Secure headers

DGA - CELAR - Laurent CAILLEUX

Plan

- Introduction
- Solutions actuelles
- Secure headers
- Conclusion
- Démonstration

Introduction

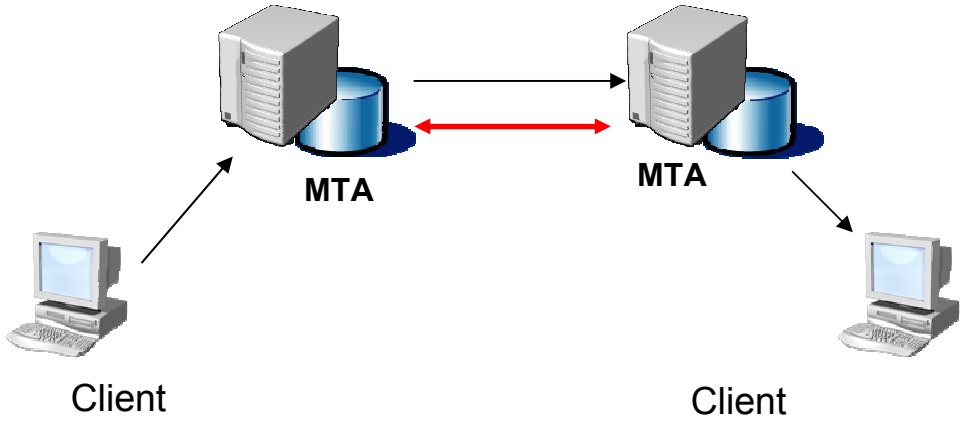
- La messagerie électronique est l'un des outils majeurs de la communication personnelle et professionnelle
- La sécurisation des échanges est un impératif actuel
- Les services d'intégrité et de non répudiation de messages sont indispensables
- Des solutions de sécurisation de messages existent, mais répondent elles vraiment totalement aux besoins ?

Problématique

- Aujourd'hui,
  - le protocole standard de transport de message est SMTP (RFC 5321)
  - le protocole standard de format de message est IMF (RFC 5322)
- Le principal protocole de sécurisation de message est SMIME (sécurisation avec engagement de responsabilité de l'émetteur)
- Le problème de SMIME est qu'il offre principalement des mécanismes de sécurisation de contenu. Dans ce cas, la sécurisation des entêtes de messages n'est pas garantie.
- Comment s'assurer que les entêtes n'ont pas été modifiés ?
- Comment assurer la confidentialité du sujet du message ?
- Certes des solutions existent, mais il faut utiliser des clients spécifiques (encapsulation complète du message)

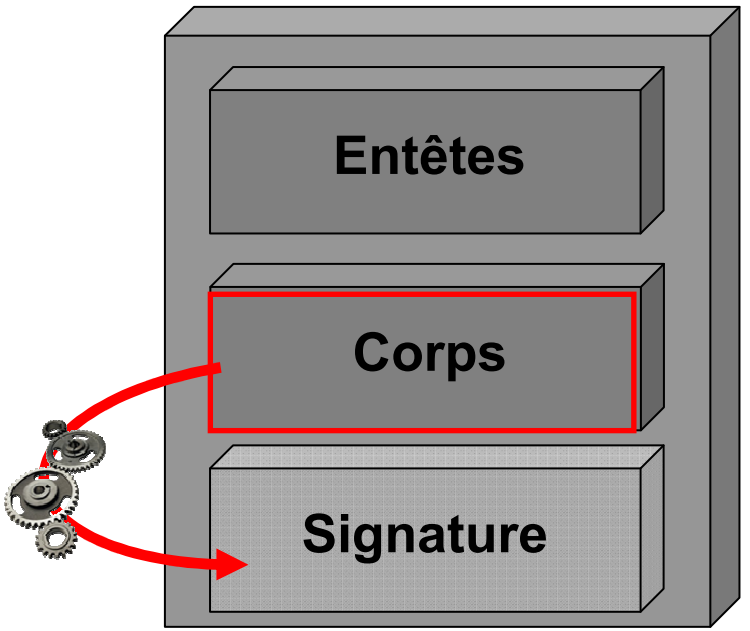
Solutions actuelles

- **DKIM**
  - **Signature du domaine par le MUA ou MTA émetteur et contrôle par le MUA ou MTA destinataire**
  - **Certificat dans le DNS**
  - **Intégrité entre le MTA émetteur et le MTA destinataire (pas de bout en bout)**
- **Pas d'engagement de responsabilité de l'émetteur**



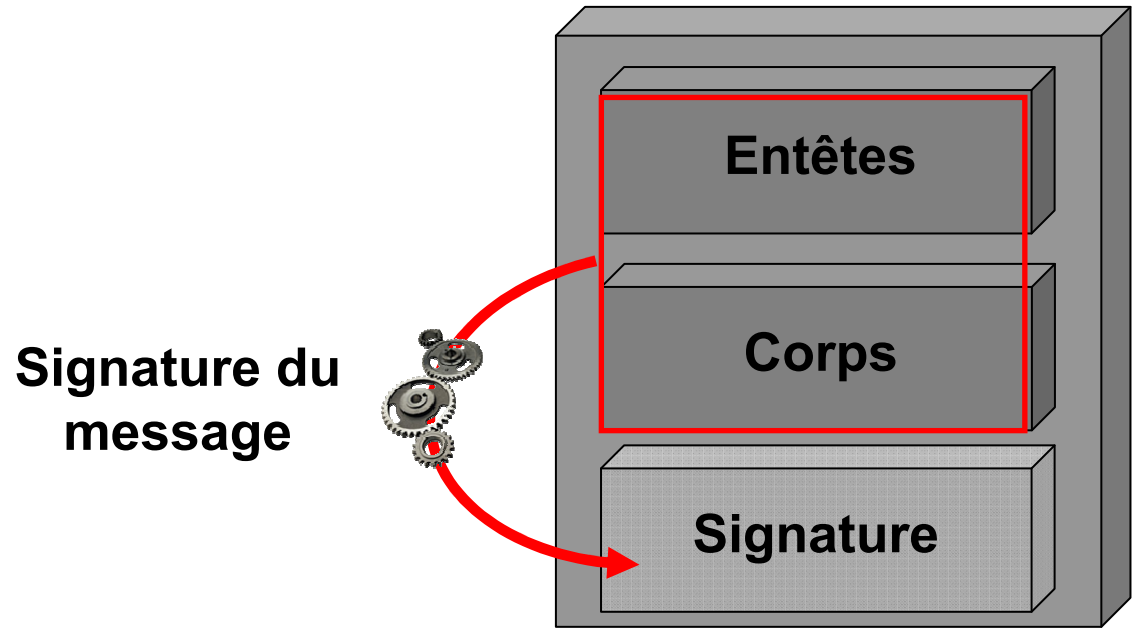
Solutions actuelles

- **SMIME**
  - **Signature du contenu du message**
  - **Protocole standard (Thunderbird, Outlook, …)**
  - **Ne sécurise pas les entêtes**



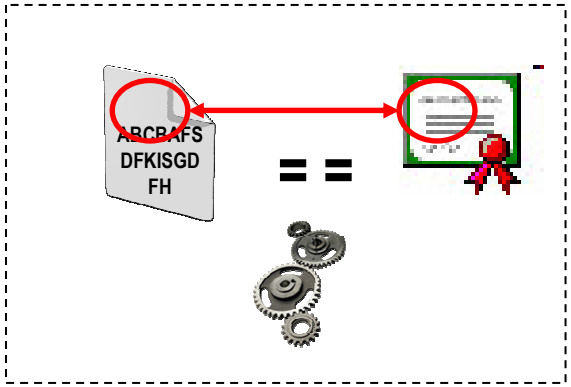
Solutions actuelles

- **SMIME**
  - **Encapsulation d'un objet MIME rfc822**
  - **Impose un client spécifique à l'émission et à la réception**



Solutions actuelles

- **Sécurisation des entêtes dans SMIME, seul l'entête From est contrôlé**
  - **corrélation entre l'adresse From du message et l'adresse présente dans le certificat**



MUA

Plan

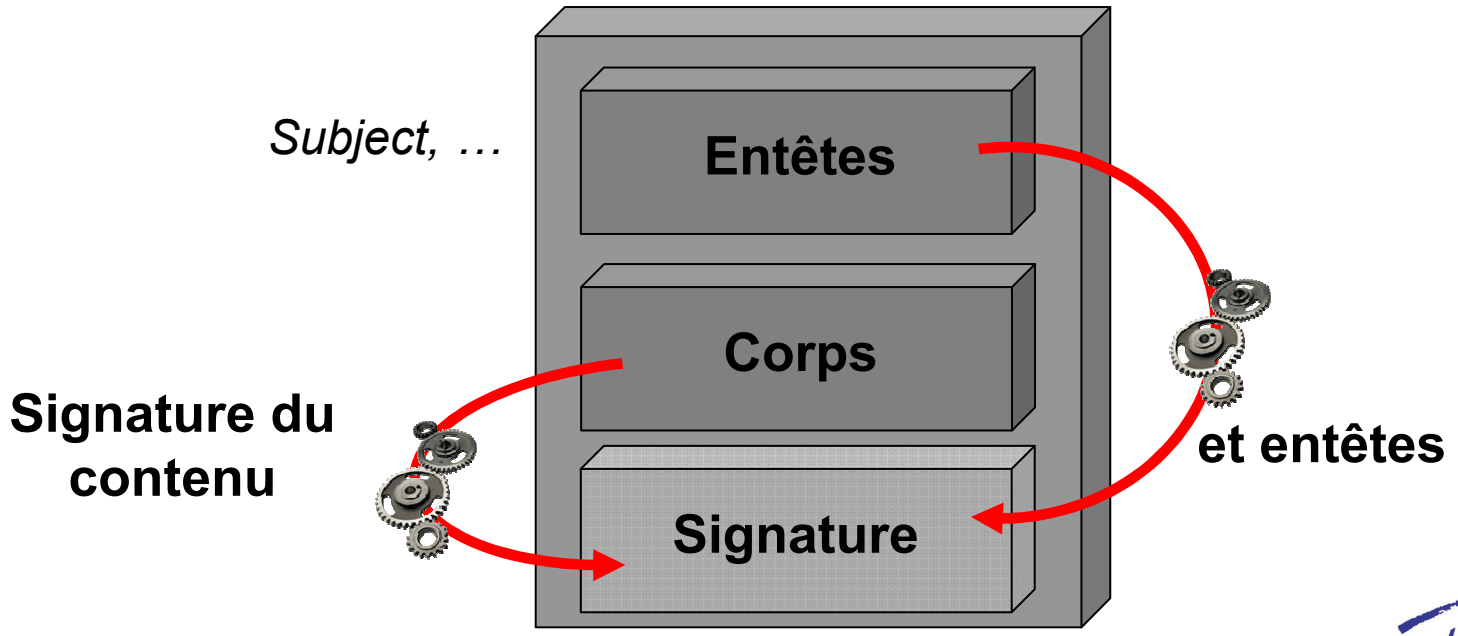
- Introduction
- Solutions actuelles
- Secure headers
- Conclusion
- Démonstration

Secure headers

- Services d'intégrité et de non répudiation
- Intégration des entêtes à sécuriser dans la signature
- Utilisation des attributs signés CMS
- Transport des entêtes et valeurs associées
- Statuts possibles (optionnels)
  - 0 . (Duplicated)
  - 1 . (Deleted)
  - 2 . (Modified)

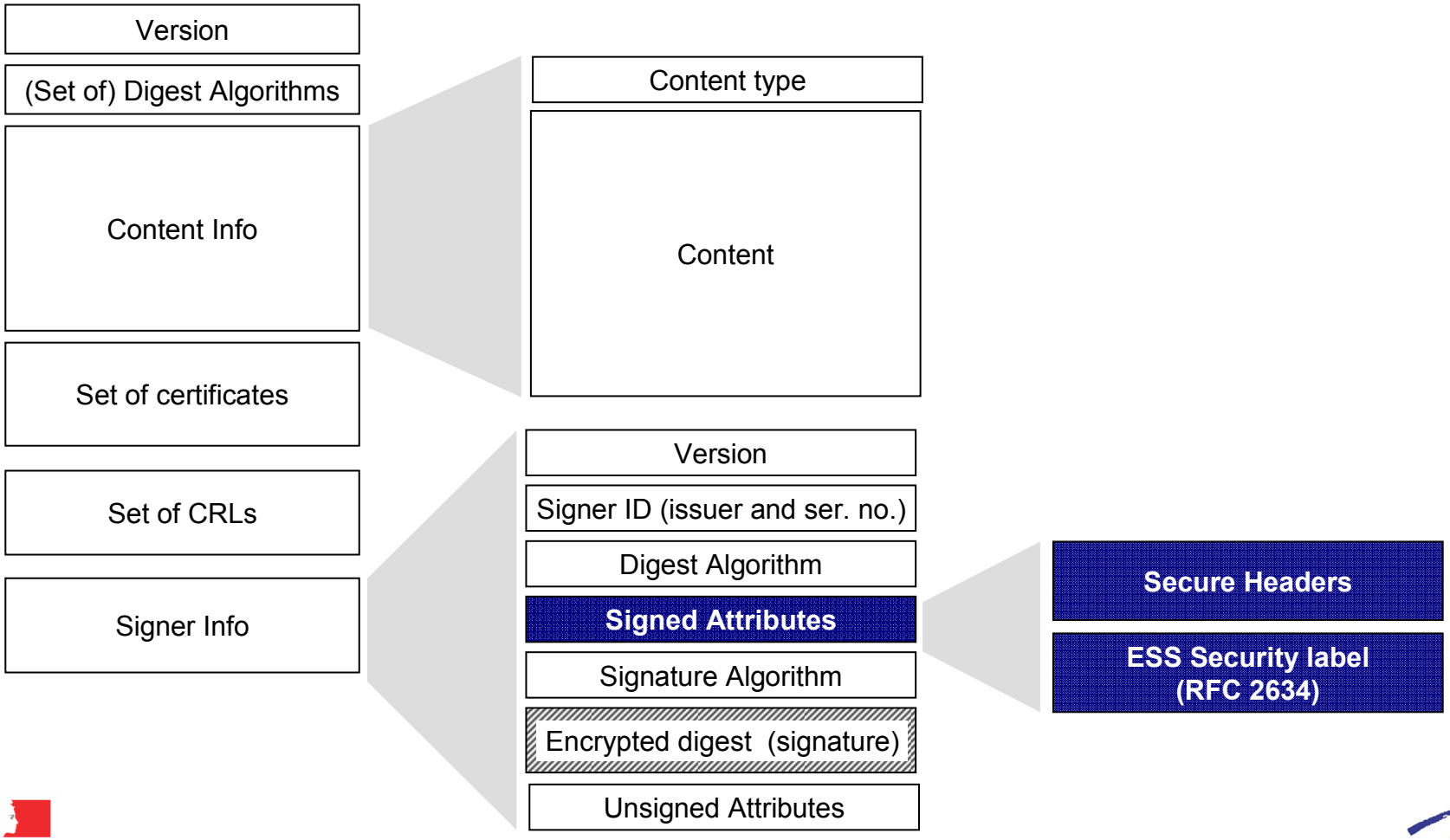
Secure headers

- Respecte les standards en cours
  - SMIME, CMS
- Permet la sécurisation des entêtes sans encapsulation du message

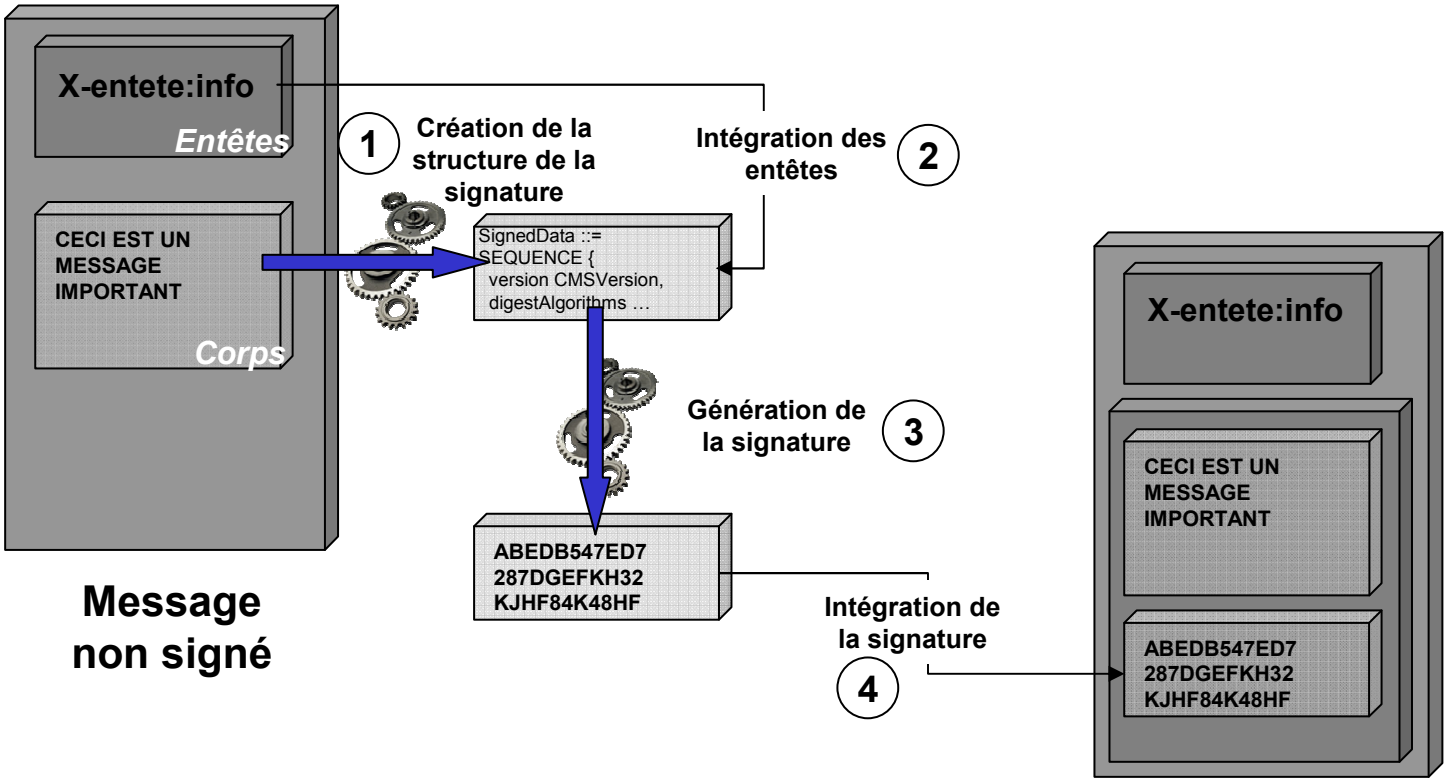


Secure headers - Structure

Structure d'un objet CMS (RFC 3852)

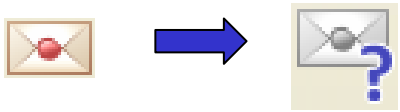


Secure headers – mécanismes de signature



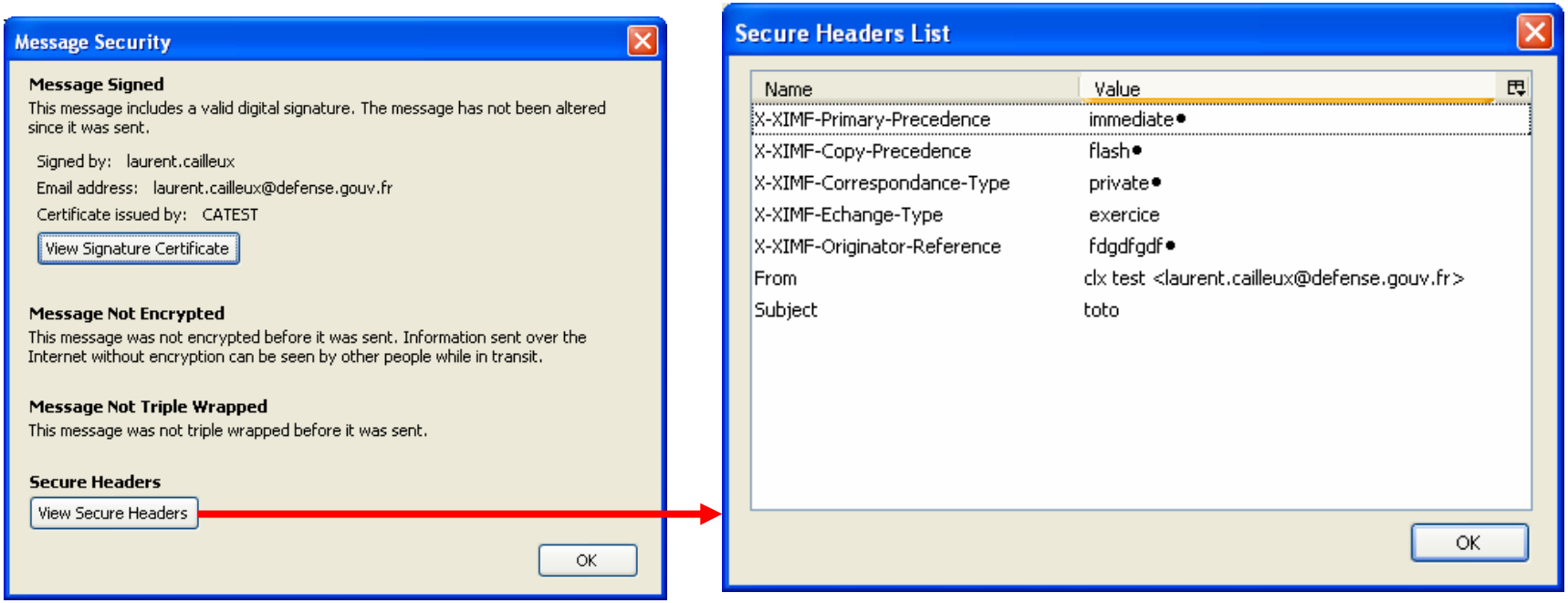
Secure headers

- Lors de la génération de la signature, le MUA doit créer une structure SecureHeaders.
- Lors de la vérification de la signature, le MUA doit effectuer une comparaison entre les entêtes du message et les entêtes présents dans la structure SecureHeaders.
- Si la comparaison est en échec, la signature est toujours valable mais affichage d'un avertissement



Secure headers

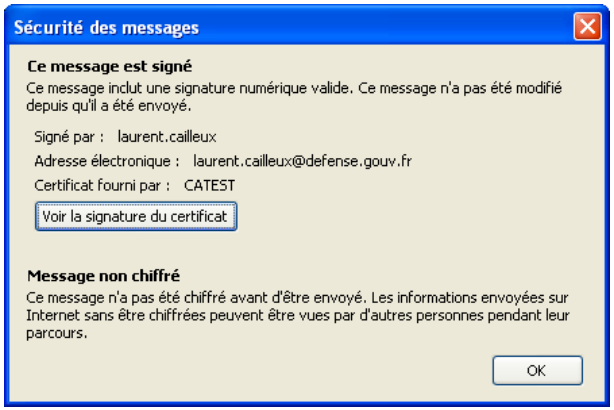
- Le MUA doit offrir un affichage des entêtes sécurisés



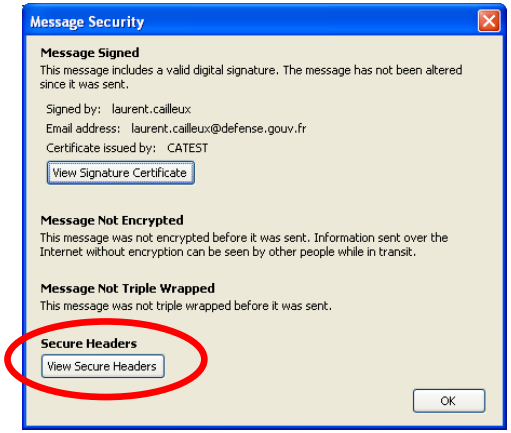
Secure headers

- **Interopérabilité avec des clients SMIME qui n'implémentent pas les Secure Headers (la signature est valable mais le destinataire n'a pas d'information sur les entêtes sécurisés)**

Fenêtre « Message Security » pour un même message



Thunderbird



Trustedbird

Avenir – Secure headers

- Version Draft (aspects chiffrement)
- Rédaction en cours d'un draft RFC
- Implémentation dans TrustedBird
- Implémentation dans NSS Mozilla (Network Security Services) ?

Demo