

EX  
E  
S  
I  
S

**...ela roda em Windows, Linux e outras plataformas.**

**...seu código é aberto\*, auditável e homologado por uma Universidade Federal brasileira.**

**...seu assinador roda em Windows, Linux e outros, reconhece vários cartões ao mesmo tempo\*\*.**

**...padroniza o acesso\*\* a todos os cartões criptográficos padrão JCOP20.**

**...provê independência de gerenciamento, integração com sistemas legados e não cobra anuidade por cada certificado emitido.**

# SIGNEXT



A sua próxima assinatura



## INFRAESTRUTURA DE CHAVES PÚBLICAS - ICP

- Utiliza linguagem C e C++, não decompilável, é estável e seguro;
- Compilável para qualquer ambiente operacional;
- ICP completa e gerenciável;
- Possui *applet* compatível com qualquer ambiente operacional e quaisquer cartões inteligentes padrão JCOP20;
- Utiliza protocolos de comunicação SSL, servidores SOAP e LOG's emaranhados, garantindo a segurança;
- Código aberto para o cliente inclusive a *applet* do cartão inteligente (sob condições);
- Implementada pelas RFC's pertinentes, criando padronização e interoperabilidade entre sistemas;
- Desenvolvida para atender às exigências do ITI e do ICP-Brasil.

# SIGNEXT



## AUTORIDADE CERTIFICADORA RAIZ

- Gera chaves assimétricas com aleatoriedade exclusiva garantindo a segurança do sistema;
- Possibilita o particionamento da chave raiz para aumentar ainda mais o seu sigilo;

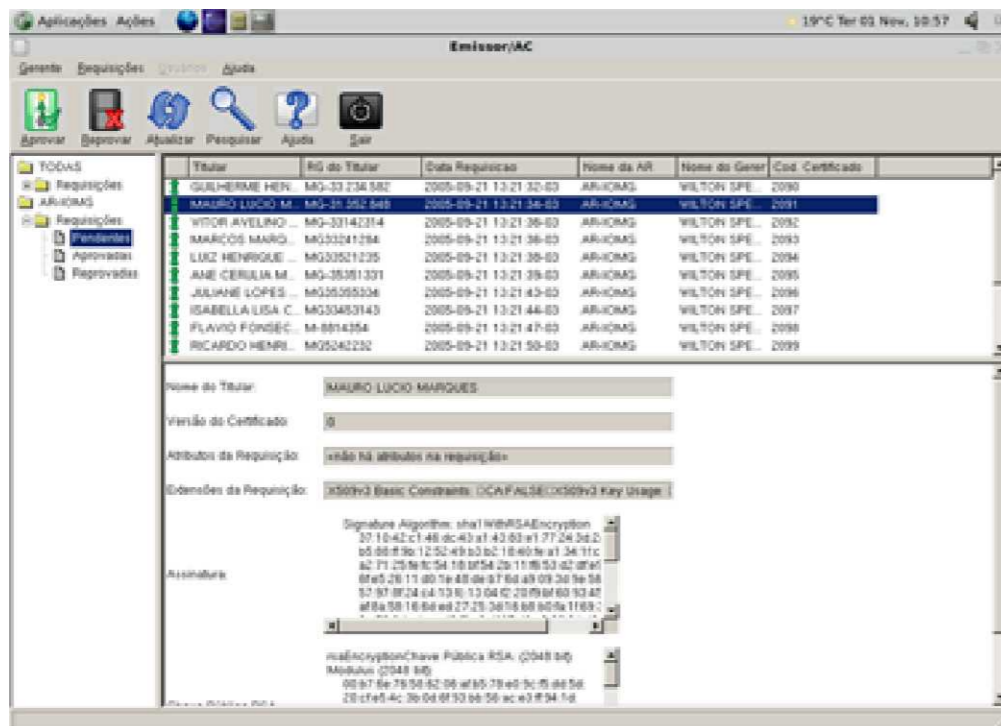


Aleatoriedade baseada no movimento de assinatura do responsável pela AC - Raiz.

# TRANSPARENTE

## AUTORIDADE CERTIFICADORA INTERMEDIÁRIA

- Gera chaves assimétricas com aleatoriedade exclusiva e assina-as com a chave raiz da ICP;
- Opção de armazenamento em HSM's;
- Interface gráfica para administração que gerencia as requisições de criação de certificados enviados pelas AR's (Autoridades Registradoras);
- LOG transacional seguro com exclusivo suporte de emaranhamento com geração de hash para a segurança e rastreabilidade das operações realizadas;



# INOVADOR

- Interfaces automáticas para geração de listas de certificados revogados (LCR) e servidor OCSP para a integração com sistemas que utilizam a certificação digital;
- Sincronização *one-pass* exclusiva com a Autoridade Registradora Central, segura e a prova de ataques externos;
- Administra várias Ac's (Autoridades Certificadoras) Intermediárias encadeadas mantendo a confiabilidade do sistema;
- Flexibilidade para definição dos tipos de certificados que serão emitidos;
- Emite certificados baseados em outra AC, como ICP-Brasil.

## **AUTORIDADE DE REGISTRO - AR**

Dois módulos são disponibilizados:

### **Gerente AR**

- Gerencia os seus atendentes, e assina as requisições de certificados para enviá-los diretamente à AC;
- Gerencia as tarefas da AR e determina quais os atendentes serão seus subordinados;
- O banco da AR possui todos os dados da requisição, inclusive a digitalização da requisição armazenada em papel.



### **Atendentes AR**

- Além das solicitações para requisições de certificados, o sistema realiza o cadastro do requerente e é capaz de digitalizar os documentos do cadastro, inicializa o cartão criptográfico e deposita os certificados no cartão;
- Revoga um certificado através de uma solicitação do requerente;
- As transações são gravadas em banco de dados com log transacional seguro e exclusivo suporte de emaranhamento, gerando a necessária segurança e rastreabilidade nas operações realizadas;
- Gerencia as operações de solicitação, verificação e entrega do certificado ou cartão criptográfico;
- As requisições e transmissões realizadas são assinadas pelo gerente e pelo atendente e transmitidas para a AC;
- Possui pontos de registros que são atendentes AR simplificados e podem ser distribuídos. Os pontos de registro são vinculados a um atendente AR master que libera as suas requisições.

# **SEGURO**

## PROTOCOLO DIGITAL E AUTORIDADE TIMESTAMP

- Garante a temporalidade dos documentos, e de todas as transações internas da ICP;
- O assinador o utiliza para assinar com hora confiável ou para protocolar, garantindo a existência da assinatura a partir daquele momento;
- O sistema de protocolo utiliza um HSM para armazenar a chaves desta autoridade.

## AUTORIDADE DE CONTRA-ASSINATURA

- Permite a criação e o gerenciamento de uma autoridade de contra-assinatura, possibilitando o cruzamento confiável de certificados de AC's diferentes;
- Um exemplo seria a criação de uma ICP interna e, para a garantia externa, os documentos assinados podem ser reassinados utilizando-se um certificado da ICP-Brasil;
- Esta autoridade garante que as assinaturas depositadas pela ICP particular são válidas e íntegras (como o reconhecimento de firma realizado pelo tabelião).

## PROTOCOLO STATUS DO CERTIFICADO

- Permite a consolidação de um arquivo assinado digitalmente através deste protocolo, que inclui uma assinatura de validação do status do certificado (se está revogado ou não) no momento em que é assinado e no momento em que é protocolado.

## APPLET PARA CARTÃO INTELIGENTE

- Interface para aplicativos, utiliza padrão PKCS#11 e permite a geração de chaves RSA até 2.048 bits, assinatura, verificação, criptografia, decifração, gravação e leitura de objetos;
- Integrável ao OpenSSL;
- Permite integração em várias plataformas (Windows, Linux, etc);
- Compatível com cartões inteligentes padrão JCOP20;
- Código Java aberto (sob condições).

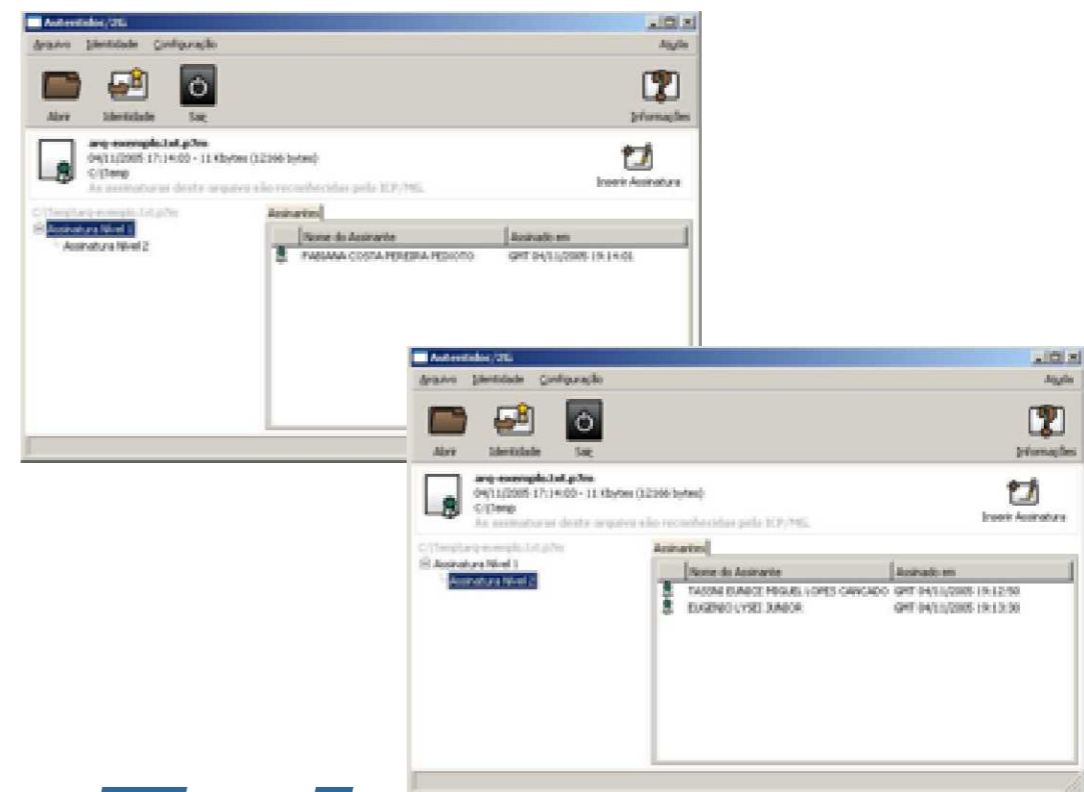
**BRASILEIRO**

## ASSINADOR - AUTHENTIDOC

- Baixa um certificado para um cartão inteligente ou arquivo;
- Assina com certificados em arquivo ou cartões com padrão OpenSC, OpenSSL ou JCOP20;
- Assina um arquivo em níveis hierárquicos e em conjunto;
- Verifica a validade do certificado (via LCR ou OCSP) e das assinaturas em arquivos;
- Verifica se o cartão é verdadeiro;
- *Pode utilizar um registro biométrico para verificar a autenticidade do certificado e do cartão;*
- Elimina arquivos de forma irrecuperável (picotador de papel);
- Pode assinar um arquivo com a hora oficial da AC;
- Pode ser executado em linha de comando;
- Procura por novas versões automaticamente;
- Assina usando vários cartões ao mesmo tempo.

Funcionalidades extras:

- Protocolo de documentos;
- Registro do status do arquivo assinado e do certificado que o assinou;
- Contra-assinatura: chancela a assinatura de um arquivo com o certificado de outra ICP.



# FLEXÍVEL

# QualiConsult

**Belo Horizonte - MG**

**(55 - 31) 3213-1715**

**Vinícius Gante**

**e-mail: [vgante@gmail.com](mailto:vgante@gmail.com)**