RESPONSABILIDADE DO TITULAR A3

Cartão

No cartão inteligente (smart card), quem controla o certificado digital são as senhas PIN e PUK. O responsável pelo certificado digital deve configurar e manter o sigilo desses controles ou senhas.

PIN - Funciona como bloqueio para restringir o uso do certificado digital armazenado no cartão inteligente.

- Todos os certificados digitais emitidos em cartões saem de fábrica com o mesmo PIN: 1234;
- O titular do certificado deve alterar esse PIN para uma senha de seu conhecimento exclusivo;
- A AC e o PSS Certisign recomendam a alteração imediata do PIN original para garantir a segurança do seu certificado digital;
- Sugerimos que o novo PIN seja guardado em local seguro;
- Para modificar o PIN, selecione no aplicativo Safesign as opções 'Token > Alterar PIN';
- Se você digitar a senha PIN incorretamente por 3 vezes consecutivas, o cartão será imediatamente bloqueado;
- É possível o desbloqueio com o uso da senha PUK;
- Se você também digitar a senha PUK incorretamente por 3 vezes consecutivas o cartão será imediatamente bloqueado e inutilizado. É então necessário a emissão de um novo certificado e compra de um novo cartão.

PUK - É utilizado para resgatar seu PIN em caso de bloqueio do cartão.

- Todos os certificados digitais emitidos em cartões saem de fábrica com o mesmo PUK: 1234;
- Assim, o PUK também deve ser alterado para uma senha que somente você conheça;
- A AC e o PSS Certisign recomendam que você altere imediatamente o PUK original para segurança de seu certificado digital;
- Sugerimos que o novo PUK seja guardado em local seguro, pois sua perda inviabilizará o desbloqueio do cartão.

ATENÇÃO: se você digitar a senha PIN incorretamente por 3 vezes consecutivas, o cartão será imediatamente bloqueado. É possível o desbloqueio com o uso da senha PUK. Se você também digitar a senha PUK incorretamente por 3 vezes consecutivas, o cartão será imediatamente bloqueado e inutilizado, e um novo cartão com novo certificado precisará ser adquirido e emitido.

Token

No token, quem controla o certificado digital é a senha PIN. O responsável pelo certificado digital deve configurar e manter em sigilo o PIN. Essa senha funciona como um mecanismo de bloqueio para restringir o uso do certificado digital armazenado no token.

Todos os certificados digitais emitidos em token têm uma senha padrão original, a saber:

- Se o modelo do seu token é o e-Token PRO da Aladdin, a senha original, pré-existente é 1234567890
- Se o modelo do seu token é o iKey 2032 da Safenet/Rainbow, a senha original, pré-existente é PASSWORD

O titular do certificado deve alterar esse PIN para uma senha de seu conhecimento exclusivo. A AC e o PSS Certisign recomendam a alteração imediata da senha original, para garantir a segurança do seu certificado em token.

ATENÇÃO: se você digitar a sua senha incorretamente por 5 vezes (para o modelo e-Token PRO Aladdin) ou 10 vezes (para o modelo iKey 2032 da Safenet/Rainbow) consecutivas, o token será imediatamente bloqueado e um novo certificado precisará ser adquirido e emitido. Não será necessário adquirir um novo token: ele poderá ser reutilizado após sua formatação. Todos os atos realizados perante à Receita Federal do Brasil utilizando o Certificado Digital é de responsabilidade única do titular.