# IAS TPC

Information Produit Edition Oct 08

## Introduction

**La carte IAS TPC de Gemalto répond aux exigences des applications d'identité et de sécurité basées sur les infrastructures à clé publique pour les administrations publiques européennes.**
Elle est notamment conforme aux exigences de l'administration française (Référentiel Général d'Interopérabilité et Référentiel General de Sécurité) et passe l'ensemble de la suite de tests définie pour l'administration française.

En particulier, la carte IAS TPC est 100% conforme aux **spécifications IAS ECC**, ainsi qu'au nouveau standard européen CEN TS 15480 (European Citizen Card).
Sur évaluation par un laboratoire sécuritaire indépendant, elle sera certifiée CC EAL4 + selon le profil de protection PP SSCD, comme requis par l'administration française, ainsi que par la directive européenne de signature digitale.
Son support des fonctions nécessaires à la gestion sécurisée des données et des services d'infrastructure à clés publiques en fait l'outil idéal pour les services de signature électronique et d'authentification. Elle répond aux besoins des administrations soucieuses de dématérialiser leurs procédures tout en assurant la non répudiation.

Comme la carte IAS TPC est multi-applicative, elle permet d'optimiser les investissements. La carte est en effet basée sur la technologie Java Card de Gemalto. Cette technologie a été adoptée internationalement par les autorités gouvernementales les plus exigeantes pour sécuriser l'accès à leurs ressources informatiques. Elle combine la conformité aux standards, la performance, l'état de l'art de la sécurité et le support de multiples applications sur une même carte.
Gemalto a déjà déployé sa technologie Java Card sur des infrastructures à clé publique (fonctionnellement équivalente au standard IAS) certifiée CC EAL4+ selon le profil de protection PP SSCD avec des partenaires aussi exigeants que CertEurope, la Poste en Lettonie ainsi que les universités de Pologne. Par ailleurs, les programmes nationaux de carte d'identité aux Emirats Arabes Unis, à Oman, au Portugal sont également basés sur la technologie Java Card de Gemalto.
La carte IAS TPC peut être déclinée sous plusieurs formes: clé USB pour une utilisation sur PC ou badge d'employé pour le contrôle d'acces physique et logique et l'identification visuelle du porteur.
Les options de corps de carte, incluant les dernières techniques de sécurité dans ce domaine (encres à effet optique variable, micro-impressions, guilloches, encres ultraviolet, etc.), lui permettent de fournir une excellente protection contre la contrefaçon ainsi qu'une durée de vie optimale.

## Principaux avantages

**Carte à microprocesseur référencée IAS ECC**
IAS ECC est un standard interopérable édité par le GIXEL (Groupement des industries de l'interconnexion des composants et des sous-ensembles électroniques), initialement pour l'administration française, mais aussi pour toutes les administrations publiques européennes, puisque IAS ECC est également conforme au standard CEN 15480 (European Citizen Card).
Gemalto étant un acteur très actif du groupement GIXEL depuis sa création, la carte à microprocesseur IAS TPC est entièrement compatible avec les spécifications IAS ECC.

**Intégrée dans une solution complète**
Gemalto est également le fournisseur de l'administration française pour le middleware IAS. De ce fait la carte IAS TPC est naturellement supportée, non seulement par le middleware IAS destiné à toutes les applications déployées par les autorités administratives françaises, mais aussi par le middleware générique proposé par Gemalto.

**Conforme à la directive européenne de signature électronique.**
La carte à microprocesseur IAS TPC est également 100 % conforme à la loi européenne de signature électronique, exigeant une certification Critères Communs EAL4+ selon le profil de protection PP SSCD (CWA-14169).
De plus elle suit la spécification CEN 15480 (European Citizen Card), qui est le nouveau standard pour les applications d'identité, d'authentification et de signature électronique en Europe.
Pour la France, elle adhère aux Référentiel Général d'Interopérabilité et Référentiel Général de Sécurité (qui inclus la PRIS v2 - politique de référencement intersectorielle de sécurité).

**L'état de l'art de la sécurité**
La carte IAS TPC bénéficie de l'ensemble du savoir-faire de Gemalto pour le développement de carte à microprocesseur offrant un haut niveau de sécurité, savoir-faire sanctionné par la prestigieuse certification CC EAL 4+. Ainsi, du design de son architecture à l'implémentation des contre-mesures de sécurité, la carte est revue et analysée dans ses moindres détails par un laboratoire indépendant.
Elle bénéficie d'autre part de l'expérience de Gemalto pour la certification sécuritaire de cartes multi-application basées sur une technologie Java Card. En effet Gemalto est de loin le leader de l'industrie en matière d'évaluation CC EAL4+ et FIPS de cartes Java Card, avec plus de 20 certifications.

**Support complet des mécanismes à clé publique**
Le jeu de fonctionnalités de la carte IAS TPC permet de mettre en œuvre tous les mécanismes à clé publique, potentiellement requis pour les applications basées sur cette technologie :
• Signature électronique
• Déchiffrement de clé de session
• Génération dans la carte de clés RSA
• Authentification mutuelle carte-terminal
• Authentification par rôle
• Support de clés RSA jusqu'à 2048 bits
• Gestion de certificats (jusqu'à 12 certificats et plus, selon le type de certificats et l'organisation de la zone EEPROM)

**Gestion dynamique de fichiers et de données**
Le jeu de fonctionnalités de la carte IAS TPC permet de gérer dynamiquement n'importe quel type de donnée et de fichier dans la carte, et d'y associer les conditions de sécurité appropriées (protection par PIN, par rôle, par authentification mutuelle, par canal sécurisé …). Elle apporte ainsi un maximum de flexibilité dans le développement d'application à base de carte à microprocesseur.

**Support d'applications indépendantes sur une même carte**
La technologie Java Card de la IAS TPC, associée au jeu d'applets Gemalto présents dans la zone ROM du composant, permet de créer très facilement dans cette carte plusieurs applications, complètement indépendantes les unes des autres tant pour les données que pour leur sécurité :
• PKI (une ou plusieurs applications IAS)
• OTP
• Gestion sécurisée de données

**Option d'interface combinée contact et sans contact**
La carte IAS TPC peut également être proposée avec en option une interface sans contact combinée à l'interface à contact.

**Bénéficie des autres avantages de la gamme Gemalto**
De même que toutes les cartes Gemalto, la carte IAS TPC intègre Java Card et une sélection d'applets Gemalto dans la zone ROM du composant, ce qui permet de réserver l'ensemble de la zone EEPROM aux données de la ou des applications. Par ailleurs, comme pour les autres cartes, la qualité de la technologie Java Card de Gemalto permet d'atteindre d'excellentes performances tant pour les opérations de gestion de données que pour les calculs cryptographiques, et ce tout en offrant les contre-mesures nécessaires à l'obtention d'un certificat CC EAL4+.

## Spécifications Techniques

### Spécifications de l'applet IAS ECC

- 100% conforme aux spécifications IAS ECC
- Conforme aux exigences de la PRIS v2 pour tout type de certificats *, ** ou ***.
- Support des services basés sur RSA (jusqu'à 2048 bits)
  - Signature digitale (SHA-1, SHA-2, PKCS#1)
  - Déchiffrement de clé de session
  - Génération à bord de bi-clés
  - Injection de bi-clés
  - Authentification par rôle (combinaison RSA et Diffie-Hellman)
  - Authentification mutuelle carte/terminal (combinaison RSA et Diffie-Hellman)
  - Capacité de stockage d'au moins 12 paires de clé et certificats, ou plus selon le type de certificat.
- Support des services basés sur 3-DES
  - Authentification par rôle
  - Authentification mutuelle carte/terminal
  - Secure messaging
- Support des services de gestion de données et fichiers
- Support des structures de données PKCS#15
- Immédiatement compatible avec la Middleware IAS de l'administration française
- Support de plusieurs applications IAS indépendantes
- PIN Global conforme à la fois aux spécifications IAS ECC et à GP2.1.1

### Spécifications générales de la plateforme JavaCard

- JavaCard Virtual Machine, RTE et API conformes à JC2.2.1
- Card Management & API conformes à GP2.1.1 (protocoles SCP01 and SCP02)
- 72 Ko d'EEPROM
- Algorithmes cryptographiques: 3DES (ECB, CBC), AES (128, 192, 256), RSA jusqu'à 2048bit, SHA-1, SHA-2, ELC P256
- Génération à bord de bi-clés RSA
- DAP à base de PK (pour un meilleur contrôle des applets qui pourraient être chargées en EEPROM)
- "Delegated Management"
- "Garbage Collection"
- Multiple canaux logiques
- Protocole contact: T=0, T=1, PPS (débit de communication jusqu'à 230 Kbps)
- Protocole sans contact (option): ISO14443, T=CL, émulation Mifare

### Autres applets présentes en ROM (activation optionnelle)

- Classic v2 applet
- OTP OATH applet

### Sécurité

La carte IAS TPC sera certifiée CC EAL4 + selon le profil de protection PP SSCD.
Elle embarque également à bord de nombreuses contre-mesures en protection aux attaques potentielles :

• Attaques "side channel"
• Attaques "invasive"
• Attaques "advanced fault"
• Et d'autres types d'attaques