

### เอกสารอ้างอิง(ฉบับที่ 3)

#### mCoupons: An Application for Near Field Communication (NFC)

#### mCoupon แอปพลิเคชันสำหรับNFC

##### บทคัดย่อ

NFC เป็นเทคโนโลยีการสื่อสารไร้สายระยะสั้น มันเป็นความสะดวกสบายมากสำหรับผู้ใช้ในการสื่อสาร โดยเริ่มต้นไม่ต้องมีการกำหนดค่าใด ๆ เมื่อนำอุปกรณ์ทั้งสองมาชิดติดกัน คุณสมบัตินี้ทำให้มาตรฐานดี เหมาะสำหรับใช้กับ mobile coupons ในปัจจุบัน คูปองเป็นวิธีที่ใช้กันมากสำหรับ บริษัท ที่จะส่งเสริมผลิตภัณฑ์หรือบริการ คูปองเหล่านี้จะสามารถใช้ได้ทั้งคูปองกระดาษหรือคูปองอิเล็กทรอนิกส์ (ซึ่งตัวอย่างที่ใช้ในเว็บ) เราได้นำเสนอรูปแบบใหม่ของคูปอง เรียกว่า mCoupons

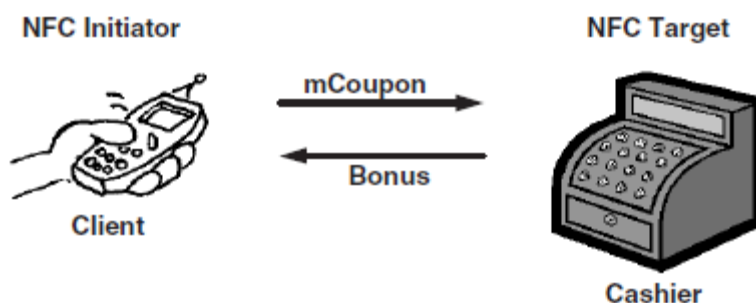
ซึ่งสามารถดาวน์โหลดได้จากโปสเตอร์หรือหนังสือพิมพ์พร้อมอุปกรณ์ NFC ไปยังอุปกรณ์มือถือ ด้วยโทรศัพท์มือถือนี้ผู้ใช้สามารถใช้ mCoupon เพื่อจ่ายเงินที่แคชเชียร์ ในกรณีส่วนใหญ่ มูลค่าของคูปองจะค่อนข้างต่ำ แต่ถ้าการนำไปใช้ในทางผิดมาก ๆ สามารถทำให้เกิดความเสียหายที่สำหรับ บริษัท ดังนั้น mCoupons จะต้องมีความปลอดภัยจากการโจมตี ในบทความนี้เราได้นำเสนอโปรโตคอลสำหรับระบบการรักษาความปลอดภัย mCoupon โดยการใช้เทคโนโลยี NFC โปรโตคอลนี้เป็นพื้นฐานสำหรับการให้บริการชำระเงินขนาดเล็กๆหรือการจองตั๋วในอนาคต

##### 1. แนวคิดของ mCoupon

mCoupons เป็นคูปองอิเล็กทรอนิกส์และสามารถจัดเก็บ และจ่ายเงินโดยการใช้มือถือ คูปองที่ออกโดยมีผู้ออกมีพร้อมอุปกรณ์ที่มี อินเทอร์เน็ต NFC ผู้ออกสามารถแนบตัวอย่างเช่นโฆษณาหนังสือพิมพ์หรือโปสเตอร์ ลูกค้านำโทรศัพท์มือถือ (พร้อมยังมีอุปกรณ์ที่มี NFC อินเทอร์เน็ต) ผู้ใช้สามารถ " สัมผัส " โฆษณาหนังสือพิมพ์หรือโปสเตอร์ และ mcoupon ที่ถูกต้องจะถูกเก็บไว้บนมือถือลูกค้าแต่ละรายสามารถมีโทรศัพท์มือถือมากกว่าหนึ่ง แต่เขาก็ยังมีตัวตนเสมือนจริงมากกว่าหนึ่ง (มีหนึ่งสำหรับแต่ละอุปกรณ์มือถือ ) ในระบบนี้ ลูกค้าสามารถใช้ mcoupon กับแคชเชียร์ ซึ่งเป็นอุปกรณ์ที่เปิดใช้งาน NFC และเงินสดในคูปอง แคชเชียร์จะตรวจสอบความถูกต้องของคูปองและมอบสินค้า สินค้าหรือบริการให้กับลูกค้า กลไกพื้นฐาน mCoupon จะแสดงในรูป 3.1และรูป 3.2



รูปที่ 4.1 การออก mCoupon



รูปที่ 4.2 กระบวนการรับจ่ายเงินของ mCoupon

ข้อมูลที่ไม่มีการป้องกันใน mcoupons สามารถคัดลอกได้อย่างง่ายดายหรือปรับเปลี่ยนแก้ไขโดยไม่มีค่าใช้จ่าย ด้วยเหตุนี้มาตรการรักษาความปลอดภัยจะต้องดำเนินการ มีปัญหาที่คู่กันด้านความปลอดภัยที่ต้องได้รับการแก้ไขเป็นดังนี้

- Multiple Cash-In (หลายเงินสดเข้า) ผู้โจมตีจะไม่สามารถใช้ mCoupon เดียวกันได้หลายครั้ง
- Unauthorized Generation (รุ่นที่ไม่ได้รับอนุญาต) ผู้โจมตีจะไม่สามารถออก mcoupons ของเขาเอง
- Manipulation (การจัดการ) ข้อมูลของ mCoupons ที่ไม่ถูกต้องจะไม่มีการจัดการ
- Unauthorized Copying (คัดลอกไม่ได้รับอนุญาต) ผู้โจมตีจะไม่สามารถสร้างสำเนาที่ถูกต้องของ mcoupon และเงินสดได้

บางส่วนของคุณสมบัติเหล่านี้เป็นตัวเลือก เช่น Multiple Cash-In หรือการคัดลอกของคูปอง ที่ได้รับอนุญาตในบางครั้ง คุณสมบัติขึ้นอยู่กับความต้องการของระบบ ในส่วน 5 เรายกเสนอเป็นระบบ mCoupon ซึ่งมีความปลอดภัย โดยวิธีการเข้ารหัสลับมาตรฐาน ระบบการดำเนินการมาตรการการรักษาความปลอดภัยจากภัยคุกคามดังกล่าวบางส่วนสามารถละเว้นลักษณะการทำงาน ส่วนถัดไปเกี่ยวข้องกับพื้นฐานของการตรวจสอบการเข้ารหัสลับซึ่งจะใช้เป็นมาตรการแก้ไขขั้นพื้นฐานในระบบของเรา