Sicurezza nelle Grid

Sommario

- **Il Problema della Sicurezza nelle Grid**
- Grid Security Infrastructure
- Autorizzazione

Il Problema della Sicurezza nelle Grid (1)

- Le risorse sono presenti in domini amministrativi multipli e distinti ("siti").
- Una singola applicazione può usare risorse di più siti.
- Ogni sito ha i propri preesistenti requisiti, politiche e meccanismi di sicurezza.

Il Problema della Sicurezza nelle Grid (2)

- Le Virtual Organization (VO) hanno le loro proprie politiche e specifiche di sicurezza.
- Un singolo utente o risorsa può far parte di più VO.
- L' insieme di utenti, risorse, e siti in una VO può essere grande, dinamico, e variabile.
- E' spesso difficile stabilire relazioni fiduciarie tra siti.

Grid Security: Requisiti Utente

- Facilità d'uso (es., singolo controllo di accesso).
- Capacità di eseguire applicazioni che usano risorse distribuite in una VO.
- Modello di affidabilità basato sugli utenti.
- Proxies / agenti.

Requisiti dei Siti

- Aderenza alle politiche del sito
  - riguardanti autorizzazione, auditing, accounting.
- Interoperabilità dei meccanismi di sicurezza locali.
- Politiche e meccanismi comprensibili e verificabili.

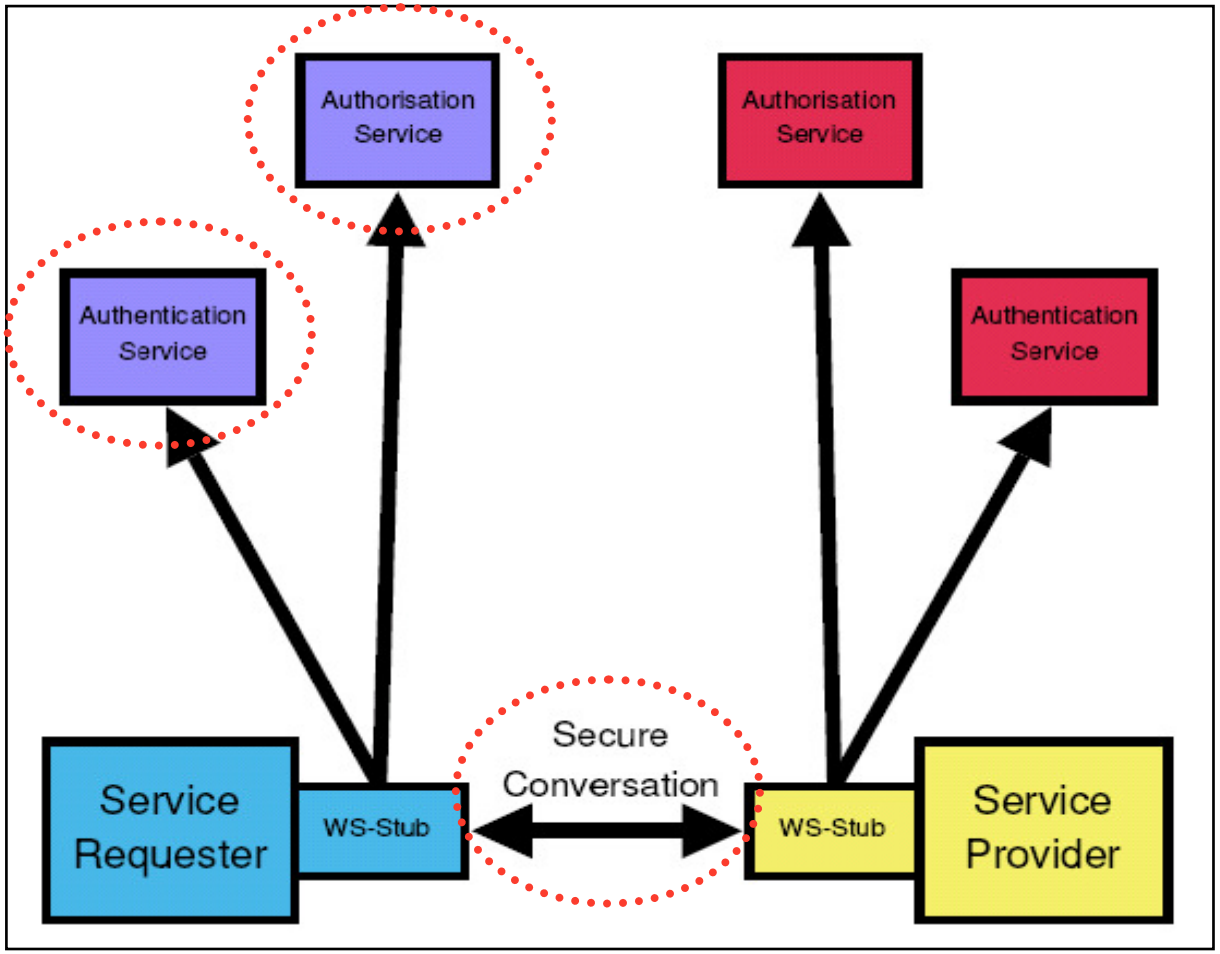
Requisiti delle VO

- Aderenza alle politiche della VO
  - riguardanti autorizzazione, auditing, accounting.
- Politiche e meccanismi comprensibili e verificabili.
- Meccanismi che gestiscano molti siti (scalabili).

Alcune Operazioni di Sicurezza

- Autenticazione
- Autorizzazione
- Revoca
- Protezione di Messaggi
  - Message integrity
  - Message confidentiality
- Delegation
- Auditing e Accounting
- Non-ripudio

Servizi di Sicurezza



Autenticazione

- Verifica dell'identità.

- Alcuni meccanismi esistono:
  - Username/password
  - Kerberos
  - Meccanismi a Chiave Pubblica
  - Biometrica

Autorizzazione

- Verifica dei diritti di uso
- Molti meccanismi esistono per la specifica e l'applicazione:
  - Offerti dai Sist. Operativi (es., permessi sui file Unix)
  - Offerti dalle applicazioni (e.g., permessi in un DBMS)
- Usualmente richiedono autenticazione, ma non sempre.

Revoca di Diritti

- Invalidare una credenziale di autenticazione o rimuovere una autorizzazione.
- I meccanismi di Revoca dipendono dai corrispondenti meccanismi di autenticazione/ autorizzazione.
- Problema principale: quanto tempo è necessario perchè una revoca abbia effetto?

Protezione di Messaggi

- Integrità
  - Autenticare il messaggio, e
  - Verificare che il messaggio ricevuto sia lo stesso messaggio inviato.
  - Una firma è un meccanismo di verifica dell'integrità anche se il mittente è offline.
- Riservatezza:
  - Assicurare che nessuno tranne il mittente e il destinatario possano leggere il messaggio.

Auditing e Accounting

- Auditing
  - Chi ha fatto che cosa su questa risorsa?
  - Richiede autenticazione

- Accounting
  - Chi ha usato e per quanto questa risorsa?
  - Politiche di costi

Non Ripudio

- Problema: come verificare un messaggio firmato quando la credenziale usata per firmarlo non è più valida?
  - La credenziale potrebbe essere stata revocata
  - La credenziale potrebbe essere scaduta
  - Il meccanismo di autenticazione usato nella firma potrebbe essere stato manomesso.

- Servizi di Non-ripudio sono servizi di terze parti che certificano e marcano temporalmente un messaggio firmato.

Certificati X.509

- Un certificato X.509 è una dichiarazione firmata da chi la fa che collega una chiave ad un nome.

- Consiste di:
  - Una struttura base contenente:
    - Un subject name
    - Una public key
    - Un validity time
    - Il nome del creatore
    - Una etichetta "CA"
    - … e altra informazione
  - Più la firma del creatore sulla struttura base.
- Il certificato può essere pubblico ma la chiave privata deve rimanere tale.

Come Acquisire un Certificato X.509

- Tipicamente, una entità genera una coppia *public/private key pair*, e mette la chiave pubblica in una richiesta di certificato che viene inviata ad una CA (certification authority).

- La CA decide se è il caso di onorare la richiesta; e nel caso la CA crea un certificato firmato e lo invia alla entità.

- Nessuno altro può "vedere" la private key.

Responsabilità di una CA

- Rilascio certificati
- Revoca certificati
- Rinnovo certificati in scadenza
- Sostituzione di certificatio di cui l'entità ha perso la password
- Autenticare/autorizzare le richieste
- Mantenere la politica dei certificati.

Grid Security Infrastructure

- Fornisce
  - Autenticazione (one-way o mutua)
  - Integrità dei messaggi e riservatezza
  - Delegation
- Estende lo standard di certificazione X.509 per includere i *proxy certificates* per delegation e singolo accesso (sign-on)
- Due modi operativi: **Transport-level** e **Message-level** security.
- GSI è stato sviluppato come parte del Globus Toolkit.

GSI con Transport-Level Security

- Implementazione originale di GSI
- Usa SSL/TLS, esteso per single-sign-on e delegation
- Assume un protocollo di trasporto connection-based (es., TCP).
- Usa certificati X.509 per autenticazione e per stabilire session keys.

GSI con Message-Level Security

- Nuova implementazione di GSI
- Usa WS-Security, XML-Signature e i procolli associati
- Fornisce sia
  - una session-based security (che assume un protocollo di trasporto connection-based e usa session keys) e
  - una per-message security (che non richiede protocollo di trasporto connection-based).

Certificati Proxy X.509

- Prodotti da entità certificata (o un altro certificato proxy), non da una Autorità di Certificazione
  - Ha (effettivamente) lo stesso nome del suo produttore
  - Ha una chiave pubblica/privata differente al suo produttore.
- Permette al possessore (del certificato e della chiave privata associata) di impersonare il produttore, con alcune restrizioni:
  - Usualmente un tempo di validità più breve
  - proxy flag limitati
  - restrizioni alle autorizzazioni
- Usata per singolo sign-on e delegation.

Autenticazione con Certificati Proxy X.509

- Simile alla autenticazione usando certificati X.509 regolari, eccetto il "certificate path" più lungo:
  1. CA_1: un "trust anchor", già noto e sicuro certif. CA

     …

  N+1. EEC: un certif. end-entity firmato da CA_N

  N+2. PC1: un certif. proxy firmato da EEC

  N+3. PC2: un certif. proxy firmato da PC1

     …
- Estensione alla sintassi X.509; non riconosciuta da software non-GSI (attualmente un Internet Draft in IETF).

Singolo Sign On

- Un utente può voler fare molte operazioni che richiedono l'autenticazione durante una sessione di lavoro o una giornata.

- Tradizionalmente, questo richiederebbe:
  - Inserire la password a chiave privata molte volte, o
  - Tenere la chiave privata decriptata sul disco, o
  - Fare tutte le operazioni che richiedono autenticazione da una istanza di un programma, o
  - Usare un hardware di autenticazione specializzato.

Usare i Certificati Proxy X.509 per Singolo Sign On

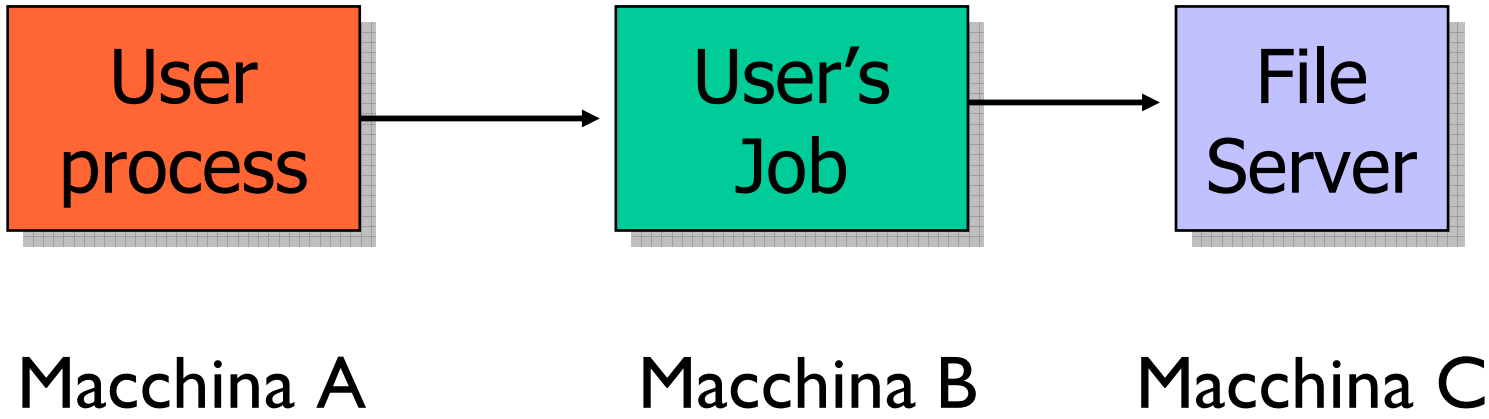
- L'utente:
  - Crea un certificato proxy di breve periodo
  - Mantiene il certificato e la chiave privata decriptata sulla memoria locale
  - Lo usa al posto di un certificato permanente
  - Al termine distrugge il proxy o lo lascia scadere.

- Vi è il rischio che la chiave privata proxy possa essere compromessa, ma il potenziale danno è limitato dal breve periodo di vita del proxy.

Usare i Certificati Proxy X.509 per Delegation

- Assumiamo che un processo utente sull' host **A** vuole delegare un processo server sull' host **B**, che deve accedere risorse sull' host **C**.
  1. Il processo server su **B** genera una coppia di chiavi e invia una richiesta (con la chiave pubblica) al processo utente dell'host **A**.
  2. Il processo utente usa il suo certificato proxy locale ($\mathbf{PC_A}$) per firmarne uno nuovo ($\mathbf{PC_B}$) in risposta alla richiesta del server
  3. Il processo server sull'host **B** quindi usa $\mathbf{PC_B}$ (e la chiave privata generata al passo 1) per autenticarsi sull' host **C**.
- Nessuna chiave privata viene inviata sulla rete.

Esempio di Delegation



Altri Usi dei Certificati Proxy

- Esistono delle varianti di certificati proxy per degli usi più specifici.

- **Restricted Proxy Certificate**:

  include una politica che limita gli usi del certificato

- **"Independent" Proxy Certificate**:

  non include diritti (i diritti devono essere delegati esplicitamente).

Obiettivi delle Autorizzazioni nelle Griglie

- Compatibile con le politiche di sicurezza esistenti nei siti.
- Compatibile con le politiche di sicurezza delle VO.
- Facile da capire e verificare.
- Facile da amministrare.
- Compatibile con i meccanismi di sicurezza dei siti.

Metodi di Autorizzazione nelle Grid

- Metodi di Autorizzazione "Classici" :
  - Mapping d'Identità
  - Autorizzazioni "Self" e "service"
  - Autorizzazione Diretta

- Altri Metodi di Autorizzazione :
  - Community Authorization Service
  - Akenti
  - PERMIS

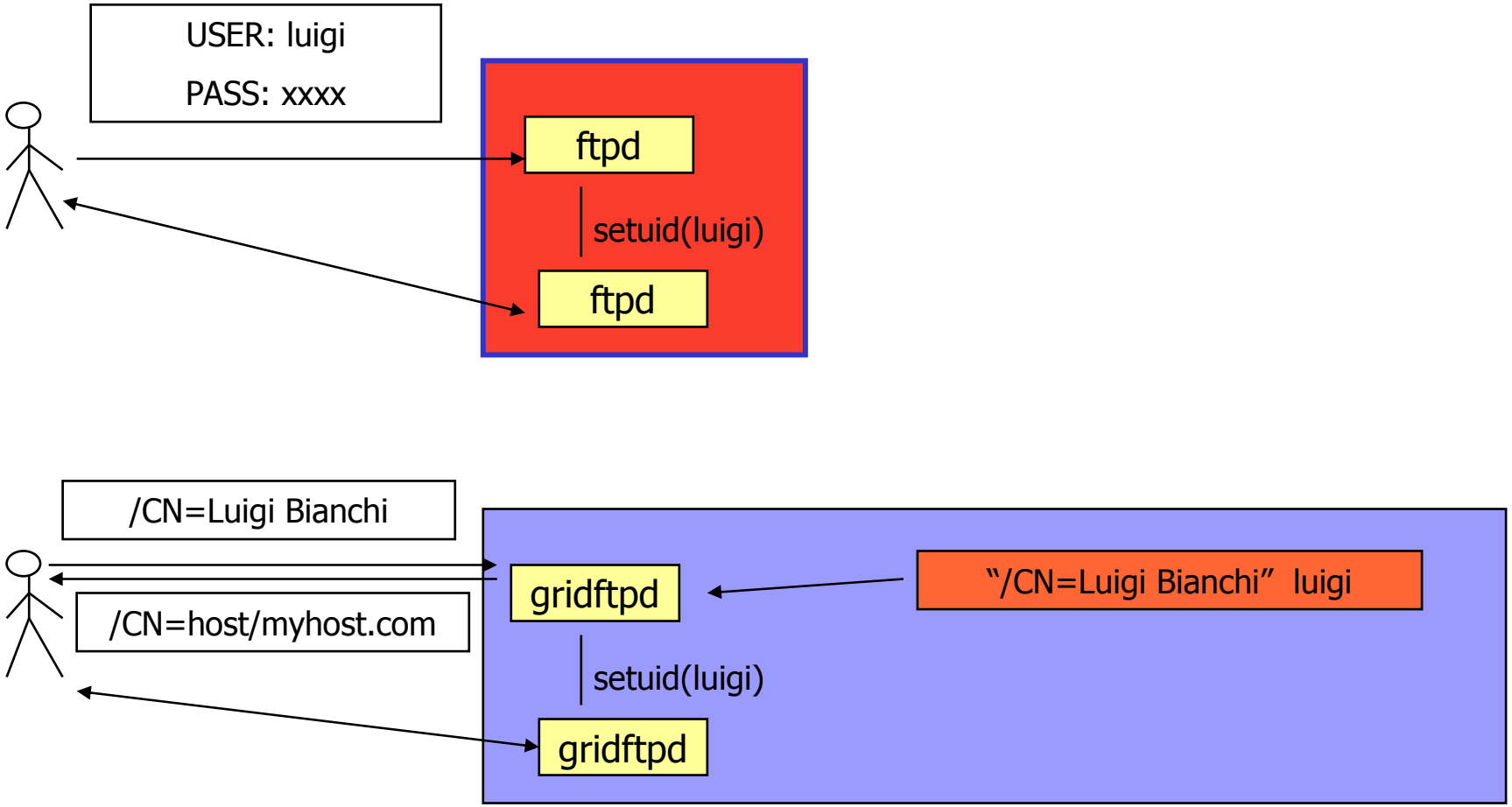
Autorizzazioni "Classiche" nelle Grid

- **Mapping d'Identità** : associa una "grid identity" (cioè, il Distinguished Name da un certificato utente X.509) ad una identità locale, che permette al sistema operativo di fare gli opportuni controlli.

- **"Self" authorization**: permette l'accesso se l'identità remota è uguale alla identità corrente.

- **"Service" authorization**: usa un algoritmo basato su *host name* e *service name* per determinare se l'identità remota è una di quelle accettabili.

Esempio di Autorizzazione : FTP e GridFTP



Caratteristiche del Mapping d'Identità

- Facile da capire e implementare per servizi che hanno un modello di autorizzazione esistente basato sull'identità locale.
- L'amministratore del sito mantiene il controllo locale.
- Richiede un accesso "root" nel sito per gestire gli utenti, e in qualche caso per garantire i permessi.
- I permessi che possono essere garantiti dipendono dalle implementazione dei siti.

Autorizzazione Diretta

- Usa un meccanismo di controllo degli accessi basato sui *subject name* di un servizio preesistente.
- Funziona per servizi che ne hanno già uno…

  … ma per questi è molto semplice.
- E' dipendente dall'implementazione:
  - L'insieme dei permessi che sono offerti dipendono dall'implementazione
  - Puo' richiedere l'intervento degli amministratori dei siti per garantire e revocare permessi.

Community Authorization Service (CAS)

- I siti eseguono il controllo degli accessi a "grana grossa" garantendo diritti di accesso a gruppi di risorse per le Virtual Organizations (VO)

- Le VO usano i CAS per eseguire il controllo degli accessi a "grana fine", garantendo diritti di accesso di singoli utenti a singole risorse.

- I server di risorse rafforzano sia la politica dei siti sia la politica delle VO.

Gestione delle Politiche CAS

- I siti mantengono le politiche locali usando metodi esistenti (es., gridmap files e unix account).
- Le politiche di comunità sono mantenute usando il CAS server e il protocollo CAS.
- I siti non devono gestire politiche per le gli utenti e i gruppi di comunità.

Community Authorization Service (CAS)

- Gli amministratori di VO usano l'interfaccia amministrativa di CAS per definite le politiche delle VO.
- Gli utenti contattano il CAS server per ottenere "asserzioni firmate" sulle operazioni possibili (basate della politica della VO)
- Gli utenti presentano le asserzioni firmate ai server di risorse durante l'autenticazione.

Signed Authorization Assertions

Subject: /O=Grid/CN=Luigi

Valid: 8/19/05 07:00 – 8/20/05 07:00

AuthorizationAssertion (non-critical extension):

Target Subject: /O=Grid/CN=Luigi

Valid: 8/19/05 12:00 –13:00

These actions are allowed:

Read gridftp://myhost/mydir/*

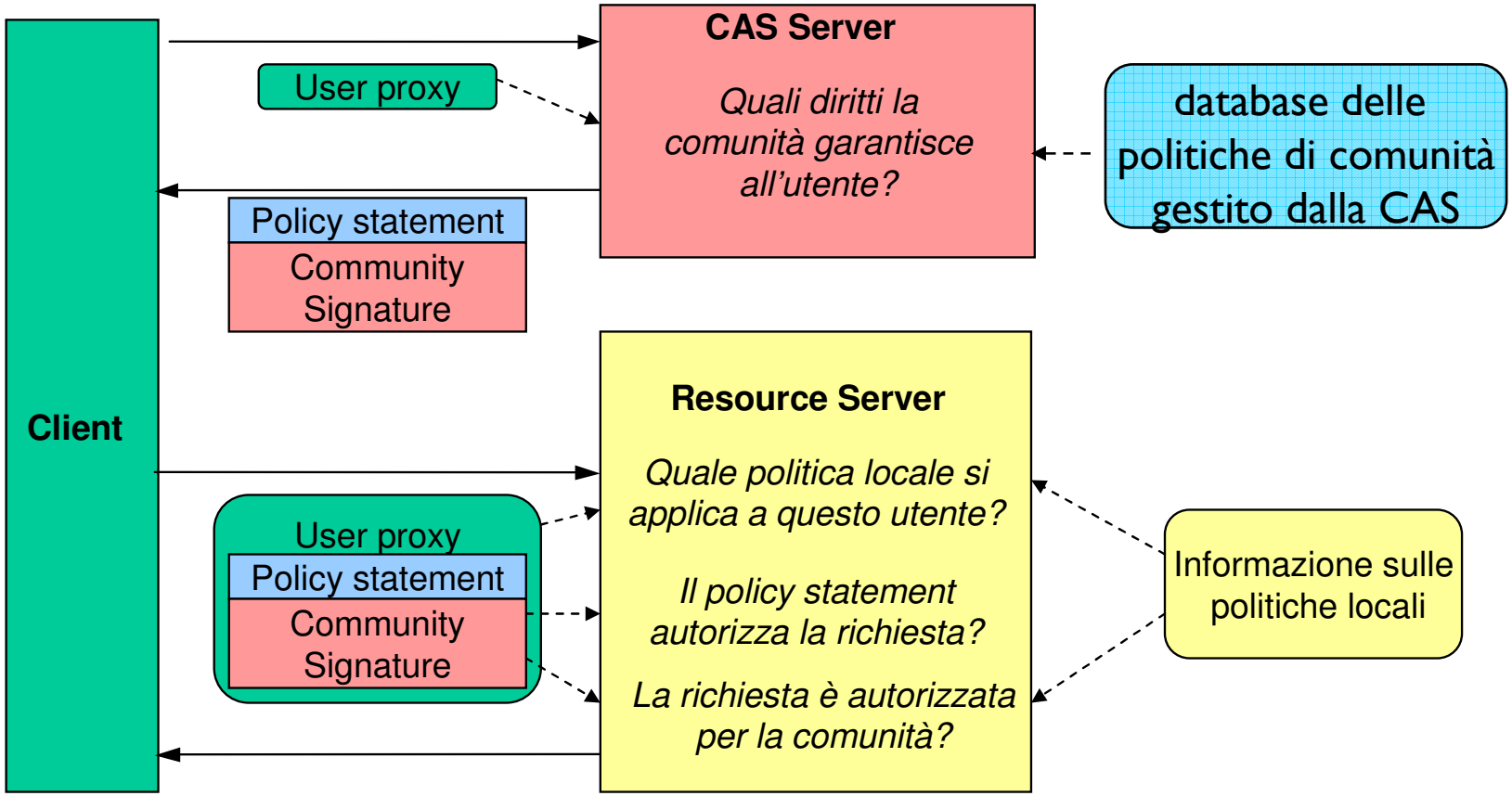
Signature (of assertion, by the VO CAS server)

Signature (di quanto detto sopra, utente)

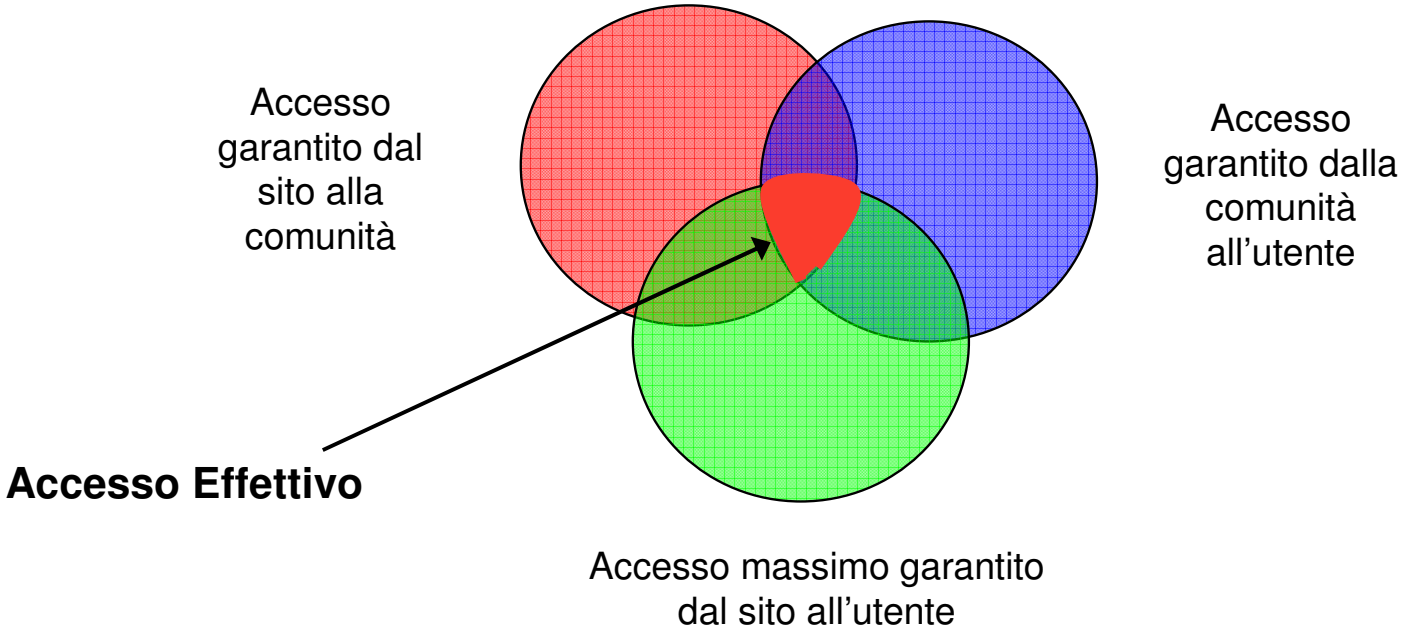
L'asserzione di autorizzazione è firmata dal CAS server della VO. Esso delega un sottoinsieme dei diritti della VO ad un utente per un dato tempo.

E' valida se usata con le credenziali di autenticazione dell'utente.

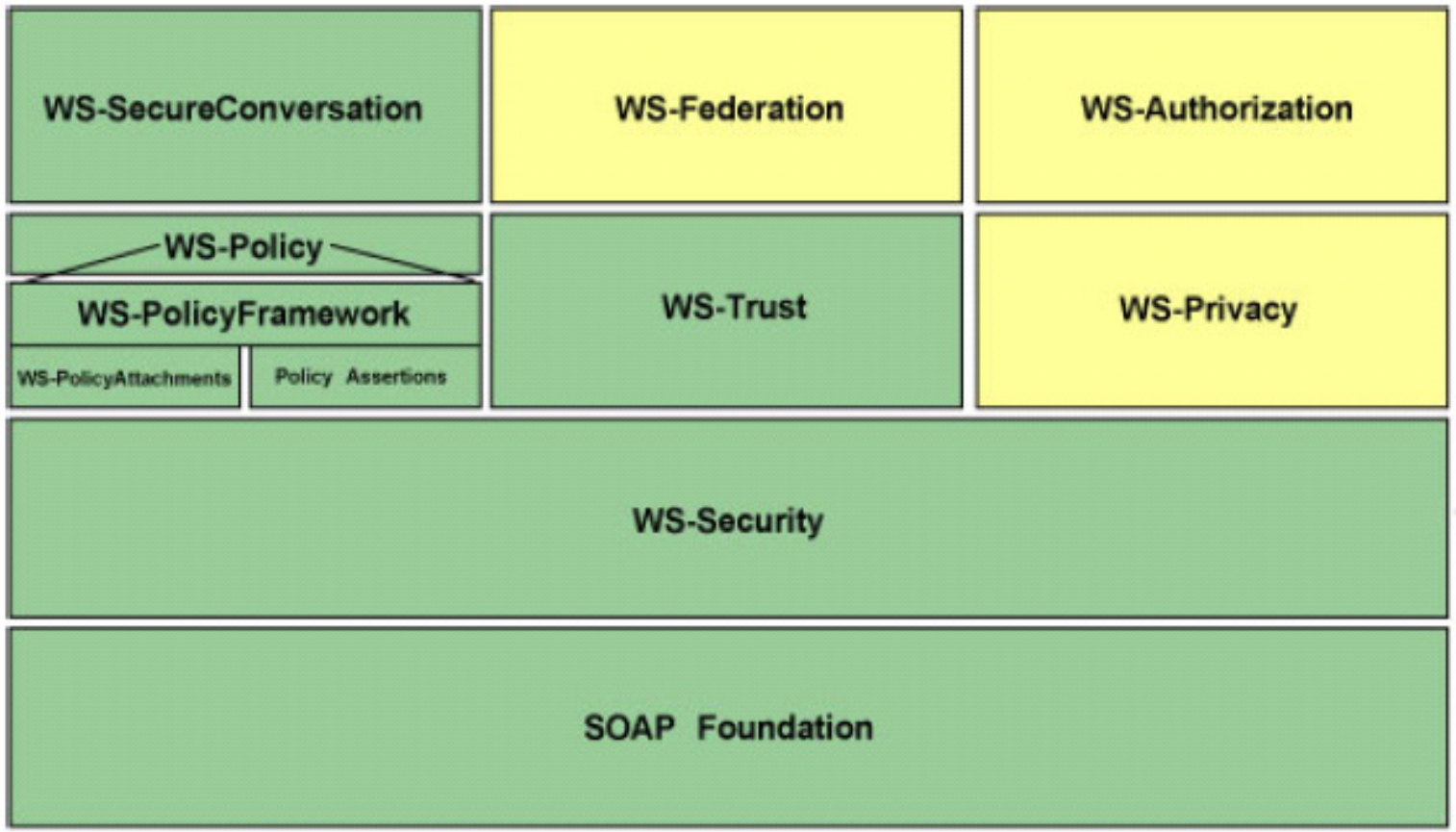
Una Richiesta CAS Tipica



Politiche Effettive CAS



WS-Security Stack



Ulteriori Informazioni

- Globus Security: http://www.globus.org/security

- Global Grid Forum security area: https://forge.gridforum.org/projects/sec