

The Avaya logo is displayed in white, bold, sans-serif capital letters on a red rectangular background. The letters are slightly shadowed, giving a 3D effect. The logo is positioned on the left side of a horizontal banner that also includes a black section with a white bar on the right.

AVAYA

Identity and Access Management

October 26, 2004

At a Glance

- **#2 in worldwide Enterprise telephony**
- **#1 in worldwide IP telephony**
- **#1 in worldwide Voice Messaging, Unified Communication and Unified Messaging**
- **#1 in Call Centers in NA, LA, APAX and EMEA**
- **#1 in US in PBX maintenance services**

- **17,000 Employees**

IAM Components

- **Identity Management** – process for managing the entire lifecycle of digital identities and profiles for people, systems, and services. It typically includes:
 - Automated provisioning of new users
 - User self-service functions (e.g., password reset, password sync)
 - Workflow processes for approving account creation, modification, and assignment to specific roles
 - Removing users when they no longer require access
- **Access Management** – process for regulating access to information assets by providing a policy-based control of:
 - Who (by role) should access specific systems
 - What that role is permitted to do
 - What permission or restrictions are on that role
- **Authentication** - The event whereby a user of a system or application adequately proves his/her identity to a system. Requesting and validating a userid and password is the most common method of performing authentication in typical IT systems.
- **Authorization** - The event whereby an authenticated user of a system is granted the ability to perform a certain operation, such as viewing or changing data, or running a certain process. Users must be authenticated before they can be authorized to do any activities.

IAM Additional Vocabulary

- **Role** - A specific job function in an organization. In the context of role-based access control, users in a specific role are granted the same access to the same systems. These roles may or may not map directly into job titles.
- **Role-based Access Control** - An access control system that bases the access and authorization permissions of a particular user on the roles they are assigned.
 - For example, if a user has the Accounts Payable Clerk role, they would be granted access to the financial systems. In addition, they would be authorized to view accounts payable records, authorize payments, etc
- **Web Access Control** -The process and/or technology used to establish authentication and authorization checkpoints for web-enabled applications

Defining the issue

- **Registration/Enrollment to current applications and systems is inconsistent.**
- **An employee may be required to register/enroll multiple times to different systems and applications to perform their job functions.**
- **Users are required to interact with different administrative teams and fill out multiple questionnaires to gain access**
- **Data is often manually entered into the required system or application.**

Business Drivers

- **Sarbanes Oxley**
 - **Enable appropriate access to information assets across enterprise**
 - **Ensure protection of enterprise information assets**
 - **Adequate and appropriate access controls for applications and systems**
- **Increase productivity and shorten administrative processing time**
- **Provide external users (business partners, customers) appropriate access to internal systems and applications**
- **Reduce administrative resources/costs**
- **Reduce ID and password complexity for users**

Value for ACSP

- **Regulatory Compliance**
 - Improving Legal/Regulatory Compliance
 - Reducing potential fines
 - Reducing risk of litigation
 - Lowering risks associated with audit findings
- **Strengthen security**
 - Maintain acceptable level of security risk.
 - Reduce risk of significant financial loss and disruption to business.
 - Protect brand image and business reputation.
 - Operationalize the enforcement of corporate security policies and procedures
 - Reducing number of inactive users with active accounts
 - Ensuring appropriate access is efficiently given to information assets

Value for ACSP

- **Improves Frustrating User-Experience (BP's, Customers, Associates)**
 - **Multiple Accounts and Passwords**
 - **Delays in obtained required access for performing their job**
- **Return on Investment (ROI)**
 - **Improved end-user productivity**
 - **Improved efficiency of user Administration.**
 - **Streamlining administration and support functions**
 - **Reduced user administrations costs.**
 - **Reducing incompatibilities**
 - **Optimize investment in strategic partner's technologies**

Avaya Common Security Platform: Vision

- **Enterprise Role Definition (ERD)**
 - Institutionalized separation of duties through appropriate controls and processes
 - Defines appropriate user access and derives User ID authorization/permissions by role
 - Roles are pre-assigned role based on job function—i.e. what is required to do their job
 - Changes to these permissions are coordinated with employee re-assignment or transfer
 - Additional access authorizations handled manually via new Central Administration Group
 - Permissions are removed at time of termination

Avaya Common Security Platform: Vision

- **Single Sign-On (SSO)**
 - **Secure gateway to user profiles for employees, customers and business partners**
 - **Authentication through one unique user ID and password for all SSO-based applications**
 - **Password security policy enforced centrally for SSO-based applications**

Avaya Common Security Platform: Vision

- **Identity Management (IM)**
 - Infrastructure that integrates both ERD and SSO to create and maintain user identities
 - Centralized ID provisioning, decommissioning and ERD assignment across all systems
 - Automated administration of user identity, ERD profiles, and additional authorizations
 - One-stop shopping for user provisioning across all Avaya applications

Avaya Common Security Platform: Vision

- **Short-term compliance with Sarbanes-Oxley and SEC Quiet Period regulations**
 - **Application and process modifications to internal controls as identified by Finance (SOX apps)**
 - **SAP access and authorization controls to eliminate manual lockout process for book close**

Avaya Common Security Platform: Elements

- **Enterprise Role Definition (ERD)**
 - **Defines user roles required for a specific job function**
 - **Assigns user profiles for each application based on job title**
 - **Changes in job function are easily reflected by changing the assigned role**
 - **Employee separation results in removal of permissions and role**
 - **Institutionalizes segregation of duties required for a controlled process**
 - **Manual assignment of additional permissions through central administration group with associated approval processes**

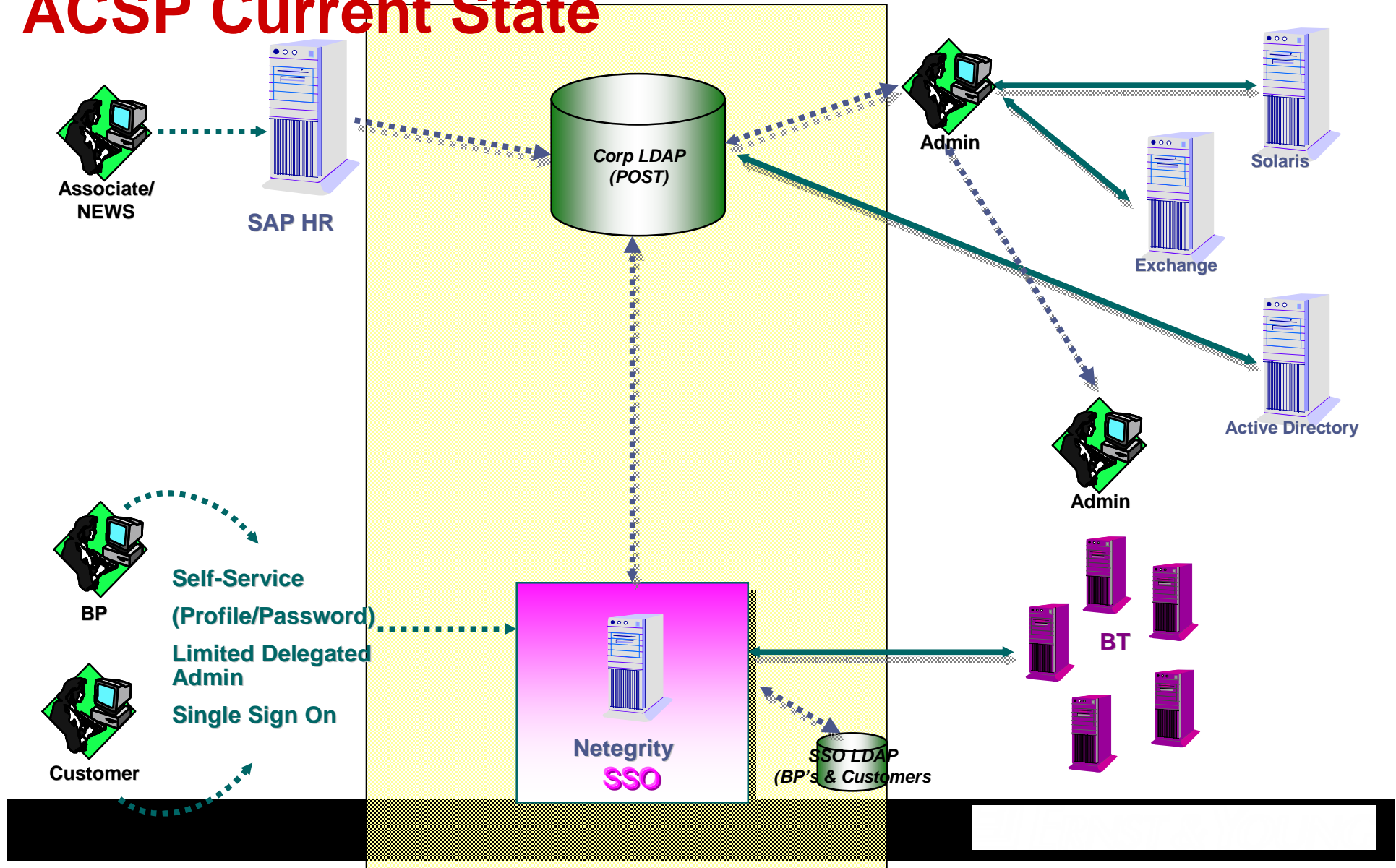
Avaya Common Security Platform: Elements

- **Single Sign-On**
 - Provides a secure gateway for application access
 - Enables a user to authenticate once for all SSO applications
 - Uses one log-in and password across all applications
 - Enforces password security policy
 - Authenticates internal users against Active Directory Server
 - Authenticates external users against the external user store (LDAP)
 - Provides authentication only; does not assign permissions
 - Provides automated enrollment to applications with a defined approval workflow

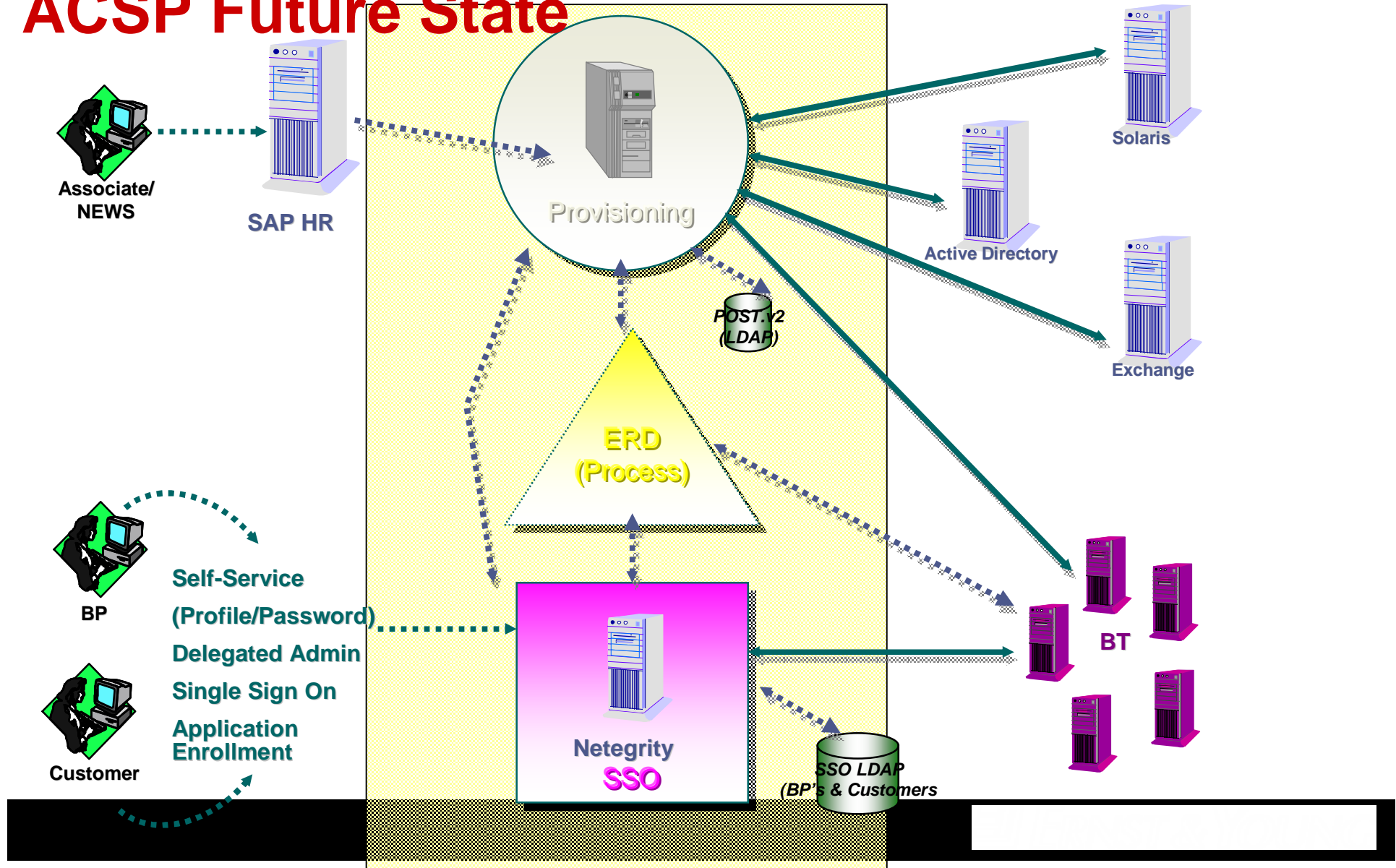
Avaya Common Security Platform: Elements

- **Identity Management**
 - Automates the User ID provisioning function
 - Provides one stop shopping for user provisioning, reducing time to gain access to business applications and resources
 - Automates the assignment of roles based on the job function
 - Changes in job function automatically result in changes in user roles
 - Defines a corporate-wide directory of record
 - Centralizes repository of application authorizations which enables centralized security administration
 - Reduces risk of unauthorized access and provides audit trails of user permission assignments

ACSP Current State



ACSP Future State



Avaya and Ernst & Young

- Engaged in October 2003 to upgrade SSO
 - Completed upgrade and integrated 9 applications July 2004
 - Added 3 international Portals July 2004
 - Implemented Business Transformation project (Siebel) in August 2004
 - Added 3 additional portals in late August 2004
- Engaged for overall IAM strategy
- Phase II – Provisioning/ERD implementation

E&Y Implementation Methodology- IAM

