Interopérabilité et sécurité des systèmes d'information

application aux systèmes de gestion de l'éducation

Abdramane BAH

LS2N - Université de Nantes

15 mars 2017

Informations de base

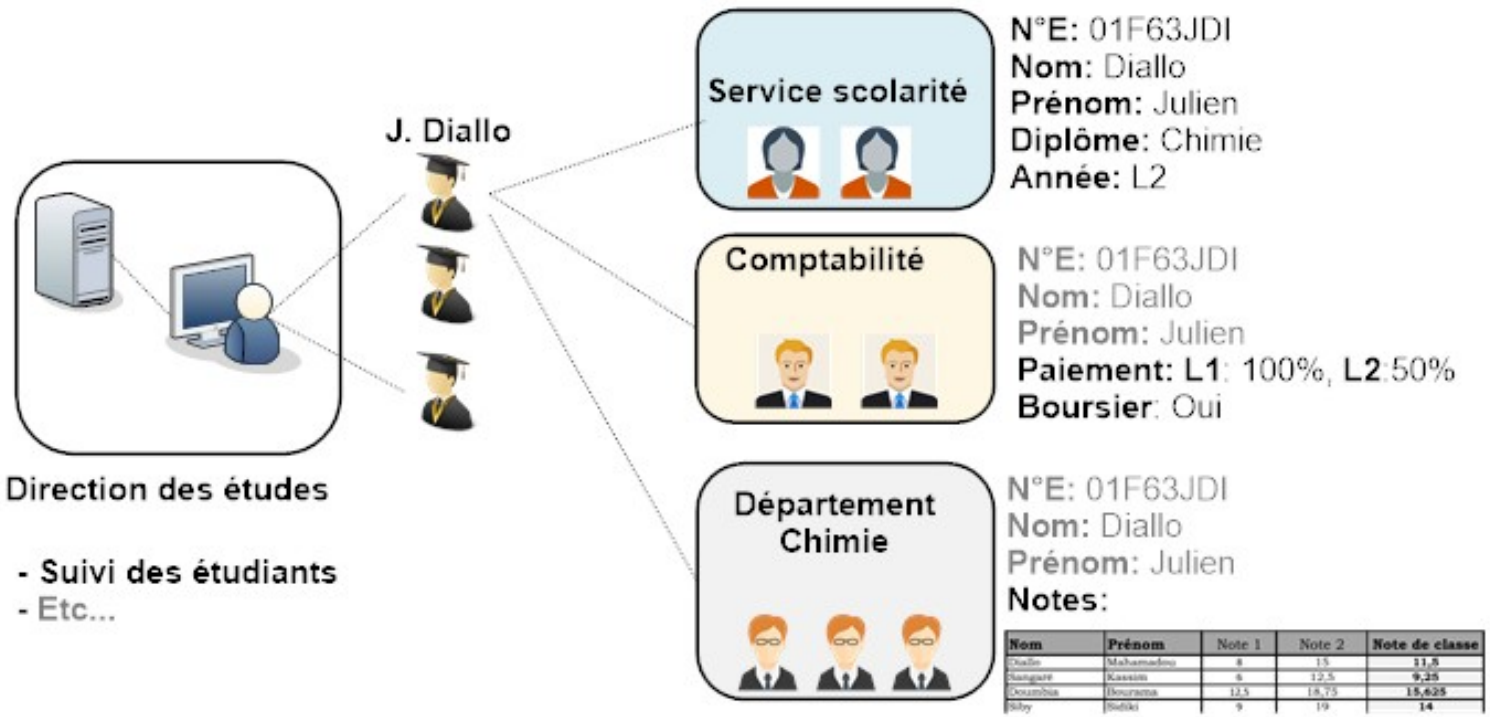
Thèse de co-tutelle

- Université de Nantes
- Université des Sciences, des Techniques et des Technologies de Bamako (USTTB)

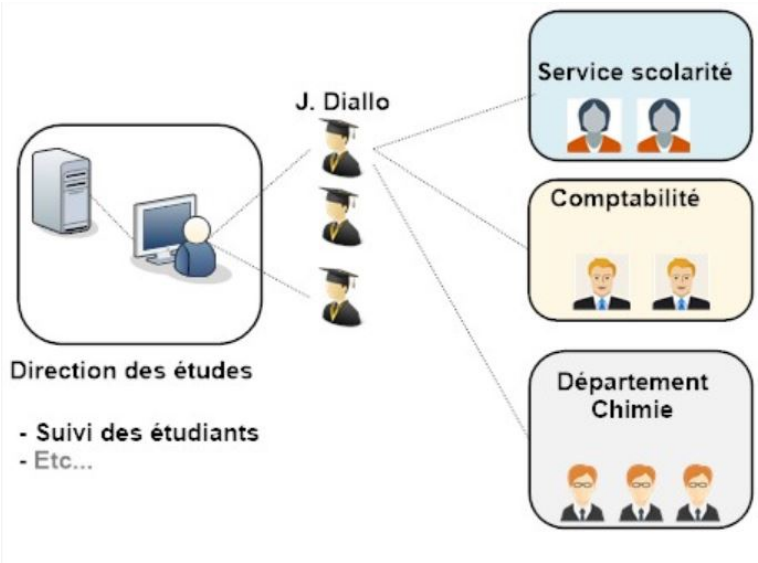
Financée par la coopération Franco-Malienne
Gérée par CAMPUS FRANCE

Direction de la thèse
Directeur de thèse : **J.C. ATTIOGBE**
Co-directeur : **P. ANDRE**
Directrice (USTTB) : **Jacqueline KONATE**

Contexte et problématique



Les systèmes sont hétérogènes, indépendants, autonomes et utilisés par un ensemble limité d'utilisateurs



Pour décider, faire le suivi : la direction a besoin de

- Service de scolarité
- Comptabilité
- Départements (e.g. Chimie)

Pour établir un diplôme, relevé de note :
le Service de scolarité a besoin de

- La Comptabilité : si tout est en règle
- les départements : notes

Problèmes :

- Incohérence des informations
- Collecte d'information difficile
- Traitement inefficace des informations
- Prise de décision sur des informations non à jour

Solutions

1. Rassembler les systèmes hétérogènes en un seul : ***Progiciel intégré*** (–> Nouveau système)
2. Faire communiquer les différents systèmes : Interopérabilité

Contexte et problématique

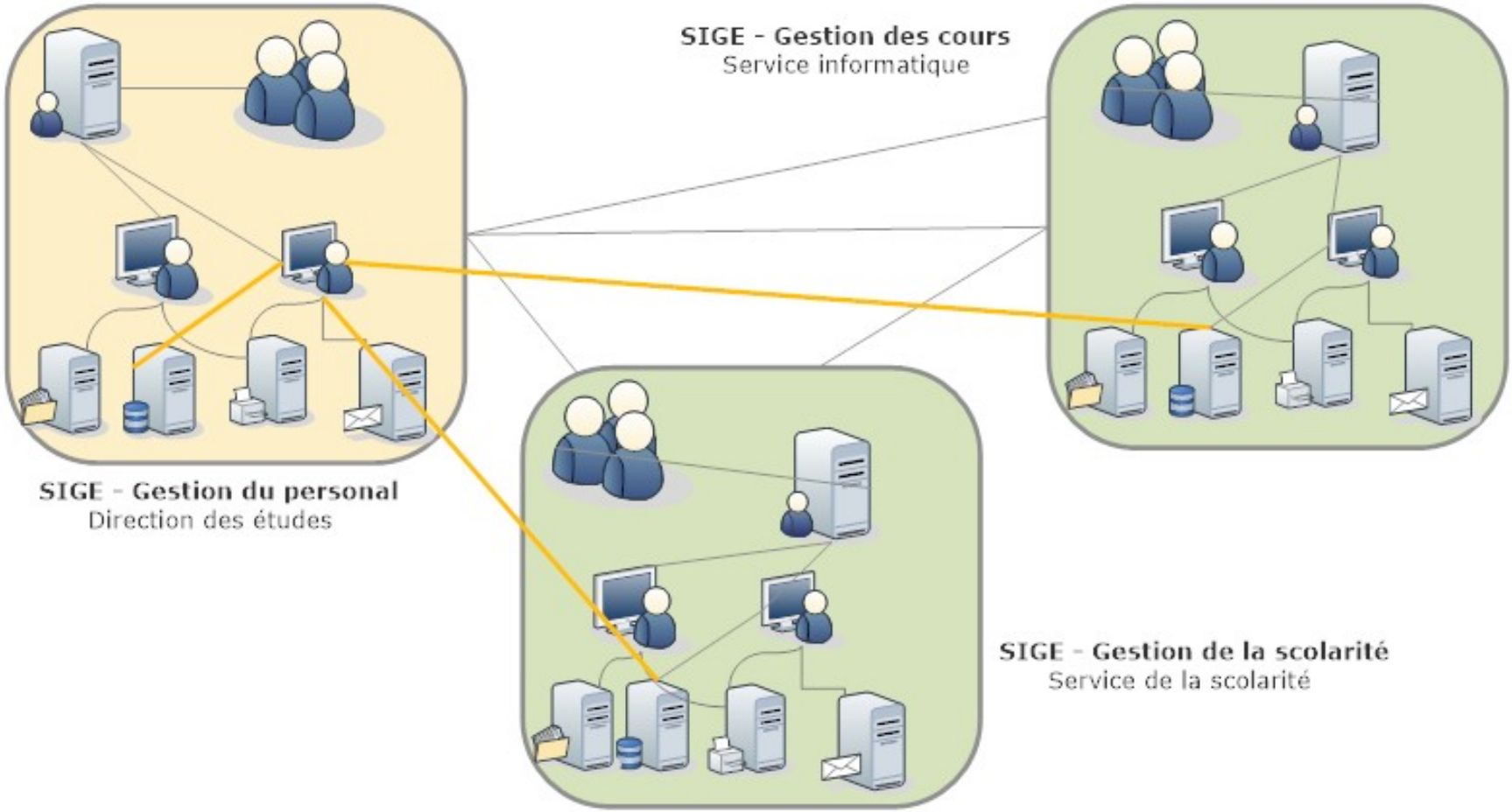


FIGURE – Interopérabilité entre plusieurs SIGE hétérogènes

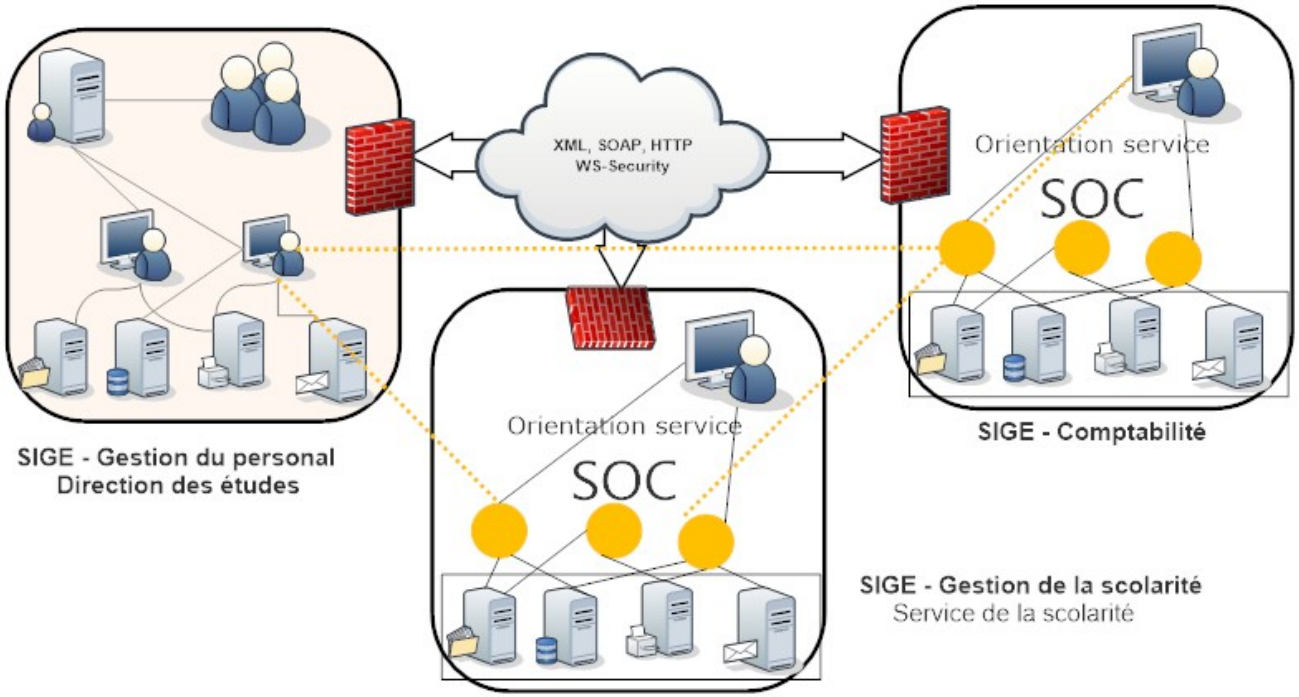
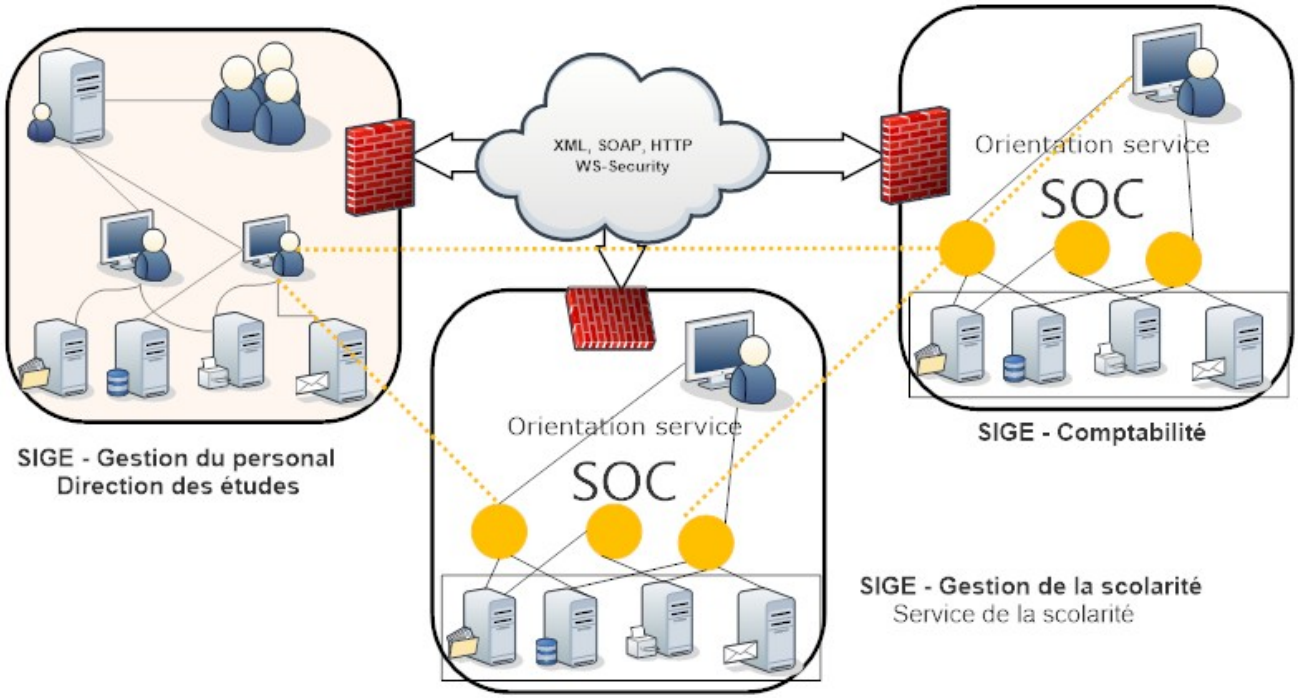


FIGURE – Interopérabilité via l'orientation service (Service Oriented Computing)

Problèmes :

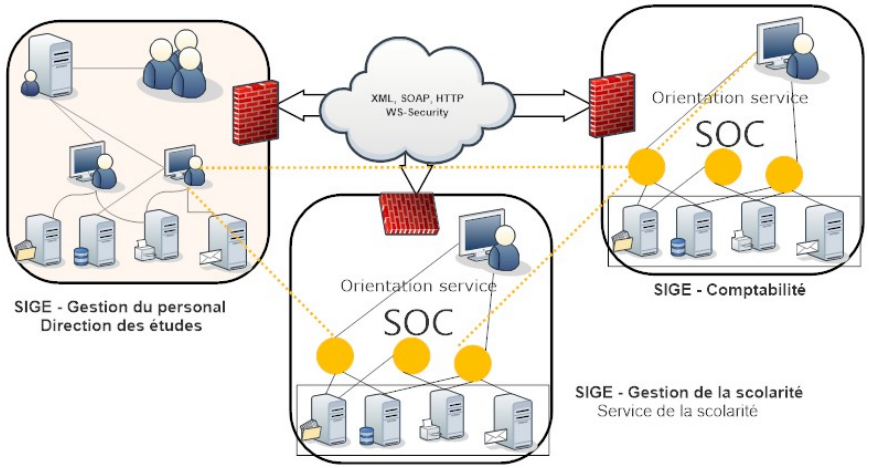
- Chaque système dispose déjà ses propres mécanismes et des protocoles de sécurité (souvent hétérogènes)
- qui doivent également inter-opérer.



Question : Comment vérifier

- l'authenticité de l'identité des utilisateurs
- et les permissions sur les différentes ressources et informations partagées ?

Défis et verrous



1. **L'interopérabilité**

   Il faut garantir l'accessibilité aux ressources contenues dans les différents SIGE malgré leur caractère hétérogène et la diversité des ***modalités d'accès***.

2. **Sécurité**

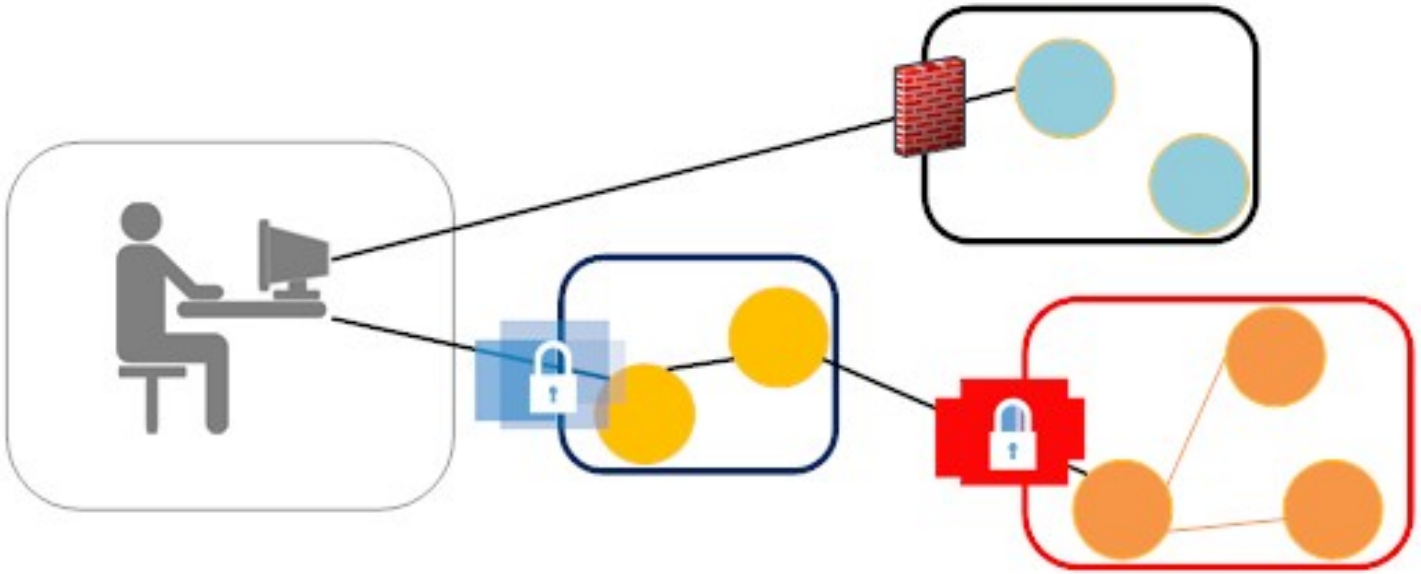
   Il faut en même temps assurer l'intégrité des données, la sécurité des accès et la sécurité mutuelle des SIGE constituant les ressources globales partagées.

Objectifs de la thèse

Mettre au point des concepts fondamentaux et des mécanismes robustes permettant :

- d'analyser, de vérifier et confirmer **l'authenticité de l'identité** des utilisateurs ;
- de **contrôler les permissions** sur les ressources et les informations partagées entre les SIGE interopérables.

Cible de la thèse



Une application répartie et ouverte constituée de plusieurs systèmes (SIGE) et d'applications partageant des informations entre elles.

Ce qui implique :

- l'agrégation de services (Mashup)
- la composition de services

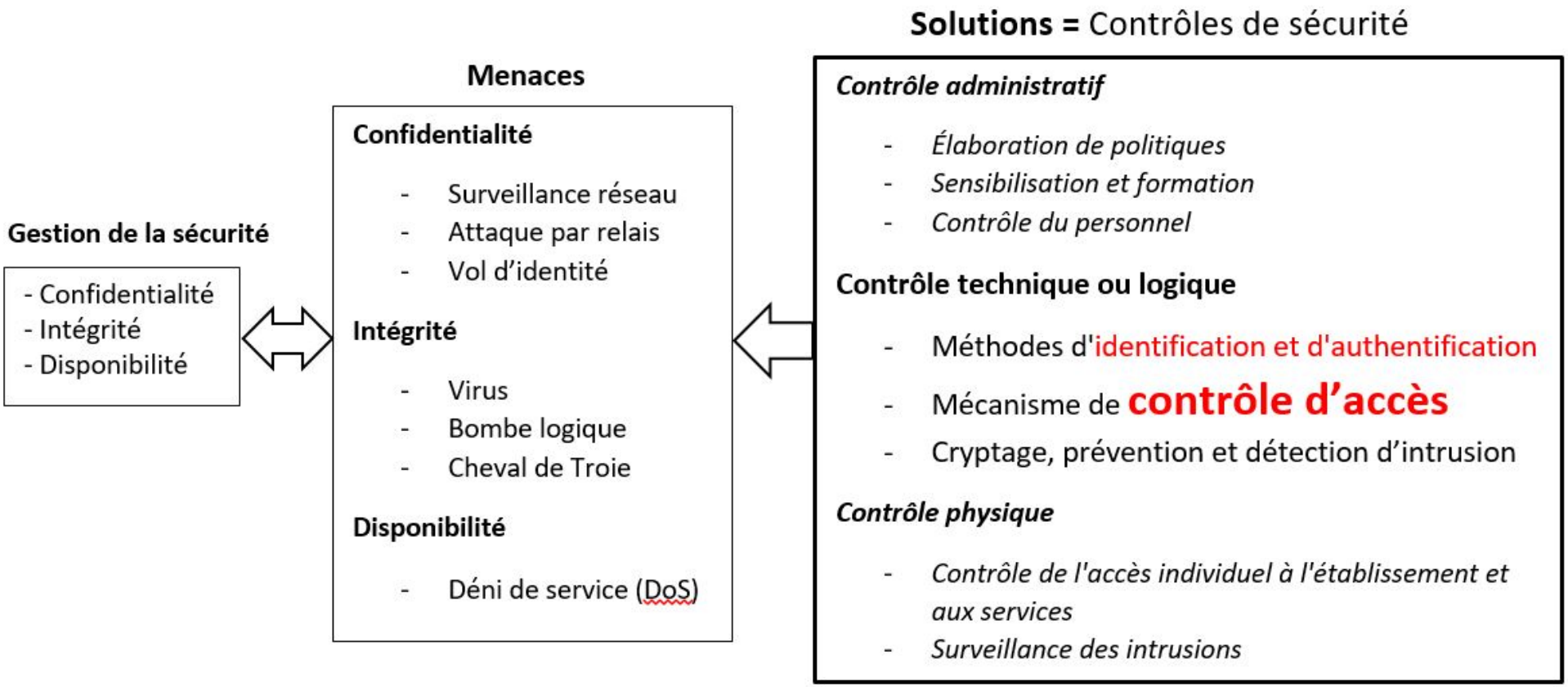
Recherches effectuées

1. La sécurité des informations
   - le contrôle d'accès ;
   - les méthodes d'authentification des utilisateurs.

2. Interopérabilité des systèmes d'information
   - l'architecture orientée services (SOA) et les services web ;
   - le contrôle d'accès dans SOA ;
   - la composition de services.

Sécurité des informations

« La protection des systèmes d'information et d'information contre l'accès, l'utilisation, la divulgation, la perturbation, la modification ou la destruction non autorisés afin de garantir la **confidentialité**, l'**intégrité** et la **disponibilité** ». (CNSS, 2010)



Le contrôle d'accès

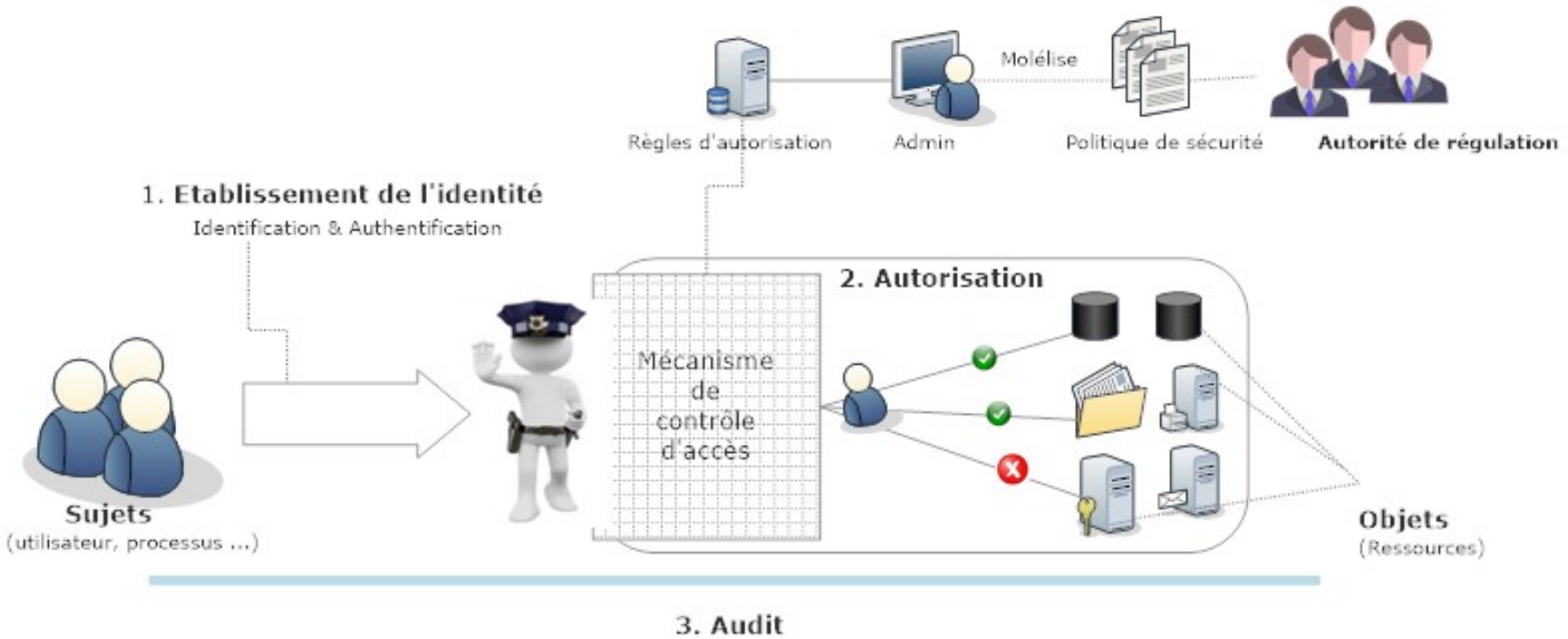


FIGURE – Le contrôle d'accès - Concepts et fonctionnement

Objectifs : Confidentialité, intégrité et disponibilité des informations

Identification et Authentification

Identité : C'est la représentation numérique des données relatives à une entité active (e.g. utilisateur humain, système hôte ou un périphérique réseau, agent de programmation). Souvent encapsulée sous forme de **compte** ou profil.

Identification : C'est le moyen par lequel un utilisateur fournit une identité revendiquée au système (e.g. un identifiant, nom d'utilisateur, pseudo)[2].

Authentification : C'est le processus de validation de l'identité présumée d'un utilisateur. L'authentification est l'identification sécurisée des entités pendant laquelle une preuve de possession d'une identité est vérifiée [1].
Cette preuve peut être :

- *Quelque chose que l'utilisateur* ***connait*** :
  un secret (e.g. Un mot de passe, un numéro d'identification personnel) ;
- *Quelque chose que l'utilisateur* ***possède*** :
  un jeton (e.g., carte d'accès, carte de crédit, jeton *USB*, ticket *kerberos*) ;
- *Quelque chose que l'utilisateur* **est** :
  les empreintes digitales, la géométrie de la main, la forme des yeux, la voix, la reconnaissance faciale, la signature de la main etc...

Modèles d'authentification

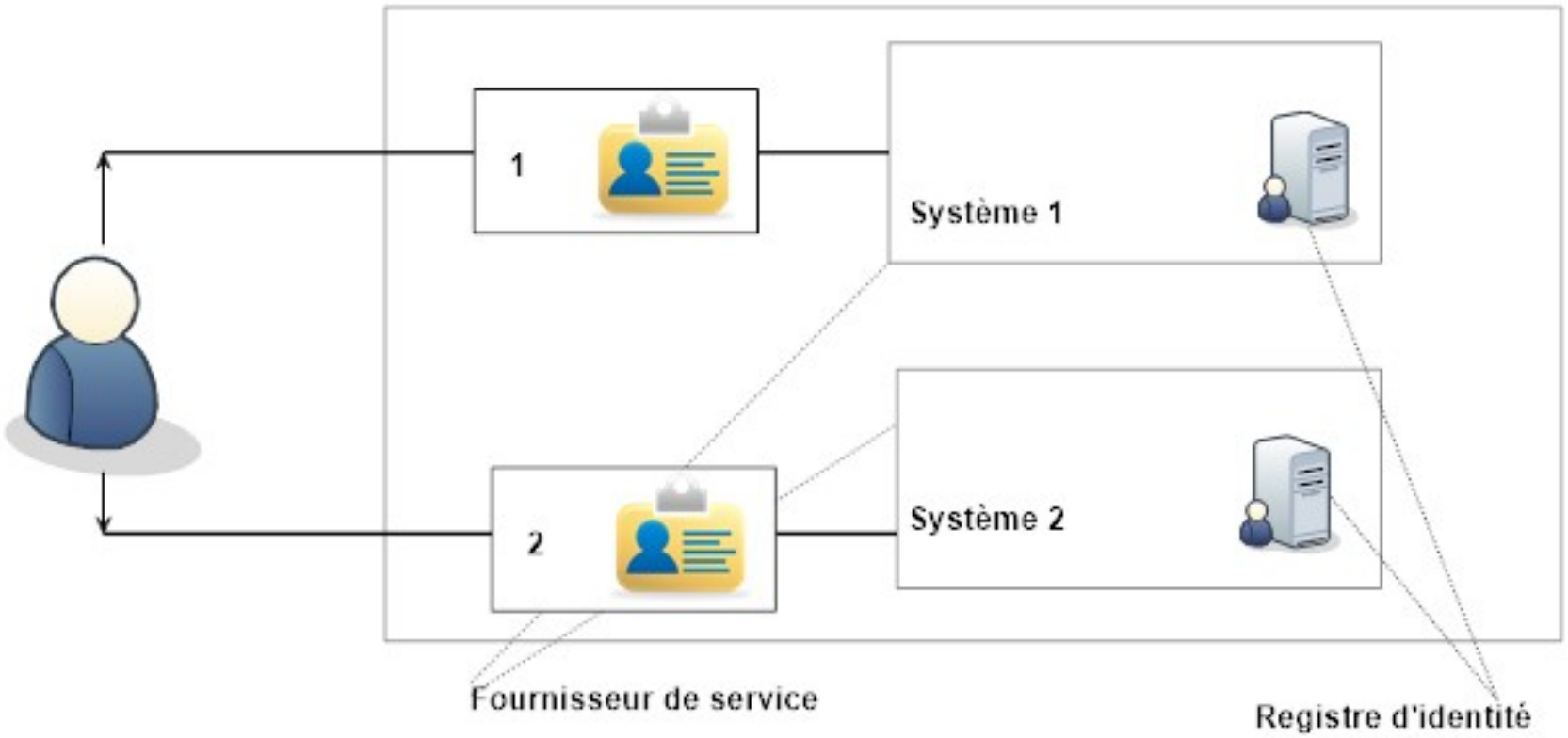


FIGURE – Modèle de gestion isolée de l'identité

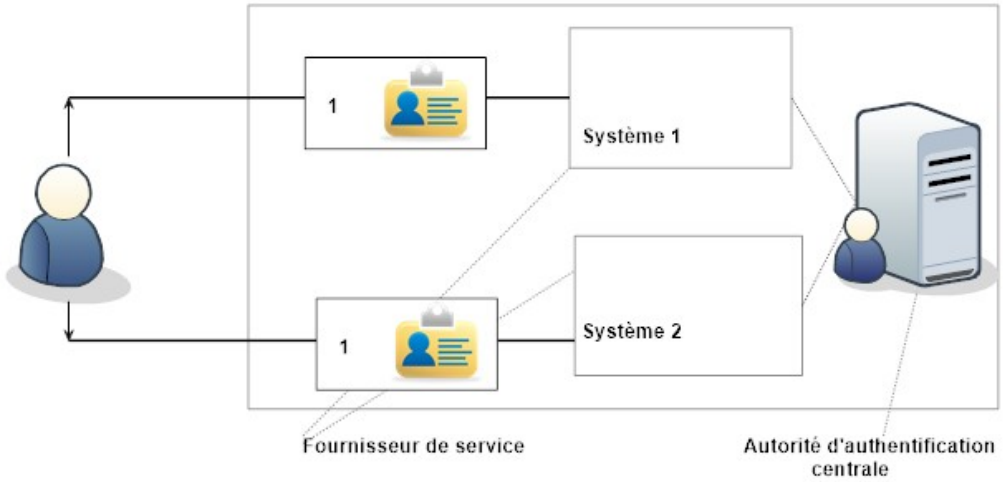


FIGURE – Modèle commun de gestion de l'identité

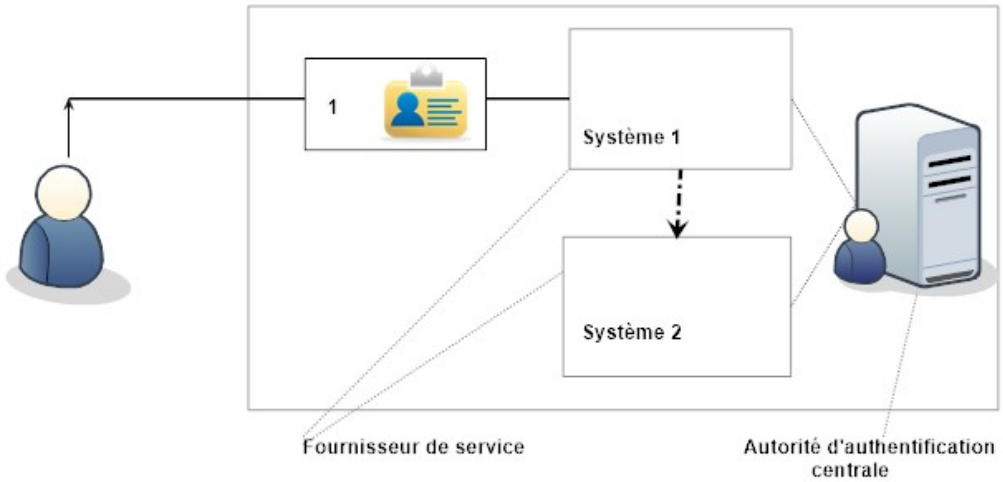


FIGURE – Gestion de l'identité avec l'authentification unique

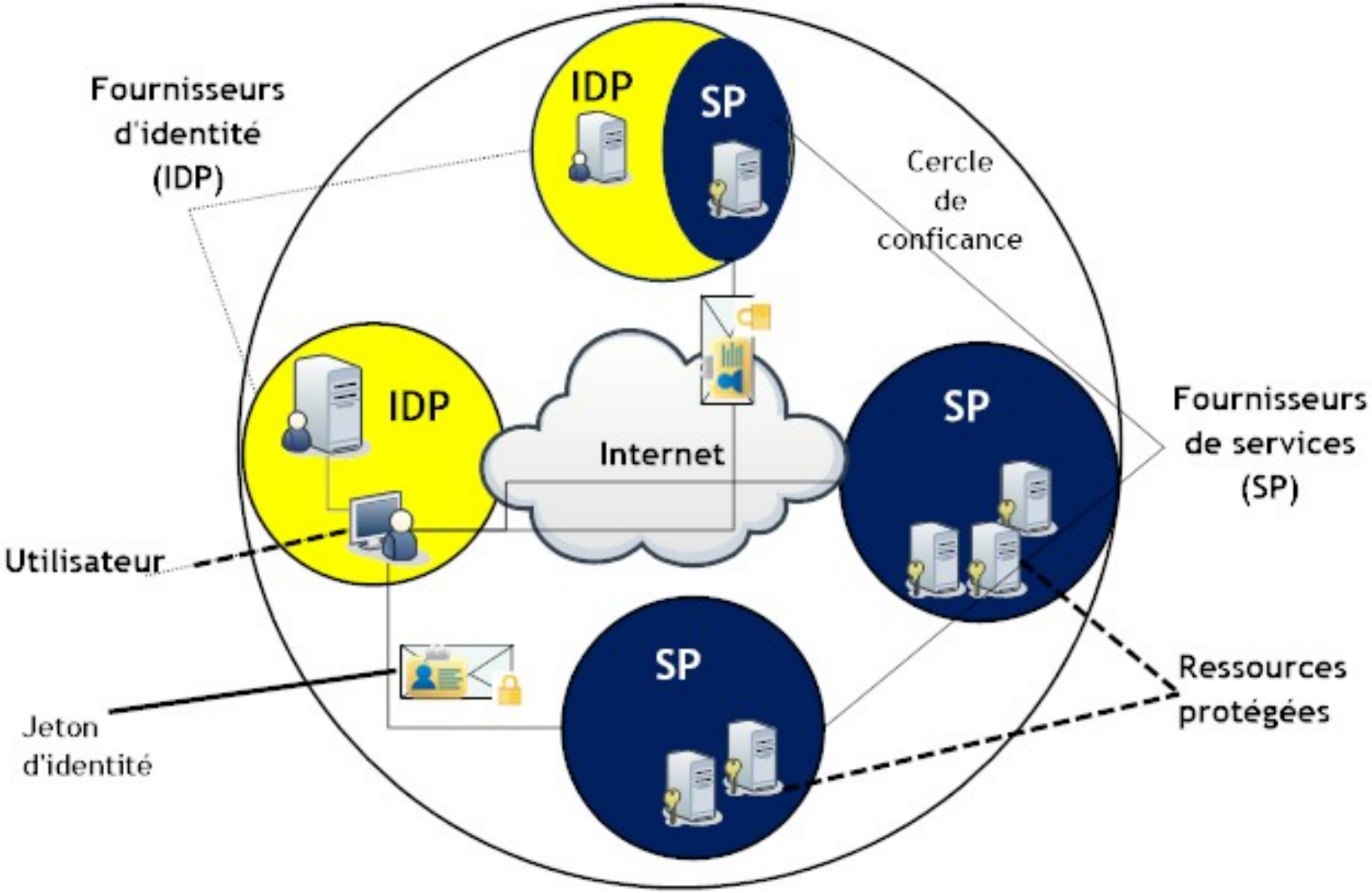


FIGURE – Modèle de gestion fédérée de l'identité

Modèles d'autorisation

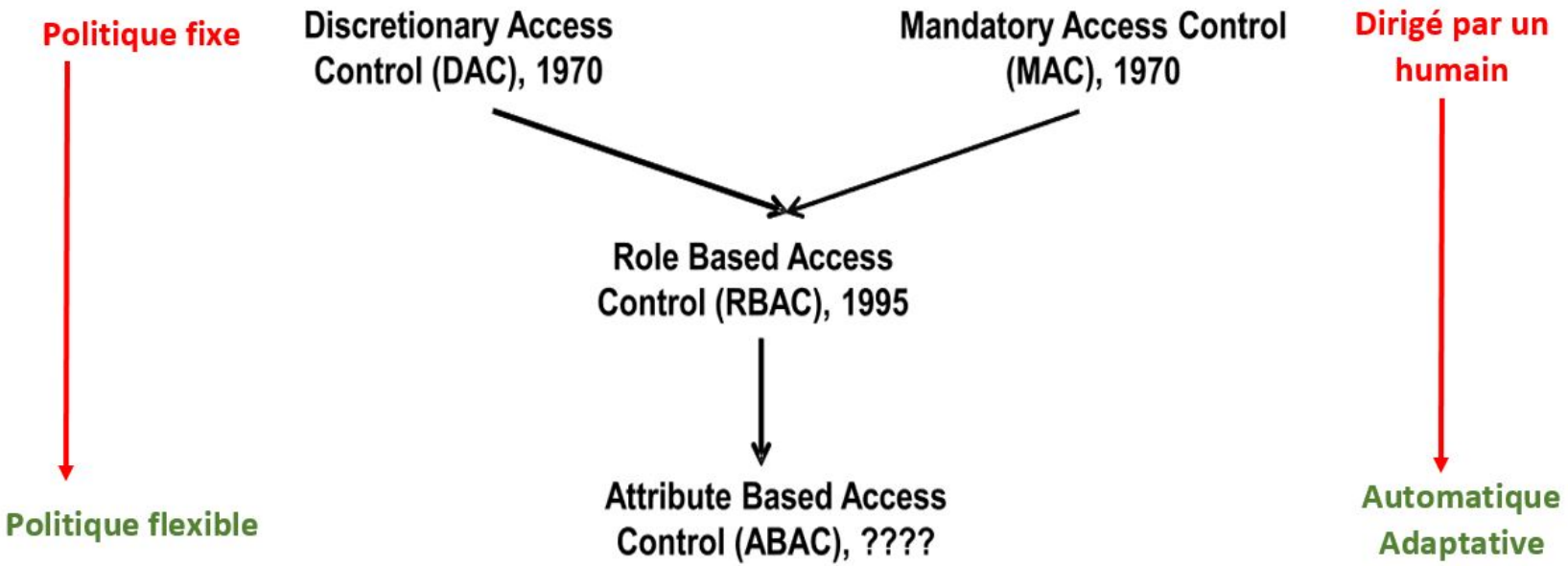
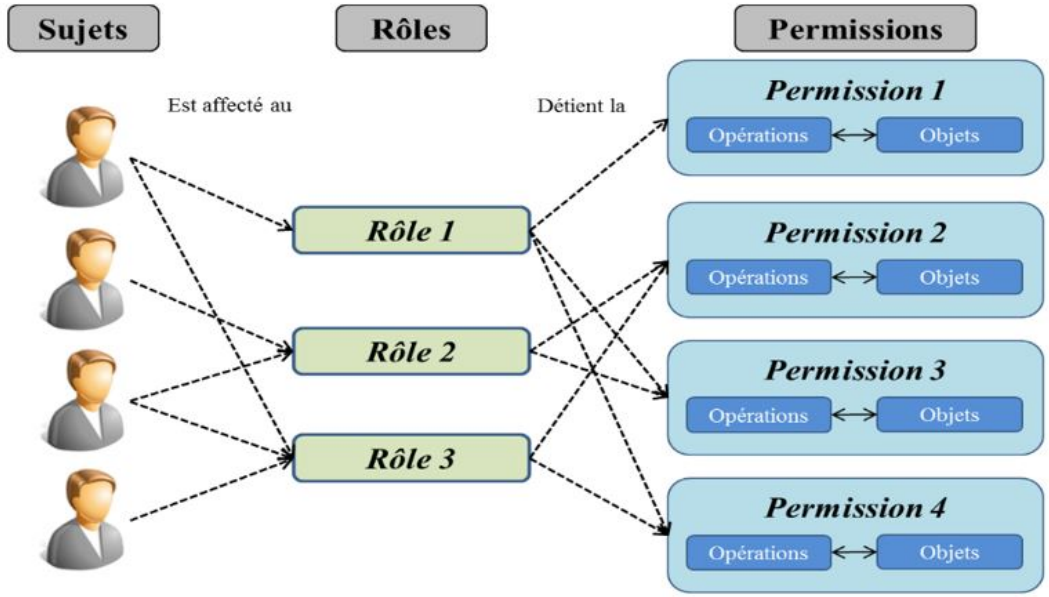
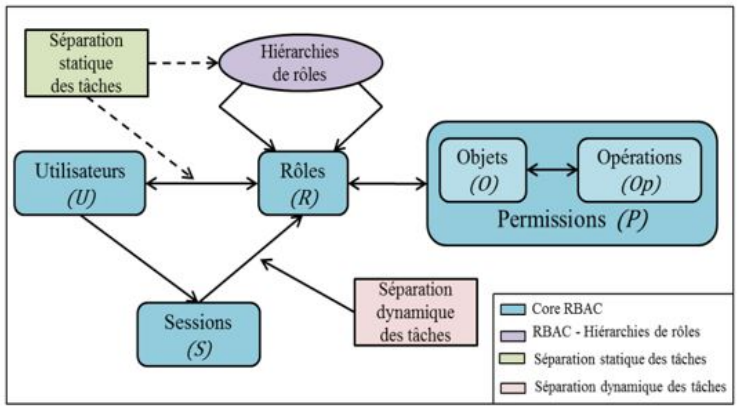


FIGURE – Chronologie des modèles classiques de contrôle d'accès [3]

Modèles d'autorisation

Contrôle d'accès basé sur les rôles (*RBAC*)





Avantages

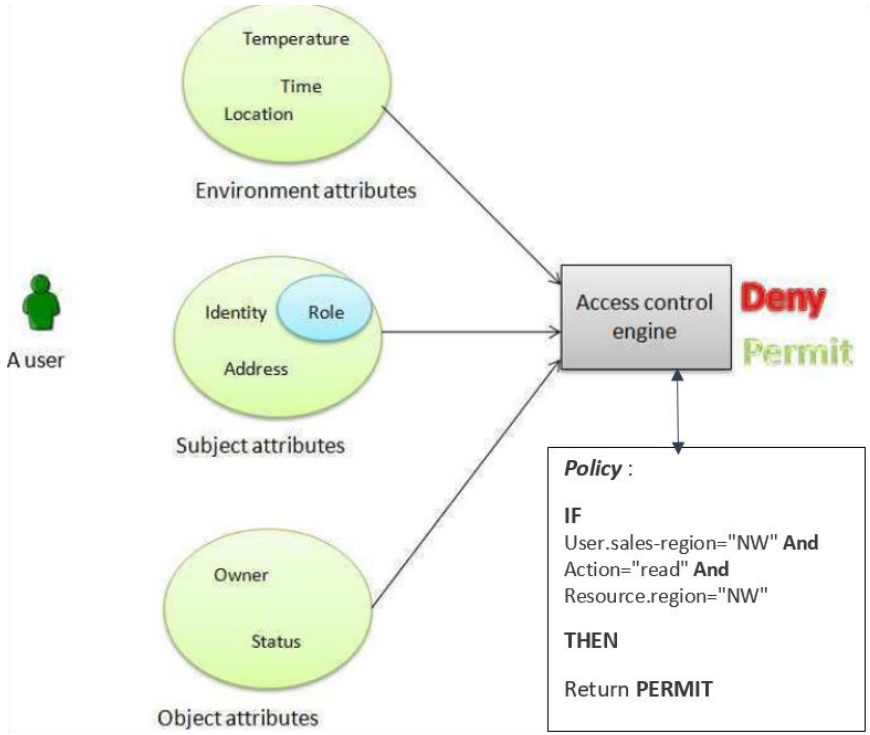
- Simple, flexible
- Administration facile

Inconvénients

- Contextes non considérés
- Expression des politiques de fine granularité difficile
- **Attribution statique des rôles aux utilisateurs**

Modèles d'autorisation

Contrôle d'accès basé sur les attributs (*ABAC*)



Avantages

- Flexible, dynamique et sécurisé
- Supporte les utilisateurs externes
- Supporte DAC, MAC et RBAC

Inconvénients

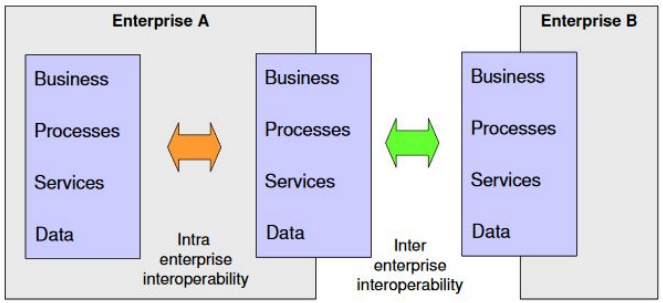
- L'audit des autorisations est difficile
- Gestion complexe des attributs
- Explosion de règles : N attributs -> 2^N règles

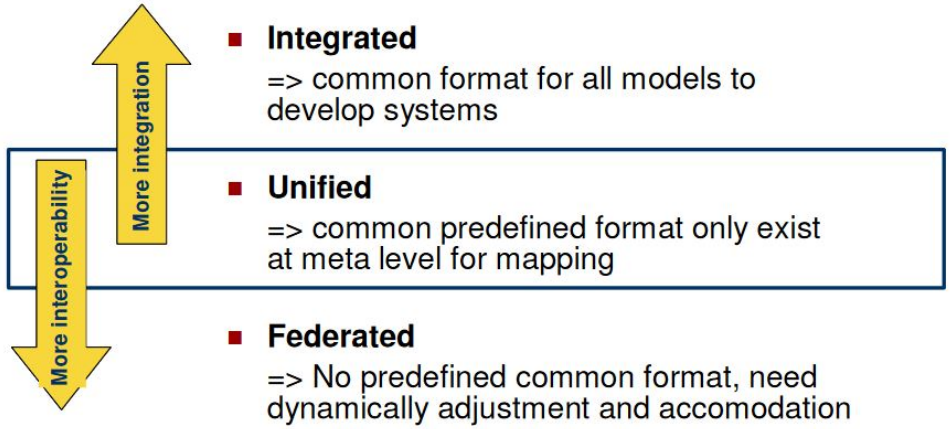
Comparaison des modèles d'autorisation

Modèle	DAC	MAC	RBAC	TBAC	TMAC	CAAC	SAC	OrBAC	O2O	Poly-ORBAC	ABAC	RadAC
Complexité	+	+	+	+	+	-	-	+	-	-	-	-
Abstraction	-	-	+	+	+	+	+	+			+	+
Expressivité	+	+	+	+	+	+	-	+			+	+
Applicabilité	+	+	+	-	-	+	-	+			+	+
Granularité	+	+	-	-	-	+	-	+			+	+
Contexte	-	-	-	+	+	+	-	+			+	+
Collaboration	-	-	-	-	-	-	+	-	+	+	+	+
Sécurité	-	+	+	+	+	+	-	+	+	+	+	+
Facilité d'utilisation	+	-	+	-	+	+	-	+	-	-	+	+
Administration	-	-	+	-	-	-	-	+	-	-	+	-

FIGURE – Comparaison des modèles de contrôle d'accès

Interopérabilité des systèmes d'information





Approches de mise en œuvre

Défi : Inter-opérer simultanément avec de multiples partenaires hétérogènes. Ce qui signifie, pouvoir ajuster et adapter ses systèmes en permanence et sans délai.

Solutions :

- **L'approche fédérée** permet aux entreprises de garder leur autonomie (modèles, protocoles, outils, identité) réduisant ainsi le temps, le coût pour établir l'interopérabilité.
- Spécifications, Standards, une architecture d'entreprise dynamique (l'**orientation Service**)

Architecture orientée services (SOA)

Service Oriented Computing (SOC) : Paradigme de l'informatique réparti qui permet de construire des réseaux d'applications en utilisant les services comme éléments fondamentaux pour le développement d'applications.

SOA : « une architecture d'application dans laquelle toutes les fonctions sont définies comme des services indépendants possédant des interfaces bien définies qui peuvent être appelées dans des séquences définies pour former des processus d'entreprise ».[Channabasavaiah et al.]

Service : « Un service est une unité de logique de solution à laquelle l'**orientation service** a été appliquée dans une mesure significative ». [Thomas Erl]

Implémentation

- Service web WS-* (SOAP, WSDL, XML), ESB (Entreprise Service Bus)
- Service web REST, Web (HTTP, JSON, WADL)
- Composants (*SCA*), *JINI (Apache River)* etc...

Sécurité dans SOA - Sécurité des services web

Dimension	Requirement	Specifications
Messaging	Confidentiality and Integrity	WS-Security
		SSL/TLS
	Authentication	WS-Security Tokens
		SSL/TLS X.509 Certificates
Resource	Authorization	XACML
		XrML
		RBAC, ABAC
	Privacy	EPAL
		XACML
	Accountability	None
Negotiation	Registries	UDDI
		ebXML
	Semantic Discovery	SWSA
		OWL-S
	Business Contracts	ebXML
Trust	Establishment	WS-Trust
		XKMS
		X.509
	Trust Proxying	SAML
		WS-Trust
	Federation	WS-Federation
		Liberty IDFF
		Shibboleth

Conclusion

L'orientation service - SOA permet d'accéder à des services et à une composition de services appartenant à différents domaines hétérogènes en une seule session.

L'approche fédérée permet de garder son autonomie (modèles, protocoles, outils, identité).

La gestion fédérée de l'identité permet d'accéder à différents services appartenant à des domaines hétérogènes avec une seule identité.

Malheureusement, il manque de solutions pour un contrôle d'accès sophistiqué impliquant différentes politiques.

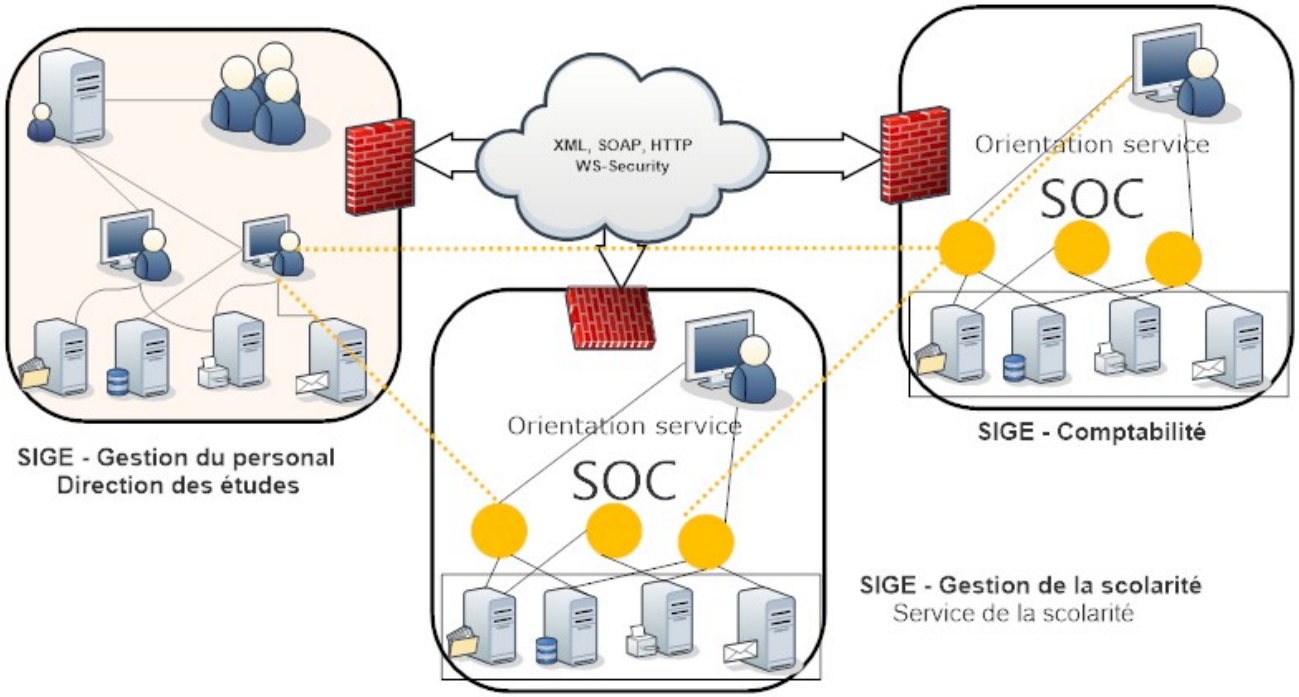
Plan pour la suite

- Traitement d'un cas d'interopérabilité impliquant différentes politiques de contrôle d'accès (e.g. ABAC et RBAC)

- Modélisation de solutions à l'aide d'automates à états ou d'algèbres de processus, pour prendre en compte l'interopérabilité des sources de données, les comportements possibles et autorisés selon les permissions accordées aux utilisateurs.

Questions

Merci pour votre attention



Messaoud Benantar.
Access control systems : security, identity management and trust models.
Springer Science - Business Media, 2006.

Barbara Guttman and Edward A. Roback.
An introduction to computer security : the NIST handbook.
DIANE Publishing, 1995.

Jin Xin.
ATTRIBUTE-BASED ACCESS CONTROL MODELS AND IMPLEMENTATION IN CLOUD INFRASTRUCTURE AS A SERVICE.
phdthesis, University of Texas at San Antonio, 2014.