PROCESSO DE CERTIFICAÇÃO DE SISTEMAS DE REGISTRO ELETRÔNICO DE SAÚDE NO BRASIL: UMA ABORDAGEM ABRANGENTE E OS PRINCIPAIS DESAFIOS

Bruno Gomes de Araújo
Laboratório de Inovação Tecnológica em Saúde (LAIS) - Hospital Universitário Onofre Lopes (HUOL). Departamento de Engenharia de Computação e Automação – Universidade Federal do Rio Grande do Norte (UFRN). Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN), Câmpus Santa Cruz.
bruno.gomes@ifrn.edu.br
Ricardo Alexsandro De Medeiros Valentim
Laboratório de Inovação Tecnológica em Saúde (LAIS) - Hospital Universitário Onofre Lopes (HUOL); Departamento de Engenharia Biomédica – Universidade Federal do Rio Grande do Norte (UFRN). ricardo.valentim@ufrnet.br
Helio Roberto Hekis
Laboratório de Inovação Tecnológica em Saúde (LAIS) - Hospital Universitário Onofre Lopes (HUOL). Departamento de Engenharia de Produção – Universidade Federal do Rio Grande do Norte (UFRN). hekis1963@gmail.com
José Diniz Júnior
Laboratório de Inovação Tecnológica em Saúde (LAIS) - Hospital Universitário Onofre Lopes (HUOL). Centro de Ciências da Saúde – Universidade Federal do Rio Grande do Norte (UFRN). diniz@ufrnet.br
Francis Solange Vieira Tourinho
Laboratório de Inovação Tecnológica em Saúde (LAIS) - Hospital Universitário Onofre Lopes (HUOL). Centro de Ciências da Saúde, Departamento de Enfermagem – Universidade Federal do Rio Grande do Norte (UFRN). francistourinho@ufrnet.br
Robinson Luís de Souza Alves
Laboratório de Inovação Tecnológica em Saúde (LAIS) - Hospital Universitário Onofre Lopes (HUOL). Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN). robinson.alves@ig.com.br

RESUMO
O artigo tem como objetivo apresentar uma visão geral sobre o processo de Certificação de Sistemas de Registro Eletrônico de Saúde no Brasil, e listar os principais desafios enfrentados atualmente. Devido a crescente informatização dos processos que antes eram feitos de forma manual, existe uma constante busca pela segurança dos dados e processos envolvidos. Sistemas que manipulam informações importantes, sigilosas ou documentos eletrônicos que devem possuir validade jurídica, devem assegurar aos usuários a Autenticação, Confidencialidade, Integridade e o Não-repúdio dos dados. Neste sentido, várias técnicas são utilizadas atualmente, entre elas a Certificação Digital. Esta técnica consiste na emissão de um Certificado Digital, com informações que garantem a autenticidade de uma das entidades da comunicação, servindo como um documento de identificação eletrônico. No Brasil, os certificados digitais são emitidos pela ICP-Brasil. Este método já vem sendo utilizado na área da saúde, por exemplo, o CRM Digital, que consiste em um *smart card* que armazena um certificado com informações que identificam o médico. Mas, não basta a utilização desta técnica para que os sistemas na área da saúde

sejam legalizados para serem utilizados no ambiente hospitalar, é preciso, além da segurança das informações, a garantia de que as suas funcionalidades estejam em completo funcionamento, pois estão relacionadas com informações e procedimentos importantes sobre a saúde dos pacientes, e qualquer erro pode comprometê-las. A partir disto, destaca-se a criação do processo de Certificação de Sistemas de Registro Eletrônico de Saúde, que consiste em uma verificação de conformidade dos sistemas baseado nos Requisitos de Conformidade definidos pelo Conselho Federal de Medicina e Sociedade Brasileira de Informática em Saúde.

Palavras-chave: Certificação, Sociedade Brasileira de Informática em Saúde, Prontuário Eletrônico do Paciente, Sistemas de Registro Eletrônico de Saúde.

CERTIFICATION PROCESS FOR ELECTRONIC HEALTH RECORD SYSTEMS IN BRAZIL: A COMPREHENSIVE APPROACH AND MAIN CHALLENGES

ABSTRACT

The paper aims to present an overview of the process of certification of Electronic Health Record Systems in Brazil, and list the major challenges that are faced currently. Due to the growing number of automated processes that were previously done manually, there is a constant search for security when it comes to data and the processes involved. Systems that handle sensitive or confidential information or electronic documents that should have legal validity, must assure users Authentication, Confidentiality, Integrity and Non-repudiation to data. Thus, several techniques are currently used, including digital certification. This technique consists of the emission of a digital certificate with information that ensures the authenticity of one of the entities of the communication, serving as an electronic identification document. In Brazil, digital certificates are issued by ICP-Brazil. This method is already in use in health care, for example, the Digital CRM, which consists of a smart card that stores a certificate with information that identifies the physician. However, this technique is not enough for validating health care systems in the hospital environment. Apart from data security, it is necessary to ensure that the functionalities are in full operation, as they relate to important information and procedures on patients' health, and any mistake can compromise such patients. From this, it is proposed the creation of the Certification Process for Electronic Health Record Systems, which consists of a compliance verification for such systems based on Conformance Requirements defined by the Federal Council of Medicine and the Brazilian Society of Health Informatics.

Keywords: Certification, Brazilian Society of Health Informatics, Patient's Electronic Health Record, Systems Electronic Registration Of Health.

INTRODUÇÃO

O mercado de software está crescendo aceleradamente nos últimos anos, principalmente devido ao número de novas tecnologias e ferramentas que são disponibilizadas. A demanda pela informatização dos mais diversos setores da indústria, educação e da saúde, por exemplo, corrobora no surgimento de uma grande variedade de sistemas no mercado e, consequentemente, no gerenciamento de um grande volume de tipos de dados.

Se não houver um controle, organização e utilização de técnicas de forma apropriada durante o processo de desenvolvimento destes sistemas, os mesmos podem apresentar falhas que podem comprometer o seu funcionamento e, principalmente, a segurança das informações envolvidas. Devido a isso, há uma constante busca por soluções que garantam a confiabilidade dos sistemas, como também a segurança das informações manipuladas por eles. Várias técnicas foram criadas ao longo dos anos, baseadas no princípio básico de que um sistema deve garantir a autenticação, confidencialidade e integridade e o não-repúdio das informações (LAUREANO e MORAES, 2005) (DHILLON e BACKHOUSE, 2000).

Uma técnica bastante conhecida é a Criptografia, que visa garantir a confidencialidade das informações. Ela é responsável por codificar os dados transmitidos, evitando que sejam acessados por pessoas não autorizadas (SANTOS *et al*., 2011). Apesar de sua eficiência, as técnicas utilizadas (chaves simétricas e chaves assimétricas) não são suficientes para comprovar a assinatura de um emissor durante uma transação. Desta forma, foi criada a Assinatura Digital, consistindo em um mecanismo que aperfeiçoa a utilização da Criptografia de Chaves Assimétricas e fica responsável por comprovar a autenticidade de documentos eletrônicos.

Posteriormente, surgiu o conceito de Certificação Digital, responsável pela emissão de um documento eletrônico, conhecido como Certificado Digital, que contém informações que comprovam a autenticidade de uma das partes durante uma transação. No Brasil, a responsabilidade pela regulamentação da emissão de Certificados Digitais é da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) (BARRA, 2006) (CASAGRANDE, 2011).

Na área da saúde, a segurança das informações é uma característica indispensável nos sistemas utilizados, pois são manipulados dados e procedimentos sobre a saúde de pacientes que, na maioria das vezes, são sigilosos. Apesar disso, um sistema utilizado na área da saúde deve apresentar um alto grau de confiabilidade e robustez, com o objetivo de evitar falhas durante os procedimentos relacionados.

Visando isto, o Conselho Federal de Medicina (CFM) em cooperação técnica com a Sociedade Brasileira de Informática em Saúde (SBIS) criaram um processo de certificação para Sistemas de Registro Eletrônico de Saúde (S-RES), que são sistemas que gerenciam informações relacionadas à saúde de indivíduos, como o Prontuário Eletrônico de Pacientes (SBIS, 2013) (SALVADOR e DE ALMEIDA FILHO, 2005).

A certificação de S-RES consiste em um processo responsável por verificar se um determinado sistema está de acordo com os Requisitos de Conformidade definidos pelo Manual de Certificação (CBIS, 2009). Estes requisitos consistem em características e funções desejáveis para sistemas que serão executados na área da saúde e estão divididos nas seguintes categorias: Segurança, Estrutura, Conteúdo e Funcionalidades. Se um determinado sistema submetido ao processo de avaliação atender aos Requisitos propostos, será emitido um selo de Certificação indicando que está apto a ser instalado e executado no ambiente destinado.

Apesar deste procedimento já ser regulamentado e executado pela SBIS, existem vários desafios para que o processo de Certificação se adeque ao atual mercado de software. Visando isto, o presente artigo visa abordar de maneira geral o processo de Certificação, apontando quais são os principais desafios enfrentados atualmente.

O artigo está estruturado da seguinte maneira, além desta seção introdutória, a seção 2 apresenta a segurança da informação digital, com destaque para a criptografia, assinatura e certificação digital. A seção 3 trata sobre Certificação digital no Brasil: ICP-Brasil. Na seção 4 apresenta-se a certificação de sistemas de registro eletrônico de saúde, com destaque para o processo de certificação, requisito de conformidade, selo de certificação SBIS/CFM e os principais desafios da certificação de S-RES. Na seção 5 as conclusões, e por fim as referências.

SEGURANÇA DA INFORMAÇÃO DIGITAL

Com a expansão acelerada da Internet e da criação de novas tecnologias, os processos que antes eram feitos de forma manual nos mais diversos setores da indústria, saúde, entre outros, estão cada vez mais sendo informatizados. Uma das principais vantagens desta informatização é a substituição de papéis por formatos eletrônicos. Exemplos disto são as transações realizadas pela internet de bancos financeiros, atendimentos e acompanhamento de pacientes no ambiente hospitalar, entre diversos outros.

Na área da saúde, houve um crescimento no desenvolvimento de aplicações de informática, como: Prontuário Eletrônico do Paciente (PEP), Internet em Saúde, Sistemas de Apoio à Decisão e Telemedicina, entre outros. A maioria desses sistemas utilizam redes de computadores para transmitir documentos e informações sobre a saúde dos pacientes. Desta forma, estes dados ficam vulneráveis a acessos não autorizados (ABRAHÃO, 2003).

Surgiu então a necessidade de garantir a autenticidade, o sigilo e a privacidade das informações enviadas pela rede destes sistemas. Uma das principais exigências era a de identificar ao receptor quem é o emissor de uma determinada mensagem, como também fazer com que os documentos eletrônicos emitidos pelos profissionais da saúde tivessem o mesmo valor jurídico de um documento assinado de próprio punho (RIBEIRO *et al*., 2011) (NETO e PINHEIRO, 2012).

Diversos estudos surgiram com o principal objetivo de garantir a autenticidade de documentos e assinaturas, para que estas fossem trocadas pela rede de forma segura. Segundo VERONESE e DE FREITAS (2007), um sistema deve assegurar, do ponto de vista técnico, basicamente:

- ✓ Autenticação: identificação pública do emissor de uma determinada mensagem;
- ✓ Confidencialidade: a mensagem não pode ser lida por outrem que não seja o destinatário pretendido;
- ✓ Integridade: garantia de que o conteúdo de uma mensagem não seja alterado; e
- ✓ Não-repúdio: garantia que o autor não negue ter assinado ou criado a informação.

Surgiram assim, as técnicas de Criptografia, Assinatura Digital e Certificação Digital.

Criptografia

A criptografia pode ser caracterizada como um conjunto de conceitos e técnicas que tem como objetivo codificar uma mensagem, mantendo a privacidade da mesma. Existem registros que desde a antiguidade a criptografia já era praticada através da substituição de símbolos em mensagens, com o objetivo de confundir um possível interceptador (SANTOS *et al*., 2011).

Na computação, ela é utilizada para garantir a troca de dados em redes abertas sem que os mesmos sejam violados. Inicialmente a criptografia era estritamente limitada às aplicações militares e diplomáticas, e, por volta dos anos de 1948 e 1949, a comunidade científica pôde elaborar novas bases para a criptografia através da publicação de dois artigos de Claude Shannon no *Bell Systems Technical Journal* (LEVY, 2000).

Devido ao poder computacional, são utilizados processamentos digitais aliados a recursos matemáticos para realizar a codificação de uma determinada mensagem, dificultando, desta forma, a decodificação da mesma. O processo é feito através da utilização de chaves de codificação.

A Chave de codificação significa o segredo utilizado para codificar e/ou decodificar uma determinada informação. É similar a uma senha, e seu tamanho é geralmente medido em quantidade de *bits* (CERT.br, 2012). Esta chave é compartilhada entre duas ou mais partes criando um canal confidencial de informação entre elas.

Uma das formas de tentar decodificar uma mensagem criptografada é testar todas as chaves possíveis até encontrar a correta. Isto é conhecido como ataque por tentativa ou erro ou força bruta (SANTOS *et al*., 2011). Mesmo com as tecnologias atuais, o esforço é muito grande para tentar desvendar o código cifrado, tornando-se numa prática inviável.

Atualmente existem dois tipos de chaves criptográficas, as chaves simétricas e chaves assimétricas, diferenciando-se de acordo com a quantidade de chaves utilizadas no processo de criptografia (SIMMONS, 1979).

A Chave Simétrica, também conhecida como chave privada ou criptografia de chave única, utiliza uma única chave para codificar e decodificar a mensagem. Esta chave é compartilhada entre o remetente e o destinatário, na proposição de que ela é conhecida apenas por eles. Esta chave é a mais indicada para grandes volumes de dados, pois o seu processamento é mais rápido (CERT.br, 2012). São exemplos de Algoritmos de Chave Simétrica o *Data Encryption Standard* (DES), o *Triple DES* (3DES) e o *Advanced Encryption Standard* (AES).

A técnica da criptografia simétrica apresenta alguns problemas fundamentais relacionados à autenticação e gerenciamento de chaves, listados a seguir (VERONESE e DE FREITAS, 2007):

- ✓ Devido utilizar apenas uma chave, esta deve ser compartilhada entre os dois envolvidos, e este compartilhamento deve ser feito utilizando um canal de transmissão inseguro, já que meios seguros são caros e de difícil gerenciamento;
- ✓ Dificulta a identificação de quem originou a mensagem codificada, já que os envolvidos na comunicação tem a mesma chave e podem trocar mensagens entre si; e
- ✓ Dependendo da quantidade de pares de usuários que necessitem se comunicar em um determinado ambiente, o gerenciamento pelas chaves se torna complexo, já que seria necessária uma grande quantidade de chaves.

Desta forma, em 1976, Whitfield Diffie e Martin Hellman, da Universidade de Stanford, Estados Unidos, apresentaram o conceito de criptografia de chave pública ou assimétrica, corrigindo os problemas apresentados pela chave simétrica. Na criptografia assimétrica,

são utilizadas duas chaves, uma para codificar a mensagem (conhecida por todos - chave pública), e outra para decodificar (reservada e de conhecimento restrito - chave privada) (OLIVEIRA, 2012). Apesar de utilizar duas chaves, elas estão relacionadas matematicamente.

A parte da comunicação que deseja receber mensagens cria uma chave pública e uma privada respectivamente. A chave pública é disponibilizada para o emissor da comunicação, que codifica a mensagem e envia ao destinatário utilizando a chave recebida. O destinatário, que criou as chaves, utiliza a chave privada para decodificar a mensagem, que somente ele tem conhecimento (chave secreta e individual). Se alguém mais desejar enviar uma mensagem para este usuário, basta obter a chave pública disponibilizada por ele e realizar o processo de codificação dos dados que serão enviados.

Neste sentido, os problemas listados pela chave simétrica são resolvidos pela chave assimétrica, fornecendo confidencialidade. Por outro lado, esta técnica utiliza algoritmos mais complexos (devido utilizar um par de chaves), se tornando num processo de criptografia muito mais lento (COPALO, 2003).

Assinatura Digital

A Criptografia de Chave Assimétrica não garante a autenticidade de uma determinada informação digital, já que qualquer pessoa que possuir a chave pública da comunicação pode emitir uma informação. Assim, o conceito de Assinatura Digital foi criado e consiste na adição de uma chave privada e pública por parte do emissor na transmissão dos dados. Inicialmente ele codifica a mensagem com a chave privada, e disponibiliza a chave pública ao destinatário para que ele possa realizar a decodificação. Desta forma, o receptor da mensagem terá a certeza da autenticidade de quem gerou a informação recebida, já que somente este possui a chave privada que gerou o conteúdo codificado (CASAGRANDE , 2011) (MENKE, 2003).

Antes de aplicar as chaves privadas e públicas na codificação da mensagem que será enviada, a Assinatura Digital utiliza ainda outro procedimento para garantir a integridade das informações que serão transmitidas, que é a Função *Hash*. Essa função realiza a codificação de uma mensagem através de um cálculo matemático utilizando um algoritmo (conhecido como função *hash*), sendo matematicamente impossível realizar o processo inverso, de decodificar a mensagem. O código gerado é chamado de resumo (CORREIA, 2011).

Desta forma, o remetente envia ao destinatário a mensagem original e o resumo. Para comprovar a integridade, o destinatário codifica novamente a mensagem original através da função *Hash*, gerando um novo resumo, e compara com o resumo recebido. Se forem idênticos, a mensagem está íntegra, caso contrário, houve alteração no seu conteúdo durante a transmissão.

Certificação Digital

A Certificação Digital consiste em um mecanismo que reforça a autenticidade de uma das entidades durante uma comunicação. Ela consiste na emissão de um documento eletrônico que é enviado junto à mensagem durante a comunicação, e contém uma assinatura digital com informações sobre uma das entidades da comunicação, como a chave pública do titular, nome e endereço de e-mail, período de validade do certificado, nome e assinatura

digital da AC (Autoridade Certificadora) que emitiu o certificado, número de série do certificado digital. Desta forma, a parte da comunicação "interessada" tem a certeza que esta se comunicando com a entidade desejada (CASAGRANDE, 2011) (GOLLMANN, 2010).

A principal função do Certificado Digital é vincular uma pessoa ou uma entidade a uma chave pública. Com isso, pode ser comparado com um documento oficial de identificação, sendo que em formato eletrônico, atestando que uma determinada mensagem recebida foi remetida por aquele que a assinou. Exemplos de utilização de Certificação Digital no Brasil são o e-CPF, e-CNPJ e o CRM Digital (VERONESE e DE FREITAS, 2007). São cartões conhecidos como *smart card* (cartões inteligentes) que possuem armazenados um Certificado Digital com toda a identificação do responsável. A leitura destas informações é feita por dispositivos eletrônicos de segurança, registrados pelo Padrão de Certificação em vigor.

Com o e-CPF e o e-CNPJ é possível enviar declaração de Imposto de Renda via Internet, consultar e atualizar cadastro como contribuinte pessoa física ou jurídica respectivamente, assinar contratos digitais, verificar a autenticidade de informações divulgadas na versão on-line do Diário Oficial da União, entre diversos outros. Já com o CRM Digital, médicos podem acessar sistemas de prontuário eletrônico do paciente, assinar contratos digitais, utilizar serviços online da Receita Federal e do sistema de Conselhos de Medicina, entre outros (CFM, 2013) (RECEITA FEDERAL, 2013).

Para que os Certificados Digitais tenham validade, é necessário que sejam emitidos por uma Entidade de Certificação reconhecida, também chamada de "terceiro de confiança", e no Brasil esta entidade é a ICP-Brasil.

CERTIFICAÇÃO DIGITAL NO BRASIL: ICP-BRASIL

No Brasil, o cidadão é livre para utilizar qualquer meio como validade de um ato jurídico, de acordo com a Lei No 5.869, de 11 de Janeiro de 1973, que trata:

- ✓ Art. 332. Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.

Em uma troca de documentos entre pessoas conhecidas, a assinatura é utilizada como comprovação de autenticidade com valor jurídico, por ser plenamente identificada pelas partes. Ela é tratada no Código Civil através da Lei Nº 10.406, de 10 de Janeiro de 2002, através dos artigos:

- ✓ Artigo 219: "As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários";
- ✓ Artigo 221: "O instrumento particular, feito e assinado, ou somente assinado por quem esteja na livre disposição e administração de seus bens, prova as obrigações convencionais de qualquer valor; mas os seus efeitos, bem como os da cessão, não se operam, a respeito de terceiros, antes de registrado no registro público".

Já no âmbito dos negócios, envolvendo pessoas desconhecidas, é necessária uma terceira parte para realizar a autenticação da titularidade da assinatura e dos documentos

envolvidos. E esta necessidade é reforçada no cenário da internet, na qual são realizadas diversas transações envolvendo informações importantes.

Com isto, houve a necessidade da criação de uma legislação que regulamentasse a assinatura digital, como também a criação de uma entidade regulamentadora para tal ação. Foi expedido, então, um decreto presidencial, n. 3.505, de 13 de junho de 2000, que definia uma política de segurança da informação aos meios eletrônicos nas diversas atividades empreendidas pelo governo federal. Posteriormente, visando à utilização da assinatura digital em aplicações internas governamentais, houve a publicação do Decreto n. 3.587, de 5 de novembro de 2000, estabelecendo normas para a Infraestrutura de Chaves Públicas do Poder Executivo Federal (ICP-Gov) (COPALO, 2003).

E por fim, através da Medida Provisória nº 2.200-2, de 24 de Agosto de 2001, foi instituída a ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira), com a finalidade de regulamentar a emissão de Certificados Digitais no Brasil, garantindo integridade e autenticidade aos documentos produzidos ou transmitidos eletronicamente. A Medida confere validade jurídica à assinatura digital (ICP-Brasil, 2013) (DA COSTA, 2013).

O modelo da ICP-Brasil baseia-se em um sistema hierárquico de certificação com raiz única, sendo o Instituto Nacional de Tecnologia da Informação (ITI) a Autoridade Certificadora Raiz (AC-Raiz), que fica responsável por credenciar e supervisionar as Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e demais prestadores de serviço habilitados na ICP-Brasil.

A Autoridade Certificadora consiste em uma entidade, pública ou privada que fica responsável pela emissão dos Certificados Digitais e estabelecer as políticas de segurança necessárias para garantir a autenticidade da identificação realizada. Atualmente existem várias Autoridades Certificadoras credenciadas, entre elas a Caixa Econômica, Receita Federal, a SERPRO, entre outras (RIBEIRO *et al*., 2011) (ICP-Brasil, 2013).

As Autoridades de Registro fazem a interface entre o usuário solicitante com a Autoridade Certificadora, controlando e encaminhando as solicitações de Certificados Digitais à Autoridade Certificadora vinculada (ICP-Brasil, 2013).

CERTIFICAÇÃO DE SISTEMAS DE REGISTRO ELETRÔNICO DE SAÚDE

O Prontuário Eletrônico de Pacientes (PEP) é um exemplo de sistema que surgiu com a informatização dos processos realizados nos hospitais, visando padronizar e digitalizar o sistema de prontuário médico. Ele é responsável por manipular todas as informações relacionadas ao histórico clínico do paciente, oferecendo recursos de apoio à decisão, alertas, entre diversos outros (ABRAHÃO, 2003) (NUNES *et al*, 2006).

Apesar das vantagens da informatização, não havia garantia de que os sistemas que estavam sendo desenvolvidos e implantados no âmbito hospitalar estavam livres de erros e que os dados manipulados por eles estavam totalmente seguros. Houve, então, a necessidade da legalização dos sistemas responsáveis por manipular dados relacionados com a saúde do paciente. Várias solicitações sobre a criação de uma regulamentação foram feitas ao Conselho Federal de Medicina (CFM), que decidiu desenvolver um processo de certificação de sistemas informatizados em saúde em cooperação técnica com a Sociedade Brasileira de Informática em Saúde (SBIS).

A primeira resolução criada foi a de n.º 1639/2002, contendo as "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico". A partir daí surgiram outras resoluções até que publicaram, em 2004, o Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES). Esta foi considerada a Fase 1 (um) do processo de Certificação SBIS/CFM (SBIS, 2009).

O Manual de Certificação foi atualizado nos anos seguintes, baseado em conhecidas normas nacionais e internacionais, e atualmente encontra-se na versão 3.3, publicado em 2009 (SIBS, 2009), chamado de Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES).

O termo Sistemas de Registro Eletrônico em Saúde (S-RES) é descrito pelas normas ABNT ISO/TR 20514 e ISO/TS18308, que definem:

- ✓ Registro Eletrônico em Saúde (RES): Um repositório de informação a respeito da saúde de indivíduos, numa forma processável eletronicamente;
- ✓ Sistema de Registro Eletrônico em Saúde (S-RES): Sistemas para registro, recuperação e manipulação das informações de um Registro Eletrônico em Saúde.

Existe uma grande variedade de S-RES no mercado. Devido a isso, o Manual de Certificação classifica-os nas categorias a seguir:

- ✓ Assistencial Ambulatorial: sistemas de automação de consultórios clínicos, de informação ambulatorial, de unidades básicas de atendimento à saúde, entre outros;
- ✓ Sistemas de Gerenciamento Eletrônicos de documentos (GED): sistemas utilizados para armazenamento e visualização de documentos relacionados à informática na saúde; e
- ✓ Troca de Informação em Saúde Suplementar (TISS): sistemas utilizados por operadoras de planos de saúde e prestadoras de serviço de saúde que trocam informações utilizando o padrão TISS.

O Processo de Certificação

O Processo padrão para a obtenção da certificação é destinado a S-RES que: ainda não foi certificado; já certificados que estejam com a validade expirada (atualização); e novas versões que possuam ajustes relevantes que necessitam ser reavaliados. Este processo é composto por um conjunto de atividades que serão executadas tanto pelo solicitante, como pela SBIS desde a solicitação, até a emissão do certificado, conforme demonstrado no Fluxograma da Figura 1.

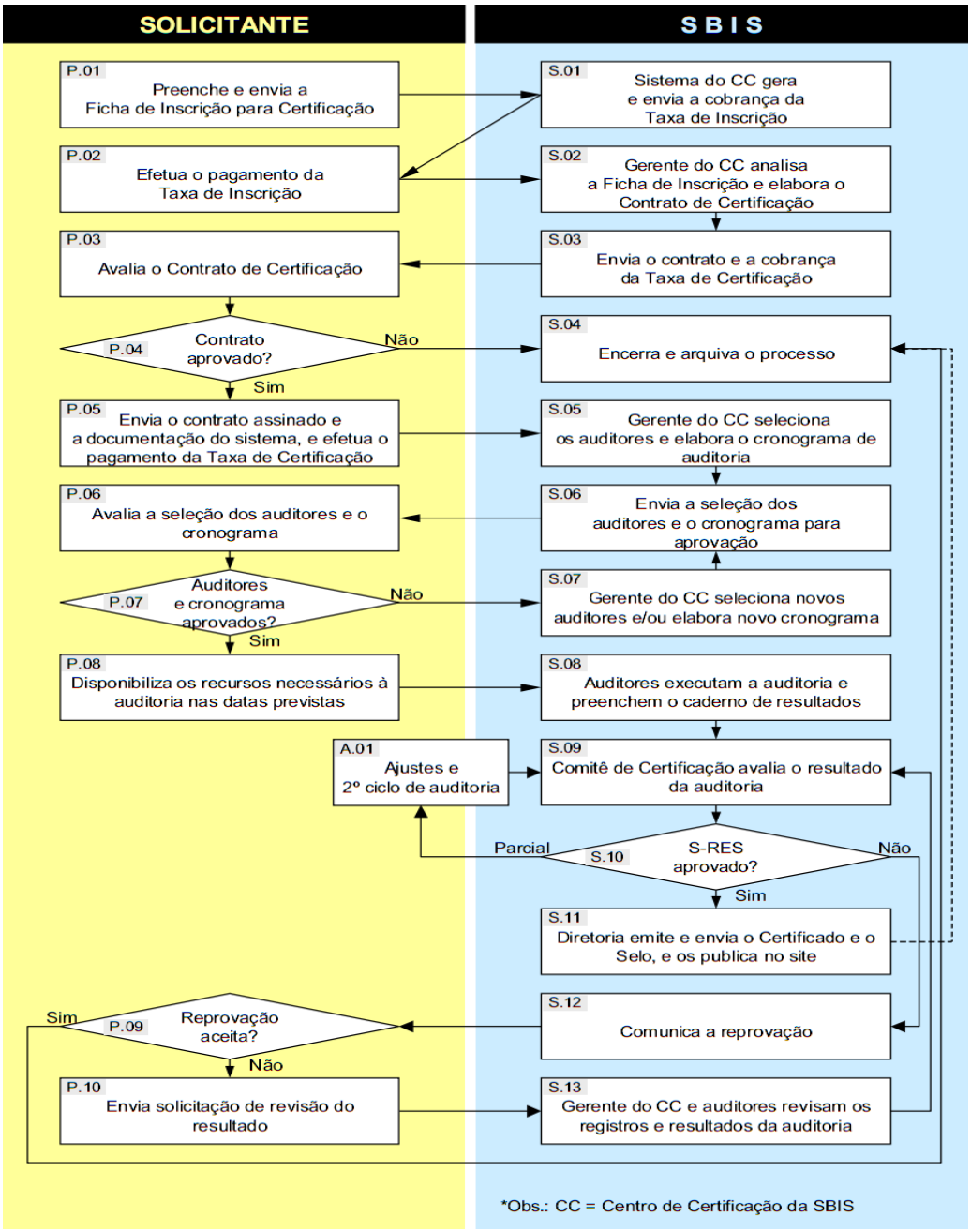

Figura 1. Fluxo do processo de certificação. Fonte: SBIS (2009).

Para dar início ao Processo de Certificação, é necessário que o interessado preencha a Ficha de Inscrição (P.01), que pode ser obtida no site da Certificação SBIS/CFM na internet. Nesta ficha são informados os dados pessoais do solicitante e informações gerais sobre o sistema e descrição de todos os componentes que é constituído, como Sistema Operacional, SGBD (Sistema de Gerenciamento de Banco de Dados) e conectores, Arquitetura do S-RES (cliente/servidor, ASP (*Active Server Pages*), Mainframe, etc.), Componentes do tipo web dinâmicos (*Applet*, ActiveX, etc.), Sistema de diretórios (AD - Active Directory, LDAP - Lightweight Directory Access Protocol, etc.), entre outros.

Em seguida, este documento deve ser enviado à SBIS (S.02) que, ao receber, gerará um boleto bancário referente à Taxa de Inscrição do processo de Certificação, e enviará por e-mail ao solicitante. Este deverá realizar o pagamento (P.02) para que de continuidade ao processo de certificação. Em seguida, se não houver nenhuma restrição à participação do

Solicitante e do S-RES inscrito no processo de certificação, a SBIS elaborará e enviará o Contrato de Certificação, junto a uma nova taxa que deverá ser paga, a Taxa de Certificação (S.03).

O Solicitante deve avaliar o Contrato de Certificação (P.04), caso não seja aprovado, o processo é arquivado (S.04). Se for aprovado, deve efetuar o pagamento da Taxa de Certificação e enviar o contrato assinado em duas vias e a documentação técnica completa do sistema à SBIS (P.05). Ao receber o contrato, o gerente do Centro de Certificação da SBIS analisará o processo e criará uma proposta de cronograma, como também selecionará os auditores (dentre os credenciados pela SBIS) para a auditoria do sistema (S.05). Ao final, enviará para o Solicitante esses dados para aprovação (S.06).

Se o solicitante não aprovar o cronograma ou mesmo algum dos auditores selecionados, deverá comunicar à SBIS expondo os motivos. Desta forma, o gerente deverá elaborar um novo cronograma ou selecionar novos auditores (S.07). No momento que o Solicitante aprovar cronograma e auditores, deverá disponibilizar todos os recursos necessários para a execução e auditoria do sistema (P.08). A auditoria é feita obrigatoriamente por três auditores através de uma análise de conformidade, que durante o processo preenchem o caderno de resultados (S.08).

Segundo o INMETRO (2013), Análise de Conformidade consiste no "Processo sistematizado, acompanhado e avaliado, de forma a propiciar adequado grau de confiança de que um produto, processo ou serviço, ou ainda um profissional, atende a requisitos pré-estabelecidos em normas e regulamentos técnicos com o menor custo para a sociedade.". No processo de Certificação de S-RES, a avaliação é feita sobre os chamados Requisitos de Conformidade, seguindo os passos (chamados de *scripts*) do Manual Operacional de Ensaios e Análises (SBIS, 2009).

Ao final da auditoria, o Comitê de Certificação realiza uma avaliação do resultado, emitindo um parecer sobre a Certificação ou não do sistema (S.09). Em alguns casos, é recomendado ao Solicitante que ele realize correções no S-RES para um novo ciclo de auditoria (A.01). Se a certificação for reprovada, é comunicado ao Solicitante (S.12), e este poderá solicitar uma revisão do resultado (P.10, S.13). Se a certificação do sistema for aprovada, a Diretoria da SBIS emite e envia o Selo e o Certificado, e realiza a publicação no site do resultado (S.11).

Requisitos de Conformidade

Os Requisitos de Conformidade são características e funcionalidades desejáveis em um S-RES. Foram selecionados das normas nacionais e internacionais que o Manual de Certificação toma como base (os mais adequados à realidade brasileira), seguindo critérios para que o processo de certificação se tornasse o mais objetivo possível.

Visando uma melhor organização, os Requisitos são descritos pelo Manual através de: um identificador (ID), único para cada requisito; nome do requisito; lista das referências que tomaram como base; descrição do requisito; e obrigatoriedade de sua presença no sistema, conforme Tabela 1.

Tabela 1. Informações sobre os Requisitos de Certificação. Fonte: SBIS (2009)

Coluna	Descrição
ID	Identificação do requisito, utilizando codificação padronizada.
Requisito	Nome do requisito.
Referência	Padrão de referência que deu origem ao requisito.
Conformidade	Descrição do requisito, incluindo exemplos sempre que apropriado. Adicionalmente, pode incluir indicações de como o requisito será avaliado durante a auditoria.
Presença	**M – Mandatório:** Deve ser obrigatoriamente atendido pelo S-RES. **R – Recomendado:** Requisito com alta probabilidade de tornar-se obrigatório nas próximas versões. **O – Opcional:** Requisito relevante, porém de adoção opcional. **X – Não se aplica:** Requisito não aplicável à situação apresentada.

Seguindo esta classificação, há uma maior compreensão sobre o objetivo de cada Requisito, e como aplicá-los nos sistemas que passarão pelo processo de Certificação. Um exemplo é a descrição do Requisito de Identificação e autenticação do usuário demonstrado na Tabela 2.

Tabela 2. Descrição do Requisito de Identificação e autenticação do usuário. Fonte: SBIS (2009)

Coluna	Descrição
ID	NGS1.02.01 I
Requisito	Identificação e autenticação do usuário
Referência	HL7 ERH-S FM IN1.1; ABNT NBR ISO/IEC 27001:2006 A.11.5.2
Conformidade	Todo usuário deve ser identificado e autenticado antes de qualquer acesso a dados do S-RES.
Local / Remoto	M

Os Requisitos são ainda agrupados nas seguintes categorias: Requisitos de Segurança; Requisitos de Estrutura, Conteúdo e Funcionalidades para S-RES Assistencial; Requisitos para GED; e Requisitos para TISS.

Os Requisitos de Segurança são importantes para garantir a privacidade, confidencialidade e integridade das informações manipuladas pelos sistemas. Eles são classificados em um dos dois Níveis de Garantia de Segurança (NGS), citados a seguir:

- ✓ NGS1: Sistemas RES que não leva em consideração o uso de certificados digitais ICP-Brasil, não eliminam a utilização do papel, impressão e aposição manuscrita da assinatura. Exemplos: controle de versão do software, identificação e autenticação de usuário, controle de sessão de usuário, entre outros;
- ✓ NGS2: Sistemas RES que eliminam a utilização de papéis, utilizando, desta forma, Certificados Digitais ICP-Brasil para os processos de assinatura digital e autenticação. Necessita atender aos requisitos da NGS1, como também os especificados para este nível. Exemplos: Certificação Digital, Assinatura Digital, Autenticação de usuário utilizando certificado digital, entre outros.

Os Requisitos de Estrutura e Conteúdo para S-RES Assistencial são destinados a sistemas como os de informação hospitalar, vigilância epidemiológica e medicina ocupacional. Exemplos: Estrutura do RES, dados estruturados, dados administrativos, entre outros. Já os Requisitos para GED tratam informações sobre a digitalização, guarda e manuseio dos prontuários em meio eletrônico, e, por fim, os Requisitos para TISS estão relacionados à verificação de conformidade dos sistemas com o padrão de Troca de Informação em Saúde Suplementar.

Todos os Requisitos são verificados pelos auditores durante o processo de Certificação, e caso o sistema esteja em conformidade com todos eles, será emitido o Selo de Certificação.

Selo de Certificação SBIS/CFM

O Selo de Certificação, representado pela Figura 2, comprova a Certificação de um determinado sistema, apresentando informações sobre Categorias do S-RES certificado, Nível de Segurança, Nome e Versão do Sistema, Número do Certificado e Ano do Manual. Ele pode ser utilizado em manuais e materiais promocionais de sistemas que tenham sido certificados, assim como em páginas *web*.

Figura 2. Selo de Certificação SBIS/CFM. Fonte: SBIS (2009)

Segundo a Cartilha que fala sobre o Prontuário Eletrônico da SBIS, "O selo da Certificação é uma opinião técnica qualificada e imparcial da SBIS sobre um S-RES" (SBIS, 2012).

Principais Desafios da Certificação de S-RES

Apesar do processo de Certificação de S-RES, elaborado pelo Concelho Federal de Medicina junto à Sociedade Brasileira de Informática em Saúde, já estar em funcionamento e ter realizado o processo de Certificação em vários sistemas, existem alguns desafios para que ele seja melhorado e se adapte ao atual mercado de software.

O primeiro deles está relacionado à forma como é feita a verificação de conformidade de um S-RES. O processo é realizado manualmente por auditores, desta forma, falhas podem passar despercebidas, consistindo num fator que causa certa preocupação, pois pode comprometer o resultado final da Certificação.

Para complementar esta problemática, a última versão do Manual de Certificação de S-RES foi publicado em 2009, baseado em algumas tecnologias e procedimentos um pouco ultrapassados. Com o surgimento acelerado de novas tecnologias, o desafio consiste em como criar um modelo de Manual que esteja adequado e constantemente atualizado. Um exemplo disto é a utilização cada vez mais dos Dispositivos Móveis no Ambiente

Hospitalar. Seria desejável uma seção no Manual que tratasse somente dos sistemas utilizados nestas plataformas, pois utilizam outros critérios de comunicação e segurança.

Um grande desafio enfrentado pelas indústrias de software consiste no desenvolvimento de sistemas que serão submetidos ao processo de Certificação. Este processo pode ocasionar maiores custos para o projeto, não só financeiros, mas relacionados ao tempo. É necessário um estudo minucioso de todo o Manual de Certificação, como também do Manual Operacional de Ensaios e Análises, para assim elaborar uma estratégia de desenvolvimento e testes de conformidade do software.

Outro desafio consiste em como incentivar a utilização de sistemas certificados na área da saúde. Estes sistemas manipulam informações que estão relacionados diretamente com a saúde do paciente, e, que na maioria das vezes, são sigilosas. Deve haver uma maior divulgação do processo de certificação para que empresas de desenvolvimento submetam os sistemas a este processo, e para que também os ambientes hospitalares não aceitem sistemas que não tenham passado pelo processo de certificação.

É desejável incentivar ainda que sistemas complexos e que realizam procedimentos importantes e sigilosos utilizem o Nível de Garantia de Segurança 2, passando a empregar Certificados Digitais emitidos pela ICP-Brasil. Apesar de uma importante prática de segurança da informação, não garante que os dados irão ficar completamente seguros, mas inibe a ação de criminosos e de falhas que venham a ocorrer que comprometam as informações armazenadas.

CONCLUSÃO

A utilização de critérios de segurança em sistemas que manipulam dados e documentos eletrônicos que necessitam ter a autenticidade comprovada, como também ter garantido a integridade e confidencialidade das informações, consiste em uma prática importante no cenário atual de desenvolvimento de software. A utilização de Certificados Digitais é uma das práticas conhecidas e bastante utilizada por existir regulamentação e uma entidade responsável por emiti-las no Brasil, a ICP-Brasil.

A criação do processo de Certificação de Sistemas de Registro Eletrônico de Saúde foi um marco importante para a área da saúde, pois a partir dele, Sistemas podem ser Certificados através de uma verificação de conformidade, garantindo que a sua execução seja de forma esperada e que os dados envolvidos estejam seguros, evitando assim, vazamento de informações e falhas nos procedimentos. Isto é importante no âmbito hospitalar, pois lida com informações e procedimentos de pacientes, que muitas vezes, são sigilosos.

Existem vários desafios a serem enfrentados para que o processo de Certificação de S-RES se torne cada vez mais eficiente. Novas tecnologias são criadas, e o processo deve estar sempre atualizado para abranger um número cada vez maior de sistemas destinados à área da saúde. É importante que o processo de certificação também seja atualizado, com o objetivo de automatizar o processo e, desta forma, minimizar as falhas durante o processo de verificação de conformidade.

Como trabalhos futuros, propor uma nova metodologia de Certificação para Sistemas de Registro Eletrônico de Saúde, visando automatizar partes do processo através da utilização

de novas Tecnologias de Desenvolvimento de Sistemas, como também de Testes de Software. Propor também um novo modelo de normas de certificação para sistemas destinados a outras arquiteturas, como Computação Móvel.

AGRADECIMENTOS

Ao Laboratório de Inovação Tecnológica em Saúde (LAIS) do Hospital Universitário Onofre Lopes (HUOL) da Universidade Federal do Rio Grande do Norte (UFRN), o qual ofereceu a infraestrutura para o desenvolvimento da pesquisa abordada.

REFERÊNCIAS BIBLIOGRÁFICAS

1. ABRAHÃO, M. S. A Segurança da Informação Digital na Saúde. In: Publicação Oficial do Instituto Israelita de Ensino e Pesquisa Albert Einstein. 2. ed. São Paulo: Einstein, 2003.
2. BARRA, M. C. Infra-estrutura de chaves públicas brasileira (ICP - BRASIL) e a formação do estado eletrônico. [Dissertação - Mestrado em Sociologia]. Universidade de Brasília. 2006.
3. CASAGRANDE, A. R. Certificação digital. [Trabalho de Conclusão de Curso - Especialização] – Universidade Tecnológica Federal do Paraná, Curitiba, 2011.
4. CERT.br. Cartilha de Segurança para Internet. V4.0, 2012 Disponível em: <http://cartilha.cert.br/> Acesso em: 13 mai 2013.
5. CFM. CRM Digital. Disponível em: <http://portal.cfm.org.br/crmdigital/crm-digital.html>. Acesso em: 01 jul 2013.
6. COPALO, E. D. R. ICP - Brasil. Revista CEJ, Brasília, n. 20, p. 58-66, jan./mar. 2003.
7. CORREIA, M. P. Sociedade de informação e direito: a assinatura digital. 2011. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/13816-13817-1-PB.htm>. Acesso em: 1 jul 2013.
8. DA COSTA, M., MARCACINI, A. T. R. O Apagão no Comércio Eletrônico no Brasil. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/27426-27436-1-PB.pdf>. Acesso em: 13 mai 2013.
9. DHILLON, G.; BACKHOUSE, J. Technical opinion: Information system security management in the new millennium. Communications of the ACM, v. 43, n. 7, p. 125-128, 2000.
10. GOLLMANN, D. Computer security. Wiley Interdisciplinary Reviews: Computational Statistics, v. 2, n. 5, p. 544-554, 2010.
11. ICP-Brasil. Infraestrutura de Chaves Públicas Brasileira. Disponível em: <http://www.iti.gov.br/icp-brasil>. Acesso em: 13 mai 2013.
12. INMETRO. Avaliação da Conformidade. Disponível em: <http://www.inmetro.gov.br/qualidade/definicaoAvalConformidade.asp> Acesso em: 12 mai 2013.

13. LAUREANO, M. A. P.; MORAES, P. E. S. Segurança como estratégia de gestão da informação. Revista Economia & Tecnologia, v. 8, p. 38-44, 2005.

14. LEVY, S. Crypto: secrecy and privacy in the new code war. London: Allen Lane, The Penguin Press, 2000.

15. MENKE, F. Assinaturas Digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a ICP alemã. Revista de Direito do Consumidor, v. 12, n. 48, 2003.

16. NUNES, D.; JÚNIOR, J. A. C.; DE SOUZA, M. O. S. O Prontuário Eletrônico do Paciente no Hospital Márcio Cunha–6 anos de sucesso. In: Anais do Congresso Brasileiro de Informática em Saúde, Florianópolis, SC, Brasil. 2006. p. 10-10.

17. OLIVEIRA, R. R. Criptografia simétrica e assimétrica - os principais algoritmos de cifragem. Segurança Digital [Revista online] 5ª Ed, 31 de março de 2012, p 11-15; 6ª Ed, 31 de maio de 2012, p 21-24.

18. PINHEIRO, D. B. M.; NETO, F. R. C. Certificação digital: a utilização da certificação digital em documentos, transações comerciais e jurídicas. Fasem Ciências, v. 2, n. 2, p. 43-60, 2012.

19. RECEITA FEDERAL. Conceitos Básicos. Disponível em: <http://www.receita.fazenda.gov.br/atendvirtual/orientacoes/conceitobasico.htm>. Acesso em: 01 jul 2013.

20. RIBEIRO, O. G., MARINHO, E. A., PEREIRA, S. R., LODDI, S. A., SOUZA, P. S. D. A CERTIFICAÇÃO DIGITAL NA ICP-BRASIL. Tekhne e Logos, v. 2, n. 2, 2011.

21. SALVADOR, V. F. M.; DE ALMEIDA FILHO, F. G. V. Aspectos Éticos e de Segurança do Prontuário Eletrônico do Paciente. II Jornada do Conhecimento e da Tecnologia. 2005.

22. SANTOS, R. S. D.; ARANTES, J. C. D. S.; MORAIS, M. R. D. Criptografia aplicada em sistemas computacionais. Anuário da Produção de Iniciação Científica Discente, v. 13, n. 16, p. 327-337, 2011.

23. SBIS. Cartilha sobre Prontuário Eletrônico - A Certificação de Sistemas de Registro Eletrônico de Saúde. 2012. Disponível em: <http://www.sbis.org.br/certificacao/Cartilha_SBIS_CFM_Prontuario_Eletronico_fev_2012.pdf>. Acesso em: 1 jul 2013.

24. SBIS. Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES). Versão 3.3. 2009. Disponível em: <http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2009_v3-3.pdf> Acesso em: 12 mai 2013

25. SBIS. Manual Operacional de Ensaios e Análises para Certificação de S-RES. Versão 1.2. 2009. Disponível em: <http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2009_v3-3.pdf> Acesso em: 12 mai 2013

26. SIMMONS, G. J. Symmetric and asymmetric encryption. ACM Computing Surveys (CSUR), v. 11, n. 4, p. 305-330, 1979.

27. VERONESE, A., DE FREITAS, C.S. Segredo e Democracia: certificação digital e software livre. Informática Pública, 2007. p. 09-26.