La sécurité, problème majeur pour les plates-formes de diffusion de flux multimédia adaptables

Ahmed Reda KACED, Jean Claude MOISSINAC
{kaced,moissinac@enst.fr}
Équipe ASTRE
Département InfRes
GET – ENST – CNRS UMR 5141

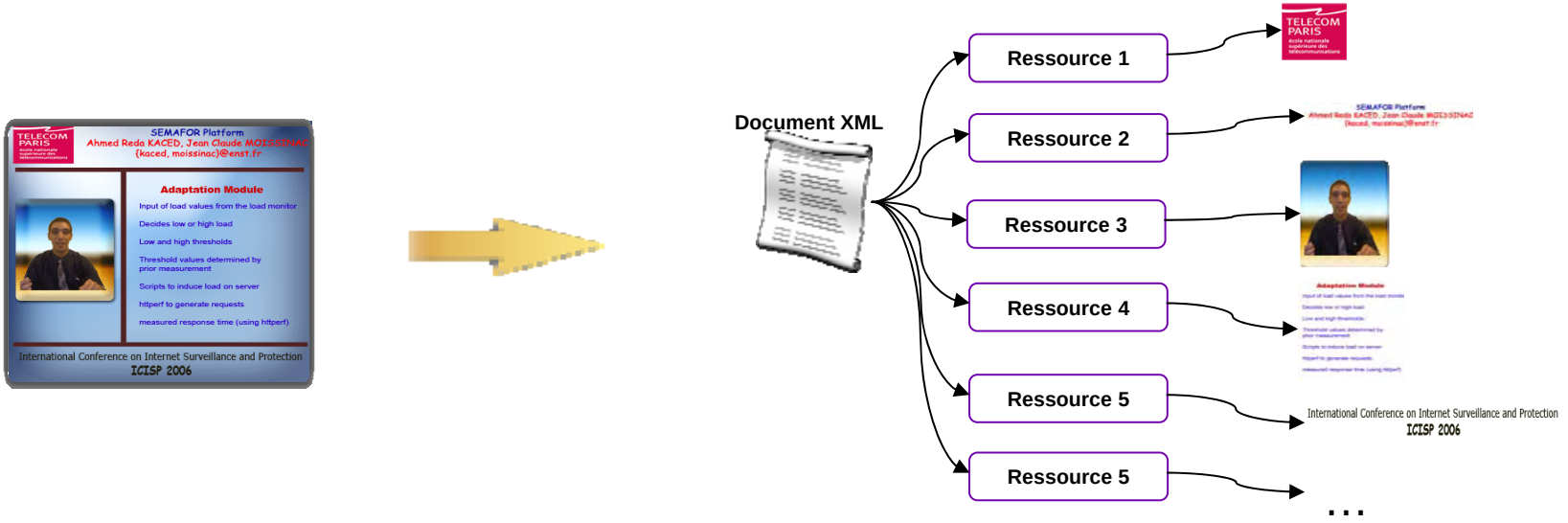
Symposium sur la Sécurité des Technologies de l'Information et des Communications 2006
31 mai - 2 juin 2006

Agenda

- **Introduction**
- **Contexte et problématiques**
- **Analyse des risques**
- **Solutions possibles**
- **Plateforme de diffusion proposée**
- **Conclusion**

Introduction

- **Document Multimédia**
  - Impliquant à la fois données, images, audio et vidéo
  - Format :
    - Meta-data + Contenu média (SMIL, SVG, etc.)
    - Un fichier binaire (AVI, MPEG, etc.)
- **Document Multimédia adaptable**
  - Autorisant des opérations d'adaptation permettant la restitution du contenu sur un ensemble de terminaux différents



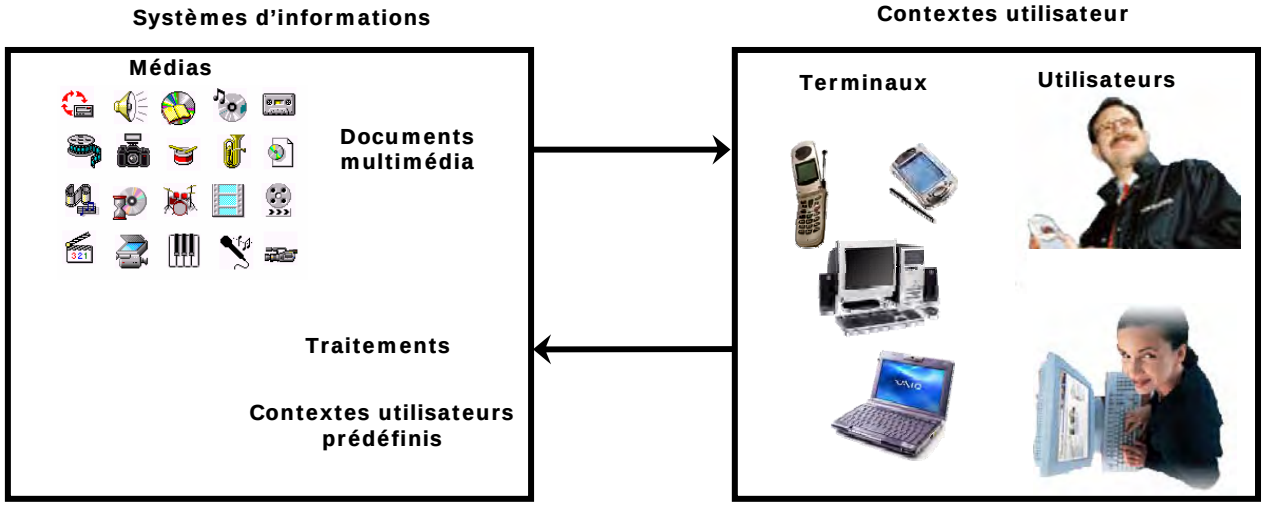
Système multimédia adaptable

Fonction principale

Restituer de l'information regroupée dans un système d'informations, tout en satisfaisant aux besoins et aux contraintes définis par le contexte de l'utilisateur

Contexte utilisateur

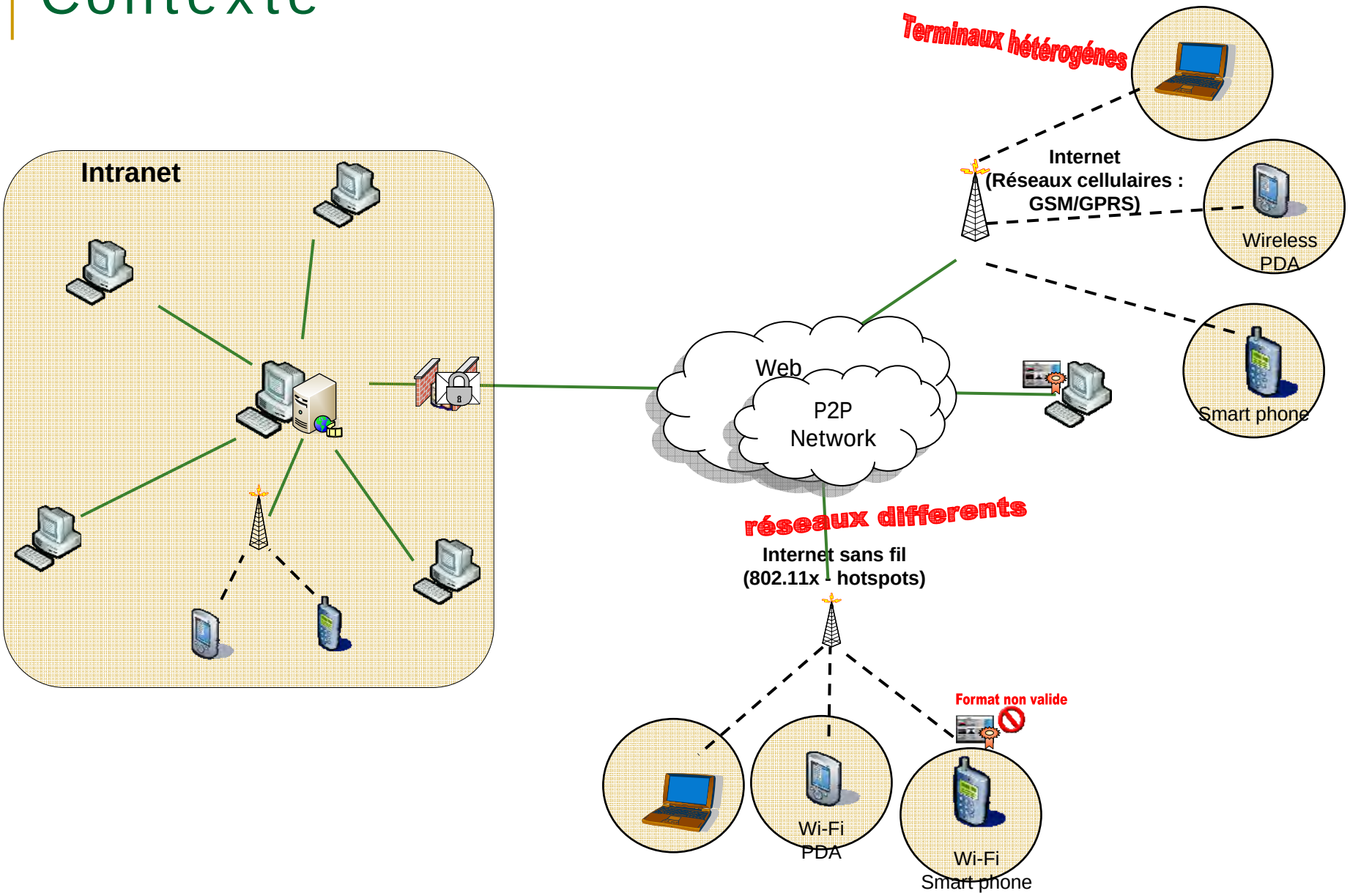
- **le terminal d'accès**
- **l'utilisateur**



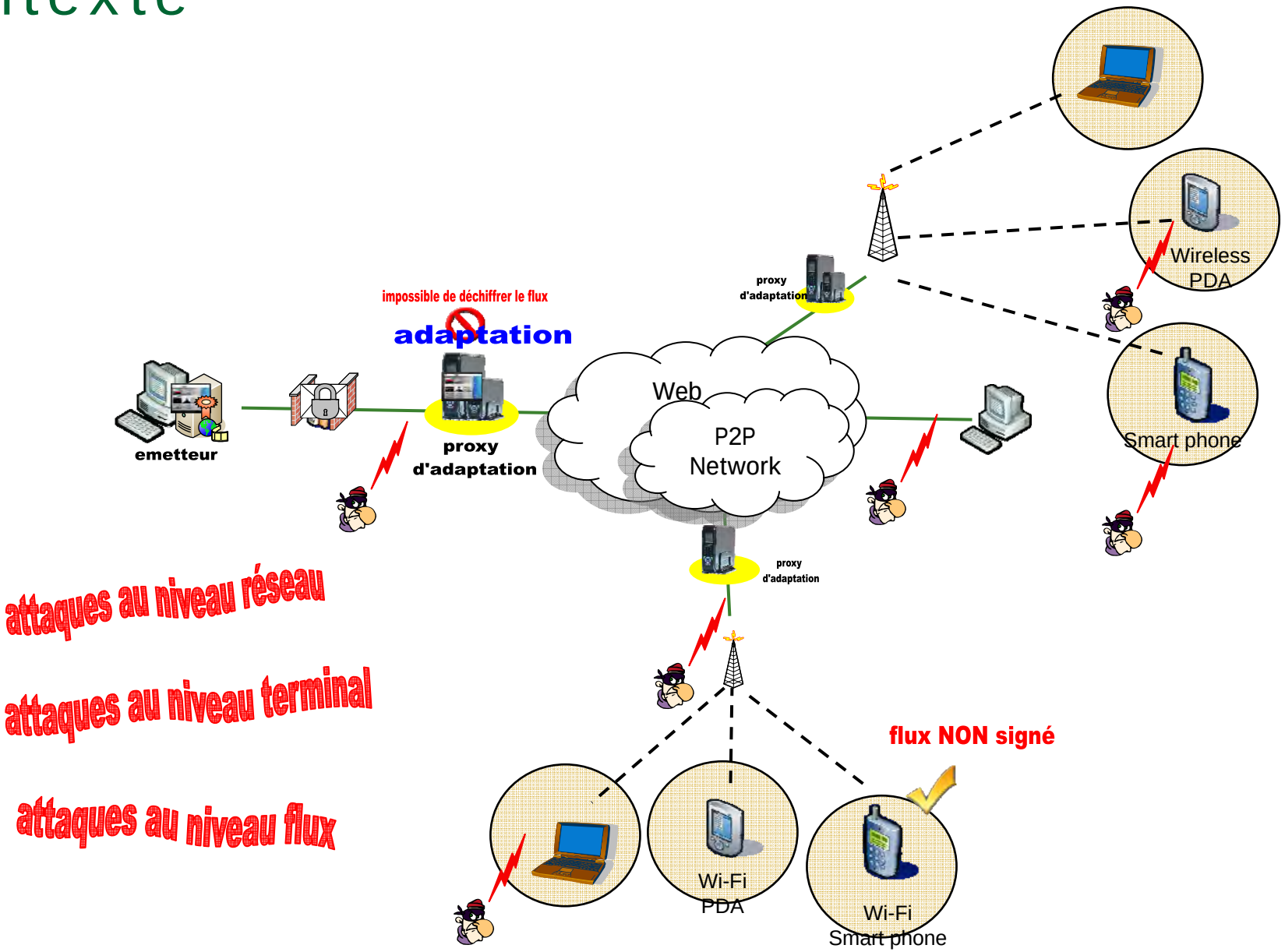
Contraintes

Diversité à de multiples niveaux : physique, culturel, intellectuel ou encore émotionnel.

Contexte


Terminaux hétérogénes
Internet
(Réseaux cellulaires :
GSM/GPRS)
Wireless
PDA
Intranet
Web
P2P
Network
Smart phone
réseaux differents
Internet sans fil
(802.11x - hotspots)
Format non valide
Wi-Fi
PDA
Wi-Fi
Smart phone

Contexte


impossible de déchiffrer le flux
adaptation
emetteur
proxy
d'adaptation
Web
P2P
Network
proxy
d'adaptation
proxy
d'adaptation
Wireless
PDA
Smart phone
attaques au niveau réseau
attaques au niveau terminal
attaques au niveau flux
flux NON signé
Wi-Fi
PDA
Wi-Fi
Smart phone

Problématiques

les contenus doivent autoriser les opérateurs d'adaptation à effectuer les changements nécessaires sur le document avant la diffusion

Comment garantir l'authenticité du document multimédia de bout en bout malgré l'adaptation?

Comment assurer l'intégrité des données du document multimédia?

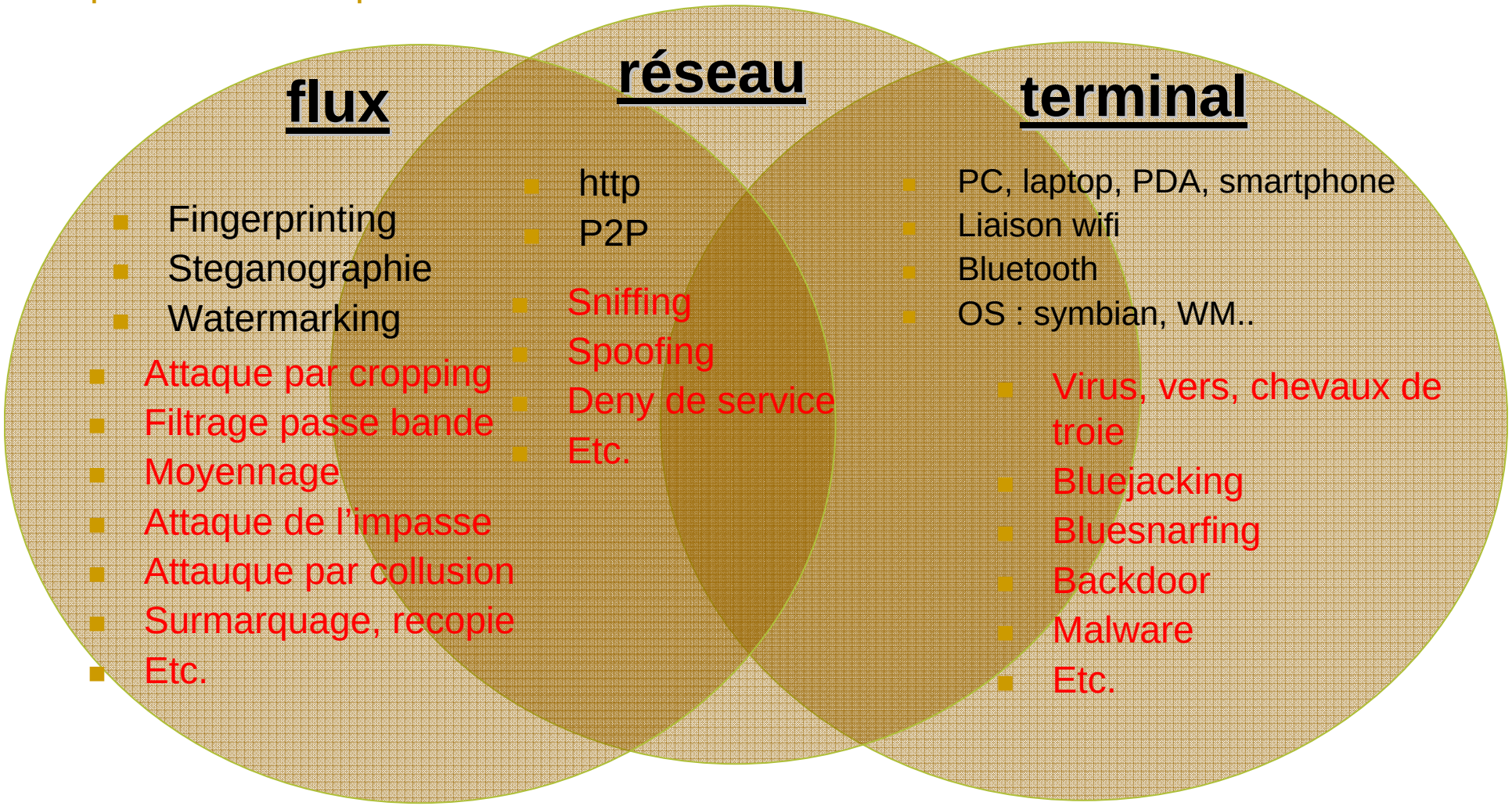
Comment obtenir la non-répudiation du document ?

Peut on utiliser un schéma de protection classique ?

Intégrité des données + Contrôle d'accès + Confidentialité + Identiefication + Non-répudiation !!

Analyse des risques

plusieurs défis pour un seul but …



Solutions possibles

plusieurs défis pour un seul but …

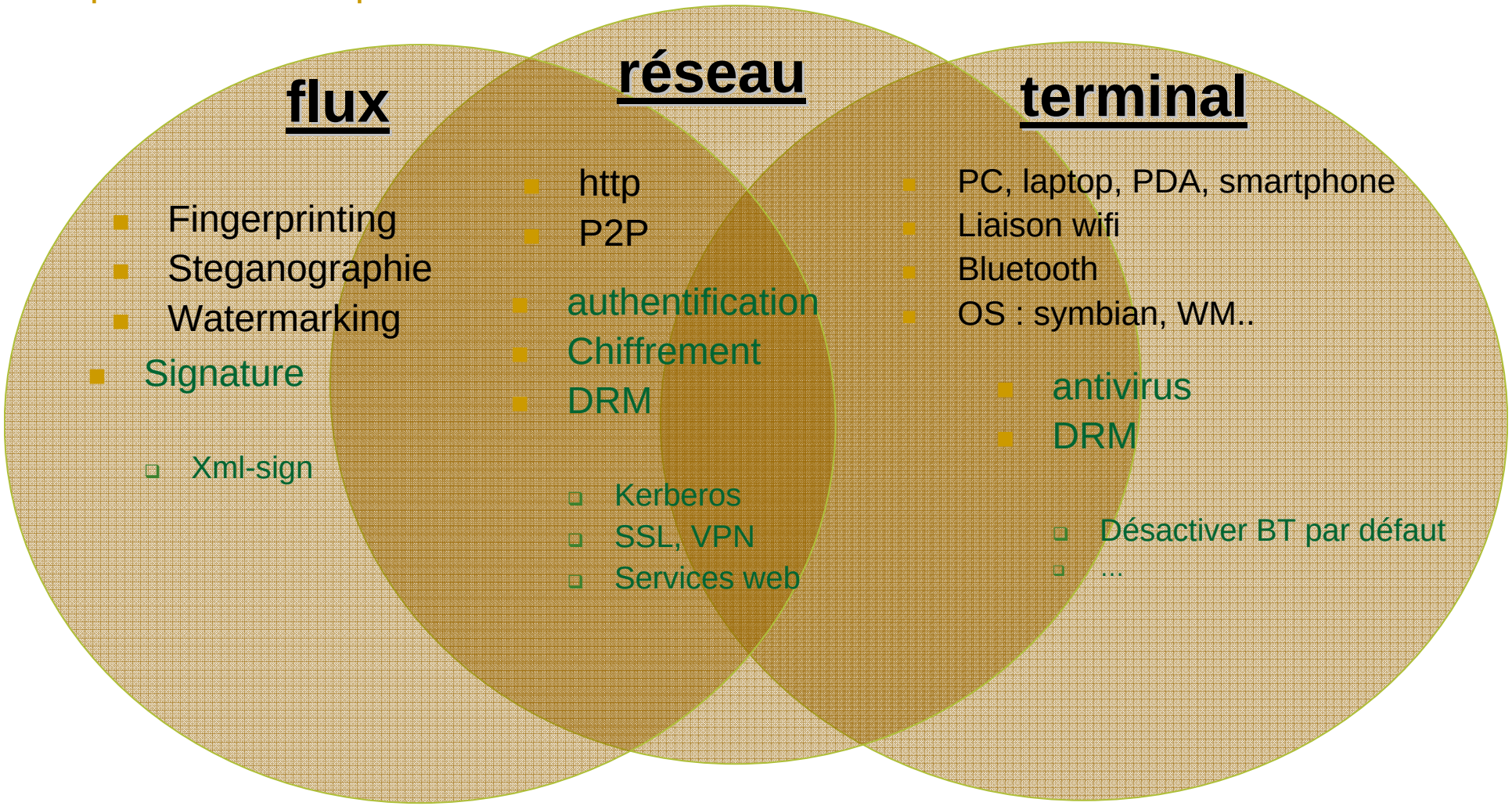
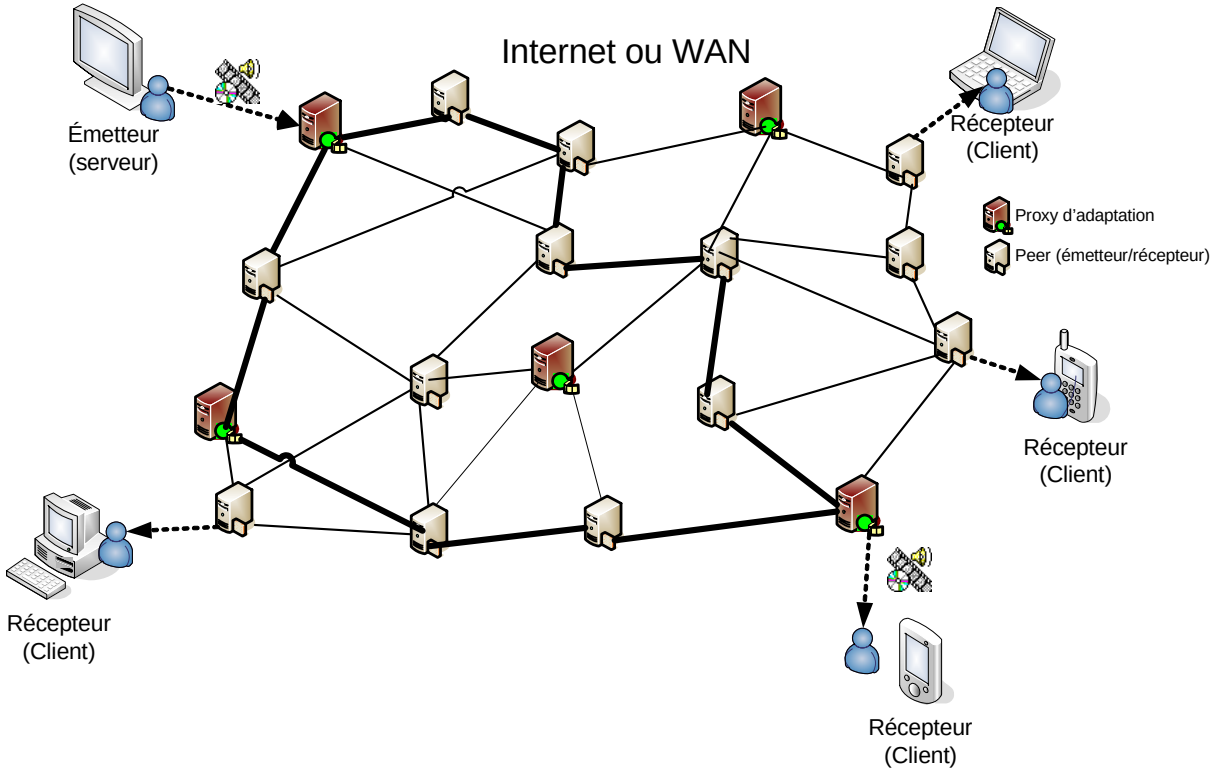


Plate-forme proposée



SEMAFOR

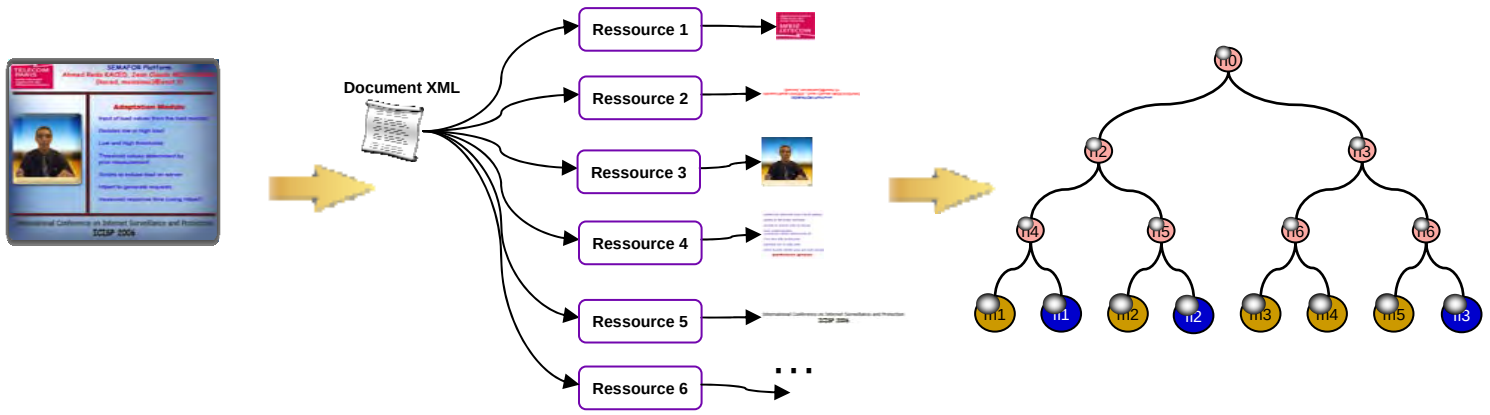
AMCA + XSST

Schéma de signature de documents multimédia

AMCA (Adaptive Multimedia Content Authentication)

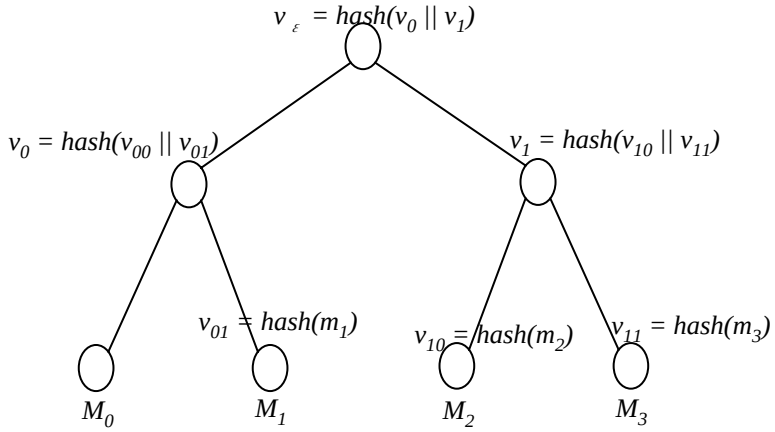
- Permet à un ou plusieurs proxies d'adaptation de modifier dynamiquement un document multimédia en supprimant ou insérant des éléments dans ce dernier, tout en préservant la capacité du client à vérifier la signature originale.

- Utilise la technique de *Merkle Hash Tree* (MHT)
  - Représenter le document sous forme d'un arbre binaire,
  - Chaque média composant ce flux sera représenté par une feuille de l'arbre,
  - Des feuilles spéciales appelées ***FreeLeaves*** lui sont ajoutées, Ces dernières permettront l'insertion de nouveaux médias ou de médias adaptés.



Arbres de Merkle

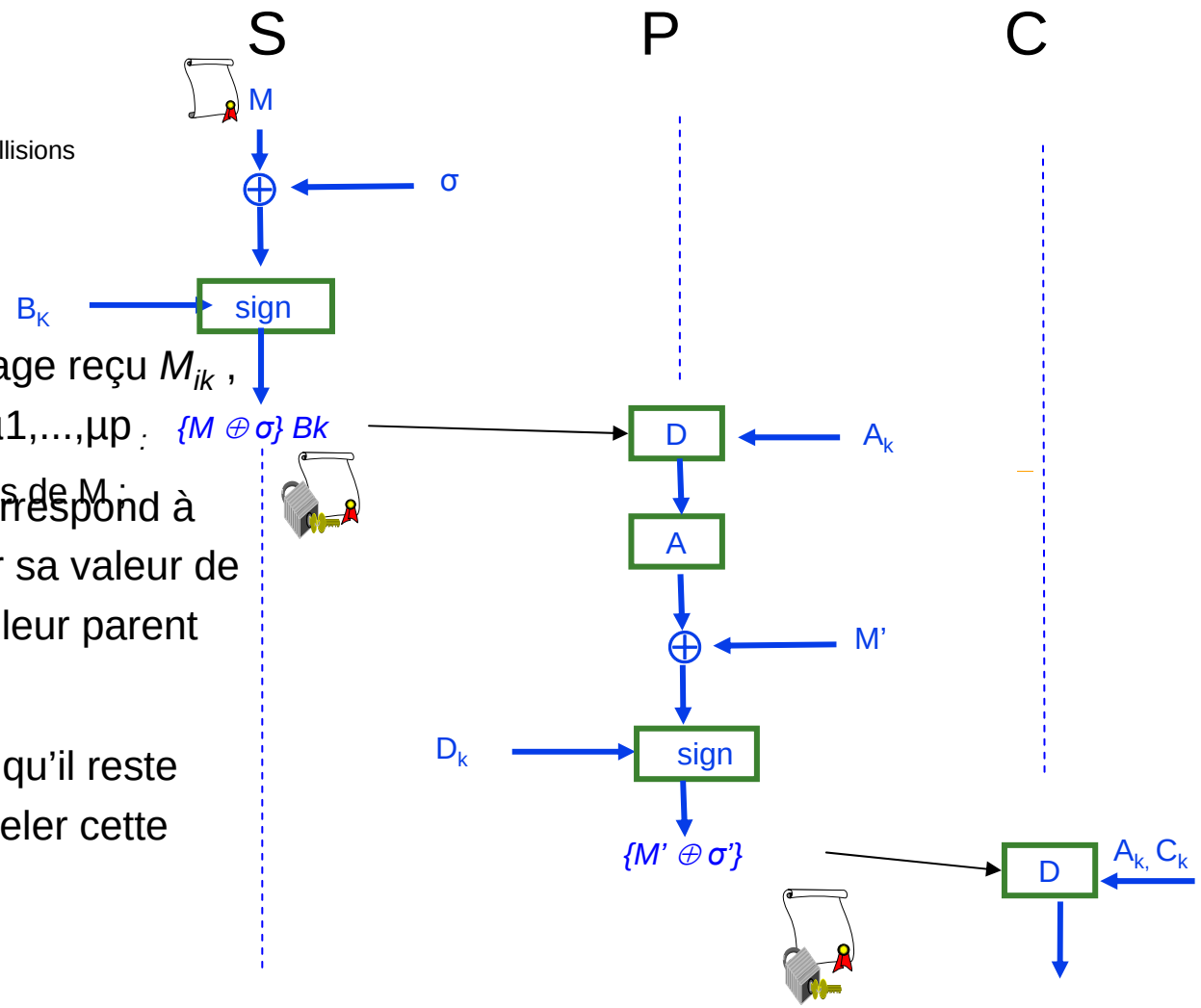
- un arbre binaire complet
- équipé d'une fonction de hachage H et d'une application Ω, qui relie l'ensemble des nœuds à l'ensemble des chaînes de longueur k : n → Ω (n) ∈ $\{0,1\}^k$.
  - $\Omega(n_{parent}) = H(\Omega(n_{gauche}) \| \Omega(n_{droit}))$.



- algorithme
  - $M = M_1M_2M_3M_{4.....}M_n$
  - $V(f_i) = hash(IV, M_i)$ → feuilles
  - $V(v_x) = hash(IV, V(v_{x0}) \| V(v_{x1}))$ → nœuds

Schéma de signature proposé

S (Ak ; Bk) Ak clé publique et Bk clé privée
S (Ck ; Dk)
Sign(Bk;M)
Verif(Ak;M; σ)
hash une fonction de hachage résistante aux collisions
IV vecteur d'initialisation



Vérification

- Pour chaque bloc de message reçu M_{ik} , calculer $v_k = hash(IV, M_{ik})$, μ1,...,μp :
  - σ = Sign(Bk, v_k)
  - *S* envoie à *P* {M ⊕ σ} B_k ;
  - *P* adapte les parties adaptables de M ;
  - *P* calcule : σ' = Sign(Bk, $v_{\varepsilon'}$) ;
  - *P* envoie à C {M' ⊕ σ'}
- Si une paire quelconque correspond à des frères, la remplacer par sa valeur de hachage (qui correspond à leur parent dans l'arbre de Merkle).
- Répéter étape 2 jusqu'à ce qu'il reste seulement une valeur - appeler cette dernière $v\varepsilon'$.
- Lancer Verif(*Ak*, $v\varepsilon'$,σ).

$$v\varepsilon' = v\varepsilon$$

adaptation

Suppression

Soit M' dénotant les données transformées après la suppression des blocs. Après avoir déterminé les données à supprimer, le proxy d'adaptation P exécute l'algorithme qui suit :

- Soit $E = \{ f \mid f$ est une feuille à supprimer$\}$
- S'il existe $u, v \in E$ tels que u, v sont frères dans l'arbre, alors $E = E - \{u,v\} \cup \{w\}$, où w est le parent de u, v.
- Répéter 2 jusqu'à ce que E n'ait aucune paire de frères. Supposons cela à la fin $E = \{wi \mid 1 \leq i \leq p\}$.
- Soit $\mu i = V(wi)$ pour $1 \leq i \leq p$. P transmet M', σ, μi, et la position du nœud de l'arbre pour chaque wi, $1 \leq i \leq p$.

Insertion.

- schéma pour la réalisation des FreeLeaves utilisant des techniques de signatures à clé publique conventionnelles (e.g., RSA)
- S place la clé publique de P (ou les instructions où la chercher) dans le bloc d'une FreeLeaf
- S crée alors un digest de l'arbre de Merkle puis signe comme décrit ci-dessus. P, alternativement, attache son contenu et le signe séparément
- R vérifie la validité des deux signatures

XSST :(*Xml Secure Semafor Transactions*).

Il y a trois grandes parties dans la structure même du message

XSST :

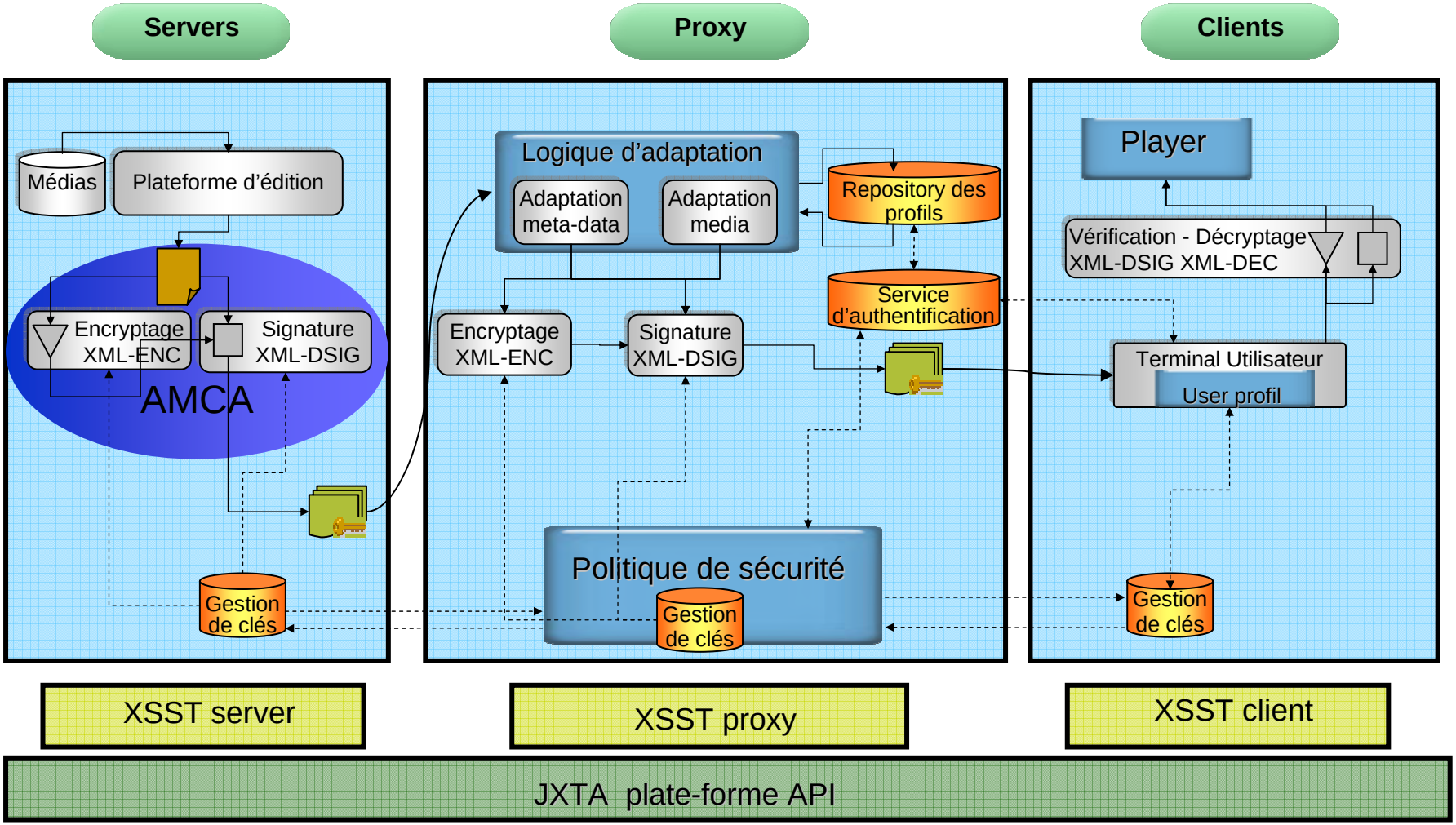
- *Encryption*
- *Data*
- *Signature*

- proxy XSST
- un reverse proxy
- le serveur XSST

```
<XSST xmlns...>
<encryption type="0-2-0-8" id="example" ...>
...
<data type=.../>
...
</data>
<signature type="1-4-1" id="example" ...>
...
</signature>
</XSST>
```

Plate-forme proposée

SEMAFOR (SEcure Multimedia Adaptation platFORm)



Exemple

```
<?xml version="1.0"?>
<smil>
<head/>
  <body>
    <seq>
      <par>
        <video src="rtsp://server/video1.rm"/>
        <video src="rtsp://server/music1.rm"/>
      </par>
      <par>
        <video flid="1"/>
      </par>
    </seq>
  </body>
</smil>
```

(Avant)

```
<?xml version="1.0"?>
<DocumentRoot>
  <Policy/>
  <smil/>
  <Signature>
    <SignedInfo>
      <CanonicalizationMethod/>
      <SignatureMethod/>
      <Reference URI=/DocumentRoot/Policy />
      <Reference URI=/DocumentRoot/smil/head />
      <Reference URI=/DocumentRoot/smil/body>
        <DigestMethod Algorithm="HTreeConst"/>
        <DigestValue> root_node_of_h_tree </DigestValue>
      </Reference>
      <TrapdoorHMethod Algorithm="Discrete Log" flid="1">
        <PublicValue> public_values_of_trapdoor_h
        </PublicValue>
        <TrapdoorHValue> trapdoor_h_value</TrapdoorHValue>
      </TrapdoorHMethod>
    </SignedInfo>
      <SignatureValue> Signature </SignatureValue>
  </Signature>
</DocumentRoot>
```

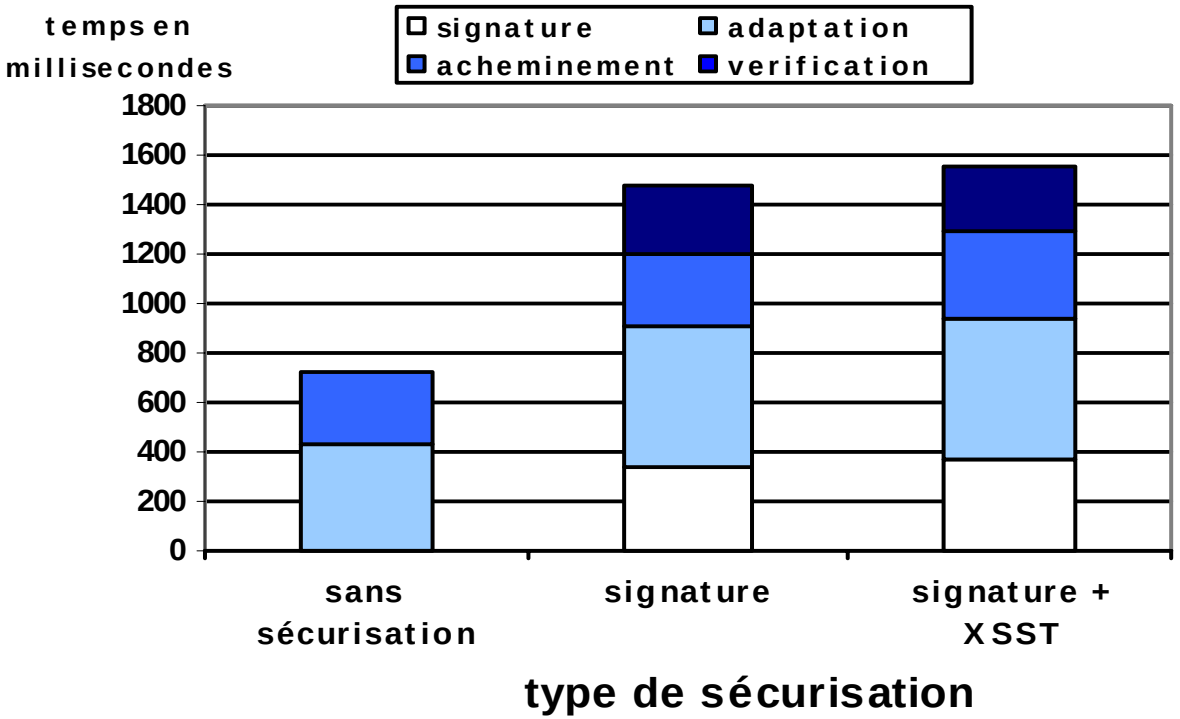
(Après)

Sécurité dans les flux XML

- XML Digital Signatures (XMLDSIG)
  - Basé sur XML (implantation grâce à la même boîte à outils utilisée par la famille des technologies XML)
  - Signatures sur des portions de documents
    - le document peut être recomposé par le récepteur
  - Signatures par plusieurs signataires
    - possibilité de ventiler les opérations d'adaptation sur plusieurs proxies
  - Signature apposée sur plusieurs objets média distincts
- XML Encryption (XMLENC)
  - Pour crypter des données qui peuvent être :
    - Des données arbitraires (y compris un document XML)
    - Un élément XML
    - Le contenu d'un élément XML
  - Très utile lorsque différentes parties du même document ont besoin d'un traitement différent
- XML Canonicalization
- XML Key Management
- Trust Extensions

Performances

- proxy : processeur Intel Pentium 4 2,7 GHz avec 1 giga de RAM sous Linux Fedora 2.6.30 ;
- le serveur : processeur Intel Centrino, 1.7 GHz avec 512 méga de RAM sous Linux Fedora 2.6.09 ;
- client : laptot de processeur Intel pentium 2, une RAM de 128 avec des capacités d'affichage réduites.



Conclusion

- Étude globale sur les risques liés à une infrastructure de diffusion de flux multimédia adaptable
- Proposition d'une plateforme d'adaptation de flux multimédia
- Proposition d'un schéma de sécurisation des flux adaptables sur cette plateforme
- Mise en œuvre d'un utilisant les standards XML-signature et XML-Encryption
- Perspectives
  - Optimiser les opérations de cryptage/décryptage
  - Portage sur d'autres formats standards de multimédia
  - Etc.

Questions