VALEURS DES CLES DE DEVELOPPEMENT

CARTES DE DEVELOPPEMENT

Référence :

Version : 1.0 Date : 29/04/2021

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1.0	29/04/2021	Reprise du document 2.7 CB Mise à jour éditoriale des index de clés

Contenu

1 OBJET DU DOCUMENT

Ce document a pour but de préciser les valeurs des différentes clés asymétriques et symétriques nécessaires à l'utilisation des cartes de développement diffusées par le service cartes de test d'Elitt. Ce service était géré initialement par le GIE CB.

2 PRESENTATION DU CONTEXTE DE DEVELOPPEMENT

Les cartes « CB » de Développement ont pour objectif d'accompagner le développement et la qualification d'applications monétiques dans un environnement de développement dédié.

Les cartes "CB" de Développement ne sont donc pas acceptées sur les terminaux du terrain. Aucun flux associé aux cartes « CB » de Développement n'est traité sur le réseau d'autorisation interbancaire e-rsb.

Les clés diffusées au travers de ce document sont nécessaires au dialogue entre les cartes « CB » de Développement et les différents éléments du système monétique. Par exemple, dans le cas d'un paiement « CB », ces plateformes de développement se composent d'au moins :

- Un simulateur ou serveur Acquéreur de test / développement permettant d'effectuer le téléparamétrage et la télécollecte du système d'acceptation.
  Le téléparamétrage permet la diffusion des clés d'authentification carte (clés asymétriques) et des paramètres de fonctionnement de l'application CB du terminal.
- Un simulateur ou serveur Emetteur de test / développement contenant les clés symétriques et clés pistes nécessaires au contrôle des cryptogrammes émis par la carte lors d'une transaction engendrant une demande d'autorisation.

Les valeurs des clés symétriques présentes dans ce document sont les valeurs dites « Racine ». Pour correspondre aux clés présentent dans chacune des cartes, une opération de dérivation peut être nécessaire conformément aux spécifications applicables.

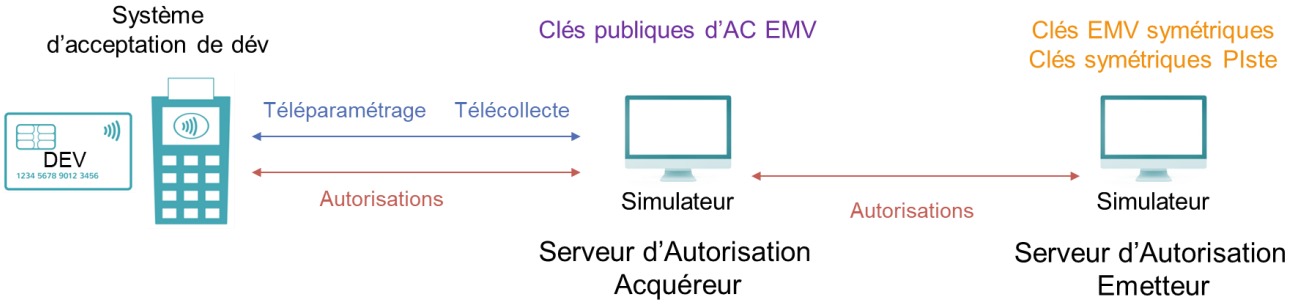

Schéma de mise en œuvre des cartes « CB » de Développement

3 Clés EMV symétriques « PUCE »

3.1 Répartition des clés EMV symétriques selon les types de cartes

	IMKac	IMKsmc	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 Rôle des clés EMV symétriques

IMKac	Clé de calcul du certifcat de la transaction. Utilisée pour le calcul de l'ARQC / ARPC	Longueur double (128 bits)
IMKsmc	Clé de chiffrement de messages échangés entre la carte et le SAT ou Simulateur / Serveur Emetteur de Test	Longueur double (128 bits)
IMKsmi	Clé de scellement de messages échangés entre la carte et le SAT ou Simulateur / Serveur Emetteur de Test	Longueur double (128 bits)
IMKdac	Non utilisé sur l'application « CB »	-
IMKidn	Clé de calcul du numéro dynamique généré lors de l'authentification offline Dynamique (DDA/CDA)	Longueur double (128 bits)

3.3 Valeurs des clés EMV symétriques

Les valeurs des composantes de clés sont fournies en valeurs complètes ou décomposées sous 2 formes : XOR et DES, selon la méthode d'imposition privilégiée.
Le KCV est une valeur de contrôle représentative de la valeur de la clé.

Type de Clé	Composante A	Composante B	Valeur	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 9BFD6ED3D6CEDA79	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 Clés symétriques « Piste »

4.1 Répartition des clés symétriques « Piste » selon les types de cartes

	KPVV9
VAxxd_V	X
VAxxd_MC	X
STxxd_V	X
STxxd_MC	X

4.2 Valeurs des clés symétriques « Piste »

Type de Clé	Composante A	Composante B	Valeur	KCV
KPVV Indice 9				
KPVV9 *XOR*	4D716CF5D7EF5A3C 3E72CCA277CA833C	B02979B686181FA2 7E459DB4DFC13002	FD58154351F7459E 40375116A80BB33E	443114

5 CLES PUBLIQUES D'AC (AUTORITE DE CERTIFICATION)

5.1 Répartition des clés publiques d'AC EMV selon les cartes et type d'application

Type de carte		Application carte	86h (1408 bits)	88h (1408 bits)	91h (1408 bits)	89h (1984 bits)	92h (1984 bits)	93h (1984 bits)
VA11d_V_17	Rang 1, 2, 4, 5, 6, 7, 8, 9, 10	CB	X	-	-	-	-	-
		VISA	-	X	-	-	-	-
	Rang 3	CB	-	-	-	-	-	-
		VISA	-	-	-	-	-	-
VA10d_MC_17	Rang 1, 2, 4, 5, 6, 7, 8, 9, 10	CB	X	-	-	-	-	-
		MC	-	-	X	-	-	-
	Rang 3	CB	-	-	-	-	-	-
		MC	-	-	-	-	-	-
ST10Dd_V_17 / 18		CB	X	-	-	-	-	-
		VISA	-	X	-	-	-	-
STxxDd_MC_17 / 18		CB	X	-	-	-	-	-
		MC	-	-	X	-	-	-
VA11d_V_18	Rang 1, 6, 7, 8, 9, 10	CB	X	-	-	-	-	-
		VISA	-	X	-	-	-	-
	Rang 2, 4, 5	CB	-	-	-	X	-	-
		VISA	-	-	-	-	X	-
	Rang 3	CB	-	-	-	-	-	-
		VISA	-	-	-	-	-	-

VA10d_MC_18	Rang 1, 6, 7, 8, 9, 10	CB	X	-	-	-	-	-
		MC	-		X	-	-	-
	Rang 2, 4, 5	CB	-	-	-	X	-	-
		MC	-	-	-	-	-	X
	Rang 3	CB	-	-	-	-	-	-
		MC	-	-	-	-	-	-

5.2 Valeurs des clés publiques d'AC

Index: **86h** (135d)	Longueur : **1408 bits**	Exposant Public : **03**
Date de fin de validité : **12 - 2024 en vérification**		
Modulo	D7686F54E4C65DFC162B455D612D918739059BA2445B79A1BD070A448CE062 BD0C6E7E5683223490C66AB4B808A4D3A59E276D8B779925752FCE140BA136 C0E05C0BDBAE0A9F751B9340BA88603967F43D40A04CFD652503B78234D188 F6B21D5A3AE99BB84B2E50235EF9D7ED7A70A117806778E9F0D1B3DADC1CE9 B25C2DDE07B3B6E1DE487E0F7E9FFEDDD4D15255CEC453631EF47E14B498A3 53844802A4A25A62B9918E9A12A00BF887AAD4799F
Hash value	96A690811AA2196E3D1090CE0149AA2935C04FE2	

Index: **88h** (136d)	Longueur : **1408 bits**	Exposant Public : **03**
Date de fin de validité : **12 - 2024 en vérification**		
Modulo	BE969CF59368DB109C0C8DE478216BE629F14CB84271EEA812362B463CA0BF B8029F2EF15DAABA453D8C531E334BDCD7BC1E09770A4EA9BC056EB482E0AB 9FF603627AC4020BE4E8B458F4B120E4B98E73823275D0E2773392DD3B7368 DE012F0B958A967B9C2D4E28B2AD59AC326D8D3544B95D36C3D55E5B76E586 7E7EBBF8CE8645B5B7415E9A316035E98082C75A1A6FE7BD80EC4186C6179C B0269C25AC82142FDC373F4FA78343949F33E034A5
Hash value	9653E24AC28DC6FF571ADC9B9DDE51FA00A27C14	

Index: **91h** (145d)	Longueur : **1408 bits**	Exposant Public : **03**
Date de fin de validité : **12 - 2024 en vérification**		
Modulo	B42596687324BE4005D22B878616082889E1CA951299A66612FF8C374F927B ACBE0FBA4960FD04C44D459A20CD09FB562364DB5B5A064A48F7980F71C5A9 1CA1D41522FC01CFC05E9A72DEA0526791270CCBB72BBD79DF67841AF8648C C2CA7EB2D1212C24F64C6976332A6A903253D8C6C3F5F71147B9ECB3778DBF 079C513041CC379BB8C5DB27739241942DDE0A1B675CC7479B311F41729288 890E17A0451DBB2812CE2FD5C9B124A5E3889D09DF
Hash value	2B296272087EA8506083554ACF7061421C0C551D	

Index: **89h** (137d)	Longueur : **1984 bits**	Exposant Public : **03**
Date de fin de validité : **12 - 2028 en vérification**		
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 en vérification**		
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 en vérification**		
Modulo	BD88F77B3D4BF7F0CFC558D9903DB64571169905D3A8DBCAC6FF9DAAA10FF6 2BB4D0C9FDEB4F0FAA982D4A2DD184FCAEED0D998D36C84A135A11903A83F5 2235D8B396223821001923A4BC2F320946EB02435E547F786BAE34267C2630 49A3017687F5FA6AD4EB4E66AE744E4840850998E2174EDA1A12FA9AAE55F9 9FB71885B751B925A394948E82C174E75DFA2B424441402EF3D0B1BCD8B433 5BB432454057FCC401DFA9F74F4AA6E1B36846142BF05EBFFF3041F18EFD21 6A4E47EE0C6F17772403D427E6DB9214F4BD7E94D3052901AB49BDA5C0E63E 08825C3DC56B6A52E07D803DA063CF4C04F814F10D61DDAFC989140188AFAD	
Hash value	5726DAE1476C54671EE68C1E4F10427297EF14ED	