Messagerie de confiance

DGA / CELAR
Laurent CAILLEUX

Plan

- Messagerie de confiance
  - Concepts
  - Besoins utilisateur
- Services nécessaires
- Architectures de messagerie
  - Type Internet
  - De confiance
- Services intégrés dans le projet TrustedBird
- XIMF
- Entêtes sécurisés
- Démonstration du client TrustedBird

Plan

- **Messagerie de confiance**
  - **Concepts**
  - **Besoins utilisateur**
- **Services nécessaires**
- **Architectures de messagerie**
  - **Type Internet**
  - **De confiance**
- **Services intégrés dans le projet TrustedBird**
- **XIMF**
- **Entêtes sécurisés**
- **Démonstration du client TrustedBird**

Concepts de confiance

- Fiabilité d'une personne, d'une entité ou d'un système
- La confiance est la base de toute relation. La recherche, puis l'analyse de preuves peut renforcer la confiance ou au contraire créer un nouveau sentiment; la méfiance
- Faire confiance a priori, c'est se déterminer spontanément en supposant un a priori positif. A l'inverse on qualifiera le sentiment de méfiance ou défiance

Offre de services permettant de garantir un niveau de confiance auprès des utilisateurs

Besoins utilisateur

- J'envoie un message enrichi (affaire, références, priorité, …)
  - à une personne de confiance, (dispose d'une identité reconnue, *certificat*),
  - avec un niveau de sensibilité du contenu,
  - en accord avec la loi et les réglementations (type de correspondance, …),
  - quand je le souhaite.
- J'exige
  - qu'il ne puisse être éventuellement lu par personne d'autre,
  - ni même modifié,
  - qu'il parvienne à destination dans un délai demandé (en fonction d'une urgence),
  - être informé des évènements associés à cet échange
- Le destinataire et moi-même ne pouvons nier cet échange

Plan

- Messagerie de confiance
  - Concepts
  - Besoins utilisateur
- Services nécessaires
- Architectures de messagerie
  - Type Internet
  - De confiance
- Services intégrés dans le projet TrustedBird
- XIMF
- Entêtes sécurisés
- Démonstration du client TrustedBird

Services nécessaires

- J'envoie un message enrichi
  - à une personne de confiance,
  - avec un niveau de sensibilité du contenu,
  - en accord avec la loi et les réglementations,
  - quand je le souhaite.
- J'exige
  - qu'il ne puisse être éventuellement lu par personne d'autre,
  - ni même modifié,
  - qu'il parvienne à destination dans un délai demandé,
  - être informé des évènements associés à cet échange
- Le destinataire et moi-même ne pouvons nier cet échange

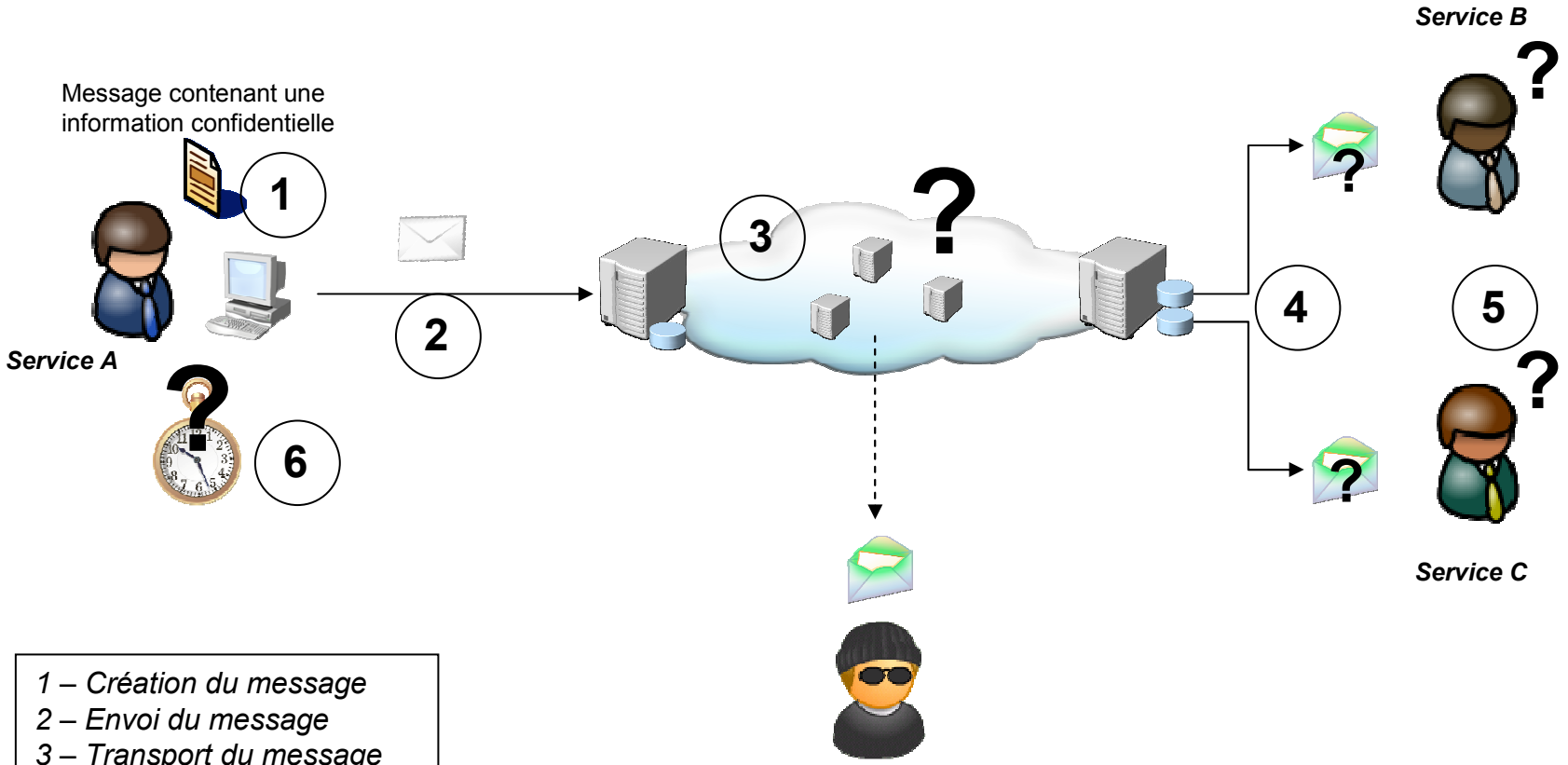
Services nécessaires

- J'envoie un message enrichi:
  - à une personne de confiance,
  - avec un niveau de sensibilité du contenu,
  - en accord avec la loi et les réglementations,
  - quand je le souhaite.
- J'exige
  - qu'il ne puisse être éventuellement lu par personne d'autre,
  - ni même modifié,
  - qu'il parvienne à destination dans un délai demandé,
  - être informé des évènements associés à cet échange
- Le destinataire et moi-même ne pouvons nier cet échange

Plan

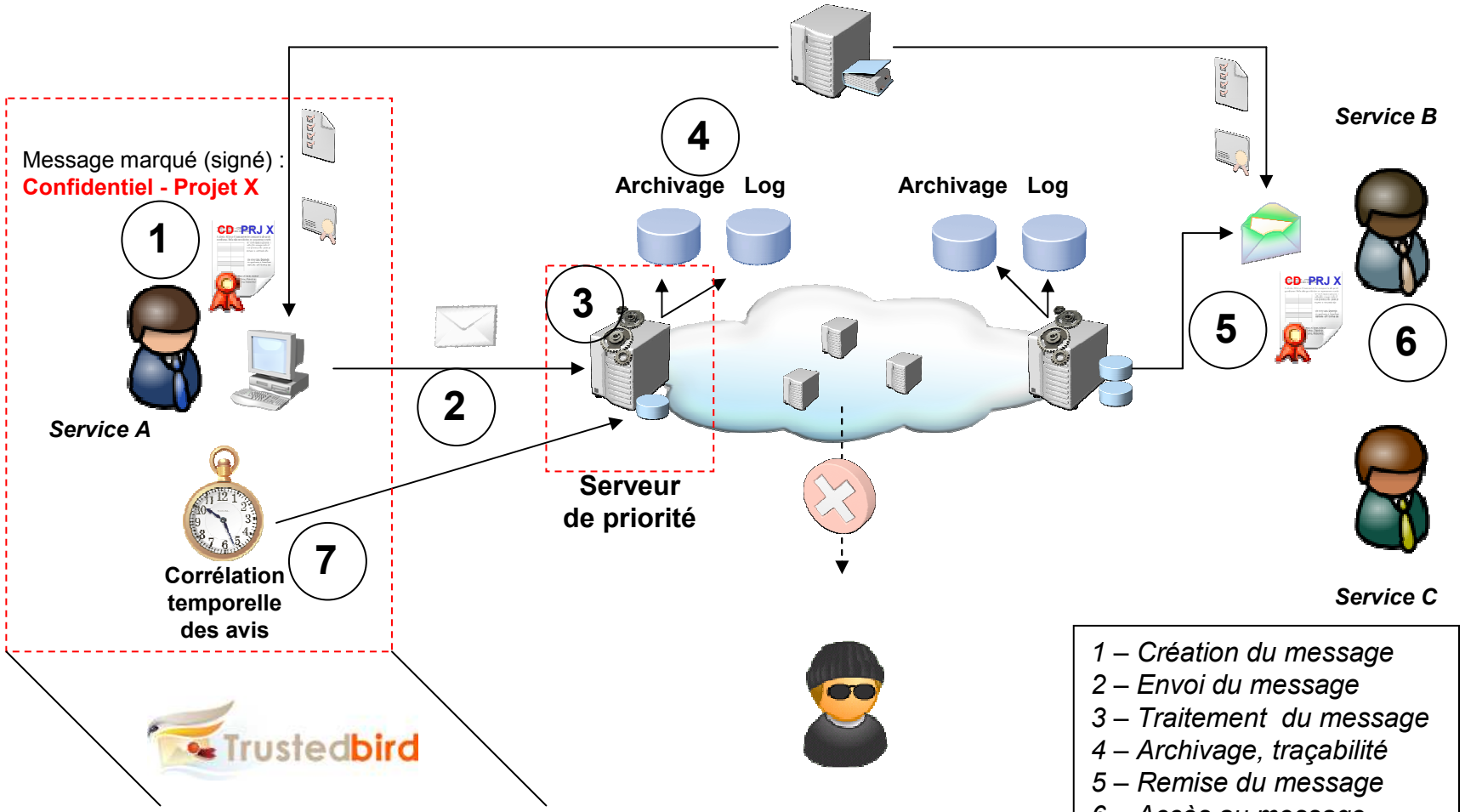
- Messagerie de confiance
  - Concepts
  - Besoins utilisateur
- Services nécessaires
- Architectures de messagerie
  - Type Internet
  - De confiance
- Services intégrés dans le projet TrustedBird
- XIMF
- Entêtes sécurisés
- Démonstration du client TrustedBird

Architecture de messagerie type Internet



1 – Création du message
2 – Envoi du message
3 – Transport du message
4 – Remise du message
5 – Accès au message
6 – Suivi des envois

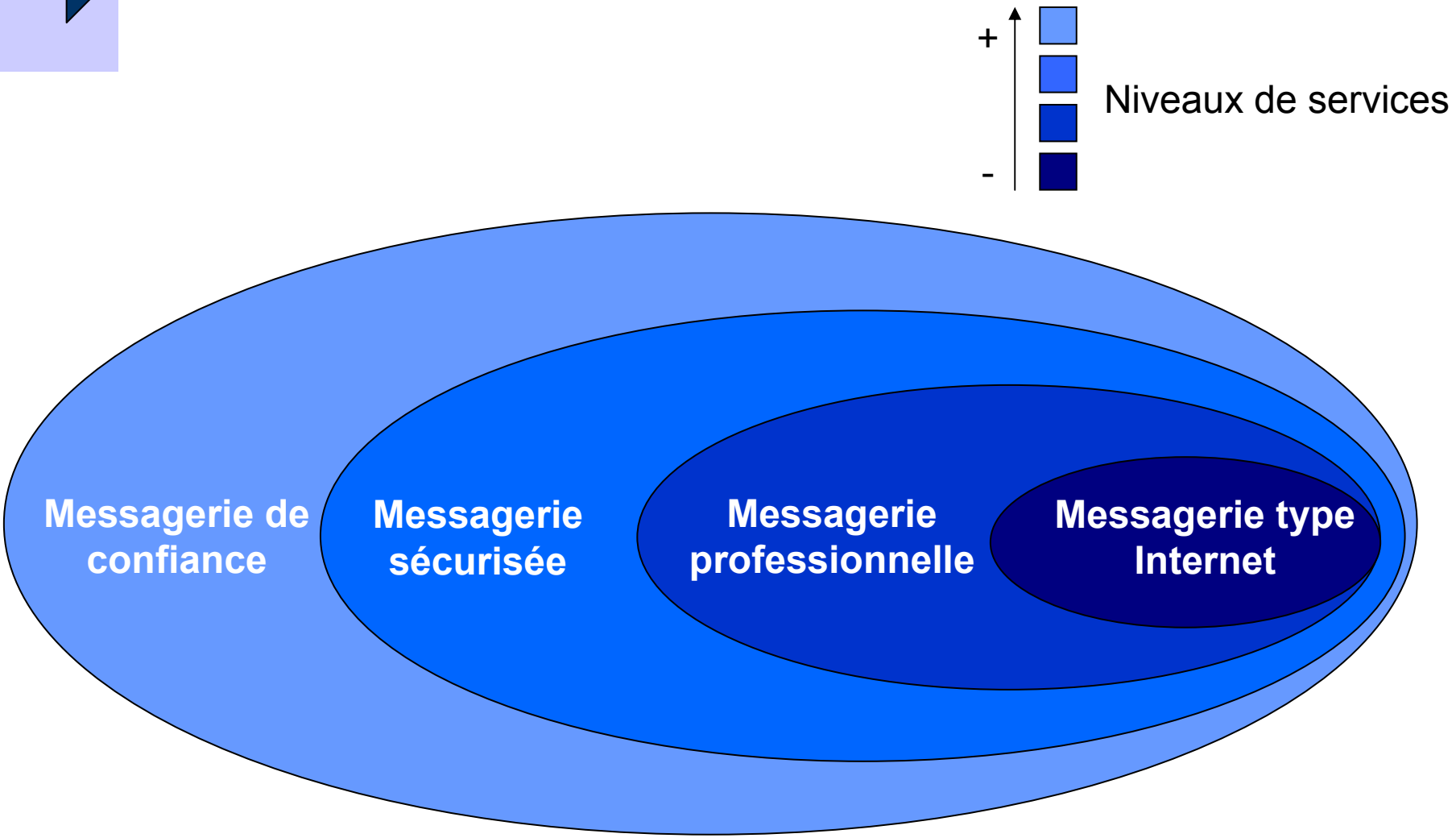
Architecture de messagerie de confiance



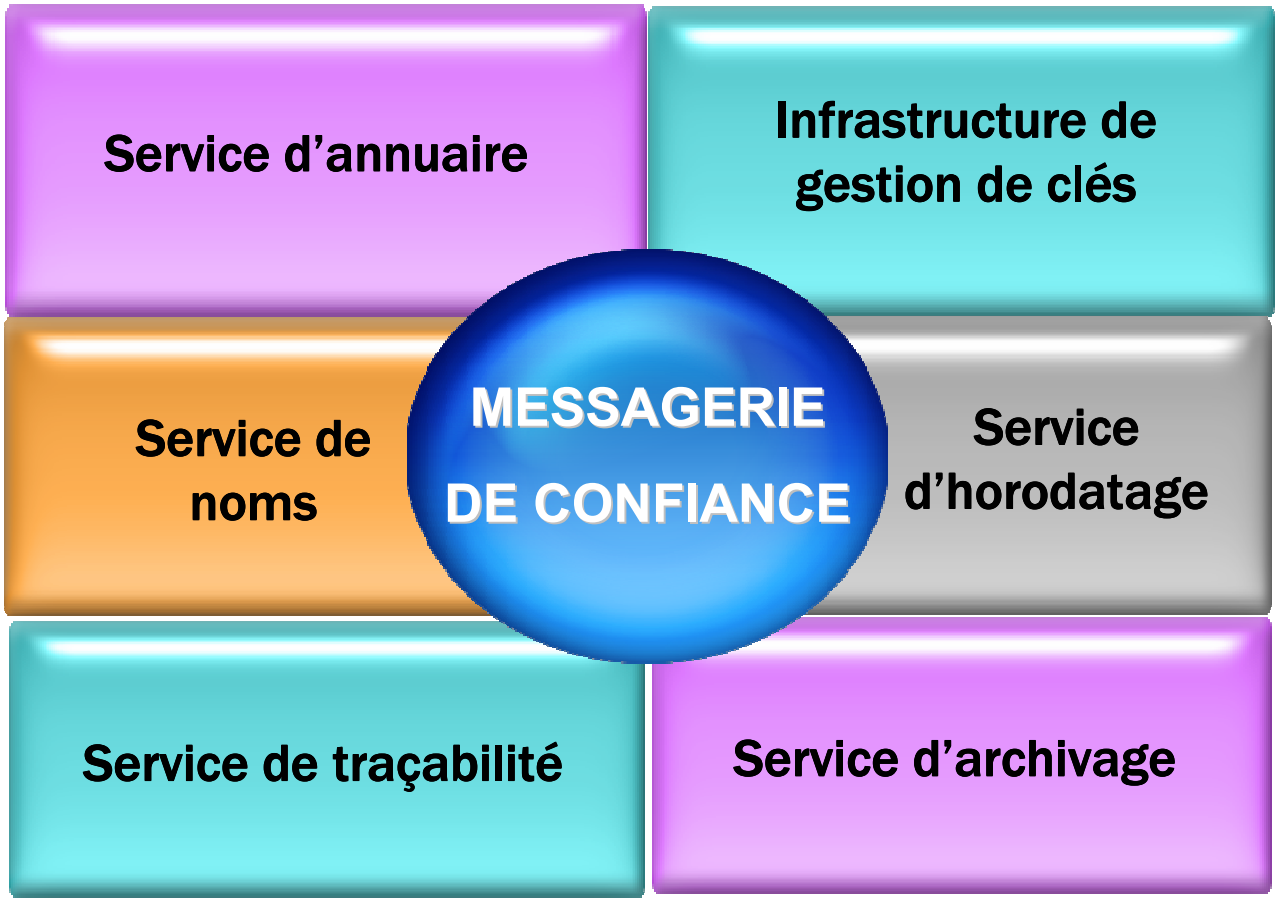
Architecture de messagerie de confiance

- Maitrise de l'architecture
- Implémentation de protocoles standards et pérennes : RFC IETF
- Intégration des services et choix des protocoles en fonction des menaces
  - Chiffrement du contenu vs données
  - Mise en œuvre d'antivirus
  - Mise en œuvre d'anti spam
  - …
- La définition d'une architecture de confiance est affaire de compromis (antivirus vs chiffrement de bout en bout, …)

Périmètres d'architectures de messageries



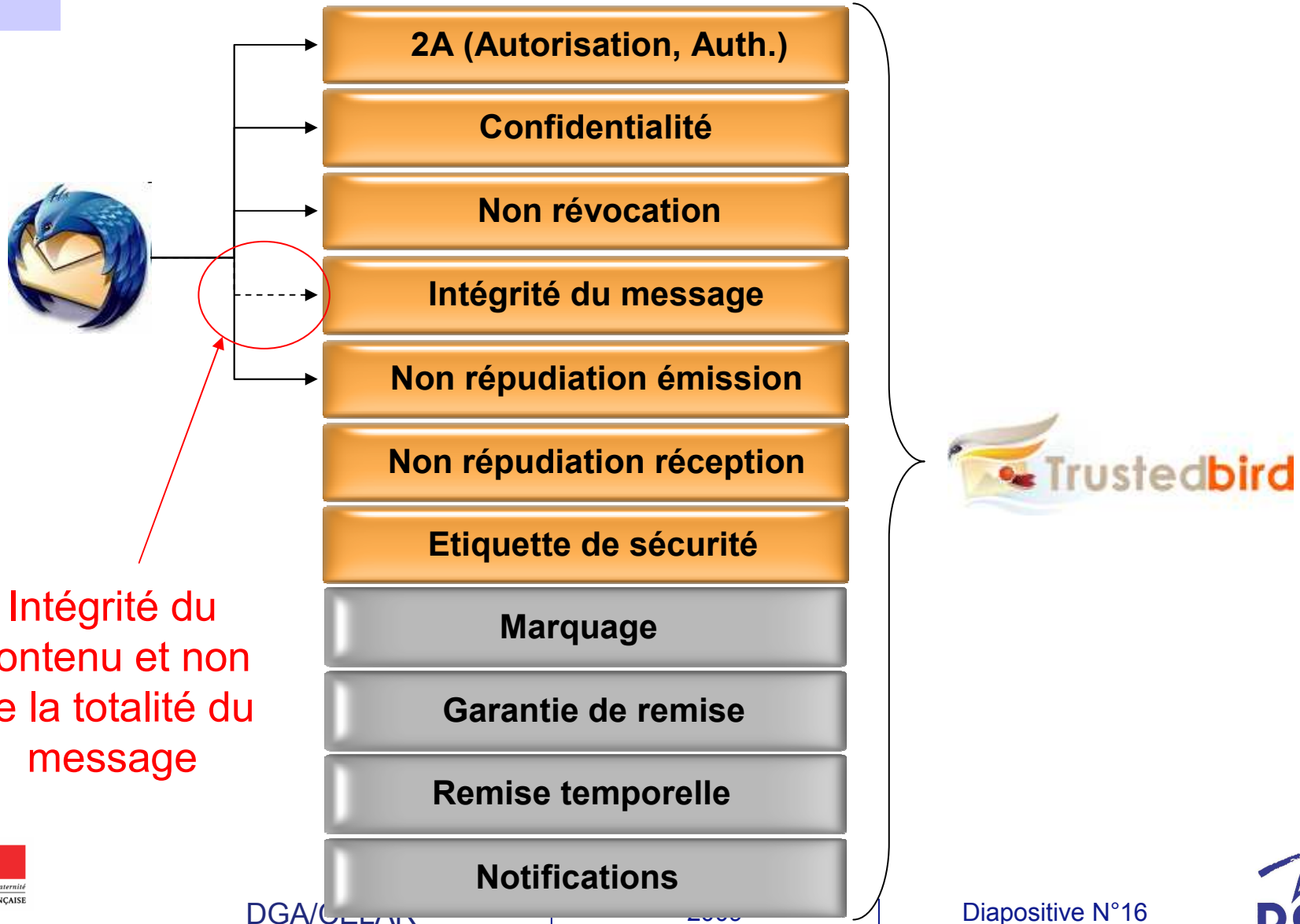
Architecture de messagerie de confiance
Services connexes



Plan

- Messagerie de confiance
  - Concepts
  - Besoins utilisateur
- Services nécessaires
- Architectures de messagerie
  - Type Internet
  - De confiance
- Services intégrés dans le projet TrustedBird
- XIMF
- Entêtes sécurisés
- Démonstration du client TrustedBird

Services intégrés dans TrustedBird

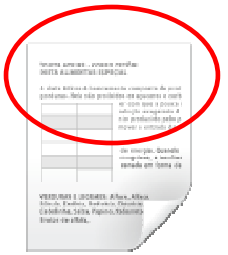


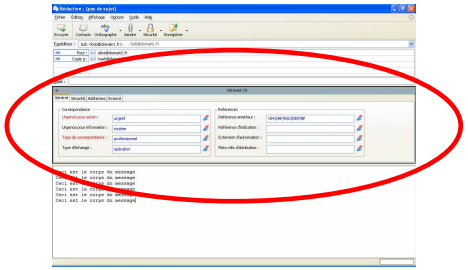
Plan

- Messagerie de confiance
  - Concepts
  - Besoins utilisateur
- Services nécessaires
- Architectures de messagerie
  - Type Internet
  - De confiance
- Services intégrés dans TrustedBird
- XIMF
- Entêtes sécurisés
- Démonstration du client TrustedBird

eXtended IMF (XIMF)

- IMF (RFC 5322) est le format par défaut des messages électroniques
- XIMF permet d'étendre IMF en ajoutant des entêtes (noms et valeurs) : service de marquage
- Technologie basée sur XML
- Instance XIMF (multiples)
  - Définition des noms et valeurs
  - Définition des règles d'association entre les champs
  - Définition du formulaire personnalisé
  - …
- Moteur XIMF (unique)
  - Interprétation de l'instance à l'aide de schéma XML
  - Mise en œuvre de l'instance

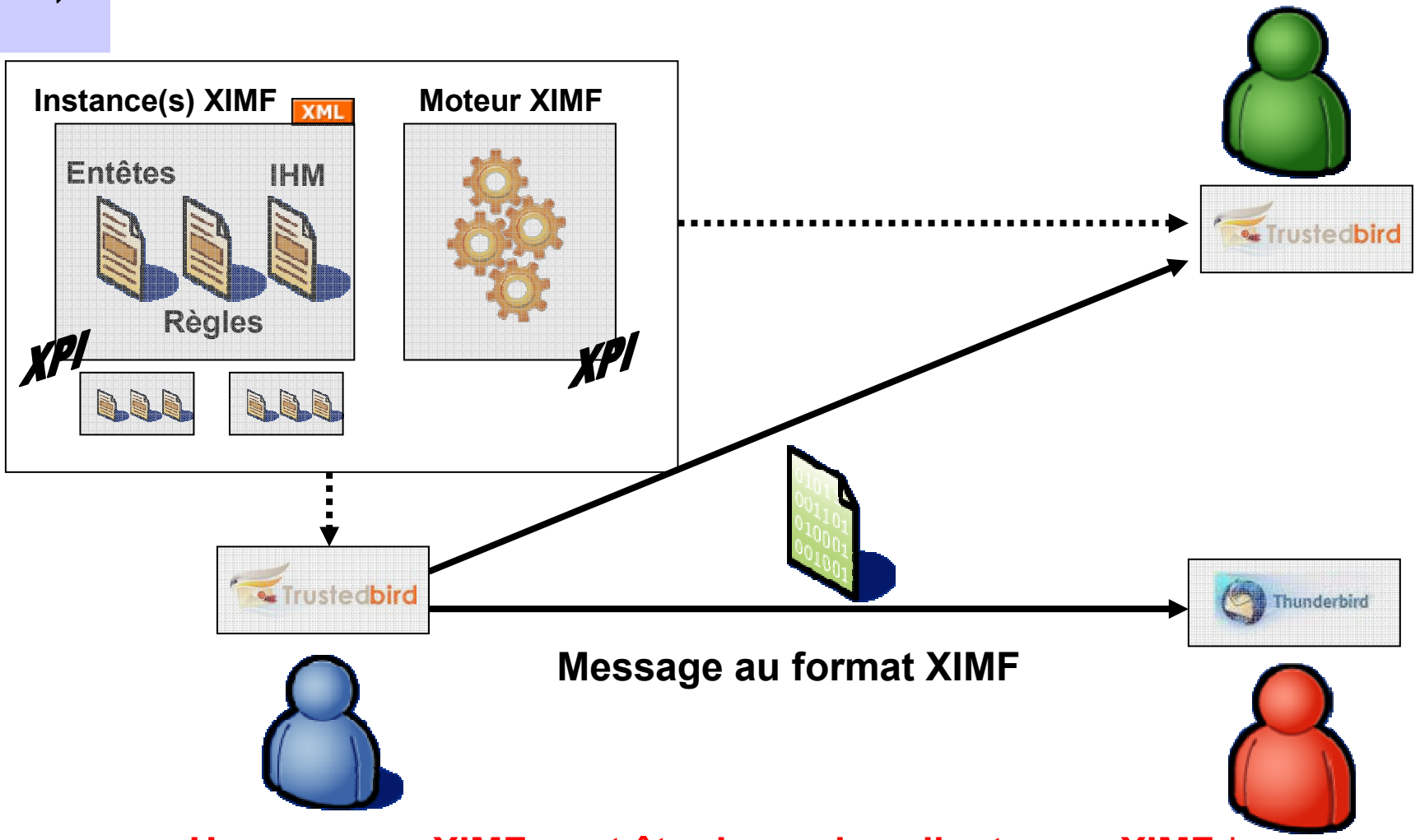




eXtended IMF (XIMF)

- Travaux CELAR
- Exemple de personnalisation d'un message
  - Type de correspondance 
    - Personnelle, professionnelle, officielle
  - Urgence du message
  - Mots clés d'attribution (projet, affaire, …)
    - de distribution automatique
  - Entêtes d'archivage
  - …
- **<u>Chaque organisation ou entreprise peut personnaliser son client de messagerie</u>**

eXtended IMF (XIMF)



➡ **Un message XIMF peut être lu par les clients non XIMF ***

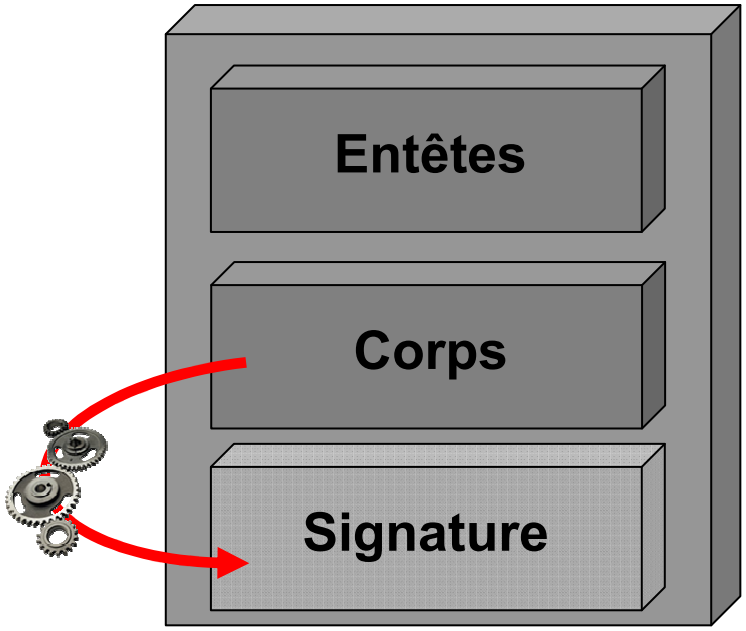
➡ **Le client peut intégrer plusieurs instances**

Plan

- Messagerie de confiance
  - Concepts
  - Besoins utilisateur
- Services nécessaires
- Architectures de messagerie
  - Type Internet
  - De confiance
- Services intégrés dans TrustedBird
- XIMF
- Entêtes sécurisés
- Démonstration du client TrustedBird

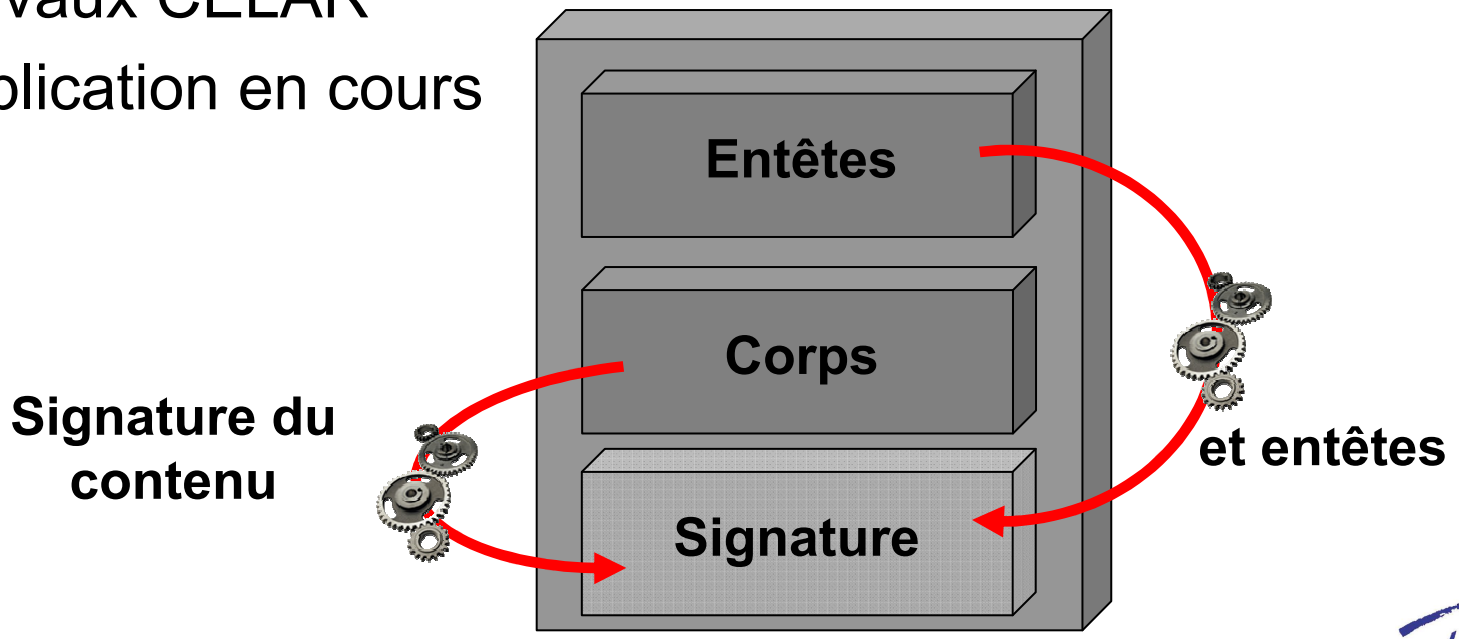
Besoin d'entêtes sécurisés

- Par défaut, une signature ne sécurise que le contenu du message et non les entêtes
- Les entêtes Sujet, XIMF, Date… peuvent être modifiés sans contrôle possible par le destinataire



Mise en œuvre d'entêtes sécurisés

- Intégration des entêtes à sécuriser dans la signature (attributs signés SMIME)
- Interopérabilité avec les clients standards, ce qui permet une migration évolutive
- Travaux CELAR
- Publication en cours



Demo