Hardware Security Module – Reliable, Secure, Fully Automated, Unattended Bacs Transactions

> " HSMs are used to secure a multitude of financial applications around the world, ranging from ATM and POS networks to inter-bank funds transfer and share dealing systems. "

An HSM is a physically secure, tamper-proof device that performs the cryptography in place of a user with a smartcard.

The HSM enables a large degree of flexibility in implementing security policies. A full range of options are available, from fully automated unattended operation to multi-user manual signing processes.

The signing of individual payment files, the signing of submissions, establishing a secure connection to Bacstel-IP and the retrieval of reports, are all activities that can engage the HSM and can have their own defined security requirements.

The Hardware Security Module
HSMs are tamper-resistant devices that provide the cryptographic facilities underpinning Public Key Infrastructure (PKI). HSMs are used to secure a multitude of financial applications around the world, ranging from ATM and POS networks to inter-bank funds transfer and share dealing systems. Our HSMs are housed at the Finastra data centers.

Certificate Signing Request
The public key, along with general information about the Service User, is presented to the sponsoring bank in a certificate signing request. The sponsoring bank issues a digital certificate to the Service User, which will be used in all Bacstel-IP transactions to authenticate the Service User. The certificate is only valid for a fixed period of time, and Finastra provides support to ensure certificates are renewed in a timely manner.
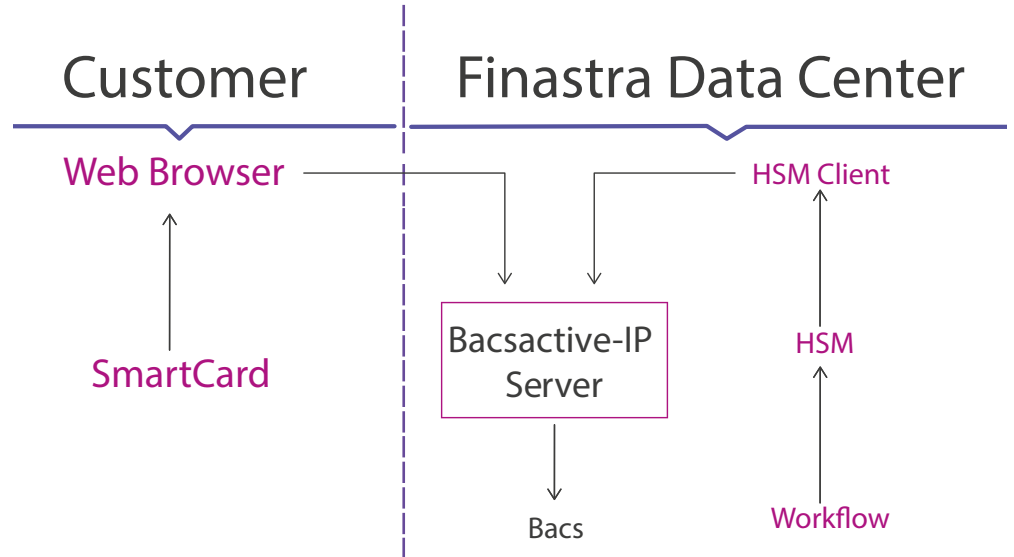
Certificate Management
Many certificates may be stored if required (for example, if multiple sponsor banks are used) and can be called upon to authorize transactions on behalf of any number of Bacs Service User Numbers or Bureau User Numbers. Usage of the certificates is managed automatically by the Bacsactive-IP Application. Keys and Certificates from both smart cards and from the HSM are seamlessly supported.

THE FUTURE OF FINANCE IS OPEN

Keys and Certificates from both smart cards and from the HSM are seamlessly supported

Features & Benefits

- Automatic operation—Fully automate all Bacstel-IP activities. Schedule out of hours submissions and report retrieval. Comprehensive support for error handling and reporting.
- Increase security—Store private keys in physically secure, tamperproof devices. Enables higher levels of security to be implemented.
- CSR and key management support— Built-in support for managing the HSM keys and for facilitating the Certificate Signing Request process.
- Flexible policies—Design security policies to suit your organization.

Customer | Finastra Data Center

Web Browser — HSM Client

SmartCard — Bacsactive-IP Server — HSM

Bacs — Workflow

Telephone
T +44 845 120 8050

Corporate Headquarters
4 Kingdom Street
Paddington
London W2 6BD
United Kingdom
T: +44 20 3320 5000

FINASTRA