

Complex EMV card issuance solution

Complex EMV card issuance solution implements the full process of EMV cards issuance, from data generation and PIN printing to cards personalization and quality assurance.

Cards

The solution personalizes any EMV cards which comply with ISO 7816 (both native and GlobalPlatform). The solution successfully personalizes Axalto, Austria Card, Gemplus, Giesecke & Devrient, Oberthur, Setec cards and cards of other vendors in the leading banks and processing centers of Russia and CIS.

Over 2/3 of all EMV cards in Russia were issued using the complex solution.

Equipment

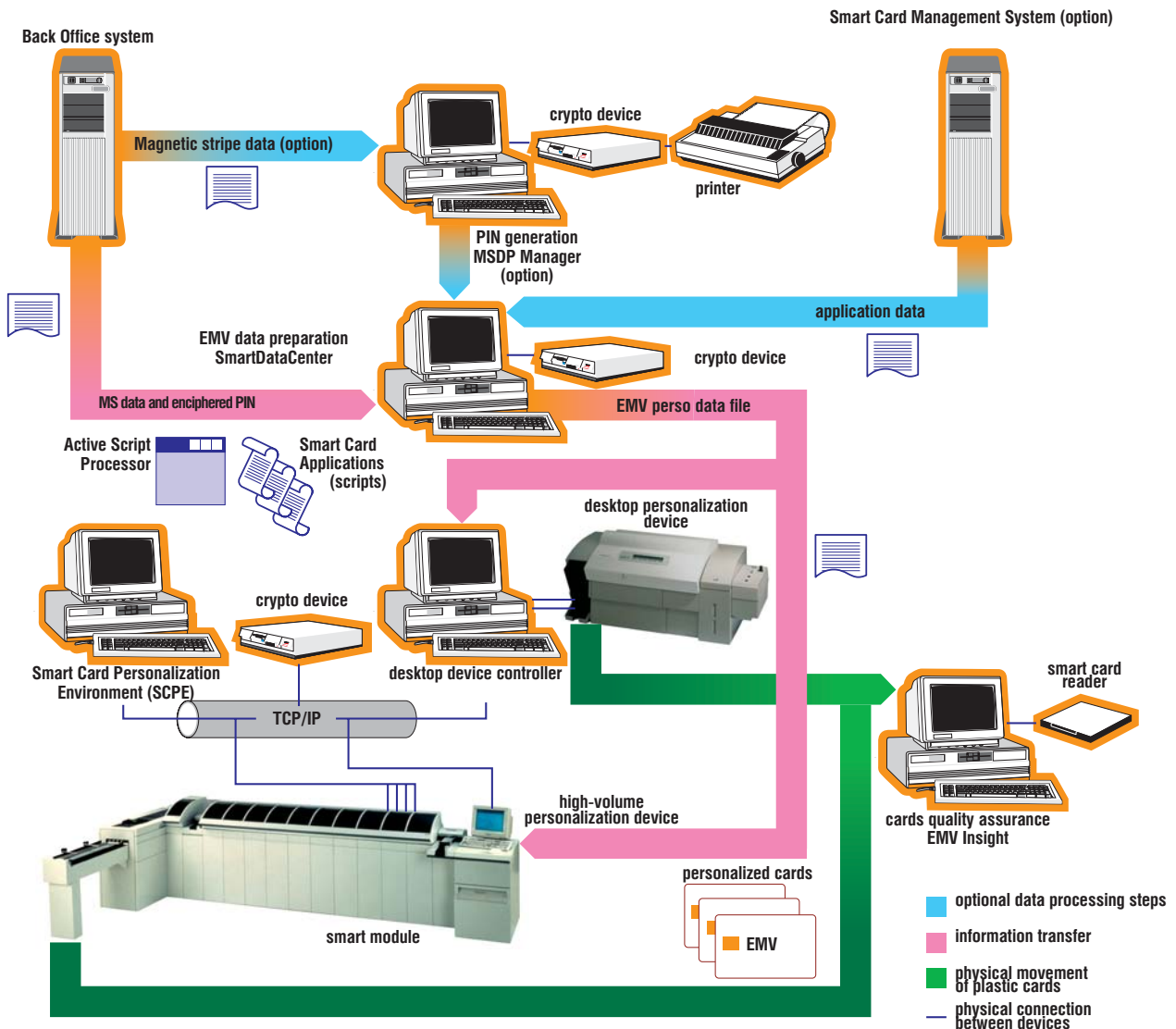
A wide range of equipment can be used to personalize cards:

- high-volume devices DC 9000/7000/500;
- desktop embossers DC 450/280P/150i;
- printers SP75/SP55/SP35 and other equipment.

The solution shares a common crypto subsystem and supports a wide range of SafeNet (Eracom) and Thales e-Security cryptographic equipment and SAM cards.

Solution components

- **Magnetic Stripe Data and PIN Manager** - magnetic stripe data and PIN generation and printing;
- **SmartDataCenter** - data preparation for EMV and additional applications;
- **Smart Card Personalization Environment** – a software framework for personalizing any ISO card in virtually any technological environment;
- Smart card personalization applications for personalizing a certain type of cards;
- **EMV Insight** – EMV card quality assurance tool.



Features

The solution is cost effective, flexible and functional:

- Solution is designed to minimize time and costs of cards certification in payment systems;
- A set of cards personalized may be flexibly increased;
- A set of applications personalized on a card may be easily managed with little cost;
- Post-issuance is supported (loading, activation and personalization of additional applications after initial personalization);
- Solution is scalable: introduction of new types and units of personalization equipment does not affect software components and thus does not produce costs;
- Transparent integration with various Back Office systems. The solution enables working with files of open formats, interact with most DBMS, personalization data may be received from several independent sources.

Solution description and sequence of operations

1. If Back Office system does not support the full range of operation with magnetic stripe data and PIN (for instance, does not allow calculating enciphered PIN), MSDP Manager may be applied.

2. Card data go into SmartDataCenter EMV data preparation system, which has the following features:

- interaction with Back Office system;
- flexible distribution of data processing functions between Back Office and data preparation system;
- ability to handle several data sources to generate a personalization file;
- supplement of constant and calculated values to input data;
- data grouping in DGIs;
- multi issuer support (ability to generate card data for several issuers);
- generation of secret values in accordance with EMV 4.1, VSDC, M/Chip requirements;
- support of several output data formats:
 - Visa Common Personalization v 1.5;
 - EMV Common Personalization v 1.0;
 - XML.

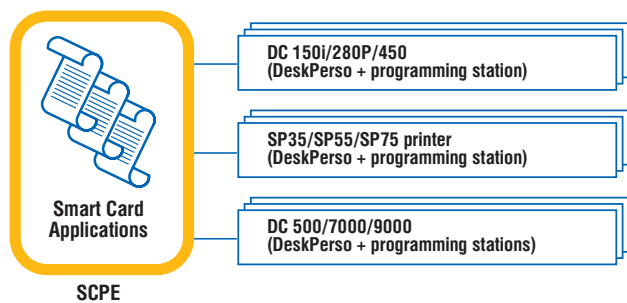
3. The core part of the solution is **Smart Card Personalization Environment (SCPE)**. Specific algorithms of personalizing a certain set of applications on a certain type of cards are implemented within the framework of **SCPE** in smart card applications (as shown in the figure). **SCPE** makes personalization units' type and number invariant.

Smart card application is a set of scripts implemented using standard programming languages (VBScript, JavaScript, ActivePerl). To add a new application to the set of applications already being personalized or to support a new card type a new script has to be developed and added to the system. This does not imply high costs and may be executed by PRONIT specialists as well as third party developers.

4. Personalized EMV cards may be tested in **EMV Insight** quality assurance system. **EMV Insight** enables to keep track of all the accessible aspects of smart card personalization results and behavior: personalized data in SFI, process of EMV application selection, authentication procedures, processing restrictions, risk management and online authorization emulation.

EMV Insight enables to:

- analyze card data consistency, non-redundancy, authenticity and compliance with the requirements of international payment systems;
- control consistency of cryptographic keys loaded into the EMV application;
 - analyze and verify SDA/DDA/CDA;
 - verify offline PIN (plaintext and enciphered);
- verify the consistency of embossed data, magnetic stripe data and chip data;
- execute Issuer-to-Host scripts, which dynamically manage application: application data modification, application block/unblock, PIN change/unblock.



Smart card applications are personalization units' type and number invariant.