www.ds3global.com

Mastercard Certified
MasterCard Worldwide

SafeNet
The Foundation of Information Security

DS3 AUTHENTICATION TOOLKIT (ATK) FOR EMV CAP

DS3 (Data Security Systems Solutions) is a leading data security provider and integrator with more than 20 years experience in Information Security. DS3 expertise ranges from building world-class security products and components, to enterprise security consulting, to deploying solutions for the Banking, Government and Enterprise environments.

The DS3 Authentication toolkit (ATK) is a suite of modular components to enable strong authentication using industry-standard algorithms and protocols. The collection includes:

- DS3 ATK for EMV CAP – Certified Mastercard CAP/AA4C and VISA DPA
- DS3 ATK for OATH OTP – Supporting HOTP (RFC 4226) and TOTP for hardware tokens, software tokens on J2ME, iPhone, iMode, Java Applet and Windows.
- DS3 ATK for SMS OTP – Supporting Out-of-band SMS OTP for user authentication as well as transaction authorization using AES with ANSI x9.9 to defeat Man-in-the-middle attacks.
- DS3 ATK for RADIUS – Providing RADIUS RFC 2138 Client and Server capability for Windows, Linux and UNIX platforms.
- DS3 ATK for PKI – Providing X.509 Certificate and CRL issuance for RSA keys, and software PKI clients on J2ME and Java Applets.
- DS3 ATK for E2E Encryption - Supporting confidentiality and end-to-end integrity with FIPS-certified HSM for the transmission of sensitive passwords and transactions from the browser (using Javascript or Java Applets) to beyond the back-end processor.

The DS3 ATK suite is already being used by world-leading financial institutions and enterprises to secure their applications ranging from Internet and Mobile Banking platforms to B-to-B transaction portals to enterprise remote-access VPNs.

About DS3 ATK for EMV CAP

The DS3 ATK for EMV CAP is a collection of libraries and Firmware Module for the SafeNet ProtectServer HSM that enables the user to build an EMV CAP Token Generation Server (CTGS) to generate CAP tokens for SMS transmission as well as CAP Token Validation server (CTVS) to verify Mastercard CAP/AA4C and VISA DPA one-time password tokens used for user authentication or transaction verification.

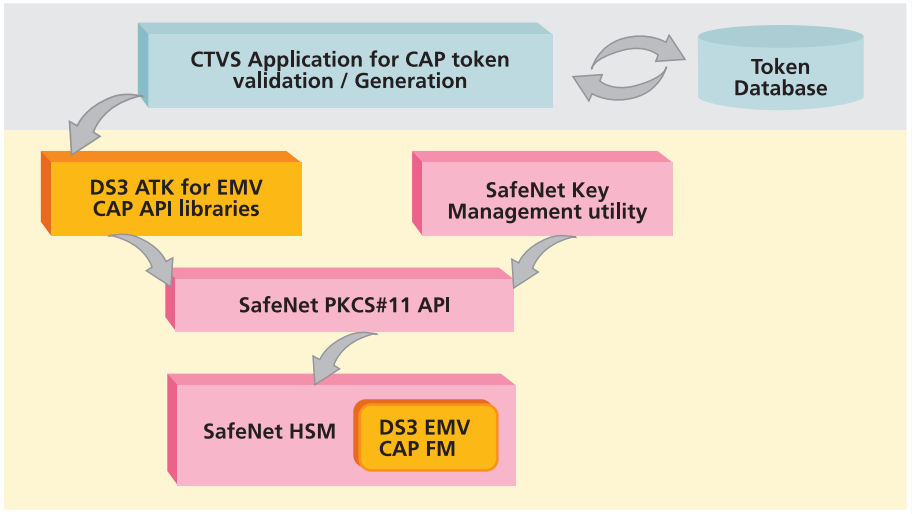
Features

- **Simple-to-Use API**
  All the complex functionality of the EMV CAP authentication is abstracted to only 4 main functions: i) CreateToken, ii) GetNextOTP, ii) AuthenticateToken and iii) ResetToken. This allows the provider to quickly build a CAP Token Validation Service (CTVS) that can be easily integrated into existing applications.
- **Scalable Standalone or Network-based architecture**
  By using the toolkit with the SafeNet PSG HSM and SafeNet PSE HSM, the toolkit allows the user to implement the CTVS as a standalone authentication module or a network-based shared authentication service. Higher performance can be achieved through additional HSMs in a Linear fashion.
- **Tamper-protected Secure Key Operations**
  The sensitive key and cryptographic operations are implemented as a Firmware Module (FM) within the FIPS-certified SafeNet PSG / PSE HSM. This ensures that the master keys and session keys used during verification are protected from compromise.

Technical Overview

The DS3 ATK for EMV CAP is delivered as a software + hardware package consisting:

- Windows & Java API for generating and authenticating CAP tokens
- DS3 EMV CAP FM (Firmware Module) for SafeNet PSG/PSE HSM
- Sample Windows and Java source programs + documentation to use the API
- SafeNet PSG/PSE HSM



The DS3 ATK for EMV CAP libraries use the standards-based PKCS#11 interface to communicate with the DS3 EMV CAP FM. To ensure secure end-to-end validation, all sensitive cryptographic operations including card key computation and CAP token validation are carried out securely in the DS3 EMV CAP FM embedded within the tamper-proof housing of the SafeNet HSM.

About SafeNet ProtectServer HSM

www.safenet-inc.com

ProtectServer Gold is a tamper-protected PCI Hardware Security Module (HSM) that provides high-performance, secure cryptographic processing in server systems, and supports applications requiring high-performance symmetric and asymmetric cryptographic operations.

Wide Range of Cryptographic Processing

ProtectServer Gold HSM incorporates 64 bit PCI interface, 4Mb secure storage capacity and a dedicated cryptographic processor to deliver high-speed cryptographic processing for cryptographic operations and fast transaction speeds. It provides a wide range of cryptographic services including encryption, user and data authentication, message integrity, secure key storage and key management for e-Commerce, PKI, document management, Electronic Bill Presentation and Payment (EBPP), database encryption, financial EFT transactions, plus many others.

Strong Security

The ultimate level of protection is afforded to sensitive cryptographic processing that often operates within the less secure environment of servers. The FIPS 140-2 level 3 validated, tamper-protected security safeguards against physical attacks on the HSM to obtain sensitive information. Upon detection of a physical attack, the complete internal key storage memory is erased. Further, cryptographic keys are never exposed outside the HSM in clear form.

Regulatory Standards Certification

- FCC Part 15 - Class B
- RoHS Compliant
- BAC and EAC ePassport Certification
- ISO– 9002 Certification
- FIPS 140-2 Level 3 Certificate 739
- FCC Part 15 Class B Unintentional Radiators ANSI C63.4-2003
- EN 55022:1998 Amendment 1:2000, Amendment 2:2003
- EN 55024:1998 Amendment 1:2001

SafeNet ProtectServer External is a network-attached HSM that connects via TCP/IP to a single machine or complete network (LAN) to perform as a central cryptographic subsystem for delivery of symmetric and asymmetric cryptographic services. All operations that would otherwise be performed on the insecure servers are securely processed within the HSM ensuring sensitive keys are always protected from compromise.

Specifications

Card Supported:
- Mastercard
  - M/Chip Lite 2.1
  - M/Chip 4 EMV 2000
  - M/Chip 4 EPI/MCI
  - M/Chip 4 EMV CSK
- VISA
  - EMV 2000
  - VIS 1.4

Standards Compliance
- Mastercard CAP 2007
- Mastercard PLA 2008
- Mastercard CTGS 2009 for SMS
- VISA DPA
- FIPS-140-2 Level 3 certification for SafeNet PSG HSM

Platforms Supported
DLL on Windows XP, 2003
Java API on
- Windows XP, 2003
- Linux
- Solaris 9, 10
- AIX 5.3
- HP-UX11i

Application Servers Supported
Microsoft IIS
Oracle WebLogic
IBM WebSphere
Sun Java Enterprise Server
Apache PHP / Tomcat

EMV Readers Supported
ACS APG 82 PinHandy
Xiring Xi-Sign
Gemalto Ezio Reader
VASCO Digipass 810