Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Uma Solução de Software de Assinatura Digital de Documentos para Instituição de Ensino Brasileira

Andrei Lima Queiroz

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientadora
Prof.ª Dr.ª Genaína Nunes Rodrigues

Brasília
2014

Ficha catalográfica elaborada pela Biblioteca Central da Universidade de Brasília. Acervo 1018269.

Queiroz, Andrei Lima.
Q3s Uma solução de software de assinatura digital de documentos para instituição de ensino brasileira / Andrei Lima Queiroz. -- 2014.
xi, 63 f. : il. ; 30 cm.

Dissertação (mestrado) - Universidade de Brasília, Instituto de Ciências Exatas, Departamento de Ciência da Computação, Programa de Pós-graduação em Computação Aplicada, 2014.
Inclui bibliografia.
Orientação: Genaína Nunes Rodrigues.

1. Universidade de Brasília. 2. Assinatura digital. 3. Certificado digital. 4. Engenharia de software. I. Rodrigues, Genaína Nunes. II. Título.

CDU 004.056

Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

Uma Solução de Software de Assinatura Digital de Documentos para Instituição de Ensino Brasileira

Andrei Lima Queiroz

Dissertação apresentada como requisito parcial para conclusão do Mestrado Profissional em Computação Aplicada

Prof.ª Dr.ª Genaína Nunes Rodrigues (Orientador)
CIC/UnB

Prof. Dr. Anderson Clayton Alves Nascimento
ENE/UnB

Prof. Dr. Diego de Freitas Aranha
Unicamp

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 30 de julho de 2014

Dedicatória

Esse trabalho é dedicado principalmente à minha mãe, Francisca Maria de Lima, por ser essa fonte de perseverança e garra na qual eu me inspiro.

Dedico ao meu irmão, Cleiton Queiroz, pelos pensamentos sempre positivos em todas as situações da vida.

Dedico ao meu pai, Severino de Queiroz (*In memoriam*), que me direcionou aos estudos e consolidou o que sou hoje. Muito de minhas conquistas devo a ele.

Dedico ao marido de minha mãe, José Inocêncio, por ser um exemplo de dedicação ao trabalho o qual eu tento seguir.

Agradecimentos

À professora e orientadora Dr.ª Genaína Nunes Rodrigues pelos direcionamentos e pela forma como me ajudou a conduzir esse trabalho. Agradeço também pela paciência nos momentos em que eu chegava em nossas reuniões cheio de dúvidas. Fica aqui minha admiração não só pela profissional, mas também pela pessoa agradável que é.

Ao professor Dr. Diego Aranha pela ajuda que me deu com as oportunas considerações feitas ao trabalho. Elas serviram para o meu crescimento profissional inclusive.

A todos os docentes escolhidos para integrar o Programa de Pós-Graduação em Computação Aplicada/CIC.

Ao consultor Brandão, por ter me passado um pouco da sua experiência de mercado com assinaturas digitais. Sua ajuda foi fundamental para o andamento da dissertação.

Aos amigos Cleison Lucas e Renato Edésio pela amizade e apoio mútuo que temos nos dado desde o início de nosso convívio profissional.

Ao professor Dr. Jacir Bordim por ter apoiado e por ter acreditado que a proposta do projeto seria benéfica tanto para o meu crescimento profissional quanto para a instituição.

Ao professor Dr. Marcelo Ladeira, por sempre ter apoiado os servidores técnico-administrativos desde a época de diretor do Centro de Informática. Ele dizia: “Preocupem-se em obter conhecimento, o resto é consequência”.

A todos os colegas de turma, principalmente aos amigos Riane Torres, Juvenal, Marcelo Karam e Jackson, pela companheirismo, pela união e pelo respeito durante todo o curso.

Resumo

Esse trabalho tem como objetivo propor e avaliar uma implementação de software de assinatura digital. O estudo foi motivado pelos problemas encontrados no processo atual de emissão dos certificados de extensão da Universidade de Brasília. Além de propor uma implementação do software de assinatura digital baseada em paradigmas da orientação a serviço, o estudo utiliza a abordagem GQM de Victor R. Basili para avaliar se as funcionalidades se adequam ao negócio da instituição. O desenvolvimento da proposta teve como base as normas e documentos da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil e a Medida Provisória 2.200-2, de 24 de agosto de 2001. Com isso garantiremos as mesmas característica jurídicas do documento físico ao documento digital, ou seja, a validade jurídica ao documento assinado eletronicamente.

Palavras-chave: Assinatura Digital, Certificado Digital, Contratos de Serviços, Computação Orientada a Serviço, Engenharia de Software, GQM, ICP-Brasil, Medida Provisória 2.200-2, Reúso, SOA

Abstract

This project aims to propose and evaluate a digital signature software implementation. The research was motivated by all problems found in the current building process of university extension certificates at Universidade de Brasília. Besides to propose the digital signature software implementation based on service-oriented architecture, this research use the Victor R. Basili's GQM approach to evaluate whether those functionalities fit the institution's goals. This development proposal was based on regulation and standards specified by Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil and the Medida Provisória 2.200-2, submitted on 24th August 2001. Thus, we can ensure the same legal characteristics of the physical documents will be in the digital one. It means that the digital document should be trusted in jurisdictional sphere.

Keywords: Digital Signature, Digital Certificate, Service Contract, Service-oriented Computation, Software Engineering, GQM, ICP-Brasil, Medida Provisória 2.200-2, Reusability, SOA

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

AC Autoridade Certificadora. 8, 10, 12, 14, 18

ACT Autoridade Certificadora de Tempo. 29, 30

BPMN Business Process Model Notation. 10

EEA Entidade Emissora de Atributo. 29

GQM Goal Questions Metrics. 4

ICP-BRASIL Infraestrutura de Chaves Públicas Brasileira. 12, 14, 15

JVM JAVA Virtual Machine. 36

LCR Lista de Certificados Revogados. 14

MP Medida Provisória. 7

OCSP Online Certificate Status Protocol. 12, 14

SOA Arquitetura Orientada a Serviço. 18, 19

XML Extensible Markup Language. 15, 16

Capítulo 1

INTRODUÇÃO

Nessa capítulo, serão discutidos os problemas que motivaram a proposta, os objetivos da pesquisa e a organização do trabalho.

1.1 DEFINIÇÃO DO PROBLEMA

A Universidade de Brasília - UnB, por ser uma instituição de ensino, precisa emitir certificados e diplomas aos alunos que concluem as atividades de graduações, pós- graduação e cursos de extensão. Não só a UnB, mas as instituições voltadas à educação, de modo geral, carregam alguns problemas no processo de emissão certificados e esses serão descritos nas seções seguintes.

GASTO DE RECURSOS: A quantidade de certificados emitidos em 2013 está em torno de 200 mil, esse número compreende somente a emissão dos certificados de extensão ofertados pela UnB. Cada certificado precisa ser impresso em papéis especiais cujo o custo é de 14,00 reais por folha. Fazendo esse cálculo percebe-se que a despesa da instituição com as emissões está em torno de 2,8 milhões de reais. Esse valor foi baseado somente no custo do papel especial. Há outras despesas que não foram contabilizadas mas também estão relacionadas ao processo de emissão, tais como os gastos com recursos humanos, toner de impressão, equipamento, energia, etc. Recursos de pessoal são necessários em todo o processo de emissão do documento, desde sua geração, passando pela fase da autenticação até a sua entrega ao destinatário. Em alguns casos, os certificados de extensão são enviados aos participantes via postal.

BUROCRACIA NA ENTREGA DO DOCUMENTO AO REQUERENTE: Toda a burocracia que envolve o processo de emissão do certificado acarreta em uma demora na entrega do documento ao seu requerente. O primeiro processo a se considerar é

a compra do papel especial para emissão do certificado, pois para aquisição de produtos e serviços pela Administração Pública devem ser firmados os contratos sob normas da lei 8.666/93 cujo o processo licitatório tem, em média, o prazo de 12 doze meses para finalização. Isso faz com que em certos períodos não tenha papel disponível para emissão do certificado. O segundo processo é o de geração, impressão e autenticação do certificados. Trata-se de um processo onde parte dele é feito de forma manual, dependendo da realização de pequenas atividades até seu estado final. Em alguns casos o certificado precisa ser enviado ao requerente via postal, atrasando ainda mais o recebimento do documento. A demora, devido à forma como são realizadas as várias atividades do processo de emissão, pode deixar de atender algumas das necessidades de urgência do requerente, como por exemplo inviabilizá-lo de fornecer o seu certificado para uma entidade que necessite de tal comprovação, causando-o algum tipo de ônus.

FALSIFICAÇÃO: A falsificação de documento comprobatório de grau ou de participação em cursos é um problema tanto para instituição que emite como para aquela que necessita atestar a veracidade das informações. Empresas públicas, autarquias, fundações, conselhos trabalhistas (CRM, CREA, etc) são exemplos de instituições que necessitam comprovar as informações de títulos fornecidas pelo requerente para a realização de uma possível contratação ou autorização de trabalho. Um documento físico, ou seja, impresso em papel, mesmo que seja um papel especial, está passível de falsificação ou alteração de dados. Alguém com um diploma falso de medicina poderia estar exercendo a profissão caso conseguisse uma autorização junto ao conselho trabalhista responsável apresentando documentação falsificada. Esse exemplo de adulteração de documento não só constitui crime mas também acarreta risco à saúde da população. Há relatos de falsificações de diplomas em instituições de ensino superior como pode ser visto em [24]. Na referência são citados casos que ocorreram na USP - Universidade de São Paulo onde foram descobertas 20 incidências de diplomas falsos. Em um dos casos, a candidata tentou pleitear uma vaga em um instituto da USP com um título falso de mestrado. A falsificação foi descoberta porque o número do registro do diploma não existia na instituição de origem.

1.2 OBJETIVO

Esse trabalho tem como objetivo validar uma implementação de software de assinatura digital de documentos da Universidade de Brasília. A implementação tem foco na resolução dos problemas da instituição relacionados à emissão dos certificados de extensão bem como prover uma forma reutilizável das funcionalidades de assinatura para outros processos da universidade. Essa proposta de implementação tem em vista:

- A resolução dos problemas inerentes ao documento físico como o gasto com suprimentos (papéis, toner, etc), a demora na entrega e a falsificação;
- O atendimento das diretrizes definidas pela Medida Provisória 2200-2, para com isso garantir ao documento digital assinado as mesmas prerrogativas de um documento físico;
- Propor uma forma de integrar e reutilizar as funcionalidades de assinatura digital aos demais sistemas da Universidade de Brasília que porventura necessitem assinar outros tipos de documentos.
- Avaliar o tempo e os custos do processo de emissão de certificados a serem obtidos pela implementação do software.

1.3 ORGANIZAÇÃO

O restante desse trabalho desse trabalho está organizado da seguinte forma:

Capítulo 2: Esse capítulo faz um resumo dos principais assuntos da proposta. Em primeiro momento, são abordados alguns princípios computacionais, de infraestrutura e legislação básica que sustentam a certificação digital no Brasil. Depois, é feito um estudo dos requisitos técnicos de software de assinatura digital definidos pela ITI. Por fim, temos uma visão do impacto das assinaturas digitais nos processos de algumas organizações e como o paradigma da computação orientada a serviço tem sido parte do planejado do desenvolvimento de software.

Capítulo 3: Esse capítulo fundamenta a proposta de arquitetura baseada em alguns princípios da computação orientada a serviço. Aqui, cada decisão arquitetural será explicada com base em um princípio. Por fim, é dada uma sugestão de implementação dos procedimentos de assinatura digital que atenda às necessidades do negócio da instituição de acordo com as normas e diretrizes definidas pela .

Capítulo 4: Nesse capítulo é apresentada a abordagem GQM para a avaliação e mensuração do software criado com base nessa proposta. Foram realizados alguns testes em nível operacional do software, bem com fora feitas pesquisas sobre impacto de sua implementação na Universidade de Brasília para a realização as assinaturas dos certificados de extensão.

Capítulo 5: Nesse capítulo serão feitas as considerações finais sobre os resultados obtidos no capítulo anterior.

Capítulo 2

Revisão de Literatura

Nesse capítulo, será feita uma revisão de assuntos pertinentes a assinatura digital no Brasil, a incorporação de sistemas de assinatura digital nas organizações e a abordagem da arquitetura orientada a serviços no planejamento do desenvolvimento de arquiteturas de software.

2.1 VISÃO GERAL ACERCA DO DOCUMENTO DIGITAL

Nessa seção, serão abordados assuntos relacionados à regulamentação, aos fundamentos computacionais que amparam assinaturas digitais e a forma como as organizações vêm adotando os documentos eletronicamente assinados.

2.1.1 Assinatura Digital, Certificação Digital e Infraestrutura de Chaves Públicas

A assinatura digital é um procedimento computacional que se utiliza de algoritmos criptográficos e funções de *hash* para garantir ao documento assinado os princípios de *autenticidade* (onde o receptor pode confirmar a assinatura feita pelo emissor), *integridade* (onde há a garantia de que o documento não foi modificado) e *irretratabilidade* (onde o emissor não pode negar a autoria da assinatura).

Para que o princípio da *autenticidade* e *irretratabilidade* sejam garantidos é necessária a implementação de outro procedimento que dê suporte à assinatura digital. Esse processo é o que chamamos de certificação digital.

A certificação digital tem como finalidade comprovar a identidade do usuário das chaves criptográficas. Através do certificado digital, podemos associar as informações

relativas ao dono das chaves tal como nome, endereço, CPF, além do valor da sua chave pública.

O certificado digital pode ser visto como um documento de identificação tal qual o RG ou CNH, no que diz respeito à conferência da veracidade do portador. Certificados digitais são emitidos por uma ICP – Infraestrutura de Chaves Públicas. As ICPs são conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais com base na criptografia assimétrica. Seu principal objetivo é a manipulação segura e eficiente das chaves públicas geradas [23].

O padrão utilizado de certificados digitais hoje em dia é o ITU-T X.509, que está em sua versão 3. Esse padrão foi criado para permitir a interoperabilidade entre aplicações que o utilizem. A RFC 5280 [13] define com detalhes o formato do certificado X.509, seus principais atributos e extensões (Apêndice A).

Em termos de legislação relacionada ao documento digital no Brasil, temos a MP Nº 2.200-2 [5] que age como instrumento legal para a sustentação das diretrizes que regem o documento assinado digitalmente, além de instituir a ICP-BRASIL, que é o órgão responsável pela garantia da autenticidade, da integridade e da validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

2.1.2 Medida Provisória nº 2.200-2

A MP Nº 2.200-2 [5] é o instrumento que normatiza e confere ao documento digital assinado as mesmas prerrogativas jurídicas do documento físico assinado a punho. A medida provisória está em vigor até que o Projeto de Lei – PL 7.316/2002 seja aprovado ou seja revogada por medida provisória ulterior.

A medida provisória instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-BRASIL e transforma o Instituto Nacional de Tecnologia da Informação em autarquia, além de prover outras regulamentações.

Uma parte extraída da legislação que diz respeito à veracidade dos documentos eletrônicos pode ser vista no seguinte trecho:

> Art 10. §1º- As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-BRASIL presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1º de janeiro de 1916 - Código Civil.

Outra parte importante da legislação a ser citada é o §2º do mesmo artigo, cujo teor indica a não proibição do uso de outras infraestruturas que não fazem parte da cadeia hierárquica da ICP-BRASIL para a criação e validação dos documentos eletrônicos.

Porém, esse documento só terá validade se for admitido pelas partes ou for aceito pela pessoa a quem o for oposto. Desse modo, não é possível garantir a validade jurídica em documentos produzidos fora do âmbito da ICP-BRASIL. Assim foi definido na medida provisória como pode-se ver no texto abaixo:

> Art 10. §2º- O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

No presente trabalho faremos a proposta a luz do artigo 10 §1º, onde documentos serão assinados por certificado digital emitido por AC pertencente à hierarquia da ICP-BRASIL.

2.1.3 A Incorporação da Assinatura Digital nos Processo Internos das Instituições

Instituições públicas e privadas estão incorporando cada vez mais o uso de documentos assinados digitalmente em seus processos. Os principais benefícios citados pelas empresas é a redução de custos como a impressão do documento, do envio e a redução do custo operacional. É citado também como benefício a facilidade de verificação da legitimidade do documento. A conferência da integridade das informações e autoria da assinatura torna-se um processo mais rápido e eficiente no documento digital do que no documento físico.

A empresa COMGÁS, responsável pela distribuição de gás canalizado no estado de São Paulo, trocou os seus processos de celebração de contratos em papel por contratos realizados através dos certificados digitais. Segundo o que foi relatado no 12º CERTFORUM 2014 em Brasília, a COMGÁS obteve uma redução de 20% com gastos de suprimentos de impressão tal qual papel, toner, etc.

O principal motivo para a COMGÁS ajustar seus processos contratuais foi devido à velocidade que esse procedimento digital poderia propiciar às novas celebrações contratuais. Devido a distância entre as partes interessadas, ao firmar um contrato com a empresa, a celebração desses levava uma média de 20 dias, e com a adoção dos procedimentos da assinatura digital esse tempo foi reduzido para 4 horas. A possibilidade das partes não necessitarem mais estar geograficamente no mesmo lugar para assinarem os papéis foi um ganho bem recebido pela empresa no que se refere à celeridade.

No campo da educação, temos a USP que já adotou os processos de certificação digital na assinatura dos diplomas de graduação. Segundo artigo encontrado em [2, Revista IDigital], a implementação da assinatura digital dos diplomas de graduação reduziu de 10 para 4 o número de etapas do processo, iniciado da confecção do documento e terminando

em sua entrega ao solicitante. Assim como a COMGÁS, a USP teve como grande benefício uma maior fluidez nas atividades e etapas realizadas, além de reduzir os custos inerentes ao documento físico. Além disso, outro benefício trazido pela certificação foi a diminuição, de forma considerável, da taxa de erros ao fim do processo de confecção do diploma de graduação.

2.1.4 Padrões de Assinatura Digital

Os padrões utilizados pela ICP-BRASIL para a assinatura digital são o CAdES[9] e o XAdES[10]. Esses padrões foram criados com o objetivo de minimizar as diferenças entre implementações e maximizar a interoperabilidade das aplicações para geração e verificação de assinaturas digitais.

O padrão CAdES é recomendado para assinaturas em qualquer tipo de documento enquanto que o XAdES é utilizado para assinar os documentos em formato `.xml`.

O ITI define em seu Documento de normas [19] o conjunto de atributos assinados e não assinados tanto do padrão CAdES quanto as propriedaes assinadas e não assinadas padrão XAdES.

2.2 REQUISITOS TÉCNICOS DEFINIDOS PELA ICP-BRASIL PARA SOFTWARE DE ASSINATURA DIGITAL

Nessa seção, será feita uma análise dos procedimentos necessários para a assinatura e a verificação de documentos digitais. Os principais procedimentos são: Validação do certificado digital, Assinatura do documento digital e Verificação do documento digital. Os requisitos técnicos fora extraídos de [14, Manual de normas técnicas] e transformados em notações BMPN para um melhor entendimento.

2.2.1 Requisitos de Validação do Certificado Digital

O processo de validação do certificado digital descrito nessa seção é importante pois se faz presente nos outros dois processos de assinatura digital ICP-BRASIL, tanto nos procedimentos de assinatura do documento digital quanto no procedimentos da verificação da assinatura. Esses procedimentos serão descritos nas seções 2.2.2 e 2.2.3.

A validação do certificado digital consiste em fazer uma verificação de conformidade em toda a cadeia de certificados. Partindo do certificado utilizado para assinar o docu-

mento, ou seja, o nível mais inferior, passando por toda a cadeia de certificados das ACs intermediárias até chegar ao nível mais superior, a AC raiz.

Assim sendo:

Um caminho de certificação consiste de uma sequência de "n" certificados digitais {1, ..., n}, sendo que o primeiro certificado corresponde ao da entidade considerada como âncora de confiança, ou seja, a AC Raiz. O n-esimo certificado corresponde ao certificado que deve ser validado, neste caso, o de entidade final [14].

Cada certificado da cadeia terá sua validação realizada da mesma forma até chegar ao último, o da AC Raiz. Utilizamos nesse trabalho a anotação BPMN de uma atividade cíclica para representar a validação de toda a cadeia de um certificado digital. Essa atividade simula a operação de *Do-While*, significa dizer que haverá validação até o último certificado da cadeia. A figura abaixo representa a anotação:

Figura 2.1: Atividade cíclica.

Nos próximos dois tópicos serão detalhados os processo de validação da cadeia de certificados e a atividade de verificação da revogação do certificado.

a) Validação da Cadeia de Certificados

A figura a seguir mostra cada atividade do processo de validação de certificado:

Para facilitar essa seção, utilizaremos com exemplo a cadeia de certificados A, B, C, D, sendo que, A é o certificado da AC raiz e o D será o certificado utilizado para a assinatura de documentos.

Sempre o primeiro certificado a ser validado é o do usuário, no nosso exemplo será o D, pois ele representa o certificado que foi utilizado para assinar os documentos digitais.

De acordo com a figura 2.2, seguem as atividades:

Verificação Criptográfica da Assinatura do Certificado: É verificado se D foi realmente assinado por C.

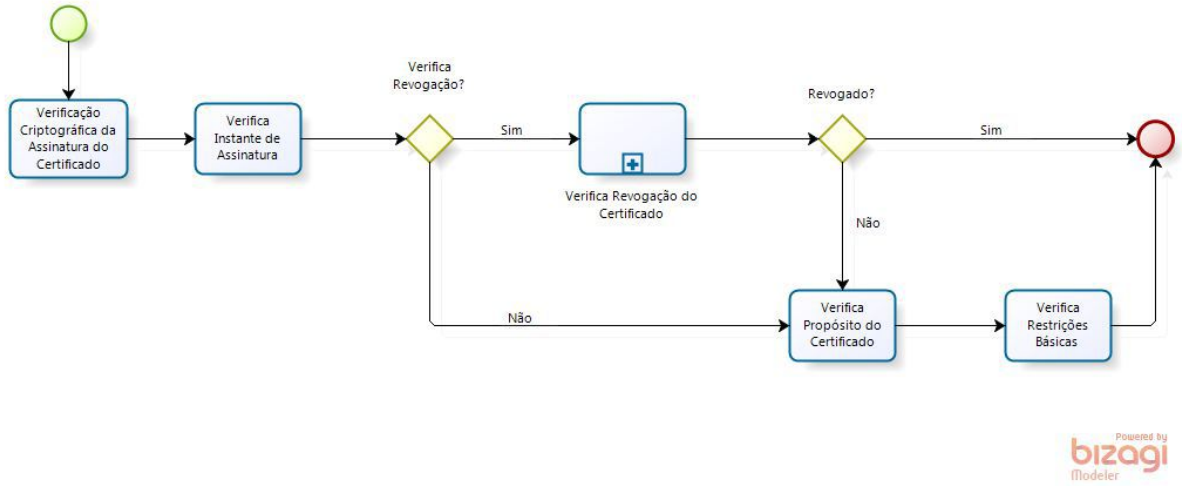

Figura 2.2: BPMN - Validação da Cadeia de Certificados.

Verifica Instante de Assinatura: É verificado se D foi realmente assinado de acordo com o período de validade do certificado C. O atributo do certificado C, *Validity (not before, not after)*, define o intervalo ao qual suas assinaturas serão válidas. Portanto, a assinatura do certificado D feita por C, para que seja válida, deverá estar dentro do período estipulado nesse atributo.

Verifica Revogação do Certificado: Tópico b) dessa seção.

Verifica Propósito do Certificado: É verificado o propósito de uso do certificado D. Nessa etapa é feita a verificação dos atributos *KeyUsage* e *extendedKeyUsage* para saber se o propósito de uso ao qual o certificado foi emitido corresponde ao tipo atividade que está sendo realizada. Os certificados podem ser emitidos com próposito de Assinatura ou Sigilo (Apêndice B), esses atributos fazer parte da extensão dos certificados x.509 v3 e são definidos pela [13, RFC 5280] da seguinte forma: *digitalSignature*, *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, *keyAgreement*, *keyCertSign*, *cRLSign*, *encipherOnly*, *decipherOnly*. No nosso exemplo, já que estamos utilizando o certificado D, cuja função é a assinatura de documento, seu atributo deverá estar declarados na extensão com os valores *digitalSignature* e o *nonRepudiation*.

Verifica Restrições Básicas: É verificada as restrições básicas de D. Essa atividade consiste em verificar se o certificado digital está sendo usado de acordo com a combinação entre seu próposito de uso definido no atributo *Key Usage* e suas restrições básicas definidas na extensão *Basic Constraints*. No caso de certificados de entidades finais, com propósitos de uso de assinatura ou sigilo, não deve conter a restrição *cA* na extensão *Basic*

Constraint. Já em certificados de autoridades certificadoras, quando o propósito *KeyCertSign* estiver declarado no atributo *Key Usage* a restrição deve aparecer obrigatoriamente na extensão *Basic Constraint*.

O ciclo de verificações continua até o final da cadeia de certificados, em nosso caso, faríamos as mesmas validações no certificado C até chegar ao certificado raiz A.

Nota-se pela figura 2.2, que o procedimento de validação de certificados definido pela ICP-BRASIL possibilita ao usuário escolher se deseja verificar o estado de revogação do certificado. Porém, os documentos assinados com certificados revogados não são válidos perante a justiça.

b) Verificação da Revogação do Certificado

Quando um certificado digital é emitido, um período de validade de uso é definido. Entretanto, sob diversas circunstâncias, um certificado digital pode tornar-se inválido antes de sua data de expiração e ser revogado pelo seu proprietário [14].

Existem dois métodos de consulta de revogação de certificados que são o LCR – Lista de Certificados Revogados [13] e o OCSP – *Online Certificate Status Protocol* [12].

A LCR é uma lista cronologicamente selada (*timestamped list*) que identifica certificados digitais revogados e, além disso, é assinada pela AC que a torna disponível em um repositório público.

Outra forma de se obter informações sobre a revogação de um certificado digital é por meio do protocolo OCSP (*Online Certificate Status Protocol*) que, de forma imediata (*on-line*), permite que o estado de revogação de um certificado digital seja verificado instantaneamente.

A ICP-BRASIL, por sua vez, não definiu nível de prioridade de uso de um ou outro método que verifica a revogação. Na especificação somente foi dito que essa verificação deverá ser realizada por uma das duas formas. Subentende-se então que o desenvolvedor do software de assinatura deverá escolher a forma de implementação mais adequada ao seu negócio no que tange a verificação de revogação.

A Figura 2.3 mostra cada atividade do processo de verificação de revogação do certificado. seguem as atividades:

Escolhe Método de Consulta de Revogação: Essa atividade corresponde à implementação feita pelo desenvolvedor, nesse caso, se a programação feita no software de assinatura fará uso da ou da OCSP para a verificação. O usuário do software assinador

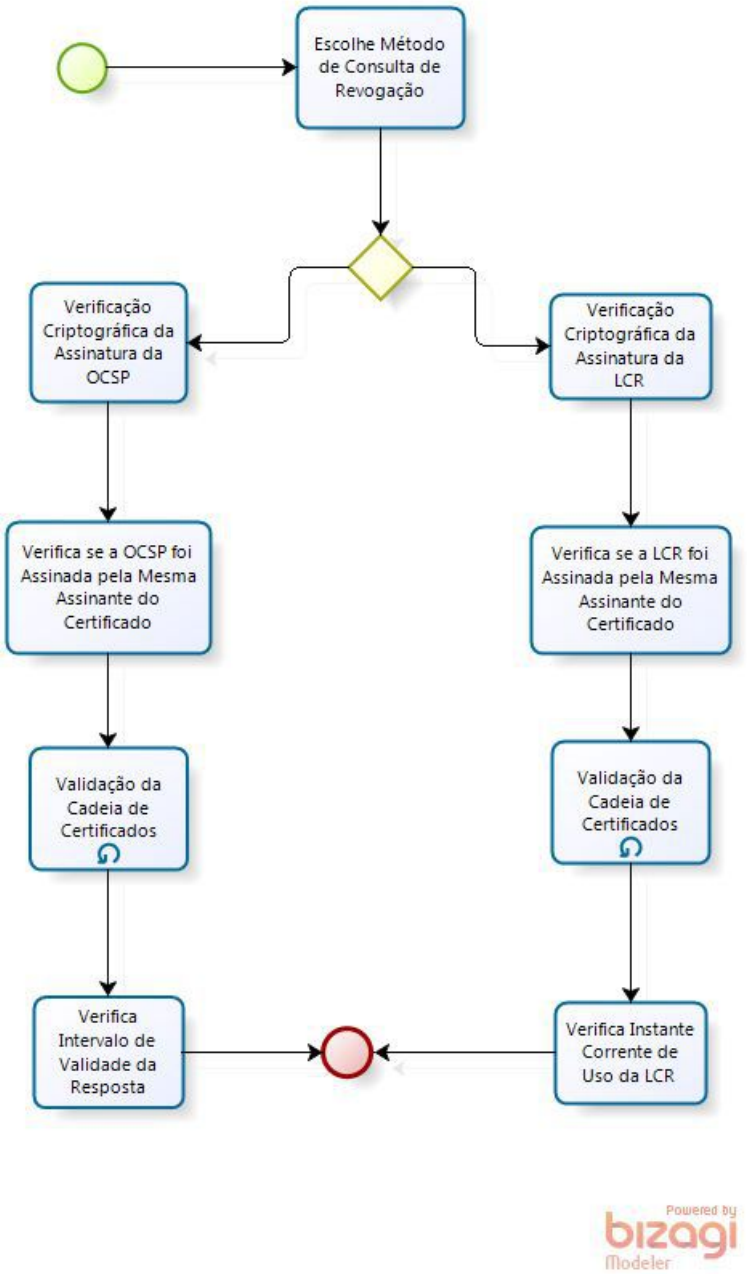

Figura 2.3: BPMN - Verifica Revogação do Certificado.

somente poderá decidir se deseja que a consulta de revogação do certificado seja feita, mas não o método de consulta utilizado para obter a informação.

Verificação Criptográfica da Assinatura da OCSP/LCR: É verificado se a LCR ou a mensagem OCSP foi realmente assinado pela chave pública especificada. Para isso é feita uma verificação através da chave pública da AC.

Verifica se a OCSP/LCR foi Assinado pela mesma Assinante do Certificado: Essa atividade verifica se a LCR ou a resposta OCSP foi assinada pela mesma AC que assinou o certificado digital ao qual estão inseridas. A finalidade desse procedimento é coibir que sejam utilizadas LCRs ou mensagens OCSP de outro lugar que não sejam da AC emissora do certificado digital verificado.

Validação da cadeia de certificados: O procedimento visto no tópico a) dessa seção é o mesmo utilizado aqui com as seguintes exceções: Quando for a LCR, é verificado em todo o certificado se a extensão *Key Usage* contém o propósito *cRLSign*. No caso da OCSP, os propósito *digitalSignature* e/ou *nonRepudiation* devem estar declarados na extensão *Key Usage* e o propósito *OCSPSigning* deve estar presente na extensão *Extended Key Usage*.

Verifica Intervalo de Validade da Resposta OCSP: Essa atividade verifica se a resposta OCSP está dentro do intervalo de validade, nesse caso o software deverá fazer essa verificação e descartá-la quando estiver fora do período estipulado.

Verifica Instante Corrente de Uso da LCR: Essa atividade verifica se o seu instante de uso não é posterior ao valor de tempo registrado em seu campo *nextUpdate*. O propósito dessa verificação é fazer com que o software assinador utilize sempre uma LCR atualizada, caso esta esteja sendo usada em um momento posterior ao tempo registrado em *nextUpdate*, deverá então ser descartada.

2.2.2 Requisitos de Assinatura do Documento Digital

O processo de assinatura do documento digital pode ser visto na figura 2.4:

Todo certificado digital a ser utilizado para a assinatura de um documento deverá ser submetido ao processo de validação da cadeia de certificados descrito na seção 2.2.1. Isso serve para garantir que a assinatura do documento será feita por certificado válido dentro

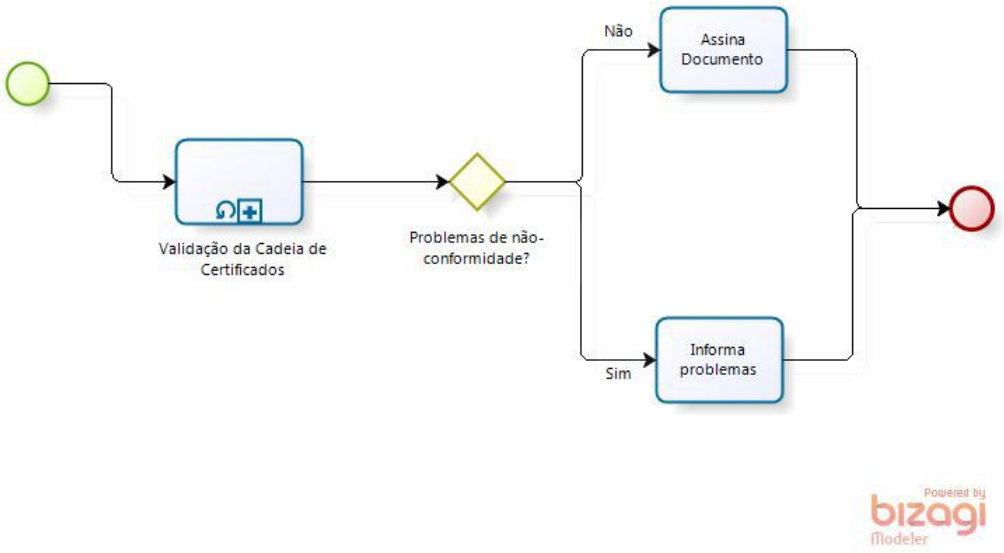

Figura 2.4: BPMN - Validação do Certificado.

da cadeia hierárquica da ICP-BRASIL.

O primeiro passo para a assinatura é a escolha do documento a ser assinado e do certificado digital do usuário responsável pela assinatura. Então temos:

Validação da Cadeia de Certificados: Ver seção anterior, 2.2.1.

Assina Documento: O documento é assinado em CMS "*SignedData*" *Attached*, CMS "*SignedData*" *Detached* ou XML *Signature*.

Informa Problemas: Informa ao usuário quais os requisitos do certificado digital escolhido não estão em conformidade.

A ICP-BRASIL define que o software de assinatura digital deve oferecer ao usuário no mínimo uma das opções de assinatura de documento que são o CMS "*SignedData*" *Attached*, CMS "*SignedData*" *Detached* ou XML *Signature*.

No momento da assinatura, o software deverá possibilitar ao usuário a escolha do certificado digital a ser utilizado para assinar o documento. O certificado digital do usuário poderá ser encontrado em equipamentos de hardware tais quais os *tokens*, os *smart cards* e HSM.

Caso o certificado digital não esteja em conformidade, o software de assinatura deverá alertar a entidade usuária ressaltando que o mesmo não deveria ser utilizado. **Veja que a**

ICP-BRASIL fala em sua especificação de alertar o usuário, mas não o proíbe de assinar o documento com um certificado digital em não conformidade, ou seja, inválido.

Com relação ao processo de geração de assinatura digital, podemos ter três contextos diferentes: assinaturas simples, coassinaturas e contra-assinaturas. A geração de assinatura digital simples ocorre quando uma única assinatura digital é gerada sobre um conteúdo digital disponível. A geração de coassinaturas digitais ocorre quando duas ou mais assinaturas digitais são geradas de forma paralela e independente pelos signatários, utilizando conteúdos digitais idênticos. Cada coassinatura gerada pode conter atributos assinados e não assinados próprios. A geração de contra-assinaturas digitais ocorre quando uma ou mais assinaturas digitais são realizadas sobre a sequência de *bytes* (bloco) que representa uma assinatura digital já existente. Uma contra-assinatura pode conter outros atributos assinados próprios [18].

Em documentos coassinados, o software assinador deverá verificar se há mais de uma assinatura e permitir ao usuário visualizar as informações delas incluindo: a identificação do assinante; data e hora; qualquer outra informação do certificado que for de interesse para o negócio.

O software assinador tem como requisitos expressos no manual de normas técnicas da ICP-BRASIL as funcionalidades de extrair o documento presente nas assinaturas do tipo CMS "*SignedData*" *Attached* e no XML *Signature* bem como ser capaz de inserir neles o certificado digital correspondente à assinatura e os respectivos certificados do caminho de certificação correspondente [14].

Recomenda-se que o Software de Assinatura Digital possa ser capaz de inserir no documento eletrônico assinado digitalmente (CMS "*SignedData*" ou XML *Signature*) as LCRs correspondentes aos certificados digitais de assinatura [14].

2.2.3 Requisitos de Verificação do Documento Digital

O Processo de assinatura do documento digital pode ser visto na figura 2.5:

Depois de selecionado e submetido o documento digital para validação de assinatura temos:

Verificação Criptográfica da Assinatura Digital: É verificado se o documento digital foi realmente assinado pelo certificado digital do usuário.

Validação da Cadeia de Certificados: Ver procedimento da seção 2.2.1.

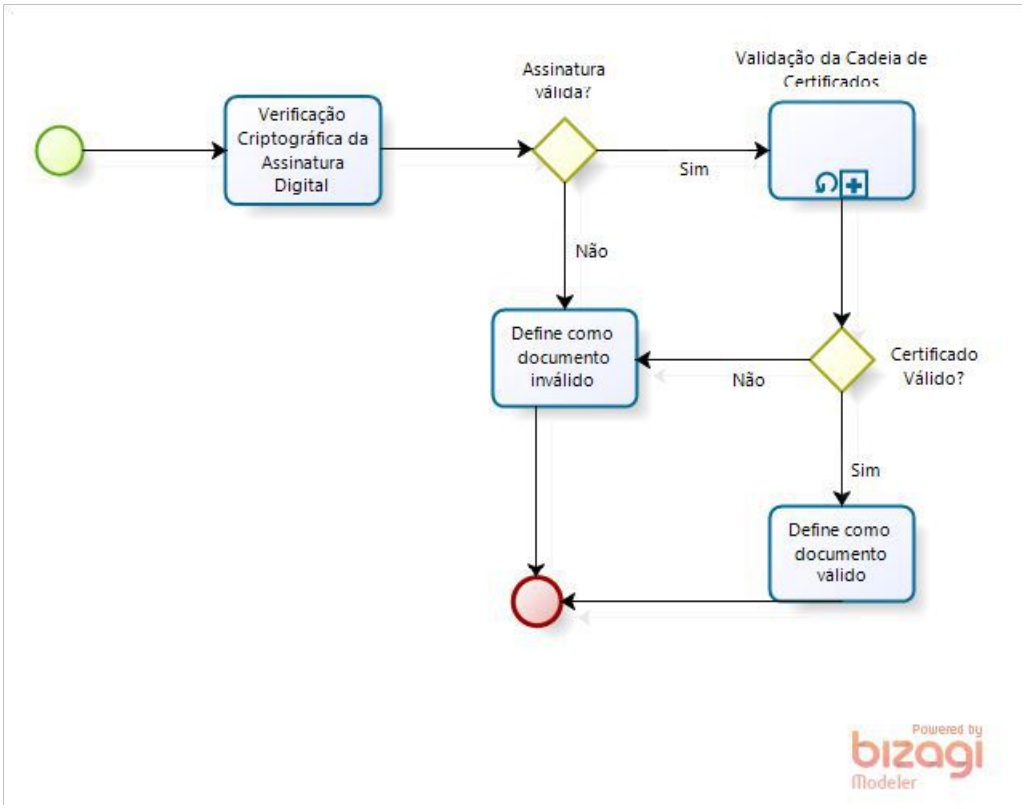

Figura 2.5: BPMN - Verificação do Documento Digital.

Define Documento como Válido: Se a assinatura digital corresponde ao certificado digital do usuário e o certificado está em conformidade com as normas da ICP-BRASIL, então o documento é autêntico.

Define Documento como Inválido: Se a assinatura digital não corresponde ao certificado digital do usuário ou o certificado não está em conformidade com as normas da ICP-BRASIL, então o documento não é autêntico. Nesse caso, o software deve alertar ao usuário sobre o quesito de nulidade do documento, ou seja, deve apresentar o motivo pelo qual aquela assinatura não o torna válido.

Outro requisito importante para o software assinador e a possibilidade da visualização do conteúdo presente no documento assinado. Em documentos assinados no formato CAdES, o documento e a assinatura são anexados em um único arquivo com extensão `.p7s` [11].

Quando existir mais de uma assinatura, software assinador deverá mostrar o resultado da verificação de cada uma junto do valor do atributo "*Signing Time*", além disso, deverá permitir que o usuário veja as informações dos certificados que assinaram o documento.

Como pode ser visto na Figura 2.5, mais uma vez se fez presente o processo de validação da cadeia de certificados, pois o documento só terá validade jurídica se tiver sido assinado por certificado digital emitido por AC pertencente à hierarquia da ICP-BRASIL.

2.3 ARQUITETURA DE SOFTWARE

Um projeto arquitetural de um software define como os diversos componentes das aplicações irão se relacionar. Nesse capítulo serão abordados os benefícios da orientação a serviços e como o SOA vem sendo adotado pela indústria na tentativa de resolução dos problemas relacionados ao desenvolvimento de softwares corporativos.

2.3.1 Benefícios da Computação Orientada a Serviços

Um dos benefícios para o negócio que o paradigma de orientação a serviços pode trazer para a Universidade de Brasília é a economia nos custos de desenvolvimento de soluções de software. Segundo Erl [8], aplicar consistentemente a orientação a serviços em uma empresa de TI resulta em um menor custo operacional e menos despesas indiretas associadas à governança e a evolução dos ativos de software

Parte do estudo da computação orientada a serviço se refere ao SOA, ou *Service-Oriented Architecture*. Nesse modelo arquitetônico os serviços são posicionados como soluções lógica alinhadas aos objetivos estratégicos da empresa [8].

O paradigma SOA não foca na tecnologia a ser utilizada e sim em serviços de software que podem ser adicionados aos ativos de informação da empresa de forma gradativa para melhor atender às necessidade do negócio.

Os benefícios específicos que o SOA pode trazer a um ambiente de desenvolvimento são [25]:

Eficiência: A modularidade dos serviços, devido ao baixo acoplamento e interfaces bem definidas permitem um desenvolvimento sem a dependência direta de outras funcionalidades, tornando o desenvolvimento dos serviços e a disponibilização dos recursos mais eficiente.

Reutilização: O SOA prega a reutilização de suas funcionalidades para a diminuição dos custos e do tempo de desenvolvimento. O baixo acoplamento entre as funcionalidades é fundamental para a reutilização eficiente dos serviços.

Simplificação da Manutenção: A simplicidade na manutenção provém do baixo acoplamento dos serviços e de uso de contratos definidos. De forma prática, significa dizer

que o desenvolvedor pode fazer a manutenção nos serviços sem temer que a alteração irá causar um impacto negativo em outras funcionalidades da aplicação.

Evolução gradativa: Adições gradativas de funcionalidades de serviços podem ser implementadas de forma planejada sem causar impacto no conjunto de serviços já existente. Toda organização requer respostas rápidas às várias mudanças no negócio da instituição, a TI deverá estar preparada para responder a essas mudanças.

2.3.2 Pesquisas Relacionadas à Utilização do SOA na Indústria

Muitas pesquisas têm sido feitas relacionadas ao paradigma de serviços e aos benefícios reais que eles podem trazer a um ambiente de desenvolvimento corporativo.

Em [4] é relatada a experiência de uma empresa de planos de saúde na adoção do SOA e quais benefícios são esperados. A companhia decidiu adotar o SOA para manter a interoperabilidade dos sistemas de informação de diferentes plataformas. Concluiu-se que a iniciativa trará benefícios ao longo do tempo desde que os esforços sejam feitos em conjunto e de forma gradativa. O desenvolvimento, a arquitetura e a governança devem se manter em um processo evolutivo e iterativo.

Em [7] é relatada a iniciativa do governo da Índia para adotar o SOA a fim de elevar os sistemas de informação do governo a um nível de maior governança onde possam trazer a população maiores facilidades de acesso aos serviços oferecidos e melhor transparência das informações. Além disso, a adoção do paradigma visava prover escalibidade, integração entre projetos e o reúso dos serviços. As autores concluem que a adoção do SOA é um processo demorado e, nesse caso, a governança dos serviços precisa ser eficiente para oferecer o nível facilidades e transparência desejados.

Capítulo 3

Fundamentação da Proposta

Nesse capítulo será apresentada a proposta de arquitetura de sistema baseada nos princípios da computação orientada a serviço, bem como a proposta para a implementação dos procedimentos de assinatura digital.

3.1 VISÃO GERAL DA ARQUITETURA DA PROPOSTA

Com base nos princípios da arquitetura orientada a serviço, será proposta uma arquitetura de software que visa atender às necessidades da Universidade de Brasília.

Para isso, levou-se em consideração o funcionamento da Universidade de Brasília e as necessidades dos seus setores e departamentos relacionados ao desenvolvimento software. Observando os processos de alguns setores, vimos que muitas de suas necessidades em relação aos sistemas de informação são similares. No que tange a assinatura digital de documentos, foi observado que há interesse de diversos setores na implantação. O setor que emite os certificados de extensão (DEX) tanto quanto o setor de compras da universidade já manifestaram interesse na utilização desses recursos. Futuramente outros sistemas poderão necessitar do uso da assinatura digital.

Pensando nisso, o presente trabalho propõe implementar uma arquitetura que vise a reutilização das funcionalidades de assinatura digital de documentos a fim de diminuir os custos relacionados ao desenvolvimento de sistemas. Com base no conceito de separação de responsabilidades, a proposta tem como objetivo a implementação modularizada dos procedimentos de assinatura de forma a desacoplá-las dos sistemas que geram os documentos, ou seja, os sistemas corporativos deverão se comunicar a outro serviço para realizar os procedimentos de assinatura digital.

As funções de assinatura serão fornecidas pelo que será chamado por esse trabalho de Módulo de Assinatura Digital. Esse módulo será responsável por gerenciar os procedimentos de assinatura de documento.

O diagrama abaixo mostra visão macro da arquitetura:

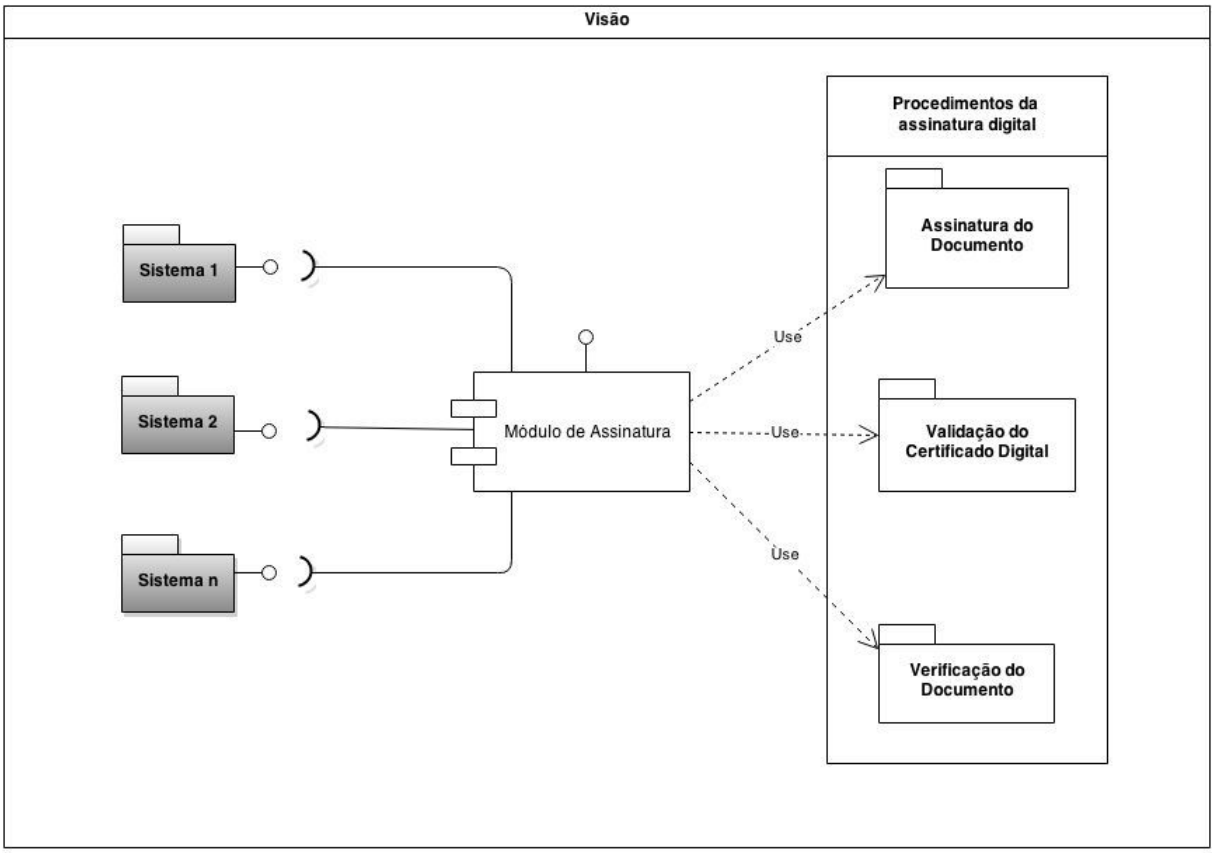

Figura 3.1: Visão arquitetural da proposta.

3.2 PRINCÍPIOS DE PROJETO

Nessa seção, as decisões de arquitetura serão detalhadas de acordo os princípios de projeto descritos em [8, Erl] e que foram adotados para propor a solução. Os princípios de projeto adotados foram o de contratos de serviços, acoplamento de serviços, abstração de serviços e capacidade de reúso do serviço.

3.2.1 Contratos de Serviços

Os contratos são o foco principal dos serviços por influenciarem o projeto como um todo no alcance do baixo acoplamento, da abstração de serviços e da reusabilidade.

Na presente proposta, os sistemas corporativos deverão oferecem ao módulo certificador, por meio de contratos estabelecidos, os serviços descritos na figura e tabela abaixo.

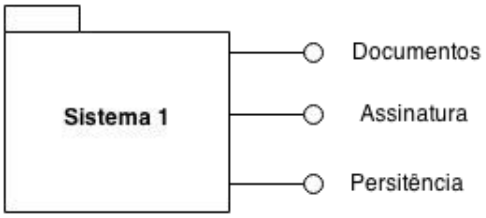

Figura 3.2: Módulo do sistema com os contratos de serviços.

Documentos	
Operação: lista	Entrada: vazio para receber a lista toda ou o número de documentos. Saída: Lista dos documentos que serão assinados.
Operação: buscarPorID	Entrada: O identificador do documento. Saída: O documento especificado.

Tabela 3.1: Serviço: Documentos

Assinatura	
Operação: tipoAssinatura	Entrada: Identificador do documento. Saída: 1 - assinatura simples; 2 - coassinatura; 3 - contra-assinatura.
Operação: carimboTempo	Entrada: Identificador do Documento. Saída: url da autoridade certificadora de tempo.
Operação: certificadoAtributo	Entrada: Certificado de atributo do assinante. Saída: *True* para permitir assinatura.

Tabela 3.2: Serviço: Assinatura

Persistência	
Operação: persisteDocumento	Entrada: O documento assinado. Saída: Sinal de *true* quando o documento for persistido.

Tabela 3.3: Serviço: Persistência

3.2.2 Acoplamento de Serviços

Acoplamento de serviços é um termo usado na TI cujo a significado remete à dependência. Espera-se, com esse princípio de design, níveis de dependência menores entre os serviços.

Para atingir o objetivo desse princípio é necessário o uso de contratos bem definidos e padronizados. O principio tem com característica o uso de contratos como forma de prover uma solução desvinculada de qualquer implementação e/ou tecnologia utilizada.

A arquitetura proposta baseou-se nesse principio como forma de propor o desacoplamento tecnológico do serviço de persistência. Para isso, foi delegado que cada sistema implemente a sua forma de persistir os documentos assinados, seja qual for a tecnologia de banco de dados ou sistemas de arquivos.

3.2.3 Abstração de Serviços

O princípio de projeto de abstração de serviços visa a ocultação de informações da implementação aos olhos do usuário.

Nessa proposta, os procedimentos de assinatura digital dos documentos serão utilizados pelo módulo de assinatura. Os procedimentos de assinatura não serão parte funcionalidades do módulo de assinatura, somente serão por ele utilizados.

Cada pacote da figura 3.3 é uma implementação proposta pelo trabalho com base no manual de normas técnicas [14]. É permitida implementações diferenciadas desses procedimentos desde que estejam contempladas pelos documentos e requisitos da ICP-Brasil. A implementação proposta por esse trabalho pode ser vista na seção 3.4.

3.2.4 Capacidade de Reúso de Serviços

A reusabilidade na arquitetura proposta está relacionada ao uso do conjunto de soluções da arquitetura por todos os sistemas sem a necessidade do desenvolvimento pontual em cada um. O reúso do módulo de certificação e dos procedimentos de assinatura digital objetiva diminuir os gastos com a programação, o retrabalho e a manutenção de funcionalidade do sistemas. Além disso, deseja-se prover o aumento escalabilidade a medida que os sistemas venham a necessitar dos procedimentos de assinatura digital.

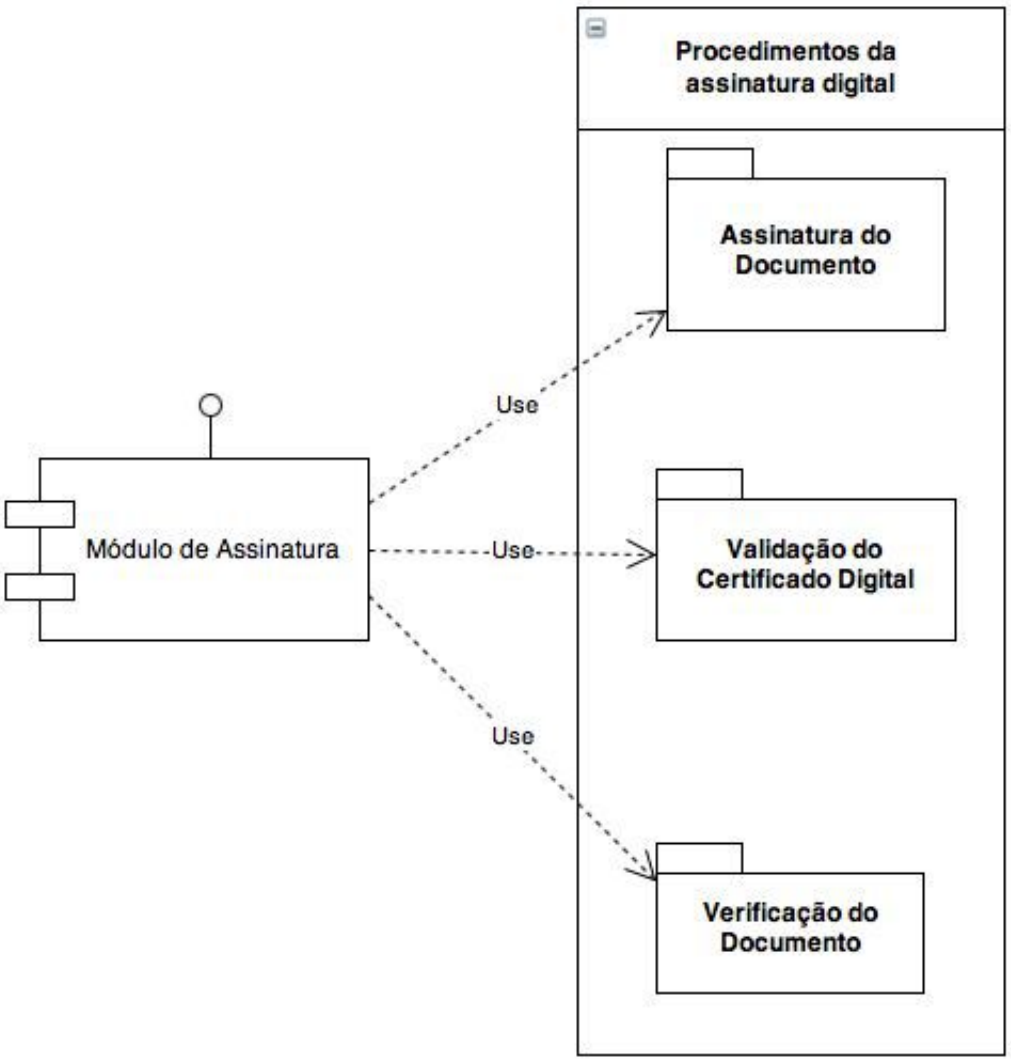

Figura 3.3: Módulo do sistema e pacotes de procedimentos de assinatura.

3.3 MÓDULO DE ASSINATURA DIGITAL

O Módulo de Assinatura Digital é a parte da arquitetura responsável por:

- Interagir com o usuário;
- Ler o dispositivo de hardware onde é feito o armazenamento da chave privada;
- Consumir os serviços dos sistemas;
- Utilizar os procedimentos de assinatura implementados nos pacotes da arquitetura;
- Fornecer serviço de Verificação do Documento Assinado.

O Módulo de Assinatura é um Applet JAVA acessado pela web mas que executa localmente no computador do cliente. Esse módulo é capaz de realizar a assinatura de um ou vários documentos de uma vez. Essa funcionalidade é chamada de assinatura em lote.

3.3.1 Requisitos de Segurança do Módulo de Assinatura

- Controle de Acesso

O acesso ao módulo será dado através da autenticação do usuário. A funcionalidade de assinatura não será pública. Somente os responsáveis pela assinatura dos documentos serão autorizados a baixar o Applet para sua máquina.

- Não manter a chave privada em memória (assinaturas em lote)

Recomenda-se que a chave privada do usuário não seja gravada em memória. A solução para isso é a criação de uma sessão de software entre a aplicação e o dispositivo de hardware. A especificação do padrão PKCS#11 [22] define como a interface da API gerencia a sessão entre o dispositivo e a aplicação.

- Garantia da origem do software

O Applet será baixado de dentro do domínio da Universidade de Brasília. O navegador irá reconhecer o domínio atraveś do certificado digital da universidade. O usuário deverá ser informando para não utilizar o módulo caso o navegador não reconheça o certificado.

- Log das operações

As operações de assinaturas serão logadas pelo módulo a fim de manter o registro das atividades de seus usuários para posterior auditoria.

3.4 IMPLEMENTAÇÃO DOS PROCEDIMENTOS DE ASSINATURA DIGITAL

Nessa seção, será feita uma proposta de implementação dos procedimentos necessários para assinar um documento digital. A proposta terá como base as normativas da ICP-BRASIL bem como as necessidades de negócio da Universidade de Brasília. Os procedimentos de validação do certificado, assinatura do documento digital e verificação do documento digital serão detalhados a seguir.

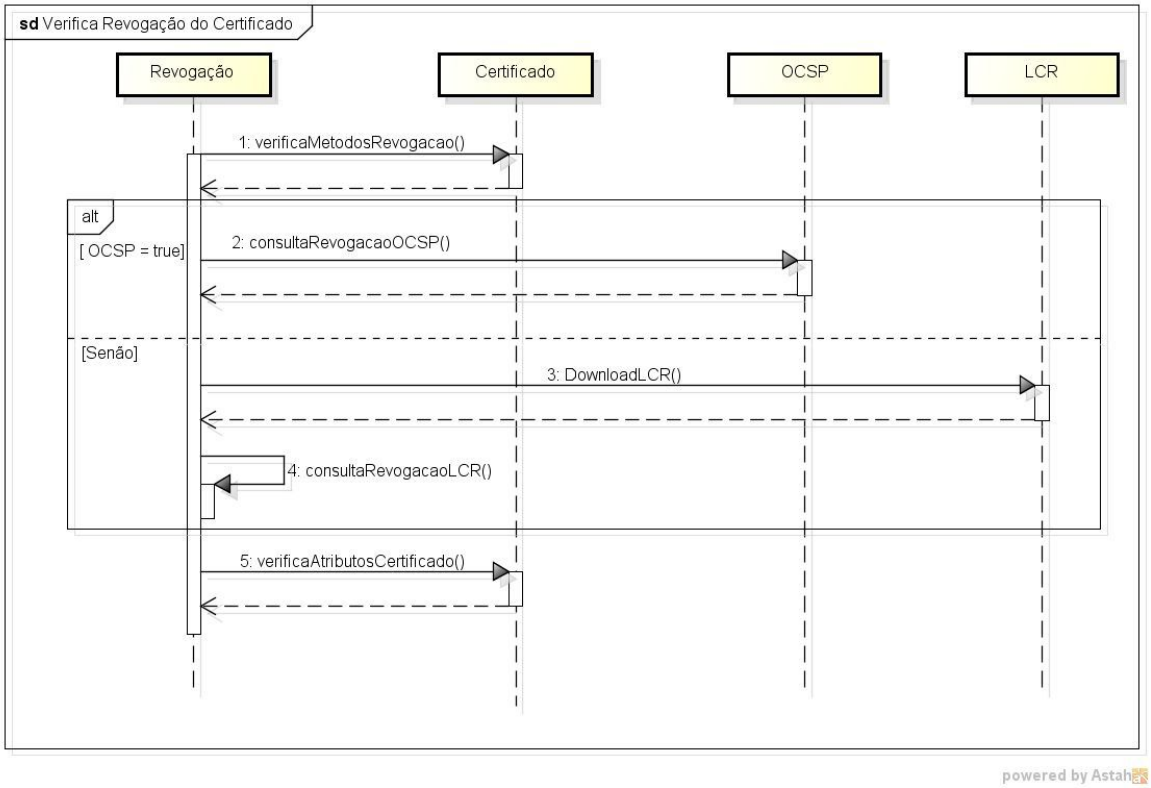

Figura 3.4: Diagrama de sequência: Proposta de validação do certificado.

3.4.1 Procedimentos de Validação do Certificado Digital

O diagrama de sequência da figura 3.4 propõe uma implementação para o processo de validação do certificado:

1: verificaMétodosRevogação – Esse método deverá ser implementado de forma que consiga extrair do certificado as formas de verificação de revogação oferecidas pela AC emissora desse. É importante saber que para a AC emissora do certificado é obrigatório o fornecimento da consulta de revogação por LCR, ficando a consulta via OCSP opcional. Nada impede a AC de fornecer as duas formas de verificação no mesmo certificado. **No entanto, a implementação proposta sugere priorizar a consulta de revogação via OCSP se ela existir, pois minimizariam os problemas inerentes às consultas LCR como: A não disponibilização da LCR no pela AC no tempo estipulado e a possibilidade assinatura de documento baseada na informação de LCR válida, porém desatualizada. Esse problemas serão expostos nos tópicos A e B da página seguinte**.

2: consultaRevogaçãoOCSP – Esse método fará a verificação da revogação do certificado via o protocolo OCSP. A vantagem de se utilizar esse protocolo é que a revogação do certificado é verificada de forma instantânea. O protocolo OCSP, de acordo com (IETF, 1999), possui três tipos de resposta à requisição: *good*, *revoked*, *unknown*. Caso a resposta tenha sido *unknown*, a implementação fará a consulta via LCR.

3: downloadLCR – Caso o protocolo OCSP não tenha sido oferecido pela AC do certificado ou a resposta OCSP tenha sido unknown, então a aplicação irá fazer a verificação através da LCR. O próximo passo é fazer o download da lista de certificados revogados mais atual.

4: consultaLCR – Com a lista armazenada do passo anterior, é feita a verificação de revogação.

5: verificaAtributosCertificado – É verificado se há alguma não conformidade em relação ao atributos de extensão do certificado, *Basic Contraints*, *Key Usage*.

O processo de validação do certificado é um passo importante para garantir a validade do documento. Documentos assinados por certificados inválidos perdem a eficácia probante e não podem ser contestados judicialmente.

Há algumas características nos métodos de consultas LCR e OCSP que precisam ser analisadas. Em consultas realizada pela LCR, por exemplo, a lista mais atual é baixada pelo software assinador e nela é verificado se o número identificador do certificado analisado está presente na lista. As ACs, geralmente, atualizam as listas em períodos de tempo determinados, podendo ser de 15 em 15, 30 em 30 minutos ou dias. O software assinador não deve utilizar a LCR se a data e hora da próxima atualização contidas no atributo *Next Update* for menor que a data e hora atual, dessa forma a LCR estaria desatualizada.

Devido ao modo como são manipuladas as LCRs, podemos incorrer nos seguintes problemas:

A) A AC não atualizar a LCR de acordo com o período estipulado em *Next Update*.

B) Um certificado foi revogado dentro do intervalo de validade da LCR.

O primeiro caso (A) acontece quando o software de assinatura tem a posse de uma LCR expirada e necessita buscar uma lista mais atual, no entanto a AC, por algum motivo, não a disponibilizou. Nesse caso, por não poder confiar em uma LCR expirada, o

estado de revogação do certificado não poderá ser verificado e como consequência o documento não poderá ser assinado naquele momento.

O segundo caso (B) será exemplificado a seguir:

1. O software de assinatura fez download da LCR às 14:00h e seu campo Next Update será 14:30h.
2. Foi verificado que o certificado A não consta nessa LCR.
3. Às 14:15h, o certificado A foi revogado pela AC emissora, mas essa revogação só será informada na próxima atualização, às 14:30h.
4. Às 14:16h, o software inicia o procedimento de assinatura do documento. Como a LCR presente em sua cache está dentro do prazo de validade e não consta nela o identificador do Certificado A, o software realizará a assinatura com um certificado revogado.

Vimos nesse caso a realização da assinatura de um documento por um certificado revogado. A consequência é que o documento assinado será tido como inválido não sendo possível gozar de seus efeitos legais.

Para minimizar esse problema, é proposto que:

a) Priorize a consulta de revogação via o protocolo OCSP.

b) Mantenha a LCR utilizada para verificar a revogação do certificado para uma posterior auditoria.

Já o protocolo OCSP, por sua vez, não apresenta a mesma lacuna que as LCRs. A consulta é feita de forma instantânea, diretamente na base de dados da AC. Um número crescente de ACs estão implementando esse protocolo que logo será tido como método padrão para consultas de revogação de certificados.

3.4.2 Procedimentos de Assinatura do Documento Digital

O diagrama de sequência a seguir propõe uma implementação para o processo de assinatura do documento digital:

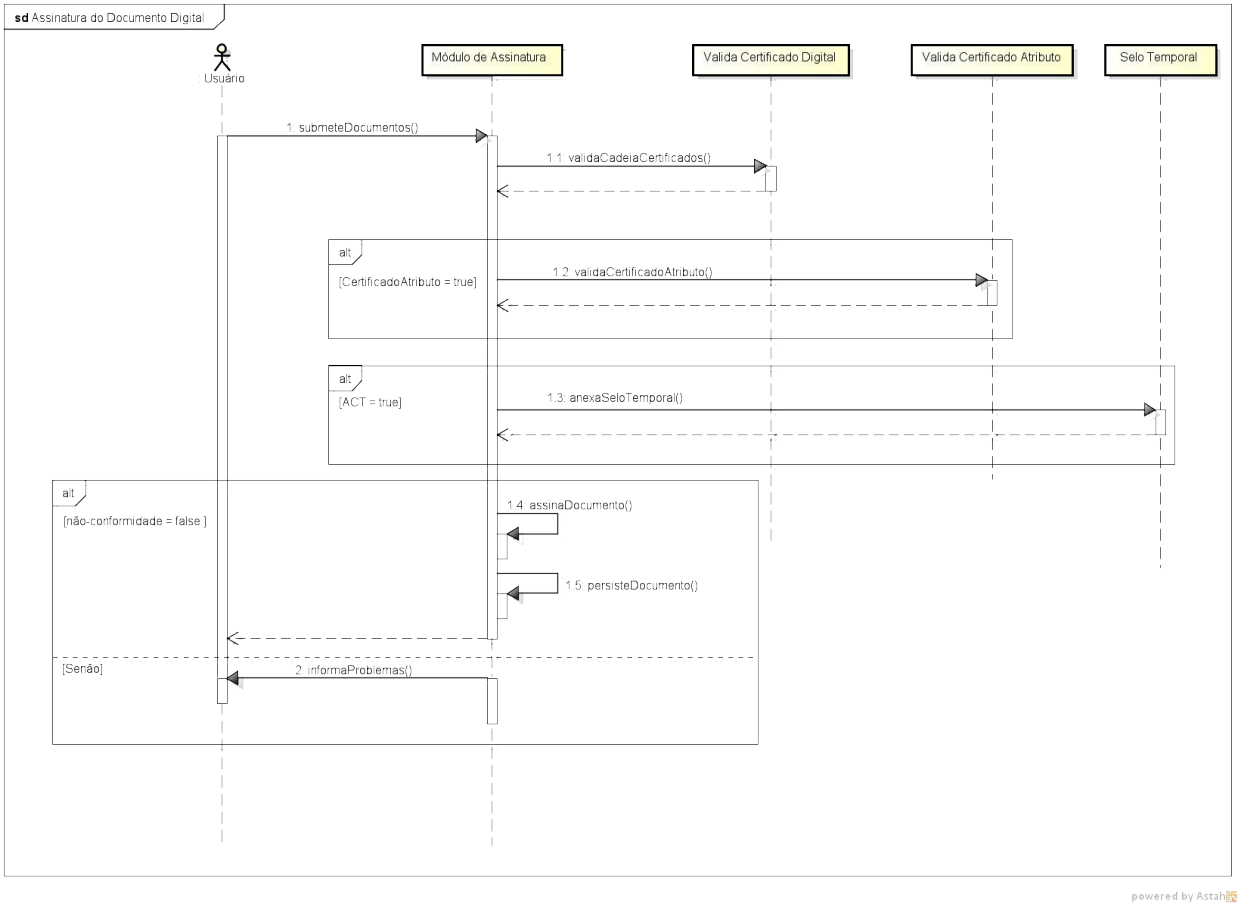

Figura 3.5: Diagrama de sequência: Proposta de assinatura do documento.

1: submeteDocumento – Nesse método o usuário deverá submeter o documento que irá ser assinado, a chave privada de assinatura e, eventualmente, o certificado de atributo, caso seja definida a opção através do contrato de serviços. Caso seja necessário o uso do selo temporal no documento, deverá ser informado o caminho da ACT responsável pela assinatura de tempo.

1.1: verificaCadeiaCertificados – Mesmo processo de verificação de cadeia de certificados proposto na seção 3.4.1.

1.2: verificaCertificadoAtributo – Nesse método, o módulo assinador fará a validação do certificado de atributo. Essa funcionalidade será realizada somente com a implementação do método da interface que define a obrigatoriedade da utilização do certificado de atributo pelo módulo assinador. A validação fará acesso à EEA – Entidade Emissora de Atributo – para a verificação de revogação. Caso o certificado de atributo informado não esteja vinculado ao certificado digital submetido ou este esteja revogado, o

documento digital não deverá ser assinado. O certificado de atributo, em nossa proposta será utilizado para garantir que o documento seja assinado por quem realmente é competente para isso, no entanto, ao implementar a funcionalidade, devemos definir os tipos de cargos (ex: diretor, decano, secretário, etc) aos quais serão dadas a permissão de assinar o documento.

1.3: anexaSeloTemporal – Nesse método, o Módulo de Assinatura irá anexar o selo temporal à assinatura do documento. Essa funcionalidade será realizada somente com a implementação do método da interface que define a obrigatoriedade da utilização do carimbo de tempo. Na implementação do método da interface, deverá ser informado a ACT a qual o módulo solicitará o selo temporal. O selo temporal, em nossa proposta, será utilizado para definir o momento da assinatura do documento e, por sua vez, o momento ao qual se torna válido.

1.4: assinaDocumento – O documento só será assinado após ser validado obrigatoriamente pelos métodos de, 1.1: validaCadeiaCertificados e, em alguns casos, passar por 1.2:validaCertificadoAtributo. Caso tenham problemas de conformidade em alguns dos certificados, o documento digital submetido não deverá ser assinado.

1.5: persisteDocumento – Esse método utiliza a implementação do serviço para persistir o documento assinado. Lembrando que cabe o desenvolvedor dos demais sistemas implementar a persistência de acordo com a sua regra de negócio e a tecnologia utilizada, seja banco de dados ou sistema de arquivos.

2: informaProblemas – Caso o documento não possa ser assinado, os problemas serão informados ao usuário.

Os documentos da Universidade de Brasília selecionados para o processo de assinatura digital deverão fornecer a mesma validade dos documentos assinados a punho. Desse modo, a proposta sugere uma direção oposta ao especificado nas normas da ICP-BRASIL. Como visto na seção 2.2.1, a ICP-BRASIL sugere uma implementação onde o usuário escolhe se deseja fazer a consulta de revogação em seu certificado para assim assinar o documento. Na presente proposta, como visto pelo diagrama de sequência apresentado, toda assinatura digital deverá passar **obrigatoriamente** pelo processo de validação e verificação de revogação do certificado, pois, desse modo, podemos garantir a validade jurídica desses documento de modo a deixá-los prontos para serem conferidos e contestados judicialmente, se assim necessário.

Em realação aos selos temporais, esse deverá ser planejadao visando à necessidade e o custo. A marcação precisa do momento da assinatura, ou seja, a necessidade de se fazer provar existência do documento naquela data e hora é o que faz do selo temporal um recurso indispensável. Caso contrário, não é necessário adquirir os selos temporais, seja criando uma infraestrutura de Autoridade Certificadora de Tempo (ACT) ou adquirindo de terceiros. Os procedimentos necessários para a criação de uma ACT são menos rígidos do que para a criação da AC, dessa formas empresas de médio porte têm uma maior facilidade para homologarem suas infraestruturas de tempo, no que tange à equipamentos necessários, espaço físico e pessoal especializado. Os procedimento para homologação de uma ACT podem ser visto em: [17] [15]

3.4.3 Procedimentos de Verificação do Documento Digital

O diagrama de sequência a seguir propõe uma implementação para o processo de assinatura do documento digital:

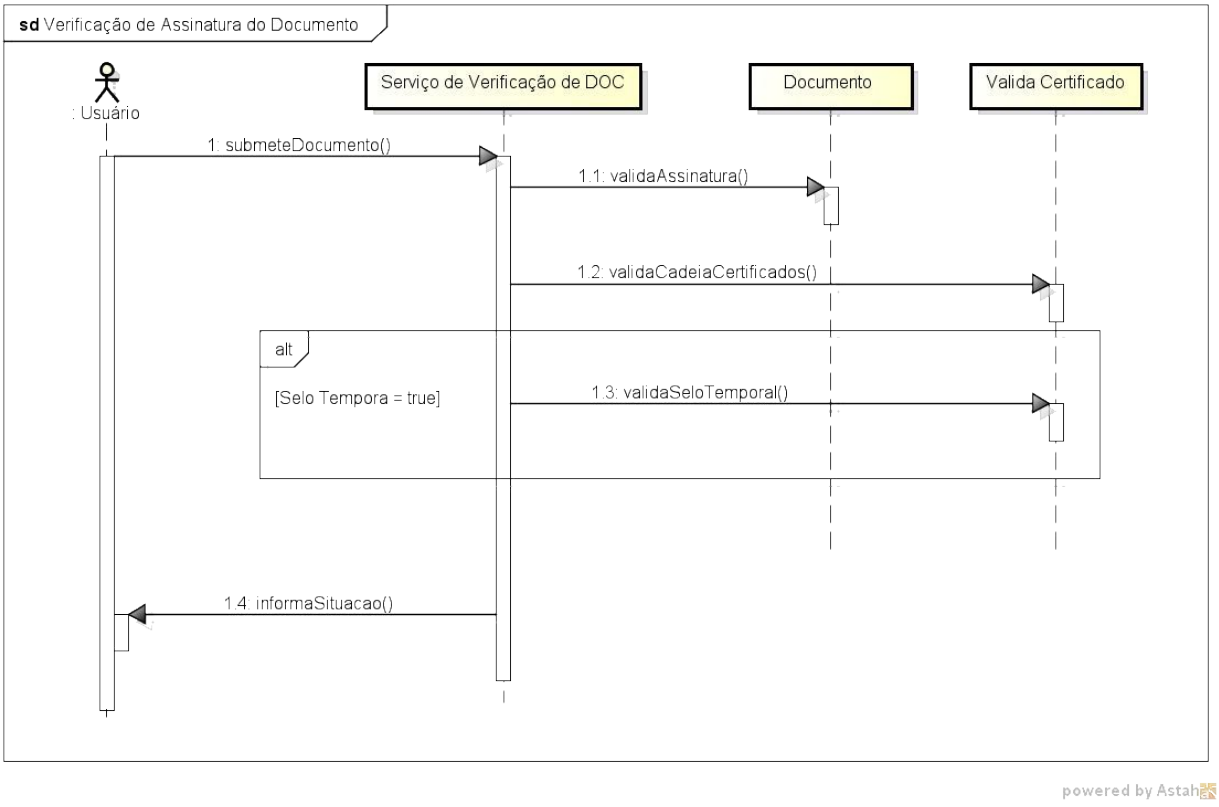

Figura 3.6: Diagrama de sequência: Verificação do documento digital.

1: submeteDocumento – Esse método recebe o documento assinado enviado pelo usuário.

1.1: validaAssinatura – Esse método é responsável pela verificação da assinatura.

1.2: validaCadeiaCertificado – Igual ao processo de validação da cadeia de certificados proposto na seção 3.4.1.

1.3: validaSeloTemporal – Esse método é responsável pela validação do carimbo de tempo. Quando o documento fizer referência a um selo temporal, adota-se a data e hora do carimbo de tempo para as validações referentes à temporalidade.

1.4: informaSituação – Informa a situação do documento ao usuário. Seja válido ou inválido. Quando o documento for inválido, os problemas de não conformidade serão listados.

3.5 ADEQUAÇÃO DO PROCESSO DE EMISSÃO DE CERTIFICADOS

O processo atual de emissão de certificados de extensão sofrerá mudanças a partir da inserção da assinatura digital em suas atividades. Hoje, para a conclusão desse processo, são necessárias diversas etapas que pode ser vistas na Figura 3.7. O módulo de assinatura digital visa diminuir a quantidade de etapas e o tempo gasto entre elas, tornando a disponibilização do certificado para o usuário final mais rápida, sem a necessidade de passar por todo o processo ao qual o documento físico é submetido.

Nota-se que nos processos atuais temos três atividades indispensáveis para a emissão do documento físico, são elas: Imprime o certificado, Verifica impressão do certificado e Autentica (o certificado) com um carimbo.

Com a implementação do software de assinatura, essas atividades serão retiradas do processo tornando a emissão do documento mais eficaz. Na Figura 3.8, verifica-se como as atividades serão organizadas com o uso da assinatura digital nos documentos de extensão.

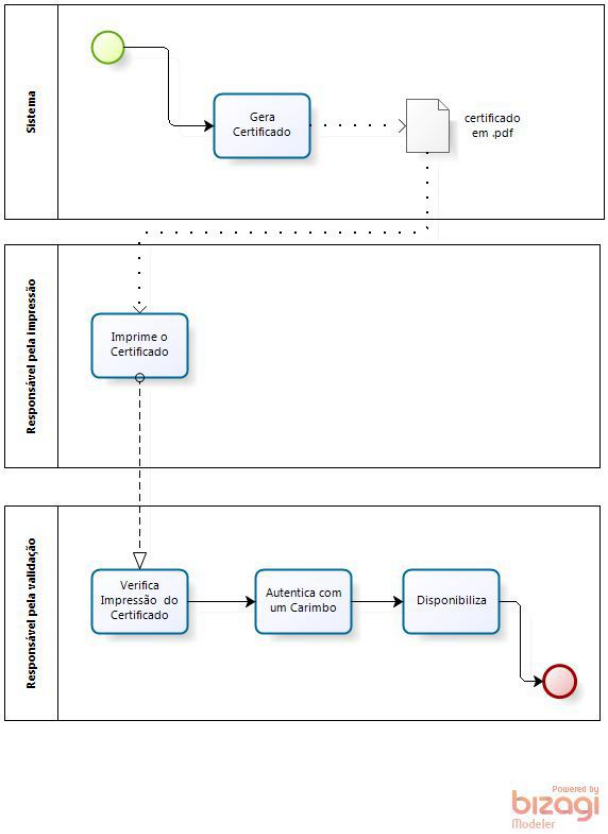

Figura 3.7: BPMN do processo de emissão do certificado (AS IS).

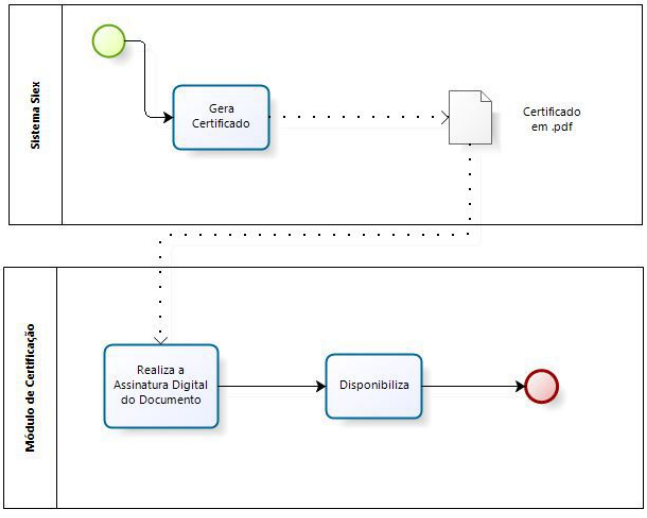

Figura 3.8: BPMN do processo de emissão do certificado (TO BE).

Capítulo 4

Análise dos Resultados

A pesquisa e os testes feitos nesse trabalho têm o objetivo de avaliar se o software implementado se adequa às necessidades e soluciona alguns problemas relacionados ao negócio da UnB.

Será realizada algumas avaliações no módulo de assinatura digital e na arquitetura proposta para saber se esses se adequam à realidade da Universidade de Brasília. Em segundo momento, serão avaliados os impactos da utilização do software na universidade.

4.1 ABORDAGEM GQM

Para avaliar a arquitetura proposta será utilizada a abordagem Goal Question Metric (GQM) proposta em [3]. Essa abordagem tem como objetivo avaliar/mensurar a qualidade do produtos, processo ou recursos de relacionados à engenharia de software. Para a avaliação, é necessário planejar o propósito do estudo identificando os objetivos de forma clara.

Goal	
Purpose	Avaliar
Issue	Benefícios e impactos
Object	A arquitetura proposta
Viewpoint	Instituição UnB

Tabela 4.1: Objetivo (GOAL) a ser avaliado

As métricas M1, M2, M3, M4, M5 serão analisadas nas seções seguintes desse trabalho.

Q & M	
Question Q1	Em termos operacionais, o software proposto atende às necessidades da Universidade de Brasília?
Metrics M1	Tempo de resposta das assinaturas.
Metrics M2	Atendimento aos requisitos de validade do documento: Autenticidade, integridade e Conformidade com a ICP-Brasil
Question Q2	Qual o espaço necessário para armazenados dos documentos?
Metrics M3	Tamanho do documento digital x quantidade de documentos.
Question Q3	Qual a economia prevista com a adoção dos procedimentos de Assinatura Digital?
Metrics M4	Gasto em R$ com o papel especial.
Metrics M5	Grau de sustentabilidade.

Tabela 4.2: Questões (*Questions*) e Métricas (*Metrics*) para avaliação

4.2 ANÁLISE DO TEMPO DE RESPOSTA DAS ASSINATURAS DIGITAIS

Nessa seção, será analisada a métrica M1, cujo objetivo é verificar o tempo de assinatura do documento digital. Tendo em vista a grande quantidade de documentos a serem assinados, foi analisado o tempo de resposta das assinatura em lote. O módulo de assinatura prevê a utilização dessa funcionalidade para assinar os certificados de extensão.

As assinaturas são realizadas no computador do cliente via Applet Java. Os procedimentos a serem realizados para assinatura são:

I - Quando a opção for pela assinatura no padrão XAdES.

1. Envio dos documentos `.xml`;
2. Leitura da chave privada do usuário pelo módulo;
3. Assinatura dos documentos `.xml`;
4. Persistência dos documentos `.xml` em banco de dados.

II - Quando a opção for pela assinatura do padrão CAdES.

1. Envio dos documentos `.pdf` ou `.doc`;
2. Leitura da chave privada do usuário pelo módulo;

3. Assinatura dos documentos `.pdf` ou `.doc`;

4. Persistência dos documentos `.p7s` em banco de dados.

No ano de 2013, foram entregues aproximadamente 200.000 certificados de extensão Universidade de Brasília. Esse teste visa avaliar o tempo que o módulo leva pra realizar a assinatura em lote utilizando a configuração média de hardware do usuário.

A análise será realizada com o seguinte hardware:

Computador	
CPU	Intel core i3, 2.53 GHz
Cache l3	3MB
Memória	4GB
Sistema Operacional	Windows 7

Tabela 4.3: Configuração do computador do usuário

Outras configurações	
Java OpenJDK	Versão 1.7.0_65
Banco de Dados PostgreSQL	Versão 9.1.14
Java Servlet	Versão 3.0

Tabela 4.4: Outras configurações de ambiente

Certificado Digital	
Dispositivo de armazenamento	Token
Algoritmo de criptografia	RSA 2048
Função *hash*	SHA512
Padrão	X.509 v3

Tabela 4.5: Configuração do dispositivo que guarda a chave privada do usuário

Consideramos falha no processo de assinatura de 100.000 lotes devido a demora na resposta do procedimento de assinatura, tanto no padrão XAdES quanto do CAdES. Os documentos eram submetidos mas não eram processados pelo módulo de assinatura.

O problema pode vir de vários fatores, alguns deles são: Sobrecarga da JVM; memória insuficiente; restrições impostas pelo sistema operacional ou browser no uso de applets java para processamento local.

1.000 documentos assinados em lote		
XAdES	Tempo de assinatura [a]	48.351 seg
	Tempo de persistência [b]	42.665 seg
	Tempo total	91.016 seg = 1,49 min
CAdES	Tempo de assinatura [a]	54.990 seg
	Tempo de persistência [b]	119.033 seg = 1,98 min
	Tempo total	174.023 segs = 2,9 min
10.000 documentos assinados em lote		
XAdES	Tempo de assinatura [a]	469.330 seg = 7,82 min
	Tempo de persistência [b]	440.234 seg = 7,34 min
	Tempo total	909.564 seg = 15,16 min
CAdES	Tempo de assinatura [a]	529.891 seg = 8,83 min
	Tempo de persistência [b]	1410.113 seg = 23,5 min
	Tempo total	1940.003 seg = 32,33 min
100.000 documentos assinados em lote		
XAdES	Tempo de assinatura [a]	não funcionou
	Tempo de persistência [b]	não funcionou
	Tempo total	não funcionou
CAdES	Tempo de assinatura [a]	não funcionou
	Tempo de persistência [b]	não funcionou
	Tempo total	não funcionou

Tabela 4.6: XAdES: Lote de 1.000 documentos

[a] Foram computados os envios dos arquivos, a leitura do *token* e a assinatura em si.
[b] A persistência foi realizada em banco de dados.

4.3 ANÁLISE DA VERIFICAÇÃO DE INTEGRIDADE DO DOCUMENTO

Nessa seção, será analisada a métrica M2, cujo objetivo é verificar se a implementação do software é capaz de atestar a assinatura do documento digital, tanto pela autenticidade e a integridade do documento assinado.

Os teste foram:

Teste no serviço de verificação do documento		
Tipo de teste	**XAdES**	**CAdES**
Autenticidade	Não houve falha	Não houve falha
Integridade	Não houve falha	Não houve falha
Assinado por certificado ICP-BRASIL	Não houve falha	Não houve falha

Tabela 4.7: Teste funcional da verificação da assinatura de documentos

Para testar a autenticidade, foram utilizadas outras combinações de chaves criptográficas na tentativa de fazer a verificação de assinatura do documento. Somente com a chave pública matematicamente ligada à chave privada do usuário foi possível chegar ao *hash* correto.

Para testar a integridade no formato XAdES, foram trocados alguns valores dos atributos do `.xml` mantendo o *hash* e a assinatura gerada anteriormente. Após isso, foi feita a verificação do documento pelo serviço de verificação de assinatura. Com o CAdES não permitido trocar os valores da assinatura como no `.xml`.

Por fim, em ambos os formatos, o software alertou o usuário quando o documento foi assinado por certificado fora da hierarquia da ICP-BRASIL.

4.4 ANÁLISE DA ESPAÇO DE ARMAZENAMENTO DOS DOCUMENTOS ASSINADOS

Nessa seção, será analisada a métrica M3, cujo objetivo é verificar o espaço necessário para a armazenagem dos documentos assinados digitalmente.

Padrão de assinatura XAdES: O arquivo depois de assinado passa de 1 kB (1.024 bytes) para 3,59 kB (3.586 bytes). Se a média de certificados de extensão emitidos durante os anos for de 200.000 teremos:

Certificados de extensão assinados em 20 anos		
Tipo	**Ano**	**Tamanho**
XAdES	2013	683,9 MB
XAdES	2023	6,6 GB
XAdES	2033	66 GB

Tabela 4.8: XAdES: tamanho do arquivo assinado

Padrão de Assinatura CAdES: O certificado em formato eletrônico não assinado tem o tamanho de 111,8 kB (114.483 bytes). Depois de assinado, o arquivos `.p7s` fica com o tamanho de 114,9 kB (117.031 bytes). Se a média de certificados emitidos durante os anos for de 200.000 teremos:

Certificados de extensão assinados em 20 anos		
Tipo	**Ano**	**Tamanho**
CAdES	2013	21,8 GB
CAdES	2023	218 GB
CAdES	2033	2,1 TB

Tabela 4.9: CAdES: tamanho do arquivo assinado

4.5 ANÁLISE DO IMPACTO DA UTILIZAÇÃO DE DOCUMENTOS DIGITAIS NA INSTITUIÇÃO

Nessa seção, será analisada a métrica M4 e M5, cujo objetivo é avaliar o impacto da implementação do software de assinatura digital na Instituição Universidade de Brasília.

Redução dos custos com papel especial num período de 20 anos: A impressão de 200.000 certificados de extensão tendo como valor de custo do papel especial para impressões em R$ 14,00 temos:

Valor da impressão dos certificados de extensão	
Por ano	2,8 milhões de reais
Total em 20 anos	56 milhões de reais

Tabela 4.10: Gasto com a impressão dos certificados de extensão

Sustentabilidade: De acordo com o artigo publicado em [6], em média, uma árvore resulta em 7500 folhas. Levando em consideração a quantidade média de 200.000 certificados de extensão emitidos por ano temos:

Redução de gastos com papel por ano	
Árvores salvas	26,6 árvores
Resmas de 500 folhas economizadas	400 resmas

Tabela 4.11: Redução de gastos com papéis

Capítulo 5

Conclusão

Esse trabalho teve como objetivo realizar um estudo relacionado à viabilização de uma implementação de software de assinatura digital na Universidade de Brasília. Foram levantados assuntos ligados à assinatura digital no Brasil tais como os procedimentos computacionais e a legislação que regulamentam o uso do certificado digital para assinaturas de documentos.

Os resultados obtidos com a pesquisa sugerem a adoção das assinaturas digitais para um contexto universitário no que tange às assinaturas dos certificados de extensão emitidos pela UnB.

A pesquisa avaliou o software implementado tanto no âmbito operacional quanto nos impactos à organização. Segue abaixo algumas constatações:

- **Tempo de assinatura**

Nessa pesquisa, o tempo total de assinatura calculado para o implementação é:

$$TTPA = TA + TP, sendo: \tag{5.1}$$

TTPA = Tempo total do procedimento de assinatura;
TA = Tempo de assinatura;
TP = Tempo de persistência.

Vimos que o tempo de assinatura entre os formatos XAdES e CAdES são bem similares para os lotes de 1.000 e 10.000. O que mudou consideravelmente foi o tempo de persistência do documento assinado. Para o lote de 1.000 no parão XAdES o tempo de persistência foi de 42.665 segundos, enquanto que no padrão CAdES o tempo de persistência foi de 1,98 minutos, ou seja, mais do que o dobro.

Com esse experimento, pôde-se perceber que o tamanho do arquivo influencia no tempo de assinatura e no tempo de persistência, que, por consequência, irá influenciar no

tempo total do procedimento. O tempo total da assinatura no formato CAdES foi de 2,9 minutos, enquanto que no XAdES foi de 1,49 minutos no lote de 1.000, e, 15,16 minutos contra 32,33 minutos no lote de 10.000. O módulo de assinatura não foi capaz de assinar o lote de 100.000.

O tempo total do procedimento em ambos os formatos é visto como viável para o negócio da instituição. Ao optar por utilizar o software de assinatura, mesmo utilizando o padrão CAdES, as atividades de emissão do certificado de extensão seriam mais eficazes do que permanecer com processo atual de emissão.

- **Verificação da integridade do documento**

A implementação se mostrou eficiente na verificação da autenticidade do documento e na integridade de suas informações bem como na verificação de correspondência do certificado do usuário à hierarquia da ICP-Brasil, ou seja, certificados adulterados ou assinados fora dos padrões serão identificados.

Com isso será possível fornecer um serviço aos usuário e colaboradores da instituição para a verificação da assinatura dos certificados de extensão.

- **Sobre o tamanho dos arquivos para o armazenamento**

Os arquivos utilizados para esse estudo foram:

1. certificado `.xml` para assinatura no padrão XAdES e
2. certificado `.pdf` para assinatura no padrão CAdES.

Com a assinatura do `.xml` no padrão XAdES, o tamanho do documento assinado aumenta em aproximadamente 3,5 vezes em relação ao seu tamanho original. Já com o padrão CAdES, o aumento do arquivo é de 0,02 vezes o tamanho do arquivo original.

O espaço estimado para o armazenamento dos documentos assinados no XAdES é de 66GB para o ano de 2033. Já os assinados em CAdES para o mesmo ano é de 2,1 TB. Percebe-se que o formato CAdES necessita de mais espaço para armazenagem. Apesar disso, ter disponível 2,1 TB de armazenamento não é algo que trará custos financeiros altos para o centro de processamento de dados, pois a capacidade de armazenagem computacional vem aumentando ao longo dos anos e seu custo vem diminuindo.

O CAdES assina documentos com formatação própria, como o .pdf, o .doc, etc. Já o XAdES carrega somente as informações que dão relevância ao documento. Por isso, para simular o uso real desses padrões, foi utilizado para o padrão CAdES um arquivo .pdf formatado para impressão e um arquivo arquivo .xml somente com os atributos de informação relevantes (Anexo A).

- **Impacto da utilização de documentos digitais na instituição**

Caso a solução seja adotada na instituição e os certificados de extensão impressos em papel sejam substituídos em sua totalidade pelo formato eletrônico, a Universidade de Brasília terá uma economia de 2.8 milhões de reais por ano só com os gastos da compra do papel especial, chegando a uma economia de 56 milhões daqui a 20 anos. A economia com outros suprimentos como toner de impressora e manutenção de equipamentos não foi calculada.

Percebe-se pelo estudo que utilização do software de assinatura digital na Universidade de Brasília é viável em termos operacionais e pode trazer benefícios à organização. Documentos com assinaturas digitais podem substituir os documentos físicos sem prejuízo à sua eficácia probante. Com o uso da solução de assinatura digital, as atividades de emissão de certificado ganharão celeridade bem como o processo de verificação de falsificações será mais eficiente, além disso, o uso do software provê uma solução sustentável e econômica.

Por fim, sabemos que o uso de papéis e assinaturas a punho estão presentes na nossa sociedade e que o documento digital deverá ser incorporado aos poucos na cultura organizacional. Apesar dos benefícios citados acima, não é possível saber qual será o nível de aceitação desse novo paradigma entre a comunidade da Universidade de Brasília.

Referências

[1] ABA. *Digital signature guidelines : legal infrastructure for certification authorities and electronic commerce*. American Bar Association, Chicago, IL, 1996. 56

[2] ABRID. Unversidade de são paulo: Diploma digital acelera emissão do documento e põe o formato como parte ativa do processo. *IDigital*, (16):10–13, 2014. 8

[3] Victor R. Basili, Gianluigi Caldiera, and H. Dieter Rombach. The goal question metric approach. In *Encyclopedia of Software Engineering*. Wiley, 1994. 34

[4] Jay Blanton, Steve Leski, Brian Nicks, and Traian Tirzaman. Making soa work in a healthcare company. In *Proceedings of the 24th ACM SIGPLAN Conference Companion on Object Oriented Programming Systems Languages and Applications*, OOPSLA '09, pages 589–596, New York, NY, USA, 2009. ACM. 19

[5] Brasil. Medida provisória n 2.200-2, de 28 de agosto de 2001. Disponível em: <`http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm`>, 2001. Acesso em Out/2013. 7

[6] NDD Green Carbon. Green carbon. Disponível em: <`http://www.nddgreencarbon.com/si/site/0500`>, 2014. Acesso em Mai/2014. 39

[7] Rama Krushna Das and Manas Ranjan Patra. Soa for e-governance in india: Potentials and pitfalls. In *Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance*, ICEGOV '09, pages 36–41, New York, NY, USA, 2009. ACM. 19

[8] T. Erl. *SOA Princípios de design de Serviços*. Pearson Prentice Hall, São Paulo, 200. 18, 21

[9] ETSI. Cms advanced eletronic signature (cades). 1.7.4. Disponível em: <`http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/01.07.04_60/ts_101733v010704p.pdf`>, 2008. Acesso em agos/2014. 9

[10] ETSI. Xml advanced eletronic signature (xades). 1.3.2. Disponível em: <`http://uri.etsi.org/01903/v1.3.2/ts_101903v010302p.pdf`>, 2008. Acesso em agos/2014. 9

[11] IETF. Rfc 2315 - pkcs 7: Crytographic message syntax. Disponível em: <`http://tools.ietf.org/html/rfc2315`>, 1998. Acesso em Mar/2014. 17

[12] IETF. Rfc 2560 - x.509 internet public key infrastructure online certificate status protocol - ocsp. Disponível em: <http://www.ietf.org/rfc/rfc2560.txt>, 1999. Acesso em Jan/2014. 12

[13] IETF. Rfc 5280 - internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. Disponível em: <http://www.ietf.org/rfc/rfc5280.txt>, 2008. Acesso em 2013. 7, 11, 12, 47

[14] ITI. *Manual de Condutas Técnicas 4 - Volume I: Requisitos, Materiais e Documentos Técnicos para Homologação de Softwares de Assinatura Digital no Âmbito da ICP-BRASIL*. ITI, 2007. Acesso em Ago/2013. 9, 10, 12, 16, 23

[15] ITI. Doc-icp-12 - requisitos mínimos para as declarações de práticas das autoridades de carimbo de tempo. Disponível em: <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-12.pdf>, 2009. Acesso em 2013. 31

[16] ITI. Doc-icp-01.01 - padrões e algoritmos criptográficos da icp-brasil. Disponível em: <http://www.iti.gov.br/images/legislacao/Docicp/DOC-ICP-01.01_-_versao_2.5_PADROES_E_ALGORITMOS_CRIPTOGRAFICOS_DA_ICP-BRASIL.pdf>, 2010. Acesso em junho de 2014. 54

[17] ITI. Doc-icp-11 - visÃo geral do sistema de carimbos do tempo na icp-brasil. Disponível em: <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-11_-_Versao_1.2.pdf>, 2010. Acesso em 2013. 31

[18] ITI. Glossário v1.4. Disponível em: <http://www.iti.gov.br/images/icp-brasil/Normas%20ICP-Brasil/Glossario/GLOSSaRIOV1.4.pdf>, 2010. Acesso em Jan/2014. 16, 51

[19] ITI. Doc-icp-15-02 - perfil de uso geral para assinaturas digitais na icp-brasil. Disponível em: <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/docs13082012/DOC-ICP-15.02_-_Versao_2.1.pdf>, 2012. Acesso em Jan/2014. 9

[20] Robson Carvalho Machado. *Certificação Digital ICP-BRASIL: Os caminhos do documento eletrônico no Brasil*. Impetus, Niterói - RJ, 2010. 46

[21] BRUCE. SCHNEIER. *Applied Cryptograph: protocols, algorithms, and source code in C*. John Wiley Sons, USA, 1996. 53, 54, 55

[22] RCA Security. Pkcs11. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30b-d6.pdf>, 2014. Acesso em agos/2014. 25

[23] W. Stallings. *Criptografia e Segurança de Redes*. Pearson, Ed., São Paulo, 2008. 7, 48

[24] USP. Usp vai adotar dispositivo inédito de diplomas com certificação digital. disponível em: <http://www.usp.br/imprensa/?p=19364>, 2012. Acesso em 2013. 3

[25] G. B. Wills. Y. W. Sim, Wang L. Gilbert. An overview of service-oriented architecture. *School of Eletronics and Computer Science*, 2005. 18

Apêndice A

Certificado Digital

A.1. CERTIFICADO DIGITAL

O certificado digital nada mais é que um arquivo eletrônico que, contendo as chaves criptográficas de uma entidade (pessoa física ou jurídica, máquina ou aplicação), associa essas chaves a informações relativas à entidade, permitindo dizer se ela é quem realmente diz ser[20]. Esses certificados são emitidos pelas AC – Autoridades Certificadores e a elas é dada a responsabilidade do gerenciamento, revogação e disponibilização dos certificados digitais.

Qualquer pessoa, física ou jurídica, pode ser titular de um certificado digital. Para isso é necessário o comparecimento do requerente a uma AR - Autoridade de Registro - devendo informar a documentação exigida. Os dados informados no ato do registro presumem-se verdadeiros e os documento produzidos pelo processo de Certificação Digital possuirão os mesmo efeitos dentro da legislação civil.

Em um certificado digital, geralmente são incluídas as informações seguintes:

- Informações relativas a entidade para o qual o certificado foi emitido (nome, e-mail, CPF/CNPJ, etc.);
- A chave pública da entidade especificada no certificado;
- Prazo de validade;
- A localização da lista de certificados revogados (endereço de onde se pode consultar se o certificado foi revogado ou não);
- No caso do modelo hierárquico, a assinatura da autoridade certificadora (AC), ou no caso do modelo de malha de confiança, as entidades que validaram e confiam nas informações do certificado.

A forma mais aceita de certificados digitais é o X.509. Hoje esse padrão já está em sua terceira versão e será visto com maiores detalhes nas próximas seções.

A.2. PADRÃO X.509 DE CERTIFICADOS

O ITU-T X.509 é um padrão de certificado mais comum definido pela RFC 5280[13], que substitui a RFC 3280, e é utilizado pela ICP-Brasil. Todos os certificados criados a partir desse padrão podem ser utilizados, em teoria, em aplicações que utilizam o mesmo procedimento.

A primeira versão do padrão X.509, chamada de X.509 v1, foi lançada em 1988. Já a segunda, X.509 v2, apareceu em 1993 trazendo melhorias e a adição de novos atributos. Já a v3 foi implementada em junho de 1997 trazendo o campo de extensões o qual proporcionou um avanço em termos de eficiência de uso em relação aos outro padrões no que diz respeito a flexibilidade.

O X .509 hoje é utilizado em vários protocolos de segurança importantes tais quais o S/MIME, IP Sec e SSL/TLS.

A tabela abaixo mostra uma série de atributos referentes à entidade para o qual foi emitido o certificado além apresentar as respectivas versões ao qual foram incluídos.

Os atributos são:

X.509	
Versão	Desde a v1
Número de série	Desde a v1
Algoritmo de Assinatura	Desde a v1
Nome do Emissor	Desde a v1
Período de Validade	Desde a v1
Nome do Titular	Desde a v1
Informações da Chave Pública	Desde a v1
Identificador Exclusivo do Emissor	Adicionado na v2
Identificador Exclusivo do Titular	Adicionado na v2
Extensões	Adicionado na v3
Assinatura	Desde a v1

Tabela A.1: Atributos do padrão X.509

Versão: Indica a versão do certificado. O padrão é a versão 1, caso o Identificador Exclusivo do Emissor e o Identificador Exclusivo do Titular esteja presente, o valor terá que ser a versão 2. Caso existam extensões

Número de Série: Contém um identificador exclusivo emitido pela AC do certificado. É esse identificador que estará presente na LCR da AC quando o certificado é revogado e não o certificado completo.

Algoritmo de Assinatura: Identifica o algoritmo utilizado para assinar o certificado. É identificado tanto o algoritmo de chave pública quanto a função *hash*. Como essa informação será repetida no campo Assinatura, ao final do certificado, o campo tem pouca ou nenhuma utilidade [23].

Nome do Emissor: É o nome padrão X.500 da AC que criou e assinou o certificado. A AC deve preencher os campos do *DN - Distinguished Name* com o país o nome da organização. Ex: DN (c=BR, o=Universidade de Brasília)

Período de Validade: Especifica o período de validade do certificado. Consiste nas datas de início de fim de validade do certificado.

Nome do Titular: Contém o nome do titular do certificado. Também é utilizado um padrão para o preenchimento desse campo. Ex: DN (c=BR, o=Universidade de Brasília, cn=Andrei Queiroz)

Informações da Chave Pública: Nesse campo irá conter duas informações: 1 - O valor da chave pública do titular e 2 – o identificador do algoritmo e da função *hash*.

Identificador Exclusivo do Emissor: É um campo opcional. Serve para identificar exclusivamente a AC emissora do certificado, caso o Nome do Emissor tenha sido reutilizado para entidades diferentes

Identificador Exclusivo do Titular: É um campo opcional. Serve para identificar exclusivamente o titular do certificado, caso o Nome do Titular tenha sido reutilizado para entidades diferentes.

Os desenvolvedores do padrão X.509 sentiram que era necessário uma forma de incluir informações no certificado de maneira mais flexível. Foi então que, na versão 3, lançaram o conceito de extensões. Cada extensão consistem em um identificador de extensão (OID), um indicador de importância e um valor de extensão.

A.3. EXTENSÕES DO X.509

O X.509 v3 criou um mecanismo de inclusão de informações adicionais ao certificado. Cada extensão adicionada deverá preencher os campos abaixo:

- Identificador
- Indicador de Obrigatoriedade
- Valor

Sendo que: o identificador define o OID da extensão a ser utilizada; o indicador de obrigatoriedade indica se a extensão poderá ser ignorada com segurança sem que o certificado seja tido com inválido e o valor será o conteúdo da extensão.

Na versão 3, foram criadas algumas especificações de extensão obrigatórias e seus respectivos OIDs. O desenvolvedores do padrão recomenda que sejam atribuídos o chamado conjunto mínimo de extensão que são: key usage, extended key usage, certificate policies, inhibit any-policy, subject alternative name, basic constraints, name constraints, policy constraints. Foi especificado e pode ser utilizado também o segundo grupo composto pelo authority e subject key identifier, e policy mapping. Abaixo será feita uma breve explicação desses atributos:

***Authority key identifier* (não crítica):** Identifica a chave pública que será utilizada para verificar a assinatura do certifcado ou da LCR. Útil quando a AC é titular de mais de uma chave de assinatura. Esse campo é utilizado também para o tratamento do par de chaves da AC.

***Subject Key Identifier* (não crítica):** Identifica todos os certificados que contenham a mesma chave pública. Esse campo é útil também quando há necessidade da atualização do par de chaves do titular.

***Key Usage* (crítica):** Descreve o propósito de uso das chaves do certificado digital. Os propósito para essa extensão são: *digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly.*

***Private Key Usage Period* (não crítica):** Indica o tempo de validade da chave privada correspondente à chave pública do certificado. Normalmente a validadade da chave privada é mais curta que a da chave pública.

***Certificate Policies*:** É usado para especificar a política aplicada ao certificado. Pode-se especificar polticas às quais o certificado suporta tanto quanto informações qualificadoras opcionais.

***Policy Mappings*:** Usado somente em certificados de ACs. Utilizada para vincular políticas equivalentes entre autoridades certificadoras.

***Subject Alternative Names*:** Permite que o certificado associe mais de um nome ao titular. É útil para aplicações que empregam suas formas próprias de nome tal como e-mail, IPsec, etc.

***Issuer Alternative Names* (não crítca):** Contém um ou mais nomes do emissor.

***Basic Constraints*:** Identifica se o titular do certificado é uma entidade certificadora. O campo é útil para definir restrições de assinatura e tamanho da cadeia quando um certificado pertence a AC.

***Name Constraints*:** É utilizada apenas em certificados de ACs. Esse campo restringe o espaço de nomes dentre os quais os certificados da cadeia subsequente devem estar incluídos.

***Policy Constraints*:** Utilizada apenas em certificados de ACs.

***Extended Key Usage*:** É mais utilizado para certificados de entidades finais. Serve para complementar o propósito de utilização do atributo *Key Usage*. Algumas propósitos definidos são: *serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, OCSPSigning.*

***Inhibit Any-Policy*:** É utilizada para indicar que políticas neutras não podem ser utilizadas em certificados da cadeia subsequente.

***CRL Distribution Points*:** Indica o local onde as LCRs da AC podem ser encontradas.

Apêndice B

Tipos de certificados da ICP-Brasil

B.1. TIPOS DE CERTIFICADOS DA ICP-BRASIL

Os tipos de certificados definidos pela ICP-BRASIL foram divididos em duas categorias, os de Assinatura (A1, A2, A3, A4) e de Sigilo (S1, S2. S3, S4)[18].

Certificado do tipo A1 e S1: Certificado em que a geração das chaves criptográficas é feita por software e seu armazenamento pode ser feito em hardware ou repositório protegido por senha, cifrado por software. Sua validade máxima é de um ano, sendo a frequência de publicação da LCR no máximo de 48 horas e o prazo máximo admitido para conclusão do processo de revogação de 72 horas.

Certificado do tipo A2 e S2: Certificado em que a geração das chaves criptográficas é feita em software e as mesmas são armazenadas em Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos por senha. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de dois anos, sendo a frequência de publicação da LCR no máximo de 36 horas e o prazo máximo admitido para conclusão do processo de revogação de 54 horas.

Certificado do tipo A3 e S3: Certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou Token, ambos com capacidade de geração de chaves e protegidos por senha, ou hardware criptográfico aprovado pela ICP-BRASIL. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de três anos, sendo a frequência de publicação da LCR no máximo de 24 horas e o prazo máximo admitido para conclusão do processo de revogação de 36 horas.

Certificado do tipo A4 e S4: Certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou Token, ambos com capacidade

de geração de chaves e protegidos por senha, ou hardware criptográfico aprovado pela ICP-BRASIL. As chaves criptográficas têm no mínimo 2048 bits. A validade máxima do certificado é de três anos, sendo a frequência de publicação da LCR no máximo de 12 horas e o prazo máximo admitido para conclusão do processo de revogação de 18 horas.

Apêndice C

Criptografia e Função *hash*

C.1. CRIPTOGRAFIA E FUNÇÃO DE *HASH*

I - Criptografia Simétrica

A criptografia simétrica utiliza-se de algoritmos onde a chave de decifração pode ser calculada (em tempo polinomial) a partir da chave de crifração e vice-versa. Na maioria dos algoritmos simétricos, as chaves de cifração e decifração são as mesmas. Esses algoritmos também são chamados de Sistemas de Chave Simétrica, criptografia de chave única, ou criptografia de chave secreta[21].

A segurança desse tipo de sistema reside na chave criptográfica, devido a isso, o conhecimento da chave por terceiros implica na possibilidade de decifração da mesma forma que o destinatário da mensagem.

$$Ek(M) = C; \tag{C.1}$$

$$Dk(C) = M, sendo: \tag{C.2}$$

M o texto em claro, C o texto criptografado e k a chave criptográfica.

Algoritmos simétricos podem ser divididos em duas categorias onde algumas podem operar bit a bit do texto em claro, comumente chamadas de cifras de fluxos, e outras podem operar em grupos de bits de tamanho fixo, chamados de cifras de bloco.

II - Criptografia Assimétrica

Diferente da criptografia simétrica, os algoritmos de criptografia assimétrica foram projetado para usar chaves diferentes de cifração e decifração. Nesse tipo de algoritmo

não é possível calcular a chave de decifração através da chave de crifração em tempo viável. Eles são chamados de algoritmos de chave pública porque podemos tornar pública a chave de cifração para que qualquer pessoa possa utilizar a fim de cifrar uma mensagem, no entanto, somente uma pessoa pode ter a posse da chave de decifração, e assim decifrar a mensagem. Nesse sistemas, a chave de cifração é chamada de chave pública e a chave de decifração é chamada de chave privada[21].

Podemos utilizar o inverso, ou seja, a chave privada para processar a mensagem e a chave pública para verificar. Esse processo é usado em assinaturas digitais para garantir a autenticidade.

III - Algoritmos Criptográficos Definidos pela ICP-BRASIL

A ICP-BRASIL tem definido no DOC-ICP-01.01 [16] os padrões de algoritmos e parâmetros criptográficos a serem empregados em todos nos processos de assinatura digital que incluem, entre outros:

- geração de chaves criptográficas;
- solicitacao, emissao e revogacao de certificados digitais;
- geracao e verificacao de assinaturas digitais;
- cifracao de mensagens;
- autenticacao com certificados digitais.

A tabela abaixo mostra a combinação dos algoritmos e funções hash utilizadas para assinaturas digitais:

Assinaturas Digitais ICP-BRASIL CAdES e XAdES	
Suite Assinatura	sha1WithRSAEncryption
	sha256WithRSAEncryption
	sha256WithECDSAEncryption
	sha512WithRSAEncryption
	sha512WithECDSAEncryption

Tabela C.1: Configuração do computador do usuário

Essas diretrizes devem ser obrigatoriamente observadas pelas Autoridades Certificadoras, Autoridades de Registro, bem como pelos titulares finais e desenvolvedores de aplicativos que utilizam certificados digitais da ICP-BRASIL.

IV - Funções de hash

As funções *hash* podem ser chamadas também de funções de resumo. A função hash tem o objetivo de receber uma entrada de tamanho variável (pode ser uma cadeia de caracteres, um arquivo, etc) e convertê-la em um valor de saída de tamanho fixo (geralmente um tamanho menor que o de entrada).

A função *hash* trabalha em um única direção, ou seja, é fácil calcular a saída a partir do valor de entrada, mas é extremamente difícil fazer o caminho contrário. É possível também, mas extremamente difícil, encontrar colisões em funções *hash*. Colisão é quando as saídas processadas através de diferentes entradas são idênticas. A segurança das funções *hash* está na saída do processamento não ser dependente da entrada e que a cada bit modificado nos dados entrada é gerado um valor de saída totalmente diferente[21].

Apêndice D

Assinatura Digital

D.1. ASSINATURA DIGITAL

Assinatura, como regra da nossa sociedade, é uma maneira para identificar uma pessoa. Ela pode ser verificada por meio de um registro de uma assinatura (por exemplo, uma pessoa faz ficha de assinatura em um banco quando vai fazer a abertura de uma conta). A assinatura tem como função validar um documento, de forma que um documento só possa ser aceito se não tenha havido modificações posteriores (por exemplo, uma assinatura em uma folha de cheque). Caso haja algum problema em relação à assinatura, é possível fazer a checagem da mesma comparando com outras realizadas anteriormente. O conceito de assinatura digital é análogo ao da assinatura comum. Para verificar este requisito, uma assinatura digital deve ter as seguintes propriedades[1]:

- Autenticidade - o receptor pode confirmar que a assinatura foi feita pelo emissor;
- Integridade - qualquer alteração da mensagem faz com que a assinatura se torne inválida;
- Irretratabilidade - o emissor não pode negar que foi o autor da mensagem.

A assinatura digital, por si só, não garante a confidencialidade dos dados. Essa confidencialidade é obtida por meio das técnicas de criptografia, que são usadas em conjunto com as assinaturas digitais.

A implementação da assinatura digital só foi possível com o uso dos algoritmos de criptografia assimétrica, pois eles provêm a garantia de autenticidade e por consequência, a irretratabilidade da mensagem. A integridade da mensagem é verificada por meio das funções de hash.

O funcionamento da Assinatura digital sem sigilo da mensagem se dá pelos seguintes passos:

Emissor:

1. cria uma mensagem em texto aberto;
2. utiliza uma função de *hash* e obtém o resumo da mensagem;
3. assina o resumo da mensagem utilizando a sua chave privada;
4. monta o envelope digital com o texto em claro e a assinatura;
5. transmite o envelope ao receptor.

Receptor:

1. recebe a o envelope transmitido;
2. verifica a assinatura utilizando a chave pública do emissor;
3. utiliza a mesma função de *hash* e obtém o resumo da mensagem;
4. compara o *hash* da assinatura com o *hash* da mensagem, para ver se são iguais. Se forem iguais, a mensagem é autêntica, ou seja, não houve alteração.

Vale lembrar que o procedimento de assinatura e verificação exemplificados nos itens 3 e 2 respectivamente baseia-se no uso do RSA, que é algoritmo mais usado em certificados digitais da ICP-BRASIL. Porém, esses não são procedimentos aplicáveis a todos os algoritmos que podem ser utilizados para a assinatura digital, tal como o ECC, *Elliptic Curve Cryptography*.

Anexo I

Conteúdo do Certificado `.xml`

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<certificadoExtensao>
<nomePessoa>XXXXX XXXXX XXXXX</nomePessoa>
<identificacao>CPF 999.999.999-99</identificacao>
<dataNascimento>999-99-99T00:00:00-02:00</dataNascimento>
<temaAtividade>Designing with words</temaAtividade>
<tipoAcao>Evento</tipoAcao>
<dataInicioRealizacao>9999-99-01T00:00:00-02:00</dataInicioRealizacao>
<dataTerminoRealizacao>
  9999-99 16T00:00:0002:00
</dataTerminoRealizacao>
<cargaHoraria>100</cargaHoraria>
<mencao>SS</mencao>
<frequencia>100</frequencia>
<unidadeGeral>Instituto de Artes</unidadeGeral>
<diretor>Nome do diretor</diretor>
<decano>Nome do decano</decano>
<titulo>DESIGNING WITH WORDS</titulo>
<turma>A</turma>
<ofertaExtesao>9999</ofertaExtesao>
<participacao>cursista</participacao>
<cargoDiretor>Secretario Adjunto de Administraca Academica</cargoDiretor>
<cargoDecano>Decano de Extensão</cargoDecano>
</certificadoExtensao>
```

Anexo II

Conteúdo do Certificado `.xml` assinado

```
<?xml version="1.0" encoding="UTF-8"?>
<certificadoExtensao>
  <nomePessoa>XXXXX XXXXX XXXXX</nomePessoa>
  <identificacao>CPF 999.999.999-999</identificacao>
  <dataNascimento>999-99-99T00:00:00-02:00</dataNascimento>
  <temaAtividade>Designing with words</temaAtividade>
  <tipoAcao>Evento</tipoAcao>
  <dataInicioRealizacao>9999-99-01T00:00:00-02:00</dataInicioRealizacao>
  <dataTerminoRealizacao>
    9999-99 16T00:00:0002:00
  </dataTerminoRealizacao>
  <cargaHoraria>100</cargaHoraria>
  <mencao>SS</mencao>
  <frequencia>100</frequencia>
  <unidadeGeral>Instituto de Artes</unidadeGeral>
  <diretor>Nome do diretor</diretor>
  <decano>Nome do decano</decano>
  <titulo>DESIGNING WITH WORDS</titulo>
  <turma>A</turma>
  <ofertaExtesao>9999</ofertaExtesao>
  <participacao>cursista</participacao>
  <cargoDiretor>Secretario Adjunto de Administraca Academica</cargoDiretor>
  <cargoDecano>Decano de Extensão</cargoDecano>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"Id="SIG77800">
  <ds:SignedInfo>
  <ds:CanonicalizationMethodAlgorithm=
```

```
"http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments">
</ds:CanonicalizationMethod>
<ds:SignatureMethodAlgorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256">
</ds:SignatureMethod>
<ds:Reference URI="">
<ds:Transforms>
<ds:TransformAlgorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256">
</ds:DigestMethod>
<ds:DigestValue>eY955YuwyWH3TGE9qYm3xf4MxejKUi8uRPaAbvBBe1s=
</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
  r2aTcJoE8pwKvvrnuqI/iHvPsCbrsTtvJZ9i1qResTi6BSmcICG9PaCSU2ImPPLCevWTC81EPVN+RDm
  nnNQUgxnR2ad+6M3Qrtq1Zu7dKBduL3Yqm+8rtLhVlB28NYdEQjM5iq7hsePyKGQhINkwO+R0LZSOlO
  XCSj2zkjdM88oYGfnH3l7gKlMZfweujOTZh1LBt4m7b2GLCnLdQQAQ6kok2kCP9jELn+y6cSDuT9+gy
  rQ9Uf2DDA9+PQqvnqXf+lwsppySAY8RlSUICd4Xngzff7qAMP2TihNQY4/BCjtjP64Ax0kxxQAwqNDc
  lS1ai7RuexE6NZVas51JBKUg==
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
  MIIEIDCCAwigAwIBAgICApEwDQYJKoZIhvcNAQELBQAwYTELMAkGA1UEBhMCQlIxITAfBgNVBAoMGFV
  uaXZlcnNpZGFkZSBkZSBCcmFzaWxpYTERMA8GA1UEBwwIQnJhc2lsaWExCzAJBgNVBAgMAkRGMQ8wDQ
  YDVQQDDAZBQy1DUEQwHhcNMTMxMTI4MTkzMTQ1WhcNMTYxMTI3MTkzMTQ1WjCBjjEXMBUGA1UEAwwOQ
  W5kcmVpIFF1ZWlyb3oxITAfBgNVBAoMGFVuaXZlcnNpZGFkZSBkZSBCcmFzaWxpYTERMA8GA1UEBwwI
  QnJhc2lsaWExCzAJBgNVBAgMAkRGMQswCQYDVQQGEwJCUjEjMCEGCSqGSIb3DQEJARYUYW5kcmVpcXV
  laXJvekB1bmIuYnIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCw9aRuzAqNqrVLTMIX86
  wDqwSdQggCQWfMgy3yYAy1MVTLIWmB43Ixs8A931ZwWMPfEW+uf8pm1Q80Vvf402VRIoBt5l4Qgccpz
  IIgfm55E1sku0IXYSlp1BM0I5v1yZGeGqPItqmVihK7I6SPnotVmNvG1gv8mmA+aZI8qJInMGPFtKbf
  GuTWQSI3lon2jAXDrLz4VKwgbJ5bbIjQJE1seucoDg4Om+pdy4x3vO5iuTgfq988yJKFBDk/W+cekJl
  i7XD8k5Hnb9RB3h2gj6A0EyKOmFlInmLOozkwhyJbeVoYosUyHOofzDwZIv9nNB/mX8evtZY0oIDRQ9
  GPt3nJAgMBAAGjgbMwgbAwHQYDVR0OBBYEFEvKX46yiA63e3HQKMGa0EOEDlZmMB8GA1UdIwQYMBaAF
  GLf0lLuEspBY9j0BECDV2x0NVkKMA4GA1UdDwEB/wQEAwIFoDBeBgNVHREBAf8EVDBSgRRhbmRyZWlx
  dWVpcm96QHVuYi5icqA6BgVgTAEDAaAxBC8wNzAzMTk4NTcyMTE4NDIzMTg3MTIzNDU2Nzg5MDEwMDA
  wMjIwNzM2NVNTUC9ERjANBgkqhkiG9w0BAQsFAAOCAQEAYeFyZ4SmVkFk2WZiLo37FYfF7P654I17wu
  ZAGU1AUnSS8mI+2aWdmTs6mDBAf5IdowmSyJJ5y/Cgso3LmTplAMkaRalmTXmOpESfm+OUG00JGJt1/
```

```
    rNZeohHI+5MI/FIdCEtIMpZFCQutjsBYQ9rkJfqriouniMZ03+EgYbbzB0VaNByIKU2Q21h94M/61zE
    2pT07ImdhpI+Jp6ZyVtAlela0xpnaJyrFrWdL3AihdGCMHWICqGC6VS2GqiW/vM6ficg2kq3L7Kwo1T
    gP8jyDJ5akbUV308U3yxEyPJczV/pbPyNbjxAE4xhbvYwZaczg/IuHuP8V84eJPm9UkDDwg==
  </ds:X509Certificate>
  </ds:X509Data>
  </ds:KeyInfo>
  </ds:Signature>

</certificadoExtensao>
```

Anexo III

Certificado `.pdf`

Certificamos que **XXXX XXXXXX XXXXXXX XXXXXX**, documento de Identificação CPF 999.999.999-99, participou como cursista da ação de extensão DESIGNING WITH WORDS - Evento, na **UNIVERSIDADE DE BRASÍLIA**, no período de 99 de Setembro de 9999 a 99 de Dezembro de 9999, com duração de 9 hora.

Brasília - DF, 99 de Novembro de 9999

Avaliação Final
Menção: SS
Frequência: 100%

Secretário Adjunto de Administração Acadêmica

Decania de Extensão

Figura III.1: Modelo de certificado.