

bankWORKS, the flexible Card Management System developed by RS2 incorporates complete support for EMV Chip Card Issuing. It features the management of the full lifecycle of chip card issuing including total control at cardholder level of offline risk management and other chip specific tags. The Chip Card Issuing module provides a *smooth* migration from magnetic stripe cards to chip cards by supporting the issuing of both magnetic stripe and chip cards together, even under the same BIN.



RS2 adheres to the specifications developed by MasterCard and Visa (EMV) to ensure that all the Chip Cards personalised by **bankWORKS** are compliant with EMV compliant terminals worldwide.

All the latest chip applications currently provided by VISA and MasterCard, as shown below, are supported by **bankWORKS**.

VISA	MasterCard	EMV
VSDC v1.4.0	M/Chip Select 2.1, 4.0	CPA*
VSDC v1.3.2	M/Chip Lite 2.1, 4.0	

The use of Integrated Chip Card technology introduces four major business benefits to the payments industry:

- ✓ Fraud Reduction, both counterfeit as well as “lost, stolen, never received” fraud
- ✓ Reduced processing costs through secure offline transactions
- ✓ Improved Credit Risk Management
- ✓ Opportunity for Value Added Services

\* **bankWORKS**’ architecture is designed to also be able to support the *Common Payment Application (CPA)* designed by *EMVCo*, as well as any other future chip applications.

## bankWORKS Integration

**bankWORKS**’ EMV components are designed as extensions that *integrate seamlessly* within the current modules. In fact chip services are still set up in the same way as magnetic stripe ones but product setup has now been extended to be able to store chip application specific information for chip services.

**bankWORKS** approach to chip cards is very flexible and has been projected to be easily upgradeable to future EMV specification versions and future chip applications. The risk parameters, referred to as tags, are completely defined at *setup level* and appropriate graphical user interfaces then allow these tags to be grouped as required in order to set up the different chip applications that need to be supported.

## Risk management

*Multiple tariffs* can be associated to the same application at product level, hence allowing the possibility of having separate risk management for different cardholder groups who have the same chip application.

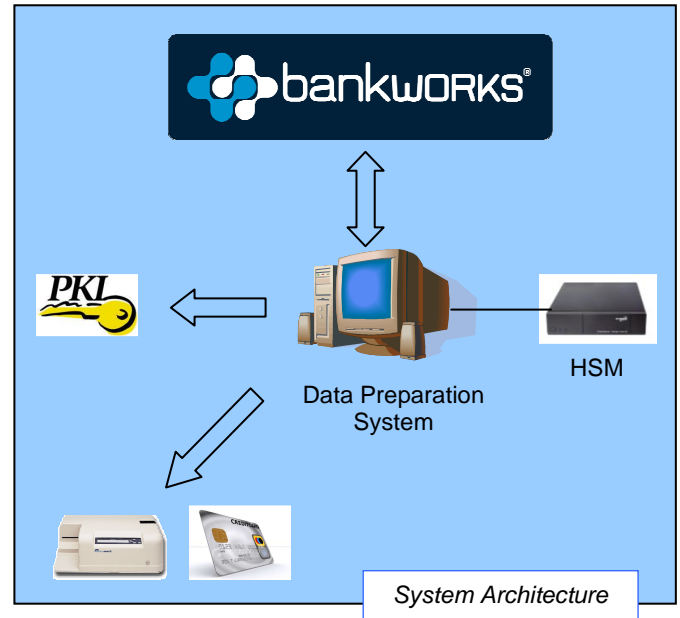
The complete integration of EMV into **bankWORKS** however also allows the user to have *cardholder level* personalisation. The application input module optionally allows the parametrisation of the risk management tags for a particular card only. Application processing then merges such specific cardholder settings to the default product setup to produce the set of risk parameters that will be personalised on the card.

Such a feature would not be possible with systems that just take magnetic stripe data and convert it into chip personalisation data.

## Post-Issuance Updates

One of the features introduced with chip cards is the possibility of updating cards that are already in circulation. This is called *scripting* and involves the sending of instructions, known as scripts, to a card during the time when the card has come online with a request for a transaction authorisation. The most common script types are scripts to block or unblock the application on a card, to unblock the card's PIN in case the cardholder has exceeded the maximum number of allowed PIN tries during cardholder verification, to change a card's PIN number and to change the value of any risk parameter that has been personalised on the card.

To this end a scripting engine has been integrated within the current **bankWORKS** modules to provide the issuer with the full post issuance update capabilities. Features such as queuing and prioritisation of scripts, script grouping as well as script status tracking ensure maximum efficiency and optimum handling of the possible multitude of scripts that can be sent for each card.



specifications (given the lack of standardisation) of smart card technology since these systems are dedicated to manage changes in personalisation interface specifications, smart card operating systems and card applications.

## Personalisation

The **bankWORKS** personalisation module generates secure PINs, PIN verification values (PVV / PIN offset) and the card verification values (CVV1, CVV2, iCVV). It also manages the various encryption keys securely, prints PIN mailers and creates the outgoing file for personalisation of the chip card. This file is then processed by a data preparation system such as P3™ from Thales e-Security or GemSense™ from Gemalto (other data prep systems supported), which systems in turn interface to an HSM (Hardware Security Module) to generate the required cryptographic keys that need to be loaded on the card.

This architecture allows for cardholder risk management parameters to be managed from within **bankWORKS** while the management of certificates and the generation of the required cryptographic keys are managed within the data preparation module. By having the risk management data managed from within **bankWORKS**, the issuer has the advantage of being able to manage all EMV data from one system apart from having the already cited advantage of cardholder level control. Moreover the data preparation system allows **bankWORKS** to quickly respond to changes in technical

## Online Authorisation Switch

The Issuer EMV update for the **bankWORKS** authorisation switch (CommServer) involves the introduction of new features, as follows, to complement the current authorisation duties.

### ✓ Online Card Authentication

Online Card Authentication entails the verification of an *ARQC* (*Authorisation Request Cryptogram*). This cryptogram is an encrypted string made up of card, terminal, and transaction data that the card formulates and sends to the issuer when it requires online authorisation. This information can only be validated by the issuer and as such, its aim is to serve as prove to the issuer that the request is indeed a genuine one coming from an authentic card.

### ✓ CVR / TVR Verification

The *CVR* (*Card Verification Results*) and *TVR* (*Terminal Verification Results*) data elements are two structures which contain a list of checks carried out during the offline authentication stage by the card, in case of the CVR, and by the terminal in case of the TVR. Examples of these checks include whether PIN verification has been performed or whether a transaction is domestic. These structures are sent to the issuer whenever

a transaction is sent online and the issuer can choose to verify these data elements before taking its decision whether to approve or decline the transaction. In this respect, **bankWORKS** provides a new graphical user interface by which the issuer is allowed to define his own online rule set, indicating on the presence of which of the criteria in these structures should a transaction be declined.

#### ✓ Online Issuer Authentication

Once the issuer decides that the transaction can be authorised, an *ARPC (Authorisation Response Cryptogram)* is generated by CommServer to be sent to the card. As well as signifying the authorisation response, the purpose of this cryptogram is to allow the card to authenticate its own issuer as the genuine sender of the response.

At the point of sending the ARPC, CommServer may also provide any command scripts to be delivered to the card via the terminal. These scripts allow the issuer to perform functions that may not necessarily be directly relevant to the current transaction but which might be required to deliver updates to the functionality of the chip card application.

## Instant Issuing

With its tight integration to the data preparation systems, **bankWORKS** is also able to support instant issuing of chip cards at branch level.

Instant or In-branch issuing allows customers to immediately leave in possession of the card that they have just entered the branch to apply for. Enrolment is done remotely at the branch by the customer service users who take the details directly from the customer in front of them. After validation of this data, the application is sent to be processed at the bank's card centre via an online network. Following application processing then, the necessary personalisation data is generated and passed on to a dedicated third party preparation module which loads the required chip application on the card and prints it.

For more details on Instant Issuing please refer to the *Chip Card Instant Issuing* brochure.



## EMV Chip Card Issuing

### *Life Cycle Management*

- ✓ Full EMV Tag Management
- ✓ Cardholder Specific Risk Management
- ✓ Graphical User Interfaces
- ✓ Version Control
- ✓ Scripting Engine

### *Card Personalisation*

- ✓ Chip Personalisation Data Generation

### *Security*

- ✓ Pin Generation
- ✓ CVV/CVC 1 and 2 Generation
- ✓ iCVV Generation

### *Authorisation and Online Switch*

- ✓ Online Card Authentication
- ✓ CVR / TVR Verification
- ✓ Online Issuer Authentication
- ✓ Script Handling Packages

RS2 Software plc  
120, The Strand  
Gzira GZR 1027  
Malta

RSConsult  
Martin-Behaim-Str. 12  
D-63263 Neu-Isenburg  
Germany

Tel: 00356 21345857  
Fax: 00356 21343001

Tel: 0049 6102 730030  
Fax: 0049 6102 730055

[www.rs2.com](http://www.rs2.com)