[PJeOffice Pro]Instrução de Segurança

28/09/2024 10:22:47

Imprimir artigo da FAQ

Categoria:	SISTEMAS::PJE OFFICE PRO	**Votos:**	0
Estado:	public (all)	**Resultado:**	0.00 %
		Última atualização:	Ter 19 Mar 10:25:41 2024

Palavras-chave

segurança PJeOfficePro

Sintoma (público)

O documento visa em instruir o usuário sobre a segurança no sistema PJEOffice PRO.

Problema (público)

Solução (público)

PROCEDIMENTO PARA EXECUÇÃO

Na versão 'Pro' o usuário tem a oportunidade de decidir entre três estratégias na informação da senha para assinaturas conforme figuras que seguem:
Acessível da tela de autenticação.

Acessível na bandeja do Windows.

A estratégia de solicitação de senha pode ser alterada facilmente e a qualquer momento de forma que o recurso será aplicado imediatamente sem que para isso seja exigido o reinício do assinador.

- Sempre solicitar senha

É a alternativa mais segura, porém a menos produtiva. Neste caso qualquer operação que envolva o uso da chave privada do certificado só prosseguirá com a digitação explícita da senha no teclado. Menos produtiva porque em dias em que houver um volume considerável de documentos a serem assinados, a senha será solicitada para cada documento (nos casos de assinatura em lote, a senha será solicitada a cada lote, ou seja, em dois lotes, cada um com 20 documentos, a senha será solicitada 2 (duas) vezes em vez de 2*20=40 vezes.

- Solicitar senha uma vez

É a alternativa mais produtiva dentre as demais. Esta opção evita o gasto de tempo com a digitação de senhas no teclado. Porém, não deve ser utilizada em máquinas compartilhadas, sendo de responsabilidade do usuário certificar-se que sua máquina não será utilizada por outros indivíduos.

- Confirmar o uso do dispositivo

É a alternativa intermediária entre produtividade e segurança. O comportamento do assinador será o mesmo que a opção “Sempre solicitar senha”, porém ao invés da senha ser digitada explicitamente no teclado, o usuário apenas confirmará com um único clique o aviso dado pelo assinador informando que o dispositivo está sendo utilizado conforme tela que segue:

Como na opção anterior, o proprietário do certificado também deve ficar atento quanto ao uso indevido do seu dispositivo em ausências temporárias do seu computador.
Ciclos de autenticação Como medidas adicionais de mitigação em segurança o PJeOffice Pro adota ciclos de autenticação. Um ciclo de autenticação é uma sequência de eventos que provocam o fechamento ou abertura de uma sessão autenticada no dispositivo/token segundo os comportamentos seguintes:

1. O comportamento padrão do assinador é ativado quando escolhida a opção de leitura de certificados com a opção "PJeOffice", conforme tela abaixo: Neste caso tanto a leitura de certificados quanto o controle de acesso ao token é realizado pelo próprio assinador PJeOffice. Neste cenário, todo evento de autenticação / login na plataforma PJe exigirá a informação da senha mesmo que a opção " Solicitar apenas uma vez" esteja habilitada e já tenha sido informada anteriormente. A praticidade de informação única da senha só se aplicará após a entrada já previamente autenticada com a senha exigida, ou seja, uma tentativa de autenticação na plataforma PJe marca o fim de um ciclo de autenticação existente e início de um novo ciclo no qual as funcionalidades de segurança estarão operacionais. Esta é a configuração padrão recomendada e pré-definida assim que o assinador é instalado.
2. O comportamento alternativo do assinador é ativado quando escolhida a opção de leitura de certificados com a opção "Windows", conforme tela que segue:

Neste comportamento alternativo o controle de acesso ao token/smart card será realizado pelo próprio Windows. O importante a considerar neste cenário é que, diferentemente da opção anterior, um evento de autenticação / login na plataforma PJe pode não exigir a informação da senha do token/smart card se ela já tiver sido informada anteriormente. Isto ocorre porque a gerência de

sessão do dispositivo passa a ser do sistema operacional cujo critério de abertura/fechamento é uma política estabelecida pelo mesmo.

Esta configuração também tem o propósito de promover a integração com o repositório de certificados digitais do sistema operacional Windows e, complementarmente, de maximizar a compatibilidade com tokens/smart cards/leitoras antigos de diferentes fabricantes. Isto quer dizer que se por alguma razão o seu certificado não seja reconhecido usando a opção anterior "PJeOffice" após todas as tentativas de instalação de drivers, a opção "Windows" pode tornar o seu dispositivo compatível com o assinador.

Independente da configuração utilizada, um logoff ou bloqueio explícito da máquina pelo usuário ou por ociosidade da estação (política de rede) colocará o assinador em modo de hibernação, finalizando a sessão do(a) token/leitora (no comportamento padrão) e marcando o fim do ciclo de autenticação atual (se houver). O assinador vai retomar o seu trabalho quando do desbloqueio / login / fim da ociosidade da estação. Este mecanismo dificulta a exploração de eventual falha de segurança minimizando o tempo de exposição da sessão aberta do(a) token/leitora a artefatos maliciosos, além da possibilidade de integração com políticas de segurança da rede aplicadas ao logoff automático das estações, acabando de vez com a inconveniente mensagem " Já existe uma instância do PJeOffice em execução" que ocorria em versões anteriores.