

PractiSIGN®

Middleware multifonctions pour carte et token de sécurité

La solution idéale de mise en œuvre des certificats et des crédits

PractiSIGN est le logiciel client associé aux authentifieurs SCRYPTO. Il permet l'exploitation des certificats numériques et des crédits personnels abrités sur carte à puce ou token USB par les applications d'authentification, de protection des données et de signature électronique les plus répandues.

Simplifier la sécurité

PractiSIGN est un logiciel « client » installé sur le poste utilisateur qui permet d'assurer de manière transparente l'interface entre son authentifieur et les applications exploitant les informations contenues et protégées par cet authentifieur : certificats et clés privées associées, déployés dans le cadre d'une PKI, et / ou mots de passe d'accès aux applications.

Tous ces crédits sont ainsi regroupés sur un support unique protégé par code PIN. Les cartes à puce et token USB permettent le transport sécurisé des crédits, facilitant ainsi leur déploiement : ils ne sont plus attribués à un poste de travail mais à une personne.

Facilite le déploiement et la gestion des certificats

PractiSIGN inclut tous les outils et fonctions permettant de faciliter le déploiement et la gestion des authentifieurs et de leurs certificats :

- Package .MSI d'installation, compatible avec l'outil de déploiement administré Microsoft SMS.
- Fonction de gestion des certificats : visualisation, importation, exportation, suppression.
- Fonction de changement de code PIN et de déblocage à distance des cartes ou token bloqués par la présentation successive de 3 codes faux.

La solution complémentaire SCRYPTO Card Manager de personnalisation et mise à jour centralisées ou réparties des cartes et token offre en outre une interface directe avec de nombreuses Autorités de Certification. Elle permet ainsi la personnalisation en une seule passe des authentifieurs, y compris l'impression du logo ou photo d'identité éventuelle, et fournit tous les outils de gestion du cycle de vie des authentifieurs (analyse des cartes, recyclage, cartes temporaires, reporting).



Interopérabilité étendue

PractiSIGN est conforme aux standards CryptoAPI (Microsoft) et PKCS#11 (RSA). Il est de ce fait directement opérationnel avec tous les logiciels compatibles avec ces standards, qui exploitent des certificats numériques et des clés privées pour assurer différentes fonctions de sécurité : chiffrement de fichiers, emails chiffrés/signés, sécurisation de connexions distantes ou WIFI, signature de formulaires WEB etc...

C'est le cas en particulier des applications les plus répandues telles que :

- Windows Smart Card Logon,
- Signature de documents Microsoft Office,
- Emails chiffrés et/ou signés avec Outlook ou Lotus Notes,
- Sécurisation des accès VPN SSL (Juniper, F5...) ou IPSEC (Microsoft, Cisco...),
- Authentification WEB SSL (Internet Explorer, Firefox),
- Chiffrement de fichiers personnels ou partagés avec Prim'x Zone Central.
- Authentification des clients de réseau Wifi 802.1X.

PractiSIGN est opérationnel aussi bien sur client lourd Windows que sur les clients légers.

Caractéristiques générales

Services cryptographiques

- Algorithme symétrique : DES, 3DES, AES, RC4
- Algorithme asymétrique : RSA signature, RSA Key Exchange 1024 et 2048 bits, certificats X509
- Algorithme de hachage : MD5, SHA-1, SSL3, SHAMD5

Authentificateurs

- Cartes Gemalto Cyberflex, Gemsafe,
- Java Card Oberthur,
- Clé USB Cyberflex Gemalto,
- Token USB mémoire à « puce virtuelle ».

La puce virtuelle est une technologie développée par SCRYPTO. Elle permet de réserver une partition mémoire d'une clé USB mémoire standard afin qu'elle soit vue par PractiSIGN comme une carte à puce.

Conformité aux standards

- Microsoft CAPI, RSA PKCS#11, S/MIME, Java Card, TLS/SSL, certificats X509

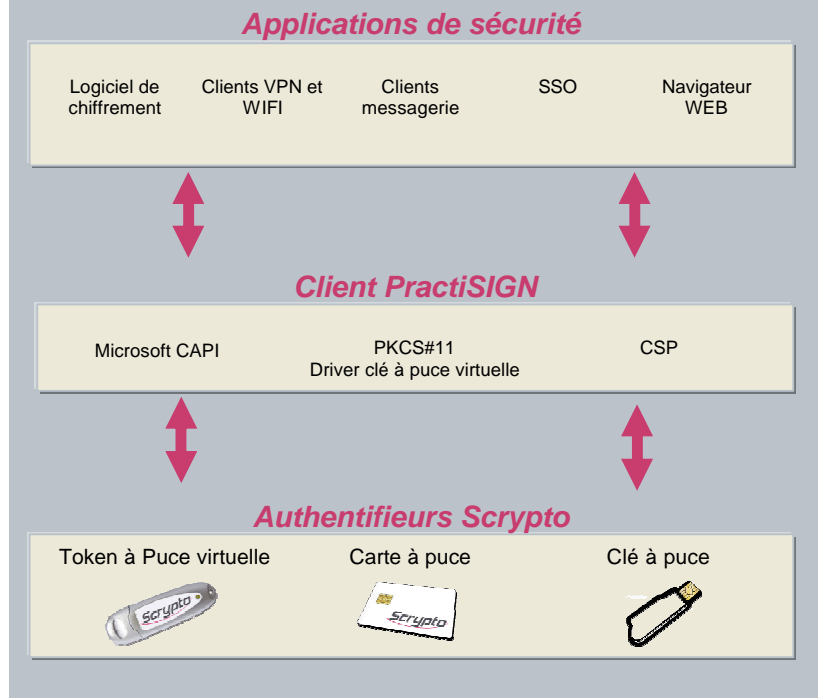
Environnement

- Windows 2000, Windows XP, Windows Server 2003
- supporte l'environnement Citrix® Présentation Server
- supporte l'environnement Microsoft Terminal Server

Fonctions de gestion

- Changement de code PIN par l'utilisateur
- Déblocage local ou à distance des tokens
- Affichage du nombre d'essais restants après saisie d'un code PIN faux
- Fonctions de gestion des certificats : visualisation, importation, exportation
- Outil de personnalisation centralisée et à distance des tokens
- Compatible avec MS Certificate Services, OPENTRUST PKI et autres autorités de certification

Intégration de PractiSIGN dans une architecture sécurisée



Principaux bénéfices

Sécurité renforcée :

Renforce la sécurité des applications des PKI en conditionnant l'accès à une authentification forte à deux facteurs.

Portabilité :

Permet le stockage et le transport des certificats et des clés privées sur un support de sécurité amovible, facilitant ainsi leur déploiement et leur utilisation par les applications.

Compatibilité SSO :

Fonctionne également avec la solution de Single Sign On SSOX, qui permet de remplacer tous les logon aux applications protégées par mot de passe, par une authentification unique par code PIN.

Évolutivité et pérennité des investissements :

Permet le déploiement progressif des applications de sécurité sans remise en cause de l'existant.