



experts in encryption & e-security

technical documentation

If you are in the encryption security business, you will already know Thales e-Security. They have been at the forefront of the global payments and IT security industry for more than 20 years. They are the trusted partner of many of the world's major financial institutions, recognized for integrity, innovation and technical excellence.

Thales e-Security is a member of the global Thales Group, which has more than 65,000 employees in 50 countries working in the aerospace, defence, and IT sectors.

Sahlin Documentation

Sahlin has provided documentation services to Thales e-Security over the last six years, and has produced a variety of User Manuals, Quick Start Guides, Programming Manuals and Online Help Systems for the majority of their products. The following is a sample of the products that the Sahlin authoring team has gained a comprehensive, hands on working knowledge of, including installation, configuration and product testing.

Host Security Module

The Thales e-Security business focuses on three strategic areas: card payments, e-security, and network security. The Host Security Module (HSM), as a hardware cryptographic unit, is employed across all these areas. The HSM is predominant in card payment security. Primarily designed to

address the ATM/EFTPOS market (and back office security services), the HSM 8000 provides all the functionality to address the needs of acquirers, switches, and issuers for the processing of magnetic stripe and chip card transactions (EMV).

P3 (Smartcard personalisation)

P3 is a Thales e-Security software product that works closely with the HSM. This innovative product provides:

- Secure data preparation for EMV Smart Cards
- 100% in-house control over cryptographic keys
- Supports major card association systems

WebSentry™ (e-commerce security)

WebSentry™ is a flexible, cost effective and comprehensive e-commerce security solution that enhances transaction throughput.

It provides tamper-resistant cryptographic hardware for encryption and digital signature applications in a PCI or freestanding unit. Easy Integration with applications using PKCS#11 (or customized interface industry standard protocols) mean WebSentry™ works with most systems, including those based on SET™ and SSL. Beyond e-commerce, it also provides cryptographic functions - including key generation, encryption and digital signatures - for a wide range of PKI applications.

3D-Security Module

This product will become increasingly important as the industry approved 3-D Secure internet payment system is rolled out. Most authorities on the subject agree that improved payment security is critical to increasing Internet sales. In accordance with Visa and MasterCard's stringent security requirements, Thales e-Security has developed the 3D-Security Module to facilitate development, integration and implementation of Access Control Servers and to provide the approved hardware security.

Datcryptor® 2000 (Network Security)

The Datcryptor 2000 range of hardware encryptors provides strong and certified perimeter security for a wide range of network architectures including dial and leased line links, Frame Relay, X.25 and IP networks. With triple DES or AES (128, 192, 256-bit)

algorithms built in, or using other customised, or national algorithms, it is the first family of encryption products to offer algorithm flexibility and protocol agility.

Features include:

- Signed Diffie-Hellman key exchange
- Digital signatures (DSA, SHA-1)
- Digital certificates (X.509)
- FIPS 140-2 (under evaluation)
- Designed to the highest security standards, FIPS & CAPS
- Physical integrity ensured
- FIPS 140-1 Level 3 / Security Sub-System certified FIPS-1 Level 4

Guardisk™

Thales Guardisk is a CESG approved hardware-based hard disk encryption device consisting of hard disk and security module that fits inside most laptop computers or desktop PCs. The Guardisk security module forms a barrier between the computer and the hard drive that cannot be circumvented. All the hard disk and temporary files are encrypted; encryption occurs transparently, on the fly, and without any perceivable performance loss.

Thales Guardisk™ reduces the classification of protectively marked data stored on the hard disk by two levels when the computer is switched off. For example, SECRET becomes treated as restricted and confidential becomes treated as unclassified. At present Guardisk™ is only available to customers eligible to receive key material from CESG and it is also under evaluation by the US Government.

Trusted VPN™ Confidence on the move - Confidence at home

The Internet's fundamental lack of security is perhaps the largest barrier to the remote workers' real productivity. The Trusted VPN™ card removes that barrier, making even the most sensitive of remote access activities secure. Trusted VPN™ enables mobile professionals to access exactly the same information and resources when they are on the move, as when they are in the office - with the same level of protection and security. This is a standard requirement for institutions such as Government, Health, and Defence - the same requirements are becoming standard in private enterprise.

THALES

To enquire further how we may help with your technical documentation, contact the experts:

Sahlin Documentation Limited

www.sahlin.co.uk

01624 833893

enquiries@sahlin.co.uk