A Bit4id aprimora o sistema de cartão de identificação eletrônica da Middle Eastern electronic com sistema de identificação digital on-line compatível com eIDAS usando os HSMs Entrust

A Bit4id desenvolve tecnologias fáceis, seguras e padronizadas para autenticação, assinaturas digitais e criptografia. Com sede na Itália, a empresa possui escritórios no Equador, Índia, Macau, Peru, Portugal, Espanha e Reino Unido.

A filosofia da Bit4id é que, assim como a identidade física de uma pessoa é única e universalmente reconhecida, a identidade digital dessa pessoa deve ser única e capaz de representá-la com segurança em redes de computadores e na internet. Ela também acredita que, para os programas de identidade digital terem sucesso, eles devem ser simples e seguros, além de fáceis e naturais de usar - tanto para as empresas que os gerenciam quanto para os indivíduos que os utilizam.

> **« Os HSMs Entrust nShield são o padrão em todo o mundo. Desenvolvemos projetos com base na extraordinária confiabilidade e disponibilidade que os HSMs Entrust nShield fornecem e os integramos a todos os nossos produtos. Confiamos na marca Entrust e em seus produtos implicitamente. »**
>
> – Pierluigi Pilla, diretor de sistemas de ID e Unidade PKI da Bit4id

SAIBA MAIS EM ENTRUST.COM/HSM

Bit4id

DESAFIO DO NEGÓCIO

Como parte de uma joint venture de integradores de sistemas, a Bit4ID ganhou um contrato com o Ministério da Informação (MIT) de um país do Oriente Médio, para fornecer uma solução de identidade digital móvel para toda a sua população, incluindo cidadãos e não cidadãos do país. O país já tinha implementado um sistema de cartão de identificação eletrônico (microchip), mas o MIT queria complementar esse sistema com uma infraestrutura de TI para gerar e gerenciar IDs digitais no ciberespaço - modelado e compatível com a Identificação Eletrônica e Serviços de Confiança da União Europeia (EU's) (eIDAS). Usar o modelo eIDAS não só garantiria uma abordagem de boas práticas, mas a conformidade permitiria o comércio com a UE e outros países que aderissem a esse padrão.

DESAFIO TÉCNICO

PKIs, certificados digitais e identidades digitais

A Infraestrutura de chave pública (PKI) ajuda a estabelecer a identidade de pessoas, dispositivos e serviços, permitindo acesso controlado a sistemas e recursos, proteção de dados e responsabilidade em transações on-line. PKI é a base que permite o uso de tecnologias como assinaturas digitais e criptografia em grandes populações de usuários. Consequentemente, as PKIs são essenciais para transações governamentais e de comércio eletrônico seguras e confiáveis.

Certificados Digitais

Os certificados digitais são as credenciais que facilitam a verificação de identidades entre os usuários em uma transação. Assim como um passaporte certifica a identidade de alguém como cidadão de um país, o certificado digital estabelece a identidade dos usuários dentro do ecossistema. Como os certificados digitais são usados para verificar a identidade do signatário das informações, proteger a autenticidade e a integridade do certificado é fundamental para manter a confiabilidade do sistema.

Autoridades Certificadoras

Uma Autoridade Certificadora (CA) é o componente central de uma PKI responsável por estabelecer uma cadeia hierárquica de confiança. As CAs emitem as credenciais digitais usadas para certificar a identidade dos usuários e sustentar a segurança do PKI e dos serviços que ele oferece. Os controles físicos e lógicos e os mecanismos de proteção de um módulo de segurança de hardware (HSM) garantem a integridade de uma PKI e reduzem o risco de ataque.

eIDAS

A eIDAS é uma regulamentação da UE que estabelece padrões para identidades eletrônicas, autenticação e assinaturas. Aplica-se a entidades governamentais e empresas que fornecem serviços online a cidadãos europeus e que reconhecem ou utilizam identidades, autenticação ou assinaturas. A eIDAS também requer o uso de HSMs certificados por Common Criteria EAL4 + (AVA_VAN.5) para emitir certificados digitais, assinaturas digitais, time stamps e outros dados transacionais.

Requisitos do sistema

O MIT já tinha uma PKI para emitir cartões de identificação eletrônicos aos seus cidadãos. O Bit4id precisava integrar recursos adicionais à PKI que pudessem:

- Permitir que os residentes assinassem digitalmente transações e documentos de desktops e dispositivos móveis, como notebooks digitais, tablets e smartphones

Bit4id

- Expandir facilmente
- Gerar certificados para milhões de usuários
- Processar muitos milhares de transações por segundo

SOLUÇÃO

Um dos motivos pelos quais o MIT concedeu este projeto à Bit4id foi sua proposta de que os certificados móveis fossem armazenados em um HSM Entrust nShield®, certificado para Common Criteria EAL4+, em vez de no próprio dispositivo, como um telefone móvel. Isso estaria de acordo com os regulamentos da eIDAS sobre credenciais digitais remotas. Sendo bem versado em conformidade com a eIDAS, a Bit4id sabia como fazer o sistema funcionar.

A empresa desenvolveu um sistema de identidade digital personalizado que facilita o tráfego entre a PKI nacional, os HSMs Entrust nShield e os residentes do país do Oriente Médio que usam o sistema. O sistema gerencia com segurança a emissão de certificados pela PKI nacional para o HSM, regula o uso de certificados do HSM para usuários e controla o gerenciamento do ciclo de vida do certificado (por exemplo, suspensão, revogação, renovação). Os certificados são necessários para que os usuários sejam identificados e autenticados no sistema e, em seguida, assinem documentos em vários aplicativos do governo, como abertura de empresa, declaração de imposto de renda eletronicamente ou assinatura e envio de documentos para correspondência legal.

A implantação atualmente usa a solução SignCloud da Bit4id junto com seu aplicativo auxiliar de middleware, Universal Key Chain, e um total de quatro HSMs nShield Connect XC: um para desenvolvimento, um para teste e dois para produção, incluindo um mecanismo de failover. Isso fornece alta disponibilidade e balanceamento de carga para uma operação suave. A Bit4id também aproveitou a arquitetura única do Security World da Entrust, que permite o armazenamento de chaves como arquivos criptografados e protegidos fora dos limites físicos do HSM. Isso fornece armazenamento de chaves virtualmente ilimitado.

O sistema de identificação digital atual está sendo usado principalmente para aplicativos do governo para os cidadãos. No entanto, existem planos em vigor para replicar a implantação atual para permitir mais casos de uso que fazem uso de assinaturas digitais em aplicativos de governo para empresa e governo para governo.

“A Bit4id trabalhou com a Entrust e usou seus HSMs nShield por muitos anos”, disse Pierluigi Pilla, ID Systems e Diretor da Unidade de PKI da Bit4id. “Os HSMs da Entrust são o padrão em todo o mundo. Desenvolvemos projetos com base na extraordinária confiabilidade e disponibilidade que os HSMs Entrust nShield fornecem e os integramos a todos os nossos produtos. Confiamos na marca Entrust e em seus produtos implicitamente.”

Bit4id

Necessidade do negócio

Criar um sistema de identificação digital on-line que complemente um sistema de cartão de identificação eletrônico existente e seja compatível com o eIDAS

Necessidade de tecnologia

Integrar na infraestrutura adicional de PKI existente que pudesse:

- Permitir que os residentes assinassem digitalmente de desktops e dispositivos móveis, como notebooks digitais, tablets, smartphones
- Expandir facilmente
- Gerar certificados para milhões de usuários
- Processar muitos milhares de transações por segundo

Soluções

Projetar um sistema de identificação digital personalizado usando:

- Bit4id SignCloud
- Bit4ID Universal Key Chain
- HS<s Entrust nShield Connect
- Arquitetura nShield Security World

Resultados

- Criação de um sistema nacional de ID digital móvel
- Satisfez os requisitos de negócios, tecnologia e segurança do cliente
- Sistema robusto em breve a ser duplicado e expandido para outros casos de uso

RESULTADOS

A Bit4id criou um sistema de identificação digital móvel compatível com a eIDAS que complementa o sistema de cartão de identificação eletrônico existente nos países do Oriente Médio. O sistema:

- Permite que os residentes assinem digitalmente em desktops e dispositivos móveis
- Expande facilmente
- Gera certificados para milhões de usuários
- Processa muitos milhares de transações por segundo
- Está programado para ser duplicado e expandido para aplicativos de governo para empresa e de governo para governo

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