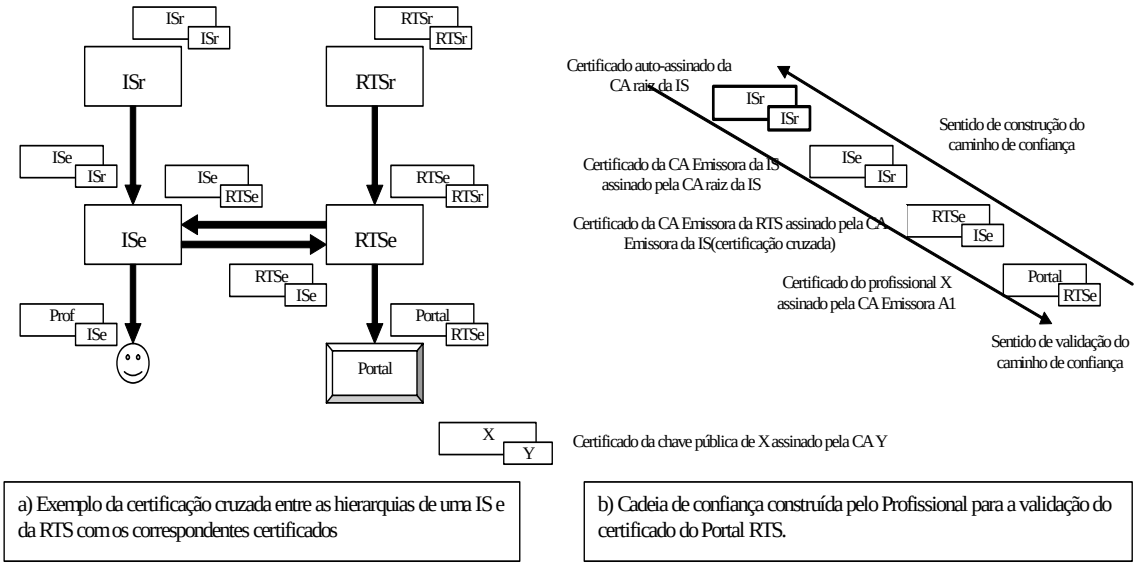
5.8.4. Cadeias de certificação

Quando um Profissional recebe um certificado do Portal da RTS, ou o contrário, devem fazer a sua validação com vista a autenticar o seu interlocutor. Para fazer esta autenticação é necessário construir um caminho de certificação com todos os certificados entre a raiz de confiança de quem valida e o certificado a validar. A construção deste caminho de certificação nem sempre é trivial por causa das dificuldades na obtenção dos certificados intermédios, sendo ainda mais complicada com a introdução de certificados cruzados. Por isso, é recomendável que quem proceda à validação possua os certificados necessários para proceder às validações dos certificados que espera necessitar de validar.

No contexto da RTS, as validações que se pressupõe necessárias são a validação dos Profissionais pelo Portal do Profissional, e vice-versa, e a validação dos serviços e servidores entre si. Estas entidades devem estar na posse dos certificados necessários para validar os certificados que lhe irão ser apresentados pelos seus interlocutores.

No caso dos Profissionais, por questões de mobilidade, estes certificados têm que ser transportados no seu *smart card*, em conjunto com o seu certificado e a sua chave privada. Dado o espaço de memória reduzido que os *smart cards* disponibilizam, o número de certificados intermédios não pode ser elevado.

Tendo em conta o modelo de confiança proposto para a RTS, que se apresenta na Figura 29-a) com os correspondentes certificados, a cadeia de certificação que um Profissional precisa de construir para validar um certificado do Portal dos Profissionais, é composta por 3 certificados (excluindo o certificado a validar), como se pode verificar na Figura 29-b). Significa isto que, para além do seu certificado e da sua chave privada, o profissional deve transportar no seu *smart card* (i) o certificado de raiz da sua IS (raiz de confiança), (ii) o certificado da CA Emissora da IS e (iii) o certificado cruzado emitido pela sua CA Emissora para a CA Emissora da RTS.



a) Exemplo da certificação cruzada entre as hierarquias de uma IS e da RTS com os correspondentes certificados

b) Cadeia de confiança construída pelo Profissional para a validação do certificado do Portal RTS.

Figura 29: Construção e validação de cadeia de certificação

Quanto ao Portal, para além do seu certificado, terá que ter na sua posse o certificado de raiz da RTS, o certificado da CA Emissora da RTS e os certificados cruzados da CA Emissora da RTS para cada uma das CA Emissoras das IS.

De igual modo, os restantes servidores/serviços deverão estar na posse do certificado da sua raiz de confiança, do certificado da sua CA Emissora e dos certificados cruzados necessários para fazer a validação dos certificados que lhe são apresentados, tipicamente os certificados cruzados para todas as IS.

A Figura 30 mostra um exemplo de uma possível interacção da RTS. Na interacção 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.

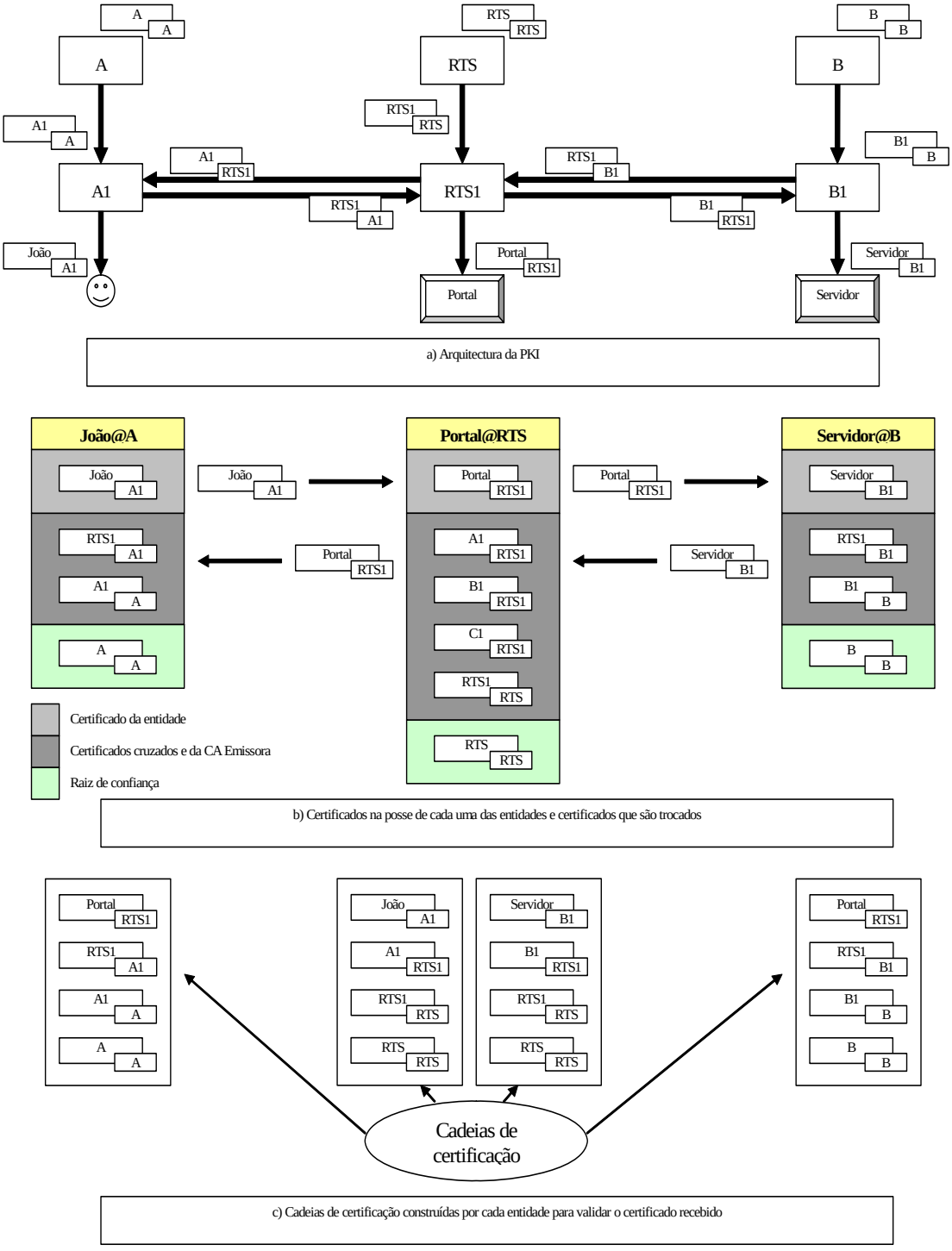


Figura 30: Exemplo de interacção na RTS com a indicação dos certificados na posse de cada entidade e as cadeias de certificação construídas para a validação dos certificados recebidos

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 da entidade C1 emitido pela CA RTS1 que está na posse do Portal não participa na transacção e

ilustra apenas que o Portal tem de estar na posse de cópias dos certificados cruzados de 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 ao Portal ter de estar na posse de um número possivelmente grande de certificados - todos os certificados cruzados emitidos pela RTS.

5.9. Autenticação dos Utentes

O Portal dos Utentes irá disponibilizar dois tipos de informação: informação de carácter genérico e de acesso geral e livre e informação de carácter pessoal disponível apenas ao utente a que ela se refere. Significa isto que vai ser necessário a autenticação mútua, do Utente e do Portal, no acesso a determinadas áreas do Portal dos Utentes e que a posterior comunicação deve ser confidencial. Para esta comunicação preconiza-se a utilização de SSL/TLS.

A autenticação dos utentes para o acesso ao Portal dos Utentes tem características diferentes da autenticação dos Profissionais no acesso ao Portal dos Profissionais. A começar pelo seu registo: não faz muito sentido registos locais dos pacientes em cada uma das IS, porque poderia levar a situações de vários registos para um mesmo utente, um em cada IS, logo, várias credenciais de acesso ao portal.

Faz então sentido um registo centralizado dos utentes que pretendem ter acesso ao Portal do Utente. No processo de registo, que pode/deve ser efectuado nas IS, o utente identifica-se, fornece a informação que for considerada pertinente na definição do processo de registo e de acordo com a legislação de controlo do acesso a dados pessoais.

A RTS deve constituir uma directoria ou base de dados com a identificação dos utentes que têm acesso ao Portal dos Utentes. Nessa directoria, além da identificação do utente devem lá constar as suas credenciais de acesso.

O desejável para a autenticação dos utentes era que fosse realizada à semelhança da dos profissionais: através da utilização do seu certificado digital de chave pública e da sua chave privada, ambos armazenados num dispositivo criptográfico (*smart card* ou *token* USB). No entanto a implementação desta solução tem um grande problema que é o seu custo. Esse custo é essencialmente devido ao dispositivo criptográfico.

Esta dificuldade pode ser ultrapassada com a utilização do Cartão do Cidadão que entrou em vigor no início de 2007. Esta utilização estaria em linha com os objectivos do Cartão do Cidadão, uma vez que uma das suas vertentes é a substituição do actual Cartão do Utente, ou Cartão do Serviço Nacional de Saúde. Para esta utilização ser possível, a RTS necessitaria de reconhecer como válidos os certificados do Cartão do Cidadão e o utente teria que ter a possibilidade de validar no seu computador o certificado do Portal do Utente.

Para a RTS reconhecer como válidos os certificados no Cartão do Cidadão, seria suficiente a emissão de um certificado cruzado da RTS a assinar o certificado da EC CC, CA intermédia na hierarquia de certificação do estado e que emite os certificados para as restantes CA que emitem os certificados do cidadão

[55]. Esta certificação cruzada nem necessita de ser nos dois sentidos, uma vez que apenas é necessário o reconhecimento dos certificados do Cartão do Cidadão na RTS e não o oposto.

Quanto ao utente, o seu registo continua a ser fundamental, porque continua a ser a forma de saber que utentes pretendem aceder ao Portal. A directoria ou base de dados da RTS com a identificação dos Utentes continua a ser indispensável. O acesso apenas deverá ser consentido aos utentes cuja identificação conste no serviço de directoria da RTS.

Para a validação pelo Utente do certificado do Portal do Utente, será necessário que este possua nos seus certificados de confiança os certificados da CA Raiz e da CA Emissora da RTS. Estes poderão ser fornecidos ao utente como resultado do processo de registo, por exemplo numa disquete, em conjunto com um *script* para fazer a sua instalação nos arquivos de certificados da máquina do utente. Em simultâneo, deveriam estar disponíveis no Portal do Utente para os utentes que os pretendessem instalar.

Nas situações em que esta solução com o Cartão do Utente não esteja disponível, a autenticação do Utente poderá ser feita com base num nome e senha fornecidos como resultado do seu processo de registo. No entanto, este acesso deve também ser confidencial. Para o estabelecimento do canal seguro, continua a ser necessário que o Utente valide o certificado do Portal, e para isso continua a ser necessário fornecer ao Utente os certificados da CA Raiz e da CA Emissora da RTS.

6 Implementação de um Protótipo

Com vista à validação da arquitectura proposta foi implementado um protótipo. Este protótipo, constituído pela RTS e por uma IS, foi implementado com base em tecnologia Windows ou desenvolvida para funcionar em ambiente Windows. O protótipo faz essencialmente a validação da solução para a autenticação dos Profissionais. Além disso a maior parte dos aspectos da arquitectura ficam cobertos apenas com a autenticação dos Profissionais, sendo a autenticação no IPSec o aspecto mais notável que fica de fora. No entanto, como o modelo de utilização e as características dos certificados para a autenticação no IPSec não fogem da utilização típica, não foi considerado muito relevante a sua inclusão no protótipo para validação experimental.

Além da arquitectura proposta, o protótipo inclui duas facilidades disponibilizadas pelos serviços de PKI do Windows: (i) renovação automática de certificados e (ii) *logon* com *smart card.* Estes serviços não estão incluídos na arquitectura porque se considera serem do âmbito das IS, a RTS não depende da sua existência. No entanto, foram incluídos no protótipo porque contribuem para a segurança global do sistema e porque o protótipo tem um carácter pedagógico funcionando como guia para a instalação nas IS.

6.1. Cenário

O cenário idealizado para a implementação de um protótipo para teste da arquitectura de autenticação proposta é composto pela RTS e por uma Instituição de Saúde, tal como ilustrado na Figura 31. Como podemos ver na figura, a RTS e IS implementam cada uma a sua PKI, com dois níveis, para emitir os certificados digitais para as suas entidades: RTS para o Portal do Profissional e IS para os seus profissionais e para os seus servidores, recorrendo esta última aos serviços de um Active Directory para a validação da identidade dos seus Profissionais e guardar os modelos de os certificados.

Todas as CA do protótipo foram implementadas exclusivamente com tecnologia Windows: Microsoft Windows Server 2003 *Enterprise Edition*. A razão para esta escolha foi o facto de as IS actuais utilizarem o *Active Directory* para a gestão do seu parque informático e este poder integrar-se com as CA Windows para a gestão dos certificados. Poderíamos ter também utilizado outras tecnologias, como OpenCA[6] ou EJB CA[7] para não implementar todas as CA com a mesma tecnologia. Aliás convém referir que o Portal dos Profissionais foi implementado numa plataforma baseada em Linux, Apache e Java. No entanto, como o interesse do desenvolvimento do protótipo foi fazer uma prova de conceito, decidiu-se utilizar apenas uma tecnologia.

[6] https://www.openca.org/

[7] http://ejbca.sourceforge.net/

A tecnologia utilizada para o computador do Profissional foi o Windows XP SP2, com um navegador da Internet: Internet Explorer, Netscape ou Firefox. Para o armazenamento e transporte dos certificados e chaves privadas do Profissional utilizou-se um token USB iKey 3000 da Rainbow Technologies. Além do iKey3000 foi também analisado um *token USB* da Axalto e um *smart card* e respectivo leitor da Infineon.

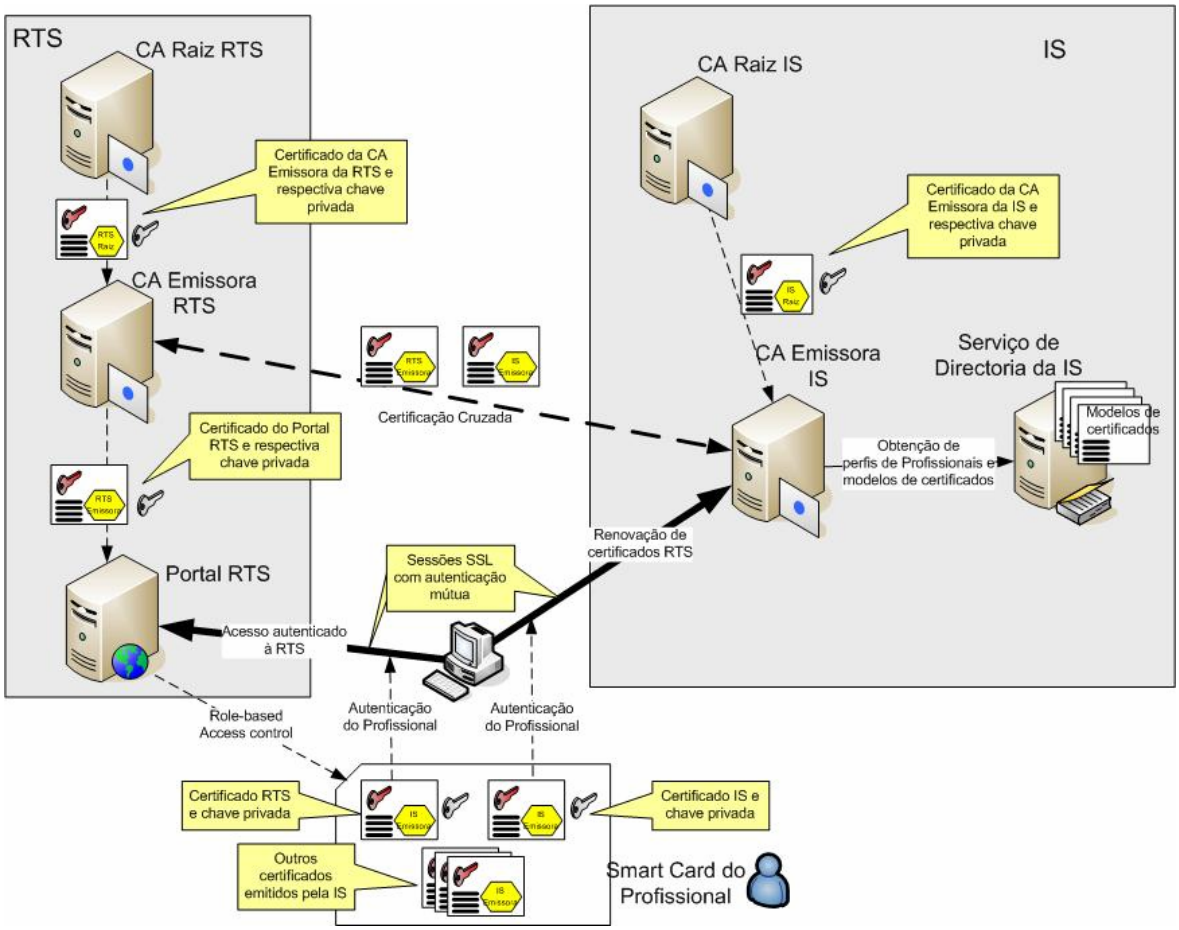


Figura 31: Arquitectura do protótipo

6.2. Serviços de PKI em ambiente Windows

Os sistemas operativos Windows Server, versão 2000 e posteriores, e Windows XP, incorporam funcionalidades de PKI, a *Windows Public Key Infastructure*. Para a implementação das CA foi utilizado o *Windows 2003 Server Enterprise Edition*, cujos principais componentes PKI são: (i) o Servidor de Certificados - *Certificate Server*, (ii) Entidades de Registo – *Registration Authorities*, (iii) *Active Directory* (AD) e (iv) a CAPI.

6.2.1. Servidor de Certificados

A Figura 32 ilustra a arquitectura do servidor de certificados da Microsoft [66].

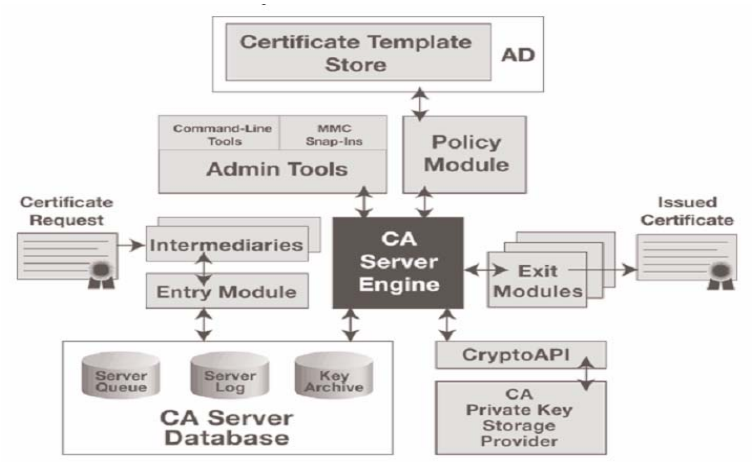


Figura 32: Arquitectura dos serviços de certificados da Microsoft (*Microsoft Certificate Services)*

O seu elemento fundamental é o *CA Server Engine* (certsrv.exe) que é o responsável pela geração dos certificados e CRLs e pelo fluxo de informação entre os restantes blocos.

O *Entry Module* aceita os pedidos para a emissão de certificados e coloca-os numa fila.

O *Policy Module* implementa as políticas da CA tal como definidas pelo administrador da CA. Informa a CA *engine* sobre os modelos (*templates*) de certificados e decide quando é que o certificado deve ser emitido, negado ou ficar pendente. Para tomar estas decisões poderá aceder a informação armazenada numa directoria ou base de dados.

O *Exit Module* distribui e publica os certificados, cadeias de certificados, CRLs e Delta CRLs. Pode escrever os dados no sistema de ficheiros ou transportá-los para uma localização remota utilizando HTTP, LDAP ou RPC. Pode haver vários *Exit Modules*, o que possibilita a distribuição da informação em paralelo para vários locais.

Tanto o Policy Module como o Exit Module podem ser alterados, ou trocado, de acordo com as necessidades. Pode também ser configurado através da aplicação *certutil.exe*, ou da consola MMC (*Microsoft Management Console*) utilizando o *snap-in Certification Authority*.

A gestão da CA é também feita através do snap-in *Certification Authority Microsoft Management Console*, ou do comando de linha certutil.exe.

O bloco Intermediário (*Intermediaries*) representa as entidades através das quais a CA comunica com os clientes da PKI. Recolhem a informação dos clientes e formatam os pedidos de certificados. As páginas Web para fazer o pedido de certificados (*enrollment*) são um exemplo de um bloco Intermediário.

O acesso a todas as funções criptográficas, incluindo o acesso e utilização da chave privada da CA, é feito através da CAPI. A chave privada da CA pode ser armazenada num disco convencional ou num dispositivo de *hardware* dedicado, tal como um dispositivo HSM (*Hardware Security Module*).

6.2.2. Modos de Instalação

Uma CA baseada no *Windows Server 2003 Enterprise Edition* pode ser instalada como CA raíz ou como CA subordinada. Pode ainda ser instalada em modo *Stand Alone* CA, ou em modo *Enterprise* CA em que há integração com os serviços do Active Directory.

Tipicamente, o modo *Enterprise* utiliza-se em CA emissoras em ambientes onde os utilizadores fazem parte de uma mesma organização. Disponibiliza serviços adicionais como sendo a renovação automática de certificados e o *logon* utilizando *smart cards*.

O modo *Stand Alone* tipicamente utiliza-se em CA emissoras em ambientes em que os utilizadores são externos à organização. Utiliza-se também em CA que são mantidas desligadas (*off line*) como é o caso das CA raiz e CA intermédias.

6.2.3. Entidades de Registo

A Entidade de Registo faz a identificação dos clientes e a recolha da informação para o pedido de emissão de certificados (*enrollment*).

O Windows disponibiliza poucas funcionalidades de Entidade de Registo. Disponibiliza no entanto, uma interface Web para fazer pedidos de certificados que pode ser considerada como sendo uma entidade de registo básica. Disponibiliza também certificados de *Enrollment Agent* cujo possuidor pode fazer pedidos de certificados para *smart cards* em nome de outros utilizadores, funcionando assim com um agente de Entidade de Registo.

6.2.4. Active Directory

A PKI do Windows utiliza o *Active Directory* (AD), para obtenção de informação acerca dos utilizadores que requisitam certificados (Profissionais) e para armazenamento das CRL, Delta CRLs e dos certificados dos utilizadores, da CA e de certificação cruzada. Apesar de ser referido que qualquer aplicação LDAP pode ser usada em substituição do AD, algumas funcionalidades da PKI, tal como a utilização de modelos (*templates*) de certificados, e aplicações com funcionalidades PKI (como o *logon* utilizando *smart cards*), apenas funcionam se utilizarmos o AD.

Como sistema de autorização num domínio Windows é gerido centralmente a partir do Active Directory, este pode desempenhar um papel útil no controlo dos acessos dos profissionais na obtenção dos seus certificados.

6.2.5. CryptoAPI

A CryptoAPI, ou CAPI, é a API do Windows que permite aos programadores incluir serviços de segurança baseados em criptografia nas suas aplicações, tais como autenticação, confidencialidade, etc. Além disso permite-lhes interagir com certificados, chaves privadas e dispositivos de armazenamento seguro, como os *smart cards*.

O acesso a um subconjunto das funções da CAPI, para assinar e cifrar dados, pode também ser feito através de um objecto COM (*Component Object Model*): a CAPICOM. Este objecto é particularmente útil para o desenvolvimento de *scripts* que necessitem de acesso a funções criptográficas.

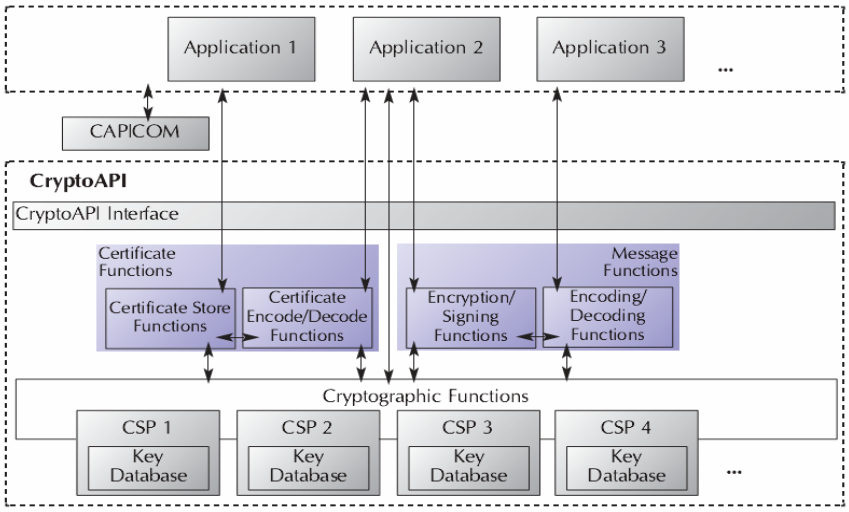


Figura 33: Arquitectura da CAPI do Windows

A arquitectura da CAPI, ilustrada na Figura 33, consiste numa interface de programação, num conjunto de módulos de software e num conjunto de Fornecedores de Serviços Criptográficos (CSP – *Cryptographic Service Providers*).

Os módulos de software disponibilizam funções para lidar com mensagens e funções para lidar com certificados. Os primeiros são utilizados para gerar chaves criptográficas, *hashs*, assinaturas digitais e cifra e decifra de dados. Os segundos são utilizados para operações tais como gerar e validar certificados e aceder a arquivos de certificados.

Os CSP são bibliotecas que contêm a implementação de algoritmos criptográficos e cifras. Estas bibliotecas são "*pluggable*", ou seja, podem ser incluídas bibliotecas adicionais de outros fornecedores.

Os CSP podem ser implementados em *hardware* ou em *software*. As implementações em *hardware*, tais como os *smart cards* e *tokens* são consideradas mais seguras do que as implementações em software.

Os CSP também lidam com o armazenamento seguro das chaves privadas. Esses arquivos seguros de chaves estão contidos dentro dos CSP sendo o seu acesso é efectuado através da CAPI.

De raiz com o Windows vem um conjunto de CSPs, que incluem suporte para alguns dos algoritmos mais populares, tais como DES (*Data Encryption Standard*), 3DES, RSA e RC4. Além disso, inclui CSP para três fabricantes de *smart cards*: Infineon, Gemplus e Schlumberger. A Figura 34 lista os CSPs que vêm incluídos de raiz no Windows.

CSP Name	Description
Microsoft Base Cryptographic Provider 1.0	Base CSP.
Microsoft Base DSS Cryptographic Provider	Superset of the CSP in the previous row, including support for DSA and SHA.
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider	Superset of the CSP in the previous row, including support for the Diffie-Hellman key agreement protocol.
Microsoft Diffie-Hellman Schannel Cryptographic Provider	Schannel CSP: used for secure Web communications using Secure Sockets Layer (SSL)/Transport Layer Security (TLS).
Microsoft RSA Schannel Cryptographic Provider	
Microsoft Enhanced Cryptographic Provider 1.0	Enhanced version of base provider; supports longer key lengths. FIPS 140-1 Level 1 compliant.
Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider	Enhanced version of base provider; supports longer key lengths. FIPS 140-1 Level 1 compliant.
Microsoft Enhanced RSA and AES Cryptographic Provider	Enhanced version of base provider; supports longer key lengths and the AES algorithm for symmetric encryption. FIPS 140-1 Level 1 compliant.
Microsoft Exchange Cryptographic Provider 1.0	Exchange-specific CSP.
Microsoft Strong Cryptographic Provider	Like the enhanced CSP, but it adds 40-bit encryption to make the strong CSP fully compatible with the base CSP.
Infineon SiCrypt Base Smart Card CSP	Infineon hardware CSP for smart-card support.
Gemplus GemSAFE Card CSP 1.0	Gemplus hardware CSP for smart-card support.
Schlumberger Cryptographic Service Provider	Schlumberger hardware CSP for smart-card support.

Figura 34: Fornecedores de Serviços Criptográficos (CSP) que vêm de raiz com o Windows

6.2.6. Interface PKCS #11

A interface PKCS #11 é uma norma definida pela RSA para a interface com dispositivos criptográficos [67]. Especifica uma API, designada Criptoki, para dispositivos de armazenamento de informação criptográfica e que realizem funções criptográficas. O seu objectivo é semelhante ao da CAPI, já analisada.

Esta norma, apesar de suportada pelo Windows, não é utilizada pelas aplicações Windows, nomeadamente o *browser*, Internet Explorer, que utilizam a CAPI. É no entanto utilizado pelos *browsers* Netscape Navigator e Mozilla Firefox e em ambiente Linux.

A Figura 35 ilustra o posicionamento das duas APIs na plataforma Windows. Os objectos Token X, Y e Z são os equivalentes PKCS #11 dos CSP da CAPI. O Netscape Navigator e o Mozilla Firefox trazem alguns de raiz. Tal como com os CSP podem ser adicionados *Tokens* de outros fornecedores. De um modo genérico, os tokens PKCS#11 e os CSP designam-se por *midleware*, uma vez que se localizam entre a aplicação e o dispositivo criptográfico.

O módulo PC/SC [68] é uma arquitectura standard que define uma interface entre os leitores de cartões e os gestores de recursos para que as aplicações vejam todos os leitores de cartões da mesma forma e com as mesmas funcionalidades. Foi desenvolvido por um grupo de empresas fabricantes de *smart cards* e PCs, liderado pela Microsoft, estando também implementado em ambiente Linux [69].

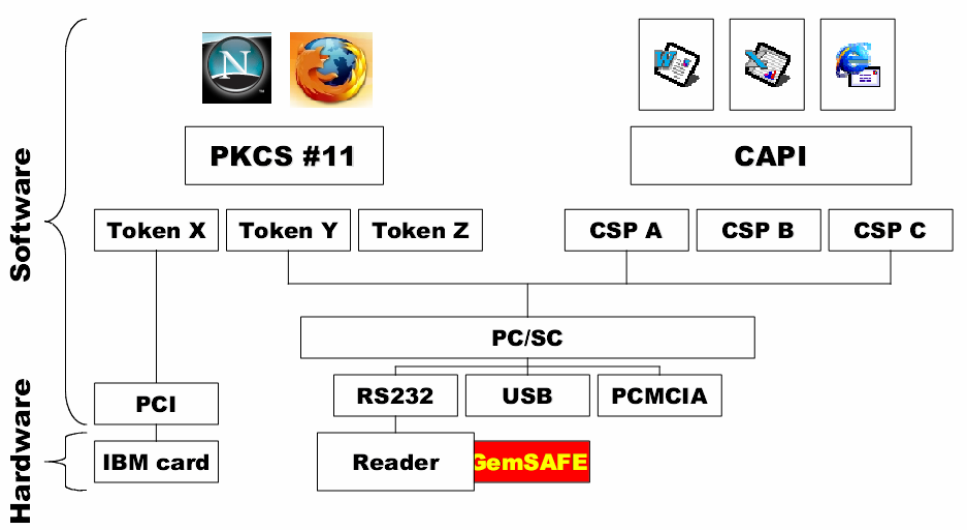


Figura 35: APIs criptográficas na plataforma Windows (adaptado de Jean Luc Giraud, Gemplus , 2001)

6.2.7. Modelos (templates) de certificados

O Windows 2003 versão *Enterprise* permite a definição de modelos de certificados baseados em modelos preexistentes. Esta característica é interessante porque permite criar modelos de certificados de acordo com as necessidades específicas de uma aplicação ou organização. No caso especifico do protótipo será utilizada para a definição dos certificados emitidos pela CA Emissora da IS.

6.3. Smart Cards, Tokens USB e Middleware

A mobilidade dos profissionais, dentro das IS a que estão vinculados e entre diferentes IS, é um requisito para a RTS. Como os *smart cards* são dispositivos portáteis, deveriam poder ser utilizados em qualquer computador para a autenticação dos Profissionais no acesso à RTS. No entanto, para que os *smart cards* possam ser utilizados, é necessário software instalado nesses computadores: (i) o *driver* do leitor de cartões e (ii) o *middleware* (PKCS#11 e CSP) para permitir que as aplicações utilizem o cartão.

A necessidade deste software implica uma escolha cuidadosa do *smart card* a utilizar. Isto porque os módulos PKCS#11 e CSP são geralmente específicos para um fabricante, ou para um modelo, além de que normalmente os fabricantes impõem limites quanto ao número de máquinas em que o software pode ser instalado, ou não existem versões para todos os sistemas operativos. Na Tabela 3 apresentam-se três possíveis soluções para este problema.

	Suportado nativamente pelo SO	Software livre	Software comercial
Windows	CSP de alguns *smart cards*/vendedores	openSC PKCS#11 CSP#11	AET SafeSign Identity Aloha Smart Card Connector
Linux	---	openSC PKCS#11 gpkcs#11	AET SafeSign Identity
MacOS X	Tokend para modulos PKCS#11 externos	openSC PKCS#11	AET SafeSign Identity

Tabela 3: Três possíveis soluções para o problema do *middleware* dos *smart cards*

A primeira solução é a escolha de *smart cards* suportados de raiz pelo sistema operativo. A maioria dos computadores das IS que actualmente pertencem à RTS utiliza o Windows XP, que suporta de raiz os seguintes *smart cards*: Gemplus Axalto Cryptoflex .NET, GemSAFE 4k/8k, Infineon/Siemens SI-CRYPT/SICRYPT v2, Schlumberger Cryptoflex 4k/8k/8k v2/ActiveCard/e-gate and Cyberflex Access 16k/Campus [70]. Para o caso concreto do protótipo, nenhum dos *smart cards* utilizados se encontra na lista dos suportados pelo Windows, o que implicou a utilização de CSPs de terceiros. Notar ainda que esta solução não inclui módulos PKCS#11, o que inviabiliza a utilização de navegadores como o Firefox e o Netscape.

A segunda solução passa pela utilização de software livre (*open source*) ou programas livres. Um exemplo é a utilização do openSC[8], um módulo PKCS#11 que suporta um grande conjunto de *smart cards* e que funciona em sistemas Windows, Linux e MAC OS. Em Windows, pode ser usado em conjunto com o CSP#11[9], um CSP que permite às aplicações Windows aceder a módulos PKCS#11, incluindo o openSC. Esta solução seria a ideal devido ao seu baixo custo. No entanto não foi possível a sua utilização estável e fiável, como se documenta na secção 6.3.5.

A terceira solução é a utilização de software comercial, tal como o AET SafeSign Identity[10] ou o Aloha Smart Card Connector[11], que disponibilizam um CSP e um módulo PKCS#11 que suportam uma grande variedade de *smart cards*. Nenhum destes softwares foi testado no protótipo. Foi no entanto testado com sucesso o SafeSign Standard que é o percursor do SafeSign Identity, como se documenta na secção 6.3.4.

A dimensão da memória do *smart card* também deve ser verificada. Ela tem que ser suficiente para armazenar (i) duas chaves privadas e os correspondentes certificados de chave pública e (ii) outros para a validação do certificado do Portal da RTS – os certificados da hierarquia de CA da IS e o certificado cruzado emitido pela CA Emissora da IS para a chave pública da CA Emissora da RTS. É necessário que os *smart cards* possuam pelo menos 32k de memória.

[8] http://www.opensc-project.org

[9] http://csp11.labs.libre-entreprise.org

[10] http://www.aeteurope.nl/SafeSign

[11] http://www.aloaha.com

No decurso do trabalho foram testados três dispositivos *smart card*: um cartão *smart card* (Infineon), e dois *tokens* USB com *smart card* embebido: um Axalto Reflex 530 E-gate Smart Card Enabler (Cyberflex e-gate 32k card chip embedded, Sealed) e um Rainbow iKey3000. Estes testes utilizaram os CSP de origem do Windows, e os CSP e módulos PKCS#11 do openSC/CSP#11, do SafeSign Standard 2.0.3 e do Cyberflex Access SDK 4.3.

Como resultado destes testes, concluiu-se que o software SafeSign é o que melhor serve os requisitos de mobilidade da RTS, uma vez que mostrou suportar dois dos *smart cards* utilizados (o SafeSign Identity reclama suportar uma grande variedade de tokens e smart cards). O CSP#11/openSC poderia ser uma solução igualmente interessante e mais económica, só que não foi possível ter uma versão estável e funcional. Qualquer que seja o modelo de *smart card* ou *token* a adquirir, recomenda-se que, caso se utilize um CSP e módulo PKCS#11 genérico, a aquisição em volume seja precedida de um teste para garantir a sua compatibilidade.

6.3.1. Infineon Sicrypt

O *Smart Card* Infineon v1, que se pode observar na Figura 36, em conjunto com um leitor embebido num teclado, foi o primeiro a ser testado. Foi fornecido pelo Hospital Infante D. Pedro (HIP) para podermos avaliar a possibilidade da sua utilização com vista a eventual reutilização de um lote que tinham na sua posse.

Figura 36: Smart Card Infineon Sicrypt v1

O HIP possuía, também, uma aplicação para *logon* seguro no Windows que utilizava este *smart card*, Sicrypt Smarty[12], mas que não estavam a utilizar. O HIP não nos forneceu nenhum software relacionado com o cartão.

Após uma série de testes, pesquisas na Web e contacto a fornecedores, concluiu-se que o *smart card* já tinha sido descontinuado, pelo que não foi possível obter o seu CSP para permitir a sua utilização em ambiente Windows. Foi possível observar o cartão em funcionamento apenas com uma versão demo da Aplicação Sicrypt Smarty, mas o acesso ao cartão era feito de forma proprietária e não através de um CSP na arquitectura CAPI.

[12] http://www.ic-compas.de/de/produkte/sicrypt-smarty

6.3.2. Axalto Cyberflex eGate 32k

Este smart-card Axalto Cyberflex eGate 32k vem embebido no token USB Reflex 530 E-gate Smart Card Enabler, que se mostra na Figura 36.

Figura 37: Axalto Reflex 530 E-gate Smart Card Enabler (Cyberflex e-gate 32k card chip)

As experiências com este *token* também não foram muito bem sucedidas porque não trazia consigo nenhum *sofware*: nem CSP, nem módulo PKCS#11, nem *driver*. No entanto, o *driver* é obtido automaticamente pelo Windows quando se introduz o *token* no computador.

O seu principal problema é o CSP. O Windows apesar de vir de origem com alguns CSPs para *smart cards* Cyberflex, não traz o deste cartão especificamente. Pela Internet não foi possível obter o CSP. Segundo informação na página Web da Axalto, a implantação (*deployment*) de um sistema com estes *smart cards* implica o pagamento de mais um valor extra, por cada computador, para a aquisição do software a instalar nesses computadores.

Este *smart card* funcionou perfeitamente com o CSP e o módulo PKCS#11 incluídos no kit para o desenvolvimento de aplicações Java Card. No entanto, este software não funcionou com mais nenhum outro *smart card*.

Em relação à utilização deste *smart card* com o CSP e módulo PKCS#11 da SafeSign, verificou-se que é possível a sua utilização, desde que a primeira iniciação do cartão seja feita pela SafeSign.

Com este *smart card* não foi testada a utilização do software CSP#11 e openSC porque na página Web da openSC ele era referido explicitamente como não suportado, havendo o risco de o danificar.

6.3.3. Rainbow iKey3000

O Rainbow iKey 3000[13], apresentado na Figura 38, é um dispositivo (*token*) criptográfico com tecnologia *smart card* e interface USB. O pacote de aquisição do dispositivo incluía o software de gestão de *smart cards* SafeSign Standard. Este software, além de uma aplicação para a gestão de smart cards inclui um CSP e um módulo PKCS#11 que reclamam suportar uma grande variedade de *smart cards*.

[13] http://www.safenet-inc.com

Como este dispositivo não faz parte da lista dos *smart cards* suportados de raiz pelo Windows, foi necessário instalar o seu *driver* e o CSP fornecidos. Instalou-se também o módulo PKCS #11 para permitir a sua utilização pelos *browsers* Netscape e Firefox.

Figura 38: Rainbow iKey3000

O dispositivo funciona em pleno com o software SafeSign, quer com o módulo PKCS#11, no Firefox e Netscape, quer com o CSP, nas aplicações Windows (Internet Explorer, Outlook, etc.).

Foi também possível a sua utilização parcial com o módulo PKCS#11 da openSC.

6.3.4. SafeSign Standard

O software SafeSign Standard foi adquirido no pacote do dispositivo iKey3000. Este software inclui um CSP, um módulo PKCS#11 e uma aplicação para a gestão do dispositivo. Além da versão para ambiente Windows inclui também a versão para ambiente Linux. Este software está na origem do já referido SafeSign Identity.

O CSP e o módulo PKCS#11 funcionaram perfeitamente com o dispositivo iKey3000. Também foi possível a sua utilização sem problemas em dispositivos Axalto cuja primeira iniciação foi feita pela aplicação de gestão da SafeSign.

A aplicação de gestão do dispositivo, Figura 39, permite a realização de um conjunto de operações tais como a iniciação do dispositivo, o desbloquear o PIN, a alteração de PIN e PUK, a importação de certificados e a visualização dos certificados contidos no dispositivo. Através do manuseamento de chaves no *registry* do Windows é possível configurar quais as operações que devem estar disponíveis em cada máquina.

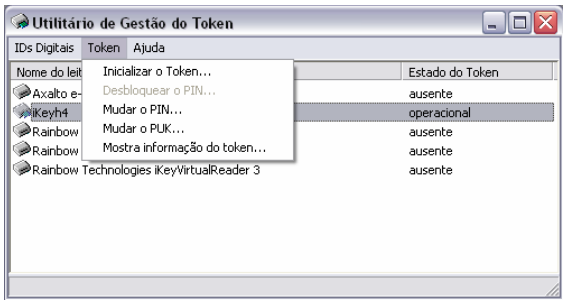


Figura 39: Utilitário de gestão do *token* SafeSign Standard 2.0.3.

A disponibilização de uma aplicação para a gestão de smart cards é pode ser importante porque permite ao utilizador a alteração do PIN do seu *smart card*. No entanto, operações como a iniciação do *token*, não devem ser disponibilizadas sem controlo, uma vez que a sua utilização apaga todos os certificados e chaves privadas contidas no *smart card*.

6.3.5. openSC / CSP#11

Como já foi referido, a aquisição do *token* Axalto não incluía o software necessário para a sua instalação em cliente: CSP e PKCS #11. A sua utilização implica a aquisição de uma licença por cada posto em seja necessário proceder à instalação do software, o que obviamente tem um grande impacto no custo global da solução.

Decidiu-se então analisar o software do projecto OpenSC. Este projecto pretende desenvolver um conjunto de bibliotecas e utilitários para aceder a *smart cards*, implementando a interface PKCS #11. No entanto, para que as aplicações Windows o possam utilizar, é necessário um CSP. Eles disponibilizam um pacote completo para Windows, o *Smart Card Bundle*, que inclui o CSP#11, software que disponibiliza uma interface CAPI a partir de uma interface PKCS #11.

A arquitectura global da solução é apresentada na Figura 40. O CSP #11 disponibiliza a interface CAPI para a aplicação e dialoga com o OpenSC através da interface PKCS #11 por este disponibilizada.

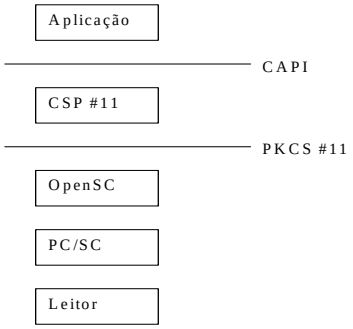


Figura 40: Arquitectura do *Smart Card Bundle* da OpenSC.

Logo à partida surgiu uma dificuldade: o OpenSC apenas suporta cartões com sistema de ficheiros e funções criptográficas (RSA), o que exclui os *Java Cards*, como é o caso do cartão Axalto Cyberflex 32k que tínhamos em mão. Na página Web da openSC, existe um aviso explicito a dizer que cartões Cyberflex 32k não são suportados, havendo o risco de o cartão ficar danificado. Como a RTS não tem nenhum requisito quanto à necessidade de utilização de *Java Cards*, decidiu-se continuar os testes com o iKey3000.

O problema maior é que o software não é estável. Não se conseguiu utilizar o CSP#11 de forma estável. Na página Web está indicado que o software não está preparado para correr em ambiente Windows XP. Foi feito algum esforço de investigação para tentar ultrapassar esta dificuldade mas não teve sucesso.

Em termos da utilização da interface PKCS#11 disponibilizada pelo openSC é possível a sua utilização para aceder a páginas Web que requerem a autenticação do cliente. No entanto, não foi possível a sua utilização para a geração de um par de chaves assimétricas e instalação do certificado.

A conclusão retirada foi que o openSC e o CSP#11 são um bom ponto de partida para a implementação de software criptográfico, uma vez que o código fonte está disponível, mas as suas versões Windows não são suficientemente estáveis para serem produto final.

6.4. Protótipo da Instituição de Saúde (IS)

Para a IS foi implementada uma PKI hierárquica com dois níveis de CA. No topo da hierarquia está a CA Raiz e no segundo nível a CA Emissora.

Ambas as CA foram implementadas utilizando o *Windows Server 2003 Enterprise Edition*: em modo *Stand Alone* na CA Raiz e em modo *Enterprise* na CA Emissora.

A CA Raiz apenas emite o seu certificado auto-assinado, que será a raiz de confiança para a IS, e o certificado para a CA Emissora, após o que é desligada (*power off*).

A Figura 41 mostra o certificado da CA Raiz da IS, designada IS Root CA.

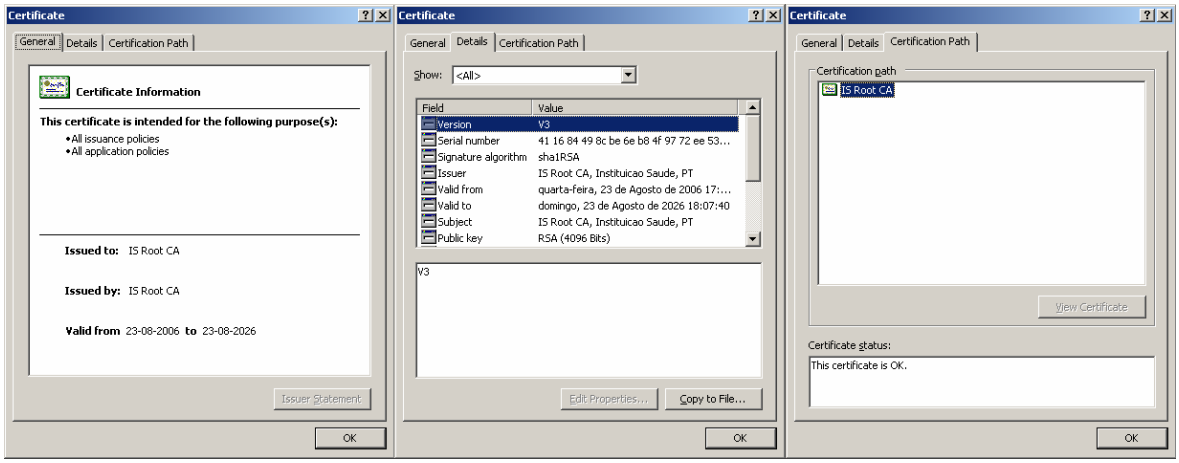


Figura 41: Certificado raiz da IS.

A CA Emissora da IS foi implementada utilizando o Windows Server 2003 Enterprise Edition em modo Enterprise devido à sua integração com o Active Directory. Esta integração permite utilizar os serviços do Active Directory para, entre outros, armazenar certificados e modelos de certificados, controlar as permissões para a emissão de certificados, disponibilizar os perfis dos utilizadores para quem são emitidos certificados.

Esta CA recebe o seu certificado da CA Raiz da IS, que se pode observar na Figura 42, e emite certificados para os Profissionais da IS.

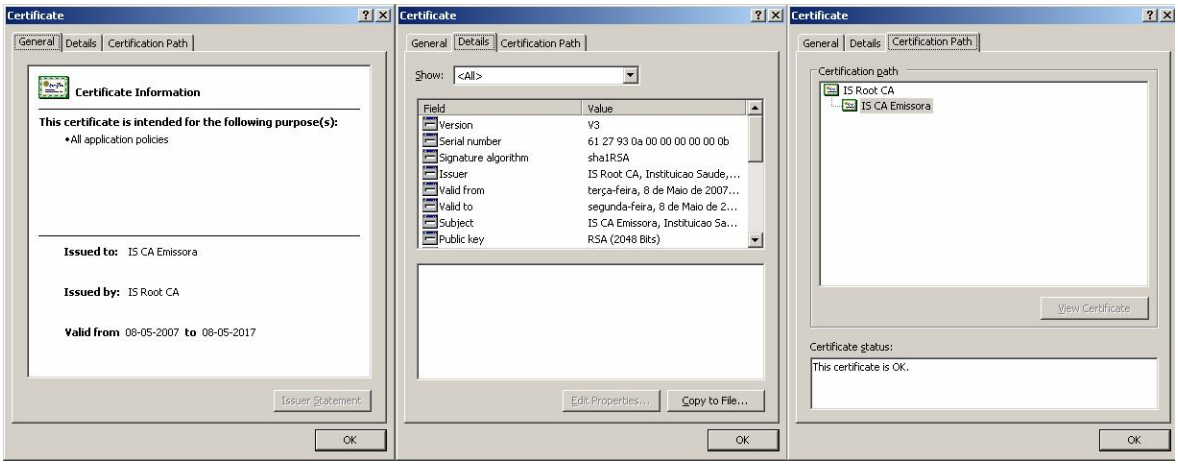


Figura 42: Certificado da CA Emissora da IS

Esta CA também disponibiliza um servidor Web, IIS 6.0, com os seguintes objectivos: (i) disponibilizar uma interface para o pedido (*enrolment*) de certificados, (ii) funcionar como CDP (*CRL Distribution Point*) para permitir o acesso público às listas de certificados revogados (CRL) publicados pela CA, e (iii) funcionar como AIA (*Authority Information Access*) para permitir o acesso público aos certificados da cadeia de certificados da IS.

6.4.1. Active Directory da IS

Como já foi referido, a IS do protótipo possui um serviço de Active Directory responsável pela gestão dos recursos da IS. Este colabora com a CA Emissora da IS para lhe fornecer a informação, de identificação e controlo, sobre os Profissionais da IS para a emissão de certificados, e como directoria para o armazenamento e publicação de certificados e de modelos de certificados.

No serviço de directoria foram criadas OUs (*Organization Unit*) para os profissionais à imagem do modelo utilizado num dos hospitais aderentes à RTS (HIP - Hospital Infante D. Pedro de Aveiro). A OU é um equivalente à pasta num sistema de ficheiros: um objecto agregador de outros objectos. Assim, foi criado uma OU por cada serviço de especialidade médica do HIP e, dentro destas, OUs que reflectem a organização interna de cada serviço. Como exemplo, para o serviço de Especialidades Cirurgicas foi criada uma OU, que contém a OU Cirurgia Geral, que por sua vez contém duas OUS: Médicos-Enfermeiros-Cir e Administrativos-Cir. A cada uma destas OUs podem depois ser atribuídos utilizadores (profissionais). A Figura 43 ilustra a organização interna do Active Directory, sendo visíveis as OUs dos serviços de Imagiologia, Imunoterapia e Especialidades Cirúrgicas.

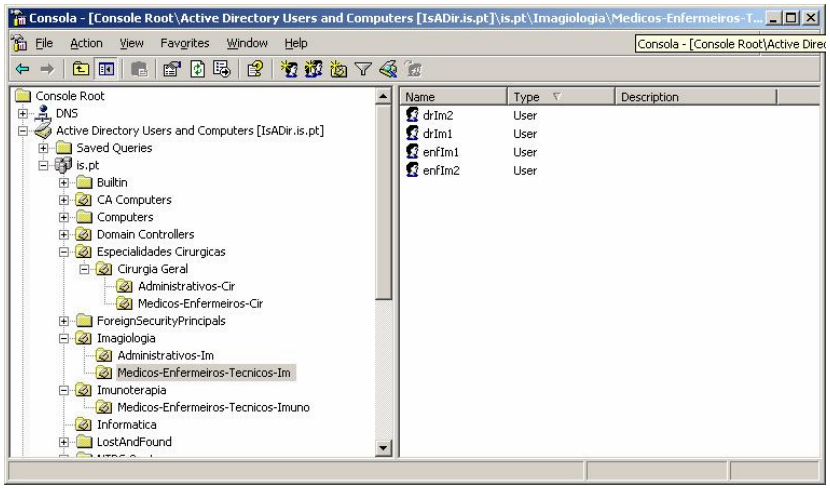


Figura 43: Estrutura da Active Directory da IS, sendo possível observar as OUs referentes aos serviços de especialidades médicas (Especialidades Cirúrgicas, Imagiologia e Imunoterapia), com as suas OUs internas que reflectem a organização interna de cada serviço (Cirurgia Geral, Administrativos-Cir, etc.), e os profissionais atribuídos à OU Médicos-Enfermeiros-Tecnico-IM.

Para o controlo do acesso dos Profissionais aos certificados RTS, foram criados grupos de utilizadores, um por cada perfil de Profissional identificado para o acesso à RTS (secção 2.4). Ou seja, numa OU designada RTS, foram criados os seguintes grupos de utilizadores RTS: RTS-Medico, RTS-Medico-ChefeServico, RTS-Enfermeiro, RTS-Enfermeiro-ChefeServico e RTS-Administrativo, como se pode observar na Figura 44.

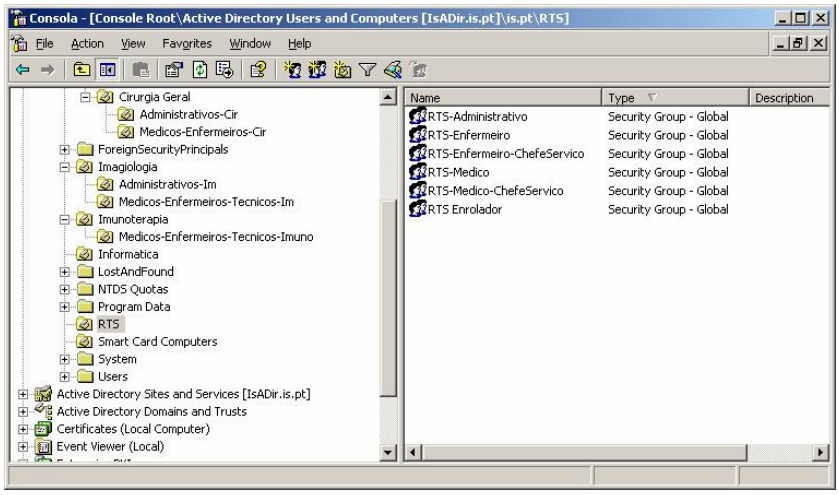


Figura 44: Grupos de utilizadores RTS criados para o controlo do acesso dos profissionais aos certificados RTS

Para um Profissional poder obter um certificado RTS correspondente ao seu perfil na IS, deve ser atribuído ao grupo correspondente a esse perfil, como se pode observar na Figura 45. Um mesmo profissional pode pertencer a mais do que um grupo, caso possua mais do que um perfil na IS. Profissionais que não sejam atribuídos a um grupo RTS não conseguem obter certificados para aceder à RTS.

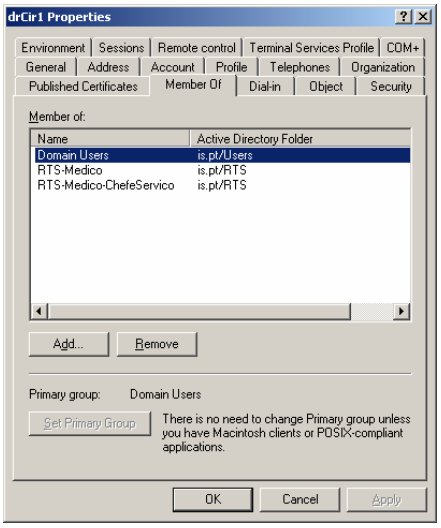


Figura 45: Grupos RTS a que o profissional drCir1 pertence: RTS-Medico e RTS-Medico-ChefeServiço. Ou seja, é um médico que exerce as funções de médico chefe de serviço na especialidade cirúrgica de Cirurgia Geral, e pode obter os certificados correspondentes a esses dois perfis.

Foi também criado um perfil para o técnico responsável pela gestão e iniciação dos smart cards a entregar aos profissionais.

6.4.2. Modelos de certificados

Os certificados emitidos pela CA Emissora da IS são baseados em modelos (*templates*) de certificados. Estes modelos permitem a definição das características dos respectivos certificados e a definição das regras para a sua obtenção.

A cada perfil de Profissional com acesso à RTS corresponde um modelo de certificado RTS. A maior parte dos valores atribuídos aos parâmetros de configuração dos modelos de certificados RTS são iguais, como por exemplo: o mesmo período de validade (2 dias), a utilização do mesmo CSP, a indicação para a não publicação e armazenamento dos certificados emitidos, a indicação para a obtenção do nome do profissional a partir do Active Directory. A indicação do CSP a utilizar impede a instalação de certificados RTS em dispositivos que utilizem outro CSP.

Os modelos de certificados RTS diferem entre si nos parâmetros de segurança e nas extensões de certificados. Para cada perfil de profissional foi definida uma politica de aplicação (*Application Policy*), que consiste num OID, que será incluída nos extensões *Application Policy* e *Extended Key Usage* dos certificados emitidos para os Profissionais com esse perfil. Alem do OID do perfil do Profissional, os modelos de certificados RTS devem conter também o OID para a política de autenticação de cliente (*Client Authentication*), como se mostra na Figura 46 para o modelo de certificado para o perfil RTS Médico.

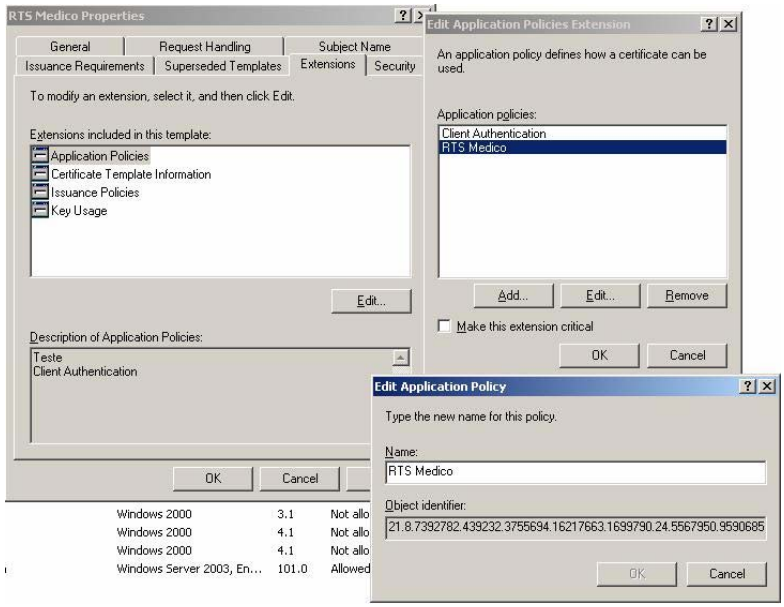


Figura 46: Definição das *Application Policies* para o modelo de certificado RTS-Medico

Para permitir o controlo do acesso aos certificados, cada modelo de certificado RTS é atribuído a um grupo RTS, criado no Active Directory, de acordo com o perfil do Profissional que contém. A esse grupo a dada permissão para a obtenção do certificados baseados no modelo a que foi atribuído, como se pode ver na Figura 47.

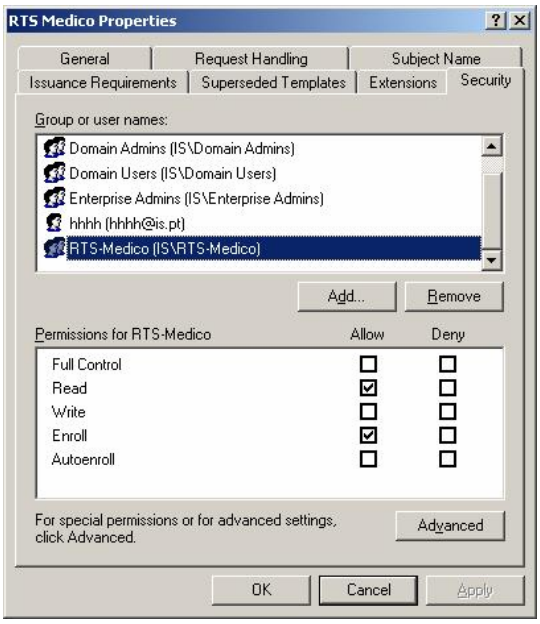


Figura 47: Configuração de segurança no acesso ao modelo de certificado RTS-Medico. Apenas o profissional correspondente deverá poder obter certificados baseados no modelo de certificados RTS-Medico

Para além dos modelos de certificados para a autenticação na RTS, foi definido um modelo de certificados (certificado IS) para a autenticação na IS para a obtenção de certificados RTS. Este modelo inclui uma política de aplicação (IS Profissional) necessária para a assinatura de pedidos de renovação automática,

e para o acesso à interface Web para a obtenção de certificados RTS. Esta política de aplicação é também inserida na extensão EKU dos certificados. Ao contrário do que sucede com os certificados RTS, estes não são de curta duração e os profissionais não podem proceder à sua renovação.

A emissão e instalação no *smart card* de certificados baseados no modelo de certificados Pessoal IS é efectuada por técnico com o perfil de responsável pela gestão e iniciação dos *smart cards*, sendo este perfil o único com direitos de acesso para a obtenção destes certificados.

Foi também criado um modelo de certificados para os técnicos responsáveis pela gestão e iniciação dos *smart cards*. Este tem uma política que lhes permite a instalação em *smart cards* de certificados emitidos para terceiros. Esta operação é realizada utilizando a interface Web disponibilizada pelo Windows para os serviços de certificados.

Para utilizar a funcionalidade de renovação automática (*auto-enrolment*) de certificados RTS disponibilizada pelo Windows, foi definido um segundo conjunto de modelos de certificados RTS (RTS Automático). Este conjunto difere do primeiro porque exige que o pedido de renovação seja assinado por um certificado válido que contenha a política de aplicação IS Profissional. Este serviço verifica a validade dos certificados do utilizador e, caso o seu prazo de validade tenha expirado ou esteja prestes a expirar, procede à sua renovação. Verifica também quais os certificados que o utilizador tem permissões para possuir e, caso não possua algum deles, desencadeia os mecanismos para a sua obtenção.

Apesar das facilidades que a utilização de modelos de certificados introduz na gestão de certificados, possui algumas limitações, tais como, o facto de nem todos os campos de um certificado poderem ser configurados desta forma, e por impor limitações aos valores permitidos para alguns campos. Um exemplo destas limitações é o facto de não ser possível definir certificados com um período de vida inferior a dois dias. Isto pode ser problemático se dois dias forem considerados como uma janela de risco muito grande para os certificados RTS. Na nossa opinião, dois dias parece ser um período de vida razoável para os certificados de curta duração.

6.4.3. Configuração das CA da IS

Ambas as CA da IS (CA Raiz e CA Emissora) foram configuradas para a inclusão dos campos AIA e CDP em todos os certificados por elas emitidos. De acordo com a arquitectura proposta nenhum destes dois campos é imprescindível para os certificados RTS, sendo no entanto o CDP imprescindível para os certificados IS.

O campo AIA especifica os locais onde podem ser obtidos os certificados da CA, que coincidem para as duas CA da IS no protótipo. Este campo, que contem um URL que aponta para uma página onde se encontram os certificados, é utilizado no processo de construção das cadeias de certificados para a localização de certificados em falta. A IS mantém um servidor WEB que permite o acesso livre ao URL referido no campo AIA.

Como na arquitectura de autenticação se preconiza que os Profissionais possuam no seu *smart card* todos os certificados da hierarquia de CA da sua IS, este serviço não será necessário. Além disso, como se

verificou que o motor de construção de cadeias de certificados do PKCS#11 não procura os certificados em falta, este campo apenas será utilizado pela CAPI. No entanto, como se verificou que funciona e como corresponde a uma recomendação PKIX, decidiu-se pela sua utilização.

O campo CDP especifica os locais onde se pode encontrar a mais recente CRL publicada pela CA que emitiu o certificado. Apesar de se propor a não utilização de CRLs para os certificados RTS, de curta duração, a sua utilização é necessária para os certificados IS, de duração "normal". O servidor Web da IS dá suporte a esta funcionalidade permitindo o acesso livro às CRL publicadas pelas CA da IS.

6.4.4. Certificação Cruzada com a RTS

Os Profissionais ao autenticarem-se para aceder ao Portal da RTS têm necessidade de autenticar o certificado do Portal, que foi emitido pela CA Emissora da RTS. Como se preconiza que cada entidade confie apenas no certificado raiz da sua instituição, é necessária a emissão de um certificado cruzado da IS para a RTS. Este certificado cruzado permite a construção de uma cadeia de certificados para a validação do certificado do Portal com a raiz no certificado de raiz da IS.

A emissão de certificados cruzados, se não for acompanhada de restrições de confiança, pode permitir o estabelecimento de relações de confiança indesejadas. Exemplos de restrições são as restrições de nome, restrições de política (restrições de emissão na Microsoft) e restrições ao comprimento da cadeia de certificados [32]. A Microsoft inclui a restrição de políticas de aplicação.

Destes mecanismos de restrição, apenas se utilizou a restrição de nome. Isto porque as restantes restrições exigem o contexto de uma aplicação para efectuar a sua validação, o que não existe num browser. As restrições de nome aplicadas no certificado cruzado emitido pela IS para a RTS, no painel Detalhes da Figura 48, restringem os nomes válidos dos sujeitos dos certificados (campo sujeito) a nomes no espaço de nomes da RTS: O=RTS, L=Aveiro e C=PT.

Figura 48: Certificado cruzado emitido pela IS para a RTS. No painel detalhe podem observar-se as restrições de nome aplicadas.

O certificado cruzado emitido pela RTS para a IS impõe restrições de nome correspondentes, limitando os nomes do sujeito do certificado (campo sujeito) ao espaço de nomes da IS.

6.4.5. Iniciação de Smart Cards

O *smart card* do Profissional deve ser-lhe entregue pessoalmente, depois da sua correcta iniciação pelo técnico responsável pela gestão e iniciação de *smart cards*, e deve conter os seguintes certificados e chaves privadas (as suas credenciais):

- **Certificado de Profissional da IS**: Certificado digital de chave pública, e correspondente chave privada, emitido pela sua IS para a autenticação do Profissional na renovação dos certificados RTS. Este certificado não é de curta duração, nem para a autenticação do Profissional no acesso à RTS. É exclusivamente para a autenticação do Profissional no processo de renovação de certificados e chaves para a RTS.
- **Certificado RTS**: Certificado digital de chave pública, e correspondente chave privada, para autenticação do Profissional no acesso à RTS. Este certificado é de curta duração e contém informação acerca do perfil do Profissional na IS a que está vinculado. Se o Profissional possuir mais do que um perfil na IS pode possuir mais do que um destes certificados.
- **Certificado digital de chave pública da CA raiz da sua IS:** É a raiz de confiança do Profissional, que deve servir para validar todos os certificados que lhe são apresentados.
- **Certificado digital de chave pública da CA Emissora que emitiu o certificado do Profissional para o acesso à RTS**: Destina-se à construção das cadeias de certificação para o cliente validar os certificados que lhe são apresentados.
- **Certificado digital de chave pública emitido pela CA Emissora da IS para a CA Emissora da RTS**: É o certificado cruzado que vai permitir a construção e validação das cadeias de certificação para o Profissional validar certificados das entidades da RTS.

Os certificados RTS, e correspondentes chaves privadas, podem ser renovados pelo Profissional sempre que haja necessidade. Quanto ao certificado de profissional da IS ele não está autorizado a renová-lo. Quando o seu prazo de validade expira, o *smart card* deixa de ser utilizável para acesso à RTS, devendo ser devolvido à IS para a sua eventual renovação pelo técnico de gestão de *smart cards*. Como este certificado é necessário para a renovação de certificados RTS, desta forma garante-se que apenas possuidores de *smart cards* correctamente iniciados conseguem obter certificados RTS.

6.4.6. Renovação de Certificados RTS Através do Servidor Web

A IS disponibiliza um servidor Web que permite ao Profissional a renovação dos certificados RTS. O acesso a este servidor é precedido da autenticação do Profissional utilizando o seu certificado de Profissional da IS, e correspondente chave privada, na qual ele tem que introduzir o PIN de protecção do *smart card*. O PIN é necessário para a assinatura de dados com a chave privada correspondente ao certificado de Profissional da IS, para a autenticação de cliente no contexto do estabelecimento de uma sessão SSL.

As páginas do servidor Web foram adaptadas das disponibilizadas pelo servidor de certificados do Windows, e contêm hiperligações para o acesso rápido aos certificados RTS, como se pode observar na Figura 49.

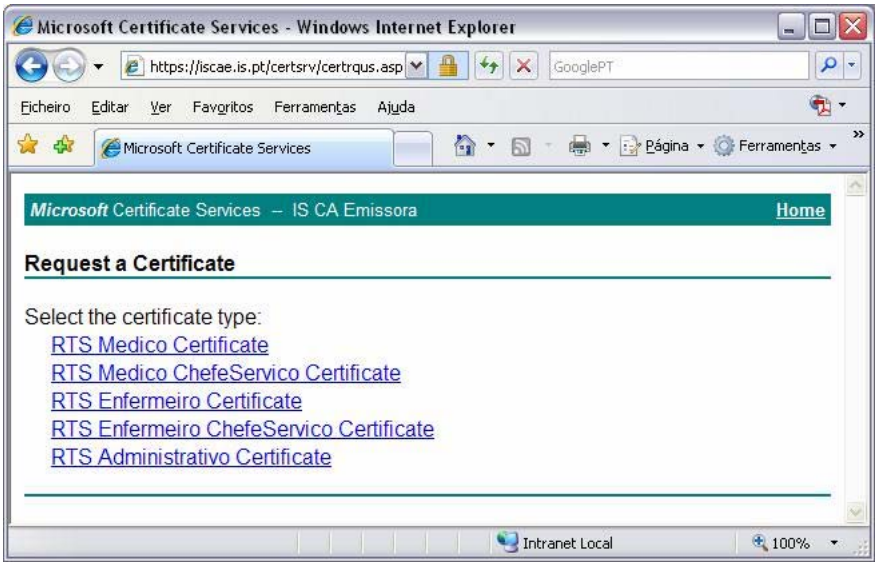


Figura 49: Página Web para a obtenção de certificados RTS.

O servidor Web utilizado é um IIS 6.0, configurado para fazer o mapeamento da autenticação através de certificados com utilizadores do domínio da IS, como se pode observar na Figura 50. Desta forma, ele adquire as permissões de acesso do Profissional, fazendo com que o controlo do acesso aos modelos de certificados seja feito pelo próprio Windows. Desta forma, o Profissional apenas consegue obter os certificados para os quais lhe foi dada permissão no respectivo modelo de certificado. O certificado pedido é logo emitido e pode ser instalado no *smart card*.

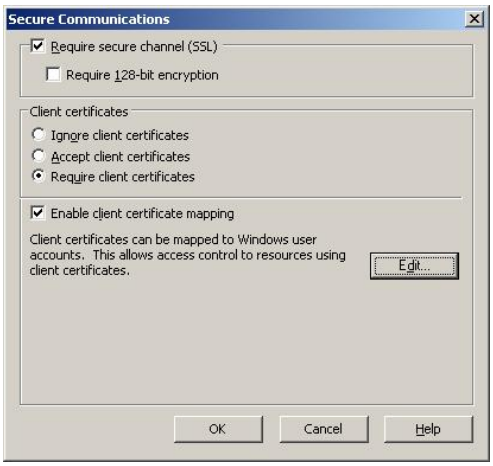


Figura 50: Configuração da autenticação no acesso ao servidor Web da IS

No pedido de um certificado de Profissional é novamente pedida a introdução do PIN do *smart card*, para que este possa gerar um novo par de chaves assimétricas para o novo certificado. Tanto navegadores

baseados na CAPI como navegadores baseados em PKCS#11 podem ser utilizados para a renovação de certificados RTS e consequente instalação do certificado no *smart card*.

Este processo de renovação de certificados têm um inconveniente que é o não remover do *smart card* os certificados expirados. Além disso, nenhum dos navegadores testados gera erro, ou uma mensagem de aviso, caso não consiga instalar o certificado por falta de espaço no *smart card.* Para a remoção dos certificados expirados é necessário recorrer a uma aplicação de gestão de certificados como o SafeSign. No entanto esta solução é perigosa porque pode invalidar o *smart card* caso o certificado de Profissional da IS seja removido. Outra hipótese é o desenvolvimento de código activo para proceder à remoção dos certificados expirados durante o processo de renovação. Notar que a instalação do certificado no *smart card* já efectuada no navegador com recurso a código activo descarregado do servidor de certificados.

A grande vantagem deste mecanismo de renovação de certificados RTS é que a renovação pode ser feita a partir de qualquer computador, pertença ou não ao domínio da IS. Os únicos requisitos para que o Profissional obtenha os certificados para os quais tem autorização de acesso, são a posse de um *smart card* correctamente iniciado e o conhecimento do respectivo PIN de protecção.

A desvantagem deste mecanismo é a necessidade de frequente acesso à página para proceder à renovação dos certificados RTS, devido à sua curta duração.

6.4.7. Renovação Automática de Certificados RTS

A renovação automática de certificados não é um requisito da arquitectura de autenticação proposta, nas foi incluída no protótipo pela simplificação que introduz no processo de renovação dos certificados RTS. Notar que a desvantagem da renovação de certificados através das páginas Web é que esta obriga a uma atitude activa do Profissional para aceder ao servidor e proceder à renovação.

Este mecanismo procede automaticamente à verificação dos certificados do Profissional e despoleta automaticamente o processo de renovação de certificados caso haja a necessidade. No entanto, o Profissional não fica completamente alheio do processo de renovação, uma vez que ele apenas ocorre se o Profissional confirmar o seu início. Além disso, ele é solicitado para introduzir o PIN de protecção do *smart card* para que possa ocorrer a geração de um novo par de chaves e a assinatura do pedido de renovação com o seu certificado de profissional da IS.

Outra vantagem deste mecanismo é que ele procede à remoção dos certificados expirados, sem necessidade de intervenção do Profissional.

A necessidade de um segundo conjunto de certificados RTS advém do facto da renovação automática de certificados por motivos de segurança ter sido configurada para exigir os pedidos de renovação autenticados com uma assinatura digital de um certificado de Profissional da IS. No caso da renovação através da página Web, a autenticação ocorre ao nível do SSL.

A grande desvantagem deste mecanismo de renovação é que ele apenas é possível em máquinas pertencentes ao domínio da IS e que possuam pelo menos o Windows XP SP2. Assim, a renovação de certifica-

dos de profissionais em mobilidade através de outras instituições não pode ser efectuada através deste mecanismo.

6.4.8. Logon Utilizando Smart Card

Esta funcionalidade também não é um requisito da arquitectura proposta. Foi também incluída porque reforça a segurança no acesso aos computadores dos Profissionais da IS. Apenas pode ser disponibilizada em computadores pertencentes ao domínio da IS e que possuam instalado pelo menos o sistema operativo WindowsXP SP2.

Esta funcionalidade permite que o acesso a um computador seja feito através da introdução do *smart card* do Profissional. Além disso permite a configuração para que a remoção do *smart card* provoque um *logout* ou a suspensão automática da sessão do Profissional. A sua configuração é efectuada através do Active Directory e pode ser configurada para cada máquina individualmente.

No protótipo o certificado utilizado para o *logon* automático foi o certificado de Profissional da IS.

6.5. Protótipo da RTS

Para a RTS foi também implementada uma PKI com dois níveis de CA, só que ao contrário da PKI da IS, ambas as CA foram implementadas utilizando o Windows 2003 Server Enterprise Edition em modo Stand Alone. A CA Raiz da RTS apenas emite o certificado para a CA Emissora, sendo depois desligada.

Tal como na IS ambas as CA estão configuradas para incluir os campos AIA e CDP em todos os certificados por elas emitidos e mantém um servidor Web para suporte a estas funcionalidades. Além disso, a CA Emissora da RTS emite um certificado cruzado para a IS para permitir a autenticação dos certificados dos profissionais através da sua raiz de confiança.

A RTS implementa também um Portal para o acesso dos Profissionais, utilizando um servidor IIS 6.0. O Portal recebe o seu certificado da CA Emissora da RTS.

A autenticação dos Profissionais pelo Portal da RTS é feita a dois níveis. Em primeiro pelo IIS, de acordo com a regras e cadeias de certificação do SSL. Num segundo nível pela aplicação, que apenas aceita certificados considerados válidos pelo Portal e que além disso possuam o OID de uma Política de Aplicação conhecida da RTS na extensão EKU. O Portal apenas inicia a sessão se o certificado for considerado válido nos dois níveis.

No protocolo SSL, quando se pretende a autenticação de cliente, o servidor envia para o navegador a lista dos nomes das CAs da qual ele aceita certificados. Estes nomes podem especificar nomes de CA raiz ou nomes de CA intermédias [25]. Portanto o servidor do Portal da RTS irá enviar aos clientes SSL (navegadores dos Profissionais) uma lista das CAs das quais aceita certificados cliente, que será utilizada pelo navegador para filtrar os certificados do Profissional que este pode utilizar para se autenticar. No entanto, verificámos que a filtragem de certificados é feita apenas baseada em certificados de raiz de confiança (*trusted root certificates*). Isto implica que o Portal da RTS tem que estar na posse dos certificados raiz de todas as IS par-

ticipantes na RTS, o que levanta a seguinte questão: se o Portal tem que confiar nos certificados raiz de todas a IS participantes na RTS, então para quê utilizar a certificação cruzada da RTS para as IS?

Há duas razões para utilizar a certificação cruzada. Primeiro porque, por motivos de performance e segurança, o IIS, no processo de construção da cadeia de certificação para a validação do certificado do cliente, não utiliza a extensão AIA nos certificados para a obtenção dos certificados intermédios em falta [71]. Isto implica que os certificados de raiz das IS não são suficientes para que o Portal valide os certificados dos Profissionais, sendo necessários os certificados de toda a hierarquia de CA de todas as IS participantes. Portanto, o certificado cruzado permite uma solução mais correcta e simples.

Em segundo, porque a certificação cruzada permite a utilização de restrições de confiança, que pode ser importante para a redução do conjunto dos certificados emitidos pelas IS e que podem ser utilizados para a autenticação na RTS.

6.6. Ambiente de Trabalho dos Profissionais

Foram testados dois browsers, o Internet Explorer 7.0 (que usa a CAPI) e o Mozilla Firefox 2.0 (que usa PKCS#11) para a avaliação da interacção do Profissional com o servidor da IS para a renovação de certificados RTS, e com o Portal da RTS. Como o Profissional pode possuir mais do que um certificado para a sua autenticação, os navegadores têm que ser configurados para pedirem ao Profissional para seleccionar qual o certificado a apresentar para a sua autenticação. Ambos os navegadores podem ser utilizados para o acesso aos dois portais, notando-se no entanto pequenas diferenças na forma como lidam com os certificados.

6.6.1. Internet Explorer

Quando o *smart card* é inserido pela primeira vez no computador, e assumindo que tem os respectivos *driver* e o CSP correctamente instalados, os certificados que ele contém são copiados para arquivos de certificados do utilizador local, sendo pedida a confirmação do utilizador apenas para certificados raiz (em caso de resposta afirmativa serão instalados no arquivo de certificados de raiz de confiança do utilizador local). A partir desse momento esses certificados ficam disponíveis para serem utilizados em todas as aplicações que utilizem a CAPI. Quando o *smart card* é removido, todos os certificados previamente copiados permanecem nos arquivos para onde foram copiados, com excepção dos certificados pessoais do cliente, como por exemplo o certificado RTS e o certificado IS, que são removidos.

Para a validação dos certificados do Portal, a CAPI constrói e valida a cadeia de certificados até atingir o certificado de raiz de confiança. Em caso de falta de certificados intermédios, ela usa o campo AIA para os procurar e obter. Só que este mecanismo não funciona com certificados cruzados. Existe um mecanismo adicional para obter certificados cruzados, mas é baseado no Active Directory, o que não serve os nossos propósitos uma vez que nem todos os acessos do Profissional à RTS são efectuados a partir de computadores do domínio da sua IS. Isto implica que para validar o certificado do Portal da RTS o Profissional necessite de ter no seu *smart card* pelo menos o certificado raiz da IS a que está vinculado e o certificado cruzado emitido pela sua IS para a RTS.

6.6.2. Mozilla Firefox

Com o PKCS#11 os certificados no *smart card* ficam imediatamente disponíveis, sendo os certificados da hierarquia da IS e o certificado cruzado colocados no arquivo de certificados de entidades de certificação, podendo ser observados utilizando o gestor de certificados do Firefox. No entanto, o Firefox necessita que as propriedades dos certificados indiquem qual o uso que se lhes pode dar, e por defeito estas propriedades indicam que nenhum uso se pode dar aos certificados no *smart card*, como se pode observar na Figura 51 com o certificado de raiz da IS

Figura 51: Propriedades por defeito do certificado raiz da IS contido no *smart card*

Este comportamento leva a que ao aceder ao Portal da RTS o Firefox não consiga validar o certificado apresentado pelo Portal, apresentando a mensagem apresentada na Figura 52.

Figura 52: Mensagem de aviso do Firefox indicando que não consegue validar o certificado apresentado pelo Portal da RTS.

Para que esta mensagem deixe de aparecer é necessário editar pelo menos as propriedades do certificado cruzado da IS para a RTS e indicar que o certificado é válido para autenticar sítios na Web.

O modo como o PKCS#11 constrói e valida as cadeias de certificados é diferente do utilizado pela CAPI. A cadeia de certificados é construída até ao primeiro certificado de confiança, seja ele um certificado de raiz ou não. Além disso, não utiliza a extensão AIS para procurar e obter certificados em falta. Como ele apenas permite que o utilizador (Profissional) se autentique utilizando certificados que ele consegue validar, implica que tenha que estar na posse de pelo menos o certificado da CA Emissora da IS: apenas com o certificado da raiz não consegue validar o certificado do Profissional porque lhe falta o certificado da CA Emissora para estabelecer a cadeia. Ou seja, para funcionar com o Firefox, o *smart card* tem que conter pelo menos o certificado cruzado da IS para a RTS e o certificado da CA Emissora da IS.

Quando se remove o *smart card* todos os certificados pessoais (certificados RTS e certificado IS) são removidos do computador, bem como todos os restantes certificados cujas propriedades não tenham sido alteradas. Aqueles cujas propriedades foram alteradas permanecem nos arquivos de certificados do PKCS#11.

7 Avaliação

Neste capítulo vamos proceder à avaliação da arquitectura proposta no capítulo 5 e da implementação do seu protótipo descrita no capítulo 6, face aos objectivos iniciais listados na secção1.1.

Em relação ao primeiro objectivo, autenticação forte baseada num mecanismo com dois factores de autenticação, ele foi conseguido na totalidade. Um Profissional apenas se autentica utilizando o seu *smart card* e conhecendo o respectivo PIN de protecção. A perda de um *smart card* representa um risco reduzido, uma vez que ele apenas pode ser utilizado conhecendo o seu PIN de protecção, sendo limitado o número de tentativas consecutivas erradas de introdução do PIN. Ainda assim, este mecanismo não impede que o Profissional ceda o seu *smart card* para outras pessoas o utilizarem. Uma solução para este problema passaria pela introdução de um terceiro factor de autenticação biométrico, que actuaria em conjunto com o PIN para desbloquear o dispositivo, tal como apresentado na secção 3.8.3.

Em relação ao segundo objectivo, a mobilidade dos profissionais, a utilização de *smart cards* embebidos em *tokens* USB é a solução mais promissora, mas ainda tem alguns problemas. Por exemplo não podem ser utilizados em PDAs e *Smartphones*. Mais problemático ainda, é que a sua utilização ainda levanta problemas em relação ao software instalado nos computadores onde vão ser usados. Como vimos na secção 6.3, não é fácil obter uma solução livre para o *middleware* necessário para as várias aplicações (navegadores) interagirem com *smart cards* de vários fabricantes.

Em relação ao terceiro objectivo, libertar a RTS da gestão dos Profissionais vinculados às IS, foi totalmente atingido. O Portal da RTS apenas exige que os Profissionais possuam um certificado válido emitido pela sua IS contendo a informação do seu perfil na IS. As IS têm controlo total na gestão dos seus profissionais e dos seus perfis, fornecendo-lhe acesso à RTS através da emissão de um certificado RTS com o conteúdo adequado.

Em relação ao quarto objectivo, permitir à RTS obter a informação do perfil dos profissionais que acedem ao Portal, para permitir a aplicação da política de autorização adequada, foi totalmente atingido. O Portal obtém o perfil do Profissional a partir do certificado por ele apresentado no processo de autenticação. Assim, se o certificado for válido e a RTS confiar no processo de certificação conduzido pela IS que o emitiu, então pode confiar que o Profissional possui o perfil indicado no certificado. Em relação ao tempo de vida do certificado, a sua duração deve ser alvo de uma política global da RTS que todas as IS participantes devem seguir rigorosamente.

Quanto ao objectivo de minimizar a comunicação com as IS para a autenticação dos seus Profissionais, foi totalmente atingido. O Portal da RTS, por si só, é capaz de autenticar Profissionais apenas validando o seu certificado, sem necessidade de consultar uma CRL, ou qualquer outro mecanismo remoto de revogação de certificados. Nenhuma comunicação *online* com qualquer IS é necessária, para a autenticação de um Profissional.

Finalmente, o sexto objectivo era a compatibilidade entre navegadores da Internet. Neste caso, pode ser difícil disponibilizar o mesmo conjunto de funcionalidades em todos os navegadores devido às diferentes

soluções de *middleware* para fazer a interface entre as aplicações e os *smart cards* (CAPI e PKCS#11). Além disso, algumas operações para a gestão de *smart cards*, como a limpeza dos certificados expirados, pode exigir a execução de código activo no navegador do Profissional.

Finalmente o sétimo objectivo era evitar o desenvolvimento de código. Foi quase atingido, uma vez que praticamente só se instalou e configurou aplicações, serviços e módulos de software previamente existentes. A única excepção foi a adequação das páginas Web para o pedido de certificados em que foi necessário alguma alteração do seu código ASP. A inclusão futura de novas funcionalidades irá com certeza exigir o desenvolvimento de mais código. Um exemplo, é a gestão de credenciais nos *smart cards*, nomeadamente a já referida operação para remover os certificados já expirados e as correspondentes chaves privadas.

8 Conclusões

Neste documento descrevemos a proposta de uma arquitectura para a autenticação das entidades que comunicam no âmbito da RTS. A vertente analisada com maior enfoque foi a do acesso à RTS pelos Profissionais vinculados às IS. Como estes acedem aos serviços da RTS, disponibilizados num servidor Web, utilizando um navegador da Internet, a sua autenticação foi mapeada em cima da autenticação de cliente do protocolo SSL. As credenciais dos Profissionais são emitidas pelas respectivas IS e são constituídas por um certificado digital de curta duração e a correspondente chave privada, ambos armazenados dentro de um *smart card*. A curta duração destes certificados permite a simplificação da PKI, uma vez que eles não são publicados e não são incluídos em nenhum serviço de revogação de certificados (CRL).

As principais características desta solução são: (i) a utilização de *smart cards* para a autenticação forte dos profissionais, para o armazenamento das suas credenciais e para potenciar a sua mobilidade; (ii) a utilização de certificados digitais com intervalos de validade curtos, contendo a identificação do Profissional e o seu perfil na IS, para a autenticação no acesso à RTS e determinação da politica de autorizações na RTS; (iii) a utilização de certificados de duração "normal" para a renovação dos certificados RTS dos Profissionais e para a autenticação dos Servidores e Serviços da RTS e das IS; (iv) uma PKI global com um modelo híbrido em que a RTS e cada uma das IS gere a sua própria PKI; e (v) a utilização de certificação cruzada para o estabelecimento de relações de confiança necessárias para a validação das credenciais dos Profissionais e dos serviços.

Como regra geral na implementação do protótipo evitou-se o desenvolvimento de código, preferindo-se a utilização e configuração de tecnologia disponível. O protótipo realizado foi baseado exclusivamente em tecnologia fornecida por sistemas Windows, ou desenvolvida para eles. Em relação aos navegadores utilizados pelos Profissionais, foram testados dois dos mais populares em ambiente Windows: o Internet Explorer e o Mozilla Firefox.

O maior benefício da utilização da tecnologia Windows é a sua integração com os serviços do Active Directory, que permite um ambiente integrado para a gestão de utilizadores (Profissionais) e certificados. Esta funcionalidade é relevante para a IS, onde é necessário um maior esforço para a montagem de toda a arquitectura da PKI. A tecnologia Windows disponibiliza ainda duas funcionalidades úteis que são (i) o serviço de renovação automática de certificados que simplifica a tarefa de renovação de certificados e (ii) um serviço de *logon* por certificados que permite uma autenticação por dois factores no acesso ao computador.

A maior dificuldade encontrada é a gestão e utilização de *smart cards* pelos Profissionais. A existência de mais do que um *middleware* para a gestão de *smart cards* e as diferentes aproximações em relação à utilização do *middleware* pelas várias aplicações, navegadores em particular, tornam difícil uma interface clara e ubíqua para utilização dos *smart cards* pelos Profissionais, em qualquer IS aderente à RTS. Este é o aspecto mais crítico a ter em conta na implementação da arquitectura pelos vários computadores das várias IS.

8.1. Trabalho futuro

Nunca uma história fica completa quando a acabamos de contar. O mesmo se passa com os trabalhos, há sempre aspectos que se podem melhorar, novos aspectos que se podem incluir, …

Em relação a este trabalho, parece-me que os aspectos mais importantes para trabalho futuro serão a implementação da interacção com o novo Cartão do Cidadão para a autenticação dos utentes no acesso ao Portal do Utente e, a inclusão da assinatura digital no sistema de autenticação da RTS.

A interacção com o Cartão do Cidadão foi já abordada em capítulos anteriores, mas será necessário concretizá-la.

Quanto à assinatura digital, apesar de no momento não se fazer sentir a sua necessidade, será, com certeza, necessário vir a incluí-la. A evolução da RTS levará à inclusão da produção de informação médica nas suas funcionalidades. Nessa altura, a assinatura digital será um serviço crítico para a RTS, uma vez que é a tecnologia universalmente utilizada para garantir a integridade e autenticidade dos documentos e a única a permitir o não-repúdio da origem da informação.

A inclusão da assinatura digital trará consigo dificuldades que será necessário abordar. Por um lado, a certificação da PKI da RTS, por uma entidade certificadora reconhecida, para permitir a produção de assinatura qualificada (com o maior grau de confiança). Por outro, o problema da difusão do seu certificado raiz para permitir uma validação dos seus certificados num universo alargado, nomeadamente fora das fronteiras da RTS.

Um outro aspecto relacionado com a assinatura de documentos será a necessidade de um serviço de estampilha temporal para permitir a datação segura dos documentos produzidos. Frequentemente, não é suficiente a garantia da autenticidade e integridade de um documento, é necessária também uma a garantia segura sobre o instante da sua produção. Uma hipótese a considerar consiste na exploração do serviço de Marca Do Dia Electrónica (MDDE) prestado pelos CTT em colaboração com a Multicert[14]

A evolução do sistema de autorização poderá também ter impactos na PKI. As recomendações sobre confidencialidade e segurança da informação médica apontam a necessidade de um controlo do acesso à informação dos pacientes cada vez mais individualizado e cada vez com uma maior intervenção do paciente no controlo dos acessos à sua informação médica. Assim, sistemas de controlo de acessos à informação mais evoluídos irão ser necessários, que irão necessariamente interferir com a autenticação e com a PKI que lhe serve de base. Nomeadamente, se o fornecimento de informação aos profissionais via RTS tiver que se sujeitar a autorizações expressas fornecidas pelos utentes, será necessário integrar a autenticação de utentes na RTS.

Finalmente, por uma questão de escalabilidade será natural que surjam diversas instâncias da RTS, interligando conjuntos diferentes, mas não necessariamente disjuntos, de Instituições de Saúde. Esse facto

[14] https://sce.ctt.pt/mdde/index.html

implicará a adopção de medidas que possam permitir a autenticação de Profissionais em qualquer instância da RTS, e não apenas numa, o que neste momento não está previsto.

Bibliografia

1. Cunha, J. P. S., et al., *The RTS Project: Promoting secure and effective clinical telematic communication within the Aveiro region, eHealth 2006 High Level Conference*. 2006: Malaga, Spain.
2. Gomes, H., Zúquete, A., and Cunha, J. P., *Arquitectura de Autenticação baseada em Certificados para a Rede Telemática da Saúde (RTS), 2ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2006)*. 2006: Aveiro, Portugal.
3. Gomes, H., Cunha, J. P., and Zúquete, A. *Authentication Architecture for e-Health Professionals*. in *2nd International Symposium on Information Security (IS'07)*. 2007. Vilamoura, Algarve, Portugal: (a publicar).
4. Cunha, J. P. S., *RTS Network: Improving Regional Health Services through Clinical Telematic Web-based Communication System, eHealth Conference 2007*. 2007: Berlin.
5. Costa, C., et al., *Relatório de planeamento estratégico de sistemas de informação*. 2005: http://www.rtsaude.org.
6. Cruz, I., et al., *Relatório de análise de processos e fluxos de informação*. 2005: http://www.rtsaude.org.
7. Guerra, A., *Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais*. 2004, Comissão Nacional de Protecção de Dados: http://www.cnpd.pt/bin/relatórios/outros/Relatorio_final.pdf.
8. *Informação genética pessoal e informação de saúde, Lei n.º 12/2005*. 26 de Janeiro de 2005.
9. *Authentication*. Wikipedia [cited 2007-01-15]; Available from: http://en.wikipedia.org/wiki/Authentication.
10. Machado, J. P., *Grande Dicionário da Língua Portuguesa.*, ed. Sociedade de Língua Portuguesa. 1981: Amigos do Livro Editores.
11. Nakhjiri, M. and Nakhjiri, M., *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility*. 2005, John Wiley & Sons, Lda.
12. Smith, R. E., *Authentication: From Passwords to Public Keys*. 2001, Addison-Wesley.
13. Anderson, R., *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2001, Wiley Computer Publishing.
14. Zúquete, A., *Segurança em Redes Informáticas*. 2006, FCA – Editora de Informática.
15. Rigney, C., et al., *Remote Authentication Dial In User Service (RADIUS), RFC2865*. June 2000, IETF.
16. Calhoun, P., et al., *Diameter Base Protocol, RFC 3588*. September 2003, IETF.
17. *802.1X, Port Based Network Access Control*. 2004, IIIE Computer Society: http://standards.ieee.org/getieee802/download/802.1X-2004.pdf.
18. Neuman, C., et al., *The Kerberos Network Authentication Service (V5), RFC 4120*. July 2005, IETF.
19. Simpson, W., *PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994*. August 1996, IETF.
20. Aboba, B., et al., *Extensible Authentication Protocol (EAP), RFC 3748*. June 2004, IETF.
21. Kamada, K. i. and Sakane, S., *Client-Friendly Cross-Realm Model for Kerberos 5, draft-kamada-krb-client-friendly-cross-01*. March 2007, IETF: Internet Draft.
22. Sakane, S., Zrelli, S., and Ishiyama, M., *Problem statement on the cross-realm operation of Kerberos in a specific system, draft-sakane-krb-cross-problem-statement-01*. October 2006, IETF: Internet Draft.
23. Zrelli, S., et al., *XKDCP, the Inter-KDC protocol for cross-realm operations in Kerberos, draft-zrelli-krb-xkdcp-00*. June 2006, IETF: Internet Draft.
24. Zhu, L. and Tung, B., *Public Key Cryptography for Initial Authentication in Kerberos (PKINIT), RFC 4556*. June 2006, IETF.
25. Dierks, T. and Rescorla, E., *The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346*. 2006, IETF.

26. Nash, A., et al., *PKI: Implementing and Managing E-Security*. 2001, Berkeley - RSA Press.
27. Choudhury, S., Bhatnagar, K., and Haque, W., *Public Key Infrastructure Implementation and Design*. 2001, M&T Books.
28. Chokhani, S., et al., *Internet X.509 Public Key Infrastructure Certificate Pol-icy and Certification Practices Framework, RFC 3647*. November 2003, IEFT.
29. *ITU-T Rec. X.509 | ISO/IEC 9594-8, The Directory: Authentication Framework*. 2000.
30. *ITU-T Recommendation X.500 | ISO/IEC 9594-1, The Directory: Overview of concepts, models and services*. August 2005.
31. Housley, R., Polk, W., Ford, W. and D. Solo, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280*. April 2002, IETF.
32. Lloyd, S., et al., *CA-CA Interoperability*. 2004, PKI Forum: http://www.pkiforum.org/resources.html.
33. Farrell, S. and Housley, R., *An Internet Attribute Certificate Profile for Authorization, RFC 3281*. April 2002, IETF.
34. *How CA Certificates Work, Windows Server 2003 Technical Reference*, Microsoft Technical Reference

http://technet2.microsoft.com/windowsserver/en/library/0e4472ff-fe9b-4fa7-b5b1-9bb6c5a7f76e1033.mspx?mfr=true.

35. Bar-El, H., *When To Use Biometrics, Security White Papers and Articles*. 2004-03-22: http://www.securitydocs.com/library/742.
36. Dierks, T. and Allen, C., *The TLS Protocol Version 1.0, RFC 2246*. January 1999, IETF.
37. Rescorla, E., *HTTP Over TLS, RFC 2818*. May 2000, IETF.
38. Kent, S. and Seo, K., *Security Architecture for the Internet Protocol, RFC 4301*. December 2005, IETF.
39. Kent, S., *IP Authentication Header, RFC 4302*. December 2005: IETF.
40. Kent, S., *IP Encapsulating Security Payload (ESP), RFC 4303*. Decemer 2005, IETF.
41. Kaufman, C., *Internet Key Exchange (IKEv2) Protocol, RFC 4306*. December 2005, IETF.
42. Katehakis, D. G., et al., *A Holistic Approach for the Delivery of the Integrated Electronic Health Record within a Regional Health Information Network, Technical Report 350 (FORTH-ICS/ TR-350)*. February 2005, Foundation for Research and Technology - Hellas, Institute of Computer Science: Heraklion, Crete, Greece.
43. Tsiknakis, M., et al., *An Architecture for Regional Health Information Networks Addressing Issues of Modularity and Interoperability*. Journal of Telecommunications and Information Technology (JTIT), December 2005: p. 26-39.
44. *HYGEIAnet*. Integrated Health Telematics Network of Crete [cited 2007-03-25]; Available from: http://www.hygeianet.gr.
45. *Extensible Markup Language (XML), WC3 Architecture Domain*: http://www.w3.org/XML.
46. *MedCom IV: Status Plans and Projects, MedCom – the Danish Healthcare Data Network*. December 2003: http://www.medcom.dk/dwn396.
47. *ISO 9735, Electronic data interchange for administration, commerce and transport (EDIFACT)*: http://www.iso.org
48. Pedersen, C. D. *An Baltic healthcare network and interoperability challenges*. in *Cisco eHealth think tank meeting*. 2005. Brussels.
49. Voss, H., Heimly, V., and Sjögren, L. H., *The Baltic ehealth Network – taking secure, Internet-based healthcare networks to the next level*. May 2005, Norwegian Centre for Informatics in Health and Social Care.
50. *The Danish eHealth experience: One Portal for Citizens and Professionals*. 30-12-2006, Sundhed.dk: http://dialog.sundhed.dk/NR/rdonlyres/ebkhhgtqfnuti6fyky74rwj7begja2grffb4cixasfccxmmopno6h3gdcgarwvagvhb76lll4kwvhoazq2snzdg2mee/The+Danish+eHealth+experience.pdf.

51. Brox, E. A., *Information Security in Distributed Health Information Systems in Scandinavia: A comparative study of external conditions and solutions for exchange and sharing of sensitive health information in Denmark, Norway and Sweeden, Department of Computer and Information Science*. June 2006, Norwegian University of Science and Technology.
52. Rossing, N., *The Health Portal (www.sundhed.dk) And The Health Data Network Of Denmark, Executive Summary of Presentaion in eHealthAthens2005 (http://www.ehealthathens2005.gr)*.
53. Ribeiro, C., Silva, F., and Zúquete, A. *A Roaming Authentication Solution for Wifi using IPSec VPNs with client certificates*. in *TERENA Networking Conference 2004*. 2004. Rhodes, Greece.
54. Zúquete, A. and Ribeiro, C. *A flexible, large-scale authentication policy for WLAN roaming users using IPSec and public key certification*. in *7ª Conferência sobre Redes de Computadores (CRC 2004)*. 2004. Leiria, Portugal.
55. *Cartão do Cidadão: Relatório Final da Prova de Conceito*. 2006: http://www.cartaodecidadao.pt.
56. *Manual de Utilização da Aplicação do Cartão de Cidadão*. Fevereiro de 2007: http://www.cartaodecidadao.pt/images/stories/manual_cart%E3o_de_cidad%E3o_v1%200.pdf.
57. *Decreto-Lei 62/2003 de 3 de Abril – Série 1-A, Aprova o regime jurídico dos documentos electrónicos e da assinatura digital*.
58. Bourka, A., Polemi, N., and Koutsouris, D., *An Overview in Healthcare Information Systems Security, MEDINFO 2001*. 2001: London.
59. Anthony Nadalin, C. K., *Web Services Security: Soap Message Security 1.0 (WS-Security 2004), OASIS, IBM, Microsoft, Verisign, Sun*. 2004: http://www.oasis-open.org/commitees/tc_home.php?wg_abbrev=wss.
60. Cantor, S., et al., *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS, Internet2, Nokia, RSA Security, Sun Microsystems*. 2004: http://xml.coverpages.org/SAML-core-20-CD-01.pdf.
61. Gudgin, M., et al., *SOAP Version 1.2 Part 1: Messaging Framework, W3C, Microsoft, Sun Microsystems, IBM, Canon*. 2003: http://www.w3c.org/TR/2003/REC-soap12-part1-20030624/.
62. Komar, B., *Microsoft Windows Server 2003 Pki And Certificate Security*. 2004, Microsoft Press.
63. Majava, J. and Immonen, A., *Registration Process in Health Care Public Key Environment, 6th Nordic Confer-ence on eHealth and Telemedicine*. September 2006: Helsinki, Finland.
64. Naor, M. and Nissim, K. *Certificate Revocation and Certificate Update*. in *Proc. 7th USENIX Security Symposium*. 1998.
65. Costa, C., Oliveira, J. L., and Silva, A., *Um Novo Mecanismo de Autenticação para Sistemas de Informação Clínica, 4ª Conferência sobre Redes de Computadores (CRC'2001)*. 2001: Covilhã, Portugal.
66. Clercq, J. D., *Keeping Your Business SAFE from Attack: Encryption and Certification Services*, Windows IT Pro eBooks: http://www.windowsitpro.com/eBooks.
67. *PKCS #11 v2.20: Cryptographic Token Interface Standard*. 2004, RSA Laboratories,: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf.
68. *PC/SC Workgroup*: http://www.pcscworkgroup.com.
69. *M.U.S.C.L.E.: Movement for the Use of Smart Cards in a Linux Environment*: http://www.linuxnet.com.
70. Microsoft TechNet, *Microsoft Windows Server TechCenter, Supported Hardware*: http://technet2.microsoft.com/windowsserver/en/library/73cfb9ef-0f4c-4a40-ac8d-f0af056431581033.mspx?mfr=true.
71. Microsoft Technical Support, *Http.sys registry settings for IIS*: http://support.microsoft.com/kb/820129/en-us.