



Spécialiste des Middleware PKI et eID pour Desktop, Smartphone et serveur

PRESENTATION GENERALE

UNE GAMME DE PRODUITS

Date : mercredi 7 juillet 2021
Référence : i-SCM – Presentation – FR – v1.doc

A PROPOS DE IDOYTE

Nom de l'entreprise	IDOYTE
Nationalité	Française
Adresse du siège	1 rue de Stockholm, 75 008 PARIS
Adresse du département technique	2 rue de l'Archevêché 38 200 VIENNE.
Numéro (SIREN)	490 032 091
Registre du commerce (RCS)	PARIS
Dirigeant	DRAY Philippe - philippe.dray@idoyte.com
Téléphone	+33(0)1 77 230 220
Domaine	MIDDLEWARE DESKTOP & MOBILE & SERVER

IDOYTE est un Editeur de logiciels spécialisé dans le domaine des Middleware PKI et eID pour PC, tablettes, smartphones et serveur.

Notre métier est de concevoir des middleware pour permettre à toutes les applications, sous n'importe quel environnement (Windows, Mac OS, Linux, iOS, Android),

- la lecture des documents d'identité (Passeport, Carte Nationale d'Identité électronique, ...)
- la faculté d'effectuer :
 - des signatures électroniques et/ou du chiffrement/déchiffrement de documents,
 - de mettre en œuvre l'authentification forte dans les navigateurs,
 - de sécuriser l'accès au PC via Windows Logon,
 - de sécuriser les réseaux via VPN,
 - de prendre le contrôle à distance en toute sécurité d'un PC via Remote Desktop Protocol (RDP), ...

Toutes ces fonctionnalités nécessitent de faire des opérations cryptographiques basées sur l'utilisation de certificats numériques et de leurs clés associées, stockées soit dans des passeports biométriques, des cartes à puce ou des Token ou encore via des cartes à puce virtuelles (VSC).

Nos logiciels répondent à des enjeux stratégiques, et sont utilisés dans des projets :

- d'ouverture sans risque des systèmes d'information aux Desktop, tablettes, smartphones,
- de signature électronique et/ou de chiffrement dans les projets de dématérialisation des échanges, ou de sécurisation des flux EDI ou transactionnels, ...
- de Card Management System (CMS) pour une administration sécurisée à distance du contenu des cartes à puce (Génération d'une paire de clé, Renouvellement d'un certificat,

Nos produits sont issus de plusieurs années de recherche et développement, et ont été déployés avec succès à grandes échelles dans le monde entier pour des applications sensibles.

Notre gamme de produits **i-SCM Desktop**, **i-SCM Mobile** et **i-SCM Server** forme une base technique innovante, homogène et présente de nombreux avantages sur le plan financier, technique et organisationnel.

Notamment, nos produits peuvent être utilisés, quel que soit le fournisseur de cartes.

UNE GAMME DE PRODUITS

Idopte dispose d'une gamme de produits logiciels « Middleware » disponibles sous Windows, Windows Server, Mac OS, Linux, iOS et Android.

I-SCM Desktop	I-SCM Mobile		SCWS Server
I-SCM Desktop Windows	I-SCM Mobile iOS	I-SCM Mobile Android	I-SCM Server Java
I-SCM Desktop MacOS	SDK Mobile iOS	SDK Mobile Android	I-SCM Server C#
I-SCM Desktop Linux			

Code source commun entre les différentes plateformes

Le code source est commun entre toutes les plateformes, quelle que soit l'OS et quelle que soit la déclinaison du logiciel: desktop/mobile/serveur. Seuls les appels à des éléments système (accès aux lecteurs, threading, ...) sont isolés dans des parties de source spécifiques.

Le cœur du middleware est développé en C++ et peut être compilé et réutilisé sur toutes les plateformes.

La maîtrise du source procure une liberté et une capacité d'agir sur le middleware pour répondre aux exigences particulières, améliorer sans cesse les performances, ou bien encore intégrer de nouvelles cartes ou de nouvelles fonctionnalités.

Langues supportées :

Français, Anglais, Espagnol, Polonais. D'autres langues peuvent être rajouter sur demande.

Lecteurs supportés

Lecteur PC/SC transparent à contact et sans contact.

Tous les PinPad compatibles PC/SC version 2.0 et supportant les commandes de Pin sécurisés : PinPad LEO Ingénico, GemPC PinPad, ...

Cartes supportées :

Nos middleware garantissent le fonctionnement avec l'ensemble des documents d'identité électronique :

- toutes les cartes conformes au standard IAS-ECC mais aussi les cartes propriétaires

IAS (Identification, Authentication and electronic Signature) ECC (European Citizen Card) est un ensemble de spécifications techniques de cartes à puces intégrant les fonctions requises afin de réaliser les opérations d'authentification, d'identification et de signature électronique sur une plateforme commune pour l'e-Administration.

IDEMIA	ID One Cosmo V7, Cosmo V8, Cosmo V10 Ideal Citiz
NXP	JCOP3 ChipDoc v2, JCOP4 ChipDoc v3

Thales	ID PRIME MD 830, 840, 930, 3930, 940, 3940 ID PRIME eToken 5110, 5300

*Authentification, signature, chiffrement, et échange de clé avec les algorithmes à clé publique RSA (jusqu'à 4096 bits) et Courbe Elliptiques (jusqu'à 521 bits), suivant les capacités de la carte et du profil. Les padding PKCS#1, PSS et OAEP sont supportés, ainsi que le hash partiel (signature qualifiée RGS***).*

- eMRTD conformes à la spécification [ICAO_9303] et eIDAS conformes à la spécification [TR-03110].

Sont supportées le Basic Access Control, l'authentification PACE (Integrated et Generic mapping), l'authentification passive, l'authentification active, ainsi que la Chip Authentication et la Terminal Authentication pour EACv1 et EACv2. Pour ces usages, sont supportés les algorithmes 3DES et AES jusqu'à 256 bits, DH, ECDH, RSA et ECDSA.

Biométrie

Le middleware supporte l'authentification biométrique par empreinte digitale ou par reconnaissance faciale avec vérification par la carte (match-on-card). Les format de données biométriques définis dans les standards ISO19794-2, ISO19794-4 et ISO7816-11 sont supportés.

I-SCM DESKTOP

Le i-SCM Desktop est un logiciel intégré aux OS (Windows, Mac OS, Linux), permettant à des applications sur Desktop, l'utilisation sécurisés des certificats numériques et de leurs clés associées, stockés dans une carte eID ou PKI lors de la mise en œuvre de fonctions cryptographiques au moment de l'authentification forte par certificat dans les navigateurs, ou de la signature électronique, ou du cryptage dans tous les logiciels respectant les différentes normes.

Interfaces disponibles

Toutes les interfaces de haut-niveau CPS, Smart Card MiniDriver, PKCS#11, CryptoTokenKit, ..., ainsi que le "Smart Card Web Service" s'appuient sur le module "Card Specific Module" approprié pour dialoguer avec la carte considérée.

	Windows	Mac OS	Linux
	Windows 10 - 11 Windows Server	Catalina 10.15 Big Sur 11.0 Monterey 12.0	RedHat CentOS Ubuntu
SCWS JS	Smart Card Web Services Interface Javascript	Smart Card Web Services Interface Javascript	Smart Card Web Services Interface Javascript
Interface Standard	Interface Standard PKCS#11	Interface Standard PKCS#11	Interface Standard PKCS#11
Interfaces spécifiques	CSP : Cryptographic Services Provider Smart Card Mini Driver KSP : Key Services Provider Credential Provider (pour la saisie des empreintes biométriques)	CryptoTokenKit	

Interface SCWS JS	Face à l'obsolescence des applets Java et des technologies ActiveX, le module Smart Card Web Service (SCWS) fournit des moyens, à partir d'une application Web, de manipuler et d'utiliser des clés, des certificats et d'autres objets cryptographiques stockés dans des cartes à puce (ou d'autres périphériques cryptographiques). L'API SCWS JS utilisable dans les applications web (à partir du code JavaScript) qui fournit un accès sécurisé aux ressources qu'offrent une carte à puce, un Token, un Passeport biométrique, une Carte Nationale d'identité électronique. Les fonctions de l'interface SCWS JS sont de bas niveau et comparables aux fonctions offertes par l'interface standard PKCS#11.
Interface PKCS#11	PKCS Public Key Cryptographic Standards / standards de cryptographie à clé publique : ensemble de spécifications conçues par les laboratoires RSA et considérée comme un standard industriel L'interface PKCS # 11 est conforme à la spécification OASIS: "PKCS # 11 v2.40 Cryptographic Token Interface Base Spécifications", 13 mai 2016.
Interface CSP	L'interface CSP est conforme aux spécifications Microsoft fournies dans le MSDN , et avec le document annexe "Smart Card Cryptographic Server Provider Notes" version 1.4.2.
Interface MiniDriver	L'interface Minidriver est présente sur les versions récentes de Windows. Elle permet une meilleure intégration de la carte à puce par le système, et l'utilisation

d'algorithmes avancés (SHA-256, Courbes Elliptiques, ...) notamment dans le cadre d'une utilisation des applications avec l'interface Modern UI.

Interface Credential Provider	L'interface Credential Provider permet la saisie des empreintes biométriques afin de mettre en œuvre le match-on-card (MoC) en lieu et place d'une saisie de PIN classique, dans le cadre de l'utilisation de l'interface MiniDriver. et pour l'utilisation du Windows Logon.
Interface CryptoTokenKit	L'interface CryptoTokenKit respecte les spécifications définies par Apple.

Module Global Cache

Le middleware dispose d'un service "Global Cache" qui est utilisé pour optimiser les performances. Les données de la carte, une fois lues, sont mémorisées dans cet espace de cache partagé entre les processus. Ceci permet également de garantir la cohérence des données manipulées par les processus dans le cas d'une modification de la carte.

Module Sign & Crypt

Disponible à travers le clic droit de la souris, ce module permet de signer, crypter, signer et crypter, n'importe quel document à partir d'un certificat électronique stocké dans une carte à puce ou dans les Store System.

Formats supportés : PKCS#7, PAdES, XAdES, CAdES..

Smart Card Manager (Gestionnaire de cartes à puce)

Synchronisation des certificats

Le Smart Card Manager a également la responsabilité, en arrière-plan, de synchroniser les certificats présents dans les magasins Windows avec le contenu de la carte. A chaque fois qu'une carte est insérée dans un lecteur, les certificats contenus dans la carte sont chargés dans les magasins appropriés.

Icône dans la barre des tâches et les fenêtre de notifications

Sous Windows, Mac OS et Linux, l'utilisabilité des certificats est immédiatement et facilement visible par l'utilisateur dans un icône situé dans la barre de tâche. Une coche verte indique que l'utilisateur peut utiliser son (ses) certificat(s). Une croix rouge informe que le(s)certificats ne peuvent pas être utilisés. Pour connaître la raison, l'utilisateur pourra ouvrir le Smart Card Manager pour diagnostiquer le problème.

Outil de gestion du contenu des cartes

L'interface utilisateur est de type web et identique sous Windows, Mac OS, Linux, iOS et Android. Cet outil, configurable en Mode Support ou en Mode Utilisateur, permet de gérer le contenu des cartes et de réaliser les opérations de maintenance du PIN.

Dans le Mode Support, l'utilisateur a accès à des toutes les fonctionnalités : Consultation des certificats et des clés privées, chargement d'un bi-clé et d'un certificat, génération d'un bi-clé, suppression d'un certificat, changement du code PIN, déblocage du code PIN, import d'un certificat d'autorité intermédiaire, d'un certificat d'autorité racine ...

Dans le Mode Utilisateur, l'utilisateur a accès à des fonctionnalités bridées. Les fonctions d' « Importation » de « suppression », de « génération d'une paire de clé » et de « déblocage » ne sont pas disponibles.

Outil de Diagnostic

Pour faciliter le diagnostic d'erreurs, le middleware permet de générer un rapport et de fournir le résultat de l'analyse de la configuration système, ainsi que la réalisation d'une série d'autotests afin de vérifier le bon fonctionnement du middleware.

L'outil permet de tester la signature selon l'interface préalablement choisie : PKCS#11, CSP, MiniDriver.

Gestion des logs

Pour faciliter le diagnostic d'erreurs, le middleware permet l'activation, la désactivation, l'extraction, la visualisation, la suppression des logs générés lorsqu'une application utilise l'une des interfaces du middleware.

Outil d'installation des mises à jour

Sous Windows et Mac OS, le middleware est en mesure de proposer sous forme d'option une mise à jour pour bénéficier des dernières améliorations à travers l'apparition d'une fenêtre indiquant la publication d'une nouvelle version.

MIDDLEWARE OU SDK SUR MOBILE COMPATIBLE AVEC LES CARTES/TOKENS PKI ET DOCUMENTS EID (PASSEPORT ET CNIE)

A travers le middleware (i-SCM Mobile) disponible sur iOS et Android, les applications sur Mobile peuvent utiliser de façon sécurisée les certificats numériques et de leurs clés associées stockés sur carte à puce ou Token pour mettre en œuvre :

- L'authentification client SSL dans les navigateurs : Chrome, Edge, Safari, ...
- La signature, chiffrement dans les logiciels de messagerie : Mail, Message, ...
- La lecture des données contenues dans un passeport biométrique ou une carte d'identité électronique ainsi que la lecture optique MRZ

Mobile		
OS	Middleware	SDK
iOS 8+ (support de NFC à partir de iOS 13)	SCM Mobile iOS	SDK Mobile iOS
Android JellyBean 4.3+	SCM Mobile Android	SDK Mobile Android

Communication supportée :

Les mobiles sont désormais dotés de capteurs de communication (NFC) qui facilitent l'utilisation des cartes à puce sur smartphone.

Cependant, Idopte propose plusieurs modes de communication afin d'offrir un maximum de souplesse, :

- Communication USB : Token, lecteur PC/SC transparent à contact ou sans contact.
- Communication NFC : Carte sans contact
- Communication Bluetooth : Lecteur Bluetooth

Installation et mise à jour :

Le i-SCM Mobile se présente sous la forme d'une application . L'installation ou les mises à jour s'effectuent à travers les store system : App store, Play Store, ...

Intégration dans les OS :

Sous iOS, l'intégration du middleware s'effectue à travers l'interface CryptoTokenKit (pour une compatibilité avec les applications natives Safari, Mail).

Sous Android, l'intégration du middleware s'effectue à travers un plugin UCM (pour une compatibilité avec toutes les applications natives Samsung Browser, Samsung Email,... conforme à KNOX).

Les applications web existantes développées sur Desktop deviennent accessibles de la même manière sur mobile à travers un canal https.

Librairie Smart Card Web Service (SCWS).

L'application i-SCM Mobile est constituée aussi de son propre browser (webview) auquel a été intégré l'interface Smart Card Web Service (SCWS). Ainsi, il est également possible d'exécuter une application web

directement au sein du i-SCM Mobile de façon autonome, autosuffisante et indépendante d'une autre application.

Smart Card Manager (Gestionnaire de cartes à puce)

Icône et notifications

Sous iOS et Android, l'utilisabilité des certificats est immédiatement et facilement visible par l'utilisateur dans un icône situé en haut à droite dans la barre de titre de l'application. Une coche verte indique que l'utilisateur peut utiliser son (ses) certificat(s). Une croix rouge informe que le(s)certificats ne peuvent pas être utilisés. Pour connaître la raison, l'utilisateur pourra ouvrir le Smart Card Manager pour diagnostiquer le problème.

Outil de gestion du contenu des cartes

L'interface utilisateur est de type web et identique sous Windows, Mac OS, Linux, iOS et Android. Cet outil, configurable en Mode Support ou en Mode Utilisateur, permet de gérer le contenu des cartes et de réaliser les opérations de maintenance du PIN.

Dans le Mode Support, l'utilisateur a accès à des toutes les fonctionnalités : Consultation des certificats et des clés privées, chargement d'un bi-clé et d'un certificat, génération d'un bi-clé, suppression d'un certificat, changement du code PIN, déblocage du code PIN, import d'un certificat d'autorité intermédiaire, d'un certificat d'autorité racine ...

Dans le Mode Utilisateur, l'utilisateur a accès à des fonctionnalités bridées. Les fonctions d' « Importation » de « suppression », de « génération d'une paire de clé » et de « déblocage » ne sont pas disponibles.

Outil de Diagnostic

Pour faciliter le diagnostic d'erreurs, le middleware permet de générer un rapport et de fournir le résultat de l'analyse de la configuration système, ainsi que la réalisation d'une série d'autotests afin de vérifier le bon fonctionnement du middleware.

Gestion des logs

Pour faciliter le diagnostic d'erreurs, le middleware permet l'activation, la désactivation, l'extraction, la visualisation, la suppression des logs générés lorsqu'une application utilise l'une des interfaces du middleware.

FIN DU DOCUMENT