

# TSS and Thales; working together to achieve compliance and efficiency

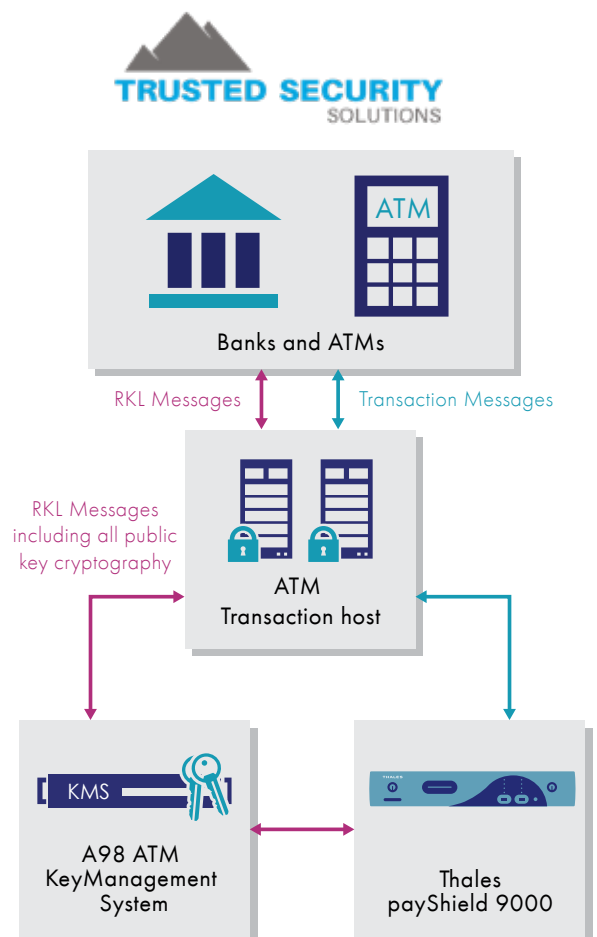


## Automating and simplifying ATM remote key loading to ensure compliance with PCI and network standards

- Comprehensive remote key loading solution for ATM networks
- Compliant with PCI 3.0 requirements and network standards
- Reduces manual steps and eliminates potential for fraud in key management Improves ATM uptime and simplifies upgrades and installations
- Includes remote key loading for ALL remote key enabled ATMs

## The problem: ATM owners need an automated and compliant means to load ATM terminal master keys

The cost of ATM ownership and the complexity of meeting compliance standards is only going one direction – UP! ATM owners can take a major stab at reducing these two headaches by implementing remote key loading (also called remote key transport or remote key distribution). Remote key loading takes advantage of the ATM's native ability to receive authenticated messages from the host, developing a "trusted path," so that a unique terminal master key can pass in a secure method directly from the host to the ATM. With remote key, there is no longer a requirement for two key custodians to physically visit the ATM when a key change is needed.



## The challenge: finding an affordable yet comprehensive remote key solution with great support

In 2004 when remote key loading for ATMs was first introduced, there were two basic flavors – Signature Based Protocol and Certificate Based Protocol. Things have changed. PCI has made new requirements to the art of remote key loading and ATM manufacturers have responded in different ways. Networks have likewise produced requirements and deadlines. ATM manufacturers are working diligently to implement both hardware and software changes to adapt to the new mandates. The remote key solution adapted by an ATM host switch or FI needs to be comprehensive, flexible, and ahead of the curve in adopting the latest requirements.

## The solution: A98 initial key establishment system and Thales payShield 9000 Hardware Security Modules (HSMs)

The A98 solution integrates with any host platform to remotely deliver terminal master keys to any remote key enabled ATM. No additional software is required to be installed on the ATMs. All legacy protocols and current PCI 3.0 protocols using SHA256 are included in the one A98 system. The A98 accesses the Thales HSM for all cryptographic calls including the use of TR-34 and TR-31.

Using manual methods for key loading requires unnecessary effort and expense and makes proving compliance an onerous task. With multiple key custodians in the field inputting secret keys into an ATMs PIN pad, there is room for error and collusion.

Remote key loading is a breath of fresh air for internal auditors and ATM operations personnel. From one central location, new random, unique terminal master keys are sent compliantly to the ATM as needed, when needed. This takes seconds versus hours and days.

## Why use Thales payShield 9000 HSM with A98 initial key management system?

The Thales payShield 9000 has all the RSA capabilities needed by the A98 System and is quick to provide additional encryption algorithms needed for the changing landscape of ATM vendor's remote key protocols. The A98 System takes full advantage of what Thales has to offer including operating in FIPS 140-2 Level 3 mode at all times.

## About Thales





The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

## Trusted Security Solutions, Inc.

Trusted Security Solutions, Inc. (TSS), a long-time leader in FI security and encryption, develops products and services that solve symmetric and asymmetric cryptographic key challenges using the latest technology available. Trusted Security Solutions, Inc. is a worldwide leader and industry trend setter in offering cryptographic solutions for ATM networks.

For more detailed technical specifications, please visit [thalescpl.com](http://thalescpl.com) or [www.trustedsecurity.com](http://www.trustedsecurity.com)

> [cpl.thalesgroup.com](http://cpl.thalesgroup.com) <    

**Americas** – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: [sales@thalessec.com](mailto:sales@thalessec.com)  
**Asia Pacific** – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: [apacsales.cpl@thalesgroup.com](mailto:apacsales.cpl@thalesgroup.com)  
**Europe, Middle East, Africa** – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: [emea.sales@thales-esecurity.com](mailto:emea.sales@thales-esecurity.com)