Title: (ilab_blk.eps)
Creator: Adobe Illustrator(R) 8.0
Preview: This EPS picture was not saved with a

AAA and PKI
(Authentication, Authorization, and Accounting)

Other PKI iLabs areas show authentication of users via X.509 certificates. However, authentication is just one of the three A's of *authentication*, *authorization*, and *accounting* which state by definition it is not sufficient just to know who you are; rather it is often equally important to know what you are allowed to do while keeping a record of everything that you do. Unfortunately, PKI does not provide this type of authorization and accounting for a population of users. Instead, PKI must be extended with a policy-based AAA server to ensure comprehensive access control.

Policy-based AAA servers offer applications, typically web-based, the ability to centralize authentication, authorization and accounting functions. Network administrators can define users, authentication methods (passwords, tokens, digital certificates, etc.) and access controls from a single point. By leveraging AAA services, applications no longer need to handle access control, but rather can hand off that function to dedicated servers.

In this demonstration Secure Computing's SafeWord Plus access control solution will interoperate with products from multiple vendors: Microsoft IIS, iPlanet Enterprise Server and Apache web servers, an LDAP server from iPlanet, digital certificates issued by Secure Computing, Baltimore, and iPlanet, hardware tokens (smartcards) provided by Rainbow, Sony, Litronic, and Datakey, and web browsers from Microsoft and iPlanet (Netscape) all running in a mixed environment (Windows 2000, Linux and Solaris). SafeWord Plus combines the strengths of both public-key infrastructure and AAA by leveraging digital certificates with role-based access control. SafeWord Plus is able to do this by integrating users, authenticators, policy, and audit logs in a central LDAP directory. Hence, AAA services and PKI are seamlessly tied together.

This demonstration will show how to integrate role-based access control with digital certificates and web-based user self-enrollment in a simple web-based application, Rocket Science. The Rocket Science application has been designed as a mock corporate extranet. Like a real enterprise extranet, Rocket Science includes sections for different types of users (e.g. sales people, managers, business partners, etc.) Naturally, not every web page or application is suitable for every user. Using SafeWord Plus and the SafeWord Web Access Agents, users can be granted access to web resources based on their actual role in the enterprise.

Unique roles are assigned to the following types of users within the SafeWord Plus database: business partners, sales managers, sales staff, and regular employees. Business partners are granted the 'Partner' role, Sales Managers are granted the 'Manager' and 'Sales' roles, and so forth. Role-based access control gives the right people the access to sensitive applications while allowing for significant personalization and customization. The SafeWord Web Access agent for IIS maps specific web resources in the Rocket Science enterprise to their respective roles.

Web-based user self-enrollment allows users to enroll themselves freeing administrators from the burden of manually populating the user database. Administrators can create reservations for a specific group of users. Then users can add themselves to the user database, be assigned roles, activate an authenticator, download an application, and more. Rocket Science has been designed with user self-enrollment in mind.

Q. What is an authenticator?

A. An authenticator can be a fixed password, a hardware token that generates a one-time password, or a digital certificate. For the sake of this demonstration, we will focus on users who are assigned digital certificates. SafeWord Plus can support all these types of authenticators either alone or in combination.

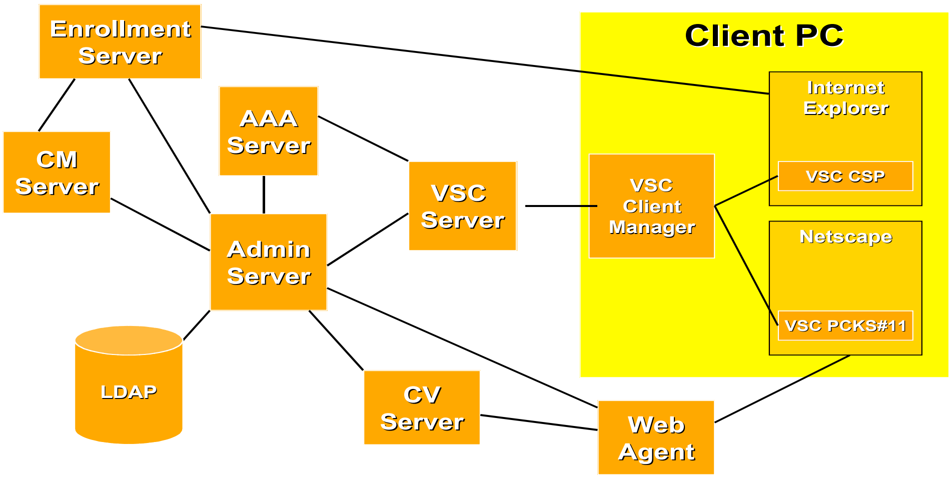
Q. Are there any limitations on what type of digital certificates that SafeWord Plus can assign to users?

A. SafeWord Plus supports generic X.509 certificates and can interoperate with a variety of third-party certificate authorities including Baltimore, iPlanet, Verisign, Entrust, and Microsoft. SafeWord Plus also includes its own certificate authority that ties seamlessly into a web-based user enrollment interface. Third-party certificates can be added into SafeWord Plus by importing the 'trusted root certificate' into the Administration Console.

Q. Where are the users' digital certificates stored?

A. User certificates for authentication can be stored in a variety of locations including locally within a web browser, inside a hardware token (smartcard, USB device, etc.), or on a virtual smartcard server that resides on the SafeWord Plus server. A virtual smartcard is a piece of software that resides locally on client computers. The software mimics the behavior of a physical smartcard and reader.

SafeWord Plus Architecture


Enrollment Server
CM Server
AAA Server
Admin Server
LDAP
VSC Server
CV Server
Web Agent
Client PC
Internet Explorer
VSC CSP
VSC Client Manager
Netscape
VSC PCKS#11