

---

# KEY VALUES DEVELOPMENT

---

## CB DEVELOPMENT CARDS

---

---

Reference:

Version: 1.2

Date: 10/19/2022

---

## SUIVI OF AMENDMENTS

| Version | Date       | Changes  |
|---------|------------|--|
| 1.0     | 29/04/2021 | Reproduction of document 2.7 BC<br>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<br>STxxDd_V_19 + STxxDd_MC_19 |
|         |            |  |

|                            |             |              |                  |            |
|----------------------------|-------------|--------------|------------------|------------|
| VALUES OF DEVELOPMENT KEYS | Reference : | Version:1. 2 | Date :19/10/2022 | Page :2/11 |
|----------------------------|-------------|--------------|------------------|------------|

## Content

|          |  |                      |
|----------|--|----------------------|
| <b>S</b> | .....  | <b>UIVI</b>          |
|          | .....  | <b>OF AMENDMENTS</b> |
|          | .....  | <b>2</b>             |
| <b>1</b> | <b>PURPOSE OF DOCUMENT</b> .....                                 | <b>4</b>             |
| <b>2</b> | <b>PRESENTATION</b> .....  | <b>OF THE</b>        |
|          | .....  | <b>DEVELOPMENT</b>   |
|          | <b>CONTEXT 4</b> .....   |                      |
| <b>3</b> | <b>Symmetric</b> .....   | <b>EMV</b>           |
|          | <b>keys "CHIP"</b> .....   | <b>"</b>             |
|          | <b>5</b> .....   |                      |
| 3.1      | Distribution of symmetric EMV keys by card types                 |                      |
|          | 5  |                      |
| 3.2      | Role of symmetric EMV keys                                       | 5                    |
| 3.3      | Symmetric values   | EMV key 6            |
| <b>4</b> | <b>Symmetrical keys</b> .....                                    | <b>"Track</b>        |
|          | <b>"</b> .....   | <b>7</b>             |
| 4.1      | Distribution of " symmetric " Track keys according to card types |                      |
|          | 7  |                      |
| 4.2      | " symmetric key  | Track " values7      |
| <b>5</b> | <b>PUBLIC KEYS OF</b> .....                                      | <b>AC</b>            |
|          | <b>(AUTHORITY</b> .....  | <b>OF</b>            |
|          | <b>THIS</b> .....  | <b>RTIFICATION)</b>  |
|          | <b>8</b> .....   |                      |
| 5.1      | Distribution of AC EMV public keys by cards and application type |                      |
|          |  | 8                    |
| 5.2      | CA Public Values   | Key 10               |



## 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

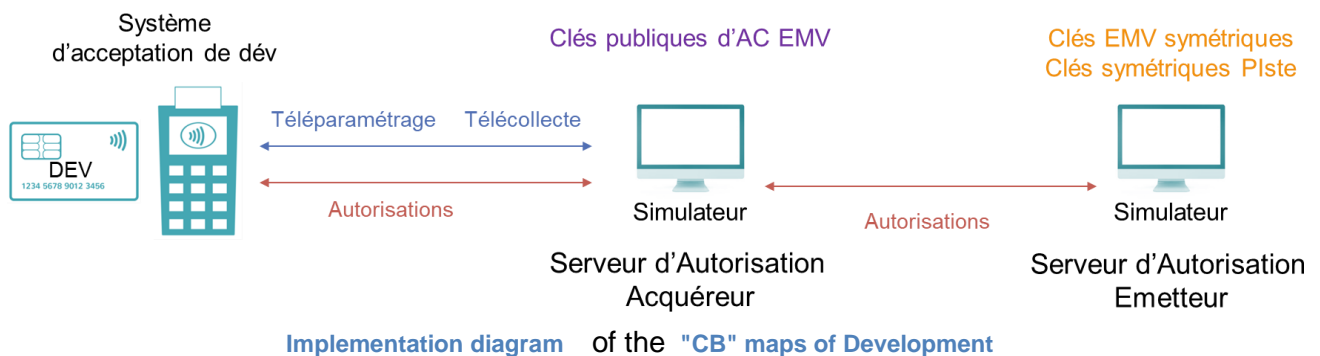
The purpose of the "CB" cards of Development is to support the development and qualification of electronic payment applications in a dedicated development environment.

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.



|                            |             |              |                  |            |
|----------------------------|-------------|--------------|------------------|------------|
| VALUES OF DEVELOPMENT KEYS | Reference : | Version:1. 2 | Date :19/10/2022 | Page :4/11 |
|----------------------------|-------------|--------------|------------------|------------|

### 3 Symmetric EMV keys "CHIP"

#### 3.1 Distribution of symmetric EMV keys by card type

|          | IMKac | IMKs™ | IMKsmi | IMKdac | IMKidn |
|----------|-------|-------|--------|--------|--------|
| VAxxd_V  | X     | X     | X      | -      | X      |
| VAxxd_MC | X     | X     | X      | -      | X      |
| 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) |
| IMKs™  | 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 board 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    |
|-----------------------|--|--------------------------------------|--|--------|
| <b>IMKac</b>          |  |                                      |  |        |
| IMKac<br><i>XOR</i>   | 255CC40604F259CC<br>15D32D3F1A0DD782         | 2DF7B25D41478004<br>0C146D7F7D6510C4 | 08AB765B45B5D9C8<br>19C740406768C746     | 8C2715 |
| IMKac<br><i>SOME</i>  | 896B730B792537B3<br>E5B9B923028345E6         | B6E203948003317C<br>2A6FCB41C43C4613 |  |        |
| <b>IMKs™</b>          |  |                                      |  |        |
| IMKs™<br><i>XOR</i>   | 7ECC8F98D77C9F86<br>550D769CF87E5CF5         | 8F7A7EAA515FAD3F<br>CEF0184F2EB0868C | F1B6F132862332B9<br>9BFD6ED3D6CEDA7<br>9 | C375CA |
| IMKs™<br><i>SOME</i>  | DA92DF43DA64B58<br>E<br>5B020458EAB3AD2<br>C | DF909DFDD5D2511C<br>CDFB8694C110DD45 |  |        |
| <b>IMKsmi</b>         |  |                                      |  |        |
| IMKsmi<br><i>XOR</i>  | 4E95105C8F6F9DAA<br>FFB87A14379B52CC         | 40628B4F50C4BD7C<br>D3BA7E571BE14226 | 0EF79B13DFAB20D6<br>2C0204432C7A10EA     | 9EA7F2 |
| IMKsmi<br><i>SOME</i> | 70FECC2AA0341CA2<br>8D8627DF56381EFD         | 4DCBD893FFBE2F12<br>C5D60815B79FC6A2 |  |        |
| <b>IMKdac</b>         |  |                                      |  |        |
| IMKdac<br><i>XOR</i>  | 53DE9A6148CC97D3<br>7A11080C9562DE66         | A8E270C7F8A420FB<br>CB3BAC984276EE9C | FB3CEAA6B068B72<br>8<br>B12AA494D71430FA | E9F279 |
| IMKdac<br><i>SOME</i> | 58DF31A0E577C901<br>66FDAE5A103C57AB         | 580A2163F1F81115<br>7325CA8B485E4A49 |  |        |
| <b>IMKidn</b>         |  |                                      |  |        |
| IMKidn<br><i>XOR</i>  | 3A52FB68137D9F64<br>A2B690C7A795C331         | DCCD0B0125B7F6A5<br>E08BC47537FDCC1E | E69FF06936CA69C1<br>423D54B290681F2E     | A3FB71 |
| IMKidn<br><i>SOME</i> | 6314DF95EA510D37<br>4E95F67BB2A001A2         | A2B6FFFEDCE3E5BD<br>FE6E77E3DF77E699 |  |        |

|                            |             |              |                  |            |
|----------------------------|-------------|--------------|------------------|------------|
| VALUES OF DEVELOPMENT KEYS | Reference : | Version:1. 2 | Date :19/10/2022 | Page :6/11 |
|----------------------------|-------------|--------------|------------------|------------|

## 4 Symmetrical "Track" keys

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

|          | KPVV9 |
|----------|-------|
| VAxxd_V  | X     |
| VAxxd_MC | X     |
| STxxd_V  | X     |
| STxxd_MC | X     |

### 4.2 Symmetric key values "Track"

| Key Type            | Component A                          | Component B                          | Value                                | KCV    |
|---------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------|
| <b>KPVV Index 9</b> |                                      |                                      |                                      |        |
| KPVV9<br><i>XOR</i> | 4D716CF5D7EF5A3C<br>3E72CCA277CA833C | B02979B686181FA2<br>7E459DB4DFC13002 | FD58154351F7459E<br>40375116A80BB33E | 443114 |



## 5 PUBLIC KQ KEYS ( CERTIFICATION AUTHORITY)

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

| Card Type         |   | Application map | 86h<br>(1408 bits) | 88h<br>(1408 bits) | 91h<br>(1408 bits) | 89h<br>(1984 bits) | 92h<br>(1984 bits) | 93h<br>(1984 bits) |
|-------------------|---|-----------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| VA11d_V_17        | Rank 1, 2, 4, 5, 6, 7, 8<br>,<br>9,<br>10 | CB              | X                  | -                  | -                  | -                  | -                  | -                  |
|                   |   | VISA            | -                  | X                  | -                  | -                  | -                  | -                  |
|                   | Rank 3                                    | CB              | -                  | -                  | -                  | -                  | -                  | -                  |
|                   |   | VISA            | -                  | -                  | -                  | -                  | -                  | -                  |
| VA10d_MC_17       | Rank 1, 2, 4, 5, 6, 7, 8<br>,<br>9,<br>10 | CB              | X                  | -                  | -                  | -                  | -                  | -                  |
|                   |   | MC              | -                  | -                  | X                  | -                  | -                  | -                  |
|                   | Rank 3                                    | CB              | -                  | -                  | -                  | -                  | -                  | -                  |
|                   |   | MC              | -                  | -                  | -                  | -                  | -                  | -                  |
| STxxDd_V_17 / 18  |   | CB              | X                  | -                  | -                  | -                  | -                  | -                  |
|                   |   | VISA            | -                  | X                  | -                  | -                  | -                  | -                  |
| STxxDd_MC_17 / 18 |   | CB              | X                  | -                  | -                  | -                  | -                  | -                  |
|                   |   | MC              | -                  | -                  | X                  | -                  | -                  | -                  |
| STxxDd_V_19       |   | CB              | -                  | -                  | -                  | X                  | -                  | -                  |
|                   |   | VISA            | -                  | -                  | -                  | -                  | X                  | -                  |
| STxxDd_MC_19      |   | CB              | -                  | -                  | -                  | X                  | -                  | -                  |
|                   |   | MC              | -                  | -                  | -                  | -                  | -                  | X                  |
| VA11d_V_18        | Rank 1, 6, 7, 8, 9, 10                    | CB              | X                  | -                  | -                  | -                  | -                  | -                  |
|                   |   | VISA            | -                  | X                  | -                  | -                  | -                  | -                  |
|                   | Rank 2, 4, 5                              | CB              | -                  | -                  | -                  | X                  | -                  | -                  |
|                   |   | VISA            | -                  | -                  | -                  | -                  | X                  | -                  |

|             |                        |      |          |   |          |          |   |          |
|-------------|------------------------|------|----------|---|----------|----------|---|----------|
|             | Rank 3                 | CB   | -        | - | -        | -        | - | -        |
|             |                        | VISA | -        | - | -        | -        | - | -        |
| VA11d_MC_18 | Rank 1, 6, 7, 8, 9, 10 | CB   | <b>X</b> | - | -        | -        | - | -        |
|             |                        | MC   | -        |   | <b>X</b> | -        | - | -        |
|             | Rank 2, 4, 5           | CB   | -        | - | -        | <b>X</b> | - | -        |
|             |                        | MC   | -        | - | -        | -        | - | <b>X</b> |
|             | Rank 3                 | CB   | -        | - | -        | -        | - | -        |
|             |                        | MC   | -        | - | -        | -        | - | -        |
|             |                        |      |          |   |          |          |   |          |

|                            |             |              |                   |            |
|----------------------------|-------------|--------------|-------------------|------------|
| VALUES OF DEVELOPMENT KEYS | Reference : | Version:1. 2 | Date : 19/10/2022 | Page :9/11 |
|----------------------------|-------------|--------------|-------------------|------------|

## 5.2 CA Public Key Values

|  |  |                              |
|--|--|------------------------------|
| Index: <b>86h</b> (135d)                       | Length : <b>1408 bits</b>  | Public Exhibitor : <b>03</b> |
| <b>Expiry date : 12 - 2024 in verification</b> |  |                              |
| Modulo   | D7686F54E4C65DFC162B455D612D918739059BA2445B79A1BD070A448CE062<br>BD0C6E7E5683223490C66AB4B808A4D3A59E276D8B779925752FCE140BA136<br>C0E05C0BDBAE0A9F751B9340BA88603967F43D40A04CFD652503B78234D188<br>F6B21D5A3AE99BB84B2E50235EF9D7ED7A70A117806778E9F0D1B3DADC1CE9<br>B25C2DDE07B3B6E1DE487E0F7E9FFEDDD4D15255CEC453631EF47E14B498A<br>3<br>53844802A4A25A62B9918E9A12A00BF887AAD4799E |                              |
| Hash value                                     | 96A690811AA2196E3D1090CE0149AA2935C04FE2   |                              |

|  |   |                              |
|--|---|------------------------------|
| Index: <b>88h</b> (136d)                       | Length : <b>1408 bits</b>   | Public Exhibitor : <b>03</b> |
| <b>Expiry date : 12 - 2024 in verification</b> |   |                              |
| Modulo   | BE969CF59368DB109C0C8DE478216BE629F14CB84271EEA812362B463CA0BF<br>B8029F2EF15DAABA453D8C531E334BD0CD7BC1E09770A4EA9BC056EB482E0A<br>B<br>9FF603627AC4020BE4E8B458F4B120E4B98E73823275D0E2773392DD3B7368<br>DE012F0B958A967B9C2D4E28B2AD59AC326D8D3544B95D36C3D55E5B76E586<br>7E7EBBF8CE8645B5B7415E9A316035E98082C75A1A6FE7BD80EC4186C6179C<br>B0269C25AC82142FDC373F4FA78343949F33E034A5 |                              |
| Hash value                                     | 9653E24AC28DC6FF571ADC9B9DDE51FA00A27C14  |                              |

|  |  |                              |
|--|--|------------------------------|
| Index: <b>91h</b> (145d)                       | Length : <b>1408 bits</b>  | Public Exhibitor : <b>03</b> |
| <b>Expiry date : 12 - 2024 in verification</b> |  |                              |
| Modulo   | B42596687324BE4005D22B878616082889E1CA951299A66612FF8C374F927B<br>ACBE0FBA4960FD04C44D459A20CD09FB562364DB5B5A064A48F7980F71C5A9<br>1CA1D41522FC01CFC05E9A72DEA0526791270CCBB72BBD79DF67841AF8648C<br>C2CA7EB2D1212C24F64C6976332A6A903253D8C6C3F5F71147B9ECB3778DBF<br>079C513041CC379BB8C5DB27739241942DDE0A1B675CC7479B311F41729288<br>890E17A0451DBB2812CE2FD5C9B124A5E3889D09DF |                              |
| Hash value                                     | 2B296272087EA8506083554ACF7061421C0C551D   |                              |

|                            |             |              |                  |             |
|----------------------------|-------------|--------------|------------------|-------------|
| VALUES OF DEVELOPMENT KEYS | Reference : | Version:1. 2 | Date :19/10/2022 | Page :10/11 |
|----------------------------|-------------|--------------|------------------|-------------|

|  |   |                              |
|--|---|------------------------------|
| Index: <b>89h</b> (137d)                       | Length : <b>1984 bits</b>   | Public Exhibitor : <b>03</b> |
| <b>Expiry date : 12 - 2028 in verification</b> |   |                              |
| Modulo   | ACD4E022CC9D7130A6EE1357E147E67900F7222D895CADE5A06595317C9637<br>2A462E1C7FA134F1CABBAF6D6BEADA4EC29C8C776DFA0EC0ED453C689CE6<br>E7<br>DFB59924FCE0EDE99A036D5E1B9CADC086322AC04F7665FD0CD13C6DEC4B1E<br>3<br>1FEC3C6FB8B05B788ED62288F458E09437D0C98132C4615AC5F8302C5C781D<br>D78CFE6A826AF047419C18FCEF4AD9464238A5DBA89C5D9939D979507B2E92<br>CB2455096E242BC8BAAEA1FE7F4DFDED2BDD36F6E282DD41C668CF5F0A5B7<br>C<br>D36D2A2D1E539A1B0A63524478BB4A196C31D55B3D46097F067A36FD41E739<br>7443F74A515C8129F22D52CF9C318B119842652D2D02E9CB8E901A8657033B |                              |
| Hash value                                     | 106177EBF846D1416C7CEA85D596D73C11781504  |                              |

|  |  |                              |
|--|--|------------------------------|
| Index: <b>92h</b> (146d)                       | Length : <b>1984 bits</b>  | Public Exhibitor : <b>03</b> |
| <b>Expiry date : 12 - 2028 in verification</b> |  |                              |
| Modulo   | A946476541122A04D506729311968F839DF5A97EB8125AEC92B3AA97868E56<br>20860CF09C676B1F25F4D7F07B2D30B2D91BE7C7D3974CD22B86A1B2616D26<br>44FB209E487A812D9C03CD7FF048D234C20DAC70D321F5E2B636270462A24D<br>A969913E8F3E5A8D8FD9FA4AEE3303153C66A2837D9527853F091A805F0867<br>273F451A1B9177E31C639153E82361B9A2503F5A1D45E232930F660BCAFB3F<br>97C6A2A4F8AB81E731EC59D751529366C1AB8CDD378327479EB8EC49207158<br>D9B4AF544CAB46EDE866F70B049D036FE019DA6CF4E47EE0D4D63ADF9CB65<br>C<br>CE56C7340DB8BE492A4FDD0EAA86F05498616D392175C8822A4BBE76AF62E5 |                              |
| Hash value                                     | 1A5568F7FC2855E6C9F65073A807454C93620CF0   |                              |

|  |  |                              |
|--|--|------------------------------|
| Index: <b>93h</b> (147d)                       | Length : <b>1984 bits</b>  | Public Exhibitor : <b>03</b> |
| <b>Expiry date : 12 - 2028 in verification</b> |  |                              |
| Modulo   | BD88F77B3D4BF7F0CFC558D9903DB64571169905D3A8DBCAC6FF9DAAA10FF6<br>2BB4D0C9FDEB4F0FAA982D4A2DD184FCAEED0D998D36C84A135A11903A83F<br>5<br>2235D8B396223821001923A4BC2F320946EB02435E547F786BAE34267C2630<br>49A3017687F5FA6AD4EB4E66AE744E4840850998E2174EDA1A12FA9AAE55F9<br>9FB71885B751B925A394948E82C174E75DFA2B424441402EF3D0B1BCD8B433<br>5BB432454057FCC401DFA9F74F4AA6E1B36846142BF05EBFFF3041F18EFD21<br>6A4E47EE0C6F17772403D427E6DB9214F4BD7E94D3052901AB49BDA5C0E63E<br>08825C3DC56B6A52E07D803DA063CF4C04F814F10D61DDAFC989140188AFAD |                              |
| Hash value                                     | 5726DAE1476C54671EE68C1E4F10427297EF14ED   |                              |

|                            |             |              |                  |             |
|----------------------------|-------------|--------------|------------------|-------------|
| VALUES OF DEVELOPMENT KEYS | Reference : | Version:1. 0 | Date :29/04/2021 | Page:11 /11 |
|----------------------------|-------------|--------------|------------------|-------------|