VALUES OF DEVELOPMENT KEYS

CB DEVELOPMENT CARDS

Référence :
Version : 1.4 Date : 06/03/2026

HISTORY

Version	Date	Modifications
1.0	29/04/2021	Reproduction of document 2.7 BC Editorial update of key indexes
1.1	26/07/2022	Updating the key table for STxxDd_V_18
1.2	19/10/2022	Updated key table AC paragraph 5.1 for STxxDd_V_19 + STxxDd_MC_19
1.3	09/01/2024	Removed information about various batches
1.4	06/03/2026	Explanatory note on hash computation

Contenu

Table des matières

1 PURPOSE OF THE DOCUMENT

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

2 PRESENTATION OF THE DEVELOPMENT CONTEXT

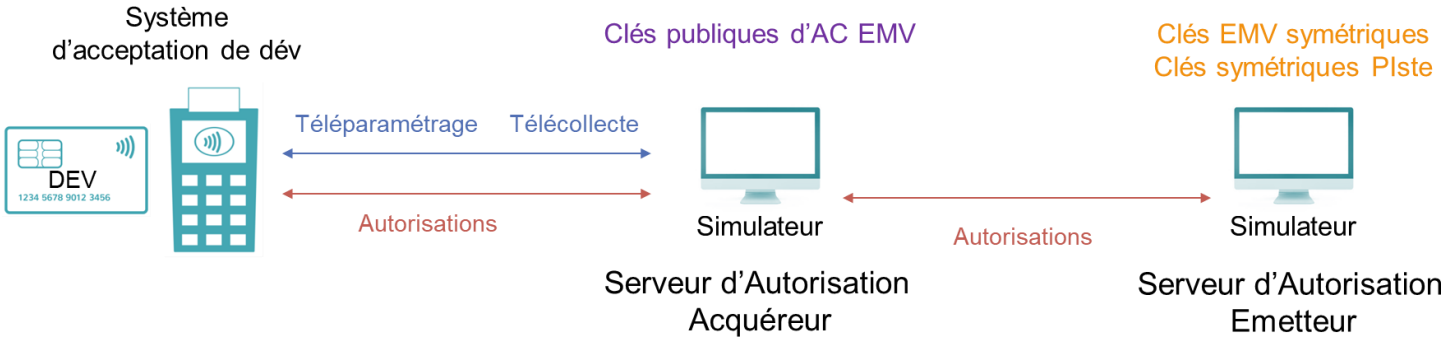
The purpose of the "CB" cards of Development is to support the development and qualification of electronic payment applications in a dedicated development environment.

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



Implementation diagram of the "CB" maps of Development

3 Symmetric EMV keys "CHIP"

3.1 Distribution of symmetric EMV keys by card type

	IMKac	IMKsmc	IMKsmi	IMKdac	IMKidn
STxxd_V	X	X	X	-	X
STxxd_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
STxxd_V	X
STxxd_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	89h (1984 bits)	92h (1984 bits)	93h (1984 bits)
STxxDd_V_19	CB	X	-	-
	VISA	-	X	-
STxxDd_MC_19	CB	X	-	-
	MC	-	-	X

5.2 CA public key values

Index: **89h** (137d)	Longueur : **1984 bits**	Exposant Public : **03**
Date de fin de validité : **12 - 2028**		
Modulo	ACD4E022CC9D7130A6EE1357E147E67900F7222D895CADE5A06595317C9637 2A462E1C7FA134F1CABBAF6D6BEADA4EC29C8C776DFA0EC0ED453C689CE6E7 DFB59924FCE0EDE99A036D5E1B9CADC086322AC04F7665FDCD13C6DEC4B1E3 1FEC3C6FB8B05B788ED62288F458E09437D0C98132C4615AC5F8302C5C781D D78CFE6A826AF047419C18FCEF4AD9464238A5DBA89C5D9939D979507B2E92 CB2455096E242BC8BAAEA1FE7F4DFDED2BDD36F6E282DD41C668CF5F0A5B7C D36D2A2D1E539A1B0A63524478BB4A196C31D55B3D46097F067A36FD41E739 7443F74A515C8129F22D52CF9C318B119842652D2D02E9CB8E901A8657033B
Hash value	106177EBF846D1416C7CEA85D596D73C11781504

Index: **92h** (146d)	Longueur : **1984 bits**	Exposant Public : **03**
Date de fin de validité : **12 - 2028**		
Modulo	A946476541122A04D506729311968F839DF5A97EB8125AEC92B3AA97868E56 20860CF09C676B1F25F4D7F07B2D30B2D91BE7C7D3974CD22B86A1B2616D26 44FB209E487A812D9C03CD7FF048D234C20DAC70D321F5E2B636270462A24D A969913E8F3E5A8D8FD9FA4AEE3303153C66A2837D9527853F091A805F0867 273F451A1B9177E31C639153E82361B9A2503F5A1D45E232930F660BCAFB3F 97C6A2A4F8AB81E731EC59D751529366C1AB8CDD378327479EB8EC49207158 D9B4AF544CAB46EDE866F70B049D036FE019DA6CF4E47EE0D4D63ADF9CB65C CE56C7340DB8BE492A4FDD0EAA86F05498616D392175C8822A4BBE76AF62E5
Hash value	1A5568F7FC2855E6C9F65073A807454C93620CF0

Index: **93h** (147d)	Longueur : **1984 bits**	Exposant Public : **03**
Date de fin de validité : **12 - 2028**		
Modulo	BD88F77B3D4BF7F0CFC558D9903DB64571169905D3A8DBCAC6FF9DAAA10FF6 2BB4D0C9FDEB4F0FAA982D4A2DD184FCAEED0D998D36C84A135A11903A83F5 2235D8B396223821001923A4BC2F320946EB02435E547F786BAE34267C2630 49A3017687F5FA6AD4EB4E66AE744E4840850998E2174EDA1A12FA9AAE55F9 9FB71885B751B925A394948E82C174E75DFA2B424441402EF3D0B1BCD8B433 5BB432454057FCC401DFA9F74F4AA6E1B36846142BF05EBFFF3041F18EFD21 6A4E47EE0C6F17772403D427E6DB9214F4BD7E94D3052901AB49BDA5C0E63E 08825C3DC56B6A52E07D803DA063CF4C04F814F10D61DDAFC989140188AFAD
Hash value	5726DAE1476C54671EE68C1E4F10427297EF14ED

Explanatory note on hash computation :
The hash of the CA key related to scheme mastercard / visa for CB development cards is computed using EMV method with RID CB instead of RID mastercard / visa for intellectual property reasons.