

RSA Keon® Web PassPort

Technical Overview

This white paper describes the RSA Keon® Web PassPort architecture. A description of the major subsystems and services provided by the product is given. In addition a high level operational description of the interactions between the desktop and server is discussed.

Table of Contents

| | |
|---|----------|
| I. Introduction | 1 |
| Core Functionality | 1 |
| II. System Concepts | 3 |
| Virtual Card | 3 |
| Web Cookies | 3 |
| III. General Description | 4 |
| RSA Keon Web PassPort Server | 4 |
| Authentication Broker | 4 |
| Credential Server | 5 |
| Software Download Service | 5 |
| Auto Registration | 6 |
| Enrollment | 6 |
| Approval | 6 |
| Pickup | 7 |
| Resource Management Service | 7 |
| RSA Keon Web PassPort Server Configuration | 7 |
| Protected URL Policies | 7 |
| URL Filter | 7 |
| Virtual Card Manager | 8 |
| RSA Keon Web PassPort Plug-in | 8 |
| IV. Operational Model | 9 |
| Session Termination | 9 |

I. Introduction

This white paper provides a high level description of the RSA Keon Web PassPort architecture. It focuses on the two main components of the architecture, namely the RSA Keon Web PassPort Server and the RSA Keon Web PassPort Plug-in. The Web PassPort Plug-in installs with minimal user interaction, much like a browser plug-in.

The Web PassPort Server resides in the customer's Web server and is used to administer authentication policy to Web resources and determine if the user is required to have PKI credentials when accessing these resources. Web PassPort automates the downloading of the Web PassPort Plug-in that is required to access the PKI credentials and allows the organization controlling the Web server to administer the policy on how these credentials are protected. Finally, Web PassPort can automate the process of issuing Public Key Certificates to end-users.

Web PassPort is targeted primarily at enterprises that require PKI credentials in conjunction with a Web application for purposes such as digital signing, VPN access and secure e-mail. Web PassPort is designed around an LDAP directory model. Users are defined as entries in an LDAP directory; Web PassPort extends the schema to add attributes to the standard user object to store private data.

Core Functionality

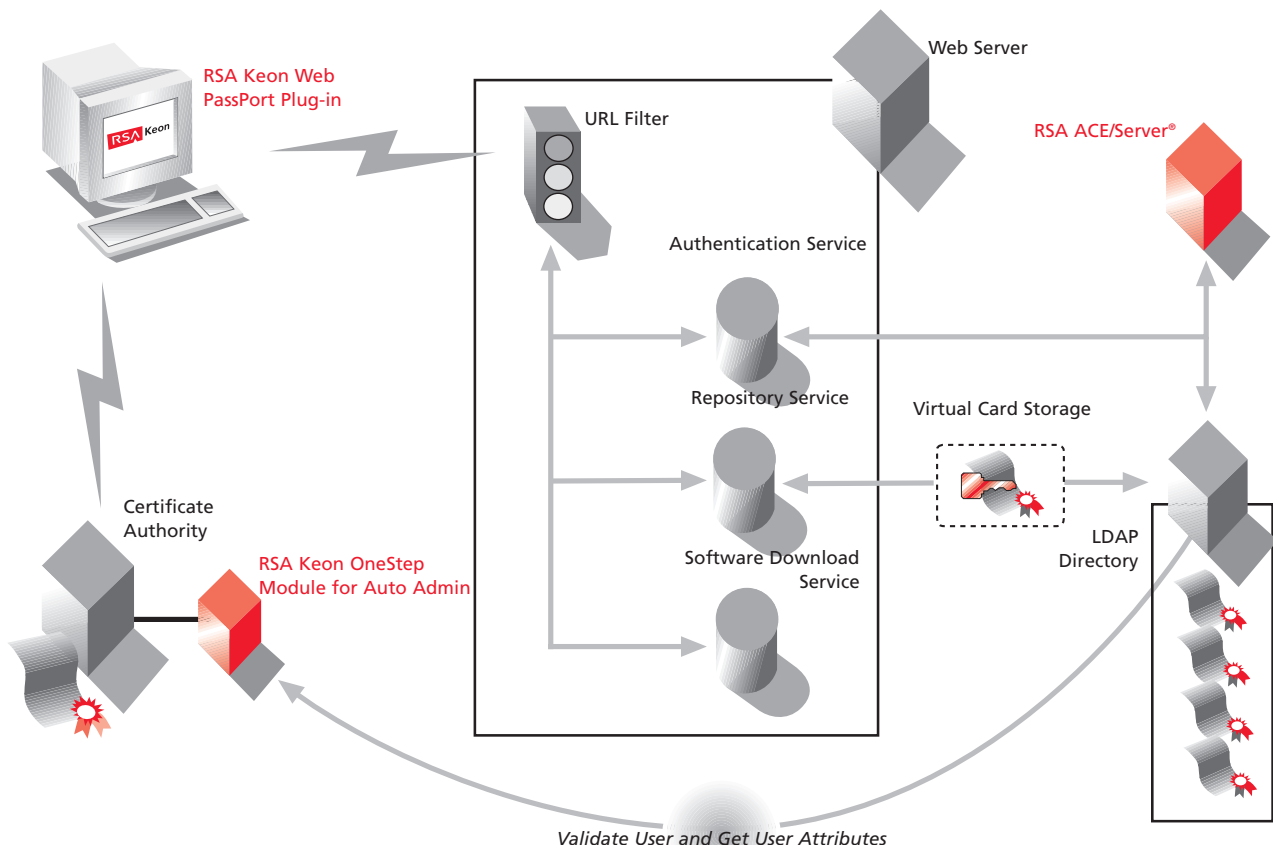
Web PassPort is a software suite that enables the use of public key infrastructure (PKI) credentials to protect Web site resources and to distribute these credentials to end users over the Internet for use in PKI-enabled applications. The product performs the following services:

Allows Issuer of PKI Credentials to Administer Security Policy on Key Protection

Today, when using PKI credentials with a Web browser, PKI credentials must be embedded within the browser key store; the issuer has no control over the policy used to protect access to the credentials. Web PassPort allows the issuer to set a security policy on the keys and thus establish a higher level of assurance that the keys have not been compromised.

Downloads RSA Keon Virtual Cards to Users

When the user authenticates successfully, the Web PassPort Server retrieves the user's virtual card from the LDAP directory and downloads it to the Web PassPort Plug-in on the user's computer. The virtual card is a secure container with the user's X.509 certificates and corresponding keys (see Section II, System Concepts, for more detail). Since different types of authentication (password, RSA SecurID® authenticators, etc.)



may be supported in the security realm, only those virtual cards protected by the type of authentication that was used can be downloaded. Once downloaded, the user's PKI credentials can be accessed through standard APIs such as Microsoft CAPI and PKCS #11. The PKI credentials are transient (that is, they are not kept in permanent storage on the desktop).

Provides Client Software to End-Users

To use the credentials in the virtual card (for example, to digitally sign data in a Web form or read secure e-mail), the user must have the Web PassPort Plug-in software. If the user does not have the Plug-in software, the Web PassPort Server automatically downloads it to the user's computer where it automatically installs.

The Web PassPort Plug-in is a small program that runs as a background process, using very little memory or hard disk space. When the Plug-in is enabled, the user sees a small red and white RSA Security icon in his or her Windows System Tray.

Simultaneous Access to Multiple Sets of PKI Credentials

Users may acquire multiple sets of PKI credentials from different companies, or even within the same company. This is particularly true in the B2B and B2C spaces; even within a single enterprise, separate operating divisions may issue certificates from their own CAs specifically for accessing the applications in that division. Thus, a user might need simultaneous access to PKI credentials issued by different CAs. The Web PassPort Plug-in can accept and store multiple sets of PKI credentials.

Enrolls First-time Users for Personal Certificates

One of the biggest problems with PKI deployment is steering the end-user through the certificate registration process. Generally the user is required to fill out a registration form that results in a certificate request being generated, some time later, the user is notified that the certificate has been issued (generally by e-mail) and must pick up and install the certificate in the browser. This process is not intuitive and generally results in the keys being bound to the particular machine where the certificate request was initiated.

Web PassPort has a certificate auto-registration service, which includes the auto-enrollment of user certificate requests, auto-approval of those requests, and a mechanism for the automatic pickup of the generated Personal certificates. The resulting keys are stored in a virtual card and can be downloaded automatically to the desktop when the user authenticates.

Protects Web Site URLs

The Web PassPort Server blocks access to URLs that you specify. Only authenticated users are permitted to access protected URLs. You can protect an entire Web site (the document root directory), specific directories on a Web site, or specific files on a Web site.

Authenticates RSA Keon Web PassPort Users

When a user attempts to access a protected resource, the user is prompted to authenticate. The user authenticates either with a password or two-factor RSA SecurID authenticator, depending on the authentication method that you have set on the URL.

Issues Cookies to Maintain a Persistent Authentication State for Users

When the user authenticates successfully, the Web PassPort Server stores cookies in the user's Web browser. The cookies act as tickets so users are not prompted to re-authenticate when they try to access additional protected resources. The period of time that the cookies remain valid (from one minute up to 24 hours) can be configured on the Web PassPort Server. The cookies are cryptographically protected and are not written to the file system (see Section II. — *System Concepts* — for more detail).

If your systems are configured for realm authentication, the user receives a cookie from every participating domain in the realm, allowing the user to access protected resources on any Web PassPort Server in the realm without being prompted to re-authenticate.

Creates and Maintains RSA Keon Virtual Cards in an LDAP Repository

Using the Web PassPort virtual card manager utility, you create virtual cards for users and store them in an LDAP directory. If the user modifies the virtual card (for example, by replacing a General certificate with a Personal certificate), the Web PassPort Server uploads a copy of the modified virtual card to the LDAP directory to replace the outdated virtual card.

Logs System Events and Traces Code Activity

Web PassPort Server records authentication and system events in the Windows NT Event Viewer or in a text file that allows for an audit log which be used to record or review activity.

Provides Mobility to Users to Access Protected URLs from Any System

The Web PassPort virtual card will download to any system and then download a users digital credentials to their current location. This allows users to work from multiple systems, home, office, laboratory etc. — a capability not available to a user who stores their credentials in the browser of a single system.


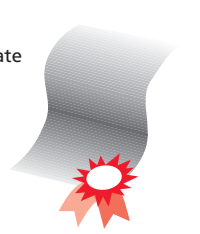



II. System Concepts

This section examines some of the key system concepts used in the RSA Keon Web PassPort Architecture.

Virtual Card

A virtual card is a software construct that allows a user's PKI credentials to be stored in a virtualized smart card. The Web PassPort Plug-in provides Microsoft cryptographic service providers and PKCS #11 drivers that allow the virtual card to integrate seamlessly into Windows operating systems and Web browsers.

The virtual card can be accessed by any Windows application that understands how to access a cryptographic service provider via Microsoft CAPI and the PKCS #11 interface. virtual cards are transient, they go away either when the machine is shut down or the user explicitly closes the virtual card; at no time are they written to permanent storage on the desktop.

| | |
|---|--|
|  Encryption Certificate |  Signing Certificate |
|  Secret Key 1 | Encrypted with PUK RC4-128 |
|  RSA Private Key 1 | Encrypted with Secret Key 1 |
|  RSA Private Key 2 | Encrypted with Secret Key 1 |

The Virtual Card

A virtual card may have either one or two keys; if it only has a single certificate and associated private key then the key is multi-purpose and can be used for both encryption and digital signatures. If the virtual card has two separate keys then the first certificate and private key is used for digital signatures and the second certificate and private key is used for encryption. The user's RSA® private keys are encrypted with a 112-bit 3DES2EDE-CBC (triple DES with two keys, encrypt/decrypt operating in cipher block chaining mode), referred to a Secret Key 1.

Secret Key 1 is encrypted and stored with a PIN Unlock Key (PUK). A PUK is a randomly generated 128-bit RC4® symmetric key. The salt is an eight byte random number stored in the virtual card, and the iteration count is 1024 times.

Web PassPort users may be issued virtual cards from many companies or organizations. To address this, the Web PassPort Plug-in allows the user to have many virtual cards open during a single session. This situation generally arises if the end user accesses internal Web applications that require PKI credentials as well as another organization's Web applications (in a B2B relationship) that require PKI credentials from that organization.

Virtual cards are created using the virtual card manager, which stores them as an attribute associated with the user object in the LDAP directory. The virtual card manager can be run in batch mode to create large numbers of virtual cards, and it may be called from external programs (such as a user's account management tool).

Web Cookies

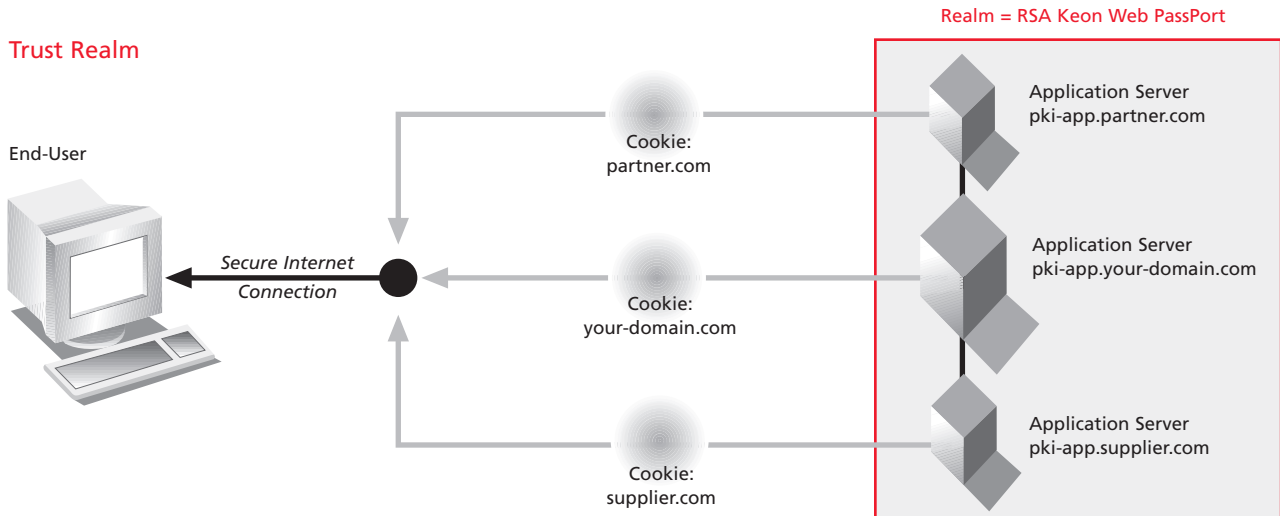
Web Cookies were created to provide context oriented applications with a means to overcome the stateless nature of the Web. Today, cookies are the primary mechanism for maintaining state across multiple interactions between a browser and a Web server. Web PassPort uses cookies to keep track of authentication state information, PKI credential state information, key container names and so on.

Web PassPort Server issues transient cookies. That is, the cookies are not written to the user's hard disk, but rather exist only in memory. The cookies are destroyed when the Web browser is closed. All sensitive information stored in cookies is heavily encrypted and checked for integrity.



Web Cookies

RSA Keon Web Passport



Trust Realm

Trust Realms

Most large enterprise networks encompass multiple IP domains. By definition, Web cookies are specific to the domain and path of the Web server, which prevents a cookie created by a Web server in one IP domain from being used by a server in another IP domain.

To create a Web Single Sign-On solution, Web PassPort Servers use a common symmetric key to establish a trust relationship. Such a collection of Web PassPort Servers is called a realm.

III. General Description

The RSA Keon Web PassPort consists of two major subsystems: the Web PassPort Server and the Web PassPort Plug-in. This section briefly describes the architecture of these two subsystems.

RSA Keon Web PassPort Server

The Web PassPort Server resides in a customer's Web server to control access to Web applications and provide other PKI related services. Web PassPort Server consists of the following services.

Authentication Broker

Interacts with the user desktop to implement various types of user authentication based on passwords, RSA SecurID tokens, physical smart cards, etc. Includes an Authentication Module for each supported authentication method.

Credential Server

Provides secure download of virtual cards to the desktop and upload of modified virtual cards from the desktop for updating the repository. Provides secure retrieval and storage of virtual card's from a LDAP directory.

LDAP Virtual Card Management Service

Provides interfaces and utilities for creating virtual cards and storing them in an LDAP directory-based Repository. Interfaces support both interactive user and scriptable batch operations. Also includes tools for extending existing standard LDAP schemas to support Web PassPort objects and attributes.

Resource Management Service

Consists of a policy database and the utilities and interfaces for managing information in the database. The policy database contains configuration and policy settings of the Web PassPort Server and its protected URLs.

Software Download Service

Provides secure download of the Web PassPort Plug-in software package.

URL Filter

Controls access to Web applications by intercepting URL requests and implementing authentication policy decisions defined by the organization.

The services are described in the following sections.

Authentication Broker

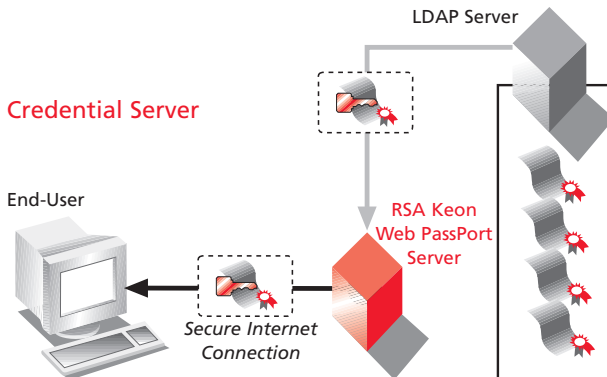
The Web PassPort Server Authentication Broker enforces the authentication policy defined for a URL. It consists of several separate hidden URLs, one for each type of supported authentication method. The Authentication Broker performs the following operations:

- Downloads user login forms and scripts.
- Calls one of the configured Web PassPort Authentication Modules to validate the authentication information that the user provides:

- RSA SecurID authentication module: validates user ID/passcode with a configured RSA ACE/Server. Passcodes may be a PIN plus a hardware token code, an RSA SecurID software token value, or an RSA ACE/Server one-time password. The module supports New PIN and next token code modes.
- LDAP authentication module: validates username/password through an LDAP BIND authentication request.
- Instructs the browser to create authentication cookies for the local domain
- Provides the browser with information to contact all trusted Web agents to build all cross-domain authentication cookies.

Credential Server

The credential service is responsible for uploading and downloading user PKI credentials (in the form of virtual cards) to the Web PassPort Plug-in. The credential server first determines if the user has been authenticated and then selects only those virtual cards belonging to the user that have a protection level at or below the authentication level of the user.



The credential server works in conjunction with the virtual card manager, which is used to create virtual cards. The credential server stores the virtual cards in an attribute associated with the user object in an LDAP directory. The virtual card itself is an encrypted container, and the attribute used to store the virtual cards is bound to the user Distinguished Name and has restricted access rights. The Credential Server is called in the following situations:

- A user has previously authenticated (an authentication cookie exists); the application URL being accessed requires PKI credentials and the Web PassPort Server URL Filter did not detect a suitable virtual card cookie.
- A virtual card has been modified on the Web PassPort Plug-in and needs to be uploaded to the LDAP Directory.

- A user must perform a manual certificate pickup/installation from a Web PassPort Plug-in, but the virtual card into which the certificate is to be placed is not present on the desktop. This can happen when significant time elapses (for example, a few days) between the certificate enrollment and the pickup/installation. The original virtual card must be retrieved before the new certificate can be installed.

The Credential Server generates a Web page (called an import page) that is used to download virtual cards to user's Plug-in. The import page contains a reference to a Multipurpose Internet Mail Extensions (MIME) type through which the virtual card data streams (in much the same way as an audio file plays across the Internet). If the object that handles the virtual card MIME type does not exist at the desktop, the browser automatically goes to the download URL to get the Web PassPort Plug-in software.

Software Download Service

The Software Download Service supports two modes of operation, automatic and manual. Both modes are handled through the Software Download URL. This URL is usually protected by the Web PassPort Server and is thus subject to the URL policy settings.

Automatic Mode

Typically, a desktop user does not install Web PassPort Plug-in software manually. As described in earlier sections, the software is downloaded automatically and installed on the desktop the first time the user attempts to access a protected Web application requiring PKI credentials. The download is triggered when the virtual card import page refers to a special Web PassPort embedded object MIME type and its associated Plug-in is not installed. This download and installation is similar to the way that browser plug-ins such as RealPlayer™ are handled when the user attempts to open a RealPlayer audio file.

Manual Mode

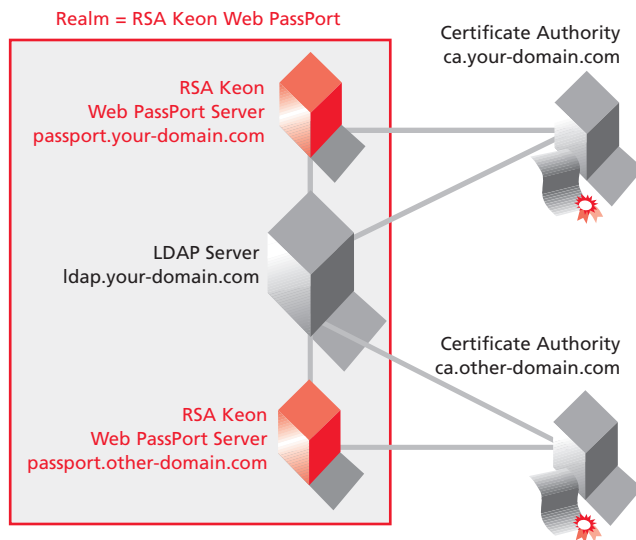
Since the download is handled through the Software Download Service URL, a user can manually request the download and installation of the Web PassPort Plug-in software package by accessing the URL directly through a browser.

The downloaded software is digitally signed by RSA Security. The user must accept the signature to all the software in order to be installed.

Auto-Registration

The Auto-Registration Service is provided to automate the certificate registration process for user Personal certificates; the Personal certificates are then placed in the user's virtual card. The certificate registration process involves three high-level functions:

- Enrollment. The process by which a request for a digital certificate is made to a registration authority.
- Approval. The process by which requests are approved and the CA issues certificates.
- Pick Up. The process by which the certificate is delivered to the end user.



Auto Registration

The RSA Keon Web Passport can automate all three processes so certificate registration is transparent to the end user. Web Passport also allows these processes to be performed manually. The Web Passport Server can be configured to provide certificate auto-enrollment using a customer's existing Web-based CA or RA, when the Web Passport Plug-in detects that the user requires a Personal certificate. In this case, the Web Passport Plug-in automatically opens a new browser window directed at the Certificate Registration URL (configured in the Web Passport policy database).

With automatic approval enabled at the CA, the requested certificate is returned immediately and will be downloaded to the browser along with a control script. The script initiates writing the certificate to the virtual card, which causes the Web Passport Plug-in to upload a modified virtual card to the LDAP directory.

When auto-registration is used, a special CA utility is required to automate the processing of the certificate request. The RSA Keon Certificate Authority supports this via the RSA Keon OneStep module (other CAs have similar mechanisms to achieve the same functionality). Web PassPort supports certificate authorities from multiple vendors and each CA may publish the user's personal certificates to different directories. However, the CA plug-in must obtain the user attributes for auto-registration from the LDAP directory where the account information is stored.

The RSA Keon OneStep module uses the Web PassPort authentication cookie to determine the user's identity. The OneStep module obtains the user ID from the cookie and uses it to retrieve the user's registration information in the LDAP directory. The registration request is then submitted to the CA.

Enrollment

The Web PassPort Plug-in triggers a certificate enrollment when it detects a virtual card with no valid Personal certificate, or an expiring Personal certificate.

The desktop initiates enrollment using an HTTP forms enrollment request. An HTTP enrollment request triggers a browser session to the enrollment URL specified in the virtual card download. The user may authenticate either by the browser supplying a cookie that is recognized by the CA/RA or by the user supplying a user ID and authentication information to the HTTP registration form.

Approval

There are two types of approval mechanisms: manual and auto-approval. In manual approval, a certificate administrator must approve the end-user enrollment request before the CA can issue the certificate. In auto-approval, the RA requests the CA to issue the certificate immediately. Generally, auto-approval requires the end-user to authenticate when making the enrollment request.

Successful authentication of the end-user does not always result in auto-approval. The Plug-in is prepared to handle this scenario. If the enrollment request is accepted but auto-approval is not granted, the certificate must be picked up manually at a later time.

When an HTTP forms enrollment request is used, the RA generally implements its auto-approval policy in customer-supplied code that is incorporated into the RA. Two such models are the RSA Keon OneStep module in the RSA Keon Certificate Authority and the auto-administration feature in VeriSign OnSite™. Both of these modules authenticate the end-user and also collect end-user attributes that they use to populate fields in the enrollment request.

Pickup

Two forms of certificate pick up are supported — manual and auto-pickup. If an enrollment request is approved automatically, it is generally (but not necessarily) followed by an auto-pickup. That is, the certificate is returned immediately and installed in the user's virtual card.

In manual pickup, the user generally is sent an e-mail message with a pickup URL and PIN. The user then accesses the pickup URL through a Web browser and downloads the certificate to their browser and hence their virtual card.

Resource Management Service

The Resource Management Service controls access to protected URLs. If a URL is marked as protected, the user must authenticate before gaining access to the URL. (Note that the Web server may then perform additional application-specific authorization checks.)

The Resource Management Service also allows configuring the URL to require that a user has PKI credentials and, if so, whether users are required to possess a personal certificate. Requiring PKI credentials simply indicates that the user must have a valid virtual card before he or she can access the URL.

Note that the strength of authentication needed to access a virtual card is not part of the URL policy information; it is a function of the virtual card manager Service and is defined when the virtual cards are created.

The Web PassPort Resource Management Service consists of a policy database, as well as the utilities and interfaces for managing the database. The policy database contains configuration and policy settings of the Web PassPort Server and its protected URLs. This policy information drives the operational model of the Web PassPort software.

RSA Keon Web PassPort Server Configuration

The policy and configuration information that must be maintained for the Web PassPort Server includes:

- General policy settings for the Server, including:
- Authentication required for software download
- Trusted realm settings (shared secret, list of domains)
- Automatic certificate registration enabled
- Plug-in software upgrade policy (forced, optional, manual, etc.)
- Authentication service types and locations
- LDAP repository location(s)
- URL for the Software Download Service
- RA/CA settings for auto-registration, if enabled

Protected URL Policies

The policy information maintained for each protected URL on the Web server includes:

- Supported authentication methods:
 - LDAP username/password — username/password maintained in LDAP.
 - RSA ACE/Server user passcode and One-Time Password (OTP) — ACE user ID and passcode or OTP that is sent to the RSA ACE/Server for validation.
 - RSA SecurID time-based token — user must enter user ID and passcode, which are validated by an RSA ACE/Server.
- Whether the application requires PKI credentials to be present. This policy determines whether or not the Plug-in software is required to download and use virtual cards.
- Whether the PKI application requires a user to possess a Personal certificate. This controls whether the virtual card certificate is verified to be an Personal certificate. If not, it triggers the certificate registration process.

URL Filter

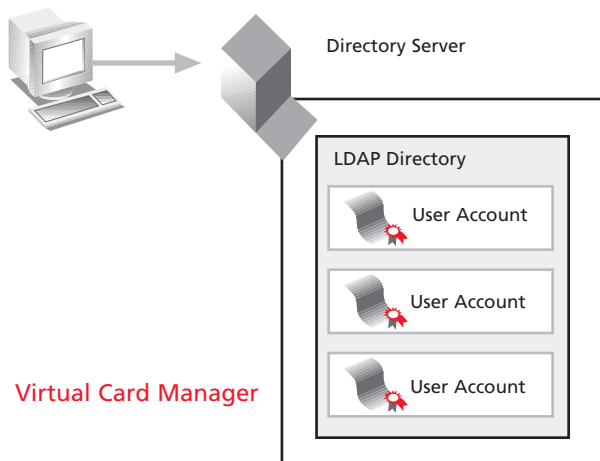
The Web PassPort server's URL filter will:

- Intercept access attempts to protected URLs.
- Check the policy requirements for protected URLs.
- Determine whether or not the browser has a valid authentication cookie that permits access to a protected URL.
- Redirect the user to the authentication service if the user has no virtual card.
- Redirect authenticated users who have no virtual card to the Web PassPort repository service.
- Pass authenticated access requests that do not require PKI credentials to the specified URL.
- Pass authenticated access requests requiring PKI credentials that are present in the Web PassPort Plug-in to the specified Web application.

Virtual Card Manager

Web PassPort provides a virtual card manager to create virtual cards for users and write them into the LDAP directory.

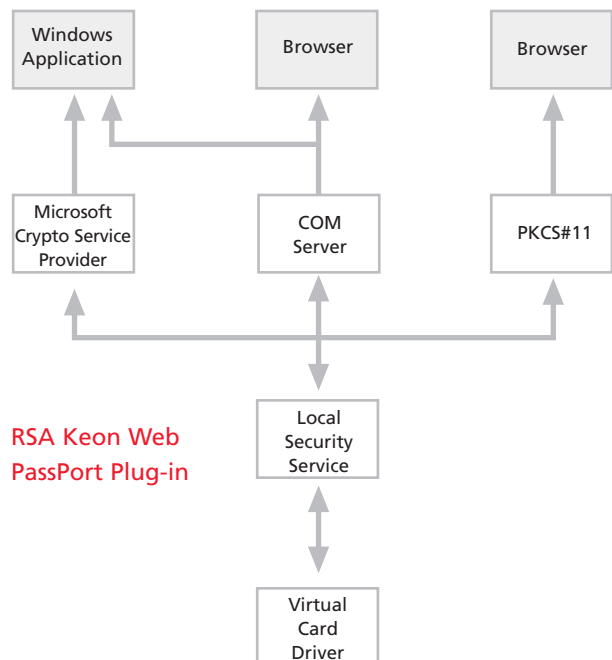
The virtual card manager uses a command line interface that issues virtual cards. The command line interface can be integrated into customer account management processes that may already exist, or integrated into a Web/CGI application. An example Web/CGI application is distributed with the virtual card manager software.



RSA Keon Web Passport Plug-in

The Web PassPort Plug-in is downloaded to users over the Internet and installed on the desktop automatically. It provides the following services and features:

- Local Security Service (LSS) — Manages access to PKI credentials stored in users' virtual cards. LSS supports simultaneous access to multiple virtual cards. This allows users to have multiple browser windows open to access applications that require different PKI credentials.
- COM Server — Provides application-independent access from a Web browser, e-mail, etc. to LSS and other desktop functionality.
- RSA Cryptographic Service Provider — Implements a Microsoft CSP for CAPI, allowing Microsoft Internet Explorer or any CAPI-aware application (such as Microsoft Outlook) to access the user PKI credentials stored on the virtual card.
- RSA PKCS #11 Driver — The RSA PKCS #11 driver allows Netscape browsers or any PKCS #11-aware application to access the user PKI credentials stored in a users' virtual card.
- Logoff Service — A Windows system tray application that forces all open sessions to be terminated and closes all open virtual cards.



IV. Operational Model

This section describes a “typical” RSA Keon Web PassPort usage scenario in order to give a general view of the operational model. The numbered steps are explained in the following sections.

The scenario assumes the user has a Web browser and access to the Internet but does not have the Web PassPort Plug-in software installed. It also assumes the company running the Web site has issued the user a single virtual card that must be updated with a Personal certificate on first use.

1. Browser

User attempts to access a protected page on a Web site.

- a. URL Filter: Checks the application URL policy; if the policy requires authentication and no authentication cookie was received it redirects the request to the Authentication Broker URL.
- b. Authentication Broker: Sends the Web PassPort login options page and login script to the user’s browser.

2. Browser

User responds to the chosen authentication method and posts their login information to the Authentication Broker URL.

- a. Authentication Broker: Validates the user’s login information.
- b. If successful, it returns the success form to the user with an authentication cookie.

3. Browser

User attempts to access the original application URL, this time with the authentication cookie.

- a. URL Filter: Checks the application’s URL policy; It detects an authentication cookie but no virtual card cookie is detected; It redirects the request to the Credential Server URL.
- b. Credential Server: Returns the virtual card import form to the browser. The Import form includes an embedded object of a special MIME type defined for virtual cards.

The following steps are executed only when the Web PassPort Plug-in is not present on the user’s computer.

- c. Browser: Attempts to create an instance of the object associated with special MIME type. If the object exists, it requests a virtual card from the repository service. (In this instance, from here the reader should proceed to step 3g.) If the object does not exist, the browser calls the Software Download URL for the object. The URL is the Web PassPort Server download URL, which requires user authentication before download.

- d. URL Filter: Detects a previous successful authentication cookie. It permits access to the Web PassPort Download Service URL.
- e. Web PassPort Download Service: Sends a browser-specific installation package to the desktop.
- f. Browser: Installs the Web PassPort Plug-in software.
- g. Credential Server: Obtains a user’s virtual card data from the LDAP directory. Sends virtual card data as streamed data to browser; also sets a virtual card cookie.

4. Browser

Retries access to the original Web application URL.

5. URL Filter

Checks policy for the URL. It detects a valid authentication and virtual card cookies; it permit access to the application URL.

6. Session Timeout

RSA Keon Web PassPort software has a customizable session time-out feature if the virtual card is not used within a prescribed period of time. The default time period is customizable by the administrator.

Session Termination

When the user’s Web PassPort session is terminated, all virtual cards are destroyed on the user’s system. The most current versions of the virtual cards have been uploaded securely and stored in the LDAP by the Server’s Repository Service. Upon subsequent re-authentication, the user’s virtual cards are securely downloaded again for use.

The user’s session can be terminated in four ways:

- The user selects “virtual card logoff” by activating the Plug-in’s system tray icon. The Plug-in remains on the user’s system, and virtual cards are destroyed.
- The user selects “uninstall plug-in” by activating the Plug-in’s system tray icon. The Plug-in is uninstalled and virtual cards are destroyed.
- The local system is rebooted. The Plug-in remains on the user’s system, and the virtual cards are destroyed.
- The local Windows session ends. When the user’s Windows session ends, the Plug-in remains and virtual cards are destroyed.

