



**BNTRA/CN03/GT8**

**NORME « APPLICATION MULTISERVICES CITOYENNE »**

**IMPLÉMENTATION SUR TÉLÉPHONE MOBILE**



#### LISTE DES RÉVISIONS

Version	Date	Modifications
1	22/04/2021	Première version.
2	07/05/2021	Modifications mineures
2.1	01/12/2021	Ajout préambule : cas d'usage
2.2	03/12/2021	Modification des données dynamiques
2.3	03/12/2021	Modification éditoriales mineures
2.4	26/09/2022	Simplification de l'encodage (suppression de l'ASN.1)
2.5	2/06/2023	Optimisation de la structure de données Aztec remplacé par QR Code Binaire remplacé par texte Base45
2.6	6/06/2023	Modification éditoriale mineure

## Table des matières

I.	Introduction .....	5
I.1	Cas d'usage .....	5
I.2	Objet du document.....	5
I.3	Définitions.....	6
I.4	Présentation des technologies envisagées.....	6
I.4.1	NFC (« Near Field Communication ») .....	6
I.4.2	BLE (« Bluetooth Low Energy ») .....	7
I.4.3	CB2D (code-barres à deux dimensions) .....	8
II.	Modes d'accès .....	9
II.1	Échanges en NFC.....	9
II.2	Affichage du CB2D .....	9
II.3	Échanges en BLE .....	10
III.	Données en CB2D ou en BLE.....	11
III.1	Présentation .....	11
III.2	Structure de données .....	12
III.3	Unicité des identifiants prédéfinis.....	14
III.4	Taille des données encodées .....	15
III.5	Cryptographie .....	15
IV.	Sécurité .....	16
IV.1	Menaces.....	16
IV.2	Contre-mesures .....	16
IV.2.1	Traçabilité.....	16
IV.2.2	Contrefaçon et clonage .....	17
V.	Outils .....	18
V.1	Cryptographie : OpenSSL.....	18
V.2	Encodage et décodage.....	18
VI.	Évolutions possibles.....	19
VI.1	Utilisation de données circonstancielles .....	19
VI.1.1	Geste volontaire en BLE.....	19
VI.1.2	Amélioration contre le clonage en CB2D ou en BLE .....	19
VI.1.3	Obtention de données circonstancielles pour la lecture en CB2D ou BLE.....	19
VI.2	NFC : mode PKI de Calypso Prime Revision 3 .....	20
VI.3	Données CB2D/BLE accessibles en NFC.....	20
VII.	Annexes.....	21
VII.1	La norme AMC .....	21
VII.1.1	Publication.....	21
VII.1.2	Secteurs d'activité .....	21

VII.1.3	Structures de données .....	21
VII.1.4	Conteneur Calypso.....	22
VII.1.5	Niveaux de sécurité .....	22
VII.1.6	Types d'AMC.....	22
VII.2	Exemples.....	23
VII.2.1	Clés utilisées .....	23
VII.2.2	Données.....	24
VII.2.3	Taille apparente .....	26
VII.2.4	Exemple 1 : trois secteurs (1, 4, 7), pas d'authentification.....	26
VII.2.5	Exemple 2 : trois secteurs (1, 4, 7), authentification statique seulement.....	27
VII.2.6	Exemple 3 : trois secteurs (1, 4, 7), authentification complète .....	27
VII.2.7	Exemple 4 : huit secteurs (1, 4, 7, 11 à 14, 22), pas d'authentification.....	28
VII.2.8	Exemple 5 : huit secteurs (1, 4, 7, 11 à 14, 22), authentification statique seulement .....	28
VII.2.9	Exemple 6 : huit secteurs (1, 4, 7, 11 à 14, 22), authentification complète.....	29
VII.2.10	Exemple 7 : 16 secteurs (1, 4, 7 à 14, 20 à 25), authentification complète .....	30
VII.2.11	Comparaison .....	31

## I. Introduction

### I.1 Cas d'usage

Il est suggéré de distinguer les catégories principales suivantes, qui vont définir des niveaux de sécurité ; ce qui peut être illustré avec les domaines du loisir, du tourisme, de la culture et du transport mais qu'on peut retrouver dans tous les domaines : à ce stade on part du principe que dans tous les cas **on est en mode connecté avec vérification des droits en ligne**.

1. Les *usages uniques* (occasionnel unique) : il s'agit du ticket dématérialisé ; le risque de fraude est faible et il ne semble pas nécessaire d'authentifier le porteur.
2. Les *usages multiples* mais à durée limitée (occasionnel multiple) : par exemple un Pass touristique qui donne accès à plusieurs sites pendant une courte durée ; en général le nombre d'accès à un même site est limité et donc le risque de fraude est relativement faible et le porteur est souvent anonyme. Cependant, il peut être préférable de se protéger contre la duplication de l'identifiant en utilisant des identifiants dynamiques.
3. Les *usages fréquents et multiples* (fréquent multiple) : en général il s'agit d'un abonnement **donnant** droit pendant une période longue (un an par exemple) à des usages multiples. Dans ce cas, il est impératif de se protéger contre la duplication de l'identifiant et d'utiliser un identifiant dynamique, sauf si on utilise une identification du porteur au moment de l'usage (photo) ou une méthode d'authentification forte (3D secure, notifications sur l'application, etc.). **Exemple** : abonnements culturels, sportifs ou de loisirs.

On ajoute **trois** remarques :

- La fréquence des usages est à pondérer par la valeur des droits associés. Par exemple, la valeur du droit d'accès à un unique événement sportif peut atteindre plusieurs centaines (voire milliers) d'euros.
- Quand **il** est en mode connecté, **même sans authentification des identifiants le système est naturellement protégé** contre la fabrication frauduleuse d'identifiants, puisque seuls les identifiants authentiques pointent sur un compte en ligne : si **un** identifiant n'est pas correct il n'y a pas de compte en ligne ; le plus important est de générer des identifiants non prédictibles. Néanmoins, un authentifiant protège contre un éventuel clonage des identifiants par accès frauduleux à la base de données d'un service, car il est absent de cette base de données : un attaquant interne ne peut pas produire de clone qui serait accepté à la lecture car il ne connaît pas l'authentifiant.
- Pour beaucoup de projets il est **capital** de ne pas obliger les fournisseurs de services à changer leurs équipements de contrôle et, dans le cas de la technologie code 2D, l'équipement le plus répandu est la douchette en mode émulation clavier : la contrainte **étant** que le code 2D doit **être composé de caractères** ASCII imprimables, et au plus 128.

**Outre les cartes Calypso et les téléphones mobiles, est également pris en compte le cas d'un code-barres imprimé**, en considérant que la surface d'impression peut être faible, jusqu'à un carré de 2 cm de côté.

### I.2 Objet du document

La norme française décrivant l'Application Multiservices Citoyenne, ou « AMC », a été publiée en octobre 2020 par l'AFNOR sous la référence « NF P 99-508 », suite aux travaux du groupe de travail GT8 de la commission de normalisation CN03 du BNTRA.

Le groupe de travail ADCET consacré à l'AMC a validé le besoin de pouvoir utiliser le téléphone mobile comme support des identifiants AMC ; c'est une exigence pour la mobilité servicielle<sup>1</sup> ou la billetterie interconnectée. Le téléphone **peut** alors être présenté aux terminaux accepteurs AMC en lieu et place d'une carte AMC.

La gestion des identifiants personnalisés, des contrats AMC et du journal AMC n'est toutefois pas retenue pour l'utilisation sur téléphone.

<sup>1</sup> « MaaS » ou « Mobility as a service ».

a supprimé: qui donne

a supprimé: ...). Par exemple des

a supprimé: ou a des sports et

a supprimé: deux

a supprimé: on

a supprimé: il n'y a pas de raison d'authentifier l'identifiant puisqu'il pointe

a supprimé: l'identifiant

a supprimé: vital

a supprimé: c'est

a supprimé: alors avoir une taille limitée

a supprimé: En fait il semble qu'une AMC dans un téléphone mobile sauf pour les cas d'usage de la catégorie 1 peut être gérée par une application qui prendra en charge les fonctions de sécurité et qui produira l'identifiant qui va bien pour le service concerné. ¶

a supprimé: ;

a supprimé: pouvant

Plusieurs technologies de communication entre téléphones et terminaux existent, chacune avec ses avantages et ses limites. Pour porter l'AMC, l'ADCET a envisagé :

- **NFC** *Near Field Communication*
- **BLE** *Bluetooth Low Energy*
- **CB2D** *Codes-barres à deux dimensions*

Ce document est une contribution de l'ADCET au GT8. Il propose une solution de mise en œuvre de ces technologies, en vue d'un ajout à une nouvelle version de la norme AMC, en s'appuyant autant que possible sur les solutions déjà décrites par les normes publiées ou en cours d'élaboration.

### I.3 Définitions

Une AMC implémentée dans un téléphone est appelée **AMC mobile**.

L'AMC est gérée dans le téléphone par une **application mobile** ou « **app** »<sup>2</sup>.

### I.4 Présentation des technologies envisagées

#### I.4.1 NFC (« Near Field Communication »)

La solution la plus proche d'une carte Calypso est le mode « émulation carte » de la technologie NFC. Dans le téléphone, l'AMC est logée dans un conteneur Calypso Prime Revision 3 identique à celui des cartes Calypso.

Ce conteneur Calypso est implémenté soit dans une app HCE<sup>3</sup>, soit dans un élément sécurisé du téléphone (« eSE », « embedded secure element »).



Le NFC présente plusieurs avantages :

- portée réduite (quelques centimètres) permettant de matérialiser la volonté de l'utilisateur d'accéder au service qui lui est proposé (« geste volontaire ») ;
- pertinence et efficacité démontrée ;
- meilleure solution pour les services acceptant déjà des cartes AMC ;
- meilleure ergonomie, car il suffit d'approcher le téléphone du terminal (éventuellement écran allumé)<sup>4</sup> ;
- possibilité d'authentifier le support sans SAM (depuis Calypso Prime Revision 3.3, voir chapitre VI.2) ;
- compatibilité avec les terminaux AMC déployés<sup>5</sup>.

#### Utilisation d'un élément sécurisé

Dans un élément sécurisé (eSE), une AMC est conforme à la totalité de la norme AMC actuelle. Le conteneur Calypso est implémenté par une applet Java Card chargée dans l'élément sécurisé, selon un processus défini et contrôlé par le propriétaire de l'élément sécurisé.

2 « Application » recouvre des significations différentes dans les expressions « Application Multiservice Citoyenne », « application Calypso » et « application mobile ». Afin de limiter les risques de confusion, la notion de « conteneur Calypso » se substitue à celle d'« application Calypso » dans ce document.

3 « Host Card Emulation », technologie d'émulation de carte sans contact gérée par le système d'exploitation du téléphone.

4 Selon les possibilités du téléphone, son paramétrage, et les choix de l'utilisateur, une transaction NFC peut être réalisée écran éteint ou téléphone seulement allumé.

5 Pour ceux compatibles NFC (par exemple conformes CEN TS/16794 ou NFC Forum).

a supprimé: celles envisagées par

a supprimé: sont

a supprimé: )

a déplacé vers le bas [1]

a supprimé: De nombreux téléphones ne permettent pas cette solution : principalement les produits Apple<sup>5</sup>, mais également les quelques modèles de téléphones Android ne disposant pas d'une interface NFC.<sup>¶</sup>

a supprimé: SIM ou

a supprimé: )

Elle est accessible via l'interface NFC du téléphone, comme pour une carte sans contact Calypso.

Elle est également accessible via une app, comme pour une carte insérée dans un lecteur à contacts. L'app assume alors les fonctions d'un terminal AMC n'ayant pas de SAM, ou connecté à un serveur éventuellement équipé d'un SAM.

#### Utilisation d'une application mobile HCE

Dans une app, une AMC est conforme à la spécification Calypso HCE, qui est l'adaptation de la spécification Calypso Prime Revision 3 aux contraintes de la technologie HCE.

Elle est accessible via l'interface NFC du téléphone, comme pour une carte sans contact Calypso <sup>7</sup>.

Elle est également accessible via une app, qui assume alors les fonctions d'un terminal AMC n'ayant pas de SAM, ou connecté à un serveur éventuellement équipé d'un SAM.

Deux documents décrivent le conteneur Calypso HCE et sa mise œuvre :

- Spécification Calypso HCE, référence CNA <sup>8</sup> : *141113-CalypsoHCEApplication*.
- Guide d'implémentation Calypso HCE, référence CNA : *150422-CalypsoHCEGuidelines*.

#### Principale limite du NFC

Bien que munis d'une interface NFC, de nombreux téléphones empêchent ou rendent très complexe son utilisation. C'est principalement le cas des produits Apple, qui ne proposent pas le mode HCE, et qui imposent de fortes contraintes techniques et contractuelles à l'utilisation de l'élément sécurisé du téléphone <sup>9</sup>.

De plus, certains modèles de téléphones Android d'entrée de gamme ne disposent pas d'une interface NFC.

#### I.4.2 BLE (« Bluetooth Low Energy »)

BLE, acronyme de « Bluetooth Low Energy », est une technologie radiofréquences, très économe en énergie.

Cette technologie, apparue en 2011, est désormais disponible avec la très grande majorité des téléphones <sup>10</sup>.

Le terminal pourrait sélectionner automatiquement l'AMC concernée, comme avec une carte Calypso.



#### Principales limites du BLE

- L'ergonomie nécessite d'être étudiée afin d'éviter la validation d'un téléphone proche de celui présenté, par exemple si deux personnes se suivent à l'entrée du service. Un geste volontaire de l'utilisateur est obligatoire pour identifier le téléphone.
- L'ergonomie est moins fluide que pour la solution NFC. L'utilisateur doit allumer le téléphone, ouvrir l'app appropriée, confirmer l'accès sur l'écran du téléphone (et éventuellement approcher le téléphone du terminal).

<sup>7</sup> Sauf pour les fonctions de personnalisation et de rechargement qui ne peuvent être réalisées qu'en interaction avec un serveur de sécurité.

<sup>8</sup> Calypso Networks Association, <https://calypsonet.org/>.

<sup>9</sup> Apple pourrait l'autoriser pour des réseaux de transport majeurs, comme celui d'Île-de-France. Mais cela pourrait ne pas être étendu à d'autres services ou à d'autres collectivités.

<sup>10</sup> Seuls n'en disposent pas les très anciens téléphones (Apple jusqu'à l'iPhone 4, Android jusqu'à sa version 4.2) ou de très bas coût.

a déplacé (et inséré) [1]: Principale limite du NFC

a supprimé: <object>

- Certains utilisateurs ont des réticences à activer les fonctionnalités Bluetooth de leur téléphone, par exemple pour préserver la charge de la batterie, ou pour des craintes relatives aux données personnelles.

#### I.4.3 CB2D (code-barres à deux dimensions)

La seule solution applicable à tous les téléphones consiste à afficher un code-barres à deux dimensions (« CB2D »), lisible de façon automatique et permettant d'identifier le compte de l'utilisateur du service.

Comme avec le NFC, la distance de lecture est faible, ce qui permet de matérialiser la volonté de l'utilisateur d'accéder au service qui lui est proposé (« geste volontaire »).



##### Principales limites du CB2D

- L'ergonomie est la moins bonne : l'utilisateur doit allumer le téléphone, ouvrir l'app appropriée, lui faire afficher le CB2D, et enfin présenter correctement l'écran du téléphone au lecteur optique du terminal.
- La quantité d'information qu'il est possible de transmettre au terminal est limitée, par la lisibilité du code-barres, qui dépend de sa taille totale (pas trop grande) et de la taille de ses modules élémentaire (pas trop petite).
- Il n'est pas possible de sélectionner automatiquement les données à afficher, par exemple entre plusieurs AMC, ou entre AMC et INTERCODE. Pour ce type de sélection une autre source d'information est nécessaire, ce qui pourrait dégrader l'expérience client.
- Dans le domaine des services, en particulier du tourisme, les terminaux existants sont peu adaptés aux codes-barres 2D. Une solution courante est l'utilisation d'un lecteur optique qui émule une saisie au clavier, et transmet donc principalement des caractères alphanumériques.

a supprimé: <object>

a supprimé: Pour le transport public, la norme INTERCODE a récemment été étendue avec l'utilisation d'un CB2D au format Aztec<sup>11</sup>.¶

a supprimé: taille des informations

a supprimé: <sup>12</sup> (moins

a supprimé: 600 octets, soit environ 350 octets

a supprimé: données utiles compte tenu

a supprimé: la présence de certificats cryptographiques

a supprimé: compliquer

a supprimé: Les

a supprimé: pourraient être inadaptés à cet usage (beaucoup de données, format Aztec, données binaires). Pour certains, une mise à jour logicielle pourrait ainsi être insuffisante (une étude préliminaire fournirait une meilleure connaissance de ces terminaux, en particulier pour ceux utilisant un

a supprimé: ).¶  
Gestion des données AMC¶  
Afin que l'organisation

a supprimé: données soit identique quelles que soient la nature du support et la technologie de communication, le conteneur est de type Calypso et conforme au chapitre 7 de la norme AMC. Les caractéristiques des structures de fichiers et des structures de données dépendent du périmètre de service, comme indiqué dans la norme AMC

a supprimé: Les structures de fichier Calypso définies par la norme AMC n'ayant aucune restriction de lecture, les données de l'AMC peuvent être fournies sous forme de CB2D ou en BLE.¶ S'il est implémenté dans un élément sécurisé du téléphone, le conteneur est totalement conforme à la norme AMC actuelle.¶ Sinon, le conteneur implémente la spécification Calypso HCE (à l'exception de la communication NFC lorsque le téléphone ne la permet pas). Ce conteneur est supervisé par connexion à un serveur Calypso HCE.¶  
Date de fin de validité HCE du conteneur¶  
Comme spécifié par le standard Calypso HCE, les deux octets de poids fort du numéro de série Calypso indiquent la date après laquelle le conteneur doit être rejeté<sup>13</sup>, en nombre de demi-journées écoulées depuis le 1<sup>er</sup> janvier 2010 à 0h00.



## II. Modes d'accès

### II.1 Échanges en NFC

En NFC, les terminaux AMC ne distinguent pas l'AMC mobile d'une AMC sur carte Calypso<sup>14</sup>. Les données de l'app Mobile sont telles que décrites dans la norme AMC actuelle.

Un terminal capable de traiter l'AMC d'une carte sans contact Calypso est donc également capable de traiter l'AMC d'un téléphone mobile NFC (sous réserve de la capacité du terminal à communiquer avec un objet NFC quelconque, non spécifique à Calypso ou à l'AMC).

### II.2 Affichage du CB2D

Les données décrites au chapitre III sont représentées avec un code-barres ayant les caractéristiques suivantes :

Paramètres	Valeurs
Symbologie	QR Code (ISO/IEC 18004)
Encodage	Alphanumérique (mode 2)
Taux de correction d'erreur <sup>16</sup>	« M » (« medium », soit environ 15%) recommandé
Zone vierge (« quiet zone »)	Au moins 4 modules sur les quatre côtés
Taille des modules	0,381 mm à 0,508 mm (15 à 20 mil <sup>17</sup> ) recommandé
Taille maximale du code-barres <sup>18</sup> , zone vierge comprise	40 mm × 40 mm recommandé
Nombre maximal de modules (hors zone vierge)	69 × 69 modules recommandé <sup>19</sup>
Taille maximale des données	483 caractères alphanumériques <sup>20</sup>

#### Résolution d'impression et d'affichage

Il est recommandé que les modules soient imprimés ou affichés avec au moins 4 × 4 points par module, et si possible avec 5 × 5 points par module ou plus.

Pour optimiser la lisibilité du CB2D, il est recommandé d'utiliser un nombre entier de points par module lorsque le système de génération de codes-barres le permet, sans compromettre significativement les autres recommandations.

14 Dans le cas d'un conteneur Calypso HCE, seule la clé de débit (clé 3) est disponible. De plus, la date de fin de validité HCE doit être contrôlée, de préférence avec une session sécurisée Calypso pour l'authentifier.

16 Le taux de correction d'erreur est déterminant pour la lisibilité du code-barres. Néanmoins, augmenter ce taux augmente le nombre de modules, ce qui peut conduire à une réduction de la lisibilité. Selon le type de dégradations attendues, le taux « Q » (« quartile », soit environ 25%) pourrait donner de meilleurs résultats.

17 1 mil = 1/1000 de pouce = 0,0254 mm.

18 Plus un code-barres 2D est grand, plus il risque d'être nécessaire de l'éloigner du lecteur afin qu'il entre en totalité dans le champ de vision. La distance de lecture est limitée par la focale de l'optique, ou éventuellement par la forme du terminal.

19 Nombre le plus proche correspondant à un code-barres de 40 mm × 40 mm ayant des modules de 20 mil.

20 Taille correspondant à un code-barres de 69 × 69 modules avec le taux de correction d'erreur « M ».

**a supprimé:** IV.3.1

**a supprimé:** encodées telles-quelles, en tant que données binaires, dans...

**a supprimé:** Aztec

**a supprimé:** AZTEC (ISO/IEC 24778)

**Commenté [SDI2]:** Retours d'intégrateurs en billettique transport (verbatim, source GT4) :

- 35 à 40 mm max. (au-delà, difficultés de lecture). 50 x 50 est trop grand.
- La taille max est une contrainte car une taille plus grande impose de reculer le CB2D. 40 mm est déjà trop grand, le plafond est de 37,6 mm
- 15 à 20 mm est l'optimum
- Recommandé : 40 mm. Maximum à ne pas dépasser : 45 mm
- Nos CB2D ont des tailles allant jusqu'à 57 mm. Même en-dehors de ce cas extrême, une taille de 50 mm est assez répandue.

Autre source, certificat Covid européen : "diagonale comprise entre 35 mm et 60 mm" (§5.2.2 de "R:\Docs Publiques\Normes-Standards-Documents\BarCodes\QR Code\Certificat Covid UE\_CELEX 32021D1073 FR TXT.pdf").

**a supprimé:** Nombre maximal de modules

**Commenté [SDI3]:** « M » est recommandé par GS1 ("R:\Docs Publiques\Normes-Standards-Documents\BarCodes\QR Code\GS1\_QR codes imprimés pour smartphone, recommandations d'usage pour la mise en oeuvre d'un symbole de qualité en environnement ouvert.pdf").

« Q » (25%) est recommandé pour le certificat Covid européen ("R:\Docs Publiques\Normes-Standards-Documents\BarCodes\QR Code\Certificat Covid UE\_CELEX 32021D1073 FR TXT.pdf").

Augmenter le taux augmente le nombre de modules, ce qui peut conduire à une réduction de la lisibilité. Ici M a été retenu, comme pour GS1, mais selon le type de dégradations attendues le taux Q pourrait donner de meilleurs résultats.

**Commenté [SDI4]:** Voir GS1 au chapitre 2.6.9, « Global Document Type Identifier for document control » & tableau 5.12.3.9-1.

Également (et semble contradictoire), voir encadré en page 10 de "R:\Docs Publiques\Normes-Standards-Documents\BarCodes\QR Code\GS1\_QR codes imprimés pour smartphone, recommandations d'usage pour la mise en oeuvre d'un symbole de qualité en environnement ouvert.pdf".

**Commenté [SDI5]:** Retours d'intégrateurs en billettique transport (verbatim, source GT4) :

- 35 à 40 mm max. (au-delà, difficultés de lecture). 50 x 50 est trop grand.
- La taille max est une contrainte car une taille plus grande impose de reculer le CB2D. 40 mm est déjà trop grand, le plafond est de 37,6 mm
- 15 à 20 mm est l'optimum
- Recommandé : 40 mm. Maximum à ne pas dépasser : 45 mm
- Nos CB2D ont des tailles allant jusqu'à 57 mm. Même en-dehors de ce cas extrême, une taille de 50 mm est assez répandue.

Autre source, certificat Covid européen : "diagonale comprise entre 35 mm et 60 mm" (§5.2.2 de "R:\Docs Publiques\Normes-Standards-Documents\BarCodes\QR Code\Certificat Covid UE\_CELEX 32021D1073 FR TXT.pdf").

#### Couleurs

Il est recommandé que les codes-barres soient imprimés ou affichés en noir sur fond blanc, afin d'obtenir un contraste aussi élevé que possible.

Il est recommandé de ne pas inverser le contraste des couleurs (support non garanti pour tous les lecteurs).  
Exemple :



### II.3 Échanges en BLE

En BLE, le terminal AMC émet en permanence un message indiquant sa disponibilité pour une transaction AMC mobile.

Dès que le téléphone se trouve à proximité du terminal, l'app AMC lui envoie les données décrites au chapitre **III**.

Les détails de ces processus d'identification en tant que terminal AMC, et de transfert des données AMC, seront définis dans une version ultérieure de la norme.

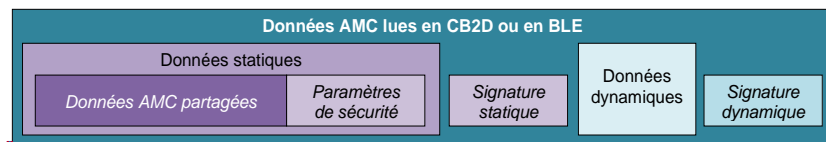
**a supprimé:** IV.3.1 (en tant que données binaires).

### III. Données en CB2D ou en BLE

#### III.1 Présentation

Les données lues sont décomposées en deux parties :

- **Données statiques et leur signature**, présentes pour l'impression et pour l'affichage. Elles sont générées par un système central. Elles incluent les données AMC partagées avec le mode NFC, ainsi que des paramètres de sécurité (clé publique du téléphone). La signature statique authentifie les données statiques.
- **Données dynamiques et leur signature**, présentes seulement pour l'affichage. Elles sont générées périodiquement par le téléphone. Elles incluent essentiellement la date et l'heure courante. La signature dynamique authentifie l'ensemble des données, statiques et dynamiques<sup>21</sup>; elle est calculée par le téléphone.



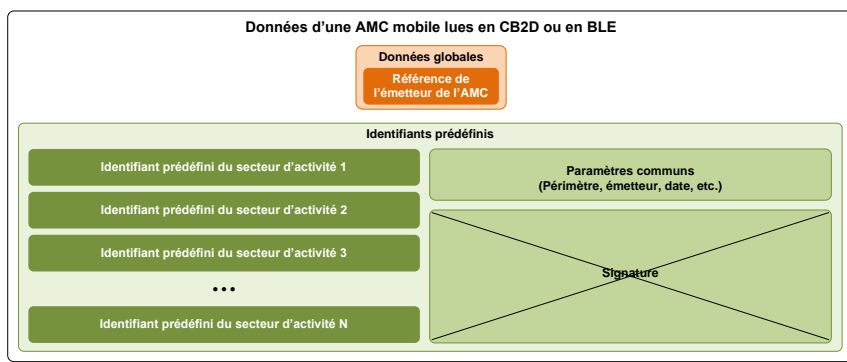
#### Données AMC partagées (données statiques)

Les données statiques d'une AMC mobile transmises aux terminaux AMC en CB2D ou en BLE sont :

- la référence de l'émetteur de l'AMC,
- les identifiants prédéfinis et leurs paramètres communs (sans la signature des données, qui est transmise en NFC, comme pour une carte Calypso).

Pour limiter autant que possible la quantité de données, les autres données AMC contenues dans le téléphone ne sont pas transmises en CB2D et BLE.

Ces données sont authentifiées par une *signature statique*, calculée par un système central, qui assure la même fonction que la signature des identifiants prédéfinis de la norme AMC (cette signature AMC est absente des données transmises afin de réduire leur taille de 64 octets).



21 Néanmoins, vérifier seulement la signature dynamique n'est pas suffisant. Pour que la signature dynamique soit acceptée, il faut que la signature statique soit correcte, car c'est elle qui authentifie la clé publique du téléphone (utilisée pour vérifier la signature dynamique).

a supprimé: ; elle est calculée par le système central

a supprimé:

Code de champ modifié

a supprimé: statiques

a supprimé: AMC

a supprimé: <#>les attributs du conteneur,¶  
les données globales,¶

a supprimé:

¶

Encodage¶

Format¶

Code de champ modifié

**Notation**

Sauf indication contraire, les valeurs numériques sont en notation décimale.

La notation hexadécimale est 'XXXX'h, par exemple 'A23B'h pour la valeur décimale 41 531.

**III.2 Structure de données**

Les données du CB2D comportent deux parties principales :

- Un entête constitué d'une chaîne de caractères alphanumériques qui référence l'AMC et qui indique la version de la structure des données qui suivent.
- Les données elles-mêmes, qui sont constituées d'une suite d'octets ordonnés par index croissant et commençant à l'index 0, encodés en texte Base45<sup>22</sup>. Les données sont différentes selon que le CB2D est imprimé ou affiché.

Le tableau ci-après présente une suite de champs de données, par ordre croissant d'index. Tous les champs comportent un nombre entier d'octets. Pour les champs comportant plusieurs octets, les valeurs ont leurs octets de poids fort en tête (« big endian »).

Les bits d'un champ sont numérotés à partir de 0 (« b0 » est le bit de poids le plus faible).

Dans ce tableau la couleur de fond indique l'émetteur du champ de données :

- En gris, les éléments fournis par le système de gestion des identifiants, présents pour tous les types de support : données statiques (obligatoires) et signature statique (optionnelle).
- En vert, les éléments générés par le téléphone : données dynamiques et signature dynamique.

Ce tableau indique également les éléments optionnels.

Champ	Taille (octets)	Description ou valeur	Présence
Entête en caractères alphanumériques			
Format	3	« AMC ».	Obligatoire
Version	1	Version de la structure des données à suivre. Pour le présent document, sa valeur est « 1 ».	
		Données binaires à encoder en Base45	

**a supprimé:** encodées

**a supprimé:** ,

**Commenté [SDI6]:** L'encodage Base45 optimise la taille des QR Codes. Il est également utilisé pour le certificat Covid européen ("R:\Docs Publiques\Normes-Standards-Documents\BarCodes\QR Code\Certificat Covid UE\_CELEX 32021D1073 FR TXT.pdf").

**a supprimé:** nul.

**a supprimé:** Dans

**a supprimé:** Dans les tableaux ci-après les champs de données sont représentés par ordre croissant d'index.

**a supprimé:** <#>Données encodées¶

**a supprimé:** <#>Dans le tableau ci-dessous les éléments de données sont identifiés selon leur émetteur : en gris les données fixes authentifiées par le serveur AMC (données statiques), En vert les données variables produites par l'app (données dynamiques).¶

**a supprimé:** Remarque

**Cellules insérées**

**a supprimé:** Version d'encodage des données AMC (01h pour ce document)

**a supprimé:** AIDLength

**a supprimé:** 1

**Cellules supprimées**

**Cellules supprimées**

**a supprimé:** Nombre d'octets significatifs au début (gauche) du champ AID (05h à 10h)...

**a supprimé:** AID

<sup>22</sup> IETF RFC 9285, « The Base45 Data Encoding » (<https://datatracker.ietf.org/doc/html/rfc9285>).

Configuration	5	Configuration de la structure de données. Valeur de 40 bits, chaque bit à 1 indiquant la présence d'un champ optionnel (bit à 0 si le champ est absent) : b0 Présence de PIDSector1Value b1 Présence de PIDSector2Value ... b34 Présence de PIDSector35Value b35 Réservé, toujours égal à 0. b36 Présence de StaticSignature, obligatoire lorsque b37=1. b37 Présence de PublicKey, et de DynamicDateTime à DynamicSignature (toujours = 0 pour un CB2D imprimé) b38 et b39 Réservés, toujours égaux à 0.	Obligatoire
GDIssuerReference	2	Référence de l'émetteur de l'AMC	Obligatoire
PIDIssuerReference	2	Référence de l'émetteur des identifiants prédéfinis.	
PIDVersion	1	'02'h, version de la structure de données Predefined IDs	
PIDScopeID	3	Identifiant du périmètre de l'application (égal à GDScopeID).	Obligatoire
PIDStartDate	4	Date de début de validité des identifiants prédéfinis (encodée YYYYMMDD en BCD).	
PIDSignKeyReference	2	Référence (subordonnée à PIDScopeID) de la clé de signature	
PIDKeyRef	2	Référence (subordonnée à PIDScopeID) de la clé TDES de génération pour tous les champs PIDSectorXValue.	
PIDSector1Value	0 ou 4	Valeur de l'identifiant pour le secteur d'activité n° 1 Présent ou non selon le bit correspondant de Configuration	Optionnel
PIDSector2Value	0 ou 4	Valeur de l'identifiant pour le secteur d'activité n° 2 Présent ou non selon le bit correspondant de Configuration	Optionnel
...	...	...	...
PIDSector35Value	0 ou 4	Valeur de l'identifiant pour le secteur d'activité n° 35 Présent ou non selon le bit correspondant de Configuration	Optionnel
PublicKey	0 ou 33	Valeur de la clé publique permettant la vérification de la signature dynamique au format avec compression de point.	Optionnel
StaticSignature	0 ou 64	Signature ECDSA de l'ensemble des données précédentes, calculée avec la paire ECC de l'autorité du périmètre de service.	Optionnel

a supprimé: 8

Cellules insérées

a supprimé: Numéro de série du conteneur sous la forme DDDDDNNNNNNNNNNh, avec :¶  
DDDDh : 2 octets, date de fin de validé en nombre de demi-journées depuis le 1<sup>er</sup> janvier 2010 à 0h00 (0 si pas de date de fin de validité)¶  
NNNNNNNNNNh : 6 octets, numéro unique du conteneur.

a supprimé: Startup Information

a supprimé: 12

a supprimé: Structure GlobalData de l'AMC (détails pages suivantes)

Cellules insérées

a supprimé: PIDLength

a supprimé: Nombre d'octets du champ PredefinedIDs

a supprimé: PredefinedIDs

a supprimé: Var.

a supprimé: Structure

a supprimé: de l'AMC, sans sa signature PIDSignature (détails pages suivantes)...

Cellules insérées

a supprimé: (voir chapitre IV.3.4)

a supprimé: (voir chapitre IV.3.4)

DynamicDateTime	0 ou 4	Date et heure de génération de la signature dynamique, en nombre de secondes écoulées depuis 0 h à la date de début de validité de la signature statique (PIDStartDate dans PredefinedIDs). La valeur 'FFFFFFFF'h est interdite.	
DynamicLatitude	0 ou 4	Latitude de la génération de la signature dynamique sous la forme : (latitude en degrés + 90) x 100 000. La valeur 'FFFFFFFF'h indique 'latitude indéterminée'. Exemples : 49,5000 → 139,5000 → 13 950 000 → '00 D4 DC 30' -49,5000 → 40,5000 → 4 050 000 → '00 03 DC 50'	Optionnel
DynamicLongitude	0 ou 4	Longitude courante de la génération de la signature dynamique sous la forme : (longitude en degrés + 180) x 100 000. La valeur 'FFFFFFFF'h indique 'longitude indéterminée'. Exemples : 123,5000 → 303,5000 → 30 350 000 → '01 CF 1A B0' -123,5000 → 56,5000 → 5 650 000 → '00 56 36 50'	
DynamicFreeData	0 ou 16	Données libres, non interoperables.	
DynamicSignature	0 ou 64	Signature ECDSA dynamique des données StaticSignature à DynamicFreeData, calculée avec la paire ECC de l'app.	

a supprimé: l'émission  
a supprimé: GDIssuingDate  
a supprimé: GlobalData avec l'heure à 00h00m00s  
a supprimé: FFFFFFFFh signifie que la date  
a supprimé: absente  
a supprimé: '(  
a supprimé: 000'  
a supprimé: FFFFFFFFh  
a supprimé: inconnue'

a supprimé: '(  
a supprimé: 000'  
a supprimé: FFFFFFFFh  
a supprimé: inconnue'

a supprimé: (voir chapitre IV.3.4)

a supprimé: Soit une taille totale de 529 octets pour l'AMC commune complète, ramenée à 369 octets si l'on ne conserve que les secteurs 1 à 15. ¶  
¶  
Le champ GlobalData contient la structure Global Data de l'AMC (voir la norme AMC NF P 99-508) :¶

a supprimé: Champ

### III.3 Unicité des identifiants prédéfinis

#### Attention

Comme défini par la norme AMC (chapitre 6.4.2.1), l'unicité d'un identifiant prédéfini n'est garantie que pour sa valeur complète sur 11 octets, composée de :

- **PIDScopeID** (3 octets), identifiant du périmètre de service.
- **Le numéro de secteur** (2 octets), déduit du champ Configuration (selon la position du bit qui indique la présence de l'identifiant).
- **PIDKeyRef** (2 octets), référence de la clé secrète de génération de la valeur de l'identifiant. C'est la même référence pour tous les identifiants de la structure de données.
- **PIDSectorXValue** (4 octets), valeur correspondant au secteur n° X.

Pour un accepteur qui traite un seul périmètre de service et un seul secteur d'activité, PIDScopeID et le numéro de secteur peuvent être gérés comme des constantes, seuls PIDKeyRef et PIDSectorXValue étant associés au compte de l'utilisateur (soit en pratique un identifiant de 6 octets). Il est en effet fortement recommandé de permettre que PIDKeyRef ne soit pas identique pour tous les utilisateurs.

### III.4 Taille des données encodées

Moins un CB2D contient d'information, plus il est lisible. Pour les caractéristiques recommandées au chapitre II.2, les données encodées ne peuvent pas dépasser 483 caractères alphanumériques.

Or, avec une AMC commune (35 secteurs d'activité), la structure complète (avec tous les champs optionnels) définie ci-dessus comporte 528 caractères alphanumériques une fois encodée.

Afin d'améliorer la lisibilité du CB2D, il est donc recommandé de ne pas inclure tous les secteurs d'activité. Par exemple, avec 16 secteurs, la taille des données encodées est de 415 caractères. C'est le choix fait dans l'exemple 7 du chapitre VII.2.10.

### III.5 Cryptographie

#### Algorithmes

Les deux signatures (StaticSignature et DynamicSignature) ont les caractéristiques suivantes :

- Algorithme de signature : ECDSA avec SHA-256.
- Algorithme de clé : ECC sur la courbe P-256 (également appelée « ansix9p256r1 », « prime256v1 » et « secp256r1 »).

Ce sont les mêmes algorithmes que ceux de la signature des identifiants prédéfinis de la norme AMC NF P 99-508.

#### Clés de signature

La paire de clés ECC pour la signature statique (StaticSignature) est celle définie par l'autorité du périmètre de service (GDSCOPEID) pour gérer la signature des identifiants prédéfinis de la norme AMC NF P 99-508. La clé publique de cette paire est supposée connue de l'app mobile et des terminaux accepteurs.

La paire de clés ECC pour la signature dynamique (DynamicSignature) est propre à l'app mobile et générée par l'app elle-même. La clé publique de cette paire a été envoyée par l'app mobile à son serveur d'enrôlement (qui lui a ensuite retourné la signature statique).

#### Format avec compression de point

Dans les données encodées, la clé publique de l'app mobile (PublicKey) est encodée selon le format avec « compression de point », qui comporte 33 octets commençant par 02h ou 03h selon que la coordonnée Y du point est paire ou impaire, suivi de la coordonnée X sur 32 octets (convention « big endian »), conformément au standard SEC 1 :

- Règle d'encodage d'un point de courbe elliptique en chaîne d'octets :  
<https://www.secg.org/sec1-v2.pdf#subsection.2.3.3>
- Règle de décodage d'une chaîne d'octets en point de courbe elliptique :  
<https://www.secg.org/sec1-v2.pdf#subsection.2.3.4>

**a supprimé:** Pour garantir la lisibilité d'un

**a supprimé:** Aztec sur l'écran d'un téléphone,

**a supprimé:** qu'il contient doivent être aussi limitées que possible, et...

**a supprimé:** devraient

**a supprimé:** 621 octets (voir chapitre III.1).

**a supprimé:** Avec l'encodage décrit,

**a supprimé:** nécessite 529 octets

**a supprimé:** proposé

**a supprimé:** réduire le nombre de Predefined IDs à 15, ramenant l'encodage à 369 octets.¶  
Pour conserver l'interopérabilité de l'AMC commune

**a supprimé:** norme pourrait alors interdire l'usage

**a supprimé:** identifiants omis.

**a supprimé:** <https://www.secg.org/sec1-v2.pdf#subsection.2.3.3>...

**a supprimé:** <https://www.secg.org/sec1-v2.pdf#subsection.2.3.4>...

**a supprimé:** <#>Stockage de la signature statique¶  
Pour faciliter l'interopérabilité des solutions d'AMC mobile en CB2D et en BLE, la signature statique doit être conservée dans le conteneur Calypso.¶  
Avec une AMC commune, cette signature statique est stockée dans le fichier *Predefined Identifiers*, à la suite de la structure *Predefined IDs*, telle que présente dans le champ *StaticSignature* (voir chapitre IV.3.1).¶  
Ce fichier ayant une capacité de 512 octets et la structure *Predefined IDs* comportant 357 octets, la place restante (155 octets) est suffisante pour la signature statique (64 octets).

## IV. Sécurité

### IV.1 Menaces

Les menaces à prendre en compte pour les identifiants AMC sont :

- Traçabilité : collecte d'identifiants d'autres secteurs d'activité, accidentelle ou intentionnelle, qui pourrait permettre un traçage de l'utilisateur dans différents secteurs d'activité (en **infraction** avec les exigences de la CNIL).
- Contrefaçon : création de faux identifiants (ex-nihilo), ou falsification de paramètres associés aux identifiants (par exemple une période de validité).
- Clonage : duplication d'identifiants authentiques, pour distribution à des tiers.

La contrefaçon et le clonage sont faciles à concevoir et à mettre en œuvre, tout particulièrement dans le cas du téléphone.

a supprimé: contravention

### IV.2 Contre-mesures

#### IV.2.1 Traçabilité

##### Affichage d'un CB2D

Le CB2D n'est affiché sur l'écran du téléphone que lorsque l'utilisateur le souhaite. Sa lecture à l'insu de l'utilisateur est donc peu probable. La solution CB2D protège donc suffisamment contre cette menace.

##### Transmission en BLE

En BLE, l'application concernée doit être au premier plan<sup>23</sup>, ce qui permet à l'utilisateur de choisir les moments où les données de l'AMC peuvent être lues.

Le standard BLE propose différents mécanismes de sécurité qui n'offrent pas la même protection<sup>24</sup> :

- Avec les versions 4.0 et 4.1 de BLE, les mécanismes ne nécessitant aucune action de l'utilisateur (par exemple la saisie d'un code) peuvent être contournés même en cas d'écoute passive.
- Avec les versions suivantes, les mécanismes ne nécessitant ni action de l'utilisateur ni échange de données par un canal tiers sécurisé peuvent être contournés par des attaques d'écoute active (de type « man in the middle »).
- Dans tous les cas, sans canal tiers authentifié (assurance de légitimité à lire l'AMC), n'importe quel équipement BLE (par exemple un téléphone) peut faire office de terminal AMC, donc peut lire l'AMC à l'insu de l'utilisateur (lorsque l'application AMC est au premier plan).

La solution BLE protège donc faiblement contre la lecture à l'insu de l'utilisateur.

<sup>23</sup> Actuellement, sous Android cette obligation est doit être assurée par l'application mobile.

<sup>24</sup> Zhang Y., Weng J., Dey R., Fu X. (2019) Bluetooth Low Energy (BLE) Security and Privacy. In: Shen X., Lin X., Zhang K. (eds) Encyclopedia of Wireless Networks. Springer, Cham. [https://doi.org/10.1007/978-3-319-32903-1\\_298-1](https://doi.org/10.1007/978-3-319-32903-1_298-1).



#### IV.2.2 Contrefaçon et clonage

Les contre-mesures définies pour le CB2D INTERCODE sont pertinentes dans le cas de l'AMC, y compris en BLE :

- Une *signature statique* protège contre la contrefaçon. Elle remplit la même fonction que la signature des identifiants prédéfinis de la norme AMC : preuve que les données de l'AMC ont été émises par une entité légitime.
- Une *signature dynamique* protège contre le clonage. Elle remplit une fonction proche de celle de la session sécurisée Calypso et prouve que le téléphone et l'app sont authentiques. Étant basée sur une horodate vérifiée par le terminal AMC, cette signature dynamique assure que le support est authentique « maintenant ».

Ces mécanismes correspondent aux trois niveaux de sécurité définis par la norme AMC :

- Aucune authentification : le terminal AMC ne vérifie aucune signature.
- Authentification statique : le terminal AMC ne vérifie que la signature statique.
- Authentification complète : le terminal vérifie la signature statique et la signature dynamique.

**a supprimé:** Sa durée de vie est celle de la date fin de validité HCE (voir chapitre II).

## V. Outils

### V.1 Cryptographie : OpenSSL

OpenSSL est une boîte à outils de chiffrement fournissant entre autres une implémentation des algorithmes cryptographiques utilisés dans ce document.

Il est libre de droits, multiplateforme, et extrêmement courant : <https://www.openssl.org/>.

### V.2 Encodage et décodage

#### Outils en ligne

<https://barcode.tec-it.com/fr/QRCode> Outil en ligne de génération de QR Code.

<https://www.dcode.fr/codage-base45> Outil en ligne d'encodage et de décodage Base45.

<https://demo.dynamsoft.com/DBR/BarcodeReaderDemo.aspx> Outil en ligne de décodage d'un code-barres en JSON.

<https://zxing.org/w/decode.jsp>

Outil en ligne fournissant la chaîne d'octets de bas niveau après correction d'erreurs et avant décodage selon la symbologie.

Remarque : ce décodeur est très sensible aux moindres défauts graphiques des codes-barres.

<https://www.onlinebarcodereader.com> Outil en ligne de décodage d'un code-barres.

#### Librairies et logiciels

<https://github.com/hwellmann/zxing> ZXing (« Zebra Crossing ») est une bibliothèque de traitement d'images de codes-barres 1D/2D multiformat et open-source, implémentée en Java, avec des ports vers d'autres langages

<http://zint.org.uk> Zint fournit une implantation open-source d'encodage de données sous multiples formats de codes-barres.

<https://www.bctester.de/en> Gratuitiel de décodage d'un code-barres.

a supprimé: Aztec

a supprimé: <https://www.bctester.de>

a supprimé: Gratuitiel

a supprimé: d'un code-barres

a supprimé: « Dynamsoft Barcode Reader »

a supprimé: Aztec

a supprimé: Décodeur Aztec « ZXing Decoder Online »

a supprimé: Aztec

a supprimé: <https://www.onlinebarcodereader.com/>

a supprimé: « OnlineBarcodeReader »

a supprimé: Aztec en texte et en binaire

a supprimé: <http://zint.org.uk/>

## VI. Évolutions possibles

### VI.1 Utilisation de données circonstancielles

#### VI.1.1 Geste volontaire en BLE

La capacité d'un terminal BLE de discriminer efficacement les téléphones qui sont à sa portée reste sujette à caution, en particulier dans le cas où plusieurs terminaux sont proches.

Pour s'assurer que l'utilisateur auquel le service est accordé (en échange d'un paiement préalable ou ultérieur) est bien celui souhaité, il serait nécessaire de conditionner la transmission BLE à des données circonstancielles obtenues selon l'une des méthodes évoquées au chapitre VI.1.3 (sauf la géolocalisation).

a supprimé: V.1.3

#### VI.1.2 Amélioration contre le clonage en CB2D ou en BLE

La protection contre le clonage peut être améliorée par l'utilisation d'un challenge auquel le téléphone doit répondre, en utilisant le champ DynamicFreeData des données dynamiques.

Ce challenge doit être spécifique à chaque transaction, fournie à l'app juste avant la génération de la signature dynamique.

Le support est alors authentifié « ici » en plus de « maintenant », et le « maintenant » provient d'une source plus sûre.

Ce mécanisme est fonctionnellement équivalent au challenge généré par le SAM lors d'une session sécurisée Calypso (carte Calypso ou AMC mobile en NFC).

Exemples :

- Valeur du challenge : nombre aléatoire, compteur, identifiant du terminal, combinaison de ces données.
- Source du challenge : voir les méthodes évoquées au chapitre VI.1.3.
- Réponse : identique au challenge, résultat d'un calcul à partir du challenge (par exemple les 8 premiers octets du SHA-256 des informations reçues).

a supprimé: V.1.3

#### VI.1.3 Obtention de données circonstancielles pour la lecture en CB2D ou BLE

En CB2D ou en BLE, les contre-mesures précédentes peuvent nécessiter des données circonstancielles.

Les sources de telles données pourraient être, par exemple :

- Une action sur l'écran du téléphone.
- La géolocalisation.
- Des données présentes dans la requête BLE émise par le terminal AMC.
- Des données lues dans une étiquette/balise NFC, CB2D ou BLE<sup>25</sup>, si nécessaire contrôlée par le terminal AMC (par exemple dans le cas d'un challenge, voir chapitre VI.1.2).

a supprimé: V.1.2

Les sources automatiques (sans action de l'utilisateur autre qu'un geste volontaire) seraient à privilégier.

<sup>25</sup> La lecture d'étiquette/balise NFC fonctionne avec tous les téléphones mobiles NFC sous Android, et les téléphones Apple à partir de iOS 11 et de l'iPhone 7. Pour le transport public, des travaux de normalisation de ce type d'étiquette/balise NFC, CB2D ou BLE sont en cours au sein du groupe de travail BNTRA/CN03/GT4.

## VI.2 NFC : mode PKI de Calypso Prime Revision 3

L'utilisation du mode PKI permettrait à tous les terminaux AMC d'empêcher le clonage des supports NFC *sans utiliser de SAM.*

Ce mode a été introduit en septembre 2019, dans la spécification Calypso Prime Revision 3.3. Il permet l'authentification d'un conteneur Calypso et de ses données en utilisant seulement une clé publique.

En janvier 2023 la première carte Calypso Prime proposant le mode PKI a été certifiée par CNA.

Ce mode pourrait également être implémenté dans un conteneur Calypso HCE.

**a supprimé:** Depuis

**a supprimé:** ,

**a supprimé:** a introduit le mode « PKI », qui

**a supprimé:** des données

**a supprimé:** sans utiliser

**a supprimé:** SAM.

**a supprimé:** peut

**a supprimé:** Le mode PKI permet ainsi à tous les terminaux AMC d'empêcher le clonage des supports NFC sans nécessiter de SAM.

## VI.3 Données CB2D/BLE accessibles en NFC

Afin d'obtenir en NFC les mêmes données qu'en CB2D ou en BLE, il serait possible de les ajouter à l'app NFC, et ainsi d'appliquer le même traitement de lecture quelle que soit la technologie utilisée.

Différentes solutions techniques sont envisageables pour héberger ces données, par exemple :

- Conteneur NFC dédié, dont l'AID serait différent de celui du conteneur AMC actuellement normalisé.
- Fichier dédié ajouté à la structure de fichiers AMC actuellement normalisée.

## VII. Annexes

### VII.1 La norme AMC

#### VII.1.1 Publication

La norme française décrivant l'Application Multiservices Citoyenne, ou « AMC », a été publiée en octobre 2020 par l'AFNOR sous la référence « NF P 99-508 ».

Elle est disponible sur la boutique en ligne de l'AFNOR : <https://www.boutique.afnor.org/>.

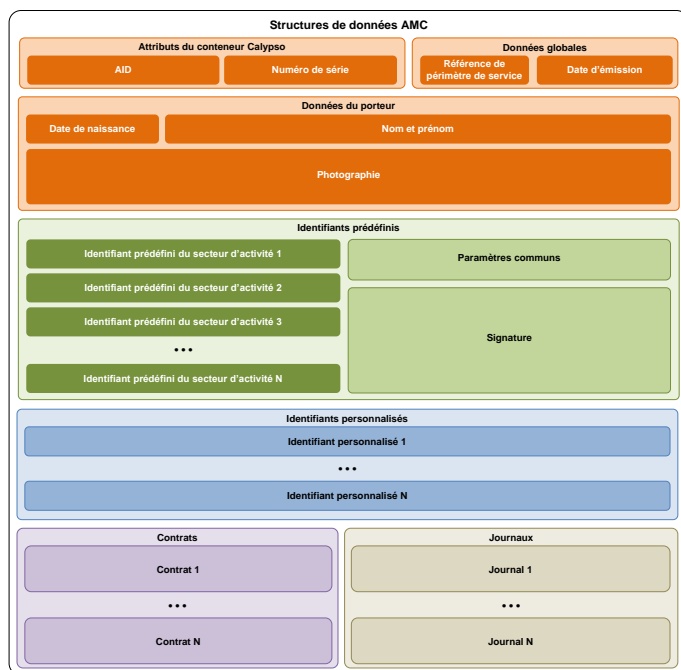
#### VII.1.2 Secteurs d'activité

La norme AMC décrit des structures de données contenant un ensemble d'identifiants.

Chaque identifiant est assigné à un secteur d'activité spécifique, afin de permettre l'étanchéité du traitement des identifiants dans les systèmes d'information des fournisseurs de service relevant de secteurs d'activité différents, conformément aux exigences de la CNIL.

#### VII.1.3 Structures de données

Le diagramme ci-dessous présente les structures de données AMC :



Les structures de données obligatoires de toute AMC sont :

- Les attributs du conteneur Calypso.
- Les données globales.
- Les identifiants prédéfinis.

La présence des autres structures de données est optionnelle.

#### VII.1.4 Conteneur Calypso

Les structures de données sont stockées dans un conteneur *Calypso*, appelé « application ». Le standard Calypso repose sur les normes internationales des cartes à puces.

Le standard Calypso permet ainsi l'hébergement d'identifiants dans des cartes sans contact (telles que celles utilisés pour l'accès aux transports publics<sup>26</sup>) et dans les téléphones NFC compatibles (voir chapitre I.3).

#### VII.1.5 Niveaux de sécurité

La norme AMC définit trois niveaux de sécurité correspondant à trois types d'authentification, au choix du terminal lisant les données :

Authentification	Traitement	Protection
Aucune	Lecture des données de l'AMC sans vérification de la signature ni authentification du conteneur Calypso	
Statique	Lecture des données de l'AMC avec vérification de la signature mais sans authentification du conteneur Calypso	Assure que les identifiants ont été générés par une autorité légitime
Complète	Lecture des données de l'AMC avec vérification de la signature et authentification du conteneur Calypso <sup>27</sup>	Assure que les identifiants ont été générés par une autorité légitime Assure que les identifiants n'ont pas été dupliqués

Un terminal lit la totalité des identifiants disponibles dans une AMC Calypso, il est ensuite de sa responsabilité de ne conserver et reporter au système central que l'identifiant qui correspond à son propre secteur d'activité. Cela s'applique également au numéro de série du conteneur Calypso.

#### VII.1.6 Types d'AMC

La norme AMC distingue deux types d'AMC : l'AMC *commune* et les AMC *spécifiques*.

L'AMC commune est une AMC totalement définie, en particulier concernant la clé publique permettant de vérifier l'authenticité des identifiants qu'elle contient, et la liste des 35 secteurs d'activité pour lesquels elle contient des identifiants (dont les 10 secteurs CNIL). Elle est administrée par l'ADCET.

Une AMC spécifique est toute AMC qui diverge d'une façon quelconque de l'AMC commune. Elle est administrée par son propre territoire.

<sup>26</sup> Cartes Pass Pass en Hauts de France, Korrigo en Bretagne, OûRA en Auvergne Rhône-Alpes, Navigo en Île-de-France, etc.

<sup>27</sup> Nécessite l'utilisation d'un SAM si le mode PKI défini par Calypso Prime Revision 3.3 n'est pas disponible, voir chapitre VI.2.

## VII.2 Exemples

### VII.2.1 Clés utilisées

Pour la génération des identifiants prédéfinis et le calcul de la signature statique (StaticSignature), les clés utilisées sont les clés de test **TDES** et **ECC** recommandées par l'ADCET, et définies dans les annexes de la norme AMC NF P 99-508.

Clé de génération des identifiants prédéfinis (PID1Value à PID35Value) :

Donnée	Taille (octets)	Valeur hexadécimale
PIDXKeyRef	2	0753
Valeur	16	12345678876543219ABCDEF00FEDCBA9

Paire ECC pour le calcul de la signature statique (StaticSignature) :

Donnée		Taille (octets)	Valeur hexadécimale
PIDSignKeyReference		2	CB32
Clé privée (d)		32	AACD74CC91F375D9CA8CEF9EA7DA2C3590C71927C0AACABC9A6EA40263E7016E
Clé publique	X	32	89575E94AC5B05F8C607F5BB2DEF11C27D4563CB2F7C1AFDC34636BC226FF405
	Y	32	7E2C3277DE9819002E3947CC987C7F781B8A189F605AF6B440FF74EE23EB88A6

La paire ECC pour le calcul de la signature dynamique (DynamicSignature) des exemples est spécifique au présent document :

Donnée	Taille (octets)	Valeur hexadécimale
Clé privée (d)	32	37C7990431396032CA378EA1C48134B23E09F615F89DECA230A55A672AFA4829
Clé publique	X	32 D6B6BAD5082B0E280ED72268E8E29A4257BF5AFD662A9230E9C62C89A9E7973D
	Y	32 F8154AA6A1E049E2642C7E9AB6A54D0874F646E869AA71692A651F5498E20CC7

**Attention :** Dans la présente version de ce document, les signatures statiques et dynamiques ont des valeurs factices. Elles ne sont destinées qu'à la génération de codes-barres représentatifs.

a supprimé: ECC

a supprimé: TDES

a supprimé: est

a supprimé: <#>Données à encoder¶  
L'exemple ci-dessous comporte 15 identifiants prédéfinis.¶  
¶  
# Version and container attributes:¶  
01 # Version¶  
0B # AID length¶  
A000000291D25008009301000000000 # AID (with padding)¶  
00000080FAEF0042 # Serial Number¶  
11223344556677 # Startup Information¶  
¶  
# Global Data:¶  
E104 # GDIssuerReference¶  
01 # GDVersion¶  
250E00 # GDScopeID¶  
20211203 # GDIssuingData¶  
0000 # GDMedia & GDPrinting¶  
¶  
#Predefined IDs:¶  
0085 # PID length (133 bytes)¶  
E104 # Issuer Reference¶  
01 # Version¶  
250E00 # Scope ID¶  
20220916 # PID Startdate (BCD YYYYMMDD)¶  
CB32 # PID SignKeyref¶  
¶  
0F # PID Count (15 in decimal)¶  
0001 0753 01E0E43 # PID 1: (Sector = 0001h ; KeyRef = 0753h , Value = 01E0E43h)¶  
0002 0753 014C8CCC¶  
0003 0753 7406FB78¶  
0004 0753 A40CF9A1¶  
0005 0753 357194EC¶  
0006 0753 E693FC8A¶  
0007 0753 25102112¶  
0008 0753 B0F5586B¶  
0009 0753 CAFD8AFC¶  
000A 0753 963458A2¶  
000B 0753 9D5964E1¶  
000C 0753 13197B7E¶  
000D 0753 3836877F¶  
000E 0753 2CFEBC2¶  
000F 0753 7A8F7331¶  
03D6B6BAD5082B0E280ED72268E8E29A4257BF5AFD662A9230E9C62C89A9E7973D # Public Key¶  
9DB94A8B73654AAAD1D2323FDA0AA71FBC21B035BF8F19F5E624E95F271E77CB96183D4E82E8CFD01D08C92E35CFF73A8BAC6B358E6F053F3FB58E70D56903B7 # Static Signature¶  
¶  
# Partie Dynamique¶  
00008CA9 # DynamicDateTime¶  
008CE79E # DynamicLatitude¶  
01163BDE # DynamicLongitude¶  
00000000000000000000000000000000 # DynamicFreeData¶  
E88AC5C9F9FF24E336230155E96AEC4E0EE96037EE7A0F1B1145B707C08297A1D205AEF1FE1F38DB67B19F171E2CF9B46606F9FE57711738DF8FD40E2F2CA # DynamicSignature¶  
¶  
Données encodées¶  
Les 369 octets de données encodées sont donc :¶  
010BA000000291D2500800930100000000000000080FAEF004211223344556677E10401250E002021120300000085E10401250E0020220916CB320F0001075301E0E4300020753014C8CCC000307537406FB7800040753A40CF9A100050753357194EC00060753E693FC8A000707532510211200080753B0F5586B00090753CAFD8AFC000A0753963458A2000B07539D5964E1000C075313197B7E000D07533836877F000E07532CFEBC2000F07537A8F733103D6B6BAD5082B0E280ED72268E8E29A4257BF5AFD662A9230E9C62C89A9E7973D9DB94A8B73654AAAD1D2323FDA0AA71FBC21B035BF8F19F5E624E95F271E77CB96183D4E82E8CFD01D08C92E35CFF73A8BAC6B358E6F053F3FB58E70D56903B7 # Static Signature¶

## VII.2.2 Données

Champ	Taille (octets)	Valeur	Remarque
Texte ASCII			
Format	3	'414D43'h	« AMC »
Version	1	'31'h	« 1 »
Encodage Base45			
Configuration	5	Exemple 1 : '000000049'h Exemple 2 : '100000049'h Exemple 3 : '300000049'h Exemple 5 : '0000403C49'h Exemple 5 : '1000403C49'h Exemple 6 : '3000403C49'h Exemple 7 : '3001F83FC9'h	Exemple 1 : secteurs 1, 4 et 7, sans signature Exemple 2 : secteurs 1, 4 et 7, signature statique seulement Exemple 3 : secteurs 1, 4 et 7, signature statique & dynamique Exemple 4 : secteurs 1, 4, 7, 11 à 14, et 22, sans signature Exemple 5 : secteurs 1, 4, 7, 11 à 14, et 22, signature statique seulement Exemple 6 : secteurs 1, 4, 7, 11 à 14, et 22, signature statique & dynamique Exemple 7 : secteurs 16, signature statique & dynamique
GDIssuerReference	2	'FEF0'h	Émetteur de test
PIDIssuerReference	2	'FEF0'h	Émetteur de test
PIDVersion	1	'02'h	
PIDScopeID	3	'250E00'h	AMC commune
PIDStartDate	4	'20231231'h	31 décembre 2023 (à 0h)
PIDSignKeyReference	2	'CB32'h	Clé ECC de test de la norme AMC
PIDKeyRef	2	'0753'h	Clé TDES de test de la norme AMC



PID1Value à PID35Value	Var.	1 : '01EDEE43'h 2 : '014C8CCC'h 3 : '7406FB78'h 4 : 'A40CF9A1'h 5 : '357194EC'h 6 : 'E693FC8A'h 7 : '25102112'h 8 : 'B0F5586B'h 9 : 'CAFD8AFC'h 10 : '963458A2'h 11 : '9D5964E1'h 12 : '13197B7E'h 13 : '3836877F'h 14 : '2CFEBCC2'h 15 : '7A8F7331'h 16 : 'A422DB34'h 17 : '437723B1'h 18 : '6F02C3AA'h 19 : '5CBD84C3'h 20 : '740417C5'h 21 : '6B07629D'h 22 : '811B8A5F'h 23 : '5D1EF11F'h 24 : 'F3DDA807'h 25 : '42E2E3E5'h 26 : 'DE7DB4F1'h 27 : 'DA7E656D'h 28 : '38032365'h 29 : '64DBA2D5'h 30 : '198F5085'h 31 : '24B4121E'h 32 : '524121C4'h 33 : '340135B9'h 34 : 'A6BB62B0'h 35 : '6EBB88FC'h	Valeurs générées à partir de la valeur unique '000ABC12'h (comme dans l'exemple A.1 de la norme AMC) Présence de chaque valeur selon le champ Configuration
PublicKey	0 ou 33	'03 D6B6BAD5082B0E28 0ED72268E8E294A2 57BF5AFD662A9230 E9C62C89A9E7973D'h	Forme avec compression de point (chapitre III.5)
StaticSignature	0 ou 64	'921A31D0BC453E49 C37A2EA4CAD8D520 34CAC5EC5D7EDFBF 4D33693AB0B5D6F0 C1C9B0FDC4C1865D 6BD316A6CC69FE8C 678084DCD99819EF 92AAB8E234B9972F'h	Valeur factice arbitraire

DynamicDateTime	0 ou 4	'0001E527'h	1 <sup>er</sup> janvier 2024 à 10h 29mn 59s
DynamicLatitude	0 ou 4	'00D3E488'h	48,866°
DynamicLongitude	0 ou 4	'01163BDE'h	2,34334°
DynamicFreeData	0 ou 16	'00...00'h	
DynamicSignature	0 ou 64	'A014F89794FF3D39 1AFEC6C504538544 12AB50F9A00103CC C4FED41FE4E12533 43E3EB712A6B73BF 0F8F1A9A11C50AB0 8D69465556CDD288 EB4913ABF31B34DD'h	Valeur factice arbitraire


### VII.2.3 Taille apparente

Dans exemples ci-après, les codes-barres sans signature dynamique sont supposés imprimés dans un carré de 20 mm de côté, les codes-barres avec signature dynamique sont supposés affichés dans un carré de 40 mm de côté.

La taille des CB2D prend en compte la zone vierge minimale requise autour du CB2D (« quiet zone »), large de quatre modules sur les quatre côtés (minimum défini par la spécification QR Code).


Pour obtenir la taille indiquée lors de l'impression de ce document, le format A4 (zoom à 100%) doit être utilisé.

### VII.2.4 Exemple 1 : trois secteurs (1, 4, 7), pas d'authentification

Données à encoder	33 octets	'0000000049FEF0FEF002250E0020231231CB32075301EDEE43A40CF9A125102112'h	
Structure complète	54 caractères	AMC1000000.F9:KUHFU U4W00NJ4CD6RE69MAP3U O8 S1XGKY12IO	
		Modules (sans quiet zone) :	29 × 29
		Taille totale (avec quiet zone) :	20 mm × 20 mm
		Taille des modules :	21,3 mil (0,541 mm)



#### VII.2.7 Exemple 4 : huit secteurs (1, 4, 7, 11 à 14, 22), pas d'authentification

Données à encoder	53 octets	'0000403C49FEF0FEF002250E0020231231CB32075301EDEF43A40CF9A1251021129D5964E113197B7E3836877F2CFEBCC2811B8A5F'h	
Structure complète	84 caractères	AMC1000J58.F9:KUHFU U4W00NJ4CD6RE69MAP3U O8 S1XGKY12+F2ODBJKS/932/F9+6L3G79WNQOUL352	
		Modules (sans quiet zone) :	33 × 33
		Taille totale (avec quiet zone) :	20 mm × 20 mm
		Taille des modules :	19,2 mil (0,488 mm)


#### VII.2.8 Exemple 5 : huit secteurs (1, 4, 7, 11 à 14, 22), authentification statique seulement

Données à encoder	117 octets	'1000403C49FEF0FEF002250E0020231231CB32075301EDEF43A40CF9A1251021129D5964E113197B7E3836877F2CFEBCC2811B8A5F921A31D0BC453E49C37A2EA4CAD8D52034CAC5EC5D7EDFBF4D33693AB0B5D6F0C1C9B0FDC4C1865D6BD316A6CC69FE8C678084DCD99819EF92AAB8E234B9972F'h	
Structure complète	180 caractères	AMC1112J58.F9:KUHFU U4W00NJ4CD6RE69MAP3U O8 S1XGKY12+F2ODBJKS/932/F9+6L3G79WNQOUL3V3C0E3LHQ-X8SE93KFL\$KOIR934OSPT*TY1GD8OLM6*I7K:MSJUHMP3W.KOK B%UQ+3L:HDXXH5BGH-RCAJ+CU9QL%QS KN21	
		Modules (sans quiet zone) :	49 × 49
		Taille totale (avec quiet zone) :	20 mm × 20 mm
		Taille des modules :	13,8 mil (0,351 mm)

## VII.2.9 Exemple 6 : huit secteurs (1, 4, 7, 11 à 14, 22), authentification complète

Données à encoder	242 octets	'3000403C49FEF0FEF002250E0020231231CB32075301EDEF43A40CF9A1251021129D5964E113197B7E3836877F2CFEBCC2811B8A5F03D6B6BAD5082B0E280ED72268E8E294A257BF5AFD662A9230E9C62C89A9E7973D921A31D0BC453E49C37A2EA4CAD8D52034CAC5EC5D7EDFBF4D33693AB0B5D6F0C1C9B0FDC4C1865D6BD316A6CC69FE8C678084DCD99819EF92AAB8E234B9972F0001E52700D3E48801163BDE00000000000000000000000000000A014F89794FF3D391AFEC6C50453854412AB50F9A00103CCC4FED41FE4E1253343E3EB712A6B73BF0F8F1A9A11C50AB08D6946556CDD288EB4913ABF31B34DD'h
Structure complète	367 caractères	AMC1336J58.F9:KUHFU U4W00NJ4CD6RE69MAP3U O8 S1XGKY12+F2ODBJKS/932/F9+6L3G79WNQOUL3N0CL6R*RNL11OZ1J*1XF4 %JTPZI84BSMB9-CTLI-OTGS5PLLH5J7LIHD62 NF*72WOF+5/SPK.QEU6/OP* B*CS8Y9SDDCFMY7RJMO*GME*OH:GISD%%2*\$P48W 3D\$ZG*MROC3GOIZGN.T635J100S/SV404+S860QP70000000000000000000 00000UAK9JVSS\$IDX7PI3Z5PRO06%G9G2TAABAKRL0U+OX Q3.SSV49Q8IYTEG5LSEN/1FG34B2 F1L*H5+8 /AVRQNX+L20XUXU6
		<p>Modules (sans quiet zone) : 61 × 61</p> <p>Taille totale (avec quiet zone) : 40 mm × 40 mm</p> <p>Taille des modules : 22,8 mil (0,580 mm)</p>

## VII.2.10 Exemple 7 : 16 secteurs (1, 4, 7 à 14, 20 à 25), authentification complète

Données à encoder	274 octets	'3001F83FC9FEF0FEF002250E0020231231CB32075301EDEE43A40CF9A125102112B0F5586BCAFD8AFC963458A29D5964E113197B7E3836877F2CFEBC C2740417C56B07629D811B8A5F5D1EF11FF3DDA80742E2E3E503D6B6BAD 5082B0E280ED72268E8E294A257BF5AFD662A9230E9C62C89A9E7973D921 A31D0BC453E49C37A2EA4CAD8D52034CAC5EC5D7EDFBF4D33693AB0B5D 6F0C1C9B0FDC4C1865D6BD316A6CC69FE8C678084DCD99819EF92AAB8E2 34B9972F0001E52700D3E48801163BDE0000000000000000000000000 0000A014F89794FF3D391AFEC6C50453854412AB50F9A00103CCC4FED41F E4E1253343E3EB712A6B73BF0F8F1A9A11C50AB08D69465556CDD288EB49 13ABF31B34DD'h
Structure complète	415 caractères	AMC1436BHV5OP:KUHFU U4W00NJ4CD6RE69MAP3U O8 S1XGKY12EG2X0V9SDG2W.- VZR64PKODBJKS/932/F9+6L3G79WAQOCN04/O0.01-JUL3N2C1-3Y14:OSD- 0XUS\$.SL6R*RNL11OZ1J*1XF4%JTPZI84BSMB9-CTLI-OTGS5PLLH5J7LIHD62 NF*72WOF+5/SPK.QEU6/OP* B*CS8Y9SDDCFMY7RJMO*GME*OH:GISD%%2*\$P48W 3D\$ZG*MROC3GOIZGN.T635J100S/SV404+S860QP70000000000000000000 00000UAK9JVS\$IDX7PI3Z5PRO06%G9G2TAABAKRL0U+OX Q3.SSV49Q8IYTEG5LSEN/1FG34B2 F1L*H5+8 /AVRQNX+L20XUXU6
		Modules (sans quiet zone) : 65 × 65 Taille totale (avec quiet zone) : 40 mm × 40 mm Taille des modules : 21,6 mil (0,548 mm)

## VII.2.11 Comparaison

Taille totale fixe : impression en 20 mm × 20 mm ou affichage en 40 mm × 40 mm (avec quiet zone)

Exemple 1	Exemple 2	Exemple 3
		
29 × 29 21,3 mil (0,541 mm)	41 × 41 16,1 mil (0,408 mm)	61 × 61 22,8 mil (0,580 mm)
Exemple 4	Exemple 5	Exemple 6
		
33 × 33 19,2 mil (0,488 mm)	49 × 49 13,8 mil (0,351 mm)	61 × 61 22,8 mil (0,580 mm)
		Exemple 7
		
		65 × 65 21,6 mil (0,548 mm)

Taille de module fixe : 20 mil (0,508 mm)

<p>Exemple 1</p>  <p>29 × 29 18,8 mm × 18,8 mm</p>	<p>Exemple 2</p>  <p>41 × 41 24,9 mm × 24,9 mm</p>	<p>Exemple 3</p>  <p>61 × 61 35,1 mm × 35,1 mm</p>
<p>Exemple 4</p>  <p>33 × 33 20,8 mm × 20,8 mm</p>	<p>Exemple 5</p>  <p>49 × 49 29,5 mm × 29,5 mm</p>	<p>Exemple 6</p>  <p>61 × 61 35,1 mm × 35,1 mm</p>
		<p>Exemple 7</p>  <p>65 × 65 37,1 mm × 37,1 mm</p>