



www.mobilitypay.com

MAXxEMV Central Issuance Solution

Version 1.2



COPYRIGHT © 2016 Mobility Payment Solutions LLC

This publication is proprietary of Mobility Payment Solutions LLC and is intended solely for the contractual use of Mobility Pay internal employees.

This publication may not be reproduced or distributed for any other purpose without the written permission of Mobility Payment Solution LLC.

NOTICE

Mobility Payment Solutions LLC reserves the right to make changes to specifications at any time and without notice. The information furnished by Mobility Payment Solutions LLC, in this publication is believed to be accurate and reliable, however, Mobility Payment Solutions LLC, assumes no responsibility for its use, or for infringements of patents or other rights of third parties resulting from its use.

If this document is distributed outside of Mobility Payment Solutions LLC, all Non Disclosure Agreements must be activated between Mobility Payment Solutions LLC and the external Company. All materials within this document are proprietary and confidential and are not to be distributed without the knowledge of Mobility Payment Solutions LLC or appropriate management approval.

For inquiries about this product please contact:

Mobility Payment Solutions LLC

P. O. Box 238925,

Dubai, U.A.E.

+971 4 2288770,

For trade enquiries Email: corporate@mobilitypay.com

For technical support Email: maxxemvsupport@mobilitypay.com

www.mobilitypay.com



Revision History

Date	Description	Author	Comments
01.01.2015	1.0	M. Asad	
10.05.2016	1.2	Parthasaradhi Sathram	Modified content and component layer image

Document Approval

The following Software Requirements Specification has been accepted and approved by:

Signature	Printed Name	Title	Date



CONTENTS

- 1. INTRODUCTION.....5**
- 1.1 ABOUT MOBILITY PAYMENT SOLUTIONS LLC 5
- 1.2 MAXxEMV CENTRAL ISSUANCE SOLUTION (MAXxEMV CIS) 5
 - 1.2.1 Purpose 5
 - 1.2.2 Scope and Advantages..... 5
 - 1.2.3 Overview..... 6
 - 1.2.4 MAXxEMV CIS Architecture..... 7
 - MAXxEMV CIS Personalization Data Flow..... 7
 - Solution Component Layers..... 7
- 2. MAXxEMV CIS MODULES:8**
- 2.1 MAXxEMV CIS WEB GUI 8
 - 2.1.1 Issuer manager 9
 - Issuers..... 9
 - Create New Issuer 10
 - Update Issuer 10
 - Remove Issuer 11
 - Products..... 11
 - Create new product 11
 - Edit Product..... 12
 - Remove Product..... 12
 - create new copy of the product from the existing one 13
 - Chip tag templates..... 13
 - Chip personalization configuration..... 15
 - signed certificate 16
 - file processing..... 16
 - 2.1.2 Job manager 17
 - File Management..... 18
 - Prepare records and work order 19
 - Work Orders 19
 - MAXxEMV File Monitoring 20
 - Expired files 21
 - Deleted Files 21
 - 2.1.5 MAXxEMV CIS Management..... 22
 - Chip management 22
 - Add new chip..... 22
 - edit chip..... 23
 - Scheme Management..... 24
 - add new scheme 24
 - update scheme 24
 - remove scheme..... 24
 - Key Management..... 25
 - key types 26
 - Scheme Profiles 27
 - Configuration..... 27
 - DMZ Accounts..... 28
 - To add a DMZ account 28
- Users Management 28
 - User Group management..... 29
 - User Management..... 29
 - User Logs 30



- Status Monitor..... 30
 - product license 31
- Machines Manager..... 31
- 2.2 MAXxEMV CIS CLIENT..... 32
 - 2.2.1 Work Order files 33
 - 2.2.2 Load Work Order..... 34
 - 2.2.3 personalized workd oder files 35
- 2.3 MAXxEMV CIS ENGINE 36
 - 2.3.1 MAXxEMV CIS DATA PREPRATION..... 36
 - 2.3.2 MAXxEMV CIS KEY MANAGEMENT..... 37
 - 2.3.3 MAXxEMV CIS CARD Personalization..... 39
- 2.4 MAXxEMV CIS SECURE FILE TRANSFER ENGINE..... 40
- 3. SYSTEM REQUIRMENTS..... 41**
- 4. PRODUCT LICENSE..... 43**
- 5. DEPLOYMENT PLAN 44**





1. INTRODUCTION

1.1 About Mobility Payment Solutions LLC

Mobility Payment Solutions is a leading technology enabler, solution provider and expert operator in the payment space. Mobility provides innovative technologies, enable secure solutions and performs services behalf of banks, retailers and third party service providers.

Mobility specializes in managed secured services with an end to end solution implementation and delivery offering managed operations that supports heterogeneous environments. Our expertise lies in managed solutions via key technology partners/global players offering a single point of deliver and operate model for payment solutions that drive payment in the regional and global market today. We work closely as preferred partners with various players in the payment eco system contributing to bank-the-unbanked and to develop and manage multi-channels for payments for consumers globally.

Mobility is focused at innovating and developing solutions that enhance secure delivery of payments by providing various form factors, secure management and personalization of consumer data, secure accessibility to services via mobility apps, and delivering enhanced business intelligence around payment services

1.2 MAXxEMV Central Issuance Solution (MAXxEMV CIS)

1.2.1 PURPOSE

MAXxEMV CIS is state-of-the-art solution that is designed to support Personalisation Service Providers to manage a heterogeneous environment in terms of EMV Chip/OS, Payment Schemes, EMV Personalisation Machines and Workflow Operational requirements of issuers with a strong control on day-to-day EMV chip cards personalization and issuance process using built in customizable operational work flow.

1.2.2 SCOPE AND ADVANTAGES

MAXxEMV CIS has a strong modular architecture to support multi-brand issuance and ensure scalability for PSP (Persoanlization Service Providers). In addition to payment applications, EMV cards can be used for applications in a wide verity of fields such as:

- ATM and POS Systems
- National ID cards
- Ticketing
- Internet Banking
- Reward/Bonus/Loyalty programs
- Access Control System

Advantages



MAXxEMV CIS is a quick to implement, quick to learn and easy to operate solution that allows issuer/PSP to maximize security compliance, operational efficiency, reduce costs and deliver high quality issuance. It allows full control of the issuance technical setups, process mapping and day to day operations by logging all user activities for daily issuance. Some of the key benefits listed below:

- Simple and Easy Use
- Resource Access Control
- Issuance Controls
- Activity Logs
- Operational Process Flow
- Operational Controls
- Reduced Wastage/Errors
- Flexibility & Scalability
- Multi-chip, multi-machine brand, multi scheme support
- Quality Assurance
- Multi-Issuer management
- Scheme Compliance

1.2.3 OVERVIEW

MAXxEMV CIS is a comprehensive EMV chip cards personalization and workflow process optimization tool that is specialized for PSPs, Issuing Banks and Financial Institutions like enabling them to manage multiple card product issuance & workflow management. This multi-card support differentiates the solution by providing an in-depth issuer product management, workflow process management and reporting requirements. The solution offers the below key features with various key benefits and impressive ROI to the service providers and issuers:

- EMV Workflow Process Management
- Multi-Scheme Support
- EMV Personalisation Machine agnostic
- EMV OS/Chip agnostic
- EMV compliant Key Management
- Secure EMV Data Preparation
- EMV Quality Assurance and Validation
- Multi-application personalisation support
- Multi-sector (banking/retail/non-banking) support

1.2.4 MAXxEMV CIS ARCHITECTURE

- MAXxEMV CIS Personalization Data Flow
- Solution Component Layers

MAXxEMV CIS PERSONALIZATION DATA FLOW

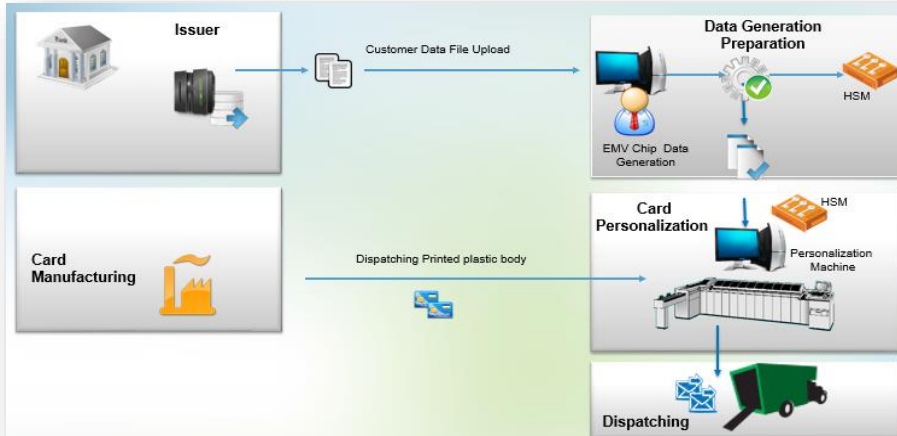


Figure 1: MAXxEMV CIS Personalization Data Flow

SOLUTION COMPONENT LAYERS

MAXxEMV Central Issuance System

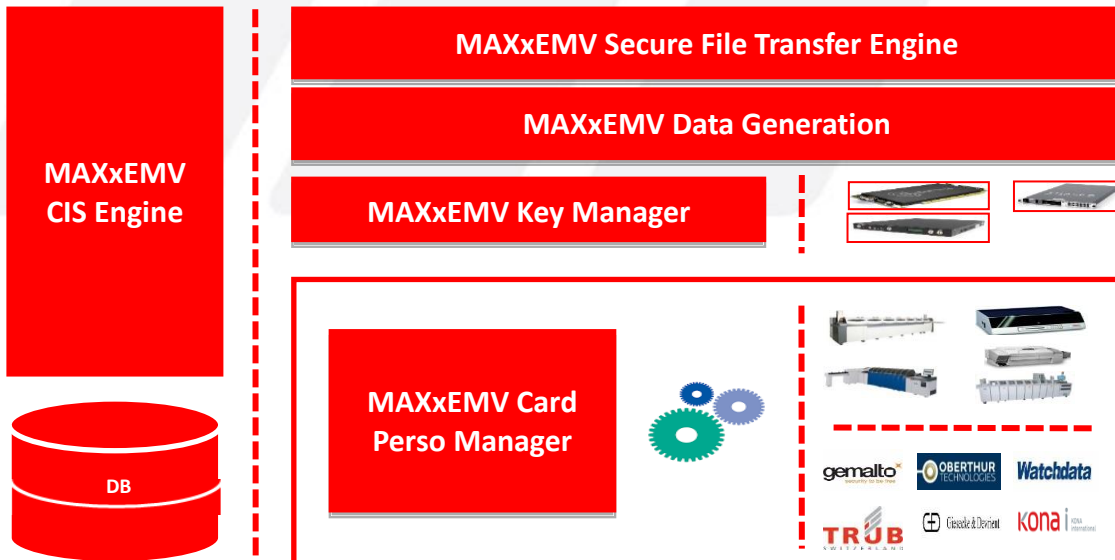


Figure 2: MAXxEMV CIS Architecture

2. MAXxEMV CIS MODULES:

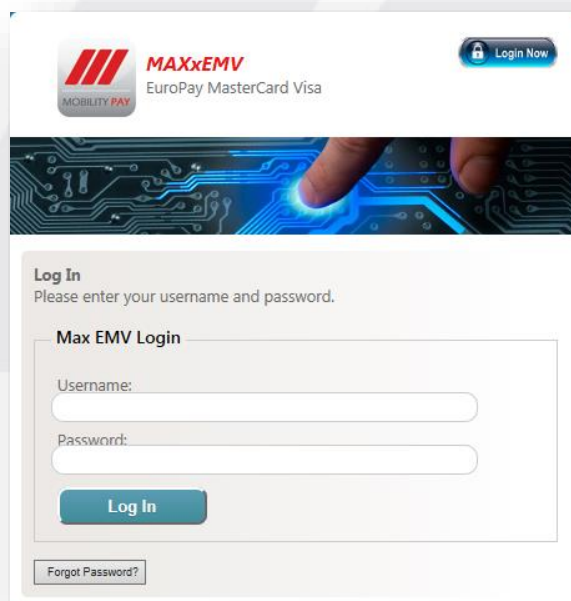
MAXxEMV CIS has a specialized modular architecture to support multi-brand issuance and ensure scalability for PSP. With various inline operational workflow requirements in today's fast pace issuance, the service providers are fully empowered to manage volume demand with MAXxEMV CIS platform providing robustness and accuracy when managing large volume issuance projects.

- MAXxEMV CIS Web GUI
- MAXxEMV CIS Engine
- MAXxEMV CIS Client App
- MAXxEMV CIS Secure File Transfer Engine

2.1 MAXxEMV CIS Web GUI

MAXxEMV CIS Web GUI enables the user to configure the issuer, products, template, data prepare and chi personalization configurations. Application activate & deactivate options based on the user associated group which is configured by the system administrator.

MAXxEMV CIS Logging screen



The screenshot shows the login interface for the MAXxEMV CIS system. At the top left, there is the MOBILITY PAY logo and the MAXxEMV logo. To the right of the MAXxEMV logo, it says "EuroPay MasterCard Visa". In the top right corner, there is a "Login Now" button. Below the logos is a decorative banner with a blue circuit board pattern and a hand pointing at it. The main content area is titled "Log In" and contains the text "Please enter your username and password." Below this is a form titled "Max EMV Login" with two input fields: "Username:" and "Password:". A "Log In" button is positioned below the password field. At the bottom left of the form, there is a "Forgot Password?" link.

Figure 3: MAXxEMV CIS Login



MAXxEMV CIS Web GUI main screen panels:

- Issuer manager
- Job manager
- Quality Manager
- Compliance Auditor
- Manage
- Users
- MAX
- Machine

2.1.1 ISSUER MANAGER

Issuer manager provides platform to define multiple issuers and their different payment scheme EMV card products. Issuer Manager powers the functionality to define different EMV chip card profiles according to scheme requirements in a user friendly interface. The same user interface can be used to assign different products (BIN wise) under the respective issuer.

ISSUERS

The issuer supplies card holder data from their card management or host system for EMV Data preparation. The data contains individual card holder information such as account / card number, card holder name, expiry date etc details and 'profile' information. A profile defines issuer & card risk parameters, cryptographic keys versions to be used, settings for PIN like try limit,etc.

The below form allows to create new issuer / update existing issuer / delete issuers.

CREATE NEW ISSUER

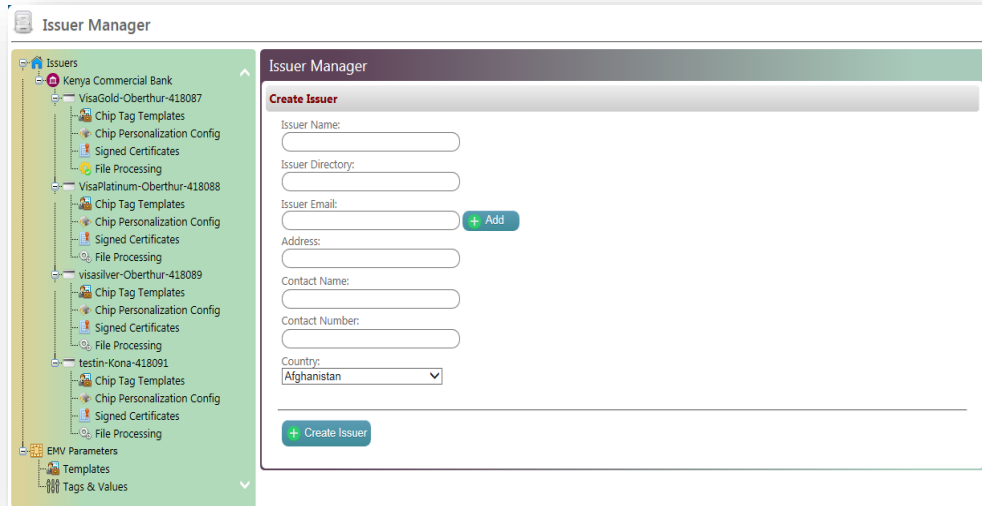



Figure 4: Create New Issuer

- Enter the Issuer information in the form.

- Click  button.

UPDATE ISSUER

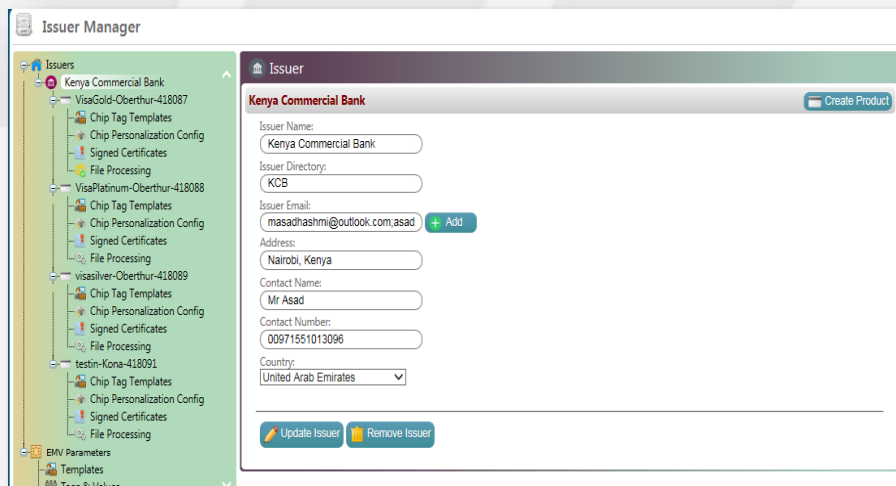

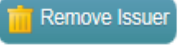


Figure 5: Update Issuer

- Select the Issuer from the navigation panel.

- Click the section that you want to change, then enter the new information.
- Click  button

REMOVE ISSUER

- Select the Issuer from the navigation panel.
- Click  button.

PRODUCTS

After creation new Issuer, products can be added to the issuer using the below form.

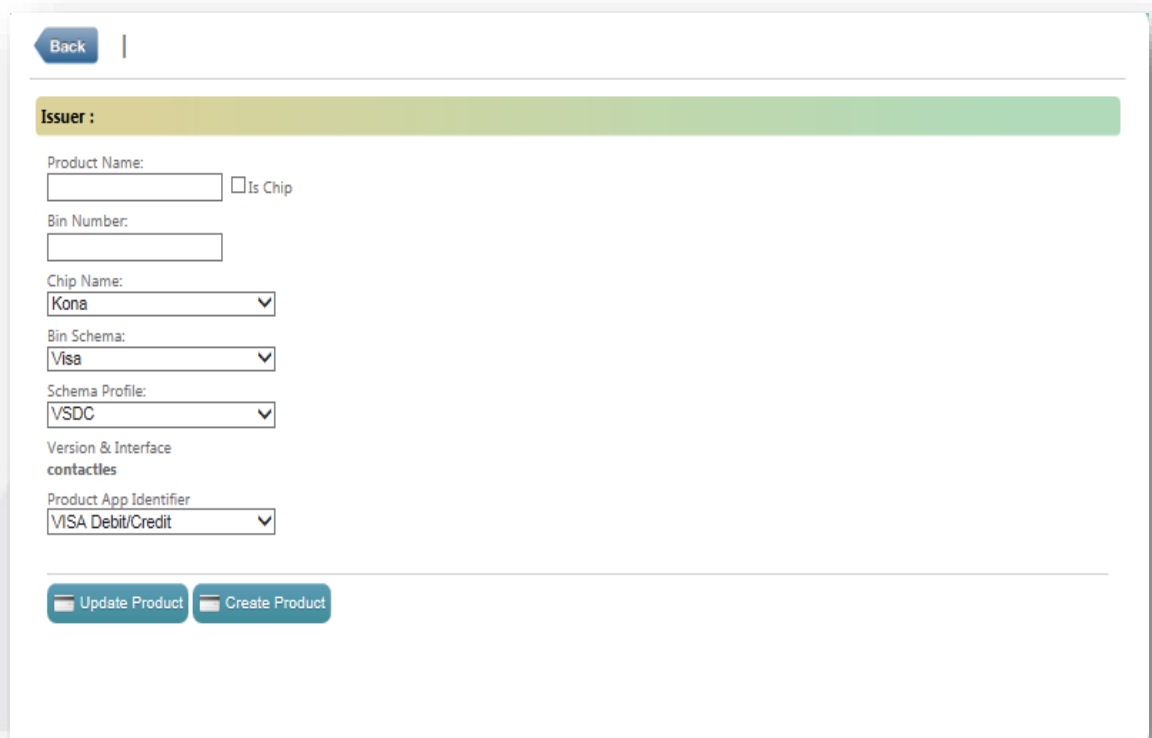




Figure 6: Create New Product

CREATE NEW PRODUCT

- Select the Issuer from the navigation panel.
- Click on  button on the right side of the form, the above form populated.
- Enter the product information.
- Click on  button.

EDIT PRODUCT

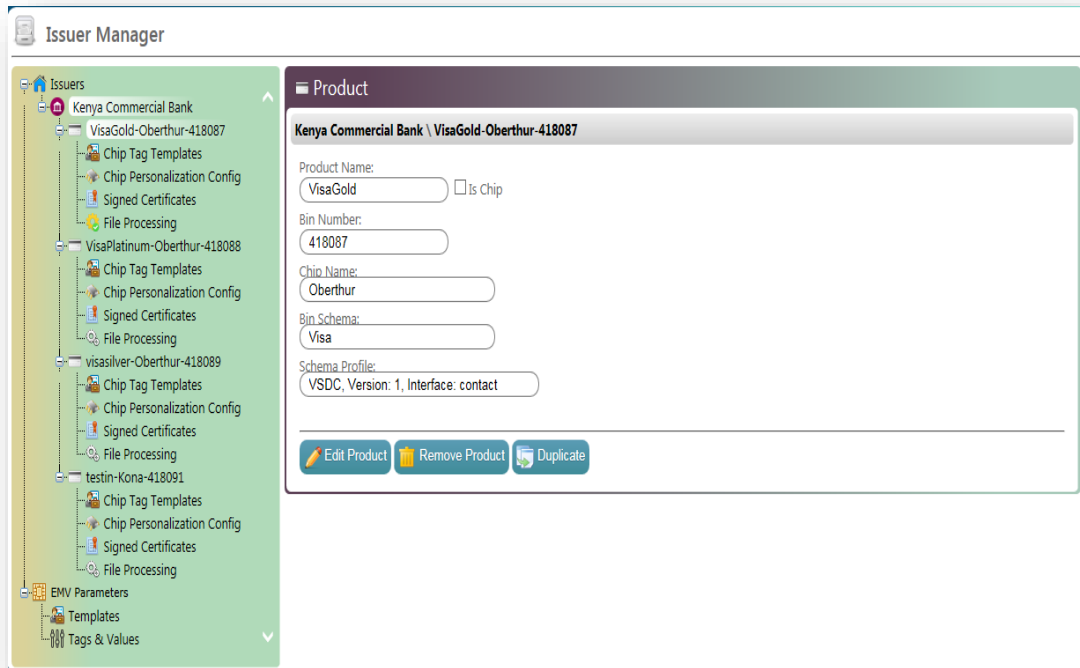




Figure 7: Edit Product

- Select the product from the navigation panel.
- Choose the appropriate entry wish to change, and enter the information.
- Click  button to save the details.

REMOVE PRODUCT

- Select the product from the navigation panel.
- Click  button.

CREATE NEW COPY OF THE PRODUCT FROM THE EXISTING ONE

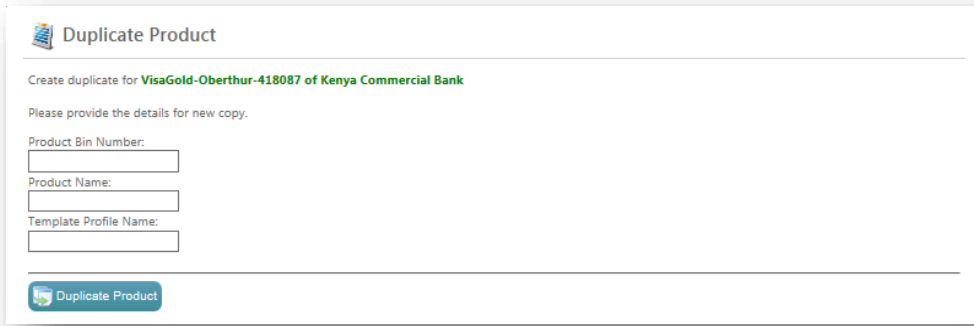


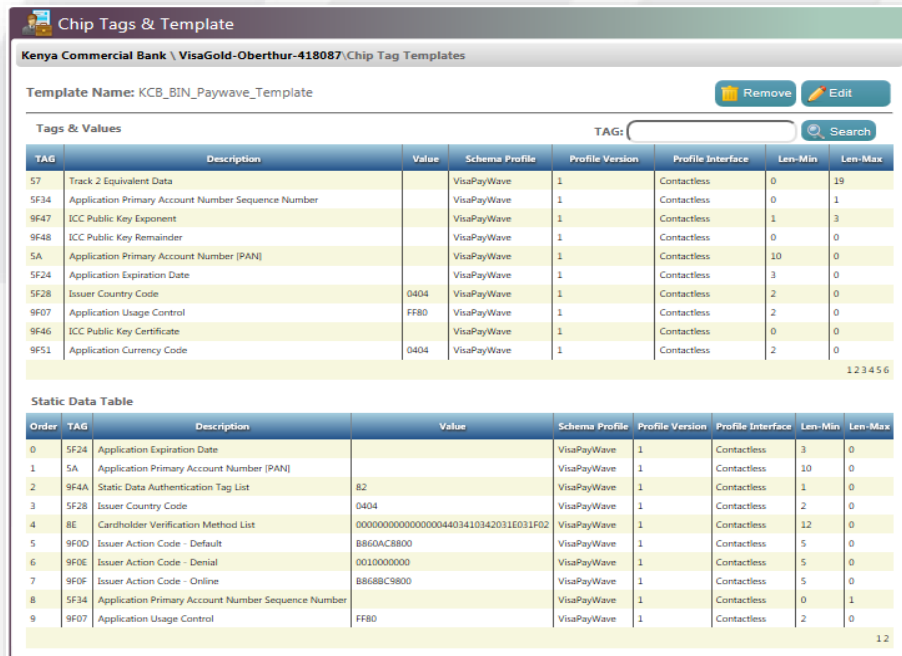


Figure 8: Duplicate Product

- Select the product which you wish to duplicate from the navigation panel.
- Click on 
- Enter product Bin number, product name and Template profile name
- Click  to effect the changes.

CHIP TAG TEMPLATES

MAXxEMV CIS maintain all the global and static tags and values.



TAG	Description	Value	Schema Profile	Profile Version	Profile Interface	Len-Min	Len-Max
57	Track 2 Equivalent Data		VisaPayWave	1	Contactless	0	19
5F34	Application Primary Account Number Sequence Number		VisaPayWave	1	Contactless	0	1
9F47	ICC Public Key Exponent		VisaPayWave	1	Contactless	1	3
9F48	ICC Public Key Remainder		VisaPayWave	1	Contactless	0	0
5A	Application Primary Account Number (PAN)		VisaPayWave	1	Contactless	10	0
5F24	Application Expiration Date		VisaPayWave	1	Contactless	3	0
5F28	Issuer Country Code	0404	VisaPayWave	1	Contactless	2	0
9F07	Application Usage Control	FF80	VisaPayWave	1	Contactless	2	0
9F46	ICC Public Key Certificate		VisaPayWave	1	Contactless	0	0
9F51	Application Currency Code	0404	VisaPayWave	1	Contactless	2	0

Order	TAG	Description	Value	Schema Profile	Profile Version	Profile Interface	Len-Min	Len-Max
0	5F24	Application Expiration Date		VisaPayWave	1	Contactless	3	0
1	5A	Application Primary Account Number (PAN)		VisaPayWave	1	Contactless	10	0
2	9F4A	Static Data Authentication Tag List	82	VisaPayWave	1	Contactless	1	0
3	5F28	Issuer Country Code	0404	VisaPayWave	1	Contactless	2	0
4	8E	Cardholder Verification Method List	000000000000000000004403410342031E031F02	VisaPayWave	1	Contactless	12	0
5	9F0D	Issuer Action Code - Default	B860AC8800	VisaPayWave	1	Contactless	5	0
6	9F0E	Issuer Action Code - Denial	0010000000	VisaPayWave	1	Contactless	5	0
7	9F0F	Issuer Action Code - Online	B868BC9800	VisaPayWave	1	Contactless	5	0
8	5F34	Application Primary Account Number Sequence Number		VisaPayWave	1	Contactless	0	1
9	9F07	Application Usage Control	FF80	VisaPayWave	1	Contactless	2	0

Figure 9: Chip Tag Template



User can perform delete & add Tags, add tag values, add to SD Table, add to SD Table as Values operations in the above form. Static Data table tags can be placed in order by choosing “Move Up” & “Move Down” buttons.

Bin Template Management

Issuer : Kenya Commercial Bank
Product : VisaGold-Oberthur-418087

Bin Template: KCB_Bin_Paywave_Template

Tags & Values TAG:

Select	ID	TAG	Description	Value	Schema Profile	Profile Version	Profile Interface	Len-Min	Len-Max
Select	356	57	Track 2 Equivalent Data		VisaPayWave	1	Contactless	0	19
Select	357	SF34	Application Primary Account Number Sequence Number		VisaPayWave	1	Contactless	0	1
Select	358	9F47	ICC Public Key Exponent		VisaPayWave	1	Contactless	1	3
Select	359	9F48	ICC Public Key Remainder		VisaPayWave	1	Contactless	0	0
Select	360	5A	Application Primary Account Number [PAN]		VisaPayWave	1	Contactless	10	0
Select	361	SF24	Application Expiration Date		VisaPayWave	1	Contactless	3	0
Select	362	SF28	Issuer Country Code	0404	VisaPayWave	1	Contactless	2	0
Select	363	9F07	Application Usage Control	FF80	VisaPayWave	1	Contactless	2	0
Select	364	9F46	ICC Public Key Certificate		VisaPayWave	1	Contactless	0	0
Select	365	9F51	Application Currency Code	0404	VisaPayWave	1	Contactless	2	0

1 2 3 4 5 6

Static Data Table

Select	ID	Order	TAG	Description	Schema Profile	Profile Version	Profile Interface	Len-Min	Len-Max
Select	55	0	SF24	Application Expiration Date	VisaPayWave	1	Contactless	3	0
Select	56	1	5A	Application Primary Account Number [PAN]	VisaPayWave	1	Contactless	10	0
Select	57	2	9F4A	Static Data Authentication Tag List	VisaPayWave	1	Contactless	1	0
Select	58	3	SF28	Issuer Country Code	VisaPayWave	1	Contactless	2	0
Select	59	4	8E	Cardholder Verification Method List	VisaPayWave	1	Contactless	12	0
Select	60	5	9F0D	Issuer Action Code - Default	VisaPayWave	1	Contactless	5	0
Select	61	6	9F0E	Issuer Action Code - Denial	VisaPayWave	1	Contactless	5	0
Select	62	7	9F0F	Issuer Action Code - Online	VisaPayWave	1	Contactless	5	0
Select	63	8	SF34	Application Primary Account Number Sequence Number	VisaPayWave	1	Contactless	0	1
Select	64	9	9F07	Application Usage Control	VisaPayWave	1	Contactless	2	0
Select	66	10	82	Application Interchange Profile	VisaPayWave	1	Contactless	2	0

Figure 10: Add to SD Table

CHIP PERSONALIZATION CONFIGURATION

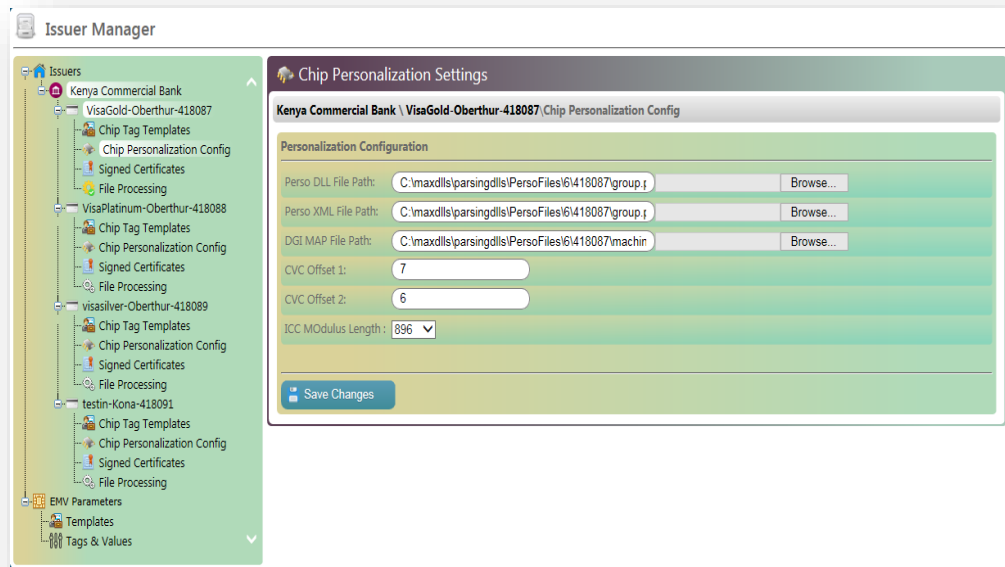


Figure 11: Chip Personalization Configuration

The following parameters can be configured in the above screen.

- Perso DLL file path
- Perso XML file path
- DGI MAP file path
- CVC offset 1
- CVC offset 2
- ICC Modulus length

SIGNED CERTIFICATE

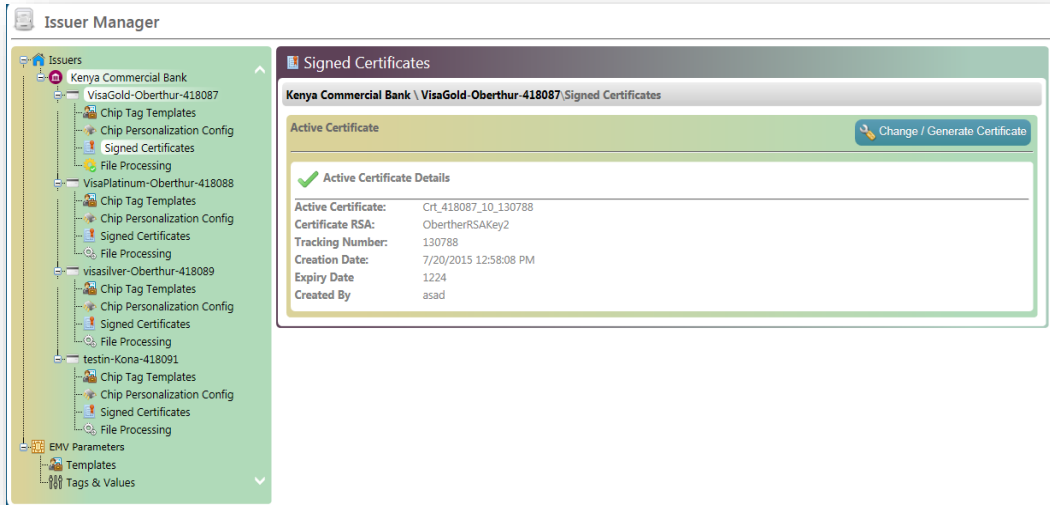


Figure 12: Signed Certificate

MAXxEMV CIS creates Signed certificate for each product to make it secured. By using a MAXxEMV CIS signed certificate, assures users that it is directly linked to the application and no 3rd party interference is permitted. The “Signed Certificate” feature gives the users a high level trust in MAXxEMV CIS and product personalization will take place based on the Signed Certificate.

FILE PROCESSING

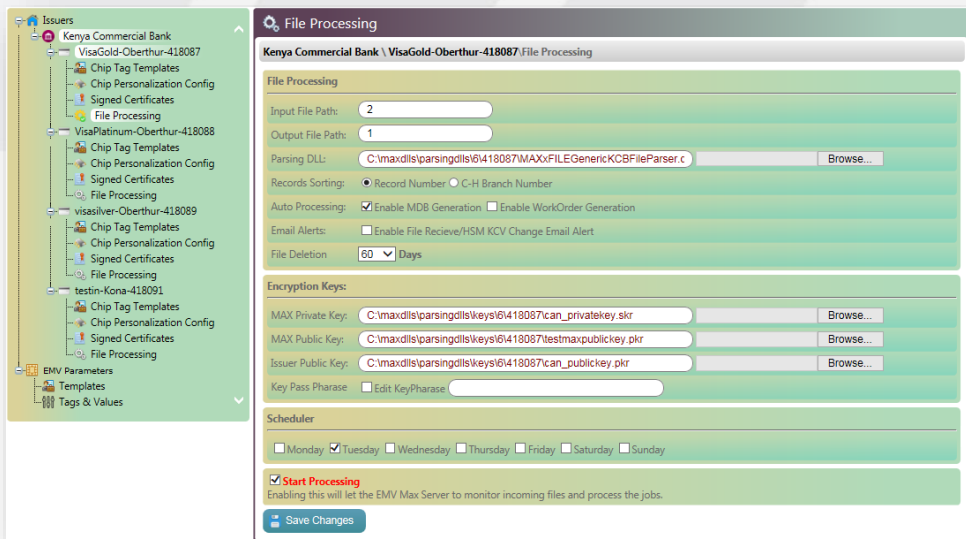


Figure 13: File Processing

To process a file in MAXxEMV CIS user need to define certain parameters.

- Input File Path
- Output File Path
- Parsing DLL
- Select Record Sorting
- Select Auto Processing
- Email Alert (Optional)

File deletion is a mandatory requirement of Payment Schemes and MAXxEMV CIS has the capability to handle this based on the interval set by the user.

MAXxEMV CIS defines Encryption Keys for all the files of each product.

- MAX Private Key
- MAX Public Key
- Issuer Public Key

MAXxEMV CIS has the capability of processing the file with Scheduler. This option helps the customers to process the files with a pre-defined time. This is mainly used in bureaus where the files are received during non-working hours where the TAT is very less.

MAXxEMV CIS validates the settings provided in the application and if the files does not meet any of the specification, the file will be rejected and a detailed report generated with the error caused.

2.1.2 JOB MANAGER

MAXxEMV CIS Job Manager provides the necessary user interfaces for data input to be processed. With the help of MAXxEMV CIS Job Manager, Issuer files (batches) can be parsed and processed according to the pre-defined profile-template of chip. MAXxEMV CIS requires a central database and the same used to store jobs, job settings and processed data which requires during card personalization. The Magstripe/EMV chip data is uploaded to the central SQL Server database and the data is accessed by the personalization machines and smart card personalization module.

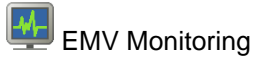
Job Manager main panels:



File management



Work Orders



FILE MANAGEMENT

User can view all the received files and its records as per search criteria. A **View** option is available to see all the records of a particular file.

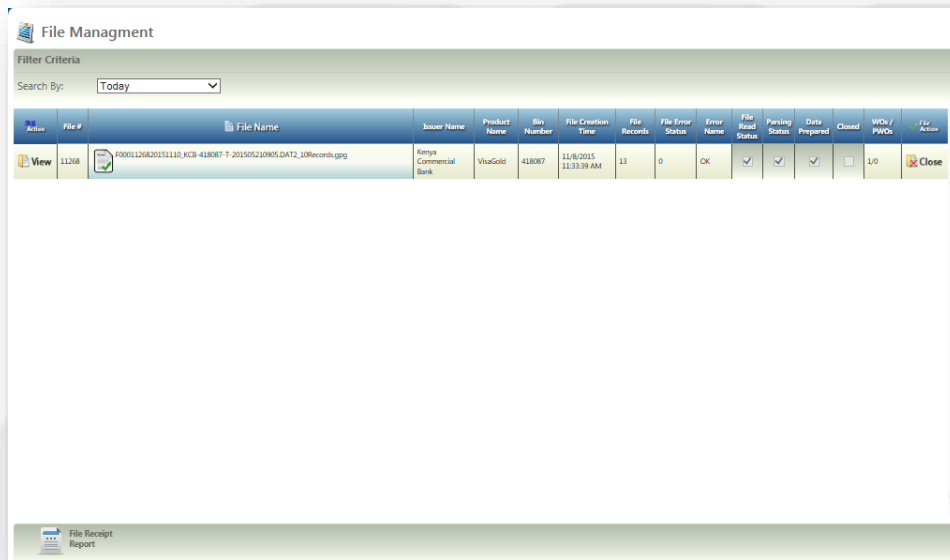


Figure 14: File Management

Search by:

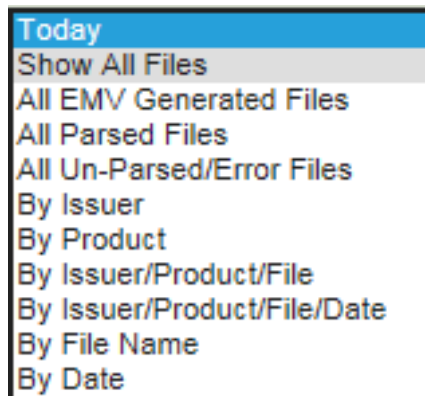


Figure 15: Search by options

PREPARE RECORDS AND WORK ORDER

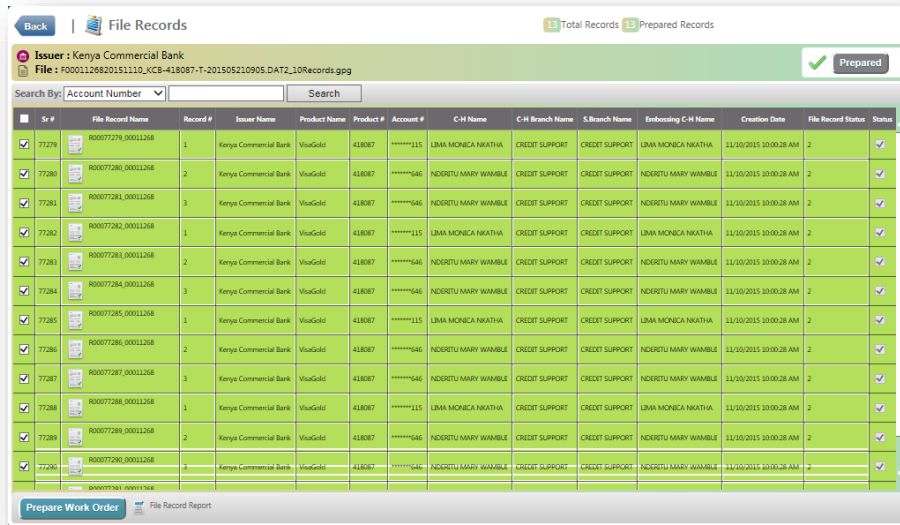




Figure 16: Prepare records & Work orders

- Select the records that you want to prepare
- Click on  button
- Click on 

It will generate a work order according to the selected records.

WORK ORDERS

This screen allows you to review the generated work order files and its details. You can either chose the file to be personalized or if scheduled, the personalization will start based on the sequence.

Generated Work Orders

Filter Criteria
Search By: Today

Serial #	Generated File Name	Parent File	Creation Date	Issuer Name	File Records	Personalized Records	Remaining Records	Rejected Records	User	Work Stage	Final Status	Action
144	F:\0000014\F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:03:10 AM	Kenya Commercial Bank	13	0	13	0	asad	1		VIEW REPORT

Work Orders Report

Figure 17: Generated Work orders

MAXxEMV FILE MONITORING

This screen provide the file details currently being in preparation. In addition, display the records which are currently in generation.

Back | Max File Monitoring

File Under EMV Data Generation 11/10/2015 10:28:07 AM

File Name	File Creation Date	issuename	Product	Product Number	Processed Records	Remaining Records	File EMV Data Status
F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	13	0	<input checked="" type="checkbox"/>

File records Under EMV Data Generation

Record Name	File Name	File Creation Date	issuename	Product	Product Number	Status	Description
R00077291_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077290_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077289_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077288_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077287_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077286_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077285_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077284_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077283_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077282_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077281_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077280_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully
R00077279_00011268	F0001126820151110_KCB-418087-T-201505210905_DAT7_10Records.gpg	11/10/2015 10:00:27 AM	Kenya Commercial Bank	VisaGold	418087	<input checked="" type="checkbox"/>	Chip Data Parsed successfully

Figure 18: MAXxEMV CIS File Monitoring

EXPIRED FILES

All the expired files displayed here. User can delete unwanted files.

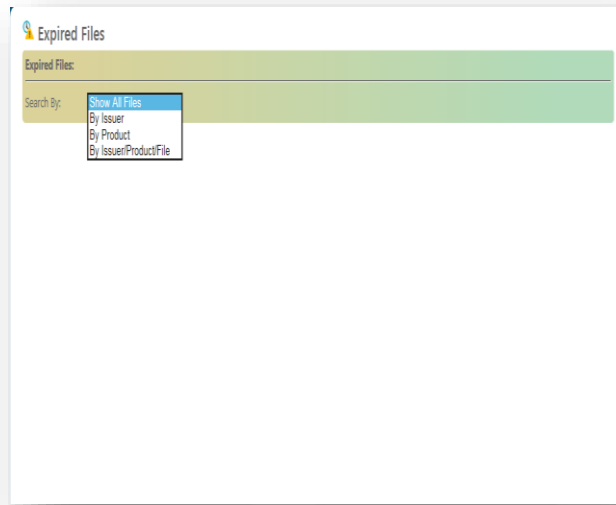


Figure 19: Expired Files

DELETED FILES

All deleted files can be viewed here.

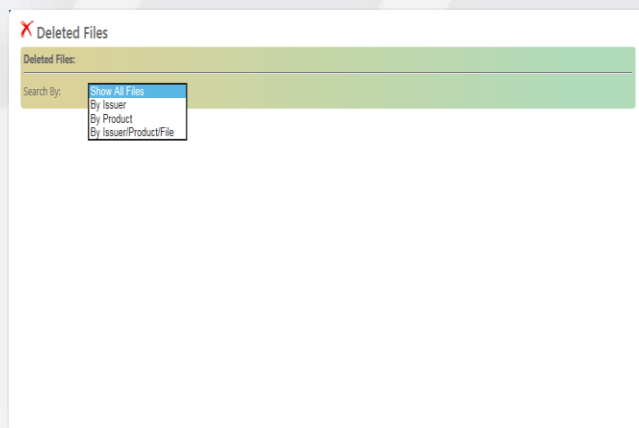



Figure 20: Deleted Files

2.1.5 MAXxEMV CIS MANAGEMENT

Manage main panels:


 Chip management

 Scheme Management

 Key Management

 Scheme Profiles

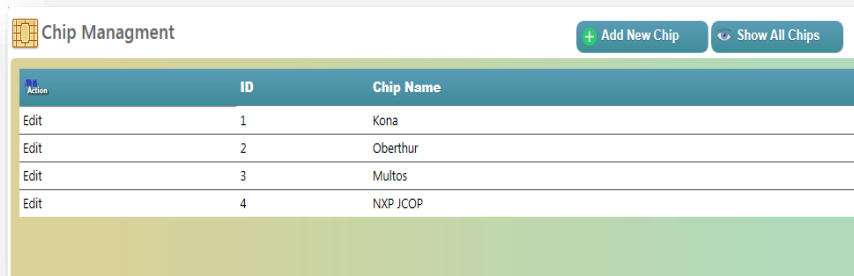
 Configuration

 DMZ Accounts

CHIP MANAGEMENT

EMV Cards are chip-based cards, however, are designed to be more secure because they compose a one-time encrypted code for each transaction. Payment chip cards are considerable less vulnerable to fraud. The information on the chip cannot be manipulated in the way information on a magnetic stripe can and chip cards cannot be skimmed or counterfeited. Chip-enabled payment products greatly enhance security through encryption and dynamic authentication. MAXxEMV CIS has the capability to deal with different chip products of different manufactures.

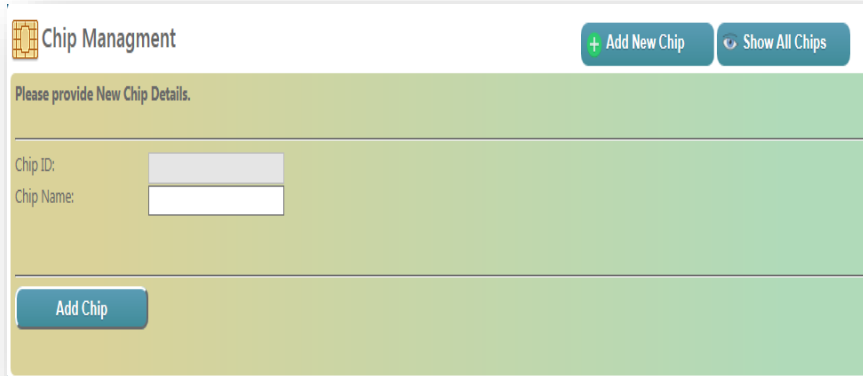
ADD NEW CHIP



Action	ID	Chip Name
Edit	1	Kona
Edit	2	Oberthur
Edit	3	Multos
Edit	4	NXP JCOP

Figure 21: Chip Management

- Click on **+ Add New Chip** button to add new chip product of particular manufacturer
- Enter the chip ID and chip name
- Click on Add Chip button

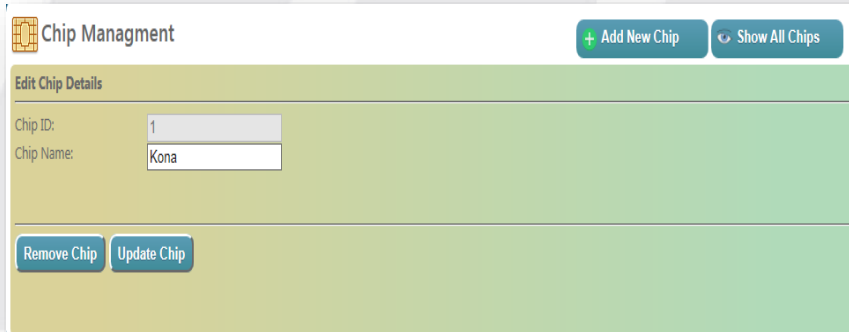


The screenshot shows the 'Chip Management' interface. At the top right, there are two buttons: '+ Add New Chip' and 'Show All Chips'. Below the header, there is a green box with the text 'Please provide New Chip Details.' followed by two input fields: 'Chip ID:' and 'Chip Name:'. At the bottom of the form is a blue button labeled 'Add Chip'.

Figure 22: Add New Chip

EDIT CHIP

- Click on “Edit” to edit the chip details, the following form gets populated. .



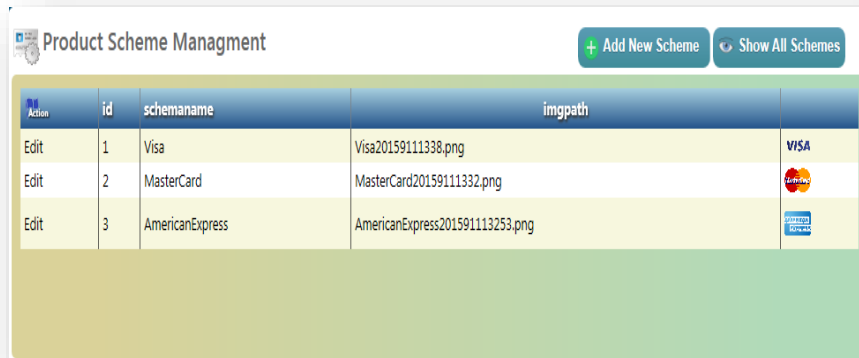
The screenshot shows the 'Edit Chip' form in the 'Chip Management' interface. At the top right, there are two buttons: '+ Add New Chip' and 'Show All Chips'. Below the header, there is a green box with the text 'Edit Chip Details'. Below this, there are two input fields: 'Chip ID:' with the value '1' and 'Chip Name:' with the value 'Kona'. At the bottom of the form are two blue buttons: 'Remove Chip' and 'Update Chip'.

Figure 23: Edit Chip

- To update the chip Click the section you want to change, then enter the new information.
- Click on **Update Chip** button.
- To remove the chip, enter the chip ID and chip name.
- Click **Remove Chip**

SCHEME MANAGEMENT

In Scheme Management user can define different payment schemes and add & edit the scheme details.





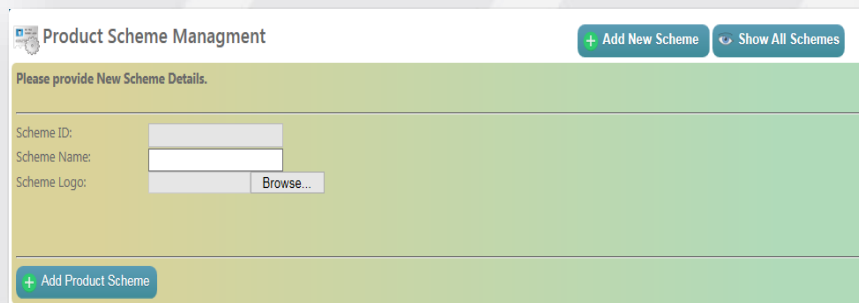
Action	id	schemaname	imgpath	
Edit	1	Visa	Visa20159111338.png	
Edit	2	MasterCard	MasterCard20159111332.png	
Edit	3	AmericanExpress	AmericanExpress201591113253.png	

Figure 24: Scheme Management

ADD NEW SCHEME

- Click on  button.



Product Scheme Management


Please provide New Scheme Details.

Scheme ID:


Scheme Name:

Scheme Logo:

Figure 25: Add New Scheme

- Enter Scheme ID, Scheme Name and Scheme Logo.
- Click on  button.

UPDATE SCHEME

- Click the section that you want to change, then enter the new information.
- Click on  button.

REMOVE SCHEME



- Enter Scheme ID, Scheme Name and Scheme Logo
- Click on **Remove Scheme** button.



Figure 26: Remove Scheme

KEY MANAGEMENT

MAXxEMV CIS Key management system strictly adheres industry KMS principles & guidelines. KMS system connected to FIPS 140-2 certified Hardware Security Module (HSM) to enable hardware security as per industry standards.

MAXxEMV CIS Key Manager System powers:

- Secure External/Internal key exchange
- Four eye principle
- Allow number of key custodians
- Easy Key Administration

MAX EMV Key Management

[All Keys](#) [Key Types](#)

ID	Key Name	Key Value	Key Type	ZMK Key	Product	Issuer	Key Creation Time	Key Check Value	Created By
50	KCB_ENC	6333C84866F96992951DC071A3E5191D	ENC	MainKEK	VisaGold	Kenya Commercial Bank	7/24/2015 10:45:20 PM	944444	Can
51	KCB_MAC	6333C84866F96992951DC071A3E5191D	MAC	MainKEK	VisaGold	Kenya Commercial Bank	7/24/2015 10:46:18 PM	944444	Can
52	MAXx_PTK	0D7515F28FCL7F85D07515F28FCL7F85	PTK	MainKEK	VisaGold	Kenya Commercial Bank	7/24/2015 10:50:32 PM	82E136	Can
53	MAXx_KEK	0D7515F28FCL7F85D07515F28FCL7F85	KEK	MainKEK	VisaGold	Kenya Commercial Bank	7/24/2015 10:53:10 PM	82E136	Can
54	KCB_AC	6333C84866F96992951DC071A3E5191D	DEC	MainKEK	VisaGold	Kenya Commercial Bank	7/24/2015 11:11:33 PM	944444	Can
55	test: key data ptk	2120A4E446324F805F0223F49599A8023	DATA_PTK	MyTestKeyZMK1	VisaGold	Kenya Commercial Bank	7/15/2015 3:37:23 PM	7C6991	Can
57	KCB_DATAPTK	F915FA88C98CC87D29026C2CDA78A52D	DATA_PTK	MainKEK	VisaGold	Kenya Commercial Bank	7/16/2015 9:05:02 PM	2D617C	Can
59	keytestMAGKEY	6333C84866F96992951DC071A3E5191D	MAG	MainKEK	VisaGold	Kenya Commercial Bank	7/16/2015 9:09:22 PM	944444	Can
62	keytestMUser	107C1A5FD0436398107C1A5FD0436398	KMC	MyTestKeyZMK1	VisaGold	Kenya Commercial Bank	8/8/2015 12:13:48 PM	D41488	Can
63	mynewkeyunderZMK786	E815486556A8088705E564C50122320C	KMC	zmktest key 786	VisaGold	Kenya Commercial Bank	8/10/2015 5:04:40 PM	AF1982	Can

12

Figure 27: MAXxEMV CIS Key Display

KEY TYPES



MAX EMV Key Management

All Keys Key Types

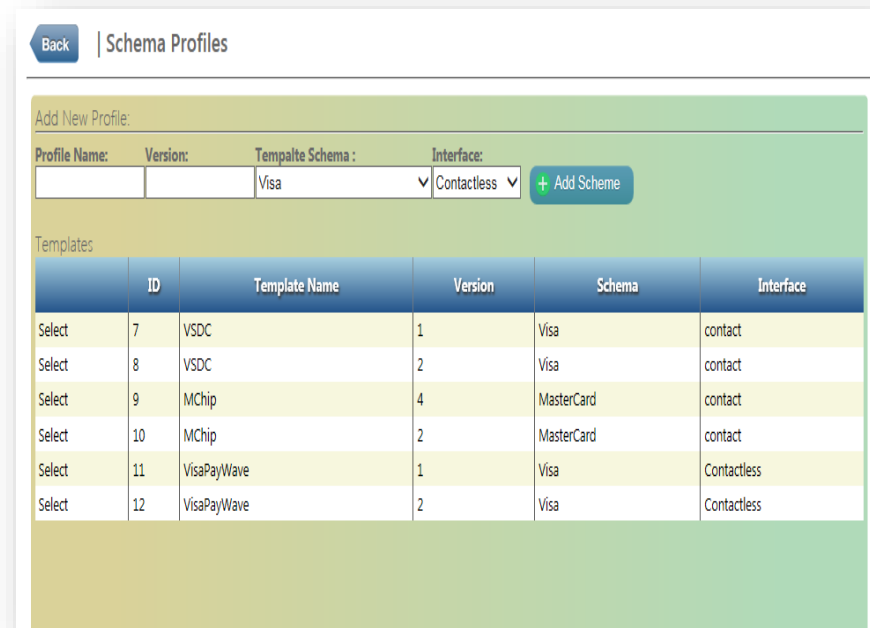
KEY TYPE
Key Type Name
KEK
DEC
ENC
MAC
PVT
PTK
PVK
MAG
DATA_PTK
DATA_KEK

12

Figure 28: MAXxEMV CIS Key Types

SCHEME PROFILES

User can add different schemas and their templates for the products



Back | Schema Profiles

Add New Profile:

Profile Name: Version: Template Schema: Interface:

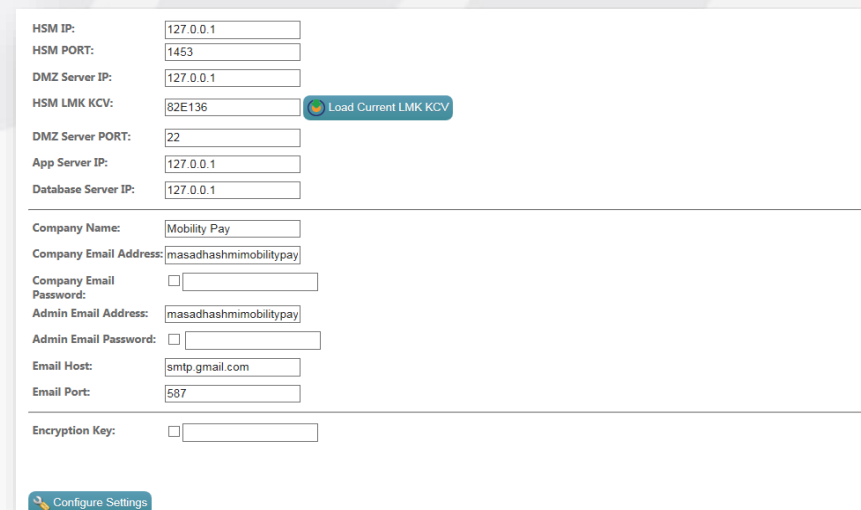
Templates

	ID	Template Name	Version	Schema	Interface
Select	7	VSDC	1	Visa	contact
Select	8	VSDC	2	Visa	contact
Select	9	MChip	4	MasterCard	contact
Select	10	MChip	2	MasterCard	contact
Select	11	VisaPayWave	1	Visa	Contactless
Select	12	VisaPayWave	2	Visa	Contactless

Figure 29: Scheme Profiles

CONFIGURATION

Here user can set MAXxEMV CIS configuration in the form.



HSM IP:

HSM PORT:

DMZ Server IP:

HSM LMK KCV:

DMZ Server PORT:

App Server IP:

Database Server IP:

Company Name:

Company Email Address:

Company Email Password:

Admin Email Address:

Admin Email Password:

Email Host:

Email Port:

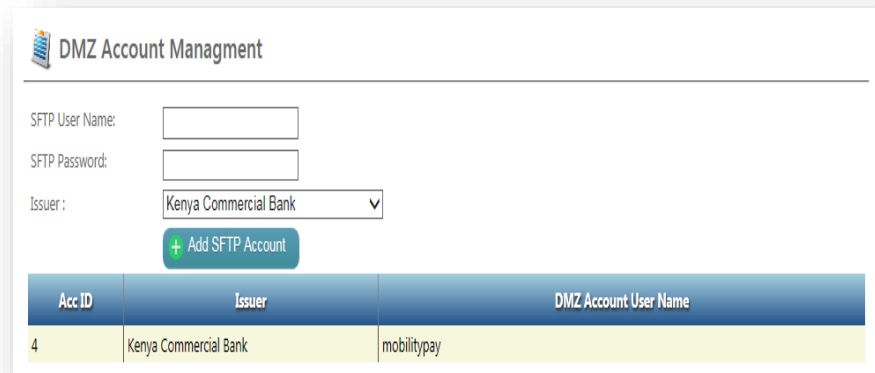
Encryption Key:

Figure 30: Configurations

DMZ ACCOUNTS

As per Bureau / financial institution logical security, a **DMZ** or **demilitarized zone** (sometimes referred to as a **perimeter network**) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.


TO ADD A DMZ ACCOUNT



The screenshot shows the 'DMZ Account Management' interface. It includes input fields for 'SFTP User Name', 'SFTP Password', and a dropdown menu for 'Issuer' (currently set to 'Kenya Commercial Bank'). A green '+ Add SFTP Account' button is located below the issuer dropdown. Below the form is a table with the following data:

Acc ID	Issuer	DMZ Account User Name
4	Kenya Commercial Bank	mobilitypay

Figure 31: Add a DMZ Account

- Enter SFTP user name.
- Enter SFTP password.
- Enter issuer name.
- Click on  button.

USERS MANAGEMENT



USER GROUP MANAGEMENT

Under User Group Management form user can add new and edit existing User groups.

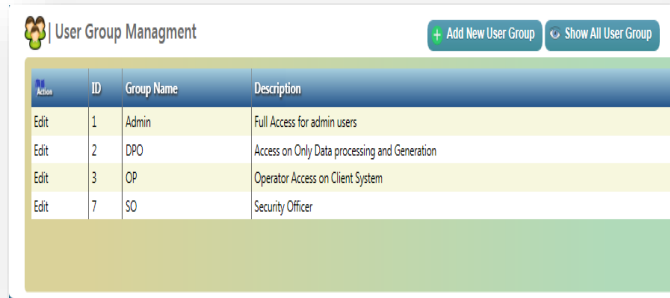


Figure 32: User Group Management

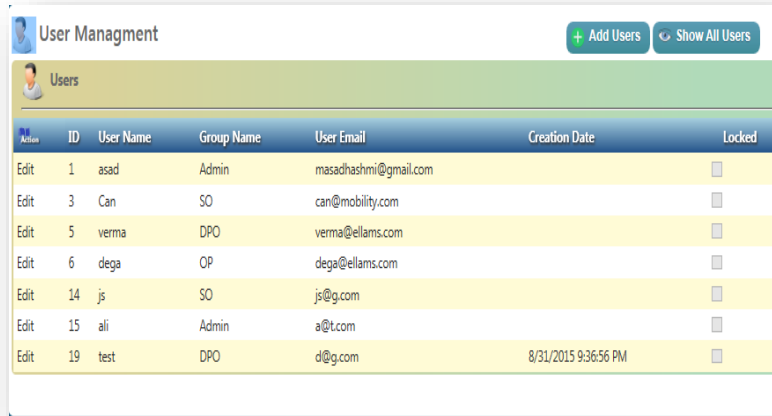
The description of the “Group Names” provided below.

Group Name	Description
Admin	Full access
DPO	Access on only data processing and generation
OP	Operator access on client system
SO	Security officer

Table 1: Groups Description

USER MANAGEMENT

Here Admin user can manage all the users.



User Management + Add Users Show All Users

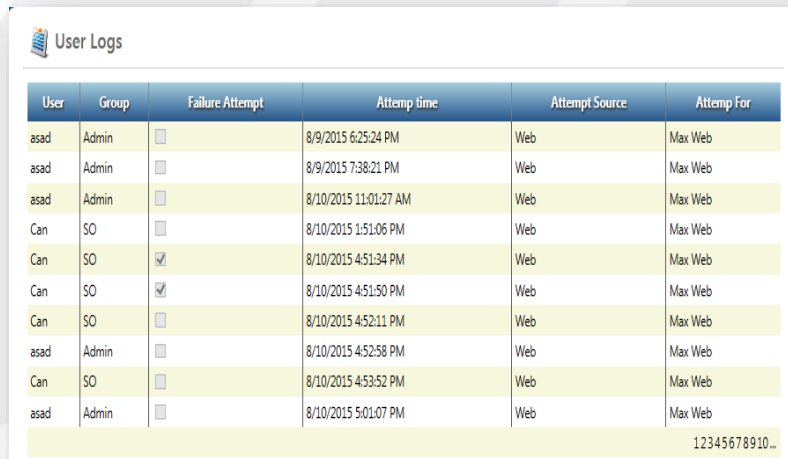
Users

Action	ID	User Name	Group Name	User Email	Creation Date	Locked
Edit	1	asad	Admin	masadhashmi@gmail.com		<input type="checkbox"/>
Edit	3	Can	SO	can@mobility.com		<input type="checkbox"/>
Edit	5	verma	DPO	verma@ellams.com		<input type="checkbox"/>
Edit	6	dega	OP	dega@ellams.com		<input type="checkbox"/>
Edit	14	js	SO	js@g.com		<input type="checkbox"/>
Edit	15	ali	Admin	a@t.com		<input type="checkbox"/>
Edit	19	test	DPO	d@g.com	8/31/2015 9:36:56 PM	<input type="checkbox"/>

Figure 33: User Management

USER LOGS

Admin user can monitor users login activities, failure attempts, login date & time stamp details etc.



User Logs

User	Group	Failure Attempt	Attempt time	Attempt Source	Attempt For
asad	Admin	<input type="checkbox"/>	8/9/2015 6:25:24 PM	Web	Max Web
asad	Admin	<input type="checkbox"/>	8/9/2015 7:38:21 PM	Web	Max Web
asad	Admin	<input type="checkbox"/>	8/10/2015 11:01:27 AM	Web	Max Web
Can	SO	<input type="checkbox"/>	8/10/2015 1:51:06 PM	Web	Max Web
Can	SO	<input checked="" type="checkbox"/>	8/10/2015 4:51:34 PM	Web	Max Web
Can	SO	<input checked="" type="checkbox"/>	8/10/2015 4:51:50 PM	Web	Max Web
Can	SO	<input type="checkbox"/>	8/10/2015 4:52:11 PM	Web	Max Web
asad	Admin	<input type="checkbox"/>	8/10/2015 4:52:58 PM	Web	Max Web
Can	SO	<input type="checkbox"/>	8/10/2015 4:53:52 PM	Web	Max Web
asad	Admin	<input type="checkbox"/>	8/10/2015 5:01:07 PM	Web	Max Web

12345678910...

Figure 34: User Logs

STATUS MONITOR

Under system navigation panel, user can perform MAXx system monitoring and product license activities.

- MAXxEMV CIS monitoring
- Product License

MAXxEMV System monitoring enables real time monitoring of all the servers, services and HSM status. User can monitor the following:

- MAX Server Status
- MAX FilePro Status
- HSM Status
- Application server
- Database Server
- FTP Server
- Active Issuers
- Active Products

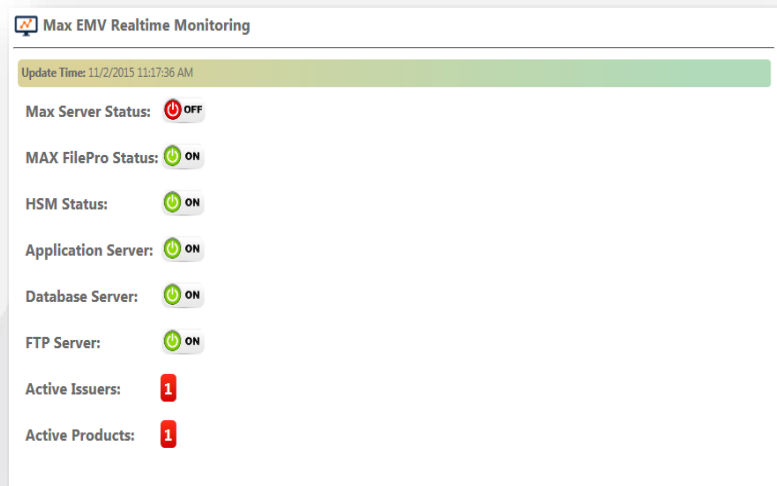


Figure 35: Status Monitor

PRODUCT LICENSE

Product license is essential to make the product functional and MobilityPay issues product license to enable the product operational once installation is completed.

MACHINES MANAGER

Machine Manager allows user to add personalization machines to the system.

To add a Machine

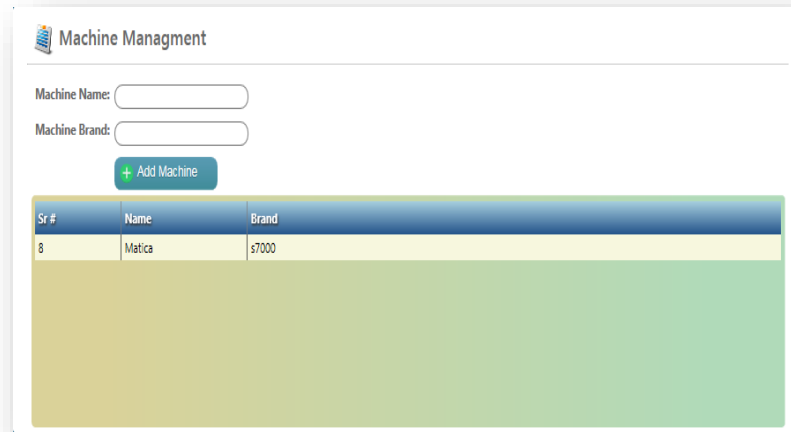



Figure 36: Machine Management

- Add Machine Name.
- Add Machine Brand.
- Click on  button to effect the changes.

2.2 MAXxEMV CIS CLIENT

MAXxEMV CIS is the total turnkey solution on card technology. MAXxEMV CIS has been designed in order to be used in banks and financial institutions that operate a Card Management System and require this Client to be installed at the Card Center to support the full cycle of the card issuance functionality.

Install this MAXxEMV CIS client application in the machine PC. Only the user with operator rights is authorized to access MAXxEMV CIS Client application.

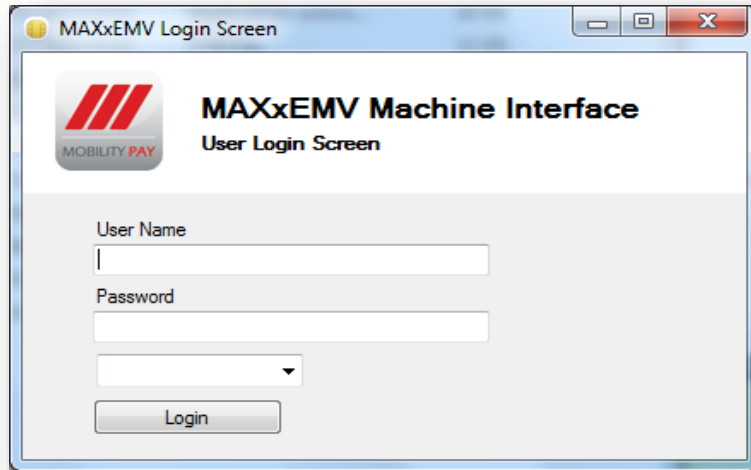


Figure 37: MAXxEMV CIS Client Login

To login the MAXxEMV CIS Client

- Enter the user name
- Enter the password
- Select the Machine

The main panels of MAXxEMV CIS Client has the following features:

- Work Order Files
- Load Work Order
- Personalise Work Order

2.2.1 WORK ORDER FILES

All the work orders those requested from the Web panel displayed in this window. After receiving a embossa file from issuer, web MAXxEMV CIS prepares the file based on your requirements and generates a work order.

To load this work order to machine

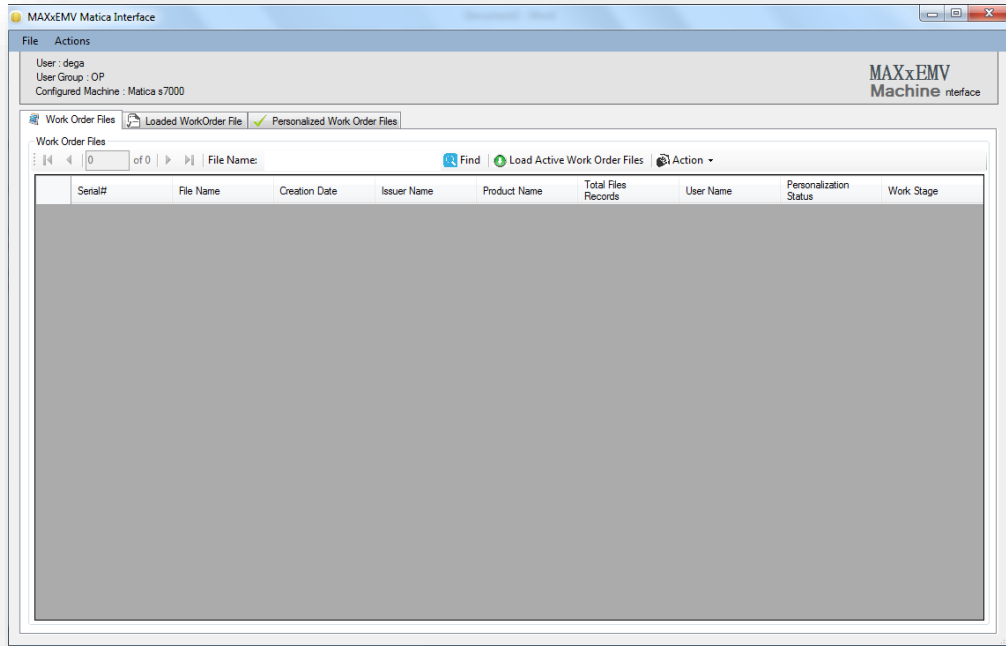


Figure 38: Workorder Files

- Select a work order
- Click on Action Tab
- Select Load to Machine

Once you loaded a work order to the machine, the system alert the customer that particular work order loaded to particular machine. Once the work order is generated, same work order can be loaded to different machine based on the availability if assigned machine is down.

2.2.2 LOAD WORK ORDER

At a given point of time, only one work order can be loaded to one machine. The loaded file displayed on the top. All the records belongs to that work order file will be displayed in the machine job area. After loading the file, machine personalize the cards and generate an alert through the system with MIS information. If any of the record is not personalized due to error, operator can verify and close the file. When the operator click on verify and close tab, a report generated on the server side with all the information like how many cards personalized successfully and how many cards failed with the reason.

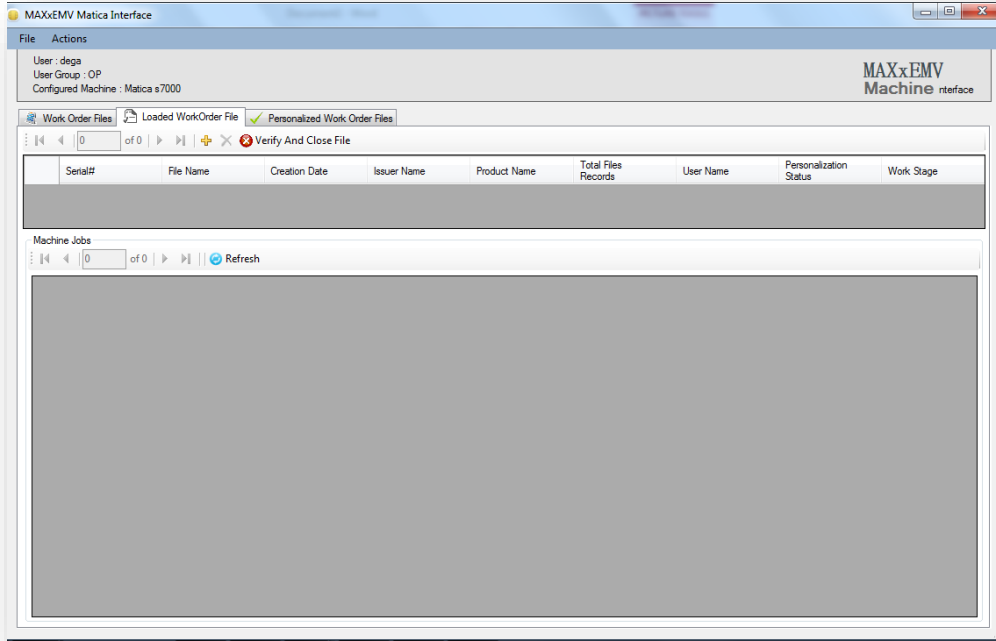


Figure 39: Loaded Workorder Files

2.2.3 PERSONALIZED WORK ORDER FILES

All the personalized work orders displayed here in this area.

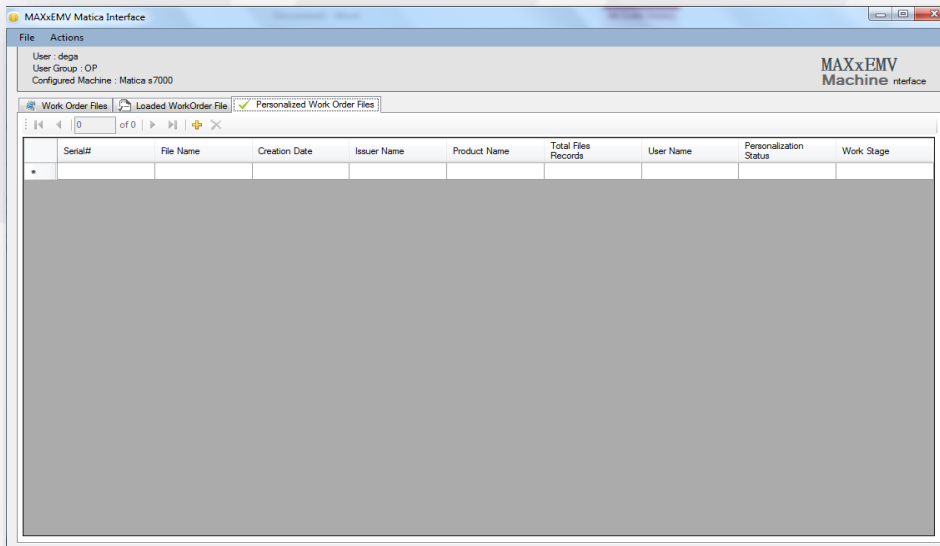


Figure 40: Personalized Workorder Files



2.3 MAXxEMV CIS ENGINE

MAXxEMV CIS sever is a back ground application. It automatically update the Database to keep the record of issuer & respective products, keys and profile information. Server retrieve card data (request); triggers the EMV data preparation module to generate EMV data; transfers required dataset to client for the physcal card personalization (response) and finally updates the card authorization system with the new card data if required.

MAXxEMV CIS server responsibilities

- Tracking and Receiving records in particular files as per agreed format.
- Preparing the files and generating EMV chip data for every record in a very highly intelligent & secured environment.
- EMV key management, EMV card personalization.
- Operation log, error log, on-line trace and audit trail log.
- Real time transaction monitoring.
- Users' definition and access control management.
- Security keys management: All records are encrypted under a particular key which inturn encrypted under LMK of HSM
- HSMs interface.
- PIN generation and PIN traversing support.
- PIN Pads Key Management support.
- Database management.

2.3.1 MAXxEMV CIS DATA PREPRATION

EMV data preparation generates the cryptographic and application data required for personalizing the smart card and is an essential part of issuing EMV cards. Every EMV application needs to be personalized with card holder details. These details include name, account number, wide range of risk management parameters, security keys, certificates and signatures. Since Payment scheme requirements are constantly changing, it is important that a smart card issuance solution not only meets today's needs, but also provides a path to meet any future smart card requirements enhancements, such as contactless, mobile, multi-application and in-branch or post-issuance scripting. MAXxEMV CIS receives issuance requests from card management systems, stores and processes the received embossing file data and generates the required EMV security data elements. MAXxEMV CIS interfaces to a host security module (HSM) in order to derive keys and encrypt sensitive data. The prepared set of data passed on to the personalization bureau for physical card personalization.



2.3.2 MAXxEMV CIS KEY MANAGEMENT

MAXxEMV CIS KMS interface is easier for non-technical key custodians to perform their designated roles as per key management principles, and designed to simplify the process of generating keys and storing them secured way. MAXxEMV KMS interface powers custodians to generate, store, distribute and delete cryptographic keys. The functionality supports best practices for implementing organizational & payment schemes policies and procedures for key management including:

- Users with specific access privileges manage the creation of keys in the MAXxEMV CIS configuration program.
- All user access is recorded in an authenticated log file that is used for compliance auditing.
- Split knowledge & Dual control is supported.
- Clear keys and PIN values never appear in the diagnostic trace files.

Key Management Features

- Manages all the keys necessary for magnetic-stripe and EMV card issuance and authorization
- Supports both static and dynamic key management.
- Simplifies implementation of the hardware security features provided by the HSM.
- MAXxEMV CIS stores Local Master Keys (LMKs) inside the HSM where encryption of all the other keys, including KEK (key encrypting key), takes place. In addition only LMK-encrypted key values are stored in the MAXxEMV CIS database on the host computer and made available for card issuance and authorization processes.
- Only encrypted key values previously generated by the HSM / multiple components of clear keys are entered and stored in the MAXxEMV CIS key vault database. Keys remain encrypted at all times - during creation, storage and use - so that the sensitivity of the key never compromised.

Many smart card issuing systems need to manage a large number of diverse cryptographic keys for different applications. These keys can be used for data encryption and decryption, verification, authentication and authorization purposes. However the process of tracking these keys, lifecycles, key types and procedures on various locations can be challenging to control. A key management system related to the issuance of EMV chip cards is concerned with the management of cryptographic keys between authorized parties and is designed to control complex configurations. while keeping cost low, MAXxEMV CIS provides a proven and secure means to manage the complex EMV issuing environments and the identity industry. It deals with the potentially complex process of generation, storage, distribution, import and lifecycle

management of cryptographic keys. MAXxEMV CIS Key Manager provides interfaces to all major HSM providers and is managed through an easy to use interface.

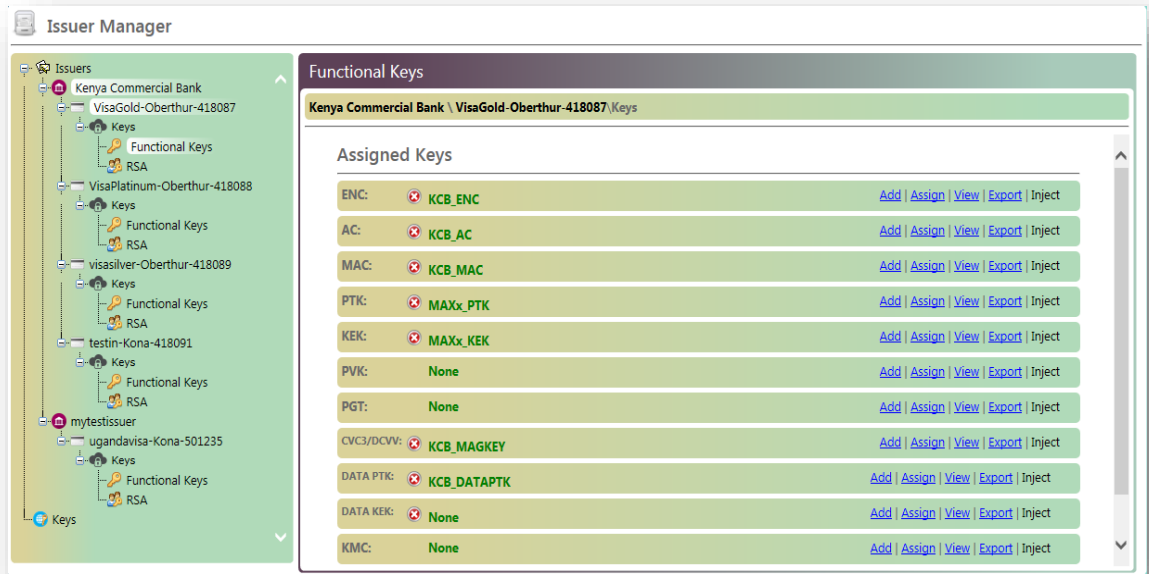


Figure 41: MAXxEMV CIS Key Types

RSA Key Management

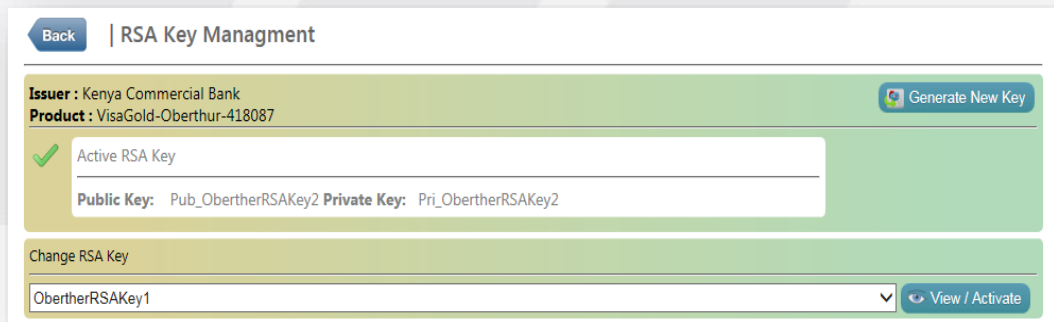


Figure 42: RSA Key Management

ZMK Management

A Zone Master Key (ZMK) is a key-encrypting key which is distributed physically in secured manner between two parties, , in order to further exchange the keys securely. The ZMK is nothing but a transport key, used to export or import keys securely between either two parties or within the organization for secure transmission purposes..

[Back](#) | ZMK Management

Create ZMK Key:

Key Name :

Key Value : [Insert Key Components](#) [Generate Key Components](#)

Enter Key Component 1: [Next](#)

ID	Name	Key Value	ZMK Key Check Value	LMK Key Check Value	User	Creation Date
34	asad	DD7515F28FCL7F85DD7515F28FCL7F85	82E136		Can	8/12/2015 5:20:49 AM
33	testellams6	CAED017060CD25F6A283064FAB2CAFD8	893628		Can	8/11/2015 12:00:23 AM
32	testellams5	B2DDABAE489E5A1888E402F83AE98DAE	A50894		Can	8/10/2015 11:46:06 PM
31	testkey	0A462733B64A5ABEB9C2722A7698E4FA	9677E2		Can	8/10/2015 11:06:17 PM
30	ZMKEllamstest2	8786086E5766C248945F381348DD7468	54865A		Can	8/10/2015 10:47:30 PM
29	ZMKTestEllams	65AAAC7EB68E25CE752058DE2C7ABD61	68CF0E		Can	8/10/2015 10:46:39 PM
28	zmktest	E2A80C8C8F422A168D6ADB80AFED87DA	359285		Can	8/7/2015 9:45:11 PM
27	MainKEK	DD7515F28FCL7F85DD7515F28FCL7F85	82E136		asad	7/14/2015 8:08:14 PM
26	my new zmk 7122015	1216972F8C0690D5757002EFS2010055	1A1209		asad	7/12/2015 12:47:36 PM
25	My Confirmed ZMK Key	31F76689BAF002884F06EA8844144489	A88842		asad	7/12/2015 11:23:20 AM

1/2

Figure 43: ZMK Key Management

2.3.3 MAXxEMV CIS CARD PERSONALIZATION

MAXxEMV CIS allowing card issuers to maintain control over their data while transitioning to more secure technology. Consisting of dedicated tamper resistant cryptographic hardware and Windows-based software, integrates easily with host systems, enabling card issuers to create EMV smart card data and keys with minimal impact on existing systems and at minimal cost. MAXx EMV Central Issuance is a perfect match for low- to medium-volume issuers and small organizations in need of a fast and cost-effective approach to enriching a batch of magnetic-stripe cardholder records into an EMV-compliant format. MAXxEMV CIS Server is a fully scalable solution that's ideal for large issuers and organizations that need the flexibility to operate in batches or through an online server. This version can be used with a central site server for issuance. It integrates easily with smart card management systems to support post-issuance download on multi-application smart cards.

Benefits of the EMV Personalization Preparation Process

- Delivers 100% in-house control over cryptographic keys.
- Supports all major card association contact and contactless applications.
- Generates keys and EMV parameters from existing magnetic stripe files.
- Supports instant card issuance and on-demand replacement of cards.
- Provides the data preparation security infrastructure.



2.4 MAXxEMV CIS Secure File Transfer Engine

The responsibility of MAXxEMV CIS Secure File Transfer Engine is to communicate with the SFTP sever and download files to local server for processing and upload any data to the SFTP server. File Pro Server is responsible for receiving all the files that are coming from a secured SFTP control server and exchanging all these files to internal Perso Bureau Server by using secured SFTP port.





3. SYSTEM REQUIRMENTS

Deployment Models	
Option 1	<ul style="list-style-type: none"> • 1 * Data generation Server • 1 * Database Server • 1 * HSM Server <p>Total 3 Servers</p> <p>(Please check MAXxEMV Central Issuing Data Generation / Database Server table for config details)</p>
Option 2	<ul style="list-style-type: none"> • 1 * Data generation Server/HSM Server • 1 * Database Server <p>Total 2 Servers</p>
Option 3	<ul style="list-style-type: none"> • 1 * Data generation Server/HSM Server/Database Server <p>Total 1 Server (Recommended 1 for PSS)</p>
Option 4	<ul style="list-style-type: none"> • 1 * Data generation PC • 1 * Database PC • 1 * HSM Server PC <p>Total 3 PCs</p> <p>PC :</p> <p>4th Generation Intel(R) Core(TM) i5-i7 processor quad-core [3.5GHz, 6MB Shared Cache]</p> <p>For example : Dell OptiFlex 7020 , i5 Quad Core, and Core™ i3 Dual Core, PDC</p>
Option 5	<ul style="list-style-type: none"> • 1 * Data generation / HSM PC • 1 * Database PC <p>Total 2 PCs</p> <p>PC config:</p> <p>4th Generation Intel(R) Core(TM) i5-i7 processor quad-core [3.5GHz, 6MB Shared Cache]</p> <p>For example : Dell OptiFlex 7020 , i5 Quad Core, and Core™ i3 Dual Core, PDC</p>

Table 2: Deployment options



Typical Hardware & Software configurations

MAXxEMV Central Issuing Data Generation / Database Server	
Hardware	<ul style="list-style-type: none"> • HP DL 380 G9 • Ram 12 GB Ram • Hard Disk 1 TB
Software	Windows Server 2012– 64 bits
Database	SQL Server 2014
Application Server	Internet Information Server IIS(6.0))
MAXxEMV Key Management	
Hardware Security Module	Safenet PSle PL 25 (SDA), PL220 (DDA) or PL600 (The hsm will be on the server)
MAXxEMV Central Issuing Data Generation Operator PC	
Hardware	<ul style="list-style-type: none"> • Intel Core 2 Duo processor • 8 GB RAM • 300 GB hard disk drive • Windows 7 64 bit
MAXxEMV Central Issuing Personalization Matica PC	
Hardware	<ul style="list-style-type: none"> • Intel Core 2 Duo processor • 8 GB RAM • 300 GB hard disk drive • Windows 7 64 bit

Table 3: Hardware & Software Configurations

Extra Software requirements

MAXxEMV Central Issuing Extra Software Requirement	
Software	<ul style="list-style-type: none"> • Net Framework(4.5) • Crystal Report 2013 • Encryption & SFTP tool just in case

Table 4: Extra Software requirements

4. PRODUCT LICENSE

To register this product.

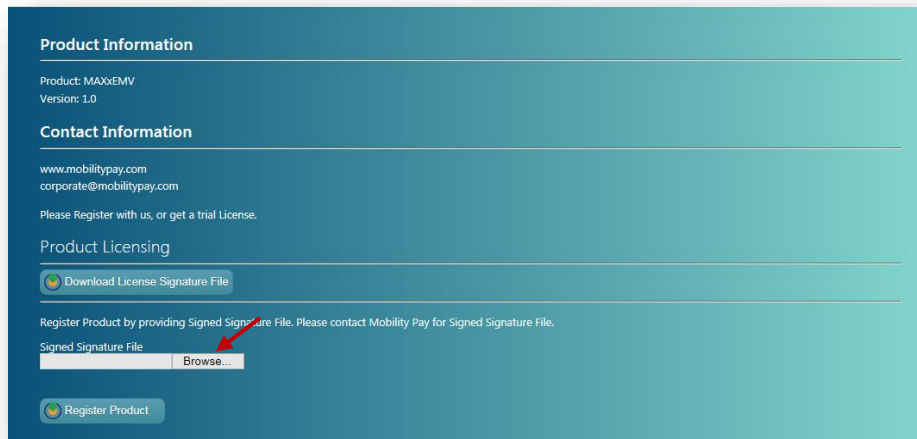


Figure 44: Download License Request File

- Click on Download License Signature File Button to download the signature file

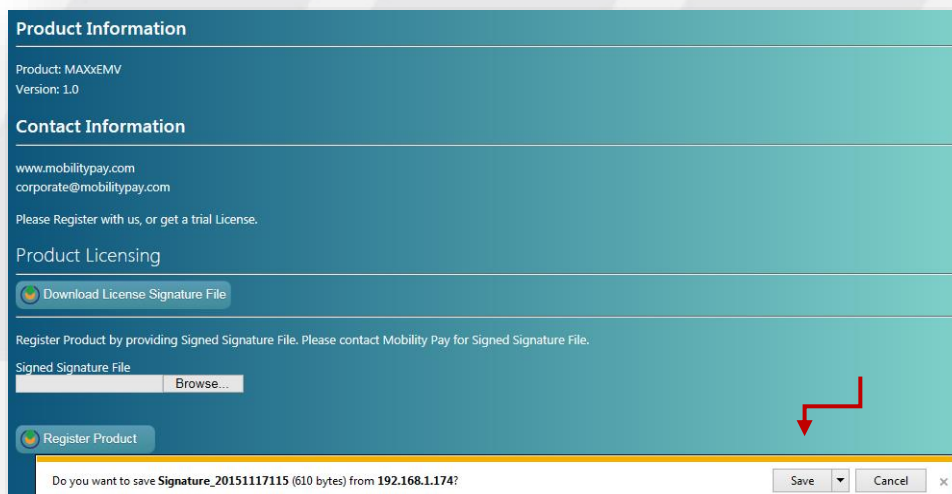


Figure 46: Save License Request File

- Save the signature file.
- Email the signature file to your representative of Mobility Payment Solutions for obtaining digitally Signed Signature file.
- Upload the signed Signature File into MAXxEMV CIS.
- Click on Register Product button to enable the system.



5. DEPLOYMENT PLAN

This part defines the sequence of operations that should be carried to deploy MAXxEMV CIS into a target system environment

No.	Activity	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th
1	Kick off Meeting	√											
2	Facility & IT Infrastructure readiness		√										
3	Hardware Delivery & Software Delivery		√										
4	Hardware and Software Installation & Configuration			√									
5	MAXxEMV CIS Bank Integration and complete chip script development as per profile			√									
6	MAXxEMV CIS Solution Deployment				√								
7	Setup of test and chip profile Injection of Keys to HSM Personalize Test and Production Card Validation of Test Card					√							



8	Training						√						
9	Accepance						√						

Table 5: Deployment Plan

