Les Architectures Orientées Services

SOA

Gérer la sécurité dans SOA et les Services Web

Plan

1. Les Services Web
2. La Pile Services Web
3. La Sécurité dans les Services Web
4. WS-Security
5. XML Encryption, XML Signature, SAML, fédération

Les Services Web

- Les Web Services sont une technologie très pertinente pour mener une démarche SOA.

- Les services web sont basés sur les protocoles et les langages du Web:
  - HTTP, XML, TCP/IP pour la couche réseau
  - Ne nécessite pas une configuration réseau particulière

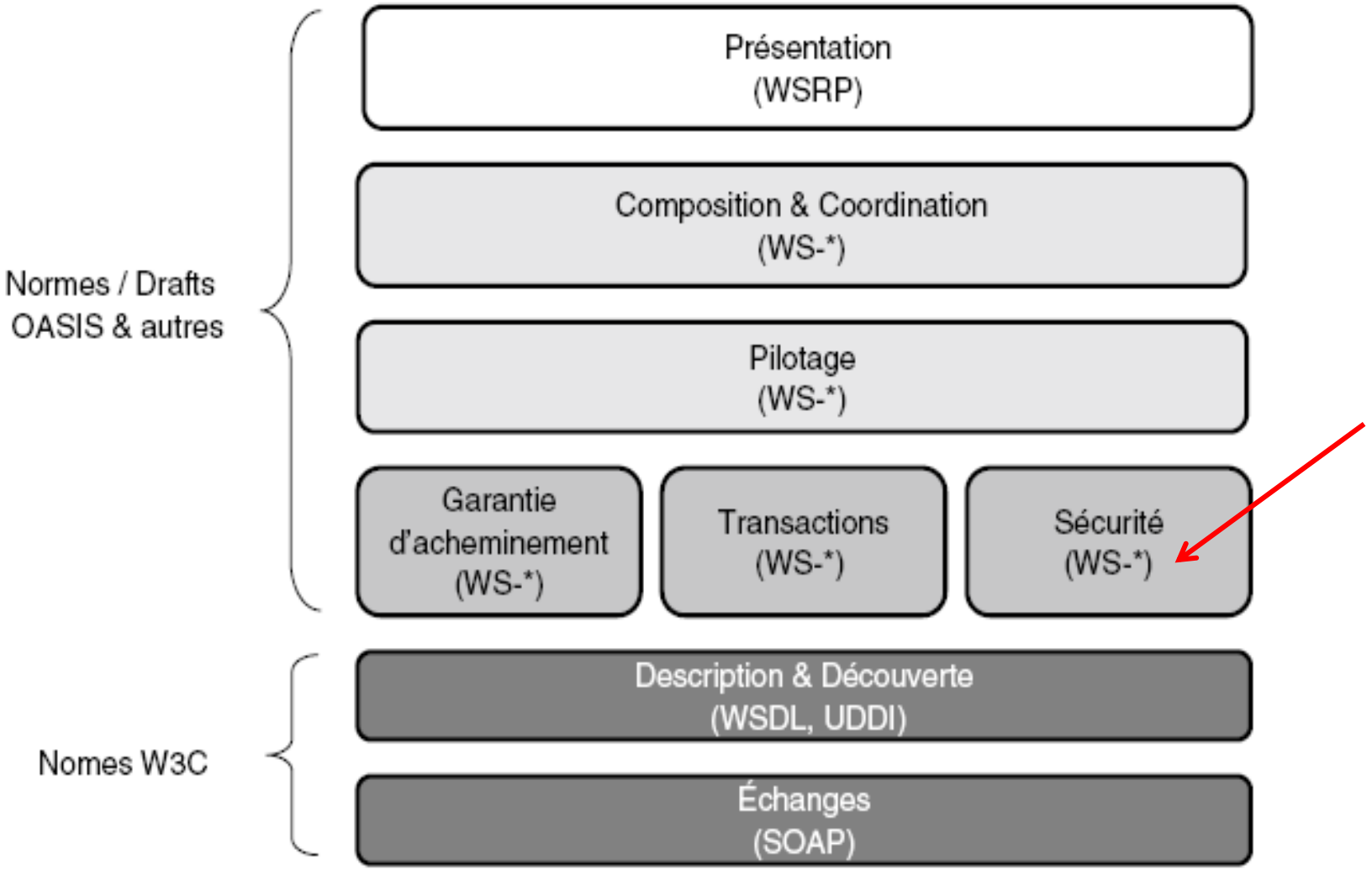
- Les services web sont auto-suffisants puisqu'ils contiennent toutes les informations à leurs utilisations.
  - Chercher, publier , et consommer.
  - Annuaire, contrat de fonctionnement, et un client pour les consommer.

- Les services web sont modulaires:
  - Une application doit être décomposée en un ensemble de services.
  - Utilisation d'une orchestration.

La pile Services Web

- La pile des grammaires Services Web regroupe 5 couches :
  - Les normes fondamentales pour la mise en œuvre des Web Services (SOAP, WSDL, UDDI).
  - Les spécifications qui répondent aux exigences de **sécurité**, de garantie d'acheminement et d'intégrité transactionnelle.
  - Les spécifications qui permettent le pilotage et la supervision des services.
  - Les spécifications permettant la coordination ou la composition des services.
  - Les spécifications qui permettent la présentation des services.

La pile Services Web



La Sécurité dans les Services Web

- Une architecture SOA doit répondre aux problématiques de sécurité:
  - Comment s'assurer de l'identité du fournisseur ou du consommateur du Service ?
  - Comment définir et exposer les droits d'accès à un Service ?
  - Comment assurer la confidentialité des échanges ?
  - Comment assurer la conservation des messages lors d'un échange sensible mettant en jeu plusieurs partenaires ?
  - Etc.

CONFIDENTIALITY

La Sécurité dans les Services Web

- La sécurité est au cœur des préoccupations de l'entreprise garantissant la cohérence et la pérennité de ses systèmes.

- Comment rendre l'information facilement accessible à un tiers tout en garantissant sa consommation que par des tiers habilités à y accéder et à la manipuler ?

- Sécurisation des Web Services possible via les **approches traditionnelles** remplissant fonctions nécessaires de :

  - Authentification
  - Habilitation/Disponibilité
  - Intégrité/Signature
  - Traçabilité
  - Confidentialité/Chiffrement

La Sécurité dans les Services Web

- Sécurisation des Web Services possible via les approches traditionnelles remplissant fonctions nécessaires de :

- Authentification: elle consiste à s'assurer de l'identité d'un utilisateur avant de lui donner l'accès à un système ou à une application.

- Disponibilité : elle concerne la garantie sur le bon fonctionnement d'une application, sa résistance vis-à-vis des pannes accidentelles et des attaques incapacitantes.

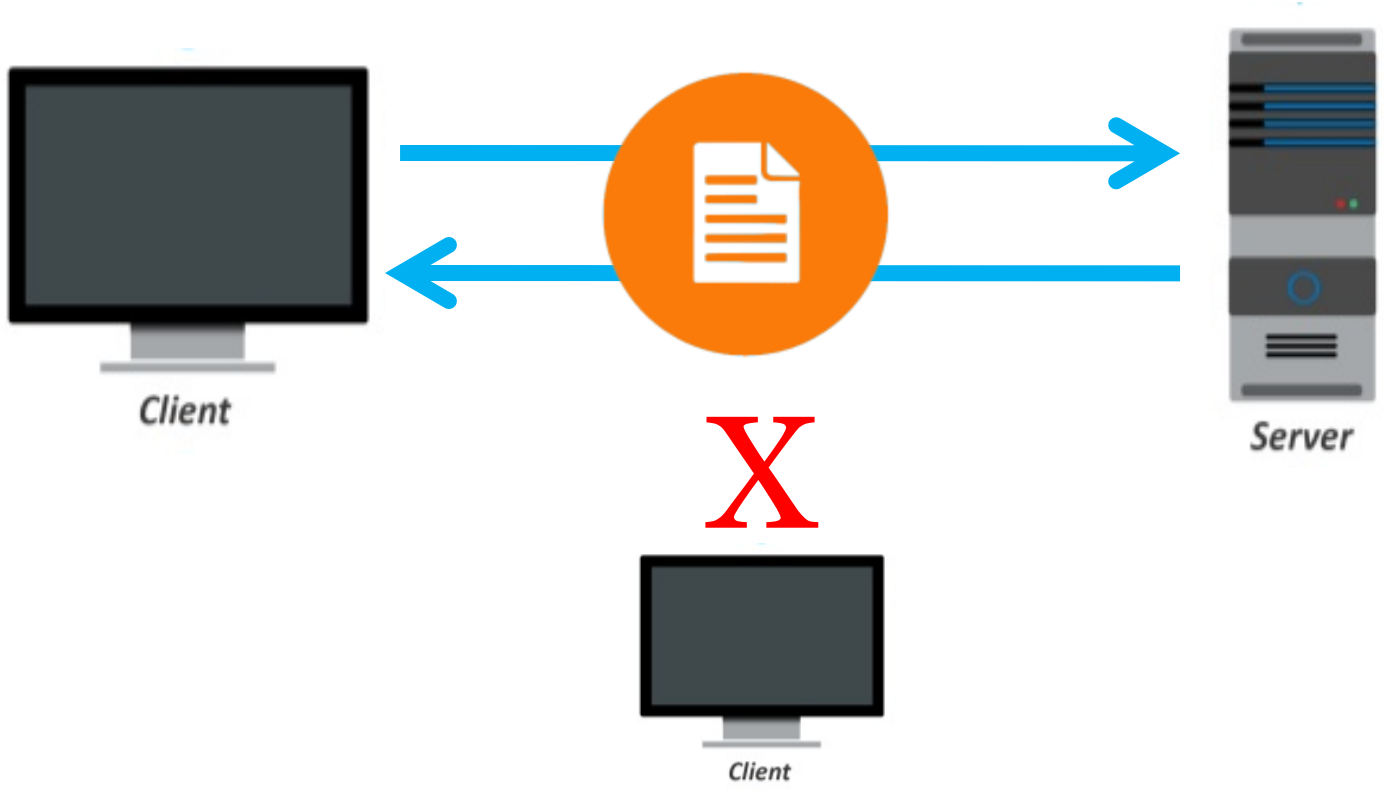
- Intégrité/Signature: elle désigne la capacité à s'assurer de la non-altération des informations d'origine, qu'elle soit accidentelle ou malveillante.

- Traçabilité: elle consiste à stocker des traces de toutes les interactions des utilisateurs avec les applications afin de pouvoir détecter des attaques ou des dysfonctionnements.

- Confidentialité/Chiffrement: elle consiste à empêcher la lecture d'informations par des personnes non habilitées ou malintentionnées.

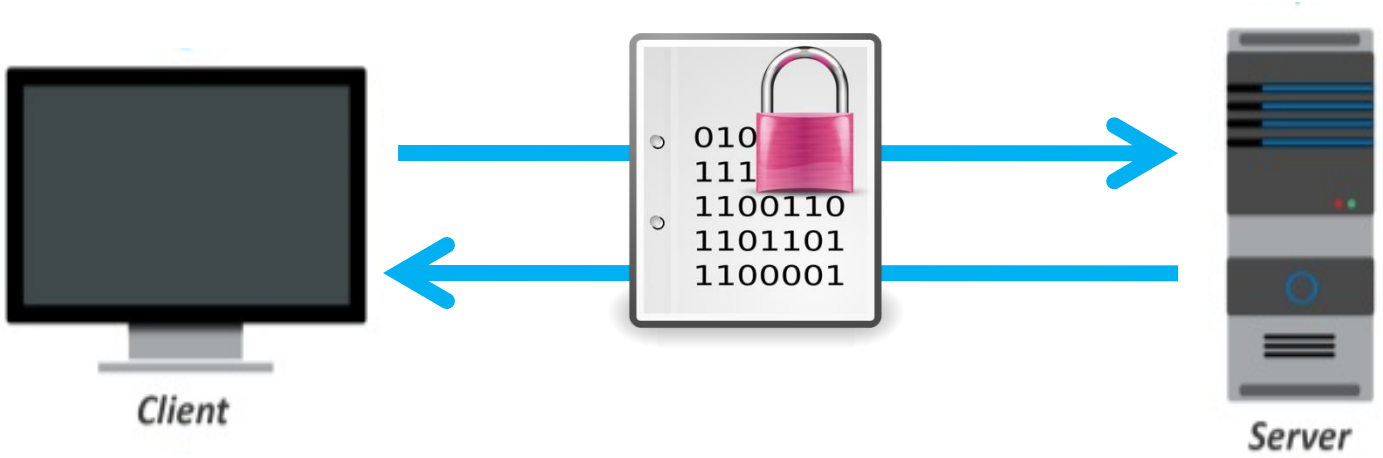
La Sécurité dans les Services Web

- Confidentialité : Les Tunnels SSL



La Sécurité dans les Services Web

- Confidentialité : Les Tunnels SSL



Clé - Chiffrement

Certificat - Identification

La Sécurité dans les Services Web

- Confidentialité : Les Tunnels SSL

La Sécurité dans les Services Web

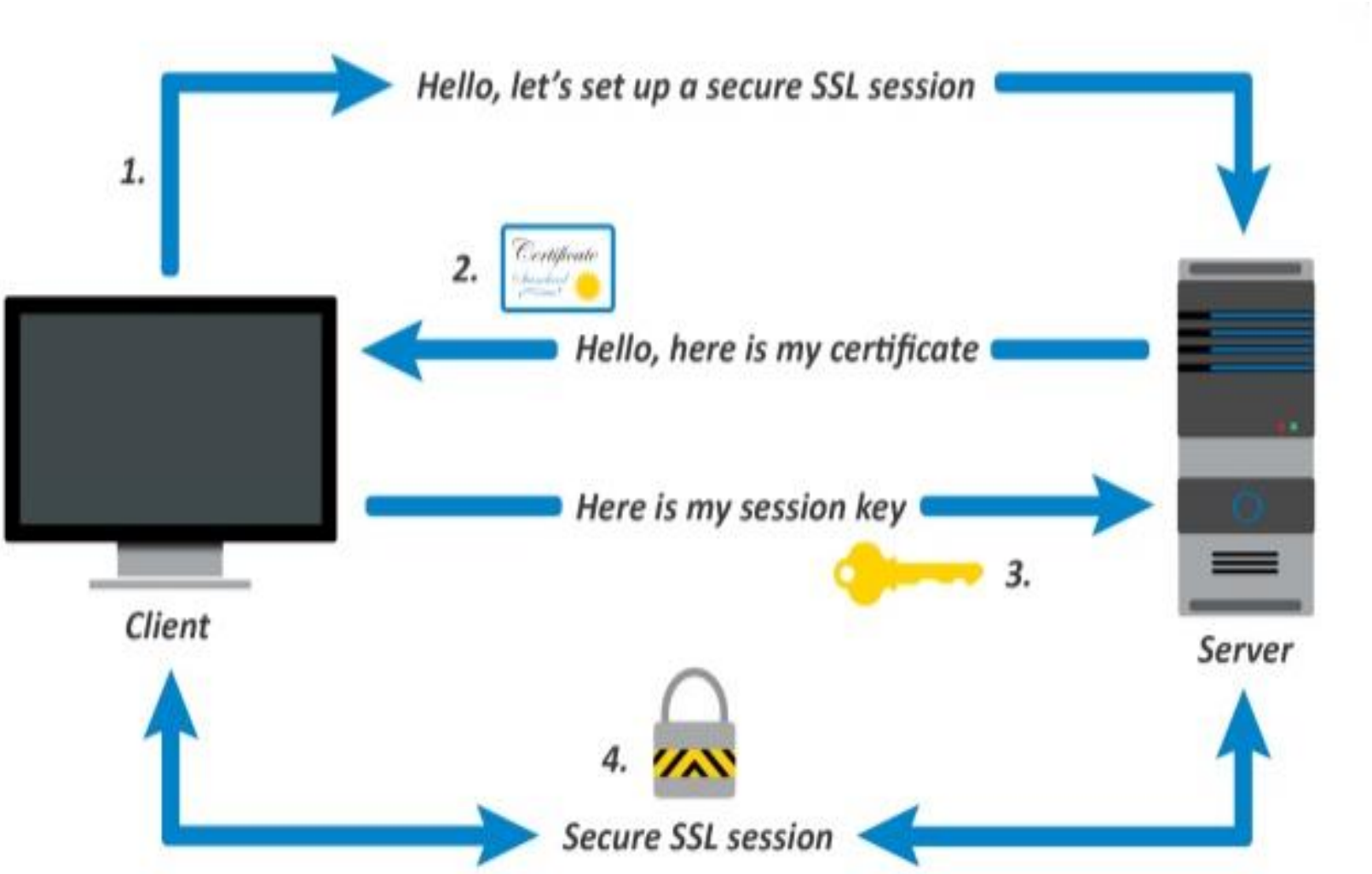
- Confidentialité : Les Tunnels SSL

La Sécurité dans les Services Web

- Confidentialité : Les Tunnels SSL

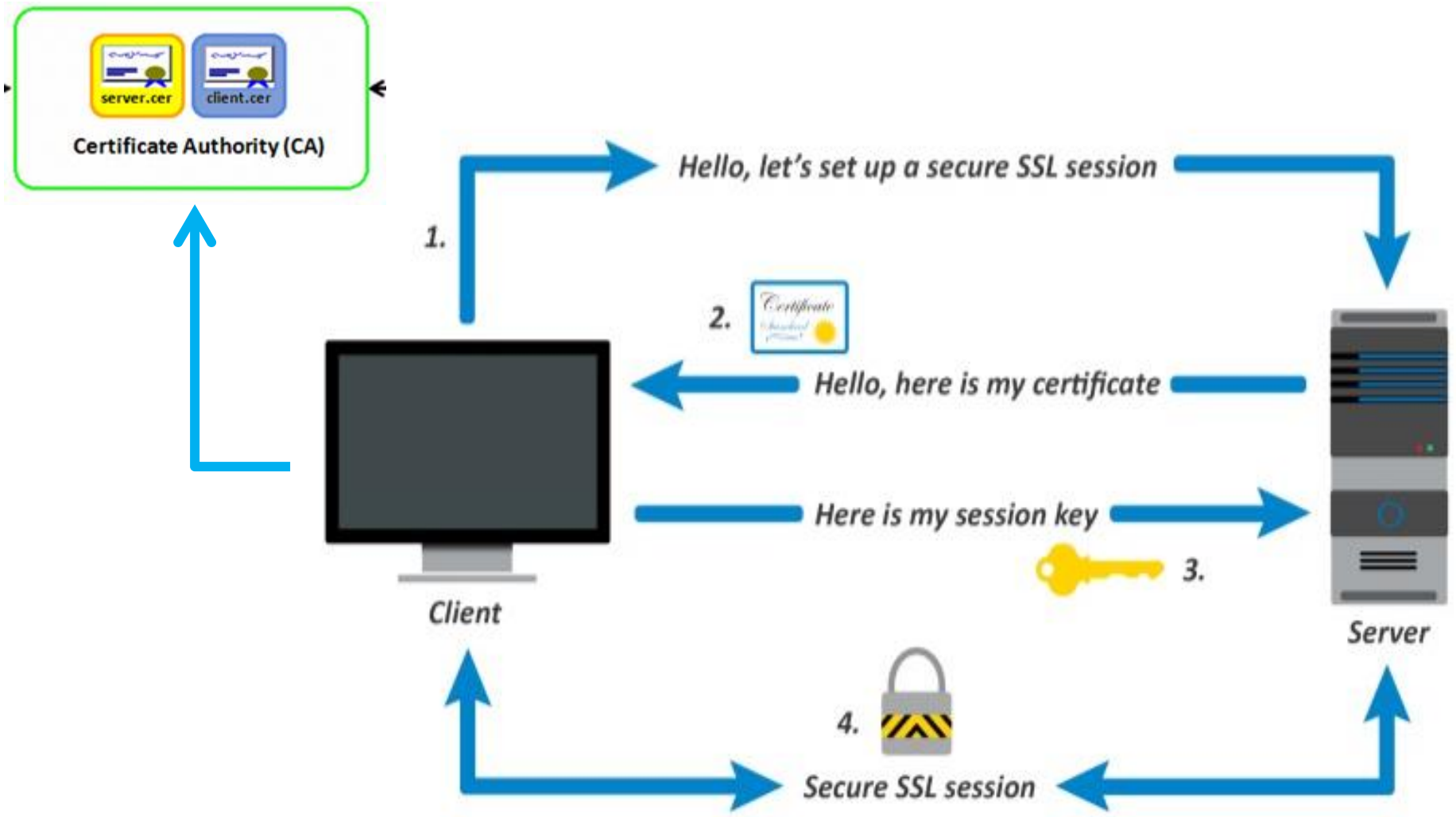
La Sécurité dans les Services Web

- Confidentialité : Les Tunnels SSL



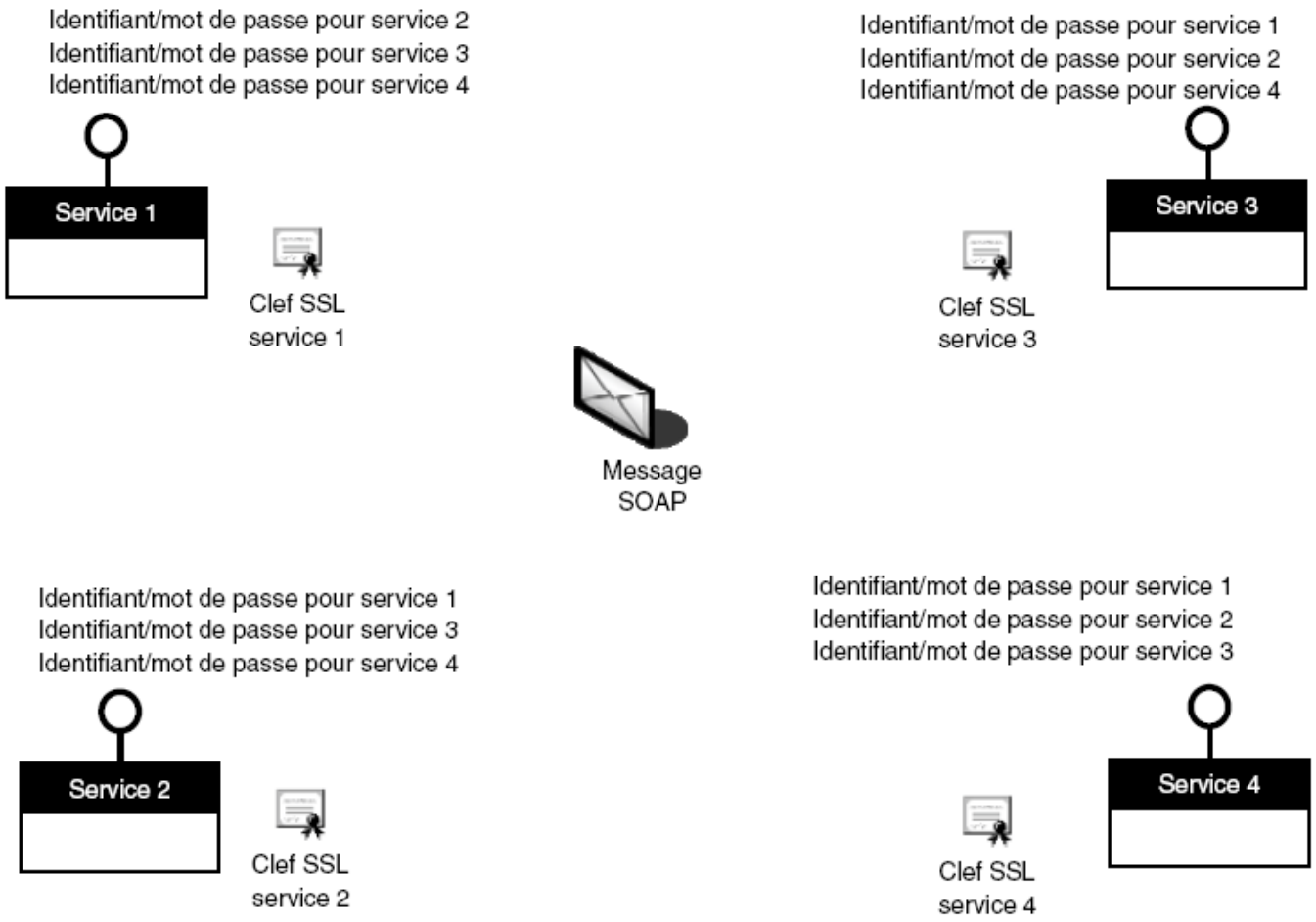
La Sécurité dans les Services Web

- Confidentialité : Les Tunnels SSL



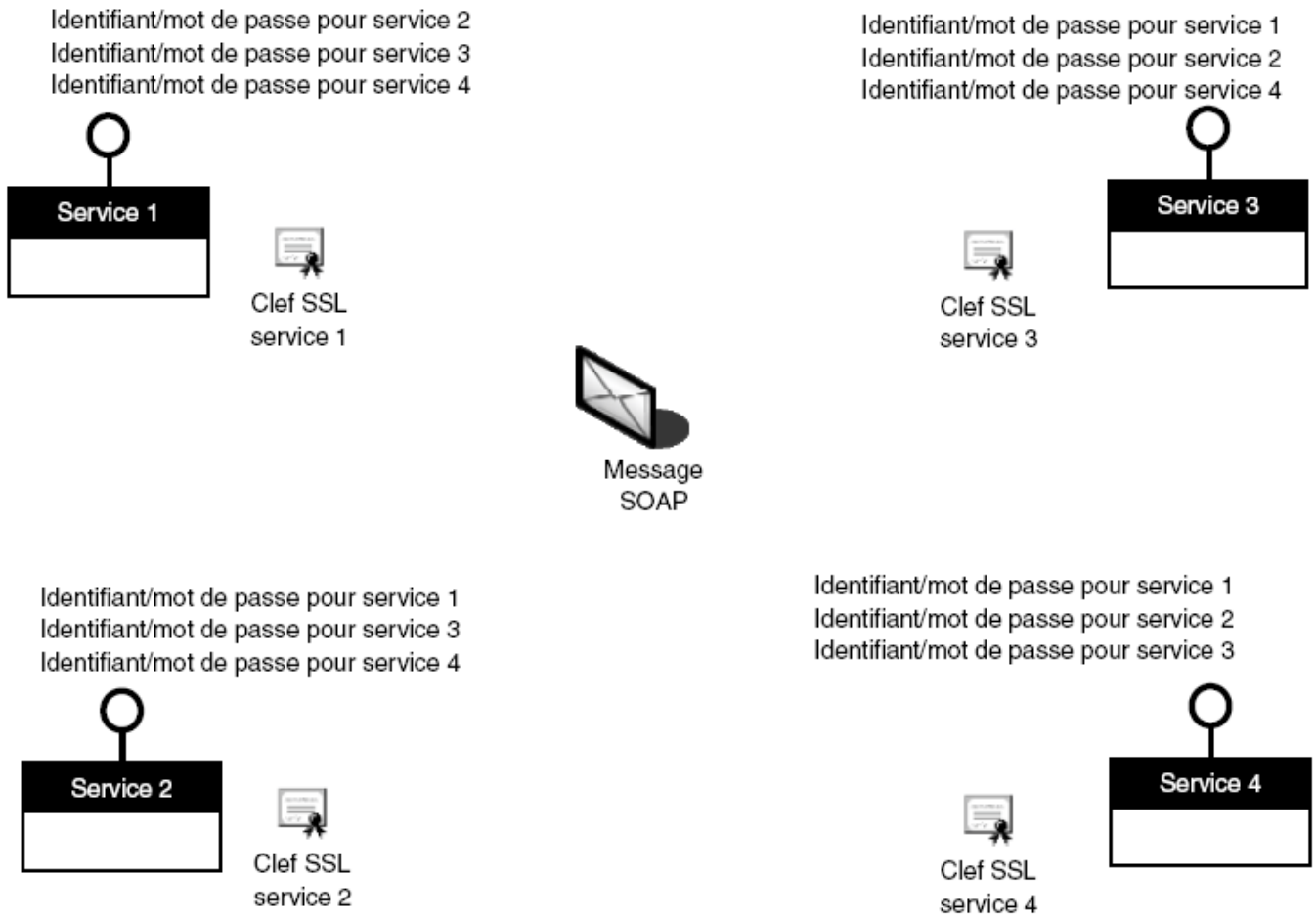
La Sécurité dans les Services Web

Inconvénient : dans le cadre d'échange de messages SOAP entre plus de deux services, le nombre de tunnels SSL devient exponentiel.



La Sécurité dans les Services Web

Préférer intégrer la gestion de la **sécurité au sein des messages SOAP**



La Sécurité dans les Services Web

- Les spécifications de la pile permettant la sécurisation des Web Services au travers de méthodes basées sur les messages SOAP eux-mêmes.

WS-Security

- WSS constitue un framework de base pour la sécurisation des Web Services.
- Initialement proposé par Microsoft, IBM, et Verisign repris par OASIS.
- Fonctions de sécurité de base + Sécurité dans les messages SOAP.
- Il repose principalement sur l'ajout d'éléments dans les en-têtes SOAP pour décrire les données liées à la sécurité..
- Il s'appuie sur les spécifications **XML** : Encryption, Signature, SAML.

La Sécurité dans les Services Web

- Les spécifications de la pile permettant la sécurisation des Web Services au travers de méthodes basées sur les messages SOAP eux-mêmes.

WS-Security

- WS-Security propose de sécuriser de manière intrinsèque les messages SOAP :

  - Assurer la confidentialité d'un fragment du message SOAP avec XML Encryption.
  - Assurer l'intégrité d'un fragment du message SOAP en le signant avec XML Signature.
  - Certifier l'identité de l'accédant auprès du serveur SOAP avec SAML.

WS-Security - **XML Encryption**

- Une spécification du W3C qui permet d'assurer la confidentialité des informations en chiffrant un message SOAP/XML.
- Mettre en œuvre des procédures automatisées pour assurer la confidentialité des échanges.
- Mode de fonctionnement : appliquer des mécanismes de chiffrement à clef secrète ou à clef publique sur une partie du message SOAP.
- Fournit une grammaire XML standardisée pour décrire les méthodes de chiffrement des données.

WS-Security - **XML Encryption**

Exemple:

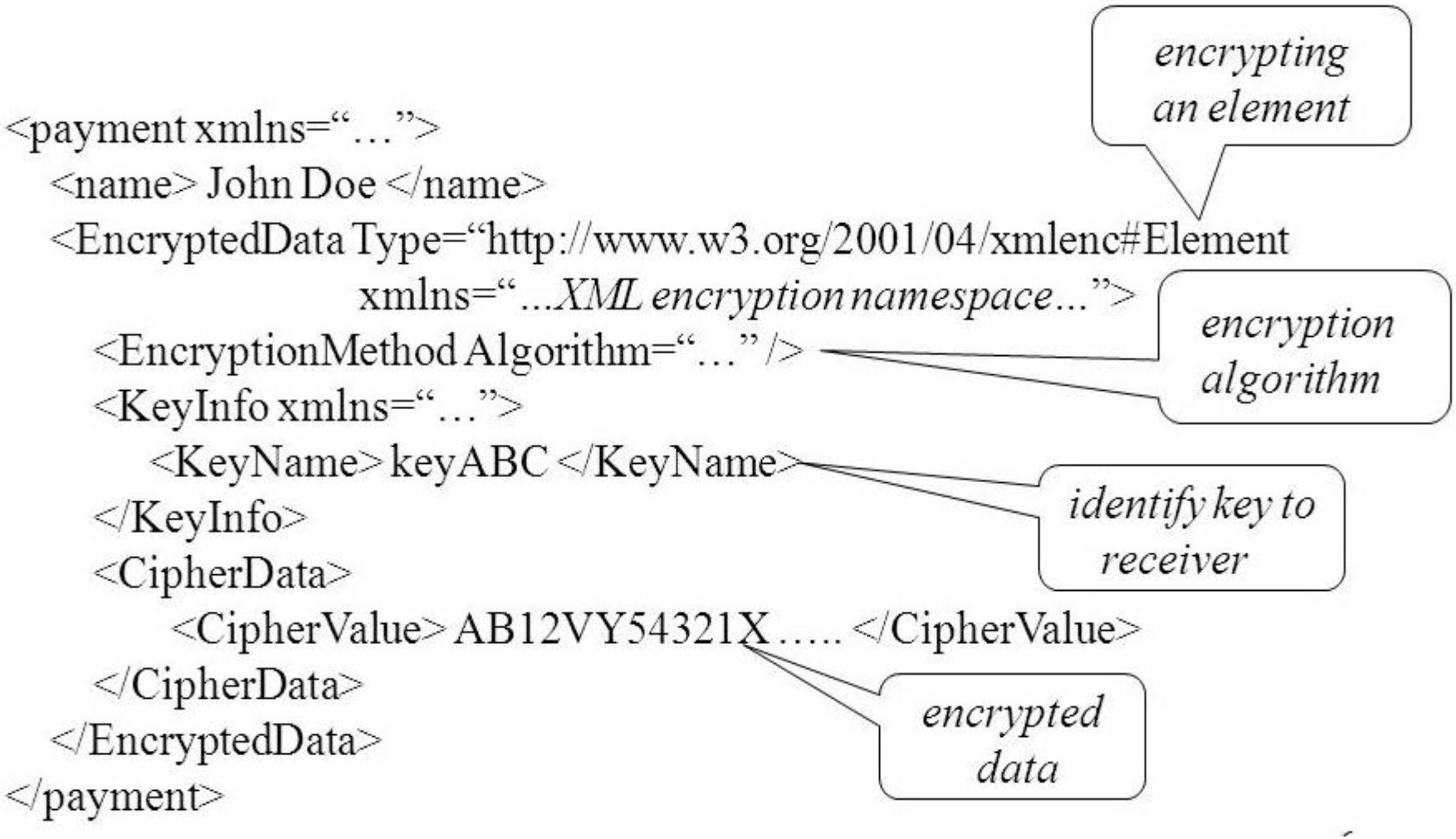
```
<?xml version='1.0'?>
 <PaymentInfo xmlns='http://example.org/paymentv2'>

          <Name>John Smith</Name>

         <CreditCard Limit='5,000' Currency='USD'>
                  <Number>4019 2445 0277 5567</Number>
                  <Issuer>Example Bank</Issuer>
                  <Expiration>04/23</Expiration>
         </CreditCard>

 </PaymentInfo>
```

WS-Security - **XML Encryption**

- Les balises indiquent l'emplacement des données chiffrées, la façon dont elles sont chiffrées et le chiffrement ou la clé utilisée pour les chiffrer.
- Avec la clé appropriée, les informations peuvent être déchiffrées.
- N'importe quelle partie du document XML peut être cryptée, voire le document entier peut également l'être.

```
<?xml version='1.0'?>
 <PaymentInfo xmlns='http://example.org/paymentv2'>
          <Name>John Smith</Name>
          <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
                  xmlns='http://www.w3.org/2001/04/xmlenc#'>
                    <CipherData>
                              <CipherValue>A23B45C56</CipherValue>
                    </CipherData>
          </EncryptedData>
 </PaymentInfo>
```

WS-Security - **XML Encryption**



WS-Security - **XML Signature**

- Une spécification du W3C permettant l'utilisation de signatures numériques dans les documents XML.
- Permet d'assurer l'intégrité des données et la non répudiation d'un message SOAP en appliquant une signature numérique sur un message SOAP/XML.
- S'assurer que l'identité (authentification) utilisée dans le message est bien celle qui a créé le message.

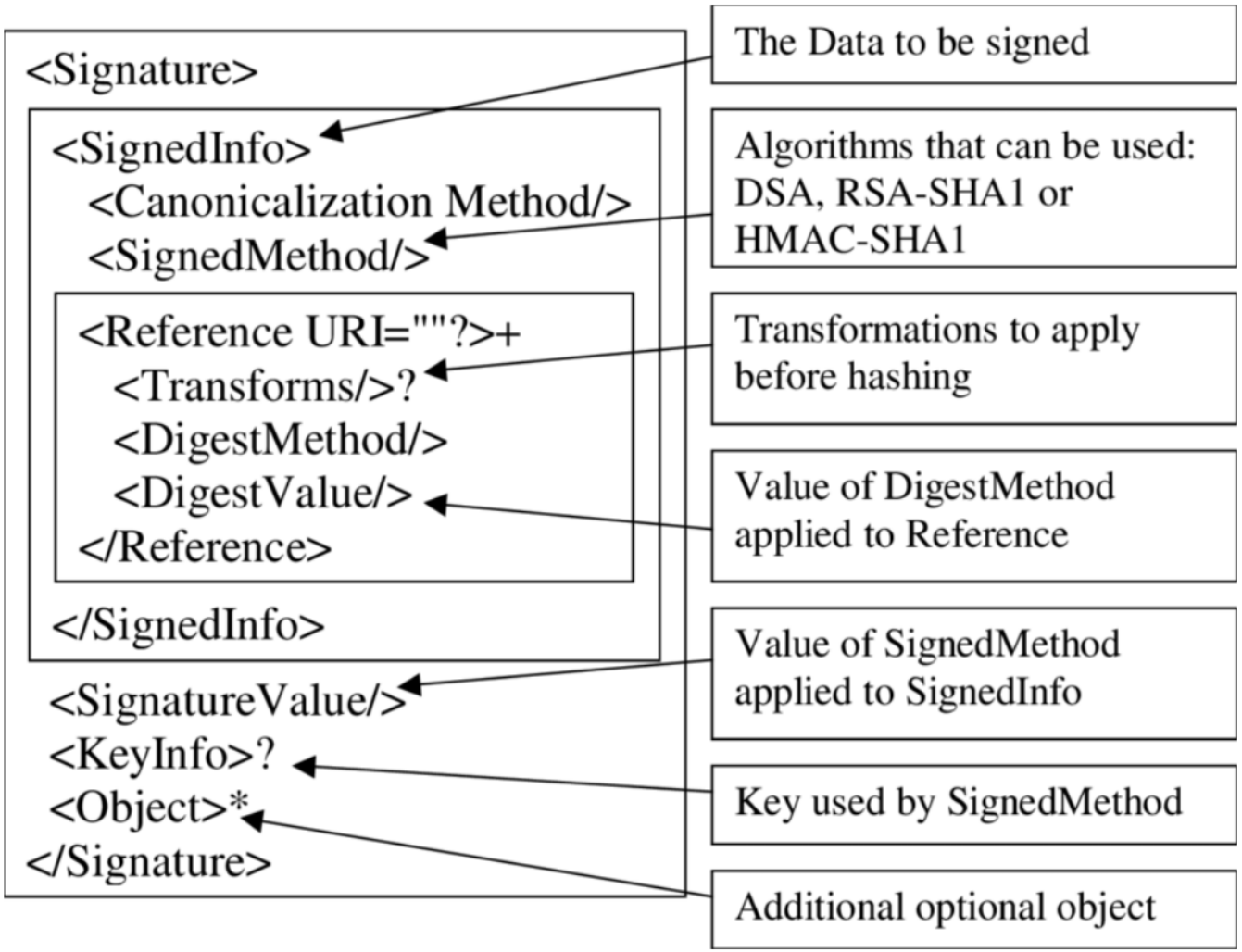
Disons que dans le cadre d'une transaction de service Web, un contrat doit être signé, et le contrat se trouve dans un document XML passé lors de la transaction. La partie de contrat du document XML ressemble à ceci:

```
<contract>
  <contract-item id="Section 1A">
     I, the undersigned, agree to pay $35,000 for delivery of 15 new computers.
  </contract-item>
 </contract>
```

WS-Security - XML Signature

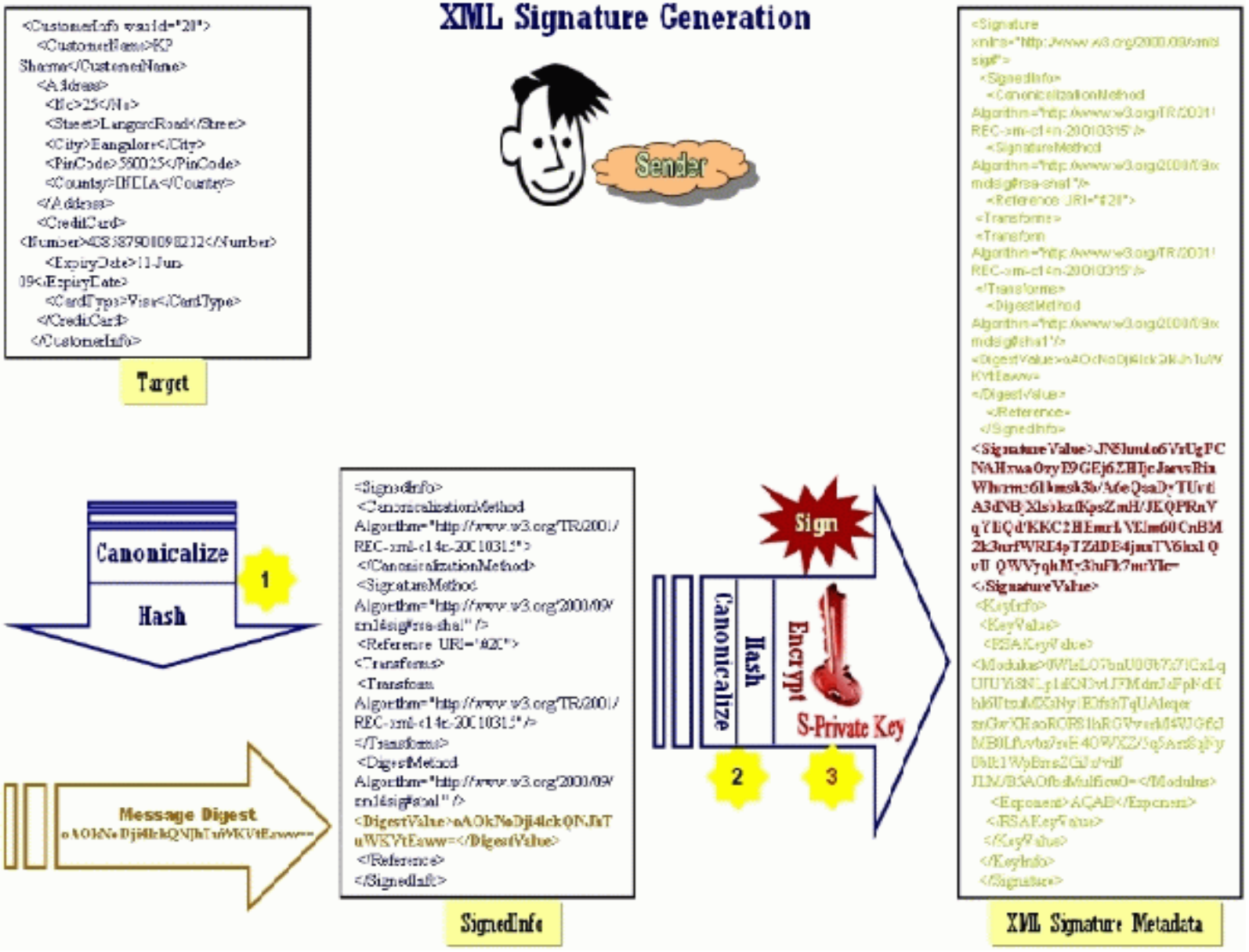
```
<Signature>
 <SignedInfo>
   <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-
        xml-c14n-20010315"/>
   <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-
        sha1"/>
   <Reference URI="#Res1">
    <Transforms>
         <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
         20010315"/>
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
  </Reference>
 </SignedInfo>

 <SignatureValue>
       jHE3lP4dilsS+CSaQ=+2dFf7yc2TXCo0K4sAWb
 </SignatureValue>
</Signature>
```

WS-Security - XML Signature



Kleiner, Emi & Roscoe, A.. (2006). On the Relationship Between Web Services Security and Traditional Protocols. Electronic Notes in Theoretical Computer Science. 155. 583-603. 10.1016/j.entcs.2005.11.074.

WS-Security - XML Signature



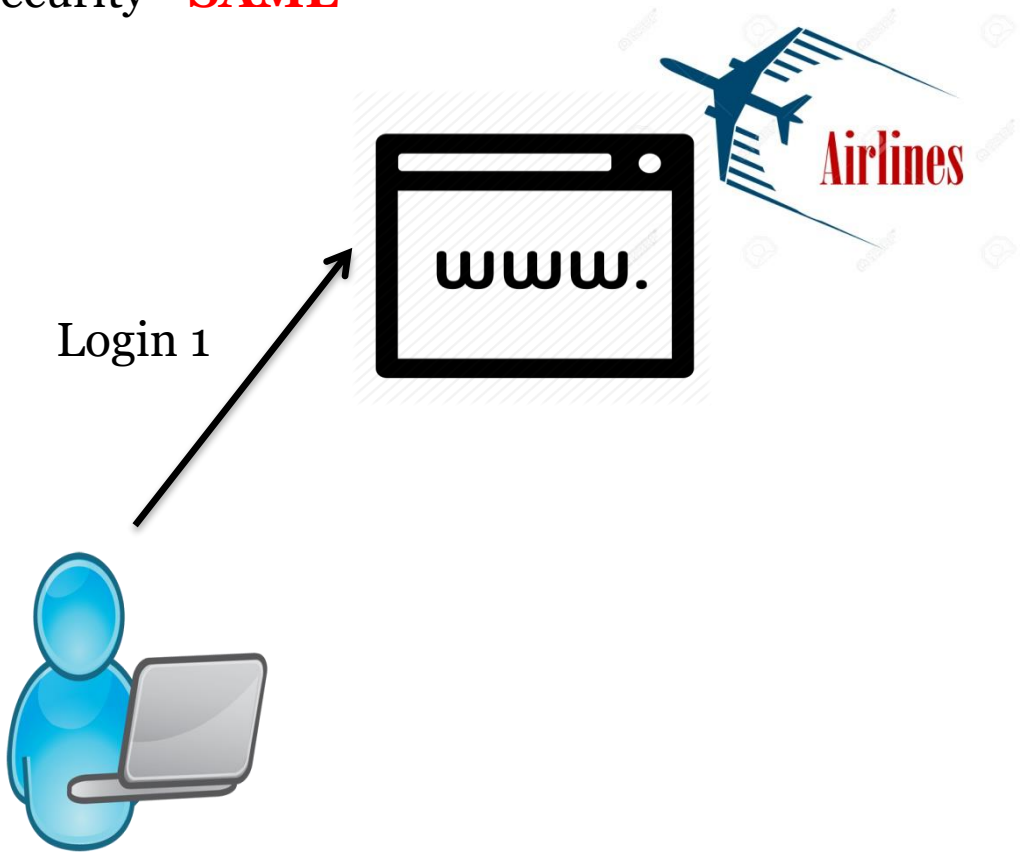
La Sécurité dans les Services Web

WS-Security - **SAML**

- SAML signifie *Security Assertion Markup Language*.
- Une grammaire XML normalisée par l'OASIS.
- Permet d'attester l'authentification d'un client souhaitant accéder à plusieurs services, en évitant ainsi à ce client de s'authentifier autant de fois qu'il y a de services invoqués.
- SAML autorisant l'authentification unique (SSO), les utilisateurs peuvent se connecter une seule fois et réutiliser ces mêmes identifiants pour se connecter à d'autres fournisseurs de service.
- Exemple :

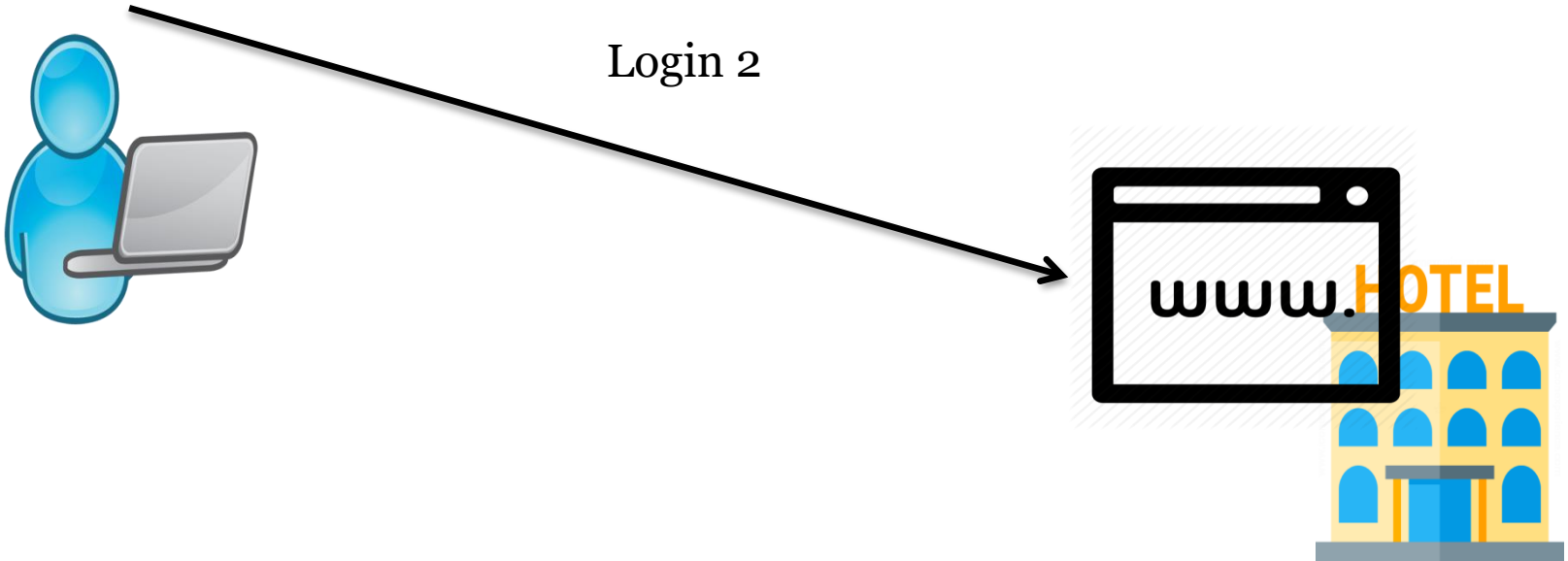
La Sécurité dans les Services Web

WS-Security - **SAML**



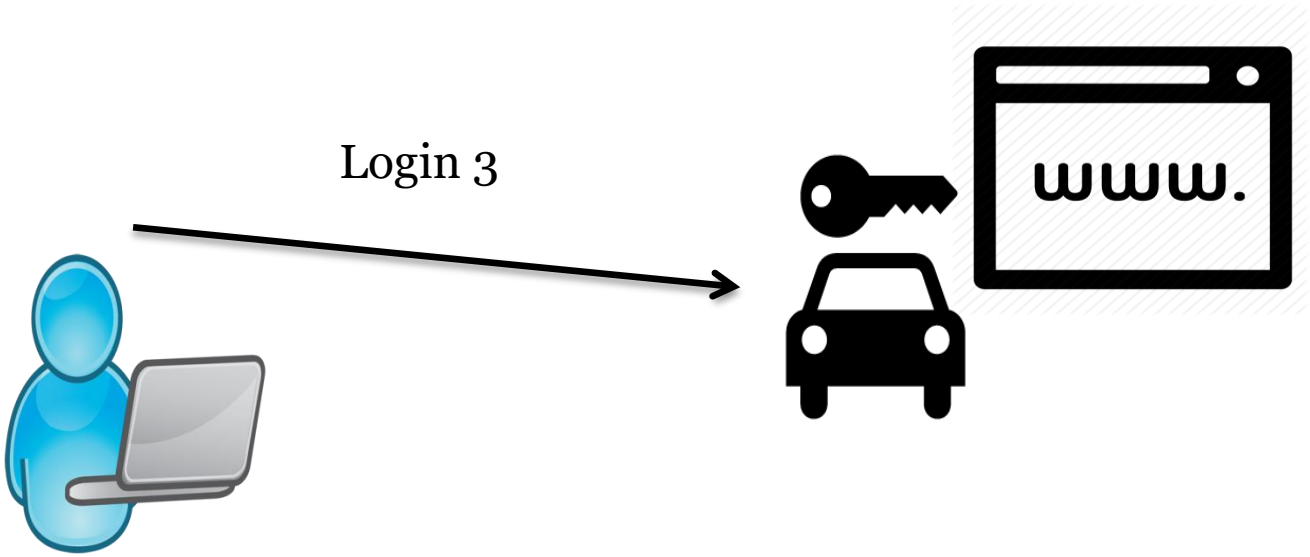
La Sécurité dans les Services Web

WS-Security - **SAML**



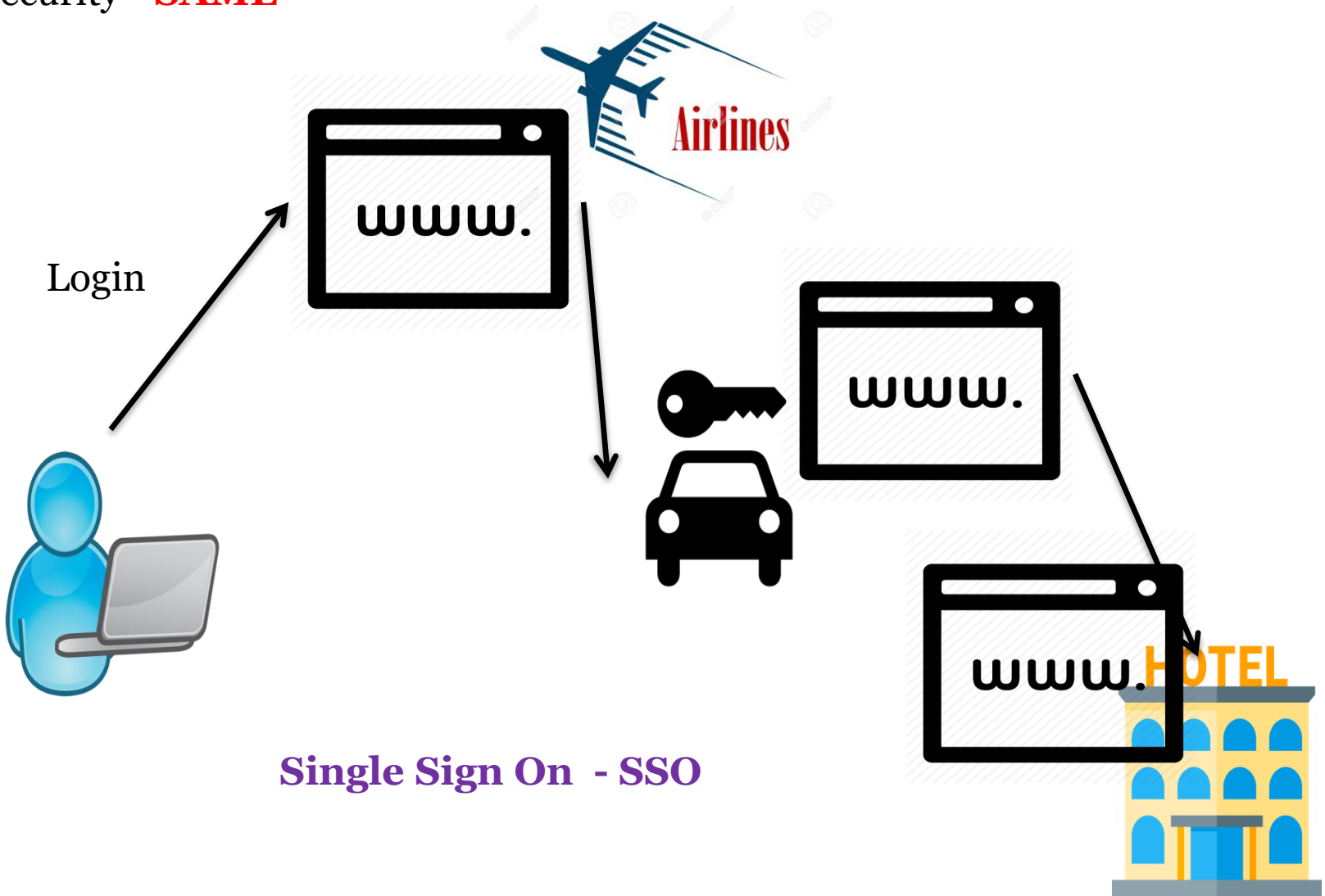
La Sécurité dans les Services Web

WS-Security - **SAML**



La Sécurité dans les Services Web

WS-Security - **SAML**



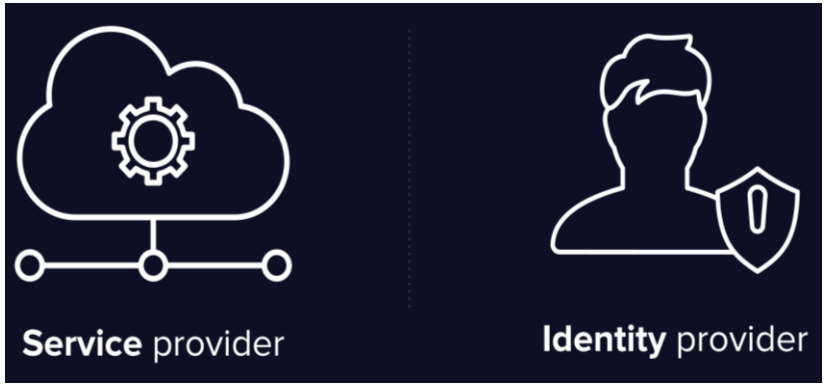
Single Sign On - SSO

La Sécurité dans les Services Web

WS-Security – **SAML**

- Une série de messages XML qui détaillent :
  - Si les utilisateurs sont authentifiés. - Authentification
  - Quels droits, rôles, et accès ont-ils. - Autorisation
  - Comment puissent-ils accéder aux données selon ces droits/rôles.

- Utilisation :
  - Single Sign On
  - Single Logout
  - Partage d'attributs
  - Lier des comptes utilisateurs



https://www.varonis.com/fr/blog/quest-ce-que-saml-et-comment-ca-marche

WS-Security – **SAML**

- SAML met en œuvre une méthode sécurisée de transfert des autorisations et authentifications entre le fournisseur d'identité et les fournisseurs de service.

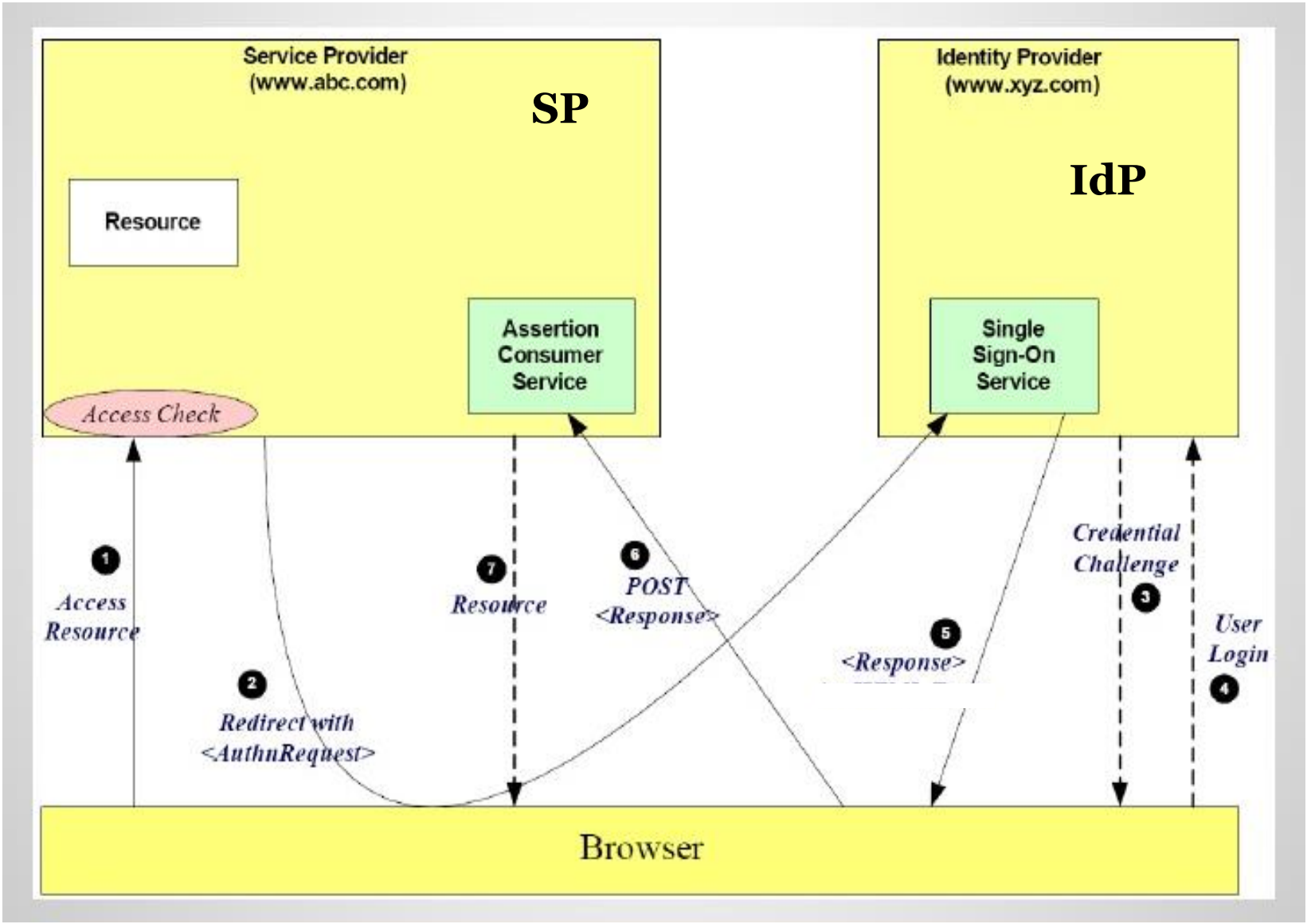
- Lorsqu'un utilisateur se connecte à une application compatible SAML, le fournisseur de service demande une autorisation auprès du fournisseur d'identité concerné.

- Le fournisseur d'identité authentifie les données d'identification de l'utilisateur puis retourne l'autorisation de l'utilisateur au fournisseur de service. L'utilisateur est alors en mesure d'utiliser l'application.

- L'authentification SAML est la procédure consistant à vérifier l'identité et les données d'identification de l'utilisateur (mot de passe, authentification à deux facteurs, etc.).

- L'autorisation SAML indique au fournisseur de service quel accès accorder à l'utilisateur authentifié.

La Sécurité dans les Services Web



WS-Security – **SAML**

Trois protocoles principaux :

- Assertions : **jetons de sécurité**.
  - Une assertion SAML est le document XML contenant l'autorisation utilisateur que le fournisseur d'identité envoie au service.

  - Trois types d'assertions: authentification, attribution, décision d'autorisation.

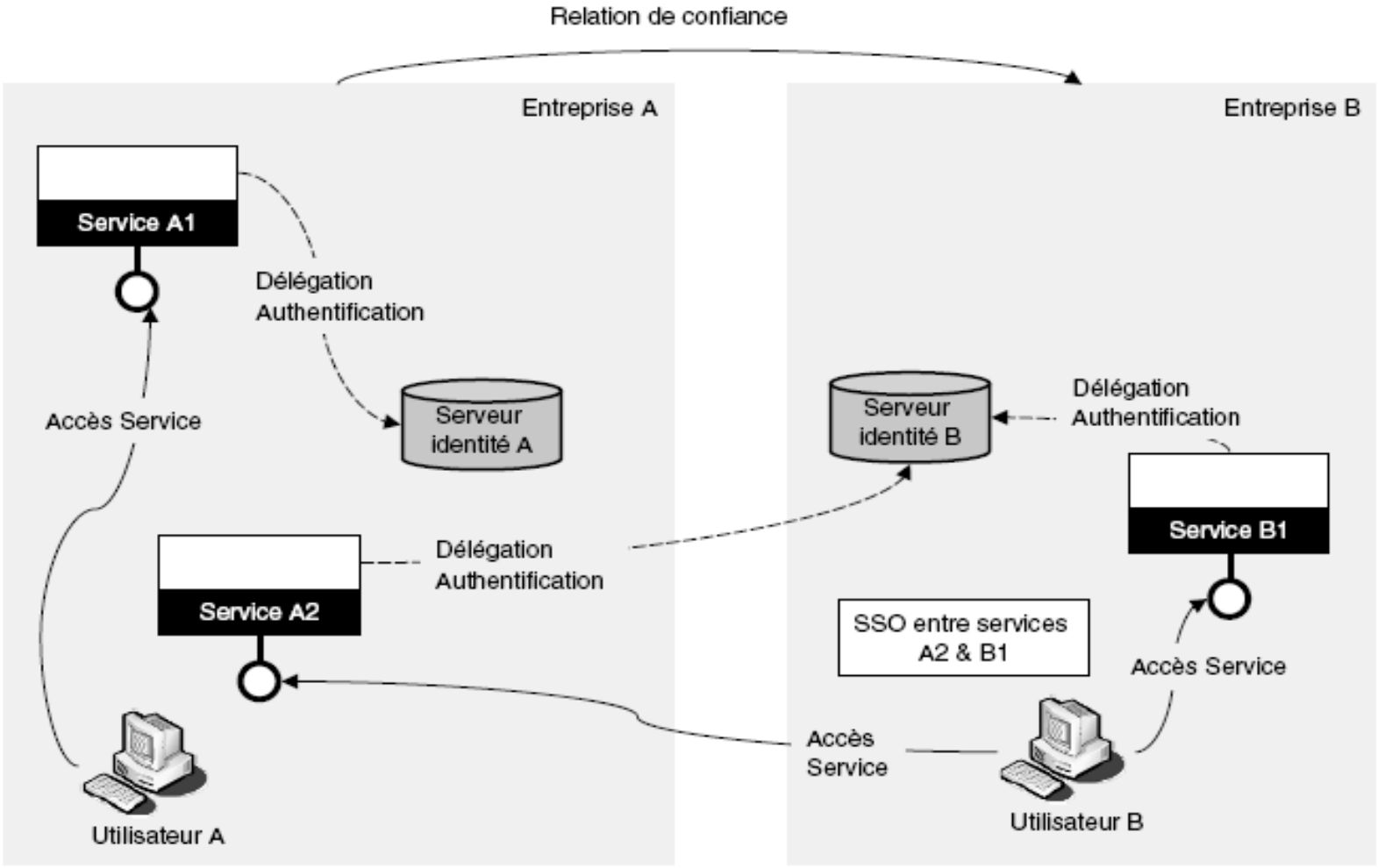
✓ Assertions d'authentification : prouvent l'identification de l'utilisateur et indiquent l'heure de connexion et la méthode d'authentification utilisée.
✓ Assertions d'attributs : contient des détails spécifiques sur l'utilisateur (ex: citizenship, credit line, etc).
✓ Assertions d'autorisation : identifie ce que l'utilisateur peut ou pas faire.

- Bindings : comment les messages SAML sont échangés – protocole de communication (SOAP, etc.)
- Protocoles : Comment SAML récupère les assertions (ex: soap over http)

La fédération d'identité

- Une approche d'architecture qui propose d'établir des liens de confiance de manière distribuée entre des Services et des référentiels utilisateurs.
- Ces liens forment les *serveurs d'identité*.
- Un serveur d'identité est une sorte d'annuaire, capable d'authentifier des accédants pour le compte d'applications internes ou externes à l'entreprise sur la base des technologies Web Services.
- Il fournit aussi des fonctions de Single Sign On.
- Objectif : faciliter les échanges entre partenaires sans avoir à dupliquer les référentiels utilisateurs.
- Project Liberty, *WS-Federation*, *etc.*

La fédération d'identité

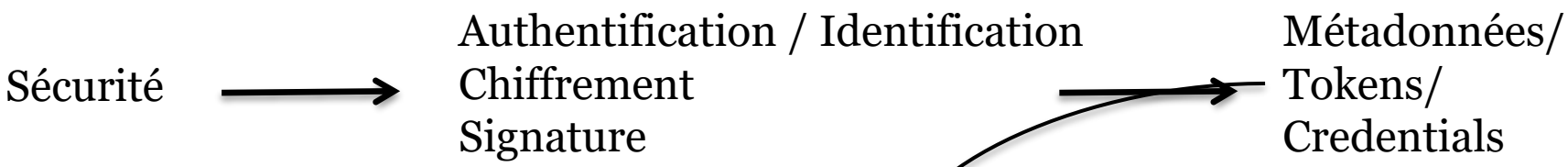


La Sécurité dans les Services Web

Sécurité → Authentification / Identification
Chiffrement
Signature → Métadonnées/
Tokens/
Credentials

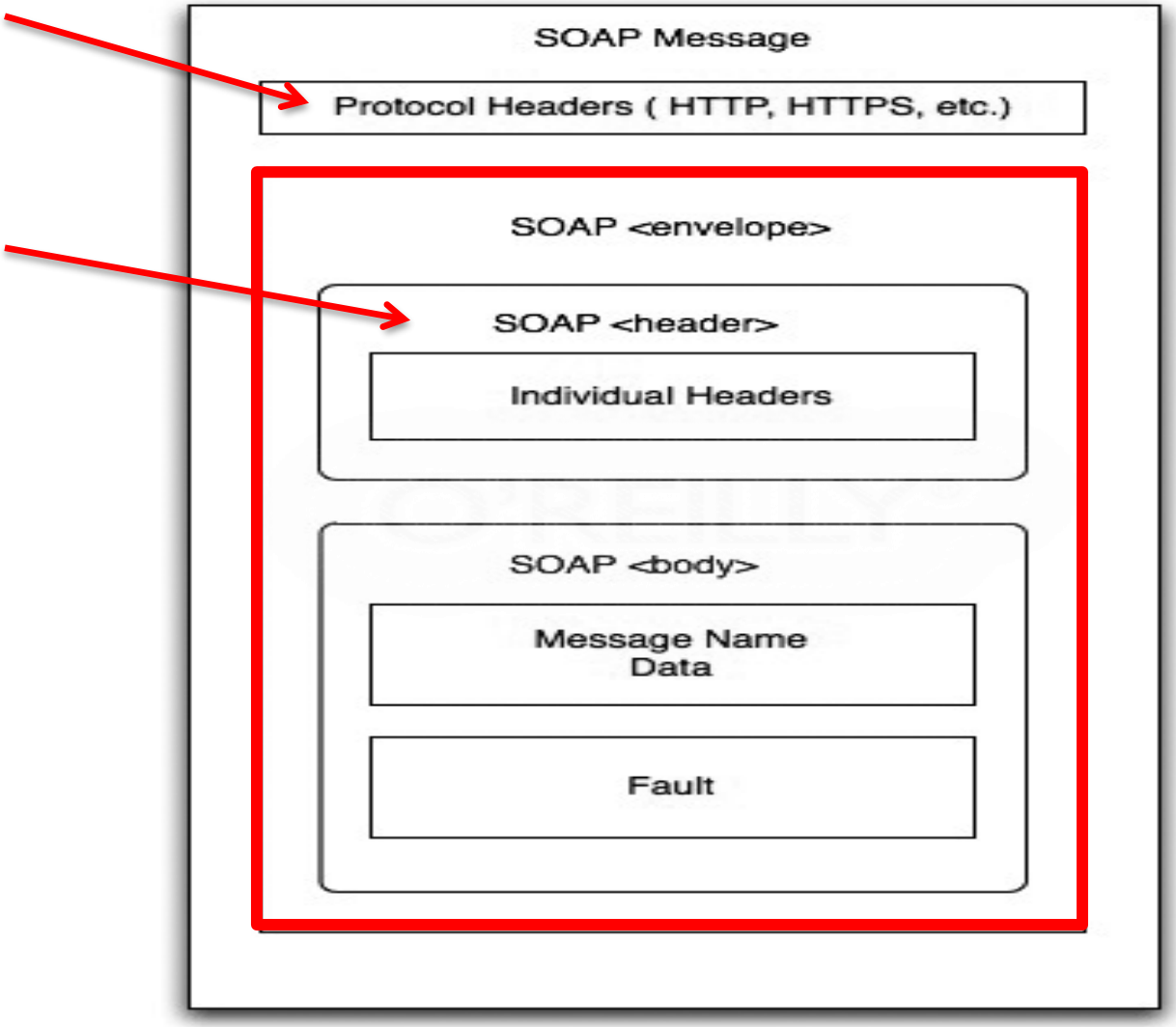
```
<soapenv:Envelope  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope">
        <soapenv:Header>
                ...
        <soapenv:Header/>
        <soapenv:Body>
                <!-- Contenu de la Requête -->
        </soapenv:Body>
</soapenv:Envelope>
```

La Sécurité dans les Services Web




```
<soapenv:Envelope  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope">
        <soapenv:Header>
                ...
        <soapenv:Header/>
        <soapenv:Body>
                <!-- Contenu de la Requête -->
        </soapenv:Body>
</soapenv:Envelope>
```

La Sécurité dans les Services Web



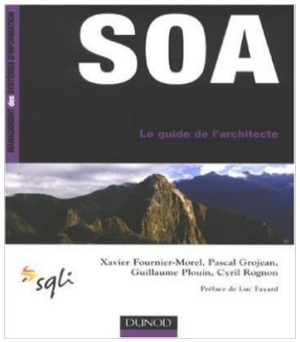
La Sécurité dans les Services Web

Sécurité → Authentification / Identification
Chiffrement
Signature → Métadonnées/
Tokens/
Credentials

Credentials
- ✓ Username / Password
- ✓ Signature - @ IP, @MAC, etc.
- ✓ SAML Token
- ✓ Certificat X509
- ✓ Ticket Kerberos

- Ces Credentials dans JAX-WS sont appelés **Message Context**

Ressources



Le guide de l'architecte du SI

- ✓ Auteur : Xavier Fournier-Morel, Pascal Grosjean, …
- ✓ Éditeur : Dunod
- ✓ Edition : Octobre 2006 - 302 pages - ISBN : 2100499726

SOA Principles of Service Design

- ✓ Auteur : Thomas Erl
- ✓ Éditeur : Prentice Hall Ptr
- ✓ Edition : Juillet 2007 - 608 pages - ISBN : 0132344823

SOA : Architecture Logique : Principes, structures et bonnes pratiques

- ✓ Auteur : Gilbert Raymond
- ✓ Éditeur : Softeam
- ✓ Edition : Livre Blanc

Ressources

URBANISATION & ARCHITECTURE ORIENTÉE SERVICE (SOA)
Quelques bonnes pratiques pour leur mise en oeuvre

- ✓ Auteur : Cyrille Devaux
- ✓ Éditeur : Aubay Management
- ✓ Edition : 2008, Livre Blanc

SOA Principles of Service Design

- ✓ Auteur : Thomas Erl
- ✓ Éditeur : Prentice Hall Ptr
- ✓ Edition : Juillet 2007 - 608 pages - ISBN : 0132344823

SOA : Architecture Logique : Principes, structures et bonnes pratiques

- ✓ Auteur : Gilbert Raymond
- ✓ Éditeur : Softeam
- ✓ Edition : Livre Blanc