Entrust CodeSafe®

Proteção de hardware certificada para aplicações confidenciais

DESTAQUES

CodeSafe: execute o código em um ambiente seguro

- Protege aplicativos confidenciais ao executá-los dentro de módulos de segurança de hardware (HSMs) resistente a falsificações
- Ajuda a garantir a integridade através da assinatura e verificação digital do código
- Oferece um ambiente seguro para gerenciamento de chaves através da a imposição da política
- Oferece forte controle de acesso associando chaves e certificados a aplicações
- Oferece uma solução conveniente usando ferramentas CodeSafe remotas

CodeSafe é um conjunto de ferramentas que permite aos desenvolvedores gravar e executar aplicações dentro do limite resistente à adulterações dos HSMs nShield certificados por FIPS. As aplicações executadas no ambiente de execução seguro podem criptografar, decriptografar e processar dados, bem como se beneficiam da execução pelo HSM de políticas que regem o uso das chaves de aplicativos.

Vasta gama de aplicações

O CodeSafe pode ser usado para proteger qualquer tipo de aplicação. Os exemplos incluem criptografia e lógica comercial de alto valor associadas a serviços bancários, medição inteligente, agentes de autenticação, assinatura digital agentes e processos de criptografia personalizados.

Garantia da integridade da aplicação CodeSafe

O CodeSafe fornece ferramentas para assinar digitalmente os aplicativos em execução no ambiente de execução segura do nShield para que sua integridade possa ser verificada pelo HSM no momento da execução.

Entrust CodeSafe®

PRINCIPAIS RECURSOS E BENEFÍCIOS

Execução da política e controle de acesso de chaves CodeSafe

O CodeSafe permite que o proprietário do software defina as políticas que regem o uso de dados do aplicativo, incluindo chaves e certificados - e executa essas políticas, fornecendo um ambiente seguro para o gerenciamento de chaves. O CodeSafe também associa com exclusividade as chaves e certificados a aplicações designadas para garantir forte controle de acesso.

Endpoints SSL/TLS seguros

Os desenvolvedores do programa CodeSafe podem incorporar a biblioteca OpenSSL em suas aplicações para encerrar sessões SSL/TLS dentro do HSM nShield, facilitando a criptografia de ponta a ponta e fortalecendo a segurança da camada de transporte de dados e reduzindo a superfície de ataque.

Implantação remota e atualizações

Os administradores podem implantar aplicativos de um local central, evitando a necessidade de acesso físico aos HSMs.

Compatibilidade do nShield

O CodeSafe está disponível com os HSMs nShield Solo PCIe e nShield Connect conectados à rede e certificados pelo FIPS 140-2 Nível 3. Os modelos compatíveis incluem todos os HSMs nShield modelo Solo e Connect incluindo a linha de produtos XC.

Ambiente de desenvolvimento do HSM

O CodeSafe é compatível com as seguintes aplicações de programação:

- Linguagens de programação C e C ++ para aplicativos integrados
- C, C++ e Java no servidor host

Introdução ao CodeSafe

Para usar o CodeSafe, você precisará de:

- HSM nShield Solo ou Connect certificado por FIPS 140-2 Nível 3
- Kit de ferramentas de desenvolvedor do CodeSafe
- Licença de ativação do CodeSafe

O kit de ferramentas do desenvolvedor CodeSafe inclui tutoriais, documentação e programas de amostra para ajudá-lo a integrar seu aplicativo com os HSMs nShield. A equipe de Serviços Profissionais da Entrust também está disponível para ajudá-lo com sua integração.

Saiba mais

Um informe técnico do CodeSafe está disponível a pedido, oferecendo uma discussão mais aprofundada sobre a tecnologia subjacente. Para saber mais sobre os HSMs Entrust nShield, visite **entrust.com/HSM**. Para saber mais sobre as soluções digitais da Entrust para identidades, acesso, comunicações e dados, visite **entrust.com**

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com