# ภาคผนวก จ.
# ความมั่นคงและความปลอดภัยในระบบเครือข่าย

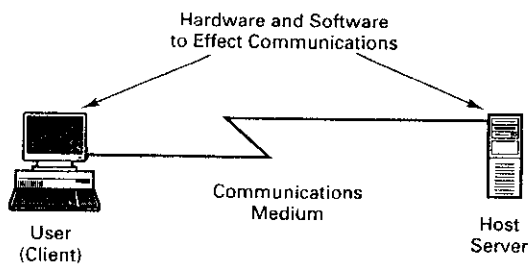
1. **แนวคิดพื้นฐานของระบบเครือข่าย**
2. **การคุกคามต่อระบบเครือข่าย**
   2.1 ประเด็นพิจารณาเกี่ยวกับความมั่นคงในระบบเครือข่าย
   2.2 การวิเคราะห์การคุกคามความมั่นคง
3. **การคุกคามความมั่นคงของเครือข่าย**
   3.1 การเข้ารหัสลับ (Encryption)
   3.2 การควบคุมการเข้าถึง (Access control)
   3.3 การระบุตัวตน (Authentication)
   3.4 บูรณภาพของข้อมูล (Message integrity)
4. **Firewall**
   4.1 ตัวกลั่นกรองเส้นทาง (Screening routers)
   4.2 Proxy gateway
   4.3 Guard
5. **ความปลอดภัยกับพานิชย์อิเล็คทรอนิกส์** (Electronic commerce)
6. **คำศัพท์**

# ภาคผนวก จ.
# ความมั่นคงและความปลอดภัยในระบบเครือข่าย

ถึงแม้ว่าในความเป็นจริงแล้ว การแยกนโยบาย กับกลไก การทำงาน เป็นหลักการที่สำคัญในเรื่องของความมั่นคงและความปลอดภัยก็ตาม แต่ในบทนี้จำเป็นต้องเชื่อมโยงระหว่างนโยบายกับการคุกคามต่อเทคโนโลยีเฉพาะ เพราะการคุกคามต่อระบบเครือข่ายนั้นเกิดขึ้นในจุดที่แตกต่างกัน บนพื้นฐานทางเทคโนโลยีที่แตกต่างกันด้วย การควบคุมที่เกิดขึ้นจึงต้องสัมพันธ์กับเทคโนโลยีนั้นๆ (อย่างไรก็ตาม เนื้อหาในบทนี้เป็นเพียงส่วนหนึ่งของการบริหารการจัดการศูนย์คอมพิวเตอร์ ดังนั้นจึงเป็นเพียงบริบทกว้างๆ เท่านั้น รายละเอียดควรศึกษาจากหนังสือที่เกี่ยวกับความมั่นคงและความปลอดภัยโดยเฉพาะ)

## 1. แนวคิดพื้นฐานของระบบเครือข่าย

เครือข่าย (Network) คือ อุปกรณ์ 2 ชิ้นขึ้นไป เชื่อมต่อผ่านสื่อรูปแบบต่างๆ โดยมีฮาร์ดแวร์และซอฟต์แวร์ ที่ทำให้การสื่อสารสมบูรณ์ ดังรูป จ.1




**รูป จ.1 รูปแบบเครือข่ายพื้นฐาน**

ในบางกรณี อุปกรณ์ด้านหนึ่งจะเป็นเครื่องคอมพิวเตอร์ (ซึ่งเรียก เครื่องให้บริการ (Server) ส่วนอุปกรณ์อีกด้านหนึ่งจะเป็นอุปกรณ์นำเข้า/นำออก (ซึ่งเรียก เครื่องรับบริการ (Client) เครื่องรับบริการขั้นต่ำสุดจะเป็นแผงแป้นอักขระเพื่อนำเข้าข้อมูล และหน้าจอสำหรับ

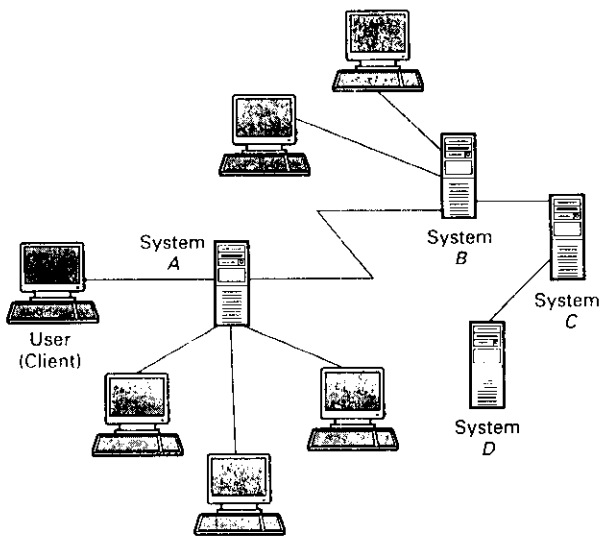
นำออกข้อมูล รูป จ.1 เป็นเพียงรูปที่สื่อตามคำจำกัดความเท่านั้น แต่ในความเป็นจริงระบบเครือข่ายจะมีความซับซ้อน โดย

- อุปกรณ์นำเข้า/นำออก มักจะเป็นเครื่องไมโครคอมพิวเตอร์ หรือ สถานีงาน ซึ่งจะทำให้เครื่องรับบริการมีพื้นที่หน่วยเก็บ และมีความสามารถในการประมวลผลสูงขึ้น

- ระบบเครือข่ายโดยปกติไม่ได้มีเครื่องให้บริการ 1 เครื่อง ต่อเชื่อมกับเครื่องรับบริการ 1 เครื่อง แต่จะเป็น เครื่องให้บริการหลายเครื่อง เชื่อมต่อกับเครื่องรับบริการหลายเครื่องเช่นกัน

- ผู้ใช้ในระบบไม่ได้ตระหนักว่าในขณะที่ใช้งานนั้น มีการสื่อสารข้อมูลจากผู้ใช้มากมายเกิดขึ้นในระบบ

ระบบเครือข่ายที่เกิดขึ้นโดยทั่วไป ดังรูป จ.2




**รูป จ.2 ระบบเครือข่ายทั่วไปที่มีความซับซ้อน**

การสื่อสารที่เกิดขึ้นนั้น ข้อมูลจะเดินทางผ่านสื่อรูปแบบต่างๆ ได้แก่ สายลวดเกลียวคู่ (Twisted pair) สายลวด Coaxial (Coax) ใยแก้วนำแสง (Optical fiber) หรือ คลื่นไมโครเวฟ ดาวเทียม

การสื่อสารระหว่างอุปกรณ์ที่มีความแตกต่างกัน จึงต้องกำหนดรูปแบบข้อตกลงในการติดต่อสื่อสารที่เรียกว่า โพรโทคอล (Protocol) ได้แก่ การเชื่อมต่อระหว่างระบบเปิด หรือ โอเอสไอ (Open system interconnection, OSI) โพรโทคอลควบคุมการส่งผ่าน และ โพรโทคอล

อินเทอร์เน็ต (Transmission Control Protocol and Internet Protocol, TCP/IP)

รูปแบบในการเชื่อมต่ออุปกรณ์ หรือ Topology พื้นฐาน ได้แก่ เครือข่ายแบบบัส (Bus) แบบวงแหวน (Ring) และแบบดาว (Star) รูปแบบการเชื่อมต่อนี้มีผลต่อความมั่นคง และความปลอดภัยของระบบเครือข่าย ระบบเครือข่ายที่ใหญ่ที่สุดและเป็นที่รู้จักกันดีคือ อินเทอร์เน็ต ซึ่งเป็นการเชื่อมต่อเครือข่ายต่างๆ รอบโลกเข้าด้วยกัน อินเตอร์เน็ตอาศัยพื้นฐานเทคโนโลยีแบบระบบรับ/ให้บริการ (Client/Server system) สามารถใช้ในการสื่อสารข้อมูลทั้งภายใน และภายนอกองค์กร องค์ประกอบของเครื่องให้บริการอินเตอร์เน็ต ดังรูป ข.3

การเชื่อมต่อเข้ากับอินเทอร์เน็ต หรือ การส่งผ่านข้อมูลผ่านเครือข่ายภายใน และเครือข่ายภายนอก ต้องมีการรักษาความปลอดภัยเป็นพิเศษ

3.4 **บูรณภาพของข้อมูล** (Message integrity)

คือความสามารถที่ทำให้เกิดความแน่ใจว่าข้อมูลที่มีการส่งไปนั้นไม่ถูกทำลายหรือ ถูกเปลี่ยนแปลง

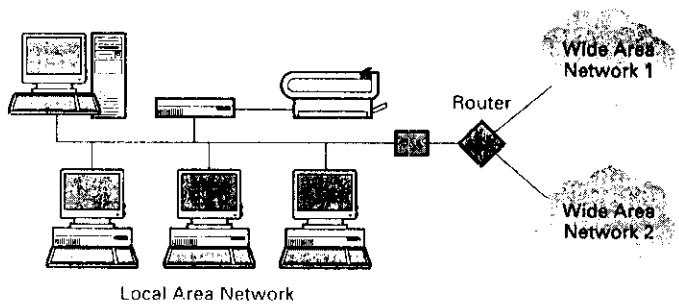
## 4. Firewall

Firewall เป็นระบบรักษาความปลอดภัย ประกอบด้วยฮาร์ดแวร์ และ ซอฟต์แวร์ที่กั้นระหว่างเครือข่ายภายในองค์กร และเครือข่ายภายนอก วัตถุประสงค์ของ Firewall คือ กั้นสิ่งไม่ดีทั้งหลายให้อยู่ภายนอกสภาพแวดล้อมที่ปกป้องไว้ ป้องกันเครือข่ายส่วนตัวจากผู้บุกรุกภายนอก โดยการทำงานของ Firewall อาจเป็นการป้องกันการเข้าถึงจากภายนอก (แต่ยินยอมให้เกิดการผ่านจากภายในไปสู่ภายนอก) หรือ ยินยอมให้เข้าถึงเฉพาะจากตำแหน่งที่กำหนด หรือจากผู้ใช้ที่กำหนด หรือจากกิจกรรมที่กำหนด

รูปแบบการรักษาความปลอดภัยที่เรียกว่าเป็น Firewall ได้แก่

4.1 **ตัวกลั่นกรองเส้นทาง** (Screening routers)

เป็นรูปแบบที่ง่ายที่สุด และในบางสถานการณ์ รูปแบบนี้จะมีประสิทธิภาพสูงสุด การทำงานของตัวกลั่นกรองเส้นทาง คือ เครื่องแม่ข่ายจะไม่ติดต่อโดยตรงกับเครือข่ายระยะไกล แต่จะเชื่อมต่อกับตัวจัดเส้นทาง (Router) ซึ่งเป็นคอมพิวเตอร์ที่จัดเส้นทางการสื่อสารไปยังเป้าหมาย ตัวจัดเส้นทางจะรับกลุ่ม (Packet) ข้อมูล แต่ละกลุ่ม พิจารณาตารางเส้นทาง แล้วส่งผ่านกลุ่มข้อมูลไปยังช่องทางต่างๆ ซึ่งจะรับและส่งไปยังจุดหมายปลายทาง ดังรูป จ.10




**รูป จ.10 ตัวจัดเส้นทางเชื่อมเครือข่ายเฉพาะที่เข้ากับ 2 เครือข่ายระยะไกล**

4.2 **Proxy gateway**

ในรูปแบบแรก ตัวกลั่นกรองเส้นทางจะพิจารณาเฉพาะส่วนแรก หรือ ส่วนหัวของกลุ่มข้อมูลเท่านั้น แต่ไม่ได้พิจารณาภายในกลุ่มข้อมูล ดังนั้น ตัวกลั่นกรองเส้นทางจะส่งผ่านอะไรก็ตามไปยังช่องทางที่กำหนด โดยยึดกฎเกณฑ์ว่ายินยอมให้ภายในเชื่อมต่อไปยังช่องทางนั้นๆ ในรูปแบบที่ 2 Proxy gateway เป็น Firewall ที่จำลองผลกระทบของงานประยุกต์ เพื่อที่งานประยุกต์จะรับเฉพาะสิ่งที่ถูกต้อง

Proxy gateway ทำงานเป็นงานประยุกต์เทียม เช่น เมื่อมีการส่งไปรษณีย์อิเล็กทรอนิกส์ มีกระบวนการส่ง และกระบวนการรับ สื่อสารกันโดยโพรโทคอลที่กำหนดกฎเกณฑ์ในการส่งผ่านไปรษณีย์ แล้วจึงส่งผ่านข้อความ Proxy gateway จะบุกรุกไปที่ส่วนกลางของโพรโทคอลการแลกเปลี่ยน เป็นเสมือนจุดหมายปลายทางโดยผู้ส่งอยู่ภายนอก Firewall และเป็นเสมือนผู้ส่งของการสื่อสารโดยมีจุดหมายปลายทางที่แท้จริงอยู่ภายใน Proxy ในส่วนกลางจะทำหน้าที่กลั่นกรองไปรษณีย์ที่มีการส่งผ่าน ให้แน่ใจว่ามีเฉพาะส่วนที่ยอมรับให้การยินยอมเท่านั้นที่ผ่านไปที่จุดหมายปลายทาง ความแตกต่างของ Proxy gateway กับตัวกลั่นกรองเส้นทาง คือ Proxy จะตีความโพรโทคอลไปยังงานประยุกต์ เพื่อควบคุมการทำงานผ่าน Firewall โดยอาศัยพื้นฐานว่าทุกอย่างในโพรโทคอลต้องโปร่งใส ไม่ใช่เฉพาะส่วนหัวของข้อมูลเท่านั้น

4.3 **Guard**

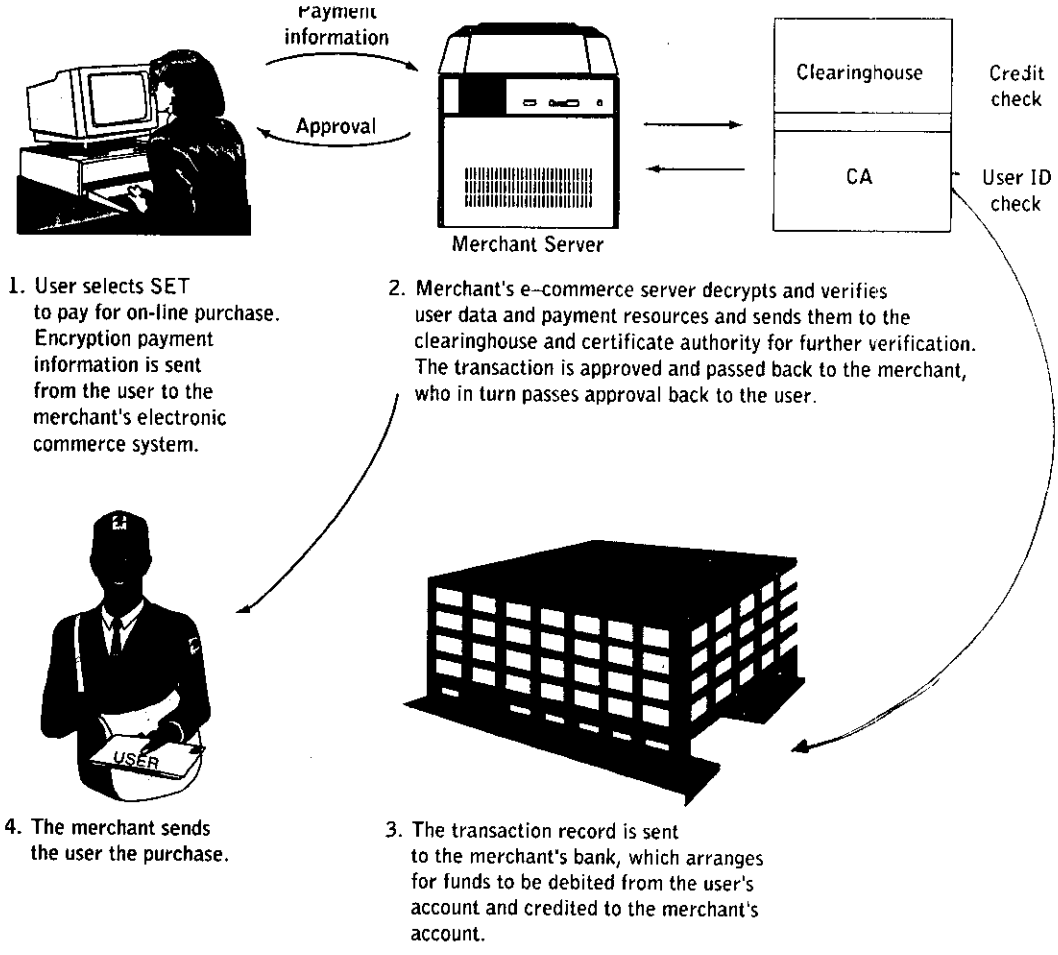
Guard เป็น Proxy firewall ที่ซับซ้อน โดย guard จะรับข้อมูลโพรโทคอล ตีความและส่งผ่านข้อมูลโพรโทคอลเดิม หรือ ที่แตกต่าง ซึ่งอาจให้ผลในรูปแบบเดิม หรือให้ผลที่แตกต่างออกไป Guard จะทำหน้าที่ตัดสินใจว่าบริการใดที่จะดำเนินการ

## 5. การรักษาความปลอดภัยกับพานิชย์อิเล็กทรอนิกส์ (Electronic commerce)

เทคโนโลยีความก้าวหน้าในการติดต่อสื่อสาร ทำให้เครือข่ายสื่อสารถูกนำมาใช้เป็นประโยชน์กับธุรกิจ เป็นการค้าทางอิเล็กทรอนิกส์ สิ่งสำคัญสำหรับพานิชย์อิเล็กทรอนิกส์ คือ ขั้นตอนการชำระเงิน เพราะจะต้องมีระบบรักษาความปลอดภัยในการชำระเงิน ซึ่งได้มีการพัฒนาระบบชำระเงินอิเล็กทรอนิกส์เป็นพิเศษ โดยบริษัทที่ดำเนินธุรกิจบัตรเครดิตทั้งหลาย ได้แก่ VISA International, MasterCard International, American Express และธนาคารต่างๆ ระบบการรักษาความปลอดภัยดังกล่าว เช่น

1. **Secure Electronic Transaction (SET)** เป็นโพรโทคอลสำหรับเข้ารหัสข้อมูลการ

ชำระเงินด้วยบัตรเครดิตผ่านเครือข่ายอินเทอร์เน็ต และเครือข่ายเปิดอื่นๆ ขั้นตอนการใช้งานนั้น ผู้ใช้จะได้รับใบรับรองดิจิทัล และกระเป๋าเงินดิจิทัล จากธนาคารที่ผู้ใช้ใช้บริการ ซึ่งจะทำหน้าที่เป็นเสมือนตัวกลางสำหรับธุรกรรมพานิชย์อิเล็กทรอนิกส์ โดยกระเป๋าเงินและใบรับรองที่ได้รับจากธนาคารนั้นจะเป็นตัวที่ระบุผู้ใช้ และบัตรเครดิตที่ใช้ เมื่อผู้ใช้ซื้อของจาก Web site และเลือกใช้วิธีการจ่ายเงินระบบ SET เครื่องให้บริการของผู้ขายจะส่งสัญญาณผ่านทางอินเทอร์เน็ตไปยังกระเป๋าดิจิทัลของผู้ใช้ จากนั้นกระเป๋าดิจิทัลจะเข้ารหัสข้อมูลการจ่ายเงิน และส่งข้อมูลไปยังผู้ขาย ผู้ขายจะทำการตรวจสอบว่าข้อมูลนั้นเป็นกลุ่มข้อมูล SET หรือไม่ แล้วใส่ใบรับรองดิจิทัลเข้าไปที่ข้อความ ทำการเข้ารหัส แล้วส่งข้อมูลไปยังสำนักหักบัญชี และผู้ออกใบรับรองเพื่อตรวจสอบข้อมูล สำนักหักบัญชีเป็นผู้ให้การยอมรับหรือปฏิเสธธุรกรรมนั้นๆ ตามสถานะเครดิตของผู้ซื้อ สำนักหักบัญชีส่งข้อมูลผ่านอินเทอร์เน็ตไปยังผู้ขาย และกลับไปที่กระเป๋าเดินทางของผู้ใช้ ธุรกรรมนี้จะถูกส่งไปที่ธนาคารของผู้ขาย ซึ่งจะจัดการโอนเงินจากผู้ซื้อไปยังผู้ขาย ดังรูป จ.11




**รูป จ.11 ขั้นตอนการทำงานของ SET**

อธิบายขั้นตอนการทำงาน

1. เมื่อผู้ใช้เลือกวิธีการจ่ายเงินแบบ SET สำหรับการซื้อในระบบเชื่อมตรง (On-line) ผู้ใช้จะส่งข้อมูลการจ่ายเงินที่เข้ารหัสแล้วไปยังระบบพานิชย์อิเล็กทรอกนิกส์ของผู้ขาย
2. เครื่องให้บริการพานิชย์อิเล็กทรอนิกส์ของผู้ขายจะถอดรหัสข้อมูล ตรวจสอบข้อมูลและการจ่ายเงินของผู้ใช้ แล้วส่งไปยังสำนักหักบัญชี เพื่อตรวจสอบขั้นต่อไป ธุรกรรมที่ได้รับการยินยอมแล้วจะถูกส่งกลับไปยังผู้ขาย ซึ่งจะเป็นผู้ส่งการยินยอมไปที่ผู้ซื้อ
3. ข้อมูลธุรกรรมจะถูกส่งไปยังธนาคารที่ผู้ขายใช้บริการ ธนาคารจะเป็นผู้ที่จัดการโอนเงินจากบัญชีของผู้ซื้อไปยังบัญชีผู้ขาย
4. ผู้ขายจัดส่งให้ผู้ซื้อ

2. **CyberCash/Checkfree Wallet** รูปแบบนี้จะไม่ใช้ซอฟต์แวร์ของลูกค้าเพื่อเข้ารหัสส่งต่อธุรกรรม และข้อมูลบัตรเครดิต ผ่านทาง Web site ไปยังผู้ขายสินค้าบนเครือข่าย แต่ผู้ขายจะเป็นผู้ส่งข้อมูลไปยังเครื่องให้บริการ CyberCash เครื่องให้บริการจะเก็บข้อมูลไว้ภายใต้กำแพงไฟ (Firewall) ทำการถอดรหัส แล้วส่งไปยังธนาคารที่ผู้ขายใช้บริการ ธนาคารจะส่งการร้องขอเป็นผู้มีสิทธิ ไปยังธนาคารที่ออกบัตรเครดิต เมื่อธนาคารที่ออกบัตรเครดิตตรวจสอบข้อมูลและให้การยินยอม หรือปฏิเสธการจ่ายเงิน ธนาคารที่ออกบัตรเครดิตจะส่งข้อมูลดังกล่าวไปยัง CyberCash CyberCash รับข้อมูลและส่งกลับไปยังผู้ขาย กระบวนการดังกล่าวหลีกเลี่ยงมิให้ผู้ขายรู้และเก็บหมายเลขบัตรเครดิตของลูกค้า ซึ่งช่วยเพิ่มระดับความปลอดภัยของระบบให้สูงขึ้น

3. **E-cash หรือ Electronic cash** Electronic cash เป็นเงินตราในรูปแบบอิเล็กทรอนิกส์ที่เคลื่อนไหวอยู่นอกเครือข่ายเงินตราปกติ (เครือข่ายเงินตราปกติ ได้แก่ ธนบัตร เหรียญ เช็ค บัตรเครดิต) เป็นเงินตราที่ไม่ได้อยู่ในบทบัญญัติของ Federal Reserve System (เป็นระบบการธนาคารของสหรัฐอเมริกา) ผู้ใช้จะได้รับซอฟต์แวร์ตัวรับบริการ และสามารถแลกเปลี่ยนเงินกับผู้ใช้ E-cash อื่นๆ ผ่านเครือข่ายอินเทอร์เน็ต เมื่อมีลูกค้าซื้อสินค้าในระบบเชื่อมตรง E-cash ซอฟต์แวร์จะสร้างเงินในปริมาณที่ผู้ใช้ระบุ และใส่ซองเสมือนส่งไปยังธนาคาร ธนาคารที่รับซองเสมือนก็จะถอนจำนวนเงินตามที่ระบุจากบัญชีของลูกค้า ปิดแสตมป์บนซองเพื่อยืนยันมูลค่าจำนวนเงิน และส่งกลับไปยังผู้ใช้ เมื่อผู้ใช้รับซองกลับไป ก็จะสามารถใช้จำนวนเงินนั้นได้

3. **Virtual PIN** First Virtual Internet Payment System เป็นระบบที่ใช้แนวคิดต่างจากแนวคิดอื่นๆ เพราะระบบนี้จะหลีกเลี่ยงการสร้างระบบความปลอดภัยในการส่งข้อมูลผ่าน

เครือข่ายอินเทอร์เน็ตโดยสิ้นเชิง แต่จะให้ลูกค้าขอหมายเลขระบุบุคคล ซึ่งเป็นหมายเลขเฉพาะแต่ละบุคคล เรียกว่า VirtualPIN หมายเลขเฉพาะ หรือ VirtualPIN นี้สามารถใช้กับ Site ใดก็ได้ VirtualPIN จะถูกเก็บไว้กับหมายเลขบัตรเครดิตในคอมพิวเตอร์ที่ไม่ได้ต่อผ่านเครือข่ายหรือต่อแบบเชื่อมตรง และมีเฉพาะ First Virtual เท่านั้นที่สามารถเข้าถึงข้อมูลได้ เมื่อลูกค้ามีการซื้อสินค้าผ่านทางอินเทอร์เน็ต จะมีเฉพาะ VirtualPIN ของลูกค้าเท่านั้นที่เดินทางอยู่ในเครือข่าย ในการชำระเงิน ผู้ขายจะส่ง VirtualPIN ของผู้ขายพร้อมกับ VirtualPIN ของผู้ซื้อไปยัง First Virtual จากนั้น First Virtual จะส่งไปรษณีย์อิเล็กทรอนิกส์ไปยังลูกค้าเพื่อยืนยันการขาย ถ้าลูกค้าให้การยอมรับธุรกรรมนั้น First Virtual ก็จะประมวลผลธุรกรรม และยืนยันไปยังผู้ขาย ผู้ขายจึงจะจัดส่งสินค้าไปยังผู้ซื้อ

5. **NetCheck** เป็นระบบการชำระเงินที่ใช้เช็คอิเล็กทรอนิกส์ โดยเช็คเหล่านี้จะผ่านการเข้ารหัสพร้อมลายเซ็นที่สามารถตรวจสอบได้ และใช้สำหรับการชำระเงินในพานิชย์อิเล็กทรอนิกส์

## 6. คำศัพท์

Access control
Authentication
Automatic call – back
Ciphertext
Client
Cybercash
Decryption
E – cash
Electronic commerce
Encryption
End – to – End encryption
Firewall
Guard
Link encryption
Plaintext
Port protection
Private key
Protocol
Proxy gateway
Public key
Server
SET
TCP/IP