



safe SIGN

SafeSign® PSM Personal Security Module

- Protects user identity
- Secures transaction information with electronic signature technology
- Smart Card plus Reader format
- No installation necessary
- Extensible platform to support multiple applications on the smart card
- Strong cryptography for maximum protection

SafeSign® PSM



Electronic Protection for the Electronic World

As the electronic world becomes increasingly part of everyday life, people's identity in the digital world becomes as important as their physical identity. Information and its availability to the right people at the right time is now a critical part of business processes, and can make or break the Enterprise. Additionally, the development of the Internet has fuelled the demand for real-time, online transaction systems to be available to everyone across the globe, anytime.

In such a complicated environment as the online networks, companies and individuals have generally omitted the importance of security and privacy, opening the door to identities being stolen and transactions being compromised, frequently resulting in loss of money or reputation.

Recognising the growing need for strong user and transaction authentication, Thales has developed the SafeSign Personal Security Module, a hardware security token for end-users of online systems.

Personal Security Module

The Personal Security Module (PSM) is a hardware-based token which offers strong security to authenticate users and transactions in business applications. Whether it is for authenticating end-users or protecting transactions, the PSM offers the highest levels of security, ensuring the best protection for critical information.

Based on a Smart Card plus unconnected Reader, the Personal Security Module provides maximum flexibility to implement

security for business applications whilst having little or no impact on the applications themselves.

Strong Two-Factor Authentication

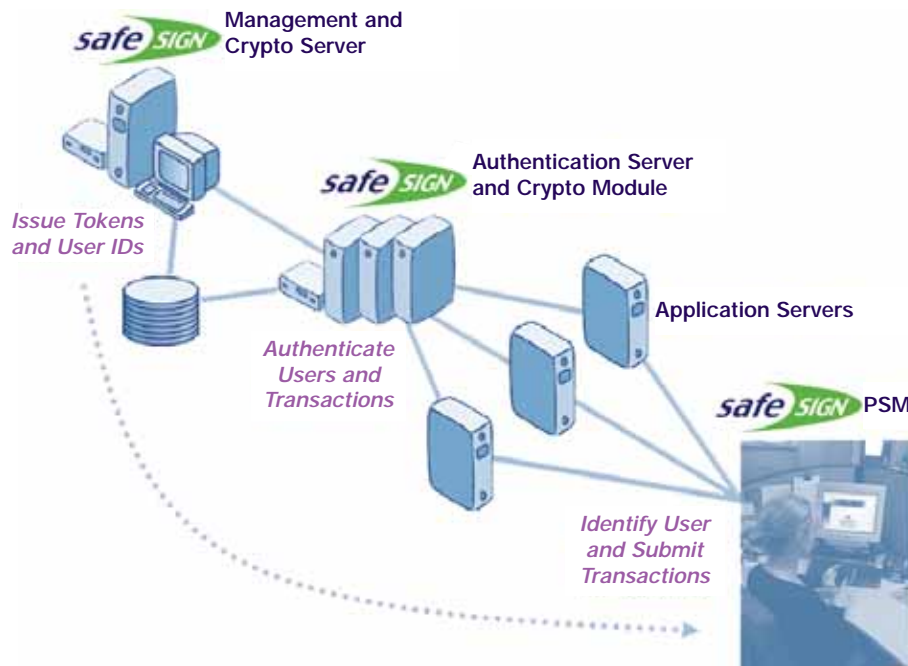
The Personal Security Module is based on two-factor authentication, widely accepted as the way to provide strong protection of users and transactions in online systems.

For users to identify themselves, they must firstly possess a PSM (card and reader) and secondly know the Personal Identification Number (PIN) of the card. Only the combination of these two factors allows for the generation of a unique "response" to a host-supplied "challenge". This "response" is sometimes referred to as a dynamic password. Capturing any Challenge/Response pair is worthless to an attacker since they will both be different next time.

In the PSM the Response is calculated using strong cryptography based on a key which is loaded onto the card when it is personalised. This key is shared only with the host system enabling it to validate the user on demand.

The PSM can also be used to protect transactions. It does this by allowing the user to enter a series of transaction data fields in response to customised prompts. When all fields have been entered, the PSM calculates a Message Authentication Code (MAC) using a cryptographic process. Again the users need to enter their PIN before the PSM will produce the MAC. The MAC (and hence the integrity of the message) can be validated by a host system which has access to the same cryptographic key used by the PSM.





Customisable Flexible Platform

Because security requirements are different from one application to another, the PSM needs to be very flexible in the functionality it offers. Initially, two different smart card based applications are available; one for user access control (challenge/response), and one for message authentication. These two applications can be configured to specific system requirements by allowing:

- Multi language support through customisable prompts
- Variable PIN length and PIN checking for maximum protection
- Customisable fields and field entries for user-defined transaction integrity

Requirements may also change during the life of a system (it may for example be necessary to support new security applications or authentication methods). The PSM is based on a platform which supports multiple applications on the same card allowing new applications to be added in the future.

Easy Integration and Management with SafeSign

As part of the SafeSign family of security products aimed at the Middle Office, the Personal Security Module integrates seamlessly with the other products of the family to deliver a true end-to-end authentication solution:

- SafeSign Authentication Server to facilitate the integration of the PSM security and authentication into business applications
- SafeSign Management Server to issue PSMs and manage users in real-time
- SafeSign Crypto Module to guarantee that all security critical and key management operations are protected by a high-grade tamper-resistant hardware platform.

Compatible with WatchWord® Systems

The PSM has been designed to be compatible with most of the features of Thales' previous generation of user and message authentication tokens known as WatchWord. The same WatchWord Challenge/Response and MAC algorithms are implemented in the PSM. The flexible approach to supporting any mix of Challenge/Response and MAC services with prompts tailored to suit the application are all carried forward from WatchWord to the PSM.

The inevitable differences between the PSM and WatchWord tokens are as a result of taking advantage of the smart card technology employed in the PSM. Whilst the end-user experience remains essentially the same, the issuing methodology is different. Users of existing WatchWord systems will need to upgrade their issuing capability to allow the PSM to be deployed. Thales can provide assistance to help ensure a smooth transition.



Technical Specifications

Card	Based on Global Platform multi-application card
PIN	Selectable up to 8 digits, verified by the card
PIN Management	Card locks after issuer-selectable number of attempts Remote card unlock capability
Services	Each smart card can be configured to provide a mix of security services as required. Maximum number of services only limited by available space on smart card
Algorithm support	DES and Triple DES
Printing	Cards available with plain white face or printed in a predefined scheme with space for user name Also special printing to customer requirements
PSM Handheld reader	2 line dot matrix (full alphanumeric) display 16 characters per line 16 key keypad plus on/off key User changeable batteries Standard colour – blue. Other colours available to special order Contains no personalized information User selectable reader language options for prompts such as “Insert Card”: English, French, German, Portuguese
Data Entry	Numeric, alphabetic and symbol entry
Battery life	One year under normal usage conditions
Environmental	Operating temperature: 5°C to 40°C Storage temperature: -10°C to 50°C Humidity: Up to 95% RH at 40°C
Dimensions/Weight	Card: Standard ISO card dimensions Reader: 73mm wide, 108mm high, 13mm deep Reader Weight: 75g

THALES

EUROPE, MIDDLE EAST, AFRICA

THALES e-SECURITY LTD.
Meadow View House
Crendon Industrial Estate
Long Crendon, Aylesbury
Buckinghamshire HP18 9EQ, UK
Tel: +44 (0)1844 201800
Fax: +44 (0)1844 208550
e-mail: emea.sales@thales-eseurity.com

AMERICAS

THALES e-SECURITY, INC.
2200 N. Commerce Parkway
Suite 200
Weston, Florida 33326, USA
Tel: +1 888 744 4976
or: +1 954 888 6200
Fax: +1 954 888 6211
e-mail: sales@thalessec.com

ASIA PACIFIC

THALES e-SECURITY (ASIA) LTD.
Asia Pacific
Units 2205-06, 22/F Vicwood Plaza
199 Des Voeux Road
Central, Hong Kong, PRC
Tel: +852 2815 8633
Fax: +852 2815 8141
e-mail: asia.sales@thales-eseurity.com

The Thales policy is one of continuous development and consequently the equipment may vary in detail from the description and specification in this publication. Safesign® and WatchWord™ are registered trademarks of Thales e-Security Ltd. Publication Number: 1536PS0A/0904/10990 ©2004



Certificate no. EVAS 73828

Certificate no. P958836