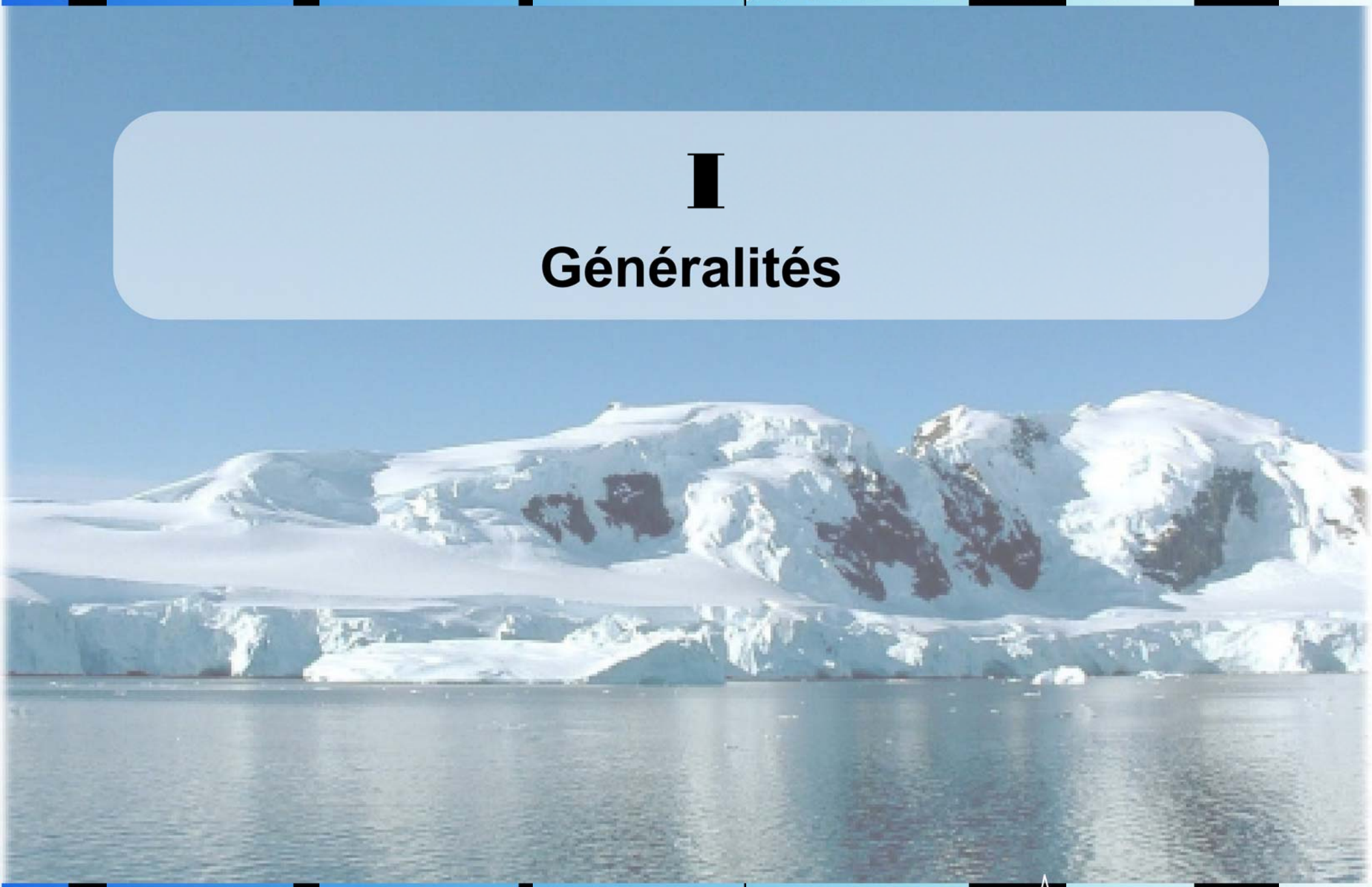

jres 2007
Architectures de fédération d'identités et interopérabilité
Mikaël Ates
JRES 2007
satin
DIOM
istase
jres 2007

Sommaire

I

Généralités



Deux types de fournisseurs de services:

- Application web: Application consommable via un navigateur web
- Service web : module applicatif accessible par les protocoles du web via un consommateur de services web

Gestion des identités pour un fournisseur de service

Une application offrant l'accès à une ressource ou un service a besoin de contrôler l'accès et donc de gérer des identités (AAAA):

- Authentifier (Authentication)
- Autoriser (Authorization)
- Gérer un ensemble de paramètres de personnalisation (Accounting)
- Auditer l'ensemble des activités (Auditing)

Les clients d'applications web

Deux types de clients permettant la consommation d'applications web:

- Le client passif: N'intéragit pas avec le SGI (Web browser)
- Le client actif: Intéragit avec le SGI (Smart client)

L'authentification unique ou Single SignOn (SSO)

Permettre à l'utilisateur de ne s'authentifier qu'une seule fois pour la consommation de multiples services. Deux types de SSO:

- Le portefeuille
- Délégation de l'authentification auprès d'une autorité

La fédération des identités

C'est d'abord une fédération d'entités, c'est à dire un partenariat entre entreprises, organisations, institutions, etc..., afin de mettre en commun des ressources.

La fédération d'identités c'est un accord sur les termes des échanges portant sur les identités et les moyens pour parvenir à faire interopérer les SGI des différents systèmes d'information.

Les problèmatiques adressées

- Pouvoir déléguer certains procédés administratifs auprès de tiers de confiance.
- Offrir l'accès à des ressources/services à des identités issues de domaines de sécurité différents de celui du SP.
- Véhiculer entre tiers de confiance des informations sur les identités et le résultats de l'exécution des procédés administratifs.

Les fonctionnalités attendues

- Mutualisation de ressources pour l'exécution de tâches administratives au sein d'un cercle de confiance (CoT):
  - Délégation de l'authentification et par la même fournir une authentification unique pour l'accès à de multiples SP
  - Déléguer l'authorisation ou obtenir des attributs permettant la prise de décision.
- Simplifier « la vie » de l'utilisateur
- Sécurisation d'architectures orientées services web.
- Interconnecter les systèmes de gestion des identités de systèmes d'information

Modèle d'architecture de fédération d'identités

- Informations de sécurité
- Architecture de confiance et cycle de vie de l'information de sécurité
- Architecture de fédération: protocoles et rôle des entités
- Le client

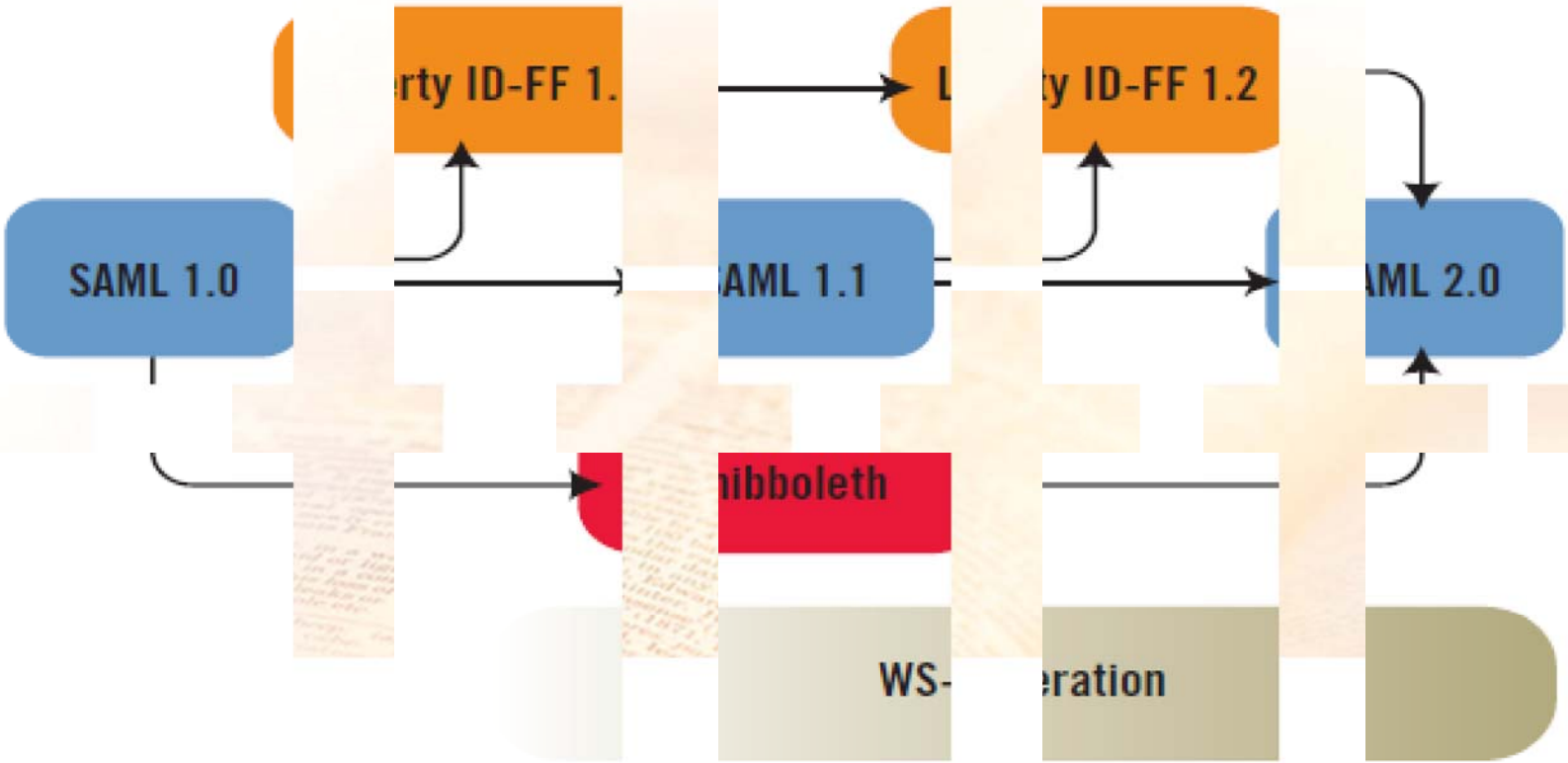
Les rôles des entités

- Principal
- Client
- Autorités:
  - Fournisseur d'identités (Identity Provider - IP)
  - Fournisseur d'attributs (Attribute Provider – AP, Attribute Authority - AA)
- Fournisseurs de services (web) (Service Provider, Relying Party, Resource Provider, Assertion Consumer)

II

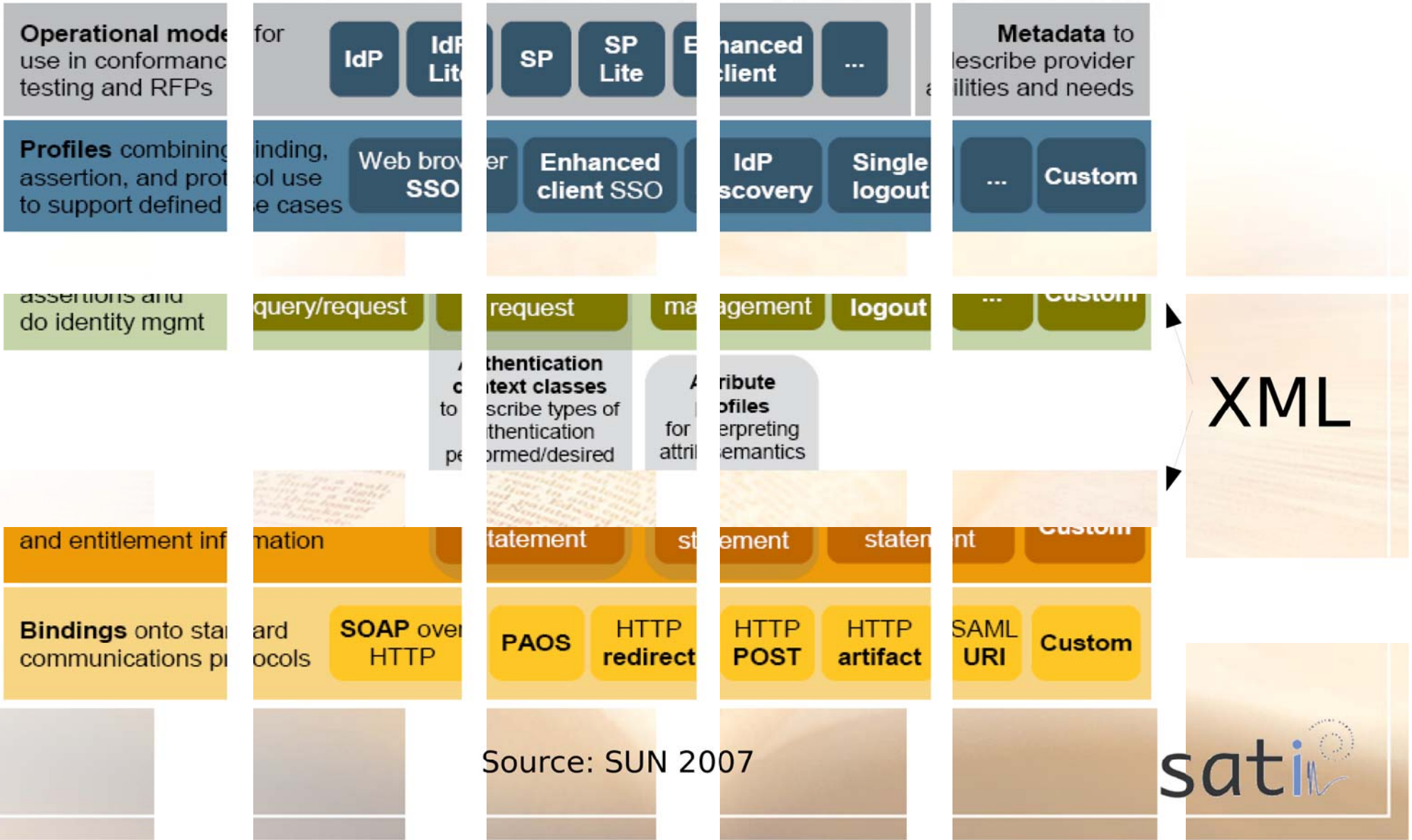
Spécifications

Les spécifications majeures



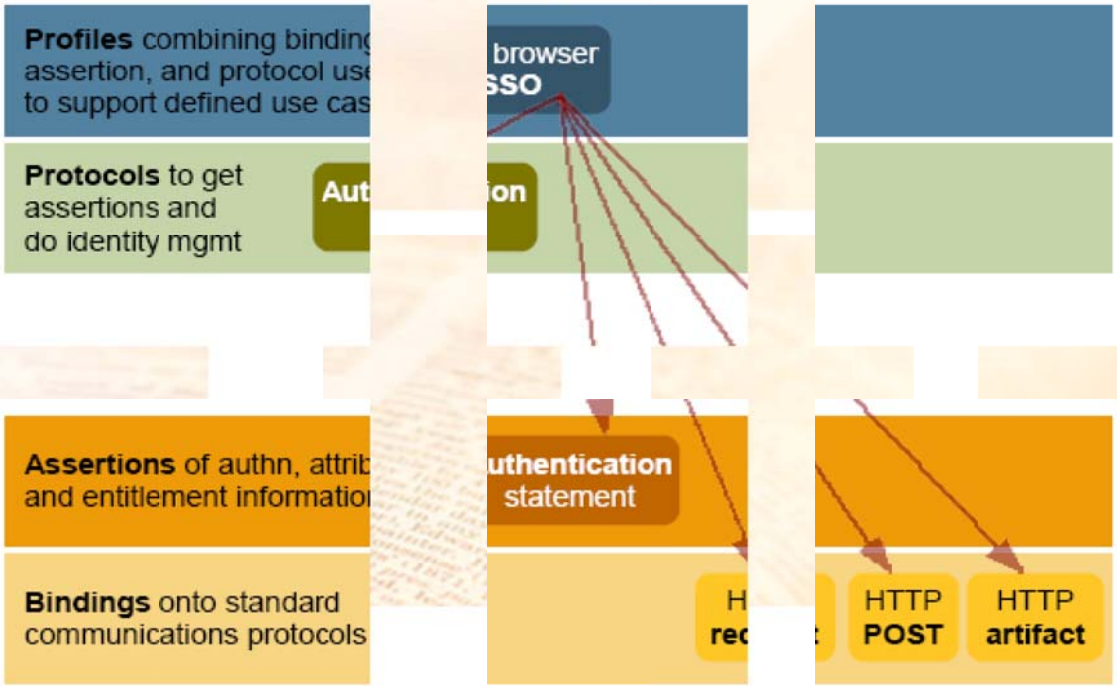
Source: Ping Identity 2006

SAML2



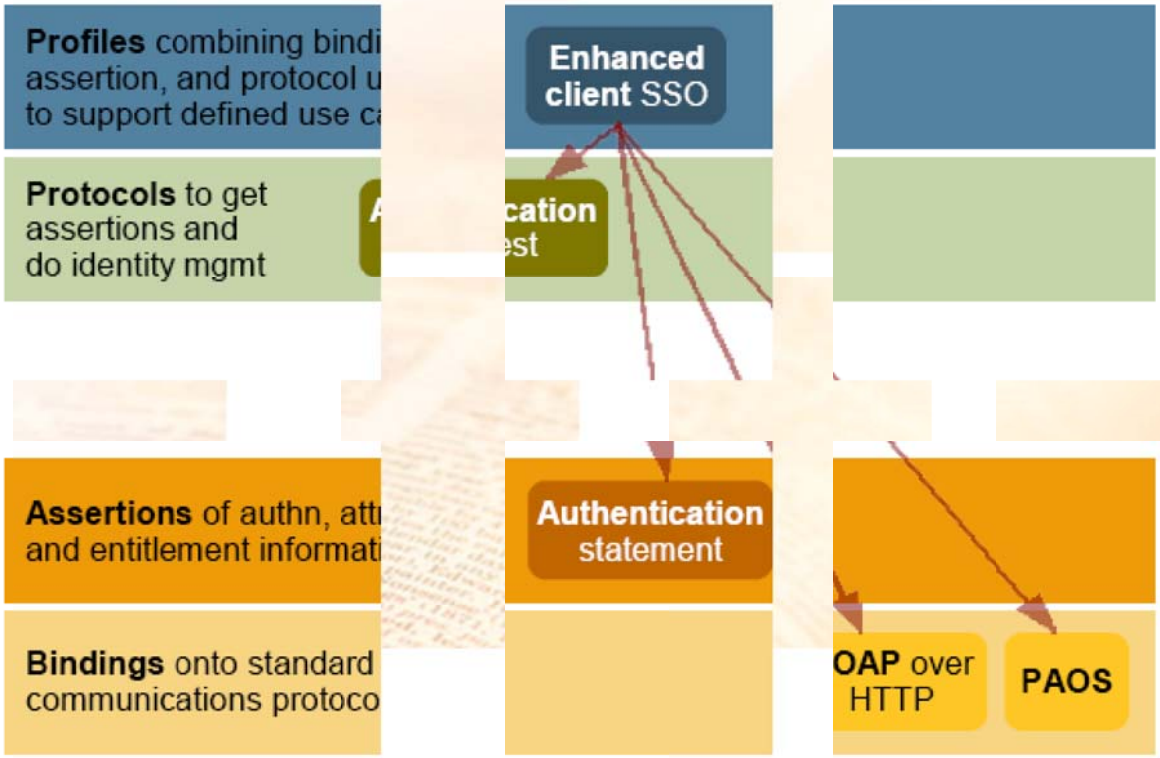
Source: SUN 2007

SAML2



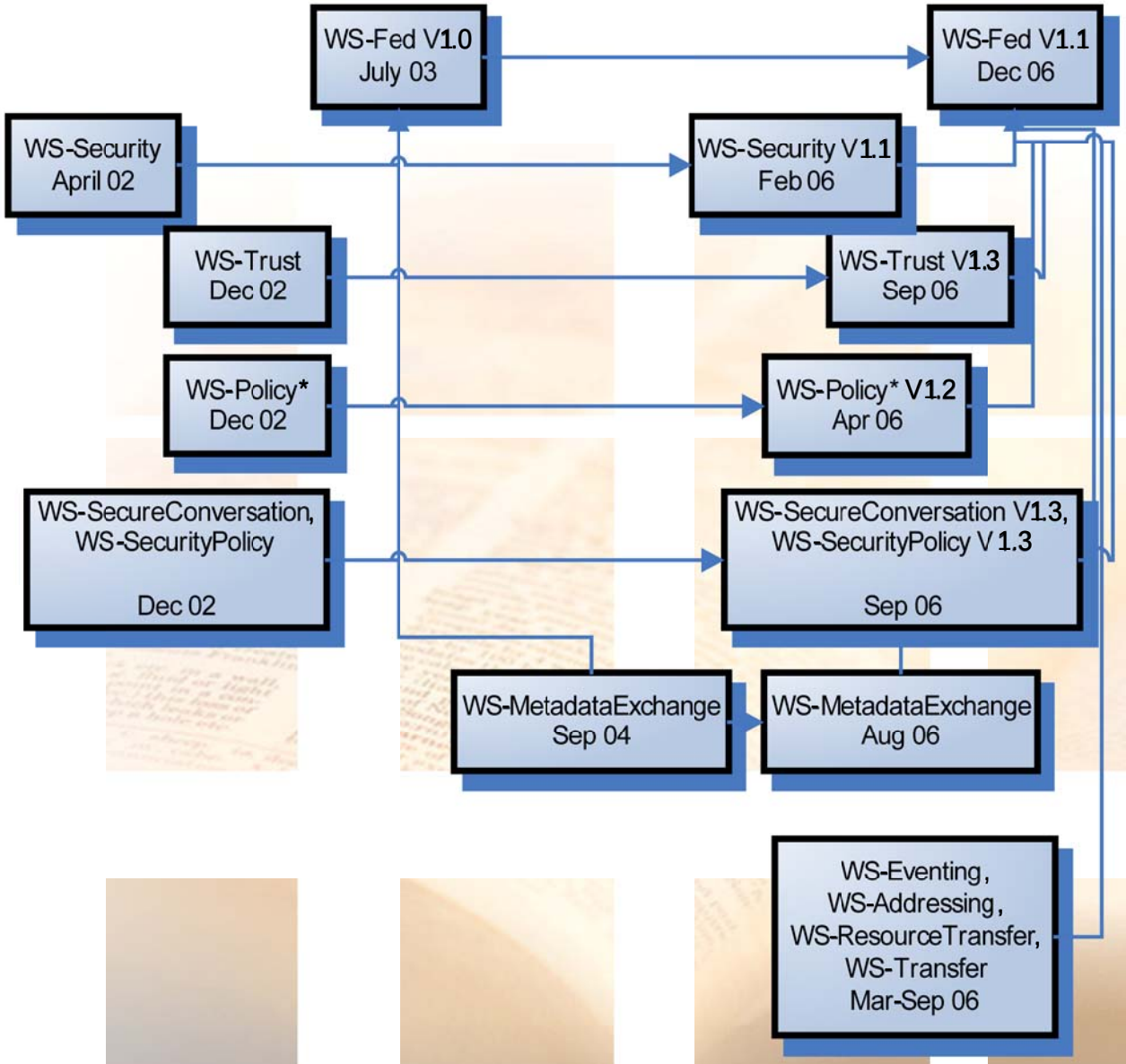
Source: SUN 2007

SAML2

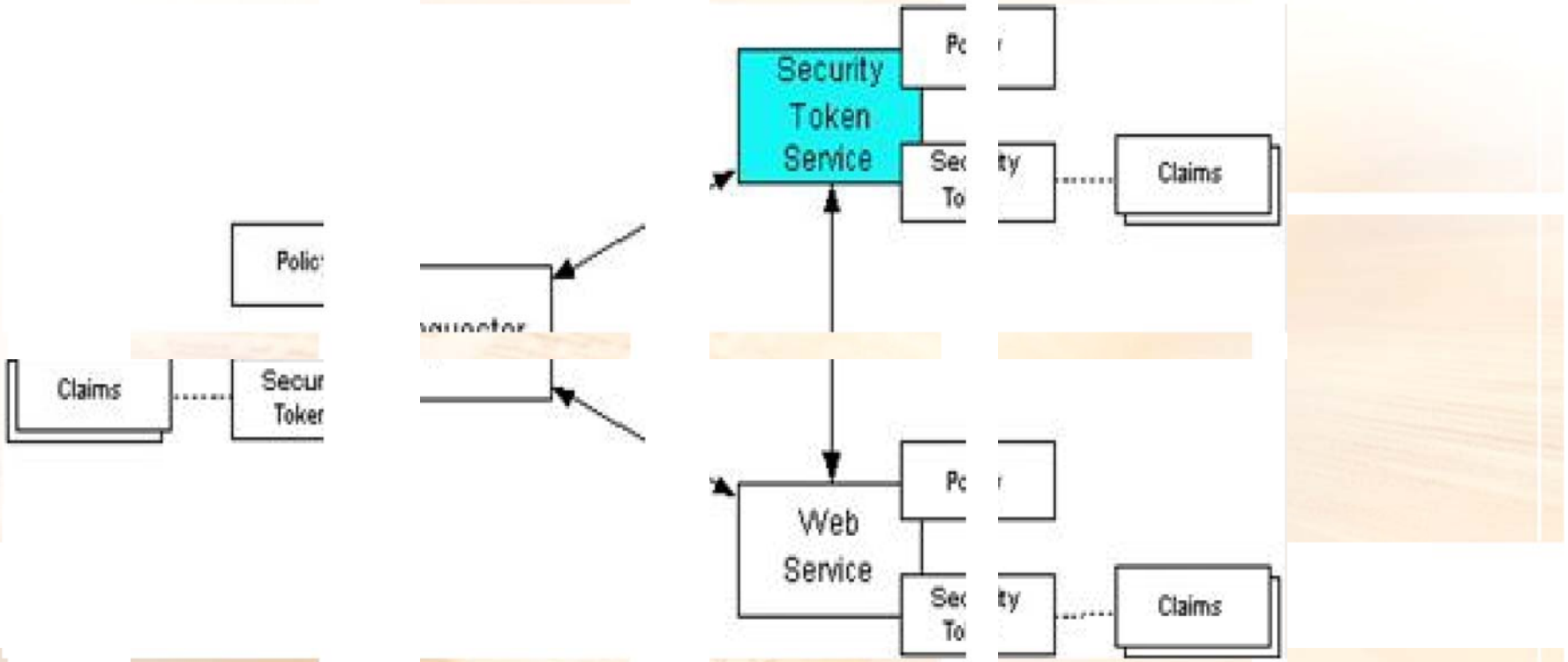


Source: SUN 2007

WS-*


WS-Fed V1.0
July 03
WS-Fed V1.1
Dec 06
WS-Security
April 02
WS-Security V1.1
Feb 06
WS-Trust
Dec 02
WS-Trust V1.3
Sep 06
WS-Policy*
Dec 02
WS-Policy* V1.2
Apr 06
WS-SecureConversation,
WS-SecurityPolicy
Dec 02
WS-SecureConversation V1.3,
WS-SecurityPolicy V 1.3
Sep 06
WS-MetadataExchange
Sep 04
WS-MetadataExchange
Aug 06
WS-Eventing,
WS-Addressing,
WS-ResourceTransfer,
WS-Transfer
Mar-Sep 06

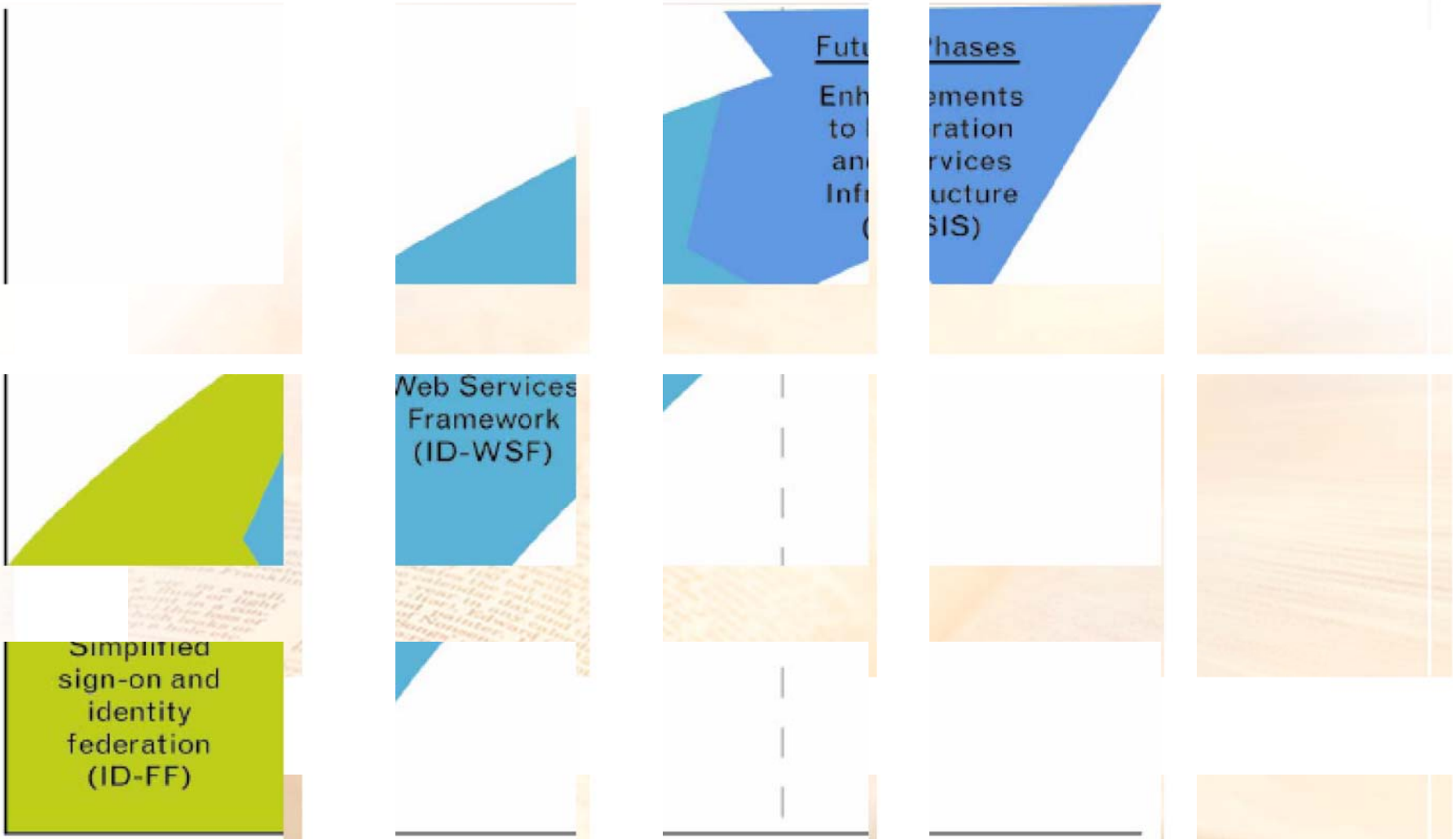
WS-Trust



WS-Federation1.1B

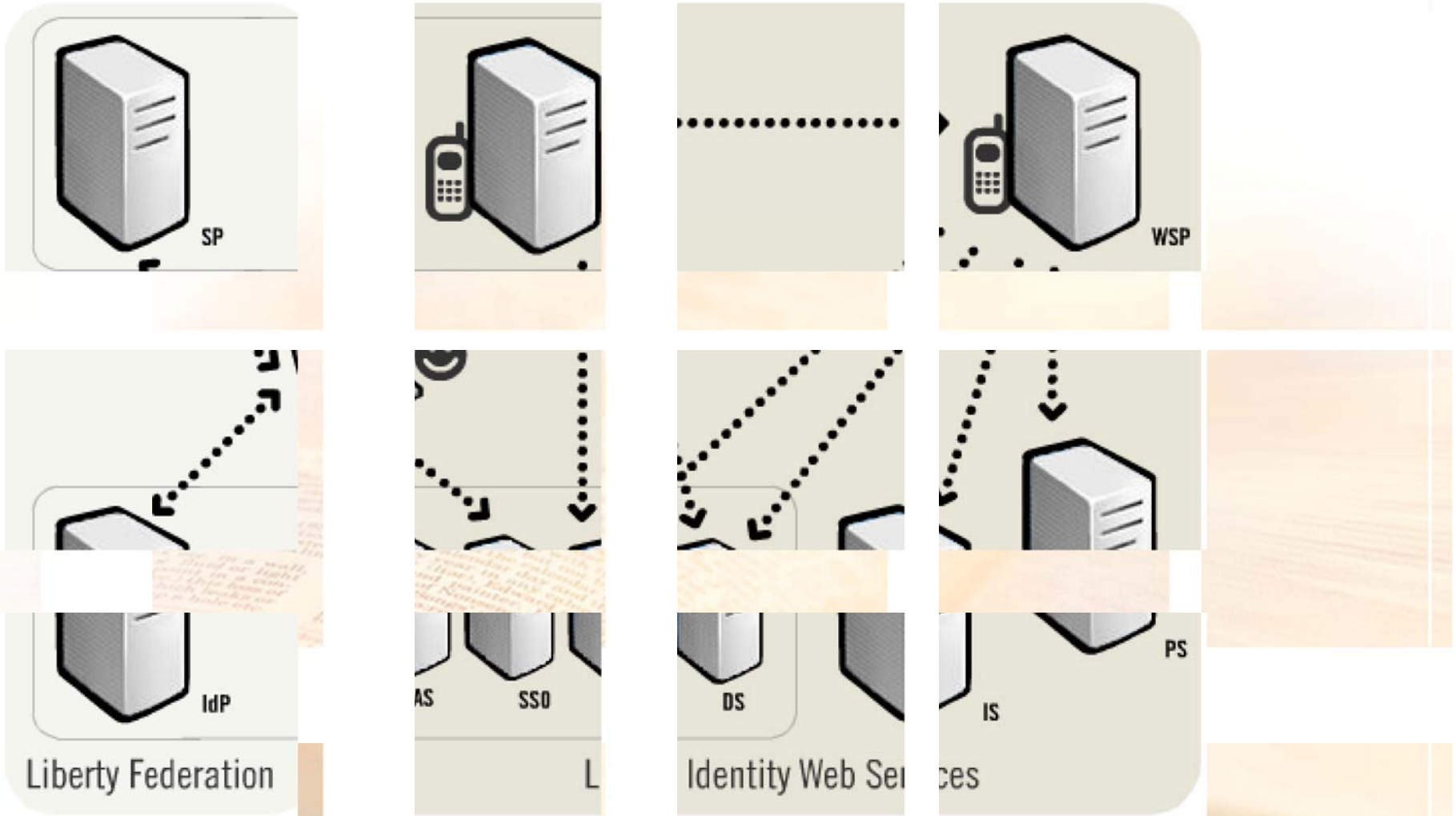
- Agrégat de spécifications
- Définition des rôles
- Architecture de confiance: Echange de jetons, validation, délégation...
- Métadonnées de fédération
- Implémentation du modèle WS-Federation: WSFL-PRP: Profile de GDI pour l'accès aux applications web.

Les spécifications Liberty Alliance



Source: Liberty Alliance 2003

ID-WSF



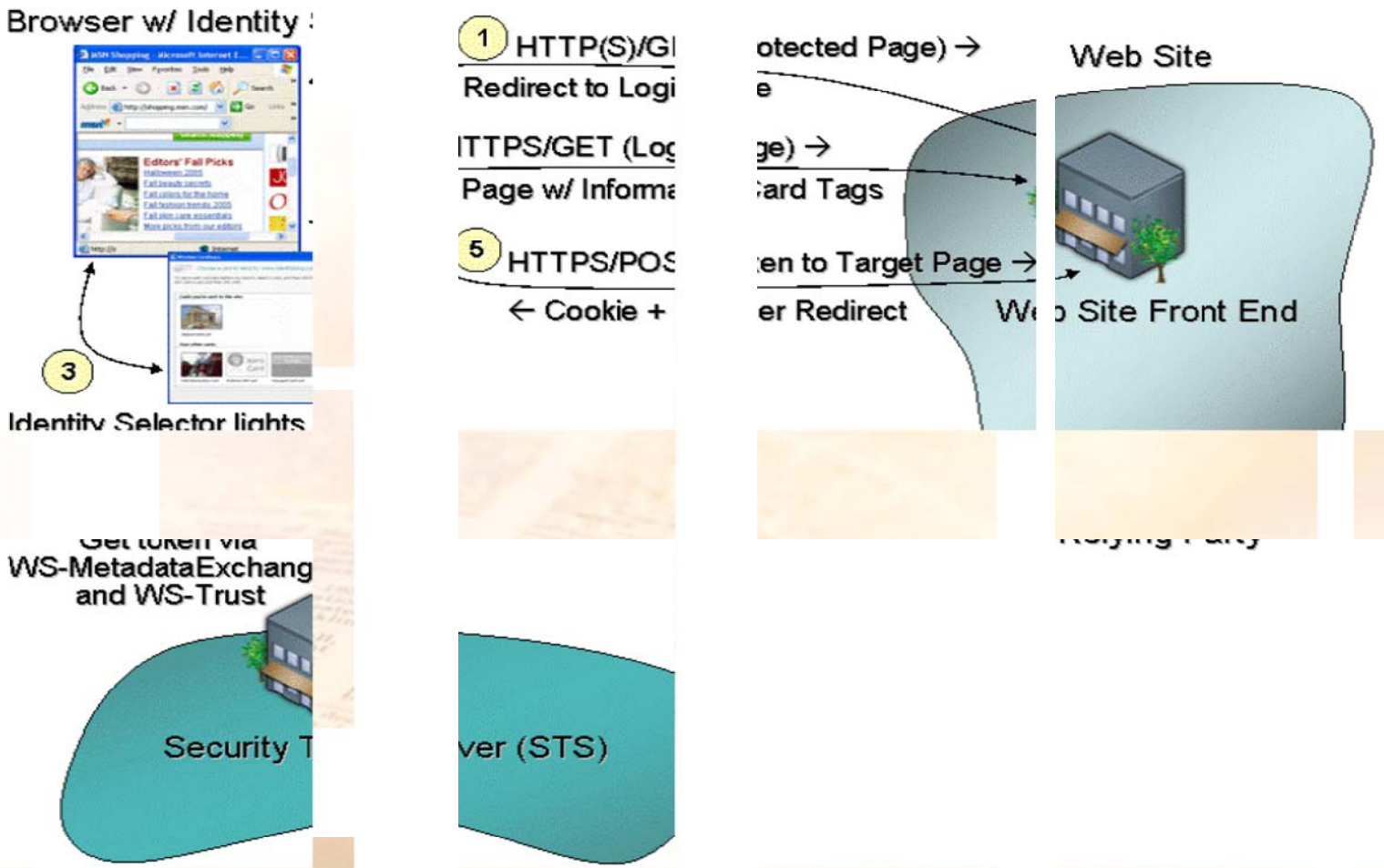
Source: Liberty Alliance 2007

Les clients ID-WSF

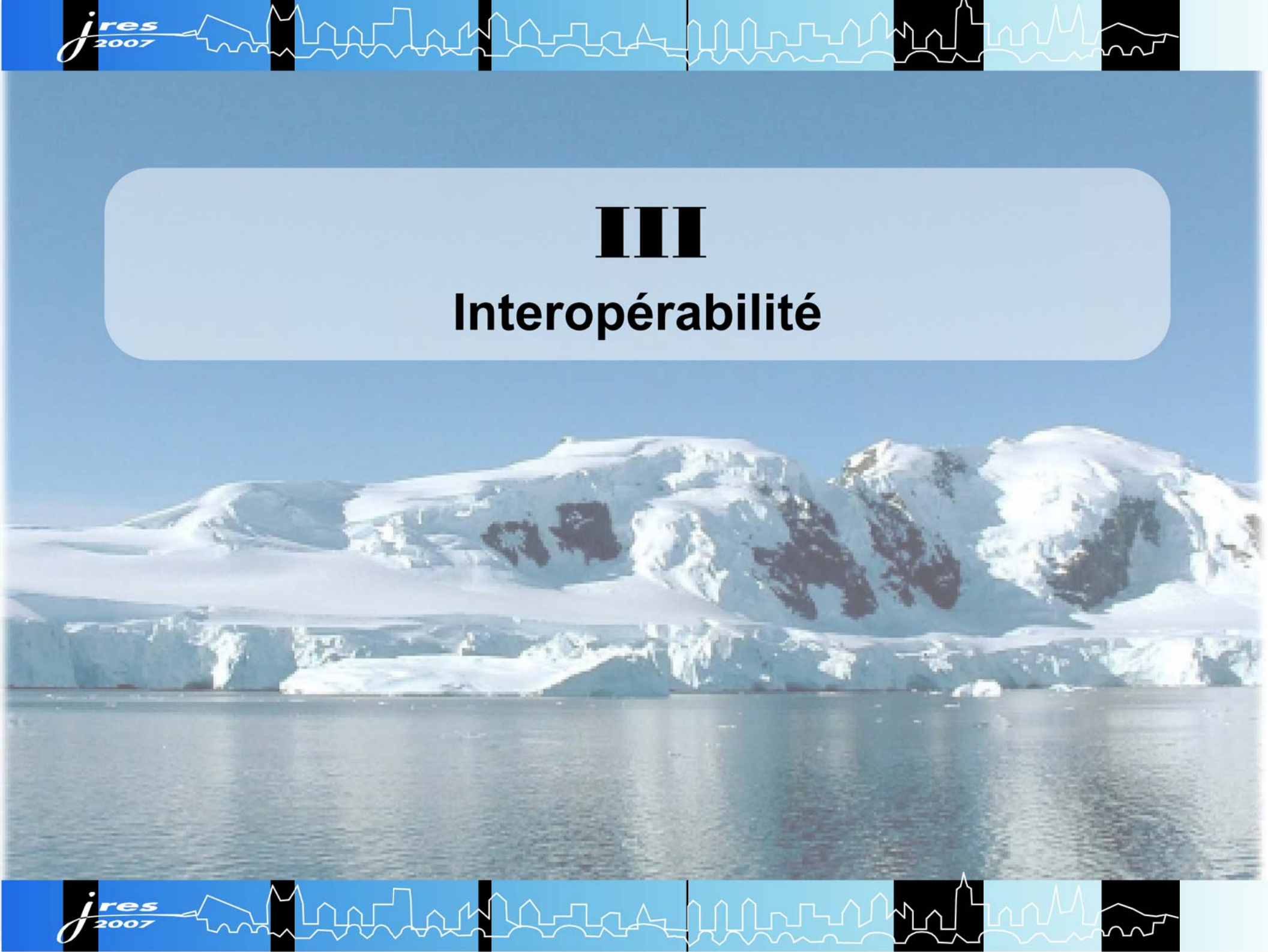
Evolution of Liberty related Clients

- Phase 1 Liberty Enabled Client Proxy (LECP)
- Phase 3 Advanced Client (aka Intelligent Client)
- Phase 4 Robust Client

CardSpace



Source: A Guide to Using the Identity Selector Interoperability Profile V1.0 within Web Applications and Browsers 2007



III

Interopérabilité

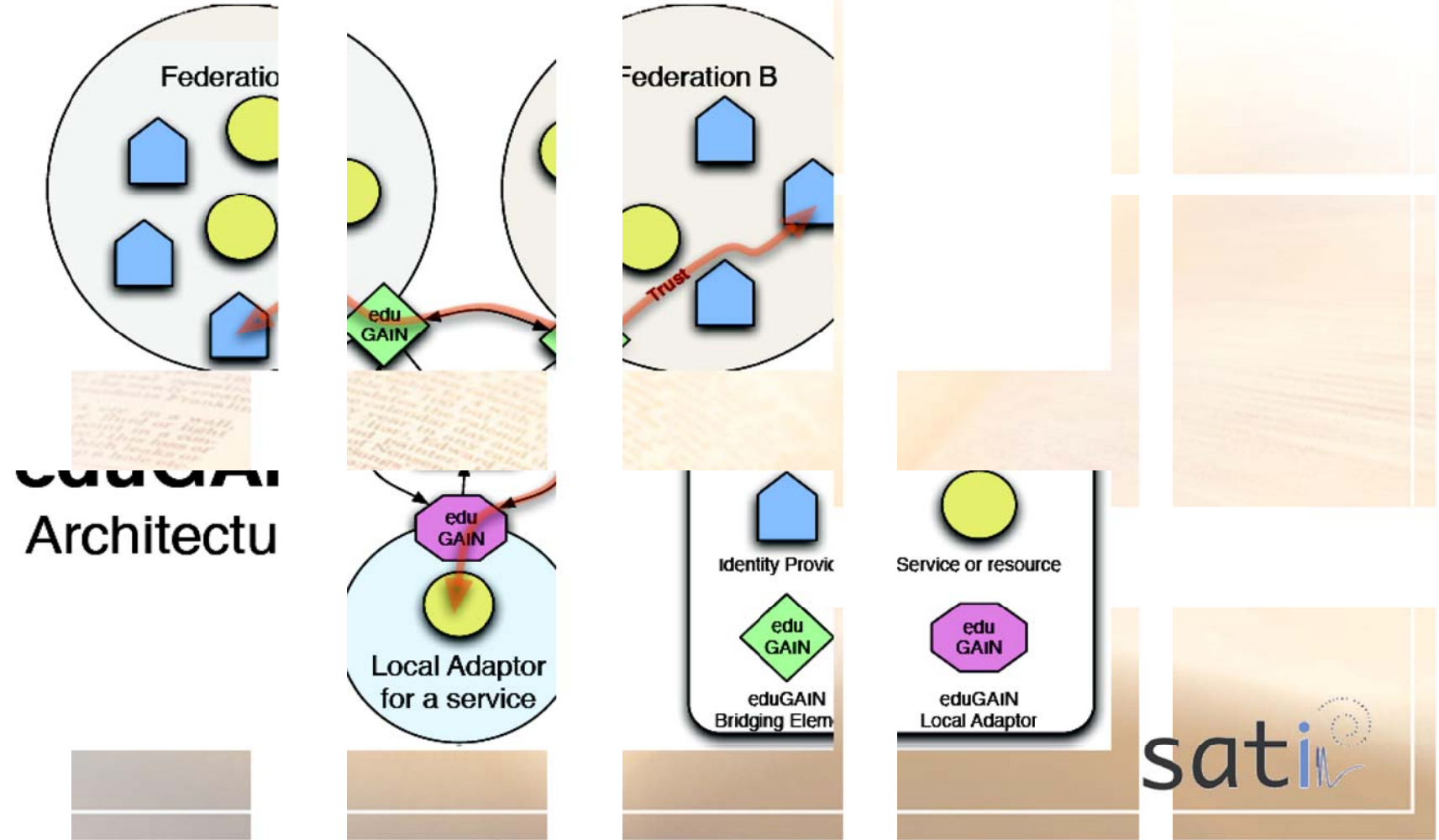
Interopérabilité

La fédération d'identité est en elle-même une solution pour faire intéroperer les SGI.

- Implémentation: Fédération - CoT & Confédération - InterCoT/CoCoT

ex: eduGAIN

Projet d'interconnexion des AAI du projet GEANT2 basé sur SAML1.1



Architectu

Interopérabilité

- Interopérabilité entre spécifications concurrentes: WSFL-PRP/SAML1.1/ID-FF1.2/SAML2/...

ex: ADFS & Shibboleth

  - ADFS: Windows 2003 server R2 - WS-Federation 1.0 Passive requestor profile (2003)

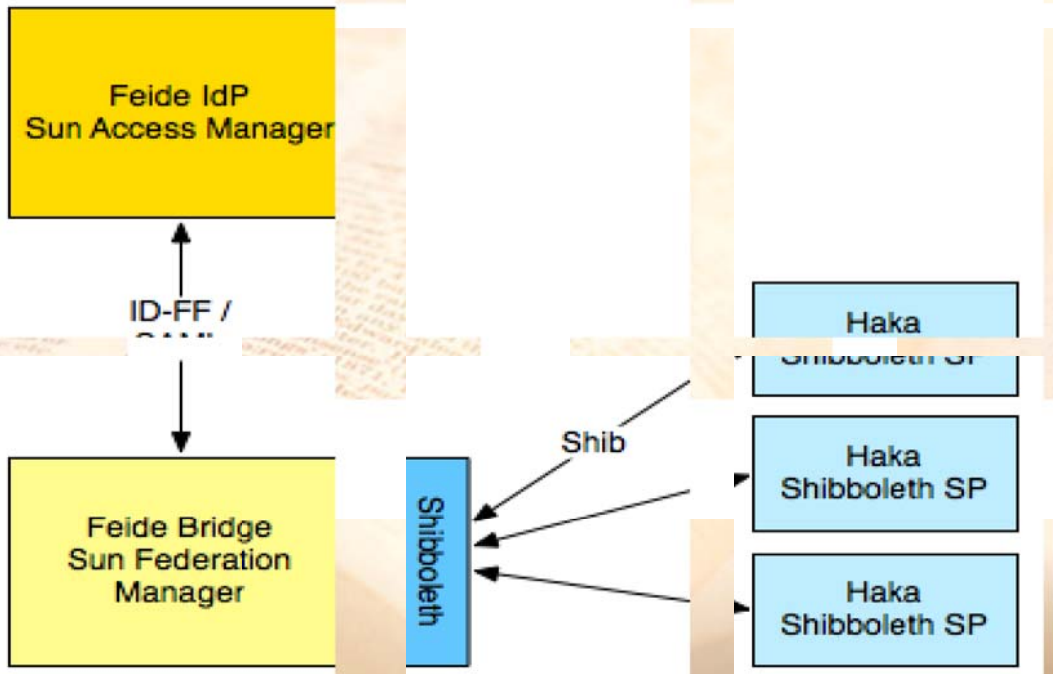
  - Shibboleth 1.3: SAML1.1 + WAYF + AuthZ sur Attributs

ADFS & Shibboleth

- FS-A : IP/STS - FS-R: RP
- Trust Policy / Métadonnées
- Développement d'un module d'extension de Shibboleth: Intégration aux IP/SP Shibboleth
- Pas de conversion RST/SAMLRequest ni RSTR/SAMLResponse

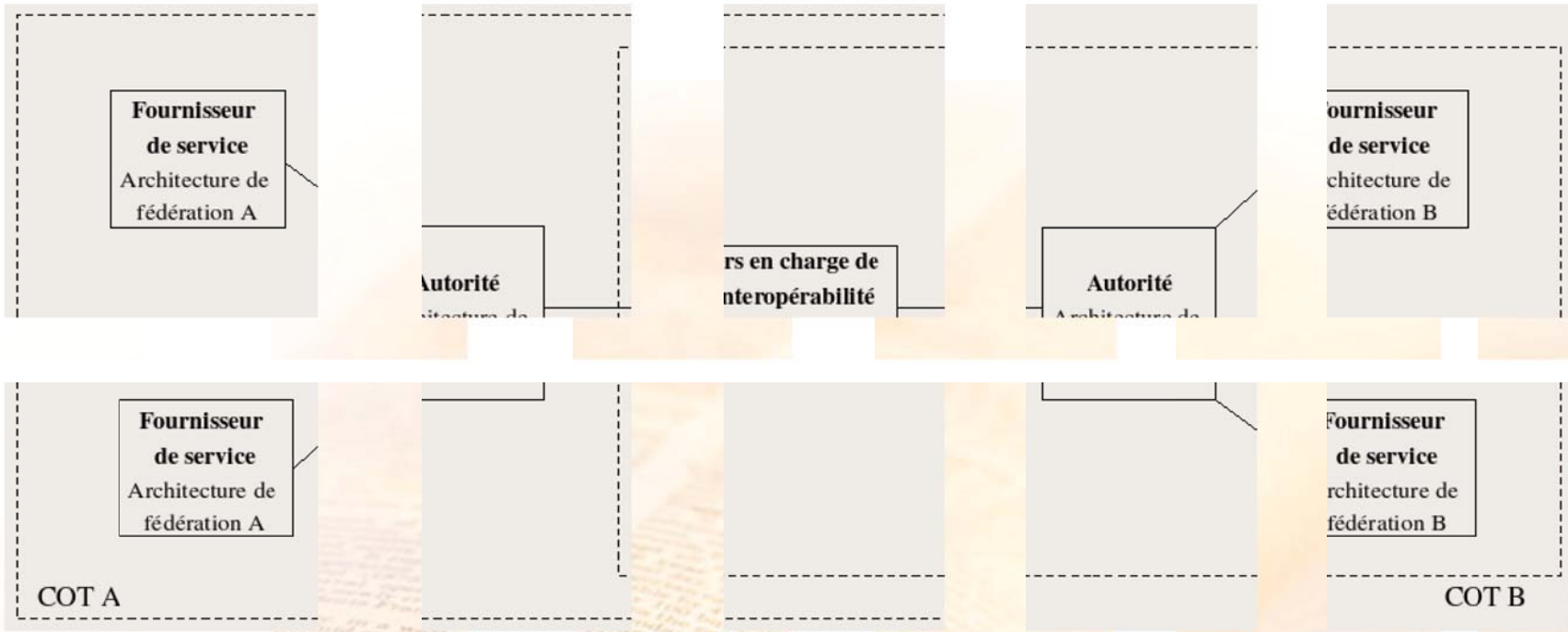
Kalmar Union: Nordic crossfederation

haka	Haka (Fin	):	Operation Shibboleth)
FEIDE	FEIDE (N	y):	Operation Moria, Liberty/Sun)
DK-AAI TEST	DK-AAI (D	nark):	Piloting (S bboleth)
swami	SWAMID	eden):	Piloting (S bboleth)



SAML2 & WSFL-PRP

Tiers de confiance dédié à l'interopérabilité.



Source: Publication Ates JRES 2007

Conversion de requêtes:
RST/SAMLRequest
RSTR/SAMLResponse

Interopérabilité

- Interopérabilité entre spécifications complémentaires: SAML2/IDWSF2 (native), WSFL-PRP/IDWSF2,etc...
- Interopérabilité visant à l'intégration de contextes d'authentification:
  - Kerberos
  - CardSpace
  - CAS
  - etc.

CONCLUSION