MỘT SỐ HỆ THỐNG PKI ĐIỂN HÌNH VÀ CÁC ỨNG DỤNG CỦA PKI

CHỨNG THỰC ĐIỆN TỬ

MỘT SỐ HỆ THỐNG PKI ĐIỂN HÌNH VÀ CÁC ỨNG DỤNG CỦA PKI

- Các hệ thống PKI điển hình
- Các ứng dụng PKI
- Các thiết bị phần cứng an toàn (HSM, USB Token)

CÁC HỆ THỐNG PKI ĐIỂN HÌNH

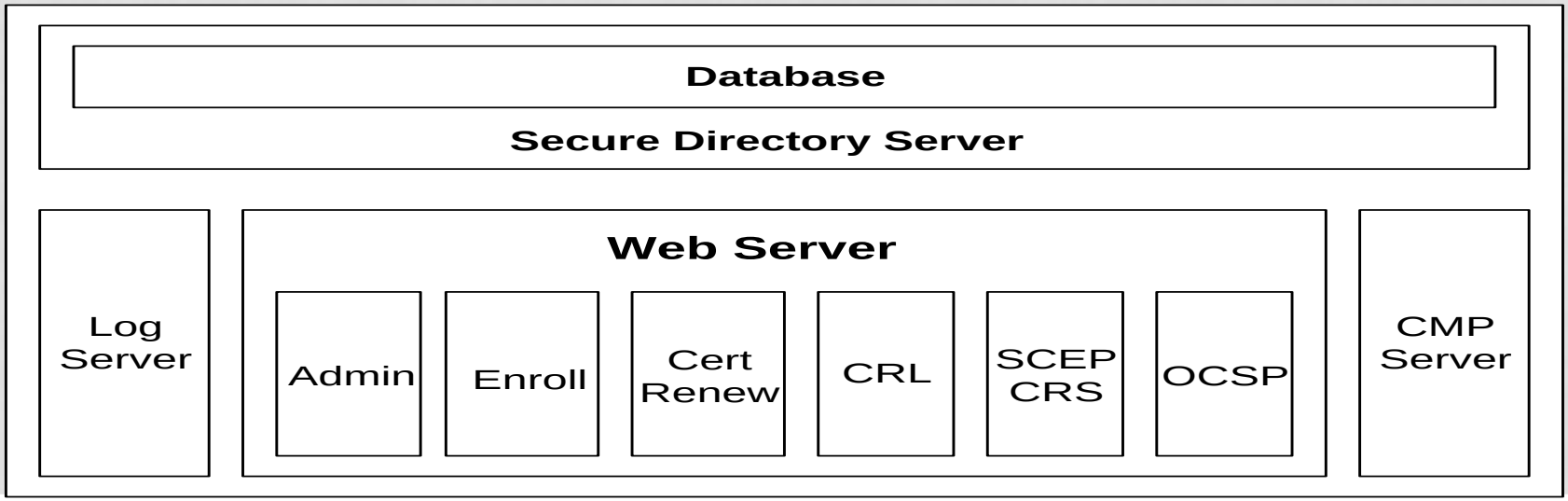
- Hệ thống mã đóng
  - Giải pháp của RSA
  - Giải pháp của Entrust
- Hệ thống mã nguồn mở
  - Open CA
  - EJBCA

HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Giải pháp RSA có tên là Quản lý chứng thư RSA
- Đảm bảo bảo mật và khả năng mở rộng các giao dịch bằng cách cung cấp một hệ thống linh hoạt có khả năng mở rộng để quan lý các định danh số.
- Cung cấp các modules có khả năng tương tác cho phép tổ chức phát triển, triển khai và mở rộng các ứng dụng an toàn bằng cách quản lý các khóa mật mã và CTS tập trung tự động

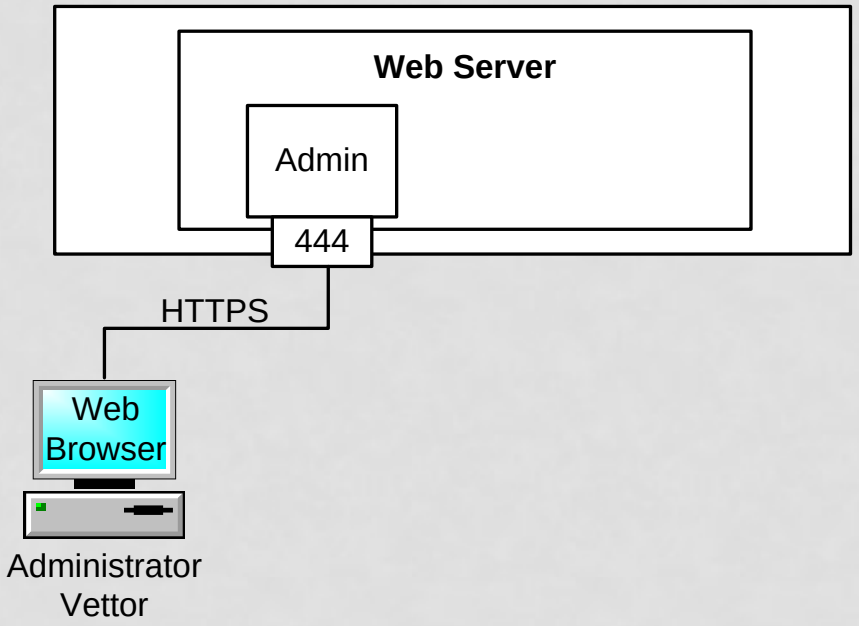
HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Giải pháp RSA bao gồm 04 sản phẩm tích hợp đầy đủ để cung cấp một hệ thống duy nhất:
  - Lỗi quản lý chứng thư RSA
  - Quản lý đăng ký
  - Quản lý quyền chứng thực VA
  - Quản lý khôi phục khóa



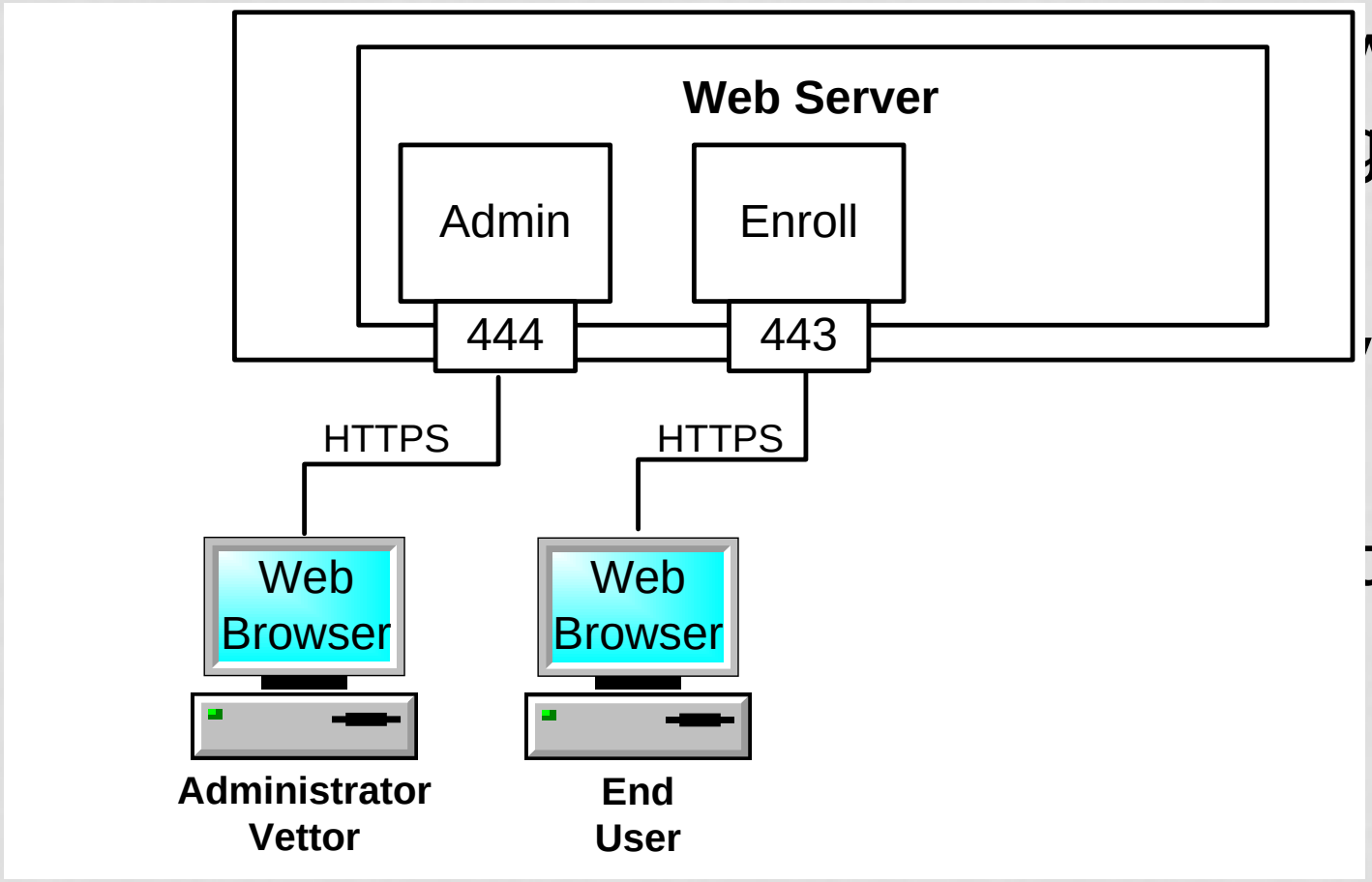
HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Module quản trị:
- Module quản trị cho phép người quản trị thực hiện qua giao diện web với giao thức https. Hệ thống sử dụng cơ chế xác thực qua chứng thư số



HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

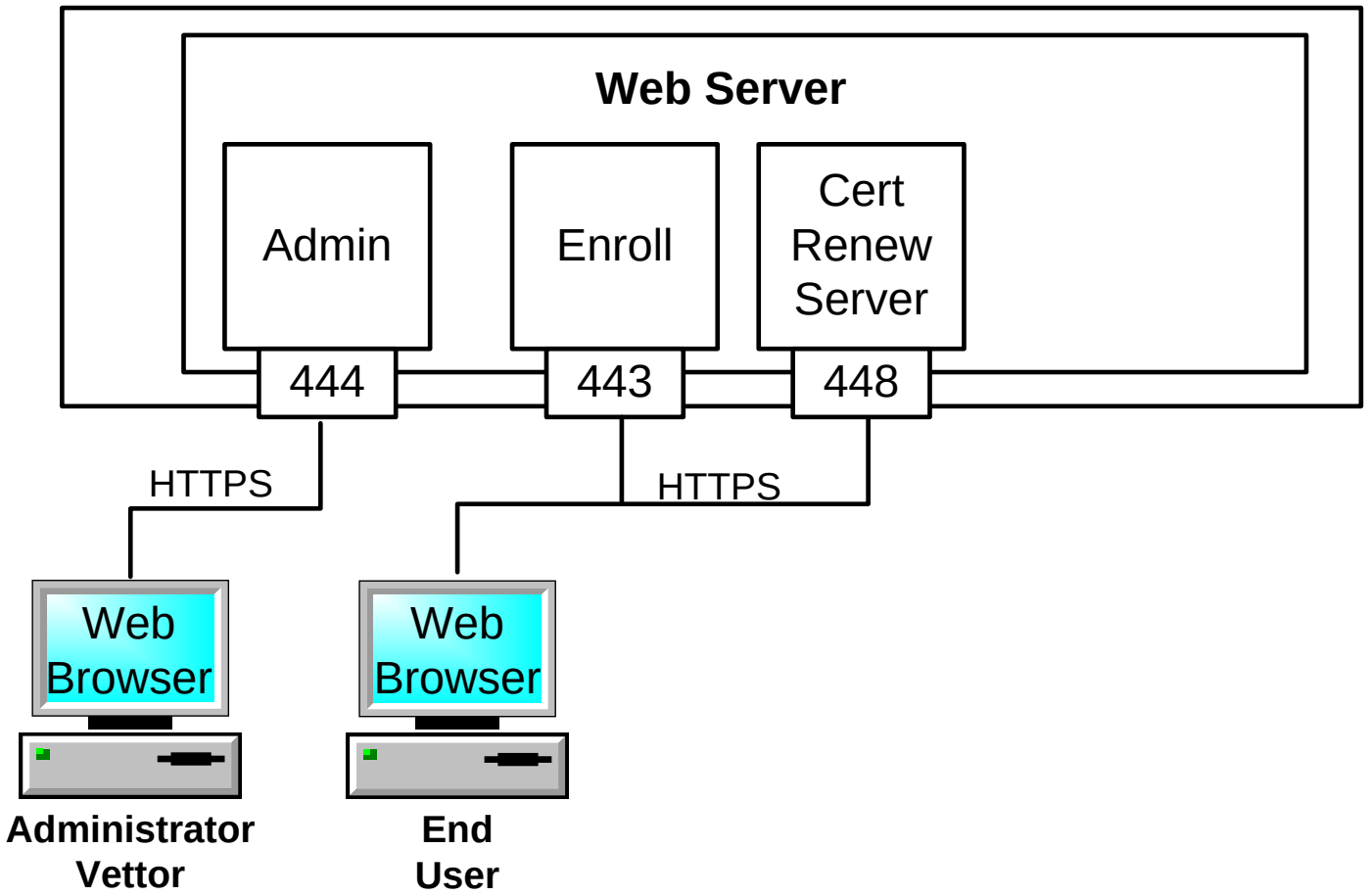
- Module đăng ký:



web, cho
g RSA
và
tới giao

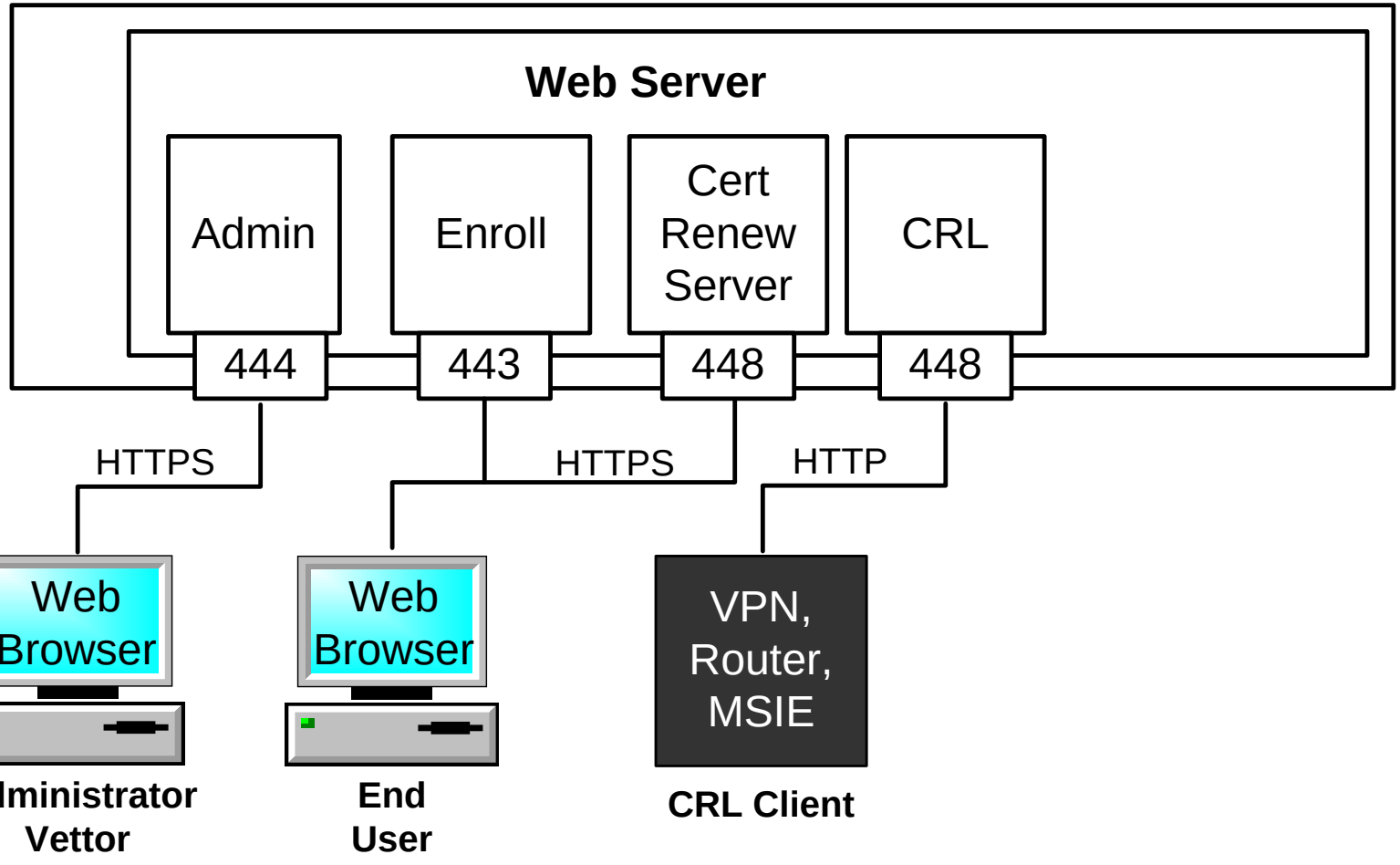
HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Module cấp mới chứng thư số:



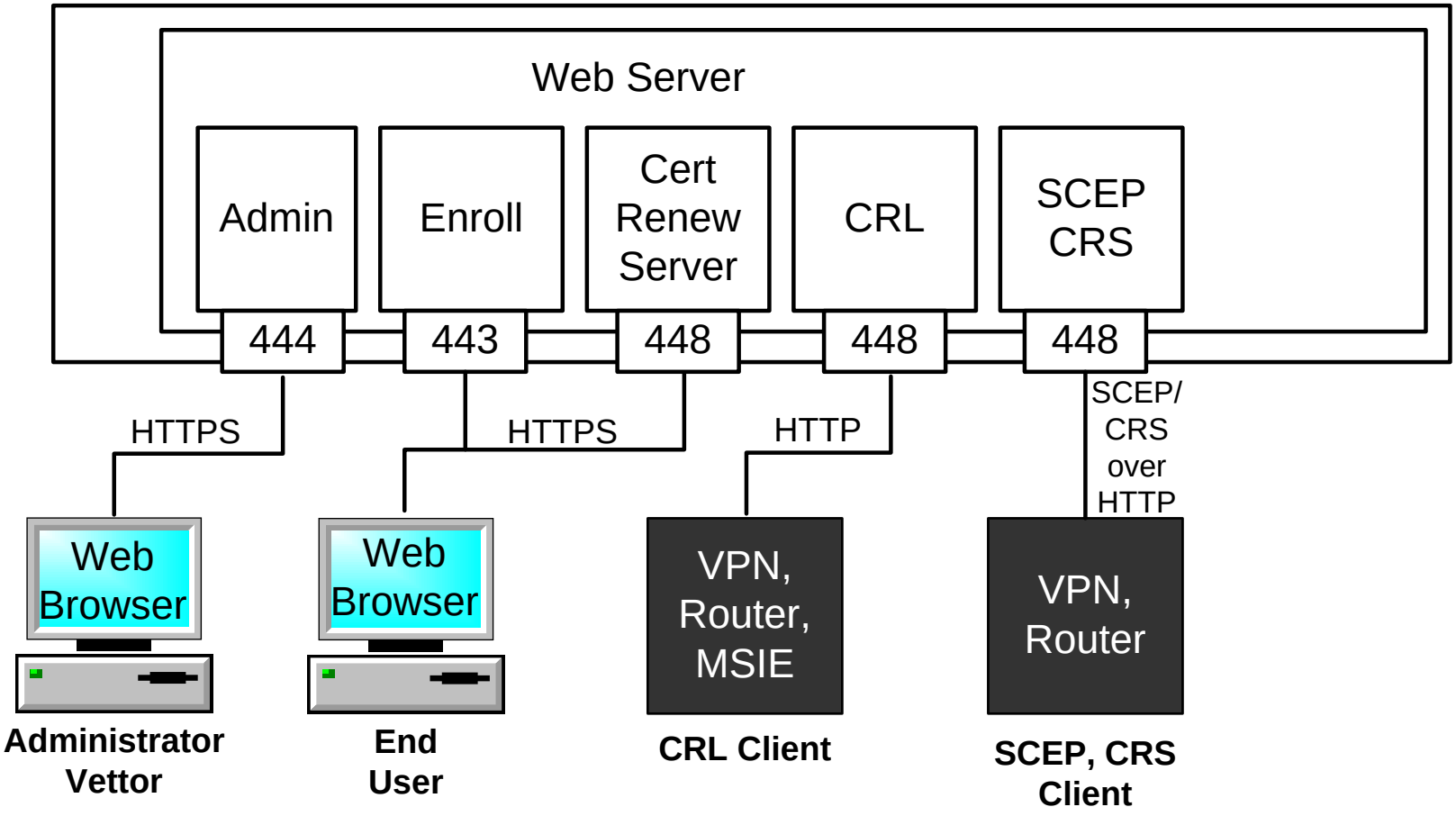
HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Module danh sách thu hồi:



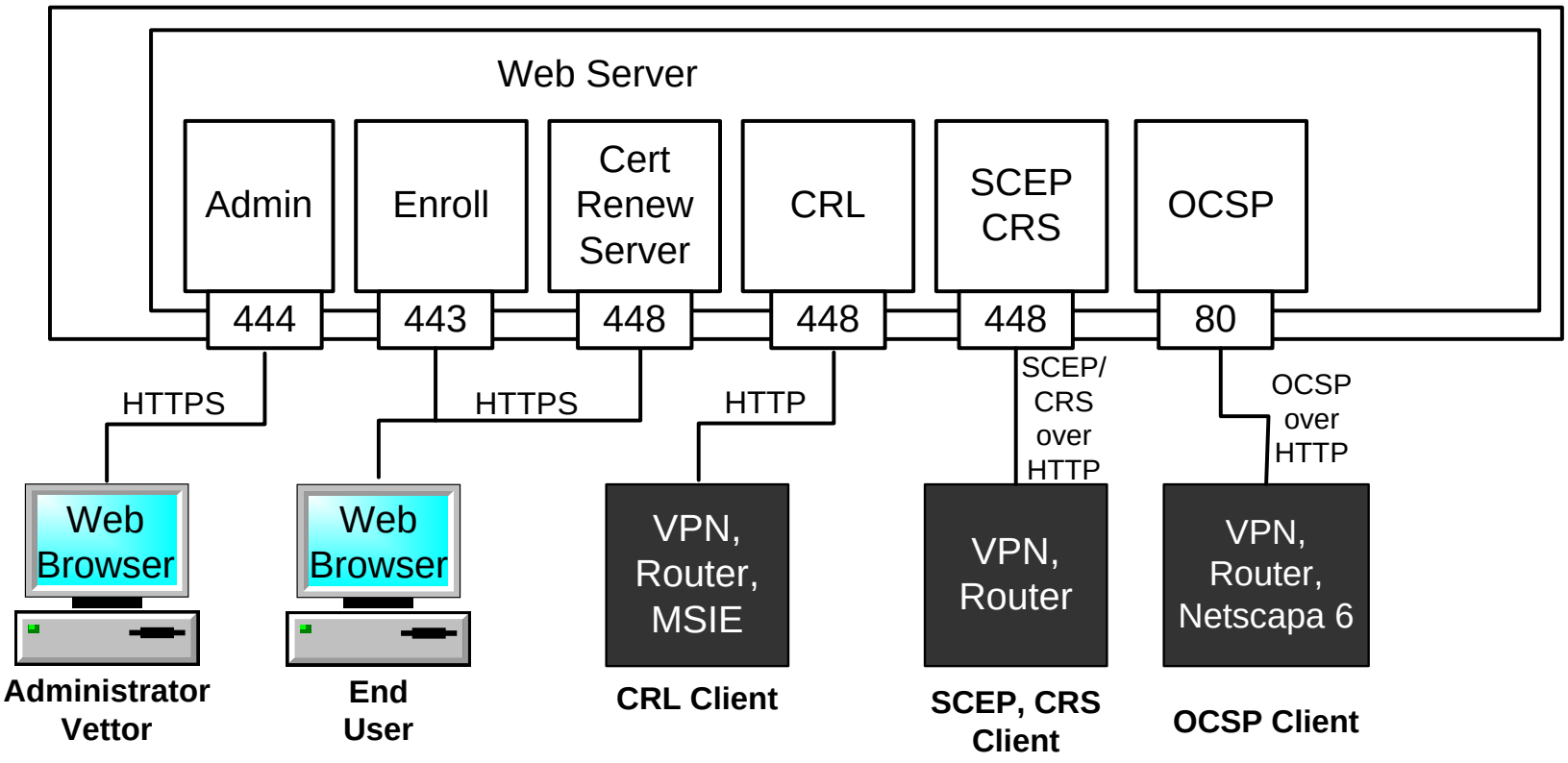
HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Module SCEP



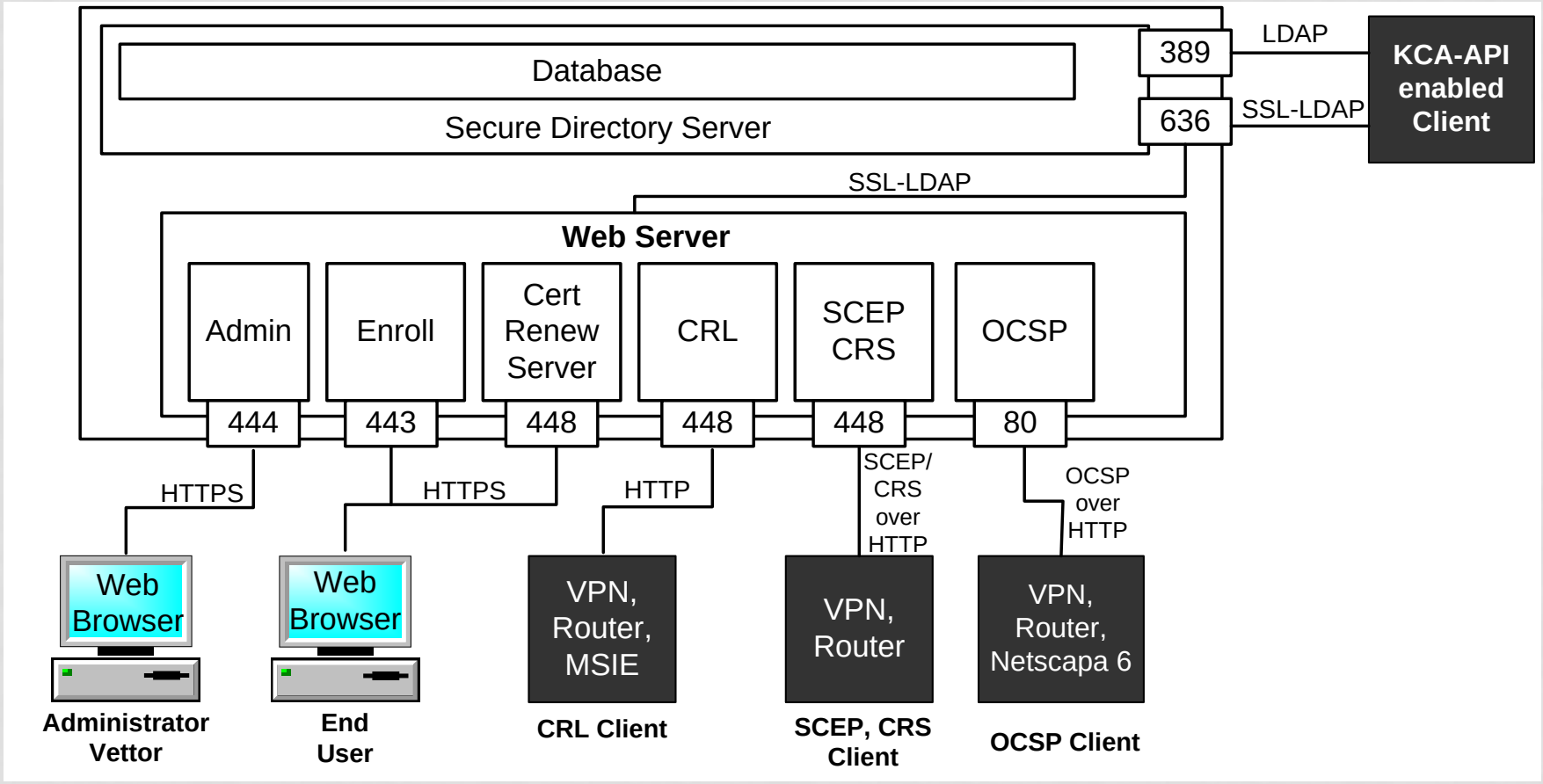
HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Module OCSP:



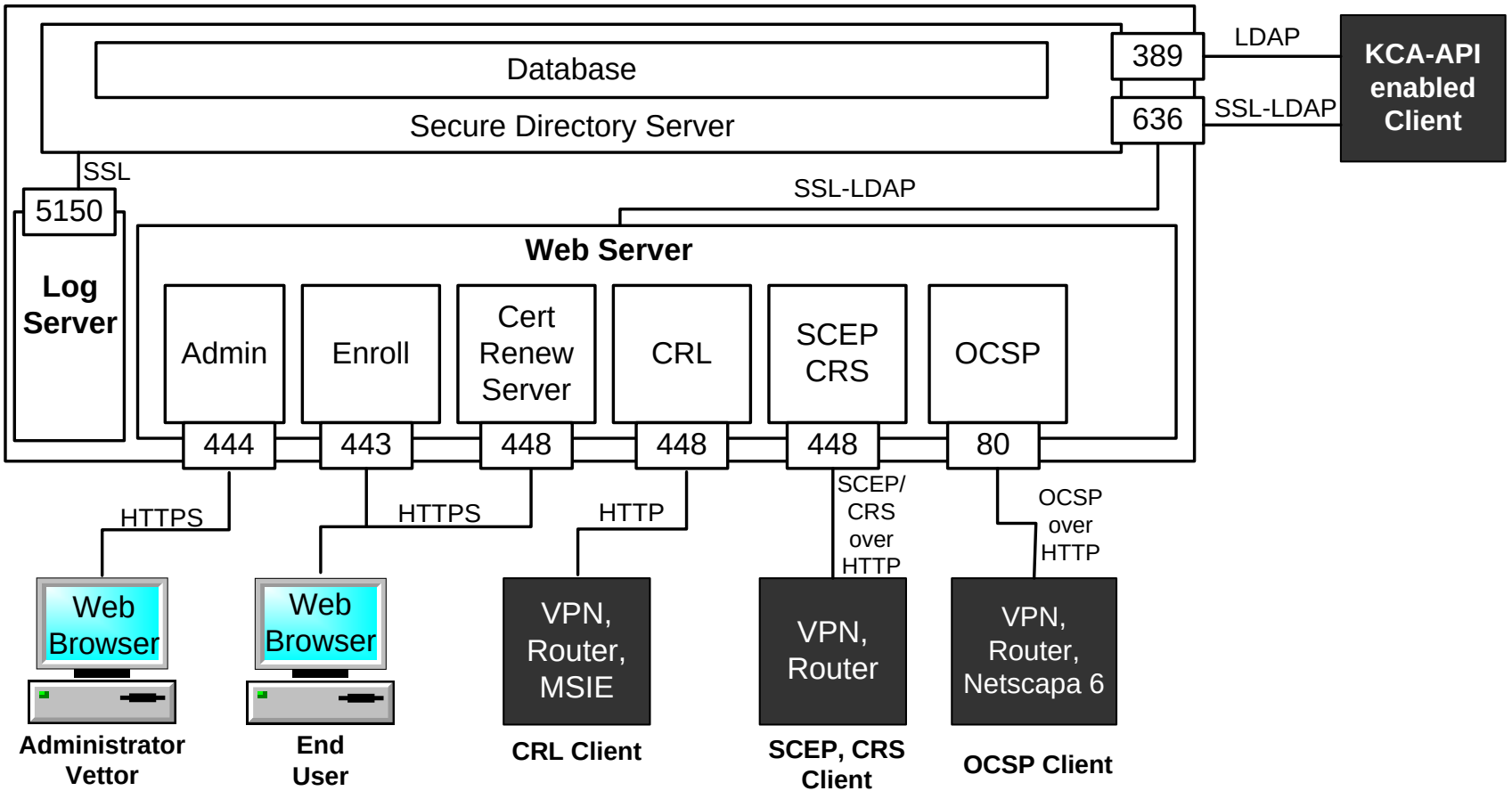
HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Module giao tiếp thư mục:



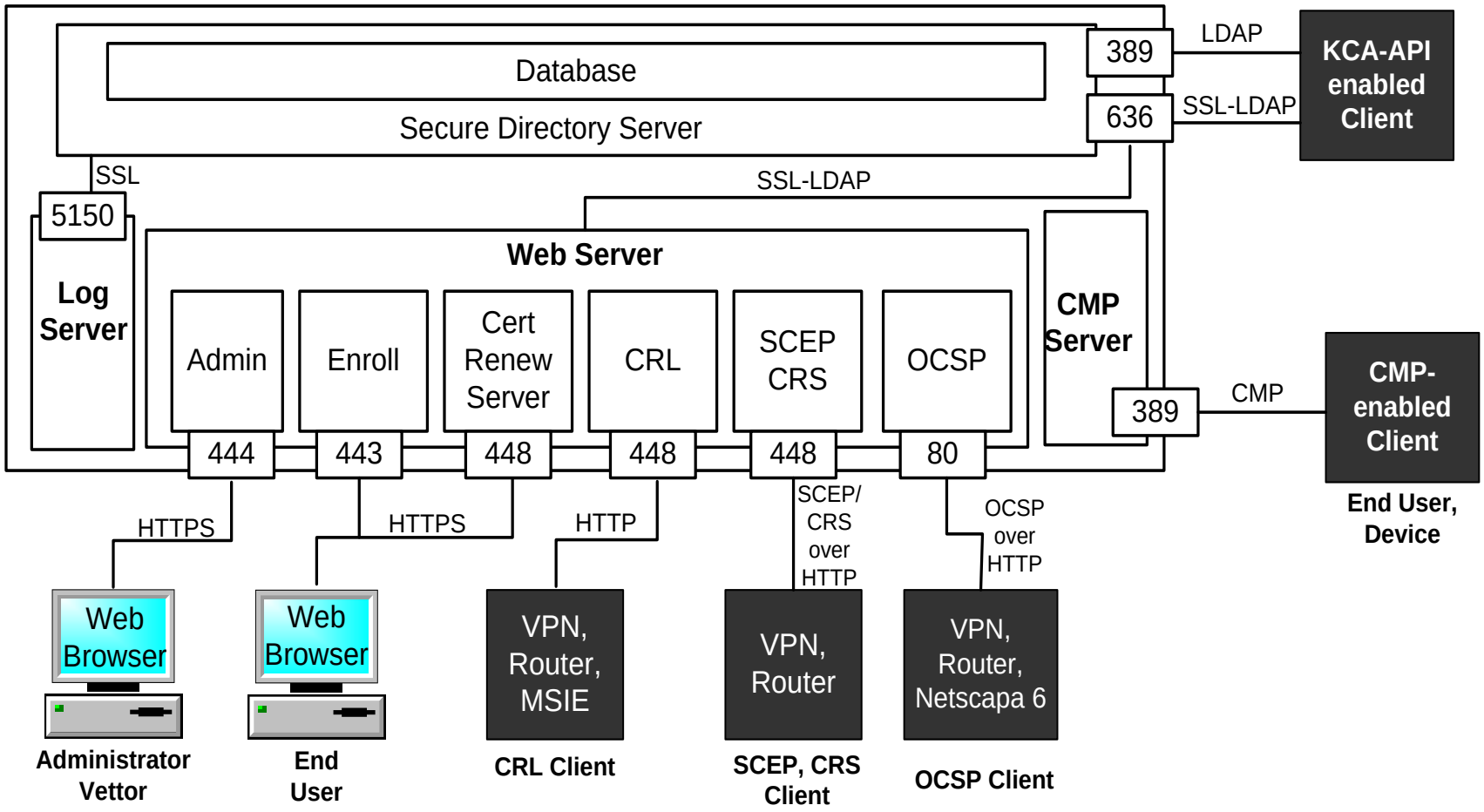
HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Module LogServer:



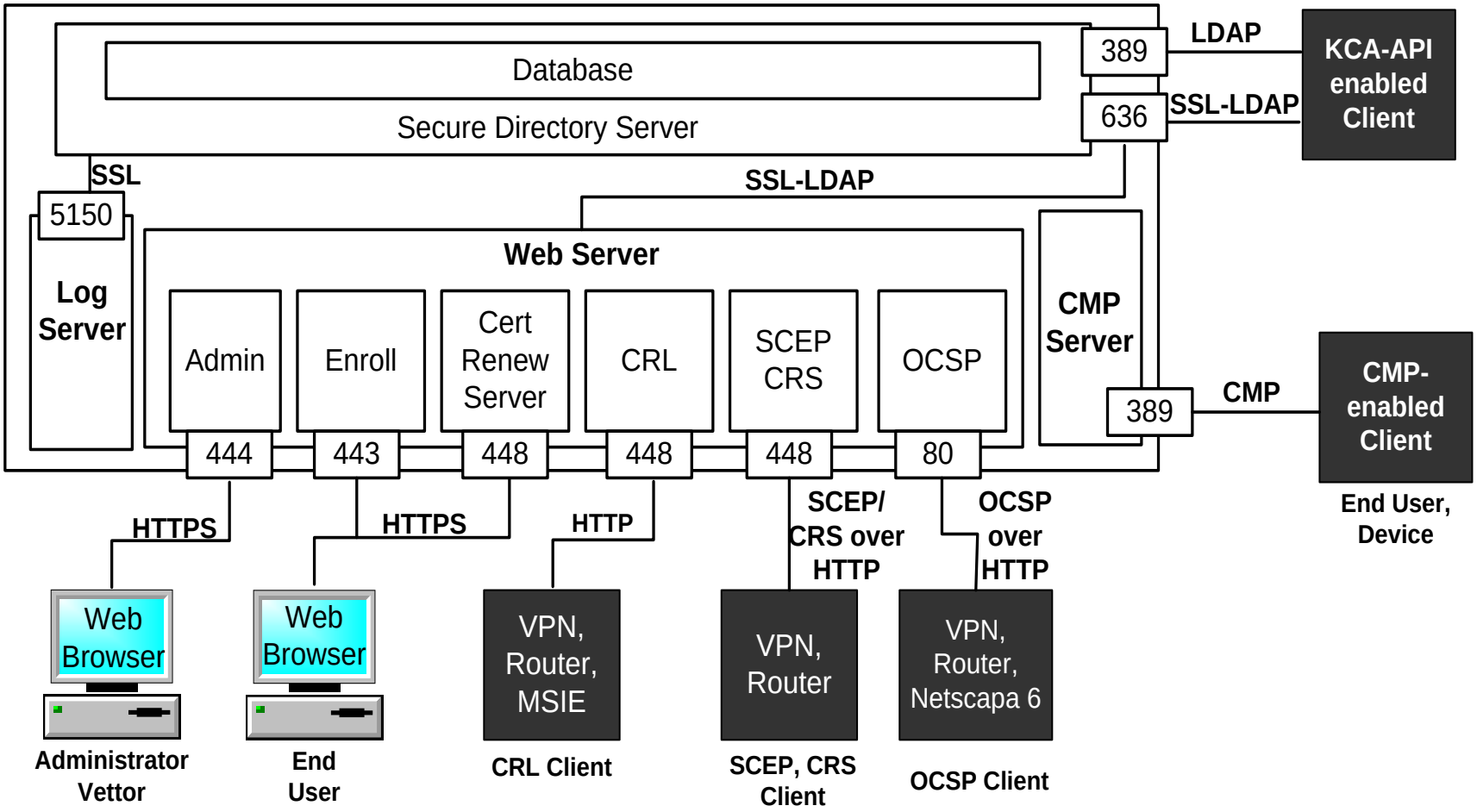
HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Module CMP server



HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Các giao thức được sử dụng



Giao thức	Mô tả
HTTP HTTPs	HyperText Transfer Protocol: Giao thức này được sử dụng để truyền dữ liệu qua môi trường web.
LDAP LDAPs	Lightweight Directory Access Protocol: được sử dụng cho việc truy nhập các dịch vụ thư mục trên môi trường mạng.
SSL	Secure Sockets Layer: được sử dụng để bảo mật các thông điệp được truyền qua môi trường mạng. Được kết hợp với LDAP và HTTP để tạo ra các kênh truyền dữ liệu an toàn.
CMP	Certificate Management Protocol: là một giao thức được sử dụng trong việc quản lý chứng thư.
OCSP	Online Certificate Status Protocol: Cho phép một máy client yêu cầu thông tin trạng thái của một chứng thư từ một máy chủ OCSP Responder.
CRS	Certificate Request Syntax: là cú pháp cho các yêu cầu chứng thư số, cú pháp này được định nghĩa trong PKCS#10.
SCEP	Simple Certificate Enrollment Protocol: giao thức này được sử dụng trong việc quản lý các yêu cầu cấp phát chứng thư số trực tuyến.

HỆ THỐNG MÃ ĐÓNG – GIẢI PHÁP RSA

- Các thành phần trong giải pháp quản lý CTS RSA
  - Quản lý chứng thư RSA
  - Quản lý đăng ký RSA
  - Quản lý ủy quyền chứng thực
  - Quản lý khôi phục khóa RSA

- Quản lý chứng thư RSA:
  - quản lý các định danh số và tự động hóa và tập trung hóa việc quản lý các khóa mật mã và chứng thư số
  - Có những lợi ích:
    - Tăng cường bảo mật
    - Khả năng mở rộng
    - Khả năng tương tác
    - Dễ dàng phát triển và quản trị

- Quản lý đăng ký RSA
  - cho phép xử lý một lượng lớn các yêu cầu về chứng thư của người dùng cuối, với các việc như kiểm tra thông tin yêu cầu chứng thư và cung chứng thư tới người yêu cầu.
  - cho phép các tổ chức thành lập Trung tâm đăng ký người dùng độc lập, cho phép triển khai tại các địa điểm địa lý phân phối từ xa hoặc địa phương
  - Lợi ích:
    - Khả năng mở rộng
    - Tăng cường bảo mật
    - Đăng ký mềm dẻo

- Giải pháp ủy quyền chứng thực:
  - cho phép kiểm tra ngay lập tức các chứng thư số để đảm bảo tính toàn vẹn của các giao dịch điện tử trong các tổ chức và cơ quan nhà nước.
  - Lợi ích:
    - Tăng cường bảo mật
    - Đạt các chứng nhận bảo mật quản lý chứng thư thương mại
    - Dễ dàng tính hợp
    - Độ tin cậy, tính sẵn sàng và hiệu năng cao

- Giải pháp khôi phục khóa RSA:
  - lưu trữ bảo mật và khôi phục khóa mã của người dùng để hạn chế các rủi ro mất dữ liệu trong trường hợp khóa mã bị mất, hoặc bị hỏng
  - có chức năng sinh khóa và lưu trên thiết bị phần cứng (HSM), đảm bảo một nền tảng quản lý khóa an toàn hơn việc sử dụng phần mềm

Nền tảng (Platform)	Solaris(Sparc), Linux, Window and VMware
Hệ điều hành hỗ trợ	- Windows 2003 R2 Service Pack 2 - Windows 2003 Service Pack 2 - Windows 2008 32 bit Service Pack 1 - Windows 2008 R2 64 bit Service Pack 1 - Sun SolarisTM 10 - Red Hat Enterprise Linux 5.5 32 bit - Red Hat Enterprise Linux 5.5 64 bit - SUSE Linux Enterprise Server 11 SP1 32 bit - SUSE Linux Enterprise Server 11 SP1 64 bit - VMware ESX Server 4.1

Yêu cầu bộ nhớ tối thiểu	- Windows: tối thiểu 1 GB RAM - Solaris: tối thiểu 512 RAM - Linux: tối thiểu 512 MB RAM
Yêu cầu ổ đĩa	- Windows NT: tối thiểu 250 MB - Solaris: tối thiểu 250 MB - Linux: tối thiểu 250 MB
Tốc độ CPU	- Windows NT: Intel Pentium IV 2.66 GHz hoặc hơn - Solaris: Sparcv9 1280MHz hoặc hơn - Linux: Intel Pentium IV 2.66 GHz hoặc hơn

Chuẩn chứng thư	X.509 v3 (including all standard extensions) - PKIX - SSL - S/MIME - IPSec - SET - Extended Validation
Chuẩn công nghiệp	Tuân thủ các chuẩn sau: - Common Criteria EAL4+ - Federal Bridge CA (FBCA) - IdenTrust Certification
Hỗ trợ thư mục	Hỗ trợ tich hợp và lưu trữ chứng thư trên LDAP theo chuẩn LDAP v2/v3 và X.500.

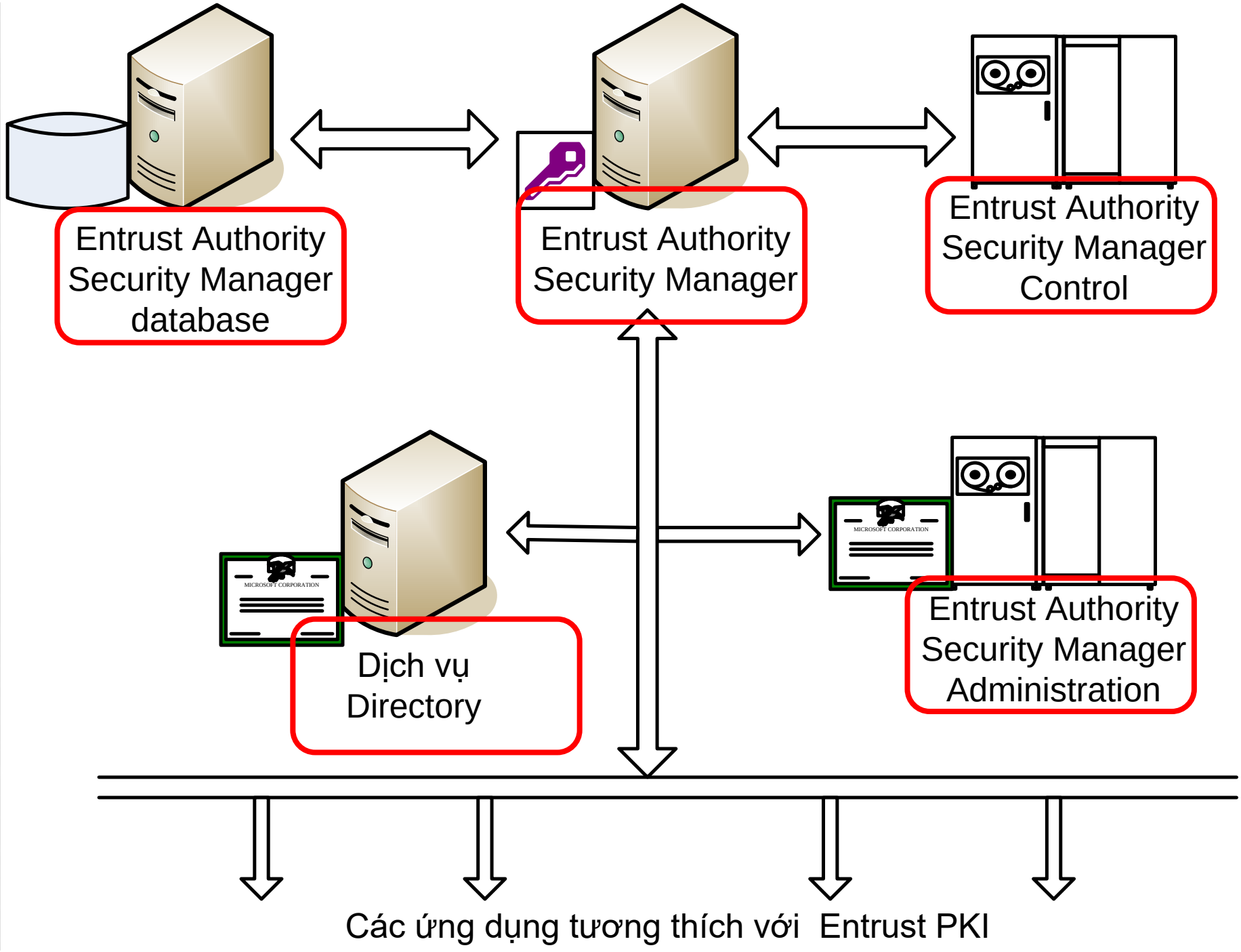
Các đặc tính PKI	- X.509 CRLs và CRLs với các tùy chọn mở rộng - Không giới hạn các Sub-CA bên dưới theo mô hình phân cấp (hierarchical PKIs)
Các đặc tính chứng thư số	- Chứng thư số theo chuẩn X.509 v1, v3 - Chứng thư số với chuẩn RSA, DSA và ECDSA - Linh hoạt trong các cấu hình DN cho chứng thư số - Chứng thư số S/MIME - Chứng thư số cho ký đối tượng (JavaApplet, ActiveX) - Các tùy chọn mở rộng phù hợp PKIX v3 - Tùy chọn mở rộng SET

Hỗ trợ các thuật toán	- RSA - DSA P-256, P-384, và P-521 - ECDSA - SHA-1 và SHA-2
Thiết bị mã hóa phần cứng	- Lưu trữ khóa bí mật của CA trên thiết bị phần cứng HSM - Việc lưu trữ/nhân bản khóa của CA dựa trên phần cứng với các thiết bị đáp ứng chuẩn PKCS#11. - Hỗ trợ các thiết bị lưu khóa theo chuẩn FIPS 140-1 level 1 tới 3 như: SafeNet, Thales, AEP và nhiều thiết bị hỗ trợ chuẩn PKCS#11.

- Tùy biến:
  - Giải pháp RSA gần như không cho phép khả năng tuỳ biến các thành phần của hệ thống như giao diện, chức năng.
  - Còn việc tuỳ biến thuật toán lại càng khó khăn hơn, vì đây là một sản phẩm thương mại nên mỗi lần tuỳ biến một thành phần là cả hệ thống cần đóng gọi lại

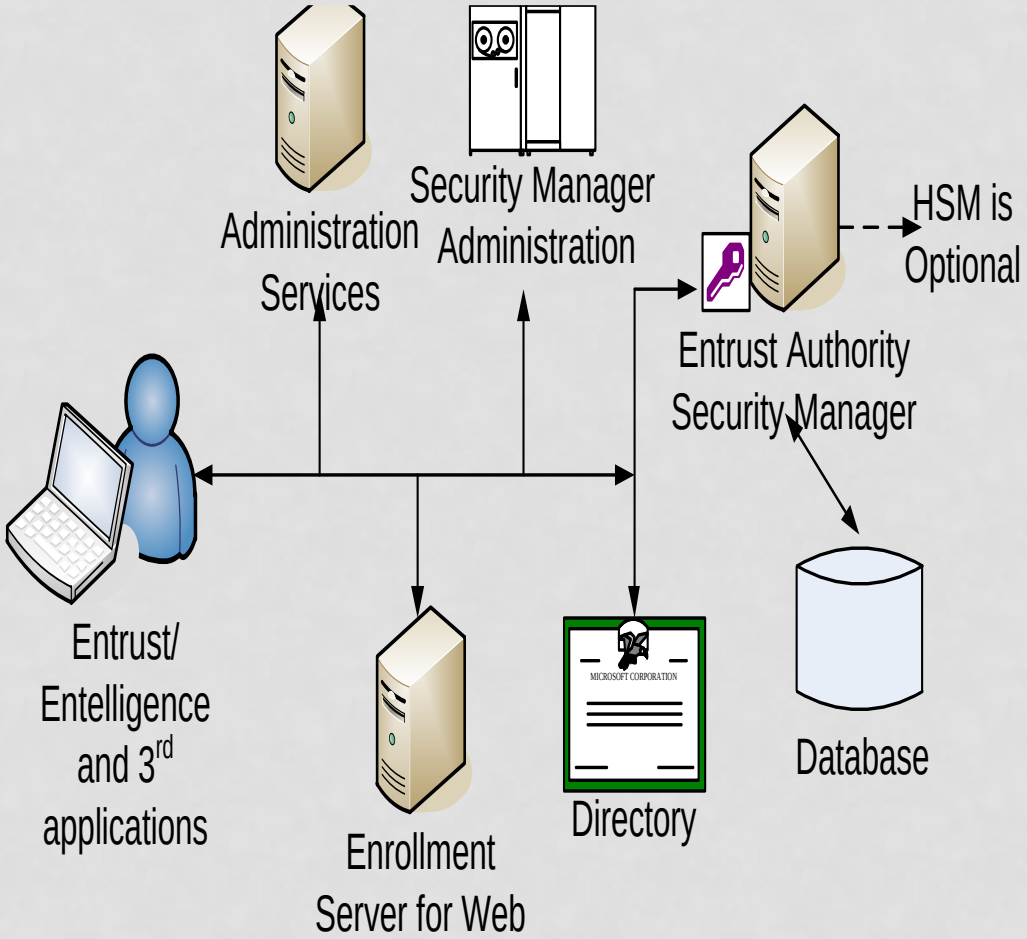
HỆ THỐNG MÃ ĐÓNG
GIẢI PHÁP CỦA ENTRUST

- Entrust PKI là một phần mềm PKI thương mại của hãng Entrust. Phần mềm Entrust PKI là một bộ các ứng dụng tương tác với nhau để tạo thành một giải pháp PKI cho tổ chức. Các ứng dụng chính của giải pháp Entrust PKI như sau:
  - Entrust Authority™ Security Manager
  - Entrust Authority™ Security Manager Control
  - Entrust Authority™ Security Manager Administration
  - Entrust Authority™ Security Manager database
  - Entrust Ready Directory


Entrust Authority Security Manager database
Entrust Authority Security Manager
Entrust Authority Security Manager Control
Dịch vụ Directory
Entrust Authority Security Manager Administration
Các ứng dụng tương thích với Entrust PKI

HỆ THỐNG MÃ ĐÓNG
GIẢI PHÁP CỦA ENTRUST

- Kiến trúc tổng thể của giải pháp Entrust PKI
  - Quản lý an ninh ủy quyền Entrust
  - Cơ sở dữ liệu
  - Thư mục lưu trữ
  - Quản trị an ninh an toàn
  - Dịch vụ quản trị ủy quyền Entrust
  - Các ứng dụng Entrust Entelligence

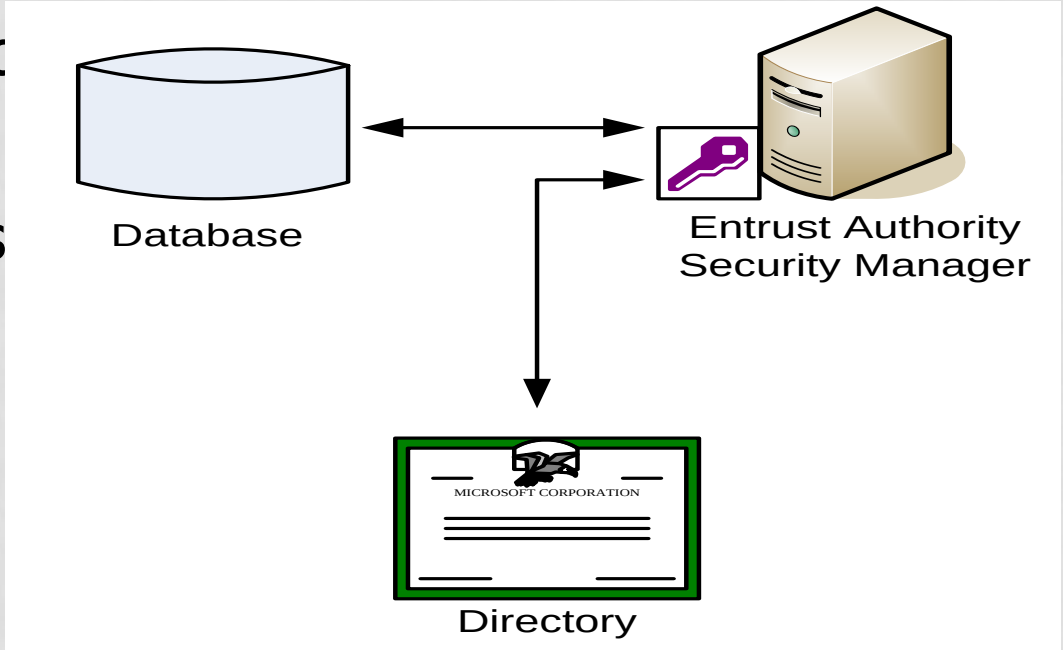


KIẾN TRÚC TỔNG THỂ CỦA GIẢI PHÁP ENTRUST PKI

- Thành phần quản lý an ninh ủy quyền Entrust
  - Cấp phát, quản lý các khóa và CTS của người dùng.
  - Quản lý vòng đời của các định danh số (khóa và chứng thư).
  - Cung cấp một giải pháp hoàn chỉnh dựa trên các định danh số (khóa và chứng thư) cho các dịch vụ xác thực, chữ ký số, và mã hóa.
  - Duy trì một cơ sở dữ liệu (Database) lịch sử sử dụng khóa/chứng thư số của người dùng để cho phép khôi phục lại khi người mất quyền truy nhập tới khóa của họ.
  - Duy trì các báo cáo và logs sự kiên đảm bảo có thể kiểm tra được tất cả các thao tác diễn ra trong hệ thống.

KIẾN TRÚC TỔNG THỂ CỦA GIẢI PHÁP ENTRUST PKI

- Cơ sở dữ liệu: lưu các thông tin
  - Thông tin trạng thái người dùng (bao gồm tên DN và các thông tin khác của người dùng).
  - Thông tin khóa và chứng thư số của mỗi người dùng.
  - Thông tin về người c
    Officer.
  - Thông tin về chính s
    mật
  - Thông tin thu hồi ch



KIẾN TRÚC TỔNG THỂ CỦA GIẢI PHÁP ENTRUST PKI

- Directory:
  - có thể tích hợp được với các dịch vụ thư mục tuân theo chuẩn X.500 như Critical Path, Microsoft AD, Sun Directory Server, IBM…
  - lưu trữ các thông tin sau:
    - Các chứng thư số của người dùng được cấp phát ra bởi hệ thống Entrust PKI
    - Danh sách các chứng thư số bị thu hồi.
    - Thông tin về chính sách các máy trạm

KIẾN TRÚC TỔNG THỂ CỦA GIẢI PHÁP ENTRUST PKI

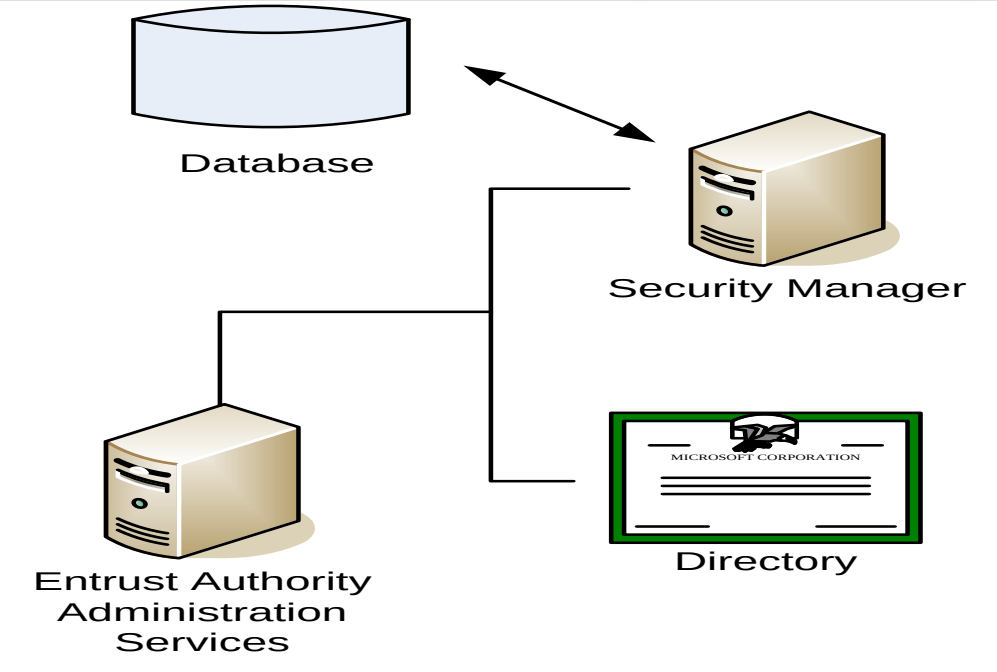
- Quản trị an ninh an toàn (SMA):
  - một giao diện GUI cho phép người quản trị có thể cấu hình và quản trị hệ thống Security Manager đơn giản
  - Giao tiếp giữa SMA với Security Manager sử dụng giao thức ASH (TCP/710)
  - Loại công việc:
    - Quản lý người dùng.
    - Quản lý cấp phát chứng thư.
    - Quản lý các chính sách bảo mật của hệ thống.
    - Thực hiện việc cấu hình chứng thực chéo với hệ thống CA khác.
    - Thiết lập kiến trúc hệ thống CA.

KIẾN TRÚC TỔNG THỂ CỦA GIẢI PHÁP ENTRUST PKI

- Các ứng dụng Entrust Entelligence :
  - tương tác với hệ thống quản lý an ninh để tự động trong quá trình quản lý khóa của người dùng
  - Xuất hiện trong các quá trình sau:
    - Tạo cặp khóa ký cho người dùng.
    - Trao đổi khóa giữa các người dùng thuộc các CA khác nhau mà không có sự tin tưởng chéo.
  - cho phép người dùng thực hiện các công việc sau:
    - Mã hóa và ký số lên dữ liệu
    - Mã hóa/giải mã dữ liệu và kiểm tra CKS trên các dữ liệu đã ký.
    - Xóa dữ liệu một cách an toàn

KIẾN TRÚC TỔNG THỂ CỦA GIẢI PHÁP ENTRUST PKI

- Dịch vụ quản trị ủy quyền Entrust:
  - cho phép người quản trị có thể quản trị hệ thống Entrust Authority Security Manager qua giao diện Web



THÀNH PHẦN CỦA GIẢI PHÁP ENTRUST PKI

- Quản lý an toàn ủy quyền Entrust
- Điều khiển quản lý an toàn ủy quyền Entrust
- Quản trị quản lý an toàn ủy quyền Entrust
- Cơ sở dữ liệu quản lý an ninh ủy quyền Entrust
- Entrust Ready Directory

THÀNH PHẦN CỦA GIẢI PHÁP ENTRUST PKI

- Quản lý an toàn ủy quyền Entrust
  - Đóng vai trò CA
  - Chức năng:
    - Tạo chứng thư số cho tất cả các khóa công khai (Public key).
    - Duy trì bảo mật cơ sở dữ liệu các thông tin của hệ thống Entrust PKI và cho phép khôi phục lại cặp khóa của người dùng (trong trường hợp họ bị mất password,…)
    - Áp đặt các chính sách của tổ chức vào hệ thống.

THÀNH PHẦN CỦA GIẢI PHÁP ENTRUST PKI

- Điều khiển quản lý an toàn ủy quyền Entrust
  - giao diện local cho phép truy cập trực tiếp vào hệ thống Security Manager
  - Chỉ người quản trị cao nhất của hệ thống có thể sử dụng công cụ này để truy cập vào Security Manager
  - Công việc:
    - Khởi động hoặc dừng dịch vụ Quản lý an ninh, an toàn
    - Khôi phục các cấu hình cho quản lý an ninh
    - Quản lý cơ sở dữ liệu của hệ thống

THÀNH PHẦN CỦA GIẢI PHÁP ENTRUST PKI

- Quản trị quản lý an toàn ủy quyền Entrust:
  - thành phần quản trị của hệ thống Entrust PKI.
  - sử dụng một giao diện đồ họa vào giao tiếp bảo mật với Security Manager
  - Công việc:
    - Quản lý người dùng
    - Quản lý chứng thư số của người dùng
    - Quản lý chính sách bảo mật được áp dụng cho hệ thống
    - Thực hiện cấu hình chứng thực chéo với hệ thống CA khác.
    - Thiết lập kiến trúc hệ thống CA

THÀNH PHẦN CỦA GIẢI PHÁP ENTRUST PKI

- Cơ sở dữ liệu quản lý an ninh ủy quyền Entrust:
  - thực hiện lưu trữ toàn bộ các thông tin liên quan tới hệ thống Entrust PKI
  - Các loại thông tin được lưu trữ :
    - Cặp khóa của CA (trường hợp không sử dụng thiết bị phần cứng để lưu khóa)
    - Thông tin trạng thái người dùng
    - Thông tin khóa và chứng thư của mỗi người dùng
    - Thông tin về người quản trị và Security Officer.
    - Thông tin về chính sách người dùng và chính sách bảo mật
    - Thông tin thu hồi chứng thư

THÀNH PHẦN CỦA GIẢI PHÁP ENTRUST PKI

- Entrust Ready Directory
  - Để cung cấp các thông tin về CTS được cấp phát bởi CA tới người dùng
  - Sử dụng dịch vụ thư mục đáp ứng chuẩn X.500 tương thích với giao thức LDAP
  - Các thông tin có thể được lưu trữ:
    - Các chứng thư số của người dùng được cấp phát ra bởi hệ thống Entrust PKI
    - Danh sách các chứng thư số bị thu hồi.
    - Thông tin về chính sách các máy trạm

CÔNG NGHỆ TRONG ENTRUST PKI

Quản lý an ninh Hệ điều hành	7.0	7.1
Windows	2000	2000, 2003
Solaris	7,8	8, 9
IBM AIX	5.1	5.1
HP-UX	11, 11i	11i
Các nền tảng nổi bật khác		
Microsoft Active Directory	2000, 2003	2000, 2003, ADAM
Các thư mục khác	CP 4.1, 4.2, Siemens 6, IBM DS 5.2, Sun ONE DS 5.1, 5.2	CP 4.2, Siemens 6, IBM DS 5.2, Sun ONE DS 5.2
Cơ sở dữ liệu	PostgreSQL, Informix 9.21, Oracle 8i, 9i	PostgreSQL, Informix 9.4, Oracle 9i
SafeNet/Chrysalis HSM	Luna CA3 & SA, nShield	Luna CA3 & SA, nShield
SMA tokens	PKCS#11v2**	PKCS#11v2

CHUẨN HỖ TRỢ TRONG ENTRUST PKI

Chuẩn	Mục đích
X.509	Định dạng chứng thư số
PKIX-CMP	Giao thức quản lý chứng thư
PKCS #7/10	Sử dụng trong quá trình đăng ký cấp phát chứng thư
PKCS#11	Chuẩn giao tiếp với các thiết bị mã hóa phần cứng
LDAP	Lightweight Directory Access Protocol
RFC 3039	Một loại định dạng chứng thư số
Cisco SCEP	Cisco Certificate Enrollment Protocol (cho giải pháp VPN của Cisco)
SPEKE	Một phương pháp mã hóa sử dụng trong xác thực p/w

CÁC THUẬT TOÁN ĐƯỢC SỬ DỤNG

Loại thuật toán	Giải thuật hỗ trợ
Mã hóa khoá đối xứng	DES, Triple-DES, CAST, RC4, IDEA, AES
Chữ ký số	RSA, DSA, ECDSA
Các hàm băm	SHA, MD5, RIPEMD-160
Trao đổi khóa	RSA key transfer, Diffie-Hellman, SPKM
Toàn vẹn khóa đối xứng	MAC, HMAC