VALUES OF DEVELOPMENT KEYS CPACE

CB DEVELOPMENT CARDS

CPACE

Référence :
Version : 1.1 Date : 07/03/2024

HISTORY

Version	Date	Modifications
1.0	11/01/2024	First version
1.1	07/03/2024	Hash added

Contenu

Table des matières

1 OBJET DU DOCUMENT

The purpose of this document is to specify the values of the various asymmetric and symmetric keys required to use the CPACE development cards distributed by the Elitt test service. This service was initially managed by GIE CB.

2 PRESENTATION DU CONTEXTE DE DEVELOPPEMENT

The purpose of the "CB" cards of Development is to support the development and qualification of electronic payment applications in a dedicated development environment.

Development "CB" boxes are therefore not accepted on field terminals. No flows associated with Development "CB" cards are processed on the e-rsb interbank authorization network.

The keys disseminated through this document are necessary for the dialogue between the "CB" cards of Development and the different elements of the electronic payment system. For example, in the case of a "CB" payment , these development platforms consist of at least:

- A simulator or server Test/ development acquirer to perform the remote parameterization and remote collection of the acceptance system. The remote parameterization allows the distribution of card authentication keys (asymmetric keys) and operating parameters of the CB application of the terminal.
- A simulator or server Test / development issuer containing the symmetric keys and track keys necessary to control the cryptograms issued by the card during a transaction generating a request for authorization.

The values of the symmetric keys present in this document are the so-called "Root". To match the keys present in each of the adapters, a bypass operation may be required according to the applicable specifications

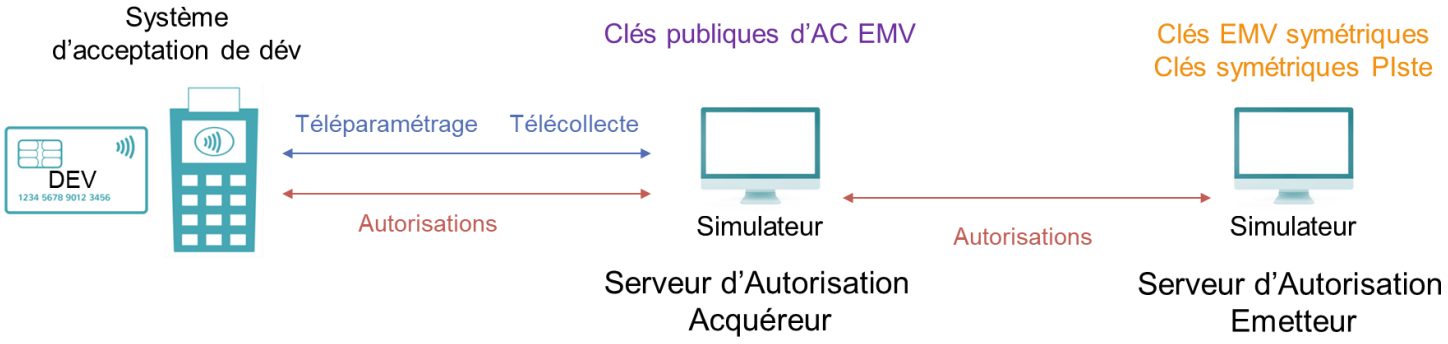

Schéma de mise en œuvre des cartes « CB » de Développement

3 Symmetric EMV keys "CHIP"

3.1 Distribution of symmetric EMV keys by card type

	IMKac	IMKsmc	IMKsmi	IMKdac	IMKidn
CPExxd_V	X	X	X	-	X
CPExxd_MC	X	X	X	-	X

3.2 Role of symmetric EMV keys

IMKac	Key for calculating the certificat of the transaction. Used for the calculation of the ARQC / ARPC	Dual length (128 bits)
IMKsmc	Key for encrypting messages exchanged between the board and SAT or Simulator / Server Test Transmitter	Dual length (128 bits)
IMKsmi	Key for sealing messages exchanged between the card and SAT or Simulator / Server Test Transmitter	Dual length (128 bits)
IMKdac	Not used on the "CB" app	-
IMKidn	Dynamic number calculation key generated during Dynamic offline authentication (DDA/CDA)	Dual length (128 bits))

3.3 Symmetric EMV key values

Key component values are provided in full or decomposed values into 2 forms XOR and DES, depending on the preferred tax method.

The KCV is a control value representative of the key value

Key Type	Component A	Component B	Value	KCV
IMKac				
IMKac *XOR*	255CC40604F259CC 15D32D3F1A0DD782	2DF7B25D41478004 0C146D7F7D6510C4	08AB765B45B5D9C8 19C740406768C746	8C2715
IMKac *DES*	896B730B792537B3 E5B9B923028345E6	B6E203948003317C 2A6FCB41C43C4613		
IMKsmc				
IMKsmc *XOR*	7ECC8F98D77C9F86 550D769CF87E5CF5	8F7A7EAA515FAD3F CEF0184F2EB0868C	F1B6F132862332B9 9BFD6ED3D6CEDA7 9	C375CA
IMKsmc *DES*	DA92DF43DA64B58F 5B020458EAB3AD2C	DF909DFDD5D2511C CDFB8694C110DD45		
IMKsmi				
IMKsmi *XOR*	4E95105C8F6F9DAA FFB87A14379B52CC	40628B4F50C4BD7C D3BA7E571BE14226	0EF79B13DFAB20D6 2C0204432C7A10EA	9EA7F2
IMKsmi *DES*	70FECC2AA0341CA2 8D8627DF56381EFD	4DCBD893FFBE2F12 C5D60815B79FC6A2		
IMKdac				
IMKdac *XOR*	53DE9A6148CC97D3 7A11080C9562DE66	A8E270C7F8A420FB CB3BAC984276EE9C	FB3CEAA6B068B728 B12AA494D71430FA	E9F279
IMKdac *DES*	58DF31A0E577C901 66DFAE5A103C57AB	580A2163F1F81115 7325CA8B485E4A49		
IMKidn				
IMKidn *XOR*	3A52FB68137D9F64 A2B690C7A795C331	DCCD0B0125B7F6A5 E08BC47537FDDC1F	E69FF06936CA69C1 423D54B290681F2E	A3FB71
IMKidn *DES*	6314DF95EA510D37 4E95F67BB2A001A2	A2B6FFFEDCE3E5BD FE6E77E3DF77E699		

4 Symmetrical "Track" Keys

4.1 Distribution of symmetric "Track" keys according to card types

	KPVV9
CPExxd_V	X
CPExxd_MC	X

4.2 Symmetric key values "Track"

Key Type	Component A	Component B	Value	KCV
KPVV Index 9				
KPVV9 *XOR*	4D716CF5D7EF5A3C 3E72CCA277CA833C	B02979B686181FA2 7E459DB4DFC13002	FD58154351F7459E 40375116A80BB33E	443114

5 PUBLIC KEYS CA (CERTIFICATION AUTHORITY)

5.1 Distribution of AC EMV public keys by cards and application type

Type de carte	Application carte	E9h (1984 bits)	EBh (1984 bits)	EAh (1984 bits)
CPExxDd_V_20	CB	X	-	-
	VISA	-	X	-
CPExxDd_MC_20	CB	X	-	-
	MC	-	-	X

5.2 CA public key values

Index: **E9h** (137d)	Length : **1984 bits**	Exponent Public : **03**
Date de fin de validité : **12 2049**		
Modulo	BA15F5F4D131F2302A11299DB3CF80EDE62960AC396F2FAA3E2E535DF0F557758 A2676C1596B5601A17AFA93AE272C03F9F66D0309ACAE8C840FB264B77E7195C CF73F424CC3CB79F756138BDA90CE91C70B79560547BA4EF9C906759F44D79EB 09D82C32D2E73DFE4C51CB71744E77C3CC361D0AD5D395F66A564F9C425F3943 B2FB7E2C24A330511B9B117E7D4FBB11974DC470809B01D74A93FB44F89064FD8 67C1799128FB18DA8D3F82E94118582EB2B5B62E7BCD7CD459880C98C1709846D AD1CF52594D09684F10CA7882AC34AFD5F74ACEE0F564151EB95D8951AA18DB2 D5871CACAD477D28A028664239BC83C36889A03356591	
Hash value	3260330E61967B451DA48609391185BAA94093C2	

Index: **EBh** (146d)	Length: **1984 bits**	Exponent Public : **03**
Date de fin de validité : **12 2049**		
Modulo	A04F8D394D295B83370301F7AF14E8E02BF912D57959F4963FC2F57561C970D7C A5EF84EDA0198F10CE13472F9083AC773CF0A4840E222F83ECA8C890B60ED3B3 E07BAAE394D128391045D69DFDD1E99B52AE4F15B92043456FC4276F1A8A7AE1 A5A03A7ABB4CB50BD868E0126A56CEFFBE714032A9BDABFB55E10C668BB7DF7 3A1795F9CBD6AD6DE7F6E48C6A21812BDF3A3361B8B6DE9A4803DEC51DAC6A5 347BA1A2DA79547848D5D14F1543D1C8F254BD9F213187FD8CA0A48FF1120C91C 951FCF2F87B0E8993FBE35F421B6855AE7A1A926885F62A74ED0C57BE0FB1FDA3 D2C0B6DDDEC426D98CFCCD406D540A4D3F4D07A993F8F5B	
Hash value	1EE7E92494D0CC9C8A0C4602D0F27959602A6A93	

Index: **EAh** (147d)	Length: **1984 bits**	Exponent Public : **03**
Date de fin de validité : **12 2049**		
Modulo	DE95AC71194712BF8A2E4D0512F2AEFE39D6C3AED1142A2B12F99C42A1ECF9A AA3E2DF4F63F0B423EE51CE78C58B26477239E6531502CEDBC7803DC3A4F03C7 3E6ADAA92778CFAB213EA1F3307B88345FC16AB3CD411E21652C1E3A68332337 D87E113B7B43FE0377F7E65546481BBB7CA9FD7E59F877E7DDA081C19E30C989 670F0E8127257F19ACBE79034589963D00AFA5B87B2D1F9F45C9011EFFA2922D8 9F9428AE858EE4DB4B5791C8EE0EBF787F01B57A1CBDB8373ECCD18B9ADEC5D 1D123B114B3423618AB6418615BB08D0AEC5EA2A3218B2C69AF6D615DF7BF3EF B753039C8CBADFFDF41E5706C027112A962D503E20083AAF9	
Hash value	74285D2404467D58956AAF480E873D5A89802AE0	