

**NORME « APPLICATION MULTISERVICES CITOYENNE »
IMPLÉMENTATION SUR AUTRES SUPPORTS (NON CALYPSO)**



LISTE DES RÉVISIONS

Version	Date	Modifications
1	12/10/2023	Première version, issue du document réf. 210315-ADCET-NormeAMC-Mobile v2.8.
1.1	25/03/2024	Clarification du calcul de la signature statique. Correction du texte encodé de certains exemples. Correction et améliorations éditoriales.
1.2	16/06/2025	Ajout de la description de la présence des données dynamiques optionnelles. Les dates et heures sont en référence UTC. Ajout dans les données statiques d'un UID optionnel. Ajout d'un tableau indiquent les signatures à vérifier selon la sécurité visée. Réorganisation et améliorations éditoriales.

Table des matières

Table des matières	2
I. Introduction	4
I.1 Cas d'usage	4
I.2 Objet du document	4
I.3 Définitions	5
I.4 Présentation des technologies envisagées	5
I.4.1 CB2D (code-barres à deux dimensions)	5
I.4.2 Sans contact et NFC (« Near Field Communication »)	6
I.4.3 BLE (« Bluetooth Low Energy »)	7
II. Modes d'accès	8
II.1 Affichage d'un CB2D	8
II.2 Échanges en sans contact / NFC	9
II.3 Échanges en BLE	9
III. Données pour supports non Calypso	10
III.1 Présentation	10
III.1.1 Entête, partie statique, partie dynamique	10
III.1.2 Partie statique	11
III.1.3 Partie dynamique	12
III.2 Structure de données détaillée	12
III.3 Unicité des identifiants prédéfinis	16
III.4 Identification du jeu d'identifiants prédéfinis	16
III.5 Taille des données encodées	17
III.6 Cryptographie	17
IV. Sécurité	19
IV.1 Menaces	19
IV.2 Contre-mesures	19

IV.2.1	Traçabilité.....	19
IV.2.2	Contrefaçon et clonage	20
V.	Outils	21
V.1	Cryptographie : OpenSSL	21
V.2	Encodage et décodage.....	21
VI.	Évolutions recommandées	22
VI.1	Utilisation de données circonstanciées sur téléphone mobile.....	22
VI.1.1	Amélioration contre le clonage en CB2D ou en BLE	22
VI.1.2	Obtention de données circonstanciées pour la lecture en CB2D ou BLE.....	22
VI.2	Sans contact / NFC : mode PKI de Calypso Prime Revision 3	22
VI.3	Données CB2D/BLE accessibles en NFC.....	23
VI.3.1	Geste volontaire en BLE.....	23
VII.	Annexes.....	24
VII.1	La norme AMC	24
VII.1.1	Publication.....	24
VII.1.2	Secteurs d'activité	24
VII.1.3	Structures de données	25
VII.1.4	Conteneur Calypso.....	25
VII.1.5	Niveaux de sécurité	26
VII.1.6	Types d'AMC.....	26
VII.2	Exemples.....	27
VII.2.1	Clés utilisées	27
VII.2.2	Données.....	28
VII.2.3	Taille apparente des CB2D	30
VII.2.4	Exemple 1 : cinq secteurs (1, 4, 5, 7 et 9), pas d'authentification	30
VII.2.5	Exemple 2 : cinq secteurs (1, 4, 5, 7 et 9), authentification statique seulement	31
VII.2.6	Exemple 3 : cinq secteurs (1, 4, 5, 7 et 9), authentification complète	31
VII.2.7	Exemple 4 : dix secteurs (1, 4, 5, 7, 9, 11 à 14, 22), pas d'authentification.....	32
VII.2.8	Exemple 5 : dix secteurs (1, 4, 5, 7, 9, 11 à 14, 22), authentification statique seulement.....	32
VII.2.9	Exemple 6 : dix secteurs (1, 4, 5, 7, 9, 11 à 14, 22), authentification complète	33
VII.2.10	Exemple 7 : 17 secteurs (1, 4, 5, 7 à 14, 20 à 25), authentification complète	34
VII.2.11	Comparaison des CB2D	35

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.

Cette spécification s'applique entre autres au cas d'un code-barres imprimé, dit **statique**, et au cas d'un code-barres évolutif, dit **dynamique**, affiché par un téléphone mobile.

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 ». Elle est disponible sur le site de l'AFNOR : [NF P 99-508](#).

Le groupe de travail ADCET consacré à l'AMC a validé la présente proposition d'évolution de la norme, qui permet d'utiliser pour les identifiants AMC des supports autres qu'une application Calypso¹, en s'appuyant autant que possible sur des solutions déjà décrites par les normes publiées ou en cours d'élaboration.

Le présent document est disponible sur le site de l'ADCET : [GT AMC](#).

1 Hébergée dans une carte sans contact, ou dans une carte « virtuelle » d'un téléphone mobile.

Technologies

Parmi les technologies de communication disponibles, ce document considère uniquement les trois suivantes :

- **CB2D** *Codes-barres à deux dimensions*
- **Sans contact / NFC** *Near Field Communication, étendue aux supports non Calypso*
- **BLE** *Bluetooth Low Energy*

Limitations

La gestion des identifiants personnalisés, des contrats AMC et du journal AMC n'est pas retenue pour l'utilisation avec les supports non Calypso.

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** »².

I.4 Présentation des technologies envisagées

I.4.1 CB2D (code-barres à deux dimensions)

Le code-barres à deux dimensions (CB2D) est une solution applicable à tous les téléphones mobiles. Il s'agit d'afficher 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 CB2D. Une solution courante est l'utilisation d'un lecteur optique qui émule une saisie au clavier, et transmet donc principalement des caractères alphanumériques.

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.

1.4.2 Sans contact et NFC (« Near Field Communication »)

Le **sans contact** recouvre le protocole défini par la norme ISO/IEC 14443, ainsi que ses variantes propriétaires³.

La technologie **NFC** est conçue pour les objets disposant d'une source d'énergie, comme les téléphones mobiles. Elle inclut une implémentation de la norme ISO/IEC 14443 : le **mode émulation carte**.

Dans le téléphone, une carte virtuelle peut être logée dans un conteneur conforme à la norme ISO/IEC 7816-4. Ce conteneur est implémenté soit dans une app HCE⁴, soit dans un élément sécurisé du téléphone (« eSE », « embedded secure element »).



Lorsque la carte virtuelle est une AMC Calypso, la norme AMC actuelle s'applique directement. La présente proposition ne concerne que les cas où la carte virtuelle n'est pas conforme au standard Calypso.

Le sans contact et le NFC présentent 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 sur téléphone mobile pour les services acceptant déjà des AMC sur carte Calypso ;
- meilleure ergonomie, car il suffit d'approcher le support du terminal⁵ ;
- possibilité d'authentifier le support sans SAM (depuis Calypso Prime Revision 3.3, voir chapitre VI.2) ;

Utilisation d'un élément sécurisé

Dans un élément sécurisé (eSE), le conteneur de l'AMC 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 (généralement de fabricant du téléphone : Samsung, etc.).

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

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

En mode HCE, le conteneur de l'AMC est une carte virtuelle implémentée dans une app du téléphone (aucun logiciel spécifique à ce conteneur n'est installé dans l'élément sécurisé du téléphone).

Cette carte virtuelle est accessible via l'interface NFC du téléphone, comme pour une carte sans contact⁶.

L'app assume également les fonctions d'un terminal AMC n'ayant pas de SAM, ou connecté à un serveur éventuellement équipé d'un SAM.

3 La variante la plus commune est celle des cartes Mifare de NXP, qui est proche du type A de la norme ISO/IEC 14443.

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

5 Pour les téléphones mobiles, 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.

6 Il est recommandé de limiter cet accès aux fonctions de lecture et de débit, et de réaliser toutes les fonctions de personnalisation et de rechargement en interaction avec un serveur de sécurité, afin de réduire les risques en cas de tentatives de piratage de l'app ou du système d'exploitation du téléphone. C'est le choix fait pour les applications Calypso HCE, qui implémentent également des mécanismes de sécurité supplémentaires.

Principale limite du NFC

La plupart des téléphones mobiles disposent d'une interface NFC, mais pas la totalité. Certains usagers pourraient donc ne pas avoir accès à cette solution technique.

NB : Depuis l'été 2024, Apple a rendu son API d'émulation de carte sans contact en mode HCE disponible à des acteurs tiers, au sein de l'Espace Économique Européen. Cette solution n'est donc plus limitée aux téléphones Android. L'utilisation de l'élément sécurisé du téléphone reste néanmoins complexe, pour tous les systèmes d'exploitation, puisqu'elle nécessite la collaboration du fabricant du téléphone ⁸.

I.4.3 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 ⁹.

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



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).
- 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.

⁸ Apple et Samsung l'ont rendu possible 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.

⁹ 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.

II. Modes d'accès

II.1 Affichage d'un 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 ¹⁰	« 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 mil¹¹) recommandé
Taille maximale du code-barres ¹² , zone vierge comprise	40 mm × 40 mm recommandé
Nombre maximal de modules (hors zone vierge)	69 × 69 modules recommandé¹³
Taille maximale des données	483 caractères alphanumériques¹⁴

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.

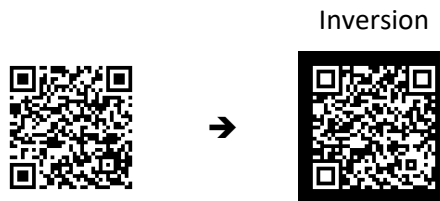
Pour optimiser la lisibilité du CB2D, il est recommandé d'utiliser un nombre entier de points par module lorsque le système de génération de codes-barres le permet, sans compromettre significativement les autres recommandations.

-
- 10 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.
- 11 1 mil = 1/1000 de pouce = 0,254 mm.
- 12 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.
- 13 Nombre le plus proche correspondant à un code-barres de 40 mm × 40 mm ayant des modules de 20 mil.
- 14 Taille correspondant à un code-barres de 69 × 69 modules avec le taux de correction d'erreur « M ».

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.2 Échanges en sans contact / NFC

Les données de l'AMC sont présentes dans la carte sans contact, ou dans la carte virtuelle. Elles sont lues par les terminaux AMC conformément aux spécifications de cette carte.

Dans le cas d'une carte Calypso, la norme AMC actuelle s'applique directement.

Pour une carte non Calypso, les données sont décrites au chapitre III. Afin de permettre l'interopérabilité des solutions techniques proposées par les industriels, une version ultérieure de la norme :

- définira les types de carte pour lesquels une normalisation est pertinente, et
- décrira les mécanismes de stockage et de lecture des données pour chaque type de carte retenu.

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.

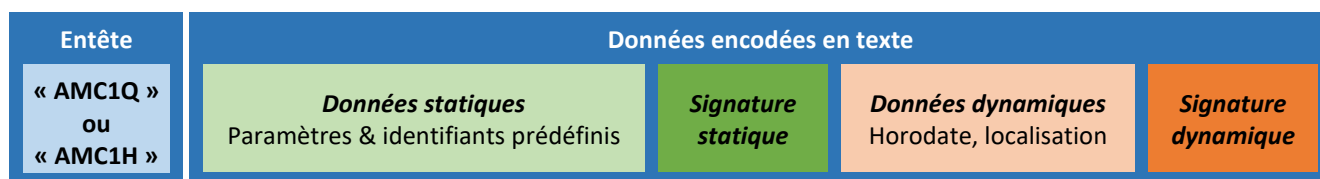
III. Données pour supports non Calypso

III.1 Présentation

III.1.1 Entête, partie statique, partie dynamique

Les données présentes dans un support non Calypso sont décomposées en deux parties :

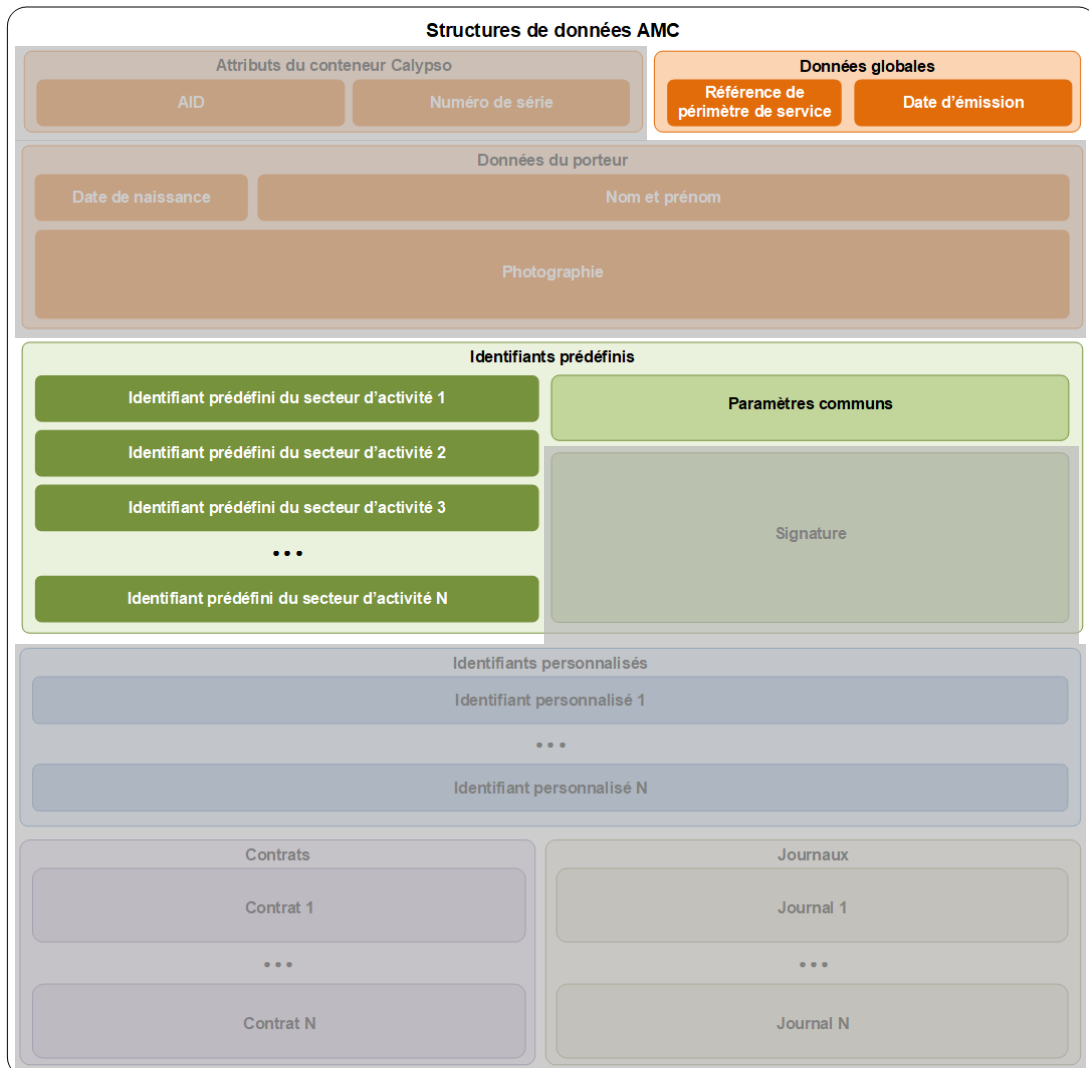
- **Entête**, composé cinq caractères indiquant que les données relèvent de la norme AMC, une version pour d'éventuelles évolutions, et un indicateur de codage des données.
- **Données**, suite de caractères encodant les données effectives de l'AMC :
 - **Données statiques, et leur signature optionnelle**, présentes pour l'impression et pour l'affichage. Elles sont générées par un système central. Elles incluent principalement les identifiants prédéfinis de l'AMC et les paramètres qui garantissent leur unicité, et si nécessaire des paramètres de sécurité (clé publique du support, pour vérifier la signature dynamique). Lorsqu'elle présente, la signature statique authentifie les données statiques.
 - **Données dynamiques et leur signature, optionnelles**, présentes seulement pour l'affichage. Elles sont générées périodiquement par le support. Elles incluent principalement la date et l'heure courante. La signature dynamique authentifie l'ensemble des données, statiques et dynamiques ¹⁵ ; elle est calculée par le support.



15 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).

III.1.2 Partie statique

Dans un support non Calypso, les données qui permettent l'identification du support sont un sous-ensemble des données définies dans la norme AMC actuelle :



L'objectif est de réduire la quantité de données utilisées du fait de la capacité de stockage limitée des supports non Calypso (voir chapitre III.4), tout en restant en mesure d'identifier que les données concernent une AMC, de garantir l'unicité et la non corrélation des identifiants de chaque secteur d'activité, et de disposer à minima des secteurs d'activité indispensables pour l'usage envisagé.

Données statiques

Les données statiques d'une AMC sur support non Calypso sont :

- la configuration des données optionnelles,
- la référence de l'émetteur de l'AMC, telle que définie dans la norme AMC actuelle,
- les identifiants prédéfinis et leurs paramètres communs, dont leur date de début de validité, tels que définis dans la norme AMC actuelle,
- en option, la clé publique permettant de vérifier la signature dynamique.

Pour limiter autant que possible la quantité de données, les autres données définies par la norme AMC actuelle sont absentes des supports non Calypso.

Signature statique

La signature statique, optionnelle, est calculée par un système central. Elle assure la même fonction que la signature des identifiants prédéfinis de la norme AMC actuelle.

III.1.3 Partie dynamique

Données dynamiques

Lorsqu'elles sont présentes, les données dynamiques d'une AMC sur support non Calypso contiennent une, deux ou trois des informations suivantes :

- la date et l'heure de génération de la signature dynamique,
- la position géographique au moment de la génération de la signature dynamique,
- des données définies par l'émetteur de l'AMC.

La valeur de ces données est déterminée par le support lui-même, éventuellement à partir d'informations d'un fournisseur tiers (par exemple des données circonstancielles, voir chapitre VI.1.2).

Signature dynamique

La signature dynamique est présente si et seulement les données dynamiques sont présentes. Elle est calculée par le support lui-même, et prouve son authenticité. Elle assure la même fonction que le mécanisme de session sécurisée des supports Calypso.

III.2 Structure de données détaillée

La structure de données se divise en deux parties principales :

- Un entête constitué d'une chaîne de caractères alphanumériques qui référence l'AMC, et qui indique le codage des données qui suivent et la version de leur structure.
- Les données elles-mêmes, qui sont constituées d'une suite d'octets ordonnés par index croissant et commençant à l'index 0, encodés selon le codage indiqué par l'entête. 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 ».	
Codage	1	Codage des données qui suivent ce champ « B » : pas d’encodage « H » : texte hexadécimal « Q » : texte Base45, optimal pour la symbologie QR Code « X », « Y », « Z » : codage propriétaire Les autres valeurs sont interdites.	
Données binaires à encoder ou décodées selon le champ Codage			
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 Présence de UidValue. b36 Présence de StaticSignature, obligatoire lorsque b37=1. b37 Présence de PublicKey, et de DynamicDateTime à DynamicSignature selon leur taille, toujours = 0 pour un CB2D imprimé b38 et b39 Réservés, toujours égaux à 0 (ignorés à la lecture).	Obligatoire
GDIssuerReference	2	Référence de l’émetteur de l’AMC	Obligatoire
PIDIssuerReference	2	Référence de l’émetteur des identifiants prédéfinis.	Obligatoire
PIDVersion	1	‘02’h, version de la structure de données Predefined Ids.	
PIDScopeID	3	Identifiant du périmètre de l’application.	
PIDStartDate	4	Date UTC de début de validité des identifiants prédéfinis (encodée YYYYMMDD en BCD), valorisée à la date de génération de la signature statique.	
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 Présente ou non selon le bit correspondant de Configuration	Optionnel
PIDSector2Value	0 ou 4	Valeur de l'identifiant pour le secteur d'activité n° 2 Présente ou non selon le bit correspondant de Configuration	Optionnel
...	...	...	...
PIDSector35Value	0 ou 4	Valeur de l'identifiant pour le secteur d'activité n° 35 Présente ou non selon le bit correspondant de Configuration	Optionnel
PublicKey	0 ou 33	Valeur de la clé publique du support, au format avec compression de point. Utilisée pour vérifier la signature dynamique. Présente ou non selon le bit b37 de Configuration.	Optionnel
UidValue	0 ou 4	Identifiant du jeu d'identifiants prédéfinis (voir chapitre III.4). Présent ou non selon le bit b35 de Configuration	Optionnel
StaticSignature	0 ou 64	Signature ECDSA des champs Format à PublicKey, calculée avec la paire ECC de l'autorité du périmètre de service. Pour ce calcul : – Les champ de l'entête sont signés selon leur codage ASCII. – Le champ Codage est valorisé à « B », quelle que soit la valeur présente dans le support. – Les données binaires ne sont pas encodées. Présente ou non selon le bit b36 de Configuration.	Optionnel
DynamicDateTime	0 ou 4	Date et heure UTC de génération de la signature dynamique, en nombre de secondes écoulées depuis 0 h à la date de génération de la signature statique (PIDStartDate). La valeur 'FFFFFFFF'h est interdite. Obligatoirement absente si bit b37 de Configuration =0.	Optionnel
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' Obligatoirement absente si bit b37 de Configuration =0.	

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 'FFFFFFF'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' Obligatoirement absente si bit b37 de Configuration =0.
DynamicFreeData	0 ou 16	Données libres, non interopérables. Obligatoirement absentes si bit b37 de Configuration =0.
DynamicSignature	0 ou 64	Signature ECDSA dynamique des données StaticSignature à DynamicFreeData, calculée avec la paire ECC de l'app. Présente ou non selon le bit b37 de Configuration.

Données dynamiques : présence des champs optionnels

Lorsque la signature dynamique est présente (dans Configuration, b37=1), au moins un des champs DynamicDateTime, DynamicLatitude, DynamicLongitude et DynamicFreeData doit également être présent ¹⁷.

La présence de ces quatre champs se déduit du nombre d'octets entre les deux signatures :

Nombre d'octets	DynamicDateTime	DynamicLatitude et DynamicLongitude ¹⁸	DynamicFreeData
4	Présent	Absents	Absent
8	Absent	Présents	Absent
12	Présent	Présents	Absent
16	Absent	Absents	Présent
20	Présent	Absents	Présent
24	Absent	Présents	Présent
28	Présent	Présents	Présent

¹⁷ Lorsque la signature dynamique est absente (dans Configuration, b37=0), les quatre champs DynamicDateTime, DynamicLatitude, DynamicLongitude et DynamicFreeData doivent également être absents.

¹⁸ Les champs DynamicLatitude et DynamicLongitude sont liés : la présence de l'un impose la présence de l'autre.

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 Identification du jeu d'identifiants prédéfinis

Le champ UidValue est présent lorsque le bit b35 de Configuration =1. Il identifie le jeu d'identifiants prédéfinis qu'il accompagne.

Cas d'usage

- Identification dans le système de gestion des supports, par exemple lorsque les mêmes identifiants prédéfinis sont utilisés dans des supports différents alloués au même usager. Si cet UID est lisible par l'utilisateur, il peut simplifier les échanges avec les agents de SAV.
- Anti-clonage à minima, si l'UID est présent sur le support, car les agents des services peuvent comparer l'UID présent sur le support à celui extrait du CB2D et affiché sur leur propre terminal. Cette protection reste néanmoins limitée par la capacité d'un fraudeur à falsifier l'UID présent sur son support et à y dupliquer le CB2D d'un autre support.

Attention

L'identifiant UidValue ne doit pas être utilisé pour gérer les services eux-mêmes, comme pour le numéro de série Calypso d'une AMC conforme à la norme actuelle.

Valeurs de UidValue

La valeur de UidValue est calculée comme pour les identifiants prédéfinis, en prenant 0 comme numéro de secteur d'activité.

Unicité de UidValue

De façon similaire aux identifiants prédéfinis, l'identifiant complet est la concaténation de UidType, PIDScopeID, PIDKeyRef et UidValue. Il est donc possible d'omettre les premiers champs, selon les règles du §III.3.

III.5 Taille des données encodées

Code-barres

Moins un CB2D contient d'information, plus il est lisible. Pour les caractéristiques recommandées au 7II.1, les données encodées ne doivent pas dépasser **483 caractères alphanumériques**.

Or, avec les 35 secteurs d'activité de l'AMC commune de la norme actuelle, la structure complète (avec tous les champs optionnels) définie ci-dessus comporte au moins **530 caractères alphanumériques**.

Afin d'améliorer la lisibilité du CB2D, il est donc recommandé de ne pas inclure tous les secteurs d'activité. Par exemple, avec 17 secteurs, la taille des données encodées est de 422 caractères. C'est le choix fait dans l'exemple 7 du chapitre VII.2.10.

Carte sans contact non Calypso

Pour certaines cartes sans contact non Calypso susceptibles d'être utilisées dans des solutions techniques existantes, l'espace disponible pour des données d'AMC peut être de seulement 128 octets.

Réduire les données AMC afin de les loger dans un tel support requiert d'omettre la signature statique (qui utilise, au minimum, 96 caractères) et d'utiliser au plus 12 secteurs d'activité.

III.6 Cryptographie

Le tableau suivant indique, selon le niveau de sécurité qu'un terminal accepteur doit atteindre, quelles signatures il doit vérifier, et avec quelles clés :

Niveau de sécurité visé	Signature statique		Signature dynamique	
	Vérification nécessaire ?	Clé utilisée	Vérification nécessaire ?	Clé utilisée
Lecture sans authentification	Non	—	Non	—
Authentification des données	Oui	Clé publique PIDSignKeyReference	Non	—
Authentification du support	Oui	Clé publique PIDSignKeyReference	Oui	Clé publique de l'app

Comme indiqué au §IV.2.2 :

- Le niveau « Authentification des données » ne protège que de la contrefaçon. Il ne permet pas de rejeter un support contenant des données clonées.
- Pour le niveau « Authentification du support », la vérification de la signature statique étant nécessaire pour authentifier la clé publique de l'app, ce niveau protège à la fois du clonage et de la contrefaçon.

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 (PIDScopeID) 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 et des terminaux accepteurs. Son identifiant est PIDSignKeyReference¹⁹.

La paire de clés ECC pour la signature dynamique (DynamicSignature) est propre à l'app et générée par l'app elle-même. La clé publique de cette paire est envoyée par l'app à son serveur d'enrôlement. Ce serveur l'inclut dans les données statiques (champ PublicKey) qu'il fournit à l'app.

Format avec compression de point

Dans les données encodées, la clé publique de l'app (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#subsubsection.2.3.3>
- Règle de décodage d'une chaîne d'octets en point de courbe elliptique :
<https://www.secg.org/sec1-v2.pdf#subsubsection.2.3.4>

19 Pour l'AMC commune, actuellement trois clés publiques sont définies, d'identifiants PIDSignKeyReference='1A01'h, '1A02'h et '1A03'h. Elles sont disponibles sur le site de l'ADCET (<https://www.adcet.org/fr/amc/la-norme/faq/58-amc-commune/1090-quelles-sont-les-cles-pour-les-identifiants-predefinis-de-l-amc-commune>).

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.

IV.2 Contre-mesures

IV.2.1 Traçabilité

Affichage d'un CB2D

Le CB2D n'est affiché sur l'écran d'un 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 plan²⁰, 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 protection²¹ :

- 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.

²⁰ Actuellement, sous Android cette obligation est doit être assurée par l'application mobile.

²¹ 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.

IV.2.2 Contrefaçon et clonage

Les contre-mesures définies aux chapitres précédents consistent en l'utilisation de deux signatures optionnelles :

- La *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.
- La *signature dynamique* protège contre le **clonage**. Elle remplit une fonction proche de celle de la session sécurisée Calypso et prouve que le support est authentique. Lorsqu'elle est basée sur des données éphémères (par exemple une horodate) et sur des données de localisation (par exemple la position géographique), elle assure que le support est authentique « ici et maintenant ».

NB : Le support n'est authentique que **si les deux signatures sont correctes**. En effet, la signature dynamique n'est authentique que si la clé publique de l'app, présente dans les données statiques (PublicKey), est également authentique (ce qui est démontré en vérifiant la signature statique).

Ces mécanismes correspondent aux trois niveaux de sécurité définis par la norme AMC (voir chapitre VII.1.5).

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.jspx	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.onlinebarcode reader.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.

VI. Évolutions recommandées

VI.1 Utilisation de données circonstanciellles sur téléphone mobile

VI.1.1 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.1.2.
- Réponse : identique au challenge, résultat d'un calcul à partir du challenge (par exemple les 8 premiers octets du SHA-256 des informations reçues).

VI.1.2 Obtention de données circonstanciellles pour la lecture en CB2D ou BLE

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

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 BLE²², si nécessaire contrôlée par le terminal AMC (par exemple dans le cas d'un challenge, voir chapitre VI.1.1).

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

VI.2 Sans contact / 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 (la liste tenue à jour des cartes certifiées est disponible à la page cna-paycert-certification.eu/card).

Ce mode pourrait également être implémenté dans une carte virtuelle (HCE ou eSE).

22 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, la norme expérimentale XP P99-520 décrit ce type d'étiquette/balise au format CB2D, et des travaux sont en cours au sein du groupe de travail BNTRA/CN03/GT4 pour une transposition en NFC ou en BLE.

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.

VI.3.1 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.1.2 (sauf la géolocalisation).

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 : [NF P 99-508](#).

VII.1.2 Secteurs d'activité

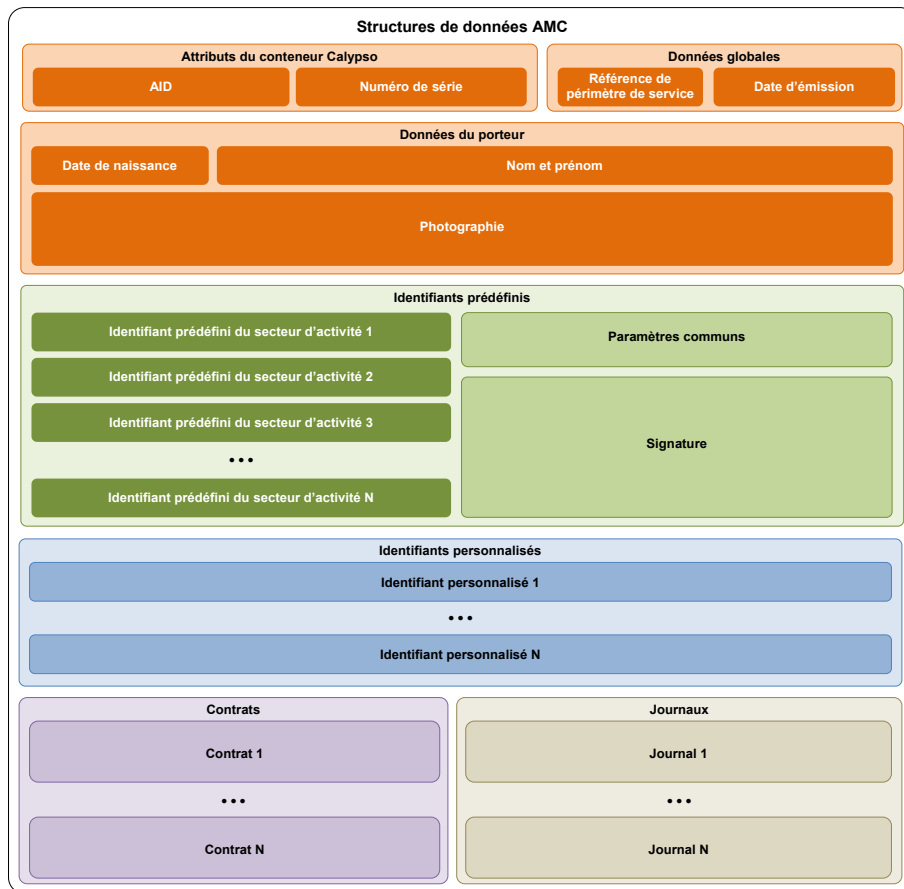
La norme AMC décrit des structures de données contenant un ensemble d'identifiants.

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.

Définition	Numéro	Secteur
CNIL (Services publics)	1	Fiscalité
	2	Travail et social
	3	Santé
	4	Transports
	5	État civil et citoyenneté
	6	Relations avec les élus
	7	Prestations scolaires/périscolaires, activités sportives/socioculturelles
	8	Économie et urbanisme
	9	Polices spéciales et voirie
	10	Relations avec les usagers
Norme AMC (Services privés ou mixtes)	11	Services aux agents (carte agent)
	12	Services de la vie étudiante
	13	Fidélité et commerce
	14	Mobilité (Maas)
	15 à 19	Réservés pour une définition future Services Publics
	20	Services à la personne
	21	Transports privés
	22	Paiements
	23	Réseaux sociaux
	24	Activités sportives, culturelles et loisirs
	25	Programme de fidélité (hors contexte « cœur de villes »)
	26 à 30	Réservés pour une définition future par la norme AMC
	31 à 61439	Disponibles pour la définition de services spécifiques (non normalisés)
	61440 à 65535	Réservés pour une définition future par la norme AMC

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 publics²³) et dans les téléphones NFC.

23 Cartes Pass Pass en Hauts de France, Korrigo en Bretagne, OURA en Auvergne Rhône-Alpes, Navigo en Île-de-France, etc.

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 :

<i>Authentification</i>	<i>Traitement</i>	<i>Protection</i>
Aucune	Lecture des données de l'AMC sans vérification de la signature ni authentification du conteneur Calypso	La sécurité repose entièrement sur le système d'information
Statique	Lecture des données de l'AMC avec vérification de la signature mais sans authentification du conteneur Calypso	Le terminal peut détecter les identifiants contrefaits , mais pas les identifiants clonés ni les fausses cartes
Complète	Lecture des données de l'AMC avec vérification de la signature et authentification du conteneur Calypso ²⁴	Le terminal peut détecter les identifiants contrefaits , les identifiants clonés , et les fausses cartes

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.

²⁴ 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	89575E94AC5B05F8C607F5BB2DEF11C27D4563CB2F7C1AFDC34636BC226FF405
	Y	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	D6B6BAD5082B0E280ED72268E8E294A257BF5AFD662A9230E9C62C89A9E7973D
	Y	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.

VII.2.2 Données

Champ	Taille (octets)	Valeur	Remarque
Entête en caractères alphanumériques			
Format	3	« AMC »	
Version	1	« 1 »	
Codage	1	« Q »	Base45, optimal pour QR Code
Données binaires à encoder ou décodées en Base45 (selon le champ Codage)			
Configuration	5	Exemple 1 : '000000159'h Exemple 2 : '100000159'h Exemple 3 : '300000159'h Exemple 4 : '0000203D59'h Exemple 5 : '1000203D59'h Exemple 6 : '3000203D59'h Exemple 7 : '3001F83FD9'h	Exemple 1 : 5 secteurs (1, 4, 5, 7 et 9), sans signature Exemple 2 : 5 secteurs (1, 4, 5, 7 et 9), signature statique seulement Exemple 3 : 5 secteurs (1, 4, 5, 7 et 9), signatures statique & dynamique Exemple 4 : 10 secteurs (1, 4, 5, 7, 9, 11 à 14, et 22), sans signature Exemple 5 : 10 secteurs (1, 4, 5, 7, 9, 11 à 14, et 22), signature statique seulement Exemple 6 : 10 secteurs (1, 4, 5, 7, 9, 11 à 14, et 22), signatures statique & dynamique Exemple 7 : 17 secteurs (1, 4, 5, 7 à 14, 20 à 25), signatures 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 : '01EDEC43'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.6)
StaticSignature	0 ou 64	'921A31D0BC453E49 C37A2EA4CAD8D520 34CAC5EC5D7EDFBF 4D33693AB0B5D6F0 C1C9B0FDC4C1865D 6BD316A6CC69FE8C 678084DCD99819EF 92AAB8E234B9972F'h	Valeur factice arbitraire

DynamicDateTime	0 ou 4	'0001E527'h	1 ^{er} 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 des CB2D

Dans les exemples ci-après, les codes-barres sans signature dynamique sont supposés *imprimés* dans un carré de 20 mm de côté, et 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 : cinq secteurs (1, 4, 5, 7 et 9), pas d'authentification

Données à encoder	41 octets	'0000000159FEF0FEF002250E0020231231CB32075301EDEE43A40CF9A1357194EC25102112CAFD8AFC'h	
Structure complète	67 caractères	AMC1Q000100/GB:KUHFU U4W00NJ4CD6RE69MAP3U O8S14HK6GEI%TY12+G2G2WR5	
		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.2.5 Exemple 2 : cinq secteurs (1, 4, 5, 7 et 9), authentification statique seulement

Données à encoder	105 octets	'1000000159FEF0FEF002250E0020231231CB32075301EDEE43A40CF9A1357194EC25102112CAFD8AFC921A31D0BC453E49C37A2EA4CAD8D52034CAC5EC5D7EDFBF4D33693AB0B5D6F0C1C9B0FDC4C1865D6BD316A6CC69FE8C678084DCD99819EF92AAB8E234B9972F'h
Structure complète	163 caractères	AMC1Q112100/GB:KUHFU U4W00NJ4CD6RE69MAP3U O8 S14HK6GEI%TY12+G2G2W%-V0E3LHQ- X8SE93KFL\$KOIR934OSPT*TY1GD8OLM6*I7K:MSJUHMP3W.KOK B%UQ+3L:HDXXH5BGH-RCAJ+CU9QL%QS KN21
		Modules (sans quiet zone) : 45 × 45 Taille totale (avec quiet zone) : 20 mm × 20 mm Taille des modules : 14,9 mil (0,377 mm)

VII.2.6 Exemple 3 : cinq secteurs (1, 4, 5, 7 et 9), authentification complète

Données à encoder	230 octets	'3000000159FEF0FEF002250E0020231231CB32075301EDEE43A40CF9A1357194EC25102112CAFD8AFC03D6B6BAD5082B0E280ED72268E8E294A257BF5AFD662A9230E9C62C89A9E7973D921A31D0BC453E49C37A2EA4CAD8D52034CAC5EC5D7EDFBF4D33693AB0B5D6F0C1C9B0FDC4C1865D6BD316A6CC69FE8C678084DCD99819EF92AAB8E234B9972F0001E52700D3E48801163BDE0000000000000000000000000000000A014F89794FF3D391AFEC6C50453854412AB50F9A00103CCC4FED41FE4E1253343E3EB712A6B73BF0F8F1A9A11C50AB08D69465556CDD288EB4913ABF31B34DD'h
Structure complète	350 caractères	AMC1Q336100/GB:KUHFU U4W00NJ4CD6RE69MAP3U O8 S14HK6GEI%TY12+G2G2WU%VL6R*RNL11OZ1J*1XF4%JTPZI84BSMB9-CTLI- OTGS5PLLH5J7LIHD62 NF*72WOF+5/SPK.QEU6/OP* B*CS8Y9SDDCFMY7RJMO*GME*OH:GISD%2*\$P48W 3D\$ZG*MROC3GOIZGN.T635J100S/SV404+S860QP70000000000000000000000000000000UAK9JVS\$IDX7PI3Z5PRO06%G9G2TAABAKRL0U+OX Q3.SSV49Q8IYTEG5LSEN/1FG34B2 F1L*H5+8 /AVRQNXT+L20XUXU6
		Modules (sans quiet zone) : 61 × 61 Taille totale (avec quiet zone) : 40 mm × 40 mm Taille des modules : 22,8 mil (0,580 mm)

VII.2.7 Exemple 4 : dix secteurs (1, 4, 5, 7, 9, 11 à 14, 22), pas d'authentification

Données à encoder	61 octets	'0000203D59FEF0FEF002250E0020231231CB32075301EDEE43A40CF9A1357194EC25102112CAFD8AFC9D5964E113197B7E3836877F2CFEBCC2811B8A5F'h
Structure complète	97 caractères	AMC1Q000I34/GB:KUHFU U4W00NJ4CD6RE69MAP3U O8 S14HK6GEI%TY12+G2G2W4.VODBJKS/932/F9+6L3G79WNQOUL352
		Modules (sans quiet zone) : 37 × 37 Taille totale (avec quiet zone) : 20 mm × 20 mm Taille des modules : 17,5 mil (0,444 mm)

VII.2.8 Exemple 5 : dix secteurs (1, 4, 5, 7, 9, 11 à 14, 22), authentification statique seulement

Données à encoder	125 octets	'1000203D59FEF0FEF002250E0020231231CB32075301EDEE43A40CF9A1357194EC25102112CAFD8AFC9D5964E113197B7E3836877F2CFEBCC2811B8A5F921A31D0BC453E49C37A2EA4CAD8D52034CAC5EC5D7EDFBF4D33693AB0B5D6F0C1C9B0FDC4C1865D6BD316A6CC69FE8C678084DCD99819EF92AAB8E234B9972F'h
Structure complète	193 caractères	AMC1Q112I34/GB:KUHFU U4W00NJ4CD6RE69MAP3U O8 S14HK6GEI%TY12+G2G2W4.VODBJKS/932/F9+6L3G79WNQOUL3V3C0E3LH Q-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 : dix secteurs (1, 4, 5, 7, 9, 11 à 14, 22), authentification complète

Données à encoder	250 octets	'3000203D59FEF0FEF002250E0020231231CB32075301EDEC43A40CF9A1357194EC25102112CAFD8AFC9D5964E113197B7E3836877F2CFEBCC2811B8A5F03D6B6BAD5082B0E280ED72268E8E294A257BF5AFD662A9230E9C62C89A9E7973D921A31D0BC453E49C37A2EA4CAD8D52034CAC5EC5D7EDFBF4D33693AB0B5D6F0C1C9B0FDC4C1865D6BD316A6CC69FE8C678084DCD99819EF92AAB8E234B9972F0001E52700D3E48801163BDE00000000000000000000000000000A014F89794FF3D391AFEC6C50453854412AB50F9A00103CCC4FED41FE4E1253343E3EB712A6B73BF0F8F1A9A11C50AB08D69465556CDD288EB4913ABF31B34DD'h
Structure complète	381 caractères	AMC1Q336I34/GB:KUHFU U4W00NJ4CD6RE69MAP3U O8 S14HK6GEI%TY12+G2G2W4.VODBJKS/932/F9+6L3G79WNQOUL3N0CL6R*R NL11OZ1J*1XF4%JTPZI84BSMB9-CTLI-OTGS5PLLH5J7LIHD62 NF*72WOF+5/SPK.QEU6/OP* B*CS8Y9SDDCFMY7RJMO*GME*OH:GISD%%2*\$P48W 3D\$ZG*MROC3GOIZGN.T635J100S/SV404+S860QP70000000000000000000000000000UAK9JVS\$IDX7PI3Z5PRO0 6%G9G2TAABAKRLOU+OX Q3.SSV49Q8IYTEG5LSEN/1FG34B2 F1L*H5+8 /AVRQNXT+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.2.10 Exemple 7 : 17 secteurs (1, 4, 5, 7 à 14, 20 à 25), authentification complète

Données à encoder	278 octets	'3001F83FD9FEF0FEF002250E0020231231CB32075301EDEE43A40CF9A1357194EC25102112B0F5586BCAFD8AFC963458A29D5964E113197B7E3836877F2CFEBCC2740417C56B07629D811B8A5F5D1EF11FF3DDA80742E2E3E503D6B6BAD5082B0E280ED72268E8E294A257BF5AFD662A9230E9C62C89A9E7973D921A31D0BC453E49C37A2EA4CAD8D52034CAC5EC5D7EDFBF4D33693AB0B5D6F0C1C9B0FDC4C1865D6BD316A6CC69FE8C678084DCD99819EF92AAB8E234B9972F0001E52700D3E48801163BDE00000000000000000000000000000000A014F89794FF3D391AFEC6C50453854412AB50F9A00103CC4FED41FE4E1253343E3EB712A6B73BF0F8F1A9A11C50AB08D69465556CD D288EB4913ABF31B34DD'h
Structure complète	422 caractères	AMC1Q436BHV6PR:KUHFU U4W00NJ4CD6RE69MAP3U O8 S14HK6GEI%TY12EG2X0V9SDG2W.- VZR64PKODBJKS/932/F9+6L3G79WAQOCN04/O0.01-JUL3N2C1-3Y14:0SD-0XUS\$.SL6R*RNL11OZ1J*1XF4%JTPZI84BSMB9-CTLI-OTGS5PLLH5J7LIHD62NF*72WOF+5/SPK.QEU6/OP* B*CS8Y9SDDCFMY7RJMO*GME*OH:GISD%%2*\$P48W 3D\$ZG*MROC3GOIZGN.T635J100S/SV404+S860QP70000000000000000000000000000000UAK9JVS\$IDX7PI3Z5PRO06%G9G2TAABAKRL0U+OX Q3.SSV49Q8IYTEG5LSEN/1FG34B2 F1L*H5+8 /AVRQNXT+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 des CB2D

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

Exemple 1  33 × 33 + 4 par côté 19,2 mil (0,488 mm)	Exemple 2  45 × 45 + 4 par côté 14,9 mil (0,377 mm)	Exemple 3  61 × 61 + 4 par côté 22,8 mil (0,580 mm)
Exemple 4  37 × 37 + 4 par côté 17,5 mil (0,444 mm)	Exemple 5  49 × 49 + 4 par côté 13,8 mil (0,351 mm)	Exemple 6  65 × 65 + 4 par côté 21,6 mil (0,548 mm)
		Exemple 7  65 × 65 + 4 par côté 21,6 mil (0,548 mm)

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

Exemple 1  33 × 33 + 4 par côté 20,8 mm × 20,8 mm	Exemple 2  45 × 45 + 4 par côté 26,9 mm × 26,9 mm	Exemple 3  61 × 61 + 4 par côté 35,1 mm × 35,1 mm
Exemple 4  37 × 37 + 4 par côté 22,9 mm × 22,9 mm	Exemple 5  49 × 49 + 4 par côté 29,5 mm × 29,5 mm	Exemple 6  65 × 65 + 4 par côté 37,1 mm × 37,1 mm
Exemple 7  65 × 65 + 4 par côté 37,1 mm × 37,1 mm		