Assinatura de código

Verifique a identidade e a integridade do aplicativo

O que a assinatura vincula

A assinatura vincula o conteúdo do executável à identidade do signatário. Na verificação, o sistema confere a integridade do conteúdo assinado e aplica sua política de confiança ao certificado. Qualquer alteração posterior no conteúdo coberto pela assinatura pode invalidá-la.

Windows e macOS

No Windows, a assinatura Authenticode pode ser conferida com SignTool. Um carimbo de tempo confiável permite avaliar quando ela foi aplicada. No macOS, para distribuir fora da App Store, assine com Developer ID e envie o software ao serviço de notarização da Apple. O resultado aprovado gera um ticket que pode ser anexado nos formatos compatíveis.

Defina o ponto da verificação

Verifique o artefato final que chegará ao usuário. Se a entrega inclui instalador e executável, valide ambos. Mantenha o acesso à chave de assinatura restrito ao processo de release.

Assinatura de código

Valide o instalador da agenda no Windows

Exemplo em PowerShell com SignTool do Windows SDK

```
signtool verify /pa /all /v /tw ".\AgendaSetup.exe"
if ($LASTEXITCODE -ne 0) {
  throw "Verificação da assinatura falhou ou emitiu aviso."
}
```

Leia o resultado

Use /pa para a política Authenticode e /all para verificar todas as assinaturas, se houver mais de uma. /v mostra detalhes e /tw emite aviso se faltar carimbo de tempo. O script reprova tanto falha quanto aviso.

Cheque a identidade esperada

Confira o signatário exibido e a cadeia de certificação. Em um pipeline, compare a identidade do certificado de assinatura com a política da sua release, que deve prever a rotação. Um arquivo pode ter assinatura válida e vir de outro editor.

Assinatura de código

Exercício resolvido

Cenário

O build anterior passou na verificação. No novo release, o instalador foi modificado depois da assinatura e a verificação falhou. O que deve mudar na ordem das etapas?

Resolução

Finalize o conteúdo antes de assinar. Assine primeiro os componentes que entrarão no instalador. Gere o instalador com esses componentes e assine o instalador final. Valide os artefatos e publique os mesmos bytes que passaram na verificação.

Critério de aceite

Compare os resultados em um instalador de teste assinado e em uma cópia sem assinatura. A cópia sem assinatura deve ser reprovada. No instalador assinado, exija código zero e o editor esperado. Se faltar carimbo de tempo, trate o aviso antes da publicação.

Referências primárias

Microsoft — SignTool

Apple — Developer ID e notarização

Assinatura de código

Verifique o arquivo que será distribuído

Separe assinatura e notarização

A assinatura vincula o código ao desenvolvedor e permite verificar sua integridade. A notarização é uma etapa adicional na distribuição fora da Mac App Store. Verifique o pacote final antes de publicar e teste sua abertura em um Mac de teste.

Exercício adicional

Uma equipe alterou um recurso no aplicativo após assinar. Como preparar a nova entrega?

Resolução

Gere o pacote com o recurso correto, assine novamente e repita a notarização aplicável. Verifique o artefato final e mantenha o mesmo arquivo no canal de distribuição.

Ao assistir ao vídeo

Observe a finalidade da notarização. Para executar o processo hoje, consulte as instruções atuais da Apple sobre notarytool.

Vídeo complementar

Apple WWDC - All About Notarization (em inglês)