
VALEURS DES CLES DE DEVELOPPEMENT CPACE

CARTES DE DEVELOPPEMENT CPACE

Référence :

Version : 1.1

Date : 07/03/2024

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1.0	11/01/2024	1ère version carte DEV CSPACE ELITT
1.1	07/03/2024	Ajout hash

Contenu

Table des matières

1	OBJET DU DOCUMENT	4
2	PRESENTATION DU CONTEXTE DE DEVELOPPEMENT.....	4
3	Clés EMV symétriques « PUCE »	5
3.1	Répartition des clés EMV symétriques selon les types de cartes	5
3.2	Rôle des clés EMV symétriques	5
3.3	Valeurs des clés EMV symétriques	6
4	Clés symétriques « Piste »	7
4.1	Répartition des clés symétriques « Piste » selon les types de cartes	7
4.2	Valeurs des clés symétriques « Piste »	7
5	CLES PUBLIQUES D'AC (AUTORITE DE CERTIFICATION).....	7
5.1	Répartition des clés publiques d'AC EMV selon les cartes et type d'application.....	7
5.2	Valeurs des clés publiques d'AC.....	8

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 CPACE 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 présentes dans chacune des cartes, une opération de dérivation peut être nécessaire conformément aux spécifications applicables.

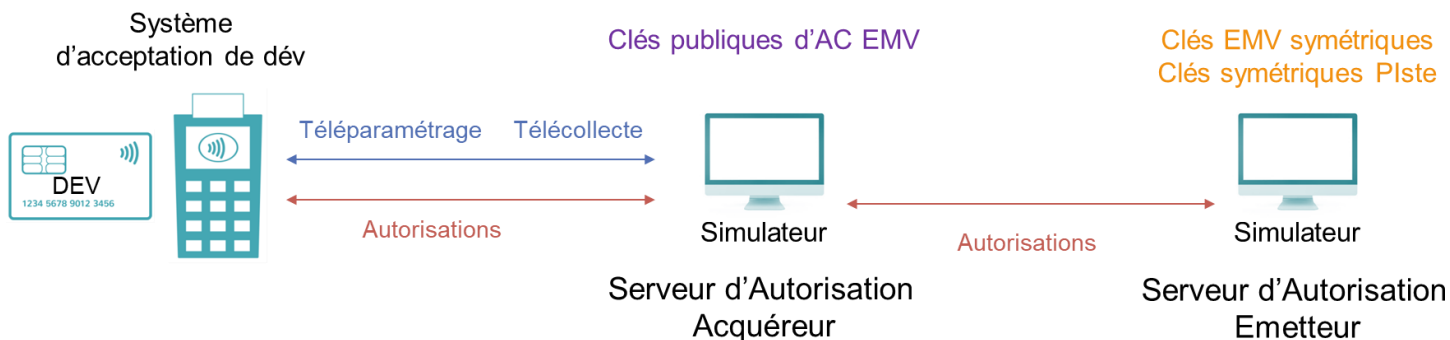


Schéma de mise en œuvre des cartes « CB » de Développement

VALEURS DES CLES DE DEVELOPPEMENT CPACE	Référence :	Version :1.1	Date :07/03/2024	Page :4 / 8
---	-------------	--------------	------------------	-------------

3 Clés EMV symétriques « PUCE »

3.1 Répartition des clés EMV symétriques selon les types de cartes

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

3.2 Rôle des clés EMV symétriques

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

4 Clés symétriques « Piste »

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

	KPVV9
CPExxd_V	X
CPExxd_MC	X

4.2 Valeurs des clés symétriques « Piste »

Type de Clé	Composante A	Composante B	Valeur	KCV
KPVV Indice 9				
KPVV9 <i>XOR</i>	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	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 Valeurs des clés publiques d'AC

Index: E9h (137d)	Longueur : 1984 bits	Exposant Public : 03
Date de fin de validité : 12 2049		
Modulo	BA15F5F4D131F2302A11299DB3CF80EDE62960AC396F2FAA3E2E535DF0F557758A2676C1596B5601A17AFA93AE272C03F9F66D0309ACAE8C840FB264B77E7195CCF73F424CC3CB79F756138BDA90CE91C70B79560547BA4EF9C906759F44D79EB09D82C32D2E73DFE4C51CB71744E77C3CC361D0AD5D395F66A564F9C425F3943B2FB7E2C24A330511B9B117E7D4FBB11974DC470809B01D74A93FB44F89064FD867C1799128FB18DA8D3F82E94118582EB2B5B62E7BCD7CD459880C98C1709846DAD1CF52594D09684F10CA7882AC34AFD5F74ACEE0F564151EB95D8951AA18DB2D5871CACAD477D28A028664239BC83C36889A03356591	
Hash value	3260330E61967B451DA48609391185BAA94093C2	

Index: EBh (146d)	Longueur : 1984 bits	Exposant Public : 03
Date de fin de validité : 12 2049		
Modulo	A04F8D394D295B83370301F7AF14E8E02BF912D57959F4963FC2F57561C970D7CA5EF84EDA0198F10CE13472F9083AC773CF0A4840E222F83ECA8C890B60ED3B3E07BAAE394D128391045D69DFDD1E99B52AE4F15B92043456FC4276F1A8A7AE1A5A03A7ABB4CB50BD868E0126A56CEFFBE714032A9BDABFB55E10C668BB7DF73A1795F9CBD6AD6DE7F6E48C6A21812BDF3A3361B8B6DE9A4803DEC51DAC6A5347BA1A2DA79547848D5D14F1543D1C8F254BD9F213187FD8CA0A48FF1120C91C951FCF2F87B0E8993FBE35F421B6855AE7A1A926885F62A74ED0C57BE0FB1FDA3D2C0B6DDDEC426D98CFCCD406D540A4D3F4D07A993F8F5B	
Hash value	1EE7E92494D0CC9C8A0C4602D0F27959602A6A93	

Index: EAh (147d)	Longueur : 1984 bits	Exposant Public : 03
Date de fin de validité : 12 2049		
Modulo	DE95AC71194712BF8A2E4D0512F2AEFE39D6C3AED1142A2B12F99C42A1ECF9AAA3E2DF4F63F0B423EE51CE78C58B26477239E6531502CEDBC7803DC3A4F03C73E6ADAA92778CFAB213EA1F3307B88345FC16AB3CD411E21652C1E3A68332337D87E113B7B43FE0377F7E65546481BBB7CA9FD7E59F877E7DDA081C19E30C989670F0E8127257F19ACBE79034589963D00AFA5B87B2D1F9F45C9011E9FA2922D89F9428AE858EE4DB4B5791C8EE0EBF787F01B57A1CBDB8373ECCD18B9ADEC5D1D123B114B3423618AB6418615BB08D0AEC5EA2A3218B2C69AF6D615DF7BF3EFB753039C8CBADFFDF41E5706C027112A962D503E20083AAF9	
Hash value	74285D2404467D58956AAF480E873D5A89802AE0	