Alessandro Neri

SICUREZZA DELLE INFORMAZIONI NELL'UNIVERSO COOPERANTE DELLE SMART CITIES

Colloquia sulle Infrastrutture Critiche
Smart Cities: opportunità di sviluppo nella Complessità
Roma 28 marzo 2011

ROMA TRE UNIVERSITÀ DEGLI STUDI

Contenuti

RadioLabs

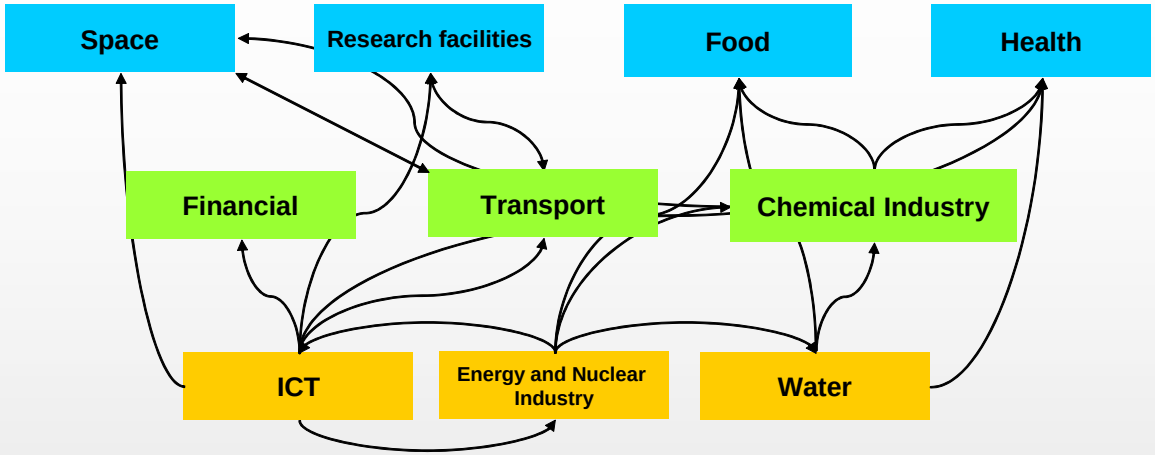
- Smart cities come sistemi di sistemi complessi
- Interdipendenze tra Infrastrutture (Critiche)
- Requisiti di sicurezza nella condivisione delle informazioni
- Modelli di sicurezza
- Architetture logiche della sicurezza
- Conclusioni

Smart cities come sistemi di sistemi complessi

- SCOPO: Migliorare la ***Qualità della vita*** preservando al tempo stesso
  - Risorse naturali (Ambiente)
  - Patrimonio e identità culturale
  - Occupazione
- ELEMENTI SFIDANTI:
  - Molteplicità di sistemi con interdipendenze complesse
  - Molteplicità di attori
  - Molteplicità di obiettivi
  - Grande quantità di dati

    (Smart Santander: 20.000 sensori)

Infrastrutture (critiche)



- Infrastrutture: di per sè elementi di potenziale debolezza essendo esposte a numerose minacce in relazione alla sicurezza (safety and security).
- Infrastrutture attuali: ancora più vulnerabili,
  - incremento dell'efficienza e riduzione dei costi provocano riduzione dei margini di sicurezza, maggiore complessità tecnologica e maggiore interdipendenza.
- Condivisione delle informazioni tra Infrastrutture: elemento chiave per
  - aumentare l'efficienza e la qualità dei servizi,
  - aumentare l'efficacia degli interventi in presenza di guasti e/o attacchi.
- Le interazioni e le dipendenze mutue implicano che la protezione deve estendersi oltre i confini della singola infrastruttura.

Mobilità: scenario evolutivo

Predizione dei flussi di traffico a lungo termine a bassa risoluzione spazio-temporale

Predizione dei flussi di traffico a breve termine ad alta risoluzione spazio-temporale

Indicazioni in tempo reale per evitare congestioni

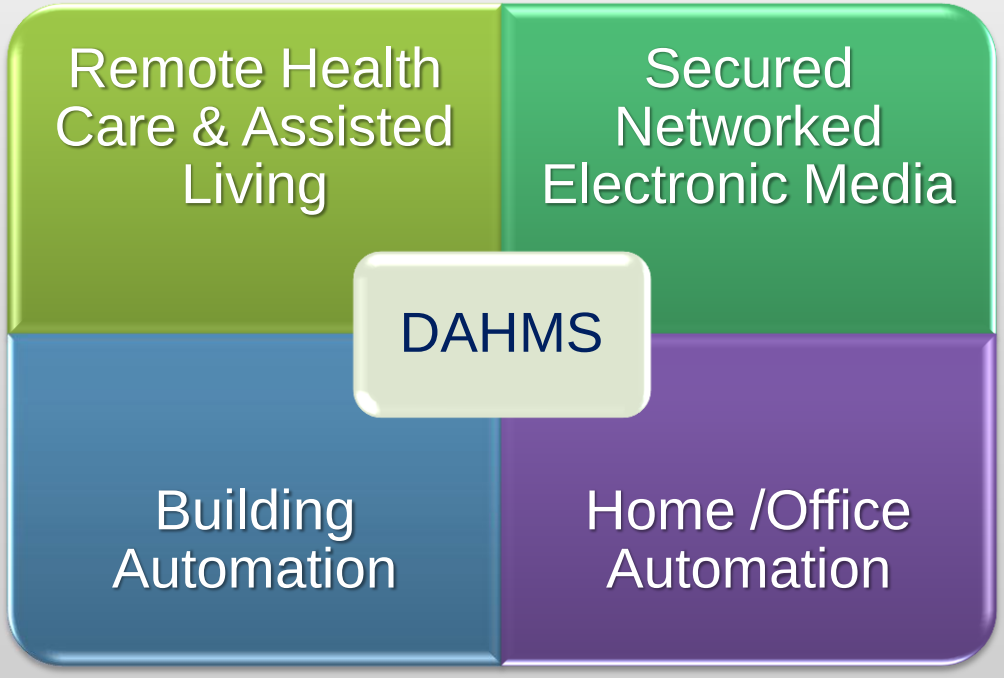
Ottimizzazione globale dei flussi di traffico con benefici individuali

Strumenti

- Modelli basati su agenti
- Monitoraggio cooperante e proattivo del traffico: ogni veicolo fornisce la propria posizione e la destinazione
- Reti dedicate alle comunicazioni tra Veicoli e tra veicoli e infrastruttura

Ambienti domestici e lavorativi

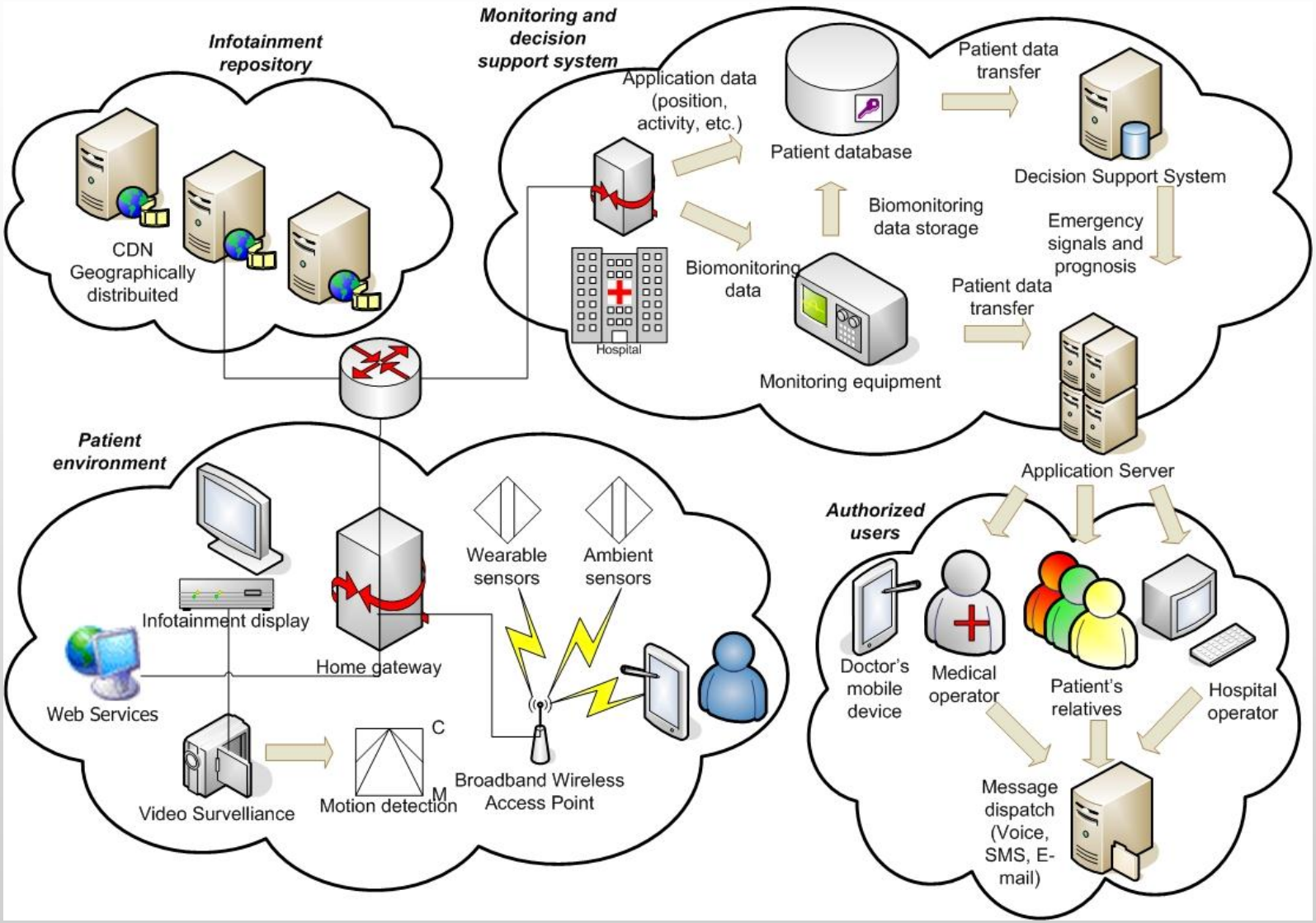
- Piattaforme unificate per "servizi immersivi" che migliorano "l'esperienza dell'utente"
  - Ex.: OMEGA project finanziato da EU-FP7
  - Ex.: DAHMS progetto cofinanziato dal Ministero Sviluppo Economico



ROMA TRE UNIVERSITÀ DEGLI STUDI

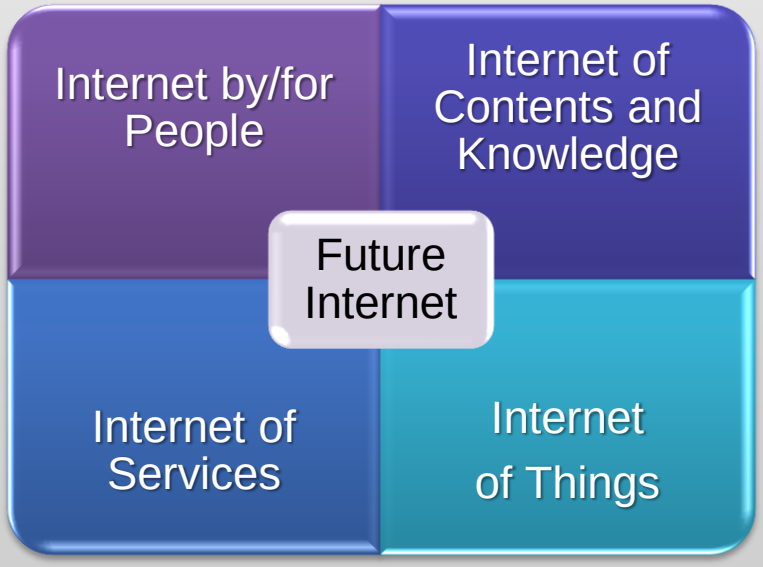
HOME 2.0

RadioLabs



Reti di sensori

- le tendenze attuali nel campo delle reti di sensori indicano, come modelli architetturali di riferimento per i prossimi anni, soluzioni in cui gli apparati sensoriali sono basati su unità in grado di elaborare i dati acquisiti e di fornire informazioni in modo autonomo alla stregua di tutti gli altri oggetti dell'Internet of Things
- Internet of Things dà un indirizzo Internet (URL) a cose tangibili o a siti.



Reti di sensori autonomiche

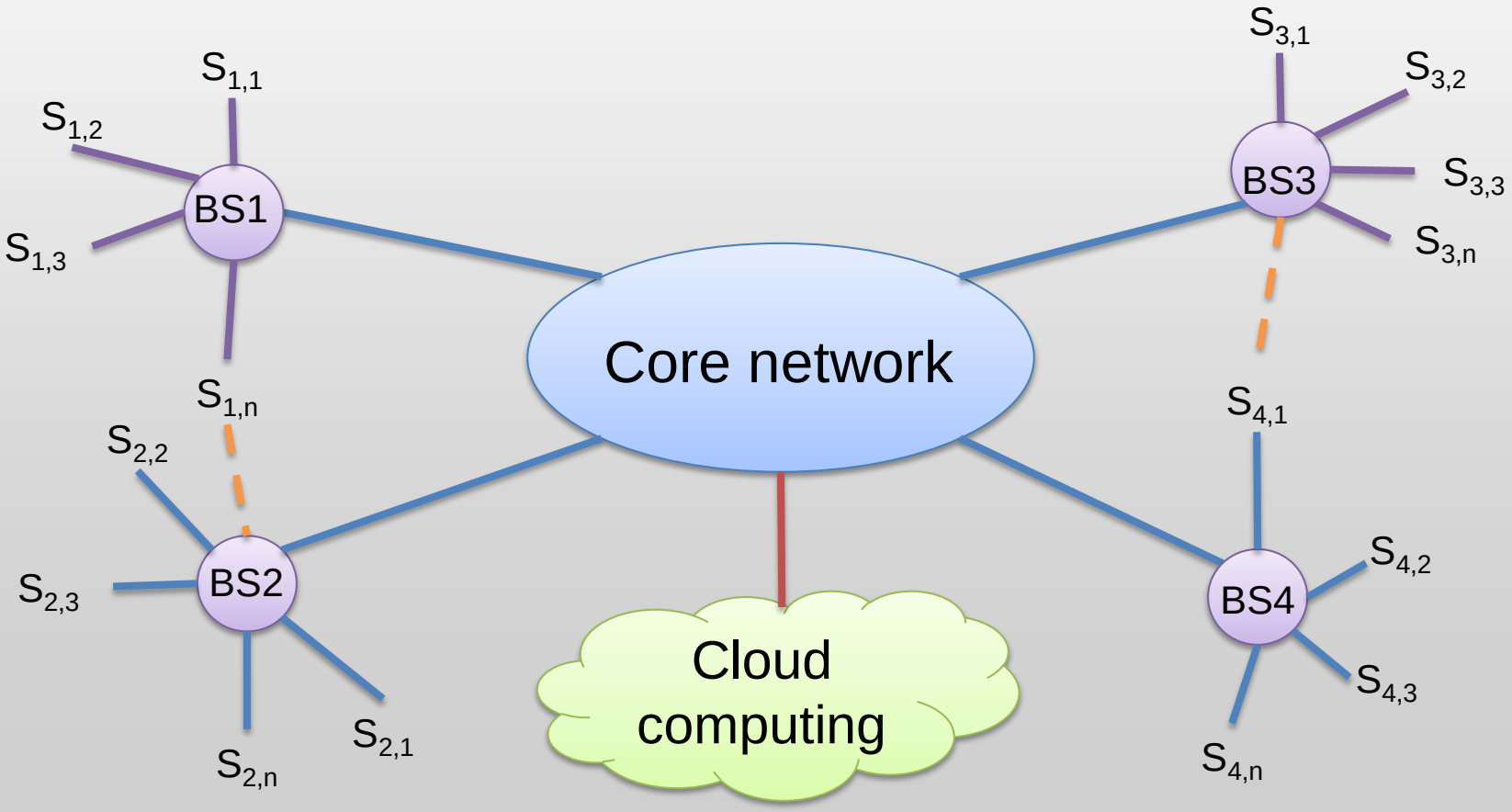
- Disporre di sensori con capacità di elaborazione locale, seppur limitata, in tutto e per tutto assimilati a nodi della rete Internet, rende possibili nuove forme di gestione delle reti di sensori di tipo **autonomico** basate su
  - condivisione della conoscenza in relazione a
    - ambiente (radio) in cui operano,
    - potenzialità, funzionalità e grado di funzionamento corrente degli apparati,
    - carico corrente,
    - topologia della rete
    - stato dei singoli collegamenti e degli apparati,
  - capacità di adattarsi rapidamente alle variazioni del contesto, mettendo eventualmente in essere anche meccanismi di autodifesa.

Reti di sensori autonomiche - Vantaggi

- Facilità di dispiegamento
- Altissima scalabilità
- Alta immunità rispetto a guasti locali
- Resistenza ad eventi catastrofici di origine naturale e umana, accidentale o intenzionale
- Bassi costi di pianificazione
- Bassi costi di gestione
- Bassi costi di manutenzione
- Possibilità di condividere risorse (ad es. Rete d'accesso) con altre reti
- Alto grado di flessibilità, di affidabilità e di sicurezza delle reti.

Architettura generale di rete

- Le architetture basate sul paradigma “Internet of Things” rendono possibili nuove modalità di interscambio e cooperazione basate **reti di reti federate** di sensori in cui i dati acquisiti da una rete sono resi disponibili ai gestori delle altre reti al fine della compilazione di un quadro della situazione corrente e/o di quelle future più completo ed affidabile.



Elementi critici indotti dalle tecnologie ICT

Internet of Thinks	Cloud computing	Open Service Platforms
• Gli oggetti possono rivelare la presenza di altri oggetti e comunicare autonomamente con essi. • Tutti gli oggetti sono potenzialmente raggiungibili via Internet	• Virtualizzazione di servizi attraverso l'uso ottimizzato flessibile e granulare di risorse di elaborazione e memorizzazione. • Nessun limite per il numero di utenti e di risorse utilizzate	• Interoperabilità di piattaforme, componenti, servizi di base, • intensa cocreazione di servizi (mesh up) e contenuti che coinvolge una molteplicità di utenti

ROMA TRE UNIVERSITÀ DEGLI STUDI

RadioLabs

"Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures"

MICIE Project

SELEX Communications A Finmeccanica Company

ROMA TRE UNIVERSITÀ DEGLI STUDI

ENEA ENTE PER LE NUOVE TECNOLOGIE, L'ENERGIA E L'AMBIENTE

itrust consulting s.à r.l.

SAPIENZA UNIVERSITÀ DI ROMA CRAT

CENTRE DE RECHERCHE PUBLIC HENRI TUDOR CENTRE D'INNOVATION PAR LES TECHNOLOGIES DE L'INFORMATION CITI

PIAP

UNIVERSITY OF BRADFORD MAKING KNOWLEDGE WORK

Multitel

SEVENTH FRAMEWORK PROGRAMME

Information Society

www.micie.eu

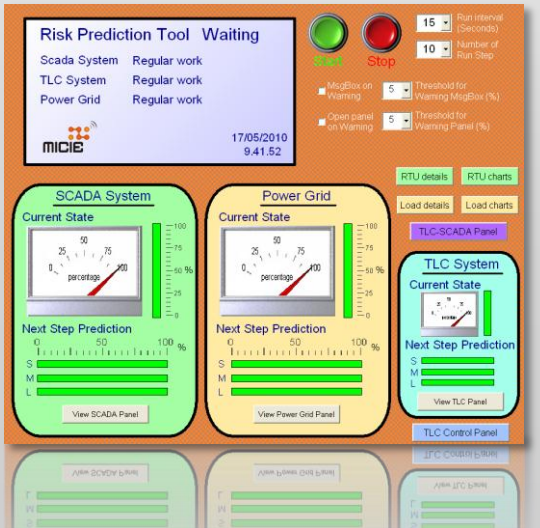
ICT-SEC 225353

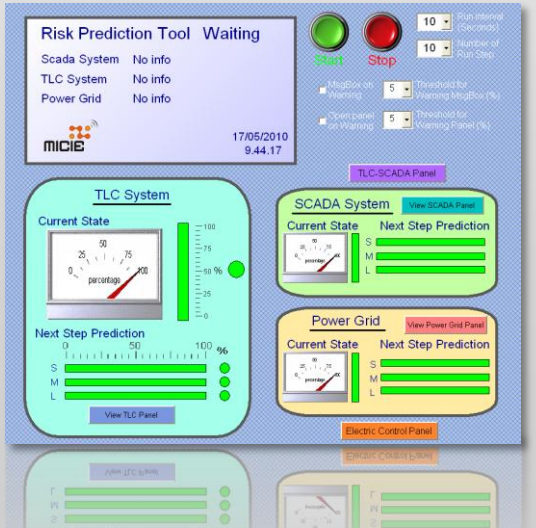
MICIE

- Il Progetto MICIE è caratterizato da un approccio sistematico alla gestione del rischio in scenari con CI fortemente interdipendenti
  - Miglioramento di modelli e strumenti per l'interdipendenza tra infrastrutture
  - Scambio on-line dell'informazione relativa ai liveli di rischio tra infrastrutture mutuamente dipendenti.
  - Strumento per la predizione dei livelli di rischio basata su
    - Elaborazione delle misure collezionate dalla strumentazione di monitoraggio e controllo (e.g. SCADA) dell'infrastruttura relativa.
    - Elaborazione dei metadati relativi allo stato di rischio ed ai livelli prestazionali dei servizi erogati dalle altre infrastrutture.
- La piattaforma è stata sperimentata su uno scenario reale nell'ambiente di test realizzato dalla Israel Electric Corporation (IEC).

Predizione del rischio

- Oltre a numerosi modelli di rischio **off-line** specializzati in grado di integrare i metodi di valutazione del rischio con i modelli di interdipendenza, MICIE propone un strumento di valutazione del rischio **on-line**.
- Il predittore del rischio on-line, basato sull'evoluzione del modello delle interdipendenze, integra
  - dettagli a basso livello
  - dipendenze ad alto livello

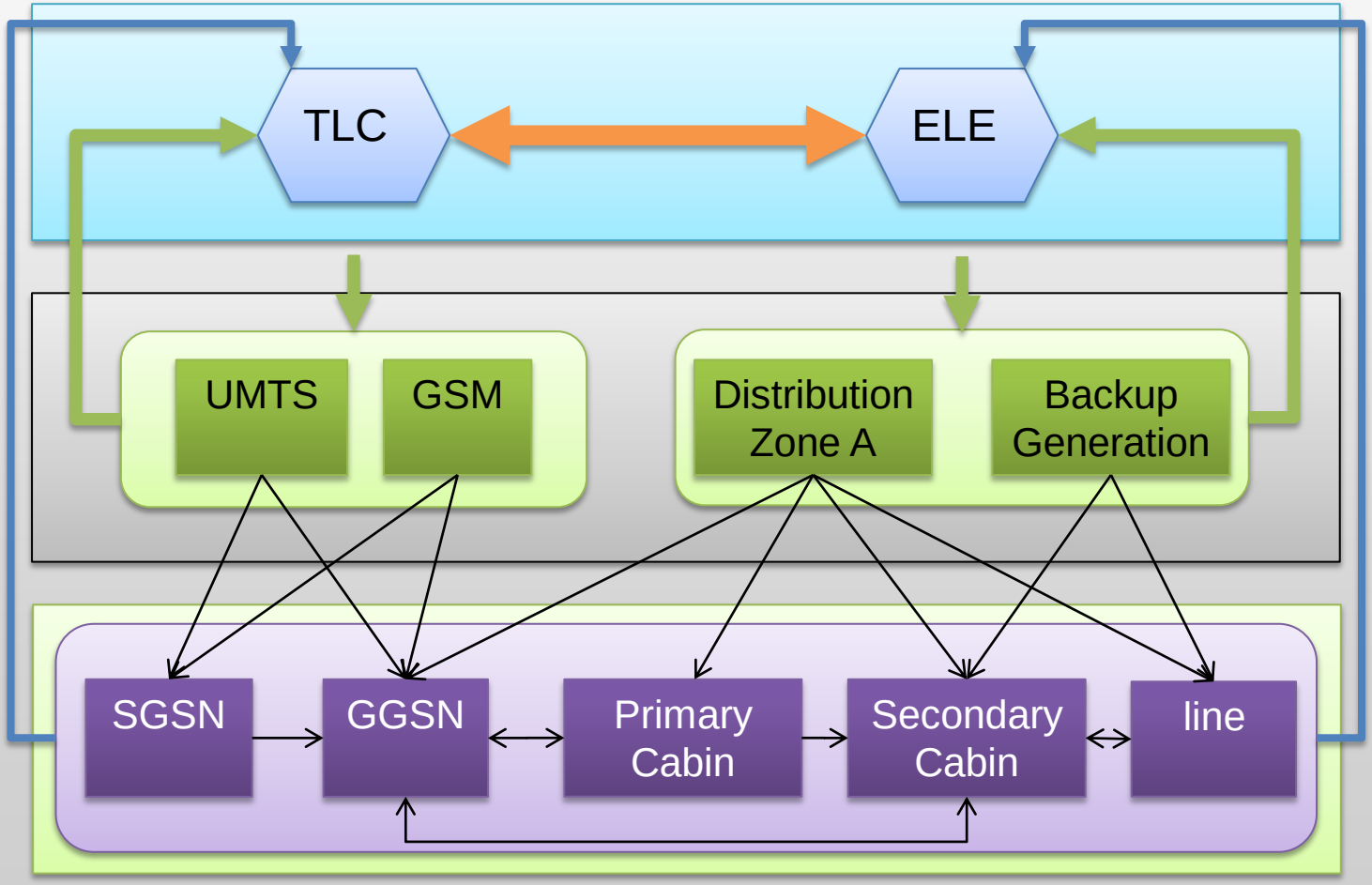




Modello Misto OLISTICO-REDUZIONISTA

- Comportamenti emergenti non predicibili dallo strato reduzionista

Holistic Layer | Service Layer | Redutionistic Layer



Predizione del rischio

- In MICIE ogni Infrastruttura Critica (CI) usa un proprio predittore del rischio, alimentato dal monitoraggio delle componenti interne alla CI e dai metadati forniti dalle CI interconnesse.
- Le uscite del predittore sono utilizzate sia dall'operatore che dai predittori delle altre infrastrutture.
- Infrastrutture interdipendenti scambiano direttamente le informazioni rilevanti, migliorando semplicità, privacy e scalabilità.
- La comunicazione da CI a CI si basa su un **Secure Mediation Gateway** (SMGW).

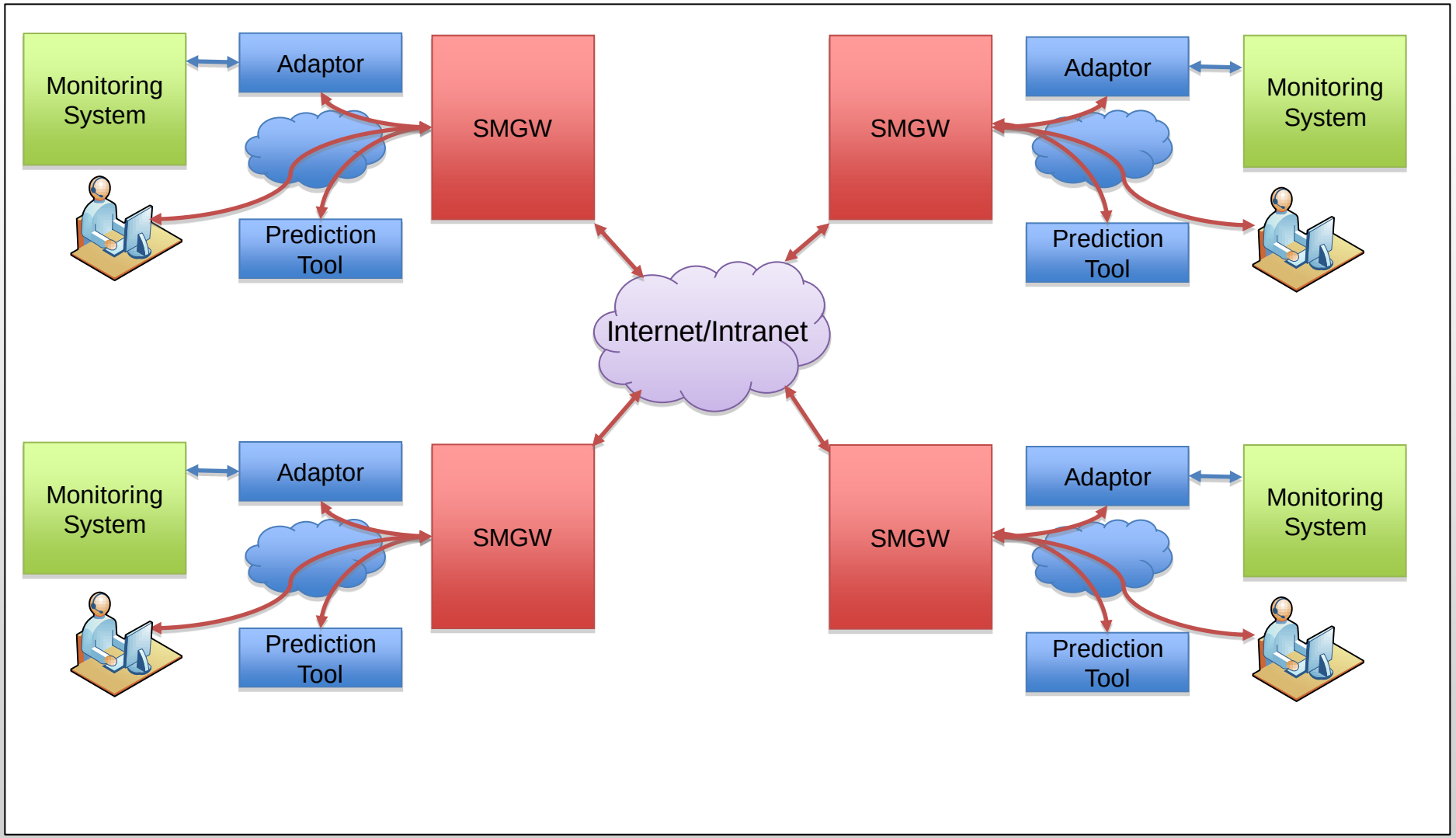
ROMA TRE UNIVERSITÀ DEGLI STUDI

SMGW

RadioLabs

- In MICIE è stato progettato e realizzato, in ogni SMGW, un middleware che fa uso di agenti che si scambiano i metadatati in modo sicuro,
- Gli agenti
  - prendono in considerazione i meccanismi di sicurezza e i livelli di sicurezza attualmente disponibili nei settori ICT coinvolti in scambi di informazioni
  - selezionano i meccanismi di sicurezza più appropriati per lo scambio dei metadati
- Il SMGW garantisce, anche in ambienti federati,
  - confidenzialità,
  - integrità,
  - disponibilità,
  - autenticità
  - non-ripudio
  - tracciabilità

MICIE - architettura generale



Modello di Sicurezza

***Modo IntraCI**:* si riferisce alle comunicazioni tra SMGW e gli adattatori per la connessione degli apparati periferici (e.g. SCADA) e tra SMGW e predittore del rischio.

Modo IntraCI

- Basato su IPSec
- Protezione delle chiamate locali al SMGW

Modo InterCI

- Livello di Trasporto
  - SSL/TLS (*HTTPS*)
- Livello Applicativo (*Web Services*)
  - Confidenzialità, Integrità, Autenticità
    - Cifratura XML, Firma XML
  - Struttura del Message, Sicurezza del Messaggio
    - WS-Security
  - Metadati
    - WS-Policy

Modello di Sicurezza

***Modo InterCI**:* si riferisce alle comunicazioni tra SMGW di infrastrutture diverse o tra SMGW e operatore.

.

Modo IntraCI

- Basato su IPSec
- Protezione delle chiamate locali al SMGW

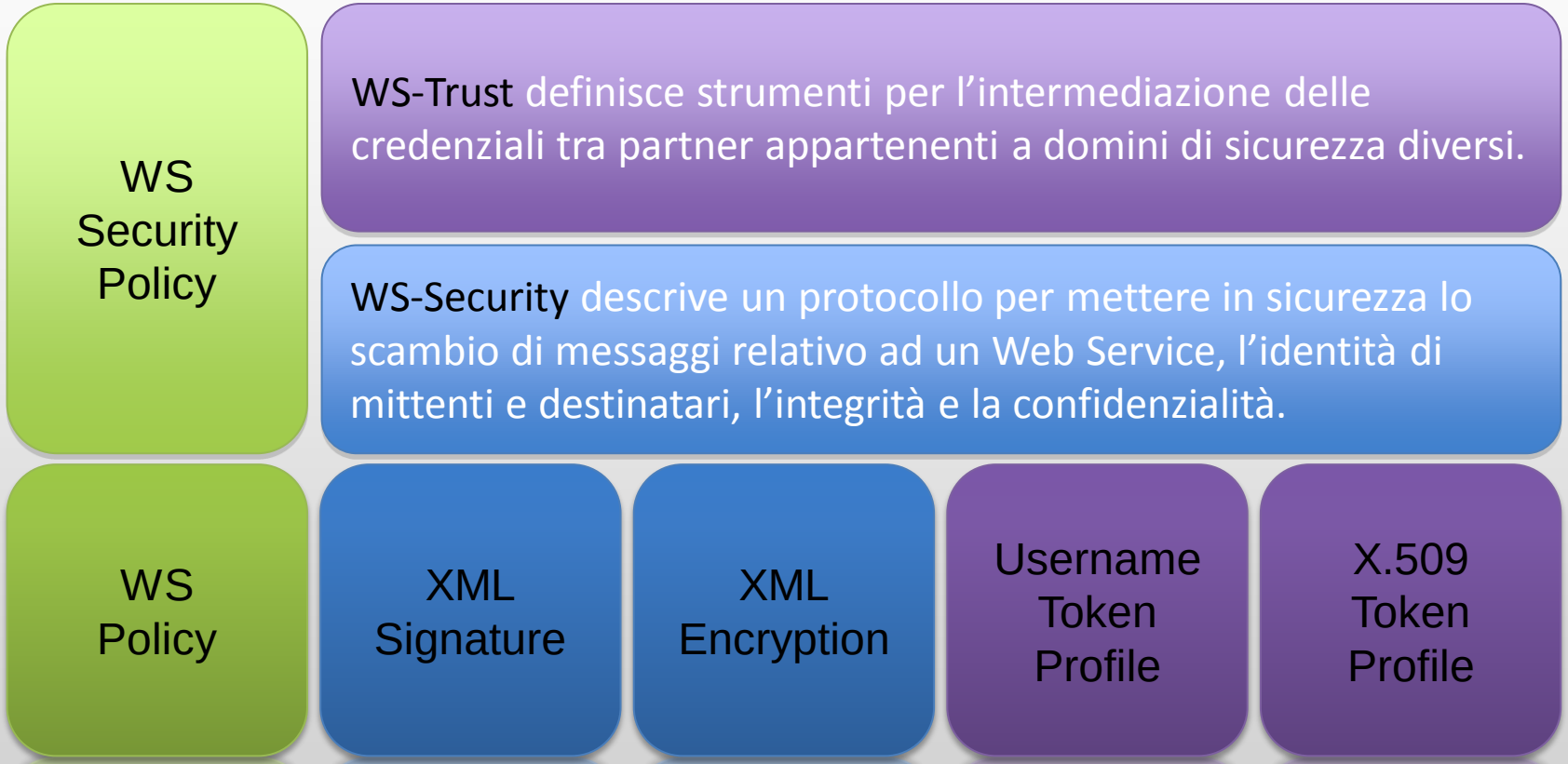
Modo InterCI

- Livello di Trasporto
  - SSL/TLS (*HTTPS*)
- Livello Applicativo (*Web Services*)
  - Confidenzialità, Integrità, Autenticità
    - Cifratura XML, Firma XML
  - Struttura del Message, Sicurezza del Messaggio
    - WS-Security
  - Metadati
    - WS-Policy

ROMA TRE UNIVERSITÀ DEGLI STUDI

Piattaforma di sicurezza per WS

RadioLabs



ROMA TRE UNIVERSITÀ DEGLI STUDI

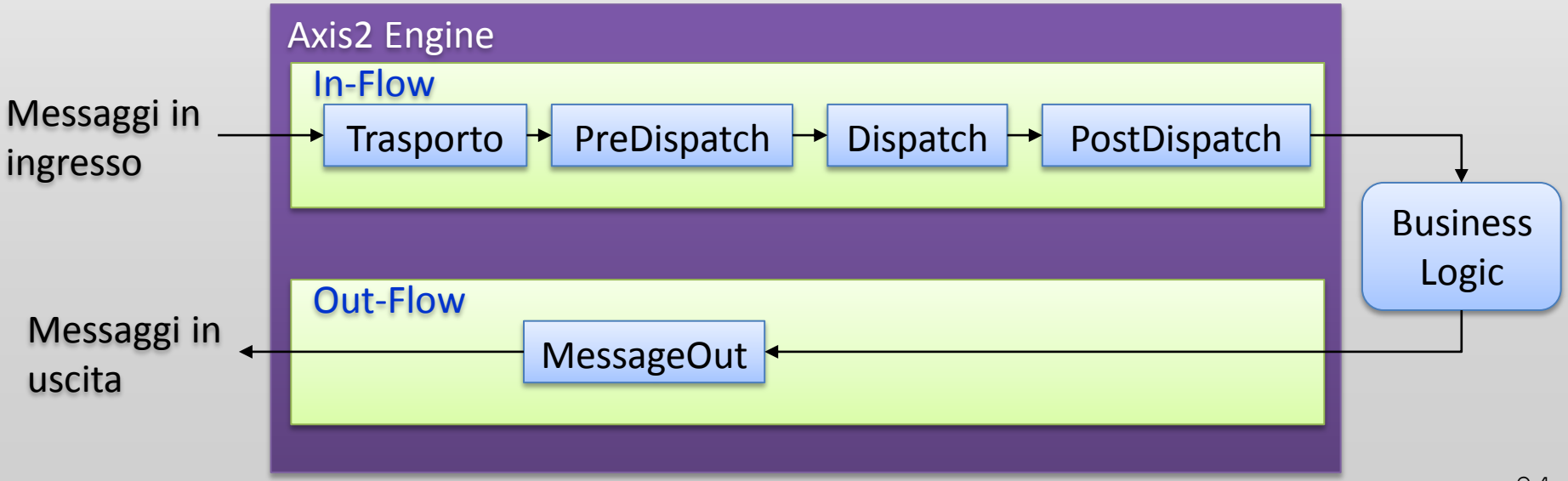
Architettura di dispiegamento

RadioLabs

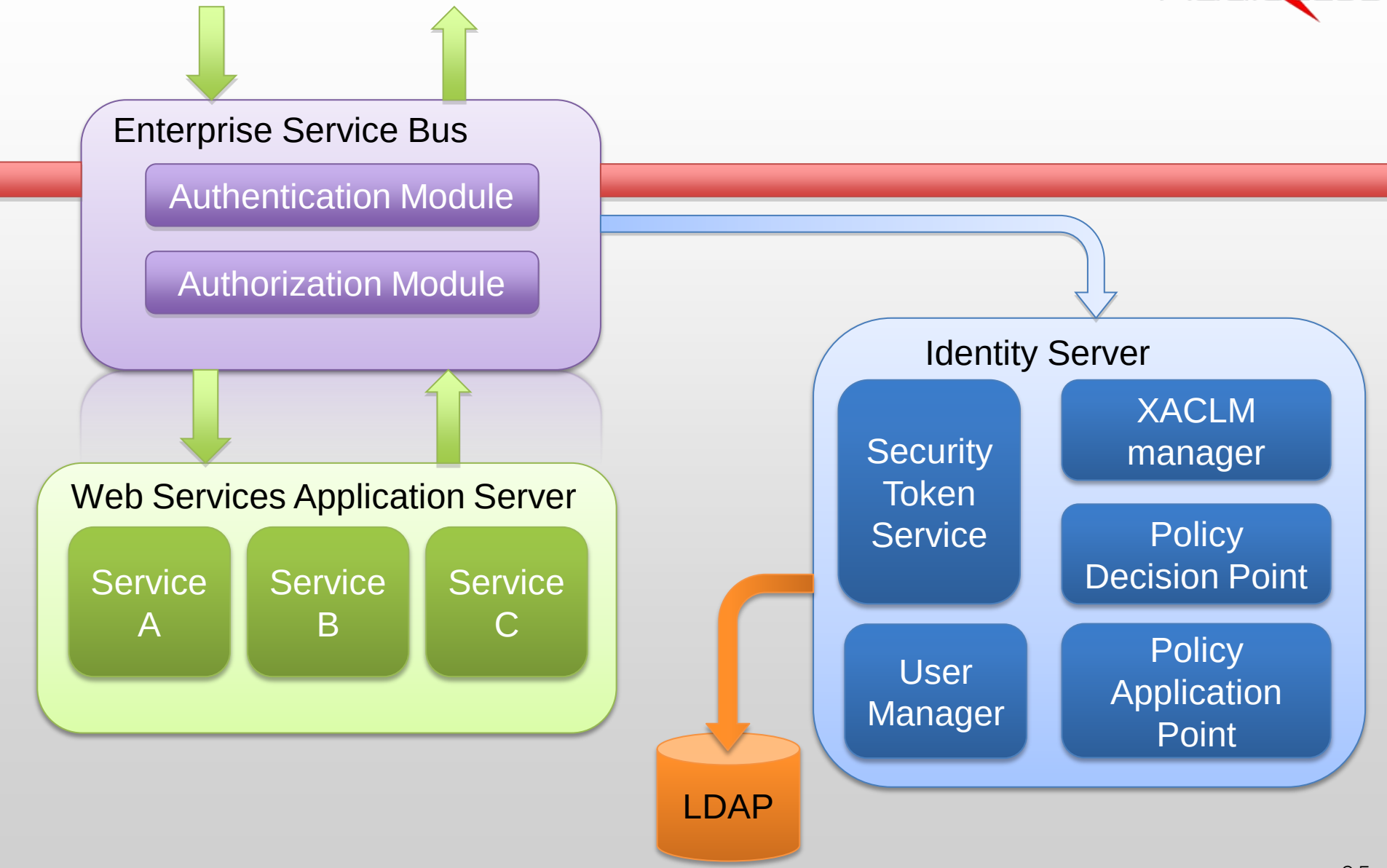
- **Piattaforme supportate:**
  - **Linux**
  - **Microsoft Widow**
  - **Mac OSX**
- **Web Service**:
  - **Apache** foundation
- **Middleware** per la configurazione dei servizi dello stack Apache:
  - **wso2 oxygen**
- **IDE**:
  - Eclipse

Axis2 Service Engine

- L'Axis2 service engine fornisce il *core web services engine* e supporta SOAP 1.1, SOAP 1.2, ed i servizi di tipo REST.
- L'Axis2 service engine è progettato come una serie di gestori di messaggi debolmente accoppiati, che effettuano la pre e la post-elaborazione dei messaggi.
- L'elaborazione dei messaggi in ingresso e in uscita è organizata in un insieme di fasi ordinate denominate flussi.
- Ogni fase è costituita da una collezione ordinata di gestori di messaggio.
- Un gestore di messaggio è la più piccola unità di invocazione dell'Axis2 engine.



Architettura di sicurezza per Web Service



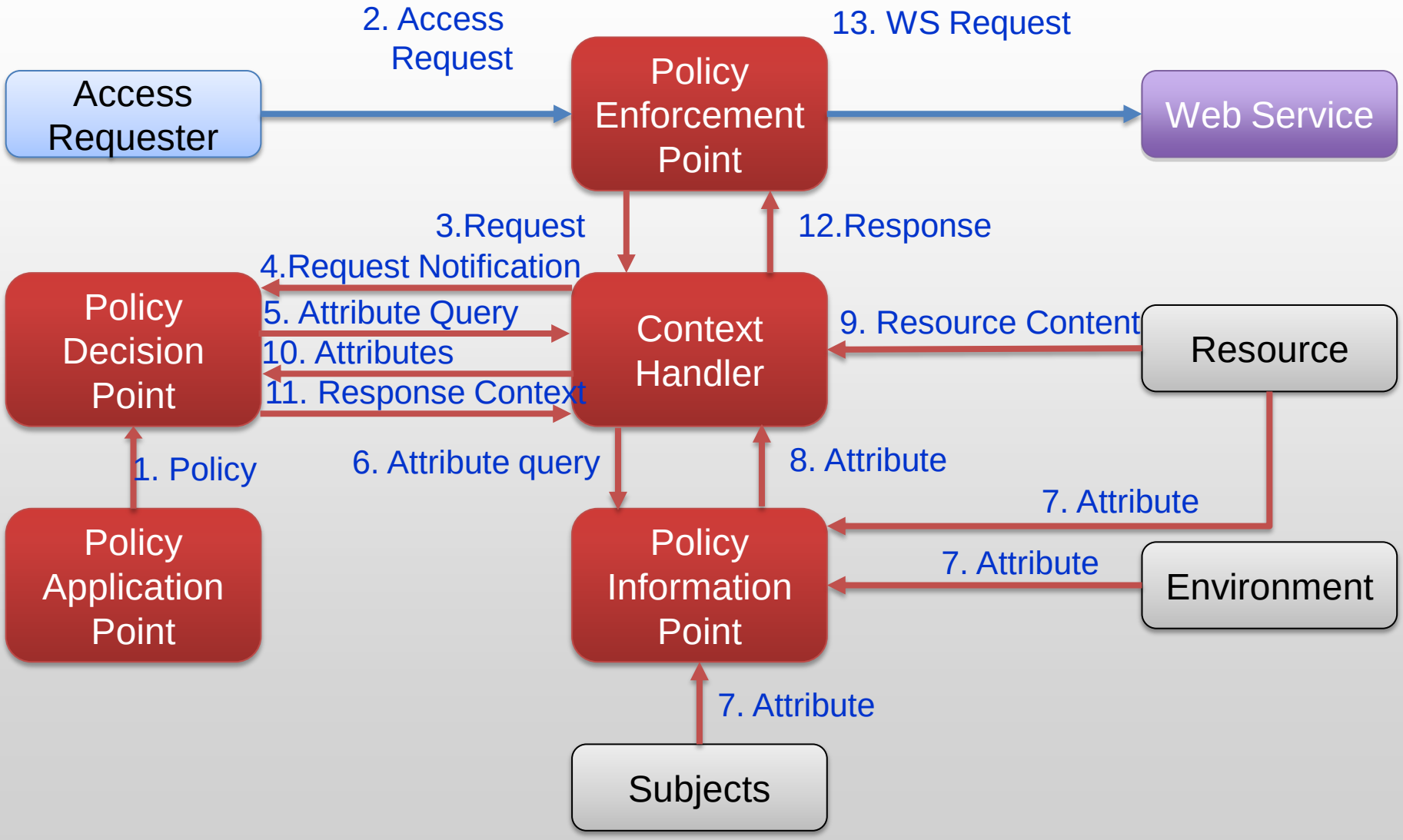
Caratteristiche dell'architettura di sicurezza

- L'architettura garantisce un'elevata granularità dei controlli sulle operazioni effettuate sui dati pur mantenendo semplicità e astrazione dai dettagli della configurazione degli apparati.
- L'uso di linee di condotta (policy) supporta la definizione, la verifica e il dispiegamento delle regole collegate alla condivisione delle informazioni.
- La gestione delle linee di condotta consente
  - La definizione da chi e in quali condizioni può essere utilizzata una particolare informazione
  - La definizione di rapporti fiduciari tra le varie infrastrutture
  - La prescrizione di particolari protocolli/tecnologie in particolari contesti
  - La prescrizione di particolari livelli di servizio tra infrastrutture
  - La specificazione di come devono essere trattati particolari eventi (ad es. tentativi di intrusione)
- Le linee di condotta sono rappresentate in modo formale e memorizzate in contenitori protetti.

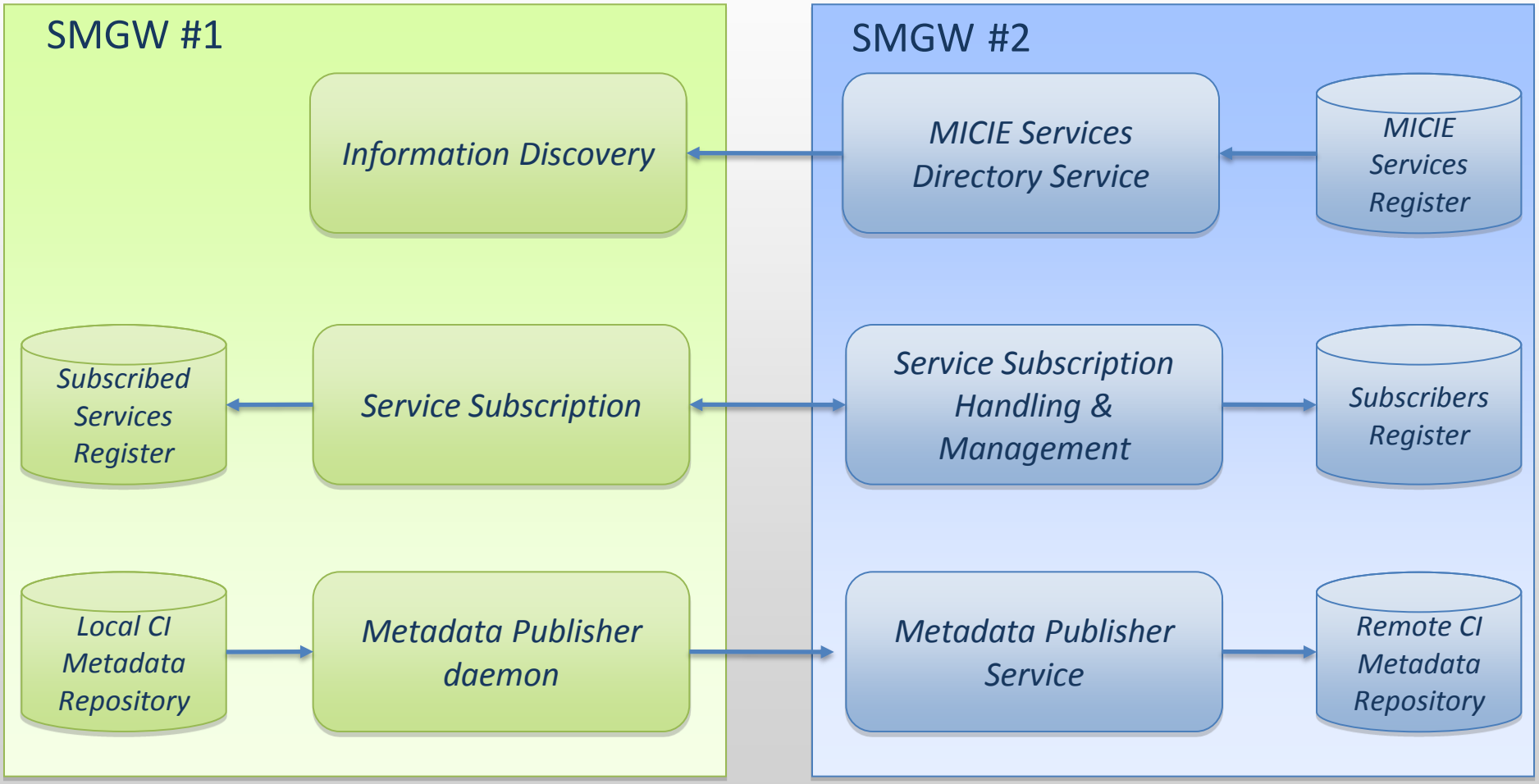
ROMA TRE UNIVERSITÀ DEGLI STUDI

Flusso dati XACML

RadioLabs



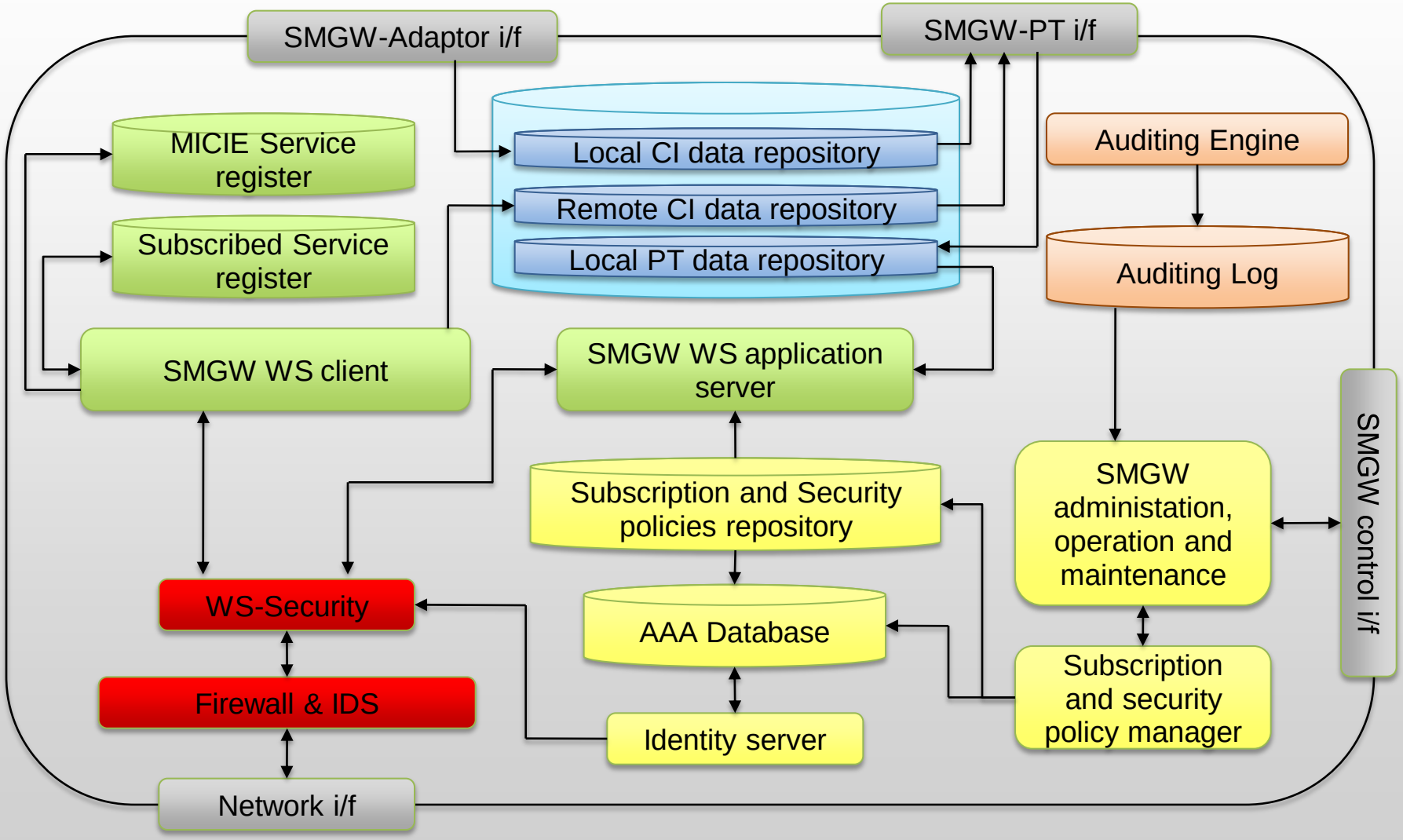
SMGW – Inter CI interactions



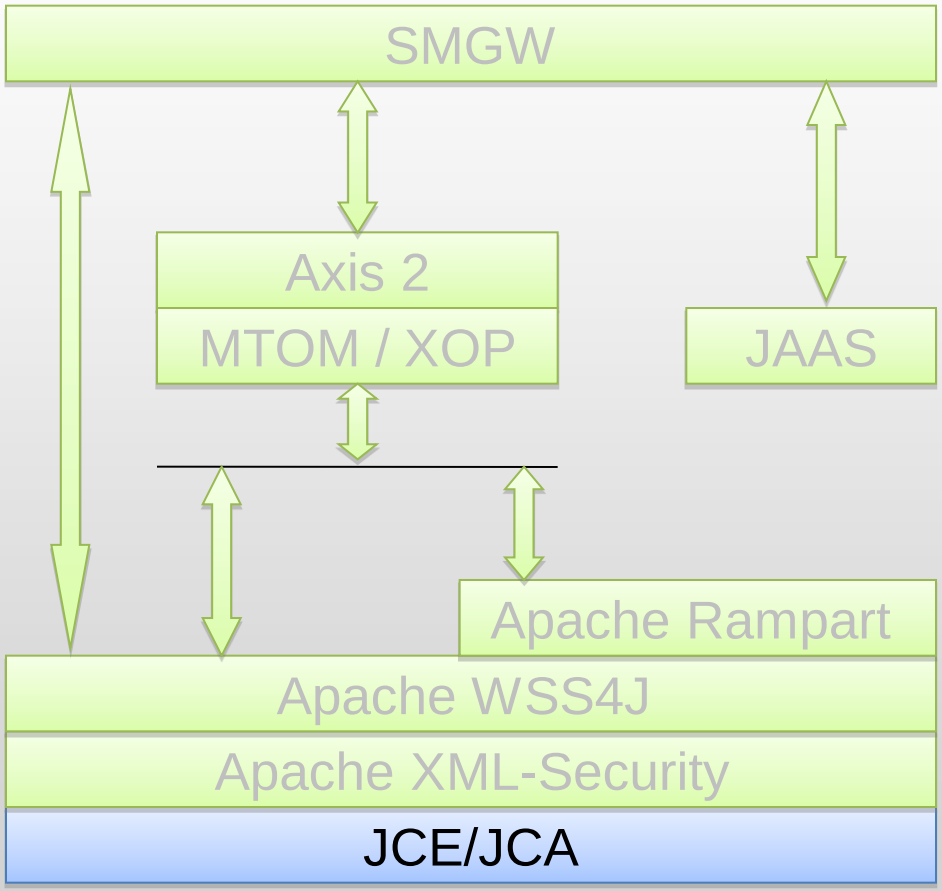
ROMA TRE UNIVERSITÀ DEGLI STUDI

MICIE SMGW Logical Architecture

RadioLabs



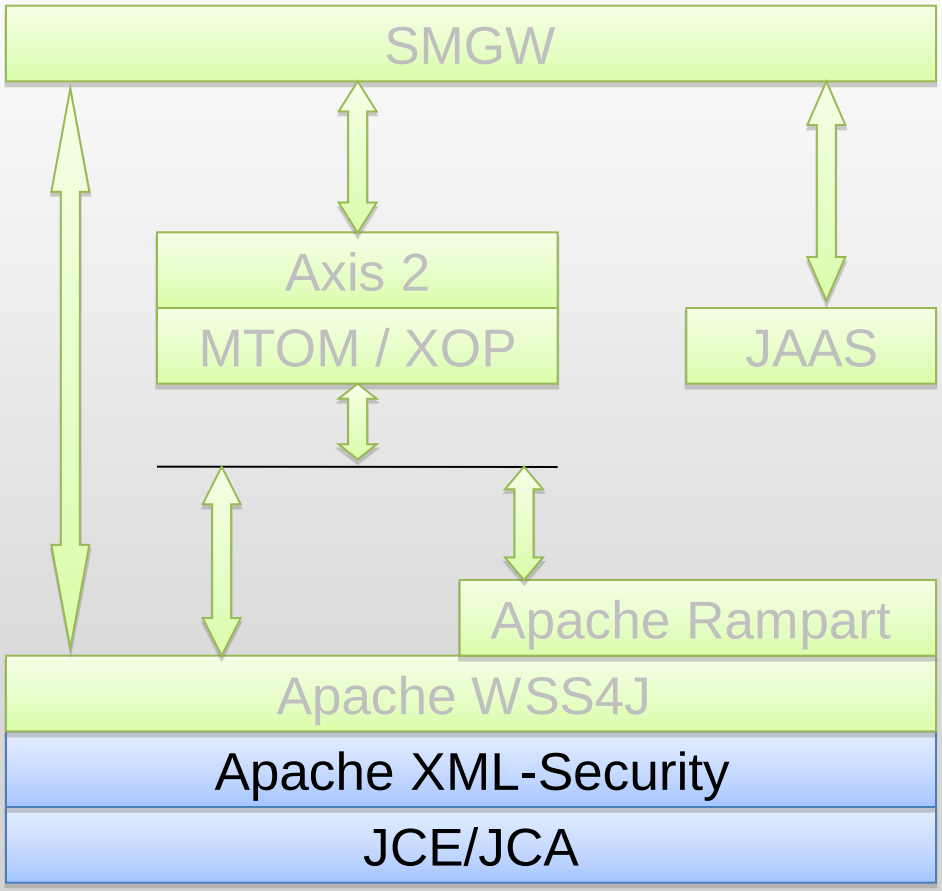
Security Technology Stack



Java Cryptography Architecture &
Java Cryptography Extensions

- *digital signature algorithms,*
- *message digest algorithms,*
- *key generation algorithms*
- *key factories,*
- *keystore creation & manag.*
- *algorithm parameter manag.*
- *algorithm parameter gen.*
- *certificate factories*

Security Technology Stack

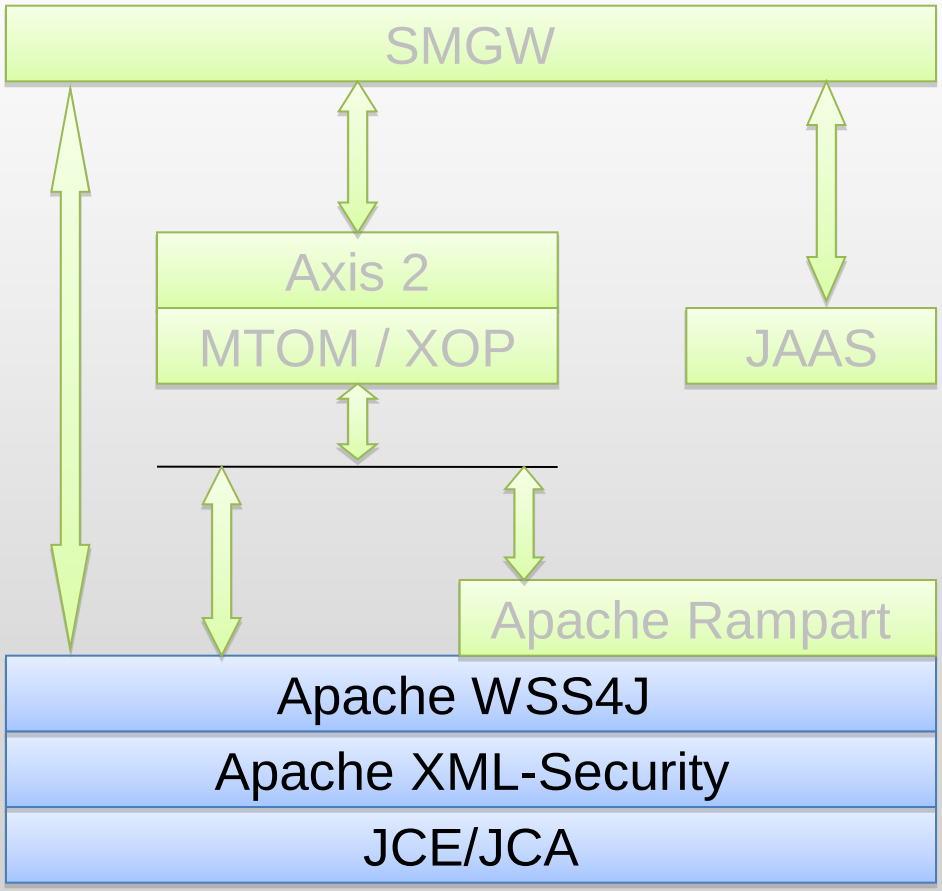


The Apache-XML-Security-J 1.4 supports

JSR-105: XML Digital Signature APIs for creating and validating XML Signatures.

JSR-106: XML Digital Encryption APIs

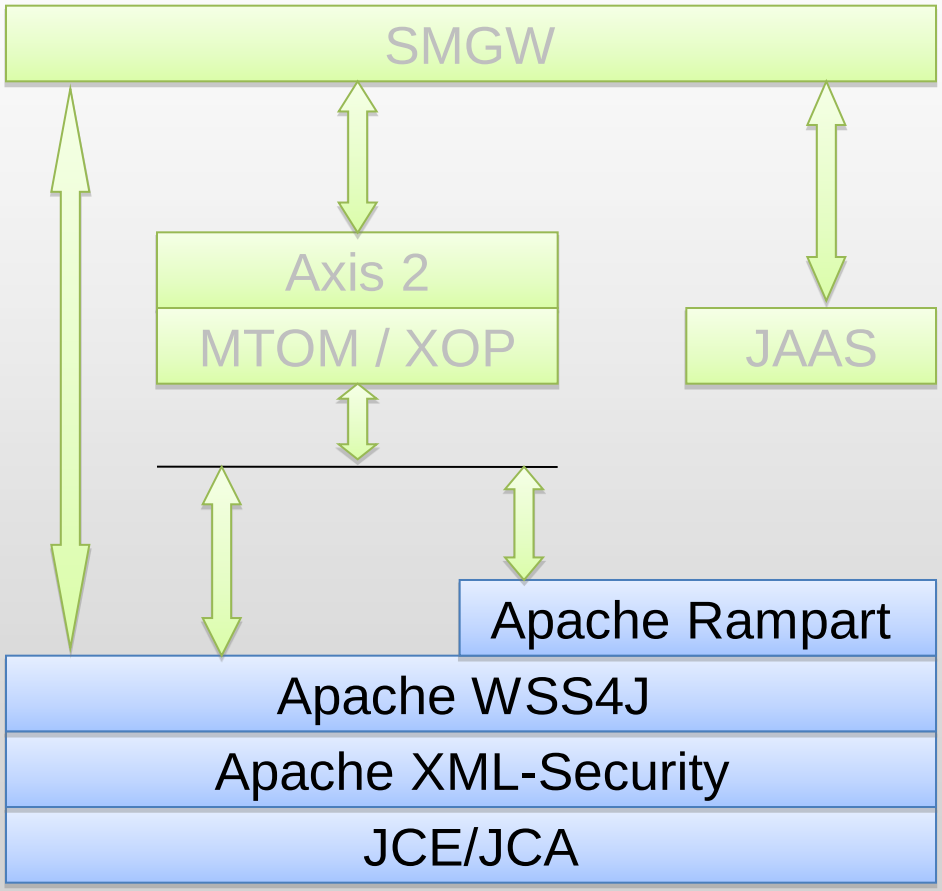
Security Technology Stack



WSS4J implements Web Services Security:

- *SOAP Message Security*
- *Username Token Profile*
- *X.509 Certificate Token Profile*

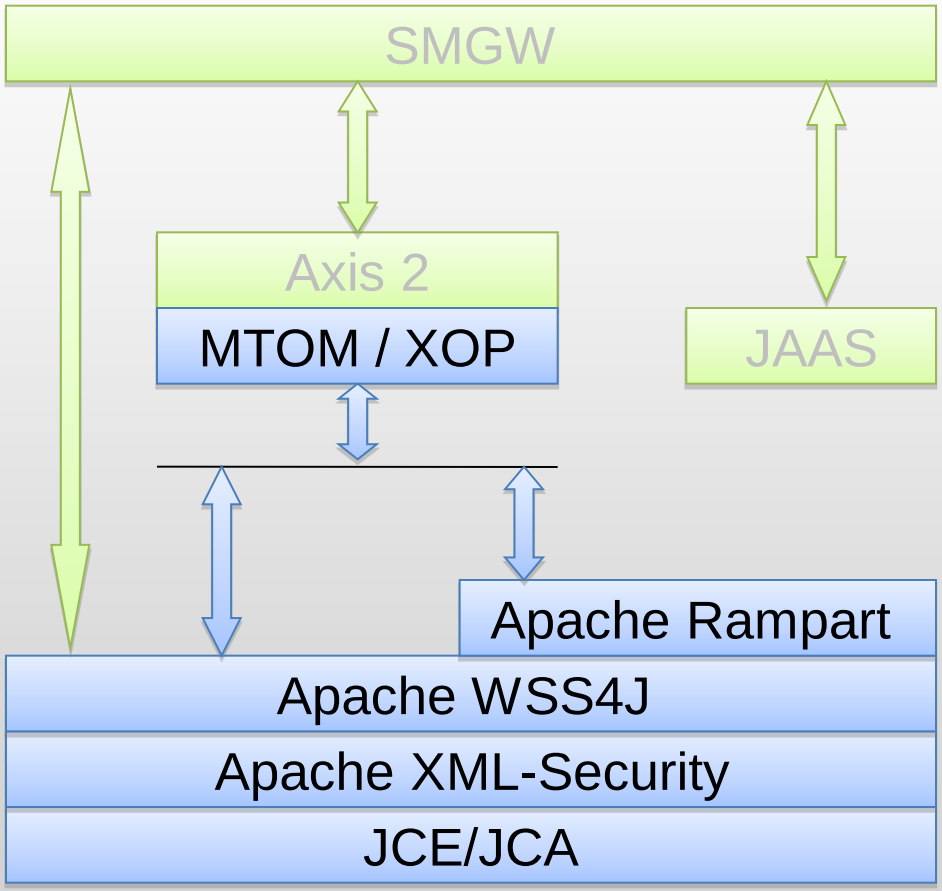
Security Technology Stack



Rampart secures SOAP messages according to specifications in the WS-Security stack
Rampart supports

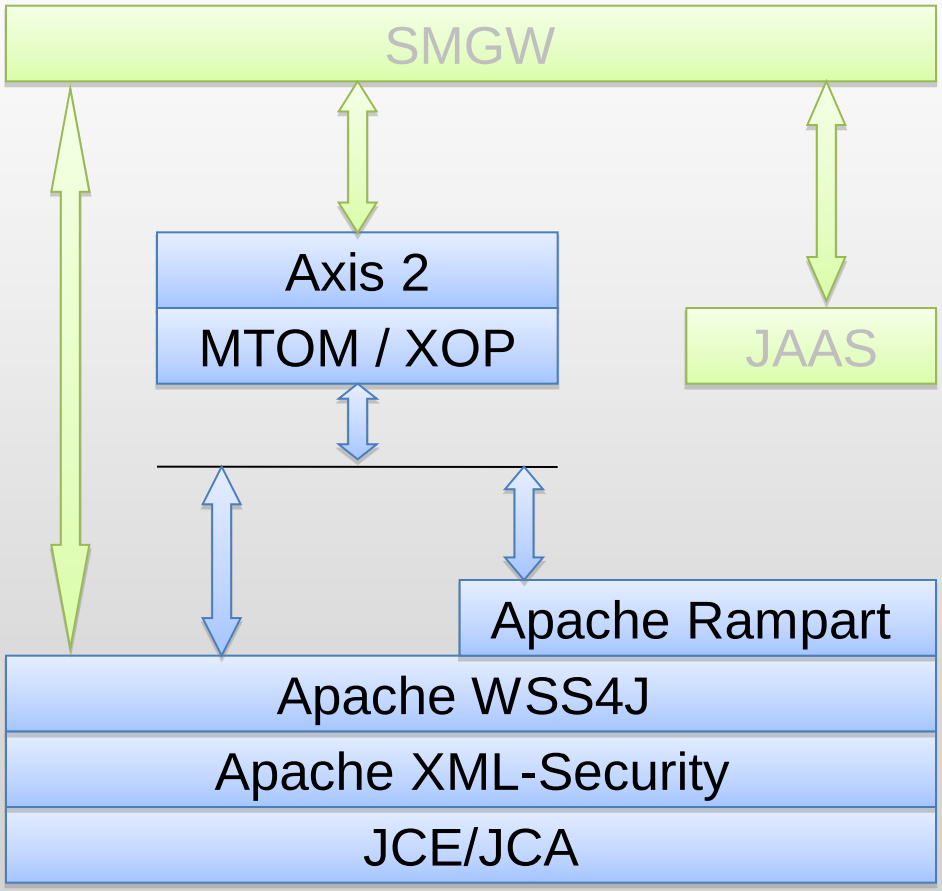
- *WS - Security*
- *WS - Security Policy*
- *WS - Trust*
- *WS-SXSAML*
- *SAML*

Security Technology Stack



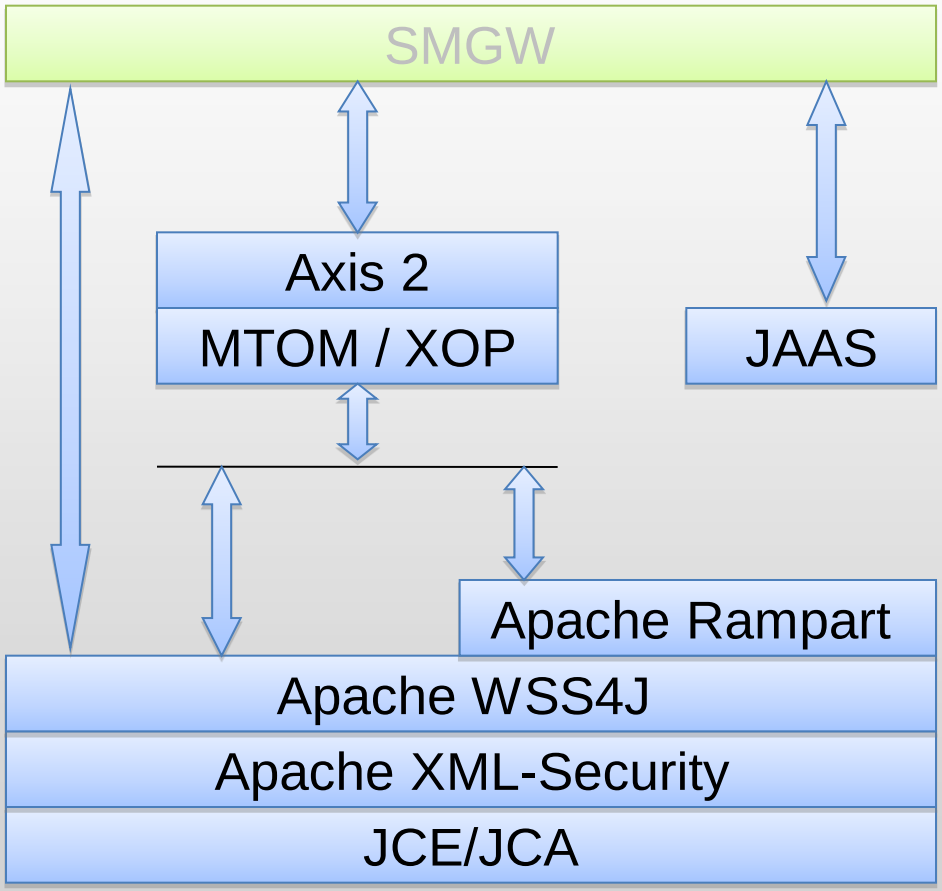
SOAP Message Transmission Optimization Mechanism optimizes the transmission and/or wire format of a SOAP message

Security Technology Stack



Axis2 (Service Engine): provides the core web services engine and supports SOAP 1.1, SOAP 1.2, and REST-style services.
The Axis engine is designed as a series of loosely coupled message handlers, which perform pre- and post-processing on messages.

Security Technology Stack



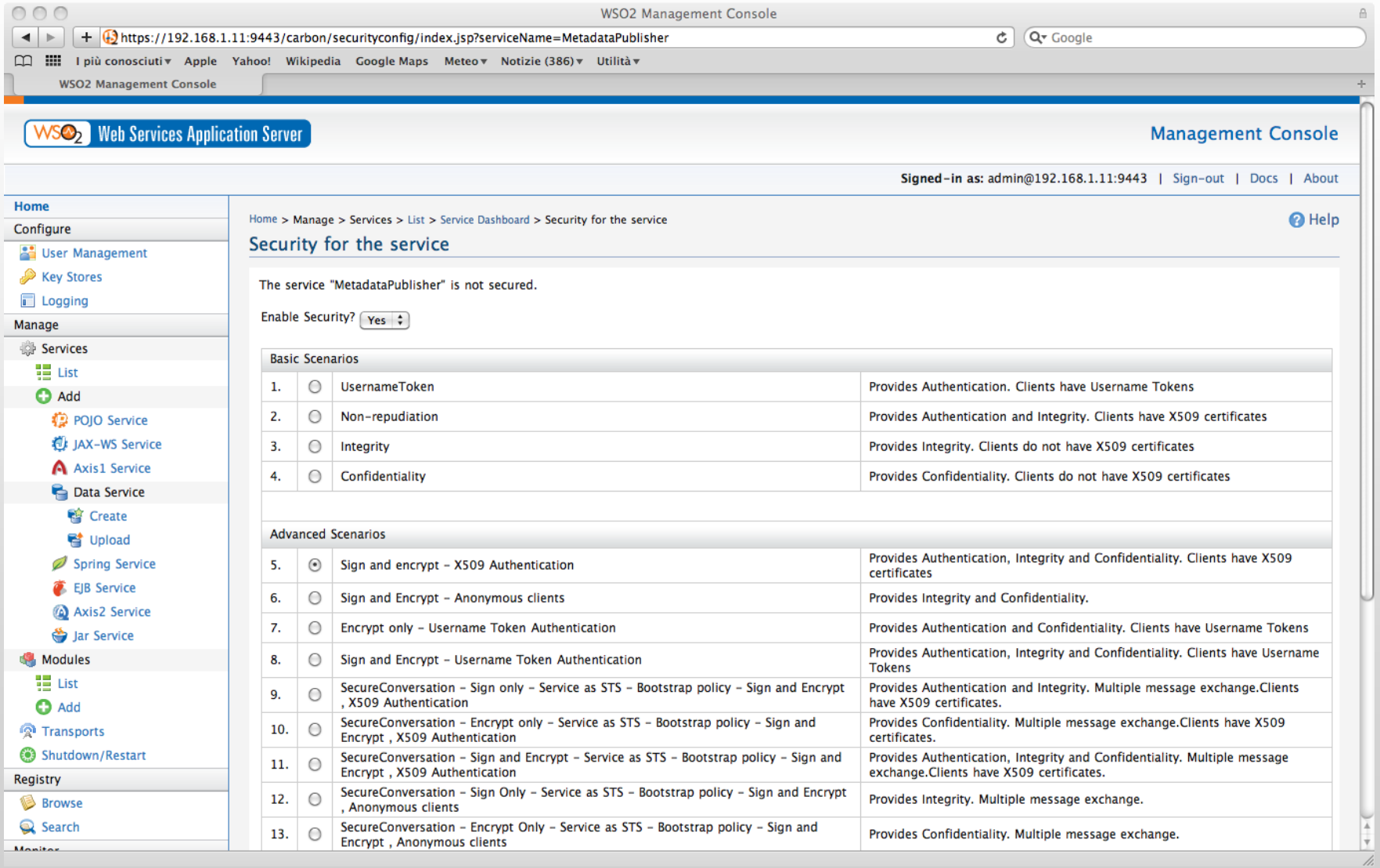
The Java Authentication and Authorization Service (JAAS) can be used for

- *authentication of users, to reliably and securely determine who is currently executing Java code,*
- *authorization of users to ensure they have the access control rights (permissions) required to do the actions performed.*

ROMA TRE UNIVERSITÀ DEGLI STUDI

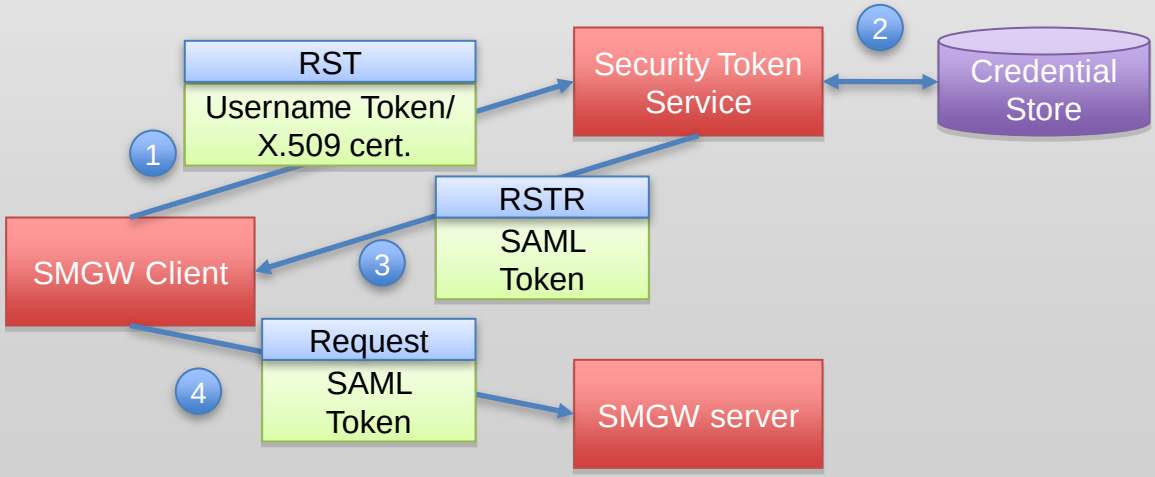
Service Security Management

RadioLabs



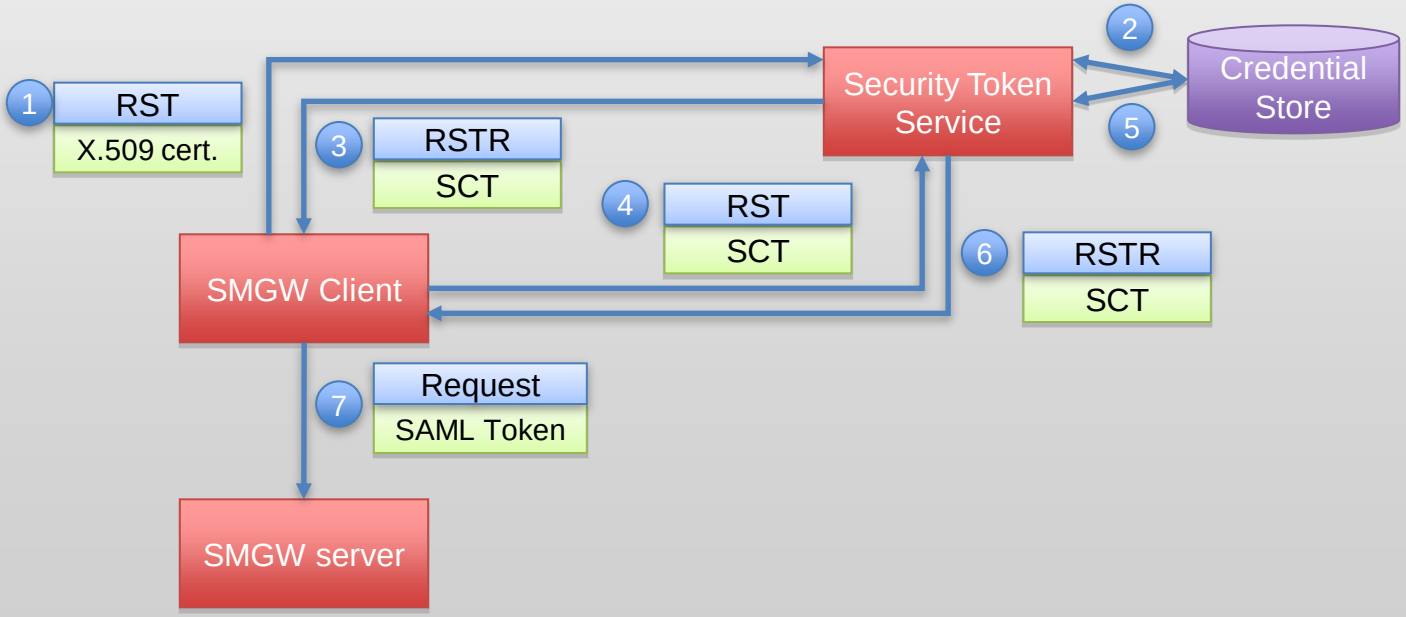
Security Assertion Markup Language

- SAML fornisce un quadro di riferimento basato su XMLper creare e scambiare informazioni relative alla sicurezza tra partner online .
- Quando viene impiegato un Security Token Service (STS) ritenuto fidato sia dal client che dal Web service, il client invia un messaggio Request Security Token (RST) al STS.
- Verificate le credenziali, il STS invia un messaggio Request Security Token Response (RSTR) contenente un security token che prova che il client è stato autenticato.
- Il security token è poi impiegato dal client per accedere al Web service.
- Per autenticare il client, il Web service verifica che il token sia stato emesso da un STS fidato.



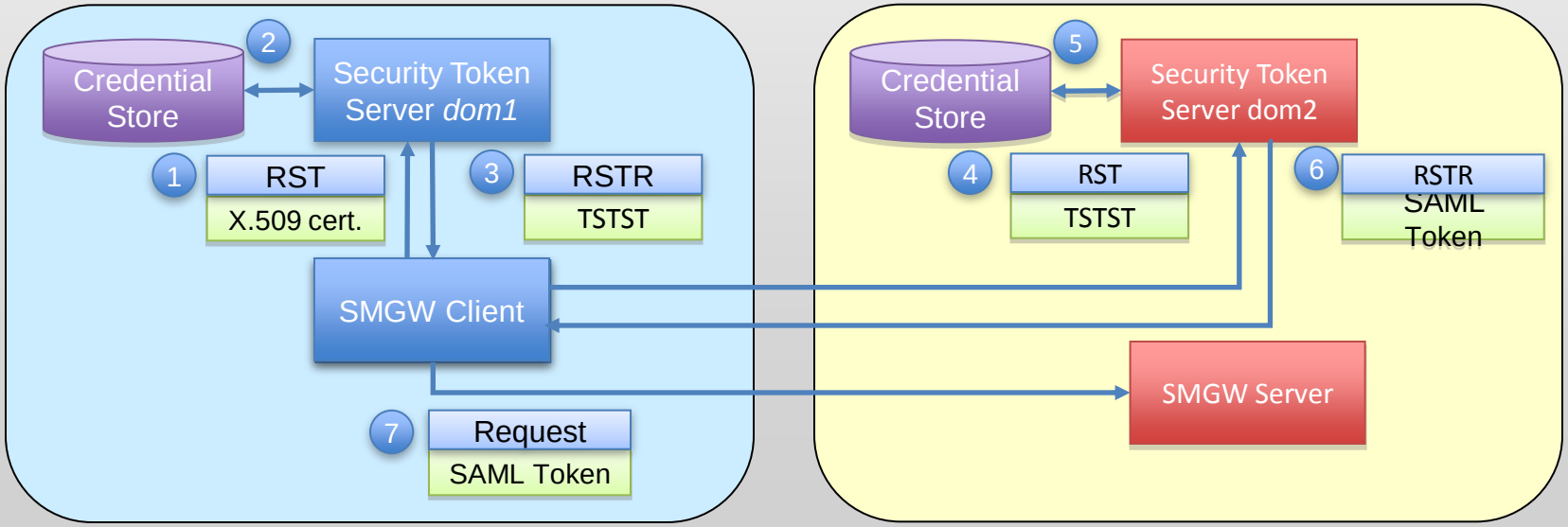
Security Assertion Markup Language

- Visto l'uso ripetuto del Web Service, per migliorare le prestazioni si può fare riscorso ad una WS-Secure Conversation con il STS.
- Il client SMGW richiede al STS un Security Context Token (SCT) che dimostra che si è autenticato e lo memorizza localmente.
- Successivamente il client usa il SCT ogni volta che deve richiedere un service token per accedere ad un servizio specifico.



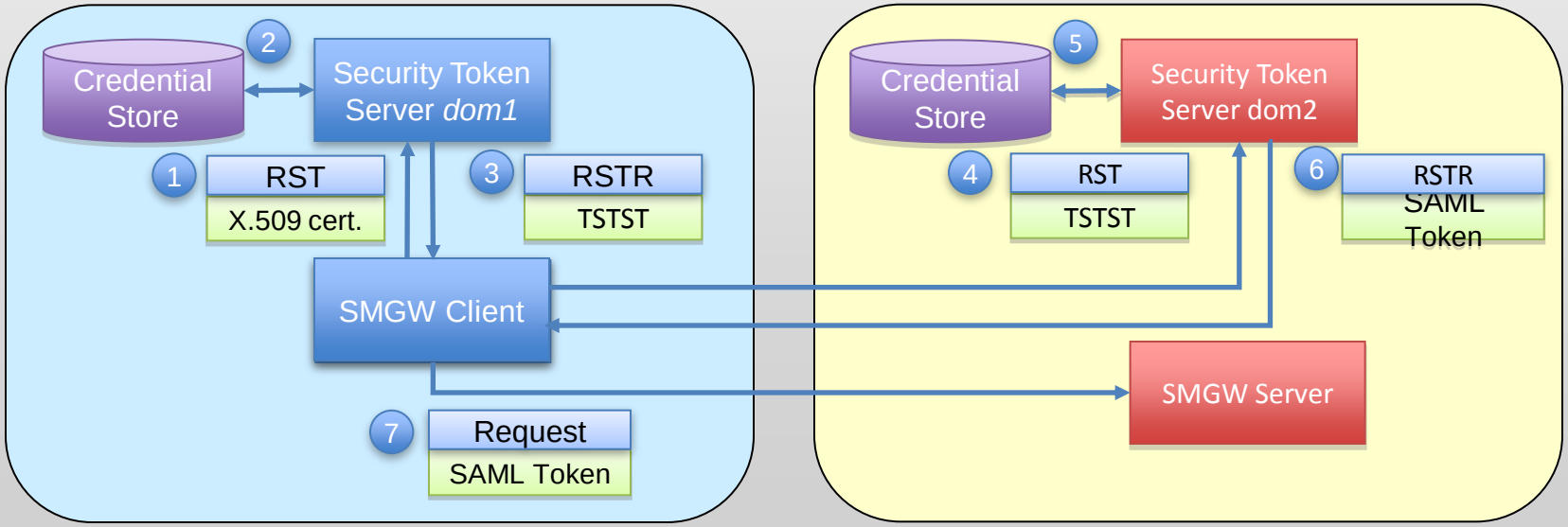
SAML

- In un sistema federato, un client SMGW potrebbe essere autenticato da un intermediario (security broker) che risiede nello stesso dominio di sicurezza del client e autorizzato e tracciato da un STS che risiede nel dominio di sicurezza del server.



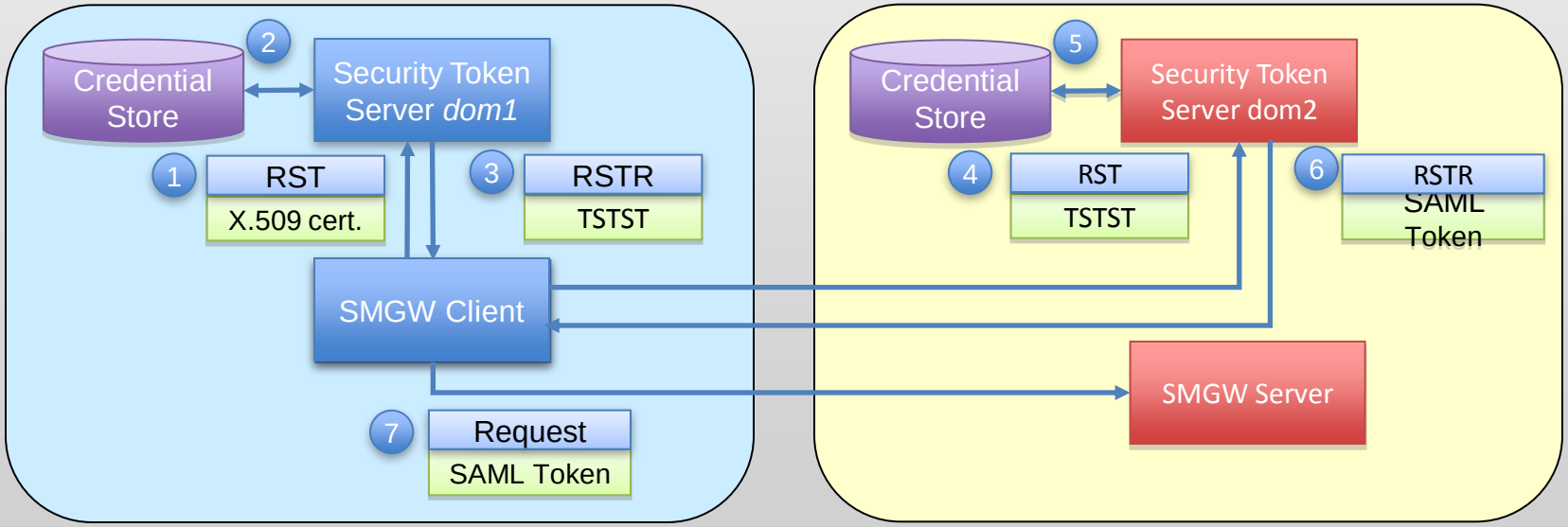
SAML

- Il client richiede al STS che risiede nel proprio dominio di sicurezza un security token per comunicare con il STS che risiede del dominio di sicurezza del server.
- Il STS che risiede nel dominio di sicurezza del client autentica il cliene e gli fornisce un security token per comunicare con il STS che risiede del dominio di sicurezza del server.
- Il client richiede al STS che risiede nel dominio di sicurezza del server un security token presentando il token che gli ha fornito il proprio STS.
- Il STS associato al server SMGW valida il security token del client ed emette un security token che può essere usato per communicare con il servizio.



SAML

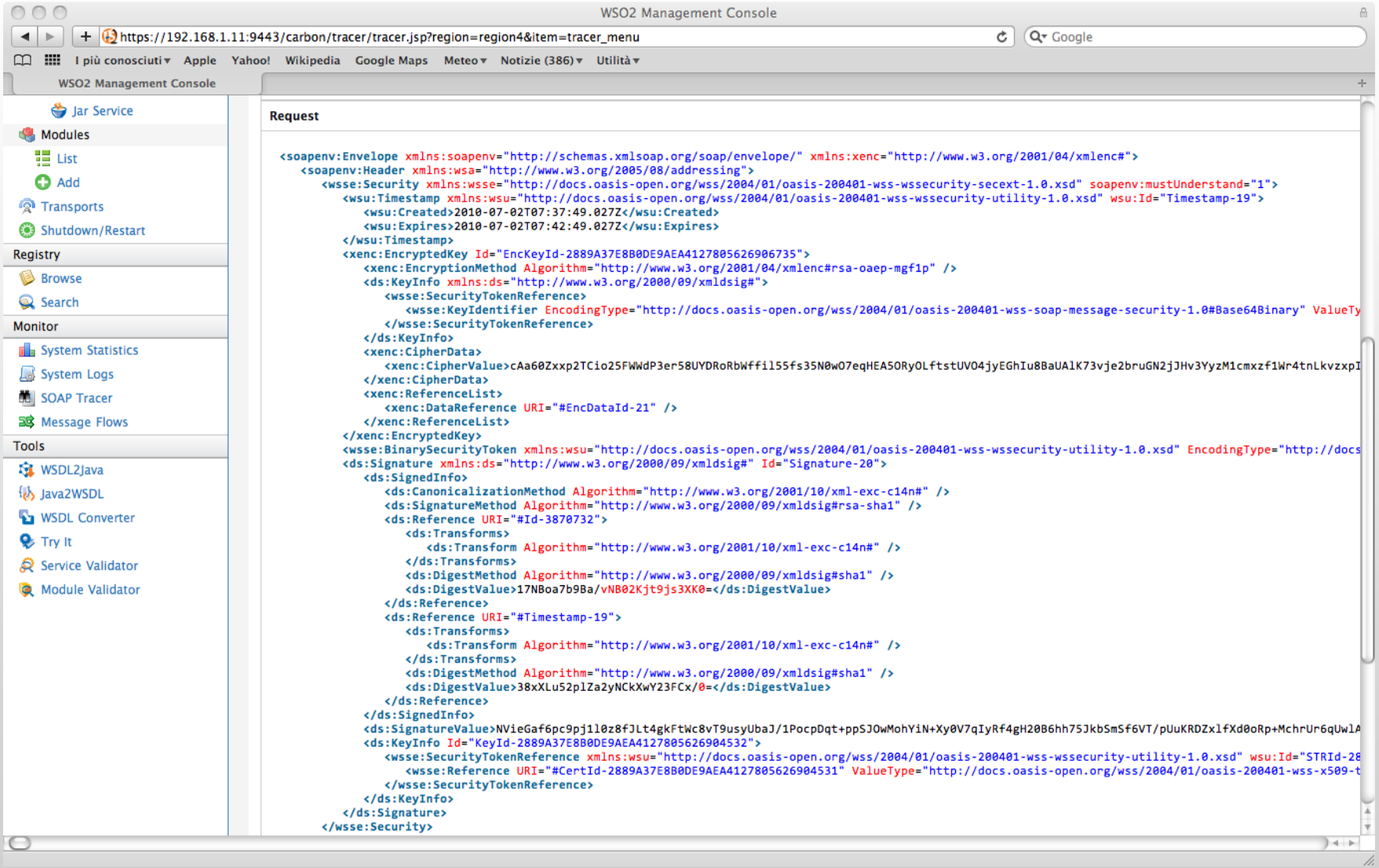
- Nel caso di una una WS-Secure Conversation il STS associato al server SMGW valida il security token del client ed emette un Security Context Token (SCT). Il SCT può essere usato dal client ogni volta che ha bisogno di un security token. Lo scope del SCT è limitato all'emissione di un STSenon può essere impiegato per accedere direttamente al servizio.
- Il client memorizza localmente il SCT.
- Successivamente il client usa il SCT ogni volta che deve richiedere un service token per accedere ad un servizio specifico.



ROMA TRE UNIVERSITÀ DEGLI STUDI

Soap Tracer

RadioLabs



Conclusioni

- Gli Standard OASIS per la sicurezza degli Web Services constituiscono un mezzo efficace per realizzare una MEDIAZIONE SICURA in sistemi federati.
- Per superare I problemi legati all'elevato volume di dati scambiati quando l'interdipendenza è pienamnete considerata può essere opportuno adottar modalità multicast
- Mettere in sicurezza flussi multicast (XML) in sistemi federati è ancora un tema aperto.
- Assicurare che una terza parte non fidata non acceda a informazioni sensibili attraverso l'analisi di dati relativi a elementi interdipendenti, richiede l'adozione una policy complessa per il controllo dello scambio dei metadati.

ROMA TRE
UNIVERSITÀ DEGLI STUDI

RadioLabs

GRAZIE PER L'ATTENZIONE