Política de Certificação

Assinatura Digital

Autoridade Certificadora Claretiano

PC DA AC CLARETIANO
Versão 2.0 - 07 de Maio de 2019

Declaração de Prática de Certificação e Política de Certificação para Assinatura Digital Tipo A1 – PRÓPRIO - da Autoridade Certificadora CLARETIANO - REDE DE EDUCAÇÃO

Com o objetivo de implantar um processo e estrutura informatizada para digitalização, assinatura digital, armazenamento e recuperação de informações acadêmicas o Claretiano - Rede de Ensino implanta a solução Secretaria Acadêmica Digital – SeAD, uma metodologia criada para transposição de documentos, procedimentos e processos que se encontram em meio físico nas secretarias acadêmicas e de cursos para o meio digital.

Para a execução desta metodologia são necessárias alterações na gestão dos documentos, processos e procedimentos acadêmicos: o papel será substituído pelo documento eletrônico; a assinatura física será substituída por uma assinatura digital; e o arquivo físico de documentos será substituído por mídias digitais.

Para o processo de assinatura digital, serão utilizados os certificados digitais disponibilizados pela Autoridade Certificadora Claretiano - Rede de Educação, criado para assegurar o cumprimento das regras estabelecidas neste documento.

Esta Declaração de Práticas de Certificação (DPC) e Política de Certificação (PC) estabelece os requisitos a serem obrigatoriamente observados pela AC CLARETIANO na emissão dos certificados digitais. Estes requisitos obedecem às exigências da legislação brasileira e se enquadram nas melhores práticas internacionais para a emissão de certificados de assinatura do tipo PRÓPRIO/INTERNO.

Este documento tem como objetivo estabelecer as regras e parâmetros para o uso da certificação digital dentro dos projetos desenvolvidos pelo Claretiano - Rede de Educação que necessitam de garantias de autenticidade, integridade e validade jurídica em meio digital.

1. Introdução

Esta "Declaração de Práticas de Certificação" (DPC) e "Política de Certificação" (PC) descreve as regras para emissão e uso de certificados de Assinatura Digital Tipo A1 – PRÓPRIO - da Autoridade Certificadora Claretiano - Rede de Educação, conforme previsto no § 2º, art. 10 da MP 2.200-2, de 24 de agosto de 2001.

A estrutura desenvolvida e implantada permite ao Claretiano - Rede de Educação emitir certificados digitais aos seus funcionários e alunos, ficando os mesmos capacitados a utilizar a certificação digital para realizar operações seguras em meio eletrônico.

Os certificados digitais emitidos na estrutura criada e descrita abaixo estão vinculados aos processos internos das Instituições de Ensino vinculadas ao Claretiano - Rede de Educação, sendo válidos exclusivamente para uso

nos procedimentos, processos, documentos e serviços ACADÊMICOS indicados pela Autoridade Certificadora Claretiano - Rede de Educação - AC CLARETIANO.

2. Identificação

Esta DPC e PC é chamada "Declaração de Práticas e Política de Certificação para Assinatura Digital Tipo A1 – PRÓPRIO - da Autoridade Certificadora Claretiano - Rede de Educação".

Este documento descreve as práticas e procedimentos empregados pela AC CLARETIANO, assim como quais são os usos relacionados os seus Certificados de Assinatura Digital.

A AC CLARETIANO irá trabalhar com emissão de certificados digitais corresponde ao tipo A1 – CERTIFICADOS PRÓPRIOS NÃO EMITIDOS PELA ICP-BRASIL - em conformidade a MP 2.200-2, de 24 de agosto de 2001, artigo 10, § 2º.

ANSI.1 OID: 1.3.6.1.4.1.48009.1.1.1.1.1.1.1

Tabela 1.1 OID desmembrado

OID	**Descrição**
1.3.6.1.4.1	Prefixo IANA private enterprises: iso(1).org(3).dod(6).internet(1).private(4).enterprise(1)
48009	Identificador registrado do Claretiano - Rede de Educação
1	Identificador interno da hierarquia Claretiano - Rede de Educação (Reitoria)
1	Identificador interno da hierarquia Claretiano - Rede de Educação (CTIC)
1	Identificação do Claretiano - Rede de Educação na Númeração de Unidades
1	Identificador para aplicação em AC CLARETIANO
1	Tipo de vínculo 1= Principal, 2= Secundário, 3= Terciário
1	Tipo de identificação 1= Documento PC/DPC
1	Versão: Número Sequencial

3. Autoridade Certificadora

Esta PC refere-se exclusivamente à AC CLARETIANO no âmbito da Infraestrutura de Pares de Chaves do Claretiano - Rede de Educação.

A AC CLARETIANO tem em sua raiz uma chave RSA de 4096 bits.

4. Práticas e Procedimentos

As práticas e procedimentos de certificação da AC CLARETIANO estão descritos neste documento que cumprirá os requisitos da Declaração de Práticas de Certificação da AC CLARETIANO (DPC da AC CLARETIANO).

5. Posto de Registro

O Posto de Registro – PR será utilizado pela AC CLARETIANO para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes.

O PR da AC CLARETIANO poderá ser estabelecido em meio físico ou eletrônico, devendo a conferência física dos documentos ser realizada por pessoa autorizada.

6. Titulares de Certificado

Pessoas físicas, que façam parte da comunidade acadêmica e corpo técnico/administrativo, do Claretiano - Rede de Educação podem ser titulares de Certificado.

7. Aplicabilidade

O certificado digital emitido pela AC CLARETIANO poderá ser utilizado para todos os documentos aos quais sejam necessárias a aplicação de assinatura, atribuindo aos mesmos a autenticidade, integridade e validade jurídica conforme § 2º do art. 10º da MP 2.200-2/01.

A AC CLARETIANO leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados – LCR e extensão do período de validade do certificado.

Os certificados emitidos pela AC CLARETIANO no âmbito desta PC podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações; assinatura de documentos digitalizados pela Instituições de Ensino vinculadas ao Claretiano - Rede de Educação; virtualização dos documentos referentes ao exercício do magistério das Instituições de Ensino vinculadas ao Claretiano - Rede de Educação; emissão de documentos como histórico escolar e declarações para corpo discente das Instituições de Ensino vinculadas ao Claretiano - Rede de Educação; arquivamento eletrônico da documentação pessoal dos alunos das Instituições de Ensino vinculadas ao Claretiano - Rede de Educação; arquivamento de informações em meio digital, conforme a Portaria SENESu nº 255, de 12 de dezembro de 1990, Portaria 1.224, de 19 de dezembro de 2013 e Despacho SERES nº 97, de 16 de maio de 2014.

O “Termo de Titularidade”, disponibilizados pela PR que recebe e valida o pedido de emissão de certificado poderá limitar as aplicações para as quais são adequados os certificados de assinatura – tipo A1 emitidos pela AC CLARETIANO, determinando restrições ou proibições de uso destes certificados.

8. Geração do Par de Chaves

O Certificado Digital, com os pares de chaves criptográficas será gerado sempre pelo próprio titular.

A geração dos pares de chaves criptográficas ocorre em ambiente seguro e monitorado.

A AC CLARETIANO irá emitir ao titular uma chave privada válida somente para uma operação, evitando o extravio ou mau uso da mesma. Essa medida visa única e exclusivamente a segurança da chave privada e de seu titular.

O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados está de acordo com os Padrões e Algoritmos Criptográficos Internacionais.

A geração dos certificados digitais seguirá o algoritmo RSA, tendo os certificados emitidos dentro da infraestrutura da AC CLARETIANO para o usuário final uma chave RSA de 2048 bits.

O meio de geração da chave privada utilizado pelo titular junto a AC CLARETIANO assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;

b) A chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) A chave privada utilizada na geração de uma assinatura está eficazmente protegida pelo legítimo titular e a AC CLARETIANO contra a utilização por terceiros, tendo em vista que será utilizado um duplo fator de segurança: chave privada temporal e senha forte (contendo letras e números).

d) A senha é gerada pelo Sistema de Gestão Organizacional - SGO usando algoritmo SHA2 e enviada para o LDAP; A política de senha exige a presença de complexidade (letras maiúsculas, minúsculas e números ou caracteres especiais), tamanho mínimo de 6 caracteres, validade de 90 dias. O histórico de senha armazena as 24 últimas entradas.

O meio de aplicação do certificado digital não poderá modificar os dados a serem assinados, nem impedir que estes dados sejam utilizados sem a permissão do signatário antes do processo de assinatura com a exigência da senha forte que protegerá o uso da chave privada de assinatura.

A responsabilidade pela adoção de controles de segurança para a garantia do sigilo, integridade e disponibilidade da chave privada será da AC CLARETIANO juntamente com o titular do certificado, conforme especificado no Termo de Titularidade.

O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC CLARETIANO será de 2048 bits.

Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão x.509 com algoritmo SHA256 RSA.

Não é permitida a recuperação (escrow) de chaves privadas de assinatura pela AC CLARETIANO.

Em nenhuma hipótese será permitida a AC CLARETIANO a cópia de segurança (backup) de chave privada, mesmo que realizada com o consentimento do respectivo titular de certificado.

É vedada a AC CLARETIANO, a possibilidade de manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

No caso de perda da senha da chave privada, o respectivo titular irá solicitar um novo certificado digital, uma vez que a senha de geração do certificado digital é de único e exclusivo conhecimento do próprio titular.

A ativação da chave privada do titular do certificado se dará por senha forte com a liberação de seu uso em ambiente virtual, disponibilizado e monitorado pela AC CLARETIANO.

A desativação e eliminação da chave privada se fará automaticamente após o fechamento do sistema pelo usuário.

As chaves privadas de assinatura dos respectivos titulares de certificados emitidos pela AC CLARETIANO são utilizadas apenas durante período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação das assinaturas geradas durante o prazo de validade dos respectivos certificados.

O Claretiano – Rede de Educação possui 2 (dois) tipos de certificados, sendo:
A1 com validade de 1 (um) ano como período máximo de validade admitido para certificados de Assinatura Digital.
A2 com validade de 1 (um) dia como período máximo de validade admitido para certificados de Assinatura Digital.

Os dados de ativação da chave privada do titular do certificado, se utilizados, são protegidos contra uso não autorizado.

9. Quebra de Sigilo e Revogação do Certificado Digital

Caso o titular do certificado digital acredite que a sua chave privada, ou senha de ativação da mesma, não esteja mais seguro ou restrito ao seu uso, deverá comunicar imediatamente à Autoridade Certificadora CLARETINAO para que o respectivo certificado digital seja revogado e um processo de auditoria seja implementado para análise do ocorrido.

Tendo o certificado digital revogado, o profissional deverá requisitar novo certificado, efetuando novamente todos os passos para criação do mesmo.

10. Alterações na PC

Alterações nesta PC podem ser solicitadas e/ou definidas pelo Comitê Gestor do Claretiano - Rede de Educação que cuida da AC CLARETIANO.

11. Políticas de Publicação e Notificação

A AC CLARETIANO mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web https://sgo.redeclaretiano.edu.br/ac.