

ICPEDU

Infra-estrutura de Chaves Públicas para Pesquisa e Ensino

RNP, LNCC, UFSC, UFF, Unicamp, UFMG

Sumário da Apresentação

- Objetivos
- Timeline
- SGCI
- HSM
- Governança
- Serviço Experimental
- ICPEDU 3: Smartcard Virtual

Objetivos

- Implantação de uma Infra-estrutura de Chaves Públicas Acadêmica
 - Aplicações Acadêmicas
 - Autenticação e atributos
 - Certificados de curta duração / sistemas
 - Cultura em Certificação Digital
 - Treinamento
 - Pesquisa e Desenvolvimento em Certificação Digital e Aplicações

Timeline

Infra-estrutura



Sistema de Gestão de Certificados

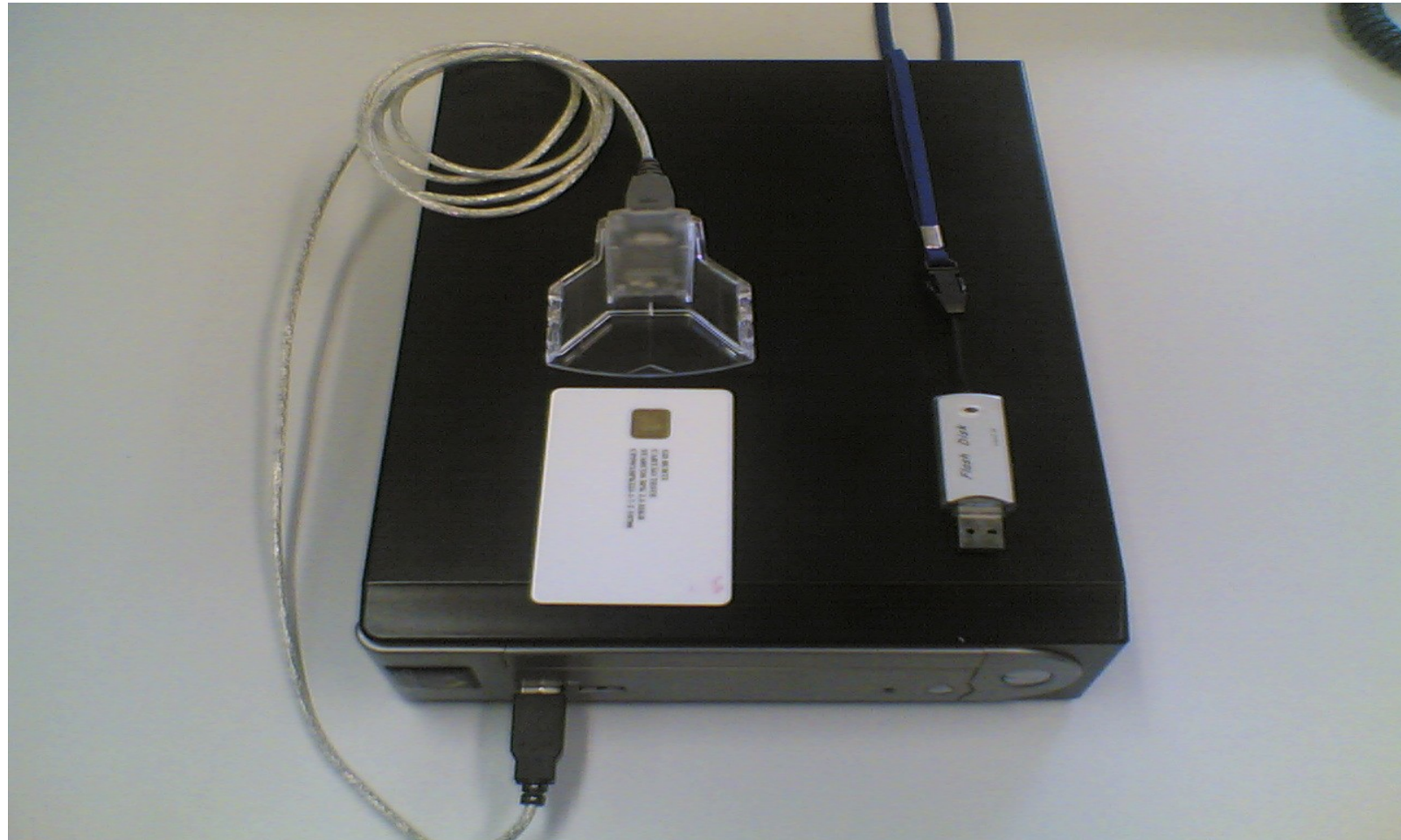
- Emissão/Revogação de Certificados
- Módulos Públicos
- Diretório Público
- Autoridades de Registro

Certificado Digital

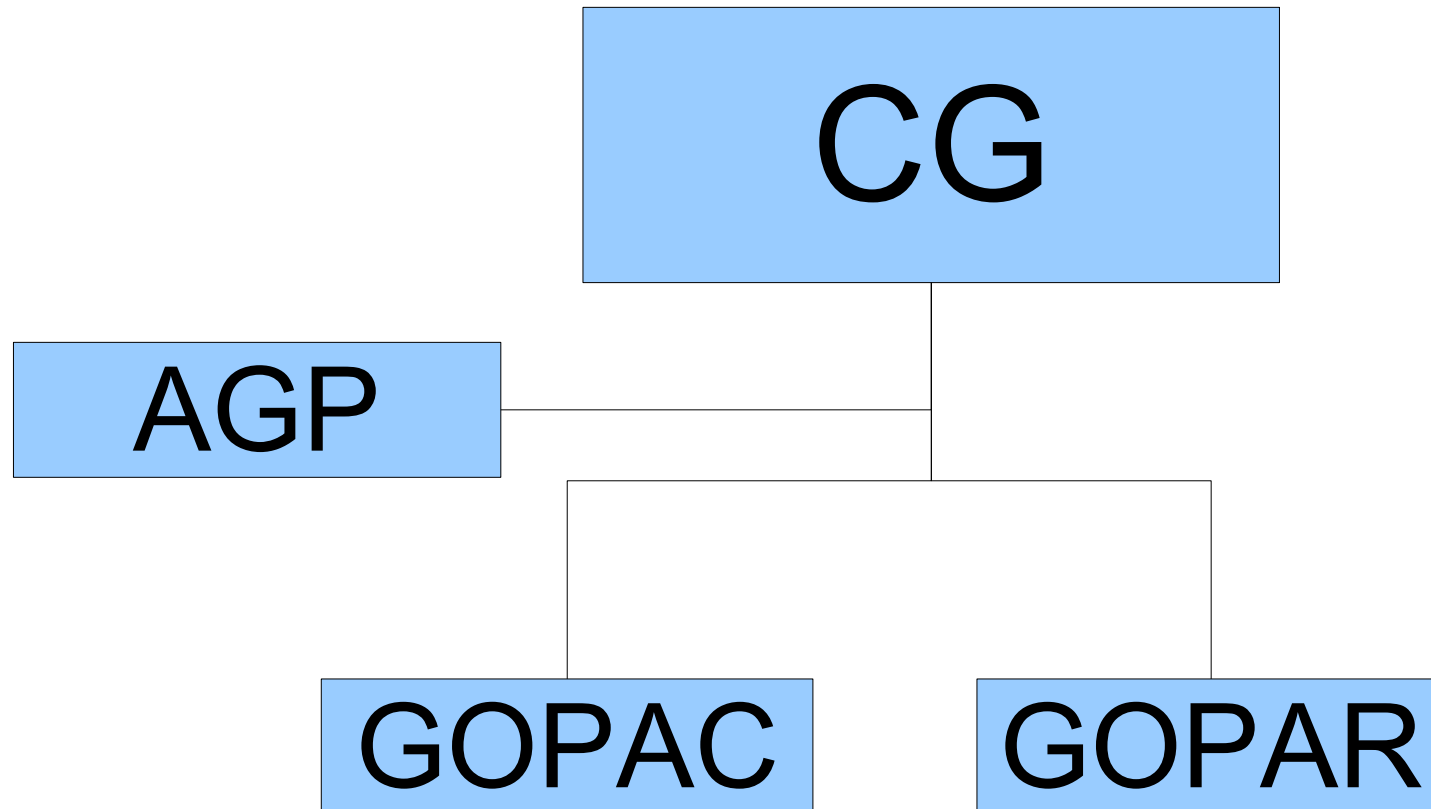
Versão
Número de Série
Assunto
Período de Validade
Chave Pública
Extensões

Assinatura da AC

HSM



Governança ICPEДУ



Comitê Gestor

CG

- Aprovar uma política para a AC Raiz
- Receber, analisar e aprovar a criação de ACs a partir de sua Política de Certificado
- Designar Comitê de Políticas e GOAC e GOAR
- Publicação do certificado da AC Raiz
- Fazer acordos entre diferentes federações de ICP para o reconhecimento mútuo dos certificados utilizados

Autoridade de Gerência de Políticas

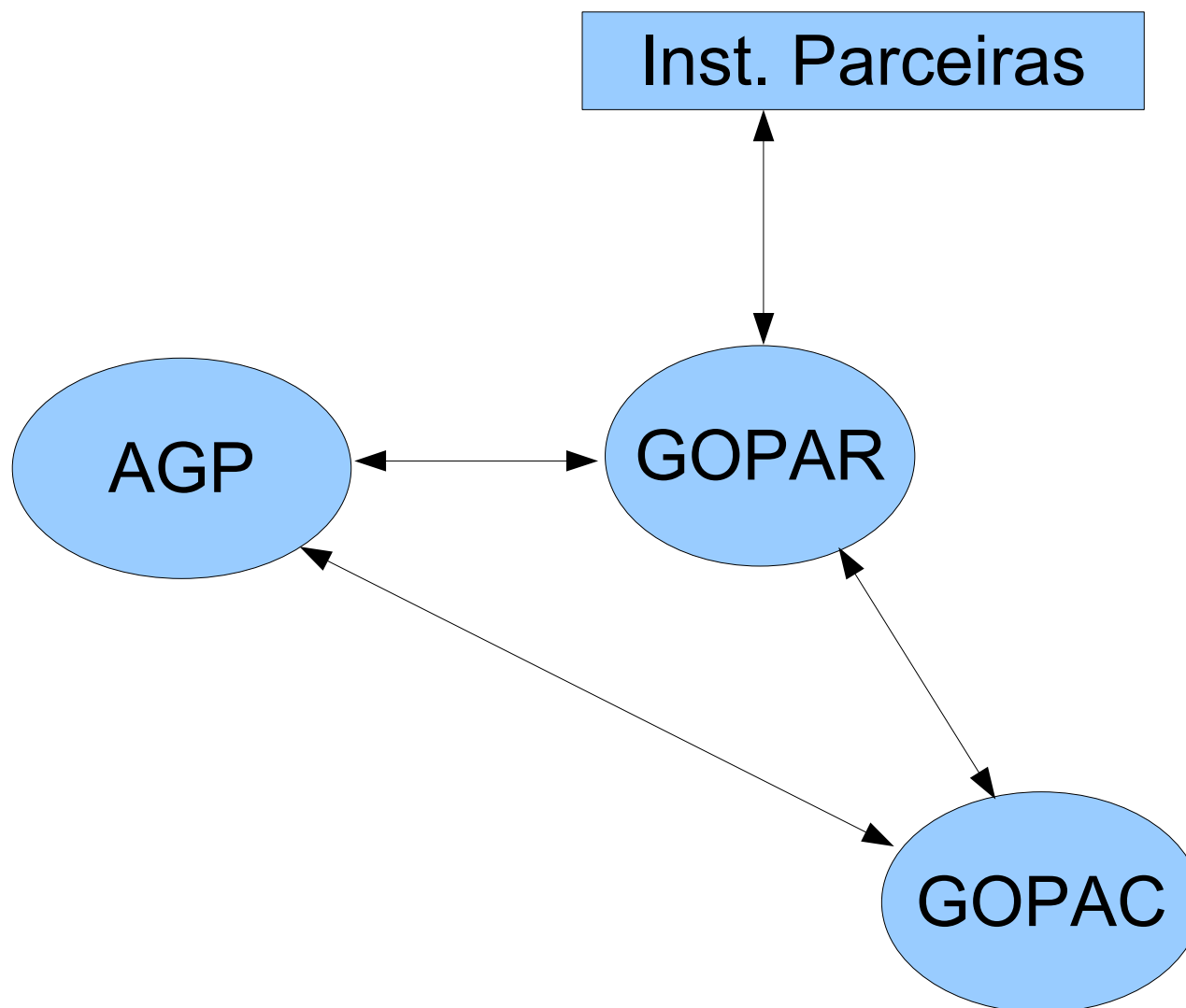
AGP

- Propor e analisar políticas de ACs Operadas
- Analisar Políticas de Certificados de Instituições Parceiras

Grupos de Operação

- Autoridade Certificadoras (**GOPAC**)
 - AC Raiz
 - AC RNP
 - AC Correio
 - AC Teste
- Autoridade de Registro (**GOPAR**)
 - AR Raiz

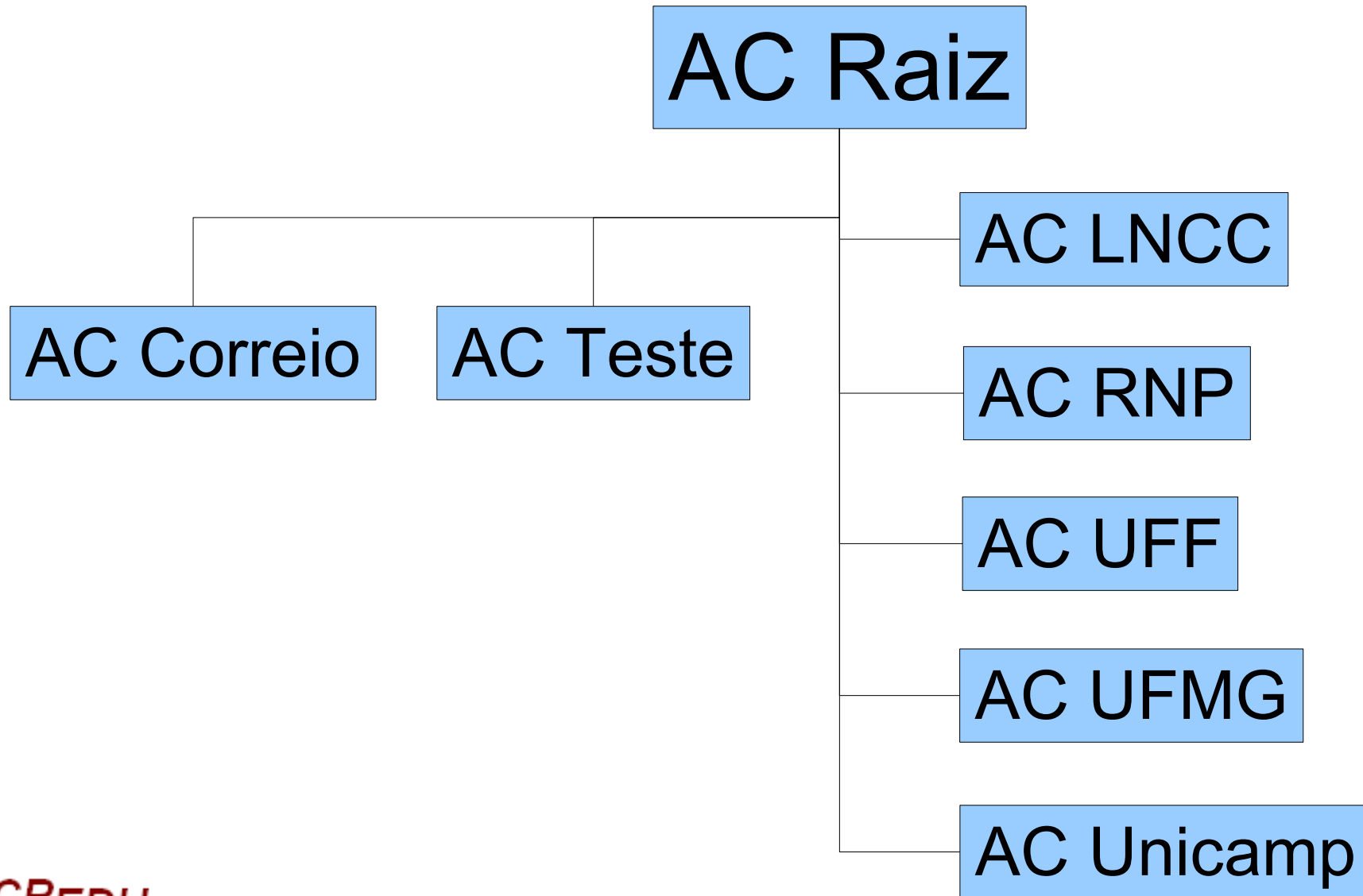
Fluxo de Informações na ICPEДУ



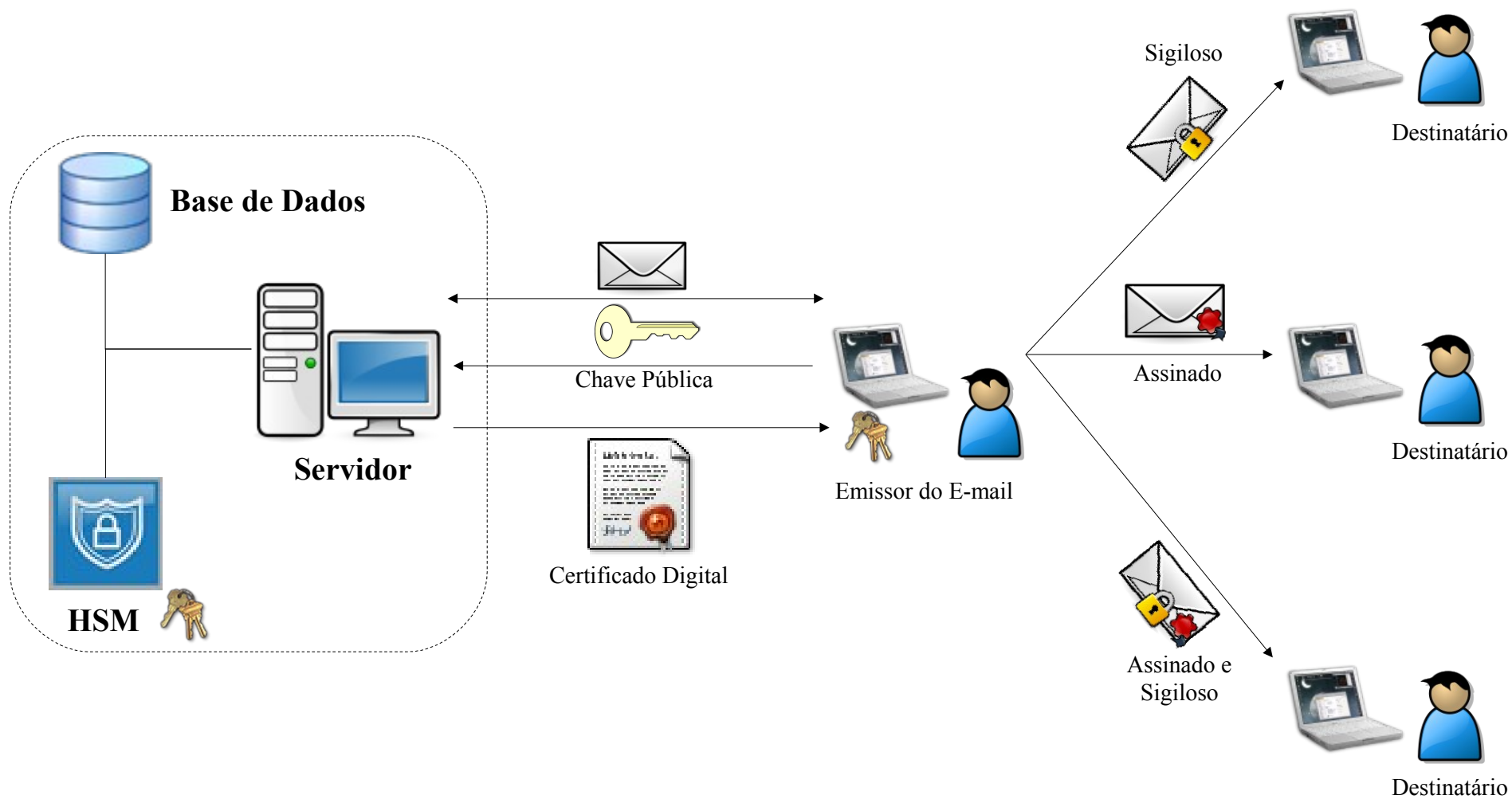
Serviço Experimental

- Comitê Gestor e AGP
- Grupo de Operação AC
- Grupo de Operação AR
- Avaliação
 - Modelo de Governança
 - SGCI, HSM
 - AC Correio, AC Teste

Topologia da ICPEДУ



AC Correio



AC UFSC

- Sala Cofre Acadêmica
- Sala de Treinamento
- Possível local para instalação, operação de ACs e backups da ICPEДУ
- ACs
 - AC UFSC, AC LabSEC
 - AC Correio, AC Teste
 - AC Otimizadora, AC Temporal

ICPEDU 3

Smartcard Virtual

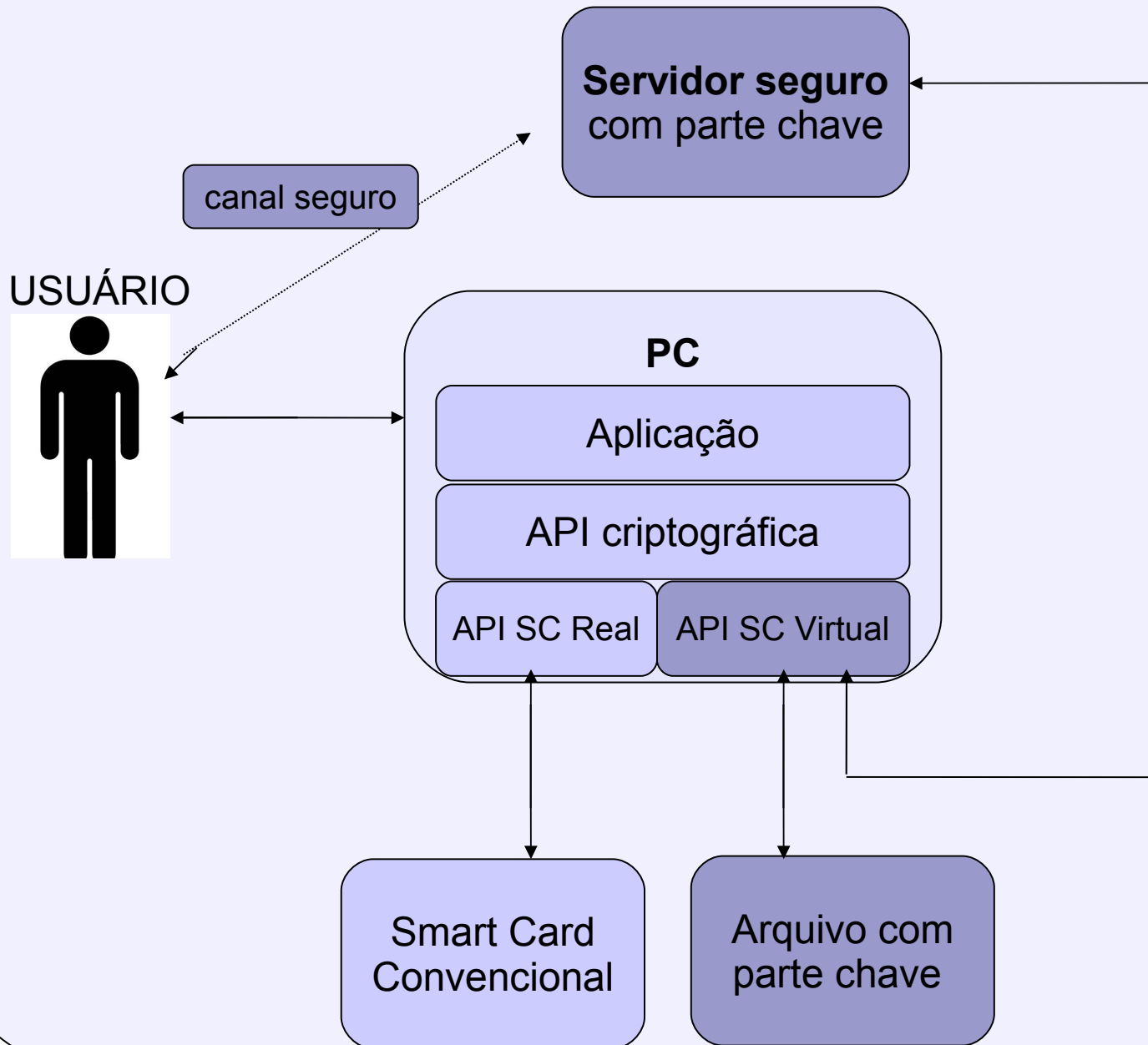
Onde o aluno guarda sua chave privada???

- Ideal: smart card/smart token
 - Caro (5 US\$/cartão)
- Guardar num arquivo
 - “Meu computador foi invadido”
- Guardar num servidor seguro
 - “O administrador abusou de sua autoridade”

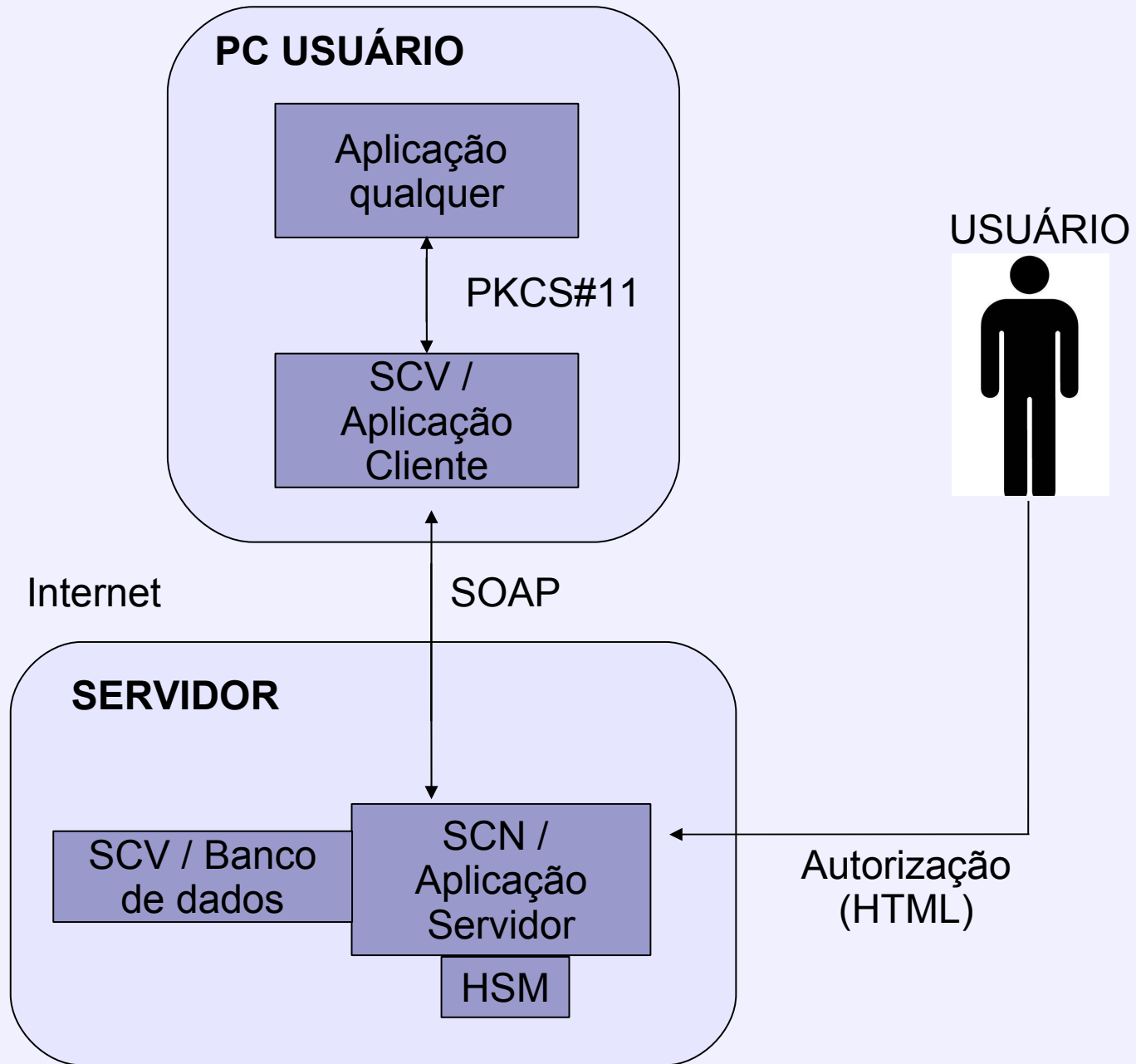
Smart Card Virtual

- Emulação em software de um Smart Card Real
- Guardar chave privada
 - arquivo cifrado, servidor com HSM, ambos
- Liberar a chave no servidor por um canal de comunicação separado
 - NIP
 - celular
- Protótipo: Thunderbird com XP

Smart Card Virtual vs. Smart Card Real



Smart Card Virtual



Vantagens

- Sistema guarda histórico das transações
- Solução com servidor fornece segurança forte
 - Posse de um objeto físico com a chave é trocado
- Custo baixo
- Permite a convivência de smart cards reais com smart cards virtuais

Equipe / Contribuições

- LNCC
- RNP, CAIS
- UFF
- UFMG
- UFSC
- Unicamp

Obrigado a Todos

Perguntas? Sugestões?

Sítio: www.icpedu.labsec.ufsc.br