บทคัดย่อ

ในการทำธุรกรรมผ่านเครือข่ายอินเทอร์เน็ต การลงลายมือชื่อตามปรกติเป็นสิ่งที่ไม่สามารถทำได้และจำเป็นต้องอาศัยการใช้ "ลายมือชื่ออิเล็กทรอนิกส์" (electronic signature) ซึ่งได้รับการรับรองความถูกต้องจากองค์กรออกใบรับรอง (certification authority) อย่างไรก็ตามในปัจจุบันประเทศไทยยังไม่มีหน่วยงานดังกล่าว

ผู้วิจัยเสนอให้ภาคเอกชนเป็นผู้ดำเนินการให้บริการในการออกใบรับรอง และให้รัฐเป็นผู้กำกับดูแลการให้บริการดังกล่าวและเสนอแนวคิดในการออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์เพื่อรองรับการใช้เทคโนโลยีลายมือชื่ออิเล็กทรอนิกส์ใน 4 ประเด็นคือ ให้ออกกฎหมายที่มีความเป็นกลางทางเทคโนโลยี (technology neutral) ซึ่งเปิดให้กลไกตลาดสามารถเลือกเทคโนโลยีที่เหมาะสม ให้ระบบการขออนุญาตจัดตั้งหน่วยงานออกใบรับรองเป็นระบบใบอนุญาตแบบอัตโนมัติ ซึ่งผู้ประกอบการที่มีคุณสมบัติสอดคล้องกับเงื่อนไขที่กำหนดสามารถขอประกอบการได้ทันที ให้รับรองลายมือชื่ออิเล็กทรอนิกส์ที่ออกในต่างประเทศเหมือนลายมือชื่อที่ออกในประเทศไทย และให้มีการกำหนดความรับผิดชอบ (liability) สูงสุดของหน่วยงานออกใบรับรองเพื่อส่งเสริมธุรกิจดังกล่าวในระยะเริ่มต้น

ต่อประเด็นนโยบายเทคโนโลยีการเข้ารหัสเพื่อรักษาความลับของข้อมูล (encryption policy) ผู้วิจัยเสนอให้ออกกฎหมายให้รัฐสามารถใช้สิทธิในการถอดรหัสข้อมูลดังกล่าวได้ในกรณีที่การใช้ข้อมูลนั้นอาจมีผลต่อความมั่นคงของชาติ อย่างไรก็ตามการใช้อำนาจดังกล่าวจะต้องมีกลไกถ่วงดุลไว้เช่น ให้ทำได้โดยอาศัยอำนาจของศาลเท่านั้น เป็นต้น

Abstract

Electronic signature is necessary for identity authentication in online transactions. To ensure a secure signature system, a trusted third party is required. Such entity is called a "certification authority" (CA). Currently, there is no CA operating in Thailand. While it is often argued that the government should play a leading role in setting up a CA, we found no market failure and proposed that the private sector, not the government, should operate a CA. The government should play only a regulatory role if the industry is in need of regulation.

We also lay down a guideline for drafting an electronic signature law, which includes four important principles. Firstly, the law should be technological neutral in order to avoid distorting market decisions. Secondly, the licensing scheme, if required by the law, should be an automatic one. Thirdly, the law should recognize signatures issued by foreign CAs. Finally, liabilities of licensed CAs may be capped to promote the industry in its infancy.

Concerning encryption policy, we argued that no import nor export control of encryption technology is necessary. However, security needs may provide a rationale for state control of the technology. In that case, a balance should be strike between security and civic liberty. State access to secret signature keys should be allowed on a condition that such action is warranted by court order.