Cryptolog Universal Token Environment

Universign

Sommaire

Présentation de la solution

Intégrez la signature électronique au sein de vos applications

Cryptolog Universal Token Environment (CUTE) est une bibliothèque de composants logiciels permettant une intégration simple des fonctionnalités de signature électronique au sein d'une application métier.

Compatible avec la plupart des certificats et dispositifs de création de signature du marché, CUTE permet de générer tous les formats de signature électronique, des plus génériques — CMS, XMLDSig et PDF — aux plus avancés que sont CAdES, PAdES, XAdES.

Disponible en Java, ce kit a particulièrement vocation à être déployé en environnement Web au sein d'applets. Il s'adresse avant tout aux éditeurs logiciels, aux opérateurs de services Saas, aux intégrateurs de solutions IT, mais aussi aux entreprises disposant d'une DSI.

Un puissant outil de signature électronique

Le module central de CUTE constitue le socle de la solution. Il apporte les fonctionnalités suivantes :

- l'accès aux dispositifs sécurisés de création de signature SSCD (Secure Signature Creation Device) ;
- un filtrage puissant sur les certificats permettant une sélection fine suivant différents attributs comme l'autorité de certification, la politique de certification ou encore les contraintes d'utilisation de la clé ;
- la création des signatures cryptographiques avec l'ajout d'un jeton d'horodatage

Les fonctionnalités

Accès transparent à la plupart des certificats du marché

Grâce à son module central, CUTE permet d'accéder de manière transparente à l'ensemble des clés et des certificats stockés sur tout support cryptographique, logiciel ou matériel.

Grâce à l'implémentation des interfaces standards, CUTE permet l'utilisation de certificats stockés sur les principaux supports cryptographiques disponibles à ce jour :

- les cartes à puce, les clés USB et les boîtiers matériels de sécurité (SSCD) via l'interface PKCS#11 ;
- les magasins de certificats de Microsoft Windows via notamment l'interface MS-CAPI ;
- les magasins de certificats du navigateur Firefox de Mozilla via l'interface NSS ;
- les magasins de certificats Keychain de Mac OS
- les fichiers PKCS#12 ;

Génération de certificats temporaires à la volée

Le module CUTE PKI offre la possibilité de générer à la volée des paires de clés publiques/privés à usage unique.

Lors de cette génération, il sera notamment possible de demander la génération d'un certificat auprès d'une autorité de certification via l'interface PKCS#10. Ce module sera particulièrement apprécié dans tous les scénarios d'intégration où les signataires ne sont pas équipés de certificats.

Intégration simplifiée en java ou JavaScript

À l'aide des exemples de code et du Guide d'installation de CUTE, il n'a jamais été aussi facile d'ajouter la signature électronique aux applications !

En Java

CUTE embarque l'ensemble des composants nécessaires à son fonctionnement au sein d'une bibliothèque Java autonome, simplifiant son intégration. Quelques lignes de code suffisent pour faire appel à CUTE et intégrer des fonctionnalités puissantes de signature électronique au sein de vos applications métier existantes.

En Javascript

CUTE est livré avec une applet Java – CUTE Applet – qui permet d'ajouter à une application web les fonctionnalités de signature électronique. Techniquement, CUTE Applet sert de passerelle entre CUTE et des applications tournant dans un navigateur Web compatible HTML/Javascript. À partir d'un document initial et de paramètres de signature, cette applet retourne le document signé à l'application web. Elle a été conçue pour pouvoir être facilement enrichie d'une interface graphique spécifique correspondant à chaque besoin.

Formats avancés de signature

CUTE permet de mettre en œuvre très simplement tous les principaux formats de signature utilisés à ce jour, dans le plus strict respect des dernières versions des standards internationaux : CMS et CAdES, XMLDsig et XAdES, PDF et PAdES.

CUTE CAdES

Au-delà de la simple signature électronique au format CMS, le module CUTE CAdES permet de formater des signatures au format avancé CAdES – CMS Advanced Electronic Signatures – dans ses différentes variantes : CAdES, CAdES-BES, CAdES-EPES et CAdES-T. CUTE CAdES apporte les fonctionnalités de signature avancées suivantes :

- les signatures de documents bruts ;
- les co-signatures de documents bruts : plusieurs signatures pour le même document ;
- les contre-signatures : signatures de signature.

CUTE XAdES

Au-delà de la simple signature électronique au format XMLDsig, le module CUTE XAdES permet de formater des signatures au format avancé XAdES – XML Advanced Electronic Signatures – dans ses différentes variantes : XAdES, XAdES-BES, XAdES-EPES et XAdES-T.

CUTE XAdES apporte les fonctionnalités de signature avancées suivantes :

- les signatures de documents bruts et XML ;
- les co-signatures de documents bruts et XML : plusieurs signatures pour le même document ;
- les contre-signatures : signatures de signature ;
- les multiples signatures de documents : signatures pour plusieurs documents.

CUTE PAdES

Au-delà de la simple signature électronique de documents PDF ISO 32000-1, le module CUTE PAdES permet de formater des signatures au format avancé PAdES – PDF Advanced Electronic Signatures – dans ses différentes variantes : PAdES, PAdES-BES et PAdES-EPES.

CUTE PAdES apporte les fonctionnalités de signature avancées suivantes :

- les signatures de documents PDF, respectant le standard ISO 32000-1 ;
- les signatures de certification : author signature ;
- les signatures d'approbation : recipient signature.

Autres services

Matérialisation visuelle des PDF signés

Dans le cas du format PDF, chaque signature électronique peut être représentée sur le document par un champ de signature pouvant contenir une ou plusieurs images ainsi que du texte relatif à la signature (nom, prénom, date de la signature, etc.). Pour chaque signature électronique d'un document PDF, vous pourrez, grâce à CUTE, positionner un champ de signature entièrement personnalisé à n'importe quel endroit du document.

Connexion à un service d'horodatage

Le module d'horodatage CUTE TSA (TimeStamp Access) permet d'ajouter des jetons d'horodatage au sein des signatures électroniques produites par les modules de signature. L'accès au serveur d'horodatage se fait dans le plus strict respect de la norme de référence RFC 3161. CUTE TSP peut donc interagir avec tout service d'horodatage respectant cette norme, comme par exemple la plate-forme Universign de Cryptolog.

Importation de politiques de signature

Le module CUTE Signature Policies permet d'intégrer des politiques de signature et de prendre en compte les contraintes de ces politiques tout au long du processus de création d'une signature électronique. Il supporte les politiques de signature conformes aux standards ETSI 102 038 pour CAdES et ETSI 102 272 pour XAdES. Vous disposez déjà de vos propres politiques de signature ? CUTE vous permet de générer instantanément des signatures électroniques avancées les respectant !

Fiches techniques

Signature

Signature formats :

- CAdES (ETSI TS 101 733 v1.8.1)
  - CMS (RFC 3852 - Cryptographic Message Syntax)
  - BES (Basic Electronic Signature)
  - EPES (Explicit Policy Based Electronic Signature)
  - T (Signature Time-Stamp)

- XAdES (ETSI TS 101 903 v1.4.1)
  - XMLdSig (XML-Signature Syntax and Processing)
  - BES (Basic Electronic Signature)
  - EPES (Explicit Policy Based Electronic Signature)
  - T (Signature Time-Stamp)

- PAdES (ETSI TS 102 778 v1.1.1)
  - ISO 32000-1
  - BES (Basic Electronic Signature)
  - EPES (Explicit Policy Based Electronic Signature)
  - T (Signature Time-Stamp)

Signature tokens :

- PKCS#12 v1.0 (Personal Information Exchange Syntax Standard)
- PKCS#11 v2.20 (Cryptographic Token Interface)
- Microsoft CryptoAPI, CSP (Cryptographic Service Provider) & CNG (Cryptographic New Generation)
- Mozilla NSS (Network Security Services)
- Apple KeyChain

Signature validation policies (EPES signatures) :

- ASN.1 format for signature policies (ETSI TR 102 272 v1.1.1)
- XML format for signature policies (ETSI TR 102 038 v1.1.1)

Signature algorithms :

- RSA PKCS#1 (RSA Cryptography Standard)
  - "RSA/Sign, padding=1.5"
  - "RSA/Sign, padding=PSS"

- DSA (Digital Signature Algorithm or Digital Signature Standard)
  - "DSS, encoding=ASN.1"
  - "DSS, encoding=RAW"

- ECDSA (Elliptic Curve Digital Signature Algorithm)
  - "ECDSA, encoding=ASN.1"
  - "ECDSA, encoding=RAW"

Digest algorithms :

- "sha-1"
- "sha-256"
- "sha-384"
- "sha-512"

MD (Message Digest) :

- "md5"

RIPEMD (RACE Integrity Primitives Evaluation Message Digest) :

- "ripemd160"

Horodatage

- RFC 3161 (Time-Stamp Protocol)
- PAdES (ETSI 102 778 - Part 4)

PKI

Software key generation (Single usage certificate)

PKCS#10 v1.7 (Certification Request Standard)

PKCS#8 v1.2 (Private-Key Information Syntax Standard)

Key generation algorithms :

- "RSA/KeyGen"
- "DSS/KeyGen"
- "EC/KeyGen, curve=P-192"
- "EC/KeyGen, curve=P-384"
- "EC/KeyGen, curve=P-521"
- "EC/KeyGen, curve=K-163"
- "EC/KeyGen, curve=B-163"

Autres fonctionnalités

- Java 1.5 and further compatible
- Advanced logging
- Advanced template configuration from properties
- Advanced signature field configuration for PAdES signatures
- PDF pre-processing for PAdES signatures
- CUTE applet for direct usage from JavaScript

Architecture

- Kernel : Core functionalities, which are always present in CUTE.
- CAdES : Support for generation of CAdES signatures
- PAdES : Support for generation of PAdES signatures
- XAdES : Support for generation of XAdES signatures
- TSA : Support for retrieval of time stamps (from external time stamp authorities)
- Sigvp : Support for decoding and analysis of signature validation policies
- PKI : Support for keys and certificate generation
- Applet : Support for CUTE applet.

www.universign.com