

ลิขสิทธิ์ : กรมทางหลวงชนบท  
ปี : 2559  
ชื่อเรื่อง : พัฒนาระบบบริหารจัดการบุคลากรและระบบพิสูจน์ยืนยันตัวตน  
เมือง : กรุงเทพฯ  
ภาษา : ไทย  
สถานที่พิมพ์ : สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์  
นักวิจัย : ผู้ช่วยศาสตราจารย์ ดร. ทวีศักดิ์ กิจกาญจนารัตน์,  
อาจารย์ วชิรา พรหมสาขา ณ สกลนคร, รองศาสตราจารย์ ดร. สัญญา มิตรเอม,  
ผู้ช่วยศาสตราจารย์ ดร. จิรพล สังข์โพธิ์, อาจารย์ ดร. ศุภกิจ พุกขอรุณ  
บทคัดย่อ :

ระบบพิสูจน์ยืนยันตัวตนเป็นระบบพื้นฐานความปลอดภัยหลักของระบบเทคโนโลยีสารสนเทศทุก ระบบ เป็นระบบสำคัญที่มีความจำเป็นตามมาตรฐานความปลอดภัยทางด้านสารสนเทศ ไม่ว่าจะ เป็นความปลอดภัยในระดับโครงสร้างพื้นฐาน เช่นระบบเครือข่ายแบบมีสายและไร้สายไปจนถึงความปลอดภัยในการเข้า ใช้ระบบงานและการเข้าถึงข้อมูลต่าง ๆ ขององค์กร การใช้ระบบเทคโนโลยีสารสนเทศใด ๆ ก็ตาม องค์กรและ ผู้ใช้งานภายในองค์กรมีสิทธิและความรับผิดชอบต่อการใช้งานระบบเทคโนโลยีสารสนเทศตามนโยบายของ องค์กรและเป็นไปตามกฎหมายต่าง ๆ หลายฉบับ เช่น พ.ร.บ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ฯ พ.ร.บ. ว่าด้วยธุรกรรมอิเล็กทรอนิกส์ฯ เป็นต้น การพิสูจน์ยืนยันตัวตน การบันทึกข้อมูลการใช้งาน ตลอดจนจนถึงการ จัดเก็บข้อมูลอื่น ๆ ของผู้ใช้ เช่น ข้อมูลการจราจรทางคอมพิวเตอร์ เป็นส่วนหนึ่งของการปฏิบัติตามกฎหมาย ดังกล่าวข้างต้น

นอกจากกฎหมายหลัก ยังมีการร่างกฎหมายลูกอื่น ๆ ตามมา เช่น พระราชกฤษฎีกากำหนด วิธีการแบบ (มั่นคง) ปลอดภัย ในการประกอบธุรกรรมอิเล็กทรอนิกส์ ซึ่งมีการอ้างอิงเนื้อหา มาจาก มาตรฐานสากล ได้แก่ มาตรฐาน ISO/IEC 270001 ซึ่งเป็นแนวทางในการบริหารจัดการระบบความมั่นคง ปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ และเป็นส่วนหนึ่งของเกณฑ์การประเมินความเสี่ยงของหน่วยงาน ภาครัฐ ดังนั้น หลังจากร่างพระราชกฤษฎีกากำหนดวิธีการแบบ (มั่นคง) ปลอดภัย ในการประกอบธุรกรรม อิเล็กทรอนิกส์ ตามมาตรา 25 ของ พรบ.ว่าด้วยธุรกรรมอิเล็กทรอนิกส์ฯ มีผลบังคับใช้ก็จะหมายความว่าทุก องค์กรในประเทศไทยที่ประกอบธุรกรรมทางอิเล็กทรอนิกส์ ต้องนำเอามาตรฐาน ISO/IEC 27001 มา ประยุกต์ใช้ในองค์กรตามข้อกำหนดในพระราชกฤษฎีกาอย่างหลีกเลี่ยงไม่ได้ในที่สุด

การบริหารจัดการและพิสูจน์ยืนยันตัวตนผู้ใช้งานเป็นส่วนหนึ่งของข้อปฏิบัติที่กำหนดไว้ในมาตรฐาน ISO/IEC 27001 เป็นเทคโนโลยีพื้นฐานในการจัดทำโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI - Public Key Infrastructure) เพื่อรองรับลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) และ ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) หรือ CA (Certificate Authority) ซึ่งการพัฒนาหรือจัดทำระบบดังกล่าวมีความซับซ้อน เกี่ยวข้องกับหน่วยงานภายในและภายนอก อาจใช้เวลาและขั้นตอนในการพัฒนาเป็นระยะเวลาอันยาวนาน อีกทั้งการ แพร่หลายในการใช้งานอุปกรณ์สื่อสารเคลื่อนที่ซึ่งมีราคาถูกลงเทียบกับประสิทธิภาพที่เพิ่มมากขึ้นกว่าเดิมมาก

ทำให้อุปกรณ์เหล่านี้ได้รับความนิยมเพิ่มขึ้นเป็นจำนวนมาก ทำให้แนวโน้มการทำธุรกรรมทางอิเล็กทรอนิกส์ผ่านอุปกรณ์ดังกล่าวเป็นสิ่งปกติธรรมดาในชีวิตประจำวัน ทำให้องค์กรมีความท้าทายใหม่ในการบริหารจัดการอุปกรณ์สื่อสารเคลื่อนที่ภายในองค์กรเหล่านี้ ให้มีการใช้งานตามนโยบายการรักษาความมั่นคงปลอดภัยขององค์กร ลดความเสี่ยงและช่องโหว่ต่อภัยคุกคามใหม่ ตลอดจนการเผยแพร่ความรู้สำหรับบุคคลในองค์กรยังมีน้อยมาก จึงควรเป็นหน้าที่ขององค์กรที่จะให้การสนับสนุนและส่งเสริมการให้ความรู้ ความเข้าใจควบคู่กันไป เช่น จัดฝึกอบรมผู้บริหารระบบ จัดฝึกอบรมการใช้งานอุปกรณ์สื่อสารเคลื่อนที่ให้มีความปลอดภัยตามมาตรฐานและนโยบายขององค์กร จัดฝึกอบรมความรู้พื้นฐานทางด้าน PKI, Digital Certificate และ Digital Signature โดยเริ่มจากการอบรมความรู้พื้นฐานด้านการเข้ารหัสข้อมูลและการถอดรหัสข้อมูล ซึ่งเป็นความรู้พื้นฐานในการศึกษาเรื่อง PKI และ CA ต่อไป เป็นต้น

จากเหตุผลที่กล่าวมา ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมทางหลวงชนบท ได้เล็งเห็นถึงความสำคัญในการปรับปรุงระบบพิสูจน์ยืนยันตัวตนหรือที่เรียกว่าระบบ Directory Service เดิมที่กรมฯ มีใช้อยู่ให้ได้มาตรฐาน มีความสอดคล้อง รองรับต่อกฎหมายและนโยบายรัฐบาลที่เกี่ยวข้อง จึงได้ดำเนินการจ้างที่ปรึกษา สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์ เพื่อดำเนินโครงการพัฒนาระบบบริหารจัดการบุคลากรพิสูจน์ยืนยันตัวตน โดยกำหนดแนวทางในการปรับปรุงระบบย่อยต่าง ๆ เพิ่มเติม ซึ่งสามารถสรุปขอบเขตงาน ได้ดังต่อไปนี้

1. การปรับปรุงระบบ Directory Service เดิมให้มีประสิทธิภาพเพียงพอในการทำหน้าที่เป็นระบบศูนย์กลางในการพิสูจน์ยืนยันตัวตนจากระบบงานต่าง ๆ ของกรมทางหลวงชนบท
2. พัฒนาระบบต้นแบบในการเชื่อมโยงระบบงานขององค์กรเข้ากับฐานข้อมูลทะเบียนราษฎร
3. จัดเตรียมซอฟต์แวร์ที่ใช้ในการเชื่อมโยงระบบพิสูจน์ยืนยันตัวตนขององค์กรเข้ากับอุปกรณ์สื่อสารเคลื่อนที่ เพื่อให้สามารถบริหารจัดการอุปกรณ์สื่อสารเคลื่อนที่ภายในองค์กรได้อย่างมีประสิทธิภาพและเป็นไปตามมาตรฐานการรักษาความปลอดภัย
4. เริ่มทำการพัฒนาระบบพิสูจน์ยืนยันตัวตนให้เป็นระบบโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) โดยสมบูรณ์ เพื่อรองรับธุรกรรมทางอิเล็กทรอนิกส์
5. การจัดฝึกอบรมบุคลากร

**Copyright** : Department of Rural Roads  
**Year** : 2016  
**Title** : Development of Human Resource Management System and Authentication System  
**City** : Bangkok  
**Language** : Thai  
**Publisher** : Thammasat University Research and Consultancy Institute  
**Researcher** : Assistant Professor Dr. Taweesak Kijkanjanarat,  
Assoc. Prof. Dr. Sanya Mitaim, Assistant Professor Dr. Jirapon Sunkpho,  
Dr. Supakit Prueksaaron

**Abstract** :

Authentication or Identity verification system is the core basic security of the information technology system. The system is compliant with the information security standard. Whether the level of infrastructure such as networking, wired and wireless or the level of application and data. An organization and its users within the organization have the right and responsibility of using any provided information technology based on its own policies and the national laws of the various editions such as Computer-Related Crime Act B.E.2550 (2007), Electronic Transaction Act B.E. 2544 (2001), etc. User authentication and their usage logs including traffic log are indicated and enforced in those Laws.

User management and user identity verification are parts of the agreement, as defined in standard ISO / IEC 27001, which is the foundation for the preparation of a public key infrastructure (PKI) to support electronic signature (Digital Signature) and Digital certificate or CA (certificate Authority), developing or producing such systems are complex. and involved with internal and external agencies and take some times to improve. The widespread use of mobile devices, which are cheaper and more powerful than ever, make these devices increasing in popularity as well. The trend of electronic transactions through such devices are common in everyday life. This gives organizations the new challenges in the management of mobile devices within their organizations. An active policy of security of the organization, Reduce risk and vulnerability to new threats. As well as the dissemination of knowledge for people in the organization, which are very few. It should be the duty of the organization to support and promote education, making better understanding as trained administrator. Training in the use of mobile devices with safety standards and corporate policies. The training of basic knowledge of PKI, Digital Certificate

and Digital Signature. Training from Fundamentals to encrypt and decrypt data. These are the basic knowledge of PKI and CA's next and so on.

For the mentioned reasons, Information Technology and Telecommunication Center, Department of Rural Roads recognizes the importance of improving identity verification system, known as the Directory Service to the department's existing standards and consistency support for the law and government policy related. It has taken the organization to hire a consultant, Thammasat University Research and Consultancy Institute (TURAC), to develop the authentication management system and the guidelines for the various sub-systems, which scope can be described as the following

1. Improving the Directory Service System to be efficient enough to serve as a central hub to verify the identity from the various systems within the organization.

2. To develop a prototype system to link enterprise applications with the ID Card information from the Population Registration Database.

3. Preparing the software to be used to link the authentication system of the mobile devices, to be able to manage mobile devices in the enterprise, effectively and in compliance with security standards.

4. Start the development of the public key infrastructure (PKI) completely devoted to electronic transactions.

5. Training of personnel