



- Problematiche di Audit relativamente all'Identity Access Management e SOA Security

(a cura di **Marco Tulliani – CISA, CGEIT, ISO27001 – Gruppo Sara Assicurazioni**)



INDICE DELLA PRESENTAZIONE :

1. Architettura di I&AM
2. Soluzione adottata per l'I&AM
3. Controlli sull'Architettura I&AM
4. SOA Principi
5. SOA e Security
6. Information Risk Management per SOA
7. Message Security per la SOA-Security
8. Modello ideale di SOA-Security

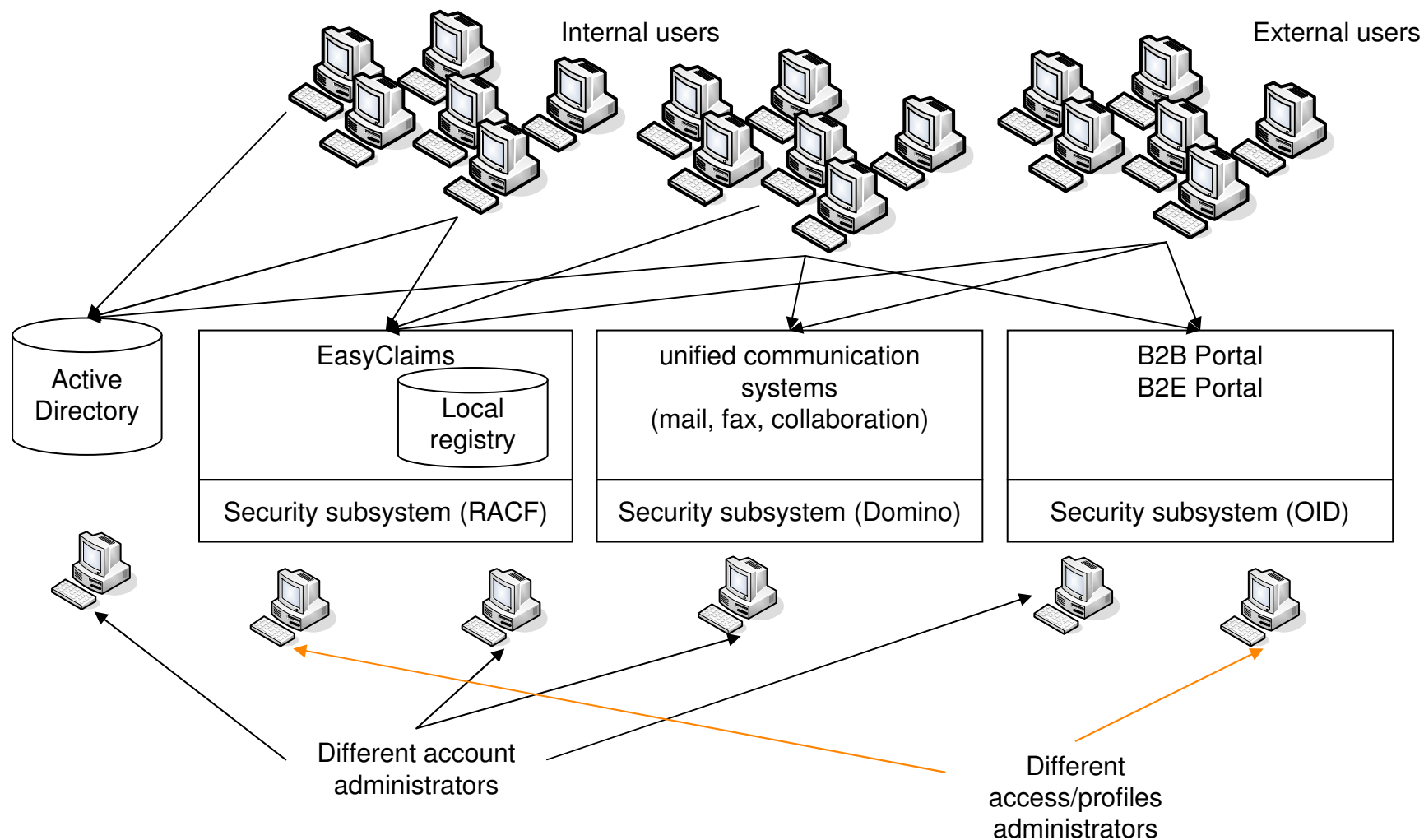


INDICE DELLA PRESENTAZIONE :

1. **Architettura di I&AM**
2. Soluzione adottata per l'I&AM
3. Controlli sull'Architettura I&AM
4. SOA Principi
5. SOA e Security
6. Information Risk Management per SOA
7. Message Security per la SOA-Security
8. Modello ideale di SOA-Security

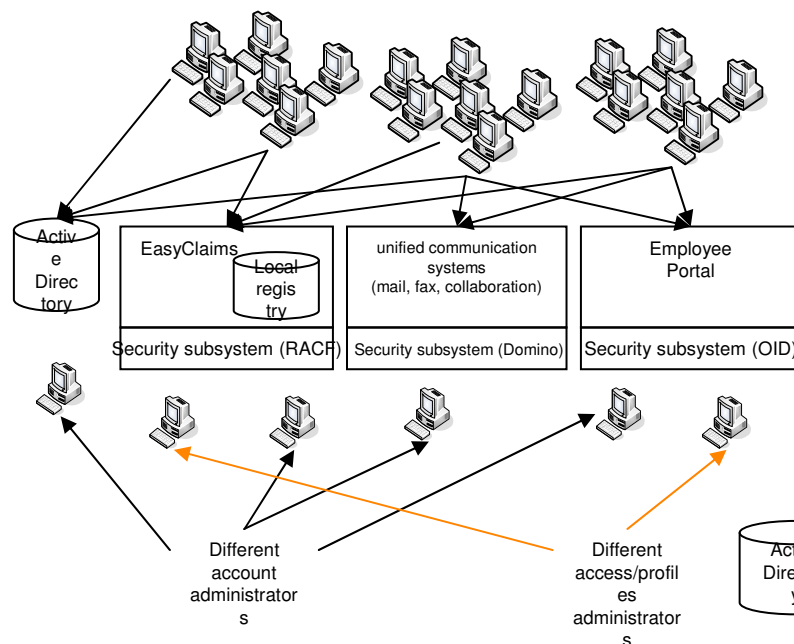


AS IS



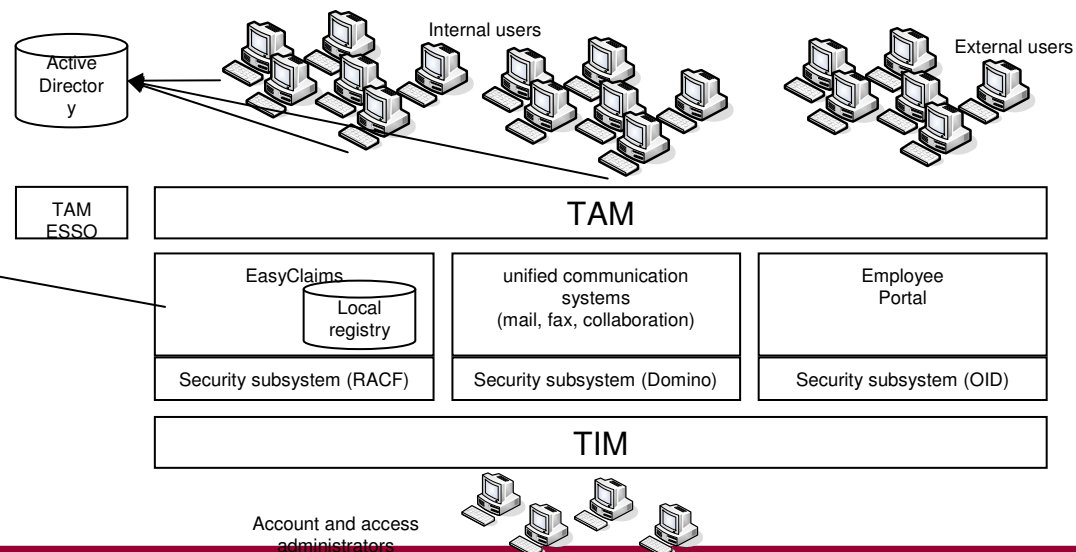


Before... compared to TODAY



From differentiated security implementations with no rules...

... to a standard and regulated security architecture.





INDICE DELLA PRESENTAZIONE :

1. Architettura di I&AM
2. **Soluzione adottata per l'I&AM**
3. Controlli sull'Architettura I&AM
4. SOA Principi
5. SOA e Security
6. Information Risk Management per SOA
7. Message Security per la SOA-Security
8. Modello ideale di SOA-Security

Motivazione del progetto



•Storicamente le logiche di accesso e le regole di profilazione delle utenze nascono all'interno delle applicazioni; la crescente numerosità delle applicazioni, e la crescente complessità delle componenti infrastrutturali degli ambienti che le accolgono, hanno portato a:

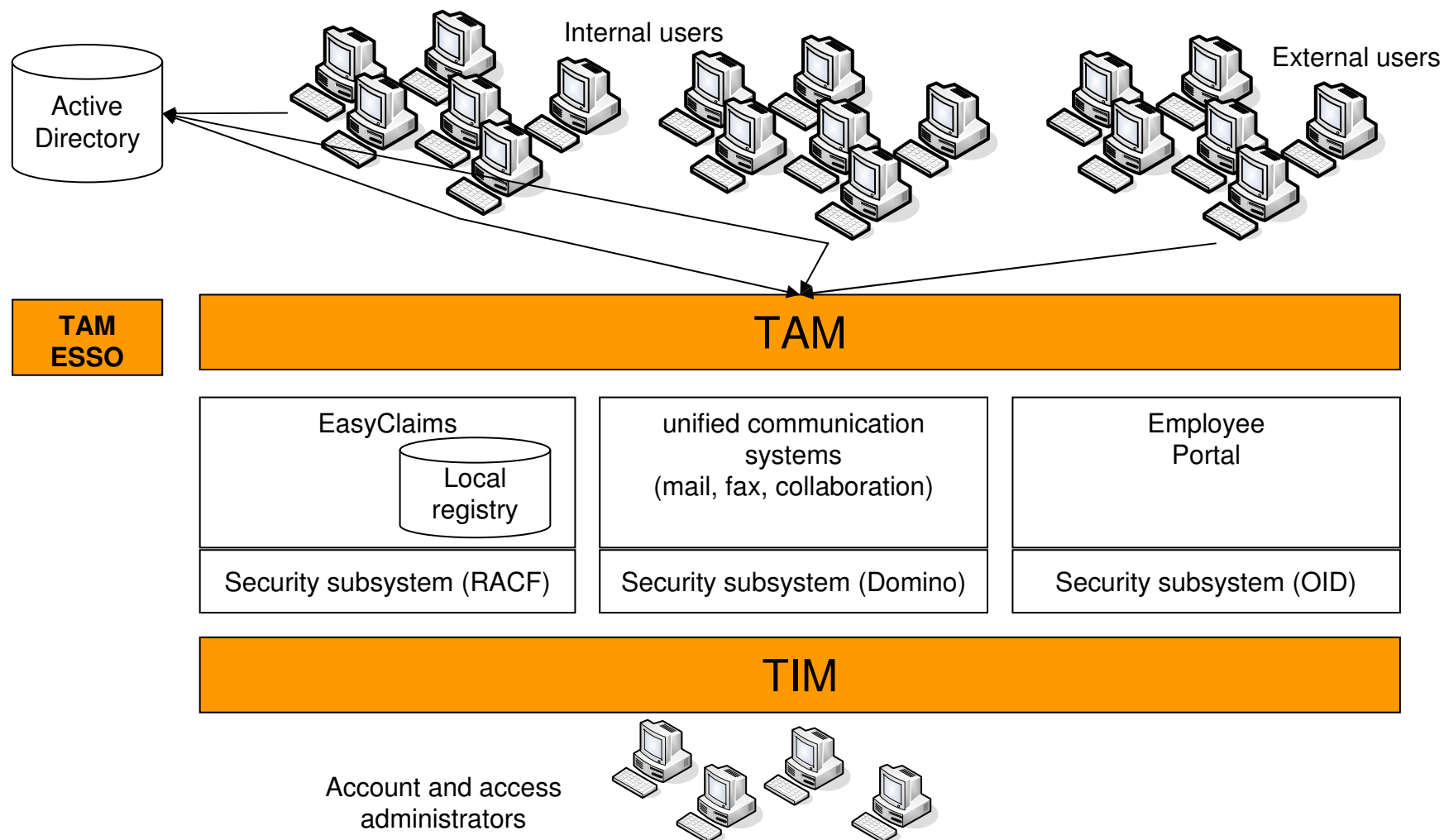
- diverse persone che gestiscono i differenti componenti del servizio, con diversi regolamenti e criteri di sicurezza
- elevato numero di credenziali di accesso (userid e password) tra loro differenti
- diversi meccanismi di auditing e rilevamento degli accessi (se previsto)

•Nel corso del 2006, SARA ha individuato alcuni interventi nel contesto della sicurezza informatica, volti a migliorare il proprio posizionamento nell'ambito del rispetto delle normative, a rendere più efficienti i processi e a migliorare il livello medio di sicurezza dei servizi IT; SARA ha avviato in tal senso un'iniziativa allo scopo di:

- adeguarsi alle recenti normative e ai requisiti di legge sulla sicurezza
- rilevare gli accessi ai servizi e le violazioni delle policy assegnate
- gestire le policy di sicurezza in modo uniforme e centralizzato
- poter rendere disponibili gli strumenti per l'approvazione e il controllo degli accessi ai servizi aziendali ai responsabili di business dei servizi stessi
- rendere più efficienti e semplificare le attività di gestione delle utenze, riducendo in tal modo i costi di gestione
- semplificare l'esperienza utente mediante il Single Sign On
- adottare una infrastruttura di autenticazione e autorizzazione comune a tutti i servizi, con regole definite e condivise di integrazione con i servizi e di gestione delle politiche di sicurezza e di accesso



To Be

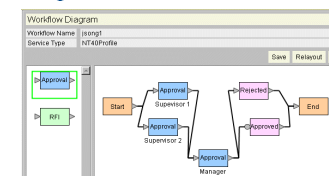




- ITIM Server - E' l'applicazione che consente il controllo centralizzato delle identità e delle utenze aziendali. Fornisce lo strumento principale automatizzabile e basato su delle politiche per la gestione dei privilegi degli utenti distribuiti su risorse IT eterogenee.
- ITIM Database - E' il repository, basato su piattaforma DB2, che contiene la totalità delle informazioni di auditing circa le attività amministrative e di provisioning di ITIM.
- Registro Utenti ITIM - E' il repository, basato su piattaforma DB2, ma a cui si accede tramite protocollo LDAP. Contiene, organizzato sotto forma di Directory, le informazioni riguardanti le identità e le utenze, oltre a tutti gli oggetti ITIM necessari alle politiche di provisioning.
- LDAP Console - Interfaccia Web per l'amministrazione del Directory Server. L'applicazione si basa su infrastruttura WebSphere.
- ITIM Adapter - Interfaccia tra l'Itim Server e l'applicativo target, oggetto del provisioning. A seconda dell'applicativo integrato, può essere costituito da tecnologia out-of the -box o ITDI e di conseguenza risiedere rispettivamente sul target o sull'ITIM Server.
- IDI HR Data Feed - Processo logico implementato tramite tecnologia ITDI, attraverso il quale è possibile popolare ITIM con delle Identità a partire da un HR Repository di riferimento.



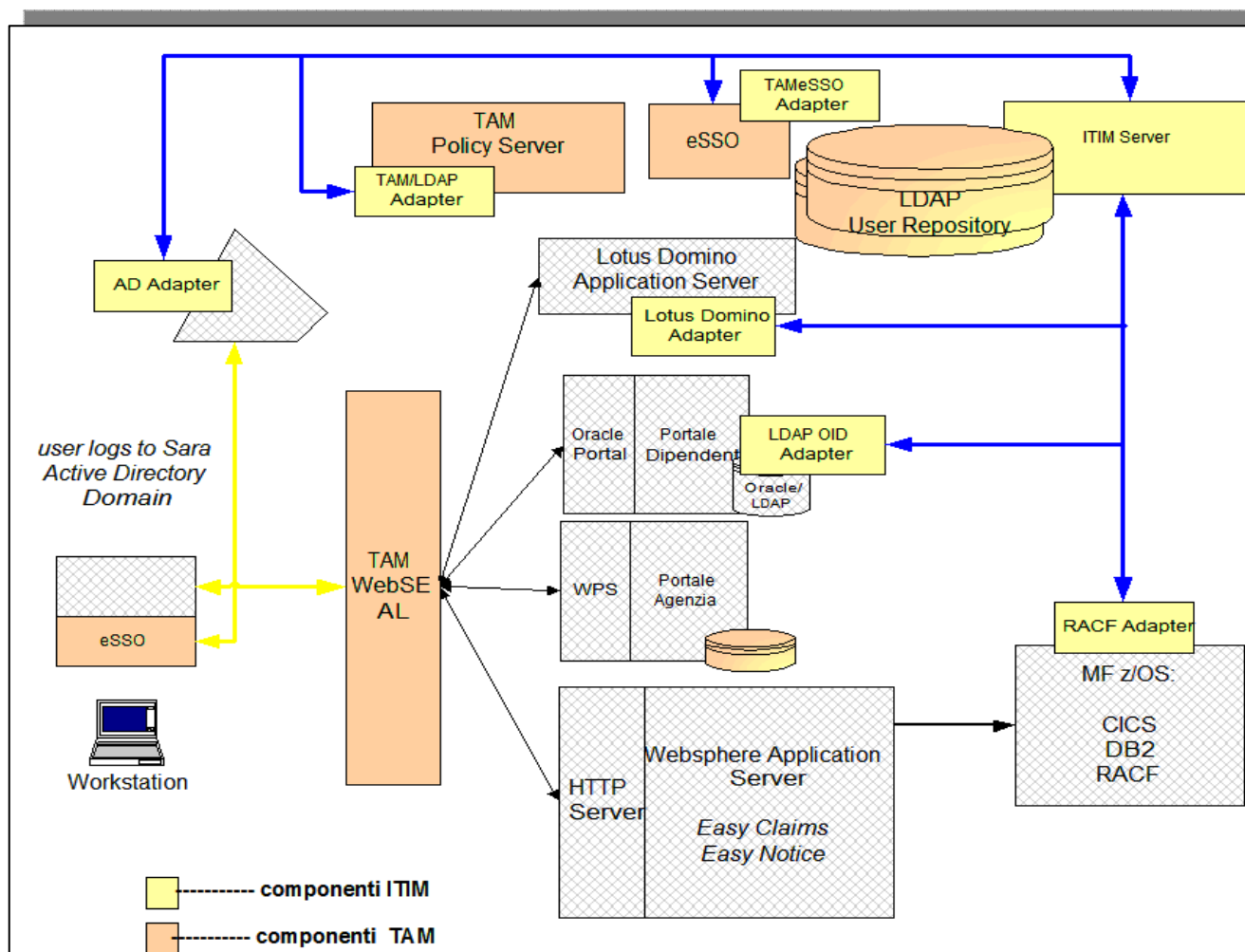
- TAM Policy Server - E' la componente responsabile del mantenimento del master policy database (Database contenente le definizioni delle politiche di sicurezza, ACL, POP e regole di autorizzazione). E' anche responsabile della corretta replica del master policy database su tutti gli authorization server presenti all'interno dell'infrastruttura;
- TAM Reverse Proxy - E' la componente responsabile della autenticazione degli utenti, verificando che abbiano una valida userid registrata nella directory LDAP, crea le credenziali ed applica le politiche di controllo degli accessi alle richieste degli utenti. Se installato in zona demilitarizzata, permette di aumentare la sicurezza e protezione delle risorse web;
- Registro utenti TAM - E' la directory di tipo LDAP che fa da repository delle informazioni relative agli utenti, informazioni utilizzate nel processo di autenticazione e di autorizzazione (ACL su utenti e gruppi)
- TAM Console - E' l'interfaccia Web del TAM che permette all'amministratore di definire le utenze, i gruppi e le politiche di sicurezza, associate alle risorse che devono essere protette;
- TAM SMS Server - Componente opzionale di TAM eseguito come servizio WebSphere. Gestisce le sessioni utente attraverso i server TAM, garantendo che il loro stato rimanga consistente nel passaggio tra un server e l'altro.
- TAM SMS Console - Sezione aggiuntiva della TAM Console per la gestione del SMS Server

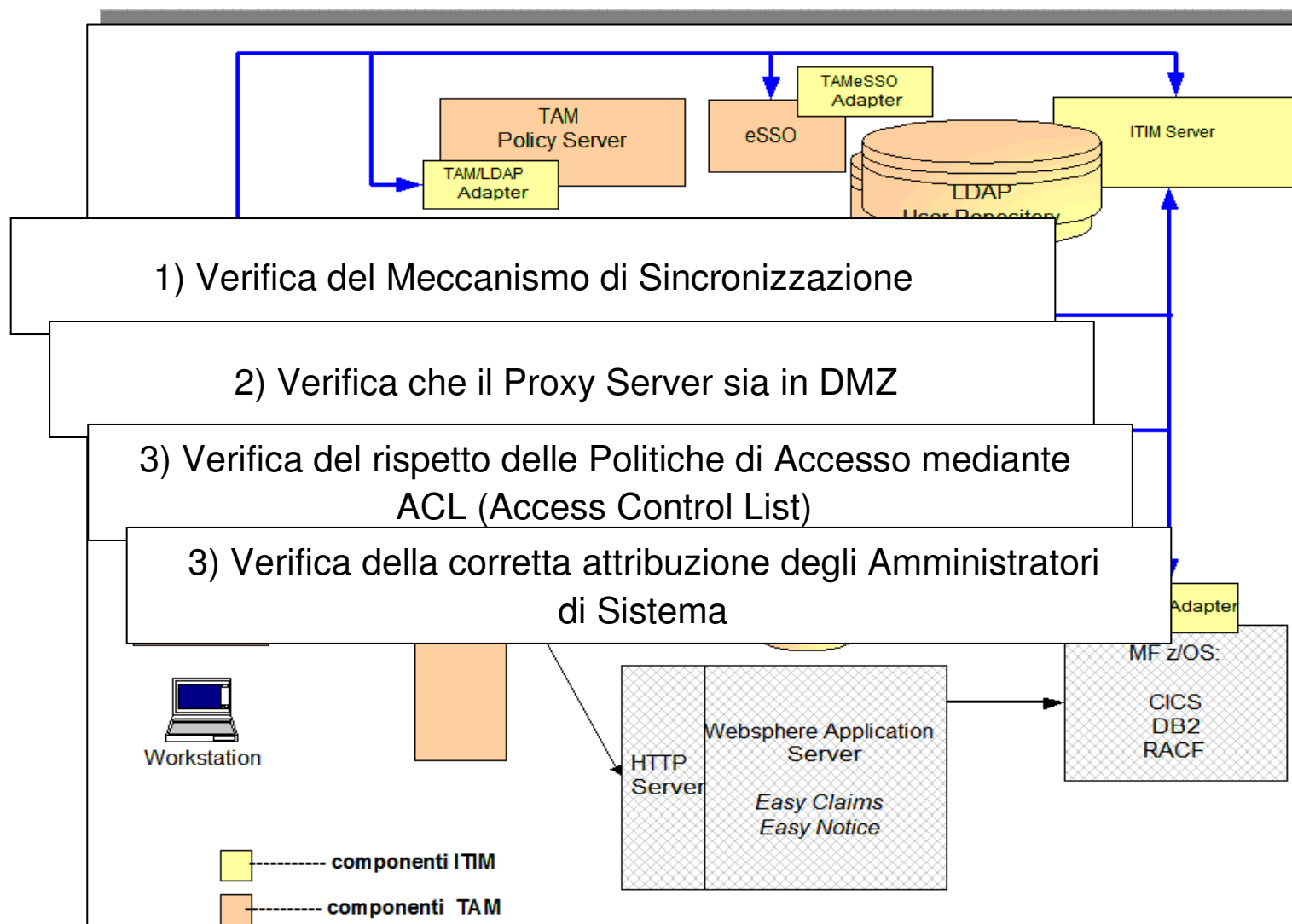




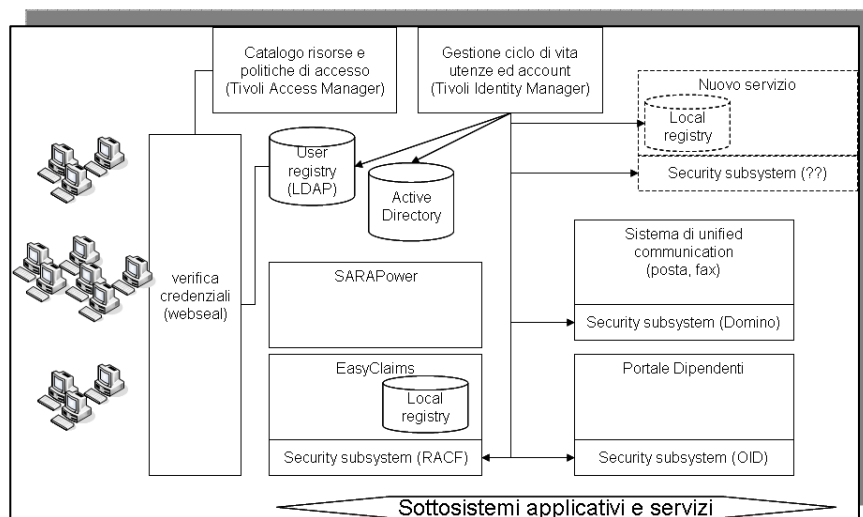
INDICE DELLA PRESENTAZIONE :

1. Architettura di I&AM
2. Soluzione adottata per l'I&AM
3. **Controlli sull'Architettura I&AM**
4. SOA Principi
5. SOA e Security
6. Information Risk Management per SOA
7. Message Security per la SOA-Security
8. Modello ideale di SOA-Security





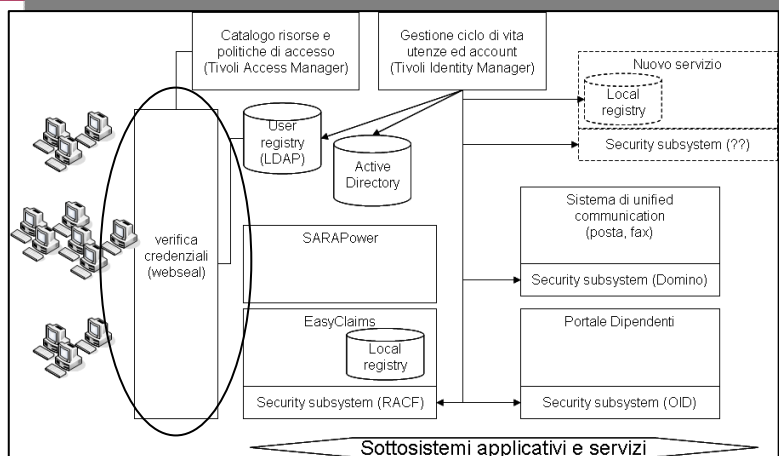
Verifica del Meccanismo di Sincronizzazione



Il Test eseguito dalla scrivente funzione consiste nel verificare che il cambio password da parte dell'utente^[1] finale sia intercettato dal prodotto di User Management (ITIM) e propagato sui rimanenti sistemi gestiti nell'architettura di riferimento sopra rappresentata.

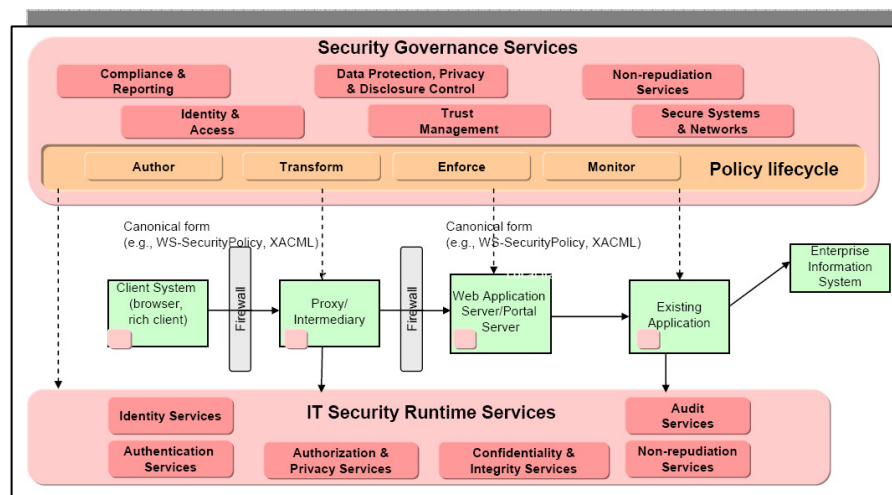
^[1] il cambio di password avviene partendo dalla piattaforma MS Windows pertanto dominio di Active Directory.

Verifica che il Proxy Server sia in DMZ



I proxy Server sono responsabili dell'autenticazione degli utenti, verificano che gli stessi abbiano una valida user id registrata nella directory LDAP, creano le credenziali ed applicano le politiche di controllo degli accessi alle richieste degli utenti.

Ne segue che il Proxy Server se installato in zona demilitarizzata, permette di aumentare la sicurezza e protezione delle risorse web.



Verifica del rispetto delle Politiche di Accesso mediante ACL



Access Manager Web Portal Manager - Windows Internet Explorer

http://ptah.sara.it/pdadmin/pdmainframe.jsp

File Modifica Visualizza Preferiti Strumenti ?

IBM Tivoli Identity Manager Access Manager Web Por...

Access Manager
Versione 6.0

Elenco attività

- ▼ Utente
 - Ricerca utenti
 - Crea utente
 - Importa utente
 - Mostra politica utente globale
 - Cambia password
- ▼ Gruppo
 - Ricerca gruppi
 - Crea gruppo
 - Importa gruppo
- ▶ Spazio oggetti
- ▶ ACL
- ▶ POP
- ▶ Regola di autorizzazione
- ▶ Risorse GSO
- ▶ Dominio protetto
- ▶ WebSEAL
- ▶ Session Management Server

Proprietà utente

Generale Gruppi Credenziali GSO Politica

ID utente
roberto.puscio

L'utente è un membro di questi gruppi

Aggiungi... Elimina

Seleziona	Nome gruppo
☐	spwusergroup

ile della gestione delle risorse è
implementazione dell'operazione
essa l'autorizzazione. Un componente
ne la politica che indirizza la richiesta
one per l'elaborazione.
ne il meccanismo di autorizzazione
al Sistema Industriale avviene, sulla
ad uno specifico gruppo LDAP,

Il test eseguito consiste nell'analizzare e verificare che le ACL siano correttamente implementate e attribuite all'utente di riferimento. Una corretta correlazione tra il gruppo di accesso TAM (Tivoli Account) e l'account ITIM (utente definito nel Tivoli Identity Manager).

IBM Tivoli Identity Manager - Windows Internet Explorer

https://sokar.sara.it/enrole/formviewer

File Modifica Visualizza Preferiti Strumenti ?

IBM Tivoli Identity Manager Access Manager Web Portal ...

Identity Manager
Version 4.6

HOME | MY ORGANIZATION | PROVISIONING | SEARCH | REPORT | CONFIGURATION | HELP |

You Are Here: Search > Modify Account

Add | Modify Account

SERITAMACNTAB1 EASY CLAIM/NOTICE SARA_POWER SERITAMACNTAB2 SERITAMACNTAB3

\$eritampvalid ☐

\$eritamsinglesign ☐

\$eritammaxfailedlogon

\$eritamgroupname reportSPW1430
spwusergroup

Search Delete

Submit Reset Cancel

Verifica della corretta attribuzione degli Amministratori di Sistema ITIM e del Sistema TAM



Anche facendo riferimento alla verifica svolta nel corrente trimestre in tema di rispetto delle disposizione del Garante Privacy circa gli amministratori di sistema, si è provveduto a verificare che gli amministratori censiti nel componente ITIM per la gestione dell'Identity Management coincidano con la lista ufficiale degli amministratori di sistema.



Il Provvedimento prevede che: *“Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante”.*

I test eseguiti hanno dato risultato parzialmente positivo, poiché è stato eseguito da parte dell'Ente Tutela Privacy, congiuntamente alla Direzione ICT, prima un censimento di tutti i sistemi, dei database e degli apparati di rete in esercizio e in seguito è stata eseguita una mappatura dei ruoli/persone fisiche da designare ad Amministratore di Sistema. In allegato è rappresentata l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato (cfr Tabelle 2, 3, 4). Di tale mappatura si fa anche cenno nel Documento Programmatico di Sicurezza (DPS) nel paragrafo relativo all'adempimento Privacy oggetto di verifica.

L'analisi della mappatura ha evidenziato la presenza di anomalie in quanto non sono stati censiti gli utenti (che svolgono attività di Amministratore di Sistema) appartenenti rispettivamente alle aree Applicative Premi e Amministrazione.



Il Provvedimento prevede che *“l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza^[1]”; inoltre “la designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato”.*

Si è riscontrata una sostanziale conformità al dettato normativo. Si è infatti appurato che l'Ente Tutela Privacy ha predisposto le lettere di nomina ad incaricato Amministratore di Sistema per tutti gli amministratori censiti, dettagliando in modo accurato gli ambiti di operatività consentiti in base ai profili assegnati.

Le nomine sono state correttamente conferite dal Responsabile dei trattamenti informatici, ovvero dal Direttore Centrale ICT.

Le nomine sono avvenute previa *“valutazione dell'esperienza, della capacità e dell'affidabilità de[i] soggett[i] designat[i]”.*

Tale circostanza, oltre ad essere stata riferita dal responsabile dell'Ente Gestione e Sviluppo infrastrutture Tecnologiche, è confermata dal fatto che i soggetti nominati hanno tutti responsabilità operative (e pertanto conoscenze tecniche ed esperienza) strettamente correlate alla nomina ricevuta ai fini del Provvedimento. Il processo di valutazione seguito non è stato documentato; al riguardo si rappresenta che il Provvedimento non ne impone la formalizzazione.

^[1] Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.



Per effetto del presente provvedimento si ha che: *“Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema”*.

Al tal fine è stato eseguito da parte dell'Ente Tutela Privacy, congiuntamente alla Direzione ICT, un censimento di tutti i sistemi, dei database, degli apparati di rete in esercizio affidati a società esterne.

In allegato (cfr Tabelle 2, 3, 4) si riportano conseguentemente gli esiti di tale mappatura.

Inoltre la scrivente funzione ha rilevato in corso di verifica che l'Ente Tutela Privacy sta predisponendo delle lettere di nomina ad incaricato Amministratore di Sistema per le società terze (censite per lo svolgimento di tali servizi), che dovranno essere accettate dai fornitori esterni.

Nel caso in cui il Garante, in sede d'ispezione, richiederà gli estremi identificativi delle persone fisiche preposte ad eseguire funzioni di Amministratore di Sistema, sarà cura della Compagnia, congiuntamente all'outsourcer a fornire, le lettere di nomina ad incaricato Amministratore di Sistema degli outsourcer e gli estremi identificativi delle persone interessate.



Il Provvedimento prevede che: *“Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi”.*

Si è riscontrato l'avvenuto acquisto ed installazione della “RSA enVision”. Tale piattaforma permette, così come verificato, di rispettare le prescrizioni del Provvedimento in quanto in grado di acquisire i log da apparati di rete, database ed applicativi, ed archiviare gli stessi per un congruo periodo^[1].

Così come chiarito dal Garante stesso^[2] i log acquisiti ed archiviati possono, in ipotesi minimale, limitarsi a registrare utenza dell'amministratore e data ora di login e logout (cfr Tabella 5). Tale è la configurazione che è stata impostata nella piattaforma della Compagnia.

I riscontri svolti hanno evidenziato che il programma installato è, allo stato, configurato per acquisire i log di tutti gli apparati di rete, database ed applicativi a meno di un DataBase (il DB2) e del sistema di autenticazione del mainframe (RACF) e del sistema ITIM.

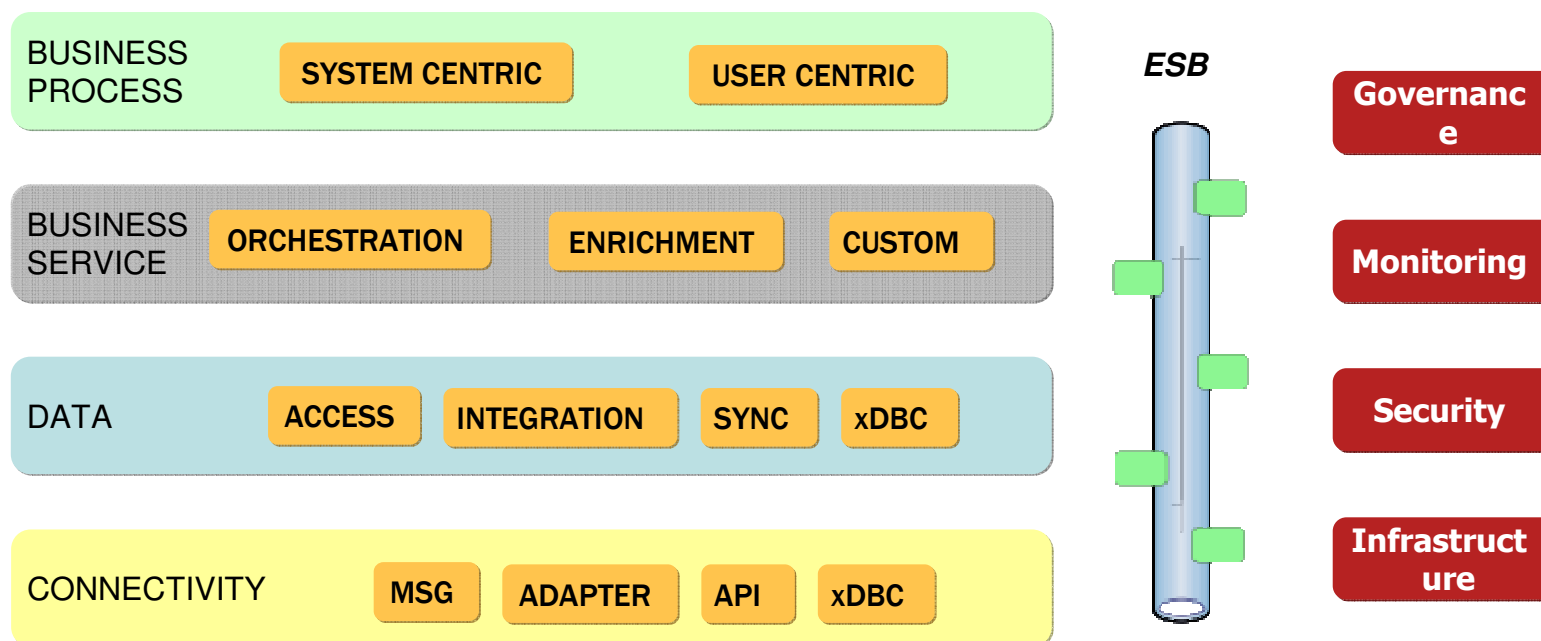
^[1] Attualmente il sistema è configurato al fine di archiviare illimitatamente le informazioni. Tale impostazione dovrà essere rivista sia per logiche di storage che di conservazione dei dati che –a fini privacy- deve essere funzionale alle motivazioni del trattamento dei dati.

^[2] Risposte alle domande più frequenti (FAQ) - Rif. comma 2, lettera f (Cosa si intende per access log (log-in, log-out), tentativi falliti di accesso, altro?...): Per access log si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software. Gli event records generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (timestamp), una descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di log-in, di log-out, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato...).



INDICE DELLA PRESENTAZIONE :

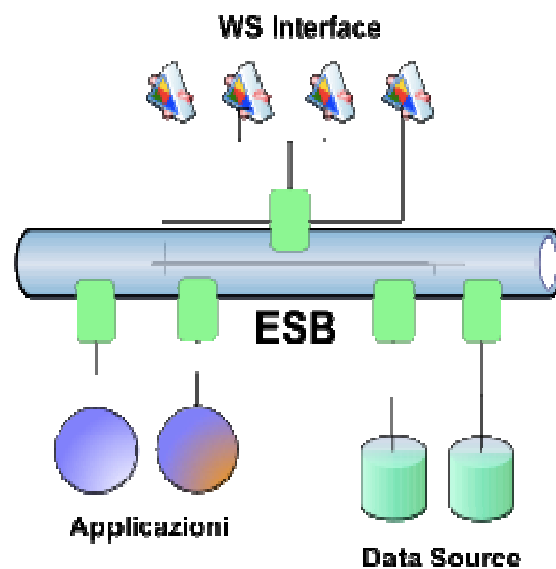
1. Architettura di I&AM
2. Soluzione adottata per l'I&AM
3. Controlli sull'Architettura I&AM
4. **SOA Principi**
5. SOA e Security
6. Information Risk Management per SOA
7. Message Security per la SOA-Security
8. Modello ideale di SOA-Security





- L'esposizione dell'interfaccia di servizio delle applicazioni è realizzata in standard WSs ed è istanziata attraverso

- Adapter
- Information BUS
- Registry
- Contratto di Servizio
- ...



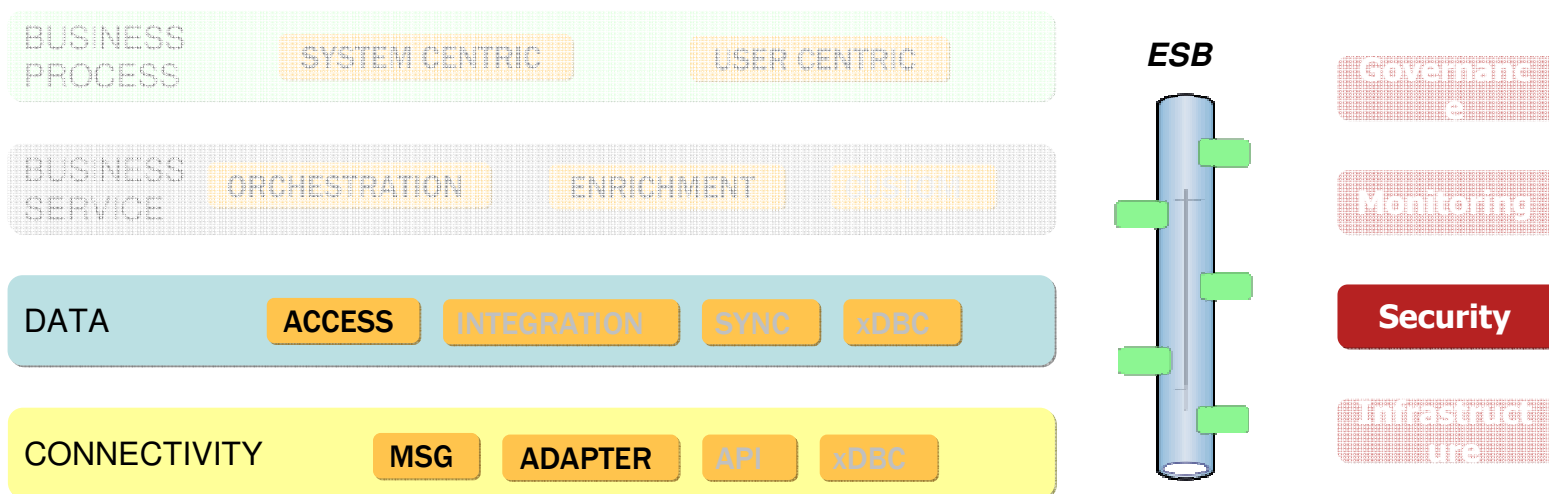


INDICE DELLA PRESENTAZIONE :

1. Architettura di I&AM
2. Soluzione adottata per l'I&AM
3. Controlli sull'Architettura I&AM
4. SOA Principi
5. **SOA e Security**
6. Information Risk Management per SOA
7. Message Security per la SOA-Security
8. Modello ideale di SOA-Security

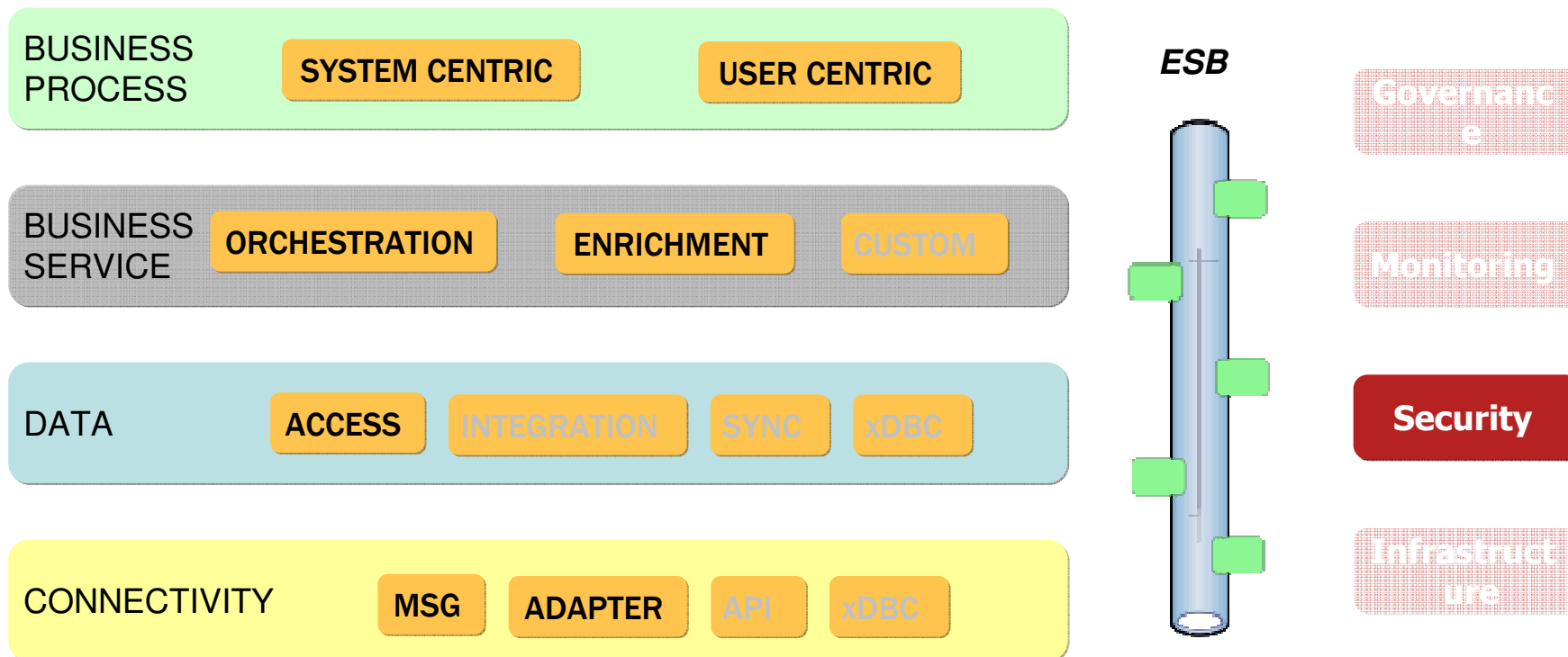


- La SOA-Security si sostanzia con la messa in sicurezza:
 - dei messaggi scambiati fra i WSs
 - degli Adapter che interfacciano le applicazioni all'ESB
 - dell'accesso ai DATI





- Evoluzioni del contesto di SOA-Security portano al controllo esteso all'orchestramento dei processi di business, alla verifica dell'enrichment dei messaggi e non ultimo all'enforcement del modello di interfacciamento fra WSs, sistemi ed utenti





INDICE DELLA PRESENTAZIONE :

1. Architettura di I&AM
2. Soluzione adottata per l'I&AM
3. Controlli sull'Architettura I&AM
4. SOA Principi
5. SOA e Security
6. **Information Risk Management per SOA**
7. Message Security per la SOA-Security
8. Modello ideale di SOA-Security



Nel passaggio dalle architetture IT tradizionali a quelle SOA, una delle strutture metodologiche che non può essere conservata è quella della *valutazione del rischio*.

Nelle architetture tradizionali difatti un servizio è comunemente erogato da un'architettura *n-tier statica* in cui le componenti, costanti in numero ed in ordine di attraversamento, costituiscono una sorta di percorso obbligatorio in cui calare lo scenario di rischio di cui si vuole effettuare il calcolo.

Nelle architetture orientate ai servizi abbiamo un nuovo panorama in cui il servizio di business può essere creato dalla composizione discrezionale di servizi elementari di volta in volta variabili nel tempo e nella sequenza di attraversamento.

Basti pensare, ad esempio, ai servizi business e consumer erogati da insiemi strutturalmente diversi di WS, che hanno però un'intersezione non vuota.

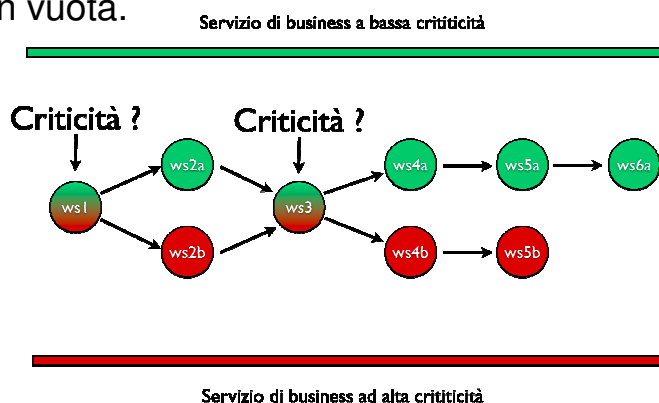


Figura 3 – Service Composition e criticità dei WS



In termini assolutamente riduttivi, l'approccio da perseguire nella valutazione del rischio di implementazioni SOA è quello di calcolare come la composizione di Web Services (WS), ognuno con il proprio livello di rischio sulle informazioni che manipola, si riversi sul calcolo del rischio complessivo del Servizio di Business (SB), senza che questo diventi troppo semplicisticamente la ricerca del massimo rischio nella somma dei rischi dei servizi attraversati ($\text{Rischio}(\text{SB}) = \text{Somma}(\text{Rischio}(\text{WS}_i))$).

Possiamo definire il rischio associato al singolo WS (Figura 4) come una funzione che assume come parametri di input i seguenti elementi:

- Criticità associata ai dati in input al servizio
- Criticità associata ai dati in output dal servizio
- Criticità associata ai dati acceduti dal servizio rispetto alla modalità di accesso
- Criticità associata alla piattaforma tecnologica di erogazione del servizio in termini di affidabilità, vulnerabilità e minacce

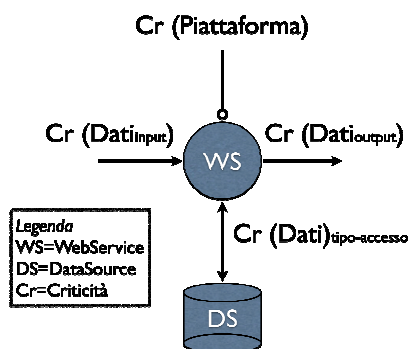


Figura 4 – Modello di calcolo del rischio per un generico WS



Abbiamo così caratterizzato il rischio tecnologico del WS relativamente alle informazioni che lo stesso accede e/o elabora e rispetto alla piattaforma tecnologica attraverso cui viene realizzato.

Prendendo a riferimento una modalità di service composition in cui può cambiare il numero di WS attraversati, nonché i dati acceduti dai singoli WS, possiamo facilmente dedurre che la criticità o il rischio associato al singolo WS risultano dipendenti dal Business Service in cui tale WS è utilizzato.

In tal senso ci viene in aiuto un modello probabilistico molto simile a quello delle equazioni d'onda (cfr. equazioni di Schrödinger), che nel nostro caso rappresentano l'ampiezza di probabilità dell'utilizzo di differenti configurazioni del WS nella composizione di servizi di business.

Definiamo quindi il livello di rischio associato al singolo WS come una funzione della probabilità del WS di accedere ad un determinato dato nella composizione del Servizio di Business (SB), il tutto moltiplicato per la criticità del dato acceduto, o in sintesi:

$$Cr(WS)_{SB} = \Psi_i Pr_{accesso}(Dato_i, SB)_{WS} \times Cr(Dato_i)$$

$$\Psi_i = \left| \sum_i \right|$$

oppure

dove Ψ è una funzione di composizione la cui modalità di applicazione può essere ricondotta ad una sommatoria normalizzata, oppure nei casi di maggior complessità alla sommatoria normalizzata con in aggiunta termini costanti, quali la criticità massima dei dati acceduti dal WS.



$$\Psi_i = \left| \max (Cr(Dato_i) + \sum_i \right|$$

Per il calcolo della funzione di rischio tecnologico del servizio di business nel suo complesso basterà comporre aritmeticamente le criticità dei WS ricavate attraverso l'uso delle nostre funzioni d'onda semplificate, che tengono già in conto i fattori di complessità della service composition nell'accesso a insiemi non costanti di dati.

$$Cr(SB) = Cr(WS1)SB + Cr(WS3)SB + Cr(WS4)SB + Cr(WS7)SB + Cr(WS9)SB + Cr(WS10)SB$$

Basterà infine aggiungere la criticità relativa alla sensibilità dello stesso rispetto al business per ottenere il livello di rischio complessivo del servizio.

$$Rischio (SB) = Cr(SB) + Sensibilità (SB)$$

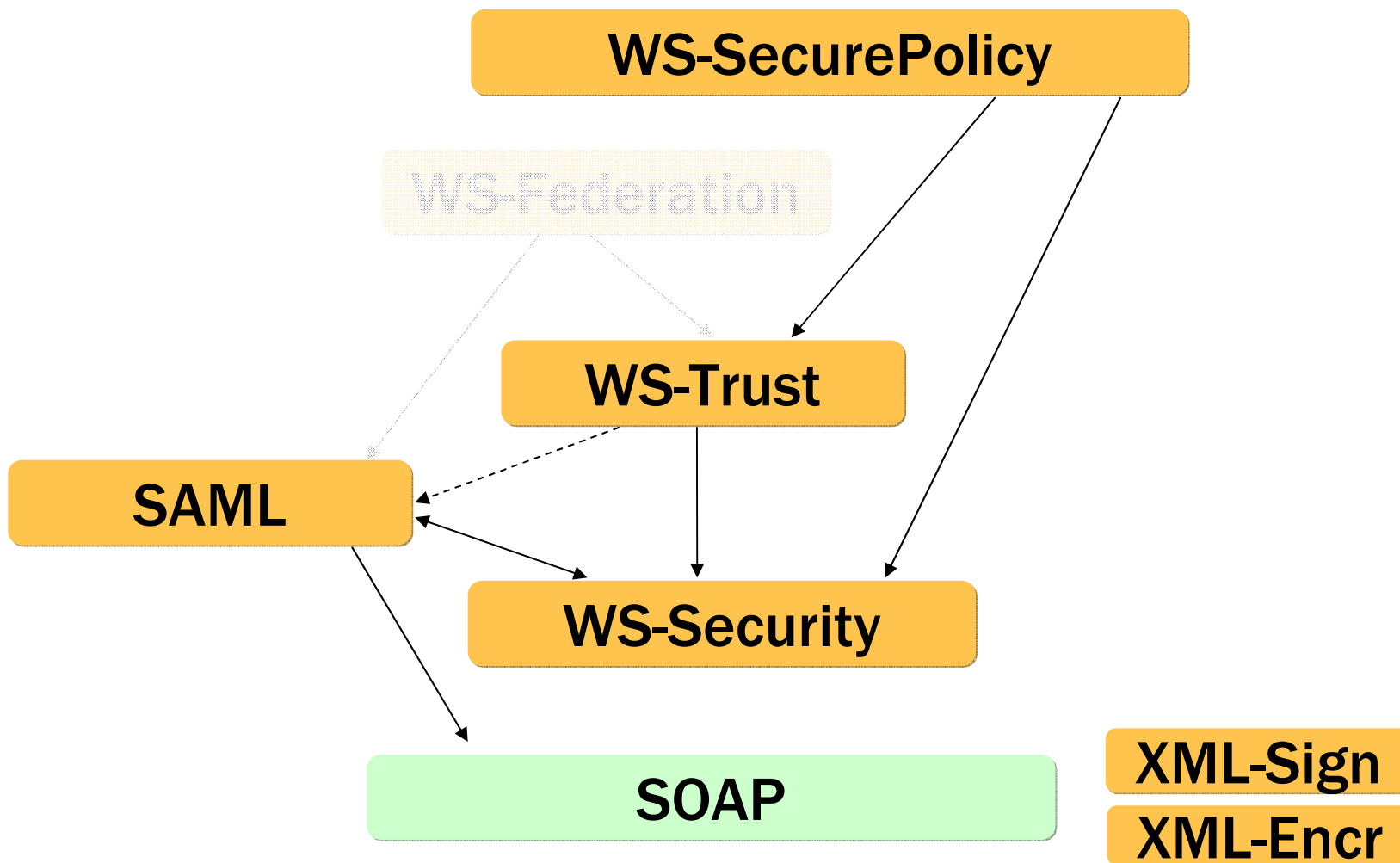
In questo modello non è ovviamente possibile, visto l'approccio olistico, ricondurre i WS ad un solo valore di rischio associato, a meno di avere dei WS specificatamente costruiti per il singolo Servizio di Business e con accesso ad un costante insieme di dati.

In tale scenario il rischio associato al singolo WS torna ad essere una costante e non più una funzione di probabilità e perde quindi d'interesse rispetto al presente lavoro.



INDICE DELLA PRESENTAZIONE :

1. Architettura di I&AM
2. Soluzione adottata per l'I&AM
3. Controlli sull'Architettura I&AM
4. SOA Principi
5. SOA e Security
6. Information Risk Management per SOA
7. **Message Security per la SOA-Security**
8. Modello ideale di SOA-Security



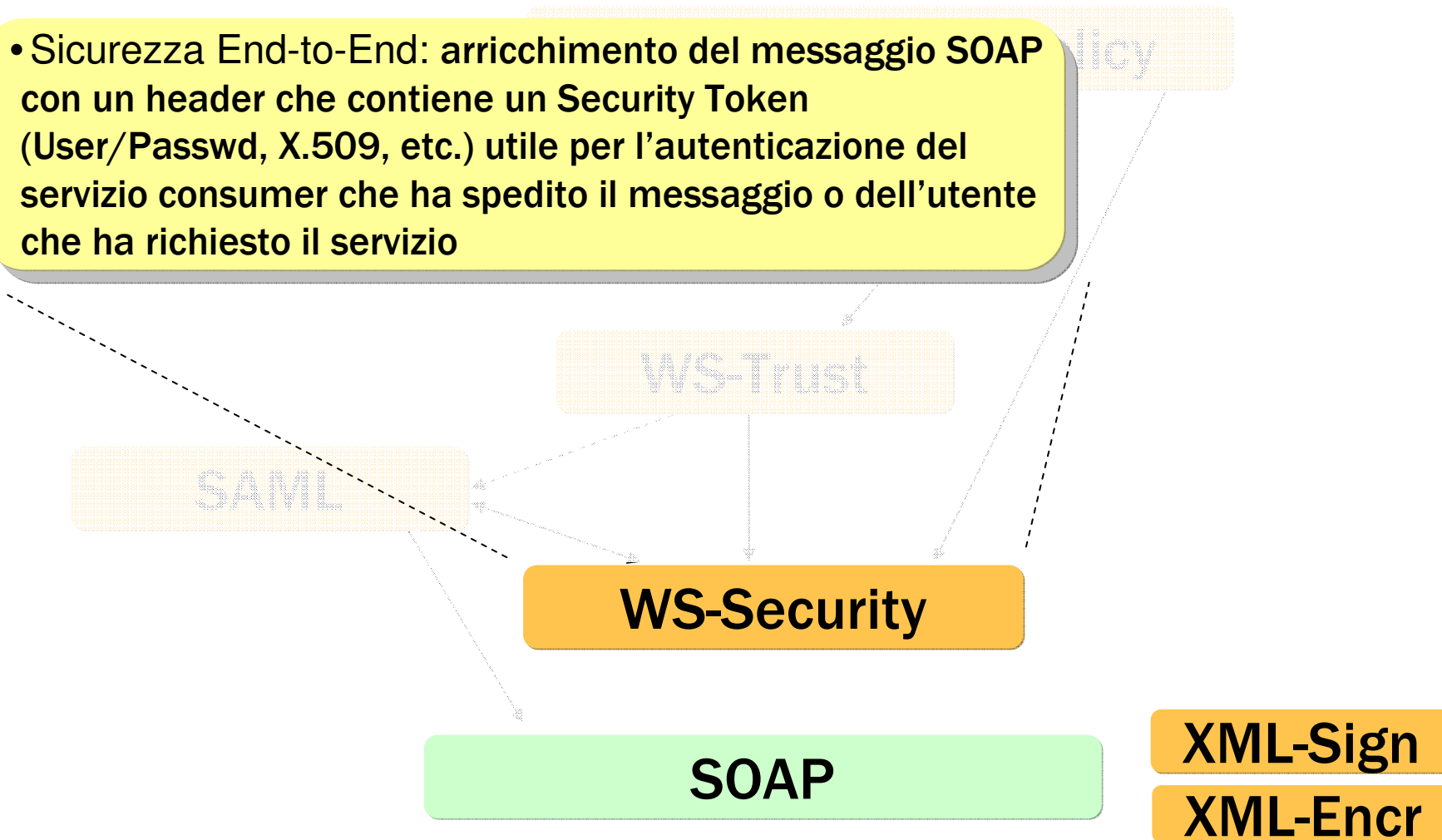
Standard di Sicurezza per SOA: message security



Standard di Sicurezza per SOA: message security



- Sicurezza End-to-End: arricchimento del messaggio SOAP con un header che contiene un Security Token (User/Passwd, X.509, etc.) utile per l'autenticazione del servizio consumer che ha spedito il messaggio o dell'utente che ha richiesto il servizio



Standard di Sicurezza per SOA: message security



- **Asserzioni di Sicurezza:** arricchimento del messaggio SOAP con informazioni utili all'autorizzazione del servizio consumer che ha spedito il messaggio o dell'utente che ha richiesto il servizio. Possibilità di handshake dei parametri di autorizzazione.

SAML

WS-Security

SOAP

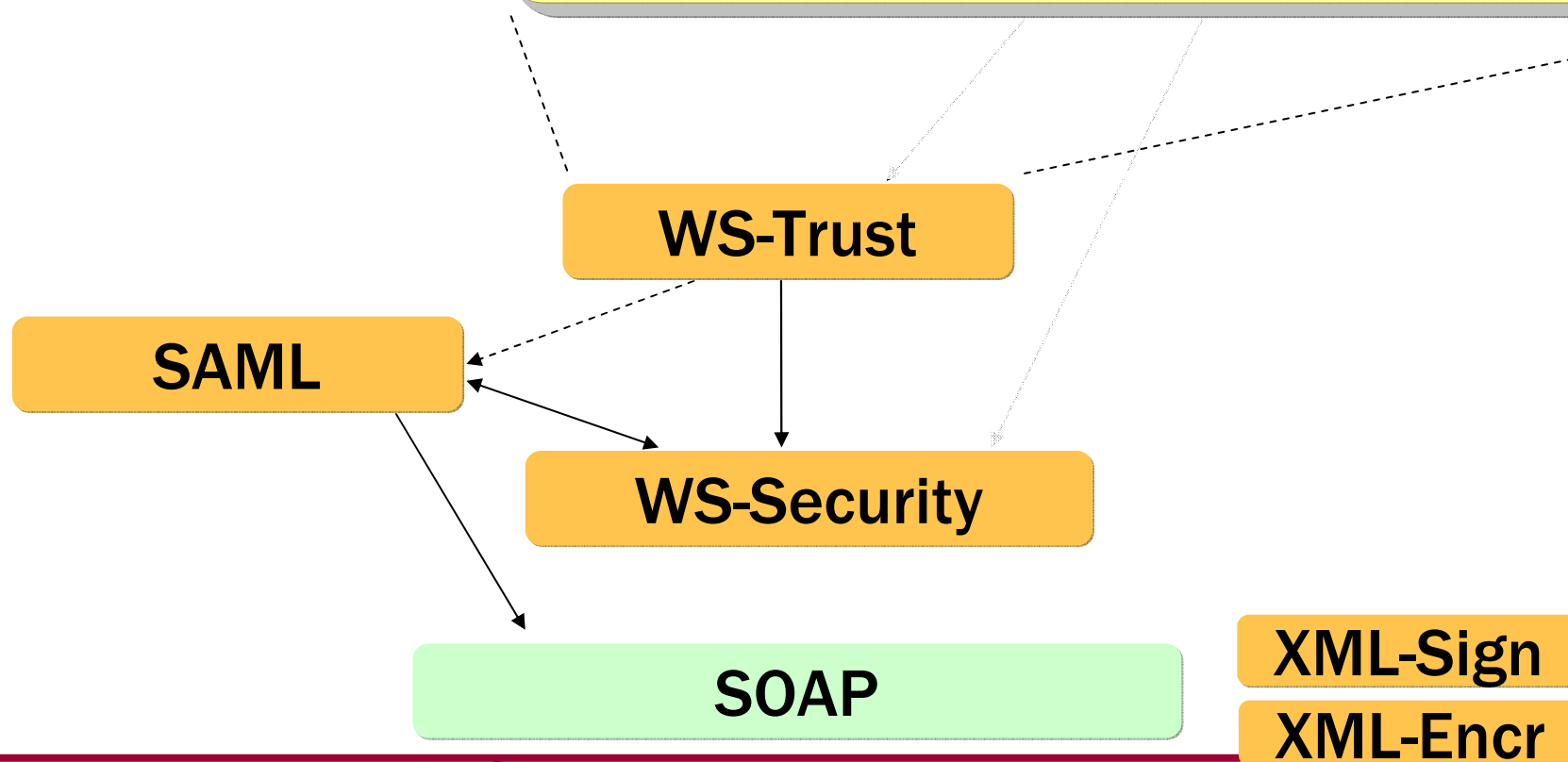
XML-Sign

XML-Encr

Standard di Sicurezza per SOA: message security

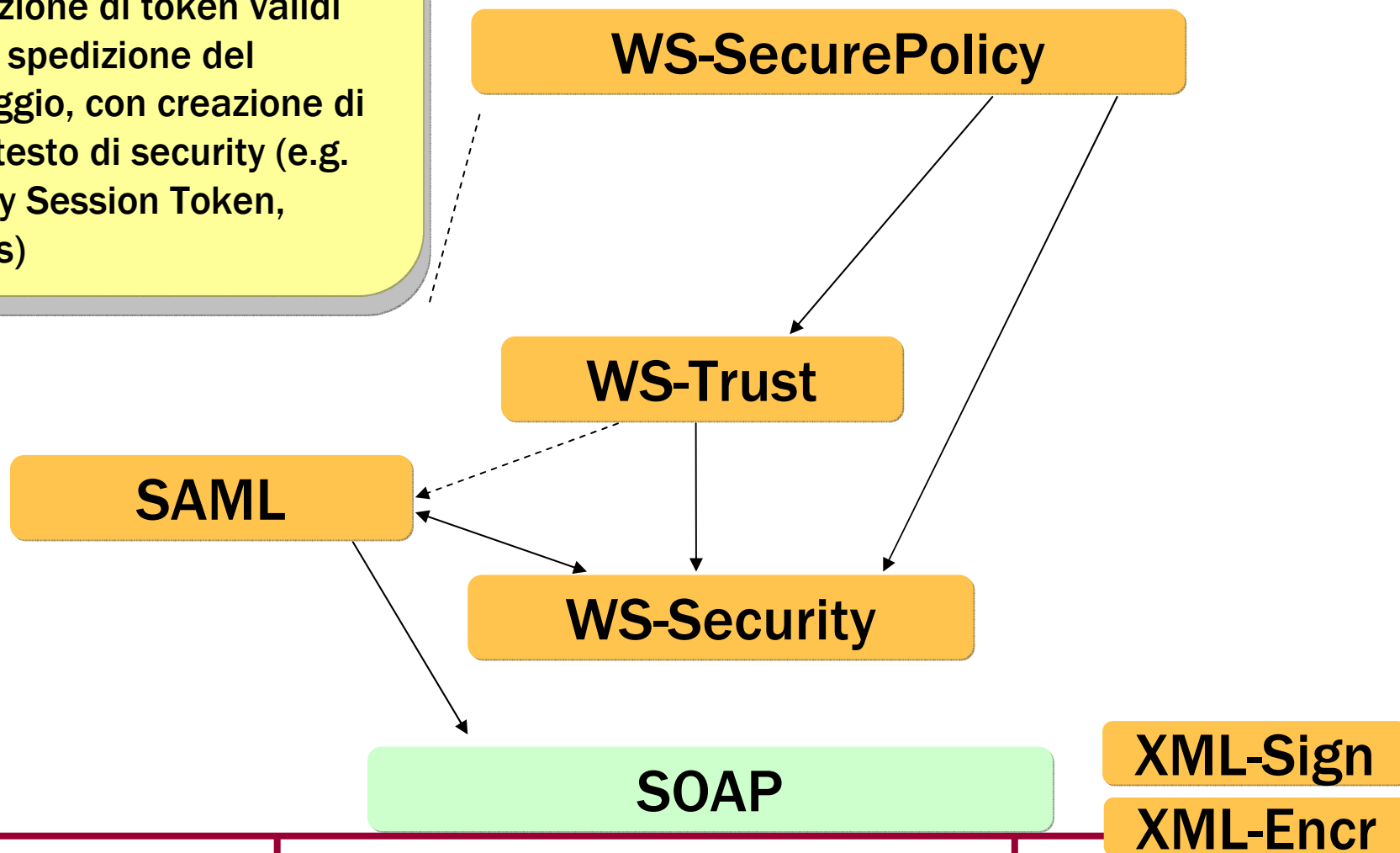


- Token Exchange: interscambio dei token di security, per interazione fra WSs con modelli di autenticazione differenti (e.g. U/P → X.509, X.509 → Kerberos, etc.)





- Security Context:
generazione di token validi
oltre la spedizione del
messaggio, con creazione di
un contesto di security (e.g.
Security Session Token,
Cookies)

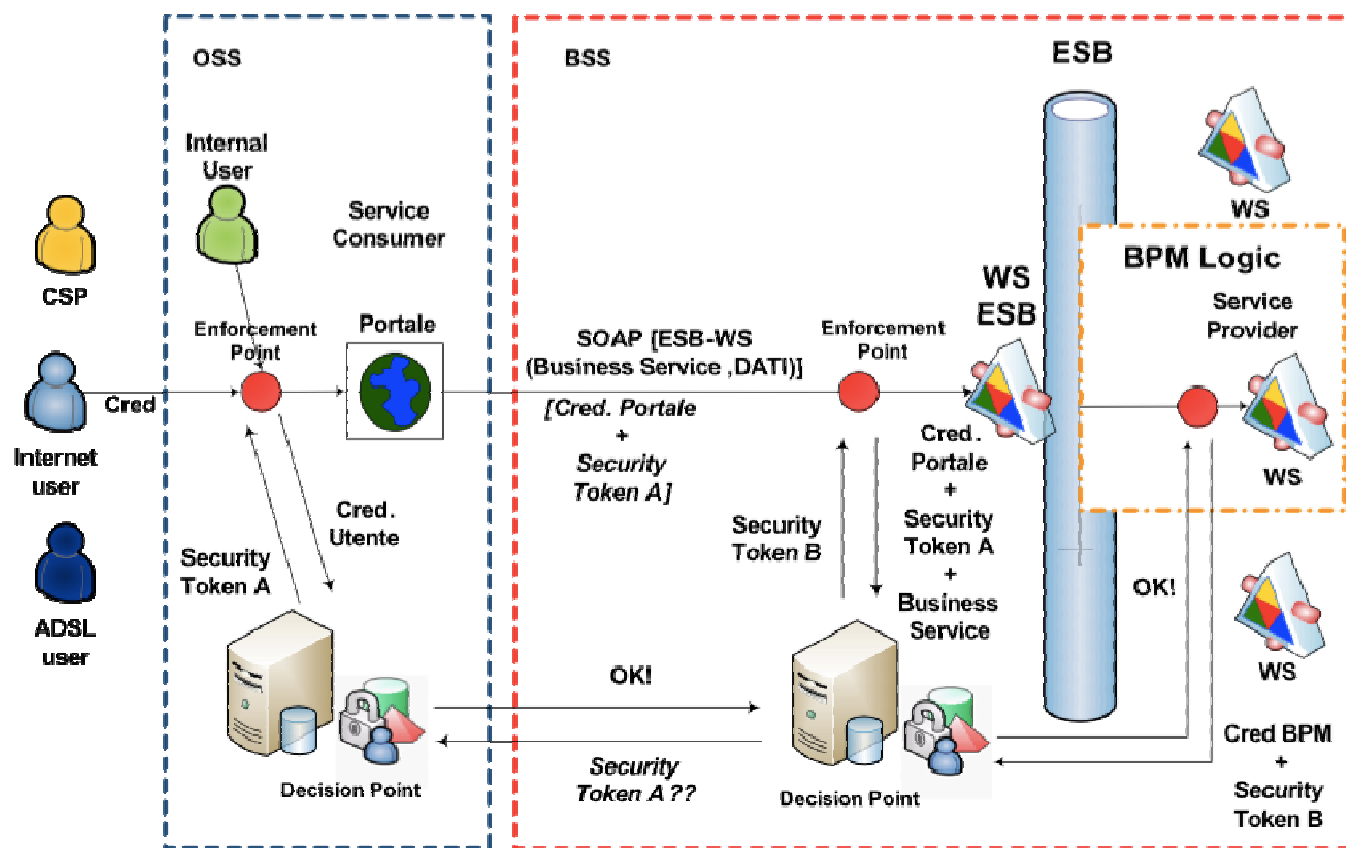




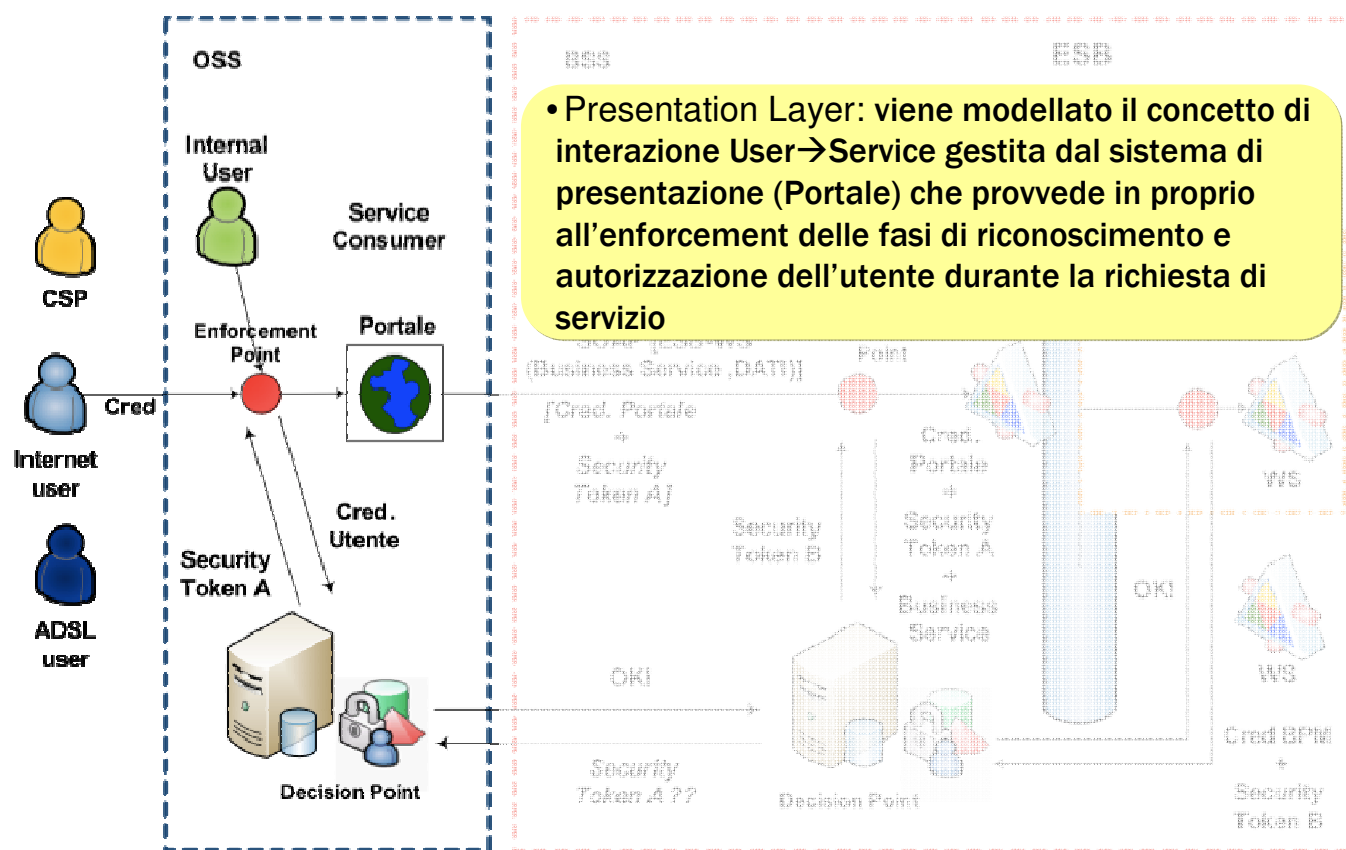
INDICE DELLA PRESENTAZIONE :

1. Architettura di I&AM
2. Soluzione adottata per l'I&AM
3. Controlli sull'Architettura I&AM
4. SOA Principi
5. SOA e Security
6. Information Risk Management per SOA
7. Message Security per la SOA-Security
8. **Modello ideale di SOA-Security**

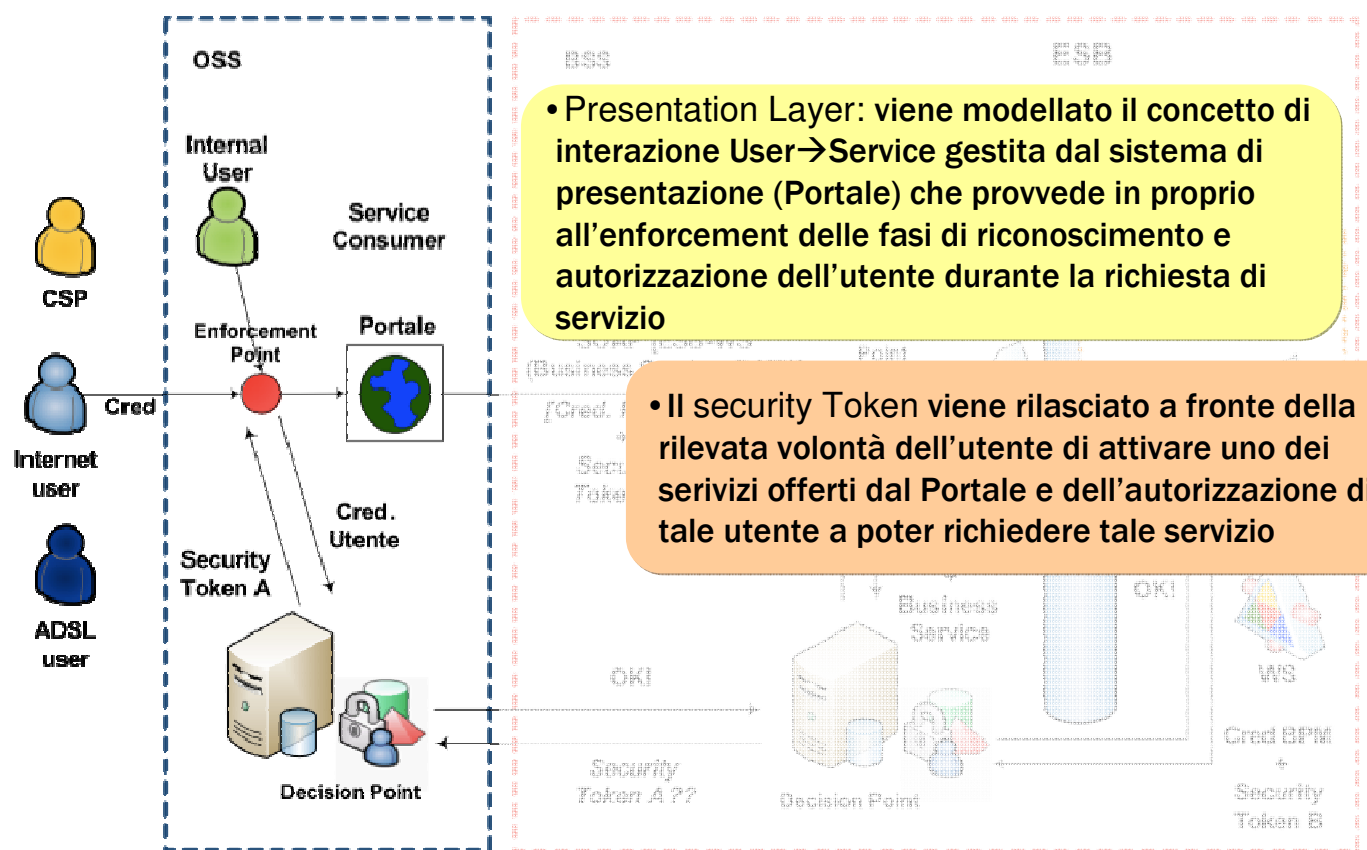
Soa Security: uno use-case

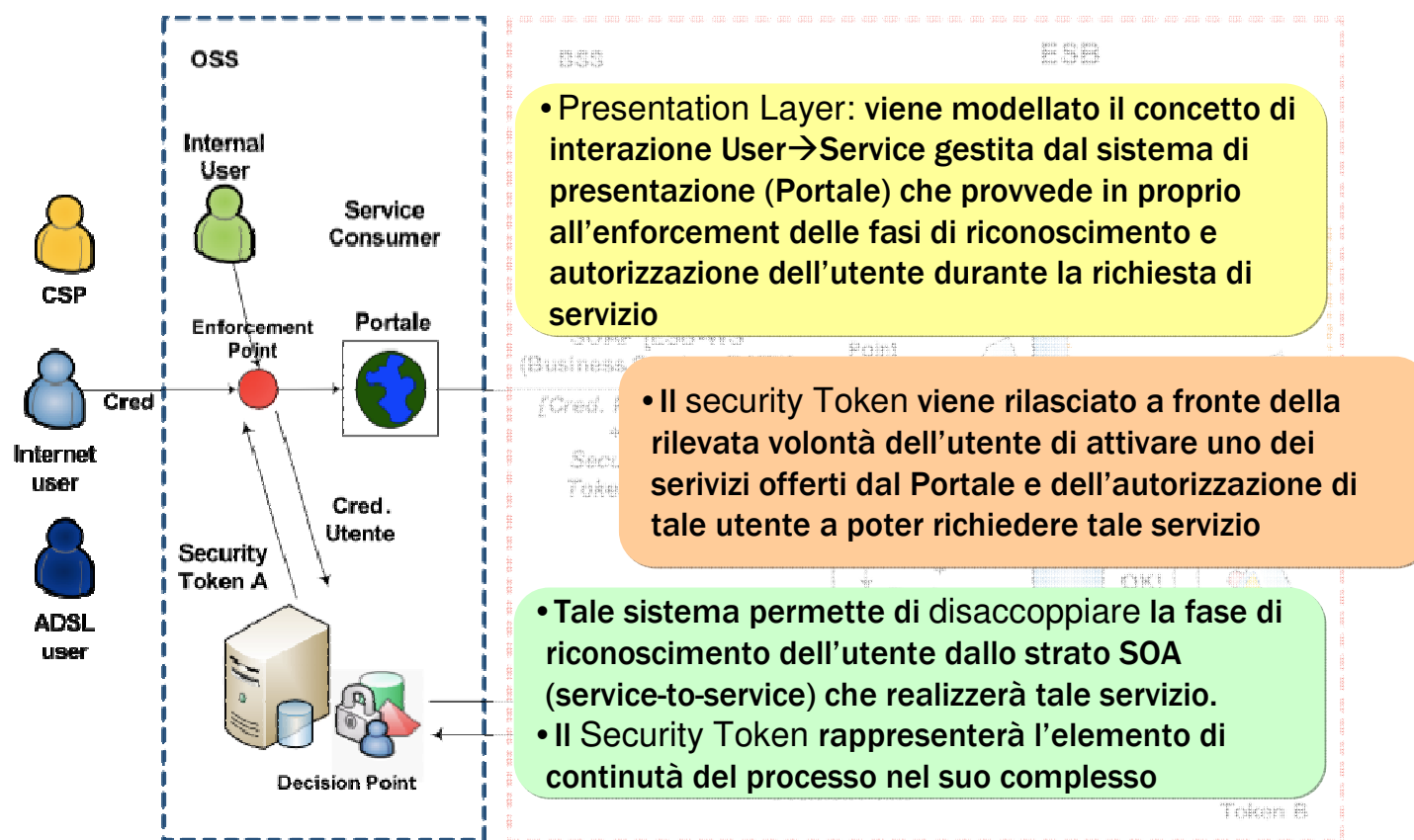


Soa Security: uno use-case



Soa Security: uno use-case

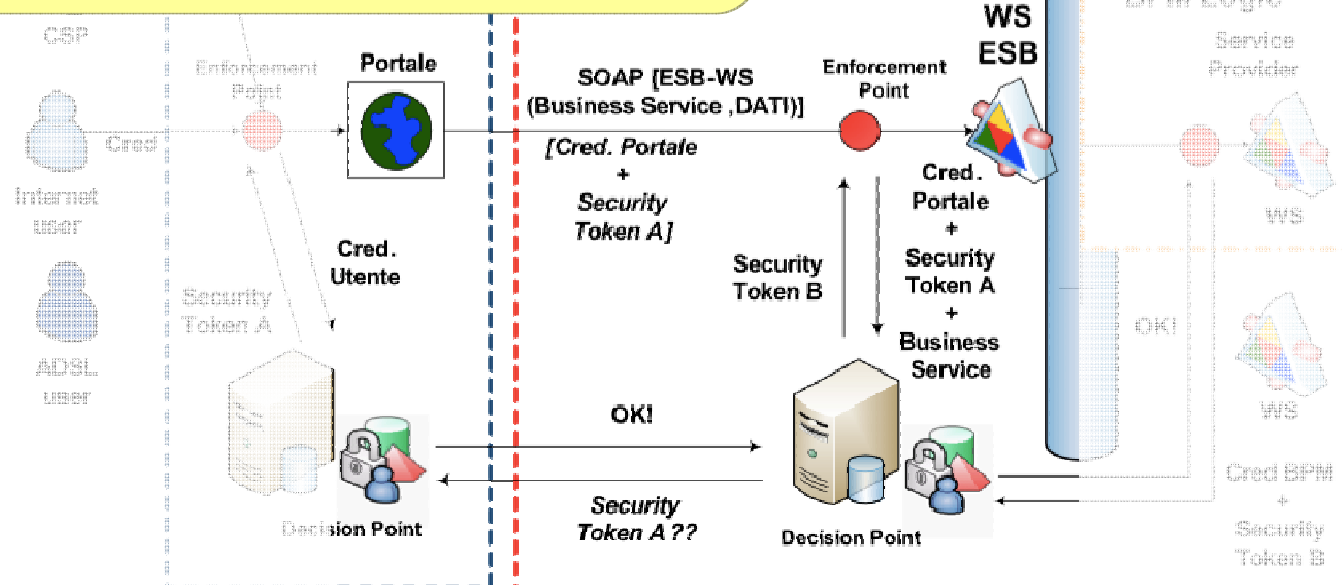




Soa Security: uno use-case

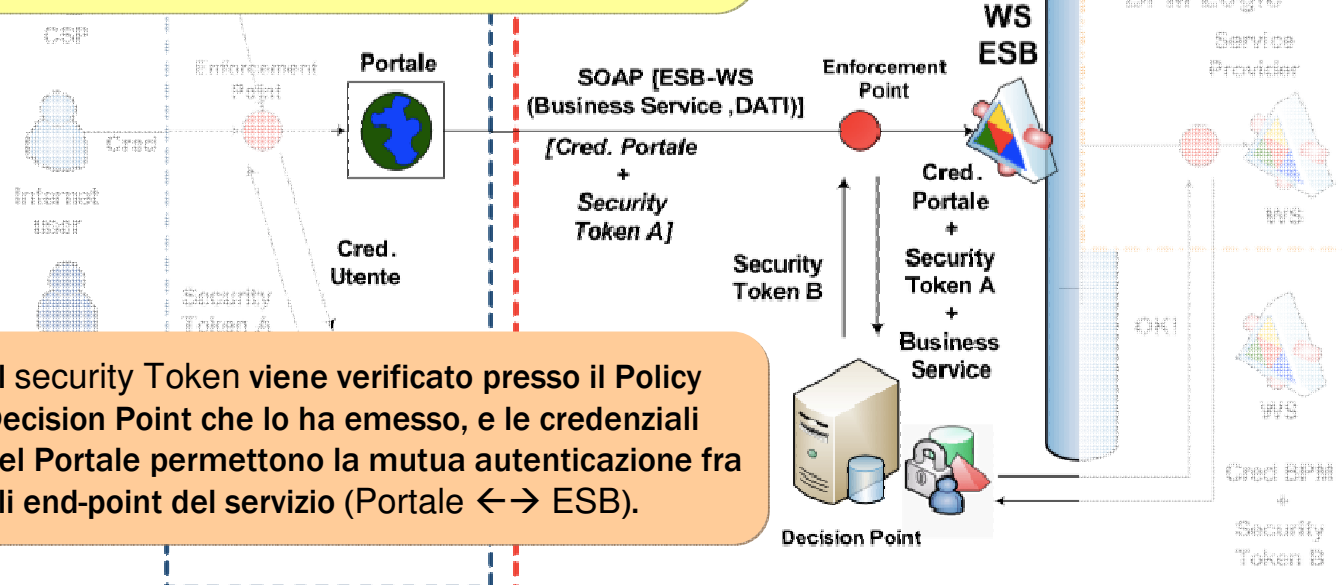


- Connectivity Layer: viene modellato il concetto di interazione Consumer→Provider fra il sistema di presentazione (Portale) e il WS che interfaccia l'ESB





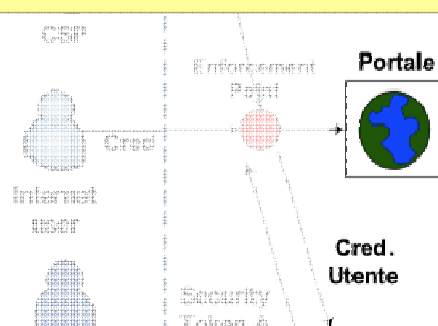
- Connectivity Layer: viene modellato il concetto di interazione Consumer→Provider fra il sistema di presentazione (Portale) e il WS che interfaccia l'ESB



- Il security Token viene verificato presso il Policy Decision Point che lo ha emesso, e le credenziali del Portale permettono la mutua autenticazione fra gli end-point del servizio (Portale ↔ ESB).



- Connectivity Layer: viene modellato il concetto di interazione Consumer→Provider fra il sistema di presentazione (Portale) e il WS che interfaccia l'ESB

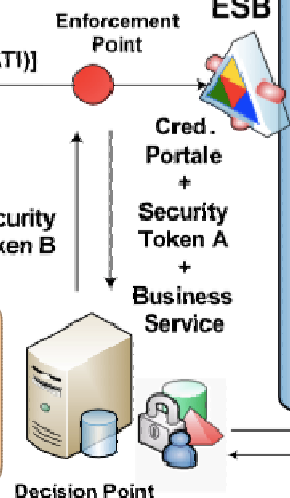


- Il security Token viene verificato presso il Policy Decision Point che lo ha emesso, e le credenziali del Portale permettono la mutua autenticazione fra gli end-point del servizio (Portale ↔ ESB).

SOAP [ESB-WS
(Business Service ,DATI)]

[Cred. Portale
+
Security
Token A]

Security
Token B



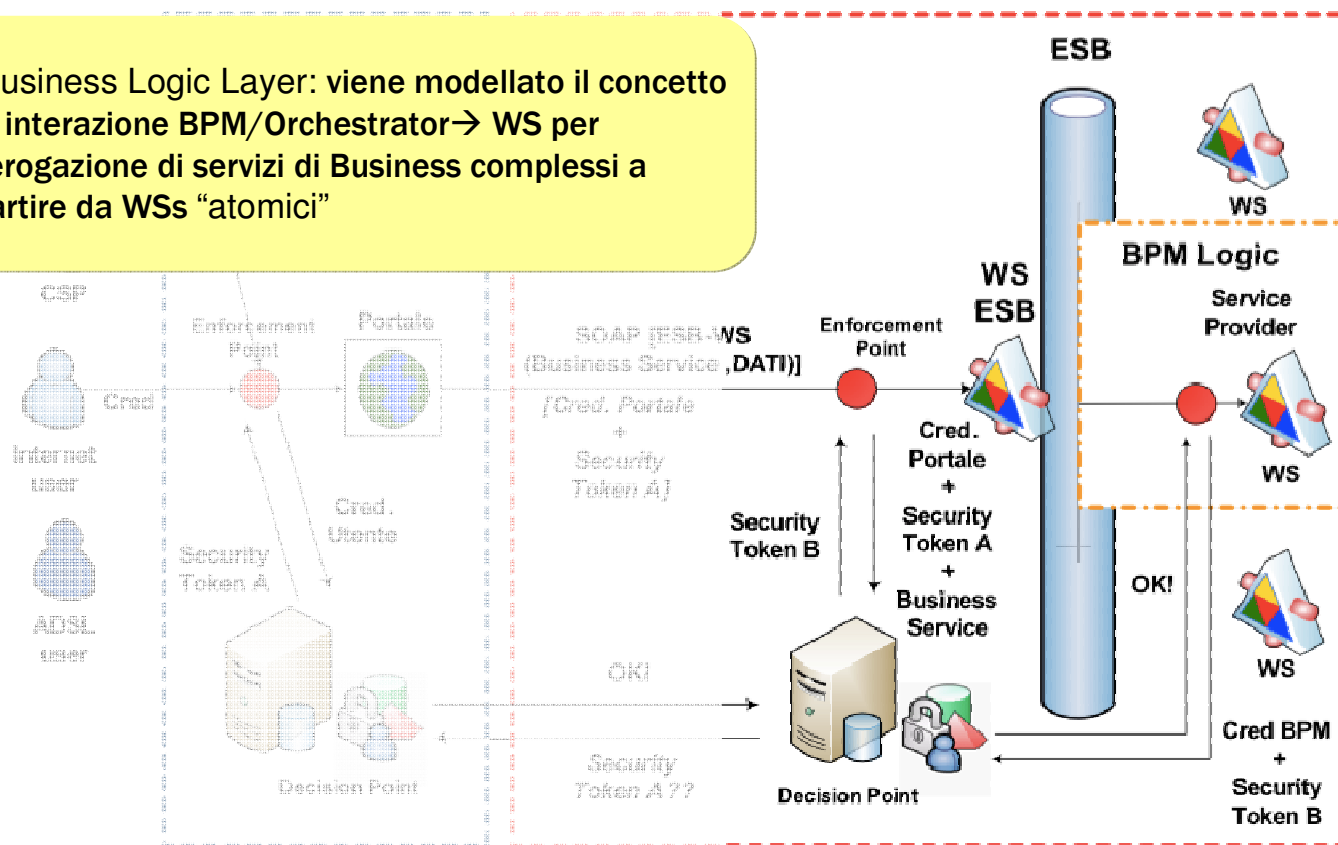
ESB

- Il Policy Decision Point è l'unico punto di contatto fra le due strutture. Potrebbe essere un'infrastruttura comune (simile ad una PKI) ad emettere il Token per tutti i partecipanti.
- Potrebbe essere utilizzato ad esempio un TIMESTAMP firmato.

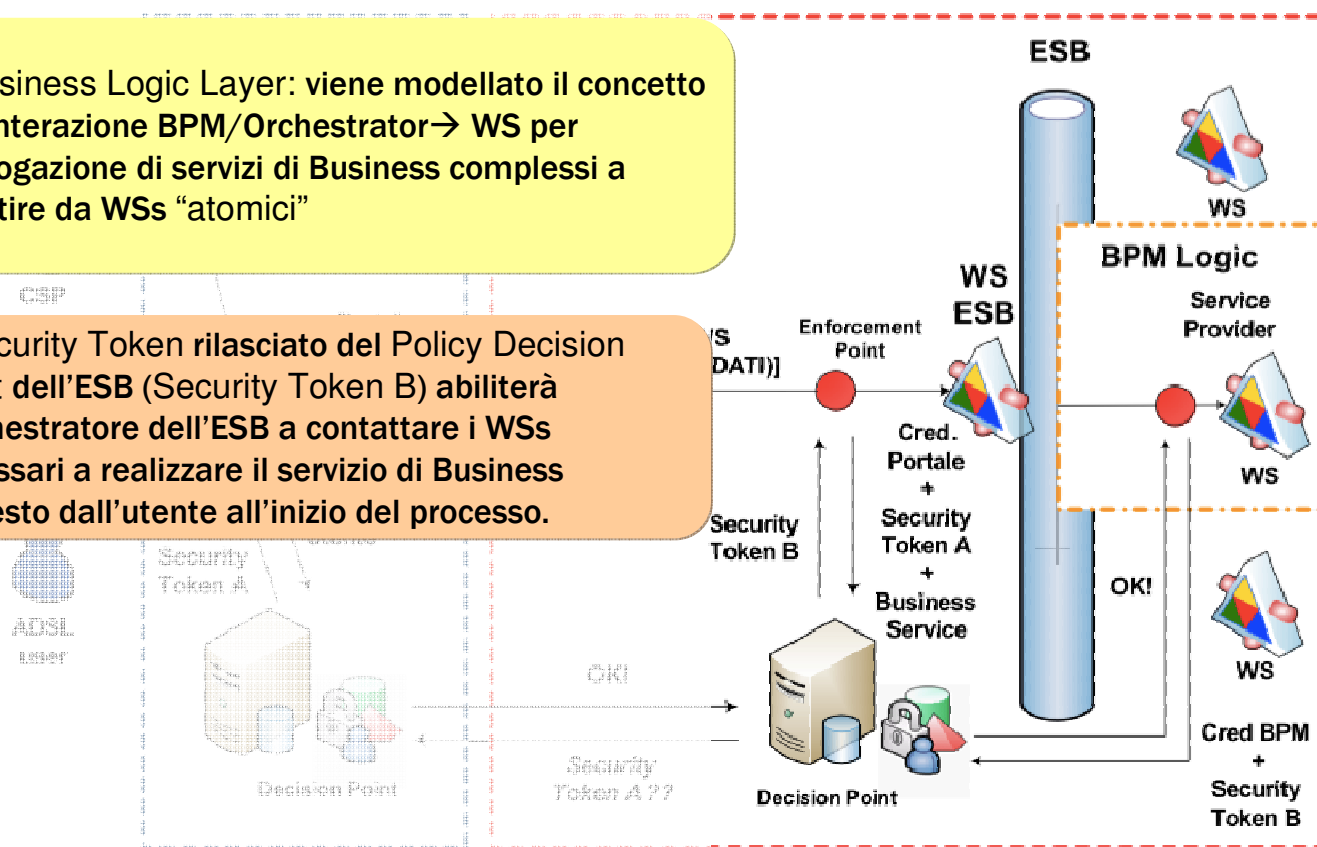
Security
Token B



- Business Logic Layer: viene modellato il concetto di interazione BPM/Orchestrator → WS per l'erogazione di servizi di Business complessi a partire da WSs "atomici"



- Il security Token rilasciato dal Policy Decision Point dell'ESB (Security Token B) abiliterà l'orchestratore dell'ESB a contattare i WSs necessari a realizzare il servizio di Business richiesto dall'utente all'inizio del processo.

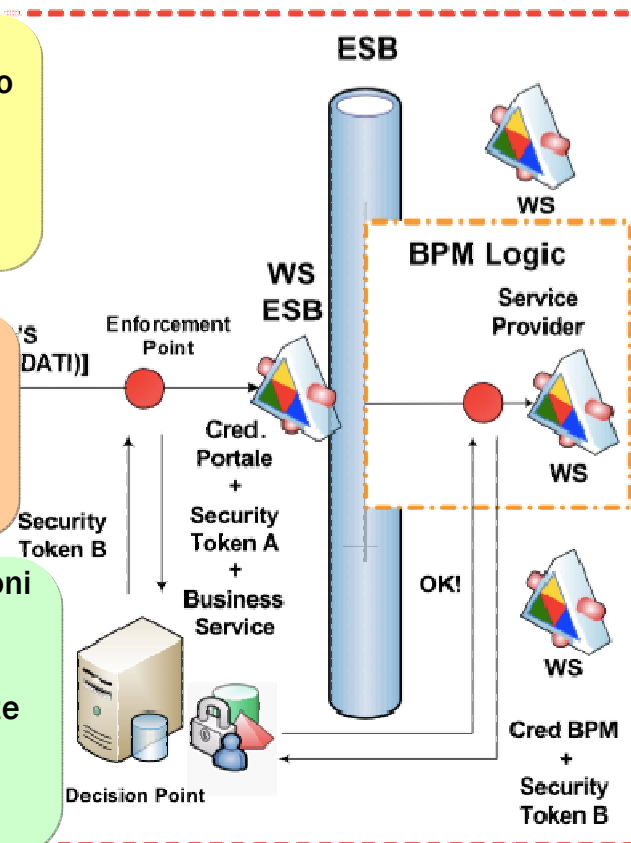




- Business Logic Layer: viene modellato il concetto di interazione BPM/Orchestrator → WS per l'erogazione di servizi di Business complessi a partire da WSs "atomici"

- Il security Token rilasciato del Policy Decision Point dell'ESB (Security Token B) abiliterà l'orchestratore dell'ESB a contattare i WSs necessari a realizzare il servizio di Business richiesto dall'utente all'inizio del processo.

- In questo modo saranno evitate eventuali attivazioni di servizi "atomici" non richieste dal modulo di orchestramento dell'ESB.
- La presentazione di un eventuale Token C da parte di un fruitore esterno all'ESB è riconducibile a caso d'interazione fra lo strato di Presentazione e il WS dell'ESB





Grazie per l'attenzione

Ing. Marco Tulliani
Email:marco.tulliani@tin.it
cell:3346065537