INSTITUTO FEDERAL DE SÃO PAULO - IFSP
ÁREA DE INFORMÁTICA
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS - ADS

GEORGIA KRAUZE SCHNEIDER

INFRAESTRUTURA SEGURA PARA DOCUMENTOS ELETRÔNICOS DE UMA INSTITUIÇÃO DE ENSINO

TRABALHO DE CONCLUSÃO DE CURSO - TCC

CARAGUATATUBA
2013

GEORGIA KRAUZE SCHNEIDER

INFRAESTRUTURA SEGURA PARA DOCUMENTOS ELETRÔNICOS DE UMA INSTITUIÇÃO DE ENSINO

Trabalho de Conclusão de Curso apresentada como requisito à obtenção do título de Tecnólogo, da Área de Informática, do Instituto Federal de São Paulo.

Orientador:
Prof. M.e Nelson Alves Pinto

CARAGUATATUBA

2013

S359i SCHNEIDER, Georgia Krauze.
Infraestrutura segura para documentos eletrônicos de uma instituição pública / Georgia Krauze Schneider. Caraguatatuba, SP - 2013.
42f.

Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas)–Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Caraguatatuba, SP, 2013.

1. Certificação – Segurança. 2. Documentos eletrônicos. I. Título

.

CDD - 005.8

Ministério da Educação
Instituto Federal de São Paulo
Campus Caraguatatuba
Adriano Aurélio Ribeiro Barbosa
Lineu Fernando Stege Mialaret
Análise e Desenvolvimento de Sistemas

TERMO DE APROVAÇÃO

INFRAESTRUTURA SEGURA PARA DOCUMENTOS ELETRÔNICOS DE UMA INSTITUIÇÃO DE ENSINO
por

GEORGIA KRAUZE SCHNEIDER

Este(a) Trabalho de Conclusão de Curso (TCC) foi apresentado(a) em 17 de Dezembro de 2013 como requisito parcial para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas (ADS). O(a) candidato(a) foi arguido pela Banca Examinadora composta pelos professores abaixo assinados, a qual após deliberação, considerou o trabalho aprovado.

_____
Prof. Nelson Alves Pinto
Orientador

_____
Prof. Lineu Fernando Stege Mialaret
Presidente

_____
Prof. Wanderson Santiago dos Reis
Membro

Dedico este trabalho à minha família.

AGRADECIMENTO

Agradeço ao meu orientador Prof. Nelson, pela disposição e paciência durante o desenvolvimento do trabalho.

Agradeço ao coordenador do curso Prof. Lineu, pela disponibilidade.

Agradeço a minha família, pela compreensão.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

RESUMO

Os documentos eletrônicos vêm cada vez mais sendo utilizados em vários ambientes organizacionais. Com isso surgiu a dificuldade em gerenciar de forma segura esses documentos. Uma solução encontrada foi a Certificação Digital, que é cada vez mais vez utilizada por órgãos públicos e privados, para garantir a segurança na transação de documentos institucionais. Para isso foi necessário que se criasse uma normatização para a padronização da utilização dos certificados da infraestrutura necessária para o uso das chaves públicas, que no Brasil é instituído como ICP-Brasil. Esse trabalho visa analisar essa estrutura para uma Instituição de Ensino e como ela poderá ser implantada.

Palavras-chave: Documentos. Certificação. Segurança. Infraestrutura. Chaves.

ABSTRACT

Electronic documents have been increasingly used in various organisational environments. As a consequence, the need to provide the management of these files with security has become a difficult requirement. One solution is the digital certification, which is increasingly used by government and private agencies to ensure more secure transactions of documents and reports. Thus the need to create a distinct regulation to standardise the use of infrastructure certificates required by public keys in Brazil, which were established as ICP-Brazil. This work aims at analysing and implementing this structure in an educational institution.

Keywords: Documents. Certification. Safety. Infrastructure. Keys.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ICPEdu	Infraestrutura de Chaves Públicas para Ensino e Pesquisa
ITI	Instituto Nacional de Tecnologia da Informação
XML	*eXtensible Markup Language*
AC Raiz	Autoridade Certificadora Raiz
AC	Autoridade Certificadora
AR	Autoridade de Registro
CG	Comitê Gestor
EJBCA	*Enterprise Java Bean Certificate Authority*
RNP	Rede Nacional de Ensino e Pequisa
GOPAR	Grupo de Operação de Autoridades de Registro
PC	Política de Certificação
DPC	Declaração de Práticas de Certificação

SUMÁRIO

1. INTRODUÇÃO

As Instituições de Ensino, devido à complexidade dos serviços que prestam, trabalham com um número cada vez maior de documentos. Nos sistemas atuais, a maior parte desses documentos é impressa, gerando custos de material e consequências ao meio ambiente. Também a manutenção, pesquisa e indexação desses documentos impressos incluem custos adicionais que somente aumentam com o tempo.

A possível substituição de documentos impressos por documentos eletrônicos traria resultados benéficos para as instituições de ensino tanto com relação a custos quanto armazenamento, pesquisa, disponibilidade e mesmo exploração e mineração de dados.

Entende-se que esses documentos precisam conservar características de segurança, tais como integridade, autenticidade, disponibilidade e sigilo. Para garantir cada uma dessas características se faz necessário uma infraestrutura adequada que também leve em conta problemas críticos de controle de acesso aos dados e segurança física. Além disso, deve-se prover um serviço que garanta a identificação do emissor dos documentos, o não-repúdio e a legalidade dos mesmos

Outro fator importante diz respeito à autorização de acesso aos documentos somente por pessoas que possuam privilégios para tal. Contudo, esses documentos também precisam suportar serviços de armazenamento, pesquisa e indexação. Assim, tem-se que a infraestrutura pretendida saiba lidar com esses interesses conflitantes.

Este trabalho propõe que tal ambiente seja modelado através da mesclagem das tecnologias de infraestrutura de chaves públicas e serviços de arquivos.

A seguir serão apresentados o escopo do trabalho, revisão bibliográfica, conceitos importantes e proposta do trabalho.

1.1. ESCOPO

O trabalho visa propor uma infraestrutura segura para documentos eletrônicos, com sugestões para implementação da mesma e análise de elementos de segurança e normas e leis vigentes sobre o assunto.

1.2. GESTÃO ELETRÔNICA DE DOCUMENTOS

Gestão Eletrônica de Documentos (GED) consiste no uso de ferramentas digitais para gerenciar documentos[1], com o objetivo de automatizar pesquisas e indexação de arquivos e até diminuir custos da empresa com cópias e papéis[2]. Existe uma grande preocupação com relação à segurança da GED. Este trabalho propõe uma outra abordagem sobre documentos eletrônicos.

1.3. CARACTERÍSTICAS DE SEGURANÇA

Para garantir que uma informação seja de fato segura, é necessário que algumas características sejam encontradas nela. As principais características da Segurança da Informação são [3]

- Autenticação - ato de confirmar existência do usuário.
- Autorização - ato de determinar o que o usuário irá acessar.
- Privacidade - ato de garantir o sigilo a informação.
- Integridade - ato de proteger os dados contra alterações indevidas.
- Não-Repúdio - ato de provar participação do usuário na transação.
- Disponibilidade - ato de garantir acesso ao sistema.

1.4. CRIPTOGRAFIA

Criptografia consiste em transformar mensagem, dado ou código em texto embaralhado que só pode ser decifrado com o conhecimento de um segredo [4].

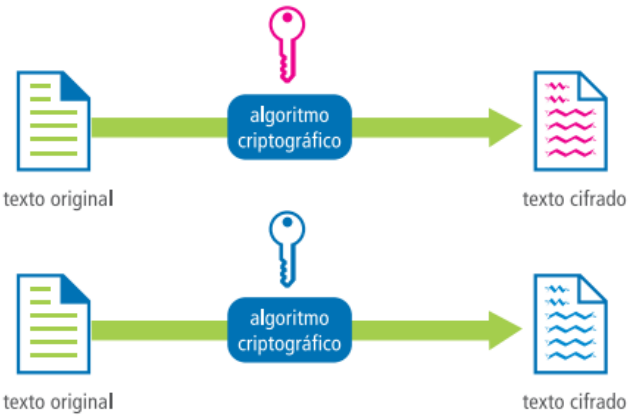

Figura 1: Algoritmo de criptografia

Imagem disponível em: http://www.iti.gov.br/images/publicacoes/cartilhas/cartilhaentenda.pdf

Desde a Idade Antiga são utilizados diversos métodos de cifrar (ou criptografar) mensagens. Tais métodos são chamados de algoritmos de criptografia e consistem basicamente de três partes básicas:

- Um método para cifrar a mensagem.
- Um método para decifrar a mensagem.
- Um segredo que serve como chave do cadeado para decifrar a mensagem.

1.4.1. Chave Ou Segredo

Trata-se de um texto que serve para decifrar a mensagem enviada. Em tempos antigos, consistia de palavras ou frases. Nos anos 1970 passou a consistir de números muito grandes[5].

1.4.2. Canais Seguros

Nos dias de hoje o grande desafio dos algoritmos de criptografia é compartilhar informação entre entidades separadas fisicamente por distâncias enormes. Para garantir as características de segurança de uma informação se faz necessário que o canal de transmissão não possa ser adulterado, falsificado, interceptado ou revelado [3] Caso o canal de transmissão consiga garantir-se dessas ameaças ele é considerado como canal seguro.

1.4.3. Algoritmos Simétricos

Os algoritmos simétricos criptografam a mensagem com um segredo compartilhado pelas entidades. São muito utilizados nos casos de armazenamento seguro de arquivos. A maior limitação dos algoritmos simétricos está no fato de que o segredo não pode ser transportado em canais inseguros.

1.4.4. Algoritmos Assimétricos

Os algoritmos assimétricos trabalham com duas chaves de criptografia. Uma denominada chave privada, conhecida somente por seu proprietário, a outra denominada chave pública que fica disponível a todos. Esses algoritmos são utilizados para trocar as chaves de forma segura[4]. Como vantagem pode-se dizer que a chave gerada pelo algoritmo assimétrico é mais forte que a gerada pelo algoritmo simétrico, porém precisa de um tempo maior de processamento, o que pode ser considerado uma desvantagem. Os Algoritmos assimétricos tentam lidar com o transporte do segredo por canais inseguros. Um exemplo de algoritmo assimétrico e o algoritmo de Diffie-Hellman[4].

Como evolução dos algoritmos assimétricos surgiu os algoritmos de criptografia de chave pública que trabalham com duas chaves para cada entidade, uma para cifrar as mensagens e outra para decifrar[4].

O principal algoritmo de criptografia de chave pública é o RSA, criado por Ronald Rivest, Adi Shamir e Leonard Adleman e trabalha com fatoração de números primos. Nesse algoritmo, o segredo é dividido em duas chaves diferentes.

A primeira destas chaves, conhecida por Chave Pública, deve ser publicada para que o receptor tenha acesso à mesma. Com essa chave é possível cifrar uma mensagem que só pode ser aberta pelo dono da chave privada.

A segunda chave, conhecida por Chave Privada, fica de posse do emissor e serve para decifrar mensagens cifradas com a Chave Pública.

1.4.5. A Criptografia Aplicada Na Proteção Da Informação

A criptografia com algoritmos assimétricos permite que sejam alcançados duas características da segurança da informação. Através do uso de cifragem com chave

privada é possível garantir integridade e a privacidade das informações contidas na mensagem.

Contudo, os algoritmos assimétricos não podem garantir que a entidade seja de fato quem diz ser. Isso ocorre porque não há garantias de que a chave pública seja vinculada diretamente a seu dono. Por consequência, não se pode provar a participação da pessoa no envio da mensagem o que impede a característica do não-repudio.

Assim, para garantir autenticidade e não-repúdio foi introduzido na comunicação segura uma terceira parte, responsável principalmente por armazenar as Chaves Públicas e garantir a identidade das outras entidades envolvidas.

Essa terceira parte é chamada de Autoridade e pode ser considerada como base para a Infraestrutura de chaves Públicas [4].

1.5. INFRAESTRUTURA DE CHAVES PÚBLICAS

Assim que surgiram os primeiros algoritmos assimétricos percebeu-se que eles eram apenas parte de uma solução e que a maioria dos problemas exigia que se estabelecesse uma entidade na qual os envolvidos pudessem confiar plenamente [3] [4].

Tal entidade deveria ser responsável por gerar o primeiro Certificado Digital e armazená-lo de forma segura. Essa mesma entidade deveria também ser responsável por emitir Certificados Digitais, armazenar e gerenciar os prazos de validade das Chaves Públicas, além de nomear outras entidades para essas tarefas. Por sua importância, essa entidade foi chamada de Autoridade.

No Brasil, a Autoridade foi outorgada ao Instituto Nacional de Tecnologia da Informação (ITI), sendo esse órgão responsável pela Autoridade Raiz, entidade que armazena o Certificado Digital, chamado de Certificado Raiz, que será base para todos os demais Certificados emitidos no Brasil [3]

A ICP-Brasil foi instituída pela Medida Provisória nº 2.200-2 e normatizou a Certificação Digital no país. O modelo adotado pelo Brasil foi o de certificação com raiz única, ou seja, todas as outras entidades de primeiro nível são diretamente credenciadas pela Autoridade Raiz.

A ICP-Brasil abrange configurações, normas e procedimentos necessários para trabalhar com os Certificados Digitais. Seu principal objetivo é manter um ambiente onde as características de segurança da informação sejam garantidas.

Para tal a ICP-Brasil:

- Determina a disposição da sala da AC em relação ao prédio,
- Define os requisitos de proteção da sala contra fatores ambientais (incêndio, enchente, queda de energia),
- Delimita o controle de acesso físico da sala da AC,
- Estabelece as funções de cada parte envolvida,
- Padroniza *hardware* e *software* utilizados,
- Testa e valida regras para geração das chaves e uso dos certificados,
- Entre outras tarefas.

A partir do estabelecimento da Autoridade Raiz se faz necessário nomear outras autoridades cuja responsabilidade será certificar as demais entidades. Assim, uma Autoridade Raiz passa a ter como principal tarefa gerenciar certificados das Autoridades Certificadoras e estas cuidam dos certificados dos demais envolvidos.

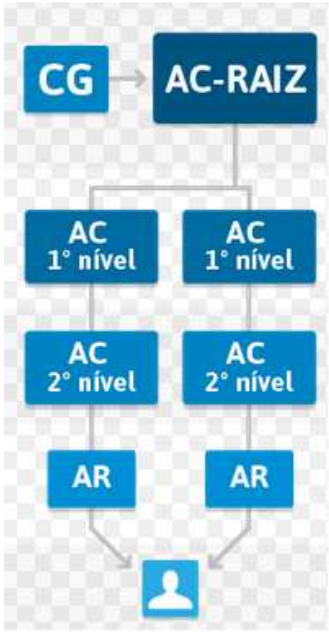

Figura 2: Hierarquia das Autoridades Certificadoras

Imagem adaptada de: http://www.beneficioscd.com.br/img/hierarquia.png

1.5.1 Autoridade Certificadora

Autoridade Certificadora (AC) é o órgão responsável por gerenciar o par de chaves privada e pública, atribuir o Certificado Digital ao usuário e definir as regras de uso do mesmo. Também deve renovar e revogar os certificados, além de manter a lista de certificados revogados. A AC deve gerenciar os *softwares* que usam o Certificado Digital como forma de autenticação, bem como auditar as Autoridades de Registro (AR) vinculadas.

1.5.2. Autoridade De Registro

A Autoridade de Registro é responsável por fazer o contato direto com o usuário. A Autoridade de Registro solicita a emissão do Certificado Digital para a AC a qual é vinculada.

1.5.3 XML

XML (*eXtensible Markup Language*) é uma linguagem de marcação criada para facilitar a descrição e transporte de dados[6]. Também ajuda a definir tipos de documentos. XML foi criado para ajudar na integração com outras linguagens, o que permite a portabilidade do sistema. Assim o XML é estruturado por *tags* que são definidas pelo autor. *Tags* são palavras-chaves que representam comandos para o sistema[7].

O XML é utilizado amplamente para formatar as informações disponibilizadas por Autoridades dentro da estrutura ICP-Brasil.

Um exemplo de arquivo XML seria:

```
<Pessoa> nome = “Fulano”
        <CPF>123.456.789-01</CPF>
        <senha>123456</senha>
 </Pessoa>
```

1.5.4 Certificado Digital

Certificado Digital é um arquivo eletrônico que associa uma chave pública de uma entidade às demais informações relacionadas a ela, o que permite identificar tal

entidade plenamente. Note-se que a chave privada não faz parte do arquivo do Certificado, sendo salva em arquivo à parte. Em geral, é um arquivo no formato XML que deve ser armazenado de forma segura pela AC. Esse arquivo segue os requisitos estabelecidos pelo padrão internacional X.509 [3]. Outro arquivo XML é disponibilizado num repositório público contendo apenas a chave pública.

Um último arquivo com a cópia da chave privada é armazenado em um *token* ou *smartcard* e fica sob responsabilidade da entidade (proprietário). Considera-se que esse arquivo é único e intransferível. Uma quebra de segurança do mesmo resulta na revogação do Certificado Digital.

1.5.5. Proprietário Do Certificado Digital

O proprietário do certificado também denominado entidade possui o par de chaves e através delas consegue ter sua identidade determinada. A chave pública permite que as outras pessoas se comuniquem com o proprietário e disponibilizem informações que ele conseguirá ler com a respectiva chave privada.

1.5.6. Algoritmos De *Hash*

Algoritmos de *hash* tem o objetivo de calcular um número que seja único para cada mensagem. A alteração de um único *bit* altera completamente o valor de *hash* gerado. Isso permite garantir que caso seja quebrada a integridade da mensagem o valor do *hash* tenha outro resultado.

1.5.7. Assinatura Digital

Assinatura Digital é uma forma de garantir a integridade e autenticidade da mensagem através das chaves criptográficas durante a transmissão do autor para o destinatário[3]. Sendo assim, o destinatário sempre terá que verificar se a chave que ele recebeu é igual com a que calculou na decriptação da mensagem. A assinatura digital é um valor de *hash* calculado sobre a mensagem criptografada.

1.6. POLÍTICAS DE SEGURANÇA DE UMA AC

Para que uma AC garanta todas as características de segurança de um Certificado Digital se faz necessário que a mesma aplique regras de segurança

conforme padrões internacionalmente estabelecidos. Tais regras são chamadas de políticas de Segurança e abrangem ambiente físico e lógico do sistema, componentes do sistema bem como o ciclo de vida do mesmo.

1.6.1 Cerimonial

Alguns processos de uma AC exigem uma série de protocolos e diversas formas de Auditoria ocorrendo simultaneamente. Tais processos são chamados de cerimoniais e envolvem rigorosas políticas de segurança para serem realizados.

1.6.2. Leis E Normas

A ICP-Brasil trabalha com os documentos regidos pelo Comitê Gestor (CG) e Comitê Organizador. Para que uma AC seja aceita como parte da ICP-Brasil se faz necessário cumprir rigorosamente todas as normas e leis estabelecidas. Eis alguns exemplos de regulamentos importantes:

- A resolução 20 determina o desenvolvimento de uma plataforma criptográfica aberta, voltada a operação da AC RAIZ, ou seja, um sistema de criptografia para os certificados.
- A resolução 51, que trata da politicas de segurança da ICP-Brasil está associada ao Documento ICP-Brasil-03 v.3.0
- A Instrução normativa 3/2007 aprova a versão 3.0 dos requisitos técnicos a serem observados nos processos de homologação de cartões inteligentes (*smarts cards*) e *tokens* criptográficos no âmbito da ICP-Brasil está associada ao DOC-ICP-10.03 v.3.0
- O Manuais de Condutas Técnicas 5 volume I define os requisitos, materiais e documentos técnicas para homologação de software de autenticação no âmbito da ICP-Brasil, ou seja, todas as regras para autenticar o usuário com o Certificado Digital.
- A Instrução normativa 6/2006 contem o formulário de solicitação de credenciamento de AC e compõe o documento ADE-ICP-03.B vol 1.0

1.6.3. Segurança Física

Segurança física é a delimitação do acesso a informação ou a infraestrutura através de barreiras físicas. Se aplicam, por exemplo, em servidores com portas, trancas e guardas que procuram garantir que o local seja acessado somente por pessoas permitidas. Essas medidas visam desencorajar possíveis ataques ao sistema.

1.6.4. Ponto De Acesso Público De Uma AC

Uma AC obrigatoriamente deve prover um ponto de acesso onde usuários anônimos se conectam e baixam os arquivos contendo Chaves Públicas das entidades identificadas pela própria AC. Os serviços de arquivos suportados por uma AC são altamente restritivos.

1.7. SERVIÇOS DE ARQUIVOS

Serviços de arquivos são fornecidos por sistemas operacionais de rede que gerenciam arquivos, usuários e listas de controle de acessos (ACL). Os serviços mais comuns são: armazenamento, indexação, pesquisa, edição, versionamento e exclusão.

1.7.1. Uma Estrutura AC Como Servidor De Arquivos

Conforme pode se inferir uma AC possui rigorosas políticas de segurança que garantem as características de informação de determinados documentos. Além disso, o uso de Certificados Digitais é o padrão de mercado para documentos que necessitam de legalidade. Documentos assinados digitalmente são aceitos como provas jurídicas em tribunais do mundo todo [4].

Contudo, uma AC não se responsabiliza pelo armazenamento do arquivo criptografado, ficando tal tarefa por conta do proprietário do mesmo. Essa limitação ocorre, principalmente pelo fato de que as tarefas de uma AC são muito específicas.

Também não se pensou em acrescentar tal função às ACs pelo fato de que os documentos não podem ser decifrados para o caso de tarefas simples, como por exemplo, pesquisa de palavras chaves.

Para fornecer tais serviços seria necessário que algumas partes do documento contivessem texto não-criptografado.

Embora isso seja inviável para alguns documentos confidenciais, o mesmo não ocorre para documentos acadêmicos onde o nível de confidencialidade é considerado baixo. Assim uma abordagem seria cifrar apenas parte do documento e deixar outra parte com informações públicas acessíveis.

Essa abordagem é possível com a utilização de arquivos XML, onde a parte criptografada poderia ter uma *tag* própria.

Um exemplo de arquivo XML seria:

```
<Pessoa> nome = “Fulano”
        <CPF>123.456.789-01</CPF>
        <senha>{&hH%$N(8</senha>
 </Pessoa>
```

Onde a *tag* senha armazena um valor criptografado por uma Chave Pública e só pode ser lida pelo dono da Chave Privada. Um programa poderia fazer busca e indexação de informações através do CPF e nome, contudo não conseguiria ler a senha do usuário.

Baseando-se nisso, a proposta desse trabalho planeja a construção de uma Autoridade cujos níveis de segurança são garantidos pela aplicação de políticas de segurança comuns a uma AC. Essa Autoridade proposta poderá utilizar como base um Certificado Digital emitido pela ICPEdu ou por uma das ACs que fazem parte da ICP-Brasil ou mesmo poderá gerar seu Certificados (que teriam apenas validade interna, nesse caso). Daqui por diante a AC com Serviços de Arquivos será chamada apenas de Autoridade proposta.

1.7.2. Diferença Entre A Autoridade Proposta E Uma AC

O maior diferencial entre a Autoridade proposta e uma AC é que a primeira armazenará também os documentos criptografados por seus usuários, servindo como repositório público para os mesmos. Tais arquivos seguirão um formato XML apropriado para arquivos eletrônicos de uma instituição acadêmica.

Qualquer entidade pode baixar um arquivo criptografado, mas somente quem possuir o Certificado Digital adequado poderá ler o conteúdo do mesmo.

Note-se que a estrutura proposta apresenta diversas dificuldades relacionadas á manutenção de arquivos, principalmente porque parte dos mesmos estarão criptografados. Dessa forma, exige-se que diversas tarefas sejam reestruturadas de forma a atender as necessidades dos usuários.

1.8. Proposta

O trabalho proposto documenta os possíveis passos para implementação de uma AC e uma abordagem para acrescentar na AC serviços de arquivos que permitem armazenar e gerenciar os documentos da instituição através da estrutura XML para definição dos níveis de acesso.

No capitulo 2 serão abordados a estrutura necessária, para implementação, as formas de obtenção do certificado raiz, os requisitos do ambiente físico, computacional e do pessoal autorizado, os cerimoniais necessários.

No capitulo 3 será apresentada a conclusão do trabalho

2. DESENVOLVIMENTO

No intuito de aplicar a proposta apresentada no capítulo anterior serão descritos a seguir os processos envolvidos na implantação e operação da Autoridade responsável por armazenar os documentos eletrônicos de uma Instituição Acadêmica.

2.1. ESTRUTURA MÍNIMA NECESSÁRIA

Considera-se que para todas as abordagens apresentadas a seguir existirá uma estrutura comum. A saber:

- Sala com um mínimo de 12 metros quadrados equipada com climatizador de temperatura, extintores de incêndio, estrutura elétrica adequada, cabeamento de redes e controle de acesso restrito por equipamentos eletrônicos mediante identificação.
- Computador servidor com um mínimo de 16 Gb de memória RAM, capacidade de armazenamento em disco superior a um Tb.
- Conexão de alta velocidade com a internet. Mínimo recomendável de 30 Mbps.
- *No-break* com capacidade adequada para mais de vinte minutos de queda de energia.
- Oito funcionários com dedicação parcial para as tarefas de gerência, administração, operação e *backup* da Autoridade.
- *Tokens* de armazenamento para as chaves privadas das entidades, sendo um *token* para cada Certificado Digital.

2.2. OBTENÇÃO DO CERTIFICADO RAIZ.

O Certificado Raiz a ser utilizado pela Autoridade pode ter três origens, listadas a seguir:

- Obtido através do ICPEdu;
- Obtido através de uma AC da ICP-Brasil;
- Criado internamente.

2.2.1. Certificado Obtido Através Da ICPEdu

A Infraestrutura de Chaves Públicas para Ensino e Pesquisa [8] trabalha com certificação digital em ambientes educacionais como instituições Federais de Ensino Superior (Ifes), Unidades de Pesquisa (UPs) e demais instituições de ensino. A AC Raiz é gerenciada pela Rede Nacional de Ensino e Pequisa (RNP).

Para se credenciar na ICPEdu é necessário seguir três passos [9]:

- O primeiro passo é uma portaria da instituição nomeando o gestor da Autoridade Certificadora. O documento deve ser enviado ao Grupo de Operação de Autoridades de Registro (GOPAR);
- O segundo passo é fazer os dois documentos exigidos, a Política de Certificação (PC) e a Declaração de Práticas de Certificação (DPC), e envia-los para GOPAR; e
- O terceiro passo é providenciar o recurso físico para sala da AC, *hardware*, *software*, equipamentos e recursos humanos.

2.2.1.1. Custos

Caso opte por filiar-se à ICPEdu a instituição passará por auditorias e testes para avaliar-se seu pleno funcionamento. Note-se que nesse caso o servidor de Arquivos terá que ficar fisicamente separado da estrutura da Autoridade, visto que o IFSP seria oficialmente uma Autoridade Certificadora. Assim, seria necessário duplicar toda a estrutura mínima, exceto funcionários. Uma das salas seria destinada para gerenciamento das operações da AC e outra destinada a gerenciar os arquivos armazenados.

O modelo é mostrado na figura 3:

Figura 3 - Estrutura de Servidores

2.2.1.2. Benefícios

Nesse caso, o IFSP teria por principal vantagem a emissão de quantos Certificados Digitais quisesse. Por exemplo, seria possível ter um certificado para cada departamento ou projeto dentro da Instituição. Ou então, emitir Certificados Digitais para todo o pessoal técnico administrativo.

2.2.2. Certificado Obtido Através De Uma AC Da ICP-Brasil

O IFSP, como pessoa jurídica, pode comprar um Certificado Digital de uma AC da ICP-Brasil e usá-lo como Certificado Raiz. Nesse caso os Certificados Digitais seriam apenas para uso interno e não teriam validade jurídica para fora do IFSP.

Para entender o que é um certificado interno deve ser lembrado que somente uma Autoridade Certificadora pode emitir certificados aceitos pela ICP-Brasil. O uso de certificados fora desse ambiente é considerado inválidos, pois seus emissores não são plenamente identificados pela ICP-Brasil.

Isso impede que entidades dentro da ICP-Brasil possam confiar nesses certificados, pois se quebra a característica de não-repúdio. No entanto esses certificados podem ser usados normalmente com algumas restrições. Por exemplo, os navegadores precisam que esses certificados sejam instalados manualmente para serem aceitos.

2.2.2.1 Custos

Os custos dessa abordagem seriam os mínimos com relação aos certificados, visto que seriam gerados dentro do IFSP.

2.2.2.2. Benefícios

Nessa opção o IFSP também poderia gerar quantos certificados quisesse, com a única desvantagem de serem todos internos. Os custos seriam mínimos.

2.2.2.3. Abordagem Com CPF Digital

Uma possível abordagem para o problema dos certificados internos seria exigir que todos os usuários submetidos à Autoridade utilizassem Certificados gerados por uma AC da ICP-Brasil, tal como o CPF Digital. Essa abordagem elevaria os custos, todavia daria aos usuários da Autoridade a validade jurídica necessária.

Em termos financeiros, essa abordagem seria a mais cara de todas.

2.2.3. Obtido Internamente

O Certificado Raiz pode ser gerado internamente. Nesse caso, os custos seriam os mínimos possíveis, sendo o IFSP responsável por escolher quais políticas de segurança implantar, bem como servidores e aplicações de *software* a serem utilizados.

2.2.3.1. Custos

Os mínimos necessários. Certificados seriam todos internos.

2.2.3.2. Benefícios

Redução das políticas de segurança para os menores custos possíveis. Deve ser ressaltado que a segurança seria reduzida aos níveis minimamente aceitáveis.

2.2.4. Considerações Sobre A Melhor Abordagem

Para fins acadêmicos, nesse trabalho considera-se que a melhor abordagem seja implantar uma Autoridade Certificado abaixo da ICPEdu. Os ganhos em tecnologia, sigilo e independência de outras tecnologias compensaria os eventuais gastos. O certificado também teria validade jurídica conforme Renato Martini, presidente do

Instituto Nacional de Tecnologia da Informação (ITI), destacou no fórum promovido pela Rede Nacional de Ensino e Pesquisa (RNP)[10]

2.3. AMBIENTE FÍSICO

O ambiente necessário para a implantação da Autoridade exige os mais diversos requisitos espalhados por diversas normas, resoluções e padrões.

A fim de simplificar a tarefa de implantação do ambiente físico optou-se pela utilização das Boas Práticas recomendadas pela ICPEdu[11]

Nesse documento o Comitê da ICPEdu aborda os requisitos de duas maneiras.

A primeira delas é exigindo os chamados requisitos mínimos. Sem estes a AC não é autorizada a operar. Na segunda abordagem segue-se as melhores práticas, que cobre muito mais do que os requisitos mínimos.

No intuito de diminuir custos os requisitos abordados a seguir fazem parte dos Requisitos Mínimos recomendados pela ICPEdu[11]:

- Sala sem janelas (ou com janelas seguras) afastadas de fontes magnéticas e interferências de rádio.
- Sala somente acessível ao pessoal autorizado através de controles de porta eletrônica, cujo acesso se dá por senhas, crachás ou identificação biométrica.
- Cada funcionário deve ter usuário único no computador.
- Arquivos do computador e do *backup* devem ser criptografados.
- Sala deve ter sistema de ar condicionado e livre de oscilações e quedas de energia.
- Sistema deve ser protegido de alagamentos, goteiras e infiltrações.
- Sala deve conter sistema de detecção e controle de incêndios.
- Toda a mídia deve ser manuseada apenas por pessoal autorizado e deve ser armazenada em local seguro e adequado. Sugere-se o uso de cofres.
- O material descartado deve ser completamente destruído. Em casos de discos rígidos os mesmos devem ser formatados pelo menos 16 vezes antes de serem descartados.
- Cópias externas devem ser feitas. Para tal, será necessário criar um cerimonial de *backup*.

2.4. PESSOAL AUTORIZADO

Cada pessoa autorizada deve possuir um papel especifico, chamado de Papel de Confiança, cujas funções são previamente determinadas pelas Boas Práticas. Os quatro Papéis de Confiança possíveis são [11]:

- Gerente: responsável pela Autoridade tanto para redigir quanto aprovar relatórios. Também é responsável por montar toda a equipe de trabalho.
- Administrador: responsável pela instalação, configuração, *backup* e manutenção dos equipamentos e *software* de gestão.
- Operador: responsáveis pelo uso da chave privada da Autoridade para a emissão de Listas de certificados revogados (LCR) e Certificados Digitais.
- Auditor: responsável pela auditoria do ciclo de vida do certificado digital, das chaves criptográficas e de todas as operações AC.

Além das funções definidas anteriormente, também são requisitos para o controle de pessoal:

- Cada indivíduo só pode assumir um Papel de Confiança.
- Devem existir equipes para cada Papel de Confiança, sendo dois indivíduos o mínimo necessário.
- Todo indivíduo deve ter usuário único e instransferível no sistema.
- Devem existir formas de autenticação seguras (biometria, senhas, *tokens*, etc).
- Não se admite que indivíduos sejam funcionários de terceiros.
- Indivíduos devem autorizar a verificação de seus antecedentes.
- Nenhum indivíduo pode assumir funções sem antes ser aprovado em treinamento para tal.
- Treinamentos e auditorias devem ser feitos com frequência previamente determinada.
- Todo indivíduo deve ser avisado sobre as consequências de ações não autorizadas.

2.5. AMBIENTE COMPUTACIONAL

O ambiente computacional necessário é formado por diversos componentes, a saber:

- Computador com processamento e memória adequados. Deve rodar um sistema Operacional auditável e com recursos para múltiplos usuários. Recomenda-se o uso do Linux com ambiente EJBCA.
- *No-break* com tempo de carga superior a vinte minutos.
- Servidor Web com recursos de criptografia habilitados. Recomenda-se o uso do Apache com SSL.
- Bancos de dados de rede. Recomenda-se o Mysql.
- Máquina virtual Java. Recomenda-se o uso do OpenJDK.

Além das necessidades em *software* e *hardware* também são requisitos necessários para o ambiente computacional:

- Dados em disco rígido devem estar criptografados.
- O sistema deve ser completamente auditável.
- Acessos em horários fora do horário de trabalho devem ser bloqueados pelo sistema operacional.
- Nenhum *software* de cliente deve ser instalado. Por exemplo: navegadores, leitores de e-mail, *players* de vídeo.

2.5.1. EJBCA

O *Enterprise Java Bean Certificate Authority* (EJBCA) é um ambiente com integração à aplicações JEE através do JBoss e trabalha com banco de dados MySQL. O ambiente permite criar e gerenciar uma Autoridade Certificadora, bem como criar e gerenciar Certificados Digitais.[12]

Os usuários criados no ambiente EJBCA deverão ter os mesmos nomes dos cargos dos funcionários estabelecidos pela ICPEdu (administrador, gerente, operador e operador de *backup*).

O EJBCA permite diversas operações sobre o Certificado Raiz, sendo as mais importantes:

- A remoção do Certificado Raiz faz com que ele seja desativado, mas possa ser restaurado.
- A renovação do certificado se faz necessária quando o certificado antigo perde o prazo de validade e se cria um novo certificado para substitui-lo. Nesse caso,

todos os certificados abaixo dele, também devem ser alterados.

- A revogação do certificado acontece quando esse não pode ser mais utilizado. Nesse caso, todos os certificados abaixo dele também não poderão mais ser utilizados.

Para lidar com os certificados revogados o EJBCA permite a disponibilidade de listas chamadas de LCR. Estas listas podem ser atualizadas automaticamente ou pode-se optar por forçar a AC verificar cada certificado em busca dos que estão vencidos.

Deve ser ressaltado que o EJBCA trabalha com certificados temporários que servem apenas para uso imediato, tais como serem usados em casos de restauração de chaves onde se necessita cifrar os dados.

2.6. CERTIFICADOS DIGITAIS PARA DEPARTAMENTOS

Considera-se que a maior parte dos documentos gerados por uma Instituição Acadêmica seja de documentos que não estão ligados a um indivíduo e sim ao departamento em que ele trabalha. Também, em muitos casos, se faz necessário que um conjunto de documentos seja compartilhado por um grupo, como por exemplo, num projeto de pesquisa.

Assim, cada departamento precisa ter um Certificado Digital para armazenar memorandos, atas e demais documentos que são amplamente utilizados pelas coordenações, gerências e direção de cada *campus*.

O uso desses Certificados Digitais fica por responsabilidade dos coordenadores do departamento ou projeto. Quando da troca de coordenador ou término do projeto o Certificado é revogado.

2.7. BANCO DE DADOS DE ASSINATURAS DIGITAIS

Alguns processos de serviços de arquivos exigem que sejam armazenados de forma segura as Assinaturas Digitais relacionadas aos arquivos. Um exemplo são os arquivos de *backup* que são cifrados utilizando-se um Certificado próprio e necessitam ser assinados em seguida.

Para tal, será necessário criar um esquema de banco de dados para armazenamento das Assinaturas Digitais sendo que a coluna deve ser criptografada.

Assim, se faz necessário um Certificado Digital somente para essa base de dados.

2.8. CERIMONIAL DE CRIAÇÃO DA CHAVE NO BD

Para gerar o Certificado Digital do BD deve acontecer um cerimonial. Os dois administradores e dois gerentes devem estar presentes. Somente com a presença dessas quatro pessoas o Certificado Digital para o BD é gerado.

A partir de sua geração a Chave Pública é enviada para o repositório de Chaves Públicas da AC.

A Chave privada é então submetida a um algoritmo que compartilha a chave entre quatro entidades, que consiste em dividir a Chave Privada em quatro partes e cifrá-las com as Chaves Públicas das Entidades envolvidas. Esse algoritmo só pode restaurar uma chave se pelo menos três das quatro entidades estiverem presentes no cerimonial de restauração.

Essa distribuição obedece à norma 6.2.10[11]. Nessa norma se deve documentar o método utilizado para distribuição da chave

2.9. CERIMONIAL DE RESTAURAÇÃO DA CHAVE PRIVADA DO BD

Em alguns casos se faz necessário recuperar a chave privada do BD, Por exemplo, para restaurar um *backup*. Nesses casos deve ser iniciado um cerimonial de recuperação de Chave privada que deve contar com a presença de pelo menos três dos quatro participantes da geração da mesma Chave Privada.

A Chave Privada é decifrada na memória e cifrada para um certificado temporário usado exclusivamente no cerimonial em questão. Em seguida, o programa utiliza a Chave Privada para executar suas tarefas. Durante o tempo que o programa ficar executando as Entidades devem estar presentes.

2.10 DOCUMENTOS ANTIGOS QUANDO OCORRE REVOGAÇÃO

Os certificados tem um prazo de validade e quando esse prazo acaba eles são revogados. Nesse caso, se deve criar um novo certificado, mas o administrador da AC deverá atualizar os documentos assinados com o certificado antigo para o novo certificado.

Essa é uma tarefa que exige muito processamento, visto que todos os documentos serão decifrados e cifrados com uma nova Chave e que não existe numa AC. Portanto, trata-se de algo que deve ser normatizado internamente pela Instituição.

A melhor forma de lidar com isso é indisponibilizar todos os arquivos da entidade até que os mesmos sejam todos criptografados com a Chave Nova.

2.11. ROTINAS DE *BACKUP*

Entre os processos mais importantes da Autoridade proposta está o gerenciamento das rotinas de *backup* dos arquivos cifrados. Todos os arquivos de *backup* podem ser armazenados em discos externos desde que estes discos residam em cofres à prova de incêndios e alagamentos. Outra possibilidade é o *backup* externo em algum servidor fora do ambiente.

Em ambos os casos os arquivos devem ser cifrados utilizando-se um Certificado próprio para o *Backup*. Este Certificado Digital deve ser propriedade dos administradores, na forma de segredo compartilhado, e a rotina de cópia deve envolver o armazenamento das Assinaturas Digitais em um Banco de Dados apropriado.

A rotina de cópia de Arquivos deve ser acionada por um Operador. Os arquivos são cifrados utilizando-se a Chave Pública do BD.

Para casos onde seja necessária a restauração de arquivos é acionado o cerimonial de restauração, descrito anteriormente.

2.12. ESTRUTURA DE ARQUIVOS DE SERVIÇOS

Para permitir que as diversas entidades possam utilizar os serviços de arquivos se faz necessário que todos os arquivos a serem armazenados utilizem uma estrutura capaz de lidar com informações cifradas e não-cifradas. Nas seções a seguir são descritos alguns procedimentos e técnicas utilizados para a elaboração do servidor de arquivos.

2.12.1. Sistema De Diretórios Por CPF

O servidor será dividido em três grandes repositórios.

- O primeiro destes repositórios será utilizado para documentos de departamentos, projetos e outras entidades externas. O nome de cada diretório seguirá um

padrão a ser determinado que impeça a duplicação de nomes.

- O segundo repositório será exclusivo para pessoas físicas. Os diretórios de pessoas físicas devem ser nomeados conforme o identificador de cadastro de pessoa Física (CPF).
- O terceiro repositório conterá arquivos mistos conforme a estrutura de cada campus, departamento, curso, turmas e área. Trata-se de um diretório para acesso público, pesquisas e uso acadêmico mais intenso que os demais. Os diretórios de turma podem ser nomeados com um identificador com o ano da turma, semestre do ano e sigla do curso, por exemplo.

2.12.2. Arquivos Embutidos

Sugere-se que os arquivos sejam todos armazenados no formato XML, sendo que arquivos com outras extensões devem ser embutidos. Um exemplo de uma planilha do Excel embutida num arquivo XML ficaria:

```
<ARQUIVO>
    <DONO>1234567</DONO>
    <NOME>planilha.xls</NOME>
    <CONTEUDO> texto criptografado </CONTEUDO>
</ARQUIVO>
```

Essa técnica permite que possam ser feitas pesquisas simples por parte das entidades, contudo o conteúdo só está acessível ao dono do arquivo. Outros dados, tais como data de criação, assunto e último acesso podem ser disponibilizados no XML, caso se opte por isso.

2.12.3 Arquivos Com Níveis Diferentes De Acesso

Em alguns casos será necessário que um mesmo arquivo guarde informações relevantes para duas ou mais entidades. Nesse caso, cada parte da informação deve ser cifrada com a chave da entidade que será proprietária.

Um exemplo ocorre no arquivo abaixo onde o professor com CPF 123 gerou as notas de seus alunos. Diversas entidades precisam ter acesso à diferentes médias.
Além da média final da turma o professor poderia disponibilizar médias para as

seguintes entidades:

- A média dos alunos que entraram pelo regime diferencial para o MEC, por exemplo.
- A média dos alunos que recebem algum tipo de assistência estudantil para a entidade de Assistência Social, por exemplo.
- A média dos alunos que fizeram dependência para a Coordenação do Curso.

O arquivo poderia ficar assim:

```
<DONO>123</DONO>
<TURMA>ano=2013 semestre=2 curso=ADS campus = ARQ</TURMA>
<nota> tabela cifrada com CPF e notas dos alunos</nota>
<medias>
    <entidade>MEC
        <descricao>...</descricao>
        <media>cifrado com chave do MEC</media>
    </entidade>
    <entidade>ASSISTENCIA SOCIAL
        <descricao>...</descricao>
        <media>cifrado com chave do AS</media>
    </entidade>
    <entidade>COORDENAÇÃO DO CURSO
        <descricao>...</descricao>
        <media>cifrado com chave da coordenacao</media>
        </entidade>
</medias>
```

Percebe-se que os níveis de acesso estão definidos para cada entidade de forma que só terá acesso ao mesmo a entidade que é proprietária da informação.

2.13. SERVIÇO DE INDEXAÇÃO DE PESQUISA

Alguns serviços de arquivos dependem completamente das informações contidas

nos cabeçalhos de arquivos XML. Portanto, é necessário que as informações públicas sejam criteriosamente avaliadas a fim de que nem se tornem insuficientes nem revelem mais do que deveriam. Segue-se algumas considerações sobre as principais tarefas de indexação e pesquisa.

2.13.1 Indexação

A indexação de arquivos exige que alguns campos contenham informações que possam ser categorizados. Por exemplo: datas, nomes e valores numéricos inteiros.
São informações candidatas para a indexação: nome do arquivo, dono, data de criação, data de último acesso, data de modificação, número da versão.

Para arquivos da Instituição devem ser pensados em campos que sejam relevantes para qualquer tipo de documento. Por exemplo: Ano letivo, semestre, campus, coordenação, etc.

2.13.2. Pesquisa

A pesquisa em arquivos pode optar por utilizar campos que não podem ser indexados. Campos de descrição, por exemplo. Assim, sugere-se que todo modelo de documento XML tenha um campo para descrição obrigatoriamente.

2.13.3. Modificação

Pode-se optar por permitir que os arquivos sejam modificados pela entidade. Nesse caso o arquivo modificado é anexado como sendo uma nova versão. Para existir tal controle se faz necessário criar rotinas e aplicativos que saibam lidar com esse versionamento em específico.

2.13.4. Exclusão

A exclusão de arquivos não pode ser feita do servidor de arquivos. Quando um arquivo deixa de ser útil deve ser armazenado em algum repositório morto.

2.14. CERIMONIAIS

Nesta seção são descritos os cerimoniais relacionados com a criação e restauração de certificados de Entidades.

2.14.1. Cerimonial De Criação De Certificados

O cerimonial de chaves começa quando o RH encaminha, por exemplo, o professor para o Centro de Certificação Digital. O professor deve apresentar os documentos necessários para dar início ao processo.

Assim que os documentos são verificados o operador realiza o processo de criação do Certificado Digital. Dois arquivos são gerados. Um deles, contendo a Chave Pública, é enviado para o repositório de Chaves Públicas. O outro arquivo, contendo a Chave Privada, é gravado no *token*. Pede-se que o proprietário do certificado digite uma senha que será utilizada para cifrar a Chave Privada dentro do *token*. Deve ser ressaltado que o *token* usa um algoritmo de cifragem simétrico.

Uma cópia da Chave Privada é salva dentro do Banco de Chaves privadas e criptografado com a Chave Pública do certificado Digital do BD.

O processo termina com o funcionário realizando alguns testes para verificar se as Chaves estão funcionando corretamente e por fim assinando um termo de recebimento de Certificado Digital. Sugere-se que o funcionário receba orientações sobre o processo antes que este seja iniciado.

2.14.2 Cerimonial De Restauração De Certificados

Caso, por algum motivo, o proprietário do certificado Digital apague a Chave Privada será necessário um cerimonial para a restauração da mesma. O cerimonial de restauração de certificados exige a participação de Administradores e Gerentes, bem como um Operador. A restauração se faz necessário para não perder os documentos assinados com aquela chave.

2.15. ANÁLISE DE RISCOS DO AMBIENTE

No intuito de melhorar o processo de segurança do ambiente optou-se por realizar-se uma Análise de Riscos para a Autoridade Proposta. Justifica-se tal medida pelo fato de que a Autoridade proposta apresenta diversas outras funcionalidades que não são comuns às Autoridades certificadoras.

Assim, através da Análise de Riscos, pode-se sugerir diversos outros controles que não existem nas normas que regem a implantação de uma AC.

Na tabela 1, os principais riscos a serem analisados quando da implantação da Autoridade proposta:

Tabela 1 - Riscos

	Riscos
1	Disco rigido perde arquivos por conta de falhas na escrita
2	O proprietário do Certificado Digital precisa restaurar seu certificado, pois não foram feitos testes suficientes depois da criação do mesmo.
3	Informações cifradas com Certificado revogado são perdidos porque não foram cifrados com o Certificado Novo.
4	Informações são reveladas a um atacante por conta da má elaboração dos dados de indexação de arquivos.
5	Arquivo de chave privada é extraviado por conta da perda do token
6	O funcionário da AC pode usar a chave privada do BD erroneamente por ficar sozinho na sala sem nenhum outro funcionário por perto
7	O professor pode ter sua chave privada descoberta por não ter ela criptografada
8	O professor pode usar a chave revogada pois o sistema não bloqueou ela
9	Os arquivos podem não ser salvo no servidor devido a queda de energia e a sala não estar preparada com no-breaks e estabilizadores

Após os riscos serem relacionados foram acrescentadas diversas contramedidas que visam melhorar a segurança da Autoridade proposta. Na Tabela 2 estão relacionadas estas medidas.

Tabela 2 - Contramedida

	Contramedida
1	Utilizar espelhamento de discos
2	Testar as chaves ao gera-las para assinar documento
3	Atualizar os documentos cifrados com a chave antiga para chave nova
4	Documentos e diretórios terão identificador único para melhor indexação, restringindo o acesso aos mesmos.
5	Armazenamento da chave privada que só pode ser restaurada através de cerimonial.
6	Deve ter três entidades (funcionários) que compartilham a chave privada do BD na sala
7	Deve-se criptografar a chave logo após sua criação e transferi-la para o *token*.
8	Bloquear o uso da chave ao emitir a lista de certificados revogados
9	AC ligada a estabilizadores e *no-breaks* para garantir que ela não pare de funcionar com a queda de energia

3. CONCLUSÕES E TRABALHOS FUTUROS

O trabalho documentou os possíveis passos para implementação de um ambiente seguro para uso de Certificados Digitais e uma infraestrutura segura para documentos digitais em ambientes educacionais. Para isso se verificou que a estrutura física deve ser muito bem elaborada a fim de manter a AC em condições ideais de uso. Também se abordou a importância da criptografia das chaves.

Foi mostrado que a estrutura estabelecida garante a segurança do sistema como um todo através das seguintes característica:

- A disponibilidade foi garantida com o acesso ao servidor de arquivos;
- A autenticação foi garantida com o uso do certificado para definir o usuário;
- A autorização está configurada através do controle de acesso;
- A privacidade se configura através da criptografia dos arquivos com as chaves públicas;
- A integridade foi garantida com as informações salvas em diretórios que só podem ser acessados pelas pessoas permitidas;
- O não-repúdio se comprova com a chave privada, pois só o usuário poderá usar a chave privada definida para ele.

Uma desvantagem da implantação desse sistema é que se exige uma mudança de processo na elaboração de documentos, que talvez possa encontrar resistência de alguns funcionários. Também seria necessário contratar pessoal especializado.

O trabalho futuro seria a implantação dessa infraestrutura documentada. Análise das normas atualizadas e manuais apresentados. Divisão das normas por custos baseado na análise de risco.

Por fim, a infraestrutura apresentada no trabalho permite que qualquer órgão público entenda melhor o funcionamento do Certificado Digital e estude a possibilidade de implantação um ambiente para trabalhar com arquivos eletrônicos seguros.

Como trabalhos futuros sugere-se uma Análise de Riscos mais detalhada e a elaboração de testes e manuais de treinamento para todos os envolvidos na implantação.

4. REFERÊNCIAS

[1] O que é GED. Disponível em: <http://www.ged.net.br/definicoes-ged.html>. Acesso em: 10 de Dezembro 2013

[2] Beneficios GED. Disponível em: <http://www.ged.net.br/beneficios-ged.html>. Acesso em: 10 de Dezembro 2013

[3] Silva, Luiz Gustavo Cordeiro et al. Certificação Digital - Conceitos e aplicações. Rio de Janeiro: Editora Ciência Moderna Ltda., 2011.

[4] Machado, Robson Carvalho. Certificação Digital ICP Brasil: os caminhos do documento eletrônico. Niteroi, RJ: Impetus, 2010.

[5] Shokranian, Salahoddin. Criptografia para Iniciantes 2ºEdição. Rio de Janeiro: Editora Ciência Moderna Ltda., 2012.

[6] What is XML?. Disponível em: <http://www.w3schools.com/xml/xml_whatis.asp> Acesso em: 26 de Novembro 2013

[7]ASSIS, Pablo. O que é TAG? Disponível em: <http://www.tecmundo.com.br/navegador/2051-o-que-e-tag-.htm> Acesso em: 27 de Novembro 2013

[8] ICPEdu. Disponível em: <http://www.rnp.br/servicos/icpedu.html> Acesso em: 04 de dezembro 2013

[9] Como aderir a ICPEdu. Disponível em: <http://portal.rnp.br/web/servicos/como-aderir-a-icpedu> Acesso em: 04 de Dezembro 2013

[10] Boletim Digital 256. Disponível em: <http://www.iti.gov.br/noticias/boletim-digital/3955-boletim-digital-256>. Acesso em: 10 de Dezembro 2013

[11] REQUISITOS Mínimos para a Política de Certificados e Boas Práticas de Certificação da ICPEDU, 2011.

[12]EJBCA. Disponível em: <http://www.ejbca.org>. Acesso em: 11 de Dezembro 2013

[13] Instituto Nacional de Tecnologia da Informação. Disponível em: <http://www.iti.gov.br> Acesso em: 25 de novembro 2013

[14] What XML is used for? Disponível em: <http://www.w3schools.com/xml/xml_usedfor.asp> Acesso em: 26 de Novembro 2013

[15] PEREIRA, Ana Paula. O que XML? Disponível em: <http://www.tecmundo.com.br/programacao/1762-o-que-e-xml-.htm> Acesso em: 27 de Novembro 2013