EMVL2 Application Library Configuration

Reference Manual

Version 1.0

September 2013

http://www.castech.com.tw

CASTLES TECHNOLOGY

Doc.#

Confidential Level: High

Table of Contents

Revision History

Version	Date	Editor	Description
V1.0	2013.9.3	Peggy	Release

WARNING

Information in this document is subject to change without prior notice.

ABOUT THIS MANUAL

1 Introduction

This document illustrates the format of configuration file used by EMVL2 Application Library. The content contains Configuration, CAPK, Application List, Default Terminal Data, and Application Specific Terminal Data.

- Configuration groups CAPK, Application List, Default Terminal Data, and Application Specific Terminal Data.
- CAPK (Certification Authority Public Key) is used for Offline Card Authentication.
- Application List is used to list all the card applications supported by the terminal.
- Default Terminal Data is a set of terminal data that is loaded into EMV kernel during EMV Initialization.
- Application Specific Terminal Data is a set of terminal data depending on each application.

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 – Config

The configuration file supports multiple configurations. Each configuration is grouped by the label “Config” and “\Config” 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 kernel during EMV 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">
   <Config index="01" active="true">
    .
    .
    .
   </Config>
   <Config index="02" active="false">
    .
    .
    .
   </Config>
   <Config index="03" active="false">
    .
    .
    .
   </Config>
   <Config index="04" active="false">
    .
    .
    .
   </Config>
</configurationDescriptor>
```

Below is the description for “Config”.

ELEMENT		
Config		
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 “Config” it contains four elements ”CAPKConfig”, “AppList”, “TerminalConfig” and “AppConfig”. The below shows the basic structure of each “Config”.

```
<?xml version="1.0"?>
<configurationDescriptor version="01">
   <Config index="01" active="true">
      <CAPKConfig>
         .
         .
         .
      </CAPKConfig>
      <AppList>
         .
         .
         .
      </AppList>
      <TerminalConfig>
         .
         .
         .
      </TerminalConfig>
      <AppConfig>
         .
         .
         .
      </AppConfig>
   </Config>
   <Config index="02" active="false">
      <CAPKConfig>
         .
         .
         .
      </CAPKConfig>
      <AppList>
         .
         .
         .
      </AppList>
      <TerminalConfig>
         .
         .
         .
      </TerminalConfig>
      <AppConfig>
         .
         .
         .
      </AppConfig>
   </Config>
</configurationDescriptor>
```


2.3.1 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.

```
<CAPKConfig>
  <Group RID="A000000004">
    <Item index="FE">
      <modules>E76317965175A08BEE510F58830E87B262C70D529803245FA8B
      <exponent>010001</exponent>
      <expirydata/>
      <hash>A9BFE5EF2F9FB4D430F6D4745DB48F2308C89380</hash>
    </Item>
    <Item index="FC">
      <modules>B3296C91F4795BD97112606903407B6EFF3AB39246E91095E51
      <exponent>010001</exponent>
      <expirydata/>
      <hash>15A0FEC7A92C0E19795DF2B0849027610BEF2CE4</hash>
    </Item>
  </Group>
  <Group RID="A000000003">
    <Item index="50">
      <modules>D11197590057B84196C2F4D11A8F3C05408F422A35D702F9010
      <exponent>010001</exponent>
      <expirydata/>
      <hash>B4538DC5FD3416852EAE56154D07341D21E3F4CE</hash>
    </Item>
    <Item index="51">
      <modules>DB5FA29D1FDA8C1634B04DCCFF148ABEE63C772035C79851D35
      <exponent>03</exponent>
      <expirydata/>
      <hash>AF08EFF20DA86FDA1259519B592372A9E0A71E2B</hash>
    </Item>
  </Group>
</CAPKConfig>
```

- 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.

2.3.2 AppList

AppList is used to list all the card applications supported by the terminal. Each supported card application is grouped by “Item” with its assigned unique and sequential index. Each “Item” has 3 elements, “Name”, “AID”, and “ASI”.

```
<AppList>
  <Item index="01">
    <Name>VISA</Name>
    <AID>A0000000031010</AID>
    <ASI>00</ASI>
  </Item>
  <Item index="02">
    <Name>MasterCard</Name>
    <AID>A0000000041010</AID>
    <ASI>00</ASI>
  </Item>
  <Item index="03">
    <Name>JCB</Name>
    <AID>A0000000651010</AID>
    <ASI>00</ASI>
  </Item>
</AppList>
```

- Below is the description for “Item”

ELEMENT		
Item		
ATTRIBUTE	VALUE	DESCRIPTION
index		sequential index
REMARK		

- Below is the description for “Name”, “AID”, “ASI”.

ELEMENT		
Name	Application name	
AID	Application Identifier	
ASI	Application Selection Indicator	
ATTRIBUTE	VALUE	DESCRIPTION
REMARK		

2.3.3 TerminalConfig

TerminalConfig is grouped by “TerminalConfig”, containing a set of terminal data. These terminal data are as default data and used for all the applications listed in AppList. Each “Item” is used for a tag data. Its attributes include the “name” for the human readable tag name, the “tag” for the tag name, and the “attribute” for the data value representation.

```
<TerminalConfig>
  <Item name="TERMINAL CAPABILITIES" tag="9F33" attribute="hex">E0E1C8</Item>
  <Item name="ADDITIONAL TERMINAL CAPABILITIES" tag="9F40" attribute="hex">F000F0A001</Item>
  <Item name="INTERFACE DEVICE (IFD) SERIAL NUMBER" tag="9F1E" attribute="asc">12345678</Item>
  <Item name="TRANSACTION CURRENCY CODE" tag="5F2A" attribute="hex">0949</Item>
  <Item name="TERMINAL COUNTRY CODE" tag="9F1A" attribute="hex">0792</Item>
  <Item name="Default TDOL" tag="DFC0" attribute="hex">9F02065F2A029A039C0195059F3704</Item>
  <Item name="Default DDOL" tag="DFC1" attribute="hex">9F3704</Item>
  <Item name="App Version" tag="9F09" attribute="hex">0084</Item>
  <Item name="Termian Floor Limit" tag="9F1B" attribute="hex">000003E8</Item>
  <Item name="Threshold Value" tag="DFC4" attribute="hex">00000005</Item>
  <Item name="Target Percent" tag="DFC2" attribute="hex">20</Item>
  <Item name="Max Target Percent" tag="DFC3" attribute="hex">40</Item>
  <Item name="TAC Denial" tag="DFC6" attribute="hex">0000000000</Item>
  <Item name="TAC Online" tag="DFC7" attribute="hex">0000000000</Item>
  <Item name="TAC Default" tag="DFC8" attribute="hex">0000000000</Item>
</TerminalConfig>
```

- Below is the description for “Item”

ELEMENT		
Item		
ATTRIBUTE	VALUE	DESCRIPTION
name		The human readable tag name
tag		Tag Name
attribute	hex/asc	Data value representation. “hex” is for binary; “asc” is for ASCII.
REMARK		

2.3.4 AppConfig

"AppConfig" is a set of terminal data depending on each application. The EMVL2 application library will load the default terminal data from "TerminalConfig" into EMV kernel for each application. Afterward, load the data in "AppConfig" into EMV kernel for each application.

Each application specific data are grouped by the label "Group" with the application name, AID, and ASI.

Note that the value of ASI field is ignored.

```
<AppConfig>
  <Group name="VISA" AID="A0000000031010" ASI="00">
    <Item name="App Version" tag="9F09" attribute="hex">008C</Item>
    <Item name="Termian Floor Limit" tag="9F1B" attribute="hex">00002710</Item>
    <Item name="Threshold Value" tag="DFC4" attribute="hex">00000005</Item>
    <Item name="Target Percent" tag="DFC2" attribute="hex">50</Item>
    <Item name="Max Target Percent" tag="DFC3" attribute="hex">99</Item>
    <Item name="TAC Denial" tag="DFC6" attribute="hex">0010000000</Item>
    <Item name="TAC Online" tag="DFC7" attribute="hex">DC4004F800</Item>
    <Item name="TAC Default" tag="DFC8" attribute="hex">DC4000A800</Item>
  </Group>
  <Group name="MasterCard" AID="A0000000041010" ASI="00">
    <Item name="App Version" tag="9F09" attribute="hex">0002</Item>
    <Item name="Termian Floor Limit" tag="9F1B" attribute="hex">000003E8</Item>
    <Item name="Threshold Value" tag="DFC4" attribute="hex">00000000</Item>
    <Item name="Target Percent" tag="DFC2" attribute="hex">0A</Item>
    <Item name="Max Target Percent" tag="DFC3" attribute="hex">14</Item>
    <Item name="TAC Denial" tag="DFC6" attribute="hex">0000000000</Item>
    <Item name="TAC Online" tag="DFC7" attribute="hex">FC508C8800</Item>
    <Item name="TAC Default" tag="DFC8" attribute="hex">FC508C8800</Item>
    <Item name="TAC Default" tag="DFC9" attribute="hex">FC508C0000</Item>
  </Group>
</AppConfig>
```

- Below is the description for "Group"

ELEMENT		
Group		
ATTRIBUTE	VALUE	DESCRIPTION
name		Application name
AID		Application Identifier
ASI		Application Selection Indicator
REMARK		
ASI is ignored		

- Below is the description for "Item"

ELEMENT		
Item		
ATTRIBUTE	VALUE	DESCRIPTION

name		The human readable tag name
tag		Tag Name
attribute	hex/asc	Data value representation. “hex” is for binary; “asc” is for ASCII.

REMARK

