Securing Electronic Boarding Passes for Airlines

SOLUTION BRIEF

Benefits & Features

- Ensure authenticity and integrity of electronic boarding passes
- Comply with TSA digital signature requirements
- Increase customer satisfaction
- Streamline processes
- Easily integrate security into existing IT infrastructure
- Security system can be applied to protect against fraudulent paper boarding passes issued via Internet

Protect electronic boarding passes and comply with TSA digital signature requirements with the most trusted and fastest hardware security solution for automating digital signature and cryptographic operations.

Since the IATA updated the Bar Coded Boarding Pass standard (BCBP) in 2008 to include support for mobile devices, electronic boarding passes have become the latest trend in passenger travel.

Now passengers can receive paperless boarding passes containing barcodes along with identification and flight information on their cell phones, smartphones, or PDAs. The barcode is scanned for verification at airport security checkpoints, the boarding gate, and when passengers enter the plane – eliminating the need for a printed paper boarding pass. This technology increases security and improves customer satisfaction. As of January 2009, thirteen airlines already offer this service in North America, Europe, Asia, and the Middle East.

Digital Signatures for Maximum Security

In October 2008, IATA amended the mobile BCBP standard to include a digital signature in order to meet TSA security requirements for ensuring the authenticity and integrity of the digital boarding pass.

In a nutshell, authenticity ensures that the boarding pass was created by the airline that signed it, while integrity ensures that no unauthorized changes were made to the boarding pass after issuance by the airline. When signed boarding passes are scanned, authenticity and integrity are automatically verified through the digital certificate, allowing security officers to immediately detect fraudulent tickets that have been forged or altered after certified issuance.

SafeNet Hardware Security Modules Protect Digital Signatures

Electronic boarding passes are digitally signed as they are issued, using a secure private key issued by a trusted certificate authority. For maximum security and performance, ticket issuers deploy cryptographic hardware security modules (HSMs) for the storage of these signing keys, as well as for automating the process of securely binding the digital signature to the electronic boarding pass.

SafeNet HSMs provide the highest commercially available level of assurance for the integrity of the cryptographic keys and digital certificates. Stored on hardened and FIPS 140-2 Level 3-certified and Common Criteria EAL 4+-certified hardware appliances, cryptographic keys never leave the confines of the HSM, virtually eliminating vulnerabilities. Robust protection of keys is vital to the overall security of the system because if the keys and digital certificates are compromised, the entire chain of trust is broken, rendering the security system obsolete.

Automation of key management and digital signing in hardware also provides the highest possible level of performance and scalability, thereby ensuring that security does not slow down the process of issuing and verifying electronic boarding passes.

By applying HSMs to protect keys and digital signature operations, airlines can securely automate electronic boarding pass issuance, and thereby streamline processes, lower costs, improve customer satisfaction, and comply with TSA security requirements.

The World Trusts SafeNet HSMs

SafeNet is the world's most trusted vendor of hardware security modules with over 75,000 HSMs shipped worldwide. The world's most security-conscious government and commercial organizations rely on SafeNet HSMs for the protection of digital identities and sensitive data through secure management of cryptographic keys, digital signatures, and the automation of cryptographic operations. For more information, visit www.safenet-inc.com.

About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies, and in over 100 countries, trust their information security needs to SafeNet.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected