ESPECIFICAÇÕES TÉCNICAS TOKEN USB

- Armazenamento de Certificados Digitais AC JUS Tipo A3
- Permitir geração de chaves, protegidas por PINs (Personal Identification Number)
- Permitir inicialização e reinicialização do token mediante a utilização de PUK (Pin Unlock Key)

APIs de Criptografia

- PKCS#11 v 2.01
- Microsoft CryptoAPI (CAPI) 2.0
- Microsoft PC/SC

Funções de Criptografia

- Criação assimétrica de pares de chaves (RSA)
- Criação simétrica de chaves (DES, 3DES (k1,k2,k3), RC2, AES)
- Armazenamento e gerenciamento de chaves protegidos por hardware
- Operações de chaves RSA de 1024 e 2048 bits

Algoritmos de Criptografia
Criptografia Assimétrica de Chaves

- RSA de 1024 bits, RSA de 2048 bits Algoritmos Simétricos de Chaves
- DES, 3DES (k1,k2,k3), RC2, AES Assinatura Digital
- RSA de 1024 bits, RSA de 2048 bits Algoritmos de Hash
- SHA-1, MD5

Middleware para Windows e Linux

- Driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores)
- Driver disponível para o sistema operacional Microsoft Windows (XP e versões superiores)

Características Físicas Hardware

- • Processador de 8 bits
- • Memória de, no mínimo, 32 K

Conectividade

- Compatível com USB 1.1/2.0

Normas Reguladoras

- Compatível com padrão ITU X.509
- Compatível com a Resolução nº 65, de 09 de junho de 2009, que descreve os padrões de algoritmos criptográficos da ICP-Brasil;
- Compatível com especificações ISO 7816
- Compatível com RFC 2315