RNP
REDE NACIONAL DE ENSINO E PESQUISA

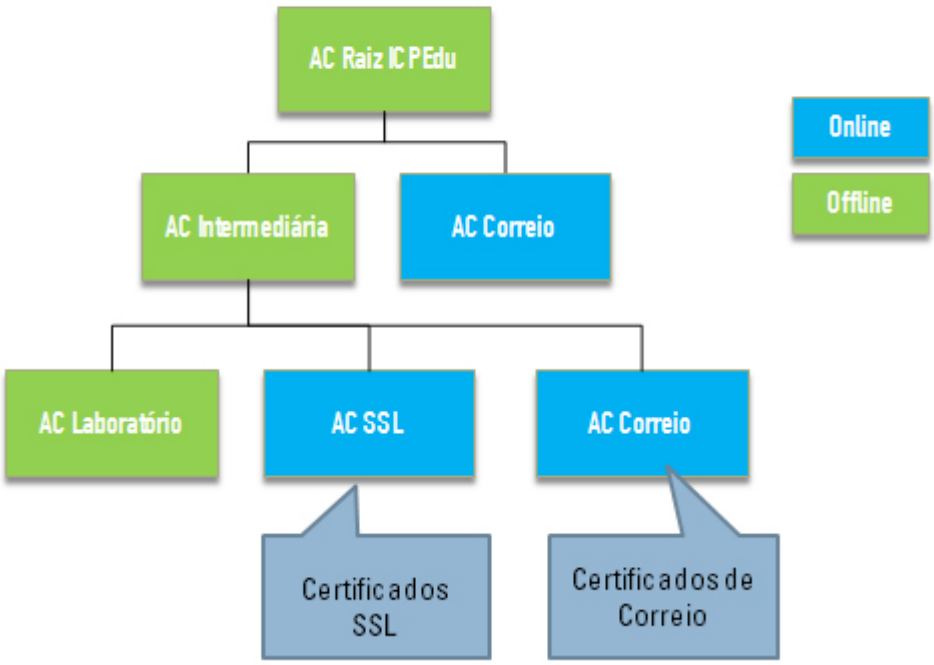
Especificações Técnicas da ICPEdu

A RNP opera a Autoridade Certificadora Raiz (AC Raiz) da ICPEdu e, com o certificado emitido por ela (1), assina o certificado emitido pelas Autoridades Certificadoras (AC's) intermediárias (2 e 3), dando autenticidade à AC da instituição.

Ao certificar uma instituição, a AC Raiz autoriza que esta crie uma estrutura própria de AC's intermediárias, utilizando a hierarquia da instituição (3) e podendo emitir certificados para os usuários finais (alunos, professores, funcionários) ou para os serviços (3, 5 e 6).

RNP
REDE NACIONAL DE ENSINO E PESQUISA

Exemplo de Cadeia de certificação da ICPEdu



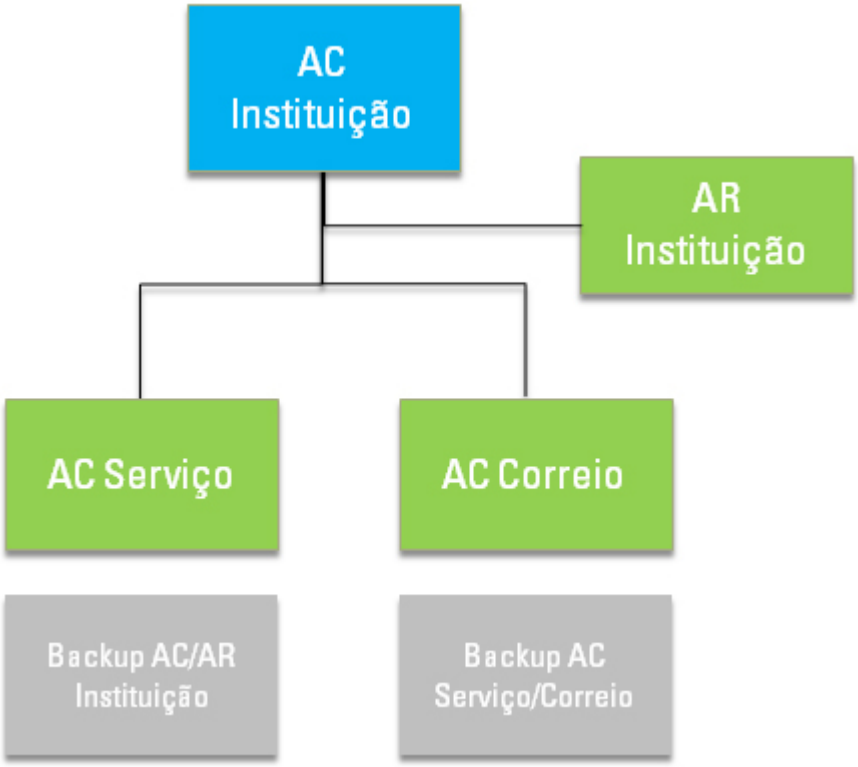
A ICPEdu requer a utilização de alguns equipamentos e programas específicos. Para ser um cliente deste serviço, a instituição deverá ter disponíveis 6 hardwares criptográficos (HSM), 4 servidores, 54 smartcards e o software para emitir e gerenciar os certificados.

O HSM é uma plataforma criptográfica para gerência e proteção de chaves criptográficas, em especial a chave privada. A segurança das chaves é garantida por proteções físicas e lógicas no equipamento. As chaves privadas protegidas são responsáveis pela assinatura de certificados digitais de autoridades certificadoras, autoridades de registro, servidores web e qualquer outra aplicação que necessite guardar as chaves de forma rígida.

O Sistema de Gerenciamento de Certificados Digitais ICPEdu (SGCI) permite gerir todo o ciclo de vida de um certificado digital, envolvendo emissão, publicação e revogação de certificados digitais, além da criação de Lista de Certificados Revogados (LCR).

As publicações das versões atuais e anteriores das LCRs, Declarações de Práticas de Certificação (DPCs), Políticas de Certificados (PCs), Certificados de Autoridades Certificadoras (ACs) e Autoridades de Registro (ARs) credenciadas, bem como os dados para contato, ficam armazenados em um repositório público.

RNP
REDE NACIONAL DE ENSINO E PESQUISA



Equipamentos necessários

AC Instituição (Offline)

- 1 HSM
- 9 Smartcards
- 1 servidor físico (Linux)

AR Instituição (Online)

- 1 HSM
- 9 smartcards
- 1 servidor físico ou virtual (Linux)

AC Serviço (Online)

- 1 HSM
- 9 smartcards
- 1 servidor físico ou virtual (Linux)

AC Correio (Online)

- 1 HSM

- 9 smartcards
- 1 servidor físico ou virtual (Linux)

Backup AC/AR Instituição (Offline)

- 1 HSM
- 9 smartcards