Entrust nShield HSMs secure Hitachi's finger vein biometrics

How Entrust is helping to secure a BioPKI solution that facilitates electronic signatures of documents in the banking sector.

THE CHALLENGE: SECURING A GROUND-BREAKING AUTHENTICATION TECHNOLOGY IN A HIGHLY REGULATED INDUSTRY

As a global leader in the development of technology for consumers, business and governments, Hitachi saw the opportunity for its Finger Vein biometric authentication system to revolutionize digital signatures in the banking sector.

Using the blood vessel pattern inside the finger to authenticate a person's identity, Finger Vein technology offers a precise, efficient and advanced form of biometric authentication. When applied to the banking industry, Hitachi's technology would allow banks to authenticate users in less than one second by comparing a real-time scan of a finger with the customer's Finger Vein profile stored in a database. Using Finger Vein technology would reduce a bank's use of paper documents, minimizing costs related to printing, scanning, indexing, transport, archiving and shredding of paper documents.

Hitachi

The key to the success of this authentication technology in the banking sector would be the security of its biometric digital signatures, or BioPKI, an alternative to the traditional model of digital signature. Finger Vein BioPKI is a mix of biometrics and PKI and requires the use of Finger Vein authentication to manage the access to the user's private key which is stored securely in the bank's back office system. Hitachi knew that for Finger Vein technology to gain wide acceptance within the banking community, it would need a highly secure solution to protect the authentication process and any associated stored data.

THE SOLUTION: ROLE OF ENTRUST HSMS

Hitachi chose Entrust nShield® hardware security modules (HSMs) for use in its BioPKI deployment in the Central Eastern Europe (CEE) market. Access to private keys for the Finger Vein authentication is protected by a certified Entrust nShield HSM, a highly secure and tamper-resistant device located in the back office of the bank, where it is responsible for the creation of the digital signature and for protecting secret keys. Entrust's unique CodeSafe capability is used to execute custom signature creation code inside the certified security boundary of the HSM.

The implementation of this innovative biometric solution for customer authentication in bank branches in Poland was the first in Europe, and based on experience gained during the practical implementation of projects in the financial sector in Poland, Hitachi now recommends its BioPKI customers to use HSMs.

The Entrust nShield HSM hardware has been successfully used to implement biometric digital signatures in Banks such as BZ WBK (pilot project in branches) and Getin Noble Bank (branches and VTMs).

Hitachi's solution is well matched to the requirements of the applicable laws in Poland. Meeting the expectations of auditors and regulators was possible thanks to, among other things, the use of HSMs for storing and protecting the private keys.

ABOUT THE SOLUTION

Entrust HSMs

Entrust nShield HSMs provide a tamper-resistant environment for secure cryptographic processing and key management. nShield HSMs are certified and meet established and emerging security standards for cryptographic systems while staying highly efficient.

nShield HSMs isolate and protect cryptographic operations and keys for organizations' most critical applications. nShield HSMs perform encryption, digital signing, and key management for an extensive range of applications including public key infrastructures (PKIs), SSL/TLS, and code signing. nShield HSMs are high-assurance alternatives to software-based cryptography – supporting all leading algorithms and featuring world-class ECC performance.

Hitachi

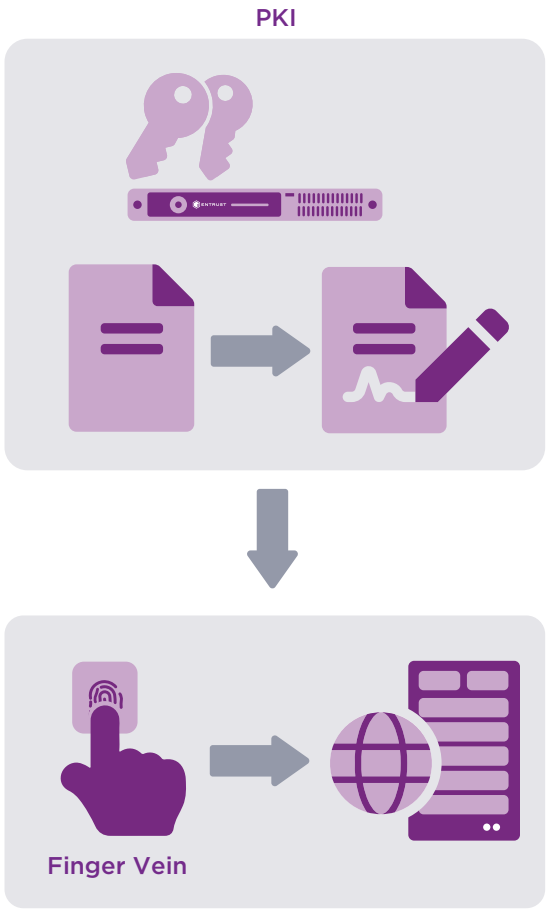
Entrust CodeSafe

CodeSafe is a unique capability of Entrust nShield HSMs which enables developers to execute applications within the certified security boundary of the HSM, protecting them from threats such as insider attacks, malware, and Trojans that they would be vulnerable to on typical server platforms.

WHY ENTRUST?

Hitachi chose Entrust nShield HSMs as the company's preferred cryptographic technology for use in its BioPKI solutions in the CEE market, for multiple reasons:

- **Security**. HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. These devices enabled Hitachi to deploy high assurance security solutions that satisfy widely established and emerging best practices for cryptographic systems and practices-while also maintaining high levels of operational efficiency.
- **Performance**. "You expect high levels of security from an HSM. HSMs also provide the superior performance, scalability, and reliability needed to protect your authentication process and allow for selected code (in our case, the signature creation code) to be installed and executed inside the boundary of the HSM", explained Przemysław Cychowski, Technical Director, Europe and CIS for Information Systems Group, Hitachi.



Triggering digital biometric signature mechanism

- **Reputation**. According to Tadeusz Woszczynski, Regional Director, Central Eastern Europe and CIS for Information Systems Group, Hitachi, "Using a proven solution such as Entrust nShield HSMs is a critical element of our strategy to provide the most secure biometric signature solution to banking sector.

Hitachi

KEY BENEFITS OF USING ENTRUST NSHIELD HSMs

- Automate risk-prone administrative tasks, guarantee key recovery, and eliminate costly manually-intensive backup processes
- Enable secure execution of custom security-critical application code within the tamper-resistant hardware boundary
- Support high volume, enterprise transactions with accelerated transaction rates
- Simplify scaling as security needs expand with flexible architecture
- Reduce the cost of traveling to data centers with nShield Remote Administration
- Establish strong separation of duties through robust administration policies including role-based multi-factor authentication and quorum-based authorization

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com