NCIPHER

www.ncipher.com

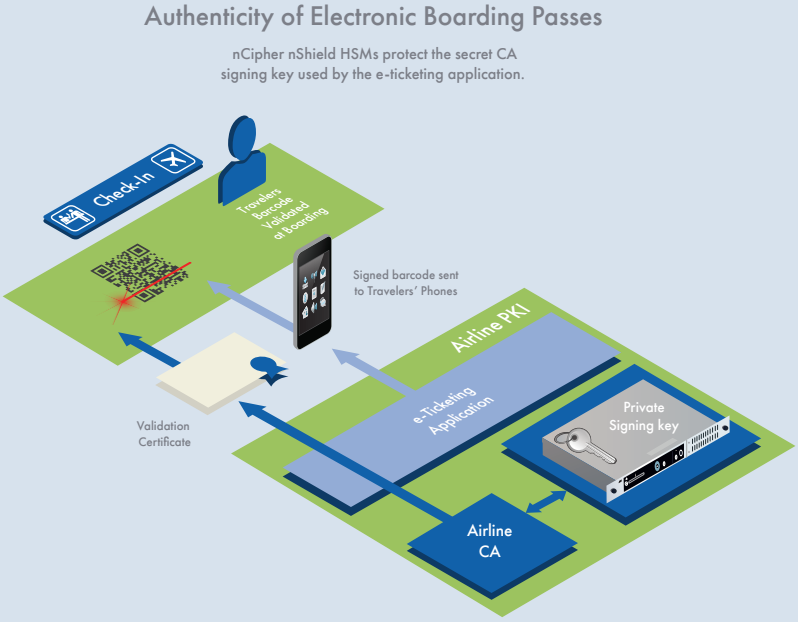
nCipher hardware security modules provide root of trust for secure electronic boarding pass issuance and validation

- Protects integrity and authenticity
- Leverages public key infrastructure
- Enables reliable and trusted validation
- Prevents misuse, counterfeit and fraud
- Safeguards critical signing keys in a FIPS 140-2 Level 3 certified module

nCipher helps airlines protect the integrity and authenticity of electronic boarding passes

THE PROBLEM: ELECTRONIC BOARDING PASSES ISSUED ONLINE MAY BE SUSCEPTIBLE TO ALTERATION AND MANIPULATION

Electronic boarding passes have quickly become ubiquitous in the airline industry, enabling their delivery over the Internet – direct to travelers' phones and portable devices. The speed, convenience and cost-savings have led to rapid adoption by carriers and swift acceptance by travelers. Electronic boarding pass systems use various forms of barcodes for validation. Alteration and manipulation of these barcodes can lead to security breaches. In today's heightened security environment, electronic boarding passes must be trusted to only grant access to authorized passengers. Protecting the systems that issue and validate them is therefore critically important.



nCipher helps airlines protect the integrity and authenticity of electronic boarding passes

THE CHALLENGE: ENSURING YOU CAN TRUST YOUR SYSTEM TO PROTECT ELECTRONIC BOARDING PASSES

The integrity and authenticity of an electronic boarding pass is validated by checking the digital signature of the barcode they use. A digitally signed barcode protects against forgery and enables validation upon check-in. Carriers use private signing keys to sign barcodes and issue associated public certificates from a public key infrastructure (PKI) for their validation. The degree to which carriers can trust their PKI depends on the protection afforded to the root and issuing CA private signing keys. The private signing keys underpin the security of the entire system, and properly safeguarding and managing them is essential.

THE SOLUTION: NCIPHER DELIVERS HIGH PERFORMANCE AND ENHANCED SECURITY FOR PKI-ENABLED E-TICKETING APPLICATIONS

The risk of boarding pass forgery can have severe effects on air safety. Today, the easiest way to issue a non-authentic boarding pass is if the carrier's private signing key is compromised. Best practices recommend the protection of private signing keys in specialized hardened devices or hardware security modules (HSMs). HSMs not only safeguard private signing keys within a protected environment, but they also let carriers set specific access control policies so they are only used for their authorized purpose.

nCipher nShield HSMs are certified to Federal Information Processing Standard (FIPS) 140-2 level 3, which is the most widely adopted security benchmark for cryptographic solutions in government and commercial enterprises. nCipher's Professional Services offers expert advice and assistance in PKI deployment and key management to help establish an efficient, cost-effective, and secure electronic boarding pass system. Other corporate applications where the organizational PKI can be leveraged include personnel identity management and device credentialing to ensure adherence to corporate security guidelines. Whether requiring assistance in deploying a new PKI, rolling out applications that need the services of an existing PKI, or just needing the hardware to protect the critical private signing keys, nCipher can help.

WHY USE NSHIELD HSMS TO PROTECT SIGNING KEYS USED BY THE E-TICKETING PKI APPLICATION?

Digital certificates can only be considered trustworthy if they are issued by a trusted certificate authority (CA) using a unique signing key. If the signing key is compromised or stolen, the perpetrator can assume the identity of the signing airline and issue what appears to be legitimate boarding passes. Because HSMs provide a tamper-resistant environment that is significantly more secure than software, their use for this PKI application is recommended for the generation, storage and protection of the CA signing keys. nCipher nShield HSMs protects the critical signing keys so they never leave the security of the hardware module.

NCIPHER

nCipher nShield HSMs provides high performance cryptographic services for mission critical applications. Available as network-attached, embedded PCI Express or USB-connected modules, nShield:

- Stores encryption and signing keys in a tightly controlled and tamper resistant environment
- Supports separation of duties to protect from insider threats
- Ensures compliance with regulatory requirements
- Delivers high performance elliptic curve cryptography (ECC)

For more detailed technical specifications, please visit www.ncipher.com.