Sécurité des Web Services
(SOAP vs REST)

Sylvain Maret
Principal Consultant / MARET Consulting / @smaret OpenID Switzerland

OWASP Switzerland - Geneva Chapter meeting
Lieu: Genève (Suisse) 6 décembre 2012

05/06.11.2012, Version 1.1 @smaret

Agenda

- Qu’est-ce qu’un Web Service ?
- SOAP
- REST
- Threat Modeling / ACME SA
- Réduction des risques
- Conclusion
- Questions

Bio

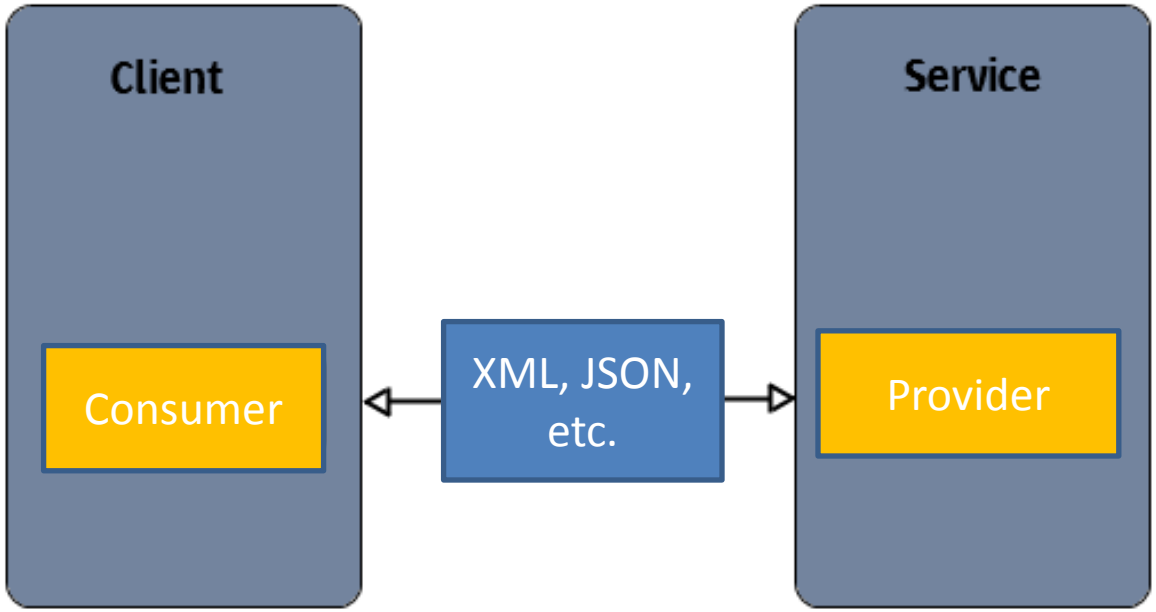
- 18 years of experience in ICT Security
- Principal Consultant at MARET Consulting
- Expert & Lecturer at University of Applied Sciences (Yverdon)
- Swiss French Area delegate at OpenID Switzerlan
- Co-founder Application Security Forum #ASFWS
- OWASP Member
- Author of the blog: la Citadelle Electronique
- http://ch.linkedin.com/in/smaret or @smaret
- http://www.slideshare.net/smaret

- Chosen field
  - AppSec / Digital Identity Security / Cyber Defense

Agenda

- Qu’est-ce qu’un Web Service ?
- SOAP
- REST
- Threat Modeling / ACME SA
- Réduction des risques
- Conclusion
- Questions

Web Service ?



Un **service web** (ou **service de la toile**[1]) est un programme informatique permettant la communication et l'échange de données entre applications et systèmes hétérogènes dans des environnements distribués. Il s'agit donc d'un ensemble de fonctionnalités exposées sur internet ou sur un intranet, par et pour des applications ou machines, sans intervention humaine, et de manière synchrone.

Un peu d'histoire

- 1990 : DCE/RPC – Distributed Computing Environment
- 1992 : CORBA – Common Object Request Broker Architecture
- 1990-1993 : Microsoft's DCOM -- Distributed Component Object Model
- 1995: RMI – Monde Java

- Pour arriver à une standardisation (toujours en cours) des protocoles, outils, langages et interfaces
  - SOAP
  - REST
  - Etc.

→ **Web Service**

Typical Web Services environment

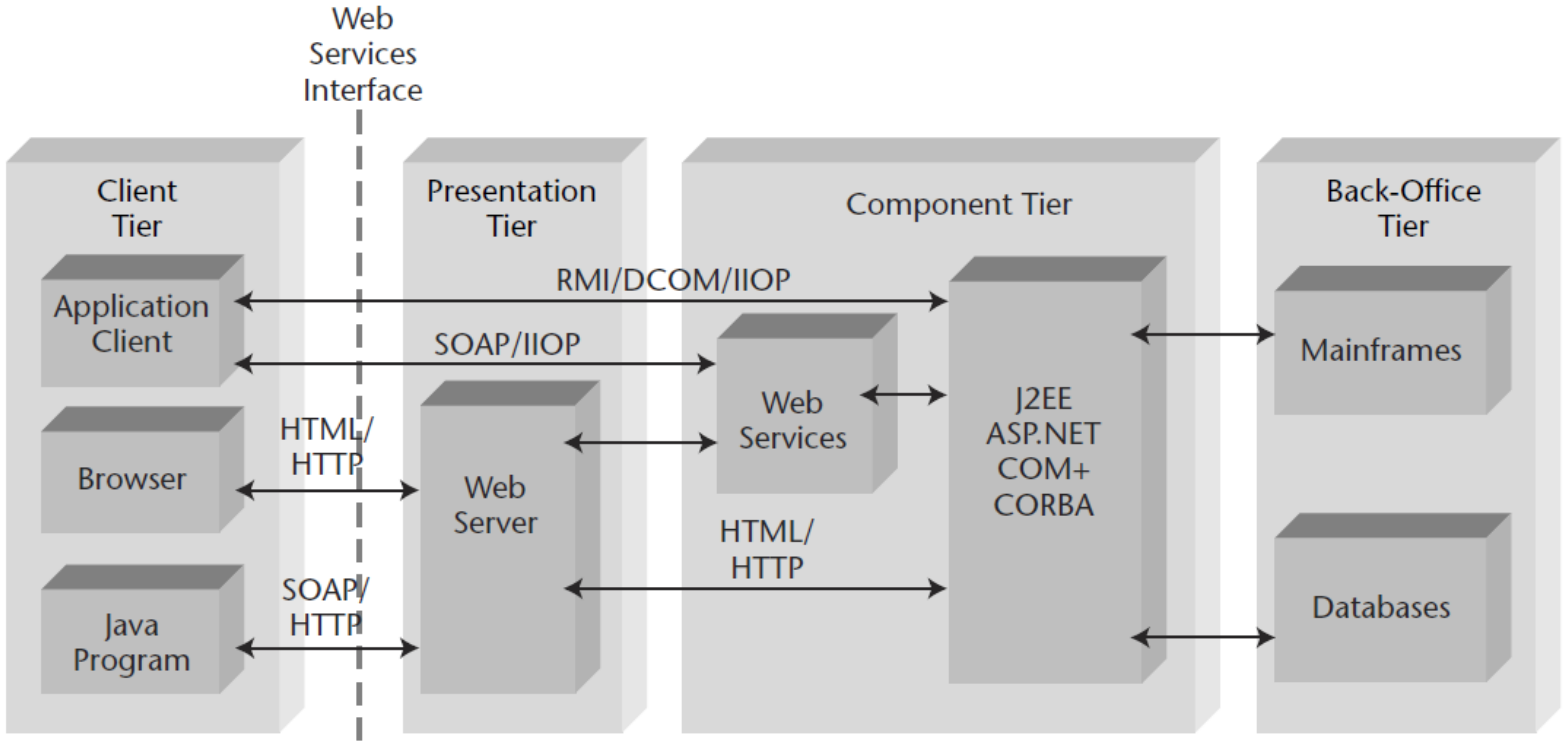


Figure 1.1 Typical Web Services environment.

Source: Mastering Web Services Security / www.wiley.com

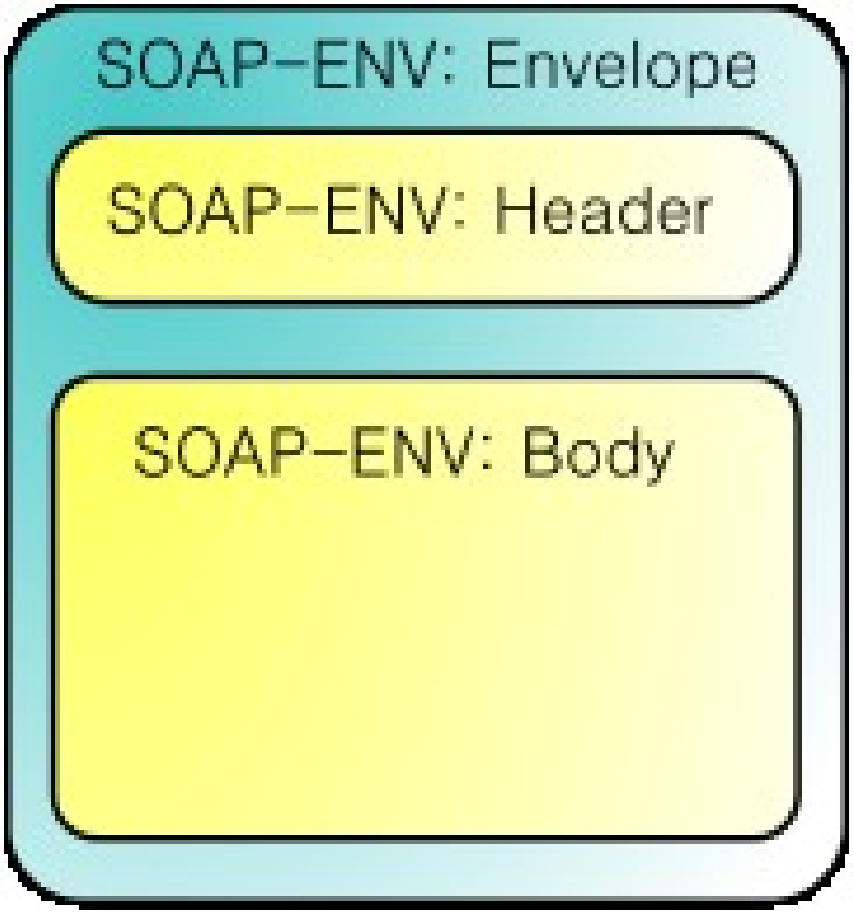
Agenda

- Qu’est-ce qu’un Web Service ?
- SOAP
- REST
- Threat Modeling / ACME SA
- Réduction des risques
- Conclusion
- Questions

SOAP: Démystification des technologies

- Langages
  - XML
  - WSDL : Descripteur du service
  - UDDI: Annuaire des services
  - Xpath
- Protocoles
  - Transport: HTTP, HTTPS, SMTP, FTP, SMS, TFTP, SSH, etc. (TCP or UDP)
  - Message: Enveloppe SOAP
- Sécurité
  - WS-Security (Signature & Chiffrement)
- Autres éléments
  - AuthN: SAML, X509, Username & Password, Kerberos, HTTP Digest, etc.

Enveloppe SOAP

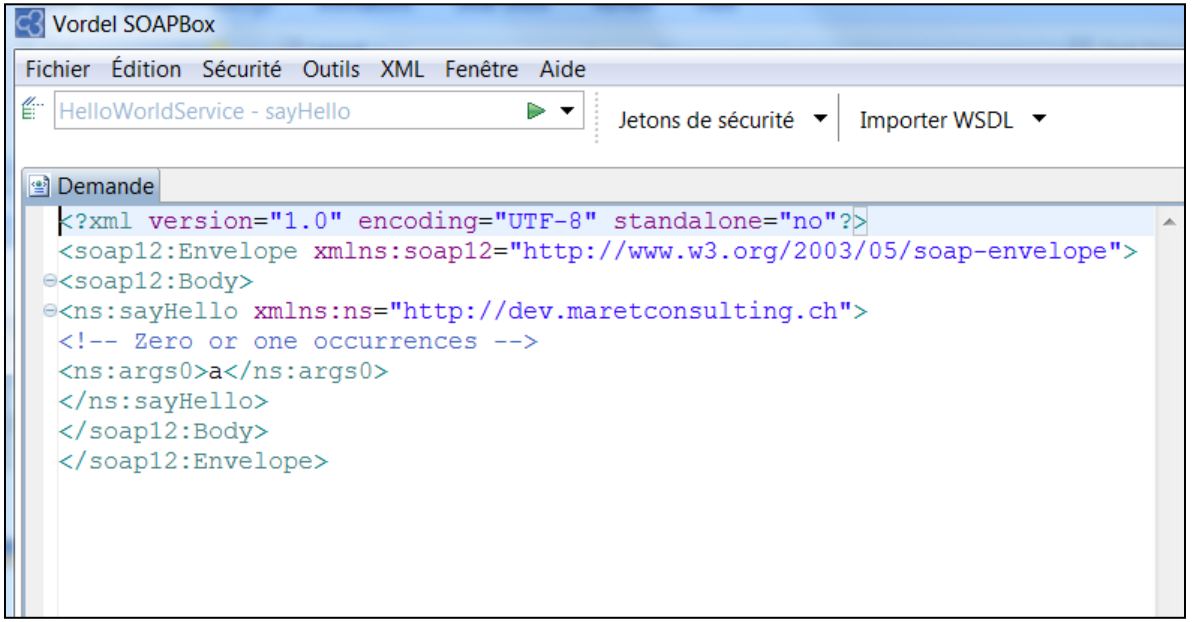


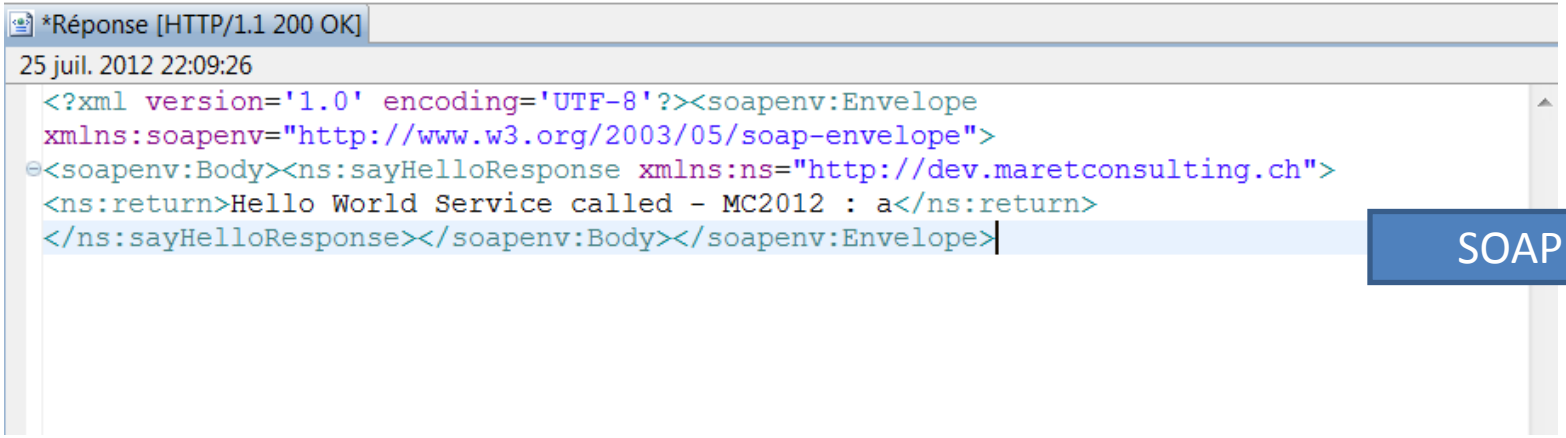
- SOAP : Simple Object Access Protocol

- Permet l'envoi de messages XML

Source= wikipédia

SOAP request



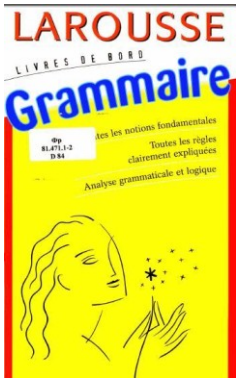


SOAP response

UDDI

- **U**niversal **D**escription **D**iscovery and **I**ntegration, connu aussi sous l'acronyme UDDI, est un annuaire de services fondé sur XML et plus particulièrement destiné aux services Web.

WSDL

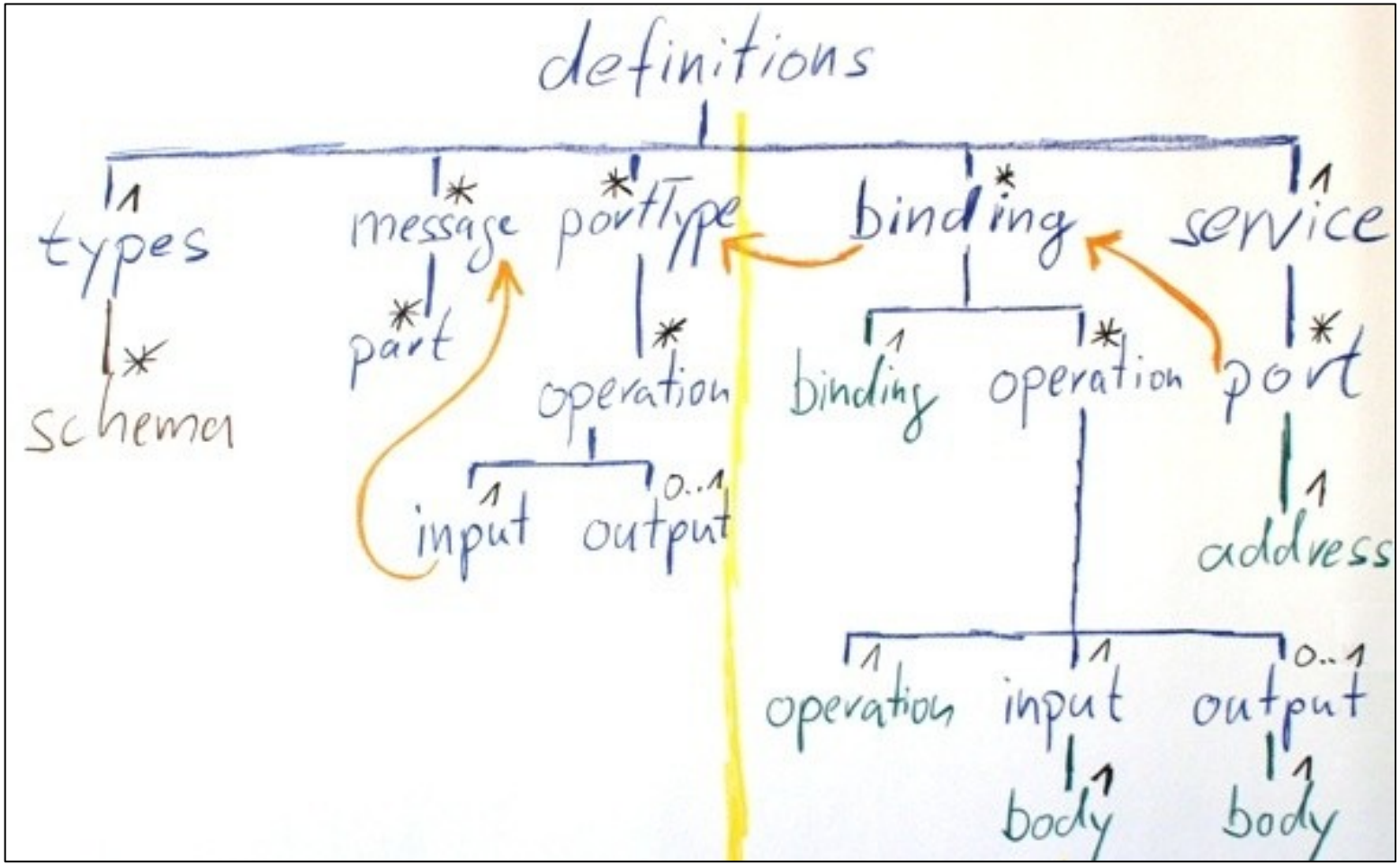


- WSDL est une grammaire XML permettant de décrire un Service Web.

- Le WSDL sert à décrire :
  - le format de messages requis pour communiquer avec ce service
  - les méthodes que le client peut invoquer
  - la localisation du service
  - le protocole de communication (SOAP RPC ou SOAP orienté message)

http://fr.wikipedia.org/wiki/Web_Services_Description_Language

WSDL



http://predic8.com/wsdl-reading.htm

WSDL: exemple

```
- <wsdl:definitions targetNamespace="http://thomas-bayer.com/blz/">
    <wsdl:documentation>BLZService</wsdl:documentation>
  - <wsdl:types>
    - <xsd:schema targetNamespace="http://thomas-bayer.com/blz/" attributeFormDefault="unqualified" elementFormDefault="qualified">
        <xsd:element name="getBank" type="tns:getBankType"/>
        <xsd:element name="getBankResponse" type="tns:getBankResponseType"/>
      - <xsd:complexType name="getBankType">
        - <xsd:sequence>
            <xsd:element name="blz" type="xsd:string"/>
          </xsd:sequence>
        </xsd:complexType>
      - <xsd:complexType name="getBankResponseType">
        - <xsd:sequence>
            <xsd:element name="details" type="tns:detailsType"/>
          </xsd:sequence>
        </xsd:complexType>
      - <xsd:complexType name="detailsType">
        - <xsd:sequence>
            <xsd:element name="bezeichnung" type="xsd:string" minOccurs="0"/>
            <xsd:element name="bic" type="xsd:string" minOccurs="0"/>
            <xsd:element name="ort" type="xsd:string" minOccurs="0"/>
            <xsd:element name="plz" type="xsd:string" minOccurs="0"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:schema>
  </wsdl:types>
- <wsdl:message name="getBank">
    <wsdl:part element="tns:getBank" name="parameters"/>
  </wsdl:message>
- <wsdl:message name="getBankResponse">
    <wsdl:part element="tns:getBankResponse" name="parameters"/>
  </wsdl:message>
- <wsdl:portType name="BLZServicePortType">
  - <wsdl:operation name="getBank">
      <wsdl:input message="tns:getBank"/>
      <wsdl:output message="tns:getBankResponse" wsaw:Action="http://thomas-bayer.com/blz/BLZService/getBankResponse"/>
    </wsdl:operation>
  </wsdl:portType>
```

SOAP: Démystification des protocoles

Découverte	UDDI
Description	WSDL
Message	SOAP / XML
Protocole	HTTP, HTTPS, FTP, SFTP, SMS, SMTP (TCP or UDP)
Transport	IP

Agenda

- Qu’est-ce qu’un Web Service ?
- SOAP
- REST
- Threat Modeling / ACME SA
- Réduction des risques
- Conclusion
- Questions

REST: Démystification des technologies

- Langages
  - XML
  - JSON
  - XHTML, HTML, PDF... as data formats
- Protocoles
  - HTTP(s) → Utilisation d'une URL
  - Méthode de communication (GET, POST, PUT, DELETE)
- Sécurité
  - Sécurité du transport (SSL/TLS)
  - Sécurité des messages: HMAC / Doseta / JWS, etc. (Like XML Signature)
- Autres éléments
  - Oauth, API Keys, etc.

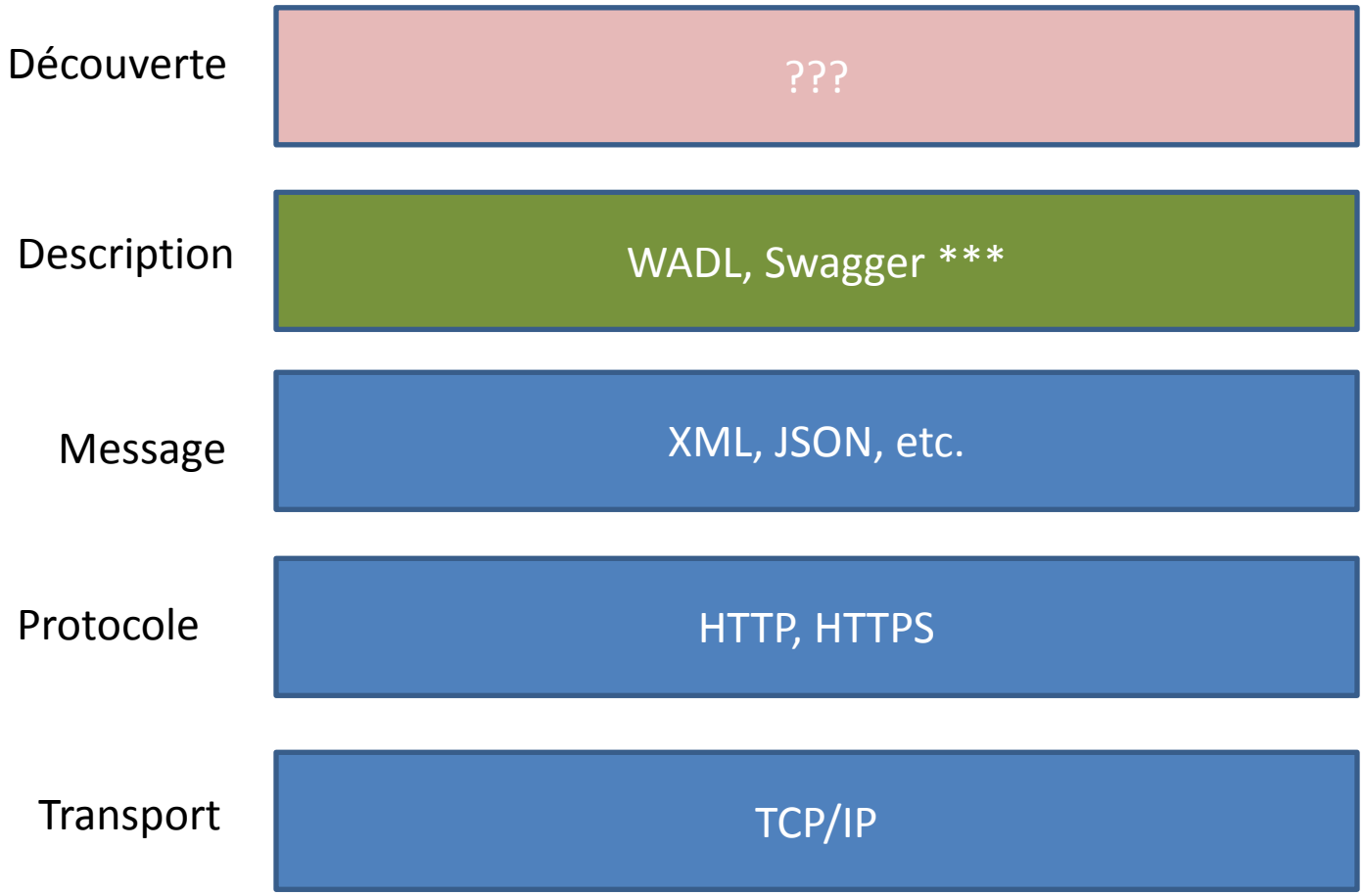
Représentation REST (exemple JSON)


```
{
   "results":    [
            {
         "profile_image_url": "http://a3.twimg.com/profile_images/97541875/t
         "created_at": "Fri, 28 May 2010 22:08:32 +0000",
         "from_user": "tibcommunity",
         "metadata": {"result_type": "recent"},
         "to_user_id": null,
         "text": "Automated tools for Integration Test?: I would go for soap
         "id": 14935096312,
         "from_user_id": 7363121,
         "geo": null,
         "iso_language_code": "en",
         "source": "&lt;a href=&quot;http://twitterfeed.com&quot; rel=&quot,
      },
            {
         "profile_image_url": "http://s.twimg.com/a/1274899949/images/defaul
         "created_at": "Fri, 28 May 2010 15:50:10 +0000",
         "from_user": "onion_soup",
```

Méthodes REST

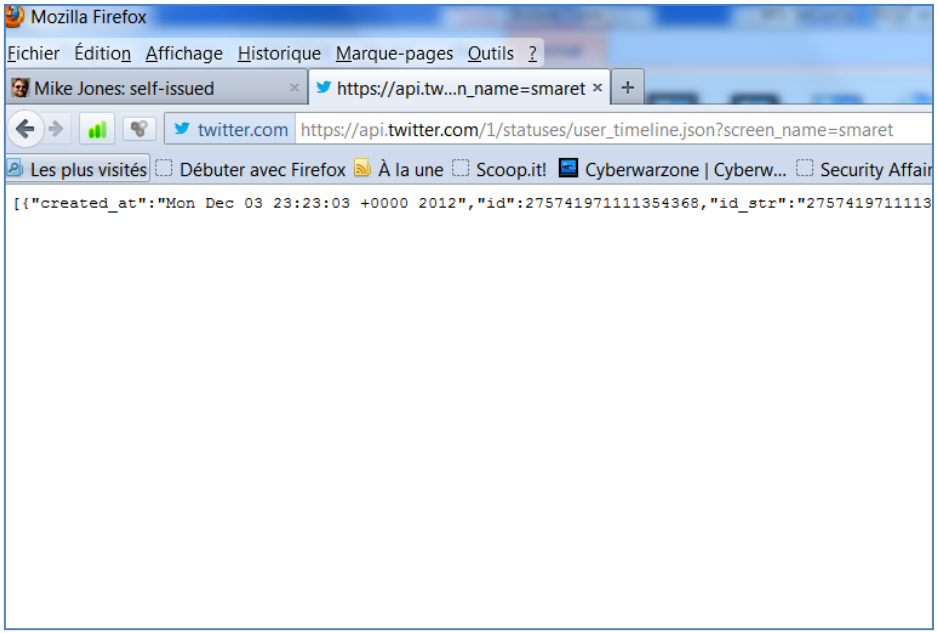
HTTP Method	Think	Description	/proc analogy
PUT	CREATE	Create a resource with the user specified id	Start a new process
GET	RETRIEVE	Retrieve a resource representation	Get the status of a process
POST	UPDATE	Update a resource/Append to a resource/Create a resource with a server assigned id	Amend a process
DELETE	DELETE	Delete a resource	Kill a process

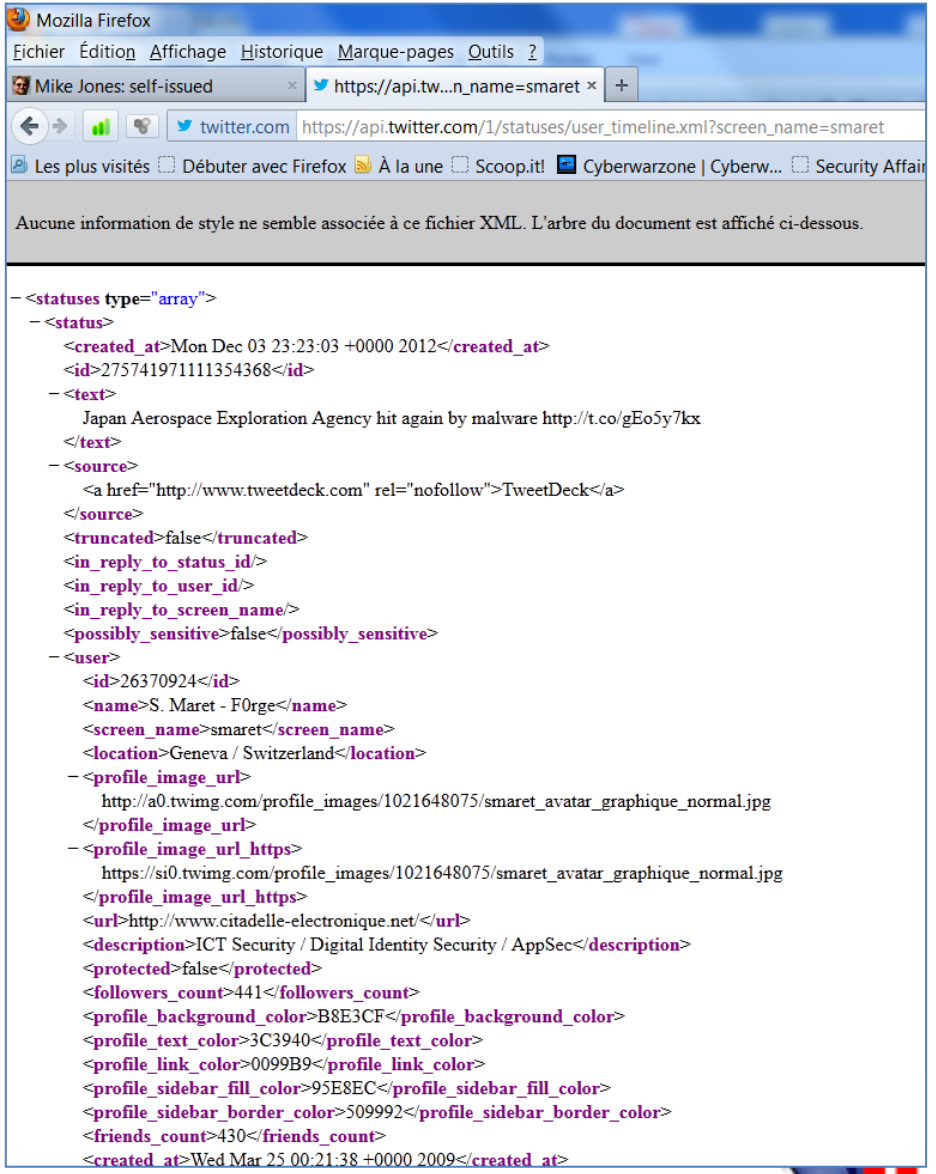
REST: Démystification des protocoles



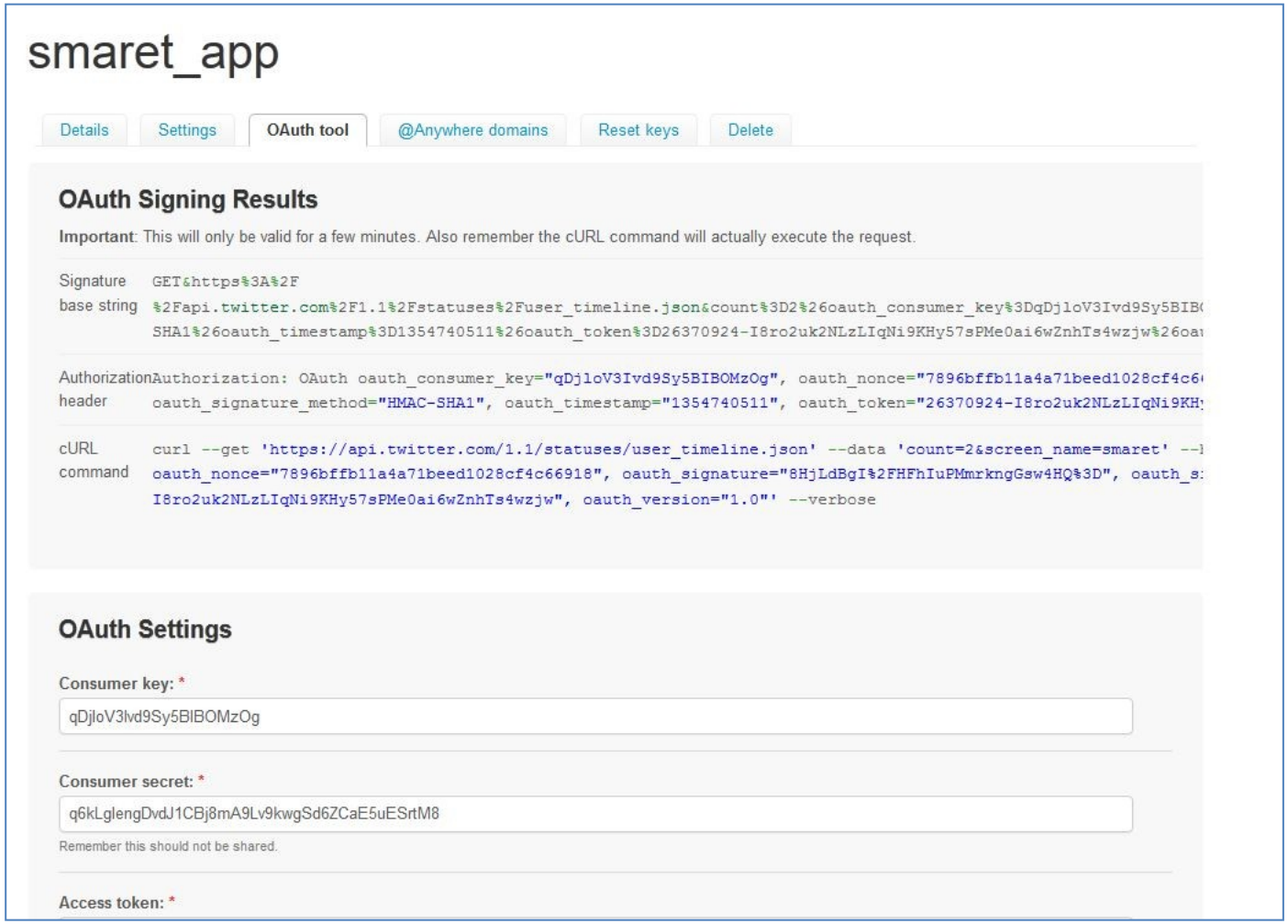
*** *Avant-gardiste!*

Example


Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Mike Jones: self-issued
https://api.tw...n_name=smaret
twitter.com
https://api.twitter.com/1/statuses/user_timeline.json?screen_name=smaret
Les plus visités
Débuter avec Firefox
À la une
Scoop.it!
Cyberwarzone | Cyberw...
Security Affair
[{"created_at":"Mon Dec 03 23:23:03 +0000 2012","id":275741971111354368,"id_str":"2757419711113

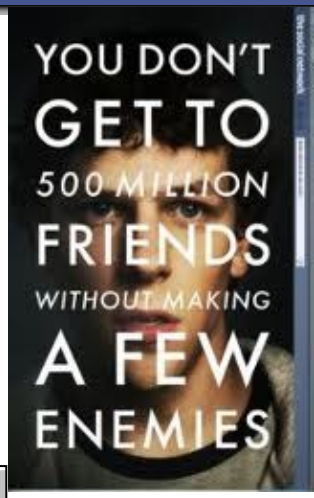

Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Mike Jones: self-issued
https://api.tw...n_name=smaret
twitter.com
https://api.twitter.com/1/statuses/user_timeline.xml?screen_name=smaret
Les plus visités
Débuter avec Firefox
À la une
Scoop.it!
Cyberwarzone | Cyberw...
Security Affair
Aucune information de style ne semble associée à ce fichier XML. L'arbre du document est affiché ci-dessous.
<statuses type="array">
<status>
<created_at>Mon Dec 03 23:23:03 +0000 2012</created_at>
<id>275741971111354368</id>
<text>
Japan Aerospace Exploration Agency hit again by malware http://t.co/gEo5y7kx
</text>
<source>
TweetDeck
</source>
<truncated>false</truncated>
<in_reply_to_status_id/>
<in_reply_to_user_id/>
<in_reply_to_screen_name/>
<possibly_sensitive>false</possibly_sensitive>
<user>
<id>26370924</id>
<name>S. Maret - F0rge</name>
<screen_name>smaret</screen_name>
<location>Geneva / Switzerland</location>
<profile_image_url>
http://a0.twimg.com/profile_images/1021648075/smaret_avatar_graphique_normal.jpg
</profile_image_url>
<profile_image_url_https>
https://si0.twimg.com/profile_images/1021648075/smaret_avatar_graphique_normal.jpg
</profile_image_url_https>
<url>http://www.citadelle-electronique.net/</url>
<description>ICT Security / Digital Identity Security / AppSec</description>
<protected>false</protected>
<followers_count>441</followers_count>
<profile_background_color>B8E3CF</profile_background_color>
<profile_text_color>3C3940</profile_text_color>
<profile_link_color>0099B9</profile_link_color>
<profile_sidebar_fill_color>95E8EC</profile_sidebar_fill_color>
<profile_sidebar_border_color>509992</profile_sidebar_border_color>
<friends_count>430</friends_count>
<created_at>Wed Mar 25 00:21:38 +0000 2009</created_at>

Example Twitter (OAuth)



REST web service API's

SOAP vs REST



Web services in the Enterprise

- Enterprise integration (EI) background
- SOAP, WSDL, UDDI
- Sophisticated infrastructure available today

- Web background
- Web API, SAAS,Cloud
- Lightweight

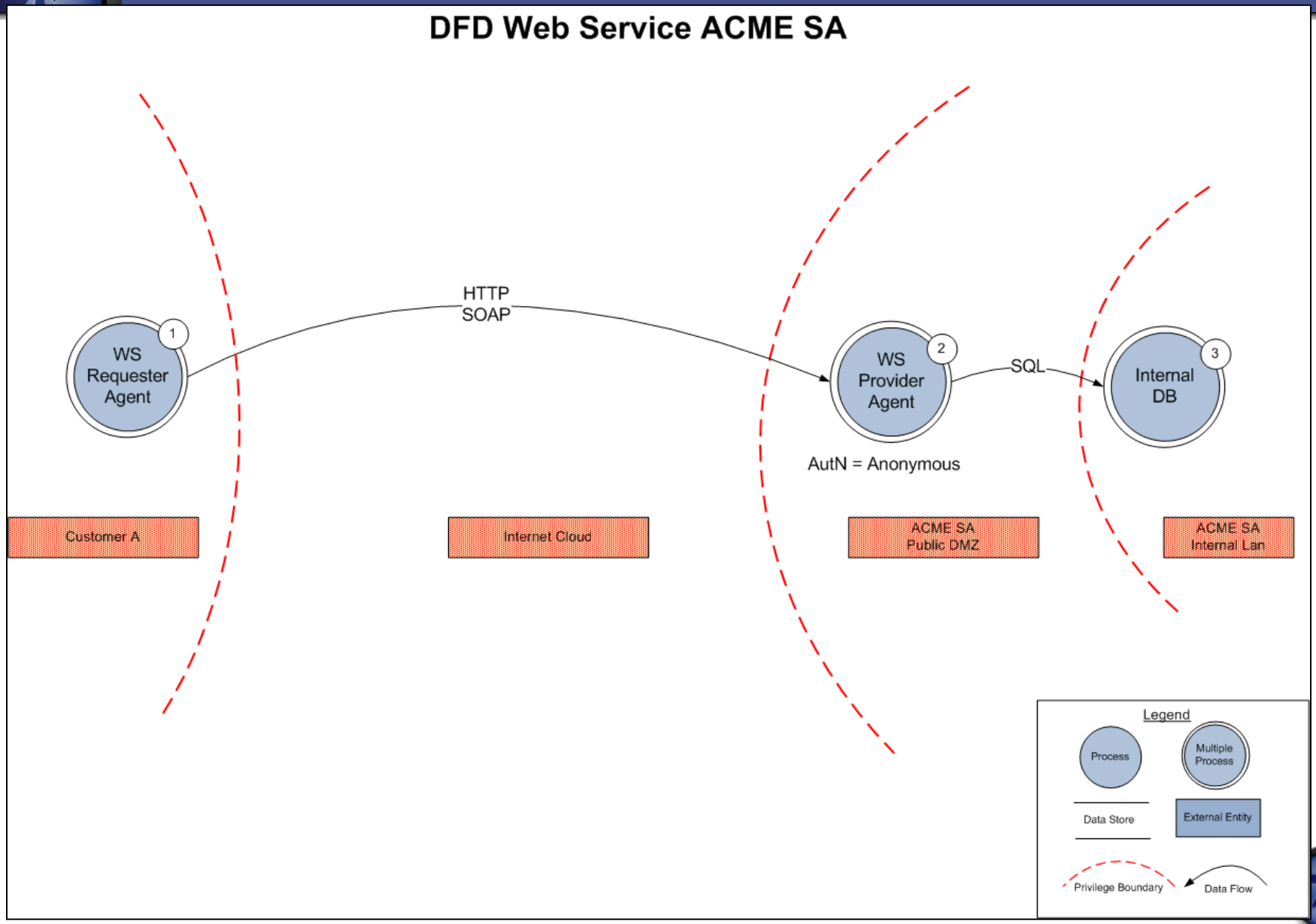
WS-*

RESTful

service orientation enablers (both styles matter)

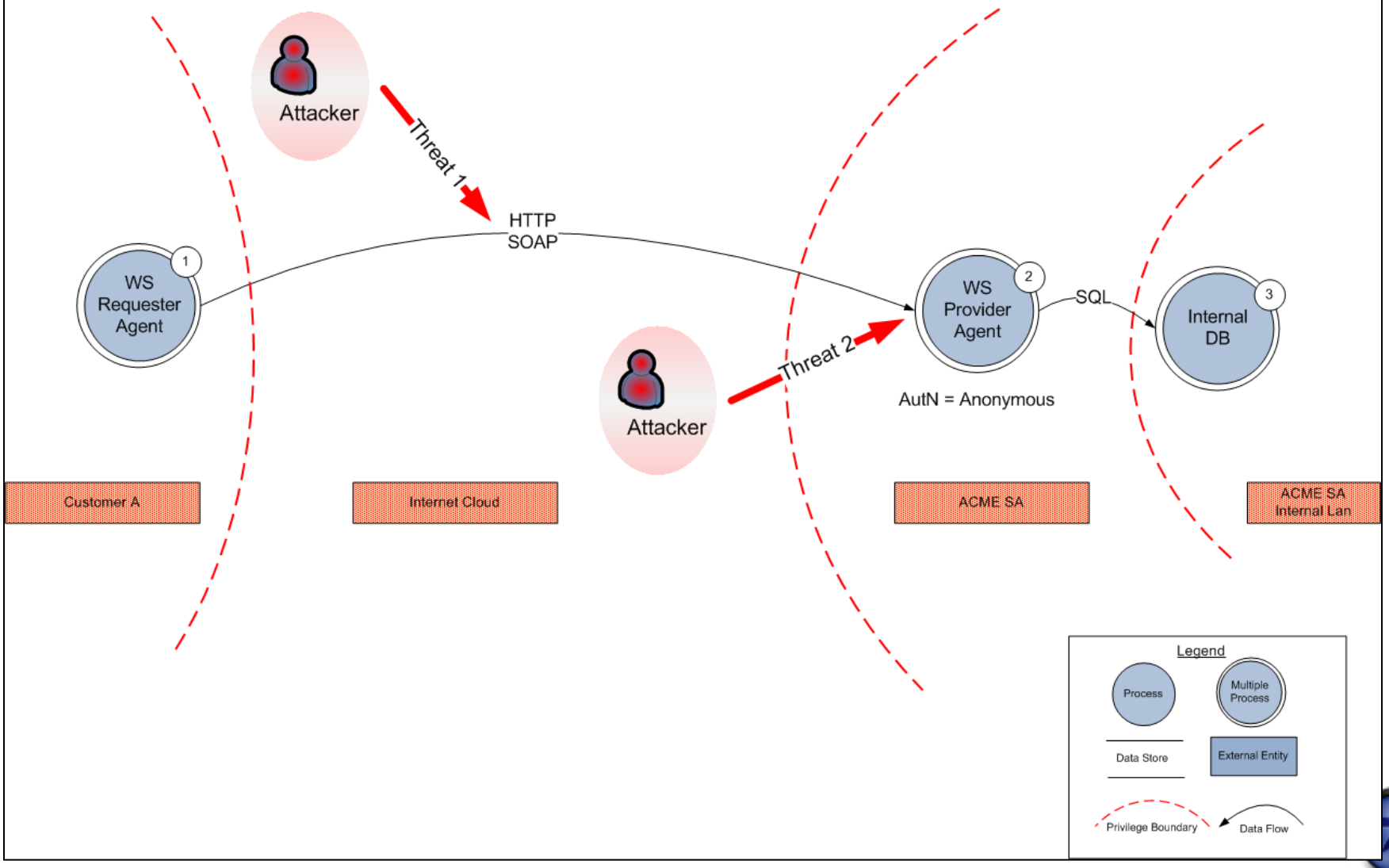
Agenda

- Qu’est-ce qu’un Web Service ?
- SOAP
- REST
- Threat Modeling / ACME SA
- Réduction des risques
- Conclusion
- Questions



http://fr.wikipedia.org/wiki/Diagramme_de_flux_de_donn%C3%A9es

DFD Web Service ACME SA
Threat Modeling



Modèle STRIDE

STRIDE Threat List		
Type	**Examples**	**Security Control**
Spoofing	Threat action aimed to illegally access and use another user's credentials, such as username and password.	Authentication
Tampering	Threat action aimed to maliciously change/modify persistent data, such as persistent data in a database, and the alteration of data in transit between two computers over an open network, such as the Internet.	Integrity
Repudiation	Threat action aimed to perform illegal operations in a system that lacks the ability to trace the prohibited operations.	Non-Repudiation
Information disclosure	Threat action to read a file that one was not granted access to, or to read data in transit.	Confidentiality
Denial of service	Threat aimed to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of privilege	Threat aimed to gain privileged access to resources for gaining unauthorized access to information or to compromise a system.	Authorization

https://www.owasp.org/index.php/Application_Threat_Modeling

Menaces - DFD Acme SA

- Threat 1
  - Interception des messages (Information disclosure)
  - Modification des messages (Tampering)
  - Usurpation d'identité (Spoofing)
- Threat 2
  - Attaque de l'application
    - BoF
    - Injection
    - DoS & DDoS
    - Etc

Agenda

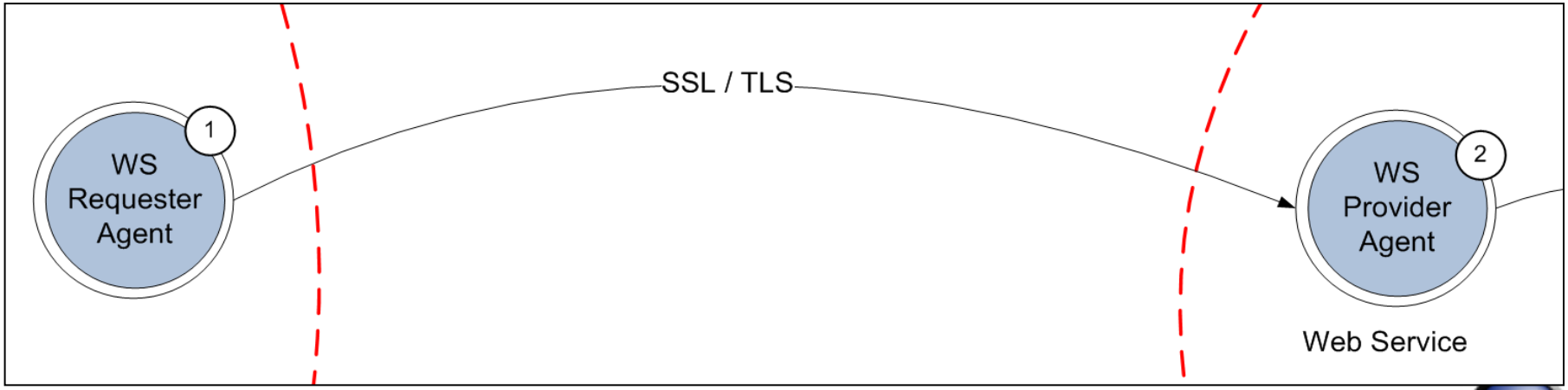
- Qu’est-ce qu’un Web Service ?
- SOAP
- REST
- Threat Modeling / ACME SA
- Réduction des risques
- Conclusion
- Questions

ACME SA: Réduction des risques ?

- Chiffrement du transport
- AuthN
- SSL Mutual AuthN / X509
- WAF / XML Gateway
- Intégrité et confidentialité des messages
- Secure Coding

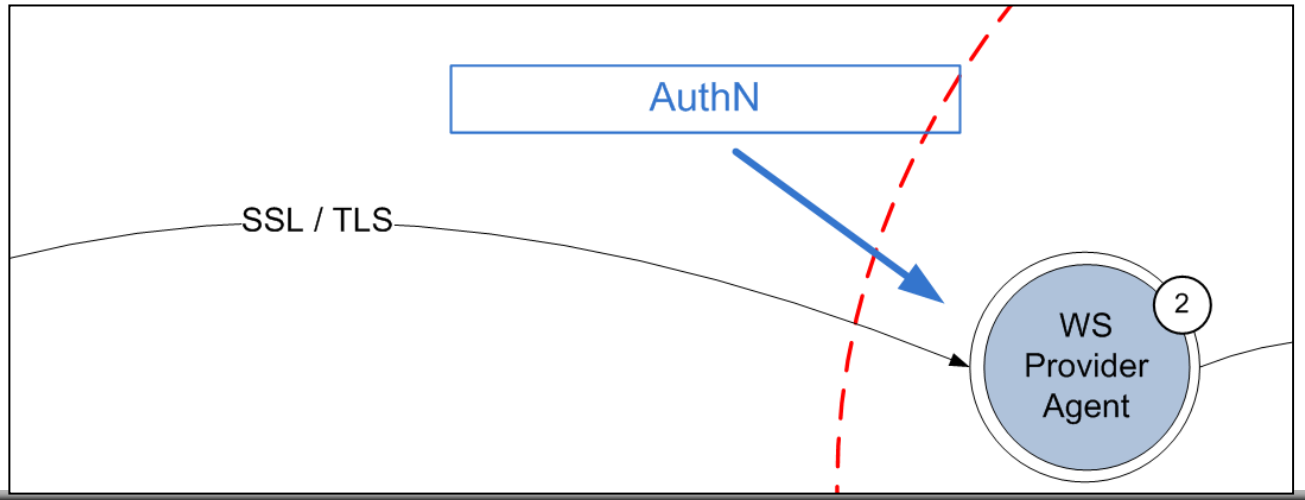
Chiffrement du transport

SOAP / XML	REST
HTTPS SSL/TLS tunnel SSH IPSEC Etc.	HTTPS



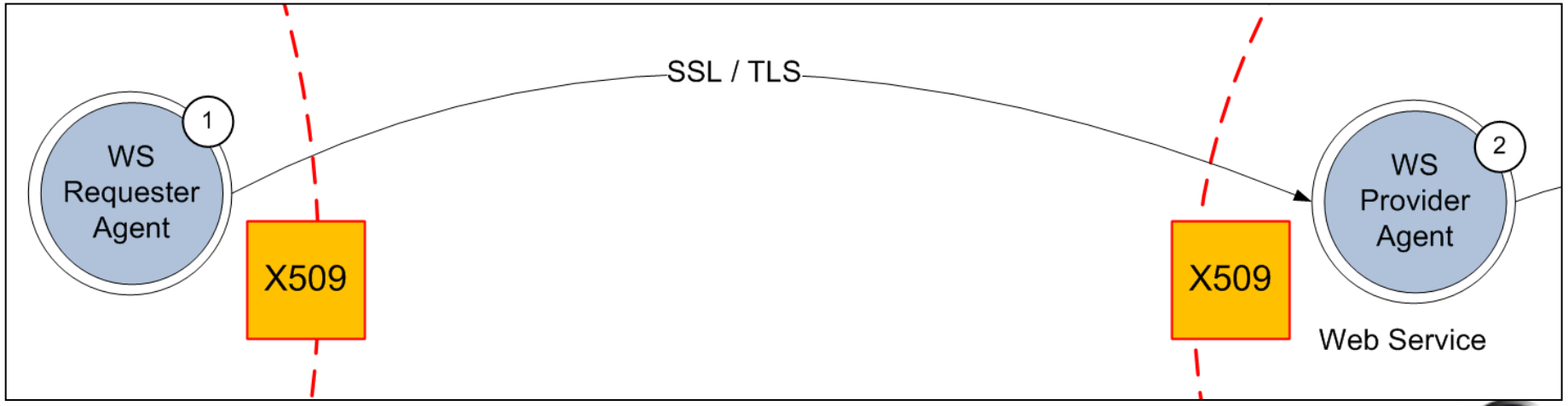
AuthN

SOAP / XML	REST
HTTP Basic, Digest, HTTP Header Mutual SSL IP trust WS Security user name password WS SAML Authentication token XML Signature Kerberos Etc.	HTTP Basic, Digest, HTTP Header Mutual SSL IP trust Oauth API Keys JSON Web Token (JWT)



SSL Mutual AuthN / X509 / PKI

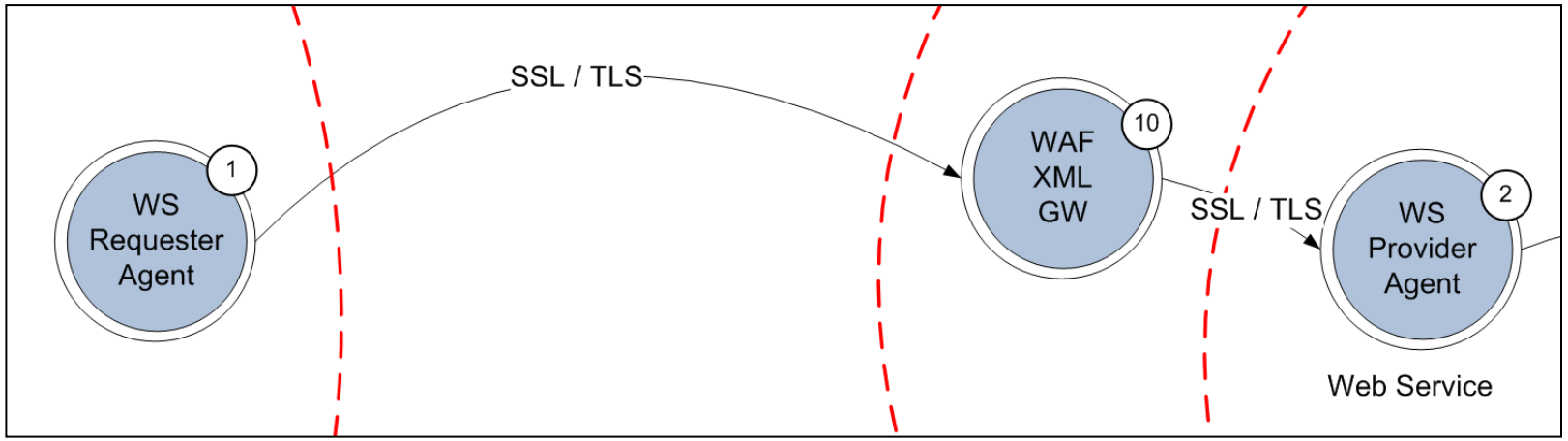
SOAP / XML	REST
SSL/TLS Mutual AuthN**	SSL/TLS Mutual AuthN**



** Man in the middle not possible… (As I Know)

WAF / XML Gateway (Protection périmétrique)

SOAP / XML	REST
Reverse Proxy Contrôle requêtes HTTP Rupture SSL/TLS Black List White List Validation WSDL Signature & Verification Encryption & Decryption SAML	Reverse Proxy Contrôle requêtes HTTP Rupture SSL/TLS Black List White List



Intégrité et confidentialité des messages

SOAP / XML	REST
XML Signature XML Encryption	•(p.ex: HMAC, Doseta) • JSON Web Signature (JWS) – Draft v7 • JSON Web Encryption

```
01. POST /resources/rest/geo/comment HTTP/1.1[\r][\n]
02. hmac: jos:+9tn0CLfxXFbzPmbYwq/KYuUSUI=[\r][\n]
03. Date: Mon, 26 Mar 2012 21:34:33 CEST[\r][\n]
04. Content-Md5: r52FDQv6V2GHN4neZBvXLQ==[\r][\n]
05. Content-Length: 69[\r][\n]
06. Content-Type: application/vnd.geo.comment+json; charset=UTF-8[\r][\n]
07. Host: localhost:9000[\r][\n]
08. Connection: Keep-Alive[\r][\n]
09. User-Agent: Apache-HttpClient/4.1.3 (java 1.5)[\r][\n]
10. [\r][\n]
11. {"comment" : {"message":"blaat" , "from":"blaat" , "commentFor":123}}
```

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/enve
        <SOAP-ENV:Header><wsse:Security><wsse:UsernameToken wsu:Id="Se
        <SOAP-ENV:Body wsu:Id="Id-9027040566202249815">
                <dss:SignRequest xmlns:css="http://www.safelayer.com/T
                <dss:OptionalInputs><dss:KeySelector><css:KeySelector>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

http://tools.ietf.org/html/draft-ietf-jose-json-web-signature-07

** Pas de chiffrement à ma connaissance

Example XML Signature (SOAP)

Demande

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap
  <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-2


    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id-
tBBsJX0YlMS81fXsuPEAXR3Grq9F8VvNLpRpVmN+CRTH/ffPof5zSMsrmLwMg9rX
5rZI66D6WG3nqVaZAYX8f33hri46i4wESkPVCWLXwmfid+W84ycwKJ00CLhC7Kvg
UqagXeVWDAbvJEab/NEP9ZSr/c7eB6axLWcd0QbZD9FSn2Y7CBQWNxO9bP7ovYyb
oYrcgY1czNHuZNU88NhClBHqIcXQtmW5Yzcwj0rRKfrw/LGzcM0JlfR4SaaHIi4y
PxRJuIFC6mbzHgoBvUX+zQ==</dsig:SignatureValue><dsig:KeyInfo Id="Id-00013547
  </wsse:Security>
  </soap:Header>

<soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-w
<ns:echo xmlns:ns="http://ws.apache.org/axis2">
<!-- Zero or one occurrences -->
<ns:args0>a</ns:args0>
</ns:echo>
</soap:Body>
</soap:Envelope>
```

Example JSON “Signature”

A.1. JWS using HMAC SHA-256

A.1.1. Encoding

The following example JWS Header declares that the data structure is a JSON Web Token (JWT) **[JWT]** and the JWS Secured Input is se

```
{"typ":"JWT",
 "alg":"HS256"}
```

The following byte array contains the UTF-8 representation of the JWS Header:

[123, 34, 116, 121, 112, 34, 58, 34, 74, 87, 84, 34, 44, 13, 10, 32, 34, 97, 108, 103, 34, 58, 34, 72, 83, 50, 53, 54, 34, 125]

Base64url encoding these bytes yields this Encoded JWS Header value:

```
eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9
```

The JWS Payload used in this example is the bytes of the UTF-8 representation of the JSON object below. (Note that the payload can be
base64url encoded JSON object.)

```
{"iss":"joe",
 "exp":1300819380,
 "http://example.com/is_root":true}
```

The following byte array, which is the UTF-8 representation of the JSON object above, is the JWS Payload:

[123, 34, 105, 115, 115, 34, 58, 34, 106, 111, 101, 34, 44, 13, 10, 32, 34, 101, 120, 112, 34, 58, 49, 51, 48, 48, 56, 49, 57, 51, 56, 4
109, 112, 108, 101, 46, 99, 111, 109, 47, 105, 115, 95, 114, 111, 111, 116, 34, 58, 116, 114, 117, 101, 125]

Base64url encoding the above yields the Encoded JWS Payload value (with line breaks for display purposes only):

```
eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt
```

Code security

SOAP / XML	REST
- Data input validation - Data output encoding - Pseudorandom data generation, high entropy - Strong / reliable data encryption algorithms - Data leakage prevention - Robust error & exception handling - Anti-automation and expiration measures	- Data input validation - Data output encoding - Pseudorandom data generation, high entropy - Strong / reliable data encryption algorithms - Data leakage prevention - Robust error & exception handling - Anti-automation and expiration measures

OWASP Application Security Verification Standard (ASVS):
https://www.owasp.org/index.php/ASVS

WASC web application weaknesses:
http://projects.webappsec.org/w/page/13246978/Threat%20Classification

Agenda

- Qu’est-ce qu’un Web Service ?
- SOAP
- REST
- Threat Modeling / ACME SA
- Réduction des risques
- Conclusion
- Questions

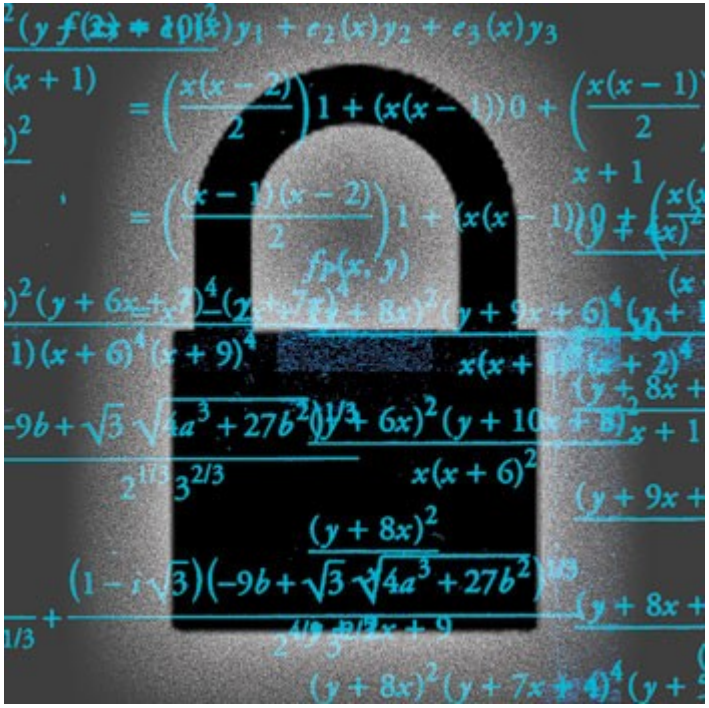
Conclusion

- SOAP:
  - Implémenter les standards WS-* liés à la sécurité?
  - Mettre en place un filtrage applicatif (WAF, XML GW)
  - Complexe à mettre en œuvre (PKI, Secure coding, Cryptography, etc.)
  - Architecture à forte contrainte de sécurité

- REST
  - Mettre en place un filtrage applicatif (WAF, XML GW)
  - Implémentation rapide et facile → tendance
  - Architecture de type Cloud, Intranet, Social Login, etc.
  - Emergence des standards (JSON Web Algorithms)

- On attend avec impatience les standards sécu pour REST ???
  - Pragmatique: protection périmétrique, chiffrement et Secure Coding ???

Approche périmétrique vs WS-Security ?



Questions?

Merci / Thank you!

Contact:

sma@maret-consulting.ch

@smaret

http://www.maret-consulting.ch

Slides:

http://slideshare.net/ASF-WS/

Backup Slides

By Sylvain Maret

MIKE JONES: SELF-ISSUED

Musings on Digital Identity

HOME ABOUT

SEARCH

Go

CATEGORIES

Bandit Project
Claims
Cryptography
Documentation
Events
Federation
Firefox
Higgins Project
I-names
Information Cards
Interoperability
JanRain
JSON
LiveID
OAuth
OpenID
Pamela Project
People
Phishing Resistance
Privacy
Safety
Shibboleth
Software
Specifications

« Simple Web Discovery (SWD) Enabling Hosted Deployments

OAuth 2.0 Multiple Response Type Encoding Practices »

JOSE and JWT specs updated for IETF 85 working group meetings

NOVEMBER 8, 2012

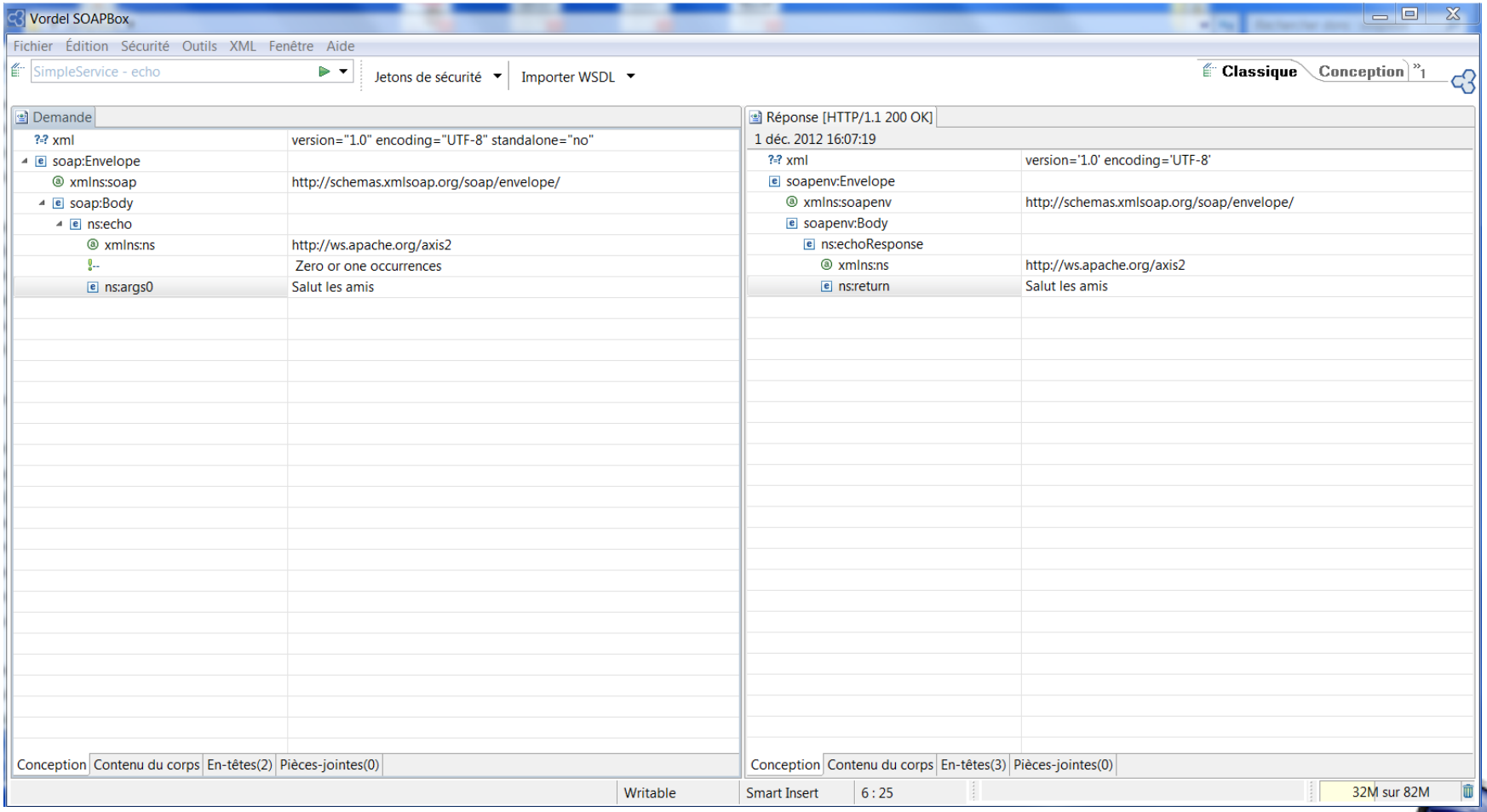
I've made a small set of updates to the JSON Object Signing and Encryption (JOSE) and JSON Web Token (JWT) specs in preparation for the JOSE and OAuth working group meetings at IETF 85. These updates incorporate resolutions to issues that have been discussed by the working groups since publication of the previous drafts.

Normative changes to the working group specs were to add length fields for PartyUInfo and PartyVInfo values for key derivation calculations and to change the JWK field identifiers for RSA keys from (mod, xpo) to (n, e). Fields for representing the RSA private key values needed for Chinese Remainder Theorem (CRT) calculations were added to the JSON Private Key specification.

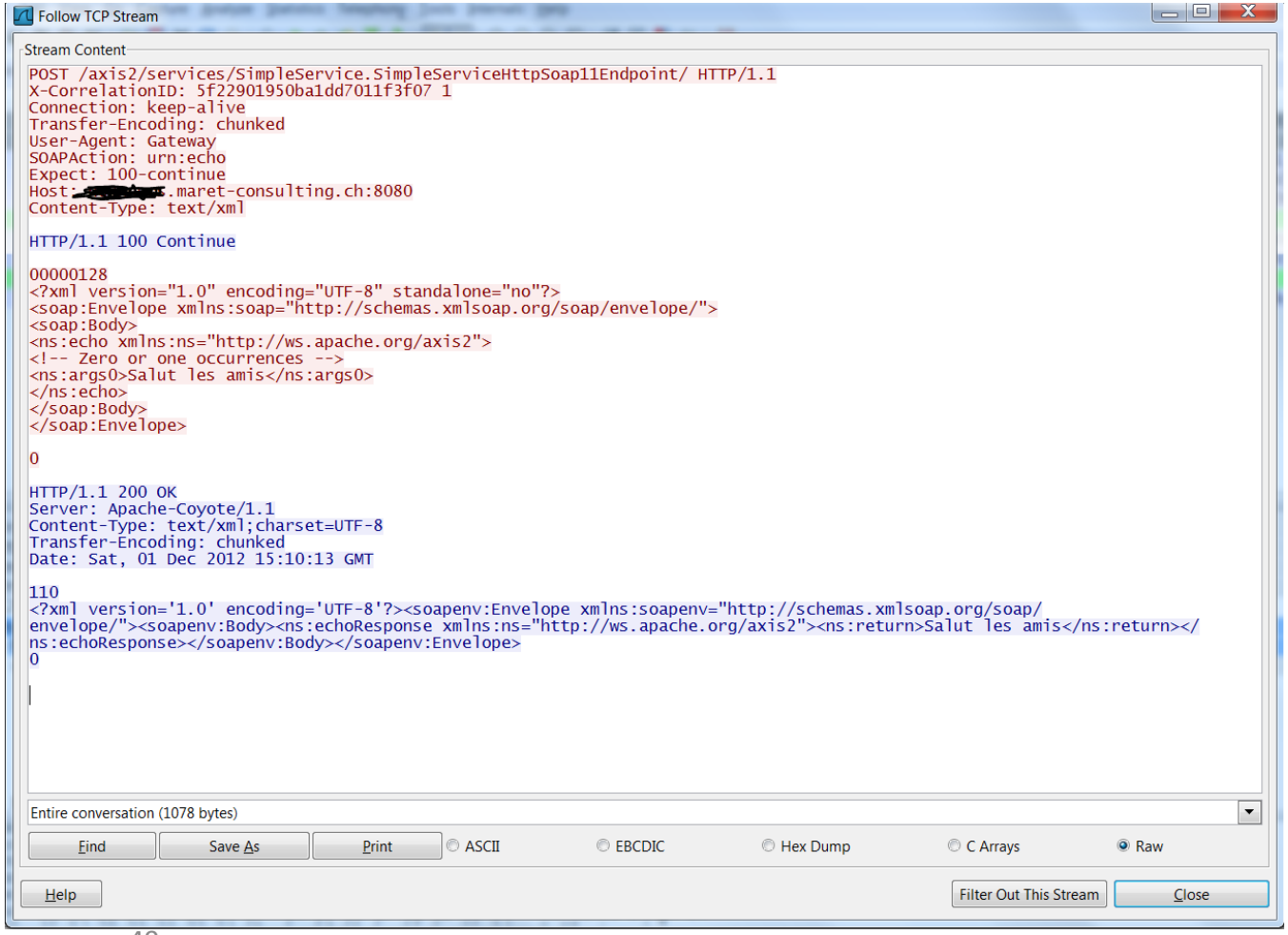
The updated specs are available at:

http://tools.ietf.org/html/draft-ietf-jose-json-web-signature-07
http://tools.ietf.org/html/draft-ietf-jose-json-web-encryption-07
http://tools.ietf.org/html/draft-ietf-jose-json-web-key-07
http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms-07
http://tools.ietf.org/html/draft-ietf-oauth-json-web-token-05
http://tools.ietf.org/html/draft-ietf-oauth-jwt-bearer-03
http://tools.ietf.org/html/draft-jones-jose-jws-json-serialization-03
http://tools.ietf.org/html/draft-jones-jose-jwe-json-serialization-03
http://tools.ietf.org/html/draft-jones-jose-json-private-key-01

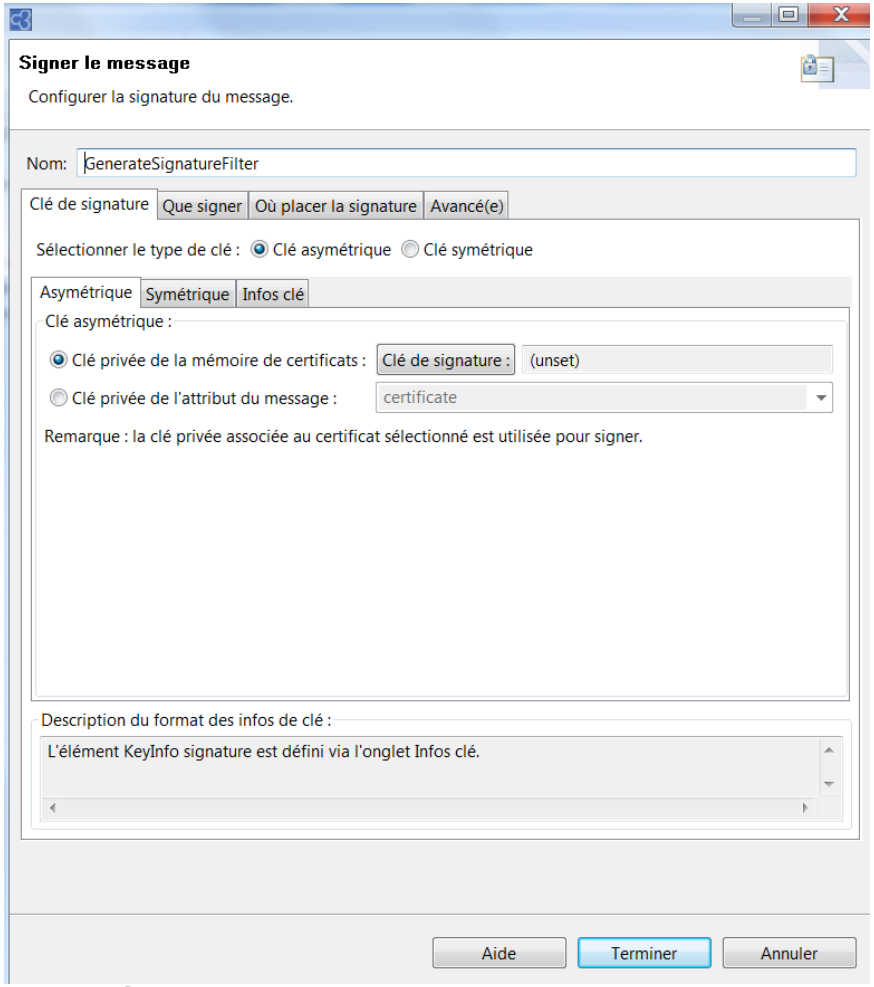
SoapBox

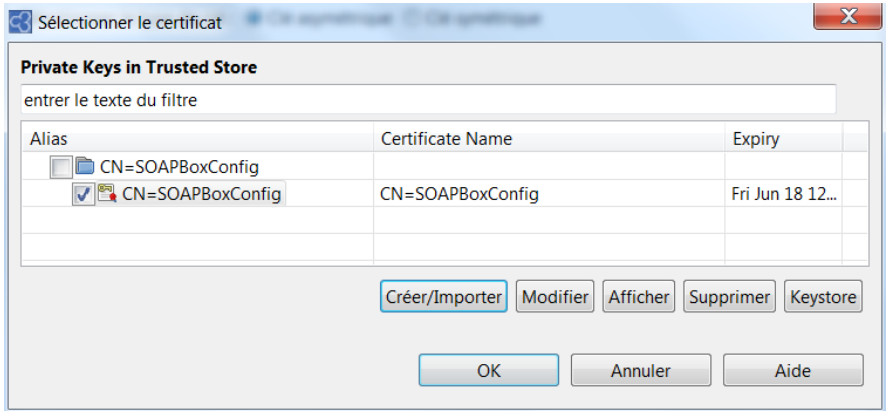

Vordel SOAPBox
Fichier Édition Sécurité Outils XML Fenêtre Aide
SimpleService - echo
Jetons de sécurité
Importer WSDL
Classique
Conception
Demande
xml
version="1.0" encoding="UTF-8" standalone="no"
soap:Envelope
xmlns:soap
http://schemas.xmlsoap.org/soap/envelope/
soap:Body
ns:echo
xmlns:ns
http://ws.apache.org/axis2
Zero or one occurrences
ns:args0
Salut les amis
Conception
Contenu du corps
En-têtes(2)
Pièces-jointes(0)
Réponse [HTTP/1.1 200 OK]
1 déc. 2012 16:07:19
xml
version='1.0' encoding='UTF-8'
soapenv:Envelope
xmlns:soapenv
http://schemas.xmlsoap.org/soap/envelope/
soapenv:Body
ns:echoResponse
xmlns:ns
http://ws.apache.org/axis2
ns:return
Salut les amis
Conception
Contenu du corps
En-têtes(3)
Pièces-jointes(0)
Writable
Smart Insert
6 : 25
32M sur 82M

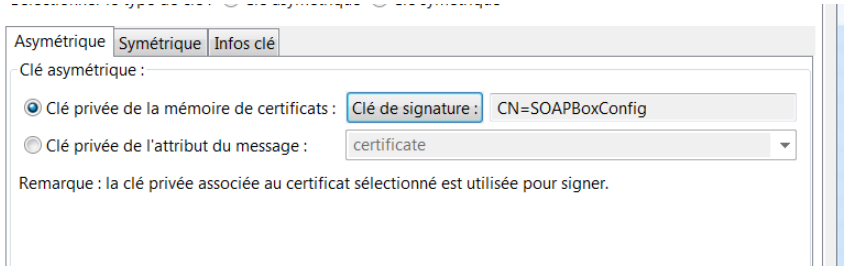
Capture HTTP



Signer le message







Signer le message

Demande

xml	version="1.0" encoding="UTF-8" standalone="no"
soap:Envelope	
xmlns:soap	http://schemas.xmlsoap.org/soap/envelope/
soap:Header	
wsse:Security	
xmlns:wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
dsig:Signature	
xmlns:dsig	http://www.w3.org/2000/09/xmldsig#
Id	Id-0001354375296344-2ce605b050ba208001050000-3
dsig:SignedInfo	
dsig:CanonicalizationMe	
Algorithm	http://www.w3.org/2001/10/xml-exc-c14n#
dsig:SignatureMethod	
Algorithm	http://www.w3.org/2000/09/xmldsig#rsa-sha1
dsig:Reference	
URI	#Id-0001354375296344-2ce605b050ba208001050000-2
dsig:Transforms	
dsig:Transform	
Algorithm	http://www.w3.org/2001/10/xml-exc-c14n#
dsig:DigestMethod	
Algorithm	http://www.w3.org/2000/09/xmldsig#sha1
dsig:DigestValue	FGocmKVuA8AXUurE4Gqh/qoLBK0=
dsig:SignatureValue	kR2y52mMeHL+ul9zgGfoh5Cd+X4+Jofz7Z2WTqr3WzPSu+/WfmNfY/RcTxIt1XEDwjDFmIn2jtrRQbp6j+GKIrYh8H
dsig:KeyInfo	
Id	Id-0001354375296344-2ce605b050ba208001050000-4
dsig:X509Data	
dsig:X509Certificate	MIIC0TCCAbmgAwIBAgIGATDa3Nm5MA0GCSqGSIb3DQEBBQUAMBgxFjAUBgNVBAMTDVNPQVBCb3hDb25m
soap:Body	
xmlns:wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
wsu:Id	Id-0001354375296344-2ce605b050ba208001050000-2
ns:echo	
xmlns:ns	http://ws.apache.org/axis2
--	Zero or one occurrences
ns:args0	a