



u/SWITCHWARE® Enterprise Transaction Processing and Management System

EMV and Smart Card Support

OVERVIEW

Support of Integrated Circuit Cards (ICC), commonly referred to as smart cards, and the Europay, MasterCard, Visa (EMV)



standards that govern their use is continuing its rapid deployment around the world to supplement and eventually replace the magnetic stripe card.

EMVCo (www.emvco.com) was formed in 1999 to manage, maintain and enhance the EMV Integrated Circuit Card Specifications for payment systems. EMV stan-

dards play an important role in ensuring that cards, terminals and systems successfully interact wherever they are in the world.

The introduction of this emerging technology addresses many key business considerations:

- Maintain the integrity of payment transactions by combating widespread fraud. This is accomplished through more secure card creation and authentication measures.
- Shift liability for fraudulent activities from card associations such as Visa and MasterCard to any link in the authorization chain that is not EMV compliant.
- Off-line verification of the card and the user's PIN and ability to support e-Purse functions.
- Risk management through the ability to interact with the smart card and deactivate certain functions.
- Support of smart card applications.

BASE RELEASE SOFTWARE

u/SWITCHWARE® 3.11 and all subsequent releases of the base software are EMV-ready, containing the additional data elements necessary to support the latest EMV mandates. These data elements include new tables used in configuring the interfaces to support EMV. A new EMV data transaction log stores all of the EMV data received from an acquirer and issuer. RSA security for authenticating the cardholder and common EMV functions used by all EMV-enabled interfaces are included in the base release. An EMV base system license is required to activate the EMV functions.

ACQUIRER SUPPORT

EMV transaction acquiring is performed at u/SWITCHWARE-driven EMV compliant devices that are sufficiently equipped to accept smart cards. EMV equipped acquisition devices include ATM and POS devices.

ATM

EMV-enabled ATM handlers support the acquisition of a smart card at an ATM terminal equipped with a smart card reader and Encrypting PIN Pad (EPP) that supports 3DES and MACing (Message Authentication Code). Available ATM handlers include:

- NCR NDC format
- Diebold 91x format
- Wincor-Nixdorf (Using NDC and 91x formats)

POS

EMV-enabled POS handlers support the acquisition of a smart card at a POS device equipped with a smart card reader and EMV compliant terminal program. Available POS terminal handlers include:

- CSFi ISO 8583 format
- Verifone Printec v1.3 (ISO 8583 message)

ISSUER SUPPORT

EMV issuer support consists of Cardholder Authentication Method (CAM) verification, the means by which a plastic card is determined genuine and not counterfeit, verifying the Authorization Request Cryptogram (ARQC), and responding with Issuer Authentication Data.

HSM Interface

Card authentication is performed through special commands sent to a Host Security Module (HSM). The HSM supports RSA Key Management, verification of the ARQC (Authorization Request Cryptogram) and generation of an ARPC (Authorization Response Cryptogram).

Available EMV-enabled HSM interfaces include:

- Thales RG7000 Series
- Thales 8000 Series

SMART CARD ISSUANCE SOLUTIONS

In addition to authorizing transactions as a smart card issuer, your organization may wish to issue smart cards with pre-loaded applications. In order to accomplish this, several components are required to support an “end-to-end” smart card issuance environment.

Pingen

The Pingen system’s main purpose is to provide PIN mailer generation and card encoding/embossing functions. To support EMV smart card issuance, Pingen is responsible for accessing u/SWITCHWARE’s cardholder data tables for magnetic stripe, embossing and EMV data. Pingen then generates a PIN and outputs a file containing track1, track2 embossing and EMV data.

Pingen P3 Interface Module

The Pingen P3 interface module is used to prepare the EMV data file for importation into the Thales P3™ card personalization process system. The import file generated for P3 will consist of the embossing/encoding details, the PIN encrypted in ZPK defined between Pingen and the card personalization system and the EMV related tags setup for the cardholder in the u/SWITCHWARE database.

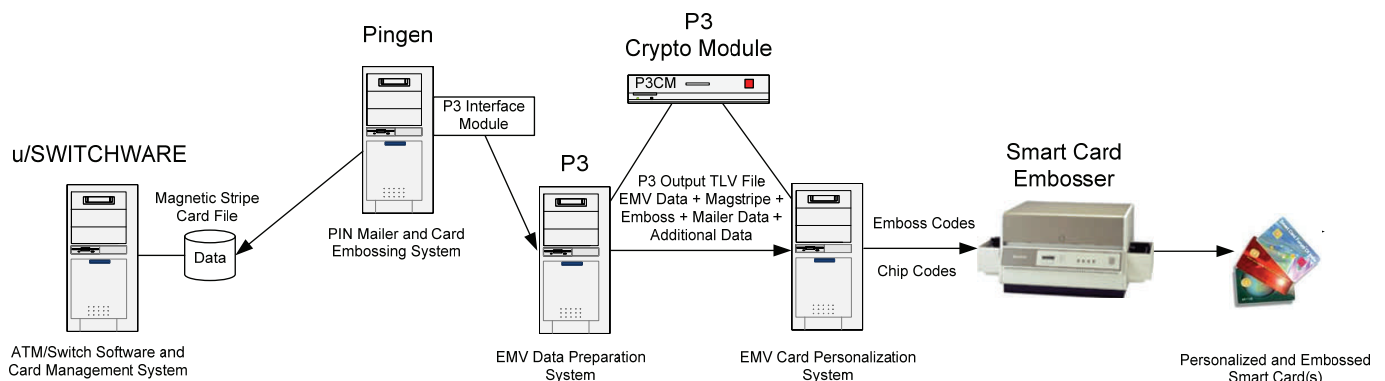
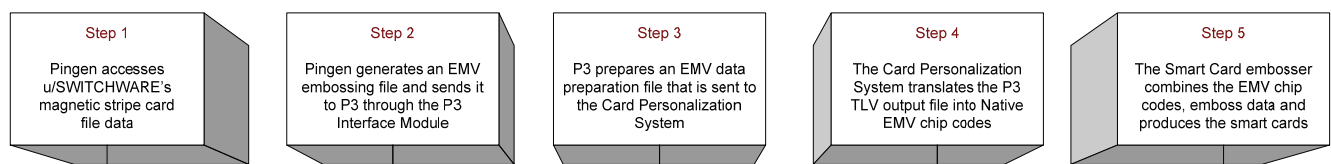
P3™

The Thales P3™ Personalization Preparation Process system provides the functionality to define, generate and store cryptographic data that will ultimately be loaded onto the smart card. There are multiple P3 software solutions available that are designed to meet the needs of your EMV smart card issuance volume and performance needs.

P3 Cryptographic Functions

A P3 Crypto Module (P3CM) is used to perform the EMV cryptographic functions required by the P3 Personalization Preparation Process System.

For Thales 8000 series HSM users, there is a new software license available that expands the HSM Model 8000’s command set so it can perform the same EMV data preparation functions as performed by the P3CM crypto module.



End-to-End Smart Card Issuance Solutions

Card association applications supported:

- MasterCard M/Chip
- Visa VSDC
- JCB J/Smart

Formats supported:

- Global Platform
- VSDC
- Java
- MULTOS

EMV Card Personalization Systems

Many popular EMV card personalization systems can work seamlessly with the Thales P3 system to translate the P3's TLV output file into native EMV chip codes. These systems are responsible for performing data preparation, card personalization and an interface to smart card issuance devices.

Issuer Components

- HSM Interface with CAM support (included in USWX-EMV)
- CCM Client (included in USWX-EMV)

ATM Handlers (Acquirer)

- NCR NDC
- Diebold 91X
- Wincor-Nixdorf NDC and 91X

The 'Advanced' version and a ConfigBuilder EMV license is required to support EMV functions for each of these ATM handlers.

POS Handlers (Acquirer)

- CSFi ISO 8583 format
- Printec Verifone (ISO 8583 message)

Network Interfaces

- Benefit (Bahrain)
- Europay
- JCC (Cyprus)
- K-Net (Kuwait)
- MasterCard
- NAPS (Qatar)
- SPAN2 (Saudi Arabia)
- Visa

External Interfaces (Third Party Applications)

- Card Tech Limited

EMV Card Personalization Systems (Supported by Thales P3)

- DataCard® Affina®
- Verisoft PowerEMV

CSF International, Inc. (CSFi) is a global provider of enterprise transaction processing and management software providing transaction processing services to hundreds of companies in over twenty countries. Clients range from de novo community banks to multi-bank holding companies and processing centers.

CSF International ... What The World Is *Switching To*

CSF International, Inc.
1629 Barber Road
Sarasota, Florida 34240-9392
Tel. +01.941.379.0881
Fax. +01.941.371.5223
sales@csfi.com
www.csfi.com



© 2007 CSF International, Inc. All rights reserved. Version 3.1

NETWORK INTERFACES

Regional, national or international networks, with direct authorization connections to your financial institution, may support the transmittal of EMV transactions. EMV-enabled network interfaces are available that allow a financial institution to process EMV transactions as an acquirer, issuer or both.

EXTERNAL INTERFACES

Some EFT environments may require transactions containing EMV data elements to be passed between u/SWITCHWARE and other applications. In these instances, u/SWITCHWARE may be responsible for sending acquired EMV transactions to an application, receiving issuer EMV transactions from an application or a bi-directional interface supporting both acquirer and issuer transactions. An EMV license is required depending on whether acquirer, issuer or acquirer/issuer functions need to be supported.

EMV SUPPORT

Base System

- u/SWITCHWARE Base Release 3.11 (USWX-311) or greater (EMV ready release)
- EMV License (USWX-EMV) - includes scripts to update 3.11 database for EMV