

### Token criptográfico – DXToken

Token criptográfico com desenvolvimento 100% nacional, compatível com todos os requisitos da ICP-Brasil / Órgão Brasileiro que regulamenta a certificação digital.

Utilizado para gerar e armazenar credenciais, chaves públicas e privadas, senhas e certificados digitais em seu ambiente seguro.

#### Indicações de uso:

- Certificados digitais
- Assinatura digital
- Emissão de Notas Fiscais
- Autenticação de portais Web

#### Informações técnicas:

**ISO 7816:** Partes 1, 2, 3 e 4;

**Bloqueio do dispositivo:** Após 5 tentativas de autenticação com códigos inválidos;

**Reinicialização:** Permitida mediante a utilização de PUK (Pin Unlock Key);

**Senhas (PIN/PUK):** Uso de caracteres alfanuméricos, letras maiúsculas e minúsculas de acordo com a preferência do usuário;

**Exportação de chave privada:** Bloqueado;

**Utilização de chave privada:** Deverá haver autenticação para liberar a utilização pretendida;

**Driver:** Dxsafe Middleware

([https://publicado.dexon.ind.br/DXSafe/Instaladores/DXSafe\\_1.x/Instalador%20DXSafe%20Middleware%20-%201.0.23.exe](https://publicado.dexon.ind.br/DXSafe/Instaladores/DXSafe_1.x/Instalador%20DXSafe%20Middleware%20-%201.0.23.exe));

**Interface:** Bibliotecas de software implementando as interfaces de programação Cryptographic Service Provider (CSP) da Microsoft CryptoAPI (CAPI), Microsoft Cryptography API: Next Generation (CNG), OASIS PKCS #11 Cryptographic. Token Interface (Cryptoki).

**Dimensões do produto:** Altura 7,8mm, Largura 15,6mm e Comprimento 36,5mm

**Comunicação:** USB 2.0 Full Speed

**Armazenamento:** 128Kb **Dados:** 32Kb

#### Módulos Habilitadas:

- Certificados:
  - Armazenamento de Certificados em Formato x509
- Chaves Simétricas
  - DES/3DES ( 64 Bits, 128 Bits e 192 Bits )

- AES ( 128 Bits, 192 Bits e 256 Bits )
- ECB, CBC e MAC
  
- Chaves Assimétricas
  - RSA – 1024 Bits e 2048 Bits.
  - PKCS#1
  
- HASH:
  - CRC32
  - SHA1
  
- Números Randômicos - TRNG
  - AES-256

**Middleware:** DXSafe, CSP, KSP, PKCS#11

**Compatibilidade:** PC/SC 2.0 e CCID

Protocolo T=0

ISO 7816 Classe A, B e C

**Interface:** Dois LEDs para indicação de funcionamento

**Sistemas Operacionais:** Windows 7 e versões superiores

MacOS 10.10 e versões superiores

Linux

**Durabilidade:** Mínimo de 100 anos de retenção de dados