THALES

SafeSign

Authentication Server

SafeSign provides a single unified platform that supports all users across all applications and access channels according to the authentication requirements of the business.

It allows central management of authentication devices in a distributed business environment minimising administration and operating costs.

Advanced Authentication

- Consolidate all authentication requirements across the entire business.
- Enhance the security of all online applications implementing the correct level of security consistent with the level of risk to each application.

Multiple Authentication Methods

- Support multiple authentication methods across multiple applications and channels from a single authentication platform.
- Support the following authentication methods:
  - Encrypted Passwords
  - Handheld Tokens - including support for SafeSign Personal Security Module
  - EMV Authentication
  - Smart Cards
  - PKI cards, soft certificates or USB tokens
  - Generic Triple DES based tokens
  - Others available on request
- Flexible architecture allows for customisation to support any authentication method.

Symmetric Token Authentication

- Support Challenge and Response, OTP and MAC verification using a range of tokens in the market, including Thales SafeSign Personal Security Module.
- Support user and transaction authentication using EMV Smart Cards. Supports all standards for EMV Authentication (MasterCard, Visa, APACS and others).

>> SAFESIGN AUTHENTICATION SERVER

Strong Authentication

Allows organisations to implement strong 2-factor authentication solutions for all their applications, ensuring online services can be accessed securely.

Token Independence

Offers a choice of authentication methods from a wide range of technologies and vendors making migration from existing legacy systems quick and easy.

Multi-application

Provides security architecture that can support all users, across all applications and for a full range of authentication methods. This ensures existing and future security requirements can be met without the need to purchase new systems.

Scalable Architecture

Flexible, scalable architecture allows organisations to expand their existing security platform, without the need to invest in other authentication or management solutions.

High Performance / Availability

Resilient, load sharing server architecture ensures the highest degree of availability and performance across the entire business.

High Security

Add multiple layers of security to existing authentication operations and transaction processing with minimum integration effort.

Interoperability

Utilises the latest web-based technology making it easy to interface to internal applications and third party solutions.

PKI, Digital Signatures & Certificates

- Full cryptographic check of digital signatures and verification of messages and certificates.
- Define a trust hierarchy based on public-key certificates and digital signature services provided to end-user applications.
- Support PKI standards and all leading Certification Authority providers in the market.

Tamper Evident Audit Trails

- Maintain a legally enforceable tamper-evident audit report identifying each stage of the transaction process and users involved in each task.
- Track transaction history to ensure the transaction has occurred, who made that transaction and whether the data has been subsequently altered

Simple Application Programming Interface (API)

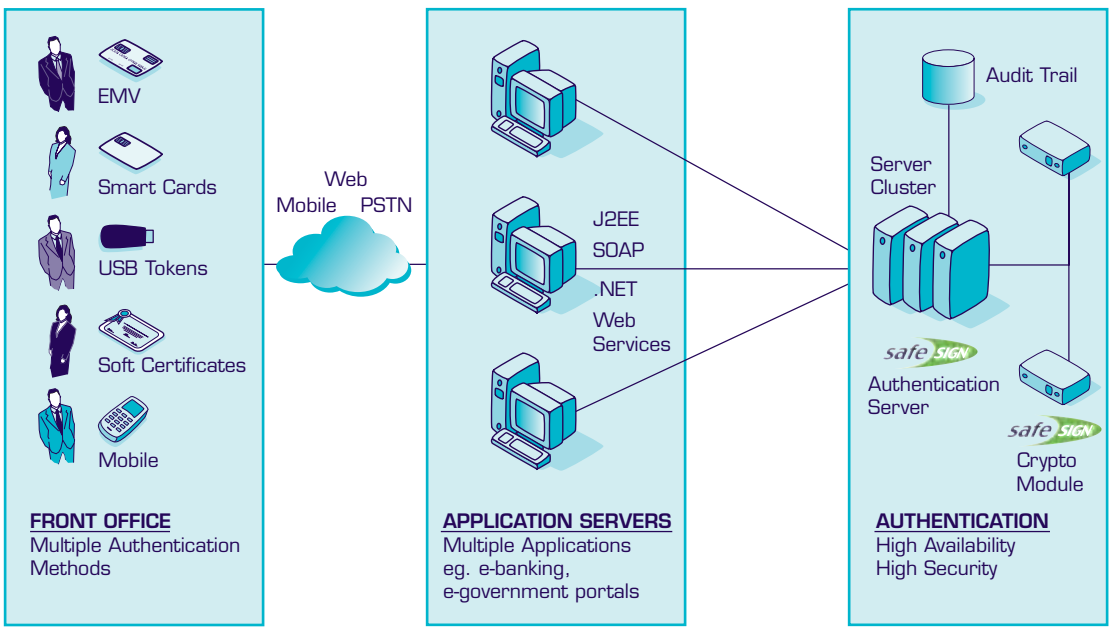
- Full suite of APIs to offer maximum flexibility and choice for application integration:
  - J2EE and Enterprise JavaBeans
  - Microsoft .NET
  - Simple Object Access Protocol (SOAP) for Web Services with support for WebServices Security (WS-S)
  - Built-in load sharing and high availability
- Optimised performance across a pool of Authentication Servers for applications requiring high transaction rates.
- Automatic recovery when a server is restored.

Key Management

- Perform the cryptographic operations necessary for delivering a range of authentication services.
- Securely manage and store keys via the SafeSign Crypto Module (or third party HSM) ensuring the best key management practices are applied.

Administration and Configuration

- Quick and easy system configuration using a graphical management console.
- Add, delete, start and stop servers.
- Create and manage all supported authentication services e.g. EMV device with OTP and Challenge and Response services.
- Process the certificate response.
- Configure multiple servers in a cluster from a single management console.
- Perform key management operations using secure hardware devices.



SafeSign Family

The SafeSign family of products offers a comprehensive end-to-end security solution. It provides high security issuance, management and advanced authentication of a diverse set of identity credentials in a single solution. All of the SafeSign products integrate seamlessly with each other. Alternatively they can be integrated with other third party products.

SafeSign Authentication Server is the authentication component in the Thales SafeSign product suite providing advanced authentication of users, messages and transactions.

SafeSign Management Server is an identity management solution for managing users and their digital credentials and issuing authentication devices.

SafeSign Personal Security Module is a hardware-based token which offers strong security to authenticate users and transactions in business applications.

SafeSign Crypto Module is the hardware security module delivering optimised cryptographic functions specific to the needs of both the SafeSign Authentication and Management Servers.

For more information on the SafeSign products visit:

www.thalesgroup.com/esecurity

Technical Specifications

Supported Platforms	Microsoft Windows NT 4.0 Microsoft Windows 2000, Service Pack 3 Microsoft Windows 2003 Pentium IV 1GHz or higher Microsoft Windows XP, Service Pack 1 Sun Solaris 7 and later I386 Linux platforms with kernel 2.5.18-27 or later (tested with RedHat Linux 8.0) IBM AIX 4.3.3, 5.1 or later, Power 3-II 400MHz or higher HP-UX 11 64-bit for PA-RISC architectures
Supported Standards	JDBC J2EE LDAP OCSP and CRLv2 certification validation PKIX PKCS#1 PKCS#7 PKCS#10 PKCS#11 Identrus X.509 3-DES RSA SHA-1 XML DSig digital signatures EMV CAP June 2003 EMV CAP Sept 2004 Visa & MasterCard Methods
Supported Interfaces	Java through RMI, JNDI or Java Bean interface Web Services through XML or SOAP with support for Web Services Security (WS-S) Microsoft.Net interface Other protocols like XML D-Sig or SAML for authentication
Java Environment	JDK 1.4.2 '06' or later Support for Java Management Extension (JMX) JSR-160 Compliant
Supported Hardware Security Modules (HSMs)	Thales SafeSign Crypto Module Supports other third party HSMs – more information available on request

EUROPE, MIDDLE EAST, AFRICA
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-esecurity.com

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

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-security.com

Publication No: 1647-PS-1/0705/11189

THALES