



PKIMS

PKI Management System

www.summitthai.com

ระบบบริหารจัดการใบรับรองอิเล็กทรอนิกส์ (Enterprise Edition 1.1)



Public Key Infrastructure (PKI) เป็นเทคโนโลยีที่มีบทบาทสำคัญในการยืนยันความถูกต้อง และการรักษาความปลอดภัยของข้อมูลที่ใช้ในการทำธุรกรรมอิเล็กทรอนิกส์ระหว่างหน่วยงานต่างๆ ทั้งภาครัฐและเอกชน ตามที่ได้กำหนดไว้ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (แก้ไขเพิ่มเติม พ.ศ. 2551)

PKI Management System (Enterprise Edition) เป็นระบบบริหารจัดการใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ภายในองค์กร ที่สามารถบริหารจัดการใบรับรองอิเล็กทรอนิกส์สำหรับ บุคคล, Servers, ระบบงาน และ Hardware Security Module (HSM) แบบเบ็ดเสร็จในระบบเดียวกัน ในเรื่องของการลงทะเบียนขอออก, การต่ออายุและการเพิกถอน รวมไปถึงระบบอนุมัติในการออกใบรับรอง และการตรวจสอบสถานะภาพใบรับรองอิเล็กทรอนิกส์ สามารถทำงานร่วมกับ Certificate Authorities (CAs) ของ Microsoft ในลักษณะ Online หรือ Offline อีกทั้งการทำงานร่วมกับ Crypto Device ต่างๆ ได้โดยตรง เช่น PKI Smart Card, PKI USB Token, Personal Information File Exchange (PKCS #12) และ HSM รวมไปถึงการเตรียมระบบจัดเก็บ Audit Logs ของการใช้บริการและ Web Services ต่างๆ เพื่อประโยชน์ในการตรวจสอบภายหลัง

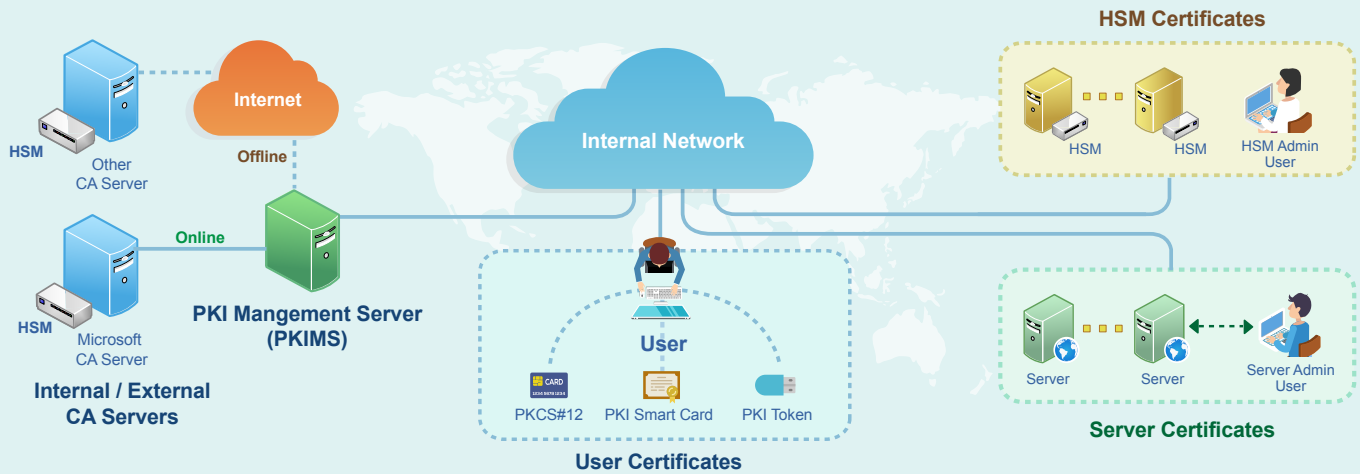
PKI Management System (Enterprise Edition) เป็น Web-based Application ที่ถูกพัฒนาขึ้นให้เป็นมาตรฐาน ที่สามารถติดตั้งบน UNIX หรือ Windows Environment โดยมีการทำงานและการจัดการข้อมูลอิงตามมาตรฐาน PKCS, S/MIME, SSL และ Digital Signature เป็นการสร้างความมั่นใจให้กับองค์กรได้ว่า ใบรับรองอิเล็กทรอนิกส์ ที่ออกให้กับบุคคล/พนักงาน, Servers, ระบบงาน และ HSMs ทั้งภายในและภายนอก สามารถนำไปใช้งานในการควบคุมความปลอดภัยของข้อมูลที่ต้องการทำธุรกรรมอิเล็กทรอนิกส์ระหว่างหน่วยงานต่างๆ ทั้งภาครัฐและเอกชน ตามที่ได้กำหนดไว้ในพระราชบัญญัติฯ ได้อย่างถูกต้องและมีประสิทธิภาพ



Benefits

- ❖ ลดความยุ่งยากในการเรียนรู้รายละเอียดของเทคโนโลยี ลดเวลาในการพัฒนาระบบงาน เนื่องจาก PKI Management System ได้เตรียม Functions ต่างๆ ไว้อย่างครบถ้วน
- ❖ เป็นศูนย์กลาง ในการจัดการใบรับรองอิเล็กทรอนิกส์ และ Digital ID เช่น ออกใหม่ ต่ออายุ เพิกถอน และการลงทะเบียนใบรับรองอิเล็กทรอนิกส์ที่มาจากระบบภายในและภายนอก รวมถึงการตรวจสอบความถูกต้องในการใช้งาน





Features

- Module การลงทะเบียนบุคคลที่ต้องการขอออก, การต่ออายุ และการเพิกถอนใบรับรองอิเล็กทรอนิกส์ของบุคคล, Servers, ระบบงาน และ HSM พร้อมระบบจัดเก็บเอกสารหลักฐานการลงทะเบียน
- Module การบริหารจัดการการอนุมัติคำขอใบรับรองอิเล็กทรอนิกส์ และระบบแจ้งผลระบบแจ้งผลการอนุมัติผ่านทาง e-Mail
- Module การสร้าง Certificate Service Request (CSR) จากข้อมูลการลงทะเบียนเพื่อจัดส่งให้ Certificate Authority (CA) ออกใบรับรองอิเล็กทรอนิกส์ พร้อมนำใบรับรองอิเล็กทรอนิกส์กลับมา Import ในระบบ
- Module การสร้าง Public/Private Key พร้อมทั้งการนำใบรับรองอิเล็กทรอนิกส์บันทึกลงใน PKI USB Token, PKI Smart Card และ Personal Information Exchange File (PKCS#12)
- Module การ Import และลงทะเบียนใบรับรองอิเล็กทรอนิกส์สำหรับ PKI USB Token, PKI Smart Card และ Personal Information Exchange File (PKCS#12) ที่ได้จากระบบอื่นๆ
- Module สำหรับ upload Certificate Service Request (CSR) จากเครื่อง Servers เพื่อจัดส่งให้ CA Server ภายในองค์กร ออกใบรับรองอิเล็กทรอนิกส์ หรือดำเนินการจัดหาจาก Certificate Provider ภายนอก นำกลับมา Import ในระบบเพื่อให้ผู้ใช้ Download และนำ Certificate ไปติดตั้งบนเครื่อง Server ที่ต้องการ
- Module สำหรับการเชื่อมต่อกับ HSM ขององค์กร (มาตรฐาน PKCS#11) เพื่อสร้าง Public/Private Keys และ Certificate Service Request (CSR) ของ HSM Certificate จัดส่งให้ CA Server ของภายในองค์กร ออกใบรับรองอิเล็กทรอนิกส์ หรือดำเนินการจัดหาจาก Certificate Provider ภายนอก และนำ HSM Certificate กลับมา Import ในระบบ PKIMS เพื่อบรรจุลงใน HSM โดยอัตโนมัติ
- สามารถเชื่อมต่อและทำงานร่วมกับ Certificate Authorities (CAs) ของ Microsoft ในลักษณะ Online หรือ Offline เพื่อการออก ต่ออายุ และเพิกถอนใบรับรองอิเล็กทรอนิกส์
- สามารถเชื่อมต่อและทำงานร่วมกับระบบ Certificate Authority Server (CA) อื่นๆ ได้ในลักษณะ Offline เพื่อการออก, ต่ออายุ และเพิกถอนใบรับรองอิเล็กทรอนิกส์
- สามารถเชื่อมต่อกับ ระบบ Microsoft AD ในการนำข้อมูลของผู้ใช้งานที่มีอยู่ มาเป็นส่วนหนึ่งของข้อมูลสำหรับใบรับรองอิเล็กทรอนิกส์ได้
- Module ในการแจ้งสถานะของใบรับรองอิเล็กทรอนิกส์สำหรับการขอ, การต่ออายุ, การเพิกถอน และการแจ้งเตือนต่ออายุใบรับรองอิเล็กทรอนิกส์
- Module การให้สิทธิ์หรือยกเลิกสิทธิ์ในการใช้ใบรับรองอิเล็กทรอนิกส์ของผู้ใช้ในระบบชั่วคราว ออกจาก Revocation List ของ Certificate Authority (CA)
- Module การสร้างรายการของใบรับรองอิเล็กทรอนิกส์ที่เพิกถอน เพื่อส่งให้ Certificate Authority (CA) สร้าง Certificate Revocation List (CRL)
- Module การบริหารจัดการ PKCS#12 File ให้สามารถจัดเก็บบน Thumb Drive และทำงานเป็นเสมือนหนึ่ง Virtual PKI USB Token ได้ โดยสามารถนำ Public/Private Keys และ Certificate โอนย้ายไปจัดเก็บอยู่ใน Security Zone ของเครื่องผู้ใช้งานชั่วคราวในขณะที่ใช้งาน และเมื่อมีการถึง Thumb drive ออก โปรแกรม Utility นี้ จะทำการลบ Keys/Certificate ใน Security Zone ของเครื่องผู้ใช้ออกโดยอัตโนมัติ
- มี Web Service ให้ Applications อื่นๆ เข้ามาเชื่อมต่อ เพื่อตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ว่าสามารถใช้งานในระยะเวลาที่อนุญาตได้หรือไม่ หรือมีการลงทะเบียนไว้ในระบบหรือไม่

Technical Specifications

Application Architecture

- J2EE Web Application
- Web Service

J2EE Application Server

- Tomcat
- Weblogic

Cryptographic Standard

- DES, 3-DES
- RSA Algorithm
- SHA-256

Cryptographic Device

- PKI Smart Card
- PKI Token
- Personal Information File Exchange (PKCS#12)

Web Browser

- Microsoft Internet Explorer

Operating System

- Microsoft Windows Server
- Unix (Solaris, Linux)

Database

- Microsoft SQL Server
- Oracle
- PostgreSQL



SUMMIT COMPUTER

12th Flr. CCT Bldg., 109 Surawong Rd. Suriyawong, Bangrak, Bangkok 10500 , Tel. 02-238-0895-9 , Fax. 02-236-7392

E-mail : summit@summitthai.com , Website : www.summitthai.com