EMV Contactless Library Configuration

Reference Manual

Version 0.9

March 2014

http://www.castech.com.tw

CASTLES TECHNOLOGY

Doc.#

Confidential Level: High

Table of Contents

Revision History

Version	Date	Editor	Description
V0.9	2014.3.25	Weber	Release

WARNING

ABOUT THIS MANUAL

1 Introduction

This document illustrates the format of configuration file used by EMV Contactless Library. The content contains Tag Configuration, CAPK, Parameter, and Revocation.

The configuration file also supports multiple configurations. The user can set multiple configurations into the file and can dynamically switch to load the configuration other than the default active one in the file.

The configuration file adopts the standard XML file format, so that it is easy to be understood and edited by any text editor software.

2 Configuration Content

2.1 Structure

The configuration file must have the follow structure.

```
<?xml version="1.0"?>
<configurationDescriptor version="01">
……
</configurationDescriptor>
```

- <?xml version="1.0"?> indicates that this file is XML format and its format version.
- <configurationDescriptor version=”01”> and </configurationDescriptor version> groups the all configurations.

Below is the description for “configurationDescriptor”.

ELEMENT		
configurationDescriptor		
ATTRIBUTE	VALUE	DESCRIPTION
version	01	Version Number
REMARK		
None		

2.2 Layer 1 – CLConfig for Contactless

The configuration file supports multiple configurations. Each configuration for EMV contactless library is grouped by the label “CLConfig” and “\CLConfig” with its corresponding “index” and “active” values. The index is used as identifier for each configuration, while the active is used to determine which configuration is the default loaded into EMV contactless library during EMV Contactless initialization.

The below shows the active configuration is “Configuration 01”. The other Configurations (02 to 04) are not active.

```
<?xml version="1.0"?>
<configurationDescriptor version="01">
   <CLConfig index="01" active="true">
   …..
   </CLConfig>
   <CLConfig index="02" active="false">
   …..
   </CLConfig>
   <CLConfig index="03" active="false">
   …..
   </CLConfig>
   <CLConfig index="04" active="false">
   …..
   </CLConfig>
</configurationDescriptor>
```

Below is the description for “CLConfig”.

ELEMENT		
CLConfig		
ATTRIBUTE	VALUE	DESCRIPTION
index	01, 02, 03…	Configuration identifier
active	true/false	Indicate if the configuration is active or not
REMARK		
Only one configuration is allowed to be active.		

2.3 Layer 2

In each “CLConfig” it contains the elements ” TagCombination”, “CAPKConfig”, “ParametersConfig”, and “Revocations”. The below shows the basic structure of “CLConfig”.

```
<?xml version="1.0"?>
<configurationDescriptor version="01">
   <CLConfig index="01" active="true">
         <TagCombination>
         ….
         </TagCombination>
         <CAPKConfig>
         ….
         </CAPKConfig>
         <ParametersConfig>
         ….
         </ParametersConfig>
         <Revocations>
         ….
         </Revocations>
   </CLConfig>

   ……

</configurationDescriptor>
```

2.3.1 TagCombination

The format of TagCombination is as below. EMV Contactless Library can maintain up to 64 TagCombinations. Each combination list {AID-KernelID-TxnType} has its own tag setting.

```
<TagCombination>
<Group AID="A0000000041010" KernelID="02" TxnType="00">
    <Item attribute="tlv">5F57009F01009F400500000000009F09020002…….. </Item>
</Group>
<Group AID="A0000000041010" KernelID="02" TxnType="01">
    <Item attribute="tlv">5F57009F01009F400500000000009F09020002…….. </Item>
</Group>
<Group AID="A0000000041010" KernelID="02" TxnType="09">
    <Item attribute="tlv">5F57009F01009F400500000000009F09020002…….. </Item>
</Group>
<Group AID="A0000000041010" KernelID="02" TxnType="20">
    <Item attribute="tlv">5F57009F01009F400500000000009F09020002…….. </Item>
</Group>
<Group AID="A0000000031010" KernelID="03" TxnType="00">
    <Item attribute="tlv">5F57009F01009F400500000000009F09020002…….. </Item>
</Group>
………
</TagCombination>
```

- Below is the description for “Group”.

ELEMENT		
Group		
ATTRIBUTE	VALUE	DESCRIPTION
AID		Registered Application Provider Identifier
KernelID		Kernel ID defined by EMVCo Contactless specification
	= 02	MasterCard
	= 03	Visa
TxnType		Transaction Type
	= 00	Purchase
	= 01	Cash

	= 09	Cashback
	= 20	Refund
REMARK		
None		

- Below is the description for “Item”.

ELEMENT		
Item		
ATTRIBUTE	VALUE	DESCRIPTION
attribute		Set tagCombination as different format
	tlv	TLV format. The data should be TLV1+TLV2+TLV3+…+TLVn ex: 9F400500000000009F09020002 ….
REMARK		
None		

2.3.2 CAPKConfig

CAPKConfig supports the settings for multiple card applications (identified by RID). The CAPKs belonging to the same application are grouped by the label “Group” with specific RID. Each CAPK is grouped by the label “Item” with specific key index (CAPKI).

Each item contains 4 elements, modulus, exponent, expirydata, and hash.

EMV Contactless Library can maintain 30 CAPK setting.

```
<CAPKConfig>
<Group RID="A000000004">
    <Item index="F0">
        <modules>7563C51B5276AA6370AB84055224146458…………... </modules>
        <exponent>03</exponent>
        <expirydata/>
        <hash>AE667445F8DE6F82C38800E5EBABA322F03F58F2</hash>
    </Item>
    <Item index="F5">
        <modules>A6E6FB72179506F860CCCA8C27F99CEC…………... </modules>
        <exponent>010001</exponent>
        <expirydata/>
        <hash>C2239804C8098170BE52D6D5D4159E81CE8466BF</hash>
    </Item>
    …….
</Group>
<Group RID="A000000003">
    <Item index="51">
        <modules>DB5FA29D1FDA8C1634B04DCCFF148AB…………... </modules>
        <exponent>03</exponent>
        <expirydata/>
        <hash>B9D248075A3F23B522FE45573E04374DC4995D71</hash>
    </Item>
……
</Group>
```

- Below is the description for “Group”.

ELEMENT		
Group		
ATTRIBUTE	VALUE	DESCRIPTION
RID		Registered Application Provider Identifier
REMARK		
None		

- Below is the description for “Item”.

ELEMENT		
Item		
ATTRIBUTE	VALUE	DESCRIPTION
index		Certification Authority Public Key Index
REMARK		

- Below are the description for “modulus”, “exponent”, “expirydata”, and “hash”.

ELEMENT		
modules	Certification Authority Public Key Modulus	
exponent	Certification Authority Public Key Exponent	
expirydata	Certification Authority Public Key Expired Date (RFU)	
hash	Hash for Certification Authority Public Key	
ATTRIBUTE	VALUE	DESCRIPTION
REMARK		
The method used and the input data to calculate for the hash data is determined by the user.		

2.3.3 Parameters

The values for the parameters set by the function EMVCL_SetParameter are groups in the below “ParametersConfig”.

```
<ParametersConfig>
    <Item ParaIndex="0002">3A98</Item>
    <Item ParaIndex="100A">00</Item>
    <Item ParaIndex="100B">00</Item>
</ParametersConfig>
```

- Below is the description for “Item”

ELEMENT		
Item		
ATTRIBUTE	VALUE	DESCRIPTION
ParaIndex		Parameter index
	= 0002	Index 0002 : Sale Timeout
	= 100A	Index 100A : UI Type
	= 100B	Index 100B : Visa EUR CL TIG Follow
REMARK		

2.3.4 Revocation

Revocation setting: RID + CAPK Index + Certificate Serial Number

```
<Revocations>
    <Group RID="A000000004">
        <Item CAPKI="F8">
            <SN>000010</SN>
            <SN>000011</SN>
            <SN>000101</SN>
            <SN>000110</SN>
        </Item>
    </Group>
    <Group RID="B012345678">
        <Item CAPKI="F8">
            <SN>000010</SN>
        </Item>
    </Group>
</Revocations>
```

From the example above, the revocations which set to EMVCL kernel are :
A000000004-F8-000010
A000000004-F8-000011
A000000004-F8-000101
A000000004-F8-000110
B012345678-F8-000010

- Below is the description for “Group”

ELEMENT		
Group		
ATTRIBUTE	VALUE	DESCRIPTION
RID		Registered Application Provider Identifier
REMARK		

- Below is the description for “Item”

ELEMENT		
Item		

ATTRIBUTE	VALUE	DESCRIPTION
CAPKI		CAPK Index
REMARK		

- Below are the description for “SN”.

ELEMENT		
SN	Certificate Serial Number	
ATTRIBUTE	VALUE	DESCRIPTION
REMARK		