REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Due applicazioni pratiche: l'autenticazione tramite Smart Card e la firma digitale massiva

Gabriella Cattaneo

Security Technical Engineer

Sun Microsystems, Inc.

REGIONE DEL VENETO

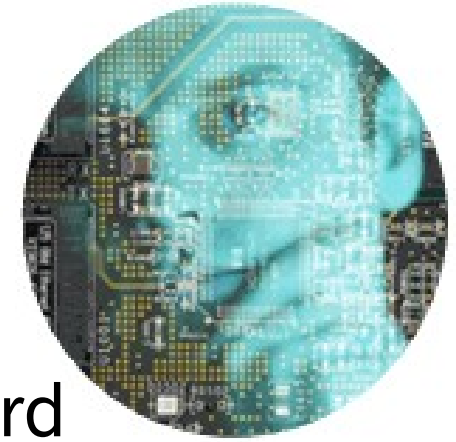
Direzione Sistema Informatico

Sun microsystems

Autenticazione in un ambiente di SSO tramite Smart Card

Autenticazione statica: password

- Veloce da realizzare, economica e attuata via software.
- Criticità:
  - Scelta e segretezza dalle password
  - Invio e conservazione della password
  - Creazione e aggiornamento della password



- Una coppia login password per ogni servizio

Autenticazione Robusta

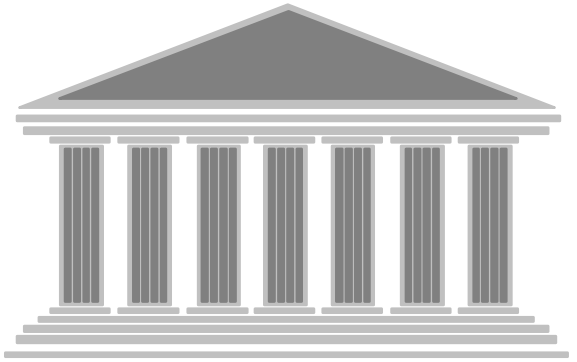
- Certificati digitale
  - Firma digitale di un identificativo di sessione sempre diverso
  - Non repudio
- Smart Card
  - Archiviazione chiavi
  - Firma in ambiente sicuro
  - Autenticazione tramite “qualcosa che uno ha”
  - Più certificati sulla stessa Smart Card

Generazione chiavi e certificati

- Generazione chiave su Smart Card
- Procedura di rilascio certificato
  - Registration Authority
  - Riconoscimento utenti
- Certificato per autenticazione
- Salvataggio certificato su Smart Card
- Gestione revoca e rinnovo certificati
  - Segnalazione rapida

Certification Authority

- Ente certificatore o Certification Authority interna
  - Costo
  - Gestione generazione, rinnovo e revoca
  - Requisiti di legge
- Diffusione liste di revoca (CRL)



Directory Server

- Archiviazione certificati utenti
- Gestisce autenticazione tramite certificati
- Archiviazione e consultazione CRL
- Infrastruttura conforme allo standard LDAP v3

Directory Server

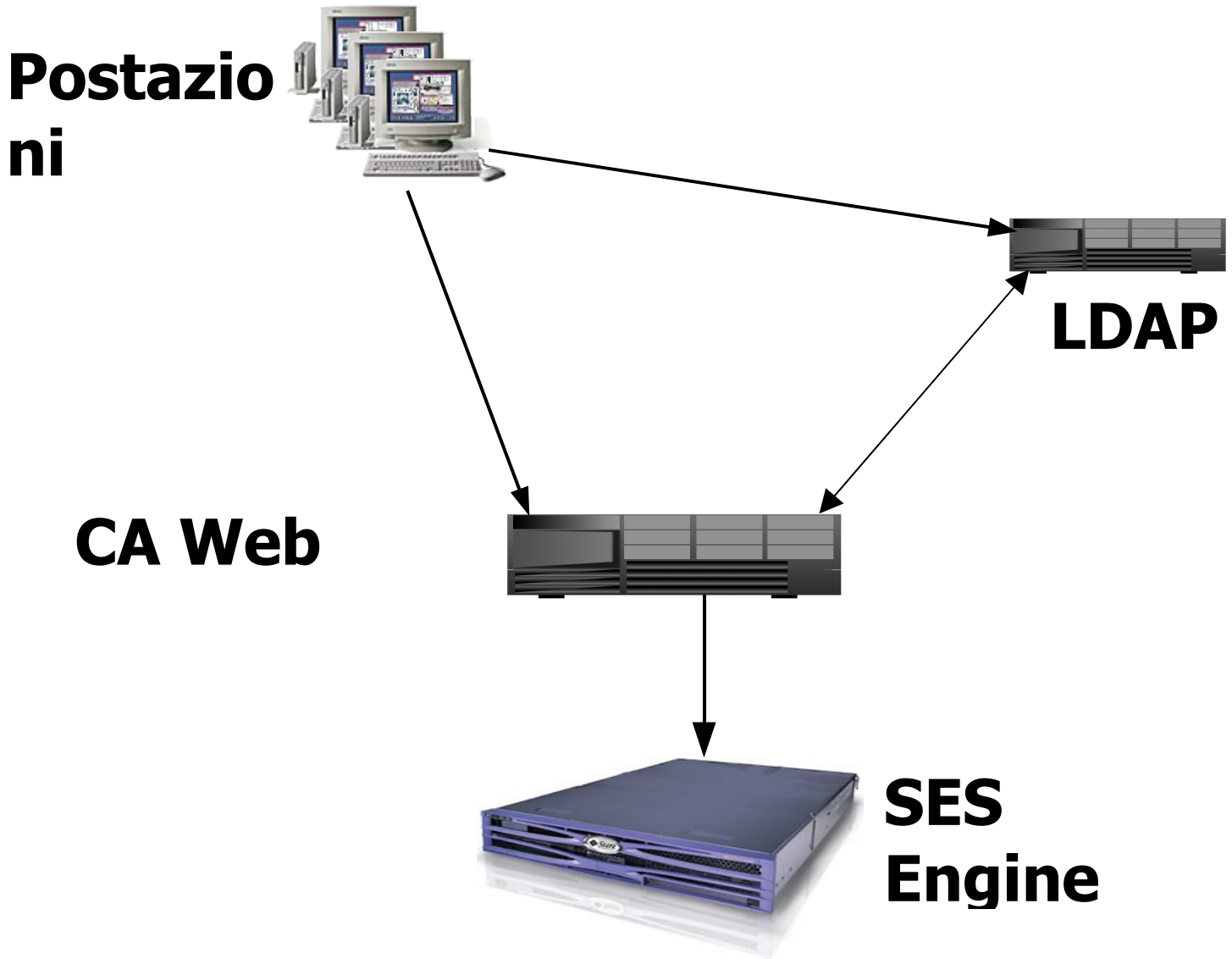
- Amministrazione da interfaccia grafica
  - ACI (Access Control Instructions)
  - Secure client e server authentication
  - Gruppi internei ed esterni
  - Attributi identificazione, autenticazione e autorizzazione
  - Informazioni di audit
- Elevata scalabilità e performance

Postazione utente

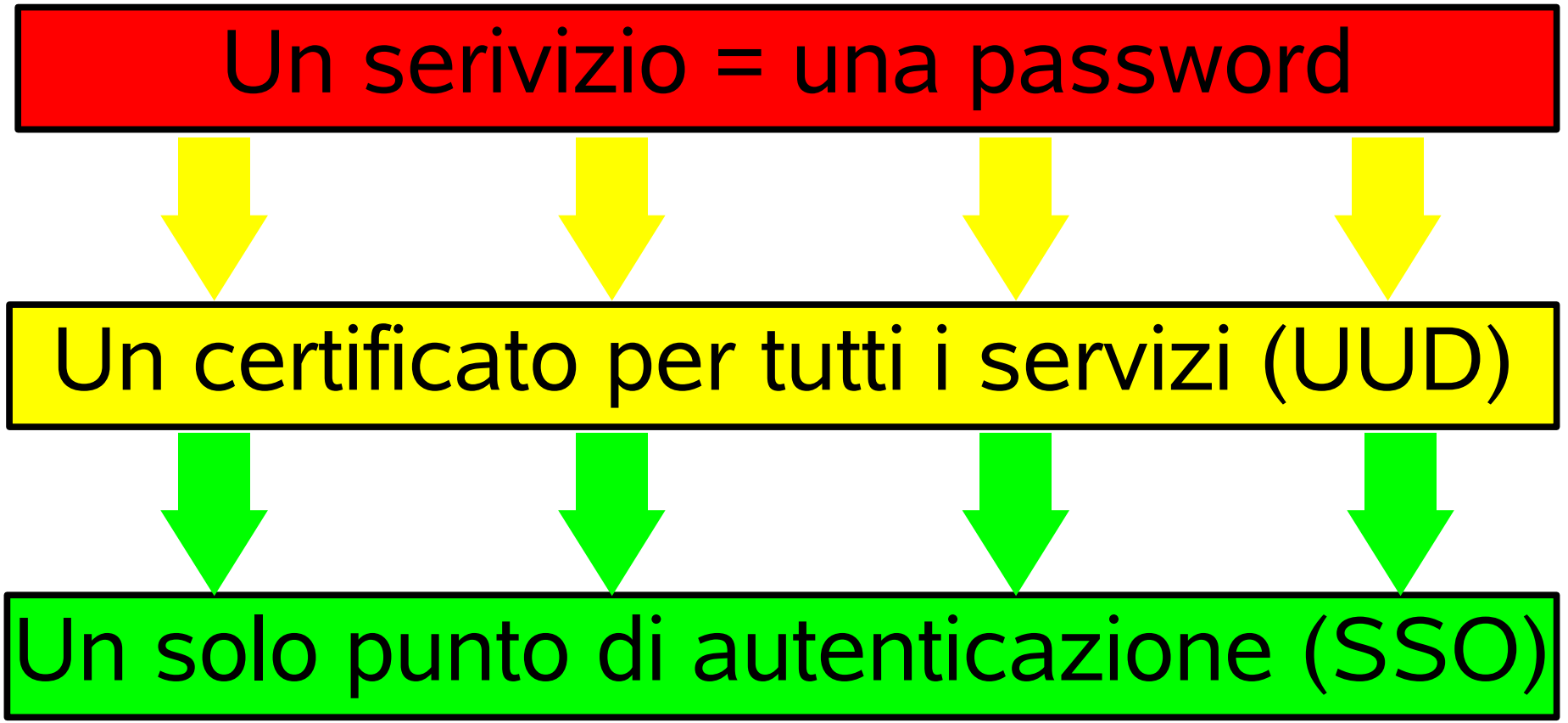
- Smart Card Reader
- Gina (Driver per Certificati di tipo autenticazione)
- Autenticazione con e senza Smart Card

- Browser web (con certificato)
  - Sicurezza certificato demandata al sistema

Disegno architetturale soluzione



Single Sigh On



Gli elementi della soluzione

Directory Server

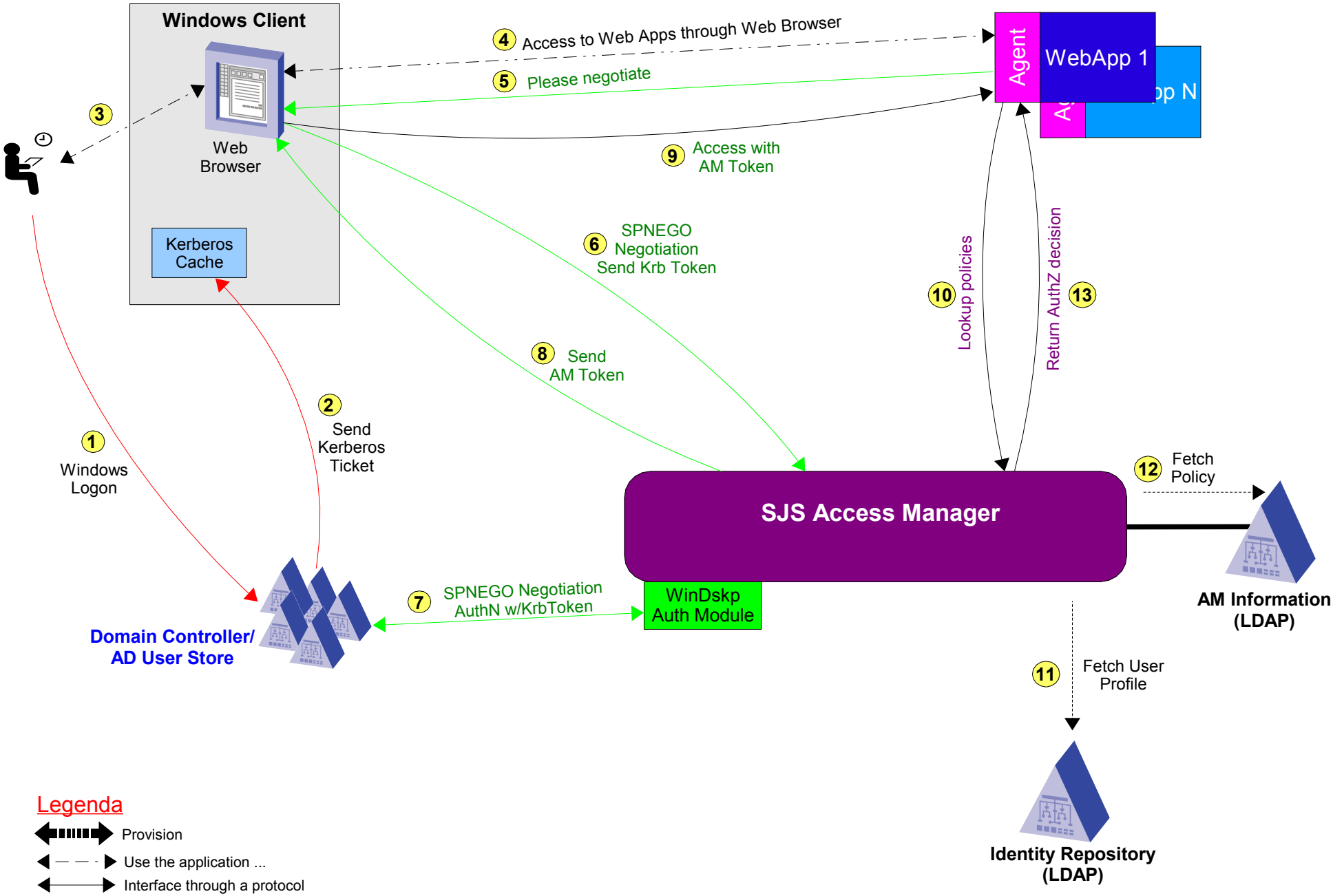
Identity Manager

Access Manager

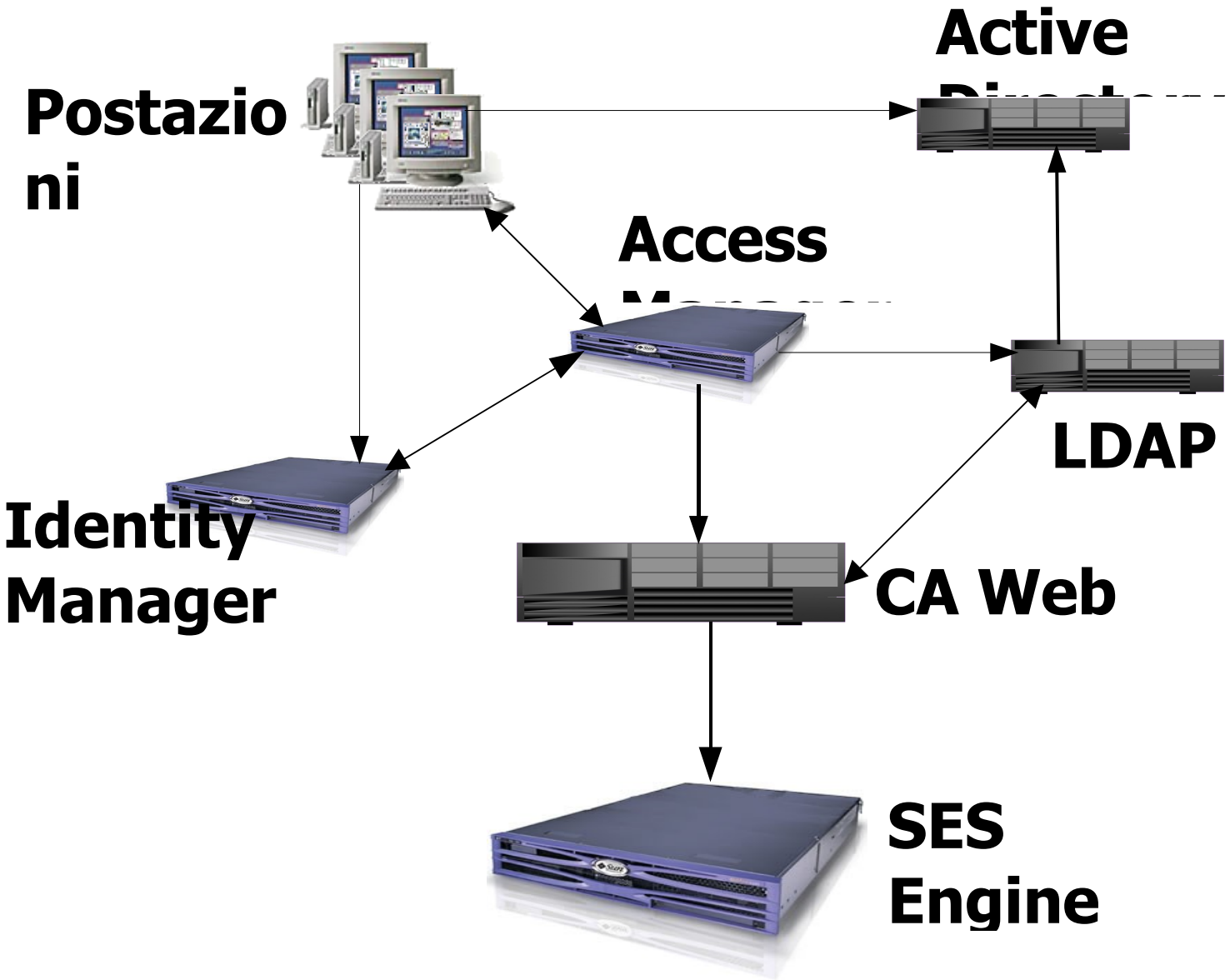
Gli elementi della soluzione

REGIONE DEL VENETO

Direzione Sistema Informatico



Disegno architetturale soluzione



Benefici della soluzione

- Abbattimento dei costi di gestione
  - Automatizzazione dei processi e flussi informativi
  - Autorizzazioni multi-punto
  - Aumento produttività degli utenti
- Aumento della sicurezza
  - Sistema centralizzato per l'autenticazione
  - Sistema centralizzato per l'autorizzazione
  - Tecnice avanzate autenticazione
  - Sistema misto di autenticazione

Benefici della soluzione

- Bassa intrusivitá
  - Non richiede l'installazione di componenti dedicate (agenti)
- Semplificazione della gestione delle identitá
  - Assenza di repositori intermedi con attributi utenze
  - Un solo punto di gestione delle utenze
- Sincronizzazione bidirezionale delle identità (funzioni di meta-directory)

Benefici della soluzione

- Elevata scalabilitá dei servizi di directory ed access management
- Capacitá di federazione delle identitá
  - Standard Liberty Alliance e SAML
  - Allineamento di Active Directory
- Massima integrazione fra i prodotti della suite

REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

La firma massiva di documenti in formato digitale

Conservazione dei documenti

- Documento in formato originale
  - Firma di autenticazione
  - Conservazione
- Informatizzazione della PA
  - Archiviazione in formato elettronico
  - Firma digitale

Documento con firma digitale

"Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto"
DLGS 23 gennaio 2002

Documento con firma digitale forte

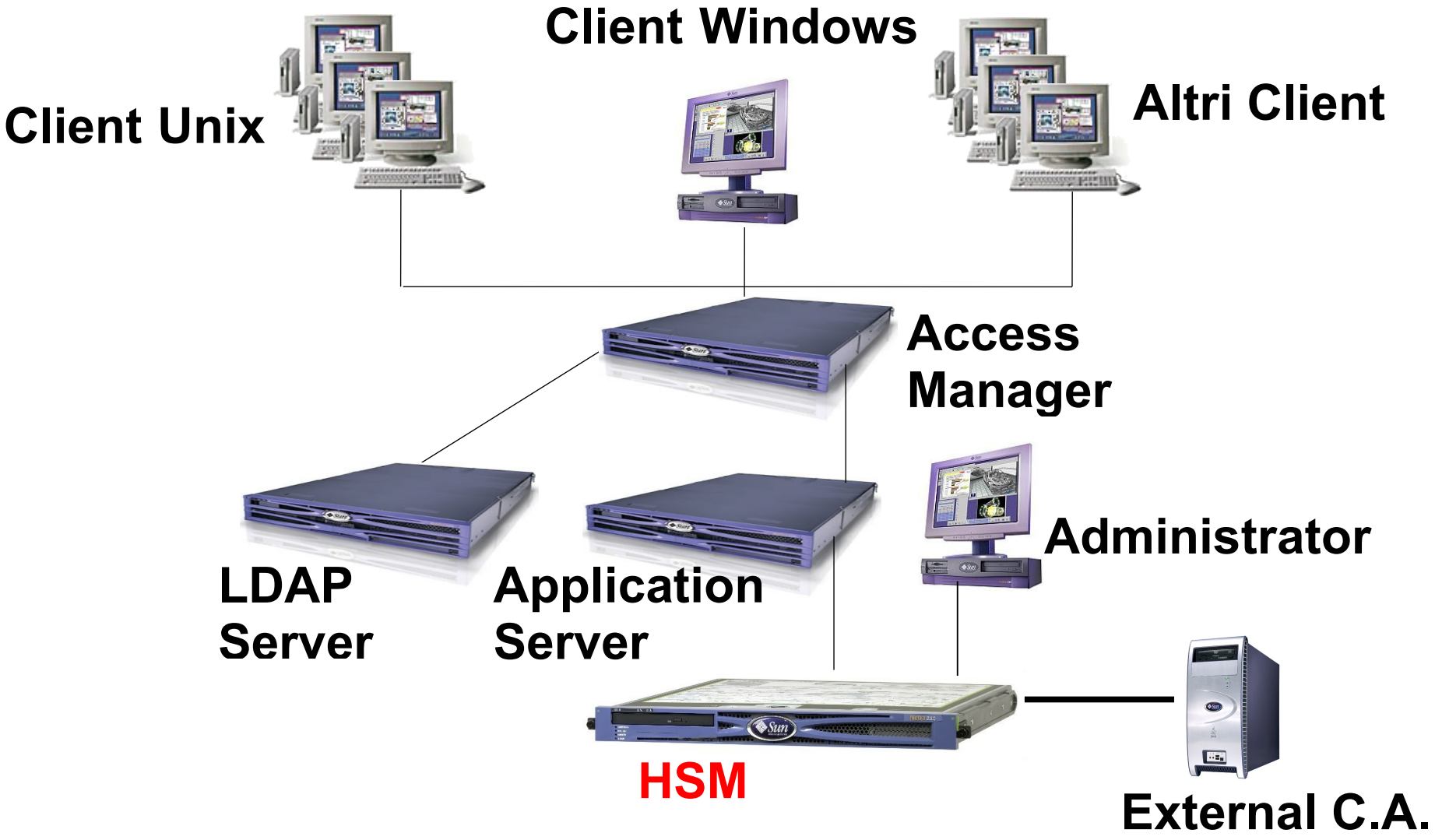
- Una firma è digitale forte se
  - è una firma elettronica avanzata
  - è basata su un certificato qualificato
  - è generata per mezzo di un dispositivo sicuro per la generazione delle firme

- A una firma digitale forte viene data la medesima validità giuridica di una firma autografa autenticata da un pubblico ufficiale.

Firma digitale massiva

- Componente dedicata alla firma
  - Hardware Security Modules (HSM)
  - Smart Card
- Coppia di chiavi crittografiche
  - Formato firma massiva
  - Ente Certificatore riconosciuto dal CNIPA
  - La chiave segreta non deve lasciare il modulo
- Autenticazione dei firmatari (PIN o Smart Card)

Esempio di Architettura



Benefici della soluzione

- Rapidità di diffusione
  - Costi inferiori di distribuzione dei documenti
- Archiviazione e ricerca più rapidata
- Integrità dei dati
  - Firma dipende dal contenuto
- Ottimizzazione del processi di firma
- Mobilità e Ubiquità

Benefici della soluzione

- Gestione centralizzata del processo di firma
- Chiavi di Firma non possono essere distribuite ma è possibile un loro export verso un altro HSM spento
- Il documento da firmare cifrare rimane sul server
- Facilità di inserimento in un'architettura esistente
  - Dati, servizi, firma e cifratura centralizzati
- Facilità di upgrades a nuove tecnologie

Benefici della soluzione

- La creazione delle chiave è gestita centralmente e non è richiesto un import di certificato da parte dell'utente (facilità d'uso)
- Nessuna possibilità di perdere la smart card contenente la chiave crittografica
- Nessun bisogno di dover gestire varie Smart Card
- Nessun costo aggiuntivo per ogni nuovo utente

REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Grazie

Gabriella Cattaneo

Security Technical Engineer

Sun Microsystems, Inc.