

Responsabilidades do Titular CT-e A3

No CT-e A3, 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 um 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 ainda 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.
- 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 ainda 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.