

Especificação para
Documento Clínico Electrónico
Relatório de Imagem

João Paulo do Nascimento Janeiro

2010

Mestrado em Informática Médica
Faculdade de Ciências | Faculdade de Medicina
Universidade do Porto

Orientador:

Prof. Doutor Luís Filipe Antunes

Faculdade de Ciências da Universidade do Porto

Co-orientador:

Prof. Doutor Eduardo Correia

Faculdade de Ciências da Universidade do Porto

Agradecimentos

Ao Prof. Doutor Altamiro Costa Pereira, pelo empenho que tornou possível a existência deste mestrado, pela atenta direcção da sua 3ª edição e, sobretudo, pelo afável acolhimento e sempre pertinentes conselhos;

Aos docentes do Mestrado em Informática Médica, por tudo o que com eles pude aprender;

À Dra. Isabel Távora, ao Dr. Schäller Dias e ao Dr. Manuel Abecasis pela disponibilidade de acesso à informação necessária e pelo apoio de sempre;

Aos meus orientadores de dissertação, Prof. Doutor Luís Filipe Antunes e Prof. Doutor Eduardo Correia, por tudo e mais ainda pela paciência de comportarem esta minha incursão em tema tão distante da minha formação de base e por me recordarem de que é sempre possível um pouco mais de esforço;

À minha família, pela tolerância às minhas ausências, físicas e mentais;

A todos o meu maior obrigado!

Preâmbulo

A radiologia, ou imagiologia médica, vive cada vez mais em estreita relação com a ciência informática, de uma forma que provavelmente não terá paralelo noutras especialidades médicas. Desde a gestão de fluxo de pacientes e horários, particularmente importante numa especialidade em que os contactos são curtos e, consequentemente, o número de pacientes elevado, até à emissão de uma opinião, sempre documentada em relatório (talvez o passo em que primeiro se difundiu o uso de computadores), existe uma enorme e crescente dependência da informática. No meio ficará porventura a fase de maior proximidade do radiologista com o computador, agora que a imagem digital substitui quase por completo a clássica película radiográfica e a visualização de imagem médica é praticamente toda feita nos monitores das estações de trabalho. É também a fase que tem merecido a maior aposta por parte da indústria de *software*, disponibilizando aplicações com múltiplas e interessantes opções de processamento de imagem.

A escolha, para tema de dissertação, de uma questão relativa à fase de produção de relatório associa-se ao facto de ser também aquela que menos se viu desenvolvida na qualidade do apoio informático. Acredito que num futuro próximo todas estas fases estarão encadeadas e o relatório será não só um texto ditado mas antes uma relação estruturada dos achados, que permita a sua integração, comparação e análise automatizada, com perspectivas inimagináveis em investigação. Mas para que isso aconteça têm de ser dados os primeiros passos na estruturação e homogeneização da informação, desde logo com os cuidados de segurança que a vida humana exige.

Sumário

Os documentos em papel continuam a ser maioritariamente usados na partilha de informação autenticada. Ainda que exista crescente aceitação dos documentos electrónicos pelos profissionais de saúde e utentes, leis específicas promovendo a utilização de assinatura digital e múltiplos grupos de trabalho ou normas publicadas definindo o formato dos documentos clínicos electrónicos, o seu uso é, em nosso entender, ainda limitado. O objectivo geral deste trabalho foi apresentar uma proposta de especificação de documento clínico electrónico no âmbito da imagem médica, mantendo como objectivos específicos; (i) identificar na literatura as normas existentes, analisar a sua disseminação mundial e o volume de experiência no seu uso, avaliar a facilidade da sua implementação em *software* e potencial para integração futura em registos electrónicos de saúde, (ii) identificar mecanismos de segurança de assinatura digital e de protecção da privacidade, (iii) definir um modelo de documento clínico electrónico e (iv) os elementos a incluir que garantam a sua autenticidade e a integridade da informação, assim como mecanismo de cifra para controlo de privacidade e, finalmente, (v) testar a exequibilidade de implementação em *software* e verificar a aplicabilidade do modelo a casos práticos.

A norma *Clinical Document Architecture* (CDA) foi, na nossa revisão, a mais citada, implementada e utilizada, seguida pela *Digital Imaging and Communications in Medicine Structured Reporting* (DICOM-SR). O formato CDA apresenta a característica única de legibilidade humana e parece mais fácil de implementar, permitindo diferentes níveis de complexidade. A norma DICOM tem origem na área da imagem médica e está bastante avançada em matéria de transferência automática de informação e de autenticação digital.

Os fundamentos criptográficos da assinatura digital foram revistos, assim como os conceitos de infra-estrutura de chave pública e validação temporal. O uso de *smartcard*, como forma de manter a privacidade da chave de assinatura, foi considerado, podendo o cartão de cidadão, englobado na infra-estrutura de chave pública do estado português, ser útil para o efeito. Discutem-se as vantagens da utilização de um cartão profissional dedicado. O esquema *XML Advanced Electronic Signatures* (XAdES) cumpre as directivas europeias sobre assinatura electrónica e é a base para o perfil de assinatura adoptado pela iniciativa *Integrating the Healthcare Enterprise*, especialmente avançada em integração de

sistemas de informação na saúde. O método *XML encryption syntax and processing* será adequado para protecção da privacidade nos documentos.

Foi construído um modelo de documento com base nas normas CDA e XAdES, incluindo uma estrutura de documento cifrado, e desenvolvida uma implementação experimental do modelo, com utilização da assinatura e validação temporal do cartão de cidadão. A avaliação do modelo foi feita por estudo descritivo em laboratório para validação da estrutura do modelo de dados e avaliação funcional básica, com conversão de uma amostra de 36 relatórios de imagem para a estrutura de documento proposta.

Verificou-se a funcionalidade esperada do protótipo, manifestando-se fácil a implementação do uso do cartão de cidadão. A aposição da assinatura do autor e da contra-assinatura da entidade responsável pela guarda do documento demorou em média 456 milissegundos e a dimensão média do ficheiro gerado, incluindo carimbo de tempo, foi em média de 12.7 KB (os ficheiros originais tinham em média 31.4 KB).

A assinatura XAdES admite uma evolução para a forma de arquivo XAdES-A, que permite manter a validade da assinatura caso a dimensão das chaves ou os algoritmos criptográficos utilizados venham a demonstrar-se fracos. A criação de uma cadeia de documentos com inclusão do valor de assinatura no próximo documento arquivado em sequência previne o desaparecimento impune de documentos do arquivo. Será necessário testar o uso por profissionais no terreno, mas a dificuldade de implementação em *software*, o tempo de computação das assinaturas ou a dimensão dos ficheiros gerados não deverão ser limitações. Decorre internacionalmente trabalho para inclusão de assinatura digital como forma de autenticação de documentos clínicos.

A adopção de um modelo de características similares ao proposto apresenta-se como uma solução para que o arquivo, na forma electrónica, de relatórios de imagem médica continue a garantir a segurança de informação e permita interoperabilidade entre as várias entidades que prestam cuidados de saúde.

PALAVRAS-CHAVE: Documento clínico, relatório electrónico, assinatura digital, cifra, infra-estrutura de chave pública, validação temporal

Abstract

Printed documents are still, most of the times, used in our current practice for authenticated information exchange. Even with growing acceptance of electronic documents by care providers and users, specific laws promoting digital signatures and multiple workgroups or published standards defining the format for clinical documents, their use is still, in our sense, negligible. The general aim of this work was to propose a specification of clinical electronic document for medical imaging, with the following specific objectives; (i) to identify in literature available standards, to analyze their spread around the world and the bulk of experience on its use, to evaluate the easiness of software implementation and future integration on health records, (ii) to identify security mechanisms for digital signing and privacy protection, (iii) to define a model of clinical electronic document and (iv) the elements to include to assure authenticity and integrity of information and also a cipher for privacy control and, finally, (v) to test the implementation on software and the use of the model over real cases.

The standard Clinical Document Architecture (CDA) was, on our review, the most referred, implemented and used followed by Digital Imaging and Communications in Medicine Structured Reporting (DICOM-SR). The CDA format presents a unique feature of human legibility and seems easier to implement, allowing different levels of complexity. DICOM derives from medical imaging and is well advanced on items of automated information transfer and digital authentication.

The cryptographic basis for current digital signature was reviewed, and also the concept of public-key infrastructure. The use of a smartcard as a way to preserve the privacy of the signature key was considered, and the Portuguese citizen card, included in the governmental public-key infrastructure, revealed itself useful. The advantages of a dedicated professional card were discussed. The scheme XML Advanced Electronic Signatures (XAdES) follows the European directives for an electronic signature and is the basis for the signature profile adopted by the Integrating the Healthcare Enterprise initiative, especially advanced on health information systems integration. The XML encryption syntax and processing is a suitable method for document privacy protection.

A document model was built following CDA and XAdES standards, including a ciphered document structure, and an experimental implementation was developed, using the citizen card's signature and time-stamping. The model evaluation was done with a descriptive laboratorial study for validation of the model data structure and basic functional evaluation, with conversion of a sample of 36 medical imaging reports to the proposed document structure.

The expected functionality of the prototype was verified, looking easy to implement the use of the citizen card. The signature by the author and the custodian take an average of 456 milliseconds and the average dimension of the created files, with timestamp, was 12.7 KB (the original files supporting the documents had an average of 31.4 KB).

The XAdES signature allows an evolution for an archive form XAdES-A, to keep the signature valid even if key size or cryptographic algorithms becomes weak. The creation of a chain with the signature value archived in the next document on sequence is an obstacle to document erasing by convenience. It will be necessary to test the professional use on the ground but difficult implementation, long computation time for signing or file size should not be obstacles. Over the world there is work in progress aiming the inclusion of a digital signature as a way to authenticate clinical documents.

The adoption of a model like the one proposed in this work can be a solution to keep the information on medical imaging reports secure and allow interoperability between different health care providers.

KEYWORDS: Clinical document, electronic report, digital signature, cipher, public-key infrastructure, time-stamping

Índice geral

Agradecimentos	iii
Preâmbulo	iv
Sumário.....	v
<i>Abstract</i>	vii
Índice geral	ix
Índice de figuras	xi
Índice de tabelas	xii
Organização da tese	xiii
Acrónimos e abreviaturas	xiv
Resultados científicos e financiamentos	xvii
1. Introdução	1
1.1. Definição do problema	1
1.2. Contexto e relevância	1
2. Objectivos	4
3. Estado da arte.....	5
3.1. Normas	5
3.1.1. CDA.....	7
3.1.2. DICOM.....	9
3.1.3. CEN 13606	10
3.1.4. GEHR	10
3.2. Segurança.....	11
3.2.1. Assinatura	11
3.2.1.1. Fundamentos.....	11
3.2.1.2. Certificados digitais e infra-estrutura de chave pública	12
3.2.1.3. <i>Smartcards</i>	14
3.2.1.4. Carimbo de tempo	17
3.2.1.5. Assinatura electrónica avançada e XAdES	19
3.2.1.6. Utilização na saúde.....	23
3.2.2. Privacidade	24

4. Material e métodos	26
4.1. Estrutura do documento.....	26
4.2. Documento clínico.....	26
4.2.1. Cabeçalho	27
4.2.2. Corpo do documento	37
4.3. Assinatura digital.....	40
4.4. Validação cronológica	44
4.5. Cifra.....	45
4.6. Implementação.....	47
4.7. Testes	48
4.7.1. Desenho do estudo.....	48
4.7.2. Amostra	48
4.7.3. Equipamento.....	49
4.7.4. Procedimento experimental	49
5. Resultados.....	51
5.1. Funcionalidade do protótipo.....	51
5.2. Plenitude de conversão de documentos	51
5.3. Tempo de computação.....	52
5.4. Dimensão dos ficheiros	53
6. Discussão	54
6.1. Da metodologia	54
6.2. Dos resultados	56
6.3. Das limitações do estudo	57
6.4. Da comparação com outros estudos	57
6.5. Da validação dos documentos	58
6.5.1. Verificação de assinaturas	58
6.5.2. Outras verificações	60
6.6. Das aplicações	61
7. Conclusões e recomendações	64
8. Trabalho futuro	65
Referências	66
Anexos.....	71

Índice de figuras

Figura 1. Exemplo simplificado de um documento CDA R2, Nível Um, visualizado em texto simples	8
Figura 2. Visualização de exemplo simplificado de um documento CDA R2, Nível Um, por aplicação de <i>XML Stylesheet</i>	9
Figura 3. Representação esquemática das entidades numa PKI e suas inter-relações	14
Figura 4. Cadeia de certificação da assinatura qualificada do cartão de cidadão.....	16
Figura 5. Processo de validação cronológica (<i>timestamping</i>)	19
Figura 6. Organização de serviços criptográficos e sua relação com <i>middleware</i> do cartão de cidadão	48
Figura 7. Correlação entre o tempo de computação e a dimensão do ficheiro gerado, após assinatura e contra-assinatura.....	52
Figura 8. Sequência de procedimentos em departamento de maior dimensão, com internos	62
Figura 9. Sequência em caso de relato de exames por telerradiologia	63

Índice de tabelas

Tabela 1. Número de artigos seleccionados que referenciam, implementam ou utilizam cada formato de documento clínico electrónico.....	6
Tabela 2. Formatos de assinatura electrónica avançada XML (XAdES).....	22
Tabela 3. Dimensão (em kilobytes) dos ficheiros originais e dos ficheiros gerados no modelo	53

Organização da tese

Esta dissertação encontra-se organizada da seguinte forma:

Introdução – definição da questão base da dissertação e contextualização no panorama nacional e internacional, com discussão da relevância e actualidade do problema;

Objectivos – apresentação de objectivos, geral e específicos, que se pretendem atingir neste trabalho;

Estado da arte – informação prévia disponível sobre normas internacionais relativas a documento clínico electrónico e mecanismos de assinatura digital e cifra de documentos;

Material e métodos – descrição do modelo de documento electrónico proposto (incluindo o documento clínico e mecanismos de segurança) e da metodologia de implementação e teste do modelo proposto;

Resultados – apresentação dos resultados dos testes efectuados à exequibilidade de utilização do modelo;

Discussão – apreciação dos resultados, discussão de limitações da metodologia utilizada e confronto com outros trabalhos publicados;

Conclusões e recomendações – ilações a retirar do estudo desenvolvido;

Trabalho futuro – novas questões levantadas ou pendentes e janelas abertas pela utilização e aprofundamento de um documento clínico electrónico.

Acrónimos e abreviaturas

3DES	Triple Data Encryption Standard (TDES)
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CA	Certification Authority
CDA	Clinical Document Architecture
CEN	Comité Européen de Normalisation
CN	Common Name
CRL	Certificate Revocation List
CWA	CEN Workshop Agreement
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DICOM	Digital Imaging and Communications in Medicine
DICOM-SR	DICOM Structured Reporting
DSG	Document Digital Signature
EEPROM	Electrically-Erasable Programmable Read-Only Memory
EMV-CAP	Europay, MasterCard and VISA Chip Authentication Program
ETSI	European Telecommunications Standards Institute
GB	GigaByte
GEHR	Good Electronic Health Record
GHz	GigaHertz
HIMSS	Healthcare Information and Management Systems Society

HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HL7	Health Level Seven
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IHE	Integrating the Healthcare Enterprise
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KB	KiloByte
LOINC	Logical Observation Identifiers Names and Codes
MAC	Message Authentication Code
MD5	Message-Digest algorithm 5
OAEP	Optimal Asymmetric Encryption Padding
OCSP	Online Certificate Status Protocol
OID	OSI Object Identifier
OpenEHR	Open Electronic Health Record
OSI	Open Systems Interconnection
PACS	Picture Archiving and Communication System
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	X.509-based Public Key Infrastructure
PUK	PIN Unlock Code
RAM	Random Access Memory
RFC	Request For Comments
RIS	Radiology Information System

RSA	Rivest, Shamir e Adleman
RSNA	Radiological Society of North America
SCEE	Sistema de Certificação Electrónica do Estado
SHA	Secure Hash Algorithm
SPI	System Program Interface
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard (3DES)
TSA	TimeStamping Authority
URI	Uniform Resource Identifier
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WWW	World Wide Web
WYSIWYS	What You See Is What You Sign
XAdES	XML Advanced Electronic Signatures
XAdES-A	XAdES Archiving validation data
XAdES-BES	XAdES Basic Electronic Signature
XAdES-C	XAdES Complete validation data
XAdES-EPES	XAdES Explicit Policy based Electronic Signature
XAdES-T	XAdES with Time-stamp
XAdES-X	XAdES eXtended validation data
XDS	Cross-Enterprise Document Sharing
XML	EXtensible Markup Language
XMLDsig	XML Signature Syntax and Processing

Resultados científicos e financiamentos

O autor declara não ter recebido qualquer financiamento para o presente trabalho, nomeadamente da indústria de *software* ou *hardware* informático, que possa condicionar conflito de interesses.

1. Introdução

1.1. Definição do problema

Os últimos anos foram acompanhados por largos avanços em tecnologias para a saúde, modificando em muitos aspectos a prática diária da medicina. Em particular, o uso generalizado da *Internet* tornou a partilha de informação mais fácil, e também menos dispendiosa.

Na área da imagiologia médica, o advento de múltiplos sistemas possibilitaram o trabalho à distância sobre imagem digital, quer seja pela integração em sistemas de comunicação e arquivo de imagem (*Picture Archiving and Communication System* – PACS), pelo acesso através da rede a um visualizador localizado num *Web server* ou apenas pela utilização de uma cópia em suporte físico digital, sem necessidade de grande investimento em *software* ou *hardware* e sem o obsoleto transporte de grande quantidade, e peso, de película radiográfica. Os relatórios de exames de imagem podem ser ditados e gravados em formato digital e enviados electronicamente para transcrição à distância. A informação clínica poderá ser também acedida remotamente pela rede.

Ainda assim, os documentos em papel, com assinatura original a tinta, continuam a ser largamente usados na partilha de informação autenticada, como por exemplo o envio de um relatório final assinado de um meio complementar de diagnóstico.

Coloca-se a questão se é exequível a utilização de um documento clínico electrónico (relatório de imagem) que cumpra todos os propósitos do seu equivalente em papel, incluindo a sua autenticação por assinatura.

1.2. Contexto e relevância

Há uma crescente aceitação dos documentos electrónicos por profissionais de saúde¹ e utentes² dos serviços de saúde em substituição das cópias impressas em papel, desde que garantidas as necessárias medidas de segurança para proteger a sua privacidade e a integridade da informação.

Nas directivas da União Europeia (EU)³ e na lei portuguesa⁴⁻⁸ existe legislação específica promovendo o uso de assinatura digital como meio de satisfazer os requisitos legais de assinatura, da mesma forma que uma assinatura pelo próprio punho em papel, e para a sua admissibilidade em procedimentos legais. A directiva EU 1999/93/EC também aponta aos estados membros a responsabilidade de assegurar que a uma assinatura electrónica não é negada efectividade legal e admissibilidade como meio de prova em procedimentos legais apenas com base em que se apresente; (i) em forma electrónica, (ii) não baseada num certificado qualificado, (iii) não baseada num certificado qualificado emitido por fornecedor de serviço de certificação acreditado ou (iv) não criada por dispositivo seguro de criação de assinatura, abrindo espaço a procedimentos menos formais de autenticação.

Internacionalmente existem múltiplos grupos de trabalho definindo formatos de documento clínico electrónico⁹⁻¹¹, e alguns desses formatos constituem já normas estáveis e publicadas. O seu uso na prática clínica em Portugal é ainda, em nossa opinião, insignificante, e impor-se-á a sua divulgação.

No nosso país as iniciativas de desmaterialização de documentos na área da imagiologia médica têm sido focadas no âmbito de centros isolados, se bem que cada vez mais numerosos, e apoiando-se em medidas de segurança assentes no controlo de acesso à criação, modificação e leitura de informação. Tais medidas permitem uma utilização mais ou menos segura dentro de cada um dos centros mas não são apropriadas à partilha de informação entre unidades de saúde, pela ausência de mecanismos comuns de controlo de integridade e autenticidade dos dados, que se sobrepõe por vezes mesmo à inexistência de compatibilidade entre os modelos de dados utilizados. A opção fácil pela integração de sistemas ponto-a-ponto rapidamente se antevê inviável face a um exponencial aumento da complexidade com o aumento do número e diversidade de sistemas envolvidos.

Perante tais dificuldades, e tendo em conta as crescentes preocupações ecológicas e exigência de rapidez e controlo de custos condicionando enorme pressão para a desmaterialização de documentos, é de temer que tal processo possa decorrer com perdas na segurança da integridade de informação e da garantia da sua autenticidade. Rapidamente seriam de prever situações de danos humanos eventualmente irreparáveis e/ou de conflito de responsabilidade, obrigando ao repensar dos sistemas e deitando por terra investimentos, porventura avultados, já realizados.

Assim, parece de extrema importância encontrar um modelo que possa ser utilizado pelos vários intervenientes na partilha segura de informação.

A adopção de um modelo de documento clínico electrónico, sob a forma de ficheiro de dados contendo informação bastante para garantir a autenticidade e integridade dos dados, afigura-se-nos preferível quer à criação de complexas redes de troca de informação quer a mecanismos centralizados de dimensões incomensuráveis.

2. Objectivos

Este trabalho pretende atingir o objectivo geral de apresentar uma proposta de especificação de documento clínico electrónico no âmbito da imagem médica, fazendo prova de conceito pelo desenvolvimento de uma implementação funcional, e perseguindo os seguintes objectivos específicos:

- 1) Rever a literatura relativamente a normas existentes para documento clínico electrónico, analisando a sua dispersão mundial e o volume de experiência na sua utilização, e avaliar a facilidade da sua implementação em *software* e potencial para integração futura em registos electrónicos de saúde;
- 2) Identificar mecanismos de segurança para aposição de assinatura digital e de controlo da privacidade dos documentos;
- 3) Descrever pormenorizadamente um modelo (especificação) de documento clínico electrónico, em conformidade com norma escolhida e numa interpretação que reflecta as necessidades e os usos na imagiologia médica portuguesa. Pretende-se estreitar a aplicação da norma de forma a facilitar a implementação do modelo e procurando garantir que implementações distintas produzam documentos electrónicos compatíveis entre si;
- 4) Definir os elementos a incluir no documento que garantam a sua autenticidade e a integridade da informação, assim como mecanismo de cifra para controlo de privacidade;
- 5) Testar a exequibilidade de implementação em *software* e verificar a aplicabilidade do modelo a relatórios de imagem reais, avaliando a abrangência do conteúdo, as dimensões dos ficheiros gerados e o tempo de computação. O estudo experimental apresentado destina-se a cumprir este último objectivo.

3. Estado da arte

3.1. Normas

Na persecução do primeiro objectivo específico foi utilizado um conjunto de critérios de pesquisa numa biblioteca *on-line* com o objectivo de quantificar a citação de cada formato. Foram pesquisados os artigos que satisfizessem o conjunto de critérios “(“electronics”[All Fields] OR “electronic”[All Fields] OR “digital”[All Fields]) AND (“clinical document”[All Fields] OR “medical document”[All Fields]) AND hasabstract[text]” e os resultados foram obtidos na biblioteca digital *PubMed* (<http://www.ncbi.nlm.nih.gov/PubMed/>) em 8 de Fevereiro de 2009.

A pesquisa assim descrita devolveu 24 artigos¹²⁻³⁵. A avaliação dos artigos encontrados está sumariada na Tabela 1. Cada simples referência ou análise a um formato de documento ou registo de saúde foi considerado. Foi contabilizada a existência de uma implementação sempre que um artigo descreveu, ainda que teoricamente, um uso específico para um formato. Finalmente, apresenta-se o número de artigos afirmando que um formato foi efectivamente utilizado na prática clínica ou na colheita de dados para investigação.

Subsequentemente foi aprofundada a pesquisa seguindo as citações nos artigos encontrados, procedimento repetido de forma recursiva várias vezes, em busca de informação sobre as normas e formatos de documento clínico electrónico, com vista a analisar a facilidade de implementação e potencial para integração em registos electrónicos de saúde.

Tabela 1. Número de artigos seleccionados que referenciam, implementam ou utilizam cada formato de documento clínico electrónico

Norma / Formato	Referência ou análise	Implementação	Uso na prática clínica ou investigação
CEN 13606 ^a	2	-	-
HL7 ^b Clinical Document Architecture (CDA)	17	11	2
DICOM SR ^c	5	2	-
GEHR ^d	2	-	-

^a CEN 13606 - Norma do *Comité Européen de Normalisation*

^b HL7 – Organização envolvida no desenvolvimento de normas internacionais em cuidados de saúde

^c DICOM SR - Digital Imaging and Communications in Medicine Structured Reporting

^d GEHR - Good Electronic Health Record

Esta metodologia enfermou de algumas limitações. O uso do termo “clinical document” nos critérios de pesquisa, que também é parte do nome de uma das normas, pode ser fonte de desvio nos resultados obtidos. No entanto tendo em conta a grande diferença no número de artigos da norma mais citada (*Clinical Document Architecture* - CDA), tal desvio poderá possivelmente ser tolerado. A restrição da pesquisa a artigos com resumo disponível poderá ter reduzido o número de artigos devolvidos mas é pouco provável que introduza viés significativo, e permite estender a avaliação a estudos em diferentes línguas. Também a utilização na pesquisa de apenas uma biblioteca, fundamentalmente médica, poderia ser questionada, mas a *PubMed* indexa um grande conjunto de publicações, teoricamente apenas seleccionadas pela sua qualidade.

Ainda que as normas encontradas sejam fundamentalmente as referidas em artigos prévios de revisão, não foi identificada anterior revisão quantitativa do número de artigos publicados com descrição ou análise das diferentes normas.

3.1.1. CDA

A norma *Clinical Document Architecture* é reconhecida pela ANSI (*American National Standards Institute*) desde Maio de 2005 (Versão R2)³⁶. Os documentos CDA são codificados em *Extensible Markup Language* (XML) e contêm um cabeçalho e um corpo. O cabeçalho identifica e classifica o documento e fornece informação sobre autenticação, a consulta, o paciente e os profissionais de saúde envolvidos. O corpo do documento inclui o relatório clínico organizado em secções cujo conteúdo narrativo pode ser codificado utilizando vocabulário normalizado.

As seguintes características são atribuídas aos documentos CDA desde a sua primeira versão³⁷:

- Persistência – um documento clínico continua a existir inalterado, por um período de tempo definido por requisitos locais ou por legislação;
- Entidade responsável – a manutenção de um documento clínico ficará ao cuidado de uma pessoa ou organização por tal responsável;
- Potencial de autenticação – um documento clínico é um conjunto de informação passível de autenticação legal;
- Integridade – a autenticação de um documento clínico aplica-se ao seu todo e não a partes do seu conteúdo fora do contexto de conjunto do documento;
- Legibilidade humana – o documento clínico é legível.

A arquitectura completa do CDA inclui um conjunto hierárquico de especificações de documentos, distribuído em três níveis de complexidade crescente. O Nível Um intencionalmente não inclui semântica complexa destinando-se a minimizar as barreiras técnicas à adopção da norma.

A norma *Clinical Document Architecture*, versão 2, apresenta o maior número de referências, maior número de implementações descritas e é a única com uso prático explícito (na pesquisa efectuada). Permitindo diferentes níveis de complexidade, esta norma parece a de mais fácil implementação no seu nível mais básico. Uma estrutura compreensível (Figura 1) e uma legibilidade humana totalmente atingida pela simples aplicação de uma *XML Stylesheet* (Figura 2) são fortes argumentos a favor da aceitação deste formato.

```

<?xml version="1.0" encoding="windows-1252"?>
<?xml-stylesheet type="text/xsl" href="CDA.xsl"?>
<ClinicalDocument xmlns="urn:hl7-org:v3" xmlns:voc="urn:hl7-org:v3/voc" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:hl7-org:v3 CDA.xsd">
<!-- CDA Header -->
  <typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040"/>
  <id extension="AAA" />
  <code/>
  <title>Relatório de Exame de Imagem</title>
  <effectiveTime value="20090205"/>
  <confidentialityCode />
  <recordTarget>
    <patientRole>
      <id extension="12345"/>
      <patient>
        <name>
          <given>António</given>
          <family>Silva</family>
        </name>
        <administrativeGenderCode code="M" />
        <birthTime value="19701224"/>
      </patient>
    </patientRole>
  </recordTarget>
  <author>
    <time value="20090208"/>
    <assignedAuthor>
      <id extension="54321"/>
    </assignedAuthor>
  </author>
  <custodian>
    <assignedCustodian>
      <representedCustodianOrganization>
        <id />
      </representedCustodianOrganization>
    </assignedCustodian>
  </custodian>
  <legalAuthenticator>
    <time value="20090208"/>
    <signatureCode code="S"/>
    <assignedEntity>
      <id extension="54321"/>
      <assignedPerson>
        <name>
          <given>Rui</given>
          <family>Alves</family>
        </name>
      </assignedPerson>
    </assignedEntity>
  </legalAuthenticator>
<!-- CDA Body -->
  <component>
    <structuredBody>
      <component>
        <section>
          <title>Ecografia Abdominal</title>
          <text>
            Sem alterações significativas.
            <paragraph/>
            <paragraph/>
          </text>
        </section>
      </component>
    </structuredBody>
  </component>
</ClinicalDocument>

```

Figura 1. Exemplo simplificado de um documento CDA R2, Nível Um, visualizado em texto simples

Relatório de Exame de Imagem	
Patient: António Silva	MRN: 12345
Birthdate: December 24, 1970	Sex: Male
Consultant: Rui Alves	Created On: February 5, 2009
Ecografia Abdominal	
Sem alterações significativas.	
Signed by: Rui Alves on February 8, 2009	

Figura 2. Visualização de exemplo simplificado de um documento CDA R2, Nível Um, por aplicação de XML Stylesheet

3.1.2. DICOM

A especificação *Digital Imaging and Communications in Medicine Structured Reporting* (DICOM-SR) é parte integrante da norma de comunicação e imagem digital em medicina e é um modelo geral para codificação de relatórios médicos numa forma estruturada, no formato definido pela norma DICOM. Ao contrário de outras, a norma DICOM usa uma codificação binária de listas hierárquicas de dados elementares, identificados por etiquetas numéricas e um complexo protocolo de rede ao nível de aplicação¹¹. Estudos publicados reflectem as dificuldades na implementação desta complexa e sofisticada parte da norma DICOM. Ferramentas genéricas embebidas nas estações de trabalho PACS e que cobrem os diferentes tipos de relatórios clínicos usados actualmente na saúde³⁸, poderão ajudar a difundir os benefícios da partilha de conhecimento clínico por utilização de documentos SR, tais como o aumento da compreensão da informação durante as consultas, possibilidade de reutilização de achados clínicos para treino e facilidade da avaliação da performance de conjunto dos sistemas. Trabalhos em curso poderão fornecer esquemas XML que serão suficientemente flexíveis para representar todos os dados contidos em DICOM-SR, facilitando a compatibilidade com outros sistemas^{29,39}. O Nível Três da CDA incluirá um modelo totalmente compatível com DICOM-SR para permitir a troca de

informação de documentos SR com equipamentos e sistemas de informação incapazes de interpretar o formato DICOM.

A norma DICOM está bastante avançada em matéria de transferência automática de informação e também em autenticação digital; o Anexo C da Parte 15 descreve um perfil de assinatura digital potencialmente preenchendo os requisitos legais⁴⁰⁻⁴².

A especificação DICOM-SR será provavelmente de fácil implementação no campo da imagem médica. DICOM tem sido, nesta área, largamente usada com sucesso no estabelecimento de comunicação entre arquitecturas muito distintas de sistemas computacionais. A dificuldade de implementação da sua estrutura complexa poderá ser um obstáculo à sua expansão para outras áreas da medicina.

3.1.3. CEN 13606

A norma 13606 do *Comité Européen de Normalisation* (CEN 13606) apresenta uma proposta de normalização europeia, correntemente com documentação incompleta. Apenas a parte 1 (modelo de referência) tem uma versão estável; as partes 2 a 5 encontram-se em desenvolvimento¹¹. O equivalente ao documento clínico electrónico será provavelmente definido sob a denominação “EHR-Extract”.

3.1.4. GEHR

A iniciativa *Good Electronic Health Record* (GEHR), com forte participação australiana, começou em 1992 como um projecto de investigação da União Europeia, denominado *Good European Health Record*. Actualmente o projecto é mantido pela Fundação *openEHR*. Não foi possível encontrar uma definição formal de uma estrutura de ficheiro partilhável. A *framework openEHR* inclui um modelo de informação de referência, uma linguagem para expressão de arquétipos, uma biblioteca de arquétipos, especificações de tecnologia de implementação (esquemas XML) e uma colecção de implementações *open source* das especificações *openEHR*¹¹.

3.2. Segurança

3.2.1. Assinatura

Uma utilização segura de um documento clínico em forma electrónica implicará o controlo da sua autenticidade, da integridade da informação nele contida e alguma forma de impossibilitar o repúdio posterior da sua autoria.

O controlo de autenticidade é aqui entendido como a possibilidade de confirmação, pelo receptor do documento, que o documento foi produzido por quem o afirma ter feito, sem que o tenha de provar a outrem.

A capacidade de verificação da integridade da informação é uma característica fundamental de um documento clínico electrónico, permitindo assegurar que, desde a sua emissão até à leitura pelo receptor, nenhuma alteração, quer propositada quer accidental, tenha ocorrido.

Necessário será também mecanismo de não-repudição, que garanta que o autor do documento não possa negar a sua autoria, por exemplo quando confrontado com a existência de imprecisões no seu conteúdo.

3.2.1.1. Fundamentos

Um processo de criação de uma assinatura digital, que permite controlo de autenticidade e integridade e não-repudição, foi pela primeira vez descrito em 1978 por Rivest, Shamir e Adleman⁴³, baseado na implementação de um conceito de criptografia de chave pública previamente apresentado, apenas do ponto de vista teórico, por Diffie e Hellman⁴⁴ em 1976. Esse conceito baseia-se num par de procedimentos (chaves), um tornado público, adiante denominado E , e outro mantido privado pelo seu detentor, D , de tal forma que (i) ambos podem ser executados em computador, (ii) o conhecimento do procedimento E não permite conhecer uma forma fácil de calcular D em tempo útil e (iii) a aplicação de E a uma cifra, pelo procedimento D , de uma mensagem (M), resulta na própria mensagem:

$$E(D(M)) = M$$

O sistema criptográfico então descrito, actualmente conhecido por RSA, segundo os apelidos dos autores, baseia-se na utilização de dois números primos secretos muito grandes (actualmente da ordem de um *kilobyte*), tomando vantagem da grande dificuldade

na computação da factorização em números primos. A mensagem é cifrada representando-a por um número M , elevando M a um expoente publicitado e , e calculando o resto da divisão do resultado por um número n que é o produto dos dois números primos referidos, denominados p e q . Para decifrar utiliza-se um processo sobreponível mas com outro expoente, d , mantido secreto, calculado tal que o resto da divisão inteira de $e.d$ por $(p-1).(q-1)$ seja igual a 1.

A assinatura digital, que é um número a ser enviado junto com a mensagem, seria calculada aplicando D à mensagem. O receptor aplica o procedimento E , que é público e reconhecido como pertencendo ao autor e se, ao fazê-lo, obtém a mensagem, considera válida a assinatura.

A assinatura digital assim criada é dependente tanto da mensagem como de quem a assina (depende do seu par de chaves pública / privada). Ao ser dependente da mensagem qualquer alteração da mesma impede a validação da assinatura e permite o controlo de integridade. Dependendo do par de chaves utilizado permite a autenticação da mensagem e impede o repúdio da assinatura pois só o detentor da chave privada D pode calcular uma assinatura válida para a chave pública E .

Na prática actual, e por razões de eficiência computacional e segurança, o que se assina não é toda a mensagem⁴⁵ mas um valor denominado *hash* (em rigor *hash* é a denominação da função que produz esse valor), de dimensão mais pequena. O valor de *hash* é calculado por uma função tal que; (i) para cada mensagem só há um valor de *hash*, (ii) o valor de *hash* é fácil de calcular a partir da mensagem, (iii) várias mensagens podem ter o mesmo *hash* mas (iv) não é tecnicamente possível calcular directamente as mensagens que podem originar um determinado *hash*, sendo também extremamente difícil identificá-las pelo método de tentativa e erro. Esta última característica dificulta extremamente a alteração de uma mensagem para outra a que corresponda o mesmo valor de *hash*.

3.2.1.2. Certificados digitais e infra-estrutura de chave pública

A implementação do mecanismo descrito torna necessário um meio de prova de que determinada chave pública e, portanto, a correspondente chave privada, se encontram atribuídas a determinada entidade. É usado com essa função o certificado digital, também designado certificado de chave pública ou certificado de identidade, que consiste num documento electrónico que usa uma assinatura digital para ligar uma chave pública a uma

identidade. Os certificados da família X-509⁴⁶, são um exemplo de estrutura desse documento electrónico. Outro tipo de certificados, tal como os OpenPGP⁴⁷ que se basearam na sua criação em conceitos diferentes, de confiança distribuída (*web of trust*), poderão vir a ser alternativas. A assinatura digital aposta no certificado pertencerá a uma entidade externa que tem a confiança dos vários interessados, que está imbuída de zelar pela veracidade da identidade e dos restantes atributos incluídos no certificado, incluindo a validade, políticas de atribuição, propósito e restrições ao uso da assinatura, assim como eventuais qualidades específicas da mesma, e que é denominada entidade certificadora (*certification authority* - CA). A lei portuguesa define a forma de credenciação destas entidades e os requisitos de uma assinatura digital para ter a força probatória de um documento assinado em papel⁴⁻⁸.

Na prática a certificação de cada chave pública de utilizador final pode ser obtida por uma cadeia de certificação incluindo entidades de certificação intermediárias, numa cadeia de certificação hierárquica tendo por base uma autoridade de certificação raiz. A possibilidade de extravio ou outra forma de compromisso da chave privada, e sua utilização indevida por outrem, obriga à existência de procedimentos de revogação dos certificados. Na realidade torna-se necessária toda uma infra-estrutura de chave pública (PKI), que pode ser definida como um conjunto de *hardware*, *software*, pessoas, políticas e procedimentos necessários para criar, gerir, armazenar, distribuir e revogar certificados digitais⁴⁸.

A infra-estrutura baseada em certificados X-509 é conhecida por PKIX (*X.509-based Public Key Infrastructure*). Um esquema de funcionamento simplificado é apresentado na Figura 3, baseando-se o modelo em repositórios de certificados e listas de revogação de certificados (CRL), que podem ser acedidos, com base em protocolos de gestão de certificados⁴⁹, durante o processo de validação de assinaturas.

Em alternativa, a interrogação de servidores OCSP (*Online Certificate Status Protocol*)⁵⁰, que mantêm actualizada uma lista de revogações de certificados e devolvem uma resposta assinada sobre a validade de determinado certificado, protocolo implementado já de base nos sistemas operativos *Windows Vista SP1* e *Windows 7*⁵¹, pode permitir uma mais fácil verificação da validade de assinaturas pelo utilizador final.

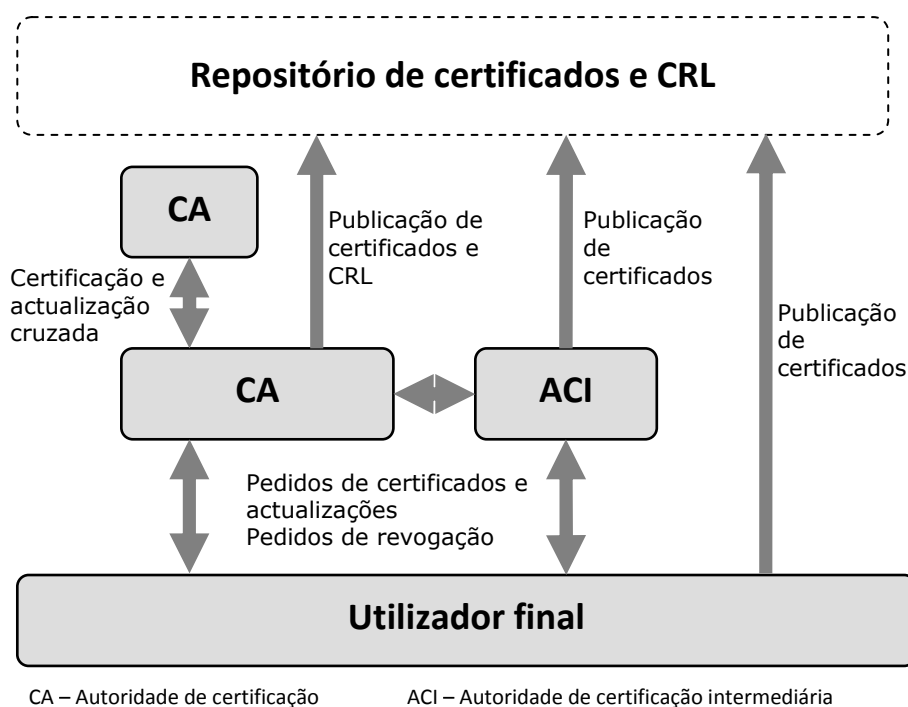


Figura 3. Representação esquemática das entidades numa PKI e suas inter-relações

3.2.1.3. Smartcards

A necessidade de manter a chave privada segura, apenas acessível ao proprietário e da qual exista apenas um exemplar, coloca uma nova questão de segurança.

Uma solução é a utilização de *smartcards*, “cartões inteligentes” que na sua forma mais corrente, definida pela norma ISO/IEC 7816, são microprocessadores de reduzidas dimensões num suporte de plástico semelhante a um cartão de crédito (85.60×53.98 mm, formato de cartão ID-1 ISO/IEC 7810⁵²), que comunicam com outros equipamentos por meio de contactos eléctricos. Existem outras especificações possibilitando a comunicação sem fios a curta distância, por radiofrequência, que têm utilização por exemplo no controlo de acesso físico ou em sistemas de transportes. O microprocessador inclui capacidade de memória da ordem das dezenas ou centenas de *kilobytes*, em grande parte sob a forma de memória não volátil, que persiste mesmo na ausência de aporte de energia eléctrica. O recurso a tecnologia *Java Card* permite a execução segura de aplicações *Java* no *chip* do cartão e a sua integração com outros sistemas, facilitando a sua utilização para operações de criptografia.

No contexto das aplicações criptográficas de assinatura digital, a chave privada é armazenada no cartão e nunca é fornecida, impedindo assim que dela seja feita cópia. No

processo de assinatura é transferida para o cartão a informação a assinar (sob a forma de sequência de *bytes*) geralmente correspondendo ao resultado da aplicação de uma função de *hash* sobre o conteúdo a autenticar. Apenas é devolvido o valor da assinatura, mantendo-se assim o segredo da chave privada.

Em Portugal, o cartão de cidadão, que substitui o bilhete de identidade nacional, é um *smartcard* que contém dois pares de chaves assimétricas que podem ser usados em assinaturas digitais; um para autenticação em sistemas de informação e o outro para produção de assinaturas legalmente vinculativas (com objectivo de não-repúdio)⁵³. Trata-se de um cartão com suporte em policarbonato com as dimensões ID-1 descritas acima. O microprocessador é um *Java Card* com um mínimo de 64KB de memória de tipo EEPROM (*Electrically-Erasable Programmable Read-Only Memory*)⁵⁴ com um motor criptográfico interno e aptidão para:

- Assinatura e verificação RSA de 1024 bits;
- Assinatura electrónica qualificada segundo a norma CEN CWA 14169 (*Secure Signature-creation devices “EAL 4+”*)⁵⁵;
- Cifras DES e TDES (*Triple Data Encryption Standard*);
- Funções de *hash* MD5, SHA-1 e SHA-256;
- Implementação de MAC (*Message Authentication Code*), PKCS#1 (*RSA Cryptography Standard*) e PKCS#15 (*Cryptographic Token Information Format Standard*);
- Compatibilidade com leitores de cartões da norma EMV-CAP, para funcionamento de autenticação multicanal baseada em *one-time password*;
- Chave de protecção da personalização inicial;
- Resistência aos ataques conhecidos do tipo *hardware attack*; *timing attack* (baseado na análise do tempo de execução dos algoritmos criptográficos), *simple power analysis* e *differential power analysis* (dirigidos ao consumo de corrente eléctrica do equipamento);
- Funcionalidade de *true random number generation*;
- Suporte a múltiplos PIN em conformidade com a norma ISO/IEC 7816-4;

- Mecanismo de bloqueio em caso de erro reiterado na introdução do PIN, com desbloqueio por PUK do cidadão e chave administrativa;
- Geração de novo PIN em caso de perda do anterior;
- Gestão de espaço de armazenamento, incluindo desfragmentação e reutilização de espaço libertado.

A assinatura electrónica do cartão de cidadão funciona com base na infra-estrutura de chave pública criada em 2006 pelo Decreto-Lei nº116-A e denominada SCEE – Sistema de Certificação Electrónica do Estado⁵⁶, que no topo da cadeia hierárquica de certificação tem a Entidade de Certificação Electrónica do Estado (CN – ECRaizEstado). O certificado raiz nacional é emitido pela *GTE CyberTrust Global Root*, entidade certificadora de raiz internacional com atribuição de confiança por defeito em sistemas operativos como o *Microsoft Windows*. Na Figura 4 está representada a cadeia de certificação da chave de assinatura digital qualificada incluída no cartão de cidadão.

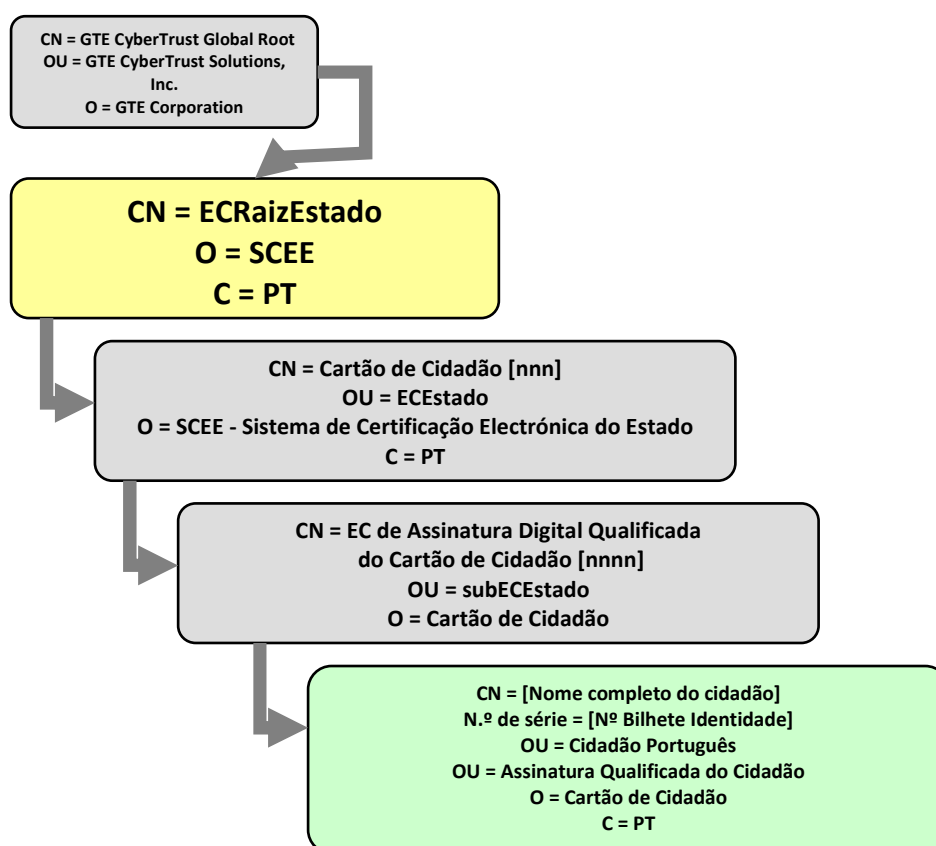


Figura 4. Cadeia de certificação da assinatura qualificada do cartão de cidadão

Cabe, de acordo com a legislação, à Entidade de Certificação Electrónica do Estado disponibilizar os seguintes serviços de certificação digital:

- Processo de registo das entidades certificadoras;
- Geração de certificados, incluindo certificados qualificados, e gestão do seu ciclo de vida;
- Disseminação dos certificados, das políticas e das práticas de certificação;
- Gestão de revogações de certificados;
- Disponibilização do estado e da situação das revogações referidas na alínea anterior.

A informação de estado de revogação relativa a um determinado certificado do cartão de cidadão pode ser acedida pelo utilizador final mediante protocolo OCSP, por HTTP, método *POST*, nos endereços <http://ocsp.asc.cartaodecidadao.pt/publico/ocsp> e <http://ocsp.root.cartaodecidadao.pt/publico/ocsp> respectivamente referentes à entidade de certificação de assinatura qualificada do cartão de cidadão e à entidade de certificação do cartão de cidadão.

O cartão de cidadão é de distribuição ubíqua aos cidadãos nacionais e está alicerçado numa infra-estrutura de chave pública do estado, funcional, tendo a sua utilização futura em sistemas de informação na saúde já sido sugerida, ainda que admitindo-se dificuldades perante a expectativa de utilização profissional de um elemento de identificação individual, e tendo em conta que profissionais de outras nacionalidades não teriam acesso ao cartão de cidadão⁵⁷. Outra hipótese seria a criação de uma PKI dedicada pela ordem profissional responsável pela credenciação dos médicos, à semelhança do que sucede já em Portugal com a ordem dos advogados, e que teria a vantagem de certificar também a qualificação para a função de médico assim como eventualmente a especialidade.

3.2.1.4. Carimbo de tempo

A aposição de um “selo” digital que prove que um documento já existia na data indicada na assinatura manifesta-se de extrema importância para subsequente não-repúdio de uma assinatura digital. Isto advém da possibilidade de revogação ou caducidade dos certificados digitais, que permitiria a falsa alegação de que a assinatura presente num documento teria sido criada após compromisso e revogação da chave, e a data de assinatura forjada (após a

assinatura de um documento desfavorável, um signatário malicioso poderia comunicar a perda ou roubo da sua chave, e repudiar nesta base um documento verídico).

A validação temporal digital baseia-se na obtenção de uma declaração de existência do documento assinada por uma terceira parte de confiança que é arquivada com a assinatura. Na realidade, pode ser atestada a existência de um *hash* extraído do documento, não sendo o documento completo enviado à autoridade de certificação temporal (TSA – *timestamping authority*) e mantendo-se assim a sua confidencialidade.

A especificação RFC 3161 define o formato do carimbo de tempo e o protocolo de comunicação com a TSA⁵⁸. O utilizador / cliente envia um pedido contendo o número de versão do pedido e um *messageImprint* contendo um *hash* do documento (ou da porção a certificar) e indicador da função de *hash* utilizada, além de outros dados opcionais. A TSA devolve uma resposta incluindo um indicador de estado do pedido (concedido, recusado, a aguardar resposta) e, se concedido, uma sequência de *bytes* em codificação DER (*Distinguished Encoding Rules*)⁵⁹ que constitui o carimbo (*timeStampToken*) a arquivar. Esta sequência é uma mensagem criptográfica assinada pela TSA e cuja informação assinada, e relevante para o carimbo, inclui um número de versão da resposta, um indicador da política de resposta, o *messageImprint* do pedido, um número de série único da resposta e data e hora de criação da resposta. O processo está representado esquematicamente na Figura 5.

São obrigações da TSA, entre outras:

- Usar uma fonte de tempo de confiança;
- Incluir um número de série inteiro único para cada novo carimbo de tempo;
- Incluir no carimbo de tempo um identificador que indique inequivocamente a política de segurança sob a qual o carimbo foi criado;
- Somente carimbar um *hash* dos dados;
- Não incluir qualquer informação da identidade do cliente no carimbo de tempo (porque essa informação não é validada pela TSA);
- Assinar cada carimbo com uma chave criada especificamente com este fim e explicitar esta propriedade no certificado correspondente.

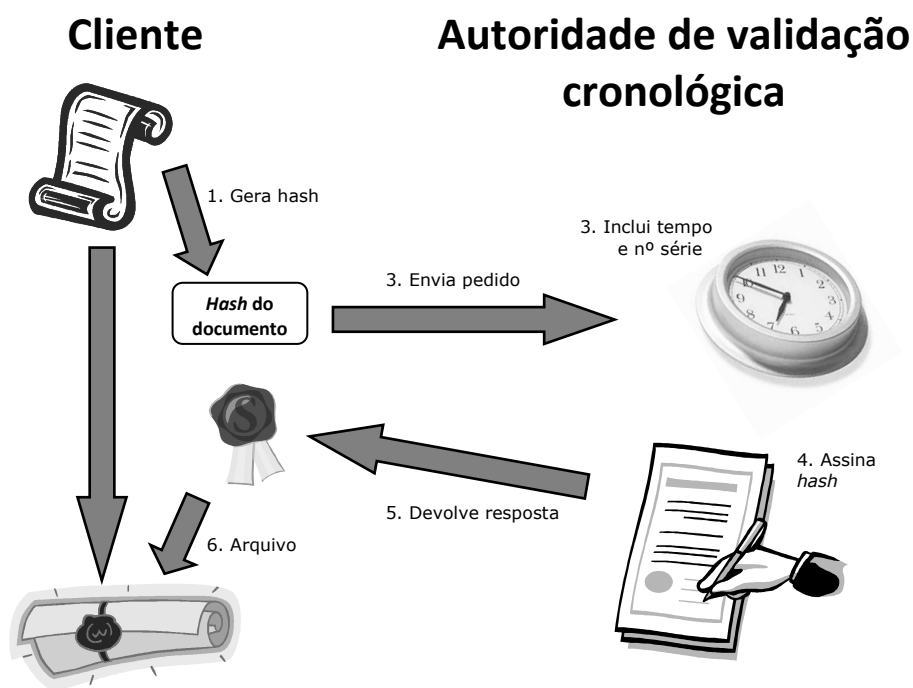


Figura 5. Processo de validação cronológica (timestamping)

A transmissão dos pedidos e respostas pode ser feita por *E-mail*, por envio de ficheiro ou pelos protocolos TCP ou HTTP.

O cartão de cidadão disponibiliza serviço de validação cronológica no endereço <http://ts.cartaodecidadao.pt/tsa/server>, por protocolo HTTP.

3.2.1.5. Assinatura electrónica avançada e XAdES

A base das assinaturas XML, especificada pela norma *XML Signature Syntax and Processing* (XMLDsig)⁶⁰, é na realidade a aplicação de um algoritmo de assinatura sobre um *hash* da forma normalizada (canónica) de um elemento da assinatura, *SignedInfo*, que por sua vez contém referência(s) a uma ou mais porções de documento a assinar, incluindo em cada referência um *hash* da forma canónica da respectiva porção do documento. A assinatura é assim aposta sobre o resultado de uma dupla aplicação de função de *hash* aos elementos a assinar.

A assinatura pode estar destacada (*detached*) do documento, estar envolvida (*enveloped*) ou envolver (*enveloping*) o documento a assinar, conforme respectivamente esteja fora dos elementos a assinar (ainda que no mesmo documento), seja um sub-elemento do objecto da assinatura ou o objecto da assinatura seja um sub-elemento da assinatura.

Na legislação portuguesa, que transcreve a directiva 1999/93/EC³ do parlamento europeu, surge definida a assinatura electrónica avançada como aquela que:

- 1) Identifica de forma unívoca o titular como autor do documento;
- 2) A sua aposição ao documento depende apenas da vontade do titular;
- 3) É criada com meios que o titular pode manter sob seu controlo exclusivo;
- 4) A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste.

O primeiro ponto obriga a que o autor do documento (ou melhor, o seu signatário), esteja identificado. Na norma XMLDsig a informação sobre a chave utilizada não está obrigatoriamente assinada, e portanto será em teoria possível que com a mesma chave, que validaria a assinatura, surjam certificados diferentes, com características diferentes, validade diferente ou mesmo titulares diferentes, colocando em causa a autoria do documento. A forma base da assinatura XML também não obriga a colocação de data na assinatura. Permite no entanto cumprir o ponto quatro acima, manutenção da integridade dos dados, desde que a referência criada para assinatura seja dirigida a todo o conteúdo do documento. Os pontos dois e três levantam algumas questões interessantes, relacionadas com a garantia de que o autor apõe assinatura por sua vontade:

- A assinatura deve ter origem num dispositivo seguro de criação de assinatura (de que são exemplo os *smartcards* atrás descritos) impedindo que a chave privada seja difundida;
- Os meios de criação de assinatura, como o cartão *smartcard*, devem ficar sob controlo exclusivo do titular, impedindo que possam ser utilizados indevidamente por outrem;
- Deve ser apresentado ao titular signatário tudo aquilo que vai assinar, no contexto correcto, garantindo o princípio geralmente conhecido como WYSIWYS (*What You See Is What You Sign*)⁶¹;
- A distância semântica entre a sequência de *bytes* assinada e a sua representação para leitura humana não deve permitir que seja assinado conteúdo díspar da pretensão do signatário (será neste contexto que a característica referida como legibilidade humana dos documentos CDA surge como franca vantagem);

- A presença de vírus do tipo “cavalo de Tróia” num computador pode fazer perigar esta garantia⁶², descrevendo-se como possíveis cenários o roubo de um PIN utilizado para uma assinatura para mais tarde usar na assinatura de outro documento ou mesmo a apresentação no monitor de determinado documento quando é enviado para assinatura no *smartcard* um conteúdo completamente distinto; assim não só os dispositivos de criação de assinatura como as interfaces com o signatário, por exemplo o computador utilizado, devem estar sob o seu controlo e serem fiáveis.

No sentido introduzido pela directiva comunitária, uma assinatura electrónica avançada deve manter-se válida ao longo do tempo, potencialmente mesmo após expirarem os certificados que lhe estão ligados, e permitir não só autenticação e controlo de integridade como não-repúdio. Surgiram assim um conjunto de normas de assinatura electrónica, do qual a norma *XML Advanced Electronic Signatures (XAdES)*⁶³ é a vertente em representação XML, que além da mensagem a assinar também promovem a assinatura (e integridade) de um conjunto de propriedades incluindo a data de criação de assinatura, o certificado utilizado, o local de assinatura, qualidade do signatário e uma política de criação e validação de assinatura, e prevêem a integração de carimbo de tempo, conteúdo relacionado com a validação da cadeia de certificados ou re-assinatura caso se preveja quebra de segurança dos algoritmos ou chaves utilizados (a vertente com sintaxe para mensagem criptográfica é denominada *CMS Advanced Electronic Signatures - CAdES*⁶⁴, correspondendo ao RFC 5126 e tecnicamente equivalente à especificação *ETSI Technical Specification TS 101 733 V.1.7.4*).

A norma XAdES prevê vários formatos ou perfis de assinatura, com diferentes níveis de protecção, sistematizados na Tabela 2, por ordem de crescente complexidade e protecção.

O formato mais básico de assinatura, XAdES-BES, satisfaz os requisitos da directiva europeia para assinatura electrónica avançada, incorporando pelo menos referências ao certificado usado na assinatura e a data e hora da assinatura. As referências ao certificado consistem no número de série, nome completo do emissor e um *hash* do certificado.

O perfil com política explícita de assinatura, XAdES-EPES, acrescenta ao formato básico uma identificação da política seguida na criação da assinatura e que deve ser usada na validação da mesma.

Tabela 2. Formatos de assinatura electrónica avançada XML (XAdES)

Formato	Abreviatura	Características
Basic electronic signature	XAdES-BES	Formato básico satisfazendo os requisitos legais de assinatura avançada
Explicit policy electronic signatures	XAdES-EPES	Incorpora a identificação da política de criação e validação de assinatura
Electronic signature with time	XAdES-T	Adiciona carimbo de tempo para protecção contra repúdio
Electronic signature with complete validation data references	XAdES-C	Inclui referências a dados de verificação (certificados, CRL ou respostas OCSP)
Extended signatures with time forms	XAdES-X	Adiciona carimbo de tempo sobre as referências introduzidas em XAdES-C
Extended long electronic signatures with time	XAdES-X-L	Incorpora os próprios certificados, listas de revogação ou respostas OCSP
Archival electronic signatures	XAdES-A	Permite a incorporação periódica de carimbos de tempo sobre o documento arquivado

A assinatura electrónica com carimbo de tempo, XAdES-T, inclui um carimbo de tempo, que na forma mais simples consiste na inclusão, como propriedade não assinada da assinatura, da mensagem de resposta assinada de uma TSA a um pedido de carimbo de tempo (sobre o valor da assinatura, elemento *SignatureValue*), descrito anteriormente (capítulo 3.2.1.4).

A assinatura com referências completas aos dados de validação, XAdES-C, adiciona aos documentos assinados referências aos dados de validação (certificados, listas de revogação ou mensagens de resposta OCSP) para permitir a validação *off-line* ou no futuro, mas sem guardar o conteúdo dos dados de validação.

Nos formatos extensos de assinatura com tempo, XAdES-X, são incluídos carimbos de tempo sobre as referências adicionadas em XAdES-C, para protecção contra possível compromisso futuro da cadeia de certificados. Existem dois tipos conforme sejam ou não incluídos carimbos de tempo sobre o valor de assinatura e eventuais carimbos de tempo de assinatura anteriormente obtidos.

A forma de longo termo de assinatura, XAdES-X-L, adiciona aos anteriores o teor dos certificados, listas de revogação ou respostas OCSP, para permitir a validação da assinatura no futuro, mesmo se a fonte original daqueles já não se encontrar disponível.

O formato de assinatura electrónica de arquivo, XAdES-A, acrescenta a possibilidade de incorporação periódica ou pontual de carimbos de tempo caso se verifique que os algoritmos criptográficos previamente utilizados podem tornar-se fracos ou se as chaves demonstrarem dimensão insuficiente face aos avanços tecnológicos. Os novos carimbos de tempo são criados sobre *hash* englobando as porções assinadas do documento e elementos relevantes da assinatura.

3.2.1.6. Utilização na saúde

Um particular impulso para as medidas de segurança de informação na saúde terá sido dado pela lei do congresso norte-americano de 1996 denominada *Health Insurance Portability and Accountability Act* (HIPAA) que teve como objectivos proteger a cobertura de seguros de saúde para trabalhadores e suas famílias e promover o desenvolvimento de um sistema de informação da saúde pelo desenvolvimento de normas e requisitos para a transmissão electrónica segura de certa informação de saúde. A sua regra de privacidade (i) dá aos pacientes maior controlo sobre a sua informação de saúde, (ii) limita o uso e difusão de registos de saúde, (iii) define salvaguardas que os fornecedores de cuidados de saúde devem estabelecer para proteger a informação de saúde e (iv) responsabiliza civil e criminalmente os violadores dos direitos de privacidade dos pacientes. A regra de segurança define as salvaguardas administrativas, físicas e técnicas destinadas a proteger a integridade, confidencialidade e disponibilidade dos dados. As tecnologias de *firewall* e rede privada virtual (VPN – *Virtual Private Network*) terão sido maioritariamente empregues, mas infra-estruturas de chave pública e *smartcards* poderão servir os mesmos objectivos, com vantagens acrescidas no controlo de acesso físico e lógico e em mecanismos de auditoria. Um *smartcard* do paciente pode ainda incluir informação médica, sobretudo a relevante em situação de emergência, informação pessoal ou dados do seguro, e possibilitar a autorização de decisões por assinatura electrónica⁶⁵.

A utilização de assinatura digital para autenticação de ficheiros ou comunicações na saúde tem sido estudada desde há vários anos, quer do ponto de vista teórico quer das suas aplicações práticas^{66,67}.

O exemplo talvez mais interessante no contexto deste trabalho será o da especificação desenvolvida pela iniciativa *Integrating the Healthcare Enterprise* (IHE) principalmente suportada na América do Norte pela *Healthcare Information and Management Systems Society* (HIMSS) e pela *Radiological Society of North America* (RSNA). No âmbito do seu

apoio ao uso das normas de integração de informação na saúde é apresentado um perfil de assinatura digital⁶⁸ identificado como *Document Digital Signature* (DSG) para aplicação no contexto de um perfil de documento específico (XDS - *Cross-Enterprise Document Sharing*) mas extensível a outras especificações de documento clínico. O perfil de assinatura definido é baseado e está em conformidade com o esquema *XML Advanced Electronic Signatures* (XAdES) para assinatura electrónica⁶³, que respeita os requisitos da directiva europeia EU 1999/93/EC³ para a criação de assinatura electrónica avançada.

Além da definição do perfil de assinatura digital, o armazenamento de documentos em forma digital, segundo o conceito supra citado, coloca outras questões pertinentes. Surge a necessidade de criação de uma infra-estrutura de chave pública (PKI)⁶⁹⁻⁷¹ capaz de fornecer os instrumentos necessários não só à assinatura de documentos pelos profissionais como à sua verificação pelos eventuais interessados, não só outros profissionais de saúde, serviços e instituições externas, como os próprios utentes. A aposição de uma assinatura necessita de uma forma segura de armazenamento da informação de chave privada, por exemplo do tipo *smartcard*, incorporado num cartão de identificação profissional ou num cartão de cidadão. É ainda necessário garantir que no acto de assinatura a mensagem assinada é realmente a que se pretende assinar, já que são conhecidos problemas de segurança nesta matéria^{61,62}. Os documentos a assinar são virtuais e como tal apenas legíveis através de sistemas que podem ser corrompidos, comprometendo todo o processo. O aumento da eficiência dos sistemas de computadores ou outro progresso científico ou tecnológico leva a que uma assinatura digital que actualmente seja segura o possa deixar de ser no futuro. O armazenamento de documentos assinados electronicamente poderá ter de prever a re-assinatura de documentos, a prazo, para manter a sua validade⁷². Tal processo acarretará custos, acrescidos à manutenção dos ficheiros electrónicos acumulados em condições de segurança que implicarão necessariamente a redundância dos sistemas de armazenamento. Estas e outras questões sobre o ciclo de vida dos documentos, nomeadamente o tempo de armazenamento previsto ou necessário para cada tipo específico de documento clínico, surgem discutidas na literatura^{73,74} mas deverão ser acauteladas, em qualquer sistema a implementar, ainda antes da emissão do primeiro documento.

3.2.2. Privacidade

Além da capacidade de guardar uma grande quantidade de informação mais estruturada e de melhor compreensão e facilitar o arquivo de informação, um documento electrónico é

muito mais facilmente partilhável. Essa característica torna também mais prementes as questões relacionadas com a privacidade dos dados. Idealmente uma especificação de documento clínico em ficheiro electrónico de dados deveria prever uma forma de cifra de informação, que permita apenas a sua leitura aos destinatários autorizados, tornando-se possível a sua transferência sobre vias potencialmente inseguras, como o correio electrónico comum. A definição de quem poderá estar autorizado a aceder a informação cairá fora do âmbito de uma especificação de documento electrónico. A utilização de uma cifra assimétrica (descrita adiante) permitirá cifrar o documento de modo que só o seu destinatário o poderá ler.

Os mecanismos de cifra históricos basearam-se na partilha de um segredo (chave), que permite ao receptor decifrar a mensagem. Tratava-se de uma cifra de tipo simétrico, com utilização da mesma chave para cifrar e decifrar. No entanto é necessário que a chave chegue antecipadamente, por um canal seguro, ao receptor, problema de difícil resolução por meio exclusivamente electrónico. Desde logo, no algoritmo por si descrito, Rivest, Shamir e Adleman⁴³ propuseram a utilização de um sistema criptográfico de chave pública na criação de uma cifra assimétrica, com chaves de cifra e decifra distintas. A mensagem pode ser cifrada por qualquer possuidor da chave pública do destinatário e só aquele a pode decifrar, com a sua chave privada. Para que o pior desempenho das cifras assimétricas não torne inviável o processo de cifrar documentos longos, é possível utilizar uma cifra assimétrica para envio de uma chave de cifra simétrica, por sua vez utilizada para decifrar o documento e não re-utilizável.

Vários processos de cifra deste tipo existem disponíveis, com utilização de diferentes algoritmos, referindo-se aqui em particular o processo de cifra proposto pelo *World Wide Web Consortium*⁷⁵ por o resultado da cifra ser representado em XML, comum ao mecanismo de assinatura já descrito. Este processo permite a escolha dos algoritmos de cifra utilizados (podendo usar por exemplo uma cifra assimétrica RSA, uma função de *hash* SHA-1 e uma cifra simétrica *Advanced Encryption Standard*, AES-256).

4. Material e métodos

4.1. Estrutura do documento

Propõe-se um documento com codificação XML, incluindo uma estrutura semântica de relatório clínico compatível com a norma CDA, e uma assinatura XAdES.

O ficheiro ou cadeia de caracteres com codificação XML⁷⁶ inclui um cabeçalho XML e um conjunto de elementos hierarquizados, com um único elemento raiz englobando todos os restantes. Os elementos podem ter atributos e conteúdo, podendo conter outros elementos.

Serão reforçados a negrito os termos ou frases a serem usados na codificação exactamente como neste trabalho apresentados.

Denominar-se-á o elemento raiz **<ClinDocEnvelope>** e os seus sub-elementos serão o documento clínico e a assinatura. Este elemento é criado sem espaço de nomes, para albergar a assinatura sem alterar o contexto dos seus espaços de nomes, como aconteceria se a assinatura fosse descendente do documento clínico e que poderia condicionar erros na validação das assinaturas. Os eventuais atributos deste elemento não seriam, segundo este modelo, assinados.

4.2. Documento clínico

O documento levará em conta a norma *Clinical Document Architecture* (Versão R2)⁷⁷, com as restrições assinaladas em proposta de 2007 para perfil de conformidade e guia de implementação destinado a relatórios de imagem médica⁷⁸.

O elemento raiz é denominado **<ClinicalDocument>** e terá atributos do espaço de nomes fixos como abaixo apresentado:

```
<ClinicalDocument xmlns="urn:hl7-org:v3" xmlns:voc="urn:hl7-org:v3/voc"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
Id="ClinicalDocument">
```

Os sub-elementos de **<ClinicalDocument>** são subdivididos em dois grupos, o cabeçalho e o corpo do documento.

Não serão abordados os elementos XML não obrigatórios e que não pareçam necessários no contexto deste trabalho. Por defeito os elementos consideram-se obrigatórios.

Por razões de segurança, discutidas adiante, apenas deverão ser incluídas duas linhas de comentário na codificação XML, uma delas antes do primeiro elemento do cabeçalho e que será exactamente:

<!--CDAHeader-->

A outra linha de comentário será incluída após o último elemento do cabeçalho e antes do corpo do documento:

<!--CDABody-->

4.2.1. Cabeçalho

O cabeçalho identifica e classifica o documento, fornece informação sobre autenticação, a consulta ou acto médico, o utente e os profissionais de saúde envolvidos. Engloba os elementos adiante discriminados:

1. realmCode

Elemento não obrigatório que permitirá indicar um domínio de país para o documento, com especificações próprias. Admite-se que no futuro possa existir um código para Portugal. Pode ser atribuído o valor **UV**, universal, ou não incluir este elemento:

<realmCode code='UV'/>

2. typeId

Elemento que define o tipo de documento, devendo ser usados os atributos abaixo para indicar a adesão às restrições impostas pela *CDA Release 2.0*:

<typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040"/>

3. templateId

Indica o perfil seguido no documento, que no caso do perfil destinado a relatórios de imagem médica seguido será:

**<templateId root="2.16.840.1.113883.10"
extension="CDAR2_II_BIMGRPTS_R1"/>**

4. id

Este elemento também não tem conteúdo e pelos seus atributos raiz e extensão identifica univocamente cada documento. A raiz (**root**) é um *OSI Object Identifier* (OID) conforme com a sintaxe adequada àquele identificador e tem no máximo 64 caracteres. Preferencialmente aquele atributo será suficiente para identificar o documento e não será utilizado atributo extensão (**extension**). A extensão poderá ser a única utilizada se, por exemplo, os documentos se destinarem apenas a uma organização; a extensão indicará assim um identificador único de documento dentro da organização, como no exemplo:

```
<id extension="AB0123"/>
```

5. code

Especifica o código do tipo de documento, dentro de um sistema de nomenclatura. É determinado por quatro atributos do elemento; **code**, **codeSystem**, **codeSystemName** e **displayName**. Deverá ser utilizado o sistema *LOINC* tomando o elemento os seguintes atributos, no caso de um relatório de imagem médica:

```
<code code="18748-4" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Diagnostic Imaging Report"/>
```

6. title

Este elemento não é obrigatório. Se o relatório se referir apenas a um exame de imagem, poderá indicar o exame relatado, por exemplo:

```
<title>TC Abdominal</title>
```

Podendo o relatório incluir vários exames de imagem sugere-se a adopção de um título genérico, como:

```
<title>Relatório de Imagem Médica</title>
```

A particularização do título do relatório ou relatórios no documento pode ser feita sob a forma de título de uma secção do corpo do documento (pág. 38).

7. effectiveTime

Elemento que especifica a data-hora do início da criação do conteúdo do documento. A data e hora surgem no formato “AAAAMMDDhhmmss”; se o documento não é criado directamente pelo autor (como no caso de transcrição por dactilógrafo) poderá aceitar-se menor precisão. Um exemplo de codificação será:

<effectiveTime value="20101231"/>

8. confidentialityCode

Especifica o grau de confidencialidade do documento. No perfil usado poderá ser escolhida confidencialidade normal, expressa pelo elemento:

<confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>

9. languageCode

Este código indica a língua (e respectivo país) usada no conteúdo do documento; em Portugal, deverá ser utilizada a seguinte representação:

<languageCode code="pt-PT"

10. recordTarget

O elemento **recordTarget** identifica o utente ao qual o relatório diz respeito e em cujo registo médico o relatório será colocado. É obrigatório (excepcionalmente pode ser múltiplo) e contém:

10.1. Um elemento **patientRole**, que contém os sub-elementos a baixo discriminados:

10.1.1. O elemento **id** (pode ser múltiplo) não tem conteúdo e pelos seus atributos raiz (**root**) e extensão (**extension**) identifica inequivocamente o indivíduo. Se o contexto for a utilização dentro de uma única organização, e apenas for identificado o atributo extensão, este elemento deve ser único. Neste último caso corresponderá à identificação do processo ou *PatientID*. Será recomendável que esta identificação contenha elementos, por exemplo letras em prefixo, que identifiquem a organização / unidade de saúde (vulgarmente o hospital ou clínica). De uma forma geral este elemento pode ser múltiplo porque o utente pode ter várias identificações, por recurso a diferentes unidades de saúde;

10.1.2. O elemento **addr** (não obrigatório, pode ser múltiplo) indica o endereço. No contexto de Portugal podem ser utilizados os sub-elementos **streetAddressLine** (em número de um ou mais), **city**, **postalCode** e eventualmente **country**;

10.1.3. O elemento **telecom** (não obrigatório, pode ser múltiplo) representa telefone, fax ou outro meio de telecomunicações, com os exemplos de representação:

<telecom value="tel:+351987654321"/>

<telecom value="fax:+351123456789"/>

<telecom value="mailto:xxx@servidor.pt"/>

10.1.4. Um elemento **patient** com os seguintes sub-elementos:

10.1.4.1. O elemento **name** (não obrigatório), definindo o nome do utente, que pode conter os sub-elementos:

10.1.4.1.1. O elemento **prefix** contém um prefixo, como título académico;

10.1.4.1.2. O elemento **given** contém o(s) nome(s) próprios;

10.1.4.1.3. O elemento **family** contém o apelido;

10.1.4.1.4. O elemento **suffix** contém um sufixo (como “Júnior”).

10.1.4.2. Um elemento **administrativeGenderCode** que indica o sexo e tem o seu atributo **codeSystem** fixo (**codeSystem="2.16.840.1.113883.5.1"**) e o atributo **code** a escolher entre **code="M"** (masculino), **code="F"** (feminino) ou **code="UN"** (indiferenciado);

10.1.4.3. O elemento **birthTime** com o atributo **value** definindo a data de nascimento, num formato semelhante ao elemento *effectiveTime* (pág. 28);

10.1.4.4. Um elemento **guardian** é obrigatório se o utente for menor, indicando o detentor do poder paternal e com o seguinte conteúdo:

10.1.4.4.1. Um elemento **id** como descrito acima (pág. 29) mas não obrigatório;

10.1.4.4.2. Elementos **addr**, **telecom** como descritos acima (pág. 29);

10.1.4.4.3. Um elemento **guardianPerson** que contém:

10.1.4.4.3.1. Um elemento **name** como definido acima. (pág. 30).

10.1.4.4.4. Ou um elemento **guardianOrganization** (em alternativa a *guardianPerson*) contendo os elementos descritivos de uma organização:

10.1.4.4.4.1. Um elemento **id** como descrito acima (pág. 29) mas não obrigatório;

10.1.4.4.4.2. Um elemento **name** contendo o nome da organização;

10.1.4.4.4.3. Elementos **telecom** como descritos acima (pág. 29);

10.1.4.4.4.4. Elementos **addr** também descritos acima (pág. 29).

10.1.4.5. Podem existir referências a estado civil, religião, etnia ou raça, com uso explicitado na norma, mas que optamos por não utilizar por parecerem desnecessários para identificação inequívoca. Qualquer discordância com qualquer destes elementos, eventualmente utilizados, não deverá ser considerada e não porá em causa uma correcta identificação.

10.1.5. Um elemento **providerOrganization** (não obrigatório), podendo representar a entidade responsável pela prestação de cuidados ao utente, com os elementos de uma organização como descrito acima para o elemento **guardianOrganization**.

11. author

O elemento **author** identifica o criador do documento, é obrigatório e pode ser múltiplo. Inclui os elementos abaixo discriminados:

11.1. Um elemento **time** que representa a data-hora do início da participação do autor na criação do documento. A sua representação segue a regra já apresentada (pág. 28);

11.2. Um elemento **assignedAuthor**, incluindo os elementos:

11.2.1. Um ou mais elementos **id** como descrito acima (pág. 29);

11.2.2. Elementos **addr**, **telecom** como descritos acima (pág. 29);

11.2.3. O elemento **assignedPerson** que inclui os dados pessoais do autor e contém:

11.2.3.1. Um elemento **name** como definido acima (pág. 30).

11.2.4. Um elemento não obrigatório **representedOrganization** que indica a organização a que pertence o autor, com os elementos de uma organização como descrito na pág. 30.

Embora a norma CDA admita a autoria por sistemas automáticos, com uma codificação própria, ela não será aqui abordada.

12. dataEnterer

O elemento **dataEnterer** não é obrigatório e identifica quem introduz os dados (por exemplo dactilógrafo), independentemente de ser ou não autor. Contém os elementos seguintes:

12.1. Um elemento não obrigatório **time**, que representa a data-hora do início da participação do introdutor dos dados, com o formato apresentado anteriormente (pág. 28);

12.2. Um elemento **assignedEntity** com os seguintes sub-elementos:

12.2.1. Um ou mais elementos **id** como descrito acima (pág. 29);

12.2.2. Um elemento não obrigatório **code**, definido por quatro atributos como descrito acima (pág. 28), que indicará o papel desempenhado pela entidade;

12.2.3. Elementos **addr**, **telecom** como descritos acima (pág. 29);

12.2.4. O elemento **assignedPerson** que inclui os dados pessoais e contém:

12.2.4.1. Um elemento **name** como definido acima (pág. 30).

12.2.5. Um elemento não obrigatório **representedOrganization** que indica a organização a que pertence a entidade, com os elementos de uma organização como descrito na pág. 30.

Ao contrário de um elemento *assignedAuthor*, o elemento *assignedEntity* não pode representar um sistema automático.

13. custodian

O elemento **custodian** identifica a entidade responsável pela guarda do documento. Os seus elementos são discriminados abaixo:

13.1. Um único elemento **assignedCustodian** com seguinte conteúdo:

13.1.1. Um elemento **representedCustodianOrganization**, com os elementos de uma organização como já descrito (pág. 30) com a particularidade de ser obrigatório o elemento *id*.

14. informationRecipient

O elemento **informationRecipient** não é obrigatório e identifica a quem é destinada a informação. Pode ser múltiplo. Na generalidade dos casos será o médico que requisita o estudo. Inclui os elementos abaixo (pelo menos um elemento *informationRecipient* ou *receivedOrganization* deverá estar presente):

14.1. Um elemento **intendedRecipient** contendo os seguintes elementos:

14.1.1. Zero ou mais elementos **id** como descrito acima (pág. 29);

14.1.2. Elementos **addr**, **telecom** como descritos acima (pág. 29);

14.1.3. Um elemento não obrigatório **informationRecipient** indicando a pessoa a quem se destina a informação e cujo conteúdo é:

14.1.3.1. Um elemento **name** como definido acima (pág. 30).

14.1.4. Um elemento não obrigatório **receivedOrganization** indicando a organização a que se destina a informação, com os elementos de uma organização como descrito na pág. 30.

15. legalAuthenticator

O elemento **legalAuthenticator** identifica um único responsável legal pela autenticação do relatório, ou seja, quem assina por último o relatório, estando plenamente habilitado para o fazer. Caso exista a possibilidade de mais de uma assinatura, os restantes responsáveis deverão ser indicados em um ou mais elementos *authenticator*. Este elemento só é obrigatório se o documento estiver assinado e contém os elementos seguintes:

15.1. Um elemento **time** que representa a data-hora de autenticação do documento. A sua representação segue a regra apresentada na pág. 28;

15.2. Um elemento **signatureCode** que deve ter o atributo fixo **<signatureCode code="S"/>** significando que o documento foi assinado e a assinatura arquivada;

15.3. Um elemento **assignedEntity** com os sub-elementos descritos na pág. 32, podendo o elemento *code* fornecer a informação sobre qual a qualidade em que o responsável assina o elemento (p.ex.: com *displayName*="Médico Radiologista").

16. authenticator

O elemento **authenticator** não é obrigatório, pode ser múltiplo e identifica outros responsáveis pela autenticação do documento. Poderá ser utilizado quando existem múltiplos responsáveis ou para indicar a autenticação preliminar de um documento por alguém não habilitado a assinar de forma definitiva o documento (por exemplo, um interno da especialidade em formação). Os seus elementos são discriminados abaixo:

16.1. Um elemento **time** que representa a data-hora de autenticação do documento. A sua representação segue a regra anteriormente apresentada (pág. 28);

16.2. Um elemento **signatureCode** que deve ter o atributo fixo **<signatureCode code="S"/>** significando que o documento foi assinado e a assinatura arquivada;

16.3. Um elemento **assignedEntity** com os sub-elementos descritos acima (pág. 32).

17. participant

O elemento **participant** não é obrigatório e indica outros participantes. No perfil de relatório de imagem deve ser único e utilizado para indicar o médico que requisita o estudo. Deve ter o atributo fixo **<participant typeCode="REF">** significando que o tipo de participação é a referência do utente. Inclui o elemento seguinte:

17.1. Um elemento **associatedEntity**, com atributo fixo **<associatedEntity classCode="PROV">** significando tratar-se de uma entidade autorizada a ministrar cuidados de saúde (do inglês *provider*). Os seus sub-elementos são:

17.1.1. Zero ou mais elementos **id** como descrito acima (pág. 29);

17.1.2. Elementos **addr**, **telecom** como descritos acima (pág. 29);

17.1.3. Um elemento **associatedPerson** que inclui os dados pessoais e contém:

17.1.3.1. Um elemento **name** como definido acima (pág. 30).

17.1.4. Um elemento não obrigatório **scopingOrganization** que indica a organização que autoriza o papel do participante (como exemplo em Portugal poderia ser a Ordem dos Médicos). Contém os sub-elementos de uma organização como descrito na pág. 30.

18. documentationOf

O elemento **documentationOf** é obrigatório em número de um ou mais e destina-se a identificar os estudos de imagem que são relatados no documento. Cada elemento englobará um único sub-elemento *serviceEvent*.

18.1. Cada elemento **serviceEvent** descreverá um procedimento unitário (com facturação unitária), com o atributo fixo **<serviceEvent classCode="ACT">** significando que o evento descrito é um acto de prestação de cuidados de saúde. Inclui os elementos abaixo indicados:

18.1.1. Zero ou mais elementos **id** representados como descrito acima (pág. 28) e que identificam os estudos relatados (pode ser o *DICOM Study Instance UID* da *Modality Worklist*);

18.1.2. Um elemento não obrigatório **code** referente ao procedimento. Deverá ser concordante com o código do tipo de documento (pág. 28);

18.1.3. Um elemento não obrigatório **effectiveTime** indicando o intervalo de tempo em que ocorreu o procedimento. A data e hora surgem no formato “AAAAMMDDhhmmss”, aceitando-se menor precisão. Os seus elementos (pode estar apenas presente um dos elementos) são:

18.1.3.1. Elemento **low** indicando a data-hora do início do procedimento no seu atributo **value**;

18.1.3.2. Elemento **high** indicando a data-hora do fim do procedimento no seu atributo **value**. Apresenta-se um exemplo indicando apenas um único dia de realização, 4 de Janeiro de 2010.

<effectiveTime>

<low value='20100104'/>

<high value='20100104'/>

</effectiveTime>

18.1.4. Zero ou mais elementos **performer** identificando os profissionais de saúde (geralmente médicos ou técnicos) envolvidos no procedimento que origina as imagens relatadas. São considerados três tipos de envolvimento, identificados no atributo *typeCode* deste elemento; (i) profissional responsável, (**typeCode=“PRF”**), (ii) principal responsável (**typeCode= “PPRF”**) ou responsável secundário (**typeCode=“SPRF”**). Inclui os seguintes elementos:

18.1.4.1. Um elemento não obrigatório **time** com o mesmo formato do elemento *effectiveTime* descrito imediatamente acima, especificando o intervalo de tempo da participação do profissional de saúde;

18.1.4.2. Um elemento **assignedEntity** com os sub-elementos descritos na pág. 32. A norma CDA prevê um código para identificação do tipo de profissional, com base na classificação SNOMED, no entanto esse dado pode ser inferido, se necessário, conhecendo-se a organização representada.

19. relatedDocument

O elemento **relatedDocument** não é obrigatório. Em número de zero ou mais, destina-se a identificar documentos relacionados. São considerados três tipos, identificados no atributo *typeCode*:

- 1) Documento substituído pelo actual, (**typeCode="RPLC"**);
- 2) Documento do qual o actual é uma adenda (**typeCode= "APND"**);
- 3) Documento no qual o actual teve origem e de que é uma transformação (**typeCode="XFRM"**).

Note-se que apenas é possível substituir um documento que ainda não tenha sido legalmente autenticado. Para corrigir um documento assinado deverá ser criada uma adenda, que conterà as alterações a introduzir ou uma nova versão do documento, mas mantendo-se em arquivo o anterior documento assinado.

Existem restrições ao número de documentos relacionados, apenas se admitindo as seguintes combinações; i) um documento de tipo 1), ii) um de tipo 2), iii) um de tipo 3), iv) dois documentos, sendo um de tipo 1) e outro de tipo 3) ou v) dois documentos, sendo um de tipo 2) e outro de tipo 3).

O conteúdo deste elemento será:

19.1. Um único elemento **parentDocument** que descreve o documento relacionado e cujo conteúdo é:

19.1.1. Um elemento **id** identificando univocamente o documento relacionado, com regras próprias descritas acima (pág. 28);

19.1.2. Um elemento não obrigatório **code** identificando o código de tipo do documento relacionado, como previamente descrito (pág. 28).

Apresenta-se um exemplo deste elemento declarando que o documento actual é uma adenda do documento com *id* discriminado:

```
<relatedDocument typeCode="APND">  
  <parentDocument>  
    <id extension="AB0123"/>  
  </parentDocument>  
</relatedDocument>
```

4.2.2. Corpo do documento

Existem na norma CDA duas opções para o corpo do documento, que poderá ser estruturado ou apenas uma ligação a informação com codificação diferente. O perfil para relatório de imagem⁷⁸ obriga a utilização do corpo estruturado. Para possibilitar a autenticação digital do documento é também necessário que toda a sua informação esteja estruturada e incluída na codificação XML a assinar. Pelo contrário, na opção de corpo de documento não estruturado (*nonXMLBody*) a multiplicidade de codificações diferentes em que a informação pode ser apresentada torna extremamente difícil definir regras de autenticação.

O corpo do documento contém o relatório clínico e é dividido em secções que podem estar reciprocamente encapsuladas, contidas em elementos *component* em hierarquia.

1. component

Toda a informação do corpo do documento está contida num único elemento **component**, inserido sob a raiz *ClinicalDocument* e incluído imediatamente após a segunda linha de comentário (*<!--CDABody-->*). O seu conteúdo é um elemento *structuredBody*:

1.1. O elemento **structuredBody** é único e contém os elementos seguintes:

1.1.1. Neste nível hierárquico um ou mais elementos **component** estão presentes. É proposto que cada um daqueles elementos encerre a informação relativa a um exame de imagem, ou a vários exames relatados em conjunto. Este conceito segue a realidade, em que por vezes um único documento contém relatórios separados de vários exames de imagem (dá-se um exemplo de um documento que pode conter um relatório conjunto de TC abdominal e pélvica e outro relatório conjunto de mamografia e ecografia mamária). O conteúdo deste elemento é:

1.1.1.1. Um elemento **section** que corresponderá ao relatório de um exame ou ao relatório conjunto de vários exames formando uma unidade narrativa única e que contém os elementos:

1.1.1.1.1. Um elemento **code** codificando o tipo de conteúdo da secção, que neste nível hierárquico deverá ser fixo e igual ao código do tipo de documento (pág. 28), referenciando de forma genérica um relatório de exame de imagem, sendo o tipo de exame(s) relatado(s) particularizado no título da secção, abaixo;

1.1.1.1.2. Um elemento **title** com o título da secção, correspondendo neste nível ao título do relatório de cada exame ou conjunto de exames, em língua portuguesa e tal como será apresentado para visualização. Por razão linguística este título não será igual ao atributo *displayName* do elemento anterior, como seria recomendado pelo perfil para relatório de imagem⁷⁸;

1.1.1.1.3. As secções deste nível hierárquico não conterão elemento *text*, que corresponde ao conteúdo textual da secção;

1.1.1.1.4. No documento proposto não serão também introduzidos elementos *entry*, já correspondendo a uma estruturação de nível três, que possibilitará por exemplo a codificação de actos e achados viabilizando o tratamento automático daquela informação mas que está fora do âmbito deste trabalho;

1.1.1.1.5. Um ou mais elementos **component**, cujo conteúdo representará nesta proposta de especificação as várias secções ou subtítulos dentro de cada relatório. O conteúdo deste elemento é:

1.1.1.1.5.1. Um elemento **section** semelhante sintacticamente ao descrito acima e que na especificação CDA permite assim aninhar hierarquicamente múltiplas secções. Nesta proposta este nível hierárquico utilizará tipos de secções predefinidos e não albergará subsecções, contendo assim os elementos:

1.1.1.1.5.1.1. Um elemento **code** codificando o tipo de conteúdo da secção, que neste nível hierárquico deverá ser uma escolha entre os tipos abaixo indicados. Também aqui o *displayName* divergirá do título da secção, por motivo da língua, e apresentam-se propostas de tradução, que no entanto poderão ser modificadas, devendo ser respeitado no entanto o tipo de informação presente em cada secção. Cada relatório deverá conter pelo menos uma secção de tipo *Study observation*. O atributo **codeSystem** será fixo e igual a "2.16.840.1.113883.6.1" e o **codeSystemName** será "LOINC" tal como no exemplo abaixo. Deverão surgir no documento pela ordem a seguir apresentada (que difere ligeiramente da recomendação no perfil de conformidade):

1.1.1.1.5.1.1.1. **Reason for study, 18785-6**, que corresponderá a um título "Informação clínica" ou "Motivo do exame" e conterá a

informação prévia ao exame, e que o motivou, assim como possíveis dúvidas a esclarecer;

1.1.1.1.5.1.1.2. **Current imaging procedure descriptions, 55111-9**, contendo a descrição dos procedimentos para obtenção das imagens, com uma tradução possível de “Protocolo técnico”;

1.1.1.1.5.1.1.3. **Study observation, 18782-3**, que deverá existir em cada relatório, a que corresponderá um título “Leitura e interpretação” e onde serão descritos em pormenor os achados imagiológicos, assim como a interpretação individual que lhes é dada. O título deverá ser omitido tratando-se da única secção do relatório que inclua toda a informação;

1.1.1.1.5.1.1.4. **X-ray impression, 19005-8**, que conterà as conclusões retiradas da avaliação do conjunto dos achados, no contexto do examinado. Propõe-se o título “Impressão diagnóstica” ou “Conclusões”. Poderão ainda ser utilizados outros códigos de secção, se necessário. Segue-se um exemplo da sintaxe do elemento:

```
<code code="18785-6" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Reason for study"/>
```

1.1.1.1.5.1.2. Um elemento **title**, correspondendo ao título da secção em língua portuguesa e tal como será apresentado para visualização, preferencialmente utilizando as sugestões anteriores;

1.1.1.1.5.1.3. Um elemento **text** contendo o bloco narrativo da secção com texto, formatado pela utilização dos elementos seguintes:

1.1.1.1.5.1.3.1. Os elementos **br** e **paragraph** permitem formatar um parágrafo no texto, diferindo entre si porque o elemento *br* se apresenta vazio (**
**) na posição em que será introduzida mudança de linha enquanto no elemento *paragraph* o texto do parágrafo é incluído como conteúdo, entre a etiqueta inicial e a etiqueta final do elemento *paragraph*;

1.1.1.1.5.1.3.2. O elemento **caption** pode definir um título num parágrafo, numa lista ou item de lista, numa tabela ou célula de uma tabela;

1.1.1.1.5.1.3.3. Os elementos **sup** e **sub** permitem a formatação de texto acima ou abaixo da linha de escrita. O texto com esta formatação é incluído também como conteúdo do elemento;

1.1.1.1.5.1.3.4. O elemento **content** permite definir um trecho de texto individualizado e que é possível referenciar. Uma das utilizações desta característica é a determinação de um atributo **styleCode** para o elemento, que permite a formatação de texto em negrito (**styleCode="Bold"**), sublinhado (**styleCode="Underline"**) ou itálico (**styleCode="Italics"**), ou ainda outros estilos adicionais que não serão aqui desenvolvidos⁷⁷;

1.1.1.1.5.1.3.5. O elemento **list** define uma lista, de sub-elementos **item**, podendo o seu primeiro elemento filho ser um elemento *caption*. O seu atributo, obrigatório, **listType**, define se a lista é ordenada (**listType="ordered"**) ou não ordenada (**listType="unordered"**);

1.1.1.1.5.1.3.6. O elemento **table** permite definir uma tabela, semelhante ao definido pela especificação HTML⁷⁹. Num exemplo simples o seu sub-elemento **tbody** contém elementos **tr** que definem linhas da tabela e que por sua vez contém elementos **th**, definindo células que são título de linha ou coluna (*headers*) ou elementos **td**, que definem células com dados.

4.3. Assinatura digital

A opção escolhida para assinatura digital foi a especificação XAdES. Esta norma prevê, no seu formato XAdES-T, a aposição de um carimbo de tempo, emitido por uma autoridade que atesta que o documento existe na data de assinatura e não foi criado posteriormente. Em complemento a esta validação cronológica foi estruturado um mecanismo, proposto neste trabalho, em que sobre a assinatura do responsável pela autenticação do documento é aposta a contra-assinatura da organização responsável pela guarda do documento, sendo ainda guardado nas propriedades assinadas por esta última o valor da contra-assinatura do documento que o antecede (o primeiro documento guarda um valor nulo) e um número de ordem de arquivo do documento, criando assim uma cadeia inquebrável de documentos.

O elemento XML que constitui a assinatura, **ds:Signature**, é definido pela norma *XML Signature Syntax and Processing* (XMLDsig)⁶⁰ e a sua extensão *XML Advanced Electronic Signatures* (XAdES)⁶³. Inclui os elementos apresentados adiante, pertencendo os identificados com o prefixo “**ds**” ao espaço de nomes “**http://www.w3.org/2000/09/xmldsig#**” definido por XMLDsig e os restantes ao espaço de nomes “**http://uri.etsi.org/01903/v1.3.2#**” definido pela especificação técnica da *European Telecommunications Standards Institute*, de 2006, relativa a XAdES⁸⁰.

O elemento **ds:Signature** contém os seguintes sub-elementos:

1. **ds:SignedInfo** – elemento que contém a informação que será assinada e que inclui:
 - 1.1. **ds:CanonicalizationMethod** – método de transformação da estrutura XML do elemento *ds:SignedInfo* do documento a assinar numa cadeia de octetos à qual pode ser aplicado um algoritmo de assinatura;
 - 1.2. **ds:SignatureMethod** – algoritmo utilizado na assinatura, no presente trabalho uma assinatura RSA⁸¹ (PKCS #1 v1.5) com função de *hash* SHA-1;
 - 1.3. **ds:Reference** – um ou mais elementos que indicam no seu atributo **URI** qual o conteúdo que é assinado (neste nível dois elementos, um indicando a raiz do documento clínico, o elemento *ClinicalDocument*, e outro as propriedades assinadas da assinatura *SignedProperties*, parágrafo 3.1.1), e que incluem:
 - 1.3.1. **ds:Transforms** – elemento (não obrigatório e não necessário se a assinatura for inserida destacada, como definido neste modelo) que agrupa um ou mais sub-elementos:
 - 1.3.1.1. **ds:Transform** – elemento que define transformações a aplicar aos dados referenciados antes de aplicação do algoritmo de *hash*.
 - 1.3.2. **ds:DigestMethod** – função utilizada para obter um *hash* do conteúdo indicado pela referência;
 - 1.3.3. **ds:DigestValue** – valor de *hash* obtido por aplicação da função anterior ao conteúdo definido, representado *base64*.
2. **ds:SignatureValue** – valor obtido pela aplicação do algoritmo de assinatura à forma canónica do elemento *ds:SignedInfo*;

3. **ds:Object** - elemento que pode ser múltiplo (é definido abaixo na contra-assinatura um segundo elemento com o mesmo nome) e contém dados, passíveis de serem ou não assinados, representando informação adicional à assinatura; este elemento contém, organizados hierarquicamente, os elementos:

3.1. **QualifyingProperties** – elemento definido pela especificação XAdES:

3.1.1. **SignedProperties** – elemento contendo informação cuja integridade e autenticidade é garantida na assinatura:

3.1.1.1. **SignedSignatureProperties** – propriedades da assinatura assinadas:

3.1.1.1.1. **SigningTime** – data e hora de assinatura, com o formato “AAAA-MM-DDThh:mm:ss” (p.ex.: 2000-11-18T12:10:00) a concatenar com “Z” se a hora for definida em tempo universal coordenado, UTC;

3.1.1.1.2. **SigningCertificate** – informação sobre o certificado utilizado na assinatura:

3.1.1.1.2.1. **Cert** – elemento que pode ser múltiplo, permitindo guardar informação de vários certificados:

3.1.1.1.2.1.1. **CertDigest** – elemento em que são guardados dados de um *hash* do certificado, nos sub-elementos:

3.1.1.1.2.1.1.1. **ds:DigestMethod** – identificação da função de *hash*;

3.1.1.1.2.1.1.2. **ds:DigestValue** – valor de *hash*.

3.1.1.1.2.1.2. **IssuerSerial** – identificação do certificado, incluindo:

3.1.1.1.2.1.2.1. **ds:X509IssuerName** – nome completo do emissor do certificado;

3.1.1.1.2.1.2.2. **ds:X509SerialNumber** – número de série do certificado.

3.1.2. **UnsignedProperties** – propriedades não assinadas, que no modelo proposto não estarão presentes antes da contra-assinatura pela organização responsável pela guarda do documento:

3.1.2.1. **UnsignedSignatureProperties** – propriedades da assinatura, não assinadas:

3.1.2.1.1. **CounterSignature** – elemento onde é integrada a contra-assinatura, contida dentro do elemento:

3.1.2.1.1.1. **ds:Signature** – assinatura da organização responsável pela custódia do documento, que tem uma estrutura semelhante à primeira assinatura comentando-se assim apenas os elementos que dela diferem:

3.1.2.1.1.1.1. **ds:SignedInfo**:

3.1.2.1.1.1.1.1. **ds:CanonicalizationMethod**;

3.1.2.1.1.1.1.2. **ds:SignatureMethod**;

3.1.2.1.1.1.1.3. **ds:Reference** (elemento em triplicado, indicando os elementos *SignatureValue* da primeira assinatura (parágrafo 2), *SignedProperties* da contra-assinatura (parágrafo 3.1.2.1.1.1.3.1.1, abaixo) e *ChainProperties* (parágrafo 3.1.2.1.1.1.4.1), e com sub-elementos semelhantes ao atrás referido (parágrafo 1.3);

3.1.2.1.1.1.2. **ds:SignatureValue** – valor da contra-assinatura;

3.1.2.1.1.1.3. **ds:Object**:

3.1.2.1.1.1.3.1. **QualifyingProperties** – contendo um elemento:

3.1.2.1.1.1.3.1.1. **SignedProperties**, com propriedades assinadas pela contra-assinatura, como definidas no parágrafo 3.1.1.

3.1.2.1.1.1.4. **ds:Object** - elemento não presente antes da contra-assinatura pela organização responsável pela guarda do documento:

3.1.2.1.1.1.4.1. **chainp:ChainProperties** – elemento de um espaço de nomes a criar, incluindo o atributo **xmlns:chainp="http://fc.up.pt/MIM3/ChainProperties#"** e contendo os elementos:

3.1.2.1.1.1.4.1.1. **chainp:ArchiveSeqNumber** – número sequencial, a atribuir quando o documento é incluído no arquivo;

3.1.2.1.1.1.4.1.2. **chainp:PreviousDocSignatureValue** – o valor da contra-assinatura (parágrafo 3.1.2.1.1.1.2) do documento com número de arquivo imediatamente anterior (igual a zero codificado *base64*, “**AA==**”, no primeiro documento da cadeia, que não tem antecessor).

Os elementos com prefixo “**chainp**” são uma extensão introduzida neste trabalho e cuja definição de esquema será:

```
<element name="ChainProperties" type="chainp:ChainPropertiesType"/>
<complexType name="ChainPropertiesType">
    <sequence>
        <element name="ArchiveSeqNumber" type="integer" />
        <element name="PreviousDocSignatureValue" type="base64Binary" />
    </sequence>
</complexType>
```

Este elemento permite criar um encadeamento de documentos que impede a substituição de documentos por outros distintos, ou simples desaparecimento de um documento. Um diferente documento originará um diferente valor de contra-assinatura e não mais estará de acordo com os documentos seguintes. Estas características, juntamente com a aposição de carimbo de tempo (pelo menos em alguns documentos da cadeia), destinam-se a evitar o repúdio da veracidade de um documento com a alegação de ter sido criado com uma data falsa em tempo ulterior.

4.4. Validação cronológica

A aposição de carimbo de tempo por terceiro, que ateste que pelo menos à data do carimbo o documento já existia, é fundamental para o não repúdio do documento, pelas razões já antes apontadas. Por depender de ligações externas, podendo trazer demora, este processo poderá ser diferido no tempo após a assinatura.

Propõe-se a inclusão de um carimbo sobre a contra-assinatura, do tipo *SignatureTimeStamp*, como definido pela especificação XAdES⁸⁰. A localização no documento XML será no elemento *QualifyingProperties* da contra-assinatura (referido no parágrafo 3.1.2.1.1.3.1 do capítulo precedente), com a seguinte estrutura hierárquica:

1. O elemento **QualifyingProperties**, que já continha *SignedProperties* da contra-assinatura englobará ainda:

- 1.1. **UnsignedProperties**, com sub-elemento:

- 1.1.1. **UnsignedSignatureProperties**, contendo:

1.1.1.1. O elemento **SignatureTimeStamp**, que reúne os dados do carimbo de tempo e inclui:

1.1.1.1.1. **ds:CanonicalizationMethod**, que descreve o método de transformação do elemento *SignatureValue*; é o resultado dessa transformação que será submetido a digestão (*hash*), para ser enviado à entidade certificadora de tempo;

1.1.1.1.2. **EncapsulatedTimeStamp**. O valor deste elemento é a codificação *base64* da mensagem (*timeStampToken*) que constitui o carimbo de tempo e que é uma sequência de *bytes* em codificação DER conforme a especificação RFC 3161⁵⁸.

4.5. Cifra

Adicionalmente foi definida uma opção de cifra da informação contida no documento clínico electrónico, que permita a transmissão dos documentos assim transformados por meios não necessariamente seguros, como *E-mail*.

A estrutura adoptada segue a recomendação W3C de Dezembro de 2002, *XML Encryption Syntax and Processing*⁷⁵, resultando da cifra um outro documento XML, cujo elemento raiz é denominado *EncryptedData* e contém toda a informação do elemento *ClinDocEnvelope*, incluindo as etiquetas inicial e final. A decifra deste elemento, que necessita da chave privada correspondente à chave pública utilizada na cifra, devolve o documento inicial, com possibilidade de verificação da validade de assinaturas nele contidas. O par de chaves utilizado na assinatura e na cifra não serão os mesmos.

A filosofia deste método assenta, como já acima descrito, na cifra do documento com uma chave simétrica, que é necessário partilhar mas é de uso mais rápido, que é depois partilhada cifrada, com recurso a uma chave assimétrica.

Descreve-se sumariamente a estrutura do elemento *EncryptedData* e dos seus sub-elementos.

1. **EncryptedData** – embora a recomendação admita vários atributos para este elemento, no contexto desta utilização não estarão presentes. O atributo *Id* identifica o documento por uma cadeia de caracteres. O atributo *Type* identifica o tipo de informação, com importância em utilizações em que a etiqueta do elemento cifrado não esteja também ela cifrada e

disponível após decifra. O atributo *MimeType* descreve o tipo de meio cifrado, sendo dispensado porque ele é sempre um documento XML. Também o atributo *Encoding*, definindo a codificação, seria redundante já que a primeira linha do documento não é cifrada (apenas é cifrado o elemento *ClinDocEnvelope*), determinando o uso da codificação UTF-8. Os sub-elementos são:

1.1. **EncryptionMethod** – este elemento define, pelo seu atributo **Algorithm**, o URI do algoritmo usado na cifra;

1.2. **KeyInfo** – este elemento, cujo tipo é definido na norma XMLDsig⁶⁰, permite incluir informação sobre a chave (neste nível uma chave simétrica, por exemplo AES-256-CBC) usada na cifra. A informação sobre a chave está cifrada no elemento:

1.2.1. **EncryptedKey** – este elemento é de tipo *EncryptedType*, semelhante a *EncryptedData*, contendo os mesmos sub-elementos:

1.2.1.1. **EncryptionMethod** – este elemento define, neste nível, o algoritmo utilizado para cifrar a chave simétrica (neste nível uma chave assimétrica, por exemplo RSA, que com o algoritmo AES-256-CBC deverá ser RSA-OAEP);

1.2.1.2. **KeyInfo** – este elemento inclui informação sobre a chave assimétrica usada na cifra. A informação sobre esta chave está nos elementos descendentes, que podem ser múltiplos e definir uma localização da chave pública, conter elementos de identificação ou um *hash* do certificado, ou o próprio certificado. A opção foi utilizar apenas um nome identificativo do certificado, pelo que este elemento contém apenas um sub-elemento:

1.2.1.2.1. **KeyName** – cujo conteúdo é uma cadeia de caracteres definindo um nome associado e identificando o certificado (e respectivo par de chaves pública / privada) utilizado.

1.2.1.3. **CipherData** – inclui um único elemento:

1.2.1.3.1. **ChipherValue** – elemento cujo conteúdo é o valor, codificado *base64*, resultante da cifra da chave simétrica.

1.3. **CipherData** – inclui um único elemento:

1.3.1. **ChipherValue** – elemento cujo conteúdo é o valor, codificado *base64*, resultado da cifra do documento.

1.4. O elemento opcional *EncryptionProperties*, que permite a inclusão de informação adicional, como data em que o documento foi cifrado ou equipamento empregue, não foi utilizado.

4.6. Implementação

Foi desenvolvida uma implementação experimental do modelo, utilizando o compilador *Microsoft Visual Basic 2005 Express Edition*, disponibilizado *on-line* pela *Microsoft*, em linguagem de programação *Visual Basic*. Nos espaços de nomes *System.Security.Cryptography* e *System.Security.Cryptography.Xml* são disponibilizadas funções que permitem acesso fácil a funções criptográficas por intermédio da *CryptoAPI* do sistema operativo, com recurso a provedor de serviços criptográficos do sistema, por defeito o provedor denominado *Microsoft Strong Cryptographic Provider*, ou a provedores externos, como o do cartão de cidadão (os provedores disponíveis encontram-se listados no registo do *Windows* em *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider*).

O *middleware* do cartão de cidadão cria um provedor de serviços criptográficos de tipo bastante completo, *PROV_RSA_FULL*, mas que apenas disponibiliza serviços para assinatura digital⁵³. Pode ser acedido através de interface *CryptoAPI*, nos sistemas operativos *Windows*, e em outros sistemas por um interface PKCS#11, também denominado *Cryptoki*. A organização dos serviços criptográficos e sua integração com os serviços do cartão de cidadão estão representadas na Figura 6.

A geração directa de assinatura digital XML mais simples (XMLDsig) sobre um documento é possível no compilador utilizado, com recurso à classe *SignedXml*. No entanto para cumprir a especificação XAdES foram programadas as referências necessárias na assinatura, tal como descrito acima (pág. 40), e calculado *hash*, depois assinado com a chave privada do cartão de cidadão. Objectos dos mesmos espaços de nomes foram utilizados para construir a funcionalidade de cifra, com recurso a outros certificados digitais e ao provedor criptográfico do sistema operativo, já que o cartão de cidadão não disponibiliza mecanismos de cifra.

O compilador permite também a construção da estrutura do ficheiro XML, por utilização de objectos do espaço de nomes *System.Xml*.

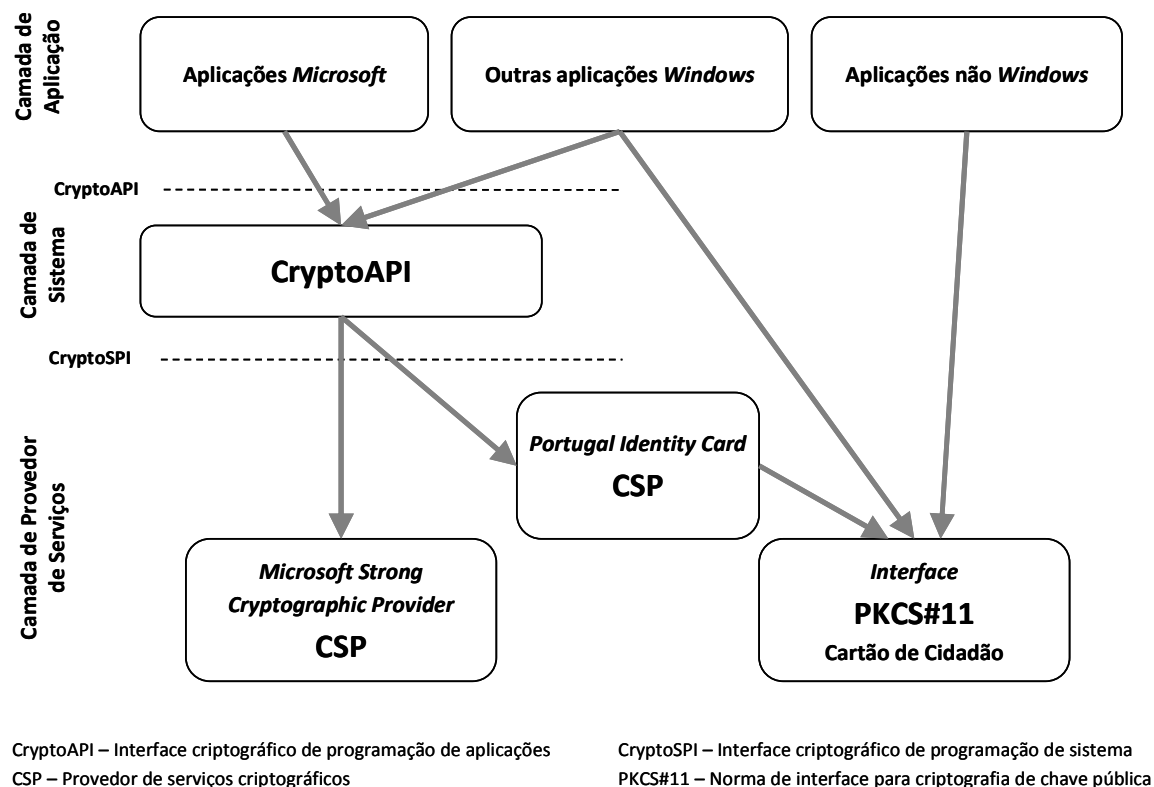


Figura 6. Organização de serviços criptográficos e sua relação com *middleware* do cartão de cidadão

Foi implementada funcionalidade de formatação de texto antes descrita (pág.40) mas não a formatação em tabela, prevista na especificação.

4.7. Testes

Utilizando a implementação referida efectuaram-se testes de conversão de dados de relatórios de imagem, reais, para a estrutura do modelo proposto.

4.7.1. Desenho do estudo

Desenvolveu-se um estudo descritivo em laboratório sobre sistema protótipo destinado a validação da estrutura do modelo de dados e avaliação funcional básica.

4.7.2. Amostra

Foram usados 36 relatórios provenientes de três departamentos de imagem integrados em unidades de saúde com internamento, identificados como A, B e C. Obtiveram-se 12 relatórios de cada departamento, produzidos no segundo semestre do ano de 2009,

anónimos por substituição das letras do nome do paciente, médico e dactilógrafo pelo carácter “X” e seleccionados com recurso a número sequencial e aleatorização por computador.

4.7.3. Equipamento

Foi utilizado computador portátil com processador *Intel Pentium M* 1.80GHz, memória RAM de 0.99GB a 1.80GHz, sistema operativo *Microsoft Windows XP Home Edition SP3*.

4.7.4. Procedimento experimental

Introduziram-se os dados presentes em cada relatório pelo preenchimento dos campos de formulário na aplicação protótipo desenvolvida; foi utilizado *copy-paste* dos diferentes campos a partir da versão digital do documento original. Após conversão para o modelo proposto foi aposta assinatura, com utilização de certificado representando o autenticador legal, e contra-assinatura, por certificado virtual da instituição responsável pela guarda do documento, pretendendo simular o processo de assinatura e arquivo do documento, em condições reais. Após confirmação da validade das assinaturas foi incorporado carimbo de tempo, com recurso ao serviço de validação cronológica do cartão de cidadão (em <http://ts.cartaodecidadao.pt/tsa/server>). Como alternativas apenas para teste verificaram-se disponíveis os servidores de tempo por protocolo HTTP em <http://timestamping.edelweb.fr/service/tsp> e por protocolo TCP em tsp.iaik.tugraz.at:318 e em dse200.ncipher.com:318.

Foram feitos testes empíricos com substituição de caracteres em partes diferentes do ficheiro gerado, em avaliação da robustez das assinaturas criadas.

Para cada documento foram registados:

- 1) A plenitude da tradução para o novo modelo, com anotação de toda a informação presente nos relatórios e que não pudesse ser traduzida, à excepção de informação presente em timbre de papel ou itens de publicidade;
- 2) Tempo de computação das assinaturas, com determinação da diferença em milissegundos entre a ordem para assinar o documento em edição e o final da verificação do documento criado. Este tempo inclui a construção da estrutura XML do documento, aposição de assinatura do autenticador legal e da organização responsável pela guarda do documento, a gravação do ficheiro e a

validação das assinaturas apostas, e decorrido o qual poderá, em condições reais, ser comunicado o sucesso na validação de assinaturas e no arquivamento;

- 3) Dimensão do ficheiro gerado, em *bytes*:
 - a. Antes de assinatura;
 - b. Após assinatura do autenticador legal;
 - c. Após assinatura e contra-assinatura;
 - d. Após assinatura, contra-assinatura e carimbo de tempo (incluindo ou não certificado da TSA);
 - e. Por cifra do documento assinado pelo autenticador legal.
- 4) Dimensão do ficheiro electrónico de suporte ao documento original (em *bytes*).

Um breve tratamento estatístico foi efectuado em folha de cálculo *Microsoft Office Excel 2003*.

5. Resultados

5.1. Funcionalidade do protótipo

Destinado a testar a estrutura do modelo, assim como dos mecanismos de assinatura, o protótipo foi construído sem preocupações de aspecto gráfico ou usabilidade. A interface permitiu no entanto a fácil introdução dos dados necessários, com utilização de *clipboard*, assim como formatação do texto introduzido, quando necessária. A utilização de comandos escalonados para as várias fases de assinatura e validação de tempo permitiu obter ficheiros nas diferentes fases do processo de autenticação.

Foi possível e fácil a aposição da assinatura digital qualificada do cartão de cidadão, assim como a verificação da sua validade. Dado que a entidade certificadora de raiz, *GTE CyberTrust Global Root*, é reconhecida de base pelo sistema operativo, não é necessário declarar confiança a nenhuma outra entidade, apenas devendo estar instalados os certificados digitais da cadeia de certificação.

Verificou-se a perda de validade da assinatura com a alteração, em qualquer ponto, do documento clínico ou das propriedades assinadas da assinatura.

A aposição de contra-assinatura permitiu a manutenção de integridade da sequência de documentos, se cumpridos os requisitos para a sua verificação definidos na norma XAdES e adiante neste trabalho, deixando de ser válida com a alteração do número de documento na sequência ou do valor da contra-assinatura do documento anterior.

Registou-se um curto período de indisponibilidade do serviço de validação cronológica do cartão de cidadão.

5.2. Plenitude de conversão de documentos

Verificou-se que, na amostra estudada, foi possível traduzir para o modelo proposto a totalidade da informação contida nos relatórios.

Nem sempre a informação do nome e endereço do departamento surge no ficheiro electrónico original (essa informação torna-se manifesta no documento em papel no seu

timbre). Por ser importante a informação do nome e endereço da organização responsável pela conservação do documento clínico electrónico, esses dados foram sempre introduzidos.

Em 3 casos o documento de origem incluía relatório de exames múltiplos, com títulos separados e com sequência narrativa distinta. A estrutura do corpo de documento criada permitiu guardar de forma explícita em secções diversas a informação relativa a cada exame.

Existiram alguns casos de utilização de formatação de texto em negrito. Não se encontrou na amostra nenhum exemplo de informação expressa em tabelas.

5.3. Tempo de computação

A computação de assinatura e contra-assinatura demorou em média 456 milissegundos (com desvio-padrão de 82 milissegundos). A correlação entre o tempo de computação e a dimensão do ficheiro gerado é apresentada na Figura 7. O coeficiente de correlação R^2 determinado foi de 0,0026.

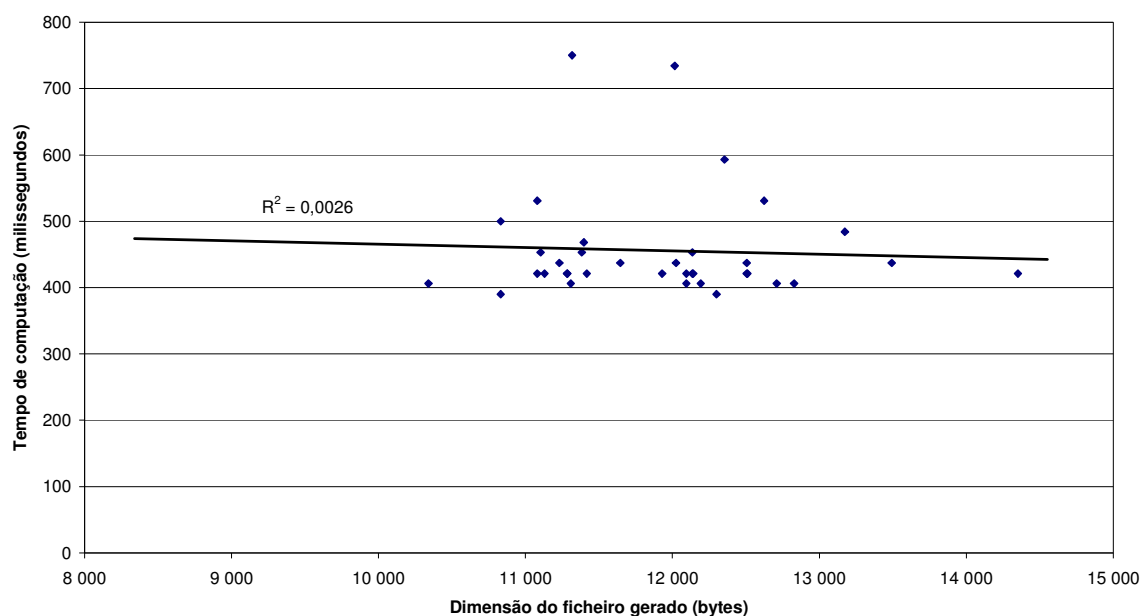


Figura 7. Correlação entre o tempo de computação e a dimensão do ficheiro gerado, após assinatura e contra-assinatura

5.4. Dimensão dos ficheiros

A dimensão dos ficheiros gerados é apresentada na Tabela 3, em confronto com a dimensão dos ficheiros electrónicos de suporte aos documentos originais. Todos aqueles se encontravam em formato *Microsoft Word 97-2003*.

Tabela 3. Dimensão (em kilobytes) dos ficheiros originais e dos ficheiros gerados no modelo

Origem do documento	Dimensão do ficheiro original (KB) ^a	Dimensão do ficheiro gerado no modelo (KB) ^a			
		Sem assinatura	Com assinatura	Com validação de tempo	
				s/certificado	c/certificado
A	43.9 ± 3.1	4.1 ± 1.0	7.1 ± 1.0	10.1 ± 0.8	12.5 ± 0.8
B	27.8 ± 1.6	4.3 ± 0.9	7.1 ± 0.9	10.2 ± 0.8	12.6 ± 0.8
C	22.5 ± 0.8	5.0 ± 0.5	8.2 ± 0.5	10.7 ± 0.5	13.0 ± 0.5
Total	31.4 ± 9.5	4.5 ± 0.9	7.5 ± 1.0	10.3 ± 0.7	12.7 ± 0.7 ^b

^a Média ± desvio-padrão

^b $p < 6.2 \times 10^{-14}$; p=probabilidade da hipótese nula (dimensão em média semelhante a ficheiro original); teste t-Student emparelhado monocaudal

A dimensão média dos ficheiros cifrados foi de 8.6 KB, com desvio-padrão de 1.1 KB.

6. Discussão

6.1. Da metodologia

Ainda que existam múltiplas iniciativas no sentido de normalizar registos e documentos clínicos, apenas as normas CDA e DICOM parecem apresentar desde já uma estrutura estável podendo servir de base a uma especificação de formato de ficheiro electrónico.

Na pesquisa efectuada a norma *Clinical Document Architecture* é largamente mais citada e existem referências a utilização no terreno, apresentando o maior potencial para se tornar um formato disseminado de um documento médico electrónico. Tem a vantagem de usar uma representação XML, de fácil implementação e legibilidade humana por utilização de aplicações ubíquas (por exemplo de processamento de texto); esta representação tem como inconveniente conhecido a sua verbosidade, originando ficheiros extensos, maiores que, por exemplo, uma representação DICOM. No seu nível mais básico a CDA apenas praticamente só define a estrutura da informação de cabeçalho, que no entanto é importante tendo em conta o objectivo de integração futura da informação contida nesses documentos em registos de saúde.

A norma DICOM é bastante dirigida à área da imagem médica e documentos com ela relacionados; o grande inconveniente será a dificuldade de implementação e a necessidade de aplicações específicas para acesso à informação.

A aposição de uma assinatura digital coloca dificuldades adicionais mas existe o reconhecimento na literatura da sua necessidade para uma coerente implantação do documento electrónico no futuro da saúde.

A escolha de uma assinatura com estrutura XML está de acordo com a estrutura do documento, com a vantagem de o conteúdo legível eventualmente facilitar a adesão ao seu uso, por mais facilmente ser compreensível o seu significado. É proposta uma assinatura XAdES com dados de validação, no formato XAdES-T.

Tendo em conta que os documentos assinados deverão suportar longos períodos de armazenamento sem perder a validade da assinatura, e que é possível que a dimensão das chaves ou os algoritmos criptográficos utilizados venham a demonstrar-se fracos, está

prevista na especificação XAdES versão 1.4.1⁸² uma forma de arquivo (XAdES-A) que permite a revalidação da assinatura com novos algoritmos ou chaves mais longas, consistindo, de modo sintético, na aposição de um carimbo de tempo sobre um *hash* reflectindo toda a parte assinada do documento, a assinatura original e os certificados das assinaturas, atributos e revogações (que são incluídos). Esta forma de validação poderá ser aplicada se houver previsão de que os algoritmos ou funções de *hash* anteriormente utilizados poderão deixar de ser seguros. A implementação desta forma implica a inclusão de novos elementos na assinatura (ou em arquivo separado, no caso de uma versão distribuída).

Não é sugerido armazenamento dos certificados digitais para cada assinatura porque se prevê uma grande repetição de certificados, poupando-se assim espaço de armazenamento. Os documentos a enviar a outras entidades deverão ser acompanhados dos certificados que permitem validação das assinaturas e carimbo de tempo, a menos que exista garantia de o receptor já os deter. Num pedido de carimbo de tempo na norma referida⁵⁸ existe opção de incluir ou não certificado. É possível formular à TSA um pedido de carimbo de tempo não acompanhado de certificados e, se não for possível a sua validação com os certificados detidos pelo requerente, formular novo pedido importando os certificados relevantes, que deverão ser guardados para posterior uso.

A construção de um encadeamento de documentos pela inclusão do elemento *ChainProperties* na contra-assinatura permitirá estabelecer uma sequência inquebrável, de forma a dificultar o desaparecimento ou substituição de documentos. Não é conveniente estabelecer essa cadeia apenas pela identificação do documento, pois esse é um dado presente no documento desde a sua criação, muito antes do seu arquivo, e deve ser previsto que alguns documentos nunca chegarão a ser incorporados no arquivo ou que tal sucederá com considerável atraso (por exemplo, um documento pode ver atrasada a sua assinatura por o autor ter dúvidas no relatório, que necessite esclarecer). Por outro lado este mecanismo reforça o papel do carimbo de tempo na validação cronológica, uma vez que cada documento sucessivo na cadeia deverá sempre ter um momento de contra-assinatura posterior. Sugere-se a aposição de carimbo de tempo sobre a contra-assinatura pois, sendo posterior à assinatura e contendo uma função de *hash* da mesma, prova que também a assinatura já existia à data do carimbo de tempo.

6.2. Dos resultados

A confirmação da adequação da assinatura na manutenção de integridade do documento era de todo esperada, tratando-se de um perfil de uma norma internacional de assinatura já bastante escrutinada. Do mesmo modo não surpreende a aplicabilidade da norma de documento clínico electrónico CDA que, com introdução de algumas particularidades, como a possibilidade de conter várias sequências narrativas no mesmo documento (permitindo relatórios de vários exames sob títulos distintos), permitiu uma conversão completa dos relatórios da amostra estudada. Ainda que apenas em 3 casos (1/12 do total) existisse uma multiplicidade de exames num documento, a impossibilidade da sua conversão poderia ser mais um factor de resistência à aceitação prática do modelo.

O elemento *ClinicalDocument* dos documentos criados está conforme a norma CDA e pode ser validado no respectivo esquema XML, utilizando por exemplo a ferramenta de validação *on-line* disponível em <http://xreg2.nist.gov/cda-validation/validation.html> (poderá ser retirado o atributo *Id* usado para referenciar a assinatura digital).

O tempo de computação da assinatura foi sempre inferior a 1 segundo, valor que parece perfeitamente aceitável e será certamente minorado em computadores mais actuais, e com implementações em *software* mais eficientes, comparativamente ao testado. De notar ainda que não existiu correlação significativa do tempo de computação com a dimensão do ficheiro gerado, sugerindo que possivelmente documentos maiores que os estudados poderão não determinar tempos de computação da assinatura mais arrastados. Estes dados permitirão afastar receios de que a aposição de uma assinatura digital venha a aumentar o tempo dispendido na validação de documentos.

Na apreciação da dimensão dos ficheiros verificou-se que os ficheiros gerados no modelo proposto são significativamente menores que os correntemente utilizados, com uma probabilidade da hipótese nula muito remota mesmo quando usados na comparação os ficheiros com validação de tempo e com inserção do certificado digital da TSA (ver Tabela 3). Se parece pouco importante esta diferença, quando pensamos que o armazenamento digital das imagens que originam estes relatórios consome espaço de memória incomparavelmente maior, da ordem das dezenas ou centenas de milhar de KB, ela não deve no entanto deixar de ser referida, já que uma das desvantagens apontadas à codificação XML é precisamente a sua verbosidade. A inclusão do certificado da autoridade de certificação temporal determinou ficheiros em média com mais 2.4 KB.

6.3. Das limitações do estudo

Tratando-se de um estudo descritivo em laboratório sobre sistema protótipo, não foi testada a aplicação no terreno, traduzindo a sua aceitação e *performance* em situações reais. A necessidade do uso de algum equipamento, na sua forma mais simples um *smartcard*, para aplicação da chave privada de assinatura, implica aceitação pelos profissionais de saúde, que em Portugal poderá necessitar mais estudos⁵⁷. Do mesmo modo não foi feita comparação com outros modelos, de documento electrónico ou de sistema de arquivo de relatórios.

Não foi avaliada a compatibilidade de documentos produzidos em aplicações distintas, e sobretudo com recurso a sistemas operativos e implementações diversas das funções criptográficas.

Embora aparentemente não problemática, não foi testada a forma de arquivo (XAdES-A), entendendo-se que provavelmente não será necessária a curto prazo, e que a sua introdução não produzirá alteração no documento base.

Não foram também abordadas as questões relacionadas com a garantia do princípio WYSIWYS, nomeadamente quanto à manutenção dos meios de criação de assinatura sob controlo exclusivo do signatário, aspecto bastante relevante sobretudo em determinados meios, como o hospitalar.

6.4. Da comparação com outros estudos

A concepção de perfis de documentos CDA para relatórios de imagem é um tema em desenvolvimento, e a organização HL7 publicou em 2009 uma versão para testes de um perfil para relatórios de imagem⁸³ que relativamente à proposta de perfil seguida neste trabalho apresenta algumas alterações; a mais significativa será a obrigatoriedade de as secções ou subtítulos de relatórios descenderem directamente do elemento *component* hierarquicamente mais elevado. No entanto esta opção impossibilitaria a inclusão de relatórios de vários exames no mesmo documento, já discutida acima, razão pela qual não foi seguida neste trabalho a versão de 2009 do perfil de documento.

A norma CDA tem também em fase de discussão uma nova versão (R3). De entre as propostas apresentadas, salientam-se aquelas que dizem respeito à introdução de assinatura digital no documento, uma sobre a introdução de um elemento *signatureText* nos

elementos relativos a participantes, no cabeçalho do documento⁸⁴, e outra advogando inclusão de assinatura digital de tipo XAdES⁸⁵.

Na revisão efectuada não foram encontrados estudos que abordem a questão da dimensão dos ficheiros XML gerados pela norma CDA, nem da avaliação da aplicabilidade prática da tradução em documentos CDA de relatórios de exames de imagem.

6.5. Da validação dos documentos

A verificação da autenticidade dos documentos deve ocorrer sempre:

- 1) Na recepção de um documento por canais de comunicação não autenticados;
- 2) Na integração do documento em sistemas de informação hospitalares ou similares;
- 3) Na apresentação dos documentos para leitura (em monitor ou impressão).

Particularmente na situação 3) interessa não só a verificação da(s) assinatura(s) como também confirmar a estrutura do documento clínico, a inclusão de informação relevante não assinada, não apresentável ou contraditória, a manutenção da sequência de documentos (no caso da validação ocorrer na organização que tem a custódia do documento e acesso aos restantes documentos da sequência) e a existência de documentos relacionados. Em 1) e 2) no mínimo deverá ser verificada a validade das assinaturas, para não propagar documentos não autênticos. Em 2) deverá ser verificado se o novo documento substitui ou é adenda de documento já existente.

6.5.1. Verificação de assinaturas

- 1) O documento deve conter no máximo uma assinatura e uma contra-assinatura, com a localização indicada no modelo;
- 2) A referência na assinatura deverá estar correctamente dirigida ao elemento *ClinicalDocument*;
- 3) A validação de assinatura e contra-assinatura seguirá as regras da especificação XAdES, como definidas no capítulo 3.2 (*Core Validation*) da especificação XMLDsig⁶⁰ e anexo G.2 (*Verification technical rules*) da especificação XAdES v.1.3.2⁸⁰. Tendo em conta o perfil de assinatura definido neste trabalho (se a assinatura utilizar um elemento *ds:KeyInfo* não está estritamente de acordo com

este modelo e deverão ser verificadas todas as regras das normas referidas), o procedimento para cada assinatura será:

- a. Obter certificado de fonte externa (identificado pelo nome de emissor e número de série nas propriedades assinadas da assinatura);
- b. Confirmar os valores de *hash* nas referências. Obter a forma canónica do método de assinatura (*ds:SignatureMethod*) usando o algoritmo especificado em *ds:CanonicalizationMethod*. Obter a forma canónica do elemento *ds:SignedInfo* e aplicar os algoritmos do método de assinatura, confirmando sobre o resultado o valor do elemento *ds:SignatureValue*;
- c. As propriedades assinadas da assinatura deverão estar presentes com os elementos descritos e existir na assinatura elemento *ds:Reference* apontando para as propriedades assinadas, com tipo *http://uri.etsi.org/01903#SignedProperties*;
- d. Confirmar que o certificado é parte de uma cadeia de certificados válida, com raiz em entidade de confiança. O estado de revogação de certificados deve ser confirmado por protocolo OCSP (ou em alternativa por listas de revogação de certificados, CRL);
- e. O tempo em que a verificação da assinatura acontece deverá ser posterior ao valor no elemento *SigningTime*;
- f. No elemento *SigningCertificate* confirmar que o valor de *ds:DigestValue* é igual à codificação *base64* do resultado da aplicação do algoritmo indicado em *ds:DigestMethod* ao certificado;
- g. Tratando-se de uma contra-assinatura, verificar que contém uma referência com tipo *http://uri.etsi.org/01903#CounterSignedSignature* apontando para o elemento *ds:SignatureValue* da assinatura;
- h. Confirmar, se existir, a validação temporal em *SignatureTimeStamp*:
 - i. Obter o carimbo de tempo (*TimeStampToken*) em codificação DER a partir da sua codificação *base64* que é o valor do elemento *EncapsulatedTimeStamp*;

- ii. Verificar a assinatura do carimbo de tempo de acordo com as regras próprias do protocolo^{58,86}, confirmando o estado de revogação dos certificados;
- iii. Obter a forma canónica do elemento *ds:SignatureValue* usando o método *ds:CanonicalizationMethod* da propriedade;
- iv. Aplicar a função de *hash* indicada no carimbo de tempo ao resultado e comparar com *hashedMessage* presente no carimbo de tempo;
- v. O tempo no carimbo de tempo deve ser posterior ao valor no elemento *SigningTime*.

6.5.2. Outras verificações

- 1) Conformidade do documento clínico:
 - a. No elemento *ClinicalDocument* devem estar presentes os elementos obrigatórios do esquema CDA, e o tipo de dados deve ser o correcto, de acordo com o esquema XML *CDA.xsd* do espaço de nomes *urn:hl7-org:v3*.
- 2) Informação não assinada, não apresentável ou contraditória:
 - a. O elemento raiz *ClinDocEnvelope* apenas deve conter o elemento *ClinicalDocument*, além da assinatura, e nenhum espaço de nomes nem atributos declarados, pois só o elemento *ClinicalDocument* é assinado;
 - b. Apenas os dois comentários definidos deverão estar presentes, pois os comentários poderão não ser assinados e não serão apresentados para leitura e assim evita-se que conteúdo eventualmente contraditório possa existir nos comentários;
 - c. Toda a informação do documento deverá ser apresentada na aplicação, e caso tal não seja possível, deverá no mínimo ser despoletado um aviso;
 - d. As datas no documento deverão ser coerentes ou seja, mantendo a sequência; $\text{data do(s) exame(s)} \leq \text{data de criação do documento} \leq \text{data de assinatura} \leq \text{data de contra-assinatura} \leq \text{data de carimbo de tempo}$.
- 3) Manutenção da cadeia de documentos:
 - a. A contra-assinatura deverá ter uma referência ao elemento *ChainProperties*;

- b. O elemento *PreviousDocSignatureValue* deverá ter valor igual ao valor de assinatura da contra-assinatura do documento antecedente;
 - c. O elemento *ArchiveSeqNumber* deverá ter valor igual ao valor de *ArchiveSeqNumber* do documento antecedente mais uma unidade;
 - d. O documento antecedente deverá ter data de contra-assinatura anterior.
- 4) Documentos relacionados:
- a. Se existir referência a um documento relacionado do tipo APND deve ser despoletada mensagem ao utilizador e o documento antecessor também apresentado. Verificar que o documento relacionado tem data de criação anterior;
 - b. Deve ser pesquisado o arquivo em busca de documentos que substituam ou sejam adenda do documento em verificação. Se existir tal documento deve ser despoletada mensagem. Em caso de substituição apenas apresentar (por defeito) o documento que substitui e em caso de existir adenda apresentar ambos os documentos.

6.6. Das aplicações

No panorama nacional presente o documento clínico electrónico, com mecanismos de assinatura intrínsecos, poderá ter uma utilização extensa, tanto em sistemas de informação hospitalares ou do departamento de imagem médica como noutras perspectivas, por exemplo no fornecimento de serviços de telemedicina, amiúde envolvendo múltiplos prestadores, obviando a necessidade de estabelecer canais seguros de comunicação, que implicam geralmente complexidade acrescida e que permitem garantir a autenticidade da informação mas carecem de mecanismos de não-repudição.

Embora o modelo de documento se pretenda válido para qualquer contexto, alguns cenários podem servir de exemplo para a sua utilização.

Numa produção de documentos integrada num sistema de informação de um departamento de imagem de maiores dimensões, com profissionais em formação (médicos internos), a sequência de eventos pode corresponder ao exemplificado na Figura 8. O dactilógrafo cria um documento a partir dos dados demográficos do examinado, dos dados do exame e do relato oral elaborado por um interno, identificado como autor, que efectua eventuais

correções e envia o documento para arquivo. O especialista, que será o autenticador legal, importa o documento, recria um documento com número diferente contendo as alterações, e assina digitalmente o documento, enviando para arquivo.

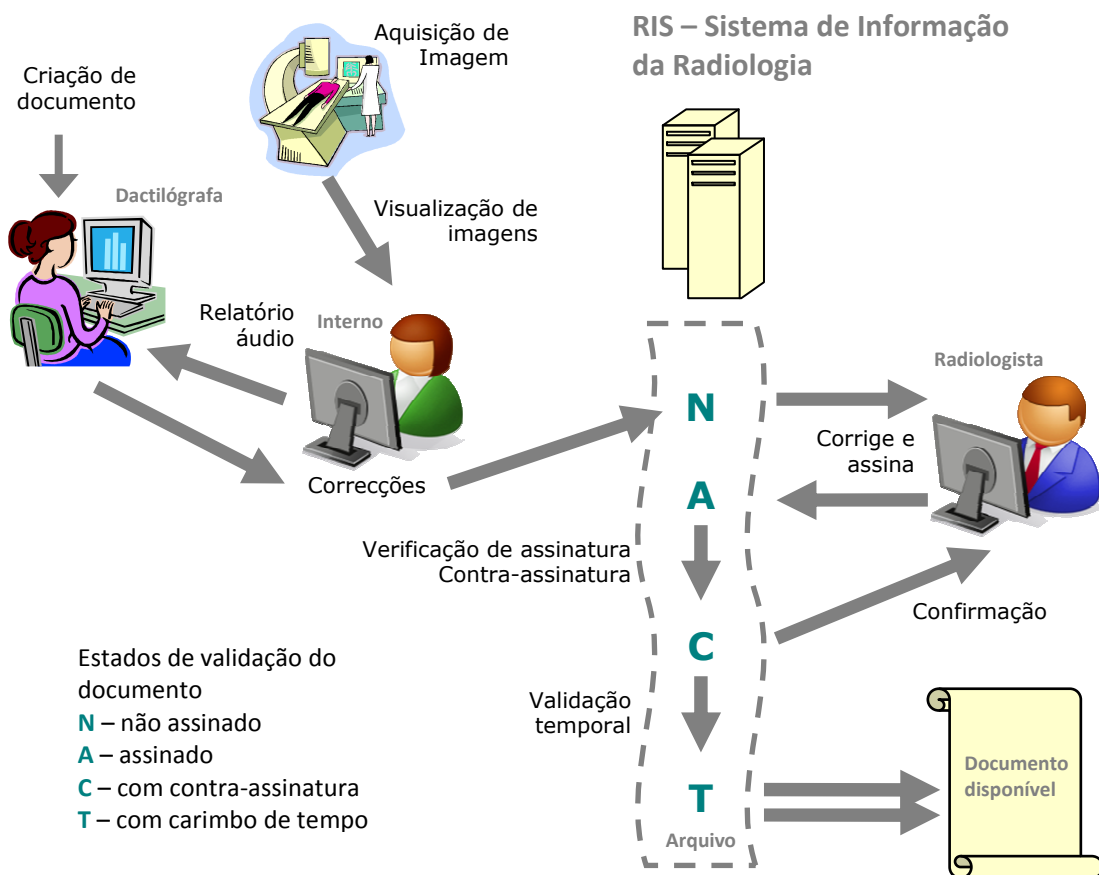


Figura 8. Sequência de procedimentos em departamento de maior dimensão, com internos

O documento e assinatura são verificados e o sistema põe uma contra-assinatura e arquiva o documento, devolvendo confirmação que o documento está assinado e arquivado. Em segundo tempo, mas num prazo curto, é adicionado carimbo de tempo. O acesso aos documentos no sistema de informação deve manter um registo de quem acede aos dados e se o documento foi disponibilizado numa forma preliminar antes de autenticação, ou se for criada uma adenda, devem ser avisados todos aqueles que já tiveram acesso ao documento.

Num contexto de telemedicina (Figura 9), o autor legal pode criar o documento e promover a sua assinatura, verificar o documento e cifrar com uma chave pública do receptor pretendido. Envia o documento por uma qualquer forma (incluindo *E-mail*). O receptor, suponhamos um hospital de menor diferenciação, decifra o documento com a sua chave

privada, verifica o documento e assinatura e apõe contra-assinatura e carimbo de tempo, arquivando o documento.

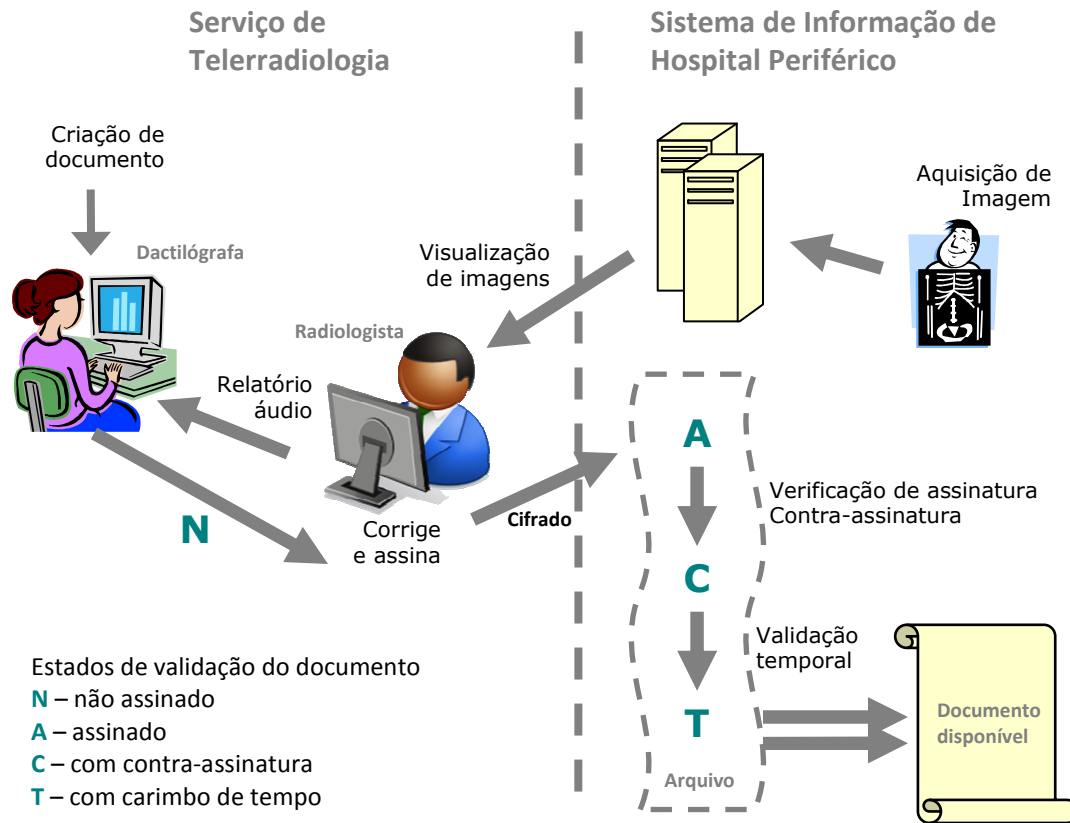


Figura 9. Sequência em caso de relato de exames por telerradiologia

7. Conclusões e recomendações

A adopção de um modelo de documento electrónico estruturado que suporte o arquivo de relatórios de imagem, assinado digitalmente, é possível com recurso a normas já universalmente aceites, e a sua implementação não é difícil e pode assentar em infra-estruturas já montadas, como a infra-estrutura de chave pública do estado e cartão de cidadão.

A conformidade com a norma CDA poderá acrescentar a vantagem da futura incorporação directa dos documentos em sistemas de informação hospital, já que aquela norma, do universo HL7, apresenta forte possibilidade de se tornar extensamente difundida. A desvantagem apontada à representação XML de verbosidade e de gerar grande volume de informação não parece ter significado neste contexto.

O uso de uma assinatura XAdES, com base em certificado digital qualificado, permite a obtenção de um documento legalmente válido perante a legislação portuguesa e europeia. A aposição de assinatura digital em documento não se prevê processo moroso, que invalide a aceitação do procedimento pelos profissionais de saúde.

A criação de uma PKI dedicada, pela ordem dos médicos, teria a vantagem de certificar também a qualificação para a função de médico e respectiva especialidade.

Face a estas conclusões, será de recomendar a rápida adopção de um modelo, como o proposto ou outro com as mesmas características que se mostre mais favorável, para que o arquivo electrónico de relatórios de imagem médica continue a garantir a segurança da informação e seja possível a interoperabilidade entre as várias entidades que prestam cuidados de saúde.

8. Trabalho futuro

O documento clínico electrónico pode, além da utilização já abordada em relatórios de exames complementares de diagnóstico por imagem, ser usado para desmaterializar notas de admissão, de alta ou de transferência, prescrição de terapêutica ou qualquer outro registo da actividade clínica.

A utilização de uma assinatura comum (como XAdES) permitirá ainda a aceitação dos documentos por intervenientes de outras áreas além da saúde, podendo vir a constituir a forma electrónica de um atestado médico.

A compatibilidade com níveis superiores de complexidade, prevista na CDA, permitirá, sem perda da informação previamente registada, uma evolução para uma maior estruturação da informação, de melhor compreensão humana, maior interoperabilidade semântica em sistemas de informação e extenso uso em investigação.

Referências

1. Thomas SM, Overhage JM, Warvel J, McDonald CJ. A comparison of a printed patient summary document with its electronic equivalent: early results. *Proc AMIA Symp.* 2001;701-5.
2. Chhanabhai P, Holt A. Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. *MedGenMed.* 2007 Jan 11; 9(1):8.
3. DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. *Official Journal of the European Communities*, 19 de Janeiro de 2000.
4. Decreto-Lei nº 290-D/99 de 2 de Agosto. *DIÁRIO DA REPÚBLICA — I SÉRIE-A*, Nº 178, Portugal, 2 de Agosto de 1999.
5. Decreto-Lei nº 62/2003 de 3 de Abril. *DIÁRIO DA REPÚBLICA — I SÉRIE-A*, Nº 79, Portugal, 3 de Abril de 2003.
6. Decreto-Lei nº 165/2004 de 6 de Julho. *DIÁRIO DA REPÚBLICA — I SÉRIE-A*, Nº 157, Portugal, 6 de Julho de 2004.
7. Decreto Regulamentar nº 25/2004 de 15 de Julho. *DIÁRIO DA REPÚBLICA — I SÉRIE-B*, Nº 165, Portugal, 15 de Julho de 2004.
8. Decreto-Lei nº 88/2009 de 9 de Abril. *DIÁRIO DA REPÚBLICA — 1ª SÉRIE*, Nº 70, Portugal, 9 de Abril de 2009.
9. Kalra D. Electronic health records: the European scene. *BMJ.* 1994 Nov 19;309(6965):1358-61.
10. Liu GC, Cooper JG, Schoeffler KM, Hammond WE. Standards for the electronic health record, emerging from health care's Tower of Babel. *Proc AMIA Symp.* 2001:388-92.
11. Eichelberg M, Aden T, Riesmeier J, Dogac A, Lacedi GB. A survey and analysis of electronic healthcare record standards. *ACM computing surveys* 2005;37(4):277-315.
12. Meystre SM, Haug PJ. Randomized controlled trial with improved sensitivity. *Int J Med Inform.* 2008 Set;77(9):602-12.
13. Li N, Yu BG. Design and implementation of the first page of electronic patient records based on HL7 clinical document architecture, R2.0. *Zhongguo Yi Liao Qi Xie Za Zhi.* 2007 Jul;31(4):263-6.
14. Klein A, Prokosch HU, Müller M, Ganslandt T. Experiences with an interoperable data acquisition platform for multi-centric research networks based on HL7 CDA. *Methods Inf Med.* 2007;46(5):580-5.
15. Doan MH, Lott PL, Václavík M, Ueckert F. K-Box: Automatic structuring and exchange of medical documents based on the clinical documentation architecture (CDA). *Stud Health Technol Inform.* 2007;129(Pt 1):513-6.
16. Blazona B, Koncar M. HL7 and DICOM based integration of radiology departments with healthcare enterprise information systems. *Int J Med Inform.* 2007 Dez;76 Suppl 3:S425-32.
17. Kush R, Alschuler L, Ruggeri R, Cassells S, Gupta N, Bain L et al. Implementing Single Source: The STARBRITE proof-of-concept study. *J Am Med Inform Assoc.* 2007 Set-Out;14(5):662-73.

18. Gerdson F, Müller S, Jablonski S, Prokosch HU. Standardized exchange of clinical documents - Towards a shared care paradigm in glaucoma treatment. *Methods Inf Med.* 2006;45(4):359-66.
19. Saadawi GM, Harrison JH Jr. Definition of an XML markup language for clinical laboratory procedures and comparison with generic XML markup. *Clin Chem.* 2006 Oct;52(10):1943-51.
20. Noumeir R. Benefits of the DICOM structured report. *J Digit Imaging.* 2006 Dez;19(4):295-306.
21. Schweiger R, Hölzer S, Dudeck J. Advanced Information Retrieval Using XML Standards. *Stud Health Technol Inform.* 2005;116:677-82.
22. Paterson GI, Abidi SS, Soroka SD. HealthInfoCDA: Case Composition Using Electronic Health Record Data Sources. *Stud Health Technol Inform.* 2005;116:137-42.
23. Blobel B. Advanced and secure architectural EHR approaches. *Int J Med Inform.* 2006 Mar-Apr;75(3-4):185-90.
24. Loeff C, Truyen R. Evidence and diagnostic reporting in the IHE context. *Acad Radiol.* 2005 Mai;12(5):620-5.
25. Poulymenopoulou M, Vassilacopoulos G. An electronic patient record implementation using clinical document architecture. *Stud Health Technol Inform.* 2004;103:50-7.
26. Müller ML, Uckert F, Bürkle T, Prokosch HU. Cross-institutional data exchange using the clinical document architecture (CDA). *Int J Med Inform.* 2005 Mar;74(2-4):245-56.
27. Müller M, Frankewitsch T, Ganslandt T, Bürkle T, Prokosch HU. The Clinical Document Architecture (CDA) enables electronic medical records to wireless mobile computing. *Stud Health Technol Inform.* 2004;107(Pt 2):1448-52.
28. Duftschmid G, Gall W. Representation of inter-patient relations within electronic healthcare record architectures. *Med Inform Internet Med.* 2004 Mar;29(1):1-14.
29. Hussein R, Engelmann U, Schroeter A, Meinzer HP. DICOM structured reporting: Part 1. Overview and characteristics. *Radiographics.* 2004 Mai-Jun;24(3):891-6.
30. Noumeir R. DICOM structured report document type definition. *IEEE Trans Inf Technol Biomed.* 2003 Dez;7(4):318-28.
31. Johnson SB, Campbell DA, Krauthammer M, Tulipano PK, Medonca EA, Friedman C et al. A native XML database design for clinical document research. *AMIA Annu Symp Proc.* 2003:883.
32. Meystre S, Haug PJ. Medical problem and document model for natural language understanding. *AMIA Annu Symp Proc.* 2003:455-9.
33. Müller ML, Butta R, Prokosch HU. Electronic discharge letters using the Clinical Document Architecture (CDA). *Stud Health Technol Inform.* 2003;95:824-8.
34. Rau WS, Schwabe C. Wish and reality in installation of a clinic-wide system for image and documentation access. *Radiologe.* 1999 Apr;39(4):304-9.
35. Schramm M, Clausen M, Wolf H, Brenner W, Bohuslavizki KH, Eberhardt JU, Henze E. DACS - A cost-advantageous nuclear medical document archiving and communication system. *Nuklearmedizin.* 1995 Oct;34(5):185-91.
36. Dolin RH, Alschuler L, Boyer S, Beebe C, Behlen FM, Biron PV et al. HL7 Clinical Document Architecture, Release 2. *J Am Med Inform Assoc.* 2006 Jan-Feb;13(1):30-9.
37. Dolin RH, Alschuler L, Beebe C, Biron PV, Boyer SL, Essin D et al. The HL7 Clinical Document Architecture. *J Am Med Inform Assoc.* 2001 Nov-Dec;8(6):552-69.

38. Hussein R, Engelmann U, Schroeter A, Meinzer HP. DICOM Structured Reporting Part 2. Problems and challenges in implementation for PACS workstations. *Radiographics*. 2004 Mai-Jun;24(3):897-909.
39. Zhao L, Lee KP, Hu J. Generating XML schemas for DICOM structured reporting templates. *J Am Med Inform Assoc*. 2005 Jan-Fev;12(1):72-83.
40. National Electrical Manufacturers Association. Digital Imaging and Communications in Medicine (DICOM) Digital Signature. 2001. Standards Publication PS3 Supplement 41. Obtido de ftp://medical.nema.org/medical/dicom/final/sup41_ft.pdf, 17 de Julho de 2009.
41. National Electrical Manufacturers Association. Digital Imaging and Communications in Medicine (DICOM) Part 15: Security and System Management Profiles. 2008. Obtido de ftp://medical.nema.org/medical/dicom/2008/08_15pu.pdf, 16 de Fevereiro de 2009.
42. Schütze B, Kroll M, Geisbe T, Braun M, Filler TJ. Does the digital signature of the DICOM standard meet the requirements of German law? *Radiologe*. 2003 Ago;43(8):665-70.
43. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978 Fev;21(2):120-6.
44. Diffie W, Hellman M. New directions in cryptography. *IEEE Trans. Inform. Theory*. 1976 Nov;22(6):644-54.
45. RSA Laboratories. PKCS #7: Cryptographic message syntax standard. 1993 Nov; Version 1.5. Obtido de <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc>, 17 de Julho de 2009.
46. Housley R, Polk W, Ford W, Solo D. Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile. 2002 Abr. Obtido de <http://www.ietf.org/rfc/rfc3280.txt>, 8 de Novembro de 2010.
47. Callas J, Donnerhake L, Finney H, Shaw D, Thayer R. OpenPGP Message Format. 2007 Nov. Obtido de <http://www.ietf.org/rfc/rfc4880.txt>, 8 de Novembro de 2010.
48. Toorani M, Shirazi AAB. LPKI - A Lightweight Public Key Infrastructure for the Mobile Environments. *Proceedings of the 11th IEEE International Conference on Communication Systems (IEEE ICCS'08)*. 2008 Nov:162-6.
49. Adams C, Farrell S, Kause T, Mononen T. Internet X.509 Public Key Infrastructure - Certificate Management Protocol (CMP). 2005 Set. Obtido de <http://www.ietf.org/rfc/rfc4210.txt>, 8 de Novembro de 2010.
50. Myers M, Ankney R, Malpani A, Galperin S, Adams C. X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP. 1999 Jun. Obtido de <http://www.ietf.org/rfc/rfc2560.txt>, 8 de Novembro de 2010.
51. Microsoft. U.S. Government Configuration Baseline (USGCB) - Windows XP vs. Windows Vista and Windows 7. Obtido de <http://www.microsoft.com/industry/government/solutions/fdcc>, 8 de Novembro de 2010.
52. International Organization for Standardization. ISO/IEC 7810. Identification cards - Physical characteristics. 2003.
53. Projecto Cartão de Cidadão. Manual técnico do Middleware Cartão de Cidadão. Versão 1.0. Julho de 2007. Obtido de http://www.cartaodecidadao.pt/images/stories/manual%20t%E9cnico%20do%20middleware%20do%20cc_v1%200.pdf, 30 de Outubro de 2010.
54. Projecto Cartão de Cidadão. Especificações - Leitor Base. Versão 1.0. 14 de Junho de 2007. Obtido de http://www.cartaodecidadao.pt/images/stories/especificacoes%20%20leitores%20base_v1.0.pdf, 30 de Outubro de 2010.

55. CEN workshop agreement 14169. Secure signature-creation devices “EAL 4+”. Março 2004. Obtido de <ftp://213.246.200.179/PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf>, 13 de Novembro de 2010.
56. Decreto-Lei nº 116-A/2006 de 16 de Junho. DIÁRIO DA REPÚBLICA — I SÉRIE-A, Nº 115, Portugal, 16 de Junho de 2006.
57. Santos R, Correia ME, Antunes L. Securing a Health Information System with a Government Issued Digital Identification Card. 42nd Annual 2008 IEEE International Carnahan Conference On Security Technology. Out 2008: 135-41.
58. Adams C, Cain P, Pinkas D, Zuccherato R. Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP). 2001 Ago. Obtido de <http://www.ietf.org/rfc/rfc3161.txt>, 8 de Novembro de 2010.
59. ITU-T Recommendation X.690 (ISO/IEC 8825-1). Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). 2003.
60. W3C World Wide Web Consortium. XML Signature Syntax and Processing (Second Edition). 2008 Jun 10. Obtido de <http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/>, 28 de Abril de 2010.
61. Josang A, Alfayyadh B. Robust WYSIWYS: A method for ensuring that what you see is what you sign. In Proc. Sixth Australasian Information Security Conference (AISC 2008), Wollongong, NSW, Australia. CRPIT, 81. Brankovic, L. and Miller, M., Eds. ACS. 53-58.
62. Weber A. See What You Sign: Secure Implementations of Digital Signatures. Proceedings of the International Conference on Intelligence and Services in Networks. 1998:509-520.
63. W3C World Wide Web Consortium. XML Advanced Electronic Signatures (XAdES). 2003 Fev 20. Obtido de <http://www.w3.org/TR/2003/NOTE-XAdES-20030220/>, 17 de Julho de 2009.
64. Pinkas D, Pope N, Ross J. CMS Advanced Electronic Signatures (CAAdES). 2008 Fev. Obtido de <http://www.ietf.org/rfc/rfc5126.txt>, 8 de Novembro de 2010.
65. Smart Card Alliance. HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements. Princeton Junction. 2003.
66. Smith JP. Authentication of digital medical images with digital signature technology. Radiology 1995; 194:771-4.
67. Zuckerman AE. Restructuring the electronic medical record to incorporate full digital signature capability. Proc AMIA Symp. 2001:791-5.
68. IHE. IHE Technical Framework Supplement – Document Digital Signature Content Profile. 2008. Obtido de http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF-Supplement_Digital_Signature-2008-10-10.pdf, 16 de Fevereiro de 2009.
69. Brandner R, van der Haak M, Hartmann M, Haux R, Schmücker P. Electronic signature for medical documents - Integration and evaluation of a public key infrastructure in hospitals. Methods Inf Med. 2002;41(4):321-30.
70. Pangalos G, Mavridis, C. Ilioudis, C. Georgiadis. Developing a Public Key Infrastructure for a Secure Regional e-Health Environment. Methods Inf Med 2002; 41: 414–8.
71. Bourka A, Kaliontzoglou A, Polemi D, Georgoulas A, Sklavos P, “PKI-based security of electronic healthcare documents”, SSGRR 2003w, International Conference on advances in infrastructure for electronic business, science, education, medicine and mobile technology. Itália. Jan 2003.

72. Pharow P, Blobel B. Electronic signatures for long-lasting storage purposes in electronic archives. *Int J Med Inform.* 2005;74:279-87.
73. Payne T, Graham G. Managing the life cycle of electronic clinical documents. *J Am Med Inform Assoc.* 2006;13(4):438–445.
74. Corn M. Archiving the phenome: clinical records deserve long-term preservation. *J Am Med Inform Assoc.* 2009;16(1):438.
75. W3C World Wide Web Consortium. XML encryption syntax and processing. 2002 Dez 10. Obtido de <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>, 17 de Julho de 2009.
76. W3C World Wide Web Consortium. Extensible Markup Language (XML) 1.0 (Fifth Edition). 2008 Nov 26. Obtido de <http://www.w3.org/TR/2008/REC-xml-20081126/>, 5 de Maio de 2010.
77. HL7. HL7 Clinical Document Architecture, Release 2.0. 2005 Set 25. Obtido de <http://www.hl7.org>, 21 de Abril de 2010.
78. HL7. Implementation Guide for CDA Release 2 – Diagnostic Imaging Report (Committee Draft for) 1st Informative Ballot. 2007 Set 16. Obtido de http://medical.nema.org/Dicom/minutes/WG-06/2007/2007-10-29/WG-20_DiagnosticImagingReportForCdaRelease2Level1to3V04.22b.doc, 21 de Abril de 2010.
79. W3C World Wide Web Consortium. HTML 4.01 Specification. 1999 Dez 24. Obtido de <http://www.w3.org/TR/1999/REC-html401-19991224/>, 11 de Maio de 2010.
80. European Telecommunications Standards Institute. XML Advanced Electronic Signatures (XAdES) - ETSI TS 101 903 V1.3.2. 2006 Mar. Obtido de <http://uri.etsi.org/01903/v1.3.2>, 11 de Maio de 2010.
81. Kaliski B, Staddon J. PKCS #1: RSA Cryptography Specifications, Version2.0. 1998 Out. Obtido de <http://www.ietf.org/rfc/rfc2437.txt>, 11 de Maio de 2010.
82. European Telecommunications Standards Institute. XML Advanced Electronic Signatures (XAdES) - ETSI TS 101 903 V1.4.1. 2009 Jun. Obtido de <http://uri.etsi.org/01903/v1.4.1>, 11 de Maio de 2010.
83. HL7. Implementation Guide for CDA Release 2: Imaging Integration. Release 1.0. 2009 Mar. Obtido de <http://www.hl7.org>, 21 de Abril de 2010.
84. Singureanu I. Digital signature for header participations - author, authenticator, legalAuthenticator. 2009 Nov 17. Obtido de http://wiki.hl7.org/index.php?title=Digital_signature_for_header_participations_-_author%2C_authenticator%2C_legalAuthenticator, 22 de Novembro de 2010.
85. Canu N (HL7 France). CDA R3 Electronic signature. 2009 Nov 18. Obtido de http://wiki.hl7.org/index.php?title=CDA_R3_Electronic_signature, 22 de Novembro de 2010.
86. Housley, R. Cryptographic Message Syntax. 2002 Ago. Obtido de <http://www.ietf.org/rfc/rfc3369.txt>, 8 de Novembro de 2010.

Anexos

A. Exemplo de documento assinado, com contra-assinatura da organização responsável pela guarda e carimbo de tempo, incluindo certificado da TSA

```
<?xml version="1.0" encoding="UTF-8"?>
<ClinDocEnvelope>
  <ClinicalDocument xmlns="urn:h17-org:v3" xmlns:voc="urn:h17-org:v3/voc"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Id="ClinicalDocument">
    <!--CDAHeader-->
    <realmCode code="uv" />
    <typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040" />
    <templateId root="2.16.840.1.113883.10" extension="CDAR2_II_BIMGRPTS_R1" />
    <id extension="1" />
    <code code="18748-4" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Diagnostic Imaging Report" />
    <title>Relatório de Imagem Médica</title>
    <effectiveTime value="20101130" />
    <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25" />
    <languageCode code="pt-PT" />
    <recordTarget>
      <patientRole>
        <id extension="99999999" />
        <addr>
          <streetAddressLine>Av. Liberdade</streetAddressLine>
          <streetAddressLine>Nº 2345</streetAddressLine>
          <city>Lisboa</city>
          <postalCode>1000 Lisboa</postalCode>
        </addr>
        <patient>
          <name>
            <given>Paciente</given>
            <family>Fictício</family>
          </name>
          <administrativeGenderCode code="M" codeSystem="2.16.840.1.113883.5.1"
/>>
            <birthTime value="19601115" />
          </patient>
        </patientRole>
      </recordTarget>
      <author>
        <time value="20101127" />
        <assignedAuthor>
          <id nullFlavor="NI" />
          <assignedPerson>
            <name>
              <given>Radiologista</given>
              <family>Fictício</family>
            </name>
          </assignedPerson>
        </assignedAuthor>
      </author>
      <dataEnterer>
        <time value="20101127" />
        <assignedEntity>
          <id nullFlavor="NI" />
          <assignedPerson>
            <name>
              <given>XXX</given>
              <family>XXXXX</family>
            </name>
          </assignedPerson>
        </assignedEntity>
      </dataEnterer>
      <custodian>
        <assignedCustodian>
```

```

    <representedCustodianOrganization>
      <id extension="CRF" />
      <name>Clínica Radiológica Fictícia</name>
      <addr>
        <streetAddressLine>Alameda das Áleas</streetAddressLine>
        <streetAddressLine>Nº4444</streetAddressLine>
        <city>Odivelas</city>
        <postalCode>2675 Odivelas</postalCode>
      </addr>
    </representedCustodianOrganization>
  </assignedCustodian>
</custodian>
<informationRecipient>
  <intendedRecipient>
    <informationRecipient>
      <name>
        <given>Médico</given>
        <family>Fictício</family>
      </name>
    </informationRecipient>
  </intendedRecipient>
</informationRecipient>
<legalAuthenticator>
  <time value="20101130" />
  <signatureCode code="S" />
  <assignedEntity>
    <id extension="99999" />
    <code displayName="Médico Radiologista" />
    <assignedPerson>
      <name>
        <given>Radiologista</given>
        <family>Fictício</family>
      </name>
    </assignedPerson>
    <representedOrganization>
      <id extension="CRF" />
      <name>Clínica Radiológica Fictícia</name>
      <addr>
        <streetAddressLine>Alameda das Áleas</streetAddressLine>
        <streetAddressLine>Nº4444</streetAddressLine>
        <city>Odivelas</city>
        <postalCode>2675 Odivelas</postalCode>
      </addr>
    </representedOrganization>
  </assignedEntity>
</legalAuthenticator>
<participant TypeCode="REF">
  <associatedEntity classCode="PROV">
    <associatedPerson>
      <name>
        <given>Médico</given>
        <family>Fictício</family>
      </name>
    </associatedPerson>
  </associatedEntity>
</participant>
<documentationOf>
  <serviceEvent classCode="ACT">
    <effectiveTime>
      <low value="20101127" />
    </effectiveTime>
  </serviceEvent>
</documentationOf>
<!-- CDABody -->
<component>
  <structuredBody>
    <component>
      <section>
        <code code="18748-4" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Diagnostic Imaging Report" />
        <title>Ecografia Abdominal</title>
        <component>
          <section>
            <code code="18785-6" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Reason for study" />
            <title>Motivo do exame</title>
            <text>Náuseas e vômitos.<br /></text>
          </section>
        </component>
      </section>
    </component>
  </structuredBody>
</component>

```

```

        </section>
    </component>
    <component>
        <section>
            <code code="18782-3" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Study observation" />
            <title>Leitura e interpretação</title>
            <text>Fígado de dimensões normais, contornos regulares e
ecostrutura homogênea.<br />Vias biliares intra e extra hepáticas não
dilatadas.<br />Vesícula biliar de parede fina, sem sinais de litíase.<br
/>Pâncreas e baço de morfologia e dimensões normais.<br />Ausência de líquido
livre intra-peritoneal.<br /></text>
        </section>
    </component>
    <component>
        <section>
            <code code="19005-8" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="X-ray impression" />
            <title>Impressão diagnóstica</title>
            <text>Exame sem alterações valorizáveis.<br />ESPÉCIMEN PARA
TESTES.<br /></text>
        </section>
    </component>
</section>
</component>
<component>
    <section>
        <code code="18748-4" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Diagnostic Imaging Report" />
        <title>TC Torácica, Abdominal e Pélvica</title>
        <component>
            <section>
                <code code="18785-6" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Reason for study" />
                <title>Motivo do exame</title>
                <text>Náuseas e vômitos.<br /></text>
            </section>
        </component>
        <component>
            <section>
                <code code="55111-9" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Current imaging procedure descriptions" />
                <title>Protocolo técnico</title>
                <text>Estudo efectuado antes e após administração e.v. de
contraste iodado.<br /></text>
            </section>
        </component>
        <component>
            <section>
                <code code="18782-3" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="Study observation" />
                <title>Leitura e interpretação</title>
                <text>No mediastino não se identificam adenomegalias.<br />A
árvore traqueo-brônquica proximal está permeável e de calibre mantido.<br />No
parênquima pulmonar não se observam alterações valorizáveis de densidade.<br
/>Ausência de derrame pleural.<br />Fígado de dimensões normais e opacificação
homogênea. Não se observam dilatações das vias biliares.<br />Pâncreas e baço de
morfologia e dimensões normais.<br />Rins de dimensões normais, com opacificação
simétrica e sem dilatações pielo-caliciais, nem sinais de litíase.<br />Segmentos
visualizados do tubo digestivo e glândulas supra-renais sem alterações.<br
/>Ausência de líquido livre intra-peritoneal.<br />Não se identificam
adenomegalias nas grandes cadeias abdomino-pélvicas.<br />Restantes aspectos
pélvicos sem alterações valorizáveis.<br /></text>
            </section>
        </component>
        <component>
            <section>
                <code code="19005-8" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC" displayName="X-ray impression" />
                <title>Impressão diagnóstica</title>
                <text>Exame dentro dos limites da normalidade.<br />ESPÉCIMEN
PARA TESTES.<br /></text>
            </section>
        </component>
    </section>
</component>
</structuredBody>

```

```

    </component>
  </ClinicalDocument>
  <ds:Signature Id="ClinicalDocumentSignature"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xm1-
c14n-20010315#withComments" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
/>
      <ds:Reference URI="#ClinicalDocument">
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>tTB+dAZOfpG4EAG6E/Roe7V27Y4=

```



```

        </SignatureTimeStamp>
      </UnsignedSignatureProperties>
    </UnsignedProperties>
  </QualifyingProperties>
</ds:Object>
<ds:Object>
  <chainp:ChainProperties
xmlns="http://uri.etsi.org/01903/v1.3.2#"
xmlns:chainp="http://fc.up.pt/MIM3/ChainProperties#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Id="CounterSignatureChainProperties" Target="#CounterSignature">
    <chainp:ArchiveSeqNumber>311</chainp:ArchiveSeqNumber>

    <chainp:PreviousDocSignatureValue>YZjqDrNqnMeXwJS+o9feP2b3/w4xU1BzkFDvI9+76evL7Dm
05VFemyfjPLGyNrEpeHailJMJPNcYzw7nMQXXznYcteY6ksuGokTEIQhAYkkxbKBaDRHdsUZ1VgBeOXGN
LSPetZAU1LvQ+Td51MDIk7Zws+4Jo5t6FJ0AN0svT+Q=</chainp:PreviousDocSignatureValue>
  </chainp:ChainProperties>
</ds:Object>
</ds:Signature>
</CounterSignature>
</UnsignedSignatureProperties>
</UnsignedProperties>
</QualifyingProperties>
</ds:Object>
</ds:Signature>
</ClinDocEnvelope>

```

B. Versão cifrada do exemplo apresentado no anexo A

```
<?xml version="1.0" encoding="UTF-8"?>
<EncryptedData xmlns="http://www.w3.org/2001/04/xmldsig#">
  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmldsig#rsa-oaep-
    mgf1p" />
  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <KeyName>Receptor de Documento Encriptado</KeyName>
  </KeyInfo>
  <CipherData>
    <CipherValue>VcBs4hI7fGT+Q3p5znfBIQ8ZEPde1d0USOYiRyRq7paJBS/vAwHv9hA83Dm1EUQMwJST
    PBZlhpQ0SejKZpxSyBz00oGTZ906B/lqxwaxKx4so1H4Q5ekwvt9IBWYzW3T3hiEW/HZMBJpzyBkQxHhT
    Nwk2xs6vcZZVhoshsvu7Qg=</CipherValue>
  </CipherData>
</EncryptedData>
</KeyInfo>
<CipherData>
  <CipherValue>u5qJ+ku30Y++fBAiMmLCJGEOS09fqkw+iVeLlAfgM+Q/Gv2XAONq3/8BMMeUSpSpckdz
  mH8abzefHjdJw8djw712bd2UEJihzqvW0Z32wvL17CJICZRUxdndt5/Gvjwzjcf7aJYZZQhzehN6FfnJW
  aystYmi+zS66oMJ2k8CRSOKwOUF25QyST0YCqkHDFBkhWfSb76q3BQrLxbReRbx/ZgGkgm+cwtqc8GmV7
  9pUvGhml7+h48pLzEx2g739zyvXzrS80Ek+tbEjTizy0Tq2NrD04xETkzuOrnbYFQBymGznp8YFv5+lC5
  20pADzim7xasNbi70Njwo8hZ6trj25qSocGMxxtf2jEbNPZwWS64mo81RDzTuvdy+1yPoClrzRxlDPNH
  CWKjsw/rkJKQt7p+azIZ5SmGC+Y76UZ+s3GaNUbjq/9R8/tl/dLYzhPQsfHERGGforFg1NqouE5eImF1c
  287zve7djd1UTvTqBUKX85fjERPO39YNeUGYDydxXorurTqmQ8oQokL4ev+eGBZ1XnoHkQVAXcTWgo1
  MBx0bHfBzQxwRvP/hwwxSbm4Q8cnpNR9sj6MmmqSbxeJ4M9CthVhozi9kGyk6RY93axqwtUCdi9whOCX1
  K6z1uJwT5xHMG8s590AZ7TPrKNf7dxaG1jIhInD8jws/9lslxqNLuocz114/nmmz7xptDnj2jjvpp14j9
  bBfpjeTAz+4xanwo86jjTeo/LjdHH1zXTGQYnX51lCh3cPCscf9PQ5vN7iitga6CoMLuPyYWIHvgTgfqE
  XCneYiwnBAMZMQdn1DjVsIhd5/l8g0fp4jbdmTtw39UwacwR0Qc629v11/2yiFeQj47dmwvtlopI9DKwc
  zUvoRLGG1QxQsGQ0/NitmjzRZoJTJz1MvR4DIXW+RBnEVOT0w695wgfvacTSgwVoY1AAHTdDua4vTDuko
  X4i5Wc0TgVue+PRFgPxsfwyu1GEQFsj7Y5cFdbGSCxURGBGNRXzdpYCsXZ8o0jmutTRN2YNAIHfq9Lbd
  cLcdZiU7fYkBe/XZCSocJPxgDg44d0TpeUAYnW2ZgC6LLR9JCckueZOBzHAWqVpyo+yJum6HbJPDze+4/qu6
  dYw6RKNDTrty55y00ZpFhjz9d+50ABC6bskftXCWtAXwAkhAESoCbMD489NYPysXMQ14n3tmy04w4vM
  v/W1VHH8m3q1sJevR4YUfhgFuj32eQnTh064/i5v2+XRpv1JFOqu4BPLKrVeVNF10SAypOMnkxee6Gj4y
  +dIxs4hu7NBSvYwmybe5sdc2xsfGd9ED8TXlgrBBBkccq30Q/H1lwikZvtvy5m50Lwqkea6Qa+ckoaFhy
  eMHZ7143UM89/i+smtMybcei6763GhzG+dR/okbSXPm8ZTLd+80tCDQ0zwcxLG0+rSEJGUyBSKhy+5FVa
  18h2AmOTrxNgwrgPVuT7jt0oBlvt08xY8i3PcowDxSctuiFWU0nv95P7TY9Lmw0xRXixAy0x0wri9Aguz
  5NwATPFH8TLmR45DFvSa8rF4/1uFasXtyG5ZxMSC/TEskiMFSpYAgzIbxbNW24DoKAZ+UCjpUjp7YrNd
  TRKTw6fCy8EbGdxCtdvc+1Khmu0/DdeTDHKS2hwnFDxh1qmmvys+7ERCexdJpX6SMstc3DXqP2RyVme1x
  6ns95Gkp1pfmt+x0lFtquz5F1xv6pBQu+ORknL25Lz7WjszZ02M4NMrh/jTXbs2Nc1JX5T64kbZkDXUA
  8t5HexMk1N3lWlLkeAyaHBtTcs89jYma3nbtDxqIp0/i3I9Q9NvPRLU1HIyE0eE8YhI10gUrZLKU2mNMO
  7EvxMu1ETSRChhVakvIT9Z4zqeDH2MBbtYTLRx4EkFbQqualpG5S5x8MSH2vH50z3ctxsS9oRo5Fdxvum8
  3TszadGr9T3Vq1fKxsAS2tAJ4c4+nyDTHVesaJ53eyiRAoix/dQ0h8EES5HRhok1s8srDHHs9fy7Mywc
  3BP+YtKqyu+Anl1SCrc7P82zyNwz1Jsv0AynW2ZgC6LLR9JCckueZOBzHAWqVpyo+yJum6HbJPDze+4/qu6
  c0D3JyMQieomzjpvPuEdrTvedtdPIHf1vbsq8fjxf1L76eYJDWQGXMy7zmbR37LifXJfBwRPXLWqKmk
  TIEcQayuwY1fM5iicWH5ChisNREXmKrINRDXzOV3qvWvdbD8rzyCnL+MjgACR4B/TfPfvwbr0wUmKA34
  mwlog9kunsgs38PqL5DTUW/j5fCgcxpEzWNjNHY6cP6Nagjb+GCv8zcbQbQ8aiHbUADYao9eDKgZWTPuq
  4ngaTi4dQARqQuvceEj17s10CnDaks7/UzqQ41iSRbDmmNtI83kmCB6svkw8U/turrdwaIOJguI8Jw1ijN
  482h631Toopm8yg8jYFq60AKASH6VQZ9jBcr45gV1w5v7whxunfZnHR152h59npYXBQyrGbOPRDKKIj/
  iip736s5GmN00Iq9kaNEVZIGcPCGvM4VulywG+LybcM2X2ECABoLW2pvQwyiwzk94D5Yunvx8vf3hae2H
  uYDrfBY8R5EGCwhIka1woDBq7SNU3pn/Dcycdb/+hqEknvkuwb395jZxwp5ek6MrbmneEwwfS87Ac842K
  57jqbzZfYMYQ8XjJAaskGbdyhcFsmRUISTcf+kyaxAh2RihSMmZc2efVrytFNR74IjEGJqctVw2XKwzi
  3o7F3zp/CarZCj1qsSPQxTfh4gvhGiNwFuBQy5Fu0uFzc80xOtxsqG1KIYKL1k3+cnOrzjZaAE2Hd+aLZ
  1FHkC5n+kys/pM3Ry98ng11211Tehq9zPLpgpU3oFV/DaePPrc1MMH1CY6IzkurLay+4sLN6mKuYsGogX
  +Sa3CrcfWDLFdChYt6I7HxwGmie4J9e8k7MjKcsN4F+F2sjB7nioqlkupyqf3WpErpOxtZHI5Z4eQrEcB
  vQFGIqQRrCuVsupMdo5xyfwUMr5bT494zyq+HMAwwKE6wZk062AMPcGwiL98gdROg0ouUws1g5tMtEstb
  pQayGX8Bqh4dJc6aACeu+OATZrxohEaIaCU2hoLHQrioVHDMcd4YpohBmNt6K0JBz8TcWwPvr+2TcxcdD
  r1mLkr5e7exJUVNjYfs91p4EOYucUUYGwx1fhaICHW9qLfsHkWDzFinzh1w2D1UHGR9j+UkhLosyKVK41
  [...truncado...]
```

```
hQwwxT5YqmoDGTi5Fueo1l6KNwDxdFTT326NNOGSvs1BfPjp4/omvgrG6rvvCiF70j18jaRrauVdCKTrw
Zxma+iJxm0jT3GUiQzB7sctqNeN08WT1D9fMag6bHHSR6GVP2xc1xvPRTQV+JJ6p1Swo518TN8KaRX+yq
Yjvw15Qq1XpSS0v+U3iClmVA/Nse3ww6ebuzpa8mtu8rk6cBh4YoyJqWFNeilKmJ6Xu8ny+ooE8ctDBm
kj0/Bm3MB43L1NRM5wvGA4ockq0cqVgpdP4BxjiZdVmx2/ltib5xvokuJmGQ+rbsxqe=</CipherValue>
</CipherData>
</EncryptedData>
```

C. Definição de esquema para o elemento ChainProperties

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://fc.up.pt/MIM3/ChainProperties#"
xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:chainp="http://fc.up.pt/MIM3/ChainProperties#"
elementFormDefault="qualified">

  <element name="ChainProperties" type="chainp:ChainPropertiesType"/>
  <complexType name="ChainPropertiesType">
    <sequence>
      <element name="ArchiveSeqNumber" type="integer"/>
      <element name="PreviousDocSignaturevalue" type="base64Binary"/>
    </sequence>
  </complexType>
</schema>
```