EDELSAFE

Partie technique

Présentation du produit

EdelSafe

Issu du "

Dossier SCSSI"

Février 1999

Version 1.2

EdelWeb

33, Avenue du Maine

B.P. 137

75755 PARIS Cedex 15

Table des matières

1 PRÉAMBULE

Ce document est très directement issu du dossier de demande d'autorisation de fourniture générale soumis au SCSSI. En tant que tel, il n'a pas la prétention d'être un véritable document de présentation de EdelSafe.

Edelweb finalise le développement d'un produit ou plus exactement d'une famille de produit de sécurisation des documents électroniques et de leurs échanges.

Ces produits apportant des services de signature numérique et de confidentialité utilise la cryptographie.

Pour répondre aux attentes du marché, une cryptographie forte est nécessaire. Les produits EdelSafe contiennent un dispositif permettant à la puissance publique d'appliquer son ses droits de "perquisition" et d'interception" en application de la loi de 1997 et des décrets et arrêtés de 1998. La fourniture de ce produit sera soumise à l'obtention d'une autorisation de fourniture par le SCSSI.

2 RÉFÉRENCES COMERCIALE DU PRODUIT

Nom : EdelSafeDoc
Version : F-1.0

Nom : EdelSafeCenter
Version : F-1.0

Nom : EdelSafeKit
Version : F-1.0

3 DESCRIPTION GÉNÉRALE DU PRODUIT

3.1 POURQUOI UN PRODUIT EDELSAFE

Aucun des produits actuels ou annoncés pour la sécurisation des documents et de leurs échanges ne présente -loin s'en faut- les caractéristiques minimales indispensables pour répondre aux besoins des organismes (entreprises ou administration) ayant un besoin réel et conscient de solution dans le domaine.

Fort de son expérience dans le domaine (passé des fondateurs EdelWeb avec le projet PassWord, projet EuroTrust, prestations diverses pour nos clients), EdelWeb a commencé par spécifier une architecture répondant aux besoins réels identifiés. Comme le marché ne donnait aucun signe de l'arrivée de solutions au moins acceptables et capitalisant sur notre savoir faire combinant ingénièrie des protocoles et sécurité, EdelWeb a finalement décidé de développer une souche de produit conforme aux spécifications ci-dessus.

Les lignes de force qui ont présidées à la conception de EdelSafe peuvent être résumées comme suit :

- Apporter une solution à la problématique de **sécurisation des documents**. *L'approche sécurisation des services d'échange (smtp, http, ftp) ne répond pas au véritable problème,* ce sont les documents -de type quelconque- qui contiennent les informations sensibles à protéger et qui doivent être authentifiables. EdelSafe repose sur le principe d'enveloppe de sécurité permettant la signature (une ou plusieurs) et la confidentialité de ces documents. EdelSafe n'est pas un complément ou un sous-produit de la messagerie du web mais est utilisable de façon simple dans tous ces environnements.
- Fourniture d'une **solution "corporate"** et *pas d'une solution pour des individus isolés*. Il est fondamental que le produit permette et **impose** la **politique de confiance et de sécurité de l'entreprise**, pas celle des choix individuels de chacun de ses personnels.
- **L'administrabilité** de la sécurité est une fonction indispensable qui requiert une "centralisation" de la gestion de la confiance. Ce la impose donc une architecture distribuée permettant d'offrir aux utilisateurs les fonctions de constitution et d'ouverture ou validation des enveloppes de sécurité et aux administrateurs les fonctions de gestion de la sécurité et de la confiance (utilisateurs habilités, interface avec les services de certification internes ou externes, interface avec les services externes de type annuaire, horodatage, CRL) reflétant la politique de l'entreprise en la matière.
- **Le respect des standards** est une obligation. Pour la sécurité, il faut un respect intelligent des standards : acceptation en entrée des standards (plus ou moins bons et finalisés) actuel, génération, conforme au standard, mais en respectant des profils rigoureux. Parmi ces standards citons, CMS, S/MIME, OCSP, DCS, X.509, etc…

- La prise en compte des **règles élémentaires d'une sécurité forte** est impérative**.** A la différence des produits actuels du marché, EdelSafe **distingue clé de chiffrement et clé de signature**, sépare les paramètres de la confiance du ressort de l'entreprise de ceux qui sont propre à chaque utilisateur, se garde de considérer un annuaire à la X.500 ou LDAP comme un composant acceptable pour la sécurité, offre l'option de service de recouvrement décidés au niveau de l'entreprise.

3.2 LA SOLUTION EDELSAFE

EdelWeb finalise le développement de la version 1.0 EdelSafe, un produit innovant de sécurisation des documents et de leurs échanges. EdelSafe regroupe une famille de produits autour d'une architecture cohérente et partageant la même base technologique.

La version 1.0 du produit comprend trois composants ; **EdelSafeDoc** basé sur **EdelSafeKit**, et **EdelSafeCenter**.

Les principes généraux de l'architecture EdelSafe sont les suivants :

La gestion de la sécurité ne doit pas se faire sur le poste client mais sur un serveur bien administré du domaine de sécurité auquel appartient le client. C'est le rôle du composant **EdelSafeCenter**

Le logiciel sur le poste client doit être générique et capable de traiter les documents aussi bien vis à vis de leur stockage sécurisé que de leurs échanges par disquette, e-mail, FTP, HTTP ou tout autre moyen. C'est le rôle de **EdelSafeDoc**.

Le logiciel sur le poste client doit, au niveau configuration locale, être réduit au strict minimum. De plus il doit être impossible pour l'utilisateur de faire fonctionner ce logiciel dans un environnement et contexte de sécurité autre que celui décidé par les administrateurs sécurité de son organisme.

Il est important qu'outre les utilisateurs humains, les applications d'un organisme puissent bénéficier des mêmes services et manipuler les mêmes documents sécurisés. Pour cela EdelSafe contient le composant **EdelSafeKit** qui est une bibliothèque permettant aux organismes d'apporter la composante EdelSafe à leurs application par utilisation de cette bibliothèque.

Le produit EdelSafe permet le recouvrement des documents chiffrés en confidentialité. Cette possibilité est incluse d'office pour les exigences de la puissance publique et disponible en option (avec des clés différentes) pour les organismes eux-mêmes s'ils en ont besoin.

Ultérieurement l'architecture EdelSafe recevra de nouveaux modules comme **EdelSafeMail** ou **EdelSafeWeb** destinés à faciliter encore plus l'utilisation de **EdelSafe** dans un contexte e-mail ou dans un contexte web. Ces modules ne font pas partie du produit à ce jour.

3.3 CARACTERISTIQUES PRINCIPALES D'EDELSAFE

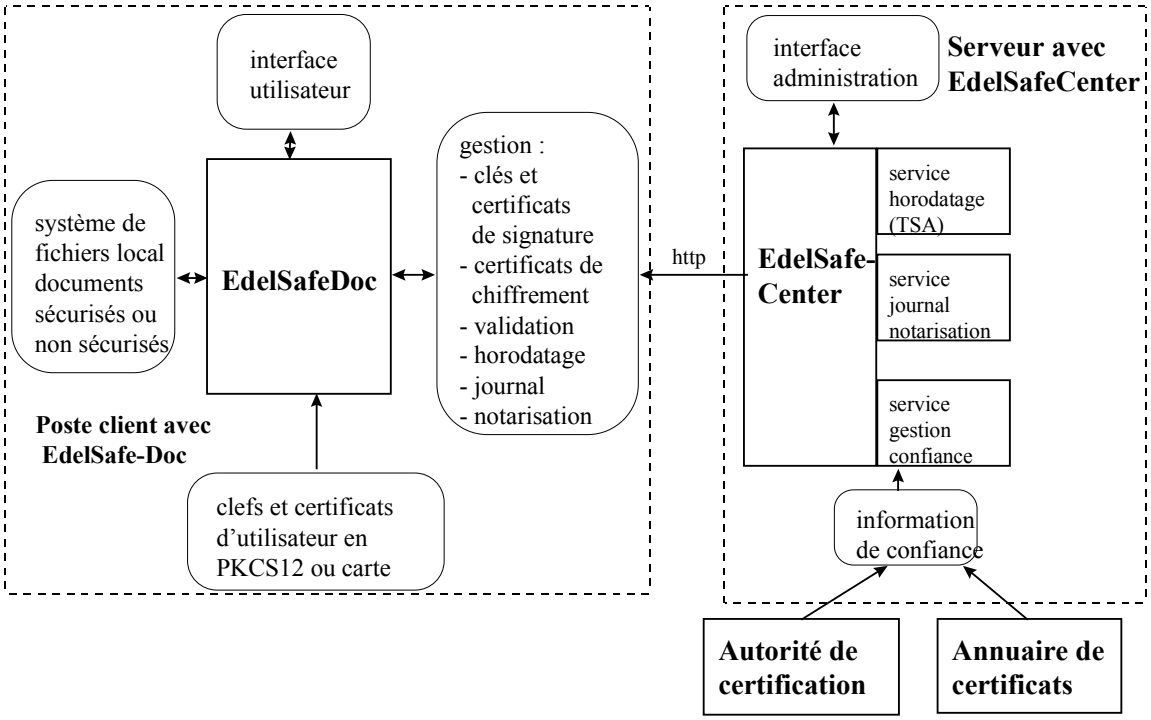
Les principales caractéristiques de la solution EdelSafe sont, en substance, les suivantes:

- ***Solution globale***: à la différence d'approches classiques, qui ne traitent que d'un aspect ou d'un service (sécurité locale, sécurité messagerie, sécurité Web, sécurité des canaux de communication), l'architecture EdelSafe permet de répondre à l'intégralité des besoins de sécurité concernant les documents. Elle est dite "*protocol-neutral*" en ce sens qu'elle permet le travail local et les échanges par tout moyen ou protocole.
- ***Architecture globale et administrabilité***: cette architecture prend en compte aussi bien les besoins et contraintes des utilisateurs (cœur du module **EdelSafeDoc** permettant de constituer, ouvrir et vérifier des enveloppes de sécurité), que celles des administrateurs grâce au module **EdelSafeCenter** qui concentre toute l'administration de la sécurité et de la confiance en un module facilement gérable par les responsables et administrateurs sécurité.
- ***Architecture modulaire, ouverte et évolutive*** : tous les modules sont bâtis à partir de la bibliothèque **EdelSafeKit** qui contient tous les standards de la cryptographie (symétrique et asymétrique) et la gestion des clés et des certificats grâce au protocole standard DCS. A partir de ce kit standard, le module **EdelSafeDoc** prend en charge la sécurisation des documents dans ce contexte de gestion "centralisée" de la sécurité. Ultérieurement, les modules additionnels **EdelSafeMail** et **Web** permettront, si cela apparaît souhaitable, une intégration plus forte dans un contexte de messagerie Internet ou de service Web. La prise en compte de la carte à puce est totalement intégrée dans l'architecture globale, en particulier au niveau de la gestion des secrets et des certificats. Enfin, la disponibilité **d'EdelSafeKit**, permet aux clients de développer par eux-mêmes d'autres produits sécurité qui seront compatibles dans leurs format et leur administration (au sens sécurité) avec ceux de la famille EdelSafe.
- ***Architecture et produits basés sur des standards***: aussi bien au niveau des algorithmes cryptographiques (RSA, D-H, DSA, DSS, DES, Triple, DES, RC4, MD5, SHA), des formats de message (CMS, PKCS#x), que des protocoles utilisés (HTTP, OCSP, LDAP, DCS), toute la famille des produits constitutifs de l'offre EdelSafe repose exclusivement sur des standards Internet reconnus et présentent dès lors toutes les garanties de pérennité.
- ***Cryptographie forte*** : la possibilité de respecter des contraintes réglementaires, comme celle de la France (SCSSI), par l'utilisation de "champs de recouvrement" (Key-Recovery Fields), permet de respecter de la confidentialité au plus haut niveau. Il faut noter que ces contraintes réglementaires ne sont pas traités de façon isolée et spécifique, mais prise en compte par la module de gestion du recouvrement.
- ***Portabilité et performance*** : du côté utilisateur, le langage Java autorise une portabilité qui permet de s'abstraire de tous les problèmes de plates-formes et de configurations. Du côté des serveurs, une implémentation en langage C apporte la performance voulue tout en préservant une excellente portabilité. Le cœur du serveur **EdelSafeCenter** est un serveur HTTP "*transactionnel*" permettant de répondre parfaitement aux exigences de trafic, de temps de réponse et de sécurité que lui confère son rôle de *service central de sécurité*.

- EdelSafe répond au besoin **d'uniformisation** et **d'indépendance** vis à vis des outils de messagerie ou de web intégré (au niveau utilisateur) ou des outils interne ou externe choisis par l'entreprise pour les fonctions CA, annuaire, etc.
- EdelSafe est une **solution ouverte** et aisément **intégrable** dans des applications (EdelSafeKit) permettant de mettre en place une politique entreprise pour l'ensemble des problèmes de sécurisation de document.

3.4 ARCHITECTURE ET COMPOSANTS

EdelSafe comprend deux éléments essentiel : un **service central de sécurité** et un **logiciel de sécurité multi-usage** sur chaque poste utilisateur. Ces éléments communiquent en utilisant le protocole http comme protcole fédérateur. Plusieurs service de sécurité sont accessibles au-dessus de http. le schéma suivant illustre l'architecture de ces deux composants et leur communication :



3.4.1 Un service central de sécurité

Un service central géré par les administrateurs sécurité de l'entreprise repose sur le composant **EdelSafeCenter**. Celui ci se présente techniquement comme un serveur HTTP jouant un rôle de frontal d'accès uniformisé à l'ensemble des services centraux de sécurités :

- Le serveur de vérification locale : il fournit en réponse le résultat d'une vérification d'une chaîne de certificats et une politique de certification. (protocole DCS), l'accès au état des certificats émis par l'entreprise est locale.
- Ce serveur utilise soit ses bases internes, soit les protocoles OCSP ou LDAP afin d'obtenir l'état de certificats émis par des autorités de certification externes reconnues dans la politique de sécurité.
- Le serveur d'horodatage de l'entreprise (sur CDS) éventuellement capable d'obtenir une heure de référence externe approuvée.
- (en option) : Le serveur de notarisation des "actions". Par action, on comprend la conservation de traces (journal) des opérations de chiffrement ou de signature d'un document, son expédition, etc. La nature des opérations mémorisée par ce "notaire électronique" sont paramétrables.
- le serveur de look-up des certificats de chiffrement des destinataires capable d'utiliser soit ses bases internes soit LDAP pour des recherhces sur des serveurs externes (pour la fonction de recherche simple des certificats des destinataires en vue de chiffrement).

3.4.2 Un logiciel de sécurité multi-usage sur chaque poste utilisateur

Sur chaque poste utilisateur concerné, un module EdelSafeDoc permet la manipulation (création, lecture) de documents sécurisés au format CMS. Chaque module est installé/fourni avec, de manière "câblée", le (seul) certificat du serveur EdelSafeCenter dont il dépend. Ce dispositif garantit la communication sécurisée avec le central de sécurité de l'entreprise, et avec lui seul. Il se compose de :

- un *moteur* comprenant tous les traitements cryptographiques de base (base EdelSafeKit). Ce moteur permet le traitement du format CMS et des *SignedData* et *EnveloppedData* pour signature et chiffrement. Il assure également la génération et le traitement des *Key Recovery Field*. Un paramétrage, non modifiable par l'utilisateur, permet de décider quels "recouvrements" sont nécessaires (0, 1 ou 2 pour les autorités légales ; 0, 1 ou 2 pour l'entreprise et les utilisateurs. La version française qui fait l'objet de cette demande contient toujours au moins un KRF pour la puissance publique française.

- un *module de gestion locale des clés* réduit, pour la sécurité et le passage simple à la carte à puce, à sa plus simple expression : gestion du certificat et du secret de signature de l'utilisateur, gestion du certificat et du secret de chiffrement de cet utilisateur, certificat du serveur central de sécurité. Les informations précédentes sont appelées le "**trousseau individuel de sécurité**"; il existe une version logicielle (le trousseau est dans un fichier sécurisé) et très bientôt l'utilisation de carte à microprocesseur. Ultérieurement, une extension permettra à un utilisateur jouant plusieurs rôles de disposer avec EdelSafeDoc et pour chaque rôle, de l'ensemble des éléments précédents (avec le passage "carte à puce" il y aura plusieurs cartes à puce, une par rôle).
- une *interface* conviviale et simple, mais parfaitement explicite quand à la sécurité. Chaque action de signature est un acte explicite et se rapporte à un document précis. Chaque vérification de signature propose explicitement un descriptif de l'ensemble de la chaîne de confiance ayant permis cette vérification (exemple: document signé par XXXX, certifié par l'autorité AAAA, elle même reconnue par le serveur central de sécurité l'entreprise).
- un *module de communication avec le serveur central de sécurité* (EdelSafeCenter) permettant, sous signature numérique, de vérifier l'authenticité et l'intégrité des informations reçues de ce serveur.

Il convient de noter que ce ensemble ne comprend pas de logiciel serveur d'annuaire LDAP, ni de logiciel de RA/CA (Autorité de Certification). Il est important de préserver la possibilité pour l'entreprise de choisir la solution de son choix (produit X ou Y exploité en interne, ou externalisé chez un opérateur de certification, ou utilisation pur et simples de certificats émis par une CA externe.

Un service basé sur EdelSafe comprend les logiciels:

- **EdelSafeDoc** sur des postes clients
- **EdelSafeCenter** sur un serveur central
- Un annuaire accessible par LDAP (*ne fait pas partie de EdelSafe*)
- Une autorité de certification avec publication par LDAP et/ou OCSP (*ne fait pas partie de EdelSafe*).

3.5 ASPECTS TECHNIQUE DU STANDARD S/MIME

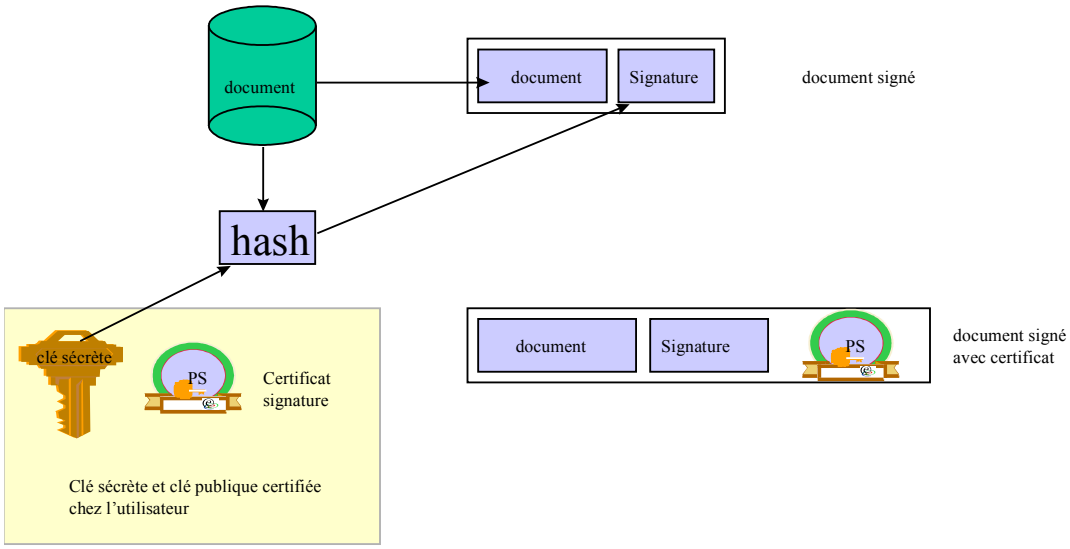
Le traitement de documents par **EdelSafeKit** est compatible avec le standard S/MIME de l'Internet. L'objectif du standard S/MIME n'est pas seulement de sécuriser la messagerie de l'Internet, mais de définir un format de véhiculer des documents sécurisés.

Le format de messages est basé l'adaptation Internet **Cryptographic Message Syntax (CMS)** de la spécification **PKCS#7** de RSA. Cela spécifie plusieurs types d'objets sécurisés. Suivant le contexte de S/MIME, dans EdelSafeKit seuls les types SignedData et EnvelopedData de CMS sont utilisés pour véhiculer des données signées et chiffrées.

SignedData permet de créer un document structuré qui contient essentiellement :

- des données en clair,
- pour un ou éventuellement plusieurs signataires une signature numérique,
- des certificats utilisés par les signataires ou d'autres certificats par exemple ceux correspondant à une ou plusieurs autorités de certification.

SignedData



EnvelopedData permet de créer un document structuré qui contient

- des données chiffrées en confidentialité avec un algorithme de chiffrement symétrique,
- pour chaque destinataire la clé de chiffrement chiffrée par un algorithme asymétrique en utilisant une clé publique (de chiffrement) de ce destinataire.
- La prise en compte des besoins de recouvrement est faite en considérant la ou les autorités habilités à intercepter ou recouvrer un document comme des destinataires potentiels et donc en incluant pour chacun d'eux un champs contenant la clé de chiffrement sous chiffrement par la clé publique choisie par cette autorité à cette fin. La version française qui fait l'objet de ce dossier contient obligatoirement un champs de cette nature et la clé publique utilisée sera celle convenue avec le SCSSI pour respecter la législation française.

- L’émetteur du message est considéré comme un destinataire ayant le doit de déchiffrer ses propres documents. En outre, il est possible d’ajouter d’autres entités ayant le droit d’accès au document, exemple dans le contexte de recouvrement de clé, une entité de sauvegarde de l’entreprise d’émetteur ou des destinataires ou des autorités.

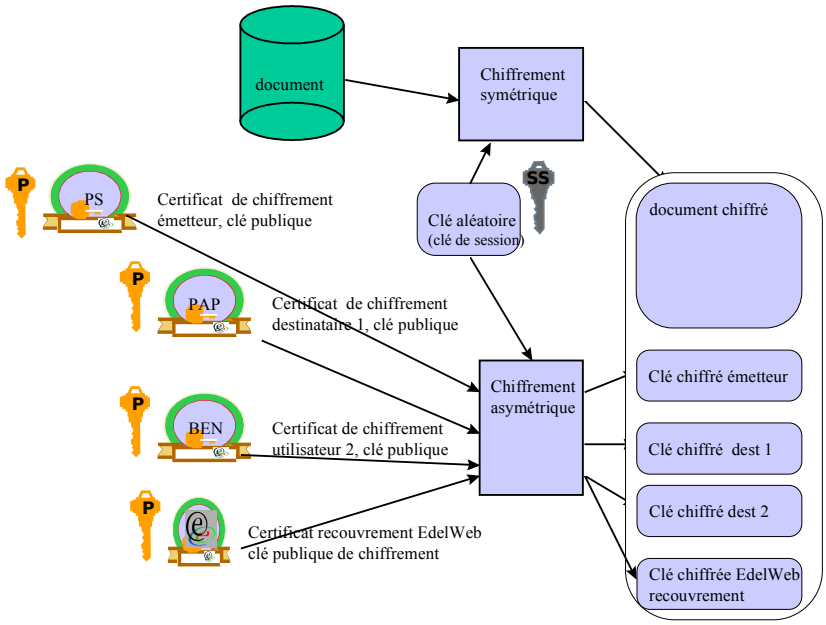
Une enveloppe de sécurité de document au sens EdelSafe, par combinaison des précédents -format CMS- permet d'apposer une ou plusieurs signatures et de chiffrer en confidentialité pour un ou plusieurs destinataires cibles.

Par mi les possibilité que permet CMS, EdelSafe impose le respect d'un profil compatible avec une sécurité de haut niveau. Ainsi, sans entrer dans les détails, :

- Le ou les certificats de signataires sont systématiquement inclus dans les documents signés (élimine la fausse problématique du Proof of Possession au moment de la certification),
- le document CMS généré contient le token d'horodatage signé par le EdelSafe Center et est donc en conformité avec la politique de l'entreprise en la matière,
- le service EdelSafe Center, peut si cela est souhaitable, garder une "main courante" de toutes les signatures apposées ou de toutes les opérations de vérification de signature.
- Tous les certificats de chiffrement utilisés sont ceux fournis par le EdelSafeCenter et donc conformes à la politique de confiance et de sécurité de l'organisme
- Toutes les vérifications de validité de signature (documents ouverts ou reçus) se font au niveau du EdelSafe-Center (en conformité avec la politique de sécurité et de confiance de l'organisme).

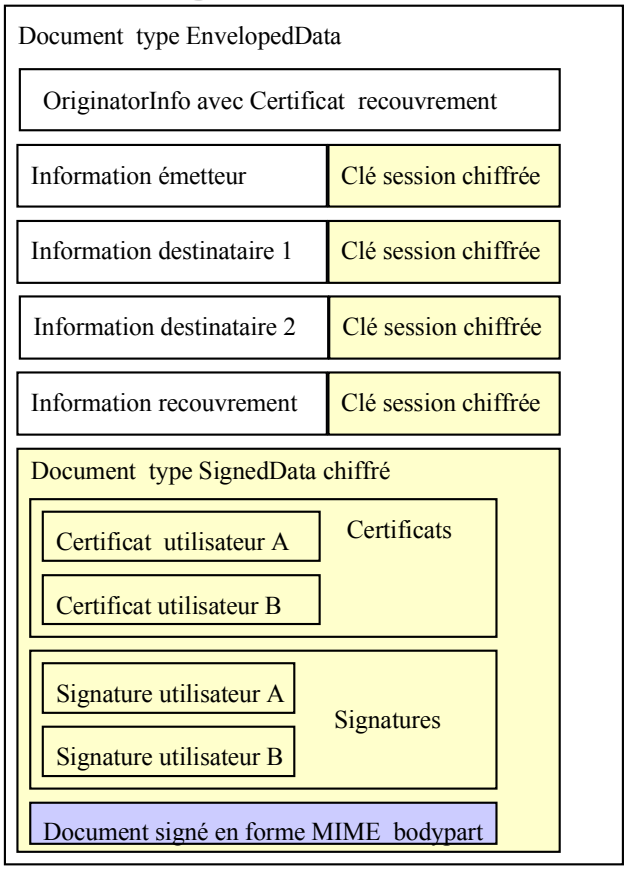
Voici deux schémas de l'utilisation de ces types de donnée par EdelSafeDoc. L'exemple montre un document signé par deux utilisateurs et destiné à deux autre utilisateur avec un champs de recouvrement.

EnvelopedData



Document chiffré, deux destinataires, recouvrement par l'émetteur et l'entreprise

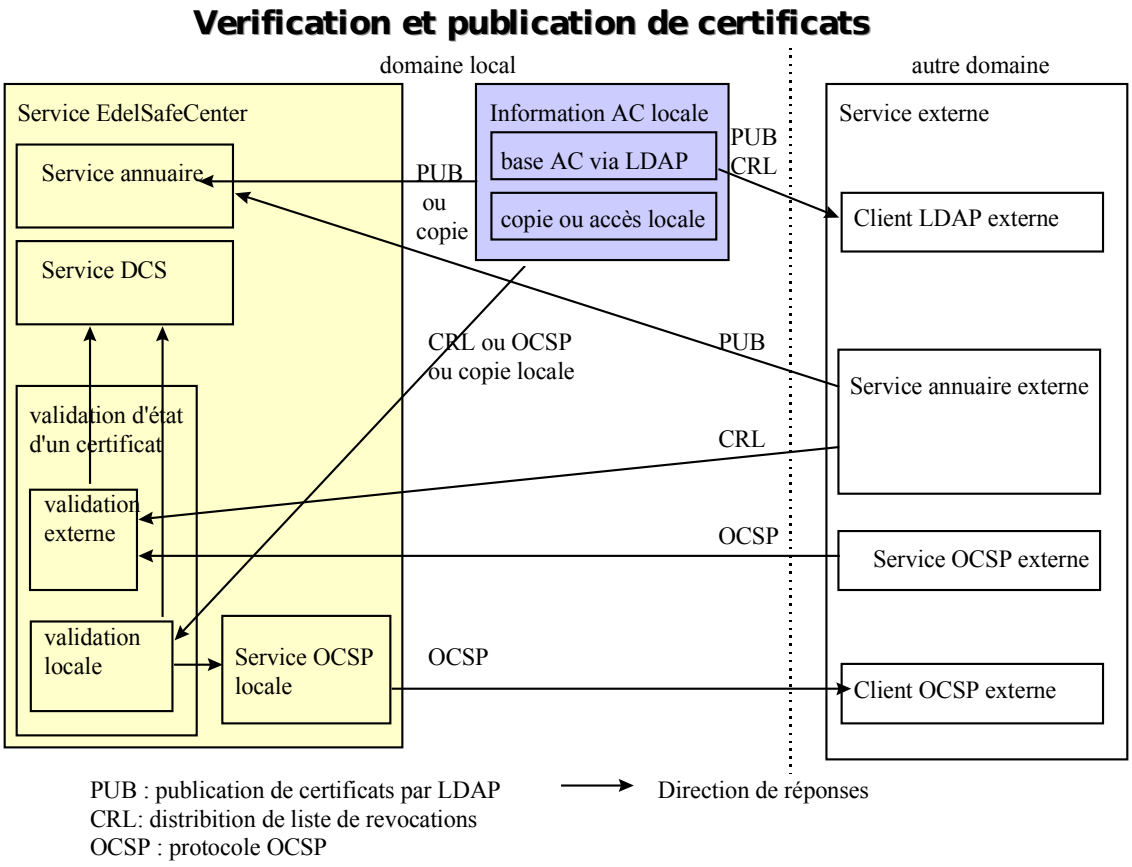
Utilisation SignedData et EnvelopedData



3.6 ORGANISATION DES SERVICES DCS ET OCSP

EdelSafeCenter comprend la fonctionnalité suivante :

- Un service DCS (Data Certification Service) pour valider une chaîne de certificats (*serveur pour les utilisateurs locaux*) ;
- Un client d'interrogation locale avec un client OCSP, un client LDAP pour obtenir des certificats et/ou des CRL ou accès à une base locale pour valider l'état d'un certificat d'un autre organisme (*clients des services des partenaires ou prestataires externe de certification*) ;
- Un service OCSP pour permettre à d'autres organisme de découvrir l'état d'un certificat d'un utilisateur local.



3.6.1 Service DCS

Le client EdelSafeKit utilise le protocole DCS (Data Certification Service) pour demander à EdelSafeCenter de valider une chaîne de certificats. Ce protocole est en cours de discussion dans le groupe de travail PKIX de l'IETF et EdelWeb participe de manière très active à cet effort de standardisation.

Dans un contexte général de certifications croisées, il est difficile pour un utilisateur final de valider un certificat. En outre, l'établissement de relations de confiance n'est pas généralement une question liée à l'utilisateur final, mais plutôt à la politique du domaine de sécurité (son organisme ou entreprise ou un département de cette entreprise).

Dans le but de simplifier la validation d'une chaîne de certificats, il est possible de séparer la validation des chaînes de certificats et les interfaces utilisateurs en utilisant le protocole DCS qui permet au poste client de sous-traiter à un serveur la validation de la chaîne.

D'abord, une interface DCS fournit à l'interface utilisateur une simple réponse de validité d'un certificat. Il est facile de comprendre que la validation d'une chaîne de certificats peut se faire dans le serveur DCS suivant des règles définies par un administrateur de sécurité. Dans de nombreux cas, l'utilisateur n'est pas intéressé dans les détails de cette validation et surtout la définition et le respect de la politique de sécurité est de la responsabilité des administrateurs sécurité et pas de l'utilisateur.

Un service DCS est exploité et configuré par le service de sécurité, cela veut dire par le personnel autorisé à définir des relations de confiance.

Notre implémentation d'un service DCS (au cœur de EdelSafe Center) contient :

- Une interface d'administration pour définir la base des relations de confiance (expression de la politique de sécurité de l'organisme).
- Cette base contient une liste d'autorités de certification (CA) et des règles d'équivalences et de correspondances entre les politiques de ces autorités.
- Plusieurs moyens pour avoir accès aux informations sur les certificats délivrés par des autorités de certification externes sont possibles. Le service peut accéder aux listes de révocation (CRL) intégrées dans un annuaire en utilisant LDAP ou le protocole OCSP pour dialoguer avec le service frontal d'une autorité de certification.
- En général, il y a au moins une base d'information sur les autorités de certification locales; cette base contient les informations de sécurité concernant le domaine local.

3.6.2 Client d'interrogation local

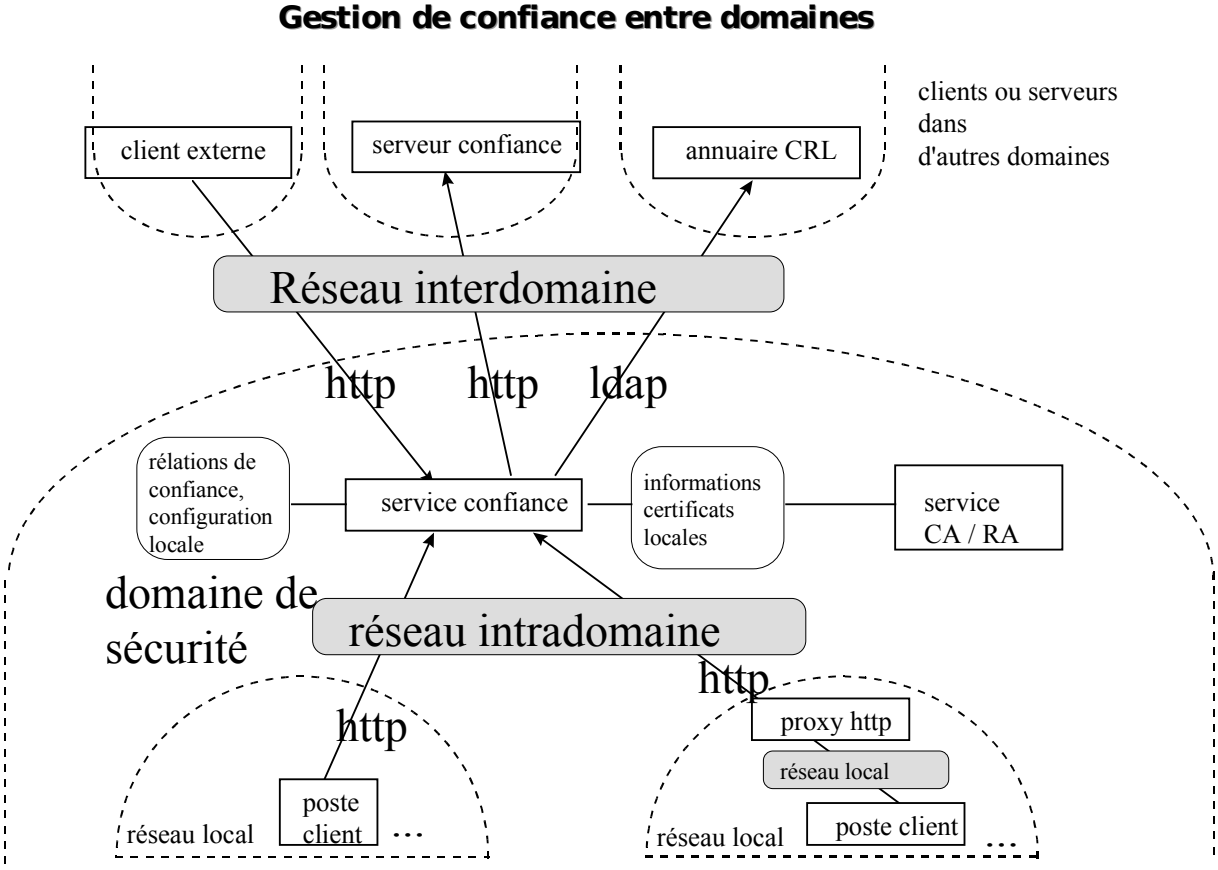
Le client d'interrogation local du EdelSafeCenter est utilisé pour obtenir des informations concernant l'état actuel des certificats locaux et des organismes externes. Le client est conçu de façon à ce que les connections avec une base de données locale de certificats puissent être faites

- Soit par des régulières copies/extractions de la base de données complète ou de la liste de révocation,
- Soit en ligne par accès à la base de donnée de l'autorité.
- Soit en utilisant le protocole OCSP
- Soit en utilisant le protocole LDAP pour obtenir la liste de révocation.

3.6.3 Service publication de certificats et de leurs états

EdelSafeCenter peut fournir un service OCSP à d'autres organisme. EdelSafeCenter se comporte comme un serveur OCSP standard vis-à-vis des autres organismes. Un base de clients avec des certificats de signature est maintenu dans EdelSafeCenter.

L'autorité locale peut choisir de publier la liste de révocation à travers LDAP soit globalement, soit au service EdelSafeCenter, afin de fournir un service OCSP.



3.7 RÉFERÉNCES TECHNIQUES

EdelSafe s'appuie sur un grand nombre de standard de l'Internet, de l'ITU et de l'ISO, et également sur certains documents de la société RSA, qui sont des standards de-facto. Il s'agit de la documentation de :

MIME : Multipurpose Internet Mail Extensions (Internet)

S/MIME : Secure/Multipurpose Internet Mail Extensions (Internet)

PKIX : Internet X.509 Public Key Infrastructure (Internet)

X.500 : The Directory (ITU et ISO)

ASN.1 : Abstract Syntax Notation 1 (ITU et ISO)

PKCS : Public-Key Cryptography Standards (RSA)

HTTP : Hypertext Transfer Protocol (Internet)

Voici une liste de documents de l'Internet qui ne sont pas encore complètement finalisés, et dont le contenu est utilisé dans l'architecture EdelSafe. Notons que EdelWeb contribue activement à ce travail de standardisation.

draft-ietf-smime-ipki-part1 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile

draft-ietf-smime-cms : Cryptographic Message Syntax

draft-ietf-smime-msg : S/MIME version 3 Message Specification

draft-ietf-smime-cert : S/MIME Version 3 Certificate Handling

draft-ietf-pkix-ocsp : Internet X.509 Public Key Infrastructure Online Certificate Status Protocol

draft-ietf-time-stamp : Internet X.509 Public Key Infrastructure Time Stamp Protocols

draft-ietf-pkix-dcs :	Internet X.509 Public Key Infrastructure Data Certification Services
draft-adams-notary :	Notary Protocols
draft-ietf-pkix-dcs :	Data Certification Services

4 LES SERVICES OFFERTS PAR EDELSAFE

La solution *standalone* EdelSafe-Doc offre les services de constitution et d'ouverture d'une enveloppe de sécurité avec signature et/ou chiffrement en respectant le format CMS (nouveau standard IETF de l'Internet) et il est donc possible d'échanger ce type de document (protégé sous enveloppe sécurité) par tous les moyens souhaitables (disques, bandes aussi bien que protocole messagerie, web ou transfert de fichiers).

Le standard CMS permet la signature et le chiffrement de documents. EdelSafeKit utilise soit le type SignedData, si aucun chiffrement est appliqué, soit EnvelopedData (avec un type SignedData imbriqué).

5 FONCTIONS DE CRYPTOLOGIE

EdelSafe comprend les fonctions classiques de chiffrement et de signature numérique.

6 PROCÉDÉS DE CRYPTOLOGIE EMPLOYÉS

EdelSafeDoc est écrit en java et utilise l'interface standard "java development" pour les services de sécurité, afin d'accéder aux service d'un prestataire de services de cryptographie. EdelSafeKit utilise le kit JCE de IAIK de l'université de Graz (URL http://jcewww.iaik.tu-graz.ac.at/).

Ce kit de JCE contient un ensemble de procédé de cryptologie, dont EdelSafe utilise les suivants :

- Condensats: SHA-1 pour la création de condensats, MD5 accepté en lecture
- Chiffrement symétrique : RC4 128 pour le chiffrement, DES, TripleDES RC4 40 acceptés pour le déchiffrement ,
- Chiffrement asymétrique : RSA

EdelSafeCenter inclus des éléments du logiciel OpenSSL (auparavant SSSLeay) pour sécuriser les échanges avec EdelSafeDoc avec des signatures. EdelSafeCenter n'utilise que les algorithme RSA et SHA pour des signatures.

7 GESTION DE CLEFS

Terminologie :

- Dans le suivant nous utilisons le mot « **bi-clé** » pour désigner un couple de clé secrète et un certificat de la clé publique correspondante.
- La création des bi-clés de signature et de ne fait pas partie du logiciel EdelSafe. Il est nécessaire de disposer des services d'autorités de certification soit de l'entreprise soit externe (commerciale) y compris un service d'enregistrement et la fabrication de bi-clé. Nous appelons ce(s) service(s) « **l'autorité locale** »
- Une deuxième service de fourniture de certificat est utilisé pour le recouvrement. Nous appelons ce service « **l'autorité de recouvrement** ». En France il s'agira d'un organisme agréé de gestion des conventions secrètes.
- Le « trousseau individuel de sécurité » : Il 'agit de l'ensemble de bi-clé de signature et de chiffrement de l'utilisateur et le certificat du service EdelSafeCenter. dans la version logicielle actuelle le trousseau est réalisé par un fichier en format PKCS#12 protégé par une « pass-phrase ». *Nota: des discussions on été entreprises avec les fournisseurs de cartes à microprocesseur pour permettre au plus vite une implémentation du "trousseau" dans une carte à puce.*

EdelSafe utilise les certificats de clefs publiques en forme X.509 version 3. Afin de distinguer les deux utilisations " signature " et " chiffrement ", EdelSafe impose que les certificats contiennent une extension de base qui en précise l'utilisation, soit « non-répudiation », soit « échange de clé de chiffrement ». L'extension doit être marquée « critical », des certificats sans extensions ne sont pas acceptés.

EdelSafeKit et EdelSafeCenter stockent les bi-clés et les certificats dans trois endroits :

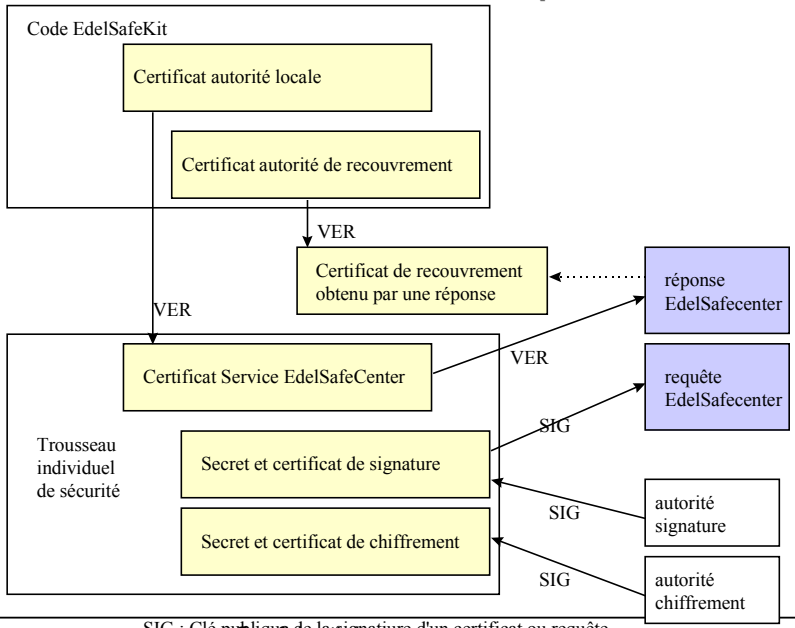
- Le code du EdelSafekit/Doc contient deux certificats, un certificat de signature de l'autorité de certification locale, et un certificat de signature d'une autorité de recouvrement; ces certificats sont "brulés" dans le code pour interdire toute modification par l'utilisateur; en outre toute utilisation impose une communication avec EdelSafeCenter ce qui permet une vérification supplémentaire.

- Le trousseau individuel de sécurité est un fichier en forme PKCS#12 sur le poste client, qui contient un bi-clé de signature, un bi-clé de chiffrement, et le certificat du service EdelSafeCenter utilisable par ce client.
- Un fichier en forme PKCS#12 associé à un service EdelSafeCenter, qui contient des bi-clé et de certificats sur les communications signées avec les clients et les autres prestataires (serveur LDAP, OCSP externe). Il s'agit du "trousseau individuel de sécurité" du service central de sécurité.
-

Les obligations des services des deux autorités sont en conséquence les suivantes :

- L'autorité locale doit certifier un bi-clé de signature pour le service EdelSafeCenter sous forme PKCS#12. Ce certificat doit comprendre une URL comme dénomination alternative. Cette URL est utilisée par EdelSafeKit/Doc pour se connecter au service EdelSafeCenter par HTTP; ceci permet également d'éviter que le logiciel EdelSafeDoc ne soit utilisé dans un autre contexte de sécurité que celui prévu et mis en place par les administrateurs de l'organisme.
- L'autorité locale doit certifier pour chaque utilisateur des bi-clé de signature et de chiffrement. A l'issue de l'opération d'enregistrement l'utilisateur possédera un fichier en forme PKCS#12, qui contiennent ces bi-clés et le certificats de son service EdelSafeCenter : son "trousseau individuel de sécurité".
- L'autorité locale doit publier les certificats des utilisateurs accessibles par EdelSafeCenter à travers un annuaire LDAP. L'autorité locale doit publier des CRL à travers un annuaire LDAP. Alternativement l'autorité locale peut fournir à tous ceux qui en ont besoin une copie de sa base de certificats valides et révoqués, ou un accès directe à ces informations.
- L'autorité de recouvrement doit fournir des certificats de clé publique de chiffrement au service EdelSafeCenter .
- Nota: Le format de message CMS nécessite que les clés publiques ne doivent être certifiées qu'avec preuve de possession de la clé sécrète. (Les certificats de signature ne font pas part de l'objet signé).
- Pour la communication avec d'autres organismes ou entreprises, l'autorité locale doit certifier les clés publiques des autres autorités de certification (« cross-certification »).

Relations certificats poste client



SIG : Clé publique de la signature d'un certificat ou requête
VER: Clé publique d'une verification de signature d'un certificat ou réponse

•

7.1 GESTION CLEFS ET CERTIFICATS DE SIGNATURE

7.1.1 Gestion de clefs et de certificats de signature sur poste client

A l'issue de l'enregistrement et de certification auprès de son autorité locale et de son service EdelSafeCenter, chaque utilisateur possède un bi-clef de signature et de chiffrement, et un certificat de signatures du service EdelSafeCenter. Ces données sont stockées dans un fichier en format PKCS#12 : le "trousseau individuel".

Le logiciel EdelSafeKit vérifie, si le certificat du service EdelSafeCenter a été signé par l'autorité locale, dont un certificat de signature est inclus dans le code du EdelSafeKit.

EdelSafeKit vérifie, si la clé privée de signature correspondent au clé publique certifié.

Chaque communication entre EdelSafeKit et EdelSafeCenter est signée avec la clé de signature de l'utilisateur, le service EdelSafeCenter connaît la liste de ses clients (utilisateurs enregistrés et autorisés à utiliser le produit).

7.1.2 Gestion de clefs et de certificats de signature dans EdelSafeCenter

EdelSafeCenter utilise un trousseau de sécurité : un fichier de configuration en format PKCS#12 pour protéger sa propre bi-clé de signature et un certificat de signature de l'autorité de certification locale.

En outre, pour chaque service externe(OCSP, LDAP, DAP, CDS, ..), il devra posséder un bi-clé clé de signature et un certificat de la clé publique du service partenaire. Les certificats des partenaires doivent être émis par l'autorité de certification locale et ceci est vérifié par le logiciel EdelSafe.

EdelSafeCenter maintient une base de certificats et leurs états pour chaque utilisateur du service. Cette base d'information peut être mise à disposition d'autres organisme connue à travers un service OCSP. EdelSafeCenter maintient également une base de certificats des autorités d'autres organismes, avec qui une communication est organisée. L'état des certificats d'utilisateurs de ces organismes peut être récupéré soit par OCSP en temps réel soit par une distribution de CRL par un annuaire LDAP.

Ces données de l'état de certificats sont utilisées pour le service CDS (certification data service). C'est le rôle de EdelSafeCenter de fournir toute information sur la validité d'une signature sur un document.

7.2 CLEFS DE CHIFFREMENT

Les documents sont chiffrés avec une clé d'algorithme symétrique. Ces clés sont générées d'une façon aléatoire. EdelSafeKit utilise une combinaison de plusieurs techniques de récupération de bruit afin d'initialiser le générateur de d'aléas, essentiellement en analysant l'utilisation du clavier et de la souris.

EdelSafeKit utilise RC4 128 pour chiffrer des données; sur demande cet algorithme peut être remplacé par un autre équivalent. Pour le déchiffrement d'autres algorithmes (DES, TRIPLE DES, RC4 40) sont acceptés.

Les clés de chiffrement sont communiquées avec les données chiffrées protégées par un chiffrement asymétrique RSA. EdelSafeKit accède aux clés publiques destinataires à travers le service EdelSafeCenter, qui comprend un annuaire de certificats en format X.509. Ces certificats doivent contenir une extension qui limitent l'utilisation de ces clés au chiffrement (interdire l'utilisation de clé de signature pour le chiffrement).

Le logiciel EdelSafe comprend l'addition automatique d'un chiffrement par une clé de recouvrement. EdelSafeKit utilise une technique simple issue des travaux de la KRA et très voisine de celle proposée par le projet ETS KRISIS : en cas de chiffrement, au minimum une clé publique d'une autorité de recouvrement est utilisée pour créer un élément RecipientInfo supplémentaire. En fait c'est un champs de recouvrement qui n'est utilisable que par l'autorité prévue (typiquement un organisme agréé).

Par un accès à un annuaire via le service EdelSafeCenter, EdelSafe récupère un certificat de clef publique de chiffrement de recouvrement. Ce certificat doit être signé par une autorité de recouvrement dont EdelSafeKit contient de façon "câblée" et non modifiable un certificat de signature.

7.2.1 Gestion de clefs et de certificats de chiffrement sur poste client

- Chaque utilisateur possède un bi-clef de chiffrement. Il est émis par une autorité de certification, soit interne à de l'entreprise soit externe. Ces informations sont stockées dans son "trousseau individuel de sécurité", à ce jour un fichier en format PKCS#12.
- Le logiciel EdelSafeKit contient dans le code le certificat de signature d'une autorité qui peut fournir des certificats de recouvrement. Le poste client interroge le service EdelSafeCenter pour obtenir un certificat de recouvrement (validé avec le certificat de signature de l'autorité dans le code) et c'est avec la clé publique contenue dans ce certificat que sera chiffré le champs de recouvrement.

7.2.2 Gestion de certificats dans EdelSafeCenter

EdelSafeCenter a accès à une base de certificats de chiffrement pour les utilisateurs et pour le recouvrement. EdelSafeCenter obtient ces certificats soit à travers un accès LDAP soit d'une base de fichiers locaux. Ces certificats sont mis à disposition du poste client à travers un protocole d'annuaire (LDAP sur HTTP).

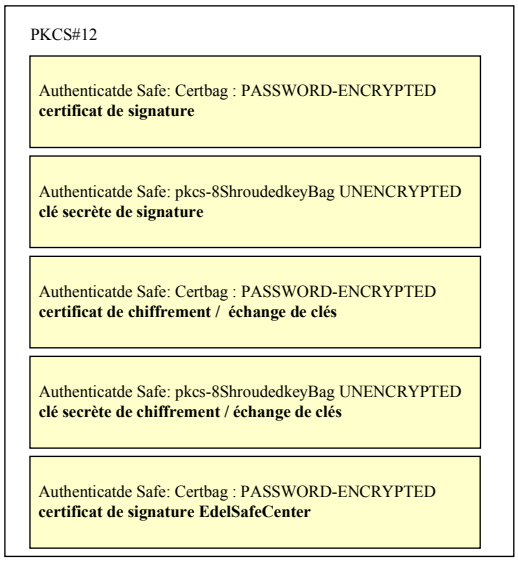
7.3 GESTION DU FICHIER PKCS#12

Le format PKCS#12 offre un grand nombre de possibilités. Il est donc probable que l'autorité locale nécessite une adaptation aux besoins de EdelSafe. A l'issue du processus d'enregistrement et certification auprès de l'autorité locale, l'utilisateur possède logiquement deux fichiers séparés pour les bi-clés de signature et de chiffrement.

EdelSafe comprend un outil permettant de combiner ces données et d'inclure le certificat du EdelSafeCenter afin d'obtenir le trousseau individuel de sécurité de chaque entité cliente EdelSafe; un fichier en format PKCS#12 protégé par une "pass-phrase". Cet outil doit être exécuté dans le même environnement de sécurité que celui de création du bi-clé de signature, afin de protéger correctement la clé privée de signature d'utilisateur.

L'outil assure la plus une grande indépendance possible entre le service de fourniture des deux bi-clés et la construction du trousseau individuel de sécurité. Il est prévu que dans une future version du logiciel la partie bi-clé de signature soit réalisé par du matériel (carte à puce).

Structure du trousseau individuel de sécurité



8 RÉCUPÉRATION DE CLEFS ET RECOUVREMENT

Les clés du chiffrement symétrique peuvent être déchiffrées par chacun des destinataires du document, y inclus l'émetteur et l'organisme agréé qui possède la clé sécrète correspondante au clé de recouvrement.

9 ALTERATION DU PROCÉDÉ OU LA GESTION

Une protection complète contre l'altération des procédés de chiffrement ou la gestion de clés n'est pas possible. Le degré de protection est lié à la difficulté de modifier le code du logiciel EdelSafeKit et de remplacer les bi-clé et de certificats; c'est la raison pour laquelle tous les éléments essentiels ne sont pas dans des fichiers de configuration mais bel et bien "câblés" dans le code même des produits.

EdelSafeKit refuse de chiffrer et de déchiffrer un document s'il n'y a aucune clef de recouvrement utilisée. EdelSafeKit contient une clef de signature d'autorité de certification pour des clé de recouvrement, le documents chiffré doit comprendre la clé de session chiffrée par une clef de recouvrement, dont un certificat signé par l'autorité de recouvrement doit également être présent dans le document dans la liste de certificat de OriginatorInfo du type EnvelopedData.

10 PRÉ- ET POST-TRAITEMENTS

Le logiciel EdelSafe utilise le format EnvelopedData et SignedData du format CMS (cryptographic message syntax) actuellement en cours de normalisation par le IETF dans le contexte de la messagerie sécurisée S/MIME. L'ancêtre de ce format est PKCS#7 de la société RSA. Le traitement d'un document à protéger comprend les étapes suivantes :

- La transformation du document en 'body-part' MIME (attachment) avec les entêtes suivantes : Content-Tranfer-Endcoding : base64 ; Content-type : application/octetstream ; Content-Disposition : attachment ; filename=nomdefichier
- En cas de signatures : Encapsulation dans un type CMS SignedData ; en cas de chiffrement du document,
- Ajout de SignerInfo et de certificats pour chaque signataire du document.
- En cas de chiffrement, encapsulation du SignedData dans un EnvelopedData, et ajout de RecipientInfo pour chaque destinataire, l'émetteur, et le recouvrement, inclusion des certificats de recouvrement dans OriginatorInfo.

11 EXEMPLE DE DOCUMENT SIGNÉ ET CHIFFRÉ :

11.1 TEXTE EN CLAIR À TRAITER (CONTENU DU FICHIER TEXTE.TXT) :

```
Ceci est un texte pour nos amis du SCSSI
```

11.2 SORTIE (PARSING ASN1) APRÈS SIGNATURE D'UN UTILISATEUR DU TEXTE EN CLAIR :

```
    0:d=0  hl=2 l=inf  cons: SEQUENCE
    2:d=1  hl=2 l=   1 prim: INTEGER           :01
```

```
    5:d=1  hl=2 l=  11 cons: SET
    7:d=2  hl=2 l=   9 cons: SEQUENCE
    9:d=3  hl=2 l=   5 prim: OBJECT            :sha1
   16:d=3  hl=2 l=   0 prim: NULL
   18:d=1  hl=2 l=inf  cons: SEQUENCE
   20:d=2  hl=2 l=   9 prim: OBJECT            :pkcs7-data
   31:d=2  hl=2 l=inf  cons: cont [ 0 ]
     33:d=3   hl=3  l=  173  prim:  OCTET  STRING          :Content-Type:
text\plain
Content-Transfert-Encoding: base64
Content-Disposition: attachment; filename=texte.txt

Q2VjaSBlc3QgdW4gdGV4dGUgcG91ciBub3MgYW1pcyBkdSBTQ1NTQ0K
  209:d=3  hl=2 l=   0 prim: EOC
  211:d=2  hl=2 l=   0 prim: EOC
  213:d=1  hl=4 l=1025 cons: cont [ 0 ]
  217:d=2  hl=4 l= 509 cons: SEQUENCE
  221:d=3  hl=4 l= 358 cons: SEQUENCE
  225:d=4  hl=2 l=   3 cons: cont [ 0 ]
  227:d=5  hl=2 l=   1 prim: INTEGER           :02
  230:d=4  hl=2 l=   1 prim: INTEGER           :03
  233:d=4  hl=2 l=  13 cons: SEQUENCE
```

```
235:d=5  hl=2 l=   9 prim: OBJECT            :md5WithRSAEncryption
246:d=5  hl=2 l=   0 prim: NULL
248:d=4  hl=2 l=  59 cons: SEQUENCE
250:d=5  hl=2 l=  11 cons: SET
252:d=6  hl=2 l=   9 cons: SEQUENCE
254:d=7  hl=2 l=   3 prim: OBJECT            :countryName
259:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :FR
263:d=5  hl=2 l=  16 cons: SET
265:d=6  hl=2 l=  14 cons: SEQUENCE
267:d=7  hl=2 l=   3 prim: OBJECT            :organizationName
272:d=7  hl=2 l=   7 prim: PRINTABLESTRING   :EdelWeb
281:d=5  hl=2 l=  13 cons: SET
283:d=6  hl=2 l=  11 cons: SEQUENCE
285:d=7  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
290:d=7  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
296:d=5  hl=2 l=  11 cons: SET
298:d=6  hl=2 l=   9 cons: SEQUENCE
300:d=7  hl=2 l=   3 prim: OBJECT            :commonName
305:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :AC
309:d=4  hl=2 l=  30 cons: SEQUENCE
311:d=5  hl=2 l=  13 prim: UTCTIME           :981108105156Z
```

```
326:d=5  hl=2 l=  13 prim: UTCTIME           :990508095156Z
341:d=4  hl=2 l=  63 cons: SEQUENCE
343:d=5  hl=2 l=  11 cons: SET
345:d=6  hl=2 l=   9 cons: SEQUENCE
347:d=7  hl=2 l=   3 prim: OBJECT            :countryName
352:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :FR
356:d=5  hl=2 l=  16 cons: SET
358:d=6  hl=2 l=  14 cons: SEQUENCE
360:d=7  hl=2 l=   3 prim: OBJECT            :organizationName
365:d=7  hl=2 l=   7 prim: PRINTABLESTRING   :EdelWeb
374:d=5  hl=2 l=  13 cons: SET
376:d=6  hl=2 l=  11 cons: SEQUENCE
378:d=7  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
383:d=7  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
389:d=5  hl=2 l=  15 cons: SET
391:d=6  hl=2 l=  13 cons: SEQUENCE
393:d=7  hl=2 l=   3 prim: OBJECT            :commonName
398:d=7  hl=2 l=   6 prim: PRINTABLESTRING   :DECOOL
406:d=4  hl=3 l= 157 cons: SEQUENCE
409:d=5  hl=2 l=  13 cons: SEQUENCE
411:d=6  hl=2 l=   9 prim: OBJECT            :rsaEncryption
```

```
422:d=6  hl=2 l=   0 prim: NULL
424:d=5  hl=3 l= 139 prim: BIT STRING
566:d=4  hl=2 l=  15 cons: cont [ 3 ]
568:d=5  hl=2 l=  13 cons: SEQUENCE
570:d=6  hl=2 l=  11 cons: SEQUENCE
572:d=7  hl=2 l=   3 prim: OBJECT            :X509v3 Key Usage
577:d=7  hl=2 l=   4 prim: OCTET STRING
583:d=3  hl=2 l=  13 cons: SEQUENCE
585:d=4  hl=2 l=   9 prim: OBJECT            :md5WithRSAEncryption
596:d=4  hl=2 l=   0 prim: NULL
598:d=3  hl=3 l= 129 prim: BIT STRING
730:d=2  hl=4 l= 508 cons: SEQUENCE
734:d=3  hl=4 l= 357 cons: SEQUENCE
738:d=4  hl=2 l=   3 cons: cont [ 0 ]
740:d=5  hl=2 l=   1 prim: INTEGER           :02
743:d=4  hl=2 l=   1 prim: INTEGER           :01
746:d=4  hl=2 l=  13 cons: SEQUENCE
748:d=5  hl=2 l=   9 prim: OBJECT            :md5WithRSAEncryption
759:d=5  hl=2 l=   0 prim: NULL
761:d=4  hl=2 l=  59 cons: SEQUENCE
763:d=5  hl=2 l=  11 cons: SET
```

```
765:d=6  hl=2 l=   9 cons: SEQUENCE
767:d=7  hl=2 l=   3 prim: OBJECT            :countryName
772:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :FR
776:d=5  hl=2 l=  16 cons: SET
778:d=6  hl=2 l=  14 cons: SEQUENCE
780:d=7  hl=2 l=   3 prim: OBJECT            :organizationName
785:d=7  hl=2 l=   7 prim: PRINTABLESTRING   :EdelWeb
794:d=5  hl=2 l=  13 cons: SET
796:d=6  hl=2 l=  11 cons: SEQUENCE
798:d=7  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
803:d=7  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
809:d=5  hl=2 l=  11 cons: SET
811:d=6  hl=2 l=   9 cons: SEQUENCE
813:d=7  hl=2 l=   3 prim: OBJECT            :commonName
818:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :AC
822:d=4  hl=2 l=  30 cons: SEQUENCE
824:d=5  hl=2 l=  13 prim: UTCTIME           :981108105134Z
839:d=5  hl=2 l=  13 prim: UTCTIME           :990508095134Z
854:d=4  hl=2 l=  59 cons: SEQUENCE
856:d=5  hl=2 l=  11 cons: SET
858:d=6  hl=2 l=   9 cons: SEQUENCE
```

```
 860:d=7  hl=2 l=   3 prim: OBJECT            :countryName
 865:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :FR
 869:d=5  hl=2 l=  16 cons: SET
 871:d=6  hl=2 l=  14 cons: SEQUENCE
 873:d=7  hl=2 l=   3 prim: OBJECT            :organizationName
 878:d=7  hl=2 l=   7 prim: PRINTABLESTRING   :EdelWeb
 887:d=5  hl=2 l=  13 cons: SET
 889:d=6  hl=2 l=  11 cons: SEQUENCE
 891:d=7  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
 896:d=7  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
 902:d=5  hl=2 l=  11 cons: SET
 904:d=6  hl=2 l=   9 cons: SEQUENCE
 906:d=7  hl=2 l=   3 prim: OBJECT            :commonName
 911:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :AC
 915:d=4  hl=3 l= 157 cons: SEQUENCE
 918:d=5  hl=2 l=  13 cons: SEQUENCE
 920:d=6  hl=2 l=   9 prim: OBJECT            :rsaEncryption
 931:d=6  hl=2 l=   0 prim: NULL
 933:d=5  hl=3 l= 139 prim: BIT STRING
1075:d=4  hl=2 l=  18 cons: cont [ 3 ]
1077:d=5  hl=2 l=  16 cons: SEQUENCE
```

```
1079:d=6  hl=2 l=  14 cons: SEQUENCE
1081:d=7  hl=2 l=   3 prim: OBJECT            :X509v3 Key Usage
1086:d=7  hl=2 l=   1 prim: BOOLEAN           :255
1089:d=7  hl=2 l=   4 prim: OCTET STRING
1095:d=3  hl=2 l=  13 cons: SEQUENCE
1097:d=4  hl=2 l=   9 prim: OBJECT            :md5WithRSAEncryption
1108:d=4  hl=2 l=   0 prim: NULL
1110:d=3  hl=3 l= 129 prim: BIT STRING
1242:d=1  hl=4 l= 325 cons: SET
1246:d=2  hl=4 l= 321 cons: SEQUENCE
1250:d=3  hl=2 l=   1 prim: INTEGER           :01
1253:d=3  hl=2 l=  64 cons: SEQUENCE
1255:d=4  hl=2 l=  59 cons: SEQUENCE
1257:d=5  hl=2 l=  11 cons: SET
1259:d=6  hl=2 l=   9 cons: SEQUENCE
1261:d=7  hl=2 l=   3 prim: OBJECT            :countryName
1266:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :FR
1270:d=5  hl=2 l=  16 cons: SET
1272:d=6  hl=2 l=  14 cons: SEQUENCE
1274:d=7  hl=2 l=   3 prim: OBJECT            :organizationName
1279:d=7  hl=2 l=   7 prim: PRINTABLESTRING   :EdelWeb
```

```
1288:d=5  hl=2 l=  13 cons: SET
1290:d=6  hl=2 l=  11 cons: SEQUENCE
1292:d=7  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
1297:d=7  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
1303:d=5  hl=2 l=  11 cons: SET
1305:d=6  hl=2 l=   9 cons: SEQUENCE
1307:d=7  hl=2 l=   3 prim: OBJECT            :commonName
1312:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :AC
1316:d=4  hl=2 l=   1 prim: INTEGER           :03
1319:d=3  hl=2 l=   9 cons: SEQUENCE
1321:d=4  hl=2 l=   5 prim: OBJECT            :sha1
1328:d=4  hl=2 l=   0 prim: NULL
1330:d=3  hl=2 l=  93 cons: cont [ 0 ]
1332:d=4  hl=2 l=  24 cons: SEQUENCE
1334:d=5  hl=2 l=   9 prim: OBJECT            :contentType
1345:d=5  hl=2 l=  11 cons: SET
1347:d=6  hl=2 l=   9 prim: OBJECT            :pkcs7-data
1358:d=4  hl=2 l=  28 cons: SEQUENCE
1360:d=5  hl=2 l=   9 prim: OBJECT            :signingTime
1371:d=5  hl=2 l=  15 cons: SET
1373:d=6  hl=2 l=  13 prim: UTCTIME           :981112150514Z
```

```
1388:d=4  hl=2 l=  35 cons: SEQUENCE
1390:d=5  hl=2 l=   9 prim: OBJECT            :messageDigest
1401:d=5  hl=2 l=  22 cons: SET
1403:d=6  hl=2 l=  20 prim: OCTET STRING
1425:d=3  hl=2 l=  13 cons: SEQUENCE
1427:d=4  hl=2 l=   9 prim: OBJECT            :rsaEncryption
1438:d=4  hl=2 l=   0 prim: NULL
1440:d=3  hl=3 l= 128 prim: OCTET STRING
1571:d=1  hl=2 l=   0 prim: EOC
```

11.3 CERTIFICAT (PARSING ASN1) DE SIGNATURE DE L'AUTORITÉ DE RECOUVREMENT :

```
 0:d=0  hl=4 l= 511 cons: SEQUENCE
 4:d=1  hl=4 l= 360 cons: SEQUENCE
 8:d=2  hl=2 l=   1 prim: INTEGER           :03
11:d=2  hl=2 l=  13 cons: SEQUENCE
13:d=3  hl=2 l=   9 prim: OBJECT            :md5WithRSAEncryption
24:d=3  hl=2 l=   0 prim: NULL
26:d=2  hl=2 l=  79 cons: SEQUENCE
28:d=3  hl=2 l=  11 cons: SET
30:d=4  hl=2 l=   9 cons: SEQUENCE
32:d=5  hl=2 l=   3 prim: OBJECT            :countryName
```

```
 37:d=5  hl=2 l=   2 prim: PRINTABLESTRING   :FR
 41:d=3  hl=2 l=  14 cons: SET
 43:d=4  hl=2 l=  12 cons: SEQUENCE
 45:d=5  hl=2 l=   3 prim: OBJECT            :organizationName
 50:d=5  hl=2 l=   5 prim: PRINTABLESTRING   :SCSSI
 57:d=3  hl=2 l=  13 cons: SET
 59:d=4  hl=2 l=  11 cons: SEQUENCE
 61:d=5  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
 66:d=5  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
 72:d=3  hl=2 l=  33 cons: SET
 74:d=4  hl=2 l=  31 cons: SEQUENCE
 76:d=5  hl=2 l=   3 prim: OBJECT            :commonName
 81:d=5  hl=2 l=  24 prim: PRINTABLESTRING   :Autorite de recouvrement
107:d=2  hl=2 l=  30 cons: SEQUENCE
109:d=3  hl=2 l=  13 prim: UTCTIME           :981109090652Z
124:d=3  hl=2 l=  13 prim: UTCTIME           :990509080652Z
139:d=2  hl=2 l=  67 cons: SEQUENCE
141:d=3  hl=2 l=  11 cons: SET
143:d=4  hl=2 l=   9 cons: SEQUENCE
145:d=5  hl=2 l=   3 prim: OBJECT            :countryName
150:d=5  hl=2 l=   2 prim: PRINTABLESTRING   :FR
```

```
154:d=3  hl=2 l=  14 cons: SET
156:d=4  hl=2 l=  12 cons: SEQUENCE
158:d=5  hl=2 l=   3 prim: OBJECT            :organizationName
163:d=5  hl=2 l=   5 prim: PRINTABLESTRING   :SCSSI
170:d=3  hl=2 l=  13 cons: SET
172:d=4  hl=2 l=  11 cons: SEQUENCE
174:d=5  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
179:d=5  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
185:d=3  hl=2 l=  21 cons: SET
187:d=4  hl=2 l=  19 cons: SEQUENCE
189:d=5  hl=2 l=   3 prim: OBJECT            :commonName
194:d=5  hl=2 l=  12 prim: PRINTABLESTRING   :recouvrement
208:d=2  hl=3 l= 157 cons: SEQUENCE
211:d=3  hl=2 l=  13 cons: SEQUENCE
213:d=4  hl=2 l=   9 prim: OBJECT            :rsaEncryption
224:d=4  hl=2 l=   0 prim: NULL
226:d=3  hl=3 l= 139 prim: BIT STRING
368:d=1  hl=2 l=  13 cons: SEQUENCE
370:d=2  hl=2 l=   9 prim: OBJECT            :md5WithRSAEncryption
381:d=2  hl=2 l=   0 prim: NULL
383:d=1  hl=3 l= 129 prim: BIT STRING
```

11.4 SORTIE (PARSING ASN.1) APRÈS CHIFFREMENT:

```
  0:d=0  hl=4 l=3271 cons: SEQUENCE
  4:d=1  hl=2 l=   1 prim: INTEGER           :02
  7:d=1  hl=4 l= 515 cons: SET
 11:d=2  hl=4 l= 511 cons: SEQUENCE
 15:d=3  hl=4 l= 360 cons: SEQUENCE
 19:d=4  hl=2 l=   1 prim: INTEGER           :03
 22:d=4  hl=2 l=  13 cons: SEQUENCE
 24:d=5  hl=2 l=   9 prim: OBJECT            :md5WithRSAEncryption
 35:d=5  hl=2 l=   0 prim: NULL
 37:d=4  hl=2 l=  79 cons: SEQUENCE
 39:d=5  hl=2 l=  11 cons: SET
 41:d=6  hl=2 l=   9 cons: SEQUENCE
 43:d=7  hl=2 l=   3 prim: OBJECT            :countryName
 48:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :FR
 52:d=5  hl=2 l=  14 cons: SET
 54:d=6  hl=2 l=  12 cons: SEQUENCE
 56:d=7  hl=2 l=   3 prim: OBJECT            :organizationName
```

```
   61:d=7  hl=2 l=   5 prim: PRINTABLESTRING   :SCSSI
   68:d=5  hl=2 l=  13 cons: SET
   70:d=6  hl=2 l=  11 cons: SEQUENCE
   72:d=7  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
   77:d=7  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
   83:d=5  hl=2 l=  33 cons: SET
   85:d=6  hl=2 l=  31 cons: SEQUENCE
   87:d=7  hl=2 l=   3 prim: OBJECT            :commonName
     92:d=7    hl=2  l=    24  prim:  PRINTABLESTRING      :Autorite  de
recouvrement
  118:d=4  hl=2 l=  30 cons: SEQUENCE
  120:d=5  hl=2 l=  13 prim: UTCTIME           :981109090652Z
  135:d=5  hl=2 l=  13 prim: UTCTIME           :990509080652Z
  150:d=4  hl=2 l=  67 cons: SEQUENCE
  152:d=5  hl=2 l=  11 cons: SET
  154:d=6  hl=2 l=   9 cons: SEQUENCE
  156:d=7  hl=2 l=   3 prim: OBJECT            :countryName
  161:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :FR
  165:d=5  hl=2 l=  14 cons: SET
  167:d=6  hl=2 l=  12 cons: SEQUENCE
  169:d=7  hl=2 l=   3 prim: OBJECT            :organizationName
  174:d=7  hl=2 l=   5 prim: PRINTABLESTRING   :SCSSI
```

```
181:d=5  hl=2 l=  13 cons: SET
183:d=6  hl=2 l=  11 cons: SEQUENCE
185:d=7  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
190:d=7  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
196:d=5  hl=2 l=  21 cons: SET
198:d=6  hl=2 l=  19 cons: SEQUENCE
200:d=7  hl=2 l=   3 prim: OBJECT            :commonName
205:d=7  hl=2 l=  12 prim: PRINTABLESTRING   :recouvrement
219:d=4  hl=3 l= 157 cons: SEQUENCE
222:d=5  hl=2 l=  13 cons: SEQUENCE
224:d=6  hl=2 l=   9 prim: OBJECT            :rsaEncryption
235:d=6  hl=2 l=   0 prim: NULL
237:d=5  hl=3 l= 139 prim: BIT STRING
379:d=3  hl=2 l=  13 cons: SEQUENCE
381:d=4  hl=2 l=   9 prim: OBJECT            :md5WithRSAEncryption
392:d=4  hl=2 l=   0 prim: NULL
394:d=3  hl=3 l= 129 prim: BIT STRING
526:d=1  hl=4 l= 456 cons: SET
530:d=2  hl=3 l= 215 cons: SEQUENCE
533:d=3  hl=2 l=   1 prim: INTEGER           :00
536:d=3  hl=2 l=  64 cons: SEQUENCE
```

```
538:d=4  hl=2 l=  59 cons: SEQUENCE
540:d=5  hl=2 l=  11 cons: SET
542:d=6  hl=2 l=   9 cons: SEQUENCE
544:d=7  hl=2 l=   3 prim: OBJECT            :countryName
549:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :FR
553:d=5  hl=2 l=  16 cons: SET
555:d=6  hl=2 l=  14 cons: SEQUENCE
557:d=7  hl=2 l=   3 prim: OBJECT            :organizationName
562:d=7  hl=2 l=   7 prim: PRINTABLESTRING   :EdelWeb
571:d=5  hl=2 l=  13 cons: SET
573:d=6  hl=2 l=  11 cons: SEQUENCE
575:d=7  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
580:d=7  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
586:d=5  hl=2 l=  11 cons: SET
588:d=6  hl=2 l=   9 cons: SEQUENCE
590:d=7  hl=2 l=   3 prim: OBJECT            :commonName
595:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :AC
599:d=4  hl=2 l=   1 prim: INTEGER           :04
602:d=3  hl=2 l=  13 cons: SEQUENCE
604:d=4  hl=2 l=   9 prim: OBJECT            :rsaEncryption
615:d=4  hl=2 l=   0 prim: NULL
```

```
  617:d=3  hl=3 l= 128 prim: OCTET STRING
  748:d=2  hl=3 l= 235 cons: SEQUENCE
  751:d=3  hl=2 l=   1 prim: INTEGER           :00
  754:d=3  hl=2 l=  84 cons: SEQUENCE
  756:d=4  hl=2 l=  79 cons: SEQUENCE
  758:d=5  hl=2 l=  11 cons: SET
  760:d=6  hl=2 l=   9 cons: SEQUENCE
  762:d=7  hl=2 l=   3 prim: OBJECT            :countryName
  767:d=7  hl=2 l=   2 prim: PRINTABLESTRING   :FR
  771:d=5  hl=2 l=  14 cons: SET
  773:d=6  hl=2 l=  12 cons: SEQUENCE
  775:d=7  hl=2 l=   3 prim: OBJECT            :organizationName
  780:d=7  hl=2 l=   5 prim: PRINTABLESTRING   :SCSSI
  787:d=5  hl=2 l=  13 cons: SET
  789:d=6  hl=2 l=  11 cons: SEQUENCE
  791:d=7  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
  796:d=7  hl=2 l=   4 prim: PRINTABLESTRING   :TEST
  802:d=5  hl=2 l=  33 cons: SET
  804:d=6  hl=2 l=  31 cons: SEQUENCE
  806:d=7  hl=2 l=   3 prim: OBJECT            :commonName
  811:d=7  hl=2 l=  24 prim: PRINTABLESTRING   :Autorite de
recouvrement
```

```
  837:d=4  hl=2 l=   1 prim: INTEGER           :03
  840:d=3  hl=2 l=  13 cons: SEQUENCE
  842:d=4  hl=2 l=   9 prim: OBJECT            :rsaEncryption
  853:d=4  hl=2 l=   0 prim: NULL
  855:d=3  hl=3 l= 128 prim: OCTET STRING
  986:d=1  hl=2 l=inf  cons: SEQUENCE
  988:d=2  hl=2 l=   9 prim: OBJECT            :pkcs7-data
  999:d=2  hl=2 l=  20 cons: SEQUENCE
 1001:d=3  hl=2 l=   8 prim: OBJECT            :des-ede3-cbc
 1011:d=3  hl=2 l=   8 prim: OCTET STRING
 1021:d=2  hl=4 l=2248 prim: cont [ 0 ]
 3273:d=2  hl=2 l=   0 prim: EOC
```

11.5 CERTIFICATS UTILISÉS

11.5.1 Certificat de signature :

```
Version: 3
Serial number: 3
Signature algorithm: md5WithRSAEncryption
Issuer: C: FR , O: EdelWeb , OU: TEST , CN: AC
Valid not before: Sun Nov 08 11:51:56 CET 1998
      not after: Sat May 08 11:51:56 CEST 1999
Subject: C: FR , O: EdelWeb , OU: TEST , CN: DECOOL
```

public exponent: 5

modulus:
ab09e680cea62b46b5d78e7c8a19571ce65d93b1eef69562b1de0f09b56d20153e1751
f46eacaddaeac594bae7a7e6551ff0f540e8f3c9dc95aab3c9b01e68d8d71538ad203c
779ba52bc795916adce930ab7a66a4ab0ae0515fc60c24599c4580306a2dfa8d
fe97daec5e7067df98ff633d2a076eb2f50479ed784531a768d1

Extensions: 1

Certificate Fingerprint:
3D:EA:42:68:C6:23:C1:3E:DD:83:3A:90:C7:67:99:54

11.5.2 Certificat de l'autorité de certification :

Version: 3

Serial number: 1

Signature algorithm: md5WithRSAEncryption

Issuer: C: FR , O: EdelWeb , OU: TEST , CN: AC

Valid not before: Sun Nov 08 11:51:34 CET 1998

not after: Sat May 08 11:51:34 CEST 1999

Subject: C: FR , O: EdelWeb , OU: TEST , CN: AC

public exponent: 3

modulus:
e818ea20fea7077c41ed93693ecfe4b70d8c88455d23ef20f256cba672e21a
6b207ea890bee3eef6fe1d1dbeeecef6d4fe715d25e665d759762fce808084c
0df9de7eb9fd2dc2291348a4b4c761e326057a3f737e58fc704285bd85adc9
7c2b4698bccf9775109a2d18a8da26e92be12ebd0f476f7af534c899c5c3e1b
e28635

Extensions: 1

Certificate Fingerprint: E6:C1:28:52:9E:6C:46:C7:14:3B:F2:6A:1E:2F:35:1A

11.5.3 Certificat de Chiffrement :

Version: 3
Serial number: 4
Signature algorithm: md5WithRSAEncryption
Issuer: C: FR , O: EdelWeb , OU: TEST , CN: AC
Valid not before: Sun Nov 08 11:51:58 CET 1998
not after: Sat May 08 11:51:58 CEST 1999
Subject: C: FR , O: EdelWeb , OU: TEST , CN: DECOOL
public exponent: 3
modulus:
a7b7d025eadee53bc0d4fb753dcd43e371f27cb45fd159b2627a48f30d0bca
3890a5bae26e6e1c511d59d5354d4bb0cd2011b7f229e3bd3bcdfbbbbf8b49
e23d0f8c3a7f665f8e7e8ac3e4275a059c68d26ddb38ba457fa57c79918848
796fe303f7342b26fcad3fbdbea2d4f09e5356ae9100d519d8d2ad058a7e8b
20e15ebf
Extensions: 1
Certificate Fingerprint: 7B:DD:F3:85:64:E9:46:04:2C:32:38:7C:0D:4D:A2:9D

11.5.4 Certificat de recouvrement :

Version: 1
Serial number: 3
Signature algorithm: md5WithRSAEncryption
Issuer: C: FR , O: SCSSI , OU: TEST , CN: Autorite de recouvrement
Valid not before: Mon Nov 09 10:06:52 CET 1998
not after: Sun May 09 10:06:52 CEST 1999
Subject: C: FR , O: SCSSI , OU: TEST , CN: recouvrement

public exponent: b

modulus:
c575826e1871b75b9dbf05c412e874d3782b80f6dfd9ef42cb1b4bca216fbee
6d4507867adceb29cddbd5e21d0d1a8d51085b4a2ac301e0a32cd47ec2650
3bd53e8796a18a437a21d77323b19a652b9ce5f7afff787bac34288ac00567
676ddb76358175614a330581ea1eebb5c8a34959bb8ca4bba37bc7929ec97
cc290c7e5

Certificate Fingerprint: 86:75:43:C9:74:56:73:AA:E3:8B:BB:0B:A9:26:60:48

11.5.5 Certificat de l'autorité de recouvrement :

Version: 1

Serial number: 1

Signature algorithm: md5WithRSAEncryption

Issuer: C: FR , O: SCSSI , OU: TEST , CN: Autorite de recouvrement

Valid not before: Mon Nov 09 10:06:30 CET 1998

not after: Sun May 09 10:06:30 CEST 1999

Subject: C: FR , O: SCSSI , OU: TEST , CN: Autorite de recouvrement

public exponent: 3

modulus:
cf87337c61c08541aeaf263573d6060a8520e6b5e5bb93fde97aa66cb1252e
a7186fd7847964d128e30d5bb75279fa931b0519de6199168cece450c54fce
a2d9c2a82c6d2d4b46904560b18a3ee4a5c97a1bc9f78f9c8930713f92b89d
20b4ec556fdc8a7176dbfbc0a55411cc5c1503fbad57192923dc6041d81108f
c0f5e9f

Certificate Fingerprint: B6:E6:51:98:56:31:5F:94:6F:28:0D:40:5E:E1:47:B8