Certificados Otimizados para a Validação Eficiente da Assinatura Digital

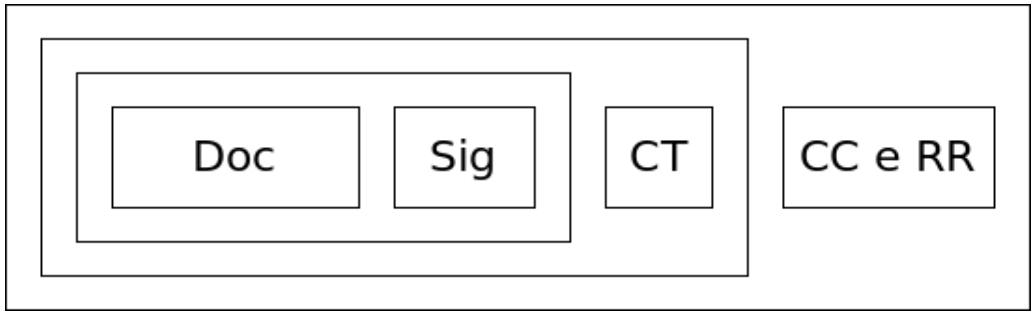
Adriana E. Notoya, Ricardo F. Custódio
Fernando C. Pereira, Joni S. Fraga

Sumário

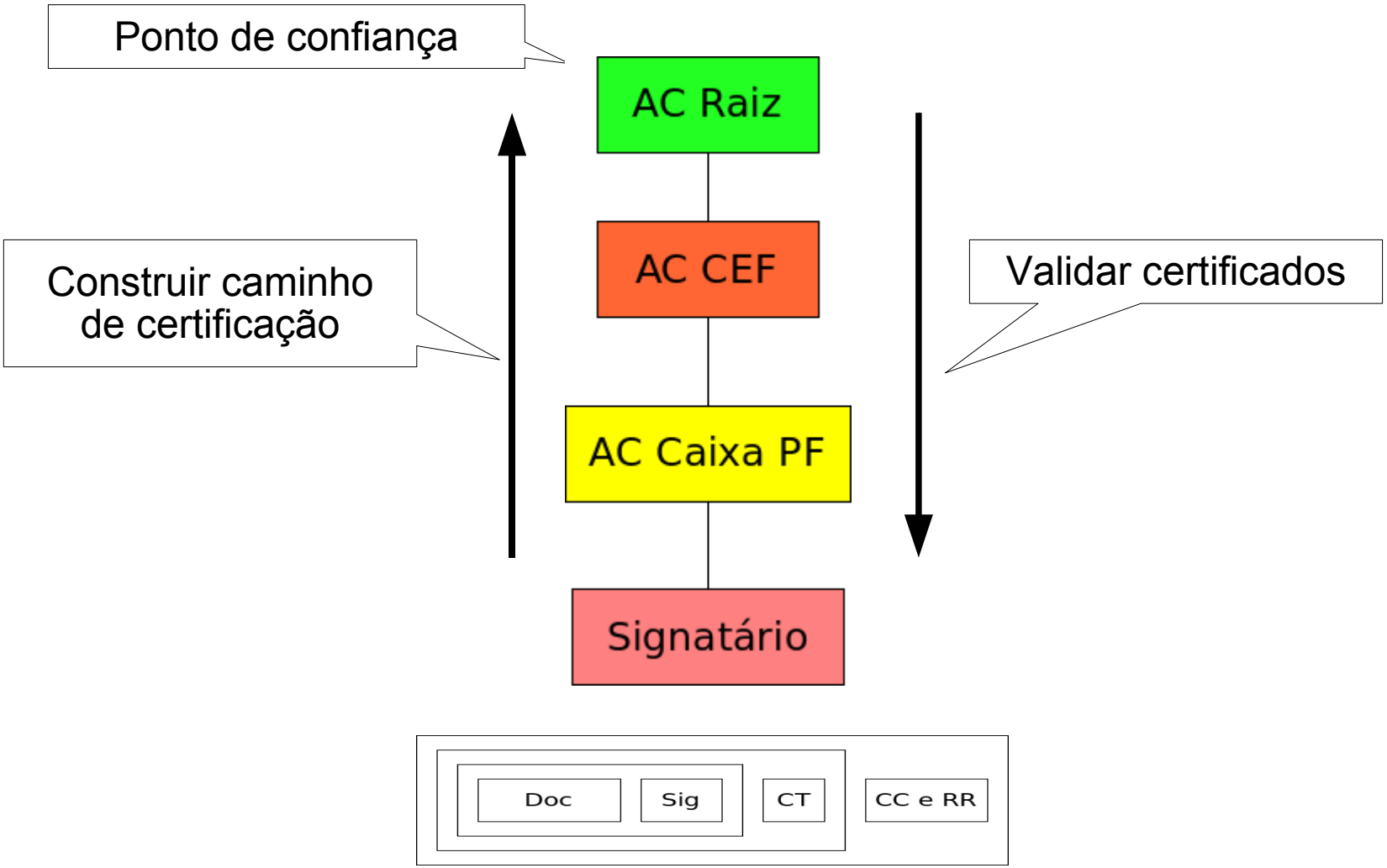
- Documentos eletrônicos - formato
- Validação de documentos eletrônicos
- Exemplo
- Certificado Otimizado
- Autoridade Certificadora Otimizadora
- Aplicações
- Conclusão

Documentos eletrônicos - formato

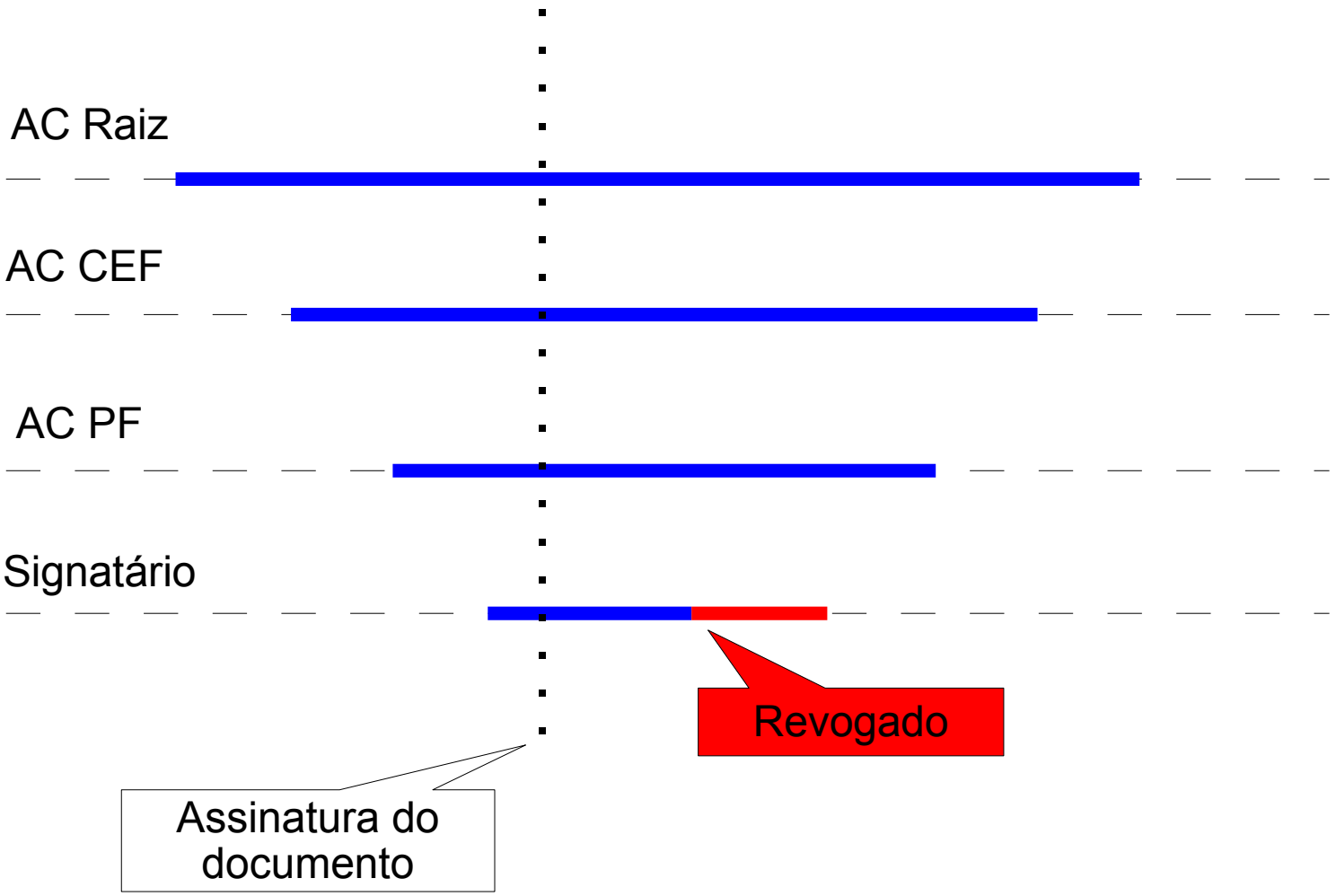
- Garantir autenticidade e integridade
- Assinatura digital
- Certificado digital



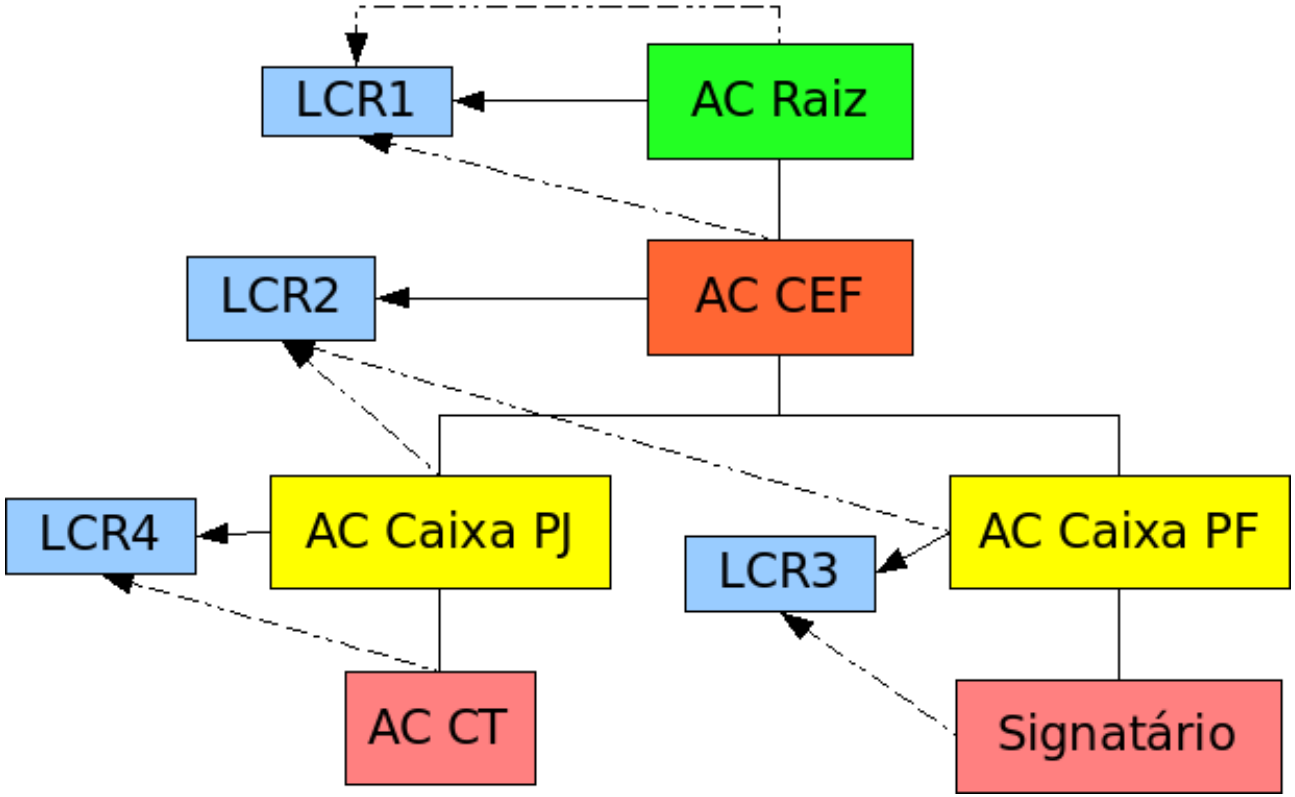
Validação de documentos eletrônicos



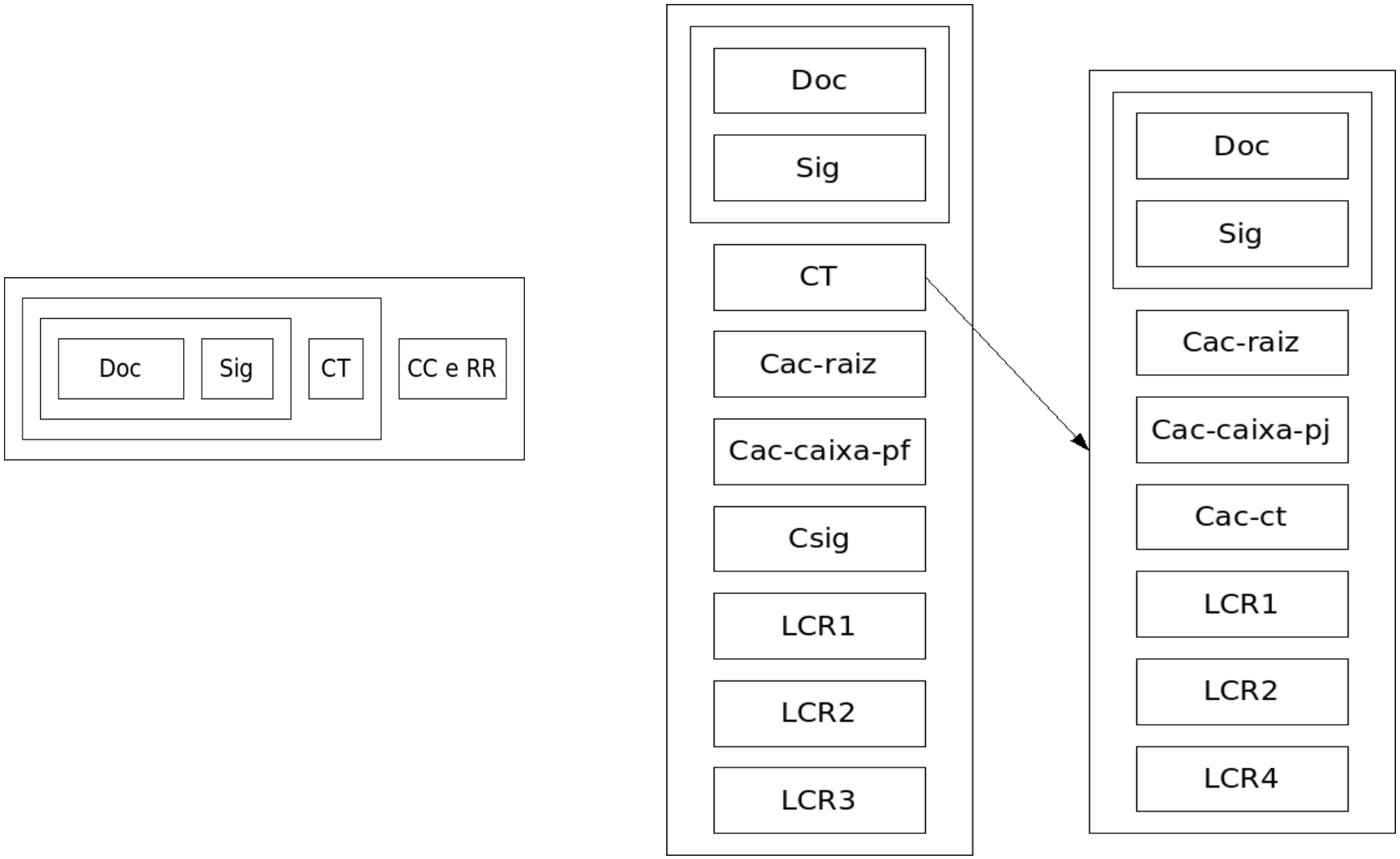
Validação de documentos eletrônicos



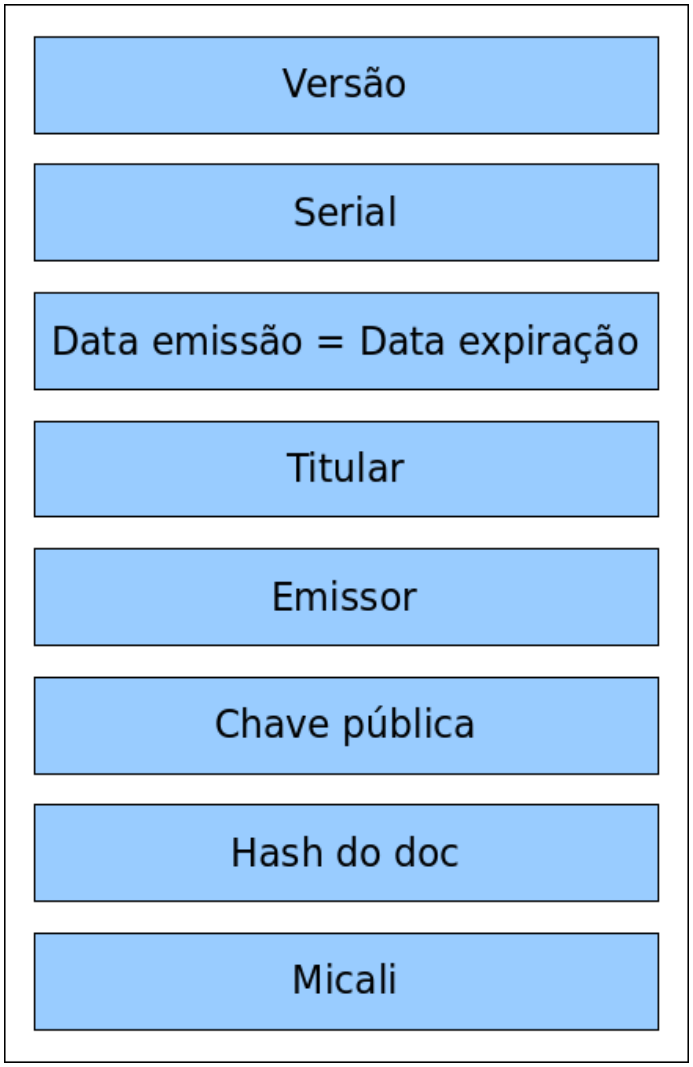
Exemplo - ICP-Brasil



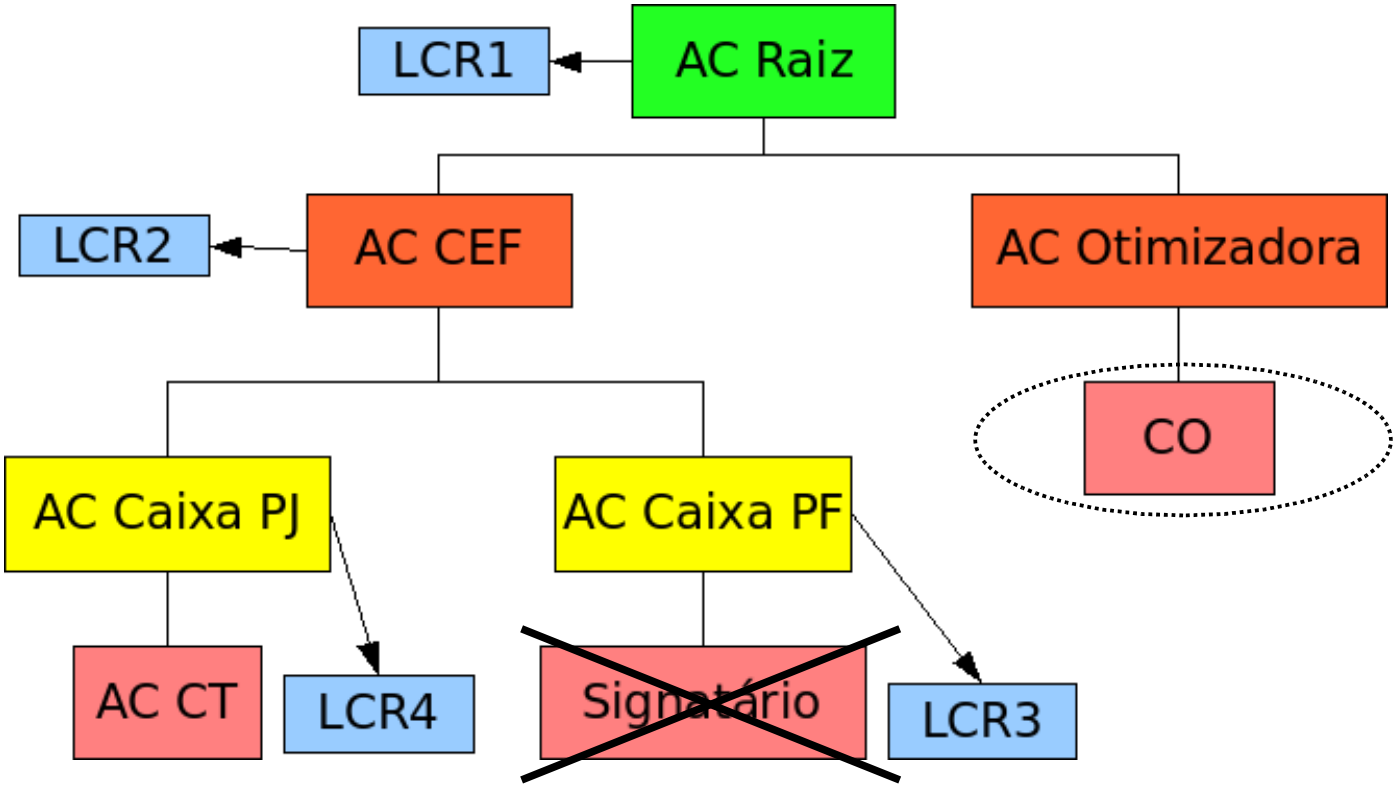
Exemplo - documento assinado



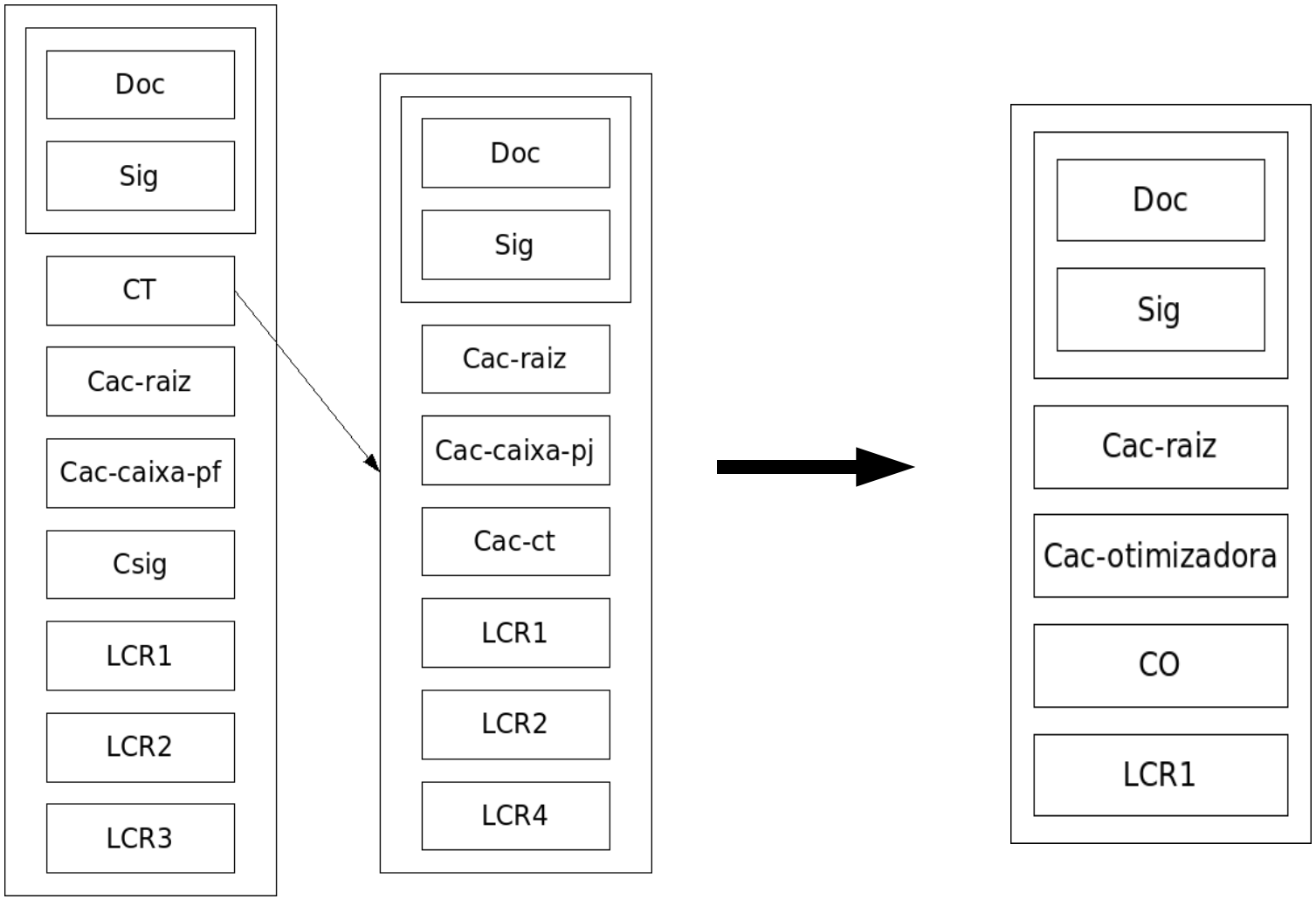
Certificado otimizado: X509



Certificado otimizado



Certificado otimizado - documento assinado



Certificado otimizado - vantagens

- Menor custo de processamento
  - local
  - escala
- Menor custo de armazenamento
- Elimina CT
- Pode ser usado
  - signatário
  - destinatário
- Não altera o certificado tradicional

Certificado otimizado - características

- Auto-validável
- Dispensa:
  - LCR para Co
  - LCR para Cac-otimizadora
  - Carimbo de tempo
- LRC para Cac-raiz é opcional

Autoridade Certificadora Otimizadora

- Diretamente subordinada à AC Raiz
- Serviço online
- Recebe do requerente
  - Hash do documento
  - Assinatura
  - Certificado do requerente
- Valida certificado e emite um certificado otimizado

Aplicações

- Documentos Eletrônicos usados em larga escala
- Dispositivos com restrições de armazenamento, processamento e energia
  - Dispositivos móveis

Conclusão

- CO para um documento
- Eficiência X Economia
- Seguem padrões (X509)
- Protótipo final de 2007
- ACO é um hardware especializado (HSM)