

# Security and Privacy in Telecommunications and Information System (SePTIS)

December 16 - 19, 2007

Jiangong Jinjiang Hotel, Shanghai, China

In conjunction with The 3rd International IEEE Conference on

**SIGNAL-IMAGE TECHNOLOGY & INTERNET- BASED SYSTEMS**

## Interoperability between heterogeneous federation architectures: Illustration with SAML and WS-Federation

[mikael.ates@univ-st-etienne.fr](mailto:mikael.ates@univ-st-etienne.fr)

DIOM Laboratory – ISTASE School of Engineering  
University of Saint-Etienne - France



# Summary

---

Outline of Identity Federation

Overviews of SAML2 and WS-Federation1.1B

Interoperability between different architectures

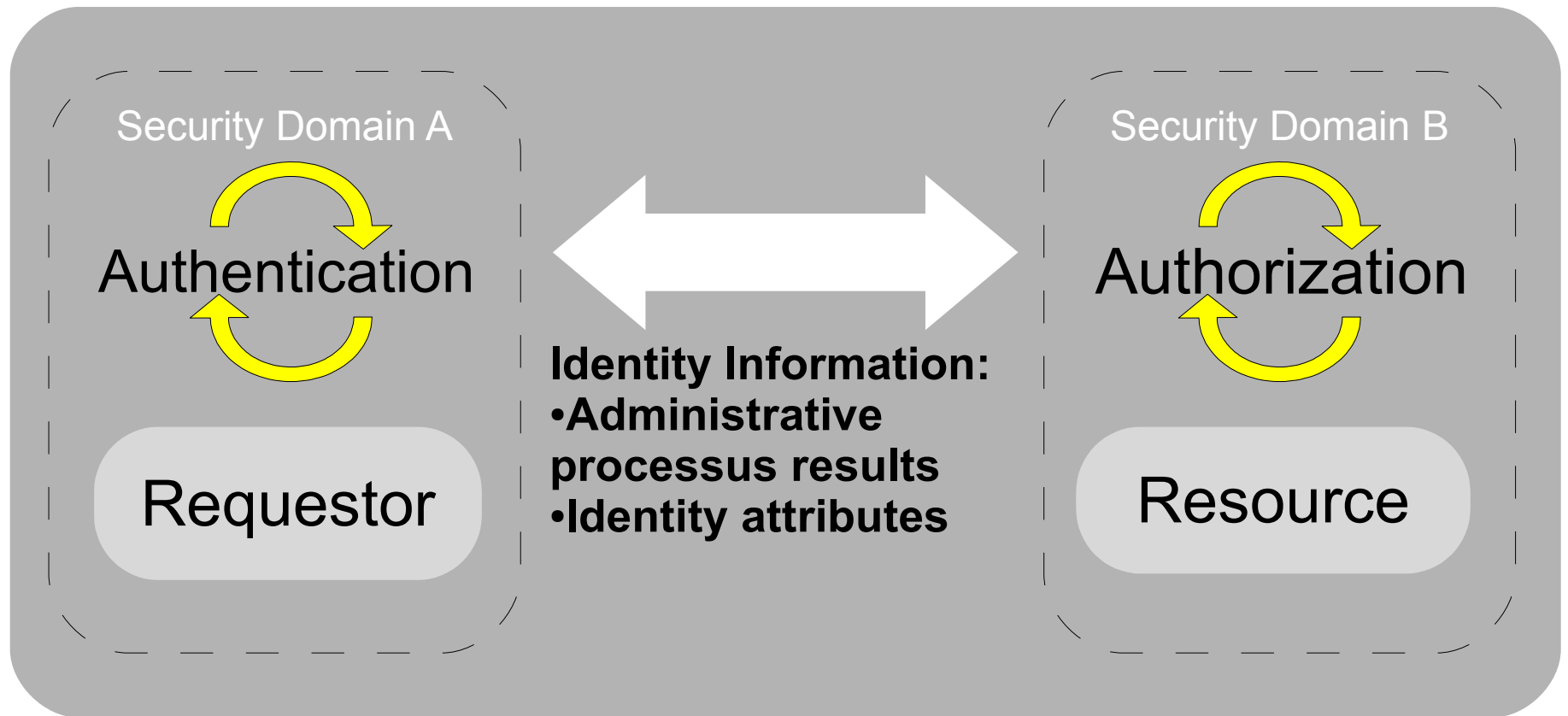
A way to make SAML2 and WS-Federation1.1B  
interoperate

The background of the slide is a teal-tinted photograph of a beach. The foreground is dominated by intricate, wavy ripples in the sand, created by wind or water. The ripples recede towards the horizon. In the distance, the ocean meets a sky filled with soft, white clouds. The overall color palette is monochromatic, consisting of various shades of teal and blue-green.

# Outline of Identity Federation

# Principle of Identity Federation

---



# Web Technologies and federation roles

---

**Resources** are provided by **Service Providers (SP)** (relying parties and assertion consumers) of two types:

- **Web applications**
- **Web services**

Which implies two types of **Requestors** (interfaces of a **Principal**):

- **Web Browser** (graphical interface of a principal: user)
- **Web Service consumer** (acting on behalf a principal: standalone application)

# Web Technologies and federation roles

---

Authorities are in charge:

- to perform the authentication process;
- to issue security informations:
  - the authentication process results;
  - the identity attributes of the principal.

# Security informations

---

An Identity Federation architecture is mainly a transport architecture of identity informations.

These informations are conveyed through the federation protocol in assertions or security tokens, issued by the authorities to the SP to make it perform the access control.

- If the information delivered by the authority is reusable (life time, renewable, etc), it is rather called token.
- If it is a one time information, it is rather called an assertion.

Tokens are generally used with active clients (enhanced web browser or standalone application) which allow their storage and reuse.

# Identity federation architecture

---

Provides two Main profiles, satisfied by the federation protocol:

- Authentication delegation and Session management on an authority, the Identity Provider (IP) which allows Single Signon and Single Logout;
- Attribute issuing. The service provider requests an authority, the Attribute Provider (AP), to obtain attributes or claims about a principal for access control and personalization purposes

# And...

---

Ensures privacy thanks use of pseudonyms.

Relies on federation metadata which allow the description of an entity, its role(s), endpoints and certificate, and provides a way for entities to exchange them easily.

Provides several bindings, mainly, HTTP redirections and SOAP over HTTP.

# Federation and trust

---


All the federation entities are trust linked and form a circle of trust.

The federation trust architecture is based on:

- pre-established lists of trusted entities (eg whitelist of trusted public key);
- common trusted third parties (eg a certification authority).

Security informations (messages) are signed to allow their authentication and if they come from a trusted party.

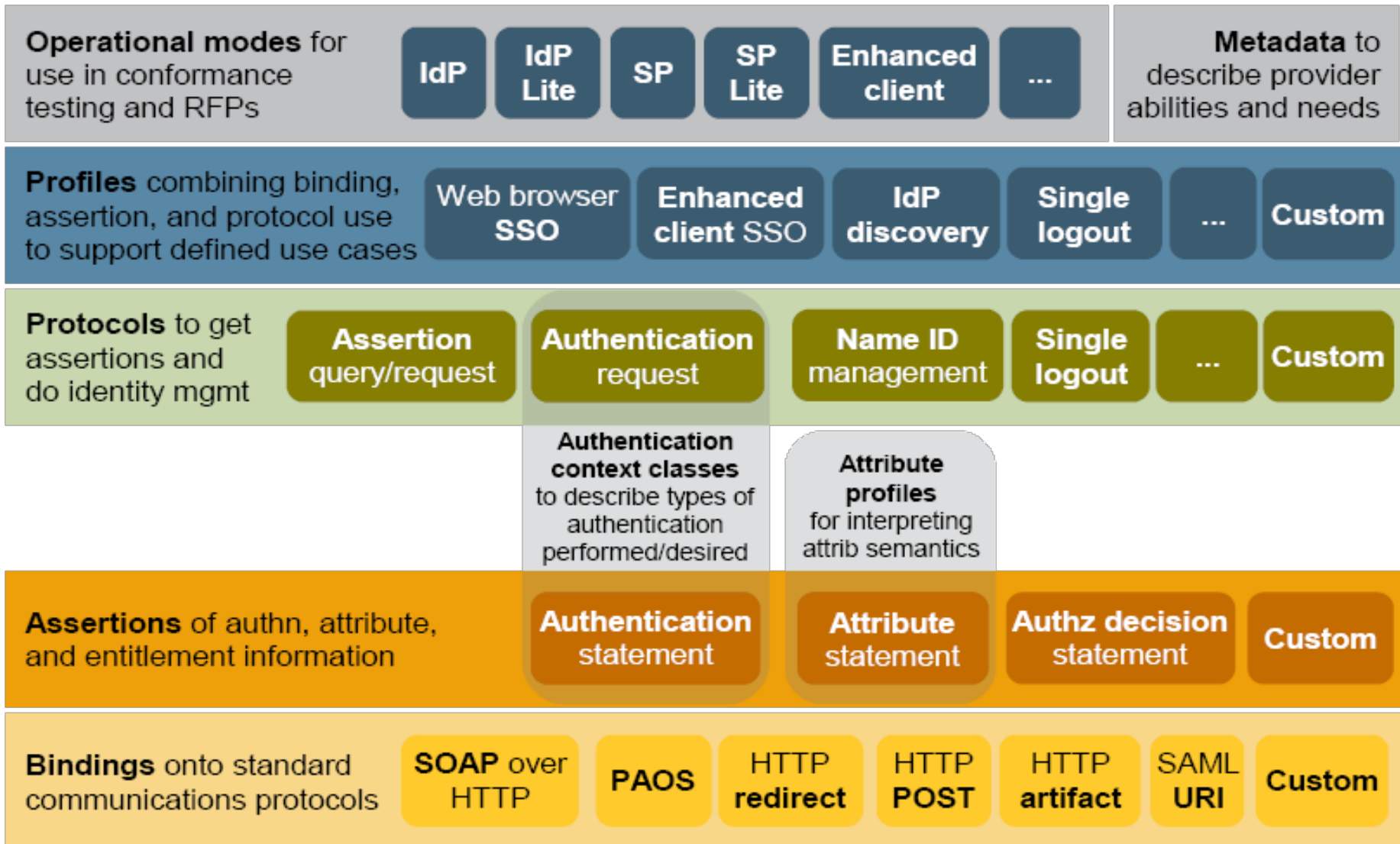
Transitive trust can be supported by two entities if they both trust a common third entity.

The background image is a teal-tinted landscape. The foreground shows a wide expanse of sand with intricate, wavy ripples that recede towards the horizon. The sky is filled with soft, layered clouds, creating a textured, atmospheric effect. The overall color palette is monochromatic, consisting of various shades of teal and blue-green.

# Overview SAML2 and WS-Federation1.1B

# SAML2

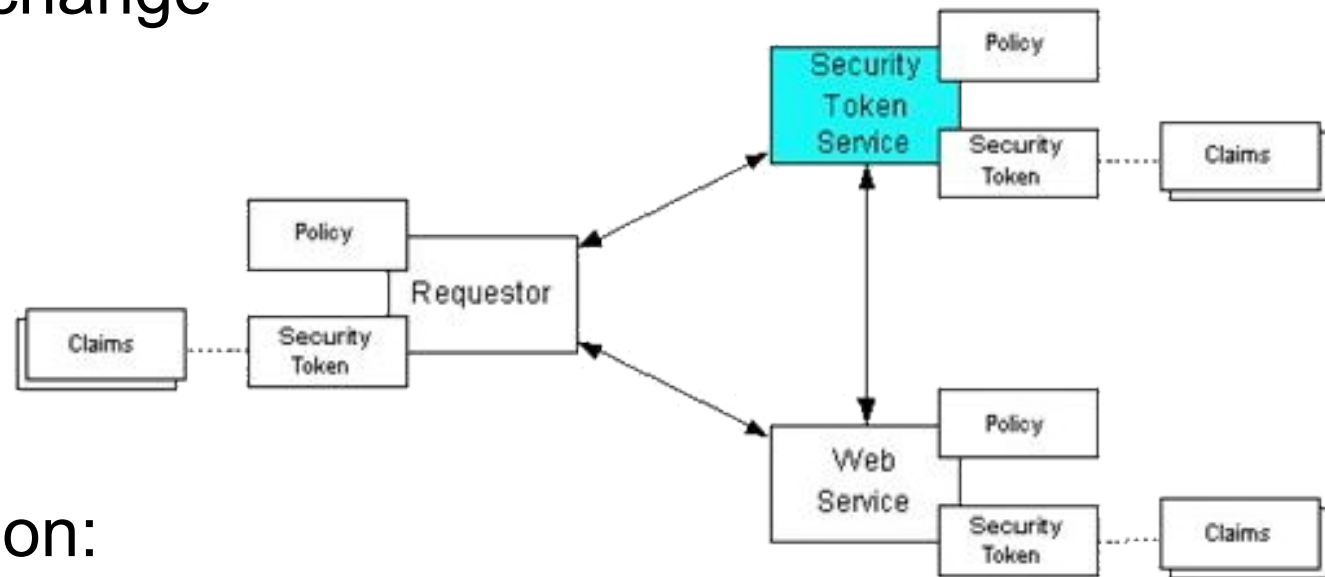
## Security Assertion Markup Language v2.0



# WS-Federation1.1B

## Web Service Federation Language v1.1B

Coming from web service security specifications.  
Mainly, WS-Security, WS-Trust, WS-SecurityPolicy and WS-MetadataExchange



WS-Federation:

- Roles of Security Token Servers
- Federation Metadata
- An application of the WS-Federation Model: WS-Federation Passive Requestor Profile which suits for web applications

The background image is a teal-tinted landscape of a beach. The foreground is dominated by intricate, wavy ripples in the sand, created by wind or water. The ripples recede towards the horizon. In the distance, the ocean meets the sky at a low horizon line. The sky is filled with soft, textured clouds, with some brighter patches where light breaks through. The overall color palette is monochromatic, consisting of various shades of teal, blue, and grey.

Interoperability between architectures of  
different specifications

# Principle of interoperability

---

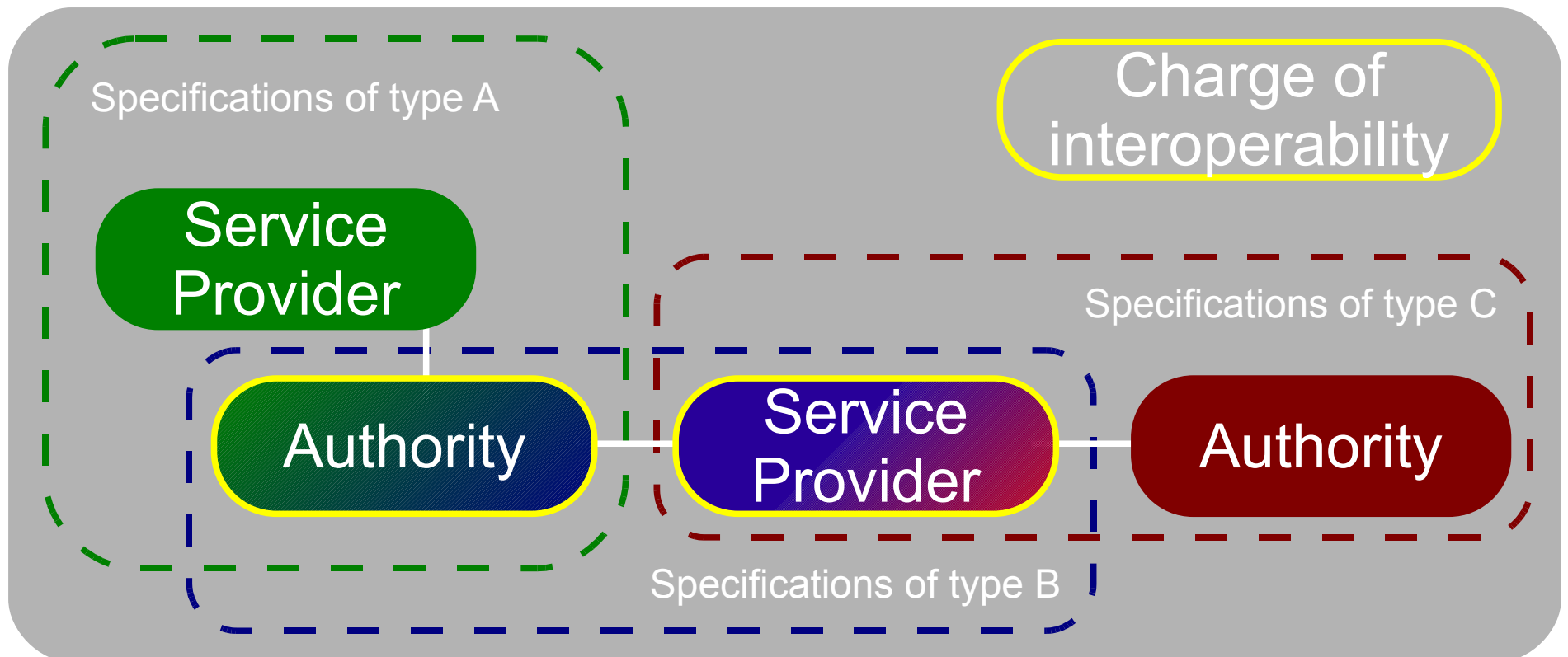
**Allow a service provider to consume and to trust the security informations issued by an authority of a different specification.**

WHICH IMPLIES IF NECESSARY:

- to translate security informations;
- to convert the requests and responses of the federation protocol;
- to negotiate a common protocol;
- to ensure transitive trust.

# Interoperability architecture

The interoperability process can be directly taken in charge by authorities or service providers:



# Interoperability architecture

---

It needs to modify entities in production.

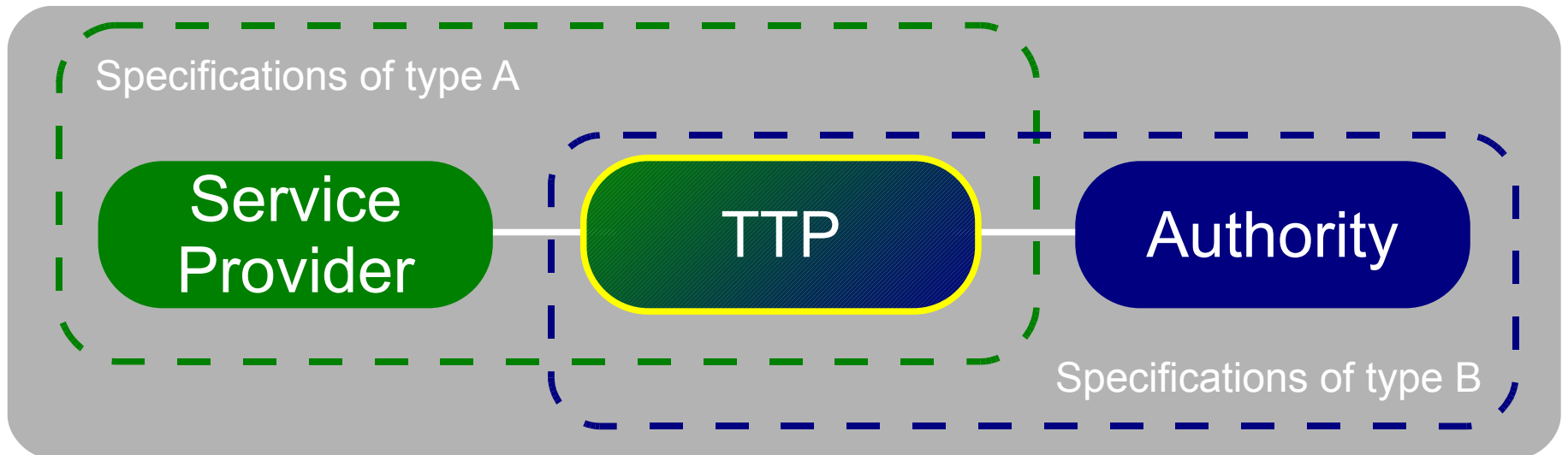
Consumer and provider of security information « speak » the same specification: negotiation on a common specification is needed.

It is not a real interoperability issue because the producer and the consumer « speak the same language ».

# Interoperability architecture

---

Interoperability can be enabled thanks to a trusted third party (TTP):



# Interoperability architecture

---

The TTP topology :

- is suitable to avoid modifications of existing entities;
- may support direct or transitive trust.

It needs to convert requests and responses, and maybe, security informations.

Represents a single point of failure.

The background of the slide is a teal-tinted photograph of a beach. The foreground is dominated by intricate, wavy ripples in the sand, created by wind or water. The ripples recede towards the horizon. In the distance, the ocean meets the sky, with a few small, dark shapes that could be birds or distant land. The sky is filled with soft, textured clouds. A semi-transparent, rounded rectangular box is centered over the middle of the image, containing the text.

A way to make SAML2 and WS-Federation 1.1B interoperate

# First comparison result

---

SAML2 only cares about principal as users and not as standalone application. The user can interface the federation architecture with a passive or an active requestors (a simple or an enhanced web browser).

WS-Federation1.1B cares about principals as users, which uses passive requestors (web browsers), or as standalone applications, which are active requestors (web service consumers).

**Hence, for the interoperability issue, we care about ressources as web applications and thus, principals are users with simple web browser.**

# Goal of the comparison

---

Determine the common profiles

Study the bindings and metadata issues

Infer the mapping of the requests and responses  
of the federation protocol

Determine how to assert the same information in  
SAML assertions and WS-Security tokens

# Common profiles

---

- Authentication delegation and session management (Single logout)
- Attribute issuing:
  - Contained in the same assertion as the authentication one.
  - In distinct responses.

# Transport

---

- For authentication delegation, HTTP redirection is required to allow the user to present his credentials to the authority (Identity Provider / Security Token Server).
- For Single logout and attribute query, WS-Federation only support HTTP redirection. SAML also support direct SOAP requests between the SP and the Authorities.
- In SAML, all the assertions can be obtained through a back channel. A reference called an artifact will be used through the front channel.

# Transport & Metadata

---

**Whatever binding is used for one profile, the content of the requests and responses of the federation protocols, and the resulting security information, will be the same.**

**Thus, the choice of a binding is a question for the TTP, not of the SP or the authorities. So the TTP will only have to allow those supported by the SP and authority indicated in their metadatas as for a normal federation architecture.**

**There is no dynamic treatment to apply on metadatas, there will be treated beforehand the communications as for a normal federation architecture.**

# Requests

---

WS-Federation offers two means for the SP to request the IP for authentication: Through a set of URL parameters or through an XML Document passed through a URL parameter.

We have chosen to use this way to make them interoperate because SAML use this principle too.

So the TTP have to translate an SAML Request into an WS-Trust Request and inversely. It is mainly for us an XML schema mapping and in production a XML Document conversion.

# Responses

---

They both use XML Documents passed through a URL parameter.

As for the requests, the TTP will have to translate an SAML Response into an WS-Trust Response and inversely.

# Security Informations

---

**The good news: WS-Federation is based on WS-Security which accepts SAML assertion as security token format.**

# So what?

---

**The TTP extracts the assertion from the XML Document Response it receives, it recreates a XML Document Response and includes in it, the assertion.**

**It resigns the assertion if it ensures transitive trust, i.e. the SP and IP are directly trust linked or it just adds its own signature.**

A teal-tinted landscape photograph of a beach. The foreground is dominated by intricate, wavy ripples in the sand, receding towards the ocean. The sky is filled with dramatic, layered clouds. A semi-transparent white rounded rectangle is centered in the upper half of the image, containing the word "Conclusion" in a black serif font.

# Conclusion

# Review

---

Now? We only provide a guideline and we have roughly treated the authentication request in the article.

Next:

- **Address privacy:**
  - **SAML: pseudonyms managed by identity providers**
  - **WS-Federation: Dedicated pseudonym authorities**
- Make a detailed schema mapping.
- Write pre-specifications for development.

# Future works

---

Infer from the litterature and the different existing federation architectures:

- an ontology to make make easier conversion for protocol and security informations
- a model which solves the puzzle which the pieces are:
  - an architecture which suits for web application consumed as well with passive an active requestors
  - the security of service oriented architecture
  - an Identity service oriented architecture (Liberty ID-WSF)
  - take in account the Identity 2.0 paradigm (Cardspace and OpenID)
  - address main « use cases »: Grid Cumputing, e-Administration, Telco operators, banking, etc...