

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA
COMPUTAÇÃO**

Maria Eloisa Mignoni

**Políticas e Declaração de Práticas de Certificação
Digital para UFSC**

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.

Orientador

`custodio@inf.ufsc.br`

Florianópolis, Junho de 2002

Políticas e Declaração de Práticas de Certificação Digital Para UFSC

Maria Eloisa Mignoni

Esta Dissertação foi julgada adequada para a obtenção do título de mestre em Ciência da Computação, área de concentração em Sistemas de Computação e aprovada em sua forma final pela Programa de Pós-Graduação em Ciência da Computação.



Pro[^]Fernando Ostuni Gauthier, Dr.

Coordenador do Curso

Gauthier@infufsc.br

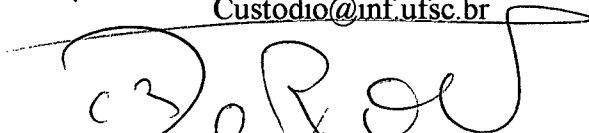
Banca Examinadora



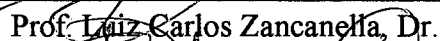
Prof. Ricardo Felipe Custódio, Dr.

Orientador

Custodio@inf.ufsc.br



Prof. Carlos Roberto De Rolt, Dr.



Prof. Luiz Carlos Zancanella, Dr.



Prof. Gilson Alberto Rosa Lima, Dr.

*''Pensar é o trabalho mais pesado que há, é talvez a razão
para tão poucos se dedicarem a isso. ''*
Henry Ford

Aos meus pais, David José Mignoni e Elina Lira Mignoni,
por acreditarem em mim e apoiarem-me
incondicionalmente. Aos meus irmãos, pela paciência e
compreensão. A todos os que se interessam pelo assunto.

Agradecimentos

A Deus primeiramente por todas as oportunidades que tem me dado de estudar e continuar a aprender.

As Faculdades Integradas Cândido Rondon - UNIRONDON, nas pessoas dos seus dirigentes, que sem o empenho dos quais, não seria possível a realização do convênio UFSC/UNIRONDON, viabilizando a realização deste mestrado.

Ao Prof. Ricardo Filipe Custódio, meu orientador e idealizador do tema, que com toda a sua sabedoria e capacidade sempre apoiou-me e incentivou-me a continuar este trabalho.

Ao Cristiano Maciel e a Patrícia C. de Souza, pelo apoio e incentivo.

Ao Luciano Ignaczak pelas contribuições fornecidas para a elaboração desta dissertação.

Ao Andre L. Lanzarine, a Ana Karina e a Anelise pela ajuda com o ambiente Latex.

A todos os meus amigos e colegas, pelo apoio e o incentivo.

A todos que acompanharam e incentivaram-me nesta caminhada, que tantas vezes fez-me ausentar.

A todos, muito obrigado!

Sumário

Lista de Figuras	xiii
Lista de Tabelas	xiv
Lista de Siglas	xviii
Resumo	xx
Abstract	xxi
1 Introdução	1
LI Objetivos.....	3
LLI Objetivo Geral.....	3
1.1.2 Objetivos Específicos.....	3
1.2 Motivação.....	3
1.3 Metodologia e Ferramentas.....	4
1.4 Conteúdo do Documento.....	5
2 Fundamentos de Criptografia	6
2.1 Introdução.....	6
2.2 Criptografia.....	7
2.3 Criptografia Simétrica.....	7
2.4 Criptografia Assimétrica.....	8
2.4.1 RSA.....	9
2.5 Função Resumo.....	9

2.6	Autenticação	10
2.7	Assinatura Digital.....	12
2.7.1	O RSA aplicado a Assinatura Digital	13
2.7.2	DSA	13
2.8	Padrões de Criptografia de Chave Pública.....	14
2.8.1	PKCS #7.....	14
2.8.2	PKCS #10	15
2.9	Conclusão.....	15
3	Infra-estrutura de Chaves Públicas	16
3.1	Introdução.....	16
3.2	Certificados Digitais	17
3.2.1	Extensões.....	19
3.3	Autoridade Certificadora.....	20
3.4	Autoridade de Registro.....	21
3.5	Diretório Público.....	22
3.5.1	Serviço de diretório X.500	22
3.5.2	LDAP.....	23
3.6	Modelos de Confiança	24
3.6.1	Modelo Isolado.....	24
3.6.2	Certificação Cruzada.....	24
3.6.3	Modelo em Floresta	26
3.6.4	Modelo Internet.....	29
3.7	Caminhos de Certificação.....	30
3.7.1	Determinação.....	30
3.7.2	Validação.....	31
3.8	Conclusão.....	32
4	Política de Certificados	33
4.1	Introdução.....	33

4.2	Políticas de Certificação	33
4.2.1	Objetivos das Políticas de Certificados.....	35
4.2.2	Qualificações da Política de Certificação.....	35
4.3	Extensões.....	36
4.3.1	Extensões de Políticas de Certificados.....	36
4.3.2	Extensão de Mapeamento de Política	36
4.3.3	Extensão de Restrição de Política.....	36
4.4	Qualificadores de Políticas.....	37
4.5	Aplicações de Políticas de Certificação.....	37
4.6	Declaração de Práticas de Certificação.....	38
4.7	Conclusão.....	38
5	Comparação entre DPCs	40
5.1	Introdução.....	40
5.2	Informações sobre a DPC.....	42
5.3	Extensões e Nomeação de Certificados.....	44
5.4	Infraestrutura de Certificação.....	45
5.5	Chaves Públicas e Privadas.....	48
5.6	Hierarquia de ICP.....	50
5.7	Base de Operações de Certificados para ACs.....	52
5.8	Responsabilidades, Obrigações e Garantias	55
5.9	Auditoria.....	59
5.10	Segurança.....	60
5.11	Funcionários	62
5.12	Detentores de Partes Secretas.....	64
5.13	Solicitação de Certificados.....	64
5.14	Validação de Solicitação de Certificados.....	65
5.15	Emissão de Certificados.....	66
5.16	Aceitação de Certificados por Assinantes.....	69
5.17	Uso de Certificados.....	70

5.18	Suspensão e Revogação de Certificados	71
5.19	Vencimento do Certificado.....	73
5.20	Disposições Gerais.....	73
5.20.1	Resolução de Controvérsias, Escolha do foro e Pressupostos ...	76
5.20.2	Emendas da DPC.....	78
5.21	conclusão.....	79
6	Estrutura da ICP da UFSC	80
6.1	Introdução.....	80
6.2	ICP da UFSC.....	80
6.3	Autoridade Certificadora Raiz (UFSC - AC).....	81
6.4	Autoridade Certificadora - AC.....	81
6.5	Autoridade de Registro - AR.....	82
6.6	Repositório.....	82
6.7	Autoridade de Aviso - AA	82
6.8	Autoridade de Certificação de Chave Privada	82
6.9	Autoridade de Datação - PDDE.....	83
6.10	Estrutura da Certificadora UFSC.....	83
6.11	Conclusão.....	84
7	Política de Certificação da UFSC	85
7.1	Introdução.....	85
7.2	Infra-estrutura de Certificação	86
7.2.1	Serviços de Certificação.....	86
7.2.2	Aplicabilidade.....	86
7.2.3	Administração dos SCP	86
7.2.4	87
7.2.5	Classes de Certificados.....	87
7.2.6	Confirmação das Informações da Identidade do Assinante	88
7.2.7	Extensões.....	88

7.2.8	Acordos de Certificação Cruzada.....	89
7.2.9	Hierarquia de ICP	90
7.3	Obrigações, Responsabilidades e Garantias	91
7.3.1	Obrigações.....	91
7.3.2	Responsabilidades.....	93
7.3.3	Garantias Limitadas	94
7.3.4	Indenização pelo Assinante.....	94
7.3.5	Indenização pela AC.....	95
7.3.6	Política de Reembolso.....	95
7.3.7	Limitações de Perdas e Danos.....	95
7.3.8	Atividades Perigosas.....	96
7.3.9	Direitos de Propriedade Intelectual.....	96
7.4	Controles Técnicos de Segurança.....	96
7.4.1	Geração e Proteção das Chaves de Assinantes.....	97
7.4.2	Auditoria.....	97
7.4.3	Programação de Retenção de Registros de Conformidade.....	97
7.4.4	Planejamento de Contingência e Recuperação de Desastre	98
7.4.5	Gerenciamento e Prática de Pessoal.....	98
7.4.6	Detentores de Partes Secretas	99
7.4.7	Instalações da AC.....	100
7.5	Ciclo de Vida dos Certificados.....	100
7.5.1	Solicitação de Certificados.....	100
7.5.2	Validação de certificados.....	101
7.5.3	Emissão de Certificados.....	102
7.5.4	Aceitação de Certificados	103
7.5.5	Uso de Certificados.....	103
7.5.6	Suspensão / Revogação de Certificados.....	104
7.5.7	Vencimento do Certificado.....	105
7.6	Definição de Termos	105
7.7	Conclusão.....	106

8	Declaração de Práticas de Certificação - DPC para a UFSC	107
8.1	Introdução.....	107
8.2	Disposições Gerais.....	108
8.2.1	Direitos.....	108
8.2.2	Publicações.....	108
8.2.3	Incorporação aos Certificados.....	109
8.2.4	Tabela de Acrônimos e Abreviações.....	109
8.2.5	contato.....	109
8.2.6	Treinamento, Assistência e Instruções.....	109
8.2.7	Avisos.....	109
8.2.8	Conflito de Cláusulas.....	110
8.2.9	Interpretação e Tradução.....	110
8.2.10	Direitos sobre as Emendas.....	110
8.2.11	Aprovação das Emendas.....	110
8.2.12	Taxas.....	111
8.2.13	Força Maior.....	111
8.2.14	Leis aplicáveis.....	111
8.2.15	Resolução de Controvérsias	111
8.2.16	Resolução formal de Controvérsia.....	111
8.3	Suporte a Operação de Certificação.....	112
8.3.1	Serviços Oferecidos pela AC-raiz.....	112
8.3.2	Solicitação de AC.....	112
8.3.3	Pré-Requisitos para Aprovação de AC.....	112
8.3.4	Aprovação para Inicia as Atividades de AC.....	112
8.3.5	Encerramento ou Cessão das Operações de AC.....	113
8.3.6	Serviços utilizados pela AC	113
8.4	Infi-a-estrutura de Certificação	114
8.4.1	Classes de Certificados.....	114
8.4.2	Confirmação das Informações da Identidade do Assinante	116
8.4.3	Informações confidenciais ^.....	116

8.4.4	Hierarquia de ICP	116
8.5	Exigências e Controles Técnicos de Segurança.....	118
8.5.1	Detentores de Partes Secretas	119
8.5.2	Instalações da AC.....	120
8.5.3	Proteção de/fári/ware.....	120
8.5.4	Escolha de Métodos Criptográficos e Assinatura Digital.....	120
8.6	Ciclo de Vida dos Certificados.....	120
8.6.1	Solicitação de Certificados.....	120
8.6.2	Validação de certificados.....	122
8.6.3	Emissão de Certificados.....	123
8.6.4	Aceitação de Certificados	124
8.6.5	Uso de Certificados.....	125
8.6.6	Suspensão / Revogação de Certificados.....	126
8.6.7	Vencimento do Certificado.....	127
8.7	Conclusão.....	128
9	Considerações Finais	129
9.1	Proposta de Trabalhos Futuros.....	131
	Referências Bibliográficas	133
	A Proposta de Ferramenta para Auxiliar no Desenvolvimento de PC e DPC	135
A.1	Introdução.....	135
A. 1.1	Objetivo.....	135
A. 1.2	Justificativa.....	135
A. 1.3	Desenvolvimento da ferramenta.....	136
A. 1.4	Vantagens.....	137
A. 1.5	Desvantagens.....	137
A. 1.6	Recursos Físicos e Lógicos Necessários.....	138

Lista de Figuras

2.1	Criptografia utilizando chaves simétricas.....	8
2.2	Criptografia utilizando chaves assimétricas.....	9
2.3	Processo de assinatura digital de dados.....	12
2.4	Assinatura Digital com RSA.....	13
3.1	Estrutura simplificada de um certificado digital	18
3.2	Organização de uma Hierarquia Isolada.....	25
3.3	Certificação Cruzada Unilateral.....	25
3.4	Certificação Cruzada Mútua	26
3.5	Modelo em Floresta.....	27
3.6	Modelo em Malha.....	28
3.7	Modelo com Ponto Central.....	29
6.1	Modelo da ICP da UFSC.....	81
6.2	Estrutura de ACs da UFSC.....	83
7.1	Ciclo de Vida de um Certificado.....	100

Lista de Tabelas

5.1	Principais Entidades de Certificação.....	41
5.2	Estrutura da DPC.....	42
5.3	Reprodução e Distribuição.....	43
5.4	Incorporação por Referência.....	43
5.5	Indicadores da DPC.....	43
5.6	Assistência, Instruções e Treinamento.....	44
5.7	Extensões e Nomeação.....	44
5.8	Infra-Estrutura de Confiança.....	45
5.9	Administração do Domínio de SCP.....	45
5.10	Confirmação da Identidade do Assinante.....	46
5.11	Informações Confidenciais.....	46
5.12	Informações não Confidenciais.....	46
5.13	Classes de Certificados.....	47
5.14	Propriedades das Classes de Certificados.....	47
5.15	Certificação Cruzada.....	47
5.16	Cadeias de Certificados e Tipos de AEs	48
5.17	Geração de Chaves.....	48
5.18	Geração das Chaves de AE ou AC.....	49
5.19	Proteção da Chave Privada da AE ou AC.....	49
5.20	Proteção da Chave Privada do Assinante.....	49
5.21	Inserção, Ativação, Desativação e Destruição da Chave Privada.....	50
5.22	Chave Pública.....	50

5.23	AC-Raiz - Autoridade Certificadora Raiz.....	50
5.24	AC - Autoridade Certificadora.....	51
5.25	AR - Autoridade de Registro.....	51
5.26	AN - Autoridade de Nomeação.....	51
5.27	Repositórios.....	52
5.28	LCR - Lista de Certificados Revogados.....	52
5.29	Publicações.....	••• 52
5.30	Tabeliães	53
5.31	Pré-Requisito para Aprovação de AC.....	53
5.32	Solicitação de AC.....	53
5.33	Aprovação para iniciar as atividades de AC	54
5.34	Disponibilidade dos Certificados de AE ou AC	54
5.35	Encerramento ou Cessão das Operações da AE ou AC.....	54
5.36	Reemissão dos Certificados por 1 AE Sucessora.....	54
5.37	Confiabilidade.....	55
5.38	Responsabilidades Financeiras.....	55
5.39	Avisos, Limitações de Responsabilidades e Isenções de Garantias.....	56
5.40	Política de Reembolso	56
5.41	Garantias Limitadas e Outras Obrigações de AEs e ACs.....	56
5.42	Obrigações de ARs.....	57
5.43	Obrigações dos Usuários e Parceiros de Confiança.....	57
5.44	Isenção de Responsabilidade e Limitações sobre as Obrigações das AEs e ACs.....	57
5.45	Limitações de Perdas e Danos	58
5.46	Responsabilidades de assinantes.....	58
5.47	Atividades Perigosas.....	58
5.48	Direitos de Propriedade Intelectual.....	59
5.49	Auditoria.....	59
5.50	Programação de Retenção de Registro.....	60
5.51	Registro de Conformidade.....	60

5.52	Planejamento de Contingência e Recuperação de Desastre	60
5.53	Serviços de Segurança	61
5.54	Plano de Proteção.....	61
5.55	Instalações.....	61
5.56	Proteção de <i>Hardware</i>	62
5.57	Escolha de Métodos Criptográficos.....	62
5.58	Gerenciamento e Prática Pessoal.....	62
5.59	Cargo de Confiança.....	63
5.60	Investigação e Conformidade.....	63
5.61	Afastamento de Pessoas que Ocupam Cargos de Confiança.....	63
5.62	Funcionários Com Cargos de Confiança.....	64
5.63	Detentores de Partes Secretas - Compartilhamento de Segredos.....	64
5.64	Procedimentos para Solicitação de Certificados.....	65
5.65	Informações e Comunicações da Solicitação de Certificados	65
5.66	Exigência para a validação de solicitação de certificado.....	65
5.67	Ítems a serem Confirmados.....	66
5.68	Aprovação de solicitação de certificados de classe 1 ou 3.....	66
5.69	Rejeição de solicitação de certificados.....	66
5.70	Certificados Normais e Provisórios.....	67
5.71	Consentimento do Assinante para Emissão do Certificado.....	67
5.72	Recusa quanto à emissão de um certificado	67
5.73	Representações da AE ou AC Mediante a Emissão do Certificado.....	68
5.74	Tempo para Emissão de Certificados.....	68
5.75	Períodos de Validade dos Certificados.....	68
5.76	Aceitação de Certificados.....	69
5.77	Representações dos Assinantes Mediante Aceitação.....	69
5.78	Indenização por Parte do Assinante.....	69
5.79	Publicações.....	70
5.80	Verificação de Assinaturas Digitais.....	70
5.81	Escritas e Assinaturas.....	71

5.82	Motivos Gerais para Suspensão ou Revogação	71
5.83	Suspensão ou Revogação de um Certificado de AE	71
5.84	Cancelamento da Suspensão de um Certificado de AE.....	72
5.85	Aviso e Confirmação Mediante Suspensão ou Revogação	72
5.86	Efeitos da Suspensão ou Revogação sobre Certificados e Obrigações Sub- jacentes	72
5.87	Proteção das Chaves Privadas Mediante Solicitação ou Revogação	73
5.88	Aviso antes do Vencimento	73
5.89	Renovação e Reinscrição do Assinante	73
5.90	Interpretação e Tradução	74
5.91	Conflito de Cláusulas	74
5.92	Avisos . . ^	75
5.93	Conformidade com Normas e Leis de Exportação	75
5.94	Lei Aplicável	75
5.95	Taxas	76
5.96	Força Maior	76
5.97	Aprovação de <i>Software e Hardware</i>	76
5.98	Notificação de Controvérsia entre as Partes	77
5.99	Resolução Formal de Controvérsias	77
5.100	Sucessores e Cessionários	77
5.101	Fusão	78
5.102	Disposições Gerais Sobre Emendas	78
5.103	Tipos de Emendas de DPCs	78
5.104	Aprovação das Emendas	79
5.105	Validade após o Término da DPC	79
7.1	Identificadores de Objetos	89
8.1	Informações Obrigatórias.....	121

Lista de Siglas

AA	Autoridade de Aviso
AC	Autoridade de Certificação
AD	Autoridade de Datação
AES	Advanced Encryption Standard
AR	Autoridade de Registro
CG	Comitê Gestor
DPC	Declaração de Práticas de Certificação
DRO	Declaração de Regras Operacionais
DSA	Digital Signature Algorithm
HW	Hardware
ICP	Infra-estrutura de Chaves Públicas
IDDE	Infra-estrutura de Datação de Documentos Eletrônicos
IETF	Internet Engineering Task Force
10	Identificador de Objeto
LabSEC	Laboratório de Segurança em Computação
LCR	Lista de Certificados Revogados
LDAP	Lightweight Directory Access protocol
MD 5	Algoritmo que calcula o resumo de um arquivo digital qualquer
NIST	National Institute of Standards and Technology
NRD	Nomes Relativos Distintos

PC	Política de Certificados
PKCS	Public Key Cryptography Standards
RFC	Request for Comments
SCP	Serviços de Certificação Pública
SW	Software
SHA1	Algoritmo que calcula o resumo de um arquivo digital qualquer
K	Chave Simétrica para cifrar e decifrar
K_{RB}	Chave privada de Beto
K_{UB}	Chave pública de Beto
RSA	Padrão de cifragem assimétrica

Resumo

O presente trabalho sobre Política de Certificados e Declaração de Práticas de Certificação, para a Infra-estrutura de Chaves Públicas da Universidade Federal de Santa Catarina - UFSC. Os modelos elaborados são simples, menos dispendioso, mais direto e de fácil entendimento para os usuários e também poderá servir de exemplo para outras Autoridades Certificadoras, que desejam estabelecer documentos deste nível.

A Política de Certificação e a Declaração de Práticas de Certificação, propostas nesta dissertação, foram desenvolvidas a partir de estudos realizados da RFC 2527, de diversas Declarações de Práticas de Certificação de Autoridades Certificadoras, da Infra-estrutura de Chaves Públicas do Brasil e das necessidades encontradas da Infra-estrutura de Chaves Públicas na Universidade Federal de Santa Catarina - UFSC, que além dos tradicionais serviços comumente disponibilizados pelas Autoridades Certificadoras, dispõe de outros serviços, tais como: Autoridade de Aviso, Autoridade Certificadora de Chave Privada e Autoridade de Datação. A implementação de uma ferramenta para auxiliar na elaboração de Políticas de Certificados e de Declarações de Práticas de Certificação é proposta em trabalhos futuros.

Palavras Chaves: criptografia. Infra-estrutura de Chaves Públicas, certificação digital, Política de Certificados e Declaração de Práticas de Certificação.

Abstract

This research presents the Certificate Policies and the Certification Practice Statements for the Public Keys Infrastructure of Federal University of Santa Catarina - UFSC. The elaborated models are simple, less expensive, more direct and easily understood for the users. They also may be used as example for others Certified Authorities that want to establish their certificate policies and practices.

The Certificate Policies and the Certification Practices Statements proposed in this dissertation were developed through studies carried out starting from RFC 2527, from many Certification Practices Statements of private and governmental Certification Authorities and particular needs of Federal University of Santa Catarina. This university besides of its traditional services has others services such as: Notice Authority, Public Key Certification Authority and Time Stamping Authority. The implementation of a tool to help in the elaboration of Certification Policies and Certification Practices Statements in here is proposed for further investigations.

Key Words: cryptography, public keys infrastructure, digital certification, certificate policies and certification practices statements.

Capítulo 1

Introdução

No final do segundo milênio e início do atual, a extraordinária disseminação e popularização da Internet e o aparecimento das chamadas “lojas virtuais” para comércio eletrônico, e dos “home-bankings”, possibilitando transações bancárias on-line, tomaram-se o ponto central de um processo revolucionário, que mudou o comércio e as finanças de forma intensa. Todavia as facilidades de acesso oferecidas pela Internet são alvos fáceis e volúveis, aguçando a má índole de pessoas mal intencionadas, o que torna necessário a utilização de mecanismos de segurança na Internet.

A constante e crescente preocupação com a evolução da segurança nas transações *on-line*, e os meios utilizados para quebrar os tradicionais mecanismos de segurança e também as constantes tentativas de quebrar-se os novos mecanismos de defesa, tomou-se necessário o desenvolvimento de novas tecnologias que atendessem os requisitos de segurança, que os tradicionais já não suportam.

Uma das tecnologias de maior êxito para tratar de forma adequada os problemas de segurança nas redes de computadores é a criptografia. A descoberta da criptografia de chaves públicas em 1976 por *Diffie e Hellman*¹ [STA 99] permitiu, entre outros benefícios, o estabelecimento da assinatura digital de documentos eletrônicos, talvez uma das maiores revoluções no tratamento eletrônico de documentos, depois do surgimento do computador [SCH 00]. Contudo, para a utilização da criptografia de chaves públicas

¹Existe evidência que o Britânicos já conheciam esta técnica em meados da década de sessenta

são necessários mecanismos confiáveis e robustos para a publicação e divulgação das chaves públicas. A solução vislumbrada para isso, proposta por *Loren Kohnfelder* em 1978 [IET 99, RIV 02] foi o certificado digital ou identidade digital, que consiste de um arquivo contendo informações sobre o sujeito associado a chave pública, além é claro da própria chave pública. Para garantir a autenticidade e integridade deste arquivo, o certificado digital deve ser assinado de forma digital por uma entidade confiável denominada Autoridade de Certificação - AC. Para a implantação de uma AC são necessários além de programas de computador para a emissão dos certificados digitais, uma série de procedimentos administrativos e outros de caráter funcional criando-se desta forma uma infra-estrutura denominada Infra-estrutura de Chaves Públicas ou simplesmente ICP.

Para que todo esse processo de segurança oferecido pelos certificados digitais, obtenham o sucesso esperado são precisos documentos que estabeleçam as regras e procedimentos do correto funcionamento da ICP. Estes documentos são normalmente conhecidos como Política de Certificados - PC e Declaração de Práticas de Certificação - DPC, São estes documentos, que determinam todas as práticas e os procedimentos implementados desde a implantação da AC até a finalização da mesma, do início do processo de certificação até o seu encerramento.

O processo de certificação é executado pela AC de acordo com a PC e DPC. A PC e a DPC são geradas pela AC e a ICP.

Com a implantação da ICP da UFSC, tomou-se necessário a elaboração da PC e da DPC para regulamentar a sua atuação. Esta necessidade, levou-nos a realizar vários estudos de como elaborar estes documentos. Os estudos realizados envolveram a RFC 2527, diversas DPCs de autoridades certificadoras conhecidas mundialmente e da ICP - Brasil, resultando em uma comparação de alguns desses documentos. A comparação realizada abrangeu três das ACs pesquisadas, a *VeriSign*, *Entrust* e a ICP-Brasil. A seleção destas DPCs deu-se devido a fatores, tais como: a *VeriSign* e a *Entrust.Net* são as duas mais conhecidas e importantes autoridades certificadoras do mundo, no âmbito da segurança mundial. A junção destas duas DPCs com a ICP-Brasil congregam características suficientes para realizar a comparação. As DPCs da *VeriSign* e a *Entrust.Net* são documentos contínuos, permitindo que o usuário entenda facilmente o

que o documentos está propondo. A *Baltimore*, *Thawte*, *ABA - ECom* e outras não citadas aqui, possuem suas DPCs divididas em vários segmentos, dificultando a compreensão global do documentos. Apesar da divisão de segmentos da DPC da *Baltimore*, a ICP - Brasil segue este mesmo estilo. Ademais, a *CertiSign* e a *GlobalSign* são afiliadas da *VeriSign*, tomando a abordagem destas redundante, pois as normalizações são iguais.

1.1 Objetivos

1.1.1 Objetivo Geral

Elaborar Políticas de Certificados e Declaração de Práticas de Certificação adequados a Universidade Federal de Santa Catarina.

1.1.2 Objetivos Específicos

- Fazer uma revisão sobre criptografia e ICP;
- Levantar os padrões de PC e DPC existentes;
- Estudar as PC e as DPCs das principais entidades certificadoras nacionais e internacionais;
- Fazer uma comparação das DPCs estudadas;
- Estudar o modelo de Certificação Digital da UFSC;
- Propor uma Política de Certificados para a UFSC;
- Propor uma DPC para a UFSC;

1.2 Motivação

o crescimento acelerado da Internet, fomentando quase todos os tipos de serviços via *on-line*, aguçando as pessoas, pela praticidade de realizar suas compras.

pagamentos, etc., sem sair de casa. Porém, todas estas facilidades provocam um certo temor quanto a segurança das informações prestadas e perda de privacidade. As facilidades geradas com o uso da Internet, deixam as informações vulneráveis às pessoas de má índole, forçando os usuários da Internet, recorrerem a cada dia, a novas tecnologias de segurança, a fim de garantirem a e integridade de suas informações. Neste contexto o uso de Certificados Digitais possibilita a autenticação da informação através da assinatura digital. Como exemplo de benefícios para a sociedade brasileira do uso do certificado digital pode-se citar a emissão de documentos pelo governo, como certidões negativas, certidões criminais, certidões de nascimento, etc. O Governo Brasileiro, através do seu projeto "e-gov"[^] vem esforçando-se em garantir a inclusão digital do cidadão brasileiro, principalmente aqueles das classes C, D e E. E a possibilidade prática e real do uso dos certificados digitais passa necessariamente por estabelecer normas e procedimentos para a implantação da ICP em nível governamental.

No entanto, para que todo este processo ocorra dentro do esperado é preciso normas e regras, para isto é preciso elaborar documentos de fácil entendimento pelos usuário. A PC e a DPC estabelecem as regras e normas para tais serviços.

1.3 Metodologia e Ferramentas

Para a realização desta dissertação de mestrado, foram realizadas amplas pesquisas bibliográficas, baseada em livros, em bibliotecas digitais, artigos científicos, revistas e dissertações de mestrado e principalmente estudando as políticas de certificação e declaração práticas de certificação de entidades de certificação existentes[^]. Após o estudo das políticas de certificados e declaração de práticas de certificação de entidades, realizou-se a comparação entre duas DPCs escolhidas (VeriSign e Entrust.NET e a ICP-Brasil).

Para a realização das pesquisas bibliográficas foram pesquisadas as RFCs e os artigos existentes sobre o assunto em revistas especializadas em segurança de redes

[^]Veja <http://www.govmoeletronico.gov.br>

³A maioria delas americanas, pois é lá que a ICP está mais disseminado

e em sítio de segurança de redes.

Com o estudo realizado das PCs e DPCs de entidades e da RFC 2527 e da comparação elaborada de 3 (três) documentos foi possível formar uma base de conhecimento, agregando valores na elaboração do modelo de PC e da DPC para UFSC.

Para a elaboração desta dissertação usou-se o ambiente LATEX, sendo o editor de texto WinEdt 5, MikTeX. Para as figuras usou-se o Corel Draw 9.0.

A conversão do documento LATEX para os formatos ps e pdf foi feita através das ferramentas dvips e ps2pdf. Para visualização e impressão dos documentos foram utilizados Acrobat Reader 4.0 e GSview 4.2.

1.4 Conteúdo do Documento

Este documento está estruturado em nove capítulos. O capítulo 1 apresenta a introdução, os objetivos, a motivação, a metodologia e ferramentas e demonstra o conteúdo apresentado na dissertação. O Capítulo 2 apresenta os princípios e as principais técnicas de criptografia e os principais padrões de criptografia, necessários para o entendimento da necessidade do assunto tratado no capítulo 3. O capítulo 3 apresenta a estrutura existente para viabilizar o processo de certificação digital, envolvendo hierarquia de certificação, caminhos de certificação, autoridades, diretórios, o qual torna indispensável o uso da DPC para garantir a segurança do processo envolvendo todos estes itens. O capítulo 4 apresenta o que é uma política de certificação, qual a sua finalidade. O capítulo 5 apresenta a comparação entre duas DPCs e a ICP-Brasil, mostrando o que elas possuem em comum e individualmente. O capítulo 6 apresenta a ICP da UFSC e a estrutura da AC da UFSC. O capítulo 7 descreve a política propostas para AC da UFSC. O capítulo 8 apresenta um modelo de declaração de práticas de certificação para a UFSC e o capítulo 9 apresenta as considerações finais da dissertação e as sugestões de trabalhos futuros.

Capítulo 2

Fundamentos de Criptografia

2.1 Introdução

Este capítulo aborda os fundamentos e as técnicas de criptografia e os serviços por ela oferecidos. A criptografia é um algoritmo que visa "esconder/ocultar" de forma embaralhada as informações sigilosas, tomando-as incompreensíveis à pessoas não autorizadas a lê-las, somente as autorizadas conseguem decifrá-las. A segurança em informática consiste na certeza de que as informações em uso não serão acessadas. O conhecimento destes fundamentos são importantes para entender a Infra-estrutura de Chaves Públicas e a certificação digital, descritos no capítulo 3. Para obter-se criptografia confiável há padrões que devem ser seguidos.

Este capítulo está dividido da seguinte forma: na seção 2.2 conceitua-se a criptografia e seus serviços; a seção 2.3 descreve a criptografia simétrica; a seção 2.4 apresenta a criptografia assimétrica e suas vantagens em relação a criptografia simétrica; a seção 2.4.1 apresenta o algoritmo RSA; a seção 2.5 descreve as características de uma função resumo; a seção 2.6 demonstra os tipos de autenticações possíveis; a seção 2.7 conceitua assinatura digital e por fim a seção 2.8 aborda os padrões de criptografia de chave pública.

2.2 Criptografia

A criptografia é uma ciência que usa a matemática (em forma de algoritmos) para ocultar dados (embaralhar informações) [STI 95]. A palavra criptografia é originária do grego, "Kriptos = escondido, oculto e grifo = escrita". A criptografia consiste na arte de escrever em cifras ou em códigos não decifráveis a olhos nus, chamados de cifragem. Para decifrar a mensagem original, o destinatário, aplica o processo inverso, a decifragem, que toma a mensagem legível novamente [STA 98].'

O nível de segurança das informações estabelecidas por criptografia, depende do tamanho da chave, quanto mais bits uma chave possuir, mais difícil será de ser descoberta.

A criptografia provê recursos para garantir os seguintes serviços:

Autenticação Garante a origem da informação, permitindo a comprovação da origem;

Integridade Assegura a veracidade e completeza da informação recebida;

Confidencialidade Garante o acesso as informações, somente pela pessoas autorizadas;

Irretratabilidade Assegura que a origem (o emissor) da mensagem, não poderá negar que foi o autor de determinada mensagem.

2.3 Criptografia Simétrica

A criptografia simétrica foi a primeira forma conhecida para cifrar/ocultar dados sigilosos.

A principal característica da criptografia simétrica é a utilização de somente uma chave para cifrar e decifrar um texto, significando que tanto o emissor como o receptor da informação cifrada devem conhecer a chave utilizada. Por este método ser muito utilizado ao longo dos anos e utilizar apenas uma chave, acarreta a necessidade de adoção de uma política de segurança para troca e guarda de chaves, a fim de evitar que intrusos raptem a chave e passem a usa-lá e também como distribuir uma chave a um novo

membro do grupo. A figura 2.1 apresenta a estrutura de como é o funcionamento do sistema de criptografia simétrica, aplicada a um texto claro, utilizando a chave do emissor. Neste caso a mensagem a ser enviada será cifrada por Alice com a sua chave, mas para que Beto consiga decifrar a mensagem cifrada, é necessária a da mesma chave utilizada por Alice para cifrá-la.

Na criptografia simétrica, o algoritmo mais conhecido e padrão por muitos anos foi o DES (Data Encryption Standard) [TER 00]. Após a definição do DES, outros algoritmos foram surgindo.

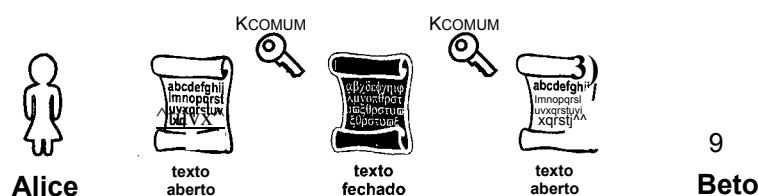


Figura 2.1: Alice de posse de um texto aberto cifra-o, utilizando um algoritmo de chave simétrica, com a chave *Kcomum* obtendo um texto cifrado. Beto de posse do texto cifrado utiliza a mesma chave *Kcomum* para decifrá-lo e lê-lo.

2.4 Criptografia Assimétrica

A criptografia assimétrica ou de chave pública baseia-se na utilização de um par de chaves distintas, conhecidas como chave privada e chave pública e cada ator (usuário) possui o seu par de chaves. A cifragem ou decifragem de uma mensagem pode ser realizada por qualquer uma das chaves, desde que uma seja usada para cifrar e a outra para decifrar a mensagem. A chave privada deve ser mantida no mais absoluto sigilo, enquanto que a chave pública deverá tornar-se pública de alguma forma [STA 98].

No ano de 1976 apresentou-se o conceito de criptografia de chave pública, por *Whitfield Diffie e Martin Hellman*, em um artigo chamado *New Directions in Cryptography na IEEE transactions on Information Theory*, este nome revolucionou os sistemas criptográficos existentes [STA 99].

A criptografia assimétrica permite a utilização de dois tipos de serviços.

A assinatura digital é criada através do uso da chave privada e sua verificação é feita utilizando a chave pública. O sigilo utiliza a chave pública do destinatário, o qual deve utilizar sua chave privada para a decifrar uma mensagem. A função de sigilo é ilustrada na figura 2.2. A assinatura digital é apresentada na seção 2.7.

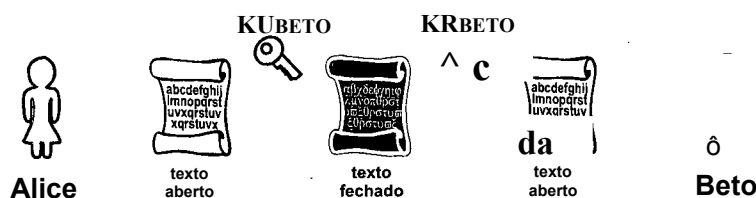


Figura 2.2: Alice cifra o texto que ela deseja enviar para Beto usando a chave K_{UBeto} do mesmo. Após o recebimento do texto cifrado Beto deverá tomá-lo legível, para isto ele utilizará sua chave privada (K_{RBeto}) para decifrá-lo.

2.4.1 RSA

O RSA foi o primeiro algoritmo assimétrico desenvolvido. Seus criadores foram Ron Rivest, Adi Shamir e Leonard Adleman em 1976, foi o primeiro algoritmo de sucesso utilizado tanto para cifrar dados como para assinatura digital, implementando os conceitos apresentados por Diffie e Helman um ano antes [STA 99]. O RSA é certamente o algoritmo mais popular. O RSA é baseado na dificuldade em fatorar dois números primos grandes [TER 00].

Os ataques ao RSA podem ocorrer por força bruta, onde o invasor tenta decifrar a chave. Para proteger-se, o tamanho da chave deverá ser acrescido e o tempo de ataque de temporização, baseado no tempo gasto para efetuar o cálculo do algoritmo, com o intuito de obter o tamanho dos fatores utilizados. O principal ataque sofrido pela RSA foi a tentativa de fatorar os números primos.

2.5 Função Resumo

A função resumo funciona como o seu próprio nome diz, um resumo e é semelhante ao dígito verificador do CPF, qualquer número do CPF que for alterado.

irá acarretar alterações no dígito [BRO 01]. A Função Resumo é uma função que recebe como entrada uma mensagem de qualquer tamanho e produz um resumo de tamanho fixo, que representa o conteúdo da mensagem. O tamanho da saída varia de acordo com o algoritmo usado. O propósito de uma função resumo é produzir uma "impressão digital" da mensagem [STA 99].

Funções Resumo são funções de caminho único, ou seja, elas só possuem um sentido, se Alice gera um resumo, e envia à Bob, ele somente poderá checar a sua integridade, através da geração de um novo resumo, sem haver um retomo de qualquer código para Alice.

Com o resultado gerado por uma Função Resumo é possível garantir a integridade de uma mensagem, pois o resumo gerado no destino por uma função resumo terá que ser igual ao resumo gerado na origem. Se houver uma alteração qualquer, a mensagem de origem foi alterada. A integridade da mensagem poderá ser garantida quando Alice enviar para Bob uma mensagem e o resumo da mesma cifrado com a sua chave privada. Bob irá decifrar o resumo com a chave pública de Alice e calcular novamente o resumo, baseado na mensagem recebida e realizando a comparação entre os dois resumos, se os dois forem iguais, significa que não houve violação de informações, e a integridade da mensagem é garantida [BRO 01].

Os algoritmos de função resumo mais utilizados no momento são o MD5, criado por Ron Rivest e FIPS PUB 180, desenvolvido pelo NIST e lançado como padrão em 1993 e em 1995 uma nova versão deste padrão tomou-se conhecida como SHA-1.

2.6 Autenticação

A autenticação provê a garantia de que as entidades envolvidas em uma transação, são quem elas dizem ser. Estas entidades podem ser pessoas ou dispositivos [FEG 99].

A autenticação poderá ser realizada considerando os seguintes fatores [IGN 02]:

Algo que você sabe A autenticação é realizada através de alguma coisa que você especifica de seu conhecimento sobre o indivíduo. Este fator conhecido poderá ser uma senha, um nome ou um número de identificação pessoal.

Algo que você tem A entidade será identificada através da posse de alguma coisa física, um objeto que possua a chave privada armazenada, tal como, um disquete ou um *smart card*.

Algo que você é A entidade utiliza alguma medida biométrica, unicamente pessoais, impossíveis de serem reproduzidas em qualquer meio para identificação. Por exemplo a impressão digital ou a íris.

Quando A data e a hora da autenticação podem ser conhecidos e verificados.

Onde você está A posição geografia do indivíduo é levada em consideração no momento em que é realizada a autenticação. A verificação deste tipo de autenticação pode ser feita utilizando, por exemplo, algo semelhante a um dispositivo de *Global Positioning System (GPS)*.

Presença de testemunha A presença de uma ou mais testemunha é necessária para a realização da autenticação. A autenticação de uma ou mais pessoas no sistema, dá ao mesmo uma segurança maior. Esta autenticação resolve o problema do comprometimento da chave privada da pessoa que vai autenticar-se perante o sistema, pois a presença da testemunha cancelará a operação.

A autenticação também poderá ser realizada, através da combinação dos fatores acima citados, podendo envolver dois ou mais. Esta forma de autenticação permite um acréscimo no nível de segurança. Por exemplo, a autenticação pode ser feita digitando uma senha, junto com a verificação da impressão digital do indivíduo ou a senha juntamente com a íris do indivíduo

2.7 Assinatura Digital

o ato de assinar um documento no papel, está efetivando a ligação entre a assinatura propriamente dita e a informação impressa no papel. Na assinatura manuscrita, existe uma ligação entre a pessoa que assina e o documento, pois no ato em que assina-se é impressa no papel uma escrita que possui dependência das biocaracterísticas da pessoa. Nos documentos eletrônicos, este efeito não ocorre, pois não há meio físico que estabeleça uma ligação entre o assinante e a assinatura.

Uma assinatura digital é um algoritmo de autenticação, que possibilita o criador de um objeto, unir ao objeto criado, um código que irá agir como uma assinatura [Gui 00]. Esta assinatura confirma que o objeto não foi alterado, desde o ato de sua assinatura e permite identificar o assinante, isto é conhecido como autenticação. Para permitir esta autenticação a assinatura usa técnicas criptográficas, que permitem a comprovação de um determinado conjunto de dados.

O processo de assinatura digital esta ilustrado na figura 2.3.

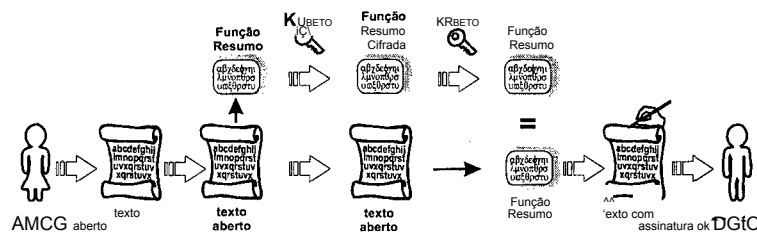


Figura 2.3: Para criar a assinatura digital de um documento, Alice executa a função resumo dele e cifra o resultado com sua chave privada. O resumo cifrado é enviado para Beto juntamente com o documento. Beto decifra o resumo com a chave pública de Alice, executa novamente a Função Resumo do documento e compara os dois resultados. Se forem iguais a assinatura é válida.

São usadas basicamente três formas para implementar a assinatura digital [STA 99]: função resumo padrões MD5 e SHA, DSS - Digital Signature Standard e o padrão RSA. A assinatura digital permite :

- verificar o autor (o assinante);
- data e hora da assinatura;

- autenticar o conteúdo original;
- passível de ser verificado por terceiros em caso de disputas judiciais.

2.7.1 O RSA aplicado a Assinatura Digital

O algoritmo RSA é usado na assinatura digital para cifrar o código gerado, a partir de uma mensagem, a qual foi aplicado alguma tipo de algoritmo para gerar uma assinatura digital, conforme ilustrado na figura 2.4. O RSA poderá também cifrar não só o código da assinatura, mas a mensagem toda inclusive a assinatura, formando apenas um bloco cifrado.

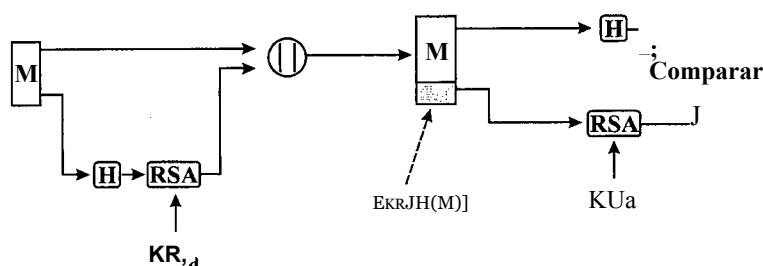


Figura 2.4: Após a aplicação da função resumo, gerando o resumo da mensagem, este é assinado com o RSA, só então é enviado ao destino.

2.7.2 DSA

O algoritmo de assinatura digital DSA - *Digital Signature Algorithm*, foi proposto em agosto de 1991, e o primeiro algoritmo assimétrico desenvolvido, pelo Instituto Nacional de Padrões e Tecnologia Norte Americano (NIST) para ser utilizado como o padrão para assinatura digital. O DSA é uma variação de outro algoritmo para assinatura digital, o ElGamal [SCH 96], e referência para o DSS (Padrão de Assinatura Digital). O DSA explora um pequeno grupo Z_p em ordem para diminuir o tamanho da assinatura [STI 02].

A fórmula matemática usada como base do DSA é diferenciada do RSA.

O DSA aplica um sistema de chave pública irreversível e a sua segurança depende da

dificuldade de cálculo do algoritmo $y = g^{modp}$.

O DSA é utilizado somente para assinatura digital, não podendo ser usado para cifragem e distribuição de chaves.

2.8 Padrões de Criptografia de Chave Pública

A Empresa *RSA Security* em cooperação com desenvolvedores definiu uma série de padrões para o uso da criptografia de chaves públicas. Eles são denominados *Public Key Cryptography Standards* - PKCS, com a finalidade de desenvolver aplicações seguras, baseadas na criptografia de chave pública. Atualmente, existem 15 padrões já definidos, que vêm sendo amplamente implementados e referenciados em experiências disponíveis pelo mundo [KIN 97].

A grande maioria das aplicações que utilizam serviços de criptografia usufruem destes padrões. Serão descritos dois destes padrões, os quais são utilizados largamente em infra-estruturas de chaves públicas.

2.8.1 PKCS #7

O padrão PKCS #7 descreve a sintaxe geral, utilizado para a transferência de dados assinados ou cifrados. Ele também permite o encapsulamento de uma mensagem, assinada ou cifrada, dentro de uma nova mensagem, com isto, uma mensagem pode ser cifrada e depois assinada [LAB 93].

O padrão é compatível com *PEM - Privacy-Enhanced Mail*, codificação utilizada na transferência de mensagens assinadas e cifradas por e-mail. Com essa compatibilidade, uma mensagem pode ser transferida através da Internet sem a necessidade de codificações adicionais [LAB 93].

A versão 1.5 do padrão PKCS #7, suporta uma variedade de chaves de gerenciamento proposto pelo PEM na RFC 1422 [LAB 93].

O padrão PKCS #7 passou por algumas adaptações, feitas pelo laboratório RSA e outros desenvolvedores, surgindo uma nova versão, a PKCS #7.1.6. Esta

nova versão não limitou-se a apenas mensagens eletrônicas, passou a ser utilizada também em transações eletrônicas seguras - SET, pagamentos com cartões de Bancos, iniciativas de assinaturas digital "W3C" [ROC 01], A versão 1.6 do PKCS #7 é uma revisão da versão 1.5 e está sendo desenvolvida para atender as especificações do SET e também entendida como o encerramento da série 1.x do padrão [KIN 97].

2.8.2 PKCS #10

O PKCS #10 é o padrão que descreve a sintaxe de uma requisições de certificados. Uma requisição é formada pela identificação do requisitante ou nome distinto e uma chave pública, juntamente com outros atributos opcionais [LAB 00], também faz parte desta requisição também um identificador do algoritmo da assinatura e a assinatura digital da informação da requisição do certificado. Todo o conjunto de dados é assinado digitalmente pela entidade que está requerendo a certificação. Requisições para certificados são enviadas para ACs, que as transformam em certificados digitais. Após criado o certificado digital, a AC o envia para o requisitante. As duas razões para incluir-se um conjunto de atributos na requisição de um certificado são:

- fornecer informações sobre a entidade requisitante a qual possibilitará a entidade requisitar a revogação do certificado;
- permitir o acréscimo de atributos no certificado X.509.

2.9 Conclusão

Para obter-se a segurança desejada e almejada pelos usuários de sistemas de criptografia existentes, é necessário que sejam conhecidos os principais tipos de criptografia e seus padrões e principalmente para que os documentos gerados sobre as normas de uso possam garantir a segurança.

Capítulo 3

Infra-estrutura de Chaves Públicas

3.1 Introdução

A infra-estrutura de chaves públicas - ICP é uma série de padrões envolvendo componentes, tais como autoridade certificadora - AC, autoridade de registro - AR, diretório público, estrutura entre múltiplas ACs, em fim é um conjunto de serviços necessários para o uso de tecnologias baseadas em chave pública, usadas em grande escala. A viabilização da comunicação e transações eletrônicas via internet em todo o seu potencial, necessitam de segurança, que possam garantir aos usuários confiar na internet. Os cinco aspectos básicos citados abaixo, são considerados fundamentais para esta confiança:

Autenticação - garante a origem da informação, permitindo a comprovação da origem;

Integridade - assegura a veracidade e completeza da informação recebida;

- garante o acesso as informações, somente pela pessoas autorizadas;

Não repúdio - garante que o emissor e nem o receptor da informação neguem a autoria ou o recebimento da informação;

Autorização - autoriza que uma determinada operação seja autorizada.

As aplicações que utilizam a ICP, conseguem assegurar estes cinco requisitos, fazendo uso de um sistema de certificados e chaves em conjunto com diversos algoritmos. O nível de segurança oferecida pela ICP, depende da infra-estrutura e do comprimento das chaves utilizadas. A natureza das aplicações abrangidas e a cobertura da ICP, varia de acordo com os tipos de AC, tomando-se o ponto mais crítico do processo de certificação. As normas para que toda a ICP possa funcionar conforme o desejado é especificada em um documento chamado DPC, descrito no capítulo 5.

Neste capítulo serão abordados os seguintes temas: a seção 3.2 faz uma introdução sobre os certificados digitais; na seção 3.3 e 3.4 são descritas as funcionalidades de uma AC e de uma AR respectivamente; a seção 3.5 caracteriza um diretório público; na seção 3.6 aborda os modelos de ICPs existentes; e por fim a seção 3.7 demonstra o funcionamento de um caminho de certificação.

3.2 Certificados Digitais

Um certificado digital ou identidade digital é um arquivo digital de computador, que como os demais documentos tradicionais de identificação, além dos dados do indivíduo ou entidade possuem também uma chave pública do assinante. Estes documentos eletrônicos são chancelados digitalmente pela entidade emissora, conhecida como Autoridade Certificadora, com o objetivo de interligar a chave pública a uma pessoa ou entidade, possuindo o mesmo valor de um documentos físico, como carteira de identidade, passaporte, cartões de créditos e utilizados da mesma forma, na identificação de indivíduos ou entidades na rede [STA 99], que ao serem apresentados servem como prova de identificação. O certificado digital serve também como um mecanismo para a divulgação da chave pública.

Na certificação digital é utilizada, como base, a tecnologia de criptografia de chave pública, onde a chave pública é armazenada no certificado e a chave privada é guardada sigilosamente pelo assinante. Qualquer mensagem ou código podem ser assinados, utilizando-se a chave privada do assinante, porém esta assinatura só será validada com a chave pública correspondente.

A AC ao emitir um certificado digital, estará garantindo que o proprietário do certificado é quem realmente diz ser. Para efetuar esta garantia, a AC assina o certificado com a sua chave privada. O indivíduo ou entidade que desejar confirmar a autenticidade do certificado, deverá realizar a verificação da assinatura do mesmo com a chave pública da AC [BRO 01].

Os certificados digitais foram inicialmente padronizados no esquema X.509. Das várias propostas de codificação de certificados, a mais conhecida, aceita e utilizada é a recomendação ITU-T X.509v3 [STA 99] e mais recentemente foi lançada a versão 4 [IT 01]. Esta versão está definida na edição do ITU-T, recomendação X.519/ISO/TEC 9594-8 2001.

A versão dos certificados digitais "X.509v3" exige no mínimo as seguintes informações: chave pública, nome do proprietário, número de série do certificado, nome da AC emitente, assinatura digital da AC. Além destas informações obrigatórias a AC poderá acrescentar outras informações que achar pertinente.

A figura 3.1 mostra a estrutura de um certificado digital.

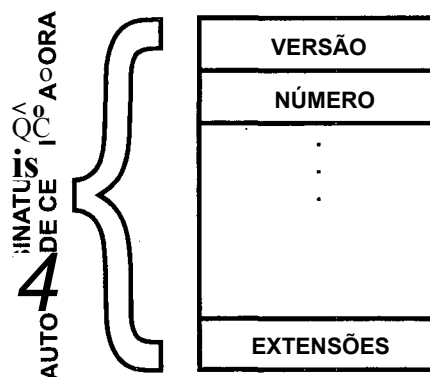


Figura 3.1: Um certificado digital é formado por um conjunto de campos padrões como, por exemplo, número da versão, número único de identificação do certificado, etc.. Além destes campos, um certificado também possui campos de extensão, eles são necessários para definir as funções do certificado, personalizar um certificado, etc..

¹na definição X.509v3 pode-se adicionar atributos na forma de extensões

3.2.1 Extensões

A “Ementa 1 à ISO/IEC 9594 - 8 : 1995” do padrão ITUT X.509, define uma série de extensões de certificados. Os certificados X.509v3 expandem os recursos das versões 1 e 2 e toma possível o ato de acrescentar extensões aos certificados. Estas extensões oferecem controles gerenciais e administrativos úteis para autenticação com objetivos distintos. As extensões de certificados possuem uma função indicada por um valor padrão de 10 (Identificador de Objeto). Cada extensão é assinada com um valor de verdadeiro/falso de importância, determinada pela AC, baseado nas informações fornecidas pelo usuário no ato da solicitação do certificado. É este valor que determina se a extensão é crítica ou não crítica. As extensões fornecem informações específicas do certificado expedido e qual a sua finalidade, provendo meios de associar informações adicionais para aplicações de ICP. Os tipos de extensões possuem funções diferenciadas e podem ser crítica ou não-crítica. A extensão do tipo crítica não poderá ser ignorada pelo usuário de certificados e também limitam o uso de assinaturas para favorecer a certificação. São poucas as extensões deste tipo e devem ser padronizadas. Já a extensão do tipo não-crítica pode ser ignorada pelo usuário de certificados. Um usuário de certificado poderá recusar um certificado se alguma extensão for perdida ou por não haver extensões.

Algumas extensões do padrão X.509v3:

informações sobre política e chaves - esta extensão fornece informações para identificar uma chave pública particular e a política usada na certificação. No caso da chave, a extensão é do tipo crítica, com o uso proposto somente para limitar as responsabilidades da AC. Já para as políticas, a extensão é do tipo não-crítica, pois pode-se ignorar a política existente do certificado;

atributo de emissão e do sujeito - esta extensão fornece informações sobre os nomes e restringe a área dentro da qual os nomes das entidades devem estar localizados. Esta extensão é do tipo crítica, pois os nomes são indispensáveis em um certificado, também apresenta outros atributos utilizados no certificado, no entanto é uma parte não-crítica, pois os atributos são opcionais;

restrições de caminho de certificação - esta extensão possibilita, que uma AC impõe condições para evitar possíveis fraudes, tais como; entidades fim se passarem por ACs. A AC poderá também, impor restrições para prevenir a formação de caminhos infinitos;

extensões de LCRs - As extensões de LCRs fornecem informações sobre qual e onde obter uma determinada LCRs. Esta é uma extensão não-crítica, não há necessidade de estar contínua no certificado, a sua inclusão favorece o usuário.

3.3 Autoridade Certificadora

As Autoridades Certificadoras - ACs são entidades de confiança, que emitem certificados digitais para outras entidades, empresas, indivíduos, que precisam se identificar e garantir as suas operações no mundo digital. Cada certificado digital emitido é certificado e garantido pela AC responsável pela sua emissão. A AC recebe e autentica a solicitação de certificado, emite e chancela digitalmente o certificado e gerencia os certificados emitidos.

O requerente no ato do pedido do certificado, envia para AC, informações pessoais, através de um formulário assegurado pela AC, junto com a chave pública, gerado pelo sistema local ou não. A AC deverá confirmar a veracidade de tais informações, antes da emissão do certificado. A forma como a AC irá confirmar as informações, dependerá da classe do certificado.

A AC define regras de atribuição, confiando suas aplicações a outra entidade, tal como; 'AR - Autoridade de Registro'. A AR recebe os pedidos de certificados, dia após dia, tratando do serviço de pessoal (segurança interna) e comercial (comércio eletrônico). As ACs podem oferecer outros tipos de serviços, tais como; autenticação de data, serviço de gerenciamento de chaves e LCR (Lista de Certificados Revogados). Cada AC define quantas entidades de apoio terá.

As responsabilidades, regras e obrigações legais da AC e dos usuários de certificados, devem ser expressas em um termo conhecido como DPC - Declaração de

Práticas de Certificação. Na DPC, estão definidos os métodos de trabalho, o grau de dos certificados, e das ACs envolvidas no processo de certificação. As ACs estão divididas em três categorias:

Interna - operacionalizada por uma instituição, para a emissão de certificados digitais internos;

Terceirizada - contratada por uma instituição ou empresa para emitir certificados internos e para clientes;

Autônoma - governamental e privada, que comercializa serviços de certificação aos usuários finais.

As AC possuem muitas obrigações, para garantir um serviço confiável, tais como: fornecer serviços de acordo com os termos e condições estabelecidas na DPC; fornecer, atualizar e publicar as DPCs; emitir e publicar diariamente de LCRs, de acordo com os termos e condições estabelecidas na DPC.

3.4 Autoridade de Registro

A AR - Autoridade de Registro é uma entidade responsável pela verificação das informações fornecidas pelos requisitantes dos certificados. A AR atua como um órgão de apoio a AC, podendo inclusive exigir que o requisitante compareça pessoalmente a AR, para garantir a veracidade das informações, também podem lhe ser confiada a tarefa de registrar outras entidades.- As AR possuem algumas obrigações específicas, estabelecidas pela AC para garantirem a das informações conferidas, como receber as informações de um requerente a certificado e conferi-las em banco de dados existentes. Se as informações fornecidas pelos requerentes, forem condizentes com as contidas em Banco de Dados existentes, a AR poderá enviar a AC a solicitação de certificado, para que esta gere, assine digitalmente e emita o certificado, contendo as informações verificadas pela AR.

3.5 Diretório Público

Os serviços do Diretório Público são responsáveis pelas permissões para que os usuários possam realizar consultas ou navegar em determinados diretórios de usuários sem as devidas permissão dos mesmos, e sem o conhecimento dos detalhes dos objetos armazenados, nestes diretórios. A gama de serviços que podem ser utilizados, variam de consultas diretamente análogas à uma lista telefônica [BRO 01].

A CCITT e a OSI - *Open System Interconnections*, definiram um conjunto de poderes para serviços de diretórios da rede, chamado de X.500, que permite os serviços de diretórios públicos.

3.5.1 Serviço de diretório X.500

O padrão X.500 é um protocolo que especifica um modelo para realizar a conexão de serviços de diretórios locais com a finalidade de localizar e prover informações sobre pessoas, organizações, endereços de correios eletrônicos e outros, para a formação de um diretório global acessível a qualquer um interessado em informações disponíveis ao público.

O X.500 é um serviço de diretório OSI, o qual definiu os seguintes componentes [HOW 95]:

modelo de informações - determina a forma e o carácter da informação do diretório;

nome - permite que a informação seja referenciada e organizada;

modelo funcional - determina que as operações possam ser realizadas;

framework **de autenticação** - permite que as informações do diretório sejam seguras;

modelo de operações distribuído - determina como os dados são distribuídos e como as operações são carregadas.

De maneira funcional, o X.500 define 03 (três) áreas de operações:

pesquisa e leitura - a operação de leitura recupera o atributo de entrada cujo nome é conhecido. A operação de pesquisa seleciona as entradas de uma área definida, baseada em algum critério de seleção conhecido, como filtro;

modificação - muda entradas existentes;

autenticação - define uma operação de ligação, permitindo o cliente iniciar uma sessão e provar sua identidade para o diretório. Diversos métodos de autenticação são suportados, desde uma simples senha a uma autenticação baseada em chave pública.

Para cada operação X.500, o resultado poderá ser assinado, a fim de resguardar a sua integridade. A assinatura é feita usando o cliente original ou a chave pública do servidor. A requisição ou resultado modificado é carregado por um protocolo, ponto-a-ponto, permitindo a integridade.

No X.500, o diretório é distribuído entre muitos servidores (chamados DSA - *Directory System Agent*), não importando ao qual servidor o cliente está conectado, caso um não consiga responder a uma requisição, a mesma poderá ser enviada para outro servidor [HOW 95].

3.5.2 LDAP

O protocolo LDAP (*Lightweight Directory Access Protocol*) é baseado nas especificações X.500, definido na RFC 1777 [IX 01]. O protocolo LDAP é um serviço de diretório público utilizado para acessar serviços de diretórios e disponibilização de LCRs [IET 97]. Os serviços deste protocolo são baseados em entradas, ou seja, um conjunto de atributos referenciados através de um nome distinto. A distribuição destes serviços são baseadas em um modelo cliente-servidor.

O protocolo LDAP prevê um mecanismo para fazer consultas, baseadas em texto de um cliente para um servidor LDAP, através da rede TCP/IP. Este protocolo realiza as seguintes operações: pesquisa, adição, exclusão, modificação e renúncia [HOW 95]

3.6 Modelos de Confiança

A Infra-estrutura de Chaves Públicas pode ser organizada em vários modelos diferentes de estrutura hierárquicas. Cada modelo possui uma denominação de acordo com a maneira que as ACs estão distribuídas. Cada um destes modelos, define em quem a entidade pode ou não confiar.

3.6.1 Modelo Isolado

O Modelo Isolado é o mais utilizado atualmente. Ele é formado por uma AC no topo, alguns níveis de ACs intermediárias e as entidades finais. O modelo isolado é ilustrado na figura 3.2.

A AC que fica localizada no topo é denominada AC Raiz. Esta AC é auto-assinada, ou seja, seu certificado é assinado usando sua própria chave privada. Abaixo da AC-Raiz podem haver vários níveis de AC intermediárias. A AC-Raiz pode definir o número máximo de níveis da ICP. Uma AC-Raiz não deve emitir certificados para usuários finais.

As ACs intermediárias podem emitir certificados para entidades finais. Se a AC-Raiz permitir, elas também podem emitir certificados para outras ACs abaixo delas.

Muitas ICPs podem existir paralelamente e cada uma delas poderá ser associada quando se fizer necessário [AJ 99]. O usuário somente obtém a chave pública da AC-raiz de cada ICP, dentro de uma sequência para verificação de certificados de usuários dentro de todas as hierarquias. Os usuários pertencentes a uma hierarquia de raiz desconhecida (ignorada) podem não serem identificados [AJ 00].

3.6.2 Certificação Cruzada

Certificação cruzada é um mecanismo muito útil quando deseja-se estabelecer a confiança entre duas ACs, pertencentes a diferentes ICPs.

Os dois tipos de certificação cruzada serão descritos abaixo:

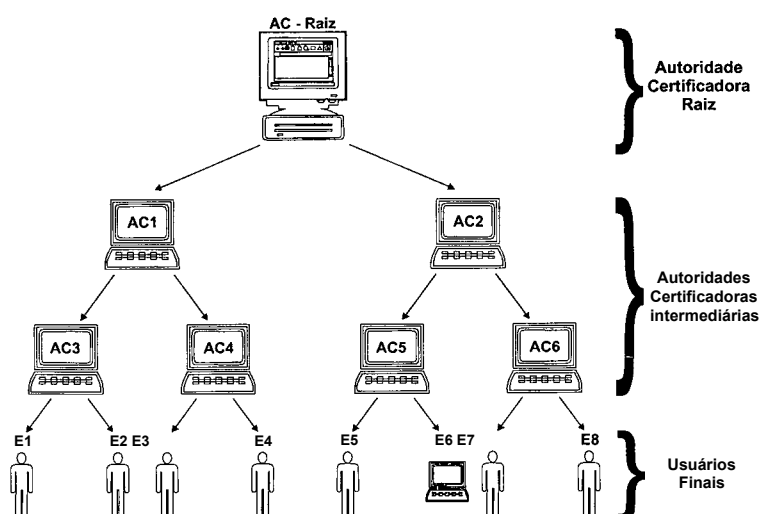


Figura 3.2: A hierarquia isolada possui apenas uma AC Raiz. Abaixo dela podem existir vários níveis de ACs Intermediárias. Uma AC intermediária pode emitir certificados para entidades finais, ou para outras ACs abaixo dela.

Unilateral - Na certificação cruzada somente um dos certificados é assinado pela outra AC, ou seja, a AC_i assina o certificado da AC_2 , porém a AC_2 não assina o certificado da AC_i .



Figura 3.3: Na certificação cruzada unilateral somente um dos lados possui confiança no outro. Na figura acima a AC_2 confia na AC_1 . Esta confiança é atribuída pela assinatura do certificado AC_2 pela AC_1 . Porém a AC_1 não confia na AC_2 , pois esta não assinou seu certificado.

Mútuo - Envolve a assinatura dos certificados de ambas ACs, ou seja, a AC_i assina o certificado da AC_2 , e esta assina o certificado da AC_i .

A certificação cruzada pode ser utilizada para garantir a confiança entre duas ICPs não ligadas. Através da certificação cruzada poderia ser determinada a

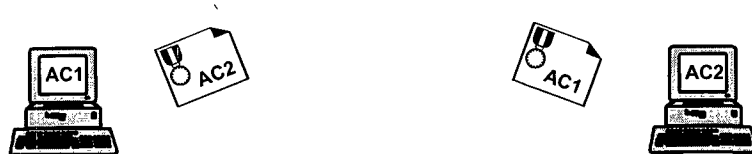


Figura 3.4: Na certificação cruzada mútua ambas as ACs possuem confiança uma na outra. Na figura acima a AC2 confia na AC1 e vice-versa. Esta confiança é atribuída porque a AC2 assina a AC1 e a AC1 assina a AC2.

confiança para a validação de um certificado emitido por uma AC *áalCPi* em um sistema com certificado assinado por alguma AC da *ICP2*.

3.6.3 Modelo em Floresta

Um Modelo em Floresta é uma ligação entre várias ICPs distintas. Estas ICPs, normalmente, são modelos isolados que necessitam estabelecer uma confiança com outras ICPs. Para evitar que os usuários executem requerimentos de diversas chaves públicas de ACs-raízes diferentes ou que não consigam a certificação de que o certificado é de origem confiável, a própria ICP, faz acordos para conectar estes modelos utilizando o mecanismo de certificação cruzada entre a AC-Raiz de um modelo com a AC-Raiz de outro [AJ 99]. Somente ACs-Raízes devem utilizar a certificação cruzada neste caso. Um exemplo de Modelo em Floresta é demonstrado na figura 3.5.

A certificação cruzada entre ICPs, simplifica a certificação de confiança de um determinado certificado, mas o problema é que atualmente, existem muitas ICPs organizadas de diferentes modos. Este tipo de hierarquia funciona bem em comunidades que não possuam um padrão de estrutura, como é o caso da internet. Não é possível, e também não será no futuro, criar uma floresta única. Isto é determinado por motivos políticos, geográficos e culturais.

3.6.3.1 Modelo em Malha

No modelo em malha, cada ICP possui imia certificação cruzada com todas as outras ICPs da floresta.

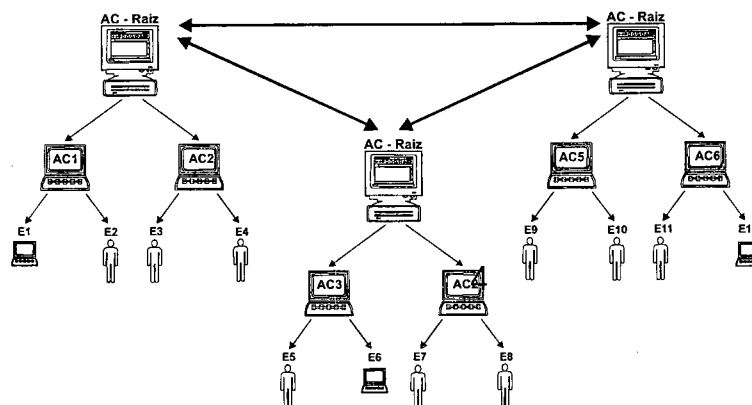


Figura 3.5: O Modelo em Floresta pode possuir várias ACs Raiz. Estas autoridades são conectadas através de certificações cruzadas. Cada ICP pode possuir vários níveis de Autoridades Certificadoras intermediárias. Cada AC intermediária pode emitir certificados para entidades finais ou para outras ACs abaixo dela.

O modelo organizado em malha requer $(N^2 - N)/2$ certificações cruzadas, onde N é o número de ICPs total da floresta. Isto não é obstáculo em ICPs que não possuem uma grande quantidade de ACs. Porém a medida que o número de ACs aumentam, o gerenciamento do sistema torna-se muito complexo.

Uma ICP organizada no modelo em malha é visto na figura 3.6.

3.6.3.2 Modelo com Ponto Central

Neste tipo de modelo cada ICP da floresta possui uma certificação cruzada com uma entidade central, denominada ponte, ou seja, a ponte é o ponto de ligação entre todas as ICP da floresta. Uma estrutura utilizando uma ponte é ilustrada na figura 3.7.

Em uma ICP, que possuem uma grande quantidade de ACs é aconselhável este tipo de modelo, pois o gerenciamento é muito mais simples do que o Modelo em Malha. O gerenciamento torna-se mais simples neste modelo devido ao menor número de certificações cruzadas que necessitam ser estabelecidas. Uma floresta com 10 ICPs, por exemplo, necessita apenas 10 certificações cruzadas com a entidade central, enquanto que no Modelo em Malha necessita de 45 certificações cruzadas.

A arquitetura ponte foi projetada para solucionar o problema da falta de

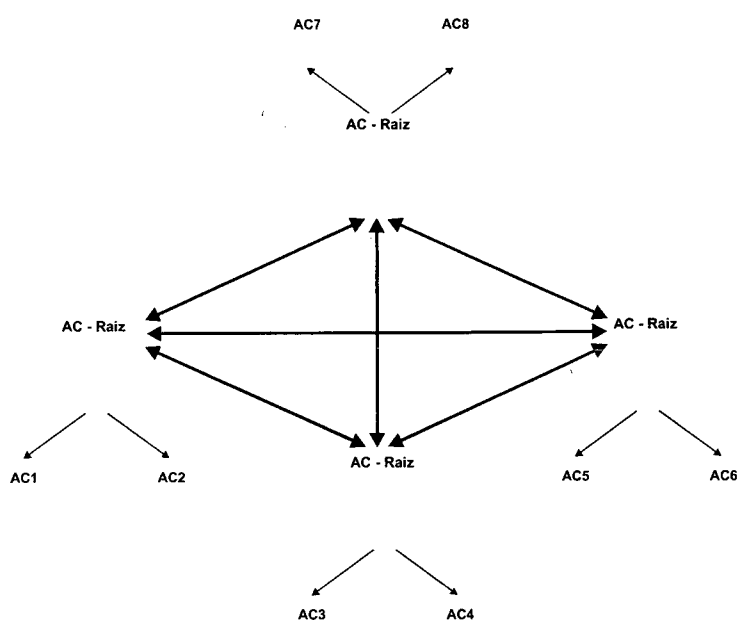


Figura 3.6: No Modelo em Malha cada ICP necessita fazer uma certificação cruzada com todas as outras ICPs da floresta.

endereço de duas ICPs diferentes e também as que implementam arquiteturas diferentes. Diferentemente do modelo malha a AC ponte não emite certificados diretamente para o usuário e sim para a AC-raiz da ICP solicitante [POL 00].

A interoperabilidade da ICP pode ser dotada de diferentes meios, tais como o uso direto de listas de AC, conexões hierárquicas direta e o uso direto de AC de validação, um dos modelos deste processo é representado por FBCA - *Federal Bridge Certification Authority* [ASS 00].

A ação da FBCA não é hierárquica. As ACs agências, recebem permissões para operar com a FBCA, através de termos que são negociados e acertados. Cada AC que opera com a FBCA pode ser capaz de operar com muitas outras, usando o certificado que FBCA emitir.

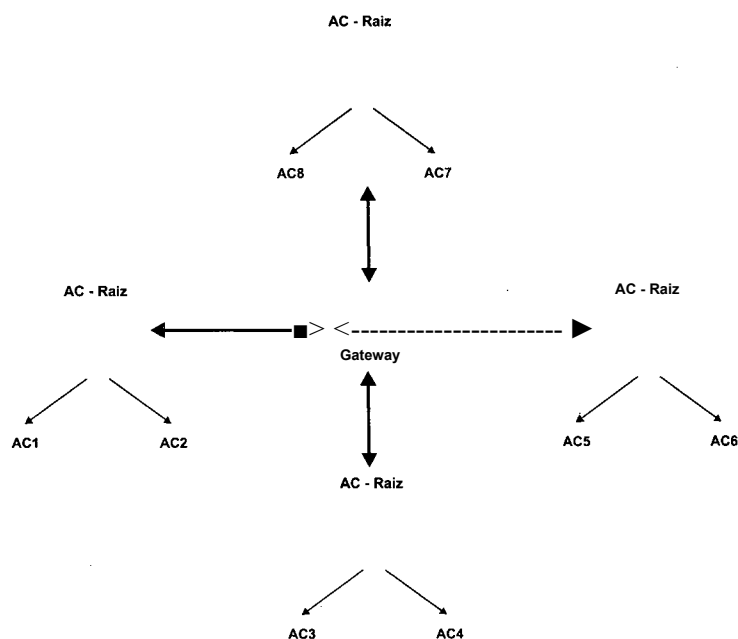


Figura 3.7: No modelo com ponto central é necessário apenas uma certificação cruzada de cada ICP com um ponto central.

3.6.4 Modelo Internet

Como na Internet existem muitas ICPs localizadas em lugares ao redor do mundo, utilizando diferentes modelos, os navegadores criaram um novo modelo para poder atender a necessidade dos usuários das mais diversas ICPs.

Os navegadores já trazem instalados os certificados das ACs-Raízes de algumas ICPs, consideradas, por eles confiáveis. Desta forma, as entidades finais que tiverem seus certificados emitidos por estas ICPs serão automaticamente confiadas pelo navegador.

Quando é estabelecido uma conexão com uma entidade que foi assinada por uma AC de um nível inferior a alguma das ACs-Raízes presentes no navegador, ou pela própria AC-Raiz, o navegador assumirá aquela entidade como confiável e estabelecerá a conexão normalmente. Se a entidade não for assinada por uma AC de nível inferior a uma das ACs-Raízes, o usuário deverá instalar o certificado da AC emissora do certificado antes de estabelecer a conexão. Caso não seja instalado, o navegador exibirá

mensagens alertando o usuário que a entidade não é confiança.

3.7 Caminhos de Certificação

A arquitetura de caminhos de certificados digitais, utilizam cadeias de certificados para transferência de confiança, onde este caminho é formado por todos os certificados, iniciando pelo certificado da entidade final, passando por todas as AC intermediárias, até a AC-Raiz.

O caminho de certificação é necessário para determinar a confiança ou não em um certificado. No momento do recebimento de um certificado, cabe ao sistema descobrir se ele deve ou não ser confiável. Isto é feito através do processamento do caminho de certificação, ou seja, a possibilidade de percorrer todo o caminho da certificação e validação do certificado, através de uma corrente de ligação entre ACs.

Antes do sistema interpretar o certificado recebido como um certificado válido, ele monta todo o caminho de certificação e descobre se este possui algum certificado considerado "confiável" por ele. Além disso, o sistema também procurará uma brecha no caminho de certificação, ou seja, algum certificado que possua restrições ou que não poderá mais ser considerado válido.

Se a AC emissora do certificado não for confiada pelo sistema e nenhuma outra AC do caminho de certificação possuir esta confiança, o certificado será assumido como não confiável pelo sistema e a conexão só continuará se o usuário assumir a responsabilidade da confiança.

O processamento do caminho de certificação é executado em duas etapas, determinação e validação.

3.7.1 Determinação

A primeira fase é a determinação do caminho de certificação. Para isto, todos os certificados entre o sujeito e a AC confiável, são buscados nos diretórios.

A busca dos certificados é efetuada começando pelo certificado da enti-

dade final e seguindo em direção a AC-Raiz. Para isto é utilizado um campo de extensão do certificado digital que aponta para o certificado da AC superior.

A determinação também é responsável pela obtenção de todas as LCRs[^] necessárias para validação, incluindo a verificação de sua integridade e validade.

3.7.2 Validação

Após determinado o caminho de certificação entre a entidade final e a autoridade no nível mais alto da hierarquia, há a necessidade de checar se não existe nada errado.

Ao contrário da determinação, a validação é iniciada na AC confiável e "desce" até a entidade final.

De acordo com a RFC 2459, o objetivo da validação é estabelecer a ligação entre o nome distinto ou o nome alternativo do sujeito e sua chave pública, de acordo com a chave pública de uma AC de "maior" confiança. Esta AC pode ser a AC-Raiz, a AC que emitiu o certificado que está sendo verificado, ou qualquer outra AC integrante da ICP.

Para a validação, as seguintes verificações são exercidas sobre cada certificado do caminho de certificação:

- se a assinatura do certificado foi exercida por uma AC de nível imediatamente superior. No caso de uma AC-Raiz, a verificação da assinatura é feita com a chave pública do próprio certificado, ou este passo é omitido;
- se o período de validade não expirou. A data e hora do computador do usuário são utilizadas para testar este passo;
- se o certificado não está revogado ou não está definido como suspenso em sua LCR, a data e hora do computador do usuário são utilizadas para testar esse passo;
- se os dados presentes no campo sujeito do certificado é idêntico aos dados do campo emissor do certificado que o assinou;

[^]Seção 4.5

- verificar se não existe alguma(s) política(s) tomando o certificado inválido;
- reconhecer e processar todas as extensões críticas presentes no certificado;
- verificar a existência de alguns campos de extensão e, caso esteja presente, verificar se as suas características não invalidam o certificado.

Caso alguma das ações acima venha a falhar, o procedimento termina e o caminho de certificação é assumido como inválido. Se todas as ações forem executadas com sucesso, o caminho de certificação é declarado válido.

3.8 Conclusão

A infra-estrutura de chave pública é uma tecnologia complexa e que envolve vários componentes, recomendações e padrões, porém toda esta estrutura criada é de extrema importância para atender as necessidades de segurança da comunidade global para o suporte de certificação digital e da manutenção dos mesmos. Sem esta infra-estrutura provavelmente não seria capaz de fornecer a segurança que se almeja.

Capítulo 4

Política de Certificados

4.1 Introdução

Neste capítulo são abordadas as políticas de certificados, as regras, as normas, o que a política de certificação estabelece na infra-estrutura de certificação digital. A política de certificados é um documento elaborado pela AC para garantir o processo de emissão e gerenciamento de um certificado e para o entendimento do processo pelo usuário.

Este capítulo aborda os seguintes temas: a seção 4.2 faz uma introdução sobre a política de certificados, falando sobre objetivos e qualificações; a seção 4.3 faz uma abordagem sobre as extensões de política de certificados; a seção 4.4 aborda os qualificadores de políticas de certificados; a seção 4.5 faz uma abordagem das aplicações de políticas e finalmente a seção 4.6 faz uma abordagem sobre o que é uma declaração de práticas de certificação - DPC.

4.2 Políticas de Certificação

A RFC (*Request for Comment*) 2527 é um documento elaborado pela IETF (*Internet Engineering Task Force*), intitulado como (*Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*), elaborado em

março de 1999, para tratar da política de certificados e da declaração de práticas de certificação. Esta RFC trata a PC e DPC de forma bastante sucinta, ou seja, apenas os principais itens que devem conter nestes dois documentos. Quando ao realizar o estudo da RFC, percebeu-se que o seu conteúdo não era suficiente para a elaboração de uma política de certificação e da declaração de práticas de certificação, e que não atendia a todos os requisitos necessários de uma ICP, foi então que realizou-se o estudo de entidades que já possuíam políticas de certificação e declaração de práticas de certificação, o que levou-nos a elaboração da comparação das DPCs. Com a realização da comparação das DPCs, pode-se verificar o que mais poderia estar sendo incluso nos documentos, e que através da estrutura da ICP ou da AC, pode-se levantar vários itens a serem inclusos na DPC e PC.

Definida no X.509 e endossada pela RFC 2527 [RFC 99] a política de certificação é definida como: um conjunto de regras nomeadas que indicam a aplicabilidade do certificado para uma comunidade particular e ou classes de aplicações com requerimentos de segurança comuns, por exemplo: uma política de certificados, poderá indicar a aplicabilidade de um tipo de certificado para uma autenticação de dados eletrônicos permutados em transações de comércio de bens [SL 01]. A versão 3 do X.509, contém um indicador de PC, que poderá ser usada pelo usuário de um certificado, para decidir se confia ou não no mesmo para um propósito particular [RFC 99].

A política de certificados é o instrumento de base para a formação da interoperabilidade entre dois ou mais domínios de ICPs. Cada certificado precisa de um identificador, com o intuito da política de certificados ser reconhecida pelo emissor e pelo o usuário do certificado, esse identificador é representado no certificado pelo 10 - identificador de objeto. Este processo é especificado na ISO/IEC e no padrão ITU [RFC 99]. Para estabelecer um vínculo entre todos os usuários de certificados, as 10 registrada no certificado, publicam a especificação textual da PC, para que os usuários possam eximir as que estiverem envolvidas em transmissões. As IOs dos certificados devem ser apropriados e conhecidos pela entidade fim.

O ato da AC, emitir um certificado para um usuário que possui uma chave pública particular, é representada por uma entidade que é autenticada de acordo

com as regras estabelecidas por uma PC [CAN 99]. Quando uma AC-raiz possui um certificado, poderá estabelecer conexões confiáveis, onde cada AC poderá organizar uma ou mais PC, para realizar as certificações [CAN 99].

As PCs apresentam o grau de segurança existente em um certificado. As PCs podem ser para mais de uma simples organização. As PCs são fundamentais para os processos de certificação, servindo como base para padrões de interoperabilidade, contendo os critérios de segurança [CAN 99].

4.2.1 Objetivos das Políticas de Certificados

O objetivo da PC é fornecer uma forma de gerenciamento da infra-estrutura de chaves públicas de uma organização. A PC estabelece e gerencia o uso da criptografia de chave pública, informações e a tecnologia da infra-estrutura [CAN 99].

4.2.2 Qualificações da Política de Certificação

As qualificações da PC, depende das informações que a companhia fornece, identificadas no certificado X.509 [RFC 99].

Quando uma AC emite um certificado para um usuário, este é fornecido perante uma declaração para o usuário de que a chave pública particular é da entidade particular emitente do certificado. Entretanto o grau ao qual o usuário do certificado deverá confiar na declaração, precisa ser avaliado, dependendo da necessidade. Diferentes certificados podem ser emitidos permitindo práticas e procedimentos diferentes, e podem ser adequados para diferentes aplicações e propósitos.

A implementação de PCs, serve de base para a aprovação de ACs. AC ao emitir um certificado para outra AC, precisa avaliar o conjunto de PCs, para o qual ela vai confiar o certificado, após a avaliação das PCs, é então indicado para a emissora.

A lógica de processamento de caminhos de certificados X.509, emprega essas indicações de PCs para a definição de um modelo confiável [RFC 99].

4.3 Extensões

Os campos de extensões no certificado X.509, suportados pela PC, são:

- extensões de políticas de certificação;
- extensões de mapeamento de políticas;
- extensões de restrições de política.

4.3.1 Extensões de Políticas de Certificados

As extensões de PCs possuem duas variáveis, sendo uma de campo de transmissão não-crítica e a outra crítica, no entanto os propósitos são distintos.

Os campos não-críticos da PC, são listados por AC, que os declara para o que são aplicáveis. Entretanto, um certificado poderá ser usado em outras funções, além do propósito indicado pela AC. Um certificado emitido para uma AC, contém um 10 para as PCs pertinentes. A PC pode também conter opcionalmente qualificadores de valores para 10 [RFC 99].

O campo não-crítico é designado para ser usado por aplicações que são configuradas para conhecer a PC requerida [RFC 99].

Quando é processado um caminho de certificação, a PC é aceita por aplicações, que usam o certificado, mas precisam estar presentes em vários caminhos.

4.3.2 Extensão de Mapeamento de Política

A extensão de mapeamento pode ser usada somente em árvores de ACs. Este campo permite que a AC indique uma determinada PC do seu próprio domínio para ser equivalente à outras do domínio da árvore [RFC 99].

4.3.3 Extensão de Restrição de Política

Estas extensões suportam duas características de ordem opcional: a habilidade de uma AC requerer uma indicação de PC explícita, presente em um certificado

existente em um caminho de certificação. Um usuário poderá considerar o início do caminho de certificação como parte de um domínio confiável, tais certificados não precisam possuir indicações explícitas de PC [RFC 99]. No entanto, a AC de um domínio confiável ao certificar um domínio externo, poderá estar ativando o requerimento de um PC explícita de um certificado do caminho de certificação.

A desativação da política de mapeamento poderá ser prudente em um domínio de certificação externo [RFC 99].

4.4 Qualificadores de Políticas

o campo extensão da PC tem uma previsão de transmissão, junto ao identificador, estas informações dependem de campos qualificadores adicionais em PCs. O padrão X.509 não mantém o propósito para o qual este campo é para ser usado, não prescrevendo uma sintaxe dele [RFC 99].

Os seguintes tipos de qualificadores de PC são definidos na ICP:

- a) A PC possui um qualificador ponto para uma PC publicada pela AC. O ponto é na forma de um identificador de recurso uniforme;
- b) O qualificador contém um texto em série, que é para ser exposto para o usuário do certificado, anterior ao uso do mesmo.

Os qualificadores de PCs podem ser usados para suportar a definição de genérico ou padronizado e definições de PC.

4.5 Aplicações de Políticas de Certificação

Toda organização responsável por uma ICP deve elaborar um documento contendo suas PC de forma a facilitar o entendimento do processo como um todo, por seus usuários. Este documento detalha todas as políticas instituídas pela organização para garantir a segurança do processo de emissão e manutenção dos certificados emitidos. Cada AC poderá adotar uma ou mais PC, mas em todos os casos, o documento tem que

estabelecer confiança para o certificado de chave pública e constituir uma base de certificado raiz.

As PCs descrevem o papel de cada componente dentro da ICP, as responsabilidades assumidas pelos seus usuários para a requisição e uso dos certificados digitais, além da manutenção do par de chaves. As políticas de certificação devem abranger desde a solicitação do certificado, até a sua expiração ou revogação.

As políticas de certificação não declaram os detalhes operacionais, pois estes podem ser alterados ao longo do tempo. Isso torna as PCs um documento estável.

Quando a ICP conter múltiplas ACs, devem ser declaradas todas as ACs que fazem parte da ICP. Além disto, diferentes ICPs poderiam utilizar as mesmas PCs, caso possuam as mesmas políticas [HOU 01].

4.6 Declaração de Práticas de Certificação

Na Declaração de Práticas de Certificação - DPC, é especificada detalhadamente como cada componente da ICP, implementa a política de certificados. A DPC declara a PC associada e especifica os mecanismos e procedimentos utilizados para alcançar as políticas de segurança.

Uma DPC pode informar os aplicativos utilizados e os procedimentos de utilização do aplicativo. Ela deverá ser detalhada suficientemente para comprovar que todas as políticas podem ser satisfeitas através de procedimentos e ferramentas [HOU 01].

Uma ICP deve declarar uma DPC para cada componente que a integra, porém muitas vezes podem haver dois componentes executando funções semelhantes. Neste caso uma única DPC pode ser usada para ambos os componentes.

4.7 Conclusão

A política de certificados é importante para que a infraestrutura de chaves públicas e a certificação ocorra de acordo com as leis e a segurança desejada. É obrigação de cada AC estabelecer uma PC para conduzir o processo de emissão de seus

certificados. Esta política poderá não estar elaborada independentemente, mas sim englobada na DPC. A DPC e a política de certificados formam apenas um documento, ficando a critério da AC.

Capítulo 5

Comparação entre DPCs

5.1 Introdução

A Declaração de Práticas de Certificação - DPC é um documento que especifica detalhadamente como cada componente da ICP, implementa a política de certificados. A DPC pode informar os aplicativos utilizados e os procedimentos de utilização do aplicativo. Cada AC ou ICP deve estabelecer uma DPC.

Este capítulo faz uma comparação entre algumas DPCs e a ICP-Brasil. A comparação das DPCs a seguir refere-se a todo o seu conteúdo. As DPCs comparadas são da *VeriSign*, *Entrust* e ICP-Brasil.

Para realizar a comparação das DPCs foram pesquisadas algumas ACs, as quais estão especificadas no Tabela 5.1, das quais foram selecionadas três, para a comparação. O critério da seleção deu-se por meio de alguns critérios a saber. A *VeriSign* e a *Entrust.Net* são as duas mais conhecidas e importantes ACs do mundo, no âmbito da segurança mundial, juntamente com a ICP-Brasil congregam características suficientes para a comparação entre as DPCs. As DPCs da *VeriSign* e a *Entrust.Net* são documentos contínuos, que permite uma certa facilidade de entendimento pelo candidato a certificação, enquanto que a *Baltimore*, *Thawte*, *ABA - ECom* e outras não citadas aqui, possuem suas DPCs divididas em vários segmentos, dificultando a compreensão global do documentos. Apesar da divisão de segmentos da DPC da *Baltimore*, a ICP-Brasil se-

gue este estilo. Ademais, tanto a a *CertiSign* como a *GlobalSign* são afiliadas da *VeriSign*, tomando a abordagem destas redundante, pois as normalizações são iguais.

A abordagem da ICP-Brasil se justifica por ser o único documento brasileiro adequado ao contexto da legislação brasileira. Além disso, a Medida Provisória 2200 de 29 de junho de 2001, instituiu a ICP-Brasil como uma documento regulamentador das entidades nacionais.

Tabela 5.1: Principais Entidades de Certificação

VeriSign	Das ACs existentes, esta é a mais conhecida no mundo inteiro, possuindo, inclusive uma filial no Brasil, a <i>CertiSign</i> . A <i>VeriSign</i> é uma empresa Americana.
Entrust.NET	No ranque das entidades mais conhecidas, a Entrust. Net está em segundo lugar, também de origem Americana.
Baltimore	A entidade Baltimore, faz parte da união européia, bastante conhecida.
Thawte	E uma entidade de propriedade da <i>VeriSign</i> , portanto a a DPC segue o mesmo padrão.
GlobalSign	É uma empresa de propriedade da <i>VeriSign</i> , portanto a DPC é igual.
CertiSign	É uma empresa instalada no Brasil, de propriedade da <i>VeriSign</i> , possuindo a mesma DPC
ICP - Brasil	A ICP-Brasil é um documento que regulariza a criação de autoridades certificadoras e a certificação no Brasil.

Este capítulo está organizado da seguinte forma: na seção 5.2 é descrita a estrutura da DPC; na seção 5.3 é descrita as extensões e a nomeação dos certificados, utilizadas pelas ACs; na seção 5.4 é descrita as classes dos certificados e a estrutura dos mesmos; na seção 5.5 é descrita a geração, proteção e o gerenciamento do par de chaves; na seção 5.6 é descrita a infra-estrutura de chaves públicas, composta por entidades, tais como AC-raiz, ACs, AR, etc.; na seção 5.7 é descrito a base e os controles para operações de SCP, processo de funcionamento de AC; na seção 5.8 é descrito as responsabilidades, obrigações e garantias de ACs, ARs, usuários, em fim de todos os componentes ligados ao certificado emitido; na seção 5.9 é descrito como é realizado o processo de auditoria das ACs; na seção 5.10 é descrito a segurança usada pelas ACs e AR, para garantir a integridade de seus certificados e de toda a sua estrutura; na seção 5.11 é descrito as formas de contratação e gerenciamento dos funcionários responsáveis pelos processos de certificação; na seção 5.12 é descrito quem e como é o acordo com os detentores da parte secreta; na seção 5.13 é descrito o processo de como é realizada a solicitação de

certificados; na seção 5.14 é descrito o tempo que um certificado permanece ativo; na seção 5.15 é descrito o processo de emissão dos certificados; na seção 5.16 é descrito como a AC e o requerente realizam a aceitação do certificado emitido; na seção 5.17 é descrito a qual finalidade o certificado emitido poderá ser usado; na seção 5.18 é descrito todo o processo de como é realizada a suspensão e a revogação de um certificado ativo; na seção 5.19 é descrito o procedimento da AC ao vencer o certificado; na seção 5.20 é descrito termos e condições gerais das DPCs, que não são abordados em outros pontos; na seção 5.20.1 é descrito como será o processo, caso ocorra alguma divergência ou o não cumprimento de alguma norma em relação ao certificado e por fim na seção 5.20.2 é descrito como a AC deverá proceder caso necessite efetuar alguma mudança na DPC ou PC.

5.2 Informações sobre a DPC

Esta seção do documento é responsável pela descrição de como é a estrutura interna do mesmo, a possibilidade de reprodução, a forma de sua distribuição e o significado dos termos e simbologias utilizadas. A tabela 5.2 apresenta as estruturas das DPCs contidas nesta seção, que estão sendo comparadas. Pode-se notar que cada DPC aborda assuntos diferenciados, neste item, mas todos voltados ao processo de certificação.

Tabela 5.2: Estrutura da DPC

VeriSign	Aborda o ciclo de vida descritos nos processos de certificação.
Entrust.NET	Descreve brevemente as práticas e os procedimentos, direitos e obrigações da AC, AR, usuários, etc.
ICP - Brasil	São especificadas as regras e práticas dos serviços de sigilo, autenticação, integridade; especifica os aspectos quanto a gerência e utilização dos certificados e também possui um outro documento chamado de DRO - Declaração de Regras Operacionais, somente para operação da AC raiz e AC, serviços oferecidos pela AC-raiz, direcionado às políticas, práticas e aos procedimentos a serem empregados pela AC-raiz.

Quanto a reprodução e distribuição, verifica-se através da tabela 5.3, que o ato de reproduzir e distribuir DPCs, poderá ocorrer normalmente, desde que a nota *copyright*, seja mantida no documento.

Tabela 5.3: Reprodução e Distribuição

VeriSign	Permite a sua reprodução e distribuição de forma não exclusiva e sem pagamento, desde que conste a nota copyright e seja na íntegra
Entrust.NET	Permite reproduzir a DPC, desde que o aviso de copyright seja mantido e o conteúdo esteja na íntegra.
ICP - Brasil	Nada Consta

A incorporação de DPCs aos certificados deverá ocorrer para facilitar ao usuário a sua leitura. A tabela 5.4 mostra que esta incorporação deverá ocorrer por referência, ou seja, em algum espaço do certificado, deverá existir um link direto para a DPC.

Tabela 5.4: Incorporação por Referência

VeriSign	As DPCs são incorporadas por referência ao certificados.
Entrust.NET	As DPCs são incorporadas por referência ao certificados.
ICP - Brasil	O 10 da política deve ser incluído no certificado.

A AC poderá utilizar links em suas páginas, colocar a DPC em diretórios públicos, ou repositórios para que os interessados em adquirir certificados digitais tenham acesso. Pode-se verificar, através da tabela 5.5, que as entidades utilizam links de acesso a DPC ou uma referência, que guie o usuário para a DPC.

Tabela 5.5: Indicadores da DPC

VeriSign	Indicadores baseados em computadores e textos são utilizados, facilitando o acesso a DPC.
Entrust.NET	Por referência, etc.
ICP - Brasil	Nada consta

Quanto a assistência, instruções e treinamento para o usuário, acham que é importante o usuário possuir conhecimento de como utilizar chaves, caso contrário o mesmo deverá procurar um treinamento. A tabela 5.6 mostra que, a AC espera que o usuário ao candidatar-se ao certificado já deve estar apto ao manuseio de chaves.

Tabela 5.6: Assistência, Instruções e Treinamento

VeriSign	Pressupõe que o requerente esteja familiarizado com o uso de chaves, caso contrário sugere-se o treinamento.
Entrust.NET	Pressupõe que o requerente esteja familiarizado com o uso de chaves, caso contrário é necessário que o mesmo procure instruções.
ICP - Brasil	Nada Consta

5.3 Extensões e Nomeação de Certificados

Esta seção do documento, é responsável pela descrição das extensões e da nomeação dos certificados, utilizados pelas ACs responsáveis pela certificação digital. A tabela 5.7 apresenta os mecanismos de extensões e a estrutura de autenticação, usados pela ACs, tipos de extensão, a forma de nomeação. Nota-se porém que somente a *VeriSign* trata de nomeação de certificados.

Tabela 5.7: Extensões e Nomeação

VeriSign	Mecanismos de extensões e a estrutura de autenticação: os certificados X.509v3 [IT 01] expandem os recursos das versões 1 e 2, permitindo o acréscimo de extensões. Extensões padrão e específicas dos serviços; a Emenda 1 à ISO/IEC 9594-8; 1995 do X.509v3 define extensões que oferecem vários controles gerenciais e administrativos úteis para a autenticação em grande escala e com objetivos distintos. Identificação e importância de extensões específicas: a função de cada extensão é indicada por 1 valor padrão de "10". Extensões de certificados do assinante/usuário final: são permitidas três: restrições básicas, uso de chaves e política de certificados. Extensões de restrições básicas definidas pela ISO: delimitam o papel e a posição de um certificado de AE ou assinante/usuário final em 1 cadeia de certificados. Extensões de uso de chave definida pela ISO: limita os objetivos técnicos para os quais a chave pública listada no certificado válido podem ser usada. Extensões de política de certificados definida pela ISO: limita um certificado às práticas exigidas pelas partes confiantes. Nomeação avançada e extensões: exceto determinados certificados S/MIME v1, todos os demais contém um campo adicional de unidade organizacional - UO.
Entrust.NET	Mecanismos de extensões e a estrutura de autenticação: os certificados emitidos estão de acordo com as especificações do protocolo SSL. Extensões padrão e específicas dos serviços: possuem a extensão <i>keyusage</i> e <i>extendedkeyusage</i> restringindo o objetivo de utilização do certificado.
ICP - Brasil	Mecanismos de extensões e a estrutura de autenticação: devem suportar os padrões de extensões previstos no item 4.2.1 da RFC 2459 e os nomes atenderem ao formato X.501 "printableString". Extensões de certificados do assinante/usuário final: os certificados e as LCRs, segundo o padrão X.509v3. Para certificados de AC-raiz ou AC seguem o padrão ISO/IEC 9594-8:1995 do X.509v3.

5.4 Infraestrutura de Certificação

Esta seção do documento, é responsável pela descrição dos itens que formam a infra-estrutura da certificação: as classes, as informações fornecidas pelo usuário, certificação cruzada entre ACs, cadeias de certificação. A tabela 5.8 mostra para quais finalidades os certificados são usados. Pode-se notar que as os certificados são usados para as mesmas finalidades.

Tabela 5.8: Infra-Estrutura de Confiança

VeriSign	Suportam o comércio eletrônico seguro e outros serviços de segurança, atendendo necessidades técnicas, de negócios e pessoais.
Entrust.NET	Comunicações seguras entre servidores e browsers da WWW, usando protocolo SSL.
ICP - Brasil	Transações eletrônicas e aplicações, autenticação, irretratabilidade e integridade de mensagens.

A administração de domínio de SCP permite que a AC distribua algumas atividades para outras entidades realizarem, desde que seja mantido o mesmo princípio. A tabela 5.9 mostra que somente a *VeriSign*, faz esta distribuição. Nota-se que este serviço facilita a operação de uma AC.

Tabela 5.9: Administração do Domínio de SCP

VeriSign	São administrados de forma que algumas atividades de SCP, possam ser executadas por outras partes, que não a <i>VeriSign</i> . O princípio subjacente da administração de domínio baseia-se em delegação rígida de autoridade.
Entrust.NET	Nada consta
ICP - Brasil	Nada Consta

A confirmação da identidade do assinante é realizada pela entidade responsável por este serviço para obter a confirmação de que o requerente é quem diz ser. A tabela 5.10 mostra que para cada classe de certificado é realizado um tipo de confirmação. Nota-se que o grau de exigência no ato da confirmação, depende do nível de segurança exigido pelo certificado.

Quanto as informações confidenciais, mostra-se que são as informações que não ficam a disposição do público. Pode-se notar através da tabela 5.11, que estas

Tabela 5.10: Confirmação da Identidade do Assinante

VeriSign	A AE toma medidas para validar a identidade dos candidatos a certificados e confirma as informações fornecidas durante o processo de solicitação, dependendo da classe, solicita ou não a presença do candidato, ou a confirmação por um tabelião.
Entrust.NET	Execução de verificação limitada das identidades individuais. Pode solicitar a presença do candidato ou de um tabelião diante da AR e também apresentar três peças de identificação de imagem. A autenticação de “10” é realizada em BD.
ICP-Brasil	Usa medidas de identificação tais como, comparar a 10 com dois tipos de identificação (fotocópia autenticada ou original), ou por meio de processo realizado em empresa e ou órgão (BD). No caso de equipamento será uma pessoa física a responsabilizar-se.

informações não podem ser vendidas ou reveladas pela entidade responsável. A revelação destas informações só poderão ocorrer perante um pedido oficial do proprietário ou ordem judicial.

Tabela 5.11: Informações Confidenciais

VeriSign	São informações não disponíveis para o público, não podem ser reveladas ou vendidas pela AC nem pela <i>VeriSign</i> , somente com pedido feito pelo proprietário ou por ordem judicial.
Entrust.NET	Nem a <i>Entrust</i> ou a AC podem revelar ou vender informações de candidatos, e informações contidas em certificados, exceto para oficiais de cobrança jurídico, para processos ou a pedido do proprietário.
ICP - Brasil	Todas as informações pessoais ou corporativas mantidas pela AC ou AR não podem ser divulgadas sem o consentimento do usuário ou determinação judicial.

Quanto as informações não-confidenciais, percebe-se pela tabela 5.12, que são as informações acessíveis ao público, sem estar presente em certificados ou LCRs.

Tabela 5.12: Informações não Confidenciais

VeriSign	Nada consta
Entrust.NET	São as informações sem um certificado ou incluídas em LCR.
ICP - Brasil	Todas as informações contidas em certificados, LCR e informações corporativas ou pessoal são confidenciais.

Os certificados digitais são geralmente divididos em classes. A tabela 5.13 mostra que as ACs dividem seus certificados em classes de acordo com o grau de segurança. Nota-se que a maioria das ACs seguem o mesmo padrão, dividindo seus certificados em ordem crescente de classe e de confiança. A ICP-Brasil, porém não segue

este padrão, seus certificados estão divididos em ordem crescente de níveis e em ordem decrescente de confiança.

Tabela 5.13: Classes de Certificados

VeriSign	Suporta três classes diferentes, com níveis de confiança e características diferenciadas, em ordem crescente: classe 1 - nível mais baixo de confiança, classe 2 - nível médio de confiança e classe 3 - mais alto nível de confiança. A <i>VeriSign</i> possui ainda um certificado teste.
Entrust.NET	Apenas um tipo de certificado.
ICP - Brasil	Oferece quatro níveis de confiança e características diferenciados, em ordem decrescente: nível 1 - alto nível de segurança; nível 2 - nível médio de segurança; nível 3 - nível básico de segurança e nível 4 - nível ordinário de segurança. E também o certificado da AC-raiz, de nível mais alto da ICP-Brasil.

A tabela 5.14 mostra que as classes de certificados possuem algumas propriedades comuns a todas e outras específicas.

Tabela 5.14: Propriedades das Classes de Certificados

VeriSign	As propriedades variam de acordo com as classes de certificados, sendo que algumas são comuns aos níveis.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

Quanto a certificação cruzada, as ACs realizam acordos que permitem uma AC, reconhecer o certificado de outra. Nota-se porém, através da tabela 5.15, que somente a ICP-Brasil relata a certificação cruzada.

Tabela 5.15: Certificação Cruzada

VeriSign	Nada consta
Entrust.NET	Nada consta
ICP - Brasil	São acordos entre a ICP-Brasil e outras ICPs aprovadas pela CG da ICP-Brasil. A solicitação da certificação cruzada pode ser feita por AR, usuários, ACs. A sua revogação poderá ser feita pela AC ou CG da ICP-Brasil.

A tabela 5.16 mostra que a verificação de certificados pode ser em ambos os sentidos, entre as entidades.

Além destas informações comparadas, a *VeriSign* ainda nesta seção, faz um breve comentário sobre a configuração entre a chave pública e a entidade, gerenciando

Tabela 5.16: Cadeias de Certificados e Tipos de AEs

VeriSign	Cada AE de uma cadeia de certificados executa procedimentos específicos, conforme o que lhe foi atribuído, podendo ser AC-raiz para AR, AE para outra AE e AE para assinantes.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

processo de certificação, níveis, solicitação, emissão, análise, aceitação e gerenciamento de certificados, volta a falar destes itens nas próximas seções.

5.5 Chaves Públicas e Privadas

Esta seção do documento é responsável pela descrição da geração, gerenciamento, proteção, ativação, desativação das chaves pública e privada tanto das ACs como dos usuários. A tabela 5.17 mostra que as ACs não geram o par de chaves do usuário, mas mostra que cada usuário deverá gerar de forma segura seu par de chaves.

Tabela 5.17: Geração de Chaves

VeriSign	Cada candidato deve gerar de forma segura seu próprio par de chaves.
Entrust.NET	Gerar um par de chaves seguro e com criptografia semelhante, para ser usado com o certificado <i>Entrust.NETSSL Web Server</i> a ser emitido.
ICP - Brasil	O requerente deve gerar o par de chaves, usando equipamentos da AR e um algoritmo aprovado pelo CG da ICP-Brasil. A chave gerada deve ser gravada em meio físico.

Quanto a geração de chaves de AE ou AC, as mesmas devem gerar suas chaves de forma segura. A tabela 5.18 mostra que as três DPCs comparadas, declaram que são as próprias ACs que geram suas chaves, devendo no entanto seguir um padrão de segurança, estabelecido pela AC-raiz, assinante do certificado da mesma.

As ACs para gerarem suas chaves devem possuir meios para protegê-las, principalmente a chave privada. A tabela 5.19 mostra de que forma as ACs fazem a proteção da chave privada. Nota-se porém, que cada AC possui seu próprio método de segurança para fazer a proteção da chave privada.

Quanto a proteção da chave privada do assinante, a tabela 5.20 mostra

Tabela 5.18: Geração das Chaves de AE ou AC

VeriSign	A AE deve gerar e proteger suas próprias chaves privadas.
Entrust.NET	Deve ser criada na inicialização do aplicativo <i>Entrust/Marter Control</i> , e protegida pela chave mestre da AC. Cria-se também uma chave de HW compatível.
ICP - Brasil	A própria AC gera seu par de chaves e encaminha a chave pública para AC-raiz. A AC-raiz possui uma política de operar off.line os equipamentos de geração de chaves e de certificados para garantir o acesso interno e não externo.

Tabela 5.19: Proteção da Chave Privada da AE ou AC

VeriSign	A proteção se da através de produtos de HW confiáveis, as AEs de classe 1 podem protege-lá apenas por SW de criptografia
Entrust.NET	A <i>Entrust.Net</i> usa o <i>Software Entrust/Authority juntamente</i> com HW certificado com nível3 doFIPS 140-1.
ICP - Brasil	Exige um controle múltiplo

que o assinante deverá ser responsável por sua chave privada. Nota-se que as ACs se isentam de tal responsabilidade.

Tabela 5.20: Proteção da Chave Privada do Assinante

VeriSign	As AEs não geram nem detém as chaves privadas, a segurança é de inteira responsabilidade do assinante. Este deve evitar o comprometimento, perda, divulgação, modificação ou utilização indevida.
Entrust.NET	É de inteira responsabilidade do assinante, a proteção da chave privada.
ICP - Brasil	Não deve ser implementada a recuperação da cópia da chave privada do usuário, mas se possuir deverá armazená-lá em meio físico de armazenamento lógico. A AC poderá opcionalmente, manter uma cópia de segurança da chave privada. O usuário é responsável pela segurança e sigilo em todos os níveis do certificado.

As chaves privadas possuem um tempo de vida, desde sua ativação até a sua destruição final. Esta sequência é tratada apenas pela ICP-Brasil, conforme a tabela 5.21.

A chave pública do assinante deverá ser encaminhada à AC pelo mesmo. Nota-se através da tabela 5.22, que as ACs normalmente não interferem no modo como o usuários irá enviar a chave pública. Com exceções, como é o caso a ICP-Brasil, que solicita o envio compatível com o padrão *PKCS#1*.

Tabela 5.21: Inserção, Ativação, Desativação e Destruição da Chave Privada

VeriSign	Nada consta
Entrust.NET	Nada consta
ICP - Brasil	A chave privada deverá ser inserida no módulo criptográfico de acordo com o protocolo de gerenciamento de certificado da RFC 2510, e ser autenticada via módulo criptográfico antes da ativação. As chaves desativadas devem ser eliminadas da memória e destruídas.

Tabela 5.22: Chave Pública

VeriSign	Nada consta
Entrust.NET	Nada consta
ICP - Brasil	A chave pública deverá ser entregue à AC pela AR ou usuário, utilizando formato compatível com padrão PKCs#1.

5.6 Hierarquia de ICP

Nesta seção do documento são descritos os serviços de certificação, os quais são implementados por uma infra-estrutura de chaves públicas, composta por entidades, tais como AC-raiz, ACs, ARs, repositórios, LCRs, formando uma hierarquia de ICP. Nota-se no decorrer desta seção, que a *Entrust* e a ICP-Brasil não falam sobre hierarquia de ICP, porém possuem várias entidades. A tabela 5.23 mostra que as ACs-Raízes são as entidades de mais alto nível de confiança em uma ICP.

Tabela 5.23: AC- Raiz - Autoridade Certificadora Raiz

VeriSign	A AC raiz é uma entidade operada e de propriedade da VeriSign, que emite certificados para chave pública de PACs.
Entrust.NET	Nada Consta
ICP - Brasil	A AC-raiz é responsável pela emissão e manutenção dos certificados das ACs integrantes da ICP-Brasil.

Quanto à AC intermediária, verifica-se que é uma entidade subordinada a uma AC-raiz. A tabela 5.24 mostra que são as ACs que realizam todo o gerenciamento de certificados, desde sua emissão até o seu vencimento ou revogação.

A tabela 5.25 mostra que as ARs são entidades subordinadas as ACs para executarem serviços pré-determinados pela AC. Nota-se que a entidade AR é parte integrante da AC.

Tabela 5.24: AC - Autoridade Certificadora

VeriSign	A AC é subordinada a uma PAC. A AC emite, gerencia e revoga certificados de assinantes/usuário final. A chave é de 1024 bits.
Entrust.NET	A AC emite, revoga e publica os certificados.
ICP - Brasil	São ACs de órgãos e entidades públicas e privadas licenciadas pela ICP à emitir e revogar certificados de usuários finais. A chave é de 2048 bits (RSA).

Tabela 5.25: AR - Autoridade de Registro

VeriSign	São entidades que avaliam e aprovam ou rejeitam as solicitações de certificados. Operam para uma única AC ou AE.
Entrust.NET	São entidades que recebem as solicitações de certificados e fazem a verificação das informações, dependendo do resultado da verificação envia ou não a solicitação para a AC.
ICP - Brasil	São responsáveis por receber as solicitações, confirmarem a identidade e também por revogarem certificados.

Quanto a AN - autoridade de nomeação, verifica-se que é uma entidade que gerencia a emissão de nomes para outras entidades, podendo ser usada também para usuários. A tabela 5.26 mostra que mesmo as ACs que não utilizam esta entidade, possuem regras de controle de emissão de nomes.

Tabela 5.26: AN - Autoridade de Nomeação

VeriSign	Controla a emissão de NRD - nomes relativos distintos para todas as AEs.
Entrust.NET	Não possuem AN, mas possuem regras para controlar a emissão de nomes.
ICP - Brasil	Não possuem AN, apenas propõe regras e procedimentos para emissão de nomes.

Os repositórios são conjuntos de dados que ficam a disposição do público para armazenar e recuperar certificados e outras informações relevantes. A tabela 5.27 mostra que a função dos repositórios é a mesma independente de AC.

A tabela 5.28 mostra que toda a AC deve publicar uma LCRs contendo as informações sobre os certificados que foram revogados.

Além destas entidades apresentadas no decorrer desta seção, a *VeriSign* apresenta as PACs - Principais Autoridades Certificados Públicas. Estas entidades são as de nível mais alto dos SCP, que emitem, revogam e suspendem certificados para e de todas as ACs.

Tabela 5.27: Repositórios

VeriSign	É um conjunto de dados a disposição do público para armazenar e recuperar certificados, DPCs, LCRs e outras informações relevantes.
Entrust.NET	Permitem o acesso a informações relacionadas aos certificados e a LCR, acessíveis através de uma interface <i>Web</i> .
ICP - Brasil	são diretórios ou páginas na <i>Web</i> para armazenar certificados, LCR, PC e outras informações relevantes.

Tabela 5.28: LCR - Lista de Certificados Revogados

VeriSign	São LCR publicadas pela AC, com as principais informações sobre os certificados.
Entrust.NET	Os campos: versão, assinatura, emissor, atualização, próxima atualização e certificados revogados são usados pela AC para publicar a LCRs.
ICP - Brasil	A AC deverá publicar a LCR no formato X.509v2* de acordo com o padrão PKIX.

5.7 Base de Operações de Certificados para ACs

Esta seção do documento é responsável pela descrição da base e dos controles das operações SCP, publicações em geral, tabeliães, pré-requisito para aprovação de AC, solicitação de AC, início das atividades de AC, encerramento de ACs, reemissão de certificados por outra AC e confiabilidade dos serviços.

Tabela 5.29: Publicações

VeriSign	As emendas de DPC, certificados, avisos de suspensão ou revogação são publicados nos repositórios pela AC. As informações podem ser publicadas a qualquer hora.
Entrust.NET	Todas as informações referentes a certificados, DPCs, LRCs e demais informações relevantes são publicadas periodicamente pela AC em repositórios.
ICP - Brasil	Todas as informações sobre certificados, PC e DRO, LCR serão publicadas diariamente pela AC em um repositório. Os certificados também serão publicados no Diário Oficial da União.

A tabela 5.29 mostra que as ACs publicam periodicamente, todas as informações referentes aos certificados, as DPCs e avisos gerais.

A tabela 5.30 mostra que as ACs podem usar tabeliães para confirmar as informações fornecidas pelo candidato ao certificado.

Quanto a AC, verifica-se que para a entidade ser aprovada é preciso cumprir pré-requisitos de segurança. A tabela 5.31 mostra que os pré-requisitos estabele-

Tabela 5.30: Tabeliões

VeriSign	Confirmam identidades de assinantes e reconhecem tipos de certificados e solicitações de AC não-VeriSign.
Entrust.NET	Não especifica na DPC apesar de usar para comprovação de informações.
ICP - Brasil	Nada Consta.

cidos pela AC-Raiz, variam de uma para outras, mas mantém a segurança como princípio das exigências.

Tabela 5.31: Pré-Requisito para Aprovação de AC

VeriSign	Deve-se seguir as exigências de controle, tais como: segurança, confirmação de identificação, etc
Entrust.NET	A Entrust deve continuar responsável pelo respectivo desempenho da AC.
ICP - Brasil	A própria AC gera o par de chaves e encaminha a cópia da chave pública em formato PKCs, por uma pessoa legalmente credenciada a AC-raiz

Quanto a solicitação de AC, verifica-se que varia de acordo com a classe do certificado a ser emitido pela AC. A tabela 5.32 mostra que a solicitação varia de uma entidade para outra.

Tabela 5.32: Solicitação de AC

VeriSign	Preencher a solicitação de AC de acordo com a classe do certificado a ser emitido, e ser reconhecida por um tabelião, devendo então ser enviada a PAC pertinente.
Entrust.NET	Os procedimentos são os mesmo para AC e usuários.
ICP - Brasil	A solicitação deve estar revestidas das formalidades legais, os nomes devem seguir o padrão ISO/IEC 9594(X.500) DN e ser enviada ao CG da ICP-Brasil.

A tabela 5.33 mostra como a *VeriSign* autoriza o início das atividades de uma AC.

A disponibilização dos certificados pela *VeriSign* é feita após a realização de uma cópia de segurança dos mesmos, conforme demonstrado na tabela 5.34.

De acordo com a tabela 5.35, as entidades necessitam revogar todos os seus certificados, entretanto cada uma utiliza uma forma de encerrar suas atividades.

A tabela 5.36 mostra que somente a *VeriSign* usa um sistema de emitir novamente um certificado.

Tabela 5.33: Aprovação para iniciar as atividades de AC

VeriSign	Após análise e investigação, a PAC deverá aprovar ou reprovar a solicitação. A aprovação dar-se-a através da assinatura do contrato e a emissão do certificado.
Entrust.NET	Nada Consta
ICP - Brasil	Nada Consta

Tabela 5.34: Disponibilidade dos Certificados de AE ou AC

VeriSign	As AEs devem fazer cópia de seus certificados e dos dados de revogação, colocando-os a disposição para verificação de assinaturas digitais.
Entrust.NET	Nada consta
ICP - Brasil	Nada Consta

Tabela 5.35: Encerramento ou Cessão das Operações da AE ou AC

VeriSign	Avisar com 90 dias de antecedência aos usuários e a AE superior sobre a cessação, efetuar transferência de responsabilidades para as entidades sucessoras, manutenção de registros.
Entrust.NET	Todos os certificados devem ser revogados
ICP - Brasil	Notificar os usuários imediatamente sobre a extinção da AC.

Tabela 5.36: Reemissão dos Certificados por 1 AE Sucessora

VeriSign	Os certificados de assinantes em circulação deverão ser reemitidos pela sucessora conforme acordo entre as AEs.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

Quanto a confiabilidade dos serviços de certificação, a tabela 5.37 mostra que todas as entidades utilizam mecanismos de segurança.

Tabela 5.37: Confiabilidade

VeriSign	As AEs, ARLs e repositórios devem usar sistemas confiáveis para desempenhar seus serviços.
Entrust.NET	Devem usar mecanismos confiáveis para desenvolver e garantir seus serviços.
ICP - Brasil	A AC deve adotar medidas de segurança e controle, manter processos, procedimentos e atividades que mantenham a segurança de seus serviços.

Além das informações descritas nesta seção, a *VeriSign* possui ainda o selo de data e hora que aumentam a integridade dos SCP e a dos certificados, contribuindo para o não-repúdio, criando uma notação que indica a data e a hora correta ou uma ação e a identidade da pessoas ou dispositivo criador da notação

5.8 Responsabilidades, Obrigações e Garantias

Os quadros abaixo comparam as responsabilidades, obrigações e garantias de ACs, ARs, usuários e de todas as demais partes envolvidas no processo. A tabela 5.38 mostra as responsabilidades financeiras das AEs ou ACs.

Tabela 5.38: Responsabilidades Financeiras

VeriSign	As AEs devem possuir recursos financeiros suficientes para manter suas operações e desempenhar suas obrigações, bem como arcar com os riscos mediante os assinantes e outras pessoas que confiem nos certificados e ainda possuir recursos para eventuais erros e omissões.
Entrust.NET	Os assinantes ou parceiros de confiança devem ser responsáveis pelas consequências financeiras diante de assinantes de certificados.
ICP - Brasil	É de responsabilidade das entidades arcar com custos de implementação, gerenciamento e manutenção de todos os processos e atividades inerentes e também para manter operações e arcar por erros e omissões.

A tabela 5.39 refere-se aos avisos e limitações de responsabilidades citadas no certificado, com referência para o texto completo.

Quanto ao reembolso, pode-se notar que, cada entidade trata o assunto de uma determinada forma. A tabela 5.40 mostra como as entidades comportam-se na

Tabela 5.39: Avisos, Limitações de Responsabilidades e Isenções de Garantias

VeriSign	Cada certificado possui uma breve declaração sobre as limitações aplicáveis e isenções de responsabilidades de garantias com indicadores para o texto completo.
Entrust.NET	Nada consta
ICP - Brasil	Nada Consta

questão financeira.

Tabela 5.40: Política de Reembolso

VeriSign	O assinante poderá solicitar revogação do certificado até 30 dias depois da emissão, após este período, poderá solicitar a revogação, mas o reembolso só será feito caso a AE viole alguma garantia.
Entrust	Não será fornecido reembolso por certificados e nem por serviços prestados.
ICP - Brasil	Nada Consta

A tabela 5.41 mostra que todas as entidades possuem basicamente as mesmas garantias de emissão, publicação de certificados, com pequenas variações de uma entidade para outra.

Tabela 5.41: Garantias Limitadas e Outras Obrigações de AEs e ACs

VeriSign	As AEs garantem e prometem que: emitirão, publicarão, suspenderão e revogarão certificados; realizarão procedimentos para validação de certificados; fornecerão controles para a ICP da VeriSign; cumprirão as cláusulas da DPC e serão responsáveis pelo vencimento, reinscrição e renovação de certificados.
Entrust.NET	Garantem aos assinantes fornecer serviços de repositório, emitir e revogar certificados, disponibilizar informações sobre os certificados em repositórios, emitir e publicar LCRs.
ICP - Brasil	As ACs sejam elas raízes ou não são responsáveis por todos os aspectos relacionados com a emissão e o gerenciamento de certificados, de acordo com as práticas e regras dispostas na DPC

Quanto as obrigações das ARs, a tabela 5.42 mostra que as funções são as mesmas, independente da entidade.

Quanto as obrigações dos usuários, a tabela 5.43 mostra que os usuários e parceiros de confiança devem cumprir as normas de uso do certificado, de acordo com a sua finalidade.

Tabela 5.42: Obrigações de ARs

VeriSign	Nada consta
Entmst.NET	Receber as candidaturas a certificados, verificar as informações contidas na candidatura, notificar o assinante sobre a emissão e sobre a revogação do certificado, etc.
ICP - Brasil	Receber as solicitações de certificados, verificar as informações da solicitação, informar o usuário sobre a emissão ou revogação do certificado, garantir a segurança da sua chave privada.

Tabela 5.43: Obrigações dos Usuários e Parceiros de Confiança

VeriSign	Nada consta
Entrust.NET	Fornecer informações corretas, usar os certificados somente para os fins válidos, proteger a chave privada, verificar a LCRs, interromper o uso do certificado quando estiver vencido, revogado, etc.
ICP - Brasil	O uso do certificado deve ser de forma apropriada, verificar a LCRs, as informações devem ser precisas e completas, proteger suas chaves.

A tabela 5.44 mostra que as ACs e ARs estão isentas de qualquer responsabilidade, exceto se disposto na DPC.

Tabela 5.44: Isenção de Responsabilidade e Limitações sobre as Obrigações das AEs e ACs

VeriSign	Exceto se disposto anteriormente nas sessões da DPC, ou vedado por lei, as AEs e AC-raiz se isentam das responsabilidades de todas as garantias e obrigações dispostas na DPC.
Entrust.NET	Exceto se disposto ao contrário na DPC, ninguém faz qualquer representações ou oferecem quaisquer garantias.
ICP - Brasil	Nada Consta

Quanto a limitações de perdas e danos, com exceção da ICP-Brasil, a tabela 5.45, mostra que as outras duas entidades, mantém recursos para eventuais despesas financeiras causadas por perdas e danos.

Tabela 5.45: Limitações de Perdas e Danos

VeriSign	As limitações serão de acordo com cada classe: classe 1 = US\$ 100,00; classe 2 = US\$ 5.000,00 e classe 3 = US\$ 100.000,00.
Entrust.NET	O valor máximo é de mil dólares americanos (US\$ 1.000,00) (máximo de danos cumulativos).
ICP - Brasil	Nada consta

Quanto a responsabilidade dos assinantes, pode-se notar que os mesmos possuem varias responsabilidades em comum. A tabela 5.46 mostra quais são as responsabilidades dos assinantes, perante cada entidade.

Tabela 5.46: Responsabilidades de assinantes

VeriSign	Os assinantes serão responsáveis por quaisquer informações falsas contidas nos certificados utilizados por terceiros que tenham confiado.
Entrust.NET	Os assinantes e parceiros de confiança serão responsáveis financeiramente por transações feitas utilizando os certificados pertencentes a si, deixando no entanto a <i>Entrust</i> isenta de qualquer responsabilidade.
ICP - Brasil	Nada consta

O USO de certificados digitais é proibido pelas ACs para atividades consideradas perigosas. A tabela 5.47 mostra quais são as atividades consideradas perigosas pelas ACs.

Tabela 5.47: Atividades Perigosas

VeriSign	Os certificados da <i>VeriSign</i> não podem ser usados em operações perigosas como: instalações nucleares, navegações aéreas, etc.
Entrust.NET	Os certificados não são elaborados, produzidos ou destinados ao uso ou em combinações com atividades de risco, que exijam desempenho sem falhas, tais como: operações nucleares, dispositivos médicos, etc
ICP - Brasil	Nada Consta.

Pode se notar através da tabela 5.48, que as ACs detém o direito de investigar compromissos relativos aos certificados emitidos.

Além do exposto acima, exceto se vedado por lei, sob nenhuma circunstância, uma AE ou AC-raiz será responsável por danos. As AEs subordinadas e a

Tabela 5.48: Direitos de Propriedade Intelectual

VeriSign	As AEs e a <i>VeriSign</i> podem investigar todos os compromissos permitidos por lei.
Entrust.NET	A <i>Entrust</i> detém todo o direito, titularidade e interesse em, para e sob todos os certificados <i>Entrust</i>.
ICP - Brasil	Nada Consta

VeriSign, são agentes fiduciários, credores ou representantes dos assinantes ou das partes confiantes.

5.9 Auditoria

Nesta seção estão sendo comparados como são realizados os processo de auditoria pelas ACs. A tabela 5.49 mostra como é determinado o processo de auditoria de uma AC.

Tabela 5.49: Auditoria

VeriSign	Implementar e manter sistemas confiáveis, a fim de preservar uma trilha de auditoria para todos os eventos materiais. A auditoria de AEs e ARLs deve ser executada por um profissional qualificado, uma vez ao ano.
Entrust.NET	São automaticamente marcados e registrados como protocolo de auditoria nos arquivos de rastreamento, possuindo um código de autenticação que impede a modificação do protocolo. Devem ser auditadas uma vez ao ano, por empresa de contabilidade pública e certificada, independente da empresa auditada.
ICP - Brasil	Verificar se todos os processos, procedimentos e atividades das ACs e ARs da ICP-Brasil estão em conformidade com a DRO e a PC. A AC deve garantir que seus registros serão analisados diariamente pelas pessoas responsáveis e explicados em um relatório de auditoria de registro. A proteção destes registros devem incluir mecanismos contra leituras, modificações e remoção não autorizada.

Quanto a programação de retenção de registros, a tabela 5.50 mostra como as entidades implementam a retenção dos registros.

A tabela 5.51 mostra como as ACs mantêm os registros e quando elas podem fornecer estes registros.

Tabela 5.50: Programação de Retenção de Registro

VeriSign	A retenção depende da classe do certificado. Para classe 1 e 2, mínimo de 5 anos e a classe 3, pelo menos 30 anos.
Entrust.NET	A retenção de registros deve ser de pelo menos 3 anos.
ICP - Brasil	Deverá manter seus registros localmente por 2 meses e então transferi-los para local específico e retido pelo menos por 6 anos.

Tabela 5.51: Registro de Conformidade

VeriSign	As AEs devem colocar os registros à disposição da <i>VeriSign</i> , mediante solicitação.
Entrust.NET	São banco de dados armazenados em locais seguros.
ICP - Brasil	Devem registrar em arquivos de registros de auditoria todos os eventos de segurança de certificados.

5.10 Segurança

Os quadros abaixo fazem uma comparação entre os diversos itens de segurança implementados pelas ACs e AR, para garantir a integridade de seus certificados. A tabela 5.52 mostra como as ACs garante, a segurança de seus serviços em caso de um desastre.

Tabela 5.52: Planejamento de Contingência e Recuperação de Desastre

VeriSign	As AEs devem implementar, documentar e testar os recursos e procedimentos de recuperação de desastres.
Entrust.NET	Possuir um plano de recuperação de desastre que permita a recuperação dos serviços. A <i>Entrust</i> exige controles de segurança rigorosos para manter a integridade da AC.
ICP - Brasil	A AC deve estabelecer um plano de contingência que estabeleça os passos a serem tomados em caso de corrupção ou perda dos recursos computacionais, dos aplicativos e/ou dados.

Quanto aos serviços de segurança utilizados pelas ACs, pode-se notar que eles podem ser iguais ou não. A tabela 5.53 mostra quais os serviços utilizados pelas ACs, citadas na comparação.

A tabela 5.54 mostra o que a entidade pode oferecer ao assinante, como proteção para o seu certificado e sua chave.

As instalações devem ser adequadas para a segurança da estrutura das ACs. Nota-se que as ACs utilizam diferentes tipos de segurança para garantir a integridade

Tabela 5.53: Serviços de Segurança

VeriSign	Supportam mecanismos de segurança para proteger a comunicação e as informações. Utiliza sistema de chave pública da RSA e também suporta outros padrões.
Entrust.NET	Usa a premiada família de produtos de <i>softwaresEntrust/PKI</i> da <i>Entrust Technologies</i> .
ICP - Brasil	A AC deve utilizar SW projetados e desenvolvidos através de metodologia rigorosa e específica para ambientes de segurança.

Tabela 5.54: Plano de Proteção

VeriSign	A <i>VeriSign</i> oferece o plano de proteção de chaves para o assinante, o <i>NetSure</i> .
Entrust.NET	Oferece os recursos de segurança do <i>Secure Exchange Protocol</i> e <i>Software Entrust/Session</i> .
ICP - Brasil	Nada consta

das suas instalações. A tabela 5.55 mostra como as ACs garantem a segurança da sua estrutura física.

Tabela 5.55: Instalações

VeriSign	Devem ser confiáveis e estarem em conformidade com a PSV ou equivalente.
Entrust.NET	O SW e HW de uma AC devem ser alocados em instalações seguras, com procedimentos de controle de acesso e segurança física. O local onde detém o SW é designado área de duas pessoas.
ICP - Brasil	O local deve ser publicamente identificado, o acesso físico deve ser controlado por sistemas de segurança, cartões/chaves de acesso deverão implantados, energia elétrica e outros.

Quanto a proteção do *hardware*, nota-se que para cada classe de certificado as ACs possuem um esquema de proteção. A tabela 5.56 mostra como as ACs fazem a proteção de seus equipamentos de *hardware*.

A escolha de métodos criptográficos pelo assinante, como mostra a tabela 5.57 é livre, a AC não interfere.

Além dos itens acima citados de segurança, a ICP-Brasil sugere a utilização de mais um controle de gerenciamento de segurança, uma metodologia formal de gerenciamento de configurações, deverá ser usadas para a instalação e manutenção contínua do sistema de AE em todos os níveis.

A *VeriSign* também utiliza aplicativos que oferecem mecanismos de

Tabela 5.56: Proteção de *Hardware*

VeriSign	O uso de módulos criptográficos aprovados e confiáveis de HW para todas as operações que usem a chave privada.
Entrust.NET	O HW é certificado com o nível 3 do FIPs 140-1 [FIP].
ICP - Brasil	Para proteger-se de qualquer ataque via rede, deverá ser instalado um dispositivo que permitir comandos e protocolos só da AC, os módulos criptográficos serão definidos pela CG da ICP - Brasil. A AC-Raiz deverá usar componente seguros de HW, à prova de violação para a geração de chaves e de certificados.

Tabela 5.57: Escolha de Métodos Criptográficos

VeriSign	O assinante escolhe o SW, HW e o algoritmos.
Entrust.NET	Nada Consta
ICP - Brasil	A ser definido

segurança, adequados para a comunicação de certificados.

5.11 Funcionários

Os quadros abaixo fazem uma comparação de como conduzir e gerenciar o pessoal responsável pelo processo de certificação e pelas entidades. A tabela 5.58 mostra que as ACs devem elaborar um plano de prática e de gerenciamento do seu pessoal, a fim de garantir a das pessoas que trabalham nas ACs.

Tabela 5.58: Gerenciamento e Prática Pessoal

VeriSign	As AEs devem elaborar práticas e gerenciamentos de pessoal, a fim de garantir a confiança de seus serviços.
Entrust.NET	O pessoal responsável pela operação de uma AC não recebe outra responsabilidade, que possam entrar em colisão com as respectivas responsabilidades operacionais junto a AC.
ICP - Brasil	A AC deve separar tarefas para funções críticas. Cada usuário do sistema de acesso será limitado somente a ações às quais foi designado.

Os cargos de confiança, referem-se a todas as pessoas que possuem acesso a operações criptográficas. A tabela 5.59 mostra como são definidos os cargos de confiança.

Quanto a investigação e a conformidade dos funcionários, nota-se que

Tabela 5.59: Cargo de Confiança

VeriSign	Todas as pessoas que tenham acesso a operações criptográficas ou de controle sobre elas e acesso as operações restritas do repositório, devem ser considerados cargos de confiança. As equipes de atendimento também possuem cargo de confiança.
Entrust.NET	Nada consta
ICP - Brasil	Os cargos de confiança são definidos de acordo com o níveis do certificado e de sigilo, as atuações são definidas de acordo com o cargo.

é extremamente necessário saber a procedência das pessoas. A tabela 5.60 mostra que as ACs fazem algum tipo de investigação, antes de efetuarem a contratação de um funcionário, principalmente se for para um cargo de confiança.

Tabela 5.60: Investigação e Conformidade

VeriSign	Todos os candidatos a cargos de confiança devem ser submetidos a investigação inicial e pós contrato, devem também serem realizadas investigações periódicas.
Entrust.NET	Todas as pessoas que trabalham em operações são submetidas a investigações.
ICP - Brasil	Todos os funcionários devem ter sua identidade e autorização antes de serem inseridos nos processos da AC e AR.

A tabela 5.61, mostra que os que não forão aprovados na investigação devem ser imediatamente afastados.

Tabela 5.61: Afastamento de Pessoas que Ocupam Cargos de Confiança

VeriSign	Os funcionários que não passarem na investigação inicial ou periódica devem ser afastados.
Entrust.NET	Nada consta
ICP - Brasil	A suspensão ocorrerá em caso real ou suspeita, caso a pessoa cometa ação não autorizada.

Os funcionários que ocupam cargos de confiança devem passar por qualificações adequadas, conforme o que demonstra a tabela 5.62.

Tabela 5.62: Funcionários Com Cargos de Confiança

VeriSign	Devem ser qualificados por uma organização externa reconhecida de qualificações.
Entrust.NET	Nada consta
ICP - Brasil	Devem receber treinamento em nível de domínio, tais como: princípios e mecanismos de segurança, versões de SW, etc., devendo haver reciclagem periódica e revisão dos requisitos uma vez a cada ano.

5.12 Detentores de Partes Secretas

Os detentores de partes secretas são entidades, que detém uma cópia da chave privada em segurança, caso ocorrer um desastre com a chave original. Porém estas entidades, devem seguir as normas disposta na DPC. A tabela 5.63 apresenta o funcionamento dos detentores das partes secretas.

Tabela 5.63: Detentores de Partes Secretas - Compartilhamento de Segredos

VeriSign	A AE devem utilizar o compartilhamento de segredos, através de detentores de partes secretas para aumentar a e recuperação de suas chaves. Os detentores possuem responsabilidades e obrigações de manter no mais absoluto sigilo a cópia da chave privada. Para isto, devem utilizar sistemas confiáveis de segurança, que não permitam a quebra do sigilo, danos, divulgação, cópias, etc. Os detentores devem manter registros de suas atividades. No entanto a detentora de partes secretas só aceita guarda-la se forem observadas a criação, e distribuição da mesma.
Entrust.NET	Em nem um momento a Entrust manifesta-se sobre algum tipo de detentor de partes secretas.
ICP - Brasil	Em nem um momento a ICP-Brasil manifesta-se sobre algum tipo de detentor de partes secretas..

5.13 Solicitação de Certificados

Os quadros a seguir fazem uma comparação dos processos de solicitação de certificados. A tabela 5.64 mostra como o candidato deverá proceder para realizar a solicitação de um certificado.

A tabela 5.65 mostra que algumas das informações solicitadas para a certificação são comuns entre as ACs e entre as classes dos certificados, entretanto para cada classe são solicitadas algumas informações específicas.

Tabela 5.64: Procedimentos para Solicitação de Certificados

VeriSign	Gerar um par de chaves e demonstrar à AE que ele funciona, determinar um nome distinto e enviar a solicitação anexando a chave pública.
Entrust.NET	Gerar um par de chaves, aceitar os termos da DPC, preencher e submeter a candidatura.
ICP - Brasil	Provar a identidade, comprovação dos atributos de identificação, assinar acordo dispondo dos termos e condições aplicados ao uso do certificado e notificação de reconhecimento, no caso de funcionários ou servidor.

Tabela 5.65: Informações e Comunicações da Solicitação de Certificados

VeriSign	As informações necessárias para solicitação de certificados, depende da classe do mesmo, sendo que algumas são comuns, tais como: nome, endereço eletrônico, informações do cartão de crédito, par de chaves, etc.
Entrust.NET	Tanto quando aceitas ou rejeitadas, as solicitações serão comunicadas ao assinante.
ICP - Brasil	Nada Consta

5.14 Validação de Solicitação de Certificados

Os quadros a seguir apresentam as exigências para a validação das solicitações de certificados, executadas por ACs ou por ARs. A tabela 5.66 mostra as exigências necessárias para validar a solicitação de certificação.

Tabela 5.66: Exigência para a validação de solicitação de certificado

VeriSign	Validações obrigatórias são executadas, tais como: o candidato é a pessoa identificada no pedido, detém a chave privada correspondente a pública, as informações são precisas, os agentes estão autorizados a fazer o pedido.
Entrust.NET	Que todas as informações sejam verdadeiras e comprometam-se a aceitar os termos e condições da DPC.
ICP - Brasil	Nada consta

Quanto aos itens a serem confirmados, a tabela 5.67 mostra que para cada classe, usa-se uma estratégia de confirmação das informações.

A tabela 5.68 mostra como a AC procede para aprovar a solicitação de certificação.

Tabela 5.67: ítems a serem Confirmados

VeriSign	As informações são confirmadas de acordo com a classe do certificado, tais como: deverá haver o comparecimento pessoal; comparação de dados pessoais por terceiros (BD) <i>on-line</i> ; confirmação de informações sobre entidades de negócios por terceiros (bancos, governo, etc); endereço postal (carta de corroboração com número de identificação pessoal); nome de domínio (<i>InterNIC</i>) e atribuição do número de série, etc
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

Tabela 5.68: Aprovação de solicitação de certificados de classe 1 ou 3

VeriSign	Após todas as informações confirmadas, a AE aprova a solicitação, e demonstra a aprovação com a emissão do certificado. Em relação a classe 2, a aprovação é provisória por dois meses, após passa a ser definitiva.
Entrust.NET	Após todas as informações confirmadas aprova e solicita a emissão, porém não possui classes de certificados.
ICP - Brasil	Nada Consta

A tabela 5.69 mostra quando e porque uma AC rejeita uma solicitação de certificação.

Tabela 5.69: Rejeição de solicitação de certificados

VeriSign	Caso não ocorra a validação, a AE deve rejeitar a solicitação e notificar a falha ao candidato. Se a controvérsia ocorrer em relação ao BD de terceiros, a AE deve fornecer ao candidato, informações de contato com o BD, para investigação.
Entrust.NET	Havendo rejeição a AR deverá utilizar esforços comercialmente válidos para notificar ao requerente os motivos do indeferimento.
ICP - Brasil	Nada consta

5.15 Emissão de Certificados

Os quadros a seguir comparam as exigências feitas pelas ACs para a emissão de certificados. A tabela 5.70 apresenta as etapas comprovadas para a emissão do certificado.

O consentimento do assinante para a emissão do certificado varia de uma AC para outra. A tabela 5.71 mostra quando o assinante consente a emissão do

Tabela 5.70: Certificados Normais e Provisórios

VeriSign	Comprovação da aprovação final da AE. No caso de certificados provisórios, estes passam a ser fixos, após dois meses de emissão
Entrust.NET	A emissão e a publicação do certificado, indicam aprovação e validação em todas as etapas do processo de certificação.
ICP - Brasil	Nada consta

certificado requerido.

Tabela 5.71: Consentimento do Assinante para Emissão do Certificado

VeriSign	Considera-se consentimento para a emissão a própria solicitação.
Entrust.NET	Nada consta
ICP - Brasil	A AC deve exigir que o requerente reconheça a aceitação do certificado.

A tabela 5.72 mostra que uma AC poderá recusar-se a emitir um determinado certificado, porém deverá restituir o assinante. No entanto, se houver alguma fi-aude a AC ficará isenta de reembolsar o assinante.

Tabela 5.72: Recusa quanto à emissão de um certificado

VeriSign	Caso haja recusa na emissão, a AC deverá reembolsar imediatamente o candidato, exceto se houver informações fraudulentas.
Entrust.NET	Deverá reembolsar imediatamente todos os valores pagos pelo candidato.
ICP - Brasil	

A tabela 5.73 mostra que somente a *VeriSign* relata a obrigação de garantir a veracidade das informações no ato de transferi-las para o certificado.

Quanto ao tempo transcorrido para emissão, a tabela 5.74 mostra que o tempo de emissão varia de uma classe para outra.

Quanto a validade dos certificados, nota-se que cada classe possui uma validade. A tabela 5.75 mostra como a AC determina a validade de cada certificado.

Tabela 5.73: Representações da AE ou AC Mediante a Emissão do Certificado

VeriSign	Perante assinantes; não há falhas de representações de fatos no certificado; não há erros de transcrições dos dados enviados a AE; atende a todas as exigências materiais da DPC. Perante partes confiantes; as informações contidas ou incorporadas por referência ao certificado são precisas.
Entrust.NET	Nada consta.
ICP - Brasil	Nada Consta.

Tabela 5.74: Tempo para Emissão de Certificados

VeriSign	Após todas as informações verificadas, o tempo de emissão varia de acordo com a classe do certificado. Classe 1 = 2 horas; classe 2 = 1 dia útil e classe 3 = 1 a 5 dias úteis.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

Tabela 5.75: Períodos de Validade dos Certificados

VeriSign	A validade depende da classe do certificado, começando na data e hora da emissão.
Entrust.NET	Deve conter uma data de vencimento.
ICP - Brasil	Nada Consta

5.16 Aceitação de Certificados por Assinantes

Os quadros a seguir apresentam e comparam as exigências para a aceitação de certificados por assinantes, representações, obrigações dos assinantes. Através da tabela 5.76, percebe-se como é realizada a aceitação de certificados.

Tabela 5.76: Aceitação de Certificados

VeriSign	Considera-se aceito o certificado , após o envio da solicitação, por correio eletrônico ou <i>on-line</i> (Internet).
Entrust.NET	Assim que o certificado for inserido em um repositório, a AR deverá avisar ao requerente por correio eletrônico, neste contem um URL para ser baixado o certificado.
ICP - Brasil	O usuário deverá reconhecer a aceitação perante a AC.

A tabela 5.77 mostra quais são as representações dos assinantes perante a aceitação do certificado emitido.

Tabela 5.77: Representações dos Assinantes Mediante Aceitação

VeriSign	Informações verdadeiras, uso não indevido, ser um assinante e não uma AC, proteger a chave privada, etc.
Entrust.NET	Informações corretas, uso exclusivo para o seu fim, proteger a chave privada, não realizar operações arriscadas, etc.
ICP - Brasil	Nada Consta

Quanto a indenização por parte do assinante, nota-se que o mesmo deverá indenizar a emitente, sempre que cometer uma infração. A tabela 5.78 mostra os atos que se o assinante cometer terá que pagar indenização.

Tabela 5.78: Indenização por Parte do Assinante

VeriSign	Indenizar e isentar a AE, por qualquer ato, ação, etc causados por displicência do assinante.
Entrust.NET	Indenizar e isentar a AC de todas e quaisquer responsabilidades, perdas, danos, etc. causados por displicência de assinantes.
ICP - Brasil	Nada Consta

A tabela 5.79 mostra que as ACs devem publicar os certificados emitidos logo após a sua emissão. Além da publicação no repositório, a ICP-Brasil recomenda a publicação no Diário Oficial da União.

Tabela 5.79: Publicações

VeriSign	Ao ser emitido um certificado, a AE deverá publica-lo no repositório da <i>VeriSign</i> e em outros.
Entrust.NET	Ao ser emitido o certificado, este já é publicado <u>no repositório</u> .
ICP - Brasil	Serão publicados no Diário Oficial da União, em diretórios ou páginas <i>Web</i> da ICP-Brasil.

5.17 Uso de Certificados

Os quadros a seguir fazem uma comparação das verificações, procedimentos em caso de falha e confiança em assinaturas. A tabela 5.80 mostra como as ACs fazem a verificação da assinatura digital.

Tabela 5.80: Verificação de Assinaturas Digitais

VeriSign	Determina se a assinatura foi criada corretamente e se a mensagem não foi alterada. A verificação dar-se-a da seguinte forma: estabelecimento e confirmação de uma cadeia de certificados para a assinatura digital; garantia de que a cadeia encontra é a mais adequada para a assinatura, indicação de hora e data de criação da assinatura digital, definição das garantias desejadas pelo signatário, etc..
Entrust.NET	As ARs aplicam testes de prova de posse de CSRs usando algoritmos assimétricos reversíveis (com RSA).
ICP - Brasil	A AC ou AR deve verificar se as chaves são correspondentes, usando o protocolo de transferência descrito na RFC 2510.

A tabela 5.81 mostra que as mensagens assinadas digitalmente, possuem o mesmo valor das mensagens escritas e assinadas fisicamente em papel.

Além das verificações das assinaturas, para garantir a validade, a *VeriSign* alerta aos usuários que ao utilizarem um certificado com falhas ou vencido, perderão todo e qualquer direito. A decisão final de confiar ou não em um certificado comprometido, fica a critério do usuário.

Tabela 5.81: Escritas e Assinaturas

VeriSign	As mensagens com assinatura digital possuem o mesmo valor das escritas e assinadas em papel. As assinaturas digitais possuem o mesmo valor de assinaturas em papel, desde que possam ser verificadas por referência a chave pública.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

5.18 Suspensão e Revogação de Certificados

Os quadros abaixo fazem uma comparação das circunstâncias sob as quais um certificado poderá ser revogado ou suspenso. A tabela 5.82 mostra quais são as condições para que ocorra a suspensão ou revogação do certificado.

Tabela 5.82: Motivos Gerais para Suspensão ou Revogação

VeriSign	Caso a chave for perdida, roubada, modificada, comprometida, violação de uma obrigação material pelo sujeito, desastre natural, etc.
Entrust.NET	Comprometimento da chave privada da AC ou do assinante, ruptura de termos da DPC ou de acordo, modificações de informações do certificado, falta de pagamento de tarifas e taxas, etc.
ICP - Brasil	Quando informações constantes no certificado forem alteradas, comprometimento da chave privada ou sua mídia, o não cumprimento da legislação vigente, de políticas, normas e regras, por parte do assinante.

Quanto a revogação de certificados de AE ou ACs, nota-se que as condições são iguais para usuário e ACs ou AEs. A tabela 5.83 mostra quais são os motivos para que um certificado de AE ou AC seja revogado.

Tabela 5.83: Suspensão ou Revogação de um Certificado de AE

VeriSign	Caso um fato material representado no certificado for falso, um pré-requisito não for satisfatório, a chave privada da AE ou o sistema de estiver comprometido, o sujeito (AE) violar uma obrigação material, etc.
Entrust.NET	Sempre que houver algo que comprometa a sua .
ICP - Brasil	Quando qualquer informação constante no certificado for alterada, comprometimento da chave privada ou da sua mídia, o não cumprimento de regras, políticas, normas, práticas e legislação vigente.

A tabela 5.84 mostra que caso ocorra um equívoco ou os motivos forem falsos, o ato de suspensão será cancelado.

Tabela 5.84: Cancelamento da Suspensão de um Certificado de AE

VeriSign	Quando houver equívoco, a suspensão for feita sem autorização da AC suspensa ou quando os motivos forem infundados.
----------	--

A tabela 5.85 mostra que as ACs devem publicar imediatamente a suspensão ou revogação de um certificado em LCRs, repositórios, e avisar o assinante.

Tabela 5.85: Aviso e Confirmação Mediante Suspensão ou Revogação

VeriSign	Deve-se publicar notas no repositório, no LCR e avisar o assinante.
Entrust.NET	Imediatamente após a revogação, deve-se anunciar o número de série de cada certificado na LCR, no repositório e avisar o assinante, via correio eletrônico.
ICP - Brasil	Devem ser emitidas e publicados as LCRs com referência a mesma.

A tabela 5.86 mostra que as atividades do certificado são imediatamente suspensas, e a validade é encerrada.

Tabela 5.86: Efeitos da Suspensão ou Revogação sobre Certificados e Obrigações Subjacentes

VeriSign	O prazo de validade é considerado finalizado. Os certificados emitidos para assinantes antes da finalização do prazo do certificado da AE, continuam válidos. As obrigações subjacentes não serão afetadas.
Entrust.NET	Nada Consta
ICP - Brasil	Nada Consta

A tabela 5.87 mostra que mesmo após a suspensão ou revogação do certificado, as chaves devem ser protegidas até a sua destruição.

Além dos motivos gerais citados para realizar a suspensão ou revogação, a *VeriSign* também realiza suspensão de certificados tanto de AC, AE ou usuário perante uma solicitação do proprietário, devidamente comprovada a autenticidade da solicitação. Quando ocorrer emissão de certificado com falhas, os mesmos serão revogados imediatamente.

Obs; nem a *Entrust* nem a ICP-Brasil implementam suspensão de certificados.

Tabela 5.87: Proteção das Chaves Privadas Mediante Solicitação ou Revogação

VeriSign	As chaves devem ser protegidas pelo assinante até a sua destruição.
Entrust.NET	Nada Consta
ICP - Brasil	Após o seu vencimento devem ser destruídas.

5.19 Vencimento do Certificado

Os quadros a seguir comparam como as ACs agem em relação ao vencimento de um certificado, aos avisos, efeitos e a renovação e reinscrição do certificado do assinante. A Tabela 5.88 mostra como a AE comunica o assinante sobre o vencimento do certificado.

Tabela 5.88: Aviso antes do Vencimento

VeriSign	As AEs notificam os assinantes, via correio eletrônico sobre o vencimento.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

Quanto a renovação e reinscrição do assinante, nota-se através da tabela 5.89 que o processo é igual ao inicial.

Tabela 5.89: Renovação e Reinscrição do Assinante

VeriSign	O processo é igual ao inicial, de acordo com a classe do certificado.
Entrust.NET	O processo é igual ao inicial.
ICP - Brasil	Nada consta

Além das obrigações da AC de avisar o assinante sobre o vencimento de um certificado, observa-se que as obrigações do assinante não são afetadas com o vencimento do mesmo.

5.20 Disposições Gerais

Os quadros a seguir comparam como as ACs resolvem eventuais problemas em relação as DPCs, leis, taxas e outros itens relacionado ao funcionamento e

emissão de certificados. A tabela 5.90 mostra como as ACs resolvem conflitos de não entendimento do conteúdo da DPC.

Tabela 5.90: Interpretação e Tradução

VeriSign	Caso ocorra conflitos entre as versões da DPC em inglês e outros idiomas, prevalecerá a versão em inglês.
Entrust.NET	Os pronomes neutros e as suas variações devem ser interpretados como abrangendo as formas femininas e masculinas; todos termos utilizados no singular devem ser interpretados como incluindo o plural, e vice-versa.
ICP - Brasil	Em qualquer circunstâncias valerá a PC.

Quanto ao conflito de cláusulas, percebe-se que as ACs possuem procedimentos semelhantes. A tabela 5.91 mostra que a DPC sempre terá valor absoluto.

Tabela 5.91: Conflito de Cláusulas

VeriSign	Havendo conflitos entre esta DPC e outras regras, diretrizes ou contratos, o assinante ficará sujeito a esta DPC.
Entrust.NET	Havendo conflitos entre as provisões desta DPC e outros acordos escritos e expressos, o acordo terá a procedência. No caso de inconsistência entre as provisões da DPC e acordos, as condições e os termos da DPC serão válidos.
ICP - Brasil	Independente de contrato ou outras opções, a PC valerá sempre.

Quanto a avisos relacionado a DPC, nota-se que as ACs devem comunicar aos assinantes qualquer tipo de aviso sobre a DPC e sempre que houve ruma solicitação de alguma informações, a AC deverá responder ao requerente, utilizando um meio seguro de comimicação. A tabela 5.92 mostra quais são os meios utilizados pela AC para comunicar os avisos.

A tabela 5.93 mostra que as ACs para exportarem certificados devem estar em conformidade com as normas e leis de exportação.

Quanto as leis aplicáveis na certificação, nota-se que há diferença nas exigências das ACs. A tabela 5.94 mostra que as AC consideram as leis de cada país, com exceção da *Entrust* que segue as leis de Ontário e proíbe a aplicação da concessão das Nações Unidas.

Tabela 5.92: Avisos

VeriSign	Os avisos, informações ou solicitações em relação a DPC, devem ser feitas através de mensagens com assinatura digital. As mensagens eletrônicas só serão validas após o remetente receber do destinatário a confirmação.
Entrust.NET	Qualquer aviso sobre a DPC ou acordo feito por assinantes ou parceiros de confiança, deve ser por correspondência registrada, fax-símile ou courier noturno, todos entram vigor no dia útil seguinte, exceto a correspondência registrada, que entra em vigor em 5 dias.
ICP - Brasil	Toda e qualquer alteração nesta PC o CG da ICP-Brasil deverá comunicar as ACs integrantes da ICP e demais ACs com as quais a AC-raiz possui acordos, por escrito em papel.

Tabela 5.93: Conformidade com Normas e Leis de Exportação

VeriSign	Para exportação de certificados de <i>software</i> , as partes devem obedecer as normas e leis de exportação aplicadas.
Entrust.NET	Os certificados e as informações relacionadas podem estar sujeitas as restrições de exportação, importação e/ou uso.
ICP - Brasil	Nada consta

Tabela 5.94: Lei Aplicável

VeriSign	Caso inexistam leis no país, serão aplicadas as leis do Estado da Califórnia (EUA).
Entrust.NET	Serão aplicadas as leis da província de Ontário, Canadá. Fica expressamente proibida a aplicação da convenção das Nações Unidas em contratos para o comércio internacional de mercadorias.
ICP - Brasil	As leis do Brasil devem regular toda e qualquer operação de certificação.

A tabela 5.95 mostra que as ACs são livre para estabelecer as taxas a serem cobradas por seus serviços de certificação.

Tabela 5.95: Taxas

VeriSign	As taxas estão disponíveis no repositório e são passíveis de mudanças.
Entrust.NET	As taxas estão estabelecidas/disponíveis no repositório, sujeitas a modificações.
ICP - Brasil	As taxas deverão ser definidas de acordo com as regras estipuladas pela ICP-Brasil.

A tabela 5.96 mostra que as ACs não se responsabilizam por danos causados por força maior, exemplo: terremotos, guerras, etc.

Tabela 5.96: Força Maior

VeriSign	A VeriSign não se responsabiliza por danos causados por força maior.
Entrust.NET	A Entrust não se responsabiliza por danos causados por força maior.
ICP - Brasil	Nada consta

A tabela 5.97 mostra que a aprovação de HW e SW depende da aprovação de um consultor.

Tabela 5.97: Aprovação de *Software e Hardware*

VeriSign	Todos os dispositivos de HW e SW relacionados aos SCP devem ser aprovados pela VeriSign, por um consultor ou autoridade reconhecida.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

Além das informações sobre a DPC, comparadas na seção 5.20, a *VeriSign* considera os anexos da DPC como parte integrante da mesma.

5.20.1 Resolução de Controvérsias, Escolha do foro e Pressupostos

Esta seção compara como as ACs resolvem as possíveis controvérsias que venham a ocorrer entre as partes envolvidas na certificação. A tabela 5.98 mostra

como o reclamante deverá proceder mediante uma controvérsia e a quem recorrer.

Tabela 5.98: Notificação de Controvérsia entre as Partes

VeriSign	Tratando-se de controvérsia envolvendo a DPC ou o certificado, deve-se notificar a VeriSign, a AE pertinente e qualquer outra parte visando resolvê-la.
Entrust.NET	Devem ser submetidas a mediação de acordo com as normas de mediação comerciais da <i>American Arbitration Association</i> , ocorrendo no idioma inglês de Ottawa, Ontario.
ICP - Brasil	Controvérsias que envolvam a PC ou certificado deve-se notificar a AC pertinente.

A tabela 5.99 mostra que quando não houver resolução da controvérsia em um determinado tempo, o reclamante poderá recorrer a outros meios, de acordo com a AC.

Tabela 5.99: Resolução Formal de Controvérsias

VeriSign	Depois que o conselho de especialistas divulgar ou não a resolução, o lesado poderá recorrer a outros mecanismos.
Entrust.NET	Não havendo uma solução em 30 dias, a contestação será submetida à arbitragem obrigatória, que deverá apresentar uma decisão por escrito em 30 dias.
TCP - Brasil	A não resolução da controvérsia em 15 dias, acarretará o envio por escrito ou por formulário eletrônico para a ICP-Brasil, por uma das partes, solicitando a avaliação do caso, a comunicação do caso deverá sair em 3 semanas.

A tabela 5.100 mostra que a VeriSign exige que os sucessores ou cessionários assumam as obrigações e deveres dos envolvidos na certificação.

Tabela 5.100: Sucessores e Cessionários

VeriSign	Obriga todos os sucessores e cessionários de forma expressa, implícita ou aparente a assumirem as obrigações e deveres dos envolvidos na certificação.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

A tabela 5.101 mostra que as ACs ou AEs não podem ser modificadas ou alteradas sem antes ocorrer acordos entre as partes.

Além das formas de resolver controvérsias comparadas nos quadros acima, a VeriSign possui um conselho de especialistas para resolver as controvérsias.

Tabela 5.101: Fusão

VeriSign	Nenhum termo ou cláusula desta DPC afeta os direitos e obrigações da <i>VeriSign</i> e nenhuma AE pode ser emendada, renunciada, complementada oralmente.
Entrust.NET	Os direitos e obrigações não devem ser alterados porque quaisquer acordos anteriores, comunicações ou entendimentos de quaisquer natureza, quer verbalizados ou por escrito.
ICP - Brasil	Nada consta.

5.20.2 Emendas da DPC

Esta seção compara como as ACs realizam as correções necessárias em suas DPCs, como estas emendas são identificadas, aprovadas, etc. A tabela 5.102 mostra que as ACs reservam o direito de efetuar as emendas e sempre que necessário.

Tabela 5.102: Disposições Gerais Sobre Emendas

VeriSign	A <i>VeriSign</i> reserva o direito de efetuar emendas de tempos em tempos e publica-las no repositório e em seção de <i>Practices Updates and Notices</i> .
Entrust.NET	Caso a <i>Entrust</i> julgue necessário modificar regularmente a DPC e os termos e condições da DPC, poderá fazê-lo, porém não há mudança de versão. As alterações de maior impacto entram em vigor após 15 (quinze) dias da publicação. A mudança de versão ocorrerá, quando haver mudanças significativas.
ICP - Brasil	Nada consta

A tabela 5.103 mostra quais os tipos de ementas elaboradas e o prazo para cada uma entrar em vigor.

Tabela 5.103: Tipos de Emendas de DPCs

VeriSign	Seção " <i>Practices updates and notices</i> " - emendas que substituem cláusulas conflitantes. Emendas Materiais - Entram em vigor 15 (quinze) dias após a publicação. Emendas não materiais - entram em vigor imediatamente após sua publicação.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta.

A tabela 5.104 mostra que caso o assinante não se-manifeste em relação a emenda da DPC, constituir-se-a como aceita.

A tabela 5.105 mostra que mesmo após o término da validade da DPC, algumas seções continuam válidas.

Tabela 5.104: Aprovação das Emendas

VeriSign	Se não houver manifestação de revogação de certificado num prazo de 15 dias após a publicação de emendas, constitui-se aceitação da mesma.
Entrust.NET	Caso o assinante não fizer manifestação de revogação este será considerado como aceito.
ICP - Brasil	Nada consta

Tabela 5.105: Validade após o Término da DPC

VeriSign	Algumas sessões devem permanecer validas mesmo após o fim de sua validade.
Entrust.NET	Nada consta
ICP - Brasil	Nada consta

5.21 conclusão

A comparação realizada das DPCs neste capítulo, forneceu conhecimentos necessários do conteúdo e das formas como as ACs devem agir nos processos de certificação e também da elaboração de DPCs. A comparação mostra que há várias diferenças e semelhanças entre as DPCs das ACs. A comparação realizada forneceu muitos subsídios para a elaboração da DPC para a UFSC, descrita no capítulo 6, desta dissertação.

Capítulo 6

Estrutura da ICP da UFSC

6.1 Introdução

Este capítulo apresenta a infra-estrutura da ICP da UFSC, os componentes que formam a ICP e a estrutura da autoridade certificadora da UFSC. Os componentes descritos a seguir, realizam todo o processo de certificação da UFSC.

Este capítulo está dividido da seguinte forma; na seção 6.2 apresenta-se os componentes da ICP da UFSC; na seção 6.3 apresenta-se a AC-Raiz da UFSC; a seção 6.4 apresenta a AC emissora de certificados para usuários finais; a seção 6.5 apresenta a AR para conferência de informações; a seção 6.6 apresenta o repositório dos certificados; a seção 6.7 apresenta a autoridade de aviso; a seção 6.8 apresenta a autoridade para emissão de chave privada; a seção 6.9 apresenta a autoridade de datação e na seção 6.10 é apresentada a estrutura das ACs da UFSC.

6.2 ICP da UFSC

A ICP da UFSC possui os componentes AC-Raiz, AC, AR, Repositório, AA e outros componentes, integrantes da cadeia de certificação encontrada na Universidade. A estrutura de certificação da UFSC é definida graficamente, conforme ilustrado na figura 6.1 e definidas textualmente, nas seções a seguir.

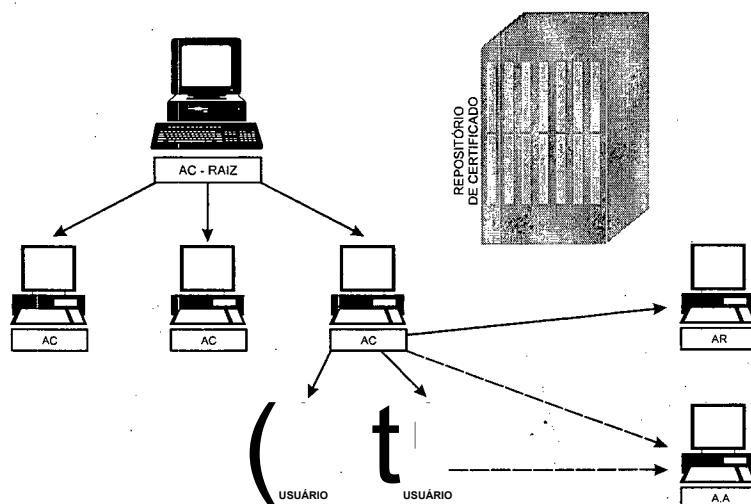


Figura 6.1: A AC-raiz, a AR, as ACs intermediárias e o repositório são componentes da ICP da UFSC

6.3 Autoridade Certificadora Raiz (UFSC - AC)

A AC Raiz da ICP da UFSC é responsável pela emissão e manutenção dos certificados das ACs integrantes da Universidade. Esta AC é a única que emite certificados auto-assinados.

O certificado da AC - Raiz é o de mais alto nível de segurança, presente na cadeia de certificação. Este contém a chave pública correspondente a chave privada usada para assinar os certificados das ACs integrantes da cadeia e para assinar a LCR da AC - raiz, publicada em diretório ou página Web.

6.4 Autoridade Certificadora - AC

As ACs integrantes da cadeia de certificação UFSC - AC, são todas ACs de órgãos e entidades públicas e privadas licenciadas pela AC - UFSC.

6.5 Autoridade de Registro - AR

As ARs são responsáveis pelos recebimentos das requisições de emissão ou de revogação de certificados de usuários, realizarem a confirmação da identidade do requerente e a validação de sua requisição e encaminhamento destes documentos para AC responsável.

6.6 Repositório

Os Repositórios são diretórios mantidos por ACs para armazenar os certificados emitidos pela AC, as LCR da AC e da AC - UFSC e de outras informações relevantes a cadeia de certificação.

6.7 Autoridade de Aviso - AA

A Autoridade de Aviso é um protocolo criptográfico, criado para ser o responsável por toda comunicação oficial, entre remetente e destinatário. A AA é utilizada para resolver o problema de recusa de recebimento de aviso através da rede [BRO 01]. A AC ao emitir um documento para um usuário, deverá enviar para a AA, esta irá protocolar o documento na PDDE e então devolver uma cópia para AC, confirmando o seu recebimento, devidamente protocolado. A AA envia o documento para o destinatário, através de um diretório público, correio tradicional ou diretamente para o usuário.

6.8 Autoridade de Certificação de Chave Privada

A autoridade de certificação de chave privada é uma autoridade que irá emitir chaves privadas específicas para um determinado usuário final, após um acordo prévio.

6.9 Autoridade de Datação - PDDE

A Autoridade de Datação - PDDE, denominada Protocoladora Digital de Documentos Eletrônicos, é um protocolo que presta serviço de registro de tempo, com suporte para provar que um determinado documento foi assinado em uma data/hora. Com este serviço é possível provar que uma assinatura digital foi gerada durante o período de validade de um certificado digital.

6.10 Estrutura da Certificadora UFSC

A Autoridade Certificadora Raiz (AC - raiz) da UFSC, emite certificados para todas as demais autoridades dentro da estrutura da Universidade Federal de Santa Catarina - SC;

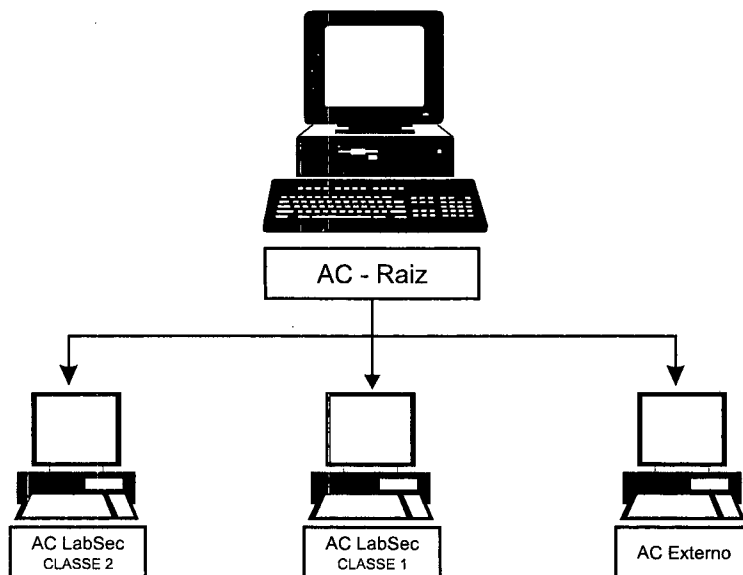


Figura 6.2: As ACs demonstradas nesta figura são integrantes da estrutura da AC da UFSC

A AC LabSEC Classe 2, está em fase de implementação, a qual irá emitir certificados comerciais de nível 2 de segurança.

A AC Lab SEC Classe 1, atualmente está em funcionamento para emitir certificados internos a UFSC. Estes certificados são de direito a todos os membros da

Universidade que possuem um e-mail com domínio UFSC.BR.

A AC Externa está em fase final de adaptações, para emitir certificados para membros de órgãos públicos como a OAB, TRE/SC, TJ/SC, MP/SC e para empresas privadas que desejem contratar os serviços de certificação do LabSEC da UFSC. Isso será feito após a devida aprovação do governo.

6.11 Conclusão

A infra-estrutura da ICP da UFSC apresenta os componentes necessários para realizar o processo de certificação com segurança, abrangendo alguns serviços a mais que outras ICPs de outros países, tais como a AA e PDDE. Componentes estes que podem garantir ainda mais a segurança da informação.

Capítulo 7

Política de Certificação da UFSC

7.1 Introdução

A presente proposta de PC - Política de Certificados para o AC a UFSC, visa a criação de um documento que estabeleça regras e normas empregadas no processo de certificação, descrevendo o papel de cada componente dentro da ICP, as responsabilidades, obrigações, direitos assumidas pelo usuário do certificado, manutenção de chaves e hierarquia de ICP, a fim de garantir o processo de emissão e manutenção dos certificados, com a segurança e também, este documento poderá ser usado como exemplo para que outras AC a utilizem na criação de suas PCs. A elaboração da PC deu-se após o estudo realizado da RFC 2527, da comparação realizadas das DPCs da *VeriSign*, da *Entrust.NET* e da ICP-Brasil, as quais foram comparadas, elencando-se os itens e verificando a existência dos mesmos e com base em livros que explicam como elaborar uma PC e a DPC [RUS 01],

Esta PC é aplicável a todos os requerentes, assinantes, parceiros de confiança, pessoas físicas ou jurídicas, entidades ou organizações que mantêm algum tipo de vínculo com a AC, a fim de garantir a autenticação e integridade de dados, irrevogabilidade e e irretratabilidade das transações eletrônicas e das aplicações que utilizem certificados digitais.

Este capítulo está dividido da seguinte forma: a seção 7.2 apresenta as

informações sobre o certificado; a seção 7.3 apresenta as obrigações, responsabilidades e garantias da AC e dos usuários; a seção 7.4 apresenta a segurança utilizada na certificação; a seção 7.5 apresenta o ciclo de vida dos certificados e a seção 7.6 apresenta as definições e os termos usados na PC.

7.2 Infra-estrutura de Certificação

Esta seção trata dos serviços de certificados, da sua aplicabilidade, dos tipos de certificados, das informações para aquisição de certificados, das extensões e da ICP da UFSC.

7.2.1 Serviços de Certificação

Os serviços de certificação fornecidos pelo repositório de certificados e LCRs e também os contatos, deverão estar disponíveis 24 horas por dia, sete dias por semana.

7.2.2 Aplicabilidade

Os certificados digitais são aplicados ao comércio eletrônico, comunicações seguras, transações eletrônicas, aplicações, autenticação, integridade e outros serviços de segurança, atendendo as necessidades técnicas e pessoais, públicas ou privadas, com relação a assinaturas digitais.

7.2.3 Administração dos SCP

Os SCP da AC principal são administrados de forma que algumas atividades possam ser executadas por outras partes, prestação de serviços, porém as outras partes precisam garantir que vão cumprir e manter a qualidade dos serviços. A AC principal determina através de contrato qual será o serviços, que a prestadora vai executar. A prestadora de serviço só poderá executar os serviços para os quais foi criada e designada.

7.2.4

As ACs devem utilizar sistemas, mecanismos confiáveis, adotar medidas de segurança e controle, manter processos, procedimentos e atividades, que garantam o desempenho de seus serviços, com segurança.

7.2.5 Classes de Certificados

A ICP da UFSC suporta duas classes de certificados. Cada classe oferece um nível de confiança e características diferenciadas e em ordem crescente, sendo a classe 1 de mais baixo nível de segurança, utilizada para e-mail e a de classe 2 mais alto nível de segurança, utilizada para *Site*. São os usuários que determinam e avaliam qual a classe ideal para atender a finalidade desejada. Todas as classes podem ser emitidas para pessoas físicas e jurídicas.

7.2.5.1 Certificados de classe 1

Os certificados de classe 1 são os de mais baixo nível de segurança, apesar de serem emitidos para todos, são indicados apenas a indivíduos para fins de uso de e-mail. Esta classe é basicamente utilizada para correio eletrônico pessoal, possibilitando a comprovação da origem de envio. Eles não devem ser usados para uso comercial.

A AC deve possuir *software ou hardware* confiável para a proteção da chave privada da AE de classe 1, a fim de evitar o comprometimento. Para os assinantes individuais, recomenda-se o uso de *software* de criptografia.

1.1.52 Classe 2

Os certificados de classe 2 possuem um nível de segurança mais alto do que a classe 1. A sua finalidade é destinada para *Sites*

A proteção da chave privada da AC de classe 2, será feita pelo uso obrigatório de *hardware* confiável. Para a chave privada do assinante, o uso de *software* de criptografia é recomendado.

7.2.6 Confirmação das Informações da Identidade do Assinante

As ACs tomam medidas adequadas para confirmar a identidade do candidato, durante o processo de certificação, estas medidas dependem da classe dos certificados, variando entre a simples verificação do não conflito de nomes em banco de dados ao comparecimento do candidato perante a AC, do representante ou a confirmação por um tabelião.

As informações dividem-se em confidenciais, que não podem serem vendidas, disponibilizadas ao público, reveladas, sem o consentimento do proprietário ou por ordem judicial; e as não-confidenciais, são as informações disponíveis ao público em geral.

7.2.7 Extensões

Todos os certificados possuem um campo chamado extensões, as quais demonstram qual é o tipo do certificado emitido.

1.2.1.1 Mecanismos de Extensões e a Estrutura de Autenticação

Os certificados digitais emitidos suportam o padrão X.509v3, que expandem os recursos das versões 1 e 2, permitindo o acréscimo de extensões de certificados.

1.1.1.2 Extensões Padrão e Específicas dos Serviços

A Emenda 1 à ISO/EIEC 9594:1995 do X.509v3, define uma série de extensões de certificado, oferecendo vários controles gerenciais e administrativos úteis para a autenticação em grande escala e objetivos distintos.

1.2.1.3 Identificação e Importância de Extensões Específicas

A função de cada extensão é indicada por um valor padrão de 10 - Identificador de Objeto (definido no X.509). As extensões específicas para cada situação

favorece o processo de uso e reconhecimento do certificado. A tabela 7.1 demonstra os IOs utilizados pela AC da UFSC.

Tabela 7.1: Identificadores de Objetos

L3.6.L4.L7687	UFSC
1.3.6.1.4.L7687.1	LabSEC
L3.6.L4.L7687.L1	LabSEC - Ostracom
L3.6.L4.L7687.2	Pessoas
1.3.6.L4.L7687.2.1	Nome do Professor
L3.6.L4.L7687.2.1.1	PSIAPE
L3.6.L4.L7687.2.2	Nome do Aluno de Graduação
L3.6.L4.L7687.2.2.1	Número de Matrícula
L3.6.L4.L7687.2.3	Nome do Servidor
L3.6.L4.L7687.2.3.1	SIAPE
L3.6.L4.L7687.2.4	Nome do Aluno de Pós-Graduação
L3.6.L4.L7687.2.4.1	Número de Matrícula
L3.6.L4.L7687.3	Nome do Curso
L3.6.1.4.L7687.4	Departamentos
L3.6.L4.L7687.5	Centro
L3.6.L4.L7687.6	Instituto

7.2.7.4 Extensões de Certificados do Assinante/Usuário Final

Os certificados para usuários devem ser emitidos segundo o X.509v3. As extensões utilizadas nos certificados emitidos pela UFSC são: identificador da chave do sujeito, uso avançado de chave, identificador da chave da autoridade, ponto de distribuição da LCR e acesso as informações da AC.

1.2.1.5 Nomeação Avançada

Todos os certificados devem possuir um campo de identificação de nomes. Os nomes devem ser únicos e correlatos ao certificado desejado e ao assinante.

7.2.8 Acordos de Certificação Cruzada

Cada AC-raiz de uma cadeia de certificados deverá possuir procedimentos específicos e acordos para a realização de certificação cruzada. As ACs deverão

executar os procedimentos de acordo com o que lhe for atribuído. A certificação cruzada poderá ser de AC-raiz para AC-raiz, de AC-raiz para AC, AC para AC.

7.2.9 Hierarquia de ICP

Os serviços de certificação digital pública, são implementados por uma hierarquia de infra-estrutura de chaves públicas, composta por entidades, as quais estão especificadas nas seções a seguir.

7.2.9.1 Autoridade Certificadora Raiz (AC - Raiz)

A AC-raiz é a AC de mais alto nível na cadeia de certificação, que emite certificados para a AC inferiores na hierarquia. Utiliza algoritmo RSA e chave de tamanho 4096 bits. O certificado da AC-Raiz da UFSC possui validade de 8 anos.

Dispositivos de *hardware* confiáveis são usados para criar, proteger, gerenciar e até destruir a chave privada. Determinadas partes secretas devem ser copiadas e asseguradas por detentores de partes secretas.

7.2.9.2 AC - Autoridade Certificadora

Cada AC é subordinada a uma AC-raiz. As ACs podem emitir, gerenciar e revogar certificados de assinantes/usuários finais, utilizando dispositivos de *hardware* confiável. A AC usa o algoritmo RSA e chave de tamanho 5048. O certificado da AC possui validade de 4 (quatro) anos. As ACs podem pertencerem a entidades públicas ou privadas.

7.2.9.3 AR - Autoridade de Registro

As ARs são entidades responsáveis pelo recebimento das solicitações de certificados, pela verificação, avaliação, aprovação ou rejeição das solicitações, dependendo do resultado, então enviam a solicitação para a AC pertinente.

1.1.9A Repositórios

Toda a AC deve manter um repositório a disposição do público para armazenar, recuperar e consultar certificados e outras informações relacionadas aos certificados. Um repositório é um banco de dados de armazenamento de certificados, DPCs, LCRs, e outras informações relevantes.

1.1.9.5 LCR - Lista de Certificados Revogados

As LCRs são listas nas quais as ACs publicam os certificados revogados ou suspensos. A publicação se dá periodicamente.

7.3 Obrigações, Responsabilidades e Garantias

Este capítulo apresenta as responsabilidade, obrigações e deveres das ACs, ARs, usuários e responsabilidades financeiras de ambos.

7.3.1 Obrigações

As ACs, os usuários e outros que venham a envolver-se no processo de certificação possuem obrigações uns com os outros. Nas seções a seguir serão demonstradas as obrigações das partes envolvidas na certificação.

7.3.1.1 Obrigações da AC-raiz

A AC-raiz compromete-se a emitir e gerenciar os certificados das ACs, de acordo com as práticas e procedimentos da DPC. Algumas das obrigações da AC-raiz são: emitir e revogar certificados, emissão e publicação de LCRs, avisar sobre a emissão e revogação de certificados á AC, publicar os certificados emitidos para ACs em repositórios e no Diário Oficial da União, fiscalizar o cumprimento da DPC pela AC.

7.3.1.2 Obrigações da AC

A AC deverá operar de acordo com a DPC, devendo realizar todos os aspectos relacionados a emissão e gerenciamento de certificados, tais como: emissão, revogação e publicação de certificados, emitir e publicar LCRs, avisar o usuário sobre a emissão e revogação do certificado, gerenciar suas chaves, manter a integridade e de seus serviços.

7.3.1.3 Obrigações da AR

A AR é responsável por, receber as candidaturas a certificação, aprová-las ou revoga-las, realizar a verificação das informações enviadas junto com a solicitação do certificado. Se as informações forem verdadeiras, submete uma solicitação de emissão de certificados à AC. Notificação dos assinantes sobre a emissão ou revogação do certificado, cumprimento de suas obrigações de acordo com o que lhe for atribuído no ato de sua criação.

7.3.1.4 Obrigações do Assinante

Os assinantes possuem obrigações, tais como: conhecer e receber instruções sobre o uso de criptografia de chaves públicas e certificados; gerar um par de chaves confiáveis; proteger as chaves privadas; utilizar os certificados de forma apropriada e para o qual foi emitido; avisar a AC sobre o recebimento do certificado; consultar a LCR; notificar a AC sobre qualquer anormalidade relacionada ao certificado, ler e concordar com os termos desta DPC.

7.3.1.5 Obrigações dos Parceiros de Confiança

Os parceiros de confiança possuem as mesmas obrigações dos assinantes, e também por seus atos em relação aos certificados tirando suas próprias conclusões e confiança dos certificados.

7.3.2 Responsabilidades

As responsabilidades são referentes as ACs, usuários e outros envolvidos no processo de certificação.

7.3.2.1 Responsabilidades Financeira

As ACs devem possuir recursos financeiros para implementação, gerenciamento e manutenção dos processos e atividades inerentes, manter suas operações, desempenhar suas obrigações e arcar com os riscos de responsabilidade diante dos assinantes e outras pessoas que confiarem nos certificados emitidos e ainda devem possuir recursos para eventuais erros ou omissões. As ACs podem possuir seguro para eventuais erros e omissões.

T.3.2.2 Responsabilidades da AC

As ACs responsabilizam-se em adotar medidas de segurança, envolvendo processos, procedimentos e atividades que garantam a segurança e a dos serviços de certificação; em executar os serviços de certificação, manter e garantir a integridade e a segurança dos dados sob sua responsabilidade.

7.3.2.3 Responsabilidades da AR

As mesmas responsabilidades da AC devem ser adotadas pela AR.

7.3.2.4 Isenção de Responsabilidades

As ACs e ARs, exceto se indicados e dispostos anteriormente e se vedado por lei, se isentam da responsabilidade de todas e quaisquer garantias e obrigações; condições e aceitação de comercialização; satisfação e/ou adequação para um determinado fim; exatidão, autenticidade, das informações fornecidas; não responsabilizam-se pelas representações de informações contidas em um certificado e ainda por negligências ou falta de cuidados adequados.

7.3.2.S Responsabilidades do Assinante

Os assinantes responsabilizam-se pela proteção da chave privada, uso adequado da mesma, pelo cumprimento das normas e regras da DPC, pela veracidade das informações contidas nos certificados. Os assinantes responsabilizam-se em não divulgar, perder, danificá-la, comprometê-la, divulgá-la, por possível roubo e por notificar a AC por qualquer um desses ocorridos.

7.3.2.Ó Responsabilidades das Partes Secretas

Os detentores de partes secretas responsabilizam-se por executarem suas obrigações de acordo com a DPC, notificar o emissor da parte secreta de haver perda, roubo, divulgação imprópria ou comprometimento da mesma, assim que estiverem cientes do ocorrido. Os detentores não serão responsáveis pelo não cumprimento de suas obrigações por motivos acima de seu controle, mas serão responsáveis por divulgar a parte secreta ou por não notificar o emissor sobre a divulgação ou comprometimento da mesma.

7.3.3 Garantias Limitadas

As ACs garantem que fornecerão a infraestrutura, os serviços de certificação, os controles para ICP, os serviços de repositório, emitir os certificados coerentes com os procedimentos estabelecidos, disponibilizar informações, emitir e publicar as LCRs.

7.3.4 Indenização pelo Assinante

Os assinantes, ao aceitar imi certificado, concordam em isentar e indenizar as AC e demais entidades pertinentes de atos ou omissões, que resultem em danos, perdas, despesas, queixas, inclusive honorários advocatícios, custos processuais e taxas decorrentes e resultantes de: falsidade ou declaração falsa de fatos pelo assinante, com intuito de enganar a AC; falha na proteção da chave privada; erros ou omissões feitas por um assinante ao usar ou requerer imi certificado; por modificações de informações

contidas no certificado; por uso indevido do certificado. O fato de não haver má intenção, não o isentará de indenizar a AC.

7.3.5 Indenização pela AC

Seja a AC-raiz ou AC, a indenização de um assinante ocorrerá somente quando houver falhas na execução das suas obrigações e responsabilidades.

A AC emissora da parte secreta isentará o detentor de responsabilidades com relação a todas as reivindicações, ações, danos, julgamentos, taxas de arbitragens, despesas, custos e outras obrigações assumidas pelo detentor, caso o mesmo não tenha sido o causador e nem contribuído para tais fatos.

7.3.6 Política de Reembolso

O reembolso de valores poderá ocorrer mediante a solicitação de revogação de certificado até 15 (quinze) dias após a sua emissão, o valor reembolsado será o mesmo pago pelo certificado. Após os 15 (quinze) dias, o assinante poderá solicitar a revogação e o reembolso, caso a AC tenha violado alguma garantia ou obrigação, caso contrário não terá direito a reembolso. O reembolso será efetuado por cheque ou por crédito em conta corrente ou em cartão de crédito. A solicitação de revogação poderá ser feita por um formulário disponível no repositório da AC.

7.3.7 Limitações de Perdas e Danos

Exceto se vedado por lei, a de uma AC e de todas as ACs superiores pertencentes a cadeia de certificação pertinente, poderá exceder os valores de responsabilidades a serem determinados pela AC pertinente. As responsabilidades agregadas de todas as ACs da cadeia, devem ser limitadas a um valor não excedente ao apresentado pela AC. Os valores de responsabilidades devem ser de acordo com a classe do certificado.

As limitações sobre danos aplicam-se a perdas e danos de todos os tipos, incluindo, mas não limitando os danos diretos, indiretos, compensatórios, especiais

ou acidentais, contraídos por qualquer pessoa incluindo, mas não limitando à candidatos, destinatários ou parte confiantes, causados pela confiança ou uso de certificados emitidos por uma AC, aplicam-se também a responsabilidades contratuais. Sob hipótese alguma a AC será obrigada a pagar um valor maior de responsabilidade agregado para cada certificado.

Os valores de responsabilidades limitados para cada certificado, devem ser aplicados a cada certificado independente do número de ações, em ordem de protocolo de entrada da ação. A moeda para indenização é a nacional (brasileira).

7.3.8 Atividades Perigosas

Os serviços de certificação não foram projetados, elaborados, produzidos ou destinados ao uso fora de suas finalidades, em circunstâncias perigosas, combinações com atividades de risco ou usos que exigem desempenhos sem falhas, tais como; instalações nucleares, navegações áreas, controle de tráfego aéreo, dispositivos de suporte direto a vida, controle de armamentos, onde uma falha qualquer poderá ocasionar mortes, danos pessoais ou danos ambientais.

7.3.9 Direitos de Propriedade Intelectual

A AC detém todo e qualquer direito, titularidade e interesse sobre todos os certificados. A AC também reserva o direito de investigar todos os compromissos permitidos por lei.

7.4 Controles Técnicos de Segurança

Esta seção apresenta o processo de geração e proteção das chaves dos assinantes, de auditoria e retenção de registros de auditoria, planejamento e contingência de recuperação de desastres, gerenciamento e prática de pessoal.

7.4.1 Geração e Proteção das Chaves de Assinantes

Antes de iniciar o processo de solicitação de certificado, o candidato deverá gerar seu par de chaves e enviar a sua chave pública para AC, juntamente com a solicitação.

A proteção e segurança da chave privada do assinante é de inteira responsabilidade do mesmo. As ACs não detêm as chaves privadas do assinante.

7.4.2 Auditoria

As ACs e ARs devem implementar e manter sistemas confiáveis para preservar um cronograma de auditoria de todos os aspectos relacionados a emissão, gerenciamento e demais processos de certificação. A auditoria verifica se todos os procedimentos, termos, normas e processos estão sendo executados de acordo com o estabelecido na DPC. Após a execução da auditoria, os auditores devem emitir relatórios e enviá-los a AC auditada, para que sejam tomadas as devidas providências. A AC auditada deve enviar uma cópia do relatório para a AC-raiz.

A auditoria deve ocorrer uma vez ao ano, e por solicitação da AC ou da AC-raiz, poderá ocorrer mais vezes em um ano. Os auditores devem ser contadores públicos, certificados e com experiência comprovada em segurança de computadores ou um profissional qualificado em segurança de computadores, independentes da AC auditada.

7.4.3 Programação de Retenção de Registros de Conformidade

A ACs mantém registros e os dispõem somente perante solicitação ou ordem judicial. Os registros a serem mantidos são: documentos de conformidade com a DPC; documentos referentes as medidas e informações materiais sobre ciclo de vida dos certificados. Os registros incluem provas de posse da ACs, referentes aos itens: identidade do assinante, identidade de quem solicitar a suspensão ou revogação do certificado, outros fatos representados no certificado, identificação de data e hora, fatos relativos a emissão

de certificados.

Todas as informações acima citadas devem ser retidas. O tempo de retenção varia de acordo com a classe do certificado. Para certificados de classe 1, durante 5 (cinco) anos e para os certificados de classe 2, durante 10 (dez) anos. Os relatórios referentes a auditoria também devem ser retidos, pelo mesmo período da retenção das informações das classes de certificado, referente a AC.

7.4.4 Planejamento de Contingência e Recuperação de Desastre

A AC deve possuir um plano de contingência implementado, documentado e testado para os recursos e procedimentos de recuperação de desastres, de forma consistente e pontual, sem grandes ou nenhum prejuízo à ambos os lados.

7.4.5 Gerenciamento e Prática de Pessoal

A AC deve formular e seguir procedimentos, práticas e gerenciamento de pessoal para garantir a competência de seus funcionários. Os funcionários só executarão as tarefas para as quais foram destinados, a fim de evitar colisão das respectivas responsabilidades e obrigações.

7.4.5.1 Cargo de Confiança

Todas as pessoas da AC, que tenham acesso a operações criptográficas ou controles sobre as mesmas de modo, que possam afetar o processo de certificação, são considerados como cargos de confiança. Os funcionários com cargo de confiança são as equipes de: atendimento ao cliente, administração de sistemas, engenharia, suporte e supervisores da infra-estrutura de sistemas confiáveis da AC. Cada funcionário com cargo de confiança receberá tarefas específicas e limitadas, definidas nas suas responsabilidades. As mesmas condições são usadas pelas ARs.

7.4.5.2 Investigação e Conformidade

As ACs devem fazer uma investigação minuciosa inicial de todos os candidatos a cargos de confiança, a fim de determinar sua competência. Para os funcionários com cargos de confiança já em exercício, as investigações devem ocorrer ao menos uma vez por ano, para verificar se os mesmos continuam confiáveis e competentes de acordo com os termos da DPC e regras da AC.

7.4.5.3 Funcionários com Cargos de Confiança

Os funcionários que ocupem cargos de confiança devem ser qualificados sobre o uso de mecanismos de segurança, versões de *software* em uso na AC, condutas, sobre a atividade que lhe foi atribuída. Os funcionários contratados devem assinar contratos, que regulem os termos e condições do cargo a ser ocupado, serem registrados, no contrato deve constar o compromisso de não divulgar informações da AC ou de usuários, e até mesmo quando não forem mais funcionários da AC.

7.4.5.4 Afastamento de Pessoas que Ocupam Cargos de Confiança

Todos os funcionários que não forem aprovados na investigação inicial ou nas periódicas, devem ser afastados imediatamente, até a comprovação dos fatos, após a comprovação, a AC deverá afastá-lo definitivamente. Caso não seja comprovado nenhum fato, o funcionário deverá passar uma seleção e treinamento, e ser realocado em outro setor.

7.4.6 Detentores de Partes Secretas

Os detentores de partes secretas são órgãos que detêm partes secretas de chaves privadas de AC, que queiram aumentar a de sua(s) chave(s) privada(s) e recuperação da mesma. O detentor deverá utilizar sistemas confiáveis para proteger a parte secreta de qualquer comprometimento.

7.4.7 Instalações da AC

A AC deverá operar em instalações confiáveis, o acesso físico deve ser controlado por sistemas de segurança. O local onde contem os *softwares e os hardwares*, devem possuir sistemas de segurança que não permita o acesso de pessoas desautorizadas e sozinhas.

7.5 Ciclo de Vida dos Certificados

Os certificados digitais apresentam um ciclo de vida, composto por 7 (sete) itens. Este itens executam todo o processo da certificação, desde a solicitação até o encerramento das atividades do certificado. A figura 7.1 ilustra o ciclo de vida dos mesmos.

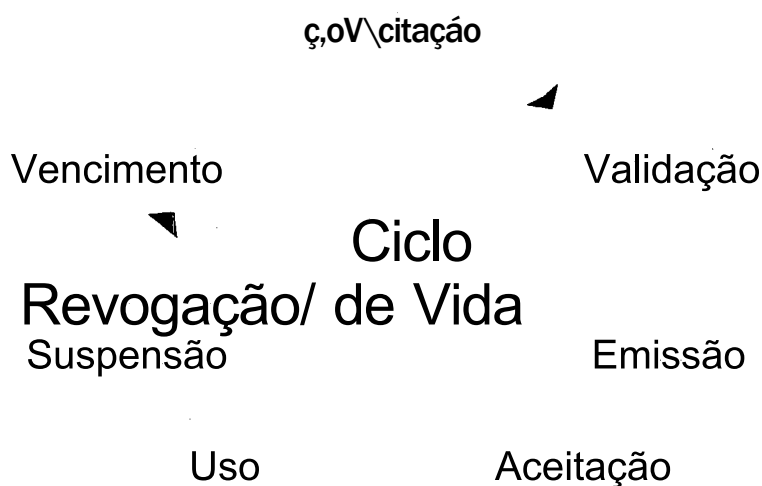


Figura 7.1: A figura Ciclo de Vida de um Certificado, demonstra desde o primeiro passo do candidato a certificado, quando o mesmo faz a solicitação até a sua finalização, o seu vencimento.

7.5.1 Solicitação de Certificados

Este capítulo descreve o processo de solicitação de certificados digitais.

7.5.1.1 Procedimentos para a Solicitação de Certificados

Os procedimentos para solicitação de certificados incluem exigências referentes à geração, proteção do par de chaves e lista de informações necessárias para cada classe de certificado, preenchimento de uma solicitação e enviá-la a AC pertinente, anexando a chave pública. O candidato deve ler os acordo de certificação.

7.5.1.2 Informações e Comunicações da Solicitação de Certificados

Para cada classe de certificado são exigidas informações, algumas são comuns entre as classes e outras específicas, as informações que não constam no certificado são mantidos em regime de confidencialidade pela AC, as demais são públicas.

7.5.2 Validação de certificados

A validação de solicitação de certificados, apresentam algumas exigências, as quais são executadas pela AC pertinente. Estas exigências estão especificadas nas próximas seções.

7.5.2.1 Exigências para a Validação da Solicitação de Certificado

Ao receber uma solicitação de certificados, a AR deverá efetuar as validações obrigatórias, estabelecidas como pré-requisito para a emissão. A AR deverá confirmar se as informações fornecidas na solicitação são verdadeiras ou não. Caso todas as informações forem confirmadas a AR envia à AC a solicitação de certificado, caso contrário, a solicitação é rejeitada.

A AR realiza a confirmação das informações fornecidas pelo candidato para a validação da solicitação de certificação. Para cada classe de certificados é exigido um tipo de confirmação coerente com o nível de segurança do certificado.

T.5.2.2 Aprovação de Solicitação de Certificados

Com êxito obtidos em todas as validações e confirmações exigidas para aprovação de um certificado, independente da classe, a AR deverá aprovar a solicitação e envia-lá para AC emitir o certificado. A emissão do certificado é a confirmação da aprovação da solicitação do certificado.

7.5.2.3 Rejeição de Solicitação de Certificado

Quando as informações não forem verdadeiras ou houver indícios de irregularidades na solicitação, a aprovação da mesma não poderá ocorrer e a AR executará a rejeição da solicitação, informando ao candidato, qual o motivo da mesma.

7.5.3 Emissão de Certificados

A emissão de um certificado ocorrerá após a AC receber uma solicitação aprovada pela AR. A emissão do certificado significa a aprovação final da solicitação pela AC. O certificado passa a ser válido a partir do momento em que o assinante o aceita.

A AC não poderá emitir certificados sem o consentimento do candidato a certificado. No entanto a solicitação juntamente com o contrato de assinante, assinado pelo candidato, é considerado como aceitação para emissão.

7.5.3.1 Recusa Quanto a Emissão de um Certificado

A AC poderá recusar-se a emitir um certificado qualquer, a seu critério, sem responsabilizar-se por prejuízos ou despesas resultantes de tal recusa. No entanto a AC deverá reembolsar, imediatamente todos os valor pagos até então pelo assinante, exceto se as informações forem falsas ou fi-audentas.

T.5.3.2 Tempo para Emissão de Certificados

Assim que todas as informações de solicitação forem confirmadas, a AC deverá emitir os certificados imediatamente. O tempo para emissão de certificados é

estabelecido de acordo com o nível de exigências para confirmação de solicitação de cada classe de certificado.

7.S.3.3 Período de Validade de Certificados

A validade de cada certificado começa assim que o assinante o aceita. Para cada classe e finalidade dos certificado, há um período pelo qual os certificados são válidos.

7.5.4 Aceitação de Certificados

Os meios de aceitação de um certificado, variam de acordo com a classe. Ao aceitar um certificado, o assinante deverá garantir a integridade de sua chave privada, a veracidade de suas informações e o certificado será de uso exclusivo para a sua finalidade. O assinante, ao aceitar um certificado, concorda com os termos e condições da DPC.

7.5.4.1 Publicações de Certificados

Imediatamente após a emissão de um certificado, a AC deverá publicá-lo em repositório e em Diário Oficial da União.

7.5.5 Uso de Certificados

A garantia de que os certificados estão sendo usados corretamente, é realizada pela conferência da assinatura digital.

7.5.5.1 Verificação de Assinaturas Digitais

A verificação da assinatura digital determina se assinatura digital foi criada pela chave privada correspondente a chave pública listada no certificado do signatário e se a mensagem associada não foi alterada desde a criação da assinatura digital.

A pessoa ou entidade que confiar em uma assinatura digital, que não possa ser confirmada ou que venha a ocorrer falhas na verificação da assinatura, estará

assumindo todas as responsabilidades de riscos e se isentando de qualquer direito em relação ao uso da assinatura.

7.5.6 Suspensão / Revogação de Certificados

A suspensão e ou revogação de certificados poderá ocorrer por vários motivos, tais como: comprometimento, roubo, perda, modificações, divulgação da chave privada do assinante; a violação de obrigações dispostas na DPC, pelo assinante, ações causadas por desastres naturais, falta de pagamento de tarifas e taxas, atraso ou impedimento no desempenho das obrigações, mudanças no estatuto, falhas em comunicações, a emissão não estar de acordo com os procedimentos exigidos na DPC e outras ações consideradas relevantes pela AC.

7.5.6.1 Suspensão ou Revogação de um Certificado de AC

A AC deverá fazer esforços adequados para suspender ou revogar um certificado de uma AC subordinada, independente do consentimento da AC subordinada, caso um fato material representado no certificado for conhecido ou tido como falso; os certificados também podem ser revogados ou suspensos pelos motivos gerais, especificados acima.

A suspensão ou revogação de certificados de ACs, poderá ocorrer mediante solicitação de um representante.

7.5.6.2 Suspensão ou Revogação Mediante Solicitação do Assinante

A AC poderá revogar ou suspender um certificado, mediante solicitação do assinante, devidamente assinado digitalmente, após a confirmação de que a pessoa solicitante é de fato o assinante.

7.5.6.3 Avisos e confirmação de Suspensão ou Revogação

Assim que a AC revogar ou suspender um certificado, deverá publicar a revogação ou suspensão na LCRs, e avisar ao assinante, notificando-o sobre a revogação

ou suspensão.

7.S.6.4 Proteção da Chave Privada após a Revogação

Mesmo após a suspensão ou revogação de certificados, as chaves privadas devem ser mantidas sob sigilo, até a possibilidade de sua destruição.

7.5.7 Vencimento do Certificado

A AC deve emitir notificação aos assinantes sobre o vencimento do certificado, através de correio eletrônico, para que o assinante fique ciente sob o vencimento do seu certificado.

7.5.7.1 Efeitos do Vencimento de um Certificado

O fato de um certificado ter vencido, não implica na validade das obrigações contratuais, criadas ou comunicadas mediante a DPC.

1.5.1.2 Utilização de um Certificado Vencido

A utilização de um certificado vencido é de inteira responsabilidade da pessoa que o está usando ou confiando. As AC não responsabilizam-se pelo uso de certificados vencidos

7.5.7.3 Renovação e Reinscrição de Assinantes

O processo para renovação e reinscrição de assinantes é igual ao inicial, de acordo com a classe de certificado.

7.6 Definição de Termos

A definição de termos fica a critério da AC, podendo ser um capítulo ou um anexo da DPC.

7.7 Conclusão

A política de Certificados - PC é responsável pelas normas e regras, que objetivam garantir o processo de certificação com segurança. Os usuários de certificados precisam submeter-se as regras e normas estabelecidas pela PC, para que o processo do seu certificado, desde o seu requerimento até o vencimento transcorra dentro da segurança prevista.

Capítulo 8

Declaração de Práticas de Certificação - DPC para a UFSC

8.1 Introdução

A DPC apresenta as práticas e os procedimentos empregados pela AC para garantir o processo de certificação com segurança desde a implantação da AC até o encerramento das atividades da mesma e do certificado. Para garantir este processo, a DPC é dividida em várias etapas a começar pelas informações sobre si, descrevendo os direitos, a sua estrutura, publicações e a incorporação aos certificados.

A presente proposta de DPC - Declaração de Práticas de Certificação Digital para a AC da UFSC, visa a criação de um documento para estabelecer o funcionamento de cada componente da ICP, como é processo de certificação para outras ACs, aplicativos e hardware utilizados pelas ACs. A presente DPC também poderá ser usada como exemplo para outras ACs elaborarem suas DPCs. A elaboração desta DPC deu-se após o estudo de várias DPCs. Entre as DPCs estudadas, estão as DPCs da *VeriSign*, da *Entrust.NET* e a ICP-Brasil, as quais foram comparadas, elencando-se os itens e verificando a existência dos mesmos nas DPCs comparadas. Após esta comparação foi criado o modelo, considerando os itens frequentes em todas as DPCs e também com base em livros que explicam como elaborar uma DPC e PC [RUS 01].

Esta DPC é aplicável a todos os requerentes, assinantes, parceiros de confiança, pessoas físicas ou jurídicas, entidades ou organizações que mantêm algum tipo de vínculo com a AC.

A seguir será proposto o modelo da DPC para UFSC.

Este capítulo começa da seguinte forma: a seção 8.2 apresenta os avisos gerais, resolução de controvérsias e leis; a seção 8.3 apresenta as operações das ACs; a seção 8.4 apresenta as informações relativas à certificação e a seção 8.6 apresenta o processo de certificação.

8.2 Disposições Gerais

Esta seção aborda os termos e condições, que não foram abordados em outros capítulos da DPC, tais como avisos gerais, treinamento, resolução de controvérsias, leis aplicáveis.

8.2.1 Direitos

A reprodução e distribuição desta DPC é permitida de forma não exclusiva e sem pagamento desde que: (I) a nota direitos autorais apareça de forma destacada no início de cada cópia; (II) a reprodução seja na íntegra, atribuído ao autor. Para outras permissões de reprodução deverá ser enviado um pedido ao endereço eletrônico ou físico da AC.

A autora reserva o direito de processar qualquer pessoa, empresa, entidade que cometer crimes, que violem os direitos autorais e que afetem os serviços da AC.

8.2.2 Publicações

A AC deverá publicar a DPC nas formas abaixo:

- formato eletrônico no repositório ou na WEB, no endereço da AC;

- formato eletrônico através de correio eletrônico pelo endereço da AC;
- papel pelo endereço da AC;
- também será incorporada por referência ao certificado digital.

8.2.3 Incorporação aos Certificados

As DPCs deverão ser incorporadas aos certificados por referência, ou seja, cada certificado deverá possuir ID que faça a ligação a DPC.

8.2.4 Tabela de Acrônimos e Abreviações

A elaboração da tabela de acrônimos e abreviaturas é para facilitar o entendimento dos mesmos utilizados no decorrer do texto.

8.2.5 contato

As informações referentes a contato devem ser enviadas para o endereço eletrônicos (e-mail); labsec@inf.ufsc.br.

8.2.6 Treinamento, Assistência e Instruções

A AC pressupõe que o candidato esteja familiarizado como uso de assinaturas digitais e ICPs, caso contrário é necessário que o candidato faça algum treinamento ou procure assistência ou instruções no uso de técnicas de chaves públicas antes de efetuar a solicitação do certificado digital.

8.2.7 Avisos

Os avisos, informações ou solicitações em relação a DPC, devem ser feitas por mensagens assinadas digitalmente, por correspondência registrada, fax-símile ou por correspondência registrada. As mensagens eletrônicas só entram em validade, após a confirmação de recebimento do remetente, as demais entram em vigor no dia seguinte,

exceto por correspondência registrada, que entra em vigor no 5 (quinto) dia, após o seu envio.

8.2.8 Conflito de Cláusulas

No caso de ocorrer conflito entre esta DPC e as versões anterior, outras regras, diretrizes e contratos, o assinante estará sujeito as cláusulas desta DPC, exceto quando as cláusulas desta, forem proibidas por lei. Em hipótese alguma será aceita cláusulas de versões anteriores a DPC vigente.

8.2.9 Interpretação e Tradução

O uso desta DPC em outros países, poderá ocasionar conflitos entre as versões em português e outro idioma, a versão em português irá prevalecer.

8.2.10 Direitos sobre as Emendas

A AC reserva o direito de efetuar emendas quando fizer-se necessário e publica-las no repositório, em uma seção de emendas de DPC. As emendas poderão ou não ocasionar a mudança de versão. A mudança de versão só ocorrerá quando houver uma reestruturação da DPC. As emendas de menor impacto entram em vigor imediatamente após sua publicação no repositório, as de maior impacto entram em vigor após 10 dias de sua publicação.

8.2.11 Aprovação das Emendas

O não manifesto de revogação do certificado por parte do assinante, após a publicação da emenda de uma DPC, constituir-se-a como aceita a ementa da mesma pelo assinante.

8.2.12 Taxas

As taxas de cobrança pelos certificados, serão definidas e estabelecidas, assim que a implantação da infra-estrutura da ICP da UFSC estiver concluída. As taxas serão estabelecidas de acordo com as classes dos certificados e disponibilizadas no repositório da AC. As taxas são passíveis de mudanças pela AC.

8.2.13 Força Maior

As ACs, ARs e parceiros de confiança não serão responsáveis por danos, atrasos ou falhas no desempenho de suas atividades, de acordos com os termos desta DPC, resultantes de eventos além de seu controle, tais como: guerras, terremotos, fogo, enchentes, e outros.

8.2.14 Leis aplicáveis

Em todo e qualquer processo, será de uso único as leis brasileira. São as leis brasileiras, que regulamentam a exigibilidade, interpretação e realização desta DPC, a fim de garantir os procedimentos uniformes e a interpretação da mesma para todos os usuários. Para exportação de certificados deverá ser obedecido, as normas e as leis de exportação aplicáveis.

8.2.15 Resolução de Controvérsias

As controvérsias envolvendo a DPC ou certificados, devem ser notificadas à AC ou a alguma outra parte responsável direta por resolução de controvérsias, visando a sua resolução imediata.

8.2.16 Resolução formal de Controvérsia

Decorrido 30 (trinta) dias e não havendo uma solução para a controvérsia, acarretará o envio por escrito ou por formulário eletrônico para o órgão responsável, por

uma das partes, solicitando a avaliação do caso. A resolução final deverá ocorrer em 15 dias.

8.3 Suporte a Operação de Certificação

Esta seção apresenta o suporte e o controle de operações de ACs. Aborda o funcionamento de ACs, inclusive a manutenção de registros e auditoria.

8.3.1 Serviços Oferecidos pela AC-raiz

Os serviços oferecidos pela AC-raiz são a geração de chaves, emissão, publicação, verificação do prazo de validade e revogação de certificados de ACs, geração de LCRs, fiscalização e auditorias de ACs.

8.3.2 Solicitação de AC

O responsável deverá preencher uma solicitação de AC, de acordo com a classe desejada, reconhece-lá em cartório e envia-lá a AC pertinente. Os demais procedimentos são os mesmo dos assinantes/usuários finais, descritos no capítulo ciclo de vida dos certificados.

8.3.3 Pré-Requisitos para Aprovação de AC

As ACs devem comprometer-se em seguir as exigências de controle, tais como: segurança, confirmação de identificação, proteção de suas chaves privadas.

8.3.4 Aprovação para Inicia as Atividades de AC

Após a conclusão das investigações das informações da solicitação a AC-raiz deverá aprovar ou reprovar a solicitação. A aprovação se dará através da assinatura de um contrato entre a AC, AC-raiz e a emissão do certificado.

8.3.5 Encerramento ou Cessão das Operações de AC

A AC avisará aos usuários e AC superior sobre a intenção de encerramento ou cessão, com 90 (noventa) dias de antecedência. A AC revoga todos os certificados no final dos 90 (noventa) dias, emite aviso para cada usuário sobre a revogação, implementa um processo para garantir a integridade de seus registros, empenhar esforços para garantir que a revogação dos certificados não causem transtornos aos usuários e restituir os assinantes pela revogação dos certificados antes do vencimento, porém o valor não deve ultrapassar o preço do certificado.

A AC encerrante poderá fazer um acordo com outra AC, para suceder as suas operações, que já estão em andamento. Os certificados que anda estão válidos devem ser reemitidos pela AC sucessora. O processo da encerrante será respeitado, porém a AC sucessora reserva o direito de investigar a veracidade das informações do assinante.

8.3.6 Serviços utilizados pela AC

Os serviços fornecidos pelas entidades citadas abaixo, são destinados a garantir a execução dos serviços oferecidos pelos certificados.

8.3.6.1 PDDE - Autoridade de Datação

A PDDE cria uma notação que indica a data e hora correta, ação e a identidade de quem ou dispositivo criador da notação. Este procedimento aumenta a integridade e a dos certificados contribuindo para o não-repúdio.

5.3.6.2 AA - Autoridade de Aviso

A AA - Autoridade de Aviso é utilizada para resolver o problema de recusa de recebimento de aviso através da rede [BRO 01]. A AC ao emitir um documento para um usuário, deverá enviar para a AA, que irá protocolar o documento na PDDE e então devolver uma cópia para AC, confirmando o seu recebimento, devidamente protocolado. A AA envia o documento para o destinatário, através de um diretório público, correio tradicional ou diretamente para o usuário.

5.3.6.3 ACCP - Autoridade de Certificação de Chave Privada

A autoridade de certificação de chave privada é uma autoridade que irá emitir chave privada específica para um determinado usuário final, após um acordo prévio, por exemplo, ao participar de uma licitação, o concorrente envia a sua proposta devidamente criptografada e para que a proposta seja aberta é emitida a chave privada.

5.3.6.4 Tabeliões

Os serviços de tabeliões serão usados para confirmarem identidades de assinantes, reconhecer certificados e autenticar as solicitações de AC e de usuários de certificados de nível mais alto de segurança.

8.3.6.5 Publicações

As publicações poderão ser efetuadas a qualquer hora pela AC. As emendas à DPC, certificados, avisos de suspensão ou revogação e informações relevantes serão publicadas nos repositórios. Os certificados ao serem emitidos e aceitos por seus requerentes, devem ser publicados no Diário Oficial da União. No caso de certificados emitidos em países estrangeiros, deverá ser feita a publicação em um Diário Oficial do País.

8.4 Infra-estrutura de Certificação

Esta seção trata dos serviços de certificados, das classes de certificados, das informações para aquisição de certificados, das extensões e da ICP da UFSC.

8.4.1 Classes de Certificados

A AC suporta duas classes de certificados. Cada classe oferece um nível de confiança e características diferenciadas e em ordem crescente, sendo a classe 1 a de mais baixo nível de segurança, destinada para uso de e-mail e o de classe 2 mais alto nível de segurança, destinado para uso de *Site*. São os usuários que determinam e avaliam

qual a classe ideal para a finalidade desejada. Todas as classes podem ser emitidos para pessoas físicas e jurídicas.

8.4.1.1 Certificados de classe 1

Os certificados de classe 1 são os de mais baixo nível de segurança, apesar de poderem ser emitidos para todos, é indicado apenas à indivíduos para fins de uso de e-mail. Os certificados de classe 1 confirmam que o nome do usuário e seu endereço de correio eletrônico formam um nome de sujeito não ambíguo.

Os certificados de classe 1 são comunicados aos usuários via correio eletrônico e acrescentados ao demais certificados disponíveis, para que o usuário faça o seu download. Esta classe é basicamente utilizado para navegação na internet e para correio eletrônico pessoal, possibilitando a comprovação da origem de envio. Eles não devem ser usados para uso comercial.

À AC deve possuir *software ou hardware* confiáveis para a proteção da chave privada da AE de classe 1, contra o comprometimento, para os assinantes individuais, recomenda-se o uso de *software* de criptografia.

8.4.1.2 Classe 2

Os certificados de classe 2 possuem um nível de segurança mais elevado do que a classe 1, também indicados para indivíduos. A sua utilização é indicada para uso de *site*. Os dados enviados na solicitação, pertinentes ao assinante são confirmados em banco de dados de terceiros, mediante a aprovação dos dados, então a AC irá verificar o endereço postal e em seguida procederá a emissão.

A proteção da chave privada da AC de classe 2 contra o comprometimento, será feita pelo uso obrigatório de *hardware* confiável, já para a chave privada do assinante, será obrigatório o uso de *software* de criptografia.

8.4.2 Confirmação das Informações da Identidade do Assinante

As ACs tomam medidas para confirmar a identidade do candidato, durante o processo de certificação, estas medidas dependem da classe de certificados, variando entre a simples verificação do e-mail ao comparecimento do candidato perante a AC, representante ou confirmação por um tabelião.

8.4.3 Informações confidenciais

São todas as informações pessoais ou corporativas mantidas pela AC ou AR, que não são disponíveis para o público, as quais não podem ser reveladas, vendidas, divulgadas sem o consentimento do usuário ou por determinação judicial. As informações confidenciais são: os registros de solicitação de AC, contratos com assinantes e registros de solicitação de certificados, registros de transações, calendário e relatório de auditoria, planejamento de contingências, planos de recuperação de desastres, procedimentos internos de segurança, medidas de segurança que controlem as operações de *hardware e software*, acordos de certificação.

As informações contidas em um certificado, repositório, LCR, *Web*, disponíveis para o público não são consideradas confidenciais.

8.4.4 Hierarquia de ICP

Os serviços de certificação digital pública são implementados por uma hierarquia de infra-estrutura de chaves públicas, comporta pelas entidades abaixo.

8.4.4.1 AC-Raiz - Autoridade Certificadora Raiz

A AC-raiz é a AC de mais alto nível em uma cadeia de certificados, que emite certificados para as AC inferiores na hierarquia. Usa algoritmo RSA e o tamanho de sua chave é de 4096 bites e a sua validade de 8 (oito) anos.

Dispositivos de *hardware* confiáveis são usados para criar, proteger, gerenciar e até destruir a chave privada. Determinadas partes secretas devem ser copiadas e

asseguradas por detentores de partes secretas.

5.4.4.2 AC - Autoridade Certificadora

Cada AC é subordinada a uma outra AC, a AC-raiz. As ACs podem emitir, gerenciar e revogar certificados de assinantes/usuários finais. Para criar, proteger, gerenciar e destruir as chaves privadas das ACs é utilizado um dispositivo de *hardware* confiável. As ACs utilizam o algoritmo RSA e o tamanho de sua chave é de 2048 bits. As ACs podem pertencerem a entidades públicas ou privadas.

5.4.4.3 AR - Autoridade de Registro

As ARs são as entidades responsáveis por receberem as solicitações de certificados, por verificar, avaliar, aprovar ou rejeitar as solicitações, dependendo do resultado da avaliação enviam a solicitação para a AC pertinente. A verificação das informações é executada de acordo com a classe do certificado. Para realizar estas verificações a AC poderá utilizar instrumentos, tais como: documentos precedentes de tabelas, executados corretamente; documentos reconhecidos de identificação, como passaporte, carteira de identidade e o comparecimento do requerente. Para a classe 1 é utilizada uma validação do e-mail para somente UFSC.

5.4.4.4 Repositórios

Toda a AC deve manter um repositório a disposição do público para armazenar, recuperar e consultar certificados e outras informações relacionadas aos certificados. Um repositório é um banco de dados para armazenar certificados, DPCs, LCRs, e outras informações relevantes. As informações são disponibilizadas pelo site da AC, neste caso <http://ac.labsec.ufsc.br>.

5.4.4.5 LCR - Lista de Certificados Revogados

A LCRs são listas nas quais as ACs publicam os certificados revogados ou suspensos. A publicação se dá periodicamente. As informações disponíveis na LCR

são: o número de série do certificado, nome do proprietário, data de vencimento.

8.5 Exigências e Controles Técnicos de Segurança

Esta seção apresenta o processo de geração e proteção das chaves do assinante, de auditoria e retenção de registros da auditoria, planejamento e contingência de recuperação de desastres, gerenciamento e prática de pessoal. Os SCP suportam uma série de mecanismos desenvolvidos e projetados para proteger a comunicação e as informações. Estes mecanismos se fazem necessários, porque os SCP por si só não constituem todos os mecanismos.

8.5.0.6 Geração de chaves de ACs

A AC deve solicitar o par de chaves, que poderá ser gerado pela AC-raiz ou por outra entidade emissora de chaves confiável e reconhecida. Após a geração do par de chaves, a AC envia a chave pública para AC superior juntamente com a solicitação de certificado.

8.5.0.7 Proteção da Chave Privada da AC

A AC usa dispositivos de *hardware e software* confiáveis para proteger a chave privada. A AC poderá usar também um detentor de partes secretas para proteger a sua chave privada. A implementação de sistemas de segurança serão de acordo com as classes de certificado.

8.5.0.8 Geração das Chaves de Assinantes

Antes de iniciar o processo de solicitação de certificado, o candidato deve gerar seu par de chaves. A chave pública deve ser enviada a AC juntamente com a solicitação de certificação. O requerente pode solicitar o par de chaves da própria AC ou de outra emissora de chaves, desde que seja confiável e reconhecida.

8.5.0.9 Proteção de Chaves Privadas de Assinante

A proteção das chaves privadas de assinantes é de inteira responsabilidade do proprietário, devendo ser protegida de acordo com a classe do certificado. As ACs não detêm as chaves privadas e a responsabilidade da segurança da mesma é inteiramente do assinante, devendo evitar perda, comprometimento, divulgação, modificação ou utilização indevida. Caso o assinante queira fazer uma cópia da chave privada e armazená-la em local próprio, estando sob inteira responsabilidade do assinante.

8.5.1 Detentores de Partes Secretas

Os detentores de partes secretas são órgãos que detêm partes secretas de chaves privadas de AC, que queiram aumentar a de sua(s) chave(s) privada(s) e recuperação da mesma. Os detentores para aceitar uma parte secreta devem ter observado a criação e distribuição da mesma. O detentor receberá a parte secreta em meio físico seguro, fará uma inspeção sobre a integridade da mesma, e irá confirmar ou não se aceita deter esta parte.

8.5.1.1 Proteção da Parte Secreta

O detentor da parte secreta deverá utilizar sistemas confiáveis para proteger a parte secreta de qualquer tipo de comprometimento, compromete-se a não divulgar, copiar, disponibilizar ou utilizá-la de forma indevida, somente perante autorização do proprietário ou autorização registrada e autenticada por cartório, poderá disponibilizar ou liberar as partes secretas. No caso de desastre, o detentor deverá entregar a parte secreta pessoalmente ao responsável pela AC e acompanhar todo o processo de recuperação do desastre, porém antes de fazer esta entrega, o detentor deverá certificar-se sobre a veracidade do desastre e autenticar uma declaração que está entregando a parte secreta à AC.

8.5.2 Instalações da AC

A AC deverá operar em instalações confiáveis o acesso físico deve ser controlado por sistemas de segurança. O local onde contém os *softwares e os hardwares*, deverá possuir sistemas de segurança que não permita o acesso de pessoas não-autorizadas e sozinhas. O acesso a este local deverá ser controlado por cartões ou chaves e a presença de apenas uma pessoa no local é proibida. Esta área é denominada área de duas pessoas.

8.5.3 Proteção de *Hardware*

A proteção do *hardware* da AC poderá ser feita usando módulos criptográficos aprovados e confiáveis, permitindo as operações que usam chave privada. O acesso ao mesmo só será feito com identificação e autenticação do usuário. Os equipamentos das ACs localizam-se em salas separadas, trancadas com chaves. O uso de um certificado para o *hardware* é de grande valia.

8.5.4 Escolha de Métodos Criptográficos e Assinatura Digital

O usuário é livre para escolher o *software, hardware* e os algoritmos a serem usados, porém é necessário que sejam compatíveis, confiáveis e conhecidos.

8.6 Ciclo de Vida dos Certificados

Esta seção apresenta os 7 (sete) itens que fazem parte do ciclo de vida dos certificados. Estes 7 (sete) itens fazem com que o processo de certificação ocorra sem erros e de maneira confiável. A figura que representa este ciclo é apresentada no capítulo 7, seção 7.5.

8.6.1 Solicitação de Certificados

Esta seção demonstra o processo de solicitação de um certificado.

8.6.1.1 Procedimentos para a Solicitação de Certificados

Os procedimentos para solicitação de certificados incluem exigências referentes à geração, proteção do par de chaves e lista de informações necessárias para cada classe de certificado. O candidato a certificado deve gerar um par de chave e demonstrar a AC pertinente, garantir a segurança da chave privada, determinar um nome distinto e preencher uma solicitação e enviá-la à AC pertinente, anexando a chave pública. O candidato deverá ler o acordo de certificação antes de solicitar um certificado.

8.6.1.2 Informações e Comunicações da Solicitação de Certificados

Para cada classe de certificado é exigida informações, algumas são comuns para todas as classes, outras são únicas para a aquela classe. Nem todas as informações aparecem no certificado, as que não aparecem em um certificado são mantidos em regime de confidencialidade pela AC. A tabela abaixo apresenta algumas informações obrigatórias para solicitação de certificado.

Tabela 8.1: Informações Obrigatórias

Classe 1	<p>Informação: nome comum (ou alias), chave pública do candidato, endereço de correio eletrônico, contrato de assinante assinado, informações da forma de pagamento. Envio da solicitação: a AC envia um protótipo de certificado e um contrato do assinante para o candidato. O candidato deverá preencher esta caixa de diálogo <i>on-line</i> através de um canal seguro da internet, com o preenchimento desta caixa o assinante está afirmando que as informações são precisas e que as leu, entendeu e concorda com os termos do candidato. Após concluídos os procedimentos pela AC, esta envia ao assinante, pelo endereço eletrônico, uma mensagem com um número de identificação pessoal, autorizando a aquisição do certificado junto a AC.</p>
Classe 2	<p>Informação: nome distinto proposto, endereço de residência completo, telefone, endereço eletrônico, chave pública do sujeito, informação sobre a forma de pagamento, número de inscrição na previdência social, data de nascimento, fi-ase de identificação (usada para identificar o assinante perante a AC), contrato de assinante assinado e carteira de identidade e CPF. Informações opcionais: Empregador, nome do cônjuge, endereços anteriores e outras informações solicitadas pela AC. O processo de envio de solicitação é igual ao da classe 1.</p>

8.6.2 Validação de certificados

A validação de solicitação de certificados apresentam exigências executadas pela AC pertinente, descritas nas próximas seções.

8.6.2.1 Exigências para a Validação da Solicitação de Certificado

Ao receber uma solicitação de certificados a AR deverá efetuar todas as validações obrigatórias como pré-requisito para a emissão. A AR deverá confirmar se: o candidato é a pessoa identificada na solicitação, se detém a chave privada correspondente a pública enviada juntamente com a solicitação, as informações fornecidas são precisas, os representantes estão devidamente autorizados e se o candidato aceita os termos e condições empregadas pela AC. Se todas as informações se confirmarem a AR envia a AC a solicitação de certificado.

8.6.2.2 Itens a Serem Confirmados

Cada classe de certificado possuem itens diferenciados a serem confirmados, para a validação da solicitação de certificados. Os itens a serem confirmados para cada classe são:

classe 1 exige uma validação do e-mail para somente UFSC;

classe 2 exige a confirmação automatizada por terceiros de dados pessoais, confirmação do endereço eletrônico

8.6.2.3 Aprovação de Solicitação de Certificados

Com o êxito obtidos em todas as validações e confirmações exigidas para aprovação de um certificado, independente da classe, a AR deverá aprovar a solicitação e enviá-la para AC emitir o certificado. A emissão do certificado é a confirmação da aprovação da solicitação do certificado.

S.6.2.4 Rejeição de Solicitação de Certificado

Quando a aprovação de uma solicitação não ocorrer, a AR deverá rejeitar a solicitação, notificando o candidato sobre a rejeição e o motivo pelo qual houve a rejeição. Caso a falha ocorra em informações contidas em banco de dados, a AR deverá fornecer ao candidato o contato com a empresa de banco de dados para investigação e solução da controvérsia. O método de envio da notificação deverá ser o mesmo de envio da solicitação.

8.6.3 Emissão de Certificados

A AC emite um certificado após receber a solicitação aprovada pela AR. A emissão do certificado significa a aprovação final da solicitação pela AC. O certificado passa a ser válido a partir do momento em que o assinante aceita-o (verificar item de aceitação).

8.6.3.1 Consentimento do Assinante para a Emissão do Certificado

A AC não pode emitir certificados sem o consentimento do candidato. A própria solicitação juntamente com o contrato de assinante assinado pelo candidato, é considerado como aceitação para emissão.

8.6.3.2 Recusa Quanto a Emissão de um Certificado

A AC poderá recusar-se a emitir um certificado qualquer, a seu critério, sem responsabilizar-se por prejuízos ou despesas resultantes da recusa. No entanto a AC deverá reembolsar, imediatamente todos os valor pagos até então pelo assinante, exceto se as informações forem falsas ou fraudulentas.

8.6.3.3 Representações de AC Mediante a Emissão de Certificados

A AC promete ao assinante, que não há falhas de representações de fatos no certificado, não há erros nas transcrições dos dados enviados a AE pelo candidato e o

certificado atende a todas as exigências da DPC. A AC também promete que empenhará os melhores esforços consistentes com a DPC para revogar ou suspender certificados e notificar os assinantes de quaisquer fatos que afetem a validade e do certificado.

5.6.3.4 Tempo para Emissão de Certificados

Assim que todas as informações de solicitação forem confirmadas, a AC deverá emitir os certificados imediatamente. O tempo para a emissão de certificados é estabelecido de acordo com o nível de exigências para confirmação de solicitação de cada classe de certificado. No caso da classe 1, a emissão dar-se-a imediatamente após a validação do e-mail somente para UFSC.

8.6.3.5 Período de Validade de Certificados

A validade de cada certificado começa assim que o assinante o aceita, porém o término da validade depende da classe e finalidade do certificado. Os certificados tanto de classe 1 como de classe 2 destinados a usuários físicos valem por um ano.

Os certificados de classe 1 e classe 2, emitidos para AC possuem validade de 4 (quatro) anos.

8.6.4 Aceitação de Certificados

Os meios de aceitação de um certificado variam de acordo com a classe do mesmo.

Os meios de aceitação de certificados são: tanto para classe 1 como para classe 2 por via *on-line*, onde o candidato digita seu número de identificação pessoal e aceita o certificado e por correio eletrônico, o candidato envia uma correspondência eletrônica aceitando o certificado.

8.6.4.1 Representações dos Assinantes Mediante a Aceitação

Ao aceitar um certificado, o assinante garante que nenhuma pessoa não-autorizada teve acesso a sua chave privada, que todas as informações contidas no certifi-

cado são verdadeiras, o uso do certificado esta sendo exclusivo para os fins legais autorizados. O assinante, ao aceitar um certificado, concorda com os termos e condições da DPC.

S.6.4.2 Publicações de Certificados

Imediatamente após a emissão de vmi certificado, a AC deverá publicá-lo em repositório e no Diário Oficial da União.

8.6.5 Uso de Certificados

O uso de certificados é autorizado através da verificação da assinatura digital.

8.6.5.1 Verificação de Assinaturas Digitais

A verificação da assinatura digital determina se assinatura digital foi criada pela chave privada correspondente a chave pública listada no certificado do signatário e se a mensagem associada não foi alterada desde a criação da assinatura digital. Algumas formas de verificação de assinaturas digitais são: estabelecimento e confirmação da cadeia de certificação para a assinatura digital, garantia de que a cadeia encontrada é a mais adequada para a assinatura digital, indicação da data e hora de criação da assinatura digital, definição das garantias desejadas pelo signatário.

8.6.5.2 Falhas na Verificação da Assinatura Digital

A pessoa ou entidade que confiar em uma assinatura digital, que não permita a sua confirmação ou que estiver com falhas, estará assumindo todas as responsabilidades de riscos e se isentando de qualquer direito pelo uso da assinatura.

8.6.5.3 Escritas e Assinaturas

As mensagens com assinaturas digitais possuem o mesmo valor das mensagens escritas e assinadas em papel. As assinaturas digitais possuem a mesma vali-

dade das assinaturas manuscritas, desde que a verificação por referência a chave pública, possa ser executada.

8.6.6 Suspensão / Revogação de Certificados

Os certificados podem ser suspensos e ou revogados caso, haja motivos que venham ocasionar tal ato. Motivos estes descritos a seguir.

8.6.6.1 Motivos Gerais para Suspensão ou Revogação

Os motivos pelos quais um certificado pode ser revogado ou suspenso são: o comprometimento, roubo, perda, modificações e divulgação da chave privada do assinante; a violação de obrigações dispostas na DPC pelo assinante, ações causadas por desastres naturais, falta de pagamento de tarifas e taxas, atraso ou impedimento no desempenho das obrigações, mudanças no estatuto, falhas em comunicações e outras ações consideradas relevantes pela AC.

5.6.6.2 Suspensão ou Revogação de um Certificado de AC

A AC deverá fazer esforços adequados e possíveis para suspender ou revogar um certificado de uma AC subordinada, independente do consentimento da AC subordinada, caso um fato material representado no certificado for conhecido ou tido como falso; os certificados também podem ser revogados ou suspensos pelos motivos gerais, especificados na seção 8.6.6.1.

5.6.6.3 Suspensão ou Revogação Mediante Solicitação da AC

A suspensão ou revogação de certificados de ACs, podem ser executados, mediante solicitação de um representante devidamente autorizado de uma AC subordinada. A solicitação de suspensão ou revogação deve estar devidamente assinada digitalmente, ou pode ser solicitação autêntica.

5.6.6.4 Suspensão ou Revogação Mediante Solicitação do Assinante

A AC poderá revogar ou suspender um certificado, mediante vima solicitação do assinante, devidamente assinado digitalmente, após a confirmação de que a pessoa solicitante é de fato o assinante.

8.6.6.5 Revogação Devido a Emissão com Falhas

A AC irá revogar um certificado imediatamente, após a descoberta e a confirmação de que a emissão não está de acordo com os procedimentos exigidos na DPC.

5.6.6.6 Avisos e confirmação de Suspensão ou Revogação

Assim que a AC revogar ou suspender um certificado, este deverá ser publicado imediatamente na LCRs, emitido um aviso ao assinante, notificando-o sobre a revogação ou suspensão, pelos mesmos meios de envio de solicitação. A emissão da LCRs devem ser periódica.

5.6.6.7 Proteção da Chave Privada após a Revogação

Mesmo após a suspensão ou revogação de certificados, as chaves privadas devem ser mantidas sob sigilo, até a possibilidade de sua destruição.

8.6.7 Vencimento do Certificado

A AC deve emitir notificação aos assinantes sobre o vencimento do certificado, através de correio eletrônico, para que o assinante fique ciente sob o vencimento do seu certificado.

8.6.7.1 Efeitos do Vencimento de um Certificado

O fato de um certificado ter vencido, não implicará na validade das obrigações contratuais, criadas ou comunicadas mediante a DPC.

8.6.T.2 Utilização de um Certificado Vencido

A utilização de um certificado vencido é de inteira responsabilidade da pessoa, que continua a usa-lo ou confiar. As ACs não responsabilizam-se pelo uso de certificados vencidos.

S.6.7.3 Renovação e Reinscrição de Assinantes

O processo para renovação e reinscrição de assinantes é igual ao inicial, de acordo com a classe de certificado.

8.7 Conclusão

o desenvolvimento deste documento servirá para que, o processo de certificação ocorra dentro das normas tanto das leis nacionais como das necessidades dos usuários e das ACs. A DPC estabelece as normas e regras para o devido cumprimento das ações pelas partes interessadas na certificação.

Capítulo 9

Considerações Finais

Pelos estudos realizados para a elaboração desta dissertação, foi possível verificar, que o uso de métodos de segurança, como criptografia, assinatura digital, ICP e certificados digitais no mundo atual tomou-se imprescindível. Com o uso da Internet, surgiram novas aplicações como o comércio eletrônico, o *home-banking* e outras, possuindo informações confidenciais como números de cartões de crédito, que são enviadas e processadas em meios de comunicação que não oferecem , observando esta questão, percebe-se a importância da segurança da Internet.

O primeiro objetivo específico desta dissertação foi estudar os "fundamentos da criptografia e da ICP". Este objetivo foi alcançado e está relatado nos capítulos 2 e 3 (Fundamentos de Criptografia e infraestrutura de chaves públicas). Este objetivo é fundamental para o entendimento do funcionamento da criptografia e da ICP e também porque estes fundamentos são utilizados na emissão de certificados digitais, e para que ocorra esta emissão é necessário documentos para regularizarem este processo, conhecido como PC e DPC. A criptografia simétricas e assimétricas garantem o sigilo em uma comunicação. O certificado digital relaciona a chave privada a um usuário, garantindo assim que a aplicação desta chave privada somente poderá ser feita por este usuário. O entendimento da Infra-estrutura de Chaves Públicas é importante, porque ela define os procedimentos para expedição de certificados digitais.

Para que as técnicas de criptografia, assinatura digital, ICP, certificados

digitais garantam a segurança e a de transações eletrônicas, existem os padrões dos quais, abordamos alguns, como PKCs #7, PKCs #10, RSA, DPC, etc.

O segundo objetivo específico alcançado foi "levantar os padrões de PC e DPC existentes". Para realizar este levantamento, foi pesquisado as entidades emitentes de certificados digitais, tanto nacionais como internacionais, a RFC 2527, que trata do conteúdo de uma PC e da DPC e também artigos científicos.

O terceiro objetivo específico alcançado foi "estudar as PC e DPCs das principais entidades certificadoras nacionais e internacionais". Para realizar este estudo, aproveitou-se o levantamento dos padrões das PCs e DPC, e pesquisou-se as entidades de renome conhecidas por sua excelência na área de segurança. Através do estudo realizado sobre as PCs e as DPCs de destas entidades, percebe-se a importância destes documentos para que as tecnologias de segurança funcionem corretamente.

O quarto objetivo específico almejado foi "fazer uma comparação das DPCs estudadas". Este objetivo foi fundamental para a elaboração do capítulo 6 desta dissertação. Para realizar a comparação, após o estudo das PCs e DPCs das principais entidades certificadoras, selecionou-se duas, *VeriSign* e *Entrust.NET* e mais a ICP-Brasil. A comparação realizada das DPCs da *VeriSign*, *Entrust.NET* e ICP-Brasil, mostrou que há muitas diferenças, e muitas semelhanças e que cada entidade elabora sua DPC de acordo com algumas regras e com suas necessidades.

O quinto objetivo específico foi realizar um "estudo do modelo de Certificação Digital da UFSC". O estudo deste modelo foi de fundamental importância para a elaboração da PC e da DPC para UFSC descrito no capítulo 6 da dissertação.

O sexto e o sétimo objetivo específico são para "propor uma Política de certificados e uma DPC para UFSC". Estes objetivos foram desenvolvidos principalmente para suprir uma falta, há de um documento que estabelecesse os procedimentos, regras e normas de funcionamento da AC da UFSC. Chegou-se a este modelo após o estudo de padrões, de DPC de outras entidades, pela comparação de DPC e principalmente pelo estudo da estrutura da UFSC.

A criação de um modelo de DPC, para uma AC, poderá tomar-se de fundamental importância para a expansão do uso dos certificados no Brasil. Este modelo

poderá ser usado por outras ACs para a elaboração de suas próprias DPC, este fato poderá estar contribuindo para o crescimento de entidades certificadoras e conseqüentemente aumentar a disseminação da certificação digital.

9.1 Proposta de Trabalhos Futuros

A constante e crescente evolução da internet e das tecnologias de segurança da internet, nos levam a cada dia buscar novos meios de garantir a segurança e o cumprimento de leis, regras e normas. Portanto o estudo constante das políticas e das DPC faz-se necessário para que as atualizações necessárias sejam feitas a fim de garantir o cumprimento das leis, normas e regras. Há portanto muito a ser estudado e feito ainda para conseguir viabilizar o processo de elaborar uma PC e uma DPC, mais rapidamente que nos dias atuais. Muito do que falta fazer, poderá estar facilitando este trabalho, tal como imia ferramenta que auxilie na geração de uma DPC ou uma PC.

O desenvolvimento de uma ferramenta deste porte será de extrema importância para as ACs em geral, até mesmo para as ACs de pequenos porte ou de uso interno, que não acham necessário a utilização de *um* documento para estabelecer as regras de uso. A existência de uma ferramenta para auxiliar na elaboração de uma PC ou DPC, eliminaria o tempo demandado para elabora-lá manualmente e em poucos minutos poderia-se ter uma PC ou DPC. A demanda de trabalho para tal, seria especificar a estrutura da AC, para que a ferramenta, de acordo com dados da AC, elaborasse a PC e DPC. A seguir será elencados alguns item a serem estudados no futuro:

- Estudar a viabilidade de se implementar uma ferramenta para auxiliar a elaboração de PCs e DPCs;
- Estudar como seria o funcionamento desta ferramenta;
- Propor um protótipo da ferramenta;
- Desenvolver a ferramenta de auxílio à elaboração de PC e DPC;
- Desenvolver a ferramenta de verificação automática;

- Testar a ferramenta desenvolvida;

Referências Bibliográficas

- [AJ 99] AUDUN JOSANG, H. M.; LU, M. The development of public key infrastructures; are we on the right path? Norwegian Informatics Conference (NIK'99), [S.I.], 1999.
- [AJ 00] AUDUN JOSANG, I. G. P.; POVEY, D. PKI seeks a trusting relationship. ACISP 2000, [S.I.], 2000.
- [ASS 00] ASSOCIATION, E. M. Federal Bridge Certification Authority - Initiative and Demonstration. Disponível em <http://crsc.nist.gov/pki/documents/emareportJ0001015.pdf>
- [BRO 01] BROCARDI, M. L. IZAC: Um Protocolo Criptográfico Para Análise Segura de Crédito. Universidade Federal de Santa Catarina - UFSC, 2001. Dissertação de Mestrado.
- [CAN 99] CANADA, G. D. Public key infrastructure management in the government of Canada. Treasury Board of Canada Secretariat, 1999. Relatório Técnico.
- [FEG 99] FEGHHI, JALAL, J. F.; WILLIAMS, P. Digital Certificates. 1. ed. Addison Wesley, Setembro, 1999.
- [FIP]
- [Gui 00] Guidelines, Methodologies and Standards to set up a CA for Digital Signature. Internet.
- [HOU 01] HOUSLEY, R.; POLK, T. Planning for PKI - Best Practices Guide for Deploying Public Key Infrastructure. 1. ed. Wiley Computer Publishing, 2001.
- [HOW 95] HOWES, T. A. The lightweight directory access protocol: X.509 lite. CITT, [S.I.], 1995.
- [IET 97] IETF, editor. Lightweight Directory Access Protocol (V3) - LDAP, <http://www.ietf.org/rfc/rfc2251>, 1997.
- [IET 99] IETF, editor. SPKI Certificate Theory, www.ietf.org/rfc/rfc2693.txt, 1999.
- [IGN 02] IGNACZAK, L. Dissertação de Mestrado. Universidade Federal de Santa Catarina - UFSC, 2002. Dissertação de Mestrado.

- [IT 01] ITU-T. Recommendation X.509. Draft.
- [KIN 97] KINGDON, K. W.; JR., B. S. K. Extensions and revisions to PKCS #7. An RSA Laboratories Technical Note, [S.I.], 1997.
- [LAB 93] LABORATORIES, R. PKCS #7: Cryptographic Message Syntax Standard. Version 1.5.
- [LAB 00] LABORATORIES, R. Pkes #10 v1.7 ; Certifi cation request syntax standard. RSA Laboratories, Maio, 2000. Relat'orio t'eenieo.
- [POL 00] POLK, W. T.; HASTINGS., N. E. Bridge certifi cation authorities: Connecting B2B public key infrastructures. Natonal Institute of Standards and Technology, [S.I.], 2000.
- [RFC 99] RFC, editor. Internet X.509 Public Key Infraestruturura - Certifi cate Policy and Certifi cation Practices Framework, <http://www.ietf.org/rfc/rfc2527.txt/number=2527>,1999. Network Working Graoup.
- [RIV 02] RIVEST, R. E-Mail. Consulta via e-mail - rivest@mit.edu.
- [ROC 01] ROCHA, J. L. F. Proteção de Software Por Certifi capo Digital. Universidade Federal de Santa Catarina - UFSC, 2001. Dissertaç ~ao de Mestrado.
- [RUS 01] RUSSHOUSLEY; POLK, T. Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure. John Wiley Sons, 2001.
- [SCH 96] SCHNEIER, B. Applied Cryptography - Protocols Algorithms, and Source Code in C. Segunda, ed. John Wiley & Sons, Inc, 1996.
- [SCH 00] SCHNEIER, B. Secrets and Lies: Digital Security in a Networked World. Editora John Wiley Computer, 2000.
- [SL 01] STEVE LLOYD, DAVID FILLINGHAM, R. L. S. O.; WEIGELT, J. CA-CA interoperability. TWG, [S.I.],2001.
- [STA 98] STALLINGS, W. Cryptografi a and Network Security. Prentice Hall, 1998.
- [STA 99] STALLINGS, W. Network Security Essentials: Applications and Standards. Ed. Prentice Hall, 1999.
- [STI 95] STINSON, D. R. Cryptography - Theory and Practice. 1. ed. CRC Press LLC, 1995.
- [STI02] STINSON, D. Cryptography: Theory and Practice. 2. ed. Chapmam & Hall, 2002.
- [TER 00] TERADA, R. Seguranç a de Dados - Criptografi a Em Redes de Computadores. Rua Pedroso Alvarenga, 1245 SP: Editora Edgard Blucher Ltda, 2000.

Apêndice A

Proposta de Ferramenta para Auxiliar no Desenvolvimento de PC e DPC

A.1 Introdução

Estudar a viabilidade de desenvolver uma ferramenta de auxílio à construção e verificação automática de PC e DPC, destinada as ACs. Com o desenvolvimento de uma ferramenta que auxilie a construção e verificação de PC e DPC, as ACs iriam automatizando o processo e eliminando o tempo gasto. O que levaria uma semana para ser elaborado, poderá ser feito em poucas horas.

A.1.1 Objetivo

Propor o desenvolvimento de uma ferramenta para auxiliar a elaboração e verificação automática de PCs e DPCs.

A. 1.2 Justificativa

As ACs precisam elaborar documentos que regulamente se processos de certificação. A elaboração destes documentos é bastante demorada, pois há necessidade de levantar as leis, normas, regras do país e também a estrutura, as necessidades da AC.

Com a existência de uma ferramenta que já contestes estas regras, normas, em fim uma estrutura que ao ser inserida a estrutura e as necessidades da AC, auxilia-se os responsáveis pela a AC, a elaborar a PC e a DPC. As ACs estariam eliminando um enorme tempo que seria gasto com tal procedimento, e ao mesmo tempo poderia estar garantindo que a DPC e a PC foram corretamente elaborados.

A possibilidade de uma ferramenta estar fazendo a verificação automática, estaria facilitando o manuseio por parte do usuário e garantindo que o mesmo não cometesse algum engano, do tipo fazer uma verificação errônea.

A. 1.3 Desenvolvimento da ferramenta

Quando se possui uma ferramenta para nos auxiliar em qualquer desenvolvimento seja de um documento ou de algum *software*, passa-se a ter vantagem e desvantagem, pois tudo possui um lado positivo e outro negativo.

A viabilização de desenvolver uma ferramenta de auxílio à construção e verificação de PC e DPC, facilitaria e agilizaria o desenvolvimento dos mesmos pela AC e proporcionaria a facilidade da verificação da PC e da DPC pelo usuário. Evitando assim a demora, que poderá ser causada pela falta de um atalho para que a verificação seja realizada, ou pela falta de prática e conhecimento do usuário, e também poderá evitar que um usuário, por inexperiência faça uma verificação errada.

Para o desenvolvimento de uma ferramenta é necessário recursos físicos, financeiro/econômicos e humanos. Hoje no Brasil e até mesmo em outros países, ainda existem poucas ACs, levando-se em consideração outras empresas de outros produtos. Este fato poderia estar dificultando o desenvolvimento, pela falta de comercialização, mas ao mesmo tempo, pode ocorrer o contrário, e ocorrer um aumento considerável de ACs. Outro fator seria o fato de que no mundo da segurança tudo é imprevisível, poderia estar ocorrendo mudanças radicais e as ACs serem obrigadas a fazerem constantes mudanças em suas estruturas e normas, se não radicalmente, mas rapidamente para atender as novas necessidades do mercado, e com isso, a ferramenta teria que estar sofrendo constantes ajustes e assim estaria compensando o investimento feito para o seu desenvolvimento.

tanto do tempo físico quanto do financeiro. Sem contar a parte financeira, pode-se pensar no tempo gasto cada vez que a AC precisasse refazer uma PC ou uma DPC manualmente, quanto tempo estaria perdendo, e possuindo a ferramenta poderá fazer tudo em muito menos tempo.

A. 1.4 Vantagens

As vantagens de se construir uma ferramenta que auxilie a elaboração e verificação automática da mesma são:

- Agilizar o processo de elaboração de PCs e DPCs, para as AC;
- Quando houvesse modificações na estrutura da AC ou até mesmo em leis, estes seriam rapidamente repassados para a PC ou DPC;
- Uma correta elaboração de PC e DPC, de acordo com a estrutura da AC, irá garantir a segurança dos seus serviços;
- A conferência automática irá favorecer a todos os usuários e principalmente aos que não possuem muita habilidade no processo de certificação;
- O tempo gasto para efetuar uma verificação seria praticamente eliminado.

A. 1.5 Desvantagens

As desvantagens de se possuir uma ferramenta que auxilie na elaboração e verificação de PC e DPC podem ser:

- Devido ao fato de que cada AC possui uma estrutura diferenciada das outras, a ferramenta terá que sofrer algumas adequações para poder atender determinada AC.
- O custo de implementação da ferramenta;

A. 1.6 Recursos Físicos e lógicos Necessários

Os equipamentos para a implementação da ferramenta terão que ser equipamentos condizentes com os utilizados hoje pelas empresas de segurança, utilizando componentes da mais alta tecnologia para garantir a segurança do serviço que será prestado pela ferramenta. As ferramentas lógicas *software* de desenvolvimento deverão do mesmo padrão tecnológico, além de algumas ferramentas específicas para estabelecer determinadas condições, tais como: ferramenta de modelagem, de agentes, etc.