





THALES

INFORMATION TECHNOLOGY SECURITY: PORTFOLIO OVERVIEW




Summary	Purpose	Business Value	Product Type	Technical function/certifications	Product Family Name
1 General purpose Hardware Security Modules (HSMs)	To securely protect cryptographic keys wherever they are used	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated cost in terms of fines and brand damage ✓ Enable deployment of cryptographic security without losing valuable business time from bottlenecks ✓ Achieve compliance/meet best practice including: <ul style="list-style-type: none"> - PCI DSS (81% of QSA's recommend the use of HSMs*) - SOX - Basel II - EU Data Protection ✓ Reduce time and money spent on compliance* <p><i>* PCI DSS Trends 2010 " QSA Insights (report is based on research conducted by The Ponemon Institute on behalf of Thales)</i></p>	Hardware (with associated user/developer software)	<ul style="list-style-type: none"> • Cryptographic key generation, protection and management • Cryptographic acceleration • FIPS 140-2 L3 Validated • Common Criteria EAL4+ 	<p>nShield Edge (USB Connected)</p>  <p>nShield Solo (PCI or PCIe)</p>  <p>nShield Connect (network connected and shareable)</p>  <p>Software Developer Kit (SDK)</p> 



INFORMATION TECHNOLOGY SECURITY: PORTFOLIO OVERVIEW


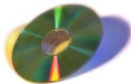


General purpose HSM use cases			
	Use summary	Purpose	Business value
a	Database Encryption	To provide strong protection and management of database encryption keys for embedded encryption technologies such as: <ul style="list-style-type: none"> • MS SQL Server 2008 and 2008 R2 • Oracle 11g (Advanced Security) 	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated costs in terms of fines and brand damage ✓ Achieve regulatory compliance
b	Web Servers and Web Services	To provide strong protection and management of Web Server SSL keys such as: <ul style="list-style-type: none"> • MS IIS and ISA • Apache • IBM HTTP Server • Sun iPlanet 	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated costs in terms of fines and brand damage ✓ Achieve regulatory compliance
c	Application Services	To provide strong protection and management of application keys such as: <ul style="list-style-type: none"> • IBM WebSphere • Oracle/BEA Weblogic • MS BizTalk Server • .Net 	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated costs in terms of fines and brand damage ✓ Achieve regulatory compliance
d	PKI	To provide strong protection and management for CA private keys used in conjunction with <ul style="list-style-type: none"> • MS Certificate Services • Entrust Security Manager • RSA Keon • CyberTrust Unicert 	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated costs in terms of fines and brand damage ✓ Achieve regulatory compliance
e	Document Management	To provide strong protection and management for digital signature keys and time stamping e.g. <ul style="list-style-type: none"> • Oracle RMS • Adobe LiveCycle Document Security • MS SharePoint 	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated costs in terms of fines and brand damage ✓ Achieve regulatory compliance
f	Strong Authentication	To provide strong protection and key management for digital signature keys used to underpin authentication solutions e.g. <ul style="list-style-type: none"> • Vasco • Gemalto • ActivIdentity • BellID • Cryptomathic • Thales Safesign (see below) 	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated costs in terms of fines and brand damage ✓ Achieve regulatory compliance

INFORMATION TECHNOLOGY SECURITY: PORTFOLIO OVERVIEW

	Summary	Purpose	Business Value	Product Type	Technical function/certifications	Product family name
2	Secure Time Stamping	<p>To prove that an electronic document or transaction was valid at the time of signing, even once the certificate has expired</p> <p>Use cases:</p> <ul style="list-style-type: none"> • Document signing • Transaction signing • Code signing 	<ul style="list-style-type: none"> ✓ Improved legal authenticity of electronically signed documents 	Appliance	<ul style="list-style-type: none"> • To provide timestamps in accordance with standards <ul style="list-style-type: none"> • RFC3161 • MS Authenticode • To deliver auditable time using DS/NTP 	<p>Time Stamp Server (TSS)</p>  <p>Time Source Master Clock (TSMC)</p> 
3	Payments-specific Hardware Security Modules (HSMs)	<p>To provide strong protection and management of payment processing keys</p> <p>Use cases:</p> <ul style="list-style-type: none"> • PIN translation • PIN printing • Transaction verification (such as CAP and 3DSecure) 	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated costs in terms of fines and brand damage ✓ Help achieve regulatory compliance (e.g. Visa, MasterCard and other national schemes) 	Hardware and associated customised firmware	<ul style="list-style-type: none"> • To protect and manage payment processing keys • Designed to meet payment processing schemes e.g. Visa, MasterCard and national schemes • FIPS 140-2 validated • Designed to meet PCI HSM standards 	<p>payShield 9000</p> 


THALES

INFORMATION TECHNOLOGY SECURITY: PORTFOLIO OVERVIEW

	Summary	Purpose	Business Value	Product Type	Technical function/certifications	Product family name
4	Card Personalisation	To provide secure card issuance Use cases: <ul style="list-style-type: none"> • EMV card issuance • Preparation of data 	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated cost in terms of fines and brand damage ✓ Save money by bringing card personalisation in-house 	Appliance and associated software	<ul style="list-style-type: none"> • Secure preparation and issuance of payment cards in accordance with EMV and other local standards 	P3 
5	Browser-based PIN Security	To ensure that customer PINs encrypted with SSL are never in the clear (e.g. between the Web Server and back end systems) Use cases: <ul style="list-style-type: none"> • Secure PIN verification 	<ul style="list-style-type: none"> ✓ Prevent interception of customer PIN and potential brand damage and fines ✓ Protect against the internal and external threat of PIN theft 	Software toolkit solution with associated hardware	<ul style="list-style-type: none"> • Termination of an SSL session within secure HSM boundary • General purpose hardware used in conjunction with toolkit is FIPS 140-2 L3 certified and CC EAL 4+ certified 	Codesafe SDK  nShield HSM 
6	Key Management for Storage Encryption Keys	To provide strong protection and management for storage encryption keys Use cases: used in conjunction with embedded encryption technologies such as: <ul style="list-style-type: none"> • Brocade Encryption Switches • IBM Tivoli Key Lifecycle Manager 	<ul style="list-style-type: none"> ✓ Reduce risk of security breaches ✓ Enable business continuity and data recovery ✓ Lower cost of maintenance encryption based storage ✓ Decrease time (and therefore cost) to deploy storage encryption ✓ Meet audit and compliance requirement 	Appliance	<ul style="list-style-type: none"> • Key management using standards-based protocols e.g. KMIP, P.1619.3 	Thales Encryption Manager for Storage (TEMS) 



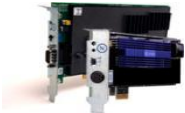


THALES

INFORMATION TECHNOLOGY SECURITY: PORTFOLIO OVERVIEW

	Summary	Purpose	Business Value	Product Type	Technical function/certifications	Product family name
7	In line Network Encryption	<p>To encrypt sensitive information passing between data centres over the network, to prevent sensitive data being intercepted</p> <p>Use cases:</p> <ul style="list-style-type: none"> • Point-to-point high speed wired or wireless • Frame Relay network • Inter & Trans-continental connectivity • SAN (Storage Area network) between data centres • WAN (Data, voice & video) 	<ul style="list-style-type: none"> ✓ Prevent loss of sensitive data and the associated cost in terms of fines and brand damage 	Appliance	<ul style="list-style-type: none"> • Point to point and point to multipoint line encryption • Fully automated centralised key management • Certifications include; <ul style="list-style-type: none"> - SGSS: FIPS 140-1 level4 - Unit: FIPS 140-2 level3 - Common Criteria 4 / 5 - UK CAPS Enhanced 	Datacryptor 2000 (DC2K) Datacryptor Advanced Performance (DCAP) 

THALES

INFORMATION TECHNOLOGY SECURITY: PORTFOLIO OVERVIEW

	Summary	Purpose	Business Value	Product Type	Technical function/certifications	Product family name
8	Strong Authentication Solution	<p>To strongly authenticate employees or customers to applications</p> <p>Use cases:</p> <ul style="list-style-type: none"> online banking transactions via tokens, smart cards (including EMV) mobile phones etc Authentication of clearing transactions e.g. bank to clearing house 	<ul style="list-style-type: none"> ✓ Improve customer confidence in on-line banking ✓ Maximise existing authentication technology investments e.g. EMV cards or tokens ✓ Reduce fraud online (saving costs of managing and compensating fraud) 	Software solution with associated hardware (general purpose HSMs – see above)	<ul style="list-style-type: none"> Authenticates Digitally signs Single Sign on User management Certifications:  <ul style="list-style-type: none"> Awards: <ol style="list-style-type: none"> Winner of the 2004 EEMA 'Award for Excellence in Secure Electronic Business' (User and vendor partnership: Thales and BACSTEL-IP) Winner of 2003 FST 'Best Use of B2B e-commerce' (User and vendor partnership: Thales and BACSTEL-IP) 2006 The Banker 'Technology Award' (For deployment of SafeSign with BankID; a Swedish service that offers secure electronic identification and signature on the Internet). 	<p>SafeSign Server</p>  <p>nShield general purpose HSM</p>   

THALES

INFORMATION TECHNOLOGY SECURITY: PORTFOLIO OVERVIEW

	Summary	Purpose	Business Value	Product Type	Technical function/certifications	Product family name
9	Professional Services	<p>To provide security and cryptographic services</p> <p>Use cases:</p> <ul style="list-style-type: none"> • Consultancy • Bespoke development • Training • Code reviews • Environment and policy review • Implementation assistance 	<ul style="list-style-type: none"> ✓ Reduce risk ✓ Decrease implementation time of security projects (reducing cost) ✓ Maximise the value of deploying encryption by filling a gap in in-house crypto knowledge ✓ Provide effective encryption systems, policies and processes 	<p>Services</p> <p>Customised code – software</p> <p>Documents and reports</p> <p>Training courses and associated materials</p>	<ul style="list-style-type: none"> • Project dependent • Thales professional staff extensively experienced in helping organisations worldwide to deploy cryptography • Many industry certified staff e.g. CISSP 	<p>Professional Services</p> 