Serviços em nuvem protegidos em nível federal com ORC e Entrust

O PIVotal ID™da ORC, uma solução de identidade federada usada pelo governo dos Estados Unidos, mostra como a identidade como serviço (IDaaS) baseada em nuvem apoiada por criptografia reforçada oferece segurança forte e ampla interoperabilidade.

Para muitas empresas que estão pensando em mover dados confidenciais para a nuvem, as questões de segurança continuam sendo uma preocupação significativa. Mas uma empresa, a Operational Research Consultants Inc. (ORC), está provando que a nuvem realmente pode se tornar tão segura ou até mais segura do que as implantações locais, mesmo para organizações tão focadas na segurança como o Governo Federal dos EUA.

ORC – UM PIONEIRO NA GESTÃO FEDERAL DE IDENTIDADE

A ORC tem sido um parceiro confiável do governo dos EUA desde meados dos anos 90, quando a empresa lançou a Infraestrutura de Chave Pública de Aquisição da Marinha para apoiar interações seguras com contratantes e fornecedores. À medida que a ênfase do governo na garantia da informação se expandiu nas duas décadas seguintes, a ORC se tornou um parceiro de referência para soluções de segurança e uma das primeiras empresas autorizadas a fornecer soluções de gerenciamento de identidade em conformidade com o governo.

Hoje, a ORC gerencia mais de três milhões de identidades e emitiu mais de 10 milhões de certificados digitais em conformidade com o governo federal para uma variedade de funcionários, contratados, aliados, veteranos e cidadãos que fazem negócios com o governo.

ORC

A NECESSIDADE DE IDENTIFICAÇÃO E AUTENTICAÇÃO SEGURA E INTEROPERÁVEL

Em agosto de 2004, o governo Bush emitiu uma Diretriz Presidencial de Segurança Interna (HSPD-12) para proteger instalações e recursos federais, estabelecendo um padrão governamental para formas seguras e confiáveis de identificação. Indo muito além da simples emissão de crachás de identificação para funcionários do governo, esta iniciativa se concentraria nos processos necessários para emitir credenciais pessoais seguras, em métodos para validar esses processos de emissão e credenciais e no gerenciamento de risco e qualidade em todo o ciclo de vida das credenciais.

O programa Personal Identity Verification (PIV) implementa esses processos e o FIPS (Federal Information Processing Standard) 201 especifica a interface e os elementos de dados do cartão inteligente PIV. Entre os elementos de dados em um cartão PIV estão uma ou mais chaves criptográficas privadas assimétricas. Departamentos e agências devem usar uma infraestrutura de chave pública (PKI) compatível para emitir certificados digitais para usuários. A iniciativa PIV também gerou outras credenciais de alta garantia que oferecem suporte a transações específicas de empresa para governo, cidadão para governo e cidadão para empresa, ao mesmo tempo que oferece suporte à interoperabilidade federada entre as credenciais emitidas. Isso inclui várias variantes PIV-Interoperável (PIV-I) e PIV, como: Credencial de Identificação do Trabalhador de Transporte (TWIC®), Credenciais de Autenticação do Primeiro Respondente (FRAC), Verificação de Identidade Comercial (CIV) e Autoridade de Certificação Externa (ECA) PIV -I que atendem a vários requisitos regulamentares e são construídos para escalar globalmente. Os processos e políticas para emissão de certificados e as proteções concedidas à raiz crítica e às chaves de autoridade de certificação de emissão nessa PKI são fatores críticos no nível de garantia geral do sistema.

OS DESAFIOS: CERTIFICAÇÃO, INTEROPERABILIDADE E CONFIANÇA

Os sistemas tradicionais de gerenciamento de identidade local não se estendem facilmente à nuvem. Reconhecendo que a segurança era um diferenciador importante para que o gerenciamento de identidade baseado em nuvem fosse confiável em todo o governo federal, o ORC sabia que a criptografia de alta segurança era a única maneira de atender aos requisitos de segurança do NIST. No contexto da PKI, isso significava que a raiz e as chaves da autoridade de certificação emissora precisavam ser geradas e protegidas em hardware certificado por FIPS de alta segurança. Os motivos iam além da simples segurança forte: o impacto operacional do comprometimento de uma dessas chaves seria que todos os certificados emitidos sob a PKI precisariam ser revogados e todas as credenciais emitidas novamente.

O ORC também enfrentou vários requisitos de certificação e acreditação, incluindo Federal Bridge, PIV/PIV-I, DoD e FISMA e a necessidade de oferecer suporte à certificação cruzada em vários níveis, exigindo uma solução que pudesse suportar uma gama flexível de níveis de garantia e políticas. A solução também precisava ser comprovada e baseada em padrões de sistemas abertos para garantir ampla interoperabilidade. Finalmente, a ORC reconheceu a importância de fornecer alta disponibilidade e confiabilidade para serviços criptográficos em um ambiente de nuvem.

ORC

A SOLUÇÃO: ORC PIVOTAL ID™ E ENTRUST

A fim de fornecer altos níveis de garantia para serviços federais em nuvem o ORC oferece um conjunto de soluções chamado PIVotal ID™. PIVotal ID™ inclui serviços gerenciados certificados e credenciados para a emissão de fortes credenciais de identidade que são confiáveis em todo o governo federal e podem federar globalmente, incluindo a emissão de certificados digitais de PKIs apoiados por módulos de segurança de hardware Entrust nShield® de alta garantia (HSMs). A ORC emitiu e gerencia milhões de credenciais compatíveis, permitindo transações seguras para agências federais dos EUA (civis e de defesa), seus funcionários, a comunidade contratante global, parceiros comerciais, veteranos e cidadãos que precisam conduzir negócios com qualquer faceta do governo dos EUA e indústrias regulamentadas. PIVotal ID™ inclui:

- Verificação de identificação pessoal (PIV)
- Emissor não federal PIV-interoperável (NFI PIV-I)
- Autoridade Certificadora Externa (ECA)
- Certificados de acesso para serviços eletrônicos (ACES)
- TWIC Autoridade de fabricação de certificados
- PIVotal Commercial™ (PIV-CIV)
- PIVotal Validation™

A ORC reconheceu que a família de HSMs Entrust nShield oferece proteção superior e recursos de aceleração criptográfica, bem como flexibilidade e escalabilidade para proteger e gerenciar chaves raiz e todas as chaves subordinadas em sua infraestrutura de serviço em nuvem segura.

SOLUÇÕES EFICAZES PARA CRIPTOGRAFIA ROBUSTA

Os HSMs Entrust nShield são construídos em uma plataforma reforçada e resistente a adulteração que protege e gerencia chaves confidenciais usadas para criptografia e assinatura digital para oferecer suporte a praticamente qualquer aplicativo, desde gerenciamento de identidade, serviços da Web e criptografia de banco de dados até tokenização, serviços de PKI e autenticação forte. Os HSMs nShield oferecem a maneira mais econômica de estabelecer os níveis apropriados de controles físicos e lógicos para sistemas onde a segurança oferecida pela criptografia baseada em software é considerada inadequada.

ORC

OS HSMs ENTRUST NSHIELD PERMITEM ÀS EMPRESAS:

- Obter flexibilidade operacional incomparável, alta disponibilidade e escalabilidade em ambientes virtualizados e em nuvem.
- Reduzir o custo de conformidade regulamentar e tarefas de gerenciamento de chaves do dia a dia, assim como backup e gerenciamento remoto.
- Obtenha alta garantia de continuidade de negócios com registro HSM simplificado, provisionamento de chave eficiente e recursos de hardware totalmente resilientes.
- Aumente a segurança de aplicativos críticos, protegendo chaves criptográficas e operações em hardware resistentes à adulteração.
- Estabeleça uma forte separação de funções por meio de políticas de administração robustas, incluindo autenticação multifator baseada em função e flexível autorização baseada em quorum.

SOBRE A ORC

A ORC, uma empresa WidePoint e parceira confiável do governo federal dos Estados Unidos, oferece soluções de segurança de informações para clientes governamentais e corporativos, garantindo assim a troca e garantia de informações totalmente compatíveis e confiáveis. Como um provedor de elite de serviços de garantia de informações e autenticação para empresas para governo, governo para governo e cidadão para governo, as soluções da ORC são interoperáveis com sistemas legados e integram-se perfeitamente com todos os principais aplicativos de software do mercado. A ORC potencializa os HSMs Entrust nShield para fornecer serviços de gerenciamento de identidade em nuvem com segurança de nível federal.

SOBRE A ENTRUST

A Entrust mantém o mundo movendo-se com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com