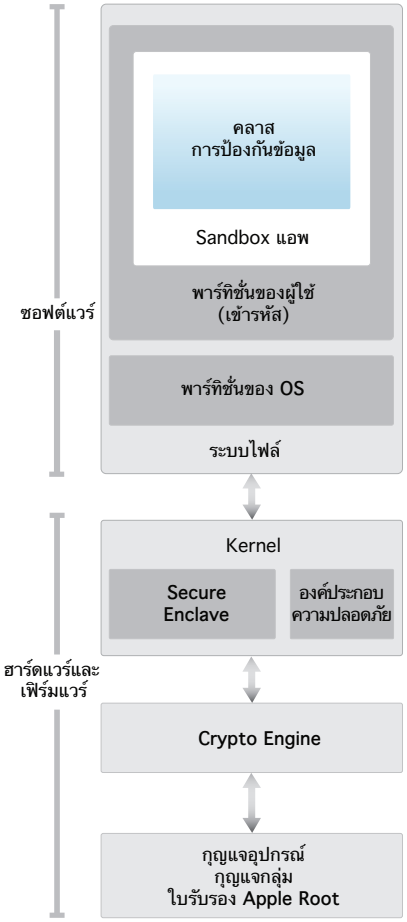
ความปลอดภัยของ iOS

iOS 9.3 ขึ้นไป

พฤษภาคม 2016

เนื้อหา

บทนำ



แผนภาพสถาปัตยกรรมด้านความปลอดภัยของ iOS จะทำให้มองเห็นภาพรวมของเทคโนโลยีต่างๆ ที่อธิบายไว้ในเอกสารนี้

Apple ออกแบบแพลตฟอร์ม iOS โดยคำนึงถึงความปลอดภัยเป็นหัวใจหลัก เมื่อเราเริ่มต้นสร้างแพลตฟอร์มอุปกรณ์เคลื่อนที่ที่ยอดเยี่ยมที่สุด เรานำประสบการณ์นับสิบปีมาใช้เพื่อสร้างสถาปัตยกรรมแบบใหม่ทั้งหมด เราคำนึงถึงภัยคุกคามความปลอดภัยของการใช้งานแบบเดสก์ท็อป และได้พัฒนาแนวคิดใหม่เรื่องความปลอดภัยในการออกแบบ iOS เราได้พัฒนาและนำคุณสมบัติที่เป็นนวัตกรรมมาใช้ซึ่งช่วยให้ความปลอดภัยของอุปกรณ์เคลื่อนที่รัดกุมขึ้นและช่วยป้องกันระบบทั้งระบบตามค่าเริ่มต้น ผลที่ได้คือ iOS ซึ่งเป็นความสำเร็จแบบก้าวกระโดดในด้านความปลอดภัยสำหรับอุปกรณ์เคลื่อนที่

อุปกรณ์ iOS ทุกเครื่องประกอบด้วยซอฟต์แวร์ ฮาร์ดแวร์ และบริการที่ออกแบบมาให้ทำงานร่วมกันเพื่อความปลอดภัยสูงสุดและประสบการณ์การใช้งานที่ชัดเจน iOS ไม่เพียงป้องกันอุปกรณ์และข้อมูลในเครื่อง แต่ยังป้องกันระบบทั้งหมด ซึ่งรวมถึงทุกอย่างที่ผู้ใช้ใช้งานบนเครื่อง บนเครือข่าย และบนบริการอินเทอร์เน็ตหลัก

iOS และอุปกรณ์ iOS มอบคุณสมบัติความปลอดภัยขั้นสูง แต่ยังคงใช้งานง่าย คุณสมบัติเหล่านี้หลายอย่างจะเปิดใช้งานไว้ตามค่าเริ่มต้น ด้วยเหตุนี้แผนก IT จึงไม่จำเป็นต้องปรับแต่งการตั้งค่า และการทำให้ไม่สามารถกำหนดค่าคุณสมบัติความปลอดภัยที่สำคัญ เช่น การเข้ารหัส ยังทำให้ผู้ใช้ไม่สามารถปิดใช้งานคุณสมบัติเหล่านั้นโดยไม่ได้ตั้งใจ คุณสมบัติอื่นๆ เช่น Touch ID ช่วยปรับปรุงประสบการณ์ของผู้ใช้โดยทำให้การรักษาความปลอดภัยอุปกรณ์เรียบง่ายขึ้นและเข้าใจได้ง่ายขึ้น

เอกสารนี้ให้รายละเอียดเกี่ยวกับวิธีที่เทคโนโลยีและคุณสมบัติความปลอดภัยถูกใช้งานภายในแพลตฟอร์ม iOS ซึ่งจะช่วยให้องค์กรสามารถปรับใช้เทคโนโลยีและคุณสมบัติความปลอดภัยของแพลตฟอร์ม iOS ร่วมกับนโยบายและขั้นตอนการทำงานของตนเองเพื่อตอบสนองความต้องการด้านความปลอดภัยเฉพาะที่มีอยู่

เอกสารฉบับนี้แบ่งออกเป็นส่วนหัวข้อต่างๆ ดังต่อไปนี้:

- **ความปลอดภัยของระบบ:** การผสานซอฟต์แวร์และฮาร์ดแวร์ที่ปลอดภัยซึ่งเป็นแพลตฟอร์มสำหรับ iPhone, iPad และ iPod touch
- **การเข้ารหัสและการป้องกันข้อมูล:** สถาปัตยกรรมและการออกแบบที่ช่วยป้องกันข้อมูลของผู้ใช้หากอุปกรณ์สูญหายหรือถูกขโมย หรือหากผู้ที่ไม่ได้รับอนุญาตพยายามใช้งานหรือแก้ไขข้อมูล
- **ความปลอดภัยของแอพ** ระบบที่ช่วยให้แอพสามารถทำงานอย่างปลอดภัยโดยไม่ทำให้ความสมบูรณ์ของแพลตฟอร์มบกพร่อง
- **ความปลอดภัยของเครือข่าย:** โปรโตคอลเครือข่ายมาตรฐานอุตสาหกรรมที่มอบการรับรองความถูกต้องที่ปลอดภัยและเข้ารหัสข้อมูลที่อยู่ระหว่างส่ง
- **Apple Pay:** การใช้งานการชำระเงินแบบปลอดภัยของ Apple
- **บริการอินเทอร์เน็ต:** โครงสร้างพื้นฐานบนเครือข่ายของ Apple สำหรับการส่งข้อความ เชื่อมข้อมูล และการสำรองข้อมูล
- **การควบคุมอุปกรณ์:** วิธีการที่ทำให้สามารถจัดการอุปกรณ์ iOS, ป้องกันการใช้โดยไม่ได้รับอนุญาต และทำให้สามารถลบข้อมูลระยะไกลได้หากอุปกรณ์สูญหายหรือถูกขโมย
- **การควบคุมความเป็นส่วนตัว:** ความสามารถของ iOS ที่สามารถใช้เพื่อควบคุมการเข้าถึงบริการหาตำแหน่งที่ตั้งและข้อมูลผู้ใช้

ความปลอดภัยของระบบ

การเข้าสู่โหมดอัพเกรดเฟิร์มแวร์อุปกรณ์ (DFU) การกู้คืนอุปกรณ์หลังจากที่เข้าสู่โหมด DFU จะทำให้อุปกรณ์นั้นกลับสู่สภาพที่ใช้งานได้และรับรองได้ว่าจะมีเฉพาะโค้ดที่ Apple ลงชื่อรับรองเท่านั้น สามารถเข้าสู่โหมด DFU ด้วยตัวเอง: ก่อนอื่นให้เชื่อมต่ออุปกรณ์เข้ากับคอมพิวเตอร์โดยใช้สาย USB แล้วกดปุ่มโฮมกับปุ่มพัก/ปลุกค้างไว้พร้อมกัน หลังจากผ่านไป 8 วินาที ให้ปล่อยปุ่มพัก/ปลุกแต่ยังกดปุ่มโฮมค้างไว้ หมายเหตุ: จะไม่มีอะไรแสดงบนหน้าจอเมื่ออุปกรณ์อยู่ในโหมด DFU หากโลโก้ Apple ปรากฏขึ้นแสดงว่ากดปุ่มพัก/ปลุกค้างไว้นานเกินไป

ความปลอดภัยของระบบออกแบบมาเพื่อให้ทั้งซอฟต์แวร์และฮาร์ดแวร์มีความปลอดภัยในทุกส่วนประกอบหลักบนอุปกรณ์ iOS ทุกตัว ซึ่งรวมถึงการบูตอุปกรณ์ การอัพเดทซอฟต์แวร์ และ Secure Enclave สถาปัตยกรรมนี้เป็นส่วนกลางของความปลอดภัยใน iOS และไม่รบกวนการใช้งานอุปกรณ์

การผสานฮาร์ดแวร์และซอฟต์แวร์อย่างกลมกลืนบนอุปกรณ์ iOS ทำให้มั่นใจได้ว่าส่วนประกอบแต่ละส่วนของระบบไว้วางใจได้ และระบบทั้งระบบน่าเชื่อถือ ตั้งแต่การบูตเริ่มแรก การอัพเดทซอฟต์แวร์ iOS ไปจนถึงแอพของบริษัทอื่น ขั้นตอนแต่ละขั้นตอนได้รับการวิเคราะห์และตรวจสอบเพื่อให้มั่นใจว่าฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันได้อย่างมีประสิทธิภาพและใช้ทรัพยากรได้อย่างเหมาะสม

ลำดับการบูตอย่างปลอดภัย

ขั้นตอนแต่ละขั้นตอนของกระบวนการเริ่มต้นทำงานประกอบด้วยส่วนประกอบที่ Apple ลงชื่อรับรองแบบเข้ารหัส เพื่อรับรองความถูกต้องและจะดำเนินการหลังจากที่ยืนยันลำดับการตรวจสอบความน่าเชื่อถือแล้วเท่านั้น การทำงานเช่นนี้รวมถึง Bootloader, Kernel, Kernel extension และเฟิร์มแวร์ Baseband

เมื่อเปิดอุปกรณ์ iOS หน่วยประมวลผลแอพพลิเคชั่นจะเรียกใช้รหัสจากหน่วยความจำแบบอ่านอย่างเดียวที่เรียกว่า Boot ROM ทันที รหัสที่เปลี่ยนไม่ได้นี้ซึ่งเรียกว่ารากของความเชื่อถือฮาร์ดแวร์ จะมีการระบุระหว่างขั้นตอนการผลิตชิป และจะมีกำหนดความเชื่อถือโดยนัย รหัส Boot ROM ประกอบด้วยกุญแจสาธารณะ Apple Root CA ซึ่งใช้เพื่อยืนยันว่า Low-Level Bootloader (LLB) มีการลงชื่อโดย Apple ก่อนอนุญาตให้โหลด นี่เป็นขั้นตอนแรกในลำดับการตรวจสอบความน่าเชื่อถือซึ่งขั้นตอนแต่ละขั้นเป็นการตรวจสอบว่าลำดับต่อไปมีการลงชื่อโดย Apple เมื่อ LLB ทำงานเสร็จ จะยืนยันและเรียกใช้งาน bootloader ขั้นต่อไปคือ iBoot ซึ่งจะยืนยันและเรียกใช้งาน Kernel ของ iOS ต่อ

ลำดับการบูตอย่างปลอดภัยนี้ช่วยให้แน่ใจว่าระดับขั้นต่ำที่สุดของซอฟต์แวร์ไม่ได้ถูกแทรกแซงและทำให้ iOS สามารถทำงานเฉพาะในอุปกรณ์ Apple ที่สมบูรณ์

สำหรับอุปกรณ์ที่มีเครือข่ายเซลลูลาร์ ระบบย่อยเบสแบนด์ยังใช้กระบวนการบูตแบบปลอดภัยของตัวเองด้วยซอฟต์แวร์ที่ลงชื่อและกุญแจที่มีการยืนยันความถูกต้องโดยหน่วยประมวลผลของเบสแบนด์ที่คล้ายคลึงกันด้วย

สำหรับอุปกรณ์ที่มีหน่วยประมวลผล A7 หรือซีรีส์ A ขึ้นไป หน่วยประมวลผลร่วม Secure Enclave ยังใช้กระบวนการบูตแบบปลอดภัยที่ช่วยให้ความมั่นใจว่าซอฟต์แวร์ที่แยกต่างหากมีการยืนยันความถูกต้องและลงชื่อโดย Apple

หากขั้นตอนหนึ่งของกระบวนการบูตนี้ไม่สามารถโหลดหรือยืนยันกระบวนการถัดไปได้ การเริ่มต้นทำงานจะสิ้นสุดและอุปกรณ์จะแสดงหน้าจอ “เชื่อมต่อกับ iTunes” ซึ่งเรียกว่าโหมดการกู้คืน หาก Boot ROM ไม่สามารถโหลดหรือยืนยัน LLB ได้ อุปกรณ์จะเข้าสู่โหมด DFU (อัพเกรดเฟิร์มแวร์อุปกรณ์) ในทั้งสองกรณี อุปกรณ์จะต้องเชื่อมต่อกับ iTunes ผ่านทาง USB และกู้คืนกลับเป็นการตั้งค่าเริ่มต้นจากโรงงาน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเข้าสู่โหมดการกู้คืนด้วยตัวเอง โปรดดู support.apple.com/kb/HT1808?viewlocale=th_TH

การอนุญาตซอฟต์แวร์ระบบ

Apple ออกรายการอัพเดทซอฟต์แวร์เพื่อแก้ไขข้อกังวลเรื่องความปลอดภัยที่เกิดขึ้นอยู่เสมอและยังออกคุณสมบัติใหม่ๆ รายการอัพเดทเหล่านี้มีให้สำหรับอุปกรณ์ที่ได้รับการสนับสนุนทั้งหมดพร้อมๆ กัน ผู้ใช้ได้รับการแจ้งเตือนการอัพเดท iOS บนอุปกรณ์และผ่าน iTunes และการอัพเดทจะมีการส่งแบบไร้สาย ซึ่งช่วยให้สามารถรับการแก้ไขความปลอดภัยล่าสุดได้อย่างรวดเร็ว

กระบวนการเริ่มต้นทำงานที่อธิบายด้านบนช่วยให้มั่นใจว่าเฉพาะโค้ดที่ Apple ลงชื่อรับรองเท่านั้นที่จะสามารถติดตั้งลงบนอุปกรณ์ได้ เพื่อช่วยป้องกันไม่ให้อุปกรณ์ถูกดาวน์เกรดเป็นเวอร์ชั่นเก่ากว่าที่ขาดการอัพเดทความปลอดภัยล่าสุด iOS ใช้กระบวนการทำงานที่เรียกว่า **การอนุญาตซอฟต์แวร์ระบบ** หากการดาวน์เกรดสามารถทำได้ ผู้ไม่ประสงค์ดีที่ได้อุปกรณ์ไปอาจติดตั้ง iOS เวอร์ชั่นเก่ากว่าและใช้ประโยชน์จากช่องโหว่ที่ได้รับการแก้ไขแล้วในเวอร์ชั่นที่ใหม่กว่า

บนอุปกรณ์ที่มีหน่วยประมวลผลซีรีส์ A รุ่น A7 ขึ้นไป หน่วยประมวลผลร่วม Secure Enclave ยังใช้การอนุญาตซอฟต์แวร์ระบบเพื่อช่วยให้มั่นใจถึงความสมบูรณ์ของซอฟต์แวร์และป้องกันการดาวน์เกรดการติดตั้ง โปรดดู “Secure Enclave” ด้านล่าง

รายการอัพเดทซอฟต์แวร์ iOS สามารถติดตั้งได้โดยใช้ iTunes หรือผ่านทางอากาศ (OTA) บนอุปกรณ์ หากทำการติดตั้งผ่าน iTunes จะทำการดาวน์โหลดและติดตั้งสำเนาแบบเต็มของ iOS ส่วนการอัพเดทโดยใช้ OTA จะทำการดาวน์โหลดเฉพาะส่วนที่จำเป็นต่อการอัพเดทให้สมบูรณ์ ซึ่งรวมถึงการปรับปรุงประสิทธิภาพเครือข่าย แต่จะไม่ดาวน์โหลดสำเนา iOS แบบเต็ม นอกจากนี้ การอัพเดทซอฟต์แวร์สามารถจัดเก็บเป็นแคชบนเซิร์ฟเวอร์เครือข่ายภายในที่ใช้งานบริการแคชบน OS X Server ดังนั้นอุปกรณ์ iOS จะไม่จำเป็นต้องเข้าถึงเซิร์ฟเวอร์ Apple เพื่อรับข้อมูลการอัพเดทที่จำเป็น

ระหว่างที่อัพเกรด iOS นั้น iTunes (หรือตัวอุปกรณ์เองในกรณีของซอฟต์แวร์ OTA) จะเชื่อมต่อเซิร์ฟเวอร์รับรองความถูกต้องการติดตั้งของ Apple และส่งรายการหน่วยที่เข้ารหัสสำหรับส่วนของบันเดิลการติดตั้งแต่ละส่วนที่ต้องติดตั้ง (ตัวอย่างเช่น LLB, iBoot, Kernel และ OS image) ค่าต่อต้านการเล่นซ้ำแบบสุ่ม (nonce) และ ID เฉพาะของอุปกรณ์ (ECID)

เซิร์ฟเวอร์การรับรองความถูกต้องจะตรวจสอบรายการหน่วยที่นำเสนอเทียบกับเวอร์ชั่นที่อนุญาตให้ทำการติดตั้ง และหากพบรายการที่ตรงกัน จะเพิ่ม ECID ไปยังหน่วยและลงชื่อในผลลัพธ์ เซิร์ฟเวอร์จะส่งชุดของข้อมูลที่ลงชื่อที่สมบูรณ์ไปยังอุปกรณ์เป็นส่วนหนึ่งของกระบวนการอัพเกรด การเพิ่ม ECID เป็นการ “ปรับเฉพาะเครื่อง” สำหรับการรับรองความถูกต้องของอุปกรณ์ที่ร้องขอ ด้วยการรับรองความถูกต้องและลงชื่อเฉพาะหน่วยที่รู้จัก เซิร์ฟเวอร์จะรับรองว่าการอัพเดทเกิดขึ้นตามที่ Apple กำหนดอย่างไม่ผิดเพี้ยน

การประเมินลำดับการตรวจสอบความน่าเชื่อถือในการบูตจะยืนยันว่าลายเซ็นมาจาก Apple และหน่วยของรายการที่โหลดจากดิสก์พร้อมกับ ECID ของอุปกรณ์ ตรงกับข้อมูลที่อยู่ในลายเซ็น

ขั้นตอนเหล่านี้ให้การรับรองว่าการตรวจสอบความถูกต้องเป็นไปสำหรับอุปกรณ์เฉพาะเครื่องและ iOS เวอร์ชั่นเก่าจากอุปกรณ์เครื่องหนึ่งไม่สามารถคัดลอกไปยังอีกเครื่องได้ ค่า nonce จะช่วยป้องกันผู้ไม่ประสงค์ดีจากการบันทึกการตอบสนองของเซิร์ฟเวอร์และใช้ข้อมูลนั้นเพื่อแทรกแซงอุปกรณ์หรือเปลี่ยนแก้ไขซอฟต์แวร์ระบบ

Secure Enclave

Secure Enclave เป็นหน่วยประมวลผลร่วมที่มีอยู่ในหน่วยประมวลผล Apple A7 หรือซีรีส์ A ขึ้นไป โดยจะใช้หน่วยความจำที่เข้ารหัสและมีตัวสร้างหมายเลขแบบสุ่มที่เป็นฮาร์ดแวร์ Secure Enclave จะมอบกระบวนการเข้ารหัสทั้งหมดสำหรับการจัดการกุญแจการป้องกันข้อมูลและรักษาความสมบูรณ์ของการป้องกันข้อมูลถึงแม้ว่า Kernel จะเกิดความหละหลวม การสื่อสารระหว่าง Secure Enclave กับหน่วยประมวลผลแอพพลิเคชั่นจำกัดอยู่ที่กล่องข้อความแบบ interrupt-driven และบัฟเฟอร์ข้อมูลหน่วยความจำที่มีการใช้งานร่วมกัน

Secure Enclave ใช้ Microkernel ตระกูล L4 ที่ Apple ปรับแต่งเอง Secure Enclave ใช้การบูตแบบปลอดภัยของตนเองและสามารถอัพเดทโดยใช้กระบวนการอัพเดทซอฟต์แวร์แบบเฉพาะตัวซึ่งแยกจากหน่วยประมวลผลแอพพลิเคชั่น

Secure Enclave แต่ละอันได้รับการกำหนดในระหว่างการผลิตโดยมี UID (ID เฉพาะ) ของตัวเองซึ่งส่วนอื่นของระบบไม่สามารถเข้าถึงได้และ Apple ไม่ทราบข้อมูล เมื่ออุปกรณ์เริ่มต้นทำงาน กุญแจแบบชั่วคราวจะถูกสร้างขึ้นผสานกับ UID ของอุปกรณ์ และถูกใช้เพื่อเข้ารหัสส่วน Secure Enclave ของพื้นที่หน่วยความจำของอุปกรณ์

นอกจากนี้ ข้อมูลที่มีการบันทึกไปยังระบบไฟล์โดย Secure Enclave จะถูกเข้ารหัสด้วยกุญแจที่ผสานกับ UID และตัวนับ anti-replay

Secure Enclave มีหน้าที่ในการประมวลผลข้อมูลลายนิ้วมือจากเซนเซอร์ Touch ID โดยระบุว่าตรงกับลายนิ้วมือที่ลงทะเบียนหรือไม่ จากนั้นเปิดใช้งานการเข้าใช้งานหรือการซื้อสินค้าในนามของผู้ใช้ การติดต่อระหว่างหน่วยประมวลผลและเซนเซอร์ Touch ID จะเกิดขึ้นบนบัสอินเทอร์เฟซอุปกรณ์ต่อพ่วงแบบอนุกรม (SPI) หน่วยประมวลผลจะส่งต่อข้อมูลไปยัง Secure Enclave แต่ไม่สามารถอ่านข้อมูลได้ ข้อมูลมีการเข้ารหัสและรับรองความถูกต้องโดยกุญแจเซสชั่นที่ติดต่อโดยใช้กุญแจที่ใช้ร่วมกันของอุปกรณ์ซึ่งได้รับการจัดหาให้สำหรับเซนเซอร์ Touch ID และ Secure Enclave การแลกเปลี่ยนกุญแจเซสชั่นจะใช้การห่อกุญแจ AES โดยทั้งสองฝั่งจะมอบกุญแจแบบสุ่มที่สร้างกุญแจเซสชั่นและใช้การเข้ารหัสการส่งต่อข้อมูล AES-CCM

Touch ID

Touch ID คือระบบการจับเซนเซอร์ลายนิ้วมือที่ทำให้การเข้าถึงอุปกรณ์แบบปลอดภัยเร็วขึ้นและง่ายขึ้น เทคโนโลยีนี้อ่านข้อมูลลายนิ้วมือจากหลายๆ มุม และเรียนรู้ลายนิ้วมือของผู้ใช้เพิ่มเติมเมื่อเวลาผ่านไป โดยเซนเซอร์จะขยายแผนที่ลายนิ้วมือเมื่อมีโหนดที่ทับซ้อนกันเพิ่มเติมซึ่งถูกระบุในแต่ละครั้ง

Touch ID ทำให้การใช้รหัสผ่านที่ยาวและซับซ้อนเป็นไปได้มากขึ้นเนื่องจากผู้ใช้ไม่จำเป็นต้องป้อนข้อมูลบ่อยๆ Touch ID ยังขจัดความไม่สะดวกของการล็อคด้วยรหัสผ่าน โดยไม่ได้ใช้แทนรหัสผ่านอย่างสิ้นเชิง แต่จะมอบการเข้าถึงอุปกรณ์อย่างปลอดภัยภายในขอบเขตและเวลาที่เหมาะสม

Touch ID และรหัสผ่าน

หากต้องการใช้ Touch ID ผู้ใช้จะต้องตั้งค่าอุปกรณ์ให้ต้องใช้รหัสผ่านเพื่อปลดล็อค เมื่อ Touch ID สแกนและจดจำลายนิ้วมือที่ลงทะเบียนได้ อุปกรณ์จะปลดล็อคโดยไม่ขอรหัสผ่านของอุปกรณ์ รหัสผ่านสามารถใช้แทน Touch ID ได้เสมอ และยังจำเป็นต้องใช้ในสถานการณ์ต่อไปนี้:

- อุปกรณ์เพิ่งถูกเปิดหรือรีสตาร์ท
- อุปกรณ์ไม่ได้ถูกปลดล็อคเป็นเวลานานกว่า 48 ชั่วโมง
- รหัสผ่านตัวเลขไม่ได้ถูกใช้เพื่อปลดล็อคอุปกรณ์ในหกวันล่าสุดและ ID ไม่ได้ปลดล็อคอุปกรณ์ในแปดชั่วโมงล่าสุด
- อุปกรณ์ได้รับคำสั่งล็อคระยะไกล
- หลังความพยายามจับคู่ลายนิ้วมือที่ไม่สำเร็จห้าครั้ง
- เมื่อตั้งค่าหรือลงทะเบียนลายนิ้วมือใหม่ด้วย Touch ID

เมื่อ Touch ID ถูกเปิดใช้งาน อุปกรณ์จะล็อคโดยทันทีเมื่อปุ่มพัก/ปลุกถูกกด ด้วยความปลอดภัยแบบใช้เฉพาะรหัสผ่าน ผู้ใช้หลายคนจะตั้งช่วงเวลาผ่อนผันการปลดล็อคเพื่อหลีกเลี่ยงการต้องป้อนรหัสผ่านในแต่ละครั้งที่อุปกรณ์มีการใช้งาน ด้วย Touch ID อุปกรณ์จะล็อคทุกครั้งที่พักเครื่อง และต้องใช้ลายนิ้วมือหรือใช้รหัสผ่านแทนทุกครั้งที่ปลุกเครื่อง

สามารถกำหนดให้ Touch ID จดจำลายนิ้วมือที่ต่างกันได้ถึงห้านิ้ว เมื่อลงทะเบียนนิ้วมือหนึ่งนิ้ว โอกาสที่ลายนิ้วมือจะตรงกับคนอื่นอยู่ที่ 1 ใน 50,000 อย่างไรก็ตาม Touch ID อนุญาตให้พยายามจับคู่ลายนิ้วมือได้ห้าครั้ง ก่อนที่ผู้ใช้จำเป็นต้องป้อนรหัสผ่านเพื่อใช้งานเครื่อง

การใช้งานอื่นๆ สำหรับ Touch ID

Touch ID ยังสามารถใช้กำหนดค่าเพื่ออนุญาตการซื้อสินค้าจาก iTunes Store, App Store และ iBooks Store ผู้ใช้จึงไม่ต้องป้อนรหัสผ่าน Apple ID เมื่อผู้ใช้เลือกอนุญาตการซื้อสินค้า โทเค็นการอนุญาตจะมีการแลกเปลี่ยนระหว่างอุปกรณ์และร้าน โทเค็นและค่า Nonce ที่เข้ารหัสจะถูกจัดเก็บใน Secure Enclave ค่า Nonce จะมีการลงชื่อกับกุญแจ Secure Enclave ที่ใช้ร่วมกันโดยอุปกรณ์ทั้งหมดและ iTunes Store

Touch ID ยังสามารถใช้กับ Apple Pay ซึ่งเป็นการใช้งานการชำระเงินแบบปลอดภัยของ Apple สำหรับข้อมูลเพิ่มเติม โปรดดูส่วน Apple Pay ของเอกสารนี้

นอกจากนี้ แอพของบริษัทอื่นสามารถใช้ API ที่ระบบให้มาเพื่อขอให้ผู้ใช้รับรองความถูกต้องโดยใช้ Touch ID หรือรหัสผ่าน แอพจะได้รับแจ้งเฉพาะเรื่องที่ว่าการรับรองความถูกต้องสำเร็จหรือไม่ แต่ไม่สามารถเข้าถึง Touch ID หรือข้อมูลที่เชื่อมโยงกับลายนิ้วมือที่ลงทะเบียนได้

รายการพวงกุญแจยังสามารถได้รับการป้องกันด้วย Touch ID โดยจะปล่อยข้อมูลจาก Secure Enclave ได้เฉพาะเมื่อลายนิ้วมือตรงกันหรือใช้รหัสผ่านอุปกรณ์ ผู้พัฒนาแอพยังมี API เพื่อใช้ยืนยันว่ารหัสผ่านมีการตั้งค่าโดยผู้ใช้และด้วยเหตุนี้สามารถรับรองความถูกต้องหรือปลดล็อครายการพวงกุญแจได้โดยใช้ Touch ID

ด้วย iOS 9 ผู้พัฒนาสามารถกำหนดให้การทำงานของ API Touch ID ไม่กลับไปเรียกขอใช้รหัสผ่านแอพพลิเคชั่นหรือรหัสผ่านอุปกรณ์แทน เมื่อรวมกับความสามารถในการเรียกคืนข้อมูลแสดงสถานะของนิ้วมือที่ลงทะเบียน ทำให้ Touch ID สามารถใช้งานเป็นปัจจัยที่สองในแอพที่เน้นเรื่องความปลอดภัย

ความปลอดภัยของ Touch ID

เซนเซอร์ลายนิ้วมือจะทำงานเฉพาะเมื่อห่วงเหล็ก Capacitive ที่ล้อมรอบปุ่มโฮมตรวจพบการสัมผัสของนิ้วมือ ซึ่งเปิดการทำงานแถวการจับภาพขั้นสูงเพื่อสแกนนิ้วมือและส่งการสแกนไปยัง Secure Enclave

การสแกนแบบแรสเตอร์จะถูกจัดเก็บไว้ชั่วคราวในหน่วยความจำที่เข้ารหัสภายใน Secure Enclave ในขณะที่ถูกเปลี่ยนเป็นเวกเตอร์เพื่อการวิเคราะห์ และจากนั้นจะถูกลบทิ้ง การวิเคราะห์ใช้การเทียบผังมุมรอยเส้นใต้ผิวหนัง ซึ่งเป็นกระบวนการแบบยึดรายละเอียดหลักซึ่งทิ้งข้อมูลรายละเอียดย่อยๆ ที่จำเป็นต่อการสร้างลายนิ้วมือจริงของผู้ใช้ขึ้นมาใหม่ แผนที่โหนดที่ได้จะถูกจัดเก็บโดยไม่มีข้อมูลประจำตัวใดๆ ในรูปแบบการเข้ารหัสที่สามารถอ่านได้โดย Secure Enclave เท่านั้นและจะไม่ถูกส่งไปยัง Apple หรือสำรองข้อมูลไปยัง iCloud หรือ iTunes ไม่ว่าในกรณีใดๆ

Touch ID ปลดล็อคอุปกรณ์ iOS ได้อย่างไร

หาก Touch ID ถูกปิด เมื่ออุปกรณ์ล็อค กุญแจสำหรับคลาสการป้องกันข้อมูลแบบสมบูรณ์ซึ่งจัดเก็บอยู่ใน Secure Enclave จะถูกลบทิ้ง ไฟล์และรายการพวงกุญแจในคลาสนั้นจะไม่สามารถเข้าใช้ได้จนกว่าผู้ใช้จะปลดล็อคอุปกรณ์โดยการป้อนรหัสผ่านของเขาหรือเธอ

เมื่อ Touch ID เปิดอยู่ กุญแจจะไม่ถูกทิ้งเมื่ออุปกรณ์ล็อค แต่จะถูกห่อไว้กับกุญแจซึ่งจะถูกมอบให้ระบบย่อย Touch ID ภายใน Secure Enclave เมื่อผู้ใช้พยายามปลดล็อคอุปกรณ์ หาก Touch ID จดจำลายนิ้วมือของผู้ใช้ได้ Touch ID จะมอบกุญแจสำหรับแกะห่อกุญแจการป้องกันข้อมูล และจะปลดล็อคอุปกรณ์ กระบวนการนี้จะให้การป้องกันเพิ่มเติมโดยการเรียกขอให้การป้องกันข้อมูลและระบบย่อย Touch ID ทำงานร่วมกันเพื่อปลดล็อคอุปกรณ์

กุญแจที่จำเป็นสำหรับ Touch ID ในการปลดล็อคอุปกรณ์จะสูญหายหากอุปกรณ์รีบูตและจะถูก Secure Enclave ทิ้งหลังจาก 48 ชั่วโมงหรือความพยายามจับคู่ลายนิ้วมือ Touch ID ล้มเหลวห้าครั้ง

การเข้ารหัสและการป้องกันข้อมูล

การลบเนื้อหาและการตั้งค่าทั้งหมด
ตัวเลือก “ลบเนื้อหาและการตั้งค่าทั้งหมด” ในการตั้งค่าจะทำลายกุญแจทั้งหมดในพื้นที่จัดเก็บที่ลบได้ และทำให้เข้าถึงข้อมูลผู้ใช้ทั้งหมดในอุปกรณ์ไม่ได้เนื่องจากไม่สามารถถอดรหัส ดังนั้น วิธีการที่ดีที่สุดคือตรวจสอบให้แน่ใจว่าได้เอาข้อมูลส่วนตัวทั้งหมดออกจากอุปกรณ์แล้วก่อนที่จะมอบให้กับผู้อื่นหรือส่งเข้ารับบริการ สิ่งสำคัญ: อย่าใช้ตัวเลือก “ลบเนื้อหาและการตั้งค่าทั้งหมด” จนกว่าจะสำรองข้อมูลอุปกรณ์แล้ว เนื่องจากไม่มีวิธีกู้คืนข้อมูลที่ถูกลบ

ลำดับการบูตอย่างปลอดภัย การลงชื่อรหัส และความปลอดภัยกระบวนการรันไทม์ทั้งหมดช่วยให้มั่นใจว่าเฉพาะรหัสและแอพที่เชื่อถือได้เท่านั้นที่สามารถทำงานบนอุปกรณ์ได้ iOS มีการเข้ารหัสและคุณสมบัติการป้องกันข้อมูลเพิ่มเติมเพื่อช่วยป้องกันข้อมูลของผู้ใช้ แม้ในกรณีที่ส่วนอื่นของโครงสร้างระบบความปลอดภัยเกิดความหละหลวม (ตัวอย่างเช่น บนอุปกรณ์ที่มีการปรับแก้ไขที่ไม่ได้รับอนุญาต) ข้อนี้ถือเป็นข้อดีสำคัญสำหรับทั้งผู้ใช้และผู้ดูแลระบบ iT โดยให้การป้องกันข้อมูลส่วนตัวและขององค์กรตลอดเวลา และให้วิธีการล้างข้อมูลระยะไกลโดยทันทีและสมบูรณ์ในกรณีที่อุปกรณ์ถูกขโมยหรือสูญหาย

คุณสมบัติความปลอดภัยของฮาร์ดแวร์

สำหรับอุปกรณ์เคลื่อนที่ ความเร็วและประสิทธิภาพของพลังงานเป็นสิ่งสำคัญที่สุด การทำงานเข้ารหัสมีความซับซ้อนและสามารถทำให้เกิดปัญหาด้านการทำงานหรืออายุแบตเตอรี่ได้หากไม่ได้รับการออกแบบและปรับใช้โดยคำนึงถึงลำดับความสำคัญเหล่านี้

อุปกรณ์ iOS ทุกอันมีกลไลการเข้ารหัส AES 256 ที่สร้างมาในพาธ DMA ระหว่างพื้นที่จัดเก็บแบบแฟลชและหน่วยความจำหลักของระบบ ซึ่งทำให้การเข้ารหัสไฟล์มีประสิทธิภาพเป็นอย่างสูง

ID เฉพาะของอุปกรณ์ (UID) และ ID กลุ่มอุปกรณ์ (GID) เป็นกุญแจ 256 บิต AES ที่ fused (UID) หรือ compiled (GID) ลงในหน่วยประมวลผลแอพพลิเคชั่นและ Secure Enclave ในระหว่างการผลิต ไม่มีซอฟต์แวร์หรือเฟิร์มแวร์ใดที่สามารถอ่านข้อมูลนี้ได้โดยตรง ทำได้เฉพาะการดูผลลัพธ์ของการเข้ารหัสหรือการทำงานถอดรหัสที่ทำโดยกลไก AES เฉพาะงานที่ปรับใช้ในซิลิคอนโดยใช้ UID หรือ GID เป็นกุญแจ นอกจากนี้ UID และ GID ของ Secure Enclave สามารถใช้ได้โดยกลไก AES ที่เป็นของ Secure Enclave เท่านั้น ค่า UID ไม่เหมือนกันในอุปกรณ์แต่ละเครื่องและไม่มีการบันทึกค่าโดย Apple หรือซัพพลายเออร์ของ Apple รายใด ค่า GID เหมือนกันทั้งหมดสำหรับหน่วยประมวลผลทั้งหมดในคลาสของอุปกรณ์ (ตัวอย่างเช่น อุปกรณ์ทั้งหมดที่ใช้หน่วยประมวลผล Apple A8) และมีการใช้สำหรับงานที่ไม่ส่งผลด้านความปลอดภัยมากนัก เช่น เมื่อส่งซอฟต์แวร์ระบบในระหว่างการติดตั้งและการกู้คืน การผสานกุญแจเหล่านี้ลงในซิลิคอนช่วยป้องกันไม่ให้กุญแจถูกรบกวนหรือถูกบายพาส หรือถูกเข้าถึงจากภายนอกกลไก AES ค่า UID และ GID ยังไม่สามารถใช้งานได้ผ่าน JTAG หรืออินเทอร์เฟซการดีบั๊กอื่นๆ

ค่า UID อนุญาตให้ข้อมูลมีการผูกแบบเข้ารหัสกับอุปกรณ์เฉพาะเครื่อง ตัวอย่างเช่น ลำดับชั้นกุญแจที่ป้องกันระบบไฟล์รวมถึงค่า UID ดังนั้นหากชิปหน่วยความจำถูกย้ายจากอุปกรณ์เครื่องหนึ่งไปอีกเครื่อง ไฟล์ก็จะไม่สามารถเข้าถึงได้ ค่า UID ไม่เกี่ยวข้องกับตัวระบุชี้อื่นๆ บนอุปกรณ์

นอกจากค่า UID และ GID กุญแจการเข้ารหัสอื่นทั้งหมดจะถูกสร้างโดยตัวสร้างหมายเลขแบบสุ่มของระบบ (RNG) โดยใช้อัลกอริธึมที่อ้างอิงจาก CTR_DRBG Entropy สร้างจากความผันแปรด้านเวลาระหว่างการบูต และสร้างเพิ่มเติมจากเวลาการรบกวนเมื่ออุปกรณ์บูตแล้ว กุญแจที่สร้างภายใน Secure Enclave ใช้ตัวสร้างหมายเลขฮาร์ดแวร์แบบสุ่มจริงของตนที่อ้างอิงตำแหน่งของออสซิลเลเตอร์วงแหวนหลายตัวที่ประมวลผลด้วย CTR_DRBG

การลบกุญแจที่บันทึกไว้อย่างปลอดภัยมีความสำคัญเท่ากับการสร้าง โดยยิ่งเป็นเรื่องท้าทายสำหรับพื้นที่จัดเก็บแฟลช ที่ wear-leveling อาจหมายถึงสำเนาหลายชุดของข้อมูลที่ต้องลบ เพื่อแก้ไขปัญหานี้ อุปกรณ์ iOS จึงมาพร้อมคุณสมบัติที่มุ่งไปที่การลบข้อมูลอย่างปลอดภัยที่เรียกว่าพื้นที่จัดเก็บที่ลบได้ คุณสมบัตินี้เข้าถึงเทคโนโลยีการจัดเก็บที่รองรับ (ตัวอย่างเช่น NAND) เพื่อแก้ไขปัญหาโดยตรงและลบบล็อคจำนวนน้อยในระดับที่ต่ำมากๆ

การป้องกันข้อมูลไฟล์

นอกจากคุณสมบัติการเข้ารหัสฮาร์ดแวร์ที่สร้างมาในอุปกรณ์ iOS Apple ยังใช้เทคโนโลยีที่เรียกว่าการป้องกันข้อมูลเพื่อป้องกันข้อมูลที่จัดเก็บในหน่วยความจำแฟลชเพิ่มเติมบนอุปกรณ์ การป้องกันข้อมูลอนุญาตให้อุปกรณ์ตอบสนองต่อเหตุการณ์ทั่วไป เช่น สายโทรศัพท์เรียกเข้า แต่ยังช่วยให้สามารถเข้ารหัสข้อมูลผู้ใช้ระดับสูงได้ แอพระบบกุญแจ เช่น ข้อความ ปฏิทิน รายชื่อ รูปภาพ และค่าข้อมูลสุขภาพใช้การป้องกันข้อมูลตามค่าเริ่มต้น และแอพของบริษัทอื่นที่ติดตั้งบน iOS 7 ขึ้นไปจะได้รับการป้องกันนี้โดยอัตโนมัติ

การป้องกันข้อมูลมีการปรับใช้โดยการสร้างและจัดการลำดับชั้นของกุญแจ และสร้างโดยใช้เทคโนโลยีการเข้ารหัสฮาร์ดแวร์ที่สร้างในอุปกรณ์ iOS แต่ละเครื่อง การป้องกันข้อมูลมีการควบคุมแบบไฟล์รายอันโดยการกำหนดคลาสให้กับไฟล์แต่ละไฟล์ ความสามารถในการเข้าถึงจะกำหนดโดยคลาสกุญแจว่ามีการปลดล็อคหรือไม่

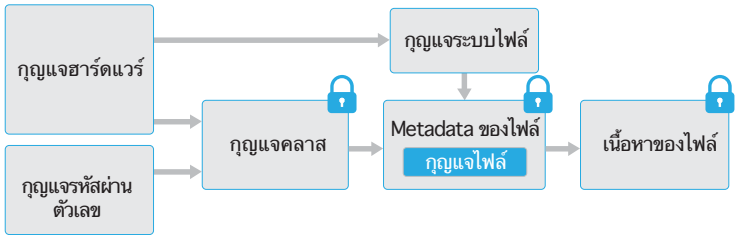
ภาพรวมสถาปัตยกรรม

ทุกครั้งที่ไฟล์บนพาร์ทิชั่นข้อมูลถูกสร้าง การป้องกันข้อมูลจะสร้างกุญแจ 256 บิตใหม่ (กุญแจ “รายไฟล์”) และมอบให้กับกลไกฮาร์ดแวร์ AES ซึ่งจะใช้กุญแจเพื่อเข้ารหัสไฟล์ตามที่มีการเขียนไปยังหน่วยความจำแฟลชโดยใช้โหมด AES CBC (บนอุปกรณ์ที่มีหน่วยประมวลผล A8, AES-XTS จะถูกใช้งาน) เวคเตอร์การเริ่มต้นทำงาน (IV) มีการคำนวณโดยค่าออฟเซตบล็อคลงในไฟล์ โดยเข้ารหัสด้วยแฮช SHA-1 ของกุญแจรายไฟล์

กุญแจรายไฟล์จะถูกห่อด้วยหนึ่งในคลาสกุญแจที่มีอยู่หลายอัน โดยขึ้นอยู่กับสถานการณ์ว่าควรจะสามารถเข้าถึงไฟล์ใดได้บ้าง เช่นเดียวการห่ออื่นๆ ทั้งหมดขั้นตอนนี้จะทำโดยใช้การห่อกุญแจ NIST AES ตาม RFC 3394 กุญแจรายไฟล์ที่ถูกห่อจะจัดเก็บไว้ใน Metadata ของไฟล์

เมื่อเปิดไฟล์ Metadata ของไฟล์นั้นจะถูกถอดรหัสด้วยกุญแจระบบไฟล์ โดยเปิดเผยกุญแจรายไฟล์ที่ถูกห่ออยู่และสัญลักษณ์ที่บอกว่าป้องกันด้วยคลาสใด กุญแจรายไฟล์จะถูกแกะห่อด้วยคลาสกุญแจ จากนั้นส่งมอบให้กับกลไก AES ของฮาร์ดแวร์ ซึ่งจะถอดรหัสไฟล์ตามที่มีการอ่านจากหน่วยความจำแฟลช การจัดการกุญแจไฟล์ที่ถูกห่อทั้งหมดจะเกิดขึ้นใน Secure Enclave โดยจะไม่เปิดเผยกุญแจไฟล์ให้กับตัวประมวลผลแอพพลิเคชั่นโดยตรง เมื่อบูตอุปกรณ์ Secure Enclave จะเจรจาขอกุญแจชั่วคราวกับกลไก AES เมื่อ Secure Enclave แกะห่อกุญแจของไฟล์ กุญแจจะถูกห่ออีกครั้งด้วยกุญแจชั่วคราวและถูกส่งกลับไปที่หน่วยประมวลผลแอพพลิเคชั่น

Metadata ของไฟล์ทั้งหมดในระบบไฟล์จะถูกเข้ารหัสด้วยกุญแจแบบสุ่ม ซึ่งจะถูกสร้างเมื่อ iOS มีการติดตั้งเป็นครั้งแรกหรือเมื่ออุปกรณ์ถูกล้างข้อมูลโดยผู้ใช้ กุญแจระบบไฟล์มีการจัดเก็บในพื้นที่จัดเก็บที่ลบได้ เนื่องจากกุญแจมีการจัดเก็บบนอุปกรณ์ กุญแจนี้จะไม่ถูกใช้เพื่อจัดเก็บความลับของข้อมูล ในทางตรงกันข้าม กุญแจได้รับการออกแบบมาให้ลบได้อย่างรวดเร็วตามคำสั่ง (เมื่อผู้ใช้เลือกตัวเลือก “ลบเนื้อหาและการตั้งค่าทั้งหมด” หรือเมื่อผู้ใช้หรือผู้ดูแลระบบออกคำสั่งล้างข้อมูลระยะไกลจากเซิร์ฟเวอร์การจัดการอุปกรณ์เคลื่อนที่ (MDM), Exchange ActiveSync หรือ iCloud) การลบกุญแจในลักษณะนี้จะทำให้ไฟล์ทั้งหมดไม่สามารถเข้าถึงได้แบบเข้ารหัส



เนื้อหาของไฟล์จะมีการเข้ารหัสด้วยกุญแจรายไฟล์ ซึ่งจะห่อด้วยคลาสกุญแจและจัดเก็บใน Metadata ของไฟล์ ซึ่งเข้ารหัสด้วยกุญแจระบบไฟล์ คลาสกุญแจได้รับการป้องกันด้วยค่า UID ฮาร์ดแวร์ และสำหรับคลาสบางคลาสป้องกันด้วยรหัสผ่านของผู้ใช้ ลำดับชั้นนี้ให้ทั้งความยืดหยุ่นและการทำงานที่ดี ตัวอย่างเช่น การเปลี่ยนคลาสของไฟล์จำเป็นต้องห่อซ้ำเฉพาะกุญแจรายไฟล์เท่านั้น และการเปลี่ยนรหัสผ่านจะห่อคลาสกุญแจซ้ำ

รหัสผ่านตัวเลข

การพิจารณารหัสผ่าน
หากป้อนรหัสผ่านที่ยาวและมีเพียงตัวเลขเท่านั้น แป้นตัวเลขจะแสดงบนหน้าจอล็อคแทนแป้นพิมพ์แบบเต็ม รหัสผ่านตัวเลขที่ยาวจะป้อนได้ง่ายกว่ารหัสผ่านตัวเลขและตัวอักษรที่สั้นกว่า ในขณะที่ให้การป้องกันในระดับเดียวกัน

โดยการตั้งค่ารหัสผ่านอุปกรณ์ ผู้ใช้จะเปิดใช้งานการป้องกันข้อมูลโดยอัตโนมัติ iOS รองรับรหัสผ่านตัวอักษรและตัวเลขหกหลัก สี่หลัก และความยาวตามที่กำหนด นอกจากการปลดล็อคอุปกรณ์ รหัสผ่านยังมอบ Entropy สำหรับกุญแจการเข้ารหัสบางอัน ซึ่งหมายความว่าผู้ไม่ประสงค์ดีที่ได้อุปกรณ์ไปจะไม่สามารถเข้าถึงข้อมูลในคลาสการป้องกันเฉพาะได้โดยไม่มีรหัสผ่าน

รหัสผ่านจะเชื่อมโยงกับ UID ของอุปกรณ์ ดังนั้นการโจมตีแบบ Brute-force จะต้องทำบนอุปกรณ์ที่จะโจมตี ตัวนับการทำซ้ำจำนวนมากใช้เพื่อทำให้การโจมตีแต่ละครั้งช้าลง ตัวนับการทำซ้ำมีการปรับเทียบเพื่อให้การโจมตีหนึ่งครั้งใช้เวลาประมาณ 80 มิลลิวินาที ซึ่งหมายความว่าการลองผสมรหัสทั้งหมดของรหัสผ่านตัวอักษรและตัวเลขหกหลักที่เป็นตัวพิมพ์เล็กและตัวเลขจะใช้เวลามากกว่า 5 ปีครึ่ง

ยิ่งรหัสผ่านผู้ใช้มีความยากมากขึ้นเท่าใด กุญแจการเข้ารหัสยิ่งมีความปลอดภัยสูงขึ้นเท่านั้น Touch ID สามารถใช้เพื่อเพิ่มประสิทธิภาพนี้ได้โดยการทำให้ผู้ใช้สามารถสร้างรหัสผ่านที่มีความปลอดภัยสูงขึ้นได้แต่ยังคงใช้งานได้จริง คุณสมบัตินี้ช่วยเพิ่มปริมาณ Entropy ที่มีประสิทธิภาพซึ่งช่วยป้องกันกุญแจการเข้ารหัสที่ใช้สำหรับการป้องกันข้อมูลโดยไม่ส่งผลด้านลบต่อประสบการณ์การใช้งานของผู้ใช้ที่ต้องปลดล็อคอุปกรณ์ iOS หลายครั้งตลอดวัน

การหน่วงเวลาระหว่างการพยายามป้อนรหัสผ่าน

ความพยายาม	การหน่วงเวลาที่บังคับใช้
1-4	ไม่มี
5	1 นาที
6	5 นาที
7-8	15 นาที
9	1 ชั่วโมง

เพื่อทำให้การโจมตีรหัสผ่านแบบ Brute-force ยากยิ่งขึ้นไปอีก อุปกรณ์มีการหน่วงเวลาที่เพิ่มขึ้นหลังจากที่ป้อนรหัสผ่านผิดในหน้าจอล็อค หาก การตั้งค่า > Touch ID และรหัสผ่าน > ลบข้อมูล เปิดอยู่ อุปกรณ์จะล้างข้อมูลโดยอัตโนมัติหลังป้อนรหัสผ่านผิด 10 ครั้งติดต่อกัน การตั้งค่านี้ยังใช้งานเป็นนโยบายการดูแลจัดการได้ผ่านการจัดการอุปกรณ์เคลื่อนที่ (MDM) และ Exchange ActiveSync และสามารถตั้งค่าเป็นค่าที่ต่ำลงมาได้

บนอุปกรณ์ที่มีหน่วยประมวลผล A7 หรือซีรีส์ A ขึ้นไป การหน่วงเวลาจะถูกบังคับใช้โดย Secure Enclave หากอุปกรณ์เริ่มการทำงานใหม่ในระหว่างช่วงการหน่วงเวลา การหน่วงเวลาจะยังคงใช้งานอยู่ โดยตัวจับเวลาจะเริ่มต้นใหม่สำหรับช่วงเวลาปัจจุบัน

คลาสการป้องกันข้อมูล

เมื่อไฟล์ใหม่ถูกสร้างบนอุปกรณ์ iOS ไฟล์จะได้รับการกำหนดคลาสโดยแอพที่สร้างไฟล์ขึ้น คลาสแต่ละคลาสจะใช้นโยบายที่ต่างกันเพื่อระบุว่าข้อมูลจะเข้าถึงได้เมื่อใด คลาสและนโยบายเบื้องต้นมีการอธิบายในส่วนต่อไปนี้

การป้องกันแบบสมบูรณ์
(`NSFileProtectionComplete`): คลาสกุญแจได้รับการป้องกันโดยกุญแจที่ได้มาจากรหัสผ่านของผู้ใช้และค่า UID ของอุปกรณ์ หลังจากที่ผู้ใช้ล็อคอุปกรณ์ไม่นาน (10 วินาที หากการตั้งค่าเรียกขอรหัสผ่านคือทันที) คลาสกุญแจที่ถูกถอดรหัส จะถูกลบทิ้ง ทำให้ข้อมูลทั้งหมดในคลาสนี้ไม่สามารถเข้าใช้ได้จนกว่าผู้ใช้จะป้อนรหัสผ่านอีกครั้งหรือปลดล็อคอุปกรณ์โดยใช้ Touch ID

ป้องกันหากไม่เปิดอยู่

(`NSFileProtectionCompleteUnlessOpen`): ไฟล์บางไฟล์อาจต้อง มีการเขียนในขณะที่อุปกรณ์ล็อคอยู่ ตัวอย่างที่ดีของกรณีนี้คือไฟล์แนบอีเมลที่ดาวน์โหลดอยู่ในพื้นหลัง ลักษณะงานเช่นนี้ทำได้โดยการใช้การเข้ารหัสเส้นโค้งรูปไข่แบบไม่สมมาตร (ECDH บน Curve25519) กุญแจรายไฟล์โดยทั่วไปจะได้รับการป้องกันโดยกุญแจที่ได้มาโดยใช้ข้อตกลงกุญแจ One-Pass Diffie-Hellman ตามที่อธิบายใน NIST SP 800-56A

กุญแจสาธารณะชั่วคราวสำหรับข้อตกลงจะจัดเก็บไปพร้อมกับกุญแจรายไฟล์ที่ถูกห่อ KDF คือ ฟังก์ชันการแปรผันกุญแจที่ต่อกัน (ตัวเลือก 1 ที่อนุมัติ) ตามที่อธิบายในข้อ 5.8.1 ของ NIST SP 800-56A ID อัลกอริธึมถูกละเว้น PartyUInfo และ PartyVInfo คือกุญแจสาธารณะชั่วคราวและกุญแจสาธารณะแบบคงที่ตามลำดับ SHA-256 ใช้เป็นฟังก์ชันการแฮช ทันทีที่ไฟล์ถูกปิด กุญแจรายไฟล์จะถูกล้างจากหน่วยความจำ หากต้องการเปิดไฟล์อีกครั้ง ความลับที่มีการแบ่งปันจะถูกสร้างอีกครั้งโดยการใช้กุญแจส่วนตัวของคลาสป้องกันหากไม่เปิดอยู่ และกุญแจสาธารณะชั่วคราวของไฟล์ ซึ่งจะถูกใช้ เพื่อแกะห่อกุญแจรายไฟล์ ซึ่งจากนั้นจะใช้เพื่อถอดรหัสไฟล์

ป้องกันจนกว่ามีการรับรองความถูกต้องของผู้ใช้รายแรก

(`NSFileProtectionCompleteUntilFirstUserAuthentication`): คลาสนี้ทำงานเหมือนกับการป้องกันแบบสมบูรณ์ เว้นแต่เพียงคลาสกุญแจที่ถูกถอดรหัสจะไม่ถูกลบออกจากหน่วยความจำเมื่ออุปกรณ์ถูกล็อค การป้องกันในคลาสนี้มีคุณลักษณะคล้ายกับการเข้ารหัสแบบเต็มในคอมพิวเตอร์เดสก์ท็อป และป้องกันข้อมูลจากการโจมตีที่เกี่ยวข้องกับการรีบูต นี่เป็นคลาสค่าเริ่มต้นสำหรับข้อมูลแอพของบริษัทอื่นทั้งหมดที่ไม่ได้ถูกกำหนดคลาสการป้องกันข้อมูลให้

ไม่มีการป้องกัน

(`NSFileProtectionNone`): คลาสกุญแจนี้ได้รับการป้องกันด้วยค่า UID เท่านั้น และมีการจัดเก็บในพื้นที่จัดเก็บที่ลบได้ เนื่องจากกุญแจทั้งหมดที่จำเป็นต้องใช้เพื่อถอดรหัสไฟล์ในคลาสนี้มีการจัดเก็บบนอุปกรณ์ การเข้ารหัสจึงให้ประโยชน์ของการล้างข้อมูลระยะไกลอย่างรวดเร็วเท่านั้น หากไฟล์ไม่ได้ถูกกำหนดคลาสการป้องกันข้อมูล ไฟล์จะยังคงถูกจัดเก็บในรูปแบบที่เข้ารหัส (เช่นเดียวกับข้อมูลทั้งหมดบนอุปกรณ์ iOS)

การป้องกันข้อมูลในพวงกุญแจ

แอพหลายตัวจำเป็นต้องจัดการรหัสผ่านและข้อมูลสั้นๆ ที่เป็นความลับ เช่น กุญแจและโทเค็นการเข้าสู่ระบบ พวงกุญแจ iOS มอบวิธีที่ปลอดภัยในการจัดเก็บรายการเหล่านี้

พวงกุญแจมีการปรับใช้เป็นฐานข้อมูล SQLite ที่จัดเก็บบนระบบไฟล์ ฐานข้อมูลมีเพียงฐานเดียว โดย Securityd Daemon จะกำหนดว่ารายการพวงกุญแจใดที่กระบวนการทำงานหรือแอพสามารถเข้าถึงได้ API การเข้าถึงพวงกุญแจทำให้มีการเรียกไปยังดีมอน ซึ่งจะสอบถามการให้สิทธิ์ “keychain-access-groups,” “application-identifier,” และ “application-group” ของแอพ กลุ่มสิทธิ์จะอนุญาตรายการพวงกุญแจให้มีการแบ่งปันระหว่างแอพ แทนที่จะจำกัดการเข้าถึงไปยังกระบวนการทำงานเดียว

รายการพวงกุญแจสามารถแบ่งปันระหว่างแอพต่างๆ จากผู้พัฒนารายเดียวกันเท่านั้น ซึ่งจะจัดการโดยกำหนดให้แอพของบริษัทอื่นต้องใช้กลุ่มสิทธิ์อนุญาตที่มีคำนำหน้าระบุหน้ารายการพวงกุญแจผ่าน Apple Developer Program ผ่านกลุ่มแอพพลิเคชั่น ข้อกำหนดคำนำหน้าและกลุ่มแอพพลิเคชั่นที่ไม่เหมือนกันมีการบังคับใช้ผ่านการลงชื่อรหัส โปรไฟล์การกำหนดสิทธิ์ และ Apple Developer Program

องค์ประกอบของรายการพวงกุญแจ

รายการพวงกุญแจแต่ละรายการจะมี Metadata ระดับผู้ดูแล (เช่น ตราประทับเวลา “สร้างเมื่อ” และ “อัพเดทล่าสุด”) พร้อมทั้งกลุ่มสิทธิ์อนุญาต

และยังมีแฮช SHA-1 ของคุณลักษณะที่เคยใช้เพื่อสอบถามรายการ (เช่น ชื่อบัญชีและเซิร์ฟเวอร์) เพื่อให้สามารถค้นหาได้โดยไม่ต้องถอดรหัสแต่ละรายการ และท้ายที่สุดคือมีข้อมูลการเข้ารหัส ซึ่งประกอบด้วยสิ่งต่อไปนี้:

- หมายเลขเวอร์ชั่น
- ข้อมูลรายการการควบคุมการเข้าถึง (ACL)
- ค่าที่กำหนดว่ารายการอยู่ในคลาสการป้องกันใด
- กุญแจตามรายการจะถูกห่อด้วยกุญแจคลาสการป้องกัน
- พจนานุกรมคุณลักษณะที่อธิบายรายการ (โดยส่งไปที่ SecItemAdd) ซึ่งเข้ารหัสเป็น plist แบบฐานสอง และเข้ารหัสด้วยกุญแจรายรายการ

การเข้ารหัสคือ AES 128 ใน GCM (โหมด Galois/Counter) การกลุ่มสิทธิ์อนุญาตจะรวมอยู่ในคุณลักษณะและได้รับการปกป้องด้วยแท็ก GMAC ที่คำนวณในระหว่างที่เข้ารหัส

ข้อมูลพวงกุญแจได้รับการป้องกันโดยใช้โครงสร้างคลาสที่คล้ายคลึงกับที่ใช้ในการป้องกันข้อมูลของไฟล์ คลาสเหล่านี้มีลักษณะการทำงานเหมือนกับคลาสการป้องกันข้อมูลของไฟล์ แต่ใช้กุญแจที่เป็นเอกลักษณ์และเป็นส่วนหนึ่งของ API ที่ตั้งชื่อต่างกัน

ความพร้อมใช้งาน	การป้องกันข้อมูลไฟล์	การป้องกันข้อมูลในพวงกุญแจ
เมื่อปลดล็อค	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
เมื่อล็อค	NSFileProtectionCompleteUnlessOpen	ไม่มี
หลังจากปลดล็อคครั้งแรก	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
ตลอดเวลา	NSFileProtectionNone	kSecAttrAccessibleAlways
รหัสผ่านถูกเปิดใช้งาน	ไม่มี	kSecAttrAccessible-WhenPasscodeSetThisDeviceOnly

แอพที่ใช้งานบริการรีเฟรชพื้นหลังสามารถใช้ `kSecAttrAccessibleAfterFirstUnlock` สำหรับรายการพวงกุญแจที่จำเป็นต้องได้รับการเข้าถึงในระหว่างการอัพเดทพื้นหลัง

คลาส `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly` จะทำงานเหมือนกับ kSecAttrAccessibleWhenUnlocked อย่างไรก็ตามคลาสจะใช้งานได้เฉพาะเมื่ออุปกรณ์ได้รับการกำหนดค่าด้วยรหัสผ่าน คลาสนี้จะมีอยู่เฉพาะใน Keybag ของระบบ โดยจะไม่ถูกเชื่อมข้อมูลไปยังพวงกุญแจ iCloud ไม่ถูกสำรองข้อมูล และไม่ถูกรวมใน Keybag การฝาก หากรหัสผ่านถูกลบหรือรีเซ็ต รายการต่างๆ จะกลายเป็นรายการที่ไร้ประโยชน์โดยการทิ้งคลาสกุญแจไป

คลาสพวงกุญแจอื่นๆ มีส่วนของ “อุปกรณ์นี้เท่านั้น” ซึ่งจะได้รับการป้องกันด้วยค่า UID เสมอ เมื่อถูกคัดลอกจากอุปกรณ์ในระหว่างการสำรองข้อมูล โดยจะกลายเป็นรายการที่ไร้ประโยชน์หากจัดเก็บลงในอุปกรณ์เครื่องอื่น

Apple ได้รักษาสมดุลระหว่างความปลอดภัยและความสามารถการใช้งานอย่างรอบคอบ โดยการเลือกคลาสพวงกุญแจที่ขึ้นอยู่กับประเภทของข้อมูลที่ถูกเก็บรักษา และเมื่อจำเป็นโดย iOS ตัวอย่างเช่น ใบรับรอง VPN จะต้องสามารถใช้งานได้เสมอ เพื่อให้อุปกรณ์รักษาการเชื่อมต่ออย่างต่อเนื่อง แต่รายการนี้จะถูกจัดเป็น “ไม่สามารถเคลื่อนย้ายได้” จึงไม่สามารถย้ายไปยังอุปกรณ์อีกเครื่องได้

สำหรับรายการพวงกุญแจที่สร้างโดย iOS การป้องกันคลาสต่อไปนี้จะถูกบังคับใช้

รายการ	สามารถเข้าถึงได้
รหัสผ่าน Wi-Fi	หลังจากปลดล็อคครั้งแรก
บัญชีเมล	หลังจากปลดล็อคครั้งแรก
บัญชี Exchange	หลังจากปลดล็อคครั้งแรก
รหัสผ่าน VPN	หลังจากปลดล็อคครั้งแรก
LDAP, CalDAV, CardDAV	หลังจากปลดล็อคครั้งแรก
โทเค็นบัญชีเครือข่ายสังคม	หลังจากปลดล็อคครั้งแรก
กุญแจการเข้ารหัสโฆษณา Handoff	หลังจากปลดล็อคครั้งแรก
โทเค็น iCloud	หลังจากปลดล็อคครั้งแรก
รหัสผ่านการแชร์ในพื้นที่	เมื่อปลดล็อค
โทเค็นค้นหา iPhone ของฉัน	ตลอดเวลา
ข้อความเสียง	ตลอดเวลา
ข้อมูลสำรอง iTunes	เมื่อปลดล็อค ไม่สามารถเคลื่อนย้ายได้
รหัสผ่าน Safari	เมื่อปลดล็อค
ที่คั่นหน้า Safari	เมื่อปลดล็อค
ใบรับรอง VPN	เสมอ ไม่สามารถเคลื่อนย้ายได้

กุญแจ Bluetooth®	เสมอ ไม่สามารถเคลื่อนย้ายได้
โทเค็นบริการการแจ้งเตือนแบบผลักข้อมูลของ Apple	เสมอ ไม่สามารถเคลื่อนย้ายได้
ใบรับรอง iCloud และกุญแจส่วนตัว	เสมอ ไม่สามารถเคลื่อนย้ายได้
กุญแจ iMessage	เสมอ ไม่สามารถเคลื่อนย้ายได้
ใบรับรองและกุญแจส่วนตัวที่ติดตั้งโดยโปรไฟล์การกำหนดค่า	เสมอ ไม่สามารถเคลื่อนย้ายได้
รหัส PIN ของซิม	เสมอ ไม่สามารถเคลื่อนย้ายได้

การควบคุมการเข้าถึงพวงกุญแจ
พวงกุญแจสามารถใช้รายการควบคุมสิทธิ์ (ACL) เพื่อตั้งค่านโยบายสำหรับความสามารถการเข้าถึงและข้อกำหนดการรับรองความถูกต้อง รายการสามารถกำหนดเงื่อนไขที่เรียกขอตัวตนของผู้ใช้โดยการกำหนดให้ไม่สามารถเข้าถึงได้หากไม่รับรองความถูกต้องด้วย Touch ID หรือโดยการป้อนรหัสผ่านของอุปกรณ์ และยังสามารถจำกัดการเข้าถึงรายการได้โดยการกำหนดว่าการลงทะเบียน Touch ID ไม่มีการเปลี่ยนแปลงนับตั้งแต่เพิ่มรายการการจำกัดนี้จะช่วยป้องกันไม่ให้ผู้ประสงค์ดีเพิ่มลายนิ้วมือของตัวเองเพื่อเข้าถึงรายการในพวงกุญแจ ACL มีการประเมินภายใน Secure Enclave และจะการปล่อยสู่ Kernel เมื่อตรงตามข้อกำหนดที่ระบุเท่านั้น

การเข้าถึงรหัสผ่าน Safari ที่บันทึกไว้

แอพ iOS สามารถติดต่อกับรายการพวงกุญแจที่บันทึกโดย Safari เพื่อใส่รหัสผ่านอัตโนมัติได้โดยใช้ API สองรายการต่อไปนี้:

- `SecRequestSharedWebCredential`
- `SecAddSharedWebCredential`

การเข้าถึงจะได้รับการอนุมัติเฉพาะเมื่อทั้งผู้พัฒนาแอพและผู้ดูแลเว็บไซต์ให้การอนุญาตและผู้ใช้ให้ความยินยอม ผู้พัฒนาแอพแสดงความตั้งใจเข้าใช้งานรหัสผ่าน Safari ที่บันทึกไว้โดยการใส่สิทธิ์ในแอพของตน สิทธิ์จะแสดงรายการชื่อโดเมนของเว็บไซต์ที่เกี่ยวข้องที่ผ่านคุณสมบัติอย่างครบถ้วน เว็บไซต์จะต้องเก็บไฟล์บนเซิร์ฟเวอร์ของตนโดยแสดงรายชื่อตัวระบุชี้แอพเฉพาะของแอพที่ได้รับอนุญาต เมื่อแอพที่มีสิทธิ์ com.apple.developer.associated-domains ถูกติดตั้ง iOS จะส่งคำขอ TLS ไปยังเว็บไซต์แต่ละเว็บในรายการและร้องขอไฟล์/เว็บไซต์ที่เชื่อมโยงกับแอพของ Apple หากไฟล์ที่แสดงรายการตัวระบุชี้แอพของแอพได้รับการติดตั้ง iOS จะทำเครื่องหมายเว็บไซต์และแอพว่ามีความสัมพันธ์ที่เชื่อถือได้ iOS จะเรียกไปยัง API สองตัวเหล่านี้เฉพาะเมื่อมีความสัมพันธ์ที่เชื่อถือได้เท่านั้น โดยจะมีการแจ้งไปยังผู้ใช้ ซึ่งต้องตกลงก่อนที่รหัสผ่านใดๆ จะถูกปล่อยไปยังแอพ หรือได้รับการอัพเดท หรือถูกลบ

Keybag

กุญแจสำหรับคลาสการป้องกันข้อมูลไฟล์และพวงกุญแจจะถูกเก็บรวบรวมและจัดการใน Keybag โดย iOS จะใช้ Keybag ห้ารายการต่อไปนี้: ผู้ใช้, อุปกรณ์, การสำรองข้อมูล, การฝาก และข้อมูลสำรอง iCloud

Keybag ผู้ใช้คือที่ที่จัดเก็บคลาสกุญแจที่ถูกห่อซึ่งใช้ในการทำงานปกติของอุปกรณ์ ตัวอย่างเช่น เมื่อป้อนรหัสผ่าน กุญแจ`NSFileProtectionComplete` จะถูกโหลดจาก Keybag ระบบและแกะห่อออก หากไฟล์ plist ไบนารีเก็บอยู่ในคลาสไม่มีการป้องกัน แต่เนื้อหาของไฟล์ถูกเข้ารหัสด้วยกุญแจที่เก็บอยู่ในพื้นที่จัดเก็บที่ลบได้ เพื่อให้ความปลอดภัยกับ Keybag กุญแจนี้จะถูกล้างและสร้างใหม่ทุกครั้งที่ผู้ใช้เปลี่ยนรหัสผ่านของตน Kernel extension ที่ชื่อ `AppleKeyStore` จะจัดการ Keybag ผู้ใช้และสามารถสอบถามเกี่ยวกับสถานะการล็อคของอุปกรณ์ได้ ส่วนขยายจะรายงานว่าอุปกรณ์ปลดล็อคอยู่เมื่อสามารถเข้าถึงคลาสกุญแจทั้งหมดใน Keybag ผู้ใช้ และได้แกะห่อสำเร็จแล้วเท่านั้น

Keybag อุปกรณ์จะถูกใช้เพื่อจัดเก็บกุญแจคลาสที่ถูกห่อซึ่งใช้สำหรับการทำงานที่เกี่ยวข้องกับข้อมูลเฉพาะของอุปกรณ์ บางครั้งอุปกรณ์ iOS ที่กำหนดค่าไว้สำหรับใช้งานร่วมกันต้องการเข้าถึงข้อมูลประจำตัวก่อนที่ผู้ใช้จะเข้าสู่ระบบ ดังนั้นจึงไม่จำเป็นต้องใช้ Keybag ที่ไม่ได้รับการปกป้องด้วยรหัสของผู้ใช้ ระบบ iOS ไม่รองรับการแยกการเข้ารหัสของเนื้อหาของระบบไฟล์รายผู้ใช้ ซึ่งหมายความว่าระบบจะใช้คลาสกุญแจจาก Keybag อุปกรณ์เพื่อห่อกุญแจรายไฟล์ อย่างไรก็ตามพวงกุญแจจะใช้คลาสกุญแจจาก Keybag ผู้ใช้เพื่อปกป้องรายการในพวงกุญแจของผู้ใช้ บนอุปกรณ์ iOS ที่กำหนดค่าสำหรับใช้โดยผู้ใช้เพียงคนเดียว (การกำหนดค่าเริ่มต้น) Keybag อุปกรณ์และ Keybag ผู้ใช้จะเป็นอันเดียวกัน และได้รับการป้องกันโดยรหัสผ่านตัวเลขของผู้ใช้

Keybag ของข้อมูลสำรองจะถูกสร้างขึ้นเมื่อ iTunes ทำการสำรองข้อมูลแบบเข้ารหัสและจัดเก็บบนคอมพิวเตอร์ที่สำรองข้อมูลของอุปกรณ์อยู่ Keybag ใหม่จะถูกสร้างขึ้นด้วยชุดของกุญแจชุดใหม่ และข้อมูลที่สำรองไว้จะถูกเข้ารหัสอีกครั้งไปยังกุญแจใหม่เหล่านั้น ตามที่อธิบายก่อนหน้านี้ รายการพวงกุญแจที่ไม่สามารถเคลื่อนย้ายได้จะถูกห่อด้วยกุญแจที่ได้จากค่า UID ซึ่งทำให้สามารถกู้คืนรายการเหล่านั้นไปที่อุปกรณ์ดั้งเดิมที่สำรองข้อมูลนั้นได้ แต่จะทำให้เข้าถึงไม่ได้บนอุปกรณ์เครื่องอื่น

Keybag ได้รับการป้องกันด้วยรหัสผ่านที่ตั้งค่าใน iTunes ซึ่งผ่านการทำซ้ำของ PBKDF2 เป็นจำนวน 10,000 ครั้ง แม้จะมีค่าการทำซ้ำที่สูง แต่ไม่มีการผูกกับอุปกรณ์เฉพาะเครื่อง ดังนั้นในทางทฤษฎีแล้ว จะสามารถพยายามทำการโจมตี Keybag ของข้อมูลสำรองด้วยการเดารหัสผ่านโดยใช้คอมพิวเตอร์หลายเครื่องพร้อมกันได้ ภัยคุกคามนี้สามารถจำกัดได้โดยใช้รหัสผ่านที่มีความปลอดภัยสูงพอ

หากผู้ใช้เลือกไม่เข้ารหัสการสำรองข้อมูล iTunes ไฟล์การสำรองข้อมูลจะไม่ถูกเข้ารหัสไม่ว่าจะอยู่ในคลาสการป้องกันข้อมูลใด แต่พวงกุญแจจะยังคงได้รับการป้องกันด้วยกุญแจที่มาจากค่า UID นี่เป็นสาเหตุที่รายการพวงกุญแจจะโอนย้ายไปยังอุปกรณ์เครื่องใหม่เฉพาะเมื่อรหัสผ่านการสำรองข้อมูลมีการตั้งไว้เท่านั้น

Keybag การฝากใช้สำหรับการเชื่อมข้อมูล iTunes และ MDM Keybag นี้อนุญาตให้ iTunes สำรองข้อมูลและเชื่อมข้อมูลโดยไม่ต้องเรียกขอให้ผู้ใช้ป้อนรหัสผ่าน และอนุญาตให้เซิร์ฟเวอร์ MDMล้างรหัสผ่านของผู้ใช้จากระยะไกล Keybag นี้มีการจัดเก็บบนคอมพิวเตอร์ที่ใช้เพื่อเชื่อมข้อมูลกับ iTunes หรือบนเซิร์ฟเวอร์ MDM ที่จัดการอุปกรณ์

Keybag การฝากจะปรับปรุงประสบการณ์ของผู้ใช้ในระหว่างการเชื่อมข้อมูลอุปกรณ์ ซึ่งต้องใช้การเข้าถึงคลาสทั้งหมดของข้อมูล เมื่ออุปกรณ์ที่ล็อคด้วยรหัสผ่านได้รับการเชื่อมต่อไปยัง iTunes ครั้งแรก ผู้ใช้จะได้รับแจ้งให้ป้อนรหัสผ่าน จากนั้นอุปกรณ์จะสร้าง Keybag การฝากที่มีคลาสกุญแจเดียวกันกับที่ใช้บนอุปกรณ์ที่ได้รับการป้องกันด้วยกุญแจที่สร้างใหม่ Keybag การฝากและกุญแจที่ป้องกันจะถูกแยกระหว่างอุปกรณ์และโฮสต์หรือเซิร์ฟเวอร์ โดยข้อมูลจะถูกจัดเก็บบนอุปกรณ์ในคลาสป้องกันจนกว่ามีการรับรองความถูกต้องของผู้ใช้รายแรก นี่เป็นสาเหตุที่รหัสผ่านอุปกรณ์จะต้องได้รับการป้อนก่อนที่ผู้ใช้จะสำรองข้อมูลกับ iTunes เป็นครั้งแรกหลังจากรีบูต

ในกรณีของการอัพเดทซอฟต์แวร์ OTA ผู้ใช้จะได้รับแจ้งขอรหัสผ่านของเขาหรือเธอเมื่อเริ่มต้นการอัพเดท ซึ่งจะใช้เพื่อสร้างโทเค็นการปลดล็อคครั้งเดียวอย่างปลอดภัย ซึ่งจะปลดล็อค Keybag ผู้ใช้หลังจากการอัพเดท โทเค็นนี้ไม่สามารถสร้างได้โดยปราศจากการป้อนรหัสผ่านของผู้ใช้ และโทเค็นที่สร้างก่อนหน้าใดๆ จะกลายเป็นโมฆะ หากรหัสผ่านของผู้ใช้เปลี่ยน

โทเค็นการปลดล็อคครั้งเดียวใช้สำหรับการติดตั้งรายการอัพเดทซอฟต์แวร์ทั้งแบบต้องจัดการหรือแบบไม่ต้องจัดการ โทเค็นจะถูกเข้ารหัสด้วยกุญแจที่มาจากค่าปัจจุบันของตัวนับทางเดียวใน Secure Enclave, ค่า UUID ของ Keybag และค่า UID ของ Secure Enclave

การเพิ่มตัวนับโทเค็นการปลดล็อคครั้งเดียวใน Secure Enclave จะทำให้โทเค็นที่มีอยู่ใดๆ กลายเป็นโมฆะ ตัวนับจะเพิ่มขึ้นเมื่อมีการใช้งานโทเค็น หลังจากการปลดล็อคครั้งแรกของอุปกรณ์ที่เริ่มต้นการทำงานใหม่ เมื่อรายการอัพเดทซอฟต์แวร์ถูกยกเลิก (โดยผู้ใช้หรือโดยระบบ) หรือเมื่อตัวจับเวลานโยบายสำหรับโทเค็นหมดอายุลง

โทเค็นการปลดล็อคครั้งเดียวสำหรับการอัพเดทซอฟต์แวร์ที่ต้องจัดการจะหมดอายุหลัง 20 นาที โทเค็นนี้จะถูกส่งออกจาก Secure Enclave และมีการเขียนไปยังพื้นที่จัดเก็บที่ลบได้ ตัวจับเวลานโยบายจะเพิ่มค่าการนับหากอุปกรณ์ไม่รีบูตภายใน 20 นาที

สำหรับการอัพเดทซอฟต์แวร์ที่ไม่ต้องจัดการ ซึ่งมีการตั้งค่าเมื่อผู้ใช้เลือก “ติดตั้งภายหลัง” เมื่อได้รับแจ้งให้อัพเดท หน่วยประมวลผลแอพพลิเคชั่นจะสามารถเก็บโทเค็นการปลดล็อคครั้งเดียวไว้ใน Secure Enclave ก่อนหมดอายุได้สูงสุด 8 ชั่วโมง หลังจากนั้น ตัวจับเวลานโยบายจะเพิ่มค่าการนับ

Keybag การสำรองข้อมูล iCloud คล้ายคลึงกับ Keybag การสำรองข้อมูล คลาสกุญแจทั้งหมดใน Keybag นี้ไม่สมมาตร (ใช้งาน Curve25519 เหมือนกับคลาสการป้องกันข้อมูลป้องกันหากไม่เปิดอยู่) ดังนั้นการสำรองข้อมูล iCloud สามารถทำได้ในพื้นหลัง สำหรับคลาสการป้องกันข้อมูลทั้งหมดยกเว้นไม่มีการป้องกัน ข้อมูลที่เข้ารหัสจะถูกอ่านจากอุปกรณ์และส่งไปยัง iCloud คลาสกุญแจที่สัมพันธ์กันจะได้รับการป้องกันโดยกุญแจ iCloud คลาสกุญแจพวงกุญแจจะถูกห่อด้วยกุญแจที่ได้จากค่า UID แบบเดียวกับข้อมูลสำรอง iTunes ที่ไม่เข้ารหัส Keybag แบบไม่สมมาตรยังใช้สำหรับการสำรองข้อมูลในส่วนการกู้คืนพวงกุญแจของพวงกุญแจ iCloud

การออกใบรับรองความปลอดภัยและโปรแกรม

หมายเหตุ: สำหรับข้อมูลเรื่องการรับรองความปลอดภัยของผลิตภัณฑ์ การตรวจสอบและคำแนะนำสำหรับ iOS โปรดดู
support.apple.com/kb/HT202739?virelocale=th_TH

การตรวจสอบความถูกต้องทางการเข้ารหัส (FIPS 140-2)

โมดูลการเข้ารหัสใน iOS ได้รับการตรวจสอบความถูกต้องว่าเป็นไปตามมาตรฐานการประมวลผลข้อมูลสหรัฐอเมริกากลาง (FIPS) 140-2 ระดับ 1 หลังจากการออกแต่ละครั้งตั้งแต่ iOS 6 โมดูลการเข้ารหัสใน iOS 9 เหมือนกับโมดูลใน iOS 8 แต่ตามแนวปฏิบัติหลังการออกแต่ละครั้ง Apple ได้ส่งโมดูลเพื่อตรวจสอบความถูกต้องอีกครั้ง โปรแกรมนี้ตรวจสอบความถูกต้องของกระบวนการเข้ารหัสสำหรับแอพของ Apple และของบริษัทอื่นที่ใช้งานบริการการเข้ารหัส iOS อย่างเหมาะสม

การรับรองเกณฑ์ทั่วไป (ISO 15408)

Apple ได้เริ่มขอใบรับรอง iOS ภายใต้โปรแกรมการออกใบรับรองเกณฑ์ที่ใช้ทั่วไป (CCC) แล้ว ใบรับรองที่เสร็จสมบูรณ์สองรายการแรกคือ VID10695 สำหรับ iOS 9 ที่ใช้กับโปรไฟล์การป้องกันพื้นฐานอุปกรณ์เคลื่อนที่ v2.0 (MDFPP2) และ VID10714 ที่ใช้กับโปรไฟล์การป้องกันไคลเอ็นต์ VPN IPSecPP1.4 (VPNIPSecPP1.4) ใบรับรองที่มีผลอยู่จะเสร็จสมบูรณ์สำหรับโปรโตคอล MDM ในตัวที่ใช้กับโปรไฟล์การป้องกัน MDM Agent EP 2.0 (MDMAgentEP2) ในเร็วๆ นี้ Apple ได้มีบทบาทอย่างแพร่หลายในชุมชนเทคนิคสากล (ITC) ในการพัฒนาโปรไฟล์การป้องกัน (PPs) ที่ยังใช้งานไม่ได้ในปัจจุบัน โดยมุ่งเน้นไปที่การประเมินเทคโนโลยีความปลอดภัยของอุปกรณ์เคลื่อนที่หลัก Apple มุ่งมั่นประเมินและติดตามเพื่อขอใบรับรองสำหรับ PP เวอร์ชั่นใหม่และเวอร์ชั่นอัพเดทของเวอร์ชั่นในปัจจุบัน

โซลูชั่นเชิงพาณิชย์สำหรับข้อมูลลับ (CSfC)

หากสามารถทำได้ Apple ยังส่งแพลตฟอร์ม iOS และบริการอื่นๆ ที่หลากหลายเพื่อให้รวมอยู่ในรายการส่วนโปรแกรมโซลูชั่นเชิงพาณิชย์สำหรับข้อมูลลับ (CSfC) โดยเฉพาะอย่างยิ่ง iOS สำหรับแพลตฟอร์มอุปกรณ์เคลื่อนที่และไคลเอ็นต์ IKEv2 สำหรับไคลเอ็นต์ IPSec VPN (VPN แบบ IKEv2 ที่เปิดเสมอเท่านั้น) เนื่องจากแพลตฟอร์มและบริการของ Apple ต้องผ่านการรับรองเกณฑ์ทั่วไป แพลตฟอร์มและบริการจะถูกส่งให้รวมอยู่ในรายการส่วนโปรแกรม CSfC เช่นกัน

คู่มือการกำหนดค่าความปลอดภัย

Apple ได้ทำงานร่วมกับรัฐบาลทั่วโลกเพื่อพัฒนาคู่มือที่ระบุวิธีและคำแนะนำในการรักษาสภาพแวดล้อมที่ปลอดภัยมากขึ้น หรือที่เรียกว่า “การทำให้อุปกรณ์ปลอดภัยยิ่งขึ้น” คู่มือเหล่านี้ให้ข้อมูลที่ละเอียดและผ่านการตรวจสอบอย่างรอบคอบเกี่ยวกับวิธีกำหนดค่าคุณสมบัติใน iOS สำหรับการป้องกันที่ดียิ่งขึ้น

ความปลอดภัยของแอพ

แอพอยู่ในกลุ่มส่วนประกอบที่สำคัญที่สุดของสถาปัตยกรรมความปลอดภัยอุปกรณ์เคลื่อนที่สมัยใหม่ ในขณะที่แอพให้ประโยชน์ด้านการทำงานที่น่ามหัศจรรย์สำหรับผู้ใช้ แต่ก็มีโอกาสที่จะส่งผลกระทบต่อความปลอดภัยระบบ ความเสถียร และข้อมูลผู้ใช้ในทางลบหากไม่ได้รับการดูแลอย่างเหมาะสม

เนื่องจากสาเหตุนี้ iOS จึงมอบการป้องกันจำนวนหลายชั้นเพื่อให้มั่นใจว่าแอพมีการลงชื่อและตรวจสอบความถูกต้อง และจะอยู่ใน Sandbox เพื่อป้องกันข้อมูลของผู้ใช้ องค์ประกอบเหล่านี้มอบแพลตฟอร์มสำหรับแอพที่มีความเสถียรและปลอดภัย และช่วยให้ผู้พัฒนาแอพหลายพันคนสามารถส่งมอบแอพหลายพันรายการบน iOS ได้โดยไม่ส่งผลกระทบต่อความสมบูรณ์ของระบบโดยรวม และผู้ใช้สามารถเข้าถึงแอพเหล่านี้ได้บนอุปกรณ์ iOS ได้โดยไม่ต้องกลัวไวรัส มัลแวร์ หรือการโจมตีที่ไม่ได้รับอนุญาต

การเซ็นชื่อรหัสของแอพ

เมื่อ Kernel ของ iOS เริ่มทำงาน Kernel นั้นจะควบคุมว่ากระบวนการทำงานของผู้ใช้และแอพใดบ้างที่สามารถทำงานได้ เพื่อให้มั่นใจว่าแอพทั้งหมดมาจากแหล่งที่รู้จักและได้รับการอนุญาต และไม่ได้ถูกรบกวน iOS กำหนดว่ารหัสที่ปฏิบัติการได้ทั้งหมดต้องได้รับการลงชื่อโดยใช้ใบรับรองที่ออกโดย Apple แอพที่มาพร้อมอุปกรณ์ เช่น แอพเมลและ Safari จะได้รับการลงชื่อโดย Apple แอพของบริษัทอื่นจะต้องได้รับการตรวจสอบความถูกต้องและลงชื่อโดยใช้ใบรับรองที่ออกโดย Apple การลงชื่อรหัสที่บังคับเป็นการต่อยอดแนวคิดลำดับการตรวจสอบความน่าเชื่อถือจาก OS ไปยังแอพ และป้องกันแอพของบริษัทอื่นจากการโหลดรหัสที่ไม่ได้ลงชื่อหรือจากการใช้รหัสที่แก้ไขตัวเอง

หากต้องการพัฒนาและติดตั้งแอพบนอุปกรณ์ iOS ผู้พัฒนาต้องลงทะเบียนกับ Apple และเข้าร่วม Apple Developer Program ตัวตนจริงของผู้พัฒนาแต่ละราย ไม่ว่าจะเป็นบุคคลหรือธุรกิจจะได้รับการยืนยันโดย Apple ก่อนที่ใบรับรองของผู้พัฒนาจะออก ใบรับรองนี้ทำให้ผู้พัฒนาสามารถลงชื่อในแอพและส่งไปยัง App Store เพื่อการกระจายได้ ผลลัพธ์ก็คือแอพทั้งหมดใน App Store ถูกส่งโดยบุคคลหรือองค์กรที่ระบุตัวตนได้ จึงเป็นการช่วยขัดขวางการสร้างแอพที่เป็นอันตราย แอพยังได้รับการตรวจสอบโดย Apple เพื่อให้แน่ใจว่าทำงานตามที่อธิบายและไม่มีข้อผิดพลาดหรือปัญหาอื่นๆ ที่เห็นได้อย่างชัดเจน นอกเหนือจากเทคโนโลยีตามที่กล่าวถึงแล้ว กระบวนการคัดสรรนี้ยังให้ความมั่นใจแก่ลูกค้าถึงคุณภาพของแอพที่พวกเขาซื้อ

iOS อนุญาตให้ผู้พัฒนาฝังเฟรมเวิร์กลงในแอพของตน ซึ่งสามารถใช้งานได้โดยตัวแอพเองหรือโดยส่วนขยายที่ฝังอยู่ภายในแอพ เพื่อป้องกันระบบและแอพอื่นจากการโหลดรหัสของบริษัทอื่นภายในพื้นที่ที่อยู่ของตน ระบบจะทำการตรวจสอบความถูกต้องลายเซ็นรหัสของคลังไดนามิคทั้งหมดที่ประมวลผลลิงก์เมื่อเวลาเริ่มทำงาน การยืนยันนี้ทำได้ผ่านตัวระบุชี้ทีม(ID ทีม) ซึ่งได้มาจากใบรับรองที่ออกโดย Apple ตัวระบุชี้ทีมคือสตริงตัวอักษรและตัวเลข 10 อักขระ ตัวอย่างเช่น 1A2B3C4D5F โปรแกรมอาจลิงก์กับคลังแพลตฟอร์มใดๆ ที่มาพร้อมระบบหรือคลังใดๆ ที่มีตัวระบุชี้ทีมเดียวกันในลายเซ็นรหัสเป็นโปรแกรมปฏิบัติงานหลัก เนื่องจากโปรแกรมปฏิบัติงานที่จัดส่งเป็นส่วนหนึ่งของระบบไม่มีตัวระบุชี้ทีม โปรแกรมจะสามารถลิงก์กับคลังที่ส่งมากับตัวระบบเองเท่านั้น

ธุรกิจยังมีความสามารถในการเขียนแอพภายในองค์กรสำหรับใช้งานภายในองค์กรของตนและแจกจ่ายให้กับพนักงานของตน ธุรกิจและองค์กรสามารถสมัครโปรแกรมผู้พัฒนา Apple แบบองค์กร (ADEP) ด้วยหมายเลข D-U-N-S ได้ Apple จะอนุมัติผู้สมัครหลังจากยืนยันตัวตนและเกณฑ์คุณสมบัติ เมื่อองค์กรกลายเป็นสมาชิกของ ADEP องค์กรจะสามารถลงทะเบียนเพื่อรับโปรไฟล์การกำหนดสิทธิ์ที่อนุญาตให้แอพภายในองค์กรสามารถทำงานบนอุปกรณ์ที่อนุญาตได้ ผู้ใช้จะต้องมีโปรไฟล์การกำหนดสิทธิ์ติดตั้งอยู่เพื่อที่จะใช้งานแอพภายในองค์กร ทั้งนี้เพื่อรับรองว่าเฉพาะผู้ใช้ที่ควรได้สิทธิ์ขององค์กรเท่านั้นที่จะ

สามารถโหลดแอพลงในอุปกรณ์ iOS ของตนได้ แอพที่ติดตั้งผ่าน MDM จะได้รับความเชื่อถือแบบโดยนัย เนื่องจากความสัมพันธ์ระหว่างองค์กรและอุปกรณ์ได้รับการจัดตั้งเรียบร้อยแล้ว ไม่เช่นนั้น ผู้ใช้จะต้องอนุญาตโปรไฟล์การกำหนดสิทธิ์ของแอพในการตั้งค่า องค์กรสามารถจำกัดผู้ใช้จากการอนุญาตแอพจากผู้พัฒนาที่ไม่รู้จักได้ เมื่อเปิดใช้แอพองค์กรใดๆ เป็นครั้งแรก อุปกรณ์จะต้องได้รับการยืนยันเชิงบวกจาก Apple ว่าแอพได้รับอนุญาตให้ทำงาน

iOS ไม่อนุญาตให้ผู้ใช้ติดตั้งแอพที่ไม่ได้ลงชื่อซึ่งอาจเป็นอันตรายจากเว็บไซต์อื่น หรือใช้งานรหัสที่ไม่ได้รับความเชื่อถือ ซึ่งแตกต่างจากแพลตฟอร์มอุปกรณ์เคลื่อนที่อื่นๆ บนรันไทม์ ลายเซ็นรหัสจะตรวจสอบหน้าหน่วยความจำโปรแกรมปฏิบัติงานทั้งหมดว่าเป็นแบบเดียวกับที่ได้รับการโหลดหรือไม่เพื่อยืนยันว่าแอพไม่ได้ถูกแก้ไขหลังจากที่ติดตั้งหรืออัพเดทล่าสุด

ความปลอดภัยของกระบวนการรันไทม์

เมื่อแอพได้รับการยืนยันว่ามาจากแหล่งที่ได้รับอนุญาต iOS จะบังคับใช้มาตรการความปลอดภัยที่ออกแบบมาเพื่อป้องกันไม่ให้ทำให้ความปลอดภัยของแอพอื่นหรือระบบที่เหลือหละหลวม

แอพบริษัทอื่นทั้งหมดจะอยู่ใน “Sandbox” จึงถูกจำกัดจากการเข้าถึงไฟล์ที่จัดเก็บโดยแอพอื่นหรือจากการทำการเปลี่ยนแปลงกับอุปกรณ์ สิ่งนี้ป้องกันแอพไม่ให้เก็บข้อมูลหรือแก้ไขข้อมูลที่จัดเก็บโดยแอพอื่น แอพแต่ละตัวมีไดเร็กเทอรี่เริ่มต้นเฉพาะสำหรับไฟล์ของแอพ ซึ่งจะมีการกำหนดแบบสุ่มเมื่อแอพมีการติดตั้ง หากแอพของบริษัทอื่นต้องการเข้าถึงข้อมูลนอกเหนือจากข้อมูลของตนเอง แอพจะต้องใช้บริการที่ iOS มีบริการให้อย่างชัดแจ้งเท่านั้น

ไฟล์ระบบและทรัพยากรยังถูกป้องกันจากแอพของผู้ใช้อีกด้วย โดยคุณสมบัติส่วนมากของ iOS จะทำงานในฐานะ “mobile” ของผู้ใช้ที่ไม่ได้รับสิทธิพิเศษ และแอพของบริษัทอื่นทั้งหมดก็จะทำงานในฐานะนี้เช่นกัน ขณะที่พาร์ทิชั่น OS ทั้งพาร์ทิชั่นจะต่อเชื่อมเป็นแบบอ่านอย่างเดียว เครื่องมือที่ไม่จำเป็น เช่น บริการการเข้าสู่ระบบระยะไกลจะไม่ถูกรวมอยู่ในซอฟต์แวร์ระบบ และ API ไม่อนุญาตให้แอพยกระดับสิทธิ์ของตนเพื่อแก้ไขแอพอื่นหรือตัว iOS เอง

การเข้าถึงข้อมูลผู้ใช้และคุณสมบัติ เช่น iCloud และความสามารถในการเพิ่มฟังก์ชันของแอพบริษัทอื่นจะถูกควบคุมโดยสิทธิ์ที่ประกาศ โดยสิทธิ์คือคู่ค่ากุญแจที่มีการลงชื่อไปยังแอพและอนุญาตการรับรองความถูกต้องเหนือไปจากปัจจัยรันไทม์เช่น ID ผู้ใช้ Unix เนื่องจากสิทธิ์มีการลงชื่อแบบดิจิตอล จึงไม่สามารถเปลี่ยนแปลงได้ สิทธิ์มีการใช้เป็นอย่างมากโดยแอพระบบและ Daemon เพื่อทำการที่ต้องได้รับสิทธิ์เฉพาะที่กระบวนการทำงานต้องทำงานในระดับราก สิ่งนี้ช่วยลดโอกาสของการยกระดับสิทธิ์โดยแอพพลิเคชั่นระบบหรือ Daemon ที่ความปลอดภัยหละหลวมได้เป็นอย่างมาก

นอกจากนี้ แอพจะสามารถทำการประมวลผลพื้นหลังผ่าน API ที่ระบบมีให้ได้เท่านั้น จุดนี้ทำให้แอพสามารถทำงานได้ต่อโดยไม่ลดประสิทธิภาพการทำงานหรือส่งผลต่ออายุแบตเตอรี่เป็นอย่างมาก

การสุ่มเค้าโครงพื้นที่ที่อยู่ (ASLR) จะป้องกันการแอบแฝงใช้ประโยชน์ของข้อผิดพลาดที่ทำให้หน่วยความจำเสียหาย แอพในตัวใช้ ASLR เพื่อรับรองว่าพื้นที่หน่วยความจำทั้งหมดมีการสุ่มเมื่อเริ่มเปิดทำงาน การกำหนดที่อยู่หน่วยความจำของรหัสโปรแกรมปฏิบัติการ คลังระบบ และส่วนโปรแกรมที่เกี่ยวข้องแบบสุ่มช่วยลดโอกาสของการแอบแฝงใช้ประโยชน์ที่ซับซ้อนจำนวนมาก ตัวอย่างเช่น ความพยายามโจมตี return-to-libc เพื่อหลอกอุปกรณ์ให้ใช้งานรหัสที่เป็นอันตรายโดยการควบคุมที่อยู่หน่วยความจำของสแตกและคลังระบบ การสุ่มตำแหน่งของสิ่งเหล่านี้ทำให้การโจมตียากขึ้นในการปฏิบัติการ โดยเฉพาะอย่างยิ่งบนอุปกรณ์หลายเครื่อง Xcode ซึ่งเป็นสภาพแวดล้อมการพัฒนา iOS จะผสานโปรแกรมของบริษัทอื่นเข้ากับการเปิดการสนับสนุน ASLR โดยอัตโนมัติ

iOS ให้การป้องกันเพิ่มเติมโดยใช้คุณสมบัติ ARM's Execute Never ซึ่งจะทำเครื่องหมายหน้าหน่วยความจำเป็นไม่สามารถปฏิบัติงานได้ หน้าหน่วยความจำที่มีเครื่องหมายเป็นทั้งเขียนได้และปฏิบัติงานได้จะสามารถใช้ได้เฉพาะแอพที่อยู่ในเงื่อนไขที่ควบคุมเหล่านี้อย่างไม่ผิดเพี้ยนเท่านั้น: Kernel จะตรวจสอบตัวตนของสิทธิ์การลงชื่อรหัสไดนามิคของ Apple เท่านั้น แม้ในกรณีนั้น เฉพาะการเรียก mmap แบบเดี่ยวเท่านั้นที่จะสามารถทำเพื่อร้องขอหน้าปฏิบัติงานได้และเขียนได้ซึ่งจะได้รับที่อยู่แบบสุ่ม Safari ใช้งานคุณสมบัตินี้สำหรับคอมไพเลอร์ JavaScript JIT ของตน

ส่วนขยาย

iOS อนุญาตให้แอพมอบคุณสมบัติการทำงานไปยังแอพอื่นโดยการมอบส่วนขยาย ส่วนขยายคือไบนารีโปรแกรมปฏิบัติงานที่ลงชื่อด้วยวัตถุประสงค์พิเศษซึ่งรวมเป็นแพ็คเกจอยู่ภายในแอพ ระบบจะตรวจสอบส่วนขยายในเวลาที่ติดตั้งและทำให้สามารถใช้งานไปยังแอพอื่นได้โดยใช้ระบบการจับคู่โดยอัตโนมัติ

พื้นที่ระบบที่สนับสนุนส่วนขยายเรียกว่าจุดขยาย จุดขยายแต่ละจุดให้ API และบังคับใช้นโยบายสำหรับพื้นที่นั้น ระบบจะกำหนดว่าส่วนขยายใดที่ใช้งานได้โดยอิงตามจุดขยายกับกฎการจับคู่เฉพาะ ระบบจะเริ่มต้นกระบวนการทำงานส่วนขยายตามที่จำเป็นและจัดการระยะเวลาใช้งานโดยอัตโนมัติ สามารถใช้สิทธิ์เพื่อจำกัดความพร้อมใช้งานของส่วนขยายกับแอพพลิเคชั่นระบบบางตัว ตัวอย่างเช่น วิดเจ็ตมุมมองวันนี้ ในศูนย์การแจ้ง และส่วนขยายการแบ่งปันสามารถใช้งานได้เฉพาะจากบานหน้าต่างการแบ่งปันเท่านั้น จุดขยายคือวิดเจ็ตวันนี้ การแชร์ การกระทำที่กำหนดเอง การแก้ไขรูปภาพ ตัวจัดหาเอกสาร และแป้นพิมพ์แบบกำหนดเอง

ส่วนขยายจะทำงานในพื้นที่ที่อยู่ของตนเอง การสื่อสารระหว่างส่วนขยายและแอพตั้งแต่ที่มีการเปิดใช้งานใช้การสื่อสารระหว่างกระบวนการทำงานซึ่งอาศัยสื่อกลางโดยเฟรมเวิร์กระบบ ส่วนขยายและแอพจะไม่มีสิทธิ์ใช้งานไฟล์หรือหน่วยความจำของอีกฝั่ง ส่วนขยายได้รับการออกแบบมาให้แยกจากส่วนอื่นๆ ตั้งแต่แอพภายใน และจากแอพที่ใช้งาน โดยจะอยู่ใน Sandbox เหมือนกับแอพของบริษัทอื่นทั้งหมด และมีคอนเทนเนอร์แยกจากคอนเทนเนอร์ของแอพ อย่างไรก็ตาม ส่วนขยายเหล่านี้จะสามารถเข้าถึงการควบคุมความเป็นส่วนตัวได้ในระดับเดียวกับแอพคอนเทนเนอร์ ดังนั้นหากผู้ใช้อนุญาตให้แอพเข้าถึงแอพรายชื่อ ส่วนขยายที่ฝังอยู่ในแอพนี้จะได้รับอนุญาตด้วย แต่ส่วนขยายที่แอพนี้เปิดใช้งานจะไม่ได้รับอนุญาต

แป้นพิมพ์แบบกำหนดเองเป็นส่วนขยายชนิดพิเศษ เนื่องจากถูกเปิดใช้งานโดยผู้ใช้ของระบบทั้งหมด เมื่อเปิดใช้งาน ส่วนขยายจะถูกใช้กับช่องข้อความทั้งหมด ยกเว้นช่องรหัสผ่านและมุมมองข้อความแบบปลอดภัย ด้วยเหตุผลด้านการรักษาความเป็นส่วนตัว แป้นพิมพ์แบบกำหนดเองจะทำงานตามค่าเริ่มต้นใน Sandbox ที่มีข้อจำกัดมากซึ่งป้องกันการเข้าถึงบริการที่ทำงานเครือข่ายแทนกระบวนการทำงาน และ API ที่จะอนุญาตส่วนขยายให้แทรกแซงการพิมพ์ข้อมูล ผู้พัฒนาแป้นพิมพ์แบบกำหนดเองสามารถร้องขอให้ส่วนขยายของตนมี Open Access ซึ่งจะช่วยให้ระบบเรียกใช้ส่วนขยายใน Sandbox เริ่มต้นหลังจากได้รับความยินยอมจากผู้ใช้

สำหรับอุปกรณ์ที่ลงทะเบียนในการจัดการอุปกรณ์เคลื่อนที่ ส่วนขยายของเอกสารและแป้นพิมพ์จะทำตามกฎของ Managed Open In ตัวอย่างเช่น เซิร์ฟเวอร์ MDM สามารถป้องกันผู้ใช้ไม่ให้ส่งออกเอกสารจากแอพที่ได้รับการจัดการไปยังผู้ให้บริการเอกสารที่ไม่ได้รับการจัดการ หรือจากการใช้แป้นพิมพ์ที่ไม่ได้รับการจัดการด้วยแอพที่ได้รับการจัดการ นอกจากนี้ ผู้พัฒนาแอพสามารถป้องกันการใช้งานส่วนขยายแป้นพิมพ์ของบริษัทอื่นภายในแอพของตนได้

กลุ่มของแอพ

แอพและส่วนขยายของบัญชีผู้พัฒนาสามารถแชร์เนื้อหาได้ เมื่อกำหนดค่าให้เป็นส่วนหนึ่งของกลุ่มของแอพ ผู้พัฒนาสามารถเลือกสร้าง กลุ่มที่เหมาะสมบนพอร์ทัลผู้พัฒนาของ Apple และใส่ชุดของแอพและส่วนขยาย ที่ต้องการได้ เมื่อกำหนดค่าให้เป็นส่วนหนึ่งของกลุ่มของแอพ แอพจะมี สิทธิ์เข้าถึงดังต่อไปนี้:

- คอนเทนเนอร์บนดิสก์ที่ใช้ร่วมกัน ซึ่งจะอยู่บนอุปกรณ์ตราบเท่าที่ยังติดตั้งแอพจากกลุ่มนี้อย่างน้อยหนึ่งแอพ
- การตั้งค่าที่ใช้ร่วมกัน
- รายการพวงกุญแจที่ใช้ร่วมกัน

พอร์ทัลผู้พัฒนาของ Apple รับประกันว่า ID กลุ่มของแอพจะไม่ซ้ำกันตลอดทั้งระบบทั้งหมดของแอพ

การป้องกันข้อมูลในแอพ

ชุดการพัฒนาซอฟต์แวร์ iOS (SDK) เสนอ API ครบชุดที่ทำให้ผู้พัฒนาของบริษัทอื่นและของ Apple สามารถใช้งานการป้องกันข้อมูลได้ง่ายขึ้น และช่วยรับรองระดับการป้องกันแอพที่สูงที่สุด การป้องกันข้อมูลสามารถใช้งานได้สำหรับ API ของไฟล์และฐานข้อมูล ซึ่งรวมถึง NSFileManager, CoreData, NSData และ SQLite

แอพเมล (รวมถึงไฟล์แนบ), หนังสือที่ถูกจัดการ, ที่คั่นหน้า Safari, ภาพเริ่มต้นแอพ และข้อมูลตำแหน่งที่ตั้งจะถูกจัดเก็บแบบเข้ารหัสด้วยกุญแจที่ได้รับการป้องกันโดยรหัสผ่านของผู้ใช้บนอุปกรณ์ด้วยเช่นกัน ปฏิทิน (ไม่รวมไฟล์แนบ), รายชื่อ, เตือนความจำโน้ต, ข้อความ และรูปภาพ จะใช้การป้องกันจนกว่ามีการรับรองความถูกต้องของผู้ใช้รายแรก

แอพที่ผู้ใช้ติดตั้งที่ไม่ได้เลือกคลาสการป้องกันข้อมูลเฉพาะจะได้รับการป้องกันจนกว่ามีการรับรองความถูกต้องของผู้ใช้รายแรกเป็นค่าเริ่มต้น

อุปกรณ์เสริม

โปรแกรมสิทธิ์การใช้งาน Made for iPhone, iPod touch และ iPad (MFi) ให้สิทธิ์ผู้ผลิตอุปกรณ์เสริมใช้งานโปรโตคอลอุปกรณ์เสริม iPod (iAP) และส่วนประกอบฮาร์ดแวร์สนับสนุนที่จำเป็น

เมื่ออุปกรณ์เสริม MFi สื่อสารกับอุปกรณ์ iOS โดยใช้ตัวเชื่อมต่อ Lightning หรือผ่านบลูทูธ อุปกรณ์จะถามอุปกรณ์เสริมให้ยืนยันว่าได้รับการรับรองความถูกต้องโดย Apple โดยการตอบสนองกับใบรับรองที่ Apple ออกให้ ซึ่งจะได้รับการยืนยันความถูกต้องโดยอุปกรณ์ จากนั้นอุปกรณ์จะส่งคำถาม ซึ่งอุปกรณ์เสริมจะต้องตอบด้วยข้อความตอบที่ลงชื่อไว้ กระบวนการทำงานนี้ทั้งหมดจะได้รับการจัดการโดยวงจรแบบผสานที่ผลิตมาเป็นการเฉพาะซึ่ง Apple จัดหาให้กับผู้ผลิตอุปกรณ์เสริมที่ได้รับอนุญาตและสามารถมองเห็นได้ชัดเจนกับตัวอุปกรณ์เสริมเอง

อุปกรณ์เสริมสามารถร้องขอการเข้าถึงวิธีการส่งข้อมูลและคุณสมบัติการทำงานต่างๆ ได้ ตัวอย่างเช่น การเข้าถึงสตรีมเสียงดิจิตอลผ่านสาย Lightning หรือรับข้อมูลตำแหน่งที่ตั้งผ่านบลูทูธ การรับรองความถูกต้อง IC จะให้การรับรองว่าเฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่ได้รับสิทธิ์เข้าถึงอุปกรณ์แบบเต็ม หากอุปกรณ์เสริมไม่ให้การรับรองความถูกต้อง สิทธิ์การเข้าถึงจะถูกจำกัดเพียงเสียงอนาล็อคและการควบคุมการเล่นเสียงแบบอนุกรม (UART) ส่วนย่อยจำนวนน้อยเท่านั้น

AirPlay ยังใช้การรับรองความถูกต้อง IC เพื่อยืนยันว่าตัวรับได้รับการรับรองความถูกต้องโดย Apple การสตรีมเสียง AirPlay และวิดีโอ CarPlay จะใช้ MFi-SAP (โปรโตคอลการเชื่อมโยงที่ปลอดภัย) ซึ่งเข้ารหัสการสื่อสารระหว่างอุปกรณ์เสริมและอุปกรณ์โดยใช้ AES-128 ในโหมด CTR กุญแจชั่วคราวจะมีการแลกเปลี่ยนโดยใช้การแลกเปลี่ยนกุญแจ ECDH (Curve25519) และลงชื่อโดยใช้กุญแจ 1024-bit RSA ของการรับรองความถูกต้อง IC เป็นส่วนหนึ่งของโปรโตคอล Station-to-Station (STS)

HomeKit

HomeKit ให้โครงสร้างการทำงานอัตโนมัติในบ้านที่ใช้งานความปลอดภัย iCloud และ iOS เพื่อป้องกันและเชื่อมข้อมูลส่วนตัวโดยไม่เปิดเผยไปยัง Apple

ข้อมูลประจำตัว HomeKit

ข้อมูลประจำตัวและความปลอดภัยของ HomeKit ใช้คู่กุญแจสาธารณะ-ส่วนตัว Ed25519 คู่กุญแจ Ed25519 มีการสร้างบนอุปกรณ์ iOS สำหรับผู้ใช้แต่ละรายสำหรับ HomeKit ซึ่งจะกลายเป็นข้อมูลประจำตัว HomeKit ของเขาหรือเธอ คู่กุญแจใช้เพื่อรับรองความถูกต้องของการสื่อสารระหว่างอุปกรณ์ iOS และระหว่างอุปกรณ์ iOS และอุปกรณ์เสริม

กุญแจถูกจัดเก็บในพวงกุญแจ และจะถูกรวมในการสำรองพวงกุญแจที่เข้ารหัสเท่านั้น กุญแจจะถูกเชื่อมข้อมูลระหว่างอุปกรณ์โดยใช้พวงกุญแจ iCloud

การติดต่อกับอุปกรณ์เสริม HomeKit

อุปกรณ์เสริม HomeKit จะสร้างคู่กุญแจ Ed25519 ของตัวเองสำหรับใช้งานในการติดต่อกับอุปกรณ์ iOS หากอุปกรณ์เสริมมีการกู้คืนไปยังการตั้งค่าโรงงาน คู่กุญแจใหม่จะถูกสร้างขึ้น

หากต้องการสร้างความสัมพันธ์ระหว่างอุปกรณ์ iOS และอุปกรณ์เสริม HomeKit กุญแจจะถูกแลกเปลี่ยนโดยใช้โปรโตคอล Secure Remote Password (3072-bit) ซึ่งใช้รหัส 8 หลักที่ผู้ผลิตอุปกรณ์เสริมให้มา และป้อนลงอุปกรณ์ iOS โดยผู้ใช้ และจากนั้นเข้ารหัสโดยใช้ ChaCha20-Poly1305 AEAD กับกุญแจที่ได้จาก HKDF-SHA-512 ใบรับรอง MFi ของอุปกรณ์เสริมจะได้รับการยืนยันในระหว่างการตั้งค่าด้วย

เมื่ออุปกรณ์ iOS และอุปกรณ์เสริม HomeKit สื่อสารระหว่างการใช้งาน แต่ละฝั่งจะรับรองความถูกต้องของอีกฝ่ายโดยใช้กุญแจที่แลกเปลี่ยนในกระบวนการทำงานเบื้องต้น เซสชั่นแต่ละเซสชั่นถูกสร้างโดยใช้โปรโตคอล Station-to-Station และมีการเข้ารหัสโดยใช้กุญแจที่ได้จาก HKDF-SHA-512 โดยอิงตามกุญแจ Curve25519 แบบ per-session การทำงานนี้ใช้กับทั้งอุปกรณ์เสริมที่ใช้งาน IP และบลูทูธพลังงานต่ำ

พื้นที่จัดเก็บข้อมูลภายใน

HomeKit จัดเก็บข้อมูลเกี่ยวกับบ้าน อุปกรณ์เสริม ฉาก และผู้ใช้บนอุปกรณ์ iOS ของผู้ใช้ ข้อมูลที่จัดเก็บนี้จะถูกเข้ารหัสโดยใช้กุญแจที่ได้จากกุญแจข้อมูลประจำตัว HomeKit ของผู้ใช้ ร่วมกับค่า Nonce แบบสุ่ม นอกจากนี้ ข้อมูล HomeKit ยังมีการจัดเก็บโดยใช้คลาสการป้องกันข้อมูลแบบป้องกันจนกว่ามีการรับรองความถูกต้องของผู้ใช้รายแรก ข้อมูล HomeKit จะมีการสำรองข้อมูลในการสำรองข้อมูลที่เข้ารหัสเท่านั้น ตัวอย่างเช่น การสำรองข้อมูล iTunes ที่ไม่ได้เข้ารหัสจะไม่มีข้อมูล HomeKit

การเชื่อมข้อมูลระหว่างอุปกรณ์และผู้ใช้

ข้อมูล HomeKit สามารถได้รับการเชื่อมข้อมูลระหว่างอุปกรณ์ iOS ของผู้ใช้โดยใช้ iCloud และพวงกุญแจ iCloud ข้อมูล HomeKit data จะถูกเข้ารหัสระหว่างการเชื่อมข้อมูลโดยใช้กุญแจที่ได้จากข้อมูลประจำตัว HomeKit ของผู้ใช้และค่า nonce แบบสุ่ม ข้อมูลนี้จะมีการจัดการเป็น blob แบบทึบในระหว่างการเชื่อมข้อมูล ข้อมูล blob ล่าสุดจะมีการจัดเก็บใน iCloud เพื่อให้สามารถเชื่อมข้อมูลได้ แต่จะไม่ถูกใช้เพื่อวัตถุประสงค์อื่นๆ เนื่องจากข้อมูลมีการเข้ารหัสโดยใช้กุญแจที่ใช้งานได้เฉพาะบนอุปกรณ์ iOS ของผู้ใช้เท่านั้น ข้อมูลภายในจะไม่สามารถเข้าถึงได้ในระหว่างการส่งข้อมูลและการจัดเก็บ iCloud

ข้อมูล HomeKit ยังมีการเชื่อมข้อมูลระหว่างผู้ใช้หลายคนที่อยู่ภายในบ้านเดียวกันด้วย กระบวนการทำงานนี้ใช้การรับรองความถูกต้องและการเข้ารหัสที่เหมือนกับที่ใช้ระหว่างอุปกรณ์ iOS และอุปกรณ์เสริม HomeKit การรับรองความถูกต้องใช้งานกุญแจสาธารณะ Ed25519 ที่มีการแลกเปลี่ยนระหว่างอุปกรณ์เมื่อผู้ใช้ถูกเพิ่มไปยังบ้าน หลังจากผู้ใช้ใหม่ถูกเพิ่มไปยังบ้าน การสื่อสารเพิ่มเติมทุกครั้งจะได้รับการรับรองความถูกต้องและเข้ารหัสโดยใช้โปรโตคอล Station-to-Station และกุญแจแบบ per-session

เฉพาะผู้ใช้รายแรกที่เป็นผู้สร้างบ้านใน HomeKit เท่านั้นที่สามารถเพิ่มผู้ใช้ใหม่ได้ อุปกรณ์ของเขาหรือเธอจะกำหนดค่าอุปกรณ์เสริมด้วยกุญแจสาธารณะของผู้ใช้ใหม่ ดังนั้นอุปกรณ์เสริมจะสามารถรับรองความถูกต้องและรับคำสั่งจากผู้ใช้รายใหม่ได้ กระบวนการทำงานสำหรับการกำหนดค่า Apple TV สำหรับใช้งานด้วย HomeKit ใช้การรับรองความถูกต้องและการเข้ารหัสเดียวกันกับที่ใช้เมื่อเพิ่มผู้ใช้ แต่มีการทำงานโดยอัตโนมัติหากผู้ใช้ที่สร้างบ้านมีการลงชื่อเข้าใช้ iCloud บน Apple TV และ Apple TV อยู่ภายในบ้าน

หากผู้ใช้ไม่มีอุปกรณ์หลายเครื่อง และไม่อนุญาตผู้ใช้เพิ่มเติมให้เข้าใช้ในบ้านของเขาหรือเธอ ข้อมูล HomeKit จะไม่ถูกเชื่อมข้อมูลไปยัง iCloud

ข้อมูลในบ้านและแอพ

การเข้าใช้งานข้อมูลในบ้านโดยแอพได้รับการควบคุมโดยการตั้งค่าความเป็นส่วนตัวของผู้ใช้ ผู้ใช้จะได้รับคำขอให้อนุญาตการเข้าถึงเมื่อแอพร้องขอข้อมูลในบ้าน คล้ายกับการขอใช้รายชื่อ รูปภาพ และแหล่งข้อมูล iOS อื่นๆ หากผู้ใช้อนุญาต แอพจะมีสิทธิ์เข้าถึงชื่อห้อง ชื่ออุปกรณ์เสริม และห้องที่อุปกรณ์เสริมแต่ละอันอยู่ และข้อมูลอื่นๆ ตามที่ระบุรายละเอียดในเอกสารประกอบผู้พัฒนา HomeKit

Siri

Siri สามารถใช้เพื่อสอบถามและควบคุมอุปกรณ์เสริม และเปิดใช้งานฉากได้ ข้อมูลส่วนน้อยเกี่ยวกับการกำหนดค่าของบ้านจะมีการมอบให้ Siri แบบไม่ระบุชื่อ ตามที่อธิบายในหัวข้อ Siri ของเอกสารนี้ เพื่อให้ชื่อห้อง อุปกรณ์เสริม และฉากที่จำเป็นสำหรับการจดจำคำสั่ง

การเข้าถึงระยะไกล iCloud สำหรับอุปกรณ์เสริม HomeKit

อุปกรณ์เสริม HomeKit สามารถเชื่อมต่อโดยตรงกับ iCloud เพื่อเปิดใช้งานอุปกรณ์ iOS เพื่อควบคุมอุปกรณ์เสริมได้เมื่อไม่สามารถใช้งานการสื่อสารแบบบลูทูธหรือ Wi-Fi ได้

การเข้าถึงระยะไกล iCloud ได้รับการออกแบบอย่างรอบคอบเพื่อให้อุปกรณ์เสริมสามารถได้รับการควบคุมและส่งการแจ้งไปยัง Apple โดยไม่เปิดเผยข้อมูลว่าอุปกรณ์เสริมคืออะไร หรือคำสั่งหรือการแจ้งเตือนใดที่ถูกส่งไปได้ HomeKit จะไม่ส่งข้อมูลเกี่ยวกับบ้านผ่านการใช้การเข้าถึงระยะไกล iCloud

เมื่อผู้ใช้ส่งคำสั่งโดยใช้การเข้าถึงระยะไกล iCloud อุปกรณ์เสริมและอุปกรณ์ iOS จะได้รับการรับรองความถูกต้องร่วมกันและข้อมูลจะถูกเข้ารหัสโดยใช้กระบวนการทำงานเดียวกันกับที่ได้อธิบายสำหรับการเชื่อมต่อภายในพื้นที่ เนื้อหาของการติดต่อสื่อสารจะถูกเข้ารหัสและ Apple ไม่สามารถเห็นได้ การติดต่อผ่าน iCloud จะใช้งานตัวระบุชี้ iCloud ที่ลงทะเบียนระหว่างขั้นตอนการตั้งค่า

อุปกรณ์เสริมที่สนับสนุนการเข้าถึงระยะไกล iCloud จะถูกเตรียมใช้งานในระหว่างขั้นตอนการตั้งค่าอุปกรณ์เสริม ขั้นตอนการเตรียมใช้งานจะเริ่มต้นเมื่อผู้ใช้ลงชื่อเข้าสู่ iCloud ต่อไปอุปกรณ์ iOS จะขอให้อุปกรณ์เสริมลงชื่อในคำถามโดยใช้หน่วยประมวลผลร่วมการรับรองความถูกต้อง Apple ที่ถูกสร้างลงใน Built ทั้งหมดสำหรับอุปกรณ์เสริม HomeKit อุปกรณ์เสริมยังสร้างกุญแจโค้งรูปไข่ prime256v1 และกุญแจสาธารณะจถูกส่งไปยังอุปกรณ์ iOS พร้อมกับคำตอบที่ลงชื่อและใบรับรอง X.509 ของหน่วยประมวลผลร่วมการรับรองความถูกต้อง รายการเหล่านี้จะถูกใช้เพื่อร้องขอใบรับรองสำหรับอุปกรณ์เสริมจากเซิร์ฟเวอร์การกำหนดสิทธิ์ของ iCloud ใบรับรองจะถูกจัดเก็บโดยอุปกรณ์เสริม แต่ไม่มีข้อมูลระบุชี้ใดๆ เกี่ยวกับอุปกรณ์เสริม นอกจากข้อมูลที่ว่าอุปกรณ์เสริมได้รับสิทธิ์เข้าใช้งานการเข้าถึงระยะไกล iCloud สำหรับ HomeKit อุปกรณ์ iOS ที่ทำการเตรียมใช้งานยังจะส่งถุงไปยังอุปกรณ์เสริมอีกด้วย ซึ่งถุงนี้จะมี URL และข้อมูลอื่นๆ ที่จำเป็นสำหรับเชื่อมต่อเซิร์ฟเวอร์การเข้าถึงระยะไกล iCloud ข้อมูลนี้ไม่ระบุชี้ผู้ใช้หรืออุปกรณ์เสริมเฉพาะคนหรือเครื่อง

อุปกรณ์เสริมแต่ละเครื่องจะลงทะเบียนรายการผู้ใช้ที่ได้รับอนุญาตให้ใช้เซิร์ฟเวอร์การเข้าถึงระยะไกล iCloud ผู้ใช้เหล่านี้ได้รับสิทธิ์สามารถควบคุมอุปกรณ์เสริมจากผู้ใช้ที่เพิ่มอุปกรณ์เสริมไปยังบ้านได้ ผู้ใช้จะได้รับตัวระบุชี้โดยเซิร์ฟเวอร์ iCloud และสามารถได้รับการเทียบผังไปยังบัญชี iCloud เพื่อการส่งข้อความแจ้งเตือนและการตอบสนองจากอุปกรณ์เสริม เช่นเดียวกัน อุปกรณ์เสริมจะมีตัวระบุชี้ที่ออกโดย iCloud แต่ตัวระบุชี้เหล่านี้ทึบ และไม่เปิดเผยข้อมูลใดๆ เกี่ยวกับตัวอุปกรณ์เสริมเอง

เมื่ออุปกรณ์เสริมเชื่อมต่อกับการเข้าถึงระยะไกล iCloud สำหรับ HomeKit อุปกรณ์เสริมนั้นจะแสดงใบรับรองและบัตรผ่านของอุปกรณ์ ใบผ่านจะได้รับจากเซิร์ฟเวอร์ iCloud อื่นและไม่ได้ต่างกันสำหรับอุปกรณ์เสริมแต่ละเครื่อง เมื่ออุปกรณ์เสริมร้องขอใบผ่าน จะแสดงข้อมูลผู้ผลิต รุ่น และเวอร์ชั่นเฟิร์มแวร์ลงในคำขอ จะไม่มีการส่งข้อมูลที่ระบุตัวผู้ใช้หรือระบุข้อมูลบ้านลงในคำขอนี้ การเชื่อมต่อไปยังเซิร์ฟเวอร์บัตรผ่านจะไม่มีการรับรองความถูกต้อง เพื่อช่วยปกป้องความเป็นส่วนตัว

อุปกรณ์เสริมเชื่อมต่อไปยังเซิร์ฟเวอร์การเข้าถึงระยะไกล iCloud โดยใช้ HTTP/2 ที่รักษาความปลอดภัยโดยใช้ TLS 1.2 กับ AES-128-GCM และ SHA-256 อุปกรณ์เสริมจะรักษาการเชื่อมต่อไปยังเซิร์ฟเวอร์การเข้าถึงระยะไกล iCloud ให้เปิดอยู่ เพื่อให้สามารถรับข้อความที่เข้ามาและส่งการตอบสนองและการแจ้งเตือนออกไปยังอุปกรณ์ iOS ได้

HealthKit

HealthKit จะจัดเก็บและรวมข้อมูลจากแอพสุขภาพและฟิตเนสโดยได้รับอนุญาตจากผู้ใช้ HealthKit ยังทำงานกับอุปกรณ์สุขภาพและฟิตเนสโดยตรงตัววัดอัตราการเต้นของหัวใจที่ใช้บลูทูธพลังงานต่ำที่ใช้งานร่วมกันได้ และหน่วยประมวลผลร่วมการเคลื่อนไหวที่รวมอยู่ในอุปกรณ์ iOS หลายรุ่น

ข้อมูลสุขภาพ

HealthKit จะจัดเก็บและรวบรวมข้อมูลมูลสุขภาพของผู้ใช้ เช่น ส่วนสูง น้ำหนัก ระยะทางที่เดิน ความดันโลหิต และอื่นๆ ข้อมูลนี้มีการจัดเก็บในคลาสการป้องกันข้อมูลการป้องกันแบบสมบูรณ์ ซึ่งหมายความว่าสามารถเข้าถึงเฉพาะหลังจากที่ผู้ใช้ป้อนรหัสผ่านของเขาหรือเธอหรือใช้ Touch ID เพื่อปลดล็อคอุปกรณ์

ฐานข้อมูลอีกอันจัดเก็บข้อมูลการทำงาน เช่น ตารางการเข้าถึงสำหรับแอพ ชื่อของอุปกรณ์ที่เชื่อมต่อกับ HealthKit และข้อมูลกำหนดการที่ใช้เพื่อเริ่มใช้งานแอพเมื่อมีข้อมูลใหม่เข้ามา ฐานข้อมูลนี้จะมีการจัดเก็บโดยใช้คลาสการป้องกันข้อมูลแบบป้องกันจนกว่ามีการรับรองความถูกต้องของผู้ใช้รายแรก

ไฟล์บันทึกชั่วคราวจะจัดเก็บบันทึกสุขภาพที่มีการสร้างเมื่ออุปกรณ์ถูกล็อค เช่น เมื่อผู้ใช้ออกกำลังกาย ข้อมูลเหล่านี้จะมีการจัดเก็บในคลาสการป้องกันข้อมูลแบบป้องกันหากไม่เปิดอยู่ เมื่ออุปกรณ์ถูกปลดล็อค ข้อมูลจะถูกนำเข้าไปยังฐานข้อมูลสุขภาพหลัก จากนั้นจะถูกลบเมื่อการผสานข้อมูลเสร็จสมบูรณ์

ข้อมูลสุขภาพจะไม่มีการเชื่อมข้อมูลระหว่างอุปกรณ์ ข้อมูลสุขภาพจะรวมอยู่ในข้อมูลสำรองของอุปกรณ์ที่สำรองไปยัง iCloud และข้อมูลสำรอง iTunes แบบเข้ารหัส ข้อมูลสุขภาพจะไม่รวมอยู่ในข้อมูลสำรอง iTunes แบบไม่เข้ารหัส

ความสมบูรณ์ของข้อมูล

ข้อมูลที่จัดเก็บในฐานข้อมูลจะรวมถึง Metadata เพื่อติดตามแหล่งที่มาของบันทึกข้อมูลแต่ละอัน Metadata นี้รวมถึงตัวระบุชี้แอพพลิเคชั่นที่ระบุชี้ว่าแอพใดที่จัดเก็บบันทึก นอกจากนี้ รายการ Metadata เพิ่มเติมอาจรวมถึงสำเนาที่ลงชื่อดิจิตอลของบันทึกด้วย ทั้งนี้เพื่อความสมบูรณ์ของข้อมูลสำหรับบันทึกที่สร้างโดยอุปกรณ์ที่ได้รับความเชื่อถือ รูปแบบที่ใช้สำหรับการลงชื่อดิจิตอลคือ Cryptographic Message Syntax (CMS) ที่ระบุใน IETF RFC 5652

การเข้าถึงโดยแอพของบริษัทอื่น

การเข้าถึงไปยัง HealthKit API ได้รับการควบคุมโดยสิทธิ์ และแอพต้องปฏิบัติตามข้อจำกัดเรื่องวิธีที่ข้อมูลจะถูกใช้ ตัวอย่างเช่น แอพไม่ได้รับอนุญาตให้ใช้งานข้อมูลสุขภาพเพื่อการโฆษณา แอพยังต้องแสดงนโยบายความเป็นส่วนตัวที่ระบุรายละเอียดการใช้งานข้อมูลสุขภาพแก่ผู้ใช้ด้วย

การเข้าใช้งานข้อมูลสุขภาพโดยแอพได้รับการควบคุมโดยการตั้งค่าความเป็นส่วนตัวของผู้ใช้ ผู้ใช้จะได้รับคำขอให้อนุญาตการเข้าถึงเมื่อแอพร้องขอข้อมูลสุขภาพ คล้ายกับการขอใช้รายชื่อ รูปภาพ และแหล่งข้อมูล iOS อื่นๆ อย่างไรก็ตามสำหรับข้อมูลสุขภาพ แอพจะได้รับสิทธิ์เข้าถึงแยกต่างหากสำหรับการอ่านและเขียนข้อมูล เช่นเดียวกับสิทธิ์แยกต่างหากสำหรับข้อมูลสุขภาพแต่ละประเภท ผู้ใช้สามารถดูและเพิกถอนสิทธิ์ที่อนุญาตให้เข้าถึงข้อมูลสุขภาพได้ในแท็บแหล่งของแอพสุขภาพ

หากอนุญาตให้เขียนข้อมูล แอพพลิคชั่นจะสามารถอ่านข้อมูลที่เขียนโดยแอพได้ด้วย หากอนุญาตให้อ่านข้อมูล แอพจะสามารถอ่านข้อมูลที่เขียนโดยแหล่งที่มาทั้งหมดได้ อย่างไรก็ตาม แอพไม่สามารถกำหนดสิทธิ์ที่อนุญาตให้กับแอพอื่นได้ นอกจากนี้ แอพไม่สามารถบอกได้ว่าตัวแอพเองได้รับสิทธิ์การอ่านข้อมูลสุขภาพหรือไม่ เมื่อแอพไม่มีสิทธิ์อ่าน การสอบถามทั้งหมดจะไม่ได้รับข้อมูลกลับมา ซึ่งเหมือนกับการตอบสนองกรณีที่ฐานข้อมูลว่างเปล่าจะส่งกลับ ข้อนี้ช่วยป้องกันแอพจากการแทรกแซงสถานะสุขภาพของผู้ใช้โดยการเรียนรู้ว่าข้อมูลประเภทใดที่ผู้ใช้ติดตามอยู่

ID ทางแพทย์

แอพสุขภาพให้ตัวเลือกแก่ผู้ใช้ในการกรอกแบบฟอร์ม ID ทางแพทย์ด้วยข้อมูลที่อาจสำคัญหากเกิดเหตุฉุกเฉินทางการแพทย์ ข้อมูลจะมีการใส่หรืออัพเดทด้วยตัวเอง และไม่ถูกเชื่อมข้อมูลกับข้อมูลในฐานข้อมูลสุขภาพ

ดูข้อมูล ID ทางแพทย์ได้โดยการแตะปุ่มฉุกเฉินบนหน้าจอล็อค ข้อมูลมีการจัดเก็บบนอุปกรณ์โดยใช้คลาสการป้องกันข้อมูลแบบไม่มีการป้องกัน ดังนั้นจะสามารถเข้าถึงได้โดยไม่ต้องป้อนรหัสผ่านของอุปกรณ์ ID ทางแพทย์เป็นคุณสมบัติเสริมที่ช่วยให้ผู้ใช้สามารถตัดสินใจได้ว่าจะเลือกสมดุลความปลอดภัยและความเป็นส่วนตัวอย่างไร

โน้ตที่ปลอดภัย

แอพโน้ตมีคุณสมบัติโน้ตที่ปลอดภัยซึ่งทำให้ผู้ใช้สามารถป้องกันเนื้อหาของโน้ตฉบับที่ต้องการป้องกันได้ โน้ตที่ปลอดภัยจะเข้ารหัสโดยใช้วลีรหัสผ่านที่ผู้ใช้กำหนดและจำเป็นต้องใช้เพื่อดูโน้ตบน iOS, OS X และเว็บไซต์ iCloud

เมื่อผู้ใช้ดำเนินการป้องกันโน้ต จะได้กุญแจแบบ 16 ไบต์จากวลีรหัสผ่านของผู้ใช้โดยใช้ PBKDF2 และ SHA256 เนื้อหาของโน้ตจะถูกเข้ารหัสโดยใช้ AES-GCM บันทึกใหม่จะถูกสร้างใน Core Data และ CloudKit เพื่อจัดเก็บโน้ตที่เข้ารหัส แท็ก และเวคเตอร์การเริ่มต้นทำงาน และโน้ตต้นฉบับจะถูกลบโดยไม่มีการเขียนข้อมูลที่เข้ารหัสแล้วลงไปแทน ไฟล์แนบก็จะถูกเข้ารหัสด้วยวิธีการเดียวกัน ไฟล์แนบที่รองรับประกอบด้วยรูปภาพ ภาพสเก็ตช์ แผนที่ และเว็บไซต์ โน้ตที่มีไฟล์แนบประเภทอื่นๆ จะเข้ารหัสไม่ได้ และจะไม่สามารถเพิ่มไฟล์แนบที่ไม่รองรับลงในโน้ตที่ปลอดภัย

เมื่อผู้ใช้ป้อนวลีรหัสผ่านเสร็จแล้ว ไม่ว่าเพื่อดูหรือสร้างโน้ตที่ปลอดภัยก็ตาม แอพโน้ตจะเปิดเซสชั่นที่ปลอดภัย ขณะที่เซสชั่นนี้เปิดอยู่ ผู้ใช้จะไม่จำเป็นต้องป้อนวลีรหัสผ่านหรือใช้ Touch ID เพื่อดูหรือป้องกันโน้ตอื่นๆ อย่างไรก็ตาม หากโน้ตบางฉบับมีวลีรหัสผ่านอื่น เซสชั่นที่ปลอดภัยจะปรับใช้กับโน้ตที่ป้องกันด้วยวลีรหัสผ่านที่ใช้อยู่ในปัจจุบันเท่านั้น เซสชั่นที่ปลอดภัยจะปิดลงเมื่อผู้ใช้แตะปุ่มล็อคตอนนี้ในแอพโน้ต เมื่อโน้ตสลับไปทำงานในเบื้องหลังนานเกินสามนาที หรือเมื่อล็อคอุปกรณ์

ผู้ใช้ที่ลืมวลีรหัสผ่านของตัวเองยังสามารถดูโน้ตที่ปลอดภัยหรือทำการป้องกันโน้ตอื่นได้หากเขาเปิดใช้งาน Touch ID บนอุปกรณ์ไว้ นอกจากนี้ แอพโน้ตยังจะแสดงคำใบ้ที่ผู้ใช้กำหนดไว้เองหลังจากป้อนวลีรหัสผ่านผิดสามครั้ง ผู้ใช้ต้องทราบวลีรหัสผ่านปัจจุบันจึงจะสามารถเปลี่ยนวลีรหัสผ่านได้

ผู้ใช้สามารถรีเซ็ตวลีรหัสผ่านได้หากลืมวลีรหัสผ่านปัจจุบัน คุณสมบัตินี้ทำให้ผู้ใช้สามารถสร้างโน้ตที่ปลอดภัยฉบับใหม่ด้วยวลีรหัสผ่านใหม่ได้ แต่จะไม่ทำให้ผู้ใช้สามารถดูโน้ตที่ได้รับการรักษาความปลอดภัยฉบับก่อนหน้า ผู้ใช้ยังคงสามารถดูโน้ตที่ได้รับการรักษาความปลอดภัยฉบับก่อนหน้าได้หากนึกวลีรหัสผ่านออก การรีเซ็ตวลีรหัสผ่านต้องใช้วลีรหัสผ่านของบัญชี iCloud ของผู้ใช้

Apple Watch

Apple Watch ใช้คุณสมบัติความปลอดภัยและเทคโนโลยีที่สร้างมาสำหรับ iOS เพื่อช่วยป้องกันข้อมูลบนอุปกรณ์ เช่นเดียวกับ การสื่อสารกับ iPhone ที่จับคู่กันอยู่และการสื่อสารกับอินเทอร์เน็ต สิ่งนี้รวมถึงเทคโนโลยี เช่น การป้องกันข้อมูลและการควบคุมการเข้าถึงพวงกุญแจ รหัสผ่านของผู้ใช้จะถูกโยงกับ UID ของอุปกรณ์เพื่อสร้างกุญแจการเข้ารหัสด้วย

การจับคู่ Apple Watch กับ iPhone ได้รับการรักษาความปลอดภัยโดยใช้กระบวนการทำงาน out-of-band (OOB) เพื่อแลกเปลี่ยนกุญแจสาธารณะ ตามด้วยความลับที่ใช้ร่วมกัน BTLE link Apple Watch จะแสดงรูปแบบเคลื่อนไหว ซึ่งจะได้รับการจับภาพบนกล้อง iPhone รูปแบบประกอบด้วยความลับที่เข้ารหัสซึ่งใช้สำหรับการจับคู่ BTLE 4.1 out-of-band การป้อน BTLE Passkey แบบมาตรฐานใช้เพื่อเป็นวิธีการจับคู่แบบสำรอง หากจำเป็น

เมื่อเซสชั่น BTLE ถูกสร้างขึ้น Apple Watch และ iPhone จะแลกเปลี่ยนกุญแจโดยใช้กระบวนการทำงานที่ปรับปรุงจาก IDS ตามที่อธิบายในส่วน iMessage ของเอกสารนี้ เมื่อกุญแจถูกแลกเปลี่ยน กุญแจเซสชั่นบลูทูธจะถูกทิ้ง และการติดต่อทั้งหมดระหว่าง Apple Watch และ iPhone จะถูกเข้ารหัสโดยใช้ IDS โดยมี BTLE และลิงก์ Wi-Fi ที่เข้ารหัสให้การเข้ารหัสอีกชั้นเป็นชั้นที่สอง การสลับกุญแจมีการใช้ทุก 15 นาทีเพื่อจำกัดช่วงที่ไร้การป้องกัน หากการจราจรเครือข่ายมีช่องโหว่

เพื่อรองรับแอพที่จำเป็นต้องสตรีมข้อมูล การเข้ารหัสทำโดยใช้วิธีตามที่อธิบายในส่วน FaceTime ของเอกสารนี้ โดยใช้บริการ IDS ที่ให้บริการโดย iPhone ที่จับคู่

Apple Watch ใช้งานพื้นที่จัดเก็บที่เข้ารหัสของฮาร์ดแวร์และการป้องกันแบบคลาสของไฟล์และรายการพวงกุญแจ ตามที่อธิบายในส่วนการป้องกันข้อมูลของเอกสารนี้ Keybag ที่ควบคุมด้วยสิทธิ์การเข้าถึงสำหรับรายการพวงกุญแจถูกใช้ด้วยเช่นกัน กุญแจที่ใช้สำหรับการติดต่อระหว่างนาฬิกาและ iPhone ยังได้รับการรักษาความปลอดภัยโดยใช้การป้องกันแบบคลาส

เมื่อ Apple Watch ไม่ได้อยู่ในระยะทำการของบลูทูธ จะสามารถใช้ Wi-Fi แทนได้ Apple Watch จะไม่เข้าร่วมเครือข่าย Wi-Fi นอกเสียจากจะมีข้อมูลประจำตัวที่ต้องใช้อยู่บน iPhone ที่จับคู่กันอยู่ ซึ่งจะมอบรายการของเครือข่ายที่รู้จักให้กับนาฬิกาโดยอัตโนมัติ

Apple Watch สามารถล็อคด้วยตัวเองได้โดยการกดปุ่มข้างค้างไว้ นอกจากนี้ยังจะใช้การตรวจจับความเคลื่อนไหวเพื่อพยายามล็อคอุปกรณ์โดยอัตโนมัติหลังจากที่ถอดนาฬิกาออกจากข้อมือเป็นเวลาไม่นาน เมื่อล็อคอยู่ จะใช้งาน Apple Pay ไม่ได้ หากปิดใช้การล็อคอัตโนมัติด้วยการตรวจจับข้อมือในการตั้งค่า จะเป็นการปิดใช้งาน Apple Pay ด้วย การตรวจสอบข้อมือปิดโดยใช้แอพ Apple Watch บน iPhone การตั้งค่านี้ยังสามารถบังคับใช้ได้โดยใช้การจัดการอุปกรณ์เคลื่อนที่

iPhone ที่จับคู่กันอยู่ยังสามารถปลดล็อคนาฬิกาได้ด้วยหากสวมนาฬิกาอยู่ ซึ่งจะทำได้โดยการสร้างการเชื่อมต่อที่ได้รับการรับรองความถูกต้องโดยใช้กุญแจที่สร้างขึ้นระหว่างการจับคู่ iPhone จะส่งกุญแจ ซึ่งนาฬิกาจะใช้เพื่อปลดล็อคกุญแจการป้องกันข้อมูลของตน iPhone จะไม่ทราบรหัสผ่านนาฬิกาและไม่มีการส่งรหัสเช่นกัน คุณสมบัตินี้สามารถปิดได้โดยใช้แอพ Apple Watch บน iPhone

Apple Watch สามารถจับคู่กับ iPhone ได้ครั้งละหนึ่งเครื่องเท่านั้น การจับคู่กับ iPhone เครื่องใหม่จะเป็นการลบเนื้อหาและข้อมูลทั้งหมดจาก Apple Watch โดยอัตโนมัติ

การเปิดใช้งาน ค้นหา iPhone ของฉัน บน iPhone ที่จับคู่ยังเป็นการเปิดใช้งานการล็อคการเข้าใช้งานเครื่องบน Apple Watch ด้วย การล็อคการเข้าใช้งานเครื่องทำให้การใช้หรือขาย Apple Watch ที่สูญหายหรือถูกขโมยเป็นเรื่องยากขึ้นด้วย การล็อคการเข้าใช้งานเครื่องต้องใช้ Apple ID และรหัสผ่านของผู้ใช้เพื่อเลิกจับคู่ ลบ หรือเปิดใช้งาน Apple Watch ใหม่

ความปลอดภัยของเครือข่าย

นอกเหนือจากความปลอดภัยในตัวที่ Apple ใช้เพื่อป้องกันข้อมูลที่จัดเก็บบนอุปกรณ์ iOS แล้ว ก็ยังมีมาตรการความปลอดภัยเครือข่ายอีกหลายมาตรการที่องค์กรสามารถใช้เพื่อรักษาข้อมูลให้ปลอดภัย เมื่อข้อมูลมีการส่งต่อไปมาบนอุปกรณ์ iOS ได้

ผู้ใช้อุปกรณ์เคลื่อนที่จะต้องสามารถเข้าถึงเครือข่ายองค์กรได้จากทุกแห่งในโลกดังนั้นจึงเป็นเรื่องสำคัญที่ต้องให้แน่ใจว่าผู้ใช้ได้รับการอนุญาตและข้อมูลของผู้ใช้ได้รับการปกป้องระหว่างส่งข้อมูล iOS ใช้โปรโตคอลเครือข่ายมาตรฐานสำหรับการติดต่อสื่อสารที่ได้รับการรับรองความถูกต้อง ที่ได้รับอนุญาต และที่เข้ารหัส และมอบการเข้าถึงแบบเดียวกันนี้ให้กับผู้พัฒนาด้วย เพื่อบรรลุวัตถุประสงค์ด้านความปลอดภัยเหล่านี้ iOS ผสานเทคโนโลยีที่ได้รับการรับรองและมาตรฐานล่าสุดสำหรับการเชื่อมต่อเครือข่ายทั้ง Wi-Fi และข้อมูลเซลลูลาร์

บนแพลตฟอร์มอื่น ซอฟต์แวร์ไฟร์วอลล์มีความจำเป็นเพื่อใช้ป้องกันพอร์ตติดต่อสื่อสารแบบเปิดจากการโจมตี เนื่องจาก iOS ประสบความสำเร็จในการลดการโจมตีให้น้อยลงโดยการจำกัดพอร์ตการฟังและนำยูทิลิตี้เครือข่ายที่ไม่จำเป็นออก เช่น เทลเน็ต เชลล์ หรือเซิร์ฟเวอร์เว็บ ซอฟต์แวร์ไฟร์วอลล์เพิ่มเติมจึงไม่มีความจำเป็นบนอุปกรณ์ iOS

TLS

iOS รองรับ Transport Layer Security (TLS v1.0, TLS v1.1, TLS v1.2) และ DTLS โดย Safari, ปฏิทิน, เมล และแอพอินเทอร์เน็ตอื่นๆ จะใช้กลไกการทำงานเหล่านี้โดยอัตโนมัติเพื่อเปิดใช้งานช่องทางการติดต่อที่เข้ารหัสระหว่างอุปกรณ์และบริการเครือข่าย API ระดับสูง (เช่น CFNetwork) ทำให้ผู้พัฒนาใช้งาน TLS ในแอพของตนได้ง่ายขึ้น ในขณะที่ API ระดับต่ำ (SecureTransport) ให้การควบคุมในระดับที่ละเอียด ตามค่าเริ่มต้น CFNetwork จะไม่อนุญาต SSLv3 และแอพที่ใช้งาน WebKit (เช่น Safari) จะถูกห้ามไม่ให้สร้างการเชื่อมต่อ SSLv3

ความปลอดภัยของการส่งข้อมูลแอพ

ความปลอดภัยของการส่งข้อมูลแอพระบุข้อกำหนดการเชื่อมต่อเพื่อให้แอพปฏิบัติตามเพื่อแนวปฏิบัติการเชื่อมต่อที่ปลอดภัยที่สุด เมื่อใช้งาน API ที่ชื่อ NSURLConnection, CFURL หรือ NSURLSession

เซิร์ฟเวอร์จะต้องรองรับ TLS 1.2, forward secrecy เป็นอย่างต่ำ และใบรับรองจะต้องถูกต้องและลงชื่อโดยใช้ SHA-256 หรือสูงกว่า พร้อมกับมีกุญแจ 2048-bit RSA หรือกุญแจโค้งรูปไข่ 256-bit เป็นอย่างต่ำ

การเชื่อมต่อเครือข่ายที่ไม่ตรงตามข้อกำหนดเหล่านี้จะล้มเหลว นอกเสียจากแอพนั้นจะแทนที่ App Transport Security ใบรับรองที่ไม่ถูกต้องจะทำให้เกิดความล้มเหลวและไม่มีการเชื่อมต่อ App Transport Security จะปรับใช้โดยอัตโนมัติกับแอพทั้งหมดที่คอมไพล์มาสำหรับ iOS 9

VPN

บริการเครือข่ายที่ปลอดภัยเช่นเครือข่ายส่วนตัวเสมือนโดยทั่วไปจะต้องใช้การตั้งค่าและกำหนดค่าขั้นต่ำเพื่อให้ทำงานได้กับอุปกรณ์ iOS อุปกรณ์ iOS ทำงานได้กับเซิร์ฟเวอร์ VPN ที่สนับสนุนโปรโตคอลและวิธีการรับรองความถูกต้องต่อไปนี้:

- IKEv2/IPSec ที่มีการรับรองความถูกต้องโดยความลับที่ใช้ร่วมกัน, ใบรับรอง RSA, ใบรับรอง ECDSA, EAP-MSCHAPv2 หรือ EAP-TLS
- Pulse Secure, Cisco, Aruba Networks, SonicWALL, Check Point, Palo Alto Networks, Open VPN, AirWatch, MobileIron, NetMotion Wireless และ F5 Networks SSL-VPN โดยใช้แอพไคลเอ็นต์ที่เหมาะสมจาก App Store
- Cisco IPSec ที่มีการรับรองความถูกต้องผู้ใช้โดยรหัสผ่าน, RSA SecurID หรือ CRYPTOCard และการรับรองความถูกต้องเครื่องโดยความลับที่ใช้ร่วมกันและใบรับรอง
- L2TP/IPSec ที่มีการรับรองความถูกต้องผู้ใช้โดยรหัสผ่าน MS-CHAPV2, RSA SecurID หรือ CRYPTOCard และการรับรองความถูกต้องเครื่องโดยความลับที่ใช้ร่วมกัน
- PPTP ที่มีการรับรองความถูกต้องผู้ใช้โดยรหัสผ่าน MS-CHAPV2 และ RSA SecurID หรือ CRYPTOCard ได้รับการรองรับแต่ไม่แนะนำ

iOS รองรับ VPN On Demand สำหรับเครือข่ายที่ใช้การรับรองความถูกต้องโดยใบรับรอง นโยบาย IT ระบุว่าโดเมนใดที่ต้องการการเชื่อมต่อ VPN โดยใช้โปรไฟล์การกำหนดค่า

iOS ยังรองรับการสนับสนุน Per App VPN โดยทำให้การเชื่อมต่อ VPN ง่ายขึ้นและใช้งานได้ละเอียดยิ่งขึ้น การจัดการอุปกรณ์เคลื่อนที่ (MDM) สามารถระบุการเชื่อมต่อสำหรับแอพที่ได้รับการจัดการแต่ละอัน และ/หรือโดเมนเฉพาะอันได้ใน Safari สิ่งนี้ช่วยรับรองว่าข้อมูลที่ปลอดภัยจะส่งไปยังและส่งจากเครือข่ายองค์กรเสมอ และข้อมูลส่วนตัวของผู้ใช้จะไม่ถูกส่งไป

iOS รองรับ VPN แบบเปิดเสมอซึ่งจะสามารถกำหนดค่าสำหรับอุปกรณ์ที่จัดการผ่าน MDM และกำกับดูแลโดยใช้ Apple Configurator หรือโปรแกรมการลงทะเบียนอุปกรณ์ การทำงานนี้จะช่วยให้ผู้ใช้ไม่ต้องเปิด VPN เพื่อเปิดทำงานการป้องกันเมื่อเชื่อมต่อเครือข่ายเซลลูลาร์และ Wi-Fi VPN แบบเปิดเสมอจะให้การควบคุมการส่งข้อมูลของอุปกรณ์แบบเต็มกับองค์กรโดยการสร้างช่องทางเชื่อมต่อข้อมูล IP ทั้งหมดกลับไปยังองค์กร โปรโตคอลการสร้างช่องทางเชื่อมต่อค่าเริ่มต้น IKEv2 จะรักษาความปลอดภัยของการส่งผ่านข้อมูลด้วยการเข้ารหัสข้อมูล องค์กรสามารถติดตามดูและกรองการส่งข้อมูลไปยังและจากอุปกรณ์ รักษาความปลอดภัยของข้อมูลภายในเครือข่าย และจำกัดการเข้าใช้งานอินเทอร์เน็ตของอุปกรณ์ได้

Wi-Fi

iOS รองรับโปรโตคอล Wi-Fi มาตรฐานอุตสาหกรรม ซึ่งรวมถึง WPA2 Enterprise เพื่อให้การเข้าถึงไปยังเครือข่ายองค์กรแบบไร้สายที่มีการรับรองความถูกต้อง WPA2 Enterprise ใช้การเข้ารหัส 128-bit AES โดยให้ระดับการรับรองสูงสุดว่าข้อมูลจะได้รับการป้องกันเมื่อส่งและรับการติดต่อสื่อสารบนการเชื่อมต่อเครือข่าย Wi-Fi ด้วยการรองรับ 802.1X อุปกรณ์ iOS สามารถผสานใช้กับสภาพแวดล้อมการรับรองความถูกต้อง RADIUS ที่กว้างขวางได้ วิธีการรับรองความถูกต้องไร้สาย 802.1X ที่รองรับบน iPhone และ iPad รวมถึง EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1 และ LEAP

iOS ใช้ที่อยู่การควบคุมการเข้าถึงสื่อ (MAC) แบบสุ่มเมื่อทำการสแกน Preferred Network Offload (PNO) เมื่ออุปกรณ์ไม่ได้เชื่อมโยงกับเครือข่าย Wi-Fi และหน่วยประมวลผลของ iOS พักอยู่ หน่วยประมวลผลของอุปกรณ์จะเข้าสู่โหมดพักเครื่องไม่นานหลังจากที่หน้าจอถูกปิด การสแกน PNO จะทำงานเพื่อระบุว่าผู้ใช้สามารถเชื่อมต่อกับเครือข่าย Wi-Fi ที่ต้องการเพื่อทำกิจกรรม เช่น การเชื่อมข้อมูลกับ iTunes แบบไร้สายได้หรือไม่

iOS ยังใช้ที่อยู่ MAC แบบสุ่มเมื่อทำการสแกน Preferred Network Offload (ePNO) เมื่ออุปกรณ์ไม่ได้เชื่อมโยงกับเครือข่าย Wi-Fi หรือหน่วยประมวลผลอยู่ระหว่างการพัก การสแกน ePNO จะทำงานเมื่ออุปกรณ์ใช้บริการหาตำแหน่งที่ตั้งสำหรับแอพซึ่งใช้กรอบภูมิศาสตร์ เช่น เตือนความจำตามตำแหน่งที่ระบุว่าอุปกรณ์อยู่ใกล้ตำแหน่งเฉพาะหรือไม่

เนื่องจากที่อยู่ MAC ของอุปกรณ์ตอนนี้จะเปลี่ยนเมื่อไม่ได้เชื่อมต่อกับเครือข่าย Wi-Fi ที่อยู่นี้จึงไม่สามารถใช้เพื่อติดตามอุปกรณ์อย่างต่อเนื่องโดยผู้ติดตามการส่งข้อมูล Wi-Fi แบบเชิงรับแม้ว่าอุปกรณ์จะเชื่อมต่อกับเครือข่ายเซลลูลาร์อยู่ก็ตาม

เราทำงานร่วมกับผู้ผลิต Wi-Fi เพื่อบอกให้ทราบว่าการสแกนพื้นหลังใช้ที่อยู่ MAC แบบสุ่ม และทั้ง Apple หรือผู้ผลิตไม่สามารถทำนายที่อยู่ MAC แบบสุ่มเหล่านี้ได้

การสุ่มที่อยู่ Wi-Fi MAC ไม่ได้รับการรองรับบน iPhone 4s

บลูทูธ

การรองรับบลูทูธใน iOS ได้รับการออกแบบมาให้มอบคุณสมบัติการทำงานที่มีประโยชน์โดยไม่เพิ่มการเข้าถึงข้อมูลส่วนตัวอย่างไม่จำเป็น อุปกรณ์ iOS สนับสนุนการเชื่อมต่อ Encryption Mode 3, Security Mode 4 และ Service Level 1 โดย iOS รองรับโปรไฟล์บลูทูธดังต่อไปนี้:

- โปรไฟล์แฮนด์ฟรี (HFP 1.5)
- โปรไฟล์การเข้าถึงสมุดโทรศัพท์ (PBAP)
- โปรไฟล์การแจกจ่ายเสียงขั้นสูง (A2DP)
- โปรไฟล์การควบคุมเสียง/วิดีโอระยะไกล (AVRCP)
- โปรไฟล์เครือข่ายพื้นที่ส่วนตัว (PAN)
- โปรไฟล์อุปกรณ์อินเทอร์เฟซมนุษย์ (HID)

การรองรับสำหรับโปรไฟล์เหล่านี้แตกต่างไปตามอุปกรณ์ สำหรับข้อมูลเพิ่มเติม โปรดดู support.apple.com/kb/ht3647?viewlocale=th_TH

การลงชื่อเข้าครั้งเดียว

iOS รองรับการรับรองความถูกต้องไปยังเครือข่ายองค์กรผ่านการลงชื่อเข้าครั้งเดียว (SSO) SSO ทำงานกับเครือข่ายที่ใช้ Kerberos เพื่อรับรองความถูกต้องผู้ใช้กับบริการที่พวกเขาได้รับอนุญาตให้เข้าถึง SSO สามารถใช้ได้สำหรับกิจกรรมเครือข่ายจำนวนมากตั้งแต่เซสชั่น Safari ที่ปลอดภัยไปจนถึงแอพของบริษัทอื่น

iOS SSO ใช้โทเค็น SPNEGO และโปรโตคอล HTTP Negotiate เพื่อทำงานร่วมกับเกตเวย์การรับรองความถูกต้องที่ใช้ Kerberos และระบบการรับรองความถูกต้องแบบผสานกับ Windows ที่รองรับตั๋ว Kerberos การรับรองความถูกต้องที่ใช้ใบรับรองได้รับการรองรับด้วยเช่นกัน การสนับสนุน SSO ใช้โปรเจ็คโอเพนซอร์ซ Heimdal

ประเภทการเข้ารหัสต่อไปนี้ได้รับการรองรับ:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari รองรับ SSO และแอพของบริษัทอื่นที่ใช้ API เครือข่าย iOS มาตรฐานก็สามารถได้รับการกำหนดค่าเพื่อใช้งานด้วยเช่นกัน หากต้องการกำหนดค่า SSO, iOS รองรับเพย์โหลดโปรไฟล์การกำหนดค่าที่อนุญาตให้เซิร์ฟเวอร์ MDM เรียกใช้การตั้งค่าที่จำเป็น ซึ่งรวมถึงการตั้งค่าชื่อหลักของผู้ใช้ (ซึ่งก็คือบัญชีผู้ใช้แอ็คทีฟไดเร็กเทอรี่) และการตั้งค่าบริเวณ Kerberos เช่นเดียวกับการกำหนดค่าว่าแอพ และ/หรือ URL เว็บ Safari ใดที่ควรได้รับอนุญาตให้ใช้ SSO

ความปลอดภัยของ AirDrop

อุปกรณ์ iOS ที่รองรับ AirDrop ใช้บลูทูธพลังงานต่ำ (BLE) และเทคโนโลยี Wi-Fi แบบเพียร์ทูเทียร์ที่ Apple สร้างเพื่อส่งไฟล์และข้อมูลไปยังอุปกรณ์ใกล้เคียง ซึ่งรวมถึงคอมพิวเตอร์ Mac ที่มีความสามารถ AirDrop ที่ใช้งาน OS X Yosemite หรือใหม่กว่า วิทยุ Wi-Fi ใช้เพื่อติดต่อโดยตรงระหว่างอุปกรณ์โดยไม่ใช้การเชื่อมต่ออินเทอร์เน็ตหรือจุดเชื่อมต่อ Wi-Fi ใดๆ

เมื่อผู้ใช้เปิดใช้งาน AirDrop ข้อมูลประจำตัว 2048-bit RSA จะถูกจัดเก็บบนอุปกรณ์ นอกจากนี้ แฮชข้อมูลประจำตัว AirDrop จะถูกสร้างโดยอิงจากที่อยู่อีเมลและหมายเลขโทรศัพท์ที่เชื่อมโยงกับ Apple ID ของผู้ใช้

เมื่อผู้ใช้เลือก AirDrop เป็นวิธีการแบ่งปันรายการ อุปกรณ์จะส่งสัญญาณ AirDrop ผ่านบลูทูธพลังงานต่ำ อุปกรณ์เครื่องอื่นที่พักอยู่ในระยะใกล้เคียงและมี AirDrop เปิดอยู่จะตรวจพบสัญญาณและตอบสนองด้วยแฮชข้อมูลประจำตัวของเจ้าของในแบบที่สั้นกว่า

AirDrop ได้รับการตั้งค่าให้แชร์กับเฉพาะรายชื่อเป็นค่าเริ่มต้น ผู้ใช้ยังสามารถเลือกได้ว่าต้องการใช้งาน AirDrop เพื่อแชร์กับทุกคนหรือปิดคุณสมบัตินี้โดยสิ้นเชิงได้ ในโหมดเฉพาะรายชื่อ แฮชข้อมูลประจำตัวที่ได้รับจะถูกเปรียบเทียบกับแฮชของบุคคลในแอพรายชื่อของผู้เริ่มต้น หากตรงกัน อุปกรณ์ที่ส่งจะสร้างเครือข่าย Wi-Fi แบบเพียร์ทูเพียร์ และประกาศแจ้งการเชื่อมต่อ AirDrop โดยใช้ Bonjour โดยใช้การเชื่อมต่อนี้ อุปกรณ์ที่รับจะส่งแฮชข้อมูลประจำตัวแบบเต็มของอุปกรณ์ไปยังผู้เริ่มต้น หากแฮชแบบเต็มยังคงตรงกับรายชื่อ ชื่อและรูปภาพของผู้รับ (หากมีอยู่ในรายชื่อ) จะถูกแสดงในหน้าการแชร์ AirDrop

เมื่อใช้งาน AirDrop ผู้ใช้ที่ส่งจะเลือกว่าต้องการแชร์กับใคร อุปกรณ์ที่ส่งจะเริ่มต้นการเชื่อมต่อแบบเข้ารหัส (TLS) กับอุปกรณ์ที่รับ ซึ่งแลกเปลี่ยนใบรับรองข้อมูลประจำตัว iCloud กัน ข้อมูลประจำตัวในใบรับรองจะได้รับการยืนยันเทียบกับแอพรายชื่อของผู้ใช้แต่ละราย จากนั้นผู้ใช้ที่รับจะได้รับคำขอให้รับการถ่ายโอนข้อมูลเข้าจากบุคคลหรืออุปกรณ์ที่ระบุ หากเลือกผู้รับหลายคน กระบวนการทำงานนี้จะมีการทำซ้ำสำหรับจุดหมายปลายทางแต่ละอัน

ในโหมดทุกคน กระบวนการทำงานเดิมจะถูกใช้หากไม่พบรายการที่ตรงกันในรายชื่อ อุปกรณ์ที่รับจะถูกแสดงในหน้าการส่ง AirDrop โดยมีเงาดำและชื่อของอุปกรณ์ ตามที่ระบุใน การตั้งค่า > ทั่วไป > เกี่ยวกับ > ชื่อ

องค์กรสามารถจำกัดการใช้งาน AirDrop สำหรับอุปกรณ์หรือแอพที่ได้รับการจัดการโดยโซลูชันการจัดการอุปกรณ์เคลื่อนที่ได้

Apple Pay

ด้วย Apple Pay ผู้ใช้สามารถใช้งานอุปกรณ์ iOS ที่รองรับและ Apple Watch เพื่อชำระเงินด้วยวิธีที่ง่าย ปลอดภัย และเป็นส่วนตัว ซึ่งเป็นวิธีที่ง่ายสำหรับผู้ใช้ และได้รับการสร้างมาด้วยความปลอดภัยแบบผสานทั้งในฮาร์ดแวร์และซอฟต์แวร์

Apple Pay ยังได้รับการออกแบบให้ป้องกันข้อมูลส่วนตัวของผู้ใช้ด้วย Apple Pay ไม่รวบรวมข้อมูลธุรกรรมใดๆ ที่สามารถโยงกลับไปยังตัวผู้ใช้ได้ ธุรกรรมการชำระเงินเกิดขึ้นระหว่างผู้ใช้ พ่อค้า และผู้ออกบัตร

ส่วนประกอบของ Apple Pay

Secure Element: Secure Element คือชิปที่ได้รับการรับรองมาตรฐานอุตสาหกรรมที่ทำงานบนแพลตฟอร์ม Java Card ซึ่งเป็นไปตามข้อกำหนดอุตสาหกรรมการเงินสำหรับการชำระเงินอิเล็กทรอนิกส์

ตัวควบคุม NFC: ตัวควบคุม NFC จัดการโปรโตคอล Near Field Communication และเปิดเส้นทางการสื่อสารระหว่างหน่วยประมวลผลแอพพลิเคชั่นและ Secure Element และระหว่าง Secure Element และเทอร์มินัลจุดการขาย

Wallet: Wallet ใช้เพื่อเพิ่มและจัดการบัตรเครดิต บัตรเดบิต บัตรรางวัล และบัตรร้านค้า และเพื่อชำระเงินด้วย Apple Pay ผู้ใช้สามารถดูบัตรของตนและข้อมูลเพิ่มเติมเกี่ยวกับผู้ออกบัตรของตน นโยบายความเป็นส่วนตัวของผู้ออกบัตรของตน รายการธุรกรรมล่าสุด และอื่นๆ เพิ่มเติมได้ใน Wallet ผู้ใช้ยังสามารถเพิ่มบัตรไปยัง Apple Pay ได้ในตัวช่วยติดตั้งและการตั้งค่า

Secure Enclave: บน iPhone และ iPad, Secure Enclave จะจัดการกระบวนการทำงานรับรองความถูกต้อง และทำให้ธุรกรรมการชำระเงินสามารถทำต่อได้ Secure Enclave จัดเก็บข้อมูลลายนิ้วมือสำหรับ Touch ID

บน Apple Watch อุปกรณ์จะต้องได้รับการปลดล็อค และผู้ใช้ต้องคลิกสองครั้งที่ปุ่มข้าง การคลิกสองครั้งจะได้รับการตรวจพบและส่งต่อไปยัง Secure Enclave โดยตรงโดยไม่ผ่านหน่วยประมวลผลแอพพลิเคชั่น

เซิร์ฟเวอร์ Apple Pay: เซิร์ฟเวอร์ Apple Pay จะจัดการสถานะของบัตรเครดิตและบัตรเดบิต ใน Wallet และหมายเลขบัญชีอุปกรณ์จะถูกจัดเก็บใน Secure Element เซิร์ฟเวอร์จะติดต่อกับทั้งอุปกรณ์และกับเซิร์ฟเวอร์เครือข่ายการชำระเงิน เซิร์ฟเวอร์ Apple Pay ยังรับผิดชอบสำหรับการเข้ารหัสข้อมูลประจำตัวการชำระเงินอีกครั้งสำหรับการชำระเงินภายในแอพ

วิธีการที่ Apple Pay ใช้งานองค์ประกอบความปลอดภัย

Secure Element มีแอพเพล็ตที่ออกแบบมาเป็นพิเศษเพื่อจัดการ Apple Pay Secure Element ยังมีแอพเพล็ตการชำระเงินที่ได้รับการรับรองโดยเครือข่ายการชำระเงิน ข้อมูลบัตรเครดิตหรือบัตรเดบิตจะถูกส่งแบบเข้ารหัสจากเครือข่ายการชำระเงินหรือผู้ออกบัตรไปยังแอพเพล็ตการชำระเงินเหล่านี้โดยใช้กุญแจที่เครือข่ายการชำระเงินและโดเมนความปลอดภัยของแอพเพล็ตการชำระเงินเท่านั้นที่รู้จัก ข้อมูลนี้จะมีการจัดเก็บภายในแอพเพล็ตการชำระเงินเหล่านี้และได้รับการป้องกันโดยใช้คุณสมบัติความปลอดภัยของ Secure Element ระหว่างธุรกรรม เทอร์มินัลจะติดต่อกับ Secure Element โดยตรงผ่านตัวควบคุม Near Field Communication (NFC) ผ่านบัสฮาร์ดแวร์สำหรับการใช้งานเฉพาะ

วิธีการที่ Apple Pay ใช้งานตัวควบคุม NFC

ในฐานะเกตเวย์ไปยัง Secure Element ตัวควบคุม NFC จะให้การรับรองว่ารายการธุรกรรมการชำระเงินโดยไม่ต้องสัมผัสทั้งหมดจะมีการทำโดยใช้เทอร์มินัลจุดการขายที่อยู่ในระยะใกล้เคียงกับอุปกรณ์ เฉพาะคำขอชำระเงินที่มาจากเทอร์มินัลในพื้นที่เท่านั้นที่จะได้รับการทำเครื่องหมายโดยตัวควบคุม NFC เป็นรายการธุรกรรมโดยไม่ต้องสัมผัส

เมื่อการชำระเงินได้รับการอนุญาตโดยผู้ถือบัตรโดยใช้ Touch ID หรือรหัสผ่าน หรือบน Apple Watch ที่ปลดล็อคโดยการคลิกสองครั้งที่ปุ่มข้าง การตอบสนองแบบไม่ต้องสัมผัสที่เตรียมโดยแอพเพล็ตการชำระเงินภายใน Secure Element จะมีการส่งโดยตัวควบคุมไปยังพื้นที่ NFC โดยเฉพาะเท่านั้น ผลลัพธ์คือ รายละเอียดสำหรับการรับรองความถูกต้องการชำระเงินสำหรับรายการธุรกรรมโดยไม่ต้องสัมผัสจะอยู่ในช่อง NFC และไม่มีการเปิดเผยไปยังหน่วยประมวลผลแอพพลิเคชั่นไม่ว่ากรณีใดๆ ในทางตรงกันข้าม รายละเอียดการรับรองความถูกต้องการชำระเงินสำหรับการชำระเงินภายในแอพจะมีการส่งไปยังหน่วยประมวลผลแอพพลิเคชั่น แต่จะส่งหลังจากที่เข้ารหัสโดย Secure Element ไปยังเซิร์ฟเวอร์ Apple Pay เท่านั้น

การจัดเตรียมบัตรเครดิตและบัตรเดบิต

เมื่อผู้ใช้เพิ่มบัตรเครดิตหรือบัตรเดบิต (รวมถึงบัตรร้านค้า) ไปยัง Apple Pay หลังจากนั้น Apple จะส่งข้อมูลบัตรแบบปลอดภัย พร้อมกับข้อมูลอื่นๆ เกี่ยวกับบัญชีและอุปกรณ์ของผู้ใช้ไปยังผู้ออกบัตร โดยการใช้ข้อมูลนี้ ผู้ออกบัตรจะตัดสินใจว่าจะอนุญาตการเพิ่มบัตรไปยัง Apple Pay หรือไม่

Apple Pay ใช้คอลล์ฝั่งเซิร์ฟเวอร์สามครั้งเพื่อรับและส่งการติดต่อกับผู้ออกบัตรหรือเครือข่ายเป็นส่วนหนึ่งของกระบวนการทำงานเตรียมใช้งานบัตร: **ช่องที่ต้องกรอก, ตรวจสอบบัตร** และ **ผูกบัตรและการเตรียมใช้งาน** ผู้ออกบัตรหรือเครือข่ายจะใช้คอลล์เหล่านี้เพื่อยืนยัน อนุญาต และเพิ่มบัตรไปยัง Apple Pay เซสชั่นเซิร์ฟเวอร์ไคลเอ็นต์เหล่านี้จะได้รับการเข้ารหัสโดยใช้ SSL

หมายเลขบัตรแบบเต็มจะไม่ถูกจัดเก็บบนอุปกรณ์หรือบนเซิร์ฟเวอร์ Apple แต่หมายเลขบัญชีอุปกรณ์ที่ไม่ซ้ำจะถูกสร้าง เข้ารหัส และจัดเก็บใน Secure Element แทน หมายเลขบัญชีอุปกรณ์ที่ไม่ซ้ำนี้จะถูกเข้ารหัสแบบที่ Apple ไม่สามารถเข้าถึงได้ หมายเลขบัญชีอุปกรณ์เป็นค่าที่ไม่ซ้ำและแตกต่างจากหมายเลขบัตรเครดิตหรือเดบิตจริง ผู้ออกบัตรสามารถป้องกันการใช้งานบัตรบนบัตรแถบแม่เหล็ก ผ่านทางโทรศัพท์ หรือทางเว็บไซต์ได้ หมายเลขบัญชีอุปกรณ์ใน Secure Element จะถูกแยกจาก iOS และ WatchOS ไม่ถูกจัดเก็บบนเซิร์ฟเวอร์ Apple Pay และไม่ถูกสำรองข้อมูลไปยัง iCloud เสมอ

บัตรสำหรับใช้งานกับ Apple Watch จะได้รับการเตรียมสำหรับ Apple Pay โดยใช้แอพ Apple Watch บน iPhone การจัดเตรียมบัตรสำหรับ Apple Watch กำหนดให้นาฬิกาต้องอยู่ภายในระยะการติดต่อของบลูทูธ บัตรจะได้รับการลงทะเบียนสำหรับใช้งานกับ Apple Watch โดยเฉพาะ และมีหมายเลขบัญชีอุปกรณ์ของตนเอง ซึ่งจะถูกจัดเก็บภายใน Secure Element บน Apple Watch

มีสามวิธีในการจัดเตรียมบัตรเครดิตหรือบัตรเดบิตลงใน Apple Pay:

- การเพิ่มบัตรเครดิตหรือบัตรเดบิตไปยัง Apple Pay ด้วยตัวเอง
- การเพิ่มบัตรเครดิตหรือบัตรเดบิตบนไฟล์จากบัญชี iTunes Store ไปยัง Apple Pay
- การเพิ่มบัตรเครดิตหรือเดบิตจากแอพของผู้ออกบัตร

การเพิ่มบัตรเครดิตหรือบัตรเดบิตไปยัง Apple Pay ด้วยตัวเอง

หากต้องการเพิ่มบัตรด้วยตัวเอง ซึ่งรวมถึงบัตรร้านค้า ชื่อ หมายเลขบัตรเครดิต วันหมดอายุ และ CVV จะถูกใช้เพื่อให้กระบวนการจัดเตรียมสะดวกขึ้น จากภายในการตั้งค่า จากแอพ Wallet หรือจากแอพ Apple Watch ผู้ใช้จะสามารถป้อนข้อมูลนั้นได้โดยการพิมพ์หรือโดยการใช้กล้อง iSight เมื่อกล้องจับภาพข้อมูลบัตรได้ Apple จะพยายามใส่ข้อมูลชื่อ หมายเลขบัตร และวันหมดอายุลงไป รูปภาพจะไม่ถูกบันทึกไปยังอุปกรณ์หรือจัดเก็บในคลังรูปภาพเสมอ เมื่อช่องทั้งหมดได้รับการกรอก กระบวนการทำงานตรวจสอบบัตรจะยืนยันช่องอื่นนอกเหนือจาก CVV ข้อมูลจะถูกเข้ารหัสและส่งไปยังเซิร์ฟเวอร์ Apple Pay

หาก ID ข้อกำหนดและเงื่อนไขถูกส่งกลับมาพร้อมกับกระบวนการตรวจสอบบัตร Apple จะดาวน์โหลดและแสดงข้อกำหนดและเงื่อนไขของผู้ออกบัตรไปยังผู้ใช้ หากผู้ใช้ยอมรับข้อกำหนดและเงื่อนไข Apple จะส่ง ID ของข้อกำหนดที่ได้รับการยอมรับ เช่นเดียวกับ CVV ไปยังกระบวนการลิงก์และกำหนดสิทธิ์ นอกจากนี้ ในฐานะส่วนหนึ่งของกระบวนการผูกบัตรและเตรียมใช้งาน Apple จะแบ่งปันข้อมูลจากอุปกรณ์กับผู้ออกบัตรหรือเครือข่าย เช่นข้อมูลเกี่ยวกับ iTunes และกิจกรรมบัญชี App Store ของคุณ (ตัวอย่างเช่น คุณมีประวัติรายการธุรกรรมภายใน iTunes ที่ยาวนานหรือไม่) ข้อมูลเกี่ยวกับอุปกรณ์ของคุณ (ตัวอย่างเช่น หมายเลขโทรศัพท์ ชื่อ และรุ่นของอุปกรณ์ของคุณร่วมกับอุปกรณ์ iOS ที่มาพร้อมกันที่จำเป็นในการตั้งค่า Apple Pay) เช่นเดียวกับตำแหน่งโดยประมาณของคุณในเวลาที่คุณเพิ่มบัตรของคุณ (หากคุณมีบริการหาตำแหน่งที่ตั้งเปิดใช้งานอยู่) โดยการใช้ข้อมูลนี้ ผู้ออกบัตรจะตัดสินใจว่าจะอนุญาตการเพิ่มบัตรไปยัง Apple Pay หรือไม่

สองสิ่งจะเกิดขึ้นเป็นผลจากกระบวนการผูกบัตรและเตรียมใช้งาน:

- อุปกรณ์จะเริ่มต้นดาวน์โหลดไฟล์บัตรผ่าน Wallet ซึ่งแสดงบัตรเครดิตหรือบัตรเดบิต
- อุปกรณ์จะเริ่มต้นผูกบัตรเข้ากับ Secure Element

ไฟล์บัตรผ่านประกอบด้วย URL เพื่อดาวน์โหลดภาพบัตร และ Metadata เกี่ยวกับบัตร เช่นข้อมูลติดต่อ แอพของผู้ออกบัตรที่เกี่ยวข้อง และคุณสมบัติที่รองรับ และยังประกอบด้วยข้อมูลสถานะบัตรผ่าน ซึ่งรวมถึงข้อมูล เช่น การปรับแต่ง Secure Element เสร็จสมบูรณ์หรือไม่ บัตรถูกระงับในปัจจุบันโดยผู้ออกบัตรหรือไม่ หรือต้องมีการยืนยันความถูกต้องเพิ่มเติมก่อนที่บัตรจะสามารถใช้ชำระเงินกับ Apple Pay หรือไม่

การเพิ่มบัตรเครดิตหรือบัตรเดบิตจากบัญชี iTunes Store ไปยัง Apple Pay

สำหรับบัตรเครดิตหรือเดบิตไฟล์กับ iTunes ผู้ใช้อาจต้องป้อนรหัสผ่าน Apple ID ของตนอีกครั้ง หมายเลขบัตรจะดึงมาจาก iTunes และกระบวนการทำงานตรวจสอบบัตรจะเริ่มต้นขึ้น หากบัตรสามารถใช้สำหรับ Apple Pay ได้ อุปกรณ์จะดาวน์โหลดและแสดงข้อกำหนดและเงื่อนไข จากนั้นส่ง ID ของข้อกำหนด และรหัสความปลอดภัยของบัตรไปยังกระบวนการผูกบัตรและเตรียมใช้งาน การยืนยันความถูกต้องเพิ่มเติมอาจเกิดขึ้นสำหรับบัตรบัญชี iTunes บนไฟล์

การเพิ่มบัตรเครดิตหรือเดบิตจากแอพของผู้ออกบัตร

เมื่อแอพได้รับการลงทะเบียนสำหรับใช้งานกับ Apple Pay กุญแจจะถูกสร้างขึ้นสำหรับแอพและเซิร์ฟเวอร์ของผู้ค้า กุญแจเหล่านี้ใช้เพื่อเข้ารหัสข้อมูลบัตรที่ถูกส่งไปยังผู้ค้า ซึ่งช่วยป้องกันข้อมูลจากการถูกอ่านโดยอุปกรณ์ iOS โฟลว์การจัดเตรียมคล้ายคลึงกับที่ใช้สำหรับบัตรที่เพิ่มด้วยตัวเองตามที่อธิบายด้านบน ยกเว้นรหัสผ่านแบบครั้งเดียวจะถูกใช้แทนที่ CVV

การยืนยันเพิ่มเติม

ผู้ออกบัตรสามารถตัดสินใจได้ว่าบัตรเครดิตหรือบัตรเดบิตต้องการการยืนยันเพิ่มเติมหรือไม่ ผู้ใช้อาจสามารถเลือกระหว่างตัวเลือกที่แตกต่างกันสำหรับการยืนยันเพิ่มเติมทั้งนี้ขึ้นอยู่กับตัวเลือกที่ผู้ออกบัตรมีให้ เช่น ข้อความตัวอักษร อีเมล การโทรหาบริการลูกค้าสัมพันธ์ หรือวิธีในแอพของบริษัทอื่นที่ได้รับการอนุญาตเพื่อทำการยืนยันให้เสร็จสมบูรณ์ สำหรับข้อความตัวอักษรหรืออีเมล ผู้ใช้จะเลือกจากข้อมูลติดต่อที่ผู้ออกบัตรมีให้บนไฟล์ รหัสจะถูกส่ง ซึ่งผู้ใช้จะต้องกรอกลงใน Wallet, การตั้งค่า หรือแอพ Apple Watch สำหรับบริการลูกค้าหรือการยืนยันโดยใช้แอพผู้ออกบัตรจะต้องดำเนินกระบวนการติดต่อสื่อสารของตัวเอง

การอนุญาตการชำระเงิน

Secure Element จะอนุญาตให้มีการชำระเงินหลังจากที่ได้รับการยืนยันความถูกต้องจาก Secure Enclave ซึ่งยืนยันว่าผู้ใช้ได้รับรองความถูกต้องด้วย Touch ID หรือรหัสผ่านอุปกรณ์เท่านั้น Touch ID คือวิธียืนยันตามค่าเริ่มต้นหากใช้ได้ แต่รหัสผ่านสามารถใช้แทน Touch ID เมื่อใดก็ได้ รหัสผ่านจะถูกเสนอให้ใช้โดยอัตโนมัติหลังจากพยายามจับคู่ลายนิ้วมือไม่สำเร็จสามครั้ง และหลังจากจับคู่ไม่สำเร็จห้าครั้ง คุณต้องใช้รหัสผ่าน รหัสผ่านยังต้องใช้เมื่อ Touch ID ไม่ได้รับการกำหนดค่าหรือเปิดใช้งานสำหรับ Apple Pay

การติดต่อระหว่าง Secure Enclave และ Secure Element จะเกิดขึ้นบนอินเทอร์เฟซแบบอนุกรม ซึ่งมี Secure Element เชื่อมต่อกับตัวควบคุม NFC ซึ่งจะเชื่อมต่อกับหน่วยประมวลผลแอพพลิเคชั่นอีกต่อหนึ่ง แม้ว่าจะไม่ถูกเชื่อมต่อโดยตรง Secure Enclave และ Secure Element จะสามารถติดต่ออย่างปลอดภัยได้โดยใช้กุญแจการจับคู่ที่แบ่งปันซึ่งได้รับการจัดเตรียมระหว่างกระบวนการผลิต การเข้ารหัสและการรับรองความถูกต้องของการติดต่อสื่อสารใช้งาน AES ซึ่งเป็นค่า nonce เข้ารหัสที่ใช้โดยทั้งสองฝ่ายเพื่อป้องกันการโจมตีการเล่นซ้ำ กุญแจการจับคู่จะถูกสร้างขึ้นภายใน Secure Enclave จากกุญแจ UID และตัวระบุชี้ Secure Element ที่ไม่ซ้ำ จากนั้นกุญแจการจับคู่จะถูกถ่ายโอนอย่างปลอดภัยจาก Secure Enclave ไปยังโมดูลความปลอดภัยฮาร์ดแวร์ (HSM) ในโรงงาน ซึ่งมีข้อมูลกุญแจที่จำเป็น จากนั้นจะถูกส่งเข้าไปยังกุญแจการจับคู่ลงใน Secure Element

เมื่อผู้ใช้อนุญาตรายการธุรกรรม Secure Enclave จะส่งข้อมูลที่ลงชื่อเกี่ยวกับประเภทของการอนุญาตและรายละเอียดเกี่ยวกับประเภทของรายการธุรกรรม (แบบไม่ต้องสัมผัสหรือภายในแอพ) ไปยัง Secure Element ซึ่งผูกอยู่กับค่า Authorization Random (AR) ค่า AR ถูกสร้างขึ้นใน Secure Enclave เมื่อผู้ใช้จัดเตรียมบัตรเครดิตเป็นครั้งแรกและค่าจะคงเดิมในขณะที่ Apple Pay มีการเปิดทำงาน โดยได้รับการป้องกันโดยการเข้ารหัสของ Secure Enclave และกลไกป้องกันการย้อนกลับ AR จะถูกส่งไปยัง Secure Element อย่างปลอดภัยผ่านกุญแจการจับคู่ เมื่อได้รับค่า AR ใหม่ Secure Element จะทำเครื่องหมายบัตรที่เพิ่มก่อนหน้าใดๆ ว่าถูกลบ

บัตรเครดิตและบัตรเดบิตที่ถูกเพิ่มไปยัง Secure Element สามารถใช้งานได้เฉพาะหาก Secure Element มีการแสดงพร้อมกับการรับรองความถูกต้องโดยใช้กุญแจการจับคู่และค่า AR เดียวกันจากที่บัตรถูกเพิ่ม ข้อนี้ช่วยให้ iOS สามารถบอกให้ Secure Enclave ระบุว่าบัตรไม่สามารถใช้ได้โดยการทำเครื่องหมายสำเนาของ AR ว่าไม่ถูกต้องภายใต้สถานการณ์ต่อไปนี้:

เมื่อรหัสผ่านถูกปิดใช้งาน

- ผู้ใช้ลงชื่อออกจาก iCloud
- ผู้ใช้เลือกลบเนื้อหาและการตั้งค่าทั้งหมด
- อุปกรณ์ถูกกู้คืนจากโหมดการกู้คืน

Apple Watch จะทำเครื่องหมายบัตรว่าไม่ถูกต้อง ในกรณีต่อไปนี้:

- รหัสผ่านของนาฬิกาถูกปิดใช้งาน
- นาฬิกาถูกเลิกจับคู่จาก iPhone
- การตรวจจับข้อมือถูกปิด

ด้วยการใช้กุญแจการจับคู่และสำเนาของค่า AR ปัจจุบัน Secure Element จะยืนยันการรับรองความถูกต้องที่ได้รับจาก Secure Enclave ก่อนที่จะเปิดใช้งานแอพเพล็ตการชำระเงินสำหรับการชำระเงินโดยไม่ต้องสัมผัส กระบวนการทำงานนี้ยังใช้กับเมื่อเรียกใช้ข้อมูลการชำระเงินที่เข้ารหัสจากแอพเพล็ตการชำระเงินสำหรับรายการธุรกรรมภายในแอพ

รหัสความปลอดภัยสำหรับธุรกรรมรายการเฉพาะที่เปลี่ยนทุกครั้ง

รายการธุรกรรมการชำระเงินทั้งหมดที่มาจากแอพเพล็ตการชำระเงินประกอบด้วยรหัสความปลอดภัยสำหรับธุรกรรมรายการเฉพาะที่เปลี่ยนทุกครั้งพร้อมกับหมายเลขบัญชีอุปกรณ์ รหัสที่ใช้ครั้งเดียวนี้ จะได้รับการคำนวณโดยใช้ตัวนับที่เพิ่มขึ้นสำหรับรายการธุรกรรมใหม่แต่ละรายการ และกุญแจที่ได้รับการจัดเตรียมในแอพเพล็ตการชำระเงินระหว่างการปรับให้บริการเฉพาะบุคคล และรหัสนี้เครือข่ายการชำระเงิน และ/หรือผู้ออกบัตรจะทราบ ข้อมูลอื่นๆ อาจถูกใช้ในการคำนวณรหัสเหล่านี้เช่นกัน ขึ้นอยู่กับรูปแบบการชำระเงิน ซึ่งประกอบด้วยข้อมูลดังต่อไปนี้:

- หมายเลขแบบสุ่มที่สร้างขึ้นโดยแอพเพล็ตการชำระเงิน
- หมายเลขแบบสุ่มอื่นที่สร้างขึ้นโดยเทอร์มินัล ในกรณีของรายการธุรกรรม NFC

หรือ

- หมายเลขแบบสุ่มอื่นที่สร้างขึ้นโดยเซิร์ฟเวอร์ ในกรณีของรายการธุรกรรมภายในแอพ

รหัสความปลอดภัยเหล่านี้จะมีการส่งมอบให้กับเครือข่ายการชำระเงินและผู้ออกบัตร ซึ่งจะทำให้พวกเขาสามารถยืนยันรายการธุรกรรมแต่ละรายการได้ ความยาวของรหัสความปลอดภัยเหล่านี้อาจแตกต่างออกไปโดยขึ้นอยู่กับประเภทของรายการธุรกรรมที่ทำ

การชำระเงินโดยไม่ต้องสัมผัสด้วย Apple Pay

หาก iPhone เปิดอยู่และตรวจพบช่อง NFC เครื่องจะแสดงข้อมูลบัตรเครดิตหรือเดบิตที่เกี่ยวข้อง หรือบัตรค่าเริ่มต้น ซึ่งมีการจัดการในการตั้งค่า ผู้ใช้ยังสามารถไปที่แอพ Wallet และเลือกบัตรเครดิตหรือเดบิต หรือเมื่ออุปกรณ์ล็อคอยู่ ให้คลิกสองครั้งที่ปุ่มโฮม

ต่อไป ผู้ใช้จะต้องรับรองความถูกต้องโดยใช้ Touch ID หรือรหัสผ่านของตนก่อนที่ข้อมูลการชำระเงินจะถูกส่งต่อ เมื่อ Apple Watch ปลดล็อคอยู่ การคลิกสองครั้งที่ปุ่มข้างจะเป็นการเปิดใช้งานบัตรค่าเริ่มต้นสำหรับการชำระเงิน ข้อมูลการชำระเงินจะไม่ถูกส่งโดยไม่ได้รับการอนุญาตจากผู้ใช้

เมื่อผู้ใช้รับรองความถูกต้อง หมายเลขบัญชีอุปกรณ์และรหัสความปลอดภัยสำหรับธุรกรรมรายการเฉพาะที่เปลี่ยนทุกครั้งจะถูกใช้เมื่อประมวลผลการชำระเงิน Apple และอุปกรณ์ของผู้ใช้จะไม่ส่งหมายเลขบัตรเครดิตหรือเดบิตจริงไปยังผู้ค้า Apple อาจได้รับข้อมูลรายการธุรกรรมที่ไม่ระบุชื่อ เช่น เวลาและตำแหน่งโดยประมาณของรายการธุรกรรม ซึ่งจะช่วยปรับปรุงผลิตภัณฑ์และบริการของ Apple Pay และผลิตภัณฑ์อื่นๆ ของ Apple

การชำระเงินด้วย Apple Pay ภายในแอพ

Apple Pay ยังสามารถใช้เพื่อทำการชำระเงินภายในแอพ iOS ได้ เมื่อผู้ใช้ชำระเงินในแอพโดยใช้ Apple Pay หลังจากนั้น Apple จะได้รับข้อมูลธุรกรรมที่เข้ารหัส และเข้ารหัสอีกครั้งด้วยกุญแจของผู้ค้าเฉพาะก่อนที่จะถูกส่งไปยังผู้ค้า Apple Pay จะรักษาข้อมูลรายการธุรกรรมที่ไม่ระบุชื่อ เช่น ยอดซื้อโดยประมาณ ข้อมูลนี้ไม่สามารถตามรอยกลับไปยังผู้ใช้ได้ และจะไม่รวมข้อมูลรายการที่ผู้ใช้ซื้อ

เมื่อแอพเริ่มต้นธุรกรรมการชำระเงิน Apple Pay เซิร์ฟเวอร์ Apple Pay จะได้รับรายการธุรกรรมที่เข้ารหัสจากอุปกรณ์ก่อนผู้ค้าจะได้รับ จากนั้นเซิร์ฟเวอร์ Apple Pay จะเข้ารหัสข้อมูลอีกครั้งโดยใช้กุญแจสำหรับผู้ค้าเฉพาะ ก่อนที่จะส่งรายการธุรกรรมต่อไปให้ผู้ค้า

เมื่อแอพร้องขอการชำระเงิน แอพจะเรียกไปยัง API เพื่อระบุว่าอุปกรณ์รองรับ Apple Pay หรือไม่ และผู้ใช้มีบัตรเครดิตหรือบัตรเดบิตที่สามารถชำระเงินบนเครือข่ายการชำระเงินที่ผู้ค้ายอมรับหรือไม่ แอพจะร้องขอชิ้นส่วนของข้อมูลใดๆ ที่จำเป็นต้องใช้เพื่อประมวลผลและทำรายการธุรกรรมให้สมบูรณ์ เช่น ที่อยู่การเรียกเก็บเงินและที่อยู่จัดส่ง และข้อมูลติดต่อ จากนั้นแอพจะขอให้ iOS แสดงหน้า Apple Pay ซึ่งจะร้องขอข้อมูลสำหรับแอพ เช่นเดียวกับข้อมูลสำคัญอื่นๆ เช่น บัตรที่ต้องใช้

ในตอนนี้ แอพจะได้รับข้อมูลเมือง รัฐ และรหัสไปรษณีย์เพื่อคำนวณค่าจัดส่งสุดท้าย ข้อมูลที่ร้องขอทั้งชุดแบบเต็มจะไม่ถูกส่งไปยังแอพจนกว่าผู้ใช้จะรับรองความถูกต้องของการชำระเงินด้วย Touch ID หรือรหัสผ่านอุปกรณ์ เมื่อการชำระเงินได้รับการรับรองความถูกต้อง ข้อมูลที่แสดงในหน้า Apple Pay จะถูกส่งไปยังผู้ค้า

เมื่อผู้ใช้รับรองความถูกต้องของการชำระเงิน จะมีการเรียกไปยังเซิร์ฟเวอร์ Apple Pay เพื่อขอรับค่า nonce ที่เข้ารหัส ซึ่งคล้ายคลึงกับค่าที่เทอร์มินัล NFC คืนกลับมาที่ใช้สำหรับรายการธุรกรรมในร้านค้า ค่า nonce พร้อมกับข้อมูลธุรกรรมอื่นๆ จะถูกส่งไปยัง Secure Element เพื่อสร้างข้อมูลประจำตัวการชำระเงินที่จะถูกเข้ารหัสด้วยกุญแจ Apple เมื่อข้อมูลประจำตัวการชำระเงินที่เข้ารหัสออกมาจาก Secure Element ข้อมูลจะส่งไปยังเซิร์ฟเวอร์ Apple Pay ซึ่งจะถอดรหัสข้อมูลประจำตัว ยืนยันค่า nonce ในข้อมูลประจำตัวเทียบกับค่า nonce ที่ส่งมาโดย Secure Element และจากนั้นเข้ารหัสข้อมูลประจำตัวการชำระเงินอีกครั้งด้วยกุญแจผู้ค้าที่เชื่อมโยงกับ ID ผู้ค้า จากนั้นจะถูกส่งกลับไปยังอุปกรณ์ ซึ่งจะส่งข้อมูลกลับไปยังแอพผ่าน API และจากนั้นแอพจะส่งข้อมูลไปยังระบบของผู้ค้าเพื่อประมวลผล ผู้ค้าสามารถถอดรหัสข้อมูลประจำตัวการชำระเงินด้วยกุญแจส่วนตัวสำหรับการประมวลผล กระบวนการนี้พร้อมกับลายเซ็นจากเซิร์ฟเวอร์ของ Apple ช่วยให้ผู้ค้าสามารถยืนยันว่ารายการธุรกรรมนั้นมีเพื่อผู้ค้ารายนี้เป็นการเฉพาะ

API จะร้องขอสิทธิ์ที่ระบุ ID ผู้ค้าที่รองรับ แอพยังสามารถรวมข้อมูลเพิ่มเติมเพื่อส่งไปยัง Secure Element ให้ลงชื่อ เช่น หมายเลขคำสั่งซื้อหรือข้อมูลประจำตัวลูกค้า ทั้งนี้เพื่อให้แน่ใจว่ารายการธุรกรรมไม่สามารถเบี่ยงเบนไปยังลูกค้ารายอื่นได้ การทำงานส่วนนี้ผู้พัฒนาแอพสามารถสร้างได้ ผู้พัฒนาแอพสามารถระบุ applicationData บน PKPaymentRequest ได้ แฮชของข้อมูลนี้จะถูกรวมอยู่ในข้อมูลการชำระเงินที่เข้ารหัส จากนั้นผู้ค้าจะเป็นผู้รับผิดชอบในการยืนยันว่าแฮช applicationData ตรงกับข้อมูลที่รวมอยู่ในข้อมูลการชำระเงิน

บัตรรางวัล

Apple Pay ใน iOS 9 รองรับโปรโตคอล Value Added Service (VAS) สำหรับการส่งข้อมูลบัตรรางวัลผู้ค้าไปยังเทอร์มินัล NFC ที่ใช้ร่วมกันได้ โปรโตคอล VAS สามารถใช้งานบนเทอร์มินัลผู้ค้า และใช้ NFC เพื่อติดต่อกับอุปกรณ์ Apple ที่รองรับได้ โปรโตคอล VAS ทำงานได้ในระยะทางที่สั้น และใช้เพื่อให้บริการเสริม เช่น การส่งข้อมูลบัตรรางวัล โดยเป็นส่วนหนึ่งของรายการธุรกรรม Apple Pay

เทอร์มินัล NFC จะเริ่มต้นรับข้อมูลบัตรโดยการส่งคำขอสำหรับบัตร หากผู้ใช้มีบัตรที่มีตัวระบุชี้ของร้านค้า ผู้ใช้จะถูกขอให้รับรองความถูกต้องของการใช้งาน หากผู้ค้ารองรับการเข้ารหัส ข้อมูลบัตร ตราประทับเวลา และกุญแจ ECDH P-256 แบบสุ่มใช้ครั้งเดียวจะถูกใช้ร่วมกับกุญแจสาธารณะของผู้ค้าเพื่อให้ได้รับกุญแจการเข้ารหัสสำหรับข้อมูลบัตร ซึ่งจะถูกส่งไปยังเทอร์มินัล หากผู้ค้าไม่รองรับการเข้ารหัส ผู้ใช้จะถูกขอให้แสดงอุปกรณ์ไปยังเทอร์มินัลอีกครั้งก่อนที่ข้อมูลบัตรรางวัลจะถูกส่ง

การระงับบัตร การเอาบัตรออก และการลบบัตร

ผู้ใช้สามารถระงับ Apple Pay บน iPhone และ iPad โดยการตั้งอุปกรณ์ให้อยู่ในโหมดสูญหายโดยใช้ ค้นหา iPhone ของฉัน ผู้ใช้ยังสามารถเอาบัตรออกและลบบัตรของตนออกจาก Apple Pay โดยใช้ ค้นหา iPhone ของฉัน, การตั้งค่า iCloud หรือลบได้โดยตรงบนอุปกรณ์ของตนโดยใช้ Wallet บน Apple Watch สามารถนำบัตรออกได้โดยใช้การตั้งค่า iCloud, แอพ Apple Watch บน iPhone หรือนำออกจากนาฬิกาได้โดยตรง ความสามารถในการชำระเงินโดยใช้บัตรบนอุปกรณ์จะถูกระงับหรือนำออกจาก Apple Pay โดยผู้ออกบัตรหรือเครือข่ายการชำระเงิน แม้ว่าอุปกรณ์จะออฟไลน์อยู่และไม่ได้เชื่อมต่อกับเครือข่ายเซลลูลาร์หรือ Wi-Fi ก็ตาม ผู้ใช้ยังสามารถโทรไปยังผู้ออกบัตรเพื่อให้ระงับหรือนำบัตรออกจาก Apple Pay ได้

นอกจากนี้ เมื่อผู้ใช้ลบอุปกรณ์ทั้งหมดโดยใช้ “ลบเนื้อหาและการตั้งค่าทั้งหมด” โดยใช้ค้นหา iPhone ของฉัน หรือกู้คืนอุปกรณ์ของตนโดยใช้โหมดการกู้คืน iOS จะบอกให้ Secure Element ทำเครื่องหมายบัตรทั้งหมดว่ามีการลบ ข้อนี้จะมีผลเหมือนกับการเปลี่ยนบัตรเป็นสถานะไม่สามารถใช้งานได้โดยทันที จนกว่าเซิร์ฟเวอร์ Apple Pay จะสามารถติดต่อให้ลบบัตรทั้งหมดออกจาก Secure Element อย่างสมบูรณ์ได้ Secure Enclave จะทำเครื่องหมาย AR ว่าไม่ถูกต้องโดยเป็นอิสระจากกัน ดังนั้นการรับรองความถูกต้องการชำระเงินเพิ่มเติมสำหรับบัตรที่ลงทะเบียนไว้ก่อนหน้านี้จึงไม่สามารถทำได้ เมื่ออุปกรณ์ออนไลน์ อุปกรณ์จะพยายามติดต่อเซิร์ฟเวอร์ Apple Pay เพื่อให้รับรองว่าบัตรทั้งหมดใน Secure Element ถูกลบ

บริการอินเทอร์เน็ต

การสร้างรหัสผ่าน Apple ID ที่มีความปลอดภัยสูง
Apple ID ใช้เพื่อเชื่อมต่อกับบริการหลายอย่าง รวมถึง iCloud, FaceTime และ iMessage เพื่อช่วยผู้ใช้สร้างรหัสผ่านที่มีความปลอดภัยสูง บัญชีใหม่ทั้งหมดจะต้องมีคุณลักษณะของรหัสผ่านดังต่อไปนี้:

- ความยาวขั้นต่ำแปดอักขระ
- มีตัวอักษรอย่างน้อยหนึ่งตัว
- มีตัวพิมพ์ใหญ่อย่างน้อยหนึ่งตัว
- มีตัวเลขอย่างน้อยหนึ่งตัว
- ไม่มีอักขระเดียวกันอยู่ติดกันเกินสามตัว
- ไม่ตรงกับชื่อบัญชี

Apple ได้สร้างชุดของบริการที่สมบูรณ์เพื่อช่วยให้ผู้ใช้ได้รับอรรถประโยชน์และประสิทธิภาพการทำงานจากอุปกรณ์ได้มากยิ่งขึ้น ซึ่งรวมถึง iMessage, FaceTime, Siri, คำแนะนำโดย Spotlight, iCloud, การสำรองข้อมูล iCloud และพวงกุญแจ iCloud

บริการอินเทอร์เน็ตเหล่านี้ถูกสร้างขึ้นด้วยเป้าหมายความปลอดภัยเดียวกับที่ iOS สนับสนุนสำหรับแพลตฟอร์มทั้งหมด เป้าหมายเหล่านี้รวมถึงการจัดการข้อมูลอย่างปลอดภัย ไม่ว่าข้อมูลที่อยู่บนอุปกรณ์หรืออยู่ระหว่างส่งผ่านเครือข่ายไร้สาย การป้องกันข้อมูลส่วนบุคคลของผู้ใช้ และการป้องกันภัยคุกคามจากการเข้าถึงข้อมูลและบริการที่อันตรายหรือไม่ได้รับอนุญาต บริการแต่ละอันจะใช้สถาปัตยกรรมความปลอดภัยที่มีประสิทธิภาพของตนเองโดยไม่ทำให้ความสะดวกในการใช้งาน iOS โดยรวมได้รับผลกระทบ

Apple ID

Apple ID คือชื่อผู้ใช้และรหัสผ่านที่ใช้เพื่อลงชื่อเข้าใช้บริการของ Apple เช่น iCloud, iMessage, FaceTime, iTunes Store, iBooks Store, App Store และอื่นๆ อีกมาก เป็นเรื่องสำคัญที่ผู้ใช้ต้องเก็บ Apple ID ของตนให้ปลอดภัยเพื่อป้องกันการเข้าถึงบัญชีของตนอย่างไม่ได้รับอนุญาต เพื่อช่วยป้องกัน Apple กำหนดให้ใช้รหัสผ่านที่มีความปลอดภัยสูงที่ต้องมีความยาวอย่างน้อยแปดตัวอักษร โดยประกอบด้วยทั้งตัวอักษรและตัวเลข โดยต้องไม่ประกอบด้วยตัวอักษรเดียวกันซ้ำกันสามตัวติดกัน และไม่สามารถเป็นรหัสผ่านที่ใช้กันอย่างแพร่หลายได้ แนะนำให้ผู้ใช้เพิ่มความปลอดภัยให้มากกว่าที่แนะนำ โดยการเพิ่มตัวอักษรพิเศษและเครื่องหมายวรรคตอนเพื่อทำให้รหัสผ่านของตนมีความปลอดภัยสูงขึ้น Apple ยังต้องการให้ผู้ใช้ตั้งค่าคำถามรักษาความปลอดภัยสามข้อที่สามารถใช้เพื่อยืนยันตัวตนของเจ้าของเมื่อทำการเปลี่ยนแปลงข้อมูลบัญชีหรือรีเซ็ตรหัสผ่านที่ลืม

Apple ยังส่งอีเมลและการแจ้งเตือนแบบผลักข้อมูลไปยังผู้ใช้เมื่อมีการเปลี่ยนแปลงสำคัญไปยังบัญชีของผู้ใช้ ตัวอย่างเช่น หากรหัสผ่านหรือข้อมูลการเรียกเก็บเงินถูกเปลี่ยน หรือเมื่อ Apple ID ถูกใช้เพื่อลงชื่อเข้าใช้บนอุปกรณ์เครื่องใหม่ หากมีจุดใดดูผิดปกติออกไป ผู้ใช้ควรเปลี่ยนรหัสผ่าน Apple ID ของตนโดยทันที

นอกจากนี้ Apple ยังใช้นโยบายและขั้นตอนหลายอย่างที่ออกแบบมาเพื่อป้องกันบัญชีผู้ใช้ ซึ่งประกอบด้วยการจำกัดจำนวนครั้งที่สามารถพยายามลงชื่อเข้าหรือพยายามรีเซ็ตรหัสผ่าน การตรวจสอบการหลอกลวงอยู่ตลอดเวลาเพื่อช่วยระบุการโจมตีที่เกิดขึ้น และการตรวจทานนโยบายอย่างสม่ำเสมอที่ทำให้สามารถปรับไปใช้ข้อมูลใหม่ซึ่งอาจส่งผลกับความปลอดภัยของผู้ใช้ได้

การรับรองความถูกต้องแบบสองปัจจัย

เพื่อช่วยรักษาความปลอดภัยให้กับบัญชีของผู้ใช้ได้มากยิ่งขึ้นไปอีก Apple จึงนำเสนอการรับรองความถูกต้องแบบสองปัจจัย การรับรองความถูกต้องแบบสองปัจจัยเป็นการเพิ่มความปลอดภัยให้ Apple ID อีกชั้นหนึ่ง ซึ่งออกแบบมาเพื่อรับรองว่าเจ้าของบัญชีเท่านั้นที่สามารถเข้าถึงบัญชีได้ แม้ว่าจะมีผู้อื่นทราบรหัสผ่านก็ตาม

เมื่อใช้การรับรองความถูกต้องแบบสองปัจจัย บัญชีของผู้ใช้จะสามารถเข้าถึงได้จากบนอุปกรณ์ที่ได้รับการเชื่อถือเท่านั้น เช่น iPhone, iPad หรือ Mac ของผู้ใช้ หากต้องการลงชื่อเข้าเป็นครั้งแรกบนอุปกรณ์เครื่องใหม่ คุณต้องใช้ข้อมูลสองชิ้นซึ่งประกอบด้วยรหัสผ่าน Apple ID และรหัสรับรองความถูกต้องหกหลักที่จะแสดงบนอุปกรณ์ที่ได้รับการเชื่อถือของผู้ใช้หรือส่งไปที่หมายเลขโทรศัพท์ที่ได้รับการเชื่อถือ โดยการป้อนรหัสนี้ ถือว่าผู้ใช้ได้ยืนยันว่าเชื่อถือในอุปกรณ์เครื่องใหม่นี้และยืนยันว่าอุปกรณ์ดังกล่าวมีความปลอดภัยที่จะลงชื่อเข้า เนื่องจากรหัสผ่านเพียงอย่างเดียวไม่เพียงพอที่จะเข้าถึงบัญชีของผู้ใช้อีกต่อไป การรับรองความถูกต้องแบบสองปัจจัยจึงจะช่วยเพิ่มความปลอดภัยให้กับ Apple ID ของผู้ใช้และข้อมูลส่วนตัวทั้งหมดที่จัดเก็บไว้กับ Apple

การรับรองความถูกต้องแบบสองปัจจัยจะช่วยเพิ่มความปลอดภัยให้กับ Apple ID ของผู้ใช้และข้อมูลส่วนตัวทั้งหมดที่จัดเก็บไว้กับ Apple คุณสมบัตินี้รวมอยู่โดยตรงใน iOS, OS X, tvOS, watchOS และระบบรับรองความถูกต้องที่เว็บไซต์ของ Apple ใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการรับรองความถูกต้องแบบสองปัจจัย โปรดดู support.apple.com/th-th/HT204915

การตรวจสอบยืนยันแบบสองขั้นตอน

ตั้งแต่ปี 2013 เป็นต้นมา Apple ยังมอบวิธีการรักษาความปลอดภัยที่มีลักษณะคล้ายกันซึ่งเรียกว่าการยืนยันความถูกต้องสองขั้นตอน เมื่อเปิดใช้งานการยืนยันความถูกต้องสองขั้นตอนอยู่ ข้อมูลประจำตัวของผู้ใช้จะต้องได้รับการยืนยันผ่านรหัสชั่วคราวที่ส่งไปยังหนึ่งในอุปกรณ์ที่ได้รับการเชื่อถือของผู้ใช้ ก่อนที่การเปลี่ยนแปลงข้อมูลบัญชี Apple ID ของผู้ใช้จะได้รับการอนุญาต, ก่อนการลงชื่อเข้าสู่ iCloud, iMessage, FaceTime และ Game Center และก่อนซื้อสินค้าใน iTunes Store, iBooks Store หรือ App Store จากอุปกรณ์เครื่องใหม่ ผู้ใช้ยังได้รับกุญแจกู้คืน 14 ตัวอักษรเพื่อจัดเก็บในสถานที่ที่ปลอดภัยในกรณีที่เกิดลืมรหัสผ่านของตนหรือสูญเสียการเข้าถึงอุปกรณ์ที่ได้รับการเชื่อถือของตน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการยืนยันสองขั้นตอนสำหรับ Apple ID โปรดดู support.apple.com/kb/ht5570?viewlocale=th_TH

Apple ID ที่ได้รับการจัดการ

ฟังก์ชั่น Apple ID ที่ได้รับการจัดการที่มีอยู่ใน iOS 9.3 ขึ้นไปเป็นฟังก์ชั่นที่คล้ายกับ Apple ID แต่สถาบันการศึกษาเป็นเจ้าของและเป็นผู้ควบคุม สถาบันสามารถรีเซ็ตรหัสผ่าน จำกัดการซื้อสินค้าและการสื่อสารต่างๆ เช่น FaceTime และแอพข้อความ และตั้งค่าการอนุญาตตามบทบาทสำหรับพนักงาน ผู้สอน และนักเรียนได้

บริการของ Apple บางอย่างจะถูกปิดใช้งานสำหรับ Apple ID ที่ได้รับการจัดการ เช่น Touch ID, Apple Pay, พวงกุญแจ iCloud, HomeKit และค้นหา iPhone ของฉัน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ Apple ID ที่ได้รับการจัดการ โปรดดู วิธีใช้ Apple School Manager

การตรวจสอบ Apple ID ที่ได้รับการจัดการ

Apple ID ที่ได้รับการจัดการยังรองรับการตรวจสอบอีกด้วย ซึ่งทำให้สถาบันสามารถปฏิบัติตามกฎหมายและระเบียบข้อบังคับเกี่ยวกับความเป็นส่วนตัวได้ บัญชีผู้ดูแลระบบหรือผู้จัดการสามารถได้รับสิทธิ์ในการตรวจสอบ Apple ID ที่ได้รับการจัดการที่ระบุ ผู้ตรวจสอบสามารถตรวจสอบได้เฉพาะบัญชีที่อยู่ต่ำกว่าตนเองในลำดับชั้นของโรงเรียนเท่านั้น นั่นหมายความว่า ครูจะสามารถตรวจสอบนักเรียน ผู้จัดการจะสามารถตรวจสอบครูและนักเรียน และผู้ดูแลระบบจะสามารถตรวจสอบผู้จัดการ ครู และนักเรียน

เมื่อมีการร้องขอข้อมูลประจำตัวของการตรวจสอบโดยใช้ Apple School Manager จะมีการสร้างบัญชีพิเศษที่สามารถเข้าถึงเฉพาะ Apple ID ที่ได้รับการจัดการที่ถูกร้องขอการตรวจสอบเท่านั้น ใบอนุญาตการตรวจสอบจะหมดอายุหลังจากครบเจ็ดวัน ในระหว่างนั้นผู้ตรวจสอบจะสามารถอ่านและแก้ไขเนื้อหาของผู้ใช้ที่จัดเก็บอยู่ใน iCloud หรือในแอพพลิเคชั่นที่เปิดใช้งาน CloudKit ได้ การร้องขอการเข้าถึงเพื่อตรวจสอบทุกครั้งจะถูกบันทึกไว้ใน Apple School Manager บันทึกจะแสดงว่าผู้ตรวจสอบเป็นใคร แสดง Apple ID ที่ได้รับการจัดการที่ผู้ตรวจสอบร้องขอการเข้าถึง แสดงเวลาที่ร้องขอ และแสดงว่าได้มีการตรวจสอบเกิดขึ้นหรือไม่

Apple ID ที่ได้รับการจัดการและอุปกรณ์ส่วนตัว

Apple ID ที่ได้รับการจัดการสามารถใช้กับอุปกรณ์ iOS ส่วนตัวได้ด้วยเช่นกัน นักเรียนจะลงชื่อเข้าสู่ iCloud โดยใช้ Apple ID ที่ได้รับการตรวจสอบที่ออกโดยสถาบันและรหัสผ่านเพิ่มเติมสำหรับใช้ในเครื่องซึ่งทำหน้าที่เป็นปัจจัยที่สองของกระบวนการรับรองความถูกต้องแบบสองปัจจัยของ Apple ID ขณะที่ใช้ Apple ID ที่ได้รับการจัดการบนอุปกรณ์ส่วนตัว จะใช้งานพวงกุญแจ iCloud ไม่ได้ และสถาบันอาจจำกัดคุณสมบัติอื่นๆ เช่น FaceTime หรือแอพข้อความ เอกสาร iCloud ทุกฉบับที่นักเรียนสร้างในขณะที่ลงชื่อเข้าจะถูกตรวจสอบได้ตามที่อธิบายไว้ก่อนหน้านี้

iMessage

Apple iMessage คือบริการส่งข้อความสำหรับอุปกรณ์ iOS และคอมพิวเตอร์ Mac โดย iMessage รองรับข้อความและไฟล์แนบ เช่น รูปภาพ รายชื่อ และตำแหน่ง ข้อความจะปรากฏบนอุปกรณ์ที่ลงทะเบียนของผู้ใช้ทั้งหมด เพื่อให้สามารถต่อบทสนทนาได้จากอุปกรณ์ของผู้ใช้เครื่องใดๆ iMessage ใช้บริการการแจ้งเตือนแบบผลักข้อมูลของ Apple (APN) ในปริมาณมาก Apple ไม่บันทึกข้อความหรือไฟล์แนบ และเนื้อหาของรายการเหล่านี้จะได้รับการป้องกันโดยการเข้ารหัสแบบครอบคลุม ดังนั้นเฉพาะผู้ส่งและผู้รับเท่านั้นที่จะสามารถเข้าถึงข้อมูลได้ Apple ไม่สามารถถอดรหัสข้อมูลได้

เมื่อผู้ใช้เปิด iMessage บนอุปกรณ์ อุปกรณ์จะสร้างกุญแจสองคู่สำหรับใช้งานกับบริการ คือกุญแจ RSA 1280-bit สำหรับการเข้ารหัส และกุญแจ ECDSA 256-bit บน NIST P-256 curve สำหรับการลงชื่อ กุญแจส่วนตัวสำหรับกุญแจทั้งสองคู่จะถูกบันทึกในพวงกุญแจของอุปกรณ์ และกุญแจสาธารณะจะถูกส่งไปยังบริการไดเร็กเทอรี่ของ Apple (IDS) ซึ่งกุญแจเหล่านี้จะถูกเชื่อมโยงกับหมายเลขโทรศัพท์หรือที่อยู่อีเมลของผู้ใช้พร้อมกับที่อยู่ APN ของอุปกรณ์

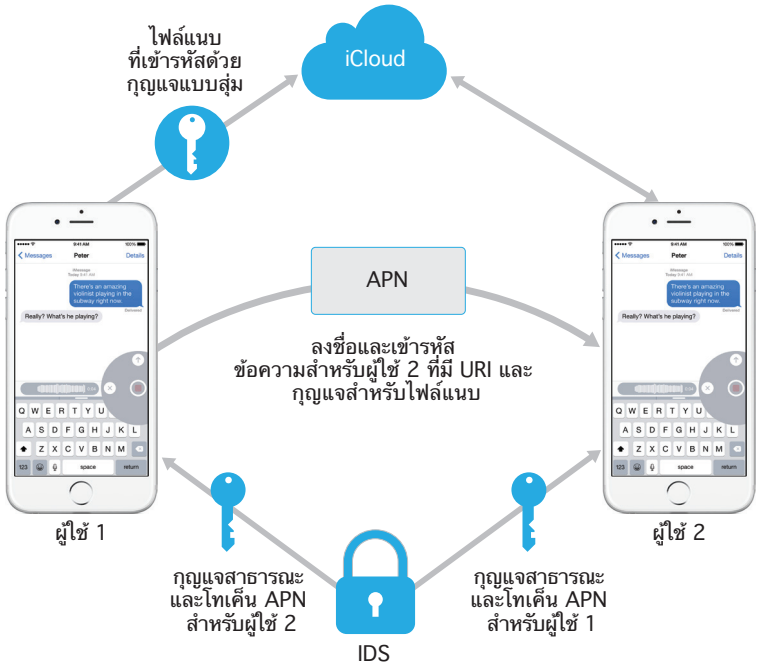
เมื่อผู้ใช้เปิดใช้งานอุปกรณ์เพิ่มเติมสำหรับใช้งานกับ iMessage กุญแจสาธารณะการเข้ารหัสและการลงชื่อ ที่อยู่ APN และหมายเลขโทรศัพท์ที่ถูกเชื่อมโยงของผู้ใช้จะถูกเพิ่มไปยังบริการไดเร็กเทอรี่ ผู้ใช้ยังสามารถเพิ่มที่อยู่อีเมลเพิ่มเติม ซึ่งจะได้รับการยืนยันโดยการส่งลิงก์ยืนยัน หมายเลขโทรศัพท์จะได้รับการยืนยันโดยเครือข่ายผู้ให้บริการและ SIM นอกเหนือจากนี้ อุปกรณ์ที่ลงทะเบียนของผู้ใช้ทั้งหมดจะแสดงข้อความเตือนเมื่ออุปกรณ์ หมายเลขโทรศัพท์ หรือที่อยู่อีเมลใหม่ถูกเพิ่ม

iMessage ส่งและรับข้อความอย่างไร

ผู้ใช้เริ่มต้นบทสนทนา iMessage ใหม่โดยการป้อนที่อยู่หรือชื่อ หากผู้ใช้ป้อนหมายเลขโทรศัพท์หรือที่อยู่อีเมล อุปกรณ์จะติดต่อ IDS เพื่อเรียกใช้กุญแจสาธารณะและที่อยู่ APN สำหรับอุปกรณ์ทั้งหมดที่เชื่อมโยงกับผู้รับนั้น หากผู้ใช้ป้อนชื่อ อันดับแรกอุปกรณ์จะใช้งานแอพรายชื่อของผู้ใช้เพื่อรวบรวมหมายเลขโทรศัพท์และที่อยู่อีเมลที่เชื่อมโยงกับชื่อนั้น จากนั้นขอกุญแจสาธารณะและที่อยู่ APN จาก IDS

ข้อความที่ส่งออกของผู้ใช้แต่ละอันจะถูกเข้ารหัสสำหรับอุปกรณ์ของผู้รับแต่ละเครื่อง กุญแจการเข้ารหัส RSA สาธารณะของอุปกรณ์ที่รับจะเรียกใช้จาก IDS สำหรับอุปกรณ์ที่รับแต่ละเครื่อง อุปกรณ์ที่ส่งจะสร้างกุญแจ 128-bit แบบสุ่ม และเข้ารหัสข้อความโดยใช้ AES ในโหมด CTR กุญแจ AES รายข้อความนี้จะถูกเข้ารหัสโดยใช้ RSA-OAEP ไปยังกุญแจสาธารณะของอุปกรณ์ที่รับ ชุดของข้อความตัวอักษรที่เข้ารหัสและกุญแจข้อความที่เข้ารหัสจะถูกแฮชด้วย SHA-1 และแฮชจะได้รับการลงชื่อด้วย ECDSA โดยใช้กุญแจการลงชื่อส่วนตัวของอุปกรณ์ที่ส่ง ข้อความผลลัพธ์ที่ได้ ซึ่งแต่ละอันสำหรับอุปกรณ์ที่รับแต่ละเครื่อง จะประกอบด้วยข้อความตัวอักษรที่เข้ารหัส กุญแจข้อความที่เข้ารหัส และลายเซ็นดิจิตอลของผู้ส่ง ข้อความจะถูกส่งไปยัง APN สำหรับการส่งต่อ Metadata เช่น ตราประทับเวลาและข้อมูลเส้นทาง APN จะไม่ถูกเข้ารหัส การติดต่อกับ APN จะถูกเข้ารหัสโดยใช้ช่องทาง forward-secret TLS

APN สามารถส่งต่อข้อความขนาดสูงสุด 4 KB หรือ 16 KB เท่านั้น ทั้งนี้ขึ้นอยู่กับเวอร์ชั่น iOS หากข้อความตัวอักษรยาวเกินไป หรือหากไฟล์แนบ เช่น รูปภาพ รวมอยู่ด้วย ไฟล์แนบจะถูกเข้ารหัสโดยใช้ AES ในโหมด CTR พร้อมกับกุญแจ 256-bit ที่สร้างแบบสุ่ม และมีการอัพโหลดไปยัง iCloud กุญแจ AES สำหรับไฟล์แนบ, URL (Uniform Resource Identifier) และแฮช SHA-1 ของรูปแบบที่เข้ารหัสจะถูกส่งไปยังผู้รับเป็นเนื้อหาของ iMessage โดยได้รับการป้องกันความลับและความสมบูรณ์ของข้อมูลผ่านการเข้ารหัส iMessage แบบปกติ ตามที่แสดงด้านล่าง



สำหรับบทสนทนากลุ่ม กระบวนการทำงานนี้จะมีการทำซ้ำสำหรับผู้รับแต่ละรายและอุปกรณ์ของผู้รับ

สำหรับฝั่งรับ อุปกรณ์แต่ละเครื่องจะได้รับสำเนาของข้อความจาก APN และหากจำเป็นจะได้รับไฟล์แนบจาก iCloud หมายเลขโทรศัพท์หรือที่อยู่อีเมลที่เข้ามาของผู้ส่งจะถูกจับคู่กับรายชื่อของผู้รับ ดังนั้นชื่ออาจมีการแสดงถ้าเป็นไปได้

เช่นเดียวกับการแจ้งเตือนแบบผลักข้อมูลทั้งหมด ข้อความจะถูกลบจาก APN เมื่อส่งเรียบร้อยแล้ว อย่างไรก็ตาม ข้อความ iMessage จะถูกจัดเข้าคิวเพื่อการส่งไปยังอุปกรณ์ออฟไลน์ ซึ่งแตกต่างจากการแจ้งเตือน APN อื่น ข้อความในปัจจุบันจะถูกจัดเก็บไว้สูงสุด 30 วัน

FaceTime

FaceTime คือบริการโทรแบบวิดีโอและเสียงของ Apple การโทรแบบ FaceTime จะใช้บริการการแจ้งเตือนแบบผลักข้อมูลของ Apple เพื่อสร้างการเชื่อมต่อเริ่มต้นไปยังอุปกรณ์ที่ลงทะเบียนของผู้ใช้ ซึ่งคล้ายคลึงกับ iMessage เนื้อหาแบบเสียง/วิดีโอของของการโทร FaceTime จะได้รับการป้องกันโดยการเข้ารหัสแบบครอบคลุม ดังนั้นเฉพาะผู้ส่งและผู้รับเท่านั้นที่จะสามารถเข้าถึงข้อมูลได้ Apple ไม่สามารถถอดรหัสข้อมูลได้

FaceTime ใช้ Internet Connectivity Establishment (ICE) เพื่อเริ่มต้นการเชื่อมต่อแบบเพียร์ทูเพียร์ระหว่างอุปกรณ์ เมื่อใช้ข้อความโปรโตคอล Session Initiation Protocol (SIP) อุปกรณ์จะยืนยันใบรับรองข้อมูลประจำตัวและสร้างความลับที่ใช้ร่วมกันสำหรับเซสชั่นแต่ละอัน ค่า nonce การเข้ารหัสที่ได้รับจากอุปกรณ์แต่ละเครื่องจะถูกผสานเข้ากับ salt key สำหรับช่องทางสื่อแต่ละช่อง ซึ่งจะถูกสตรีมผ่าน Secure Real Time Protocol (SRTP) โดยใช้การเข้ารหัส AES-256

iCloud

iCloud จัดเก็บรายชื่อ ปฏิทิน รูปภาพ เอกสาร และอื่นๆ ของผู้ใช้และเก็บข้อมูลให้อัพเดทบนอุปกรณ์ทุกเครื่องของผู้ใช้โดยอัตโนมัติ iCloud ยังสามารถใช้โดยแอพของบริษัทอื่นเพื่อจัดเก็บและเชื่อมข้อมูลเอกสาร เช่นเดียวกับค่าสำหรับข้อมูลแอพตามที่ระบุโดยผู้พัฒนา ผู้ใช้ตั้งค่า iCloud โดยการลงชื่อเข้าใช้ด้วย Apple ID และเลือกว่าต้องการใช้บริการใด คุณสมบัติ iCloud ซึ่งรวมถึงสตรีมรูปภาพ, iCloud Drive และการสำรองข้อมูลสามารถปิดใช้งานได้โดยผู้ดูแลระบบ IT ผ่านโปรไฟล์การกำหนดค่า บริการนี้ไม่สนใจว่าจะจัดเก็บอะไรอยู่และจะจัดการกับเนื้อหาของไฟล์ทั้งหมดในลักษณะเดียวกัน คือเป็นไบต์ที่รวมกันเป็นชุด

ไฟล์แต่ละไฟล์จะแตกออกเป็นชิ้นเล็กๆ และเข้ารหัสด้วย iCloud โดยใช้ AES-128 และกุญแจที่ได้จากเนื้อหาของชิ้นส่วนแต่ละอันที่ใช้งาน SHA-256 กุญแจและ Metadata ของไฟล์จะถูกจัดเก็บโดย Apple ในบัญชี iCloud ของผู้ใช้ ชิ้นส่วนที่เข้ารหัสของไฟล์จะถูกจัดเก็บ โดยไม่มีข้อมูลที่ระบุตัวผู้ใช้ โดยใช้บริการจัดเก็บของบริษัทอื่น เช่น Amazon S3 และ Windows Azure

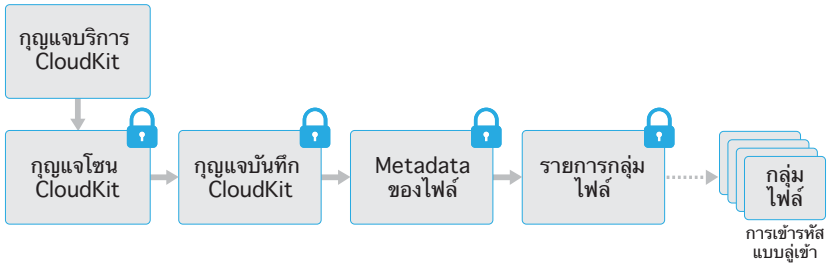
iCloud Drive

iCloud Drive จะเพิ่มกุญแจที่อิงตามบัญชีเพื่อป้องกันเอกสารที่จัดเก็บใน iCloud เช่นเดียวกับบริการ iCloud ที่มีอยู่ใดๆ บริการจะแตกเนื้อหาไฟล์และเข้ารหัส และจัดเก็บชิ้นส่วนที่เข้ารหัสโดยใช้บริการของบริษัทอื่น อย่างไรก็ตาม กุญแจเนื้อหาไฟล์จะถูกห่อด้วยกุญแจบันทึกที่จัดเก็บพร้อมกับ Metadata ของ iCloud Drive กุญแจบันทึกเหล่านี้จะได้รับการป้องกันโดยกุญแจบริการ iCloud Drive ของผู้ใช้ ซึ่งจะถูกจัดเก็บพร้อมกับบัญชี iCloud ของผู้ใช้ ผู้ใช้จะได้รับการเข้าถึง Metadata เอกสาร iCloud ของตนโดยการรับรองความถูกต้องกับ iCloud แต่จะต้องมีกุญแจบริการ iCloud Drive ด้วยเพื่อแสดงส่วนที่ได้รับการป้องกันของพื้นที่จัดเก็บ iCloud Drive

CloudKit

CloudKit อนุญาตให้ผู้พัฒนาแอพจัดเก็บข้อมูลค่ากุญแจ ข้อมูลโครงสร้าง และข้อมูลแอสเซทใน iCloud การเข้าถึง CloudKit ได้รับการควบคุมโดยใช้สิทธิ์ของแอพ CloudKit รองรับทั้งฐานข้อมูลแบบสาธารณะและส่วนตัว ฐานข้อมูลสาธารณะจะถูกใช้โดยสำเนาทั้งหมดของแอพ โดยเฉพาะสำหรับแอสเซทโดยทั่วไป และไม่ได้รับการเข้ารหัส ฐานข้อมูลส่วนตัวจัดเก็บข้อมูลของผู้ใช้

เช่นเดียวกับ iCloud Drive, CloudKit ใช้กุญแจที่อิงตามบัญชีเพื่อป้องกันข้อมูลที่จัดเก็บในฐานข้อมูลส่วนตัวของผู้ใช้ และไฟล์จะถูกทำให้แตกออก เข้ารหัส และจัดเก็บโดยใช้บริการของบริษัทอื่น ซึ่งคล้ายคลึงกับบริการของ iCloud อื่น CloudKit ใช้ลำดับชั้นของกุญแจ คล้ายคลึงกับการป้องกันข้อมูล กุญแจรายไฟล์จะถูกห่อด้วยกุญแจบันทึก CloudKit กุญแจบันทึกจะได้รับการป้องกันโดยกุญแจโซน ซึ่งได้รับการป้องกันโดยกุญแจบริการ CloudKit ของผู้ใช้ กุญแจบริการ CloudKit จะถูกจัดเก็บในบัญชี iCloud ของผู้ใช้ และสามารถใช้งานได้เฉพาะหลังจากที่ผู้ใช้รับรองความถูกต้องกับ iCloud



ข้อมูลสำรอง iCloud

iCloud ยังสำรองข้อมูล ซึ่งรวมถึงการตั้งค่าอุปกรณ์ ข้อมูลแอพ รูปภาพและวิดีโอในม้วนฟิล์ม และการสนทนาในแอพข้อความทุกวันผ่าน Wi-Fi โดย iCloud จะรักษาความปลอดภัยของเนื้อหาโดยการเข้ารหัสเนื้อหาเมื่อส่งผ่านอินเทอร์เน็ต จัดเก็บในรูปแบบการเข้ารหัส และใช้งานโทเค็นที่ปลอดภัยสำหรับการรับรองความถูกต้อง การสำรองข้อมูล iCloud เกิดขึ้นเฉพาะเมื่ออุปกรณ์ถูกล็อค มีการเชื่อมต่อกับแหล่งจ่ายไฟ และมีการเข้าถึงอินเทอร์เน็ตผ่าน Wi-Fi เนื่องจากการเข้ารหัสที่ใช้ใน iOS ระบบได้รับการออกแบบให้เก็บรักษาข้อมูลให้ปลอดภัยในขณะที่อนุญาตให้มีการสำรองข้อมูลและกู้คืนข้อมูลส่วนที่เพิ่มแบบที่ไม่ต้องจัดการ

ต่อไปนี้คือสิ่งที่ iCloud สำรองข้อมูล:

- ข้อมูลเกี่ยวกับเพลง ภาพยนตร์ รายการทีวี แอพ และหนังสือที่ซื้อ แต่ไม่ใช่ตัวเนื้อหาที่ซื้อเอง
- รูปภาพและวิดีโอในม้วนฟิล์ม
- รายชื่อ กิจกรรมปฏิทิน รายการเตือนความจำ และโน้ต
- การตั้งค่าอุปกรณ์
- ข้อมูลแอพ
- PDF และหนังสือที่เพิ่มไปยัง iBooks แต่ไม่ได้ซื้อ
- ประวัติการโทร
- หน้าจอโฮมและการจัดการแอพ
- iMessage, ข้อความตัวอักษร (SMS) และข้อความ MMS
- เสียงเรียกเข้า
- ข้อมูล HomeKit
- ข้อมูล HealthKit
- ข้อความเสียงแบบเห็นภาพ

เมื่อไฟล์ถูกสร้างในคลาสการป้องกันข้อมูลที่ไม่สามารถเข้าถึงได้เมื่ออุปกรณ์ล็อคอยู่ กุญแจรายไฟล์ของข้อมูลจะถูกเข้ารหัสโดยใช้คลาสกุญแจจาก Keybag การสำรองข้อมูล iCloud ไฟล์จะถูกสำรองข้อมูลไปยัง iCloud ในสถานะเริ่มแรกที่มีการเข้ารหัส ไฟล์ในคลาสการป้องกันข้อมูลไม่มีการป้องกันจะถูกเข้ารหัสในระหว่างการส่งข้อมูล

Keybag การสำรองข้อมูล iCloud ประกอบด้วยกุญแจ (Curve25519) ที่ไม่สมมาตรสำหรับคลาสการป้องกันข้อมูลแต่ละอัน ซึ่งจะถูกใช้เพื่อเข้ารหัสกุญแจรายไฟล์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเนื้อหาของ Keybag การสำรองข้อมูล และ Keybag การสำรองข้อมูล iCloud โปรดดูหัวข้อ “การป้องกันข้อมูลในพวงกุญแจ” ในส่วนการเข้ารหัสและการป้องกันข้อมูล

ชุดการสำรองข้อมูลจะถูกจัดเก็บในบัญชี iCloud ของผู้ใช้ และประกอบด้วยสำเนาของไฟล์ของผู้ใช้ และ Keybag การสำรองข้อมูล iCloud Keybag ข้อมูลสำรอง iCloud จะได้รับการป้องกันด้วยกุญแจแบบสุ่ม ซึ่งจะได้รับการจัดเก็บพร้อมกับชุดการสำรองข้อมูลด้วยเช่นกัน (รหัสผ่าน iCloud ของผู้ใช้จะไม่ถูกใช้งานสำหรับการเข้ารหัส ดังนั้นการเปลี่ยนแปลงรหัสผ่าน iCloud จะไม่ทำให้การสำรองข้อมูลที่มีอยู่ไม่สามารถใช้งานได้)

ในขณะที่ฐานข้อมูลพวงกุญแจของผู้ใช้ได้รับการสำรองข้อมูลไปยัง iCloud ฐานข้อมูลจะยังคงได้รับการป้องกันโดยกุญแจที่โยงกับค่า UID ซึ่งจะทำให้สามารถกู้คืนพวงกุญแจไปยังอุปกรณ์เครื่องเดียวกับที่สร้างพวงกุญแจขึ้นมาเท่านั้น และหมายความว่าคนอื่นซึ่งรวมถึง Apple ไม่สามารถอ่านรายการพวงกุญแจของผู้ใช้ได้

เมื่อกู้คืน ไฟล์ที่ได้รับการสำรองข้อมูล, Keybag การสำรองข้อมูล iCloud และกุญแจสำหรับ Keybag จะถูกเรียกใช้จากบัญชี iCloud ของผู้ใช้ Keybag การสำรองข้อมูล iCloud จะถูกถอดรหัสโดยใช้กุญแจของ Keybag จากนั้นกุญแจรายไฟล์ใน Keybag จะถูกใช้เพื่อถอดรหัสไฟล์ในชุดการสำรองข้อมูล ซึ่งจะถูกเขียนเป็นไฟล์ใหม่ไปยังระบบไฟล์ จึงเป็นการเข้ารหัสรายการใหม่ตามคลาสการป้องกันข้อมูล

การรวม Safari กับพวงกุญแจ iCloud
Safari สามารถสร้างสตริงแบบสุ่มเข้ารหัสที่มีความปลอดภัยสูงเพื่อใช้เป็นรหัสผ่านของเว็บไซต์ได้ ซึ่งจะจัดเก็บไว้ในพวงกุญแจและเชื่อมข้อมูลกับอุปกรณ์อื่นๆ ของคุณ รายการพวงกุญแจจะถ่ายโอนจากอุปกรณ์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งโดยผ่านเซิร์ฟเวอร์ของ Apple แต่จะเข้ารหัสด้วยวิธีการที่ทำให้ Apple และอุปกรณ์เครื่องอื่นๆ อ่านเนื้อหาไม่ได้

พวงกุญแจ iCloud

พวงกุญแจ iCloud ช่วยให้ผู้ใช้สามารถเชื่อมข้อมูลรหัสผ่านของเขาหรือเธอระหว่างอุปกรณ์ iOS และคอมพิวเตอร์ Mac ได้อย่างปลอดภัย โดยไม่เปิดเผยข้อมูลนั้นไปยัง Apple นอกเหนือจากความเป็นส่วนตัวและความปลอดภัยที่หนาแน่น เป้าหมายอื่นที่ส่งผลกระทบต่อการออกแบบและสถาปัตยกรรมของพวงกุญแจ iCloud เป็นอย่างสูงคือความสะดวกในการใช้งาน และความสามารถในการกู้คืนพวงกุญแจ พวงกุญแจ iCloud ประกอบด้วยบริการสองอย่าง คือการเชื่อมข้อมูลพวงกุญแจและการกู้คืนพวงกุญแจ

Apple ออกแบบพวงกุญแจ iCloud และการกู้คืนพวงกุญแจ เพื่อให้รหัสผ่านของผู้ใช้ยังคงได้รับการป้องกันภายในเงื่อนไขต่อไปนี้:

- บัญชี iCloud ของผู้ใช้มีช่องโหว่ความปลอดภัย
- iCloud มีความปลอดภัยที่หละหลวมเนื่องจากผู้โจมตีภายนอกหรือพนักงาน
- การเข้าใช้งานบัญชีผู้ใช้ของบุคคลอื่น

การเชื่อมข้อมูลพวงกุญแจ

เมื่อผู้ใช้เปิดใช้งานพวงกุญแจ iCloud เป็นครั้งแรก อุปกรณ์จะสร้างวงจรที่เชื่อถือได้ และสร้างข้อมูลประจำตัวในการเชื่อมข้อมูลสำหรับตัวเอง ข้อมูลประจำตัวในการเชื่อมข้อมูลประกอบด้วยกุญแจส่วนตัวและกุญแจสาธารณะ กุญแจสาธารณะของข้อมูลประจำตัวการเชื่อมข้อมูลจะถูกวางอยู่ในวงจร และวงจรนั้นจะถูกลงชื่อสองครั้ง ครั้งแรกโดยกุญแจส่วนตัวของข้อมูลประจำตัวการเชื่อมข้อมูล จากนั้นลงชื่ออีกครั้งด้วยกุญแจรูปไข่แบบไม่สมมาตร (โดยใช้ P256) ที่ได้จากรหัสผ่านบัญชีiCloud ของผู้ใช้ ข้อมูลที่เก็บพร้อมกับวงจรด้วยคือพารามิเตอร์ (ค่า salt และ iteration แบบสุ่ม) ที่ใช้เพื่อสร้างกุญแจที่อิงมาจากรหัสผ่าน iCloud ของผู้ใช้

วงจรเชื่อมข้อมูลที่ลงชื่อจะถูกวางในพื้นที่จัดเก็บข้อมูลค่ากุญแจ iCloud ของผู้ใช้ ซึ่งไม่สามารถอ่านได้โดยไม่ทราบรหัสผ่าน iCloud ของผู้ใช้ และไม่สามารถแก้ไขได้อย่างถูกต้องโดยไม่มีกุญแจส่วนตัวของข้อมูลประจำตัวการเชื่อมข้อมูลของสมาชิก

เมื่อผู้ใช้เปิดพวงกุญแจ iCloud บนอุปกรณ์อีกเครื่อง อุปกรณ์ใหม่จะสังเกตเห็นใน iCloud ว่าผู้ใช้มีวงจรเชื่อมข้อมูลที่สร้างไว้ก่อนหน้า ซึ่งอุปกรณ์ไม่ได้เป็นสมาชิก อุปกรณ์จะสร้างคู่กุญแจข้อมูลประจำตัวการเชื่อมข้อมูล จากนั้นสร้างบัตรผ่านแอพพลิเคชั่นเพื่อร้องขอการเป็นสมาชิกวงจร บัตรผ่านประกอบด้วยกุญแจสาธารณะของข้อมูลประจำตัวการเชื่อมข้อมูลของอุปกรณ์ และผู้ใช้จะได้รับคำขอให้รับรองความถูกต้องด้วยรหัสผ่าน iCloud ของเขาหรือเธอ พารามิเตอร์การสร้างกุญแจรูปไข่จะเรียกใช้จาก iCloud และสร้างกุญแจซึ่งถูกใช้เพื่อลงชื่อในบัตรผ่านแอพพลิเคชั่น ขั้นตอนสุดท้าย ทิกเก็ตแอพพลิเคชั่นจะถูกวางใน iCloud

เมื่ออุปกรณ์แรกเห็นว่ามีบัตรผ่านแอพพลิเคชั่นมาถึง อุปกรณ์จะแสดงข้อความเตือนสำหรับผู้ใช้ให้รับทราบว่าอุปกรณ์ใหม่ร้องขอการเข้าร่วมวงจรเชื่อมข้อมูล ผู้ใช้จะป้อนรหัสผ่าน iCloud ของเขาหรือเธอ และบัตรผ่านแอพพลิเคชั่นจะได้รับการยืนยันว่ามีการลงชื่อโดยกุญแจส่วนตัวที่ตรงกัน สิ่งนี้หมายความว่าผู้ที่สร้างคำขอเข้าร่วมวงจรได้ป้อนรหัสผ่าน iCloud ของผู้ใช้ในเวลาที่ส่งคำขอ

เมื่อได้รับการรับรองจากผู้ใช้ให้เพิ่มอุปกรณ์ใหม่เข้าสู่วงจร อุปกรณ์แรกจะเพิ่มกุญแจสาธารณะของสมาชิกใหม่เข้าสู่วงจรเชื่อมข้อมูล ให้ลงชื่ออีกครั้งด้วยข้อมูลประจำตัวสำหรับเชื่อมข้อมูลของอุปกรณ์นั้นและกุญแจที่ได้จากรหัสผ่าน iCloud ของผู้ใช้ วงจรเชื่อมข้อมูลใหม่จะอยู่ใน iCloud ซึ่งจะลงชื่อในลักษณะเดียวกันโดยสมาชิกของวงจร

ขณะนี้จะมีสมาชิกของวงจรลงชื่อสองราย และแต่ละรายจะมีกุญแจสาธารณะของเพียร์ของตัวเอง สมาชิกเหล่านั้นจะเริ่มแลกเปลี่ยนแต่ละรายการในพวงกุญแจผ่านทางการจัดเก็บค่ากุญแจ iCloud หากสมาชิกวงจรทั้งสองรายมีรายการเดียวกัน จะเชื่อมข้อมูลรายการที่มีการแก้ไขล่าสุด รายการจะถูกข้ามหากสมาชิกอีกรายหนึ่งมีรายการนั้นและวันที่แก้ไขตรงกัน รายการแต่ละรายการที่เชื่อมข้อมูลจะเข้ารหัสเฉพาะสำหรับอุปกรณ์ที่กำลังส่งรายการนั้นให้ โดยอุปกรณ์เครื่องอื่นหรือ Apple จะไม่สามารถถอดรหัสนั้น นอกจากนี้ รายการที่เข้ารหัสจะอยู่ใน iCloud เพียงชั่วคราว โดยจะถูกเขียนทับด้วยรายการใหม่ที่เชื่อมข้อมูลแต่ละรายการ

กระบวนการนี้จะทำซ้ำเมื่ออุปกรณ์ใหม่เข้าร่วมวงจรเชื่อมข้อมูล ตัวอย่างเช่น เมื่ออุปกรณ์เครื่องที่สามเข้าร่วม การยืนยันจะปรากฏบนอุปกรณ์ของผู้ใช้อื่นทั้งสองราย ผู้ใช้สามารถรับรองสมาชิกใหม่จากอุปกรณ์เหล่านั้นเครื่องใดก็ได้ เมื่อเพิ่มเพียร์ใหม่แล้ว เพียร์แต่ละเพียร์จะเชื่อมข้อมูลกับเพียร์ใหม่เพื่อให้แน่ใจได้ว่าสมาชิกทุกรายมีรายการในพวงกุญแจเหมือนกัน

อย่างไรก็ตาม พวงกุญแจจะไม่เชื่อมข้อมูลทั้งหมด รายการบางอย่างเป็นรายการเฉพาะอุปกรณ์ เช่น ตัวตน VPN และไม่ควรส่งออกจากตัวอุปกรณ์นั้น เฉพาะรายการที่มีคุณลักษณะ `kSecAttrSynchronizable` เท่านั้นที่จะเชื่อมข้อมูล Apple ได้ตั้งคุณลักษณะนี้ให้กับข้อมูลผู้ใช้ Safari (รวมถึงชื่อผู้ใช้ รหัสผ่าน และหมายเลขบัตรเครดิต) เช่นเดียวกับรหัสผ่าน Wi-Fi และกุญแจเข้ารหัส HomeKit

นอกจากนี้ รายการในพวงกุญแจที่เพิ่มโดยแอพของบริษัทอื่นก็จะมีค่าเริ่มต้นเป็นไม่เชื่อมข้อมูลด้วย ผู้พัฒนาต้องตั้ง `kSecAttrSynchronizable` เมื่อเพิ่มรายการลงในพวงกุญแจ

การกู้คืนพวงกุญแจ

การกู้คืนพวงกุญแจทำให้ผู้ใช้สามารถเลือกที่จะฝากพวงกุญแจของเขาไว้กับ Apple ได้โดยไม่ต้องอนุญาตให้ Apple อ่านรหัสผ่านหรือข้อมูลอื่นๆ ที่อยู่ในพวงกุญแจ ถึงแม้ว่าผู้ใช้จะมีอุปกรณ์เพียงแค่เครื่องเดียว การกู้คืนพวงกุญแจก็จะเป็นมาตรการขั้นสุดท้ายในการป้องกันข้อมูลสูญหาย ซึ่งเป็นเรื่องสำคัญอย่างยิ่งเมื่อใช้ Safari สร้างรหัสผ่านแบบสุ่มที่มีความปลอดภัยสูงสำหรับบัญชีบนเว็บ เนื่องจากรหัสผ่านเหล่านั้นจะบันทึกอยู่ในพวงกุญแจเพียงที่เดียวเท่านั้น

หลักสำคัญของการกู้คืนพวงกุญแจคือการรับรองความถูกต้องครั้งที่สองและบริการรับฝากที่ปลอดภัย ซึ่งสร้างขึ้นโดย Apple เพื่อรองรับคุณสมบัตินี้โดยเฉพาะ พวงกุญแจของผู้ใช้จะเข้ารหัสด้วยรหัสผ่านตัวเลขที่มีความปลอดภัยสูง และบริการรับฝากจะมอบพวงกุญแจสำรองให้เมื่อเกิดเหตุการณ์ที่ตรงตามเงื่อนไขอันเข้มงวดเท่านั้น

เมื่อเปิดใช้พวงกุญแจ iCloud ผู้ใช้จะถูกขอให้สร้างรหัสรักษาความปลอดภัย iCloud จำเป็นต้องใช้รหัสนี้เพื่อกู้คืนพวงกุญแจที่ฝากไว้ ตามค่าเริ่มต้นแล้ว ผู้ใช้จะถูกขอให้ตั้งรหัสรักษาความปลอดภัยอย่างง่ายเป็นค่าสี่หลัก อย่างไรก็ตาม ผู้ใช้สามารถกำหนดรหัสของตัวเองให้ยาวขึ้น หรือให้อุปกรณ์สร้างรหัสลับแบบสุ่มซึ่งพวกเขาสามารถบันทึกและเก็บไว้เองได้

จากนั้นอุปกรณ์ iOS จะส่งออกพวงกุญแจของผู้ใช้หนึ่งชุด โดยเข้ารหัสห่อด้วยกุญแจใน Keybag อสมมาตร และเก็บไว้ในพื้นที่จัดเก็บค่ากุญแจ iCloud ของผู้ใช้ Keybag จะถูกห่อด้วยรหัสรักษาความปลอดภัย iCloud ของผู้ใช้และกุญแจสาธารณะของคลัสเตอร์ HSM (โมดูลรักษาความปลอดภัยฮาร์ดแวร์) ที่จะจัดเก็บข้อมูลที่ฝาก และจะกลายเป็นข้อมูลที่ฝาก iCloud ของผู้ใช้

หากผู้ใช้ตัดสินใจใช้รหัสรักษาความปลอดภัยที่สุ่มแบบลับ แทนที่จะกำหนดรหัสของตัวเองหรือใช้ค่าสี่หลัก จะไม่จำเป็นต้องใช้ข้อมูลที่ฝาก แต่จะใช้รหัสรักษาความปลอดภัย iCloud เพื่อห่อกุญแจแบบสุ่มโดยตรงแทน

นอกจากนี้ ผู้ใช้ยังต้องลงทะเบียนหมายเลขโทรศัพท์เพื่อสร้างรหัสรักษาความปลอดภัยอีกด้วย โดยจะใช้เพื่อให้การรับรองความถูกต้องเป็นชั้นที่สองในระหว่างการกู้คืนพวงกุญแจ ผู้ใช้จะได้รับ SMS ที่จำเป็นต้องตอบกลับจึงจะสามารถดำเนินการกู้คืนได้

ความปลอดภัยของข้อมูลที่ฝาก

iCloud มอบโครงสร้างพื้นฐานที่ปลอดภัยสำหรับการฝากพวงกุญแจที่ทำให้มั่นใจได้ว่าเฉพาะผู้ใช้และอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่จะสามารถทำการกู้คืนได้ สิ่งที่อยู่เบื้องหลัง iCloud คือคลัสเตอร์โมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM) คลัสเตอร์เหล่านี้จะปกป้องข้อมูลที่ฝาก แต่ละคลัสเตอร์จะดูแลกุญแจที่ใช้เพื่อเข้ารหัสข้อมูลที่ฝาก ตามที่ได้อธิบายไว้ก่อนหน้านี้

หากต้องการกู้คืนพวงกุญแจ ผู้ใช้ต้องรับรองความถูกต้องด้วยบัญชีและรหัสผ่าน iCloud และตอบสนองต่อ SMS ที่ส่งไปที่หมายเลขโทรศัพท์ที่ลงทะเบียนไว้ เมื่อเสร็จแล้ว ผู้ใช้จะต้องป้อนรหัสรักษาความปลอดภัย iCloud ของตนเอง คลัสเตอร์ HSM จะตรวจสอบว่าผู้ใช้รู้รหัสรักษาความปลอดภัย iCloud หรือไม่โดยใช้โปรโตคอลรหัสผ่านระยะไกลแบบปลอดภัย (SRP) โดยจะไม่ส่งตัวรหัสผ่านไปที่ Apple แต่ละส่วนของคลัสเตอร์จะตรวจสอบว่าผู้ใช้พยายามขอรับข้อมูลของตัวเองจนครบจำนวนครั้งที่อนุญาตแล้วหรือยัง ตามที่อธิบายไว้ทางด้านล่าง หากส่วนใหญ่ยินยอม คลัสเตอร์จะแกะห่อข้อมูลที่ฝากและส่งไปที่อุปกรณ์ของผู้ใช้

จากนั้น อุปกรณ์จะใช้รหัสรักษาความปลอดภัย iCloud เพื่อแกะห่อกุญแจแบบสุ่มที่ใช้เข้ารหัสพวงกุญแจของผู้ใช้ ด้วยกุญแจนั้น พวงกุญแจที่ได้รับจากที่จัดเก็บค่ากุญแจ iCloud จะถูกถอดรหัสและกู้คืนไปที่อุปกรณ์ มีโอกาสเพียง 10 ครั้งเท่านั้นที่จะรับรองความถูกต้องและรับข้อมูลที่ฝาก หลังจากพยายามไม่สำเร็จหลายครั้ง ข้อมูลจะถูกล็อคและผู้ใช้จะต้องโทรหาฝ่ายสนับสนุนของ Apple เพื่อขอให้เพิ่มจำนวนครั้งในการลอง หลังจากพยายามไม่สำเร็จเป็นครั้งที่ 10 คลัสเตอร์ HSM จะทำลายข้อมูลที่ฝากไว้และพวงกุญแจจะหายไปเป็นการถาวร ซึ่งจะช่วยปกป้องจากการพยายามเจาะข้อมูลด้วยการเดารหัสผ่าน โดยแลกกับการสูญเสียข้อมูลพวงกุญแจ

นโยบายเหล่านี้เขียนเป็นโค้ดไว้ในเฟิร์มแวร์ของ HSM การ์ดที่มีสิทธิ์เข้าถึงระดับผู้ดูแลที่อนุญาตให้ทำการเปลี่ยนแปลงกับเฟิร์มแวร์ได้ได้ถูกทำลายไปแล้ว การพยายามดัดแปลงเฟิร์มแวร์หรือเข้าถึงกุญแจส่วนตัวจะทำให้คลัสเตอร์ HSM ลบกุญแจส่วนตัวนั้น หากเกิดเหตุการณ์เช่นนี้ขึ้น เจ้าของพวงกุญแจทั้งหมดที่คลัสเตอร์นั้นปกป้องอยู่จะได้รับข้อความแจ้งว่าสูญเสียข้อมูลที่ฝากไว้แล้ว พวกเขาสามารถเลือกที่จะฝากใหม่ได้

Siri

เพียงแค่พูดตามธรรมชาติ ผู้ใช้ก็จะสามารถสั่งให้ Siri ส่งข้อความ กำหนดเวลาการประชุม โทรออก และอื่นๆ อีกมาก Siri จะใช้คุณสมบัติการรู้จำคำพูด แปลงข้อความเป็นคำพูด และโมเดลไคลเอนต์-เซิร์ฟเวอร์ เพื่อตอบสนองต่อคำขอในหลายๆ รูปแบบ งานที่ Siri รองรับได้ถูกออกแบบมาเพื่อให้มั่นใจได้ว่าใช้ข้อมูลส่วนตัวในปริมาณที่น้อยที่สุด และได้รับการปกป้องอย่างเต็มที่

เมื่อเปิดใช้ Siri อุปกรณ์จะสร้างตัวระบุแบบสุ่มสำหรับใช้กับคุณสมบัติการรู้จำคำพูดและเซิร์ฟเวอร์ Siri ตัวระบุเหล่านี้จะใช้ภายใน Siri เท่านั้น และจะใช้เพื่อปรับปรุงบริการ หากปิด Siri หลังจากนั้น อุปกรณ์จะสร้างตัวระบุแบบสุ่มขึ้นใหม่เพื่อใช้เมื่อเปิด Siri อีกครั้ง

เพื่อให้คุณสมบัติต่างๆ ของ Siri ทำงานได้ ข้อมูลของผู้ใช้บางอย่างจะถูกส่งจากอุปกรณ์ไปที่เซิร์ฟเวอร์ ซึ่งรวมถึงข้อมูลเกี่ยวกับคลังเพลง (ชื่อเพลง ศิลปิน และเพลย์ลิสต์) ชื่อรายการเตือนความจำ และชื่อและความสัมพันธ์ที่กำหนดไว้ในแอพรายชื่อ การสื่อสารกับเซิร์ฟเวอร์ทั้งหมดจะผ่าน HTTPS

เมื่อเริ่มเซสชั่น Siri ชื่อและนามสกุลของผู้ใช้ (จากแอพรายชื่อ) รวมถึงตำแหน่งที่ตั้งทางภูมิศาสตร์โดยประมาณจะถูกส่งไปที่เซิร์ฟเวอร์ เพื่อให้ Siri สามารถตอบสนองด้วยชื่อหรือตอบคำถามที่ต้องการตำแหน่งที่ตั้งโดยประมาณ เช่น คำถามเกี่ยวกับสภาพอากาศ

หากจำเป็นต้องใช้ตำแหน่งที่ตั้งที่แม่นยำกว่านี้ ตัวอย่างเช่น เพื่อหาตำแหน่งที่ตั้งของโรงภาพยนตร์ที่อยู่ใกล้เคียง เซิร์ฟเวอร์จะขอให้อุปกรณ์ส่งตำแหน่งที่ตั้งที่ละเอียดขึ้น นี่คือตัวอย่างที่แสดงว่า ตามค่าเริ่มต้นแล้วข้อมูลจะถูกส่งให้กับเซิร์ฟเวอร์เมื่อจำเป็นต้องใช้ในการประมวลผลคำขอของผู้ใช้เท่านั้น และจะทิ้งข้อมูลเซสชั่นหลังจากไม่ได้ใช้งานเป็นเวลา 10 นาที ไม่ว่าในกรณีใด

เมื่อใช้ Siri จาก Apple Watch นาฬิกาจะสร้างตัวระบุเฉพาะตัวแบบสุ่มของตัวเอง ตามที่อธิบายไว้ทางด้านบน อย่างไรก็ตาม คำขอของนาฬิกาจะส่งตัวระบุของ Siri ของ iPhone ที่จับคู่กันอยู่ไปด้วยเพื่ออ้างอิงข้อมูลนั้นแทนการส่งข้อมูลของผู้ใช้อีกครั้ง

เสียงบันทึกคำพูดของผู้ใช้จะถูกส่งไปที่เซิร์ฟเวอร์การรู้จำเสียงของ Apple หากงานเกี่ยวข้องกับการป้อนตามคำบอกเท่านั้น ข้อความที่รู้จำจะถูกส่งกลับมาที่อุปกรณ์ หากไม่ใช่ Siri จะวิเคราะห์ข้อความนั้น และหากจำเป็นก็จะรวมเข้ากับข้อมูลจากโปรไฟล์ที่เชื่อมโยงกับอุปกรณ์ ตัวอย่างเช่น หากคำขอคือ “ส่งข้อความให้คุณแม่” จะใช้ความสัมพันธ์และชื่อที่อัพโหลดจากแอพรายชื่อ จากนั้นจะส่งคำสั่งสำหรับการกระทำที่ระบุกลับมาที่อุปกรณ์เพื่อทำต่อ

ฟังก์ชั่นหลายอย่างของ Siri จะทำให้เสร็จด้วยอุปกรณ์โดยใช้คำแนะนำจากเซิร์ฟเวอร์ ตัวอย่างเช่น หากผู้ใช้ขอให้ Siri อ่านข้อความเข้า เซิร์ฟเวอร์จะบอกให้อุปกรณ์พูดเนื้อหาของข้อความที่ยังไม่ได้อ่าน โดยจะไม่ส่งเนื้อหาและผู้ส่งข้อความไปที่เซิร์ฟเวอร์

เสียงบันทึกของผู้ใช้จะถูกบันทึกไว้เป็นเวลาหกเดือน เพื่อให้ระบบรู้จำสามารถใช้เสียงบันทึกเหล่านั้นเพื่อทำความเข้าใจเสียงของผู้ใช้ได้ดียิ่งขึ้น หลังจากหกเดือน จะทำการบันทึกอีกชุดหนึ่งโดยไม่บันทึกตัวระบุของเสียงบันทึกใหม่ สำหรับให้ Apple ใช้เพื่อปรับปรุงและพัฒนา Siri เป็นเวลาไม่เกินสองปี นอกจากนี้ เสียงบันทึกบางรายการที่อ้างอิงถึงเพลง ทีมกีฬาและนักกีฬา และธุรกิจหรือหัวข้อที่สนใจจะถูกบันทึกในลักษณะเดียวกันเพื่อวัตถุประสงค์ในการปรับปรุง Siri

คุณสามารถใช้งาน Siri แบบแฮนด์ฟรีได้ผ่านการเปิดใช้งานด้วยเสียง โดยจะทำการตรวจจับคำสั่งเสียงภายในตัวอุปกรณ์เอง ในโหมดนี้ Siri จะเปิดใช้งานเมื่อรูปแบบเสียงเข้าตรงกับเสียงของวลีคำสั่งที่ระบุมากพอเท่านั้น เมื่อตรวจพบคำสั่ง เสียงที่เกี่ยวข้องรวมถึงคำสั่ง Siri ต่อจากนั้นจะถูกส่งไปที่เซิร์ฟเวอร์การรู้จำเสียงของ Apple เพื่อประมวลผลต่อ ซึ่งจะปฏิบัติตามกฎเดียวกันกับเสียงบันทึกของผู้ใช้อื่นๆ ที่ทำผ่าน Siri

ความต่อเนื่อง

คุณสมบัติความต่อเนื่องจะใช้ประโยชน์จากเทคโนโลยีต่างๆ เช่น iCloud, บลูทูธ และ Wi-Fi เพื่อทำให้ผู้ใช้สามารถทำกิจกรรมจากอุปกรณ์เครื่องหนึ่งต่อในอุปกรณ์อีกเครื่องหนึ่ง โทรออกและรับสาย ส่งและรับข้อความตัวอักษร และแชร์การเชื่อมต่ออินเทอร์เน็ตแบบเซลลูลาร์ได้

Handoff

เมื่อใช้ Handoff ผู้ใช้จะสามารถส่งสิ่งที่กำลังทำอยู่จากอุปกรณ์เครื่องหนึ่งไปที่อีกเครื่องหนึ่งได้เมื่อ Mac และอุปกรณ์ iOS ของผู้ใช้อยู่ใกล้กัน Handoff ทำให้ผู้ใช้สามารถสลับอุปกรณ์แล้วทำงานต่อได้ทันที

เมื่อผู้ใช้ลงชื่อเข้าสู่ iCloud บนอุปกรณ์ที่สามารถใช้ Handoff ได้เครื่องที่สอง อุปกรณ์สองเครื่องนั้นจะสร้างการจับคู่แบบนอกความถี่สื่อสารปกติด้วยบลูทูธพลังงานต่ำ 4.0 โดยใช้บริการการแจ้งเตือนแบบผลักข้อมูลของ Apple (APN) ข้อความแต่ละข้อความจะเข้ารหัสในลักษณะคล้ายกันกับ iMessage เมื่ออุปกรณ์จับคู่กันแล้ว แต่ละเครื่องจะสร้างกุญแจ AES 256 บิตแบบอสมมาตร ซึ่งจะจัดเก็บไว้ในพวงกุญแจของอุปกรณ์ กุญแจนี้จะใช้เพื่อเข้ารหัสและรับรองความถูกต้องของโฆษณาบลูทูธพลังงานต่ำที่จะส่งข้อมูลกิจกรรมปัจจุบันของอุปกรณ์ไปที่อุปกรณ์ iCloud เครื่องอื่นๆ ที่จับคู่กันอยู่ โดยใช้ AES-256 ในโหมด GCM พร้อมมาตรการป้องกันการเล่นซ้ำ เมื่ออุปกรณ์ได้รับโฆษณาจากกุญแจใหม่เป็นครั้งแรก อุปกรณ์เครื่องนั้นจะสร้างการเชื่อมต่อบลูทูธพลังงานต่ำกับอุปกรณ์เครื่องแรกแล้วทำการแลกเปลี่ยนกุญแจการเข้ารหัสโฆษณา การเชื่อมต่อนี้ได้รับการรักษาความปลอดภัยด้วยการเข้ารหัสบลูทูธพลังงานต่ำ 4.0 และการเข้ารหัสของข้อความแต่ละข้อความ ซึ่งมีลักษณะคล้ายกันกับการเข้ารหัส iMessage ในบางสถานการณ์ ข้อความเหล่านี้จะส่งผ่านบริการการแจ้งเตือนแบบผลักข้อมูลของ Apple แทนบลูทูธพลังงานต่ำ เพย์โหลดของกิจกรรมจะได้รับการปกป้องและส่งในลักษณะเดียวกันกับ iMessage

Handoff ระหว่างแอพดั้งเดิมกับเว็บไซต์

Handoff ทำให้แอพดั้งเดิมของ iOS สามารถเปิดเว็บเพจในโดเมนที่ผู้พัฒนาแอพเป็นผู้ควบคุมต่อจากที่ค้างไว้ได้ และยังทำให้สามารถทำกิจกรรมผู้ใช้ของแอพดั้งเดิมต่อในเว็บเบราว์เซอร์ได้อีกด้วย

เพื่อป้องกันไม่ให้แอพดั้งเดิมเปิดเว็บไซต์ที่ไม่ได้ควบคุมโดยผู้พัฒนาต่อจากที่ค้างไว้ แอพจะต้องแสดงหลักฐานที่เชื่อถือได้ว่าเป็นผู้ควบคุมโดเมนที่ต้องการเปิดต่อ การควบคุมโดเมนเว็บไซต์จะสร้างผ่านกลไกที่ใช้สำหรับข้อมูลประจำตัวของเว็บที่แชร์ สำหรับรายละเอียดโปรดดู “การเข้าถึงรหัสผ่าน Safari ที่บันทึกไว้” ในส่วนการเข้ารหัสและการป้องกันข้อมูล ระบบจะต้องตรวจสอบความถูกต้องการควบคุมชื่อโดเมนของแอพก่อนที่แอพนั้นจะได้รับอนุญาตให้ยอมรับ Handoff กิจกรรมของผู้ใช้

แหล่งข้อมูลของ Handoff หน้าเว็บสามารถเป็นเบราว์เซอร์ใดก็ได้ที่ใช้ API ของ Handoff เมื่อผู้ใช้ดูหน้าเว็บ ระบบจะโฆษณาชื่อโดเมนของหน้าเว็บเป็นไบต์โฆษณา Handoff แบบเข้ารหัส เฉพาะอุปกรณ์เครื่องอื่นของผู้ใช้เท่านั้นที่สามารถถอดรหัสไบต์โฆษณาได้ (ตามที่ได้อธิบายไว้ก่อนหน้านี้ในส่วนที่อยู่ด้านบน)

ระบบของอุปกรณ์ที่เป็นฝ่ายรับจะตรวจสอบว่าแอพดั้งเดิมที่ติดตั้งอยู่ยอมรับ Handoff จากชื่อโดเมนที่โฆษณาหรือไม่ แล้วแสดงไอคอนของแอพดั้งเดิมนั้นเป็นตัวเลือก Handoff เมื่อเปิดทำงาน แอพดั้งเดิมจะรับ URL แบบเต็มและชื่อของหน้าเว็บ โดยจะไม่มีการส่งข้อมูลอื่นจากเบราว์เซอร์ไปที่แอพดั้งเดิม

และในทางกลับกัน แอพดั้งเดิมสามารถระบุ URL สำรองเมื่ออุปกรณ์ที่เป็นฝ่ายรับ Handoff ไม่ได้ติดตั้งแอพดั้งเดิมเดียวกันได้ ในกรณีนี้ ระบบจะแสดงเบราว์เซอร์เริ่มต้นของผู้ใช้เป็นตัวเลือกแอพ Handoff (หากเบราว์เซอร์นั้นใช้ API ของ Handoff) เมื่อร้องขอ Handoff เบราว์เซอร์จะเปิดทำงานและมอบ URL สำรองที่แอพต้นทางให้มา โดย URL สำรองไม่จำเป็นต้องจำกัดอยู่เพียงชื่อโดเมนที่ผู้พัฒนาแอพดั้งเดิมเป็นผู้ควบคุม

Handoff ข้อมูลขนาดใหญ่

นอกจากคุณสมบัติพื้นฐานของ Hadoff แล้ว แอพบางแอพอาจเลือกใช้ API ที่รองรับการส่งข้อมูลขนาดใหญ่ผ่านทางเทคโนโลยี Wi-Fi แบบเพียร์ทูเพียร์ที่ Apple สร้างขึ้น (ในลักษณะคล้ายกันกับ AirDrop) ตัวอย่างเช่น แอพเมลจะใช้ API เหล่านี้เพื่อรองรับการ Handoff เมลฉบับร่าง ซึ่งอาจมีไฟล์แนบขนาดใหญ่

เมื่อแอพใช้คุณสมบัตินี้ การแลกเปลี่ยนระหว่างอุปกรณ์สองเครื่องจะเริ่มต้นเหมือนใน Handoff (ดูส่วนก่อนหน้า) อย่างไรก็ตาม หลังจากที่รับเพย์โหลดเริ่มต้นโดยใช้บลูทูธพลังงานต่ำแล้ว อุปกรณ์ที่เป็นฝ่ายรับจะเริ่มการเชื่อมต่อใหม่ผ่าน Wi-Fi การเชื่อมต่อนี้จะถูกเข้ารหัส (TLS) ซึ่งจะแลกเปลี่ยนใบรับรองตัวตน iCloud ของอุปกรณ์แต่ละเครื่อง ข้อมูลประจำตัวในใบรับรองจะได้รับการยืนยันเทียบกับตัวตนของผู้ใช้ ข้อมูลเพย์โหลดนอกเหนือจากนี้จะส่งผ่านการเชื่อมต่อแบบเข้ารหัสนี้จนกว่าจะถ่ายโอนเสร็จสมบูรณ์

การส่งต่อสายโทรเซลลูลาร์ iPhone

เมื่อ Mac, iPad หรือ iPod ของคุณอยู่บนเครือข่าย Wi-Fi เดียวกับ iPhone อุปกรณ์เหล่านั้นจะสามารถโทรออกและรับสายได้โดยใช้การเชื่อมต่อเซลลูลาร์ของ iPhone การกำหนดค่าจำเป็นต้องให้อุปกรณ์ต่างๆ ของคุณลงชื่อเข้าทั้ง iCloud และ FaceTime โดยใช้บัญชี Apple ID เดียวกัน

เมื่อมีสายเรียกเข้า อุปกรณ์ที่กำหนดค่าไว้ทั้งหมดจะได้รับการแจ้งเตือนผ่านบริการการแจ้งเตือนแบบผลักข้อมูลของ Apple (APN) โดยการแจ้งเตือนแต่ละรายการจะใช้การเข้ารหัสแบบครอบคลุมเหมือนกับที่ iMessage ใช้ อุปกรณ์ที่อยู่บนเครือข่ายเดียวกันจะแสดง UI การแจ้งเตือนสายเรียกเข้า เมื่อรับสาย เสียงจะถูกส่งจาก iPhone ของคุณอย่างไม่สะดุดโดยใช้การเชื่อมต่อแบบเพียร์ทูเพียร์ที่ปลอดภัยระหว่างอุปกรณ์สองเครื่อง

เมื่อรับสายบนอุปกรณ์เครื่องหนึ่ง เสียงเรียกเข้าของอุปกรณ์ที่จับคู่ผ่าน iCloud ที่อยู่ใกล้เคียงจะหยุดลงโดยการโฆษณาผ่านบลูทูธพลังงานต่ำ 4.0 เป็นเวลาสั้นๆ ไบต์ของการประกาศจะถูกเข้ารหัสโดยใช้วิธีการเดียวกับการโฆษณาของ Handoff

สายโทรออกจะส่งต่อไปที่ iPhone ผ่านบริการการแจ้งเตือนแบบผลักข้อมูลของ Apple ด้วยเช่นกัน และเสียงจะถูกส่งผ่านลิงก์เพียร์ทูเพียร์ที่ปลอดภัยระหว่างอุปกรณ์สองเครื่องในลักษณะเดียวกัน

ผู้ใช้สามารถปิดใช้งานการส่งต่อสายโทรบนอุปกรณ์ได้โดยการปิดสายโทรเซลลูลาร์ iPhone ในการตั้งค่า FaceTime

การส่งต่อข้อความตัวอักษร iPhone

การส่งต่อข้อความตัวอักษรจะส่งข้อความตัวอักษร SMS ที่ได้รับบน iPhone ไปที่ iPad, iPod touch หรือ Mac ของผู้ใช้ที่ลงทะเบียนไว้โดยอัตโนมัติ อุปกรณ์แต่ละเครื่องต้องลงชื่อเข้าสู่บริการ iMessage โดยใช้บัญชี Apple ID เดียวกัน เมื่อเปิดใช้บริการส่งต่อข้อความ SMS อยู่ การลงทะเบียนจะได้รับการยืนยันบนอุปกรณ์แต่ละเครื่องโดยการป้อนรหัสตัวเลขแบบสุ่มหกหลักที่ iPhone สร้างขึ้น

เมื่อเชื่อมโยงอุปกรณ์แล้ว iPhone จะเข้ารหัสและส่งต่อข้อความตัวอักษร SMS ไปที่อุปกรณ์แต่ละเครื่องโดยใช้วิธีการที่อธิบายไว้ในส่วน iMessage ของเอกสารฉบับนี้ การตอบกลับจะถูกส่งกลับไปที่ iPhone โดยใช้วิธีการเดียวกัน จากนั้น iPhone จะส่งการตอบกลับเป็นข้อความตัวอักษรโดยใช้กลไกการส่ง SMS ของผู้ให้บริการ สามารถเปิดหรือปิดการส่งต่อข้อความตัวอักษรได้ในการตั้งค่าข้อความ

Instant Hotspot

อุปกรณ์ iOS ที่รองรับ Instant Hotspot จะใช้บลูทูธพลังงานต่ำเพื่อค้นหาและสื่อสารกับอุปกรณ์ที่ลงชื่อเข้าสู่บัญชี iCloud เดียวกัน คอมพิวเตอร์ Mac ที่เข้ากันได้และใช้งาน OS X Yosemite ขึ้นไปจะใช้เทคโนโลยีเดียวกันเพื่อค้นหาและสื่อสารกับอุปกรณ์ iOS ที่ใช้ Instant Hotspot

เมื่อผู้ใช้ป้อนการตั้งค่า Wi-Fi บนอุปกรณ์ iOS อุปกรณ์นั้นจะส่งสัญญาณบลูทูธพลังงานต่ำที่มีตัวระบุที่อุปกรณ์ทุกเครื่องที่ลงชื่อเข้าสู่บัญชี iCloud เดียวกันตกลงยอมรับ ตัวระบุนั้นสร้างจาก DSID (Destination Signaling Identifier) ที่ผูกอยู่กับบัญชี iCloud และจะสลับสับเปลี่ยนเป็นระยะๆ เมื่ออุปกรณ์อื่นที่ลงชื่อเข้าสู่บัญชี iCloud เดียวกันอยู่ในระยะใกล้และรองรับฮอตสปอตส่วนบุคคล อุปกรณ์เหล่านั้นจะตรวจหาสัญญาณแล้วทำการตอบสนองเพื่อบ่งบอกความพร้อมใช้งาน

เมื่อผู้ใช้เลือกอุปกรณ์ที่พร้อมใช้งานฮอตสปอตส่วนบุคคล จะมีการส่งคำขอให้เปิดใช้ฮอตสปอตส่วนบุคคลไปที่อุปกรณ์นั้น คำขอจะถูกส่งผ่านลิงก์ที่เข้ารหัสโดยใช้การเข้ารหัสบลูทูธพลังงานต่ำแบบมาตรฐาน และคำขอจะถูกเข้ารหัสในลักษณะคล้ายกันกับการเข้ารหัส iMessage จากนั้นอุปกรณ์จะตอบสนองต่อลิงก์บลูทูธพลังงานต่ำเดียวกันทั้งหมดโดยใช้การเข้ารหัสรายข้อความเดียวกันกับข้อมูลการเชื่อมต่อฮอตสปอตส่วนบุคคล

คำแนะนำโดย Spotlight

การค้นหาโดย Safari และการค้นหาโดย Spotlight จะรวมคำแนะนำการค้นหาจากอินเทอร์เน็ต, แอพ, iTunes, App Store, เวลาฉายภาพยนตร์, สถานที่ใกล้เคียง และอื่นๆ อีกมาก

เพื่อให้คำแนะนำตรงกับที่ผู้ใช้ต้องการมากขึ้น บริบทการใช้งานและผลตอบรับการค้นหาพร้อมคำขอค้นหาจะถูกส่งไปที่ Apple บริบทที่ส่งไปพร้อมกันคำขอค้นหาจะมอบสิ่งต่อไปนี้ให้กับ Apple: i) ตำแหน่งที่ตั้งโดยประมาณของอุปกรณ์ ii) ประเภทอุปกรณ์ (เช่น Mac, iPhone, iPad หรือ iPod) iii) แอพไคลเอนต์ ซึ่งอาจเป็น Spotlight หรือ Safari ก็ได้ iv) ภาษาเริ่มต้นและการตั้งค่าภูมิภาคของอุปกรณ์ v) แอพที่ใช้ล่าสุดบนอุปกรณ์สามแอพ และ vi) ID เซสชั่นแบบไม่ระบุตัวตน การสื่อสารกับเซิร์ฟเวอร์ทั้งหมดจะเข้ารหัสผ่าน HTTPS

เพื่อช่วยปกป้องความเป็นส่วนตัวของผู้ใช้ คำแนะนำโดย Spotlight จะไม่ส่งตำแหน่งที่ตั้งที่แท้จริง แต่จะทำให้ตำแหน่งที่ตั้งมีความไม่ชัดเจนบนตัวไคลเอนต์ก่อนที่จะส่ง ระดับการทำให้ไม่ชัดเจนจะขึ้นอยู่กับความหนาแน่นของประชากรโดยประมาณในตำแหน่งที่ตั้งของอุปกรณ์ ตัวอย่างเช่น จะทำให้ไม่ชัดเจนมากขึ้นเมื่ออยู่ในชนบท แต่จะทำน้อยลงเมื่ออยู่ใจกลางเมืองและผู้ใช้มักจะอยู่ใกล้กัน นอกจากนี้ ผู้ใช้ยังสามารถปิดใช้งานการส่งข้อมูลตำแหน่งที่ตั้งทั้งหมดให้กับ Apple ได้ในการตั้งค่า โดยการปิดใช้บริการหาตำแหน่งที่ตั้งสำหรับคำแนะนำโดย Spotlight หากปิดใช้งานบริการหาตำแหน่งที่ตั้งอยู่ Apple อาจใช้ที่อยู่ IP ของไคลเอนต์เพื่อกำหนดตำแหน่งโดยประมาณ

ID เซสชั่นแบบไม่ระบุตัวตนทำให้ Apple สามารถวิเคราะห์รูปแบบระหว่างคำขอที่ทำในระยะเวลา 15 นาทีได้ ตัวอย่างเช่น หากผู้ใช้มักจะค้นหา “หมายเลขโทรศัพท์ร้านอาหาร” หลังจากค้นหา “ร้านอาหาร” เป็นเวลาไม่นาน Apple อาจเรียนรู้ที่จะแสดงหมายเลขโทรศัพท์ในผลการค้นหาได้ ซึ่งจะต่างจากเครื่องมือค้นหาส่วนใหญ่ อย่างไรก็ตาม บริการค้นหาของ Apple ไม่ได้ใช้ตัวระบุส่วนบุคคลนี้กับประวัติการค้นหาของผู้ใช้ทั้งหมดเพื่อผูกคำขอต่างๆ เข้ากับผู้ใช้หรืออุปกรณ์ แต่อุปกรณ์ของ Apple จะใช้ ID เซสชั่นชั่วคราวแบบไม่ระบุตัวตนเป็นระยะเวลาไม่เกิน 15 นาที ก่อนที่จะทิ้ง ID นั้นไป

ข้อมูลบนแอพล่าสุดสามแอพที่ใช้บนอุปกรณ์จะรวมไว้เป็นบริบทการค้นหาเพิ่มเติม โดยจะรวมเฉพาะแอพที่อยู่ในบัญชีขาวของแอพยอดนิยมที่ Apple เป็นผู้จัดทำ และมีการเข้าถึงภายในสามชั่วโมงล่าสุดเท่านั้น เพื่อปกป้องความเป็นส่วนตัวของผู้ใช้

ผลตอบรับการค้นหาที่ส่งไปที่ Apple จะมอบสิ่งต่อไปนี้ให้กับ Apple: i) ระยะเวลาระหว่างการกระทำของผู้ใช้ เช่น การกดปุ่ม กับการเลือกผลการค้นหา ii) คำแนะนำโดย Spotlight ที่เลือก (หากเลือก) และ iii) ประเภทผลการค้นหาในเครื่องที่เลือก (เช่น “ที่คั่นหน้า” หรือ “รายชื่อ”) เช่นเดียวกับบริบทการค้นหา ผลตอบรับการค้นหาจะไม่ผูกกับบุคคลหรืออุปกรณ์ใด

Apple จะเก็บรักษาบันทึกคำแนะนำโดย Spotlight พร้อมคำขอ บริบท และผลตอบรับ เป็นเวลาไม่เกิน 18 เดือน บันทึกที่ลดข้อมูลให้เหลือเพียงคำขอ ประเทศ ภาษา วันที่ (ละเอียดในระดับชั่วโมง) และประเภทอุปกรณ์ จะถูกเก็บไว้เป็นเวลาไม่เกินสองปี โดยจะไม่เก็บที่อยู่ IP ไว้กับบันทึกคำขอ

ในบางกรณี คำแนะนำโดย Spotlight อาจส่งต่อคำขอที่เป็นคำและวลีทั่วไปให้กับคู่ค้าที่ผ่านคุณสมบัติ เพื่อรับและแสดงผลการค้นหาของคู่ค้านั้น โดยคู่ค้าที่ผ่านคุณสมบัติจะไม่จัดเก็บคำขอเหล่านี้ไว้ และคู่ค้าจะไม่ได้รับผลตอบรับการค้นหา คู่ค้ายังจะไม่ได้รับที่อยู่ IP อีกด้วย การสื่อสารกับคู่ค้าจะเข้ารหัสผ่าน HTTPS Apple จะมอบข้อมูลตำแหน่งที่ตั้งในระดับเมือง ประเภทอุปกรณ์ และภาษาของไคลเอนต์ให้กับคู่ค้าในฐานะบริบทการค้นหาโดยอิงจากตำแหน่งที่ตั้ง ประเภทอุปกรณ์ และภาษาที่ Apple ได้รับคำขอซ้ำๆ

สามารถปิดใช้คำแนะนำโดย Spotlight ได้ในการตั้งค่าสำหรับ Spotlight หรือสำหรับ Safari หรือทั้งสองอย่าง หากปิดใช้สำหรับ Spotlight จะเป็นการแปลง Spotlight กลับเป็นไคลเอนต์ค้นหาในอุปกรณ์เท่านั้น ซึ่งจะไม่ส่งข้อมูลไปที่ Apple หากปิดใช้ใน Safari จะทำให้ไม่ส่งคำค้นหาของผู้ใช้ บริบทการค้นหา และผลตอบรับการค้นหาไปที่ Apple

Spotlight ยังมีกลไกสำหรับทำให้สามารถค้นหาเนื้อหาในอุปกรณ์ได้ด้วยเช่นกัน:

- CoreSpotlight API จะทำให้แอพของ Apple และบริษัทอื่นสามารถส่งเนื้อหาที่ทำดัชนีได้ไปที่ Spotlight
- NSUserActivity API จะทำให้แอพของ Apple และบริษัทอื่นสามารถส่งข้อมูลที่เกี่ยวกับหน้าของแอพที่ผู้ใช้เข้าเยี่ยมชมไปที่ Spotlight ได้

Spotlight จะเก็บข้อมูลที่ได้รับเป็นดัชนีบนอุปกรณ์โดยใช้สองวิธีต่อไปนี้ เพื่อให้สามารถแสดงผลการค้นหาจากข้อมูลนี้เมื่อผู้ใช้ทำการค้นหา หรือแสดงโดยอัตโนมัติเมื่อเรียกใช้ Spotlight และยังมี API การค้นหาแบบรวมอยู่บนอุปกรณ์ ซึ่งจะมีให้ใช้งานในแอพที่ Apple มอบให้เท่านั้น โดยจะทำให้ Spotlight สามารถส่งคำขอของผู้ใช้ให้กับแอพเพื่อประมวลผลและรับผลการค้นหาได้

การควบคุมอุปกรณ์

iOS รองรับนโยบายและการกำหนดค่าความปลอดภัยแบบยืดหยุ่น ที่บังคับใช้และจัดการได้ง่าย ซึ่งจะทำให้องค์กรสามารถปกป้องข้อมูลขององค์กรและมั่นใจได้ว่าพนักงานปฏิบัติตามความต้องการขององค์กร ถึงแม้ว่าพวกเขาจะใช้อุปกรณ์ที่จัดหามาเอง ตัวอย่างเช่น เมื่อเข้าร่วมโปรแกรม “นำอุปกรณ์ของคุณมาเอง” (BYOD)

องค์กรสามารถใช้ทรัพยากรต่างๆ เช่น การป้องกันโดยรหัสผ่านตัวเลข โปรไฟล์การกำหนดค่า การล้างข้อมูลระยะไกล และโซลูชั่น MDM ของบริษัทอื่น เพื่อจัดการอุปกรณ์จำนวนมากและรักษาความปลอดภัยของข้อมูลบริษัท ถึงแม้ว่าพนักงานจะเข้าถึงข้อมูลนี้บนอุปกรณ์ iOS ของตัวเองก็ตาม

การป้องกันโดยรหัสผ่านตัวเลข

ตามค่าเริ่มต้นแล้ว จะสามารถกำหนดรหัสผ่านของผู้ใช้เป็น PIN ตัวเลขได้ ความยาวขั้นต่ำของรหัสผ่านบนอุปกรณ์ที่มี Touch ID คือหกหลัก ความยาวขั้นต่ำของอุปกรณ์อื่นๆ คือสี่หลัก ผู้ใช้สามารถกำหนดรหัสผ่านตัวเลขและตัวอักษรที่ยาวขึ้นได้โดยเลือก รหัสผ่านตัวเลขและตัวอักษรแบบกำหนดเอง ใน ตัวเลือกรหัสผ่านตัวเลข ใน การตั้งค่า > รหัสผ่านตัวเลข รหัสผ่านที่ยาวขึ้นและซับซ้อนขึ้นจะทำให้เดาหรือโจมตีได้ยากขึ้น และขอแนะนำให้องค์กรใช้

ผู้ดูแลระบบสามารถบังคับให้ต้องใช้รหัสผ่านแบบซับซ้อนและนโยบายอื่นๆ ได้โดยใช้ MDM หรือ Exchange ActiveSync หรือโดยการบังคับให้ผู้ใช้ต้องติดตั้งโปรไฟล์การกำหนดค่าด้วยตัวเอง นโยบายเกี่ยวกับรหัสผ่านตัวเลขต่อไปนี้มีให้ใช้งาน:

- อนุญาตค่าอย่างง่าย
- ต้องใช้ค่าตัวเลขและอักษร
- ความยาวรหัสผ่านต่ำสุด
- จำนวนอักขระซับซ้อนสูงสุด
- อายุรหัสผ่านนานสุด
- ประวัติรหัสผ่าน
- ล็อคอัตโนมัติเมื่อหมดเวลา
- ช่วงเวลาผ่อนผันของการล็อคอุปกรณ์
- จำนวนความพยายามที่ไม่สำเร็จสูงสุด
- อนุญาต Touch ID

สำหรับรายละเอียดเกี่ยวกับนโยบายแต่ละข้อ โปรดดูเอกสารประกอบ การอ้างอิงกุญแจโปรไฟล์กำหนดค่า ที่ developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef

โมเดลการจับคู่ iOS

iOS ใช้โมเดลการจับคู่เพื่อควบคุมการเข้าถึงอุปกรณ์จากคอมพิวเตอร์โฮสต์ การจับคู่จะสร้างความสัมพันธ์ที่เชื่อถือได้ระหว่างอุปกรณ์กับโฮสต์ที่อุปกรณ์เชื่อมต่ออยู่ ซึ่งบ่งบอกโดยการแลกเปลี่ยนกุญแจสาธารณะ iOS จะใช้สัญลักษณ์ความเชื่อถือนี้เพื่อเปิดใช้งานฟังก์ชั่นเพิ่มเติมกับโฮสต์ที่เชื่อมต่ออยู่ เช่น การเชื่อมข้อมูล ใน iOS 9 บริการต่างๆ ที่ต้องใช้การจับคู่จะไม่สามารถเริ่มต้นได้จนกว่าผู้ใช้จะปลดล็อคอุปกรณ์

กระบวนการจับคู่จำเป็นต้องให้ผู้ใช้ปลดล็อคอุปกรณ์และยอมรับคำขอจับคู่จากโฮสต์ หลังจากที่ผู้ใช้ทำเสร็จแล้ว โฮสต์และอุปกรณ์จะแลกเปลี่ยนและบันทึกกุญแจสาธารณะ RSA แบบ 2048 บิต จากนั้นโฮสต์จะได้รับกุญแจแบบ 256 บิตที่สามารถปลดล็อค Keybag ที่ฝากไว้ที่จัดเก็บอยู่ในอุปกรณ์ (โปรดดู Keybag การฝากในส่วน Keybag) กุญแจที่แลกเปลี่ยนกันจะใช้เพื่อเริ่มเซสชั่น SSL แบบเข้ารหัส ซึ่งอุปกรณ์ต้องใช้ก่อนที่จะส่งข้อมูลที่ได้รับการป้องกันไปที่โฮสต์หรือเริ่มบริการ (เชื่อมข้อมูล iTunes, ถ่ายโอนไฟล์, การพัฒนา XCode เป็นต้น) อุปกรณ์ต้องใช้การเชื่อมต่อจากโฮสต์ผ่าน Wi-Fi เพื่อใช้เซสชั่นแบบเข้ารหัสนี้กับการสื่อสารทั้งหมด ดังนั้นจึงต้องเคยจับคู่กันผ่าน USB มาก่อน การจับคู่ยังทำให้สามารถทำการวิเคราะห์หลายอย่างได้อีกด้วย ใน iOS 9 หากไม่ได้ใช้บันทึกการจับคู่เป็นเวลานานกว่าหกเดือน บันทึกนั้นจะหมดอายุ สำหรับข้อมูลเพิ่มเติม โปรดดู support.apple.com/kb/HT6331?viewlocale=th_TH

บริการบางอย่าง รวมถึง com.apple.pcapd จะถูกจำกัดให้ทำงานผ่าน USB เท่านั้น นอกจากนี้ บริการ com.apple.file_relay ยังต้องใช้โปรไฟล์กำหนดค่าที่ Apple ลงชื่อรับรองเพื่อติดตั้งอีกด้วย

ผู้ใช้สามารถล้างรายการโฮสต์ที่เชื่อถือได้โดยใช้ตัวเลือก “รีเซ็ตการตั้งค่าเครือข่าย” หรือ “รีเซ็ตตำแหน่งที่ตั้งและความเป็นส่วนตัว” สำหรับข้อมูลเพิ่มเติม โปรดดู support.apple.com/kb/HT5868?viewlocale=th_TH

การบังคับใช้การกำหนดค่า

โปรไฟล์กำหนดค่าคือไฟล์ XML ที่ทำให้ผู้ดูแลระบบสามารถแจกจ่ายข้อมูลกำหนดค่าไปที่อุปกรณ์ iOS ได้ ผู้ใช้จะไม่สามารถเปลี่ยนการตั้งค่าที่กำหนดโดยโปรไฟล์กำหนดค่าที่ติดตั้ง หากผู้ใช้ลบโปรไฟล์กำหนดค่า การตั้งค่าทั้งหมดที่กำหนดโดยโปรไฟล์นั้นจะถูกเอาออก ในกรณีนี้ ผู้ดูแลระบบสามารถบังคับใช้การตั้งค่าได้โดยการผูกนโยบายเข้ากับการเข้าถึง ตัวอย่างเช่น โปรไฟล์กำหนดค่าที่มอบการกำหนดค่าอีเมลจะสามารถกำหนดนโยบายรหัสผ่านของอุปกรณ์ได้ด้วย ผู้ใช้จะไม่สามารถเข้าถึงเมลได้นอกเสียจากรหัสผ่านของเขาจะตรงกับความต้องการของผู้ดูแลระบบ

โปรไฟล์กำหนดค่า iOS จะมีการตั้งค่าจำนวนหนึ่งที่สามารถกำหนดได้ รวมถึง:

- นโยบายเกี่ยวกับรหัสผ่านตัวเลข
- การจำกัดคุณสมบัติของอุปกรณ์ (ปิดใช้งานกล้อง เป็นต้น)
- การตั้งค่า Wi-Fi
- การตั้งค่า VPN
- การตั้งค่าเซิร์ฟเวอร์เมล
- การตั้งค่าการแลกเปลี่ยน
- การตั้งค่าบริการไดเร็กเทอรี่ LDAP
- การตั้งค่าบริการปฏิทิน CalDAV
- Web clip
- ข้อมูลประจำตัวและกุญแจ
- การตั้งค่าเครือข่ายเซลลูลาร์ขั้นสูง

โปรไฟล์กำหนดค่าสามารถลงชื่อและเข้ารหัสเพื่อยืนยันแหล่งที่มา รับรองความถูกต้อง และปกป้องเนื้อหาได้ โปรไฟล์กำหนดค่าจะเข้ารหัสโดยใช้ CMS (RFC 3852) ซึ่งรองรับ 3DES และ AES-128

และยังสามารถล็อคโปรไฟล์กำหนดค่าเข้ากับอุปกรณ์เพื่อป้องกันการเอาออก หรือเพื่ออนุญาตให้เอาออกได้เมื่อมีรหัสผ่านเท่านั้น เนื่องจากผู้ใช้ระดับองค์กรจำนวนมากใช้อุปกรณ์ iOS ของตัวเอง จึงสามารถเอาโปรไฟล์กำหนดค่าที่ผูกมัดอุปกรณ์เข้ากับเซิร์ฟเวอร์ MDM ออกได้ แต่การทำเช่นนั้นจะเอาข้อมูลการกำหนดค่า ข้อมูล และแอพที่ได้รับการจัดการออกด้วยเช่นกัน

ผู้ใช้สามารถติดตั้งโปรไฟล์กำหนดค่าบนอุปกรณ์ของพวกเขาโดยตรงได้โดยใช้ Apple Configurator หรือดาวน์โหลดผ่าน Safari ส่งผ่านข้อความเมล หรือส่งแบบไร้สายโดยใช้เซิร์ฟเวอร์ MDM

การจัดการอุปกรณ์เคลื่อนที่ (MDM)

iOS รองรับ MDM จึงทำให้ธุรกิจต่างๆ สามารถกำหนดค่าและจัดการการนำ iPhone และ iPad ไปใช้ในองค์กรได้อย่างปลอดภัย ความสามารถของ MDM สร้างขึ้นบนเทคโนโลยี iOS ที่มีอยู่แล้ว เช่น โปรไฟล์กำหนดค่า การลงทะเบียนแบบไร้สาย และบริการการแจ้งเตือนแบบผลักข้อมูลของ Apple (APN) ตัวอย่างเช่น จะใช้ APN เพื่อปลุกอุปกรณ์เพื่อให้สามารถสื่อสารกับเซิร์ฟเวอร์ MDM ได้โดยตรงผ่านการเชื่อมต่อที่ปลอดภัย ข้อมูลลับหรือข้อมูลความเป็นเจ้าของจะไม่ส่งผ่าน APN

เมื่อใช้ MDM แผนก IT จะสามารถลงทะเบียนอุปกรณ์ iOS ในสภาพแวดล้อมองค์กร กำหนดค่าและอัพเดทการตั้งค่าแบบไร้สาย ตรวจสอบการปฏิบัติตามนโยบายองค์กร และแม้กระทั่งล้างข้อมูลหรือล็อคอุปกรณ์ที่จัดการอยู่ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการอุปกรณ์เคลื่อนที่ โปรดดู www.apple.com/iphone/business/it/management.html

iPad ที่ใช้ร่วมกัน

iPad ที่ใช้ร่วมกันคือโหมดหลายผู้ใช้สำหรับใช้ในการใช้งาน iPad เพื่อการศึกษา ซึ่งจะทำให้นักเรียนสามารถใช้ iPad ร่วมกันได้โดยไม่ใช้เอกสารและข้อมูลร่วมกัน iPad ที่ใช้ร่วมกันต้องใช้ Apple ID ที่ได้รับการจัดการซึ่งโรงเรียนเป็นผู้ออกและผู้ควบคุม iPad ที่ใช้ร่วมกันทำให้นักเรียนสามารถลงชื่อเข้าใช้อุปกรณ์ที่องค์กรเป็นเจ้าของทุกเครื่องที่กำหนดค่าสำหรับใช้โดยนักเรียนหลายคนได้

ข้อมูลของนักเรียนจะถูกแบ่งเป็นไดเร็กเทอรี่เริ่มต้นแยกจากกัน โดยแต่ละไดเร็กเทอรี่จะได้รับการป้องกันจากทั้งสิทธิ์อนุญาตของ UNIX และ Sandbox เมื่อนักเรียนลงชื่อเข้า Apple ID ที่ได้รับการจัดการจะถูกรับรองความถูกต้องกับเซิร์ฟเวอร์ข้อมูลประจำตัวของ Apple โดยใช้โปรโตคอล SRP หากสำเร็จ จะได้รับโทเค็นการเข้าถึงระยะสั้นเฉพาะอุปกรณ์ หากนักเรียนเคยใช้อุปกรณ์มาก่อน เขาจะมีบัญชีผู้ใช้ในเครื่องที่ปลดล็อคอยู่แล้ว หากนักเรียนไม่เคยใช้อุปกรณ์มาก่อน จะได้รับการจัดเตรียม ID ผู้ใช้ของ UNIX ไดเร็กเทอรี่เริ่มต้น และพวงกุญแจใหม่ (หากอุปกรณ์ไม่ได้เชื่อมต่ออยู่กับอินเทอร์เน็ต ผู้ใช้ที่มีบัญชีในเครื่องอยู่ก่อนแล้วเท่านั้นที่จะสามารถลงชื่อเข้าได้)

หลังจากที่บัญชีในเครื่องของนักเรียนถูกปลดล็อคหรือถูกสร้างแล้ว หากบัญชีนั้นได้รับการรับรองความถูกต้องจากระยะไกล โทเค็นระยะสั้นที่ออกโดยเซิร์ฟเวอร์ของ Apple จะถูกแปลงเป็นโทเค็น iCloud ที่อนุญาตให้ลงชื่อเข้าสู่ iCloud การตั้งค่าของนักเรียนคนถัดไปจะถูกกู้คืนและเอกสารและข้อมูลของเขาจะถูกเชื่อมข้อมูลจาก iCloud

ขณะที่เซสชั่นของนักเรียนยังทำงานอยู่และอุปกรณ์ยังออนไลน์ เอกสารและข้อมูลจะถูกจัดเก็บบน iCloud เมื่อสร้างหรือแก้ไข นอกจากนี้ กลไกเชื่อมข้อมูลเบื้องหลังจะช่วยให้มั่นใจได้ว่าการเปลี่ยนแปลงจะถูกผลักไปที่ iCloud หลังจากที่นักเรียนลงชื่อออก

Apple School Manager

Apple School Manager เป็นบริการสำหรับสถาบันการศึกษาที่ทำให้สามารถซื้อเนื้อหา กำหนดค่าการลงทะเบียนอุปกรณ์โดยอัตโนมัติในโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) สร้างบัญชีสำหรับนักเรียนและพนักงาน และตั้งค่าหลักสูตร iTunes U Apple School Manager สามารถเข้าถึงได้บนเว็บและออกแบบมาสำหรับผู้จัดการฝ่ายเทคโนโลยีและผู้ดูแลระบบ IT พนักงาน และผู้สอน

การลงทะเบียนอุปกรณ์

โปรแกรมการลงทะเบียนอุปกรณ์ (DEP) จะมอบวิธีที่รวดเร็วและไม่ซับซ้อนในการเปิดใช้งานอุปกรณ์ iOS ที่องค์กรซื้อโดยตรงจาก Apple หรือซื้อผ่านผู้ค้าที่ได้รับอนุญาตจาก Apple และผู้ให้บริการที่เข้าร่วม การลงทะเบียนอุปกรณ์ยังเป็นคุณสมบัติที่รวมอยู่ใน Apple School Manager สำหรับสถาบันการศึกษาอีกด้วย

องค์กรสามารถลงทะเบียนอุปกรณ์ใน MDM โดยอัตโนมัติได้โดยไม่ต้องแตะหรือเตรียมอุปกรณ์ก่อนที่ผู้ใช้จะได้รับ หลังจากที่ลงทะเบียนในโปรแกรมแล้ว ให้ผู้ดูแลระบบลงชื่อเข้าสู่เว็บไซต์ของโปรแกรม จากนั้นเชื่อมโยงโปรแกรมเข้ากับเซิร์ฟเวอร์ MDM จากนั้นจะสามารถกำหนดอุปกรณ์ที่ซื้อให้กับผู้ใช้ผ่าน MDM ได้ เมื่อกำหนดผู้ใช้แล้ว จะติดตั้งการกำหนดค่า ข้อจำกัด หรือการควบคุมทั้งหมดที่ MDM ระบุ การสื่อสารทั้งหมดระหว่างอุปกรณ์กับเซิร์ฟเวอร์ของ Apple จะถูกเข้ารหัสในระหว่างที่ส่งผ่าน HTTPS (SSL)

และสามารถทำให้กระบวนการตั้งค่าสำหรับผู้ใช้ง่ายดายขึ้นไปอีกได้ด้วยการเอาขั้นตอนบางอย่างในผู้ช่วยตั้งค่าออก เพื่อให้ผู้ใช้สามารถเริ่มต้นใช้งานได้อย่างรวดเร็ว ผู้ดูแลระบบยังสามารถควบคุมว่าผู้ใช้จะสามารถเอาโปรไฟล์ MDM ออกจากอุปกรณ์ได้หรือไม่ ซึ่งจะช่วยให้มั่นใจได้ว่าข้อจำกัดของอุปกรณ์จะอยู่ในเครื่องตั้งแต่ต้น เมื่อแกะกล่องและเปิดใช้งานอุปกรณ์แล้ว อุปกรณ์จะลงทะเบียนใน MDM ขององค์กร แล้วการตั้งค่าการจัดการ แอพ และหนังสือทั้งหมดจะถูกติดตั้ง

สำหรับข้อมูลเพิ่มเติม โปรดดู วิธีใช้โปรแกรมการลงทะเบียนอุปกรณ์ หรือสำหรับสถาบันการศึกษา โปรดดู วิธีใช้ Apple School Manager

หมายเหตุ: การลงทะเบียนอุปกรณ์อาจไม่มีให้ใช้งานในบางประเทศหรือภูมิภาค

Apple Configurator 2

นอกจาก MDM แล้ว Apple Configurator สำหรับ OS X ก็เป็นอีกวิธีที่ทำให้การตั้งค่าและ การกำหนดค่าล่วงหน้าก่อนที่จะส่งอุปกรณ์ให้กับผู้ใช้เป็นเรื่องง่าย Apple Configurator สามารถ ใช้เพื่อกำหนดค่าอุปกรณ์ล่วงหน้าด้วยแอพ ข้อมูล การจำกัด และการตั้งค่าต่างๆ

Apple Configurator 2 ทำให้คุณสามารถใช้ Apple School Manager (สำหรับการศึกษา) หรือ โปรแกรมการลงทะเบียนอุปกรณ์ (สำหรับธุรกิจ) เพื่อลงทะเบียนอุปกรณ์ในโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) โดยผู้ใช้ไม่ต้องใช้ผู้ช่วยตั้งค่า

การกำกับดูแล

ในระหว่างที่ตั้งค่าอุปกรณ์ องค์กรจะสามารถกำหนดค่าอุปกรณ์ให้ได้รับการกำกับดูแลได้ การกำกับดูแลหมายถึงอุปกรณ์นั้นจะเป็นของสถาบัน ซึ่งจะมอบการควบคุมเพิ่มเติมเกี่ยวกับการกำหนดค่าและข้อจำกัด อุปกรณ์สามารถได้รับการกำกับดูแลในระหว่างที่ตั้งค่าผ่านทาง Apple School Manager, โปรแกรมการลงทะเบียนอุปกรณ์หรือ Apple Configurator

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดค่าและการจัดการอุปกรณ์โดยใช้ MDM หรือ Apple Configurator โปรดดูการอ้างอิงการเปิดใช้งาน iOS

การจำกัด

ผู้ดูแลระบบสามารถจำกัดคุณสมบัติของอุปกรณ์ได้โดยการติดตั้งโปรไฟล์กำหนดค่า ข้อจำกัดที่มีให้ใช้บางส่วนประกอบด้วย:

- อนุญาตให้ติดตั้งแอพ
- อนุญาตให้เชื่อถือแอพขององค์กร
- อนุญาตให้ใช้กล้อง
- อนุญาตให้ใช้ FaceTime
- อนุญาตให้ถ่ายภาพหน้าจอ
- อนุญาตให้โทรออกด้วยเสียงเมื่อล็อคอยู่
- อนุญาตให้เชื่อมข้อมูลโดยอัตโนมัติขณะโรมมิ่ง
- อนุญาตให้ทำการซื้อภายในแอพ
- อนุญาตให้เชื่อมข้อมูลของเมลล่าสุด
- บังคับให้ผู้ใช้ป้อนรหัสผ่านของร้านค้าทุกครั้งที่ซื้อ
- อนุญาตให้ใช้ Siri ขณะที่อุปกรณ์ล็อคอยู่
- อนุญาตให้ใช้ iTunes Store
- อนุญาตเอกสารจากแหล่งที่จัดการอยู่ในปลายทางที่ไม่ได้จัดการ
- อนุญาตเอกสารจากแหล่งที่ไม่ได้จัดการอยู่ในปลายทางที่จัดการ
- อนุญาตให้เชื่อมข้อมูลพวงกุญแจ iCloud
- อนุญาตให้อัพเดทฐานข้อมูลที่เชื่อถือของใบรับรองแบบไร้สาย
- อนุญาตให้แสดงการแจ้งเตือนบนหน้าจอล็อค
- บังคับให้การเชื่อมต่อ AirPlay ใช้รหัสผ่านการจับคู่
- อนุญาตให้ Spotlight แสดงเนื้อหาที่ผู้ใช้สร้างจากอินเทอร์เน็ต
- เปิดใช้งานคำแนะนำโดย Spotlight ใน Spotlight
- อนุญาตให้ใช้ Handoff
- ถือว่า AirDrop เป็นปลายทางที่ไม่ได้จัดการ
- อนุญาตให้สำรองข้อมูลหนังสือขององค์กร
- อนุญาตให้เชื่อมข้อมูลโน้ตและที่คั่นหน้าในหนังสือขององค์กรกับอุปกรณ์ของผู้ใช้ทั้งหมด
- อนุญาตให้ใช้ Safari
- เปิดใช้งานการป้อนอัตโนมัติใน Safari
- บังคับเตือนเว็บไซต์หลอกลวง
- เปิดใช้งาน JavaScript
- จำกัดการติดตามโฆษณาใน Safari
- ปิดกั้นป๊อปอัพ
- ยอมรับคุกกี้
- อนุญาตข้อมูลสำรอง iCloud
- อนุญาตให้เชื่อมข้อมูลเอกสาร iCloud และค่ากุญแจ
- อนุญาตการแชร์รูปภาพ iCloud
- อนุญาตให้ส่งการวินิจฉัยให้กับ Apple
- อนุญาตให้ผู้ใช้ยอมรับใบรับรอง TLS ที่ไม่เป็นที่เชื่อถือ
- บังคับให้เข้ารหัสข้อมูลสำรอง
- อนุญาต Touch ID
- อนุญาตให้เข้าถึงศูนย์ควบคุมได้จากหน้าจอล็อค
- อนุญาตมุมมองวันนี้จากหน้าจอล็อค
- ต้องใช้การตรวจจับข้อมือของ Apple Watch
- อนุญาตให้แอพห้องเรียนดูหน้าจอ
- ใช้ AirDrop จากแอพที่ได้รับการจัดการ
- เชื่อถือผู้พัฒนาแอพองค์กรใหม่
- ใช้คลังรูปภาพ iCloud

ข้อจำกัดสำหรับผู้ดูแลเท่านั้น

- อนุญาตให้ใช้ iMessage
- อนุญาตให้เอาแอพออก
- อนุญาตให้ติดตั้งโปรไฟล์กำหนดค่าด้วยตัวเอง
- พร็อกซี่เครือข่ายส่วนกลางสำหรับ HTTP
- อนุญาตให้จับคู่กับคอมพิวเตอร์เพื่อเชื่อมข้อมูลเนื้อหา
- จำกัดการเชื่อมต่อ AirPlay ด้วยบัญชีขาวและรหัสผ่านการเชื่อมต่อ (ไม่บังคับ)
- อนุญาตให้ใช้ AirDrop
- อนุญาตให้แก้ไขคุณสมบัติค้นหาเพื่อนๆ ของฉัน
- อนุญาตให้แอพที่จัดการบางแอพใช้ Single App Mode ด้วยตนเอง
- อนุญาตให้แก้ไขบัญชี
- อนุญาตให้แก้ไขข้อมูลเซลลูลาร์
- อนุญาตให้จับคู่กับโฮสต์ (iTunes)
- อนุญาตให้ล็อคการเข้าใช้งานเครื่อง
- ป้องกันการลบข้อมูลและการตั้งค่าทั้งหมด
- ป้องกันการเปิดใช้งานข้อจำกัด
- กรองเนื้อหาของบริษัทอื่น
- โหมดแอพหนึ่งเดียว
- VPN แบบเปิดตลอดเวลา
- อนุญาตให้แก้ไขรหัสผ่านตัวเลข
- อนุญาตให้จับคู่ Apple Watch
- อนุญาตให้ดาวน์โหลดแอพโดยอัตโนมัติ
- อนุญาตให้ใช้การคาดเดาข้อความ เสนอคำอัตโนมัติ การตรวจการสะกดคำ และปุ่มลัดของแป้นพิมพ์
- อนุญาตให้ใช้ Apple Music
- อนุญาตให้ใช้วิทยุ
- การดูหน้าจอโดยแอพห้องเรียน
- การเปลี่ยนแปลงการตั้งค่าการแจ้งเตือน
- แสดงหรือซ่อนแอพใดแอพหนึ่งบนหน้าจอโฮม
- ติดตั้งแอพโดยใช้ App Store
- ดาวน์โหลดแอพโดยอัตโนมัติ
- ปุ่มลัดแป้นพิมพ์
- อนุญาตให้กำหนด
- แก้ไขชื่ออุปกรณ์
- การเปลี่ยนภาพพื้นหลัง
- ซ่อนแอพข่าว
- จับคู่กับ Apple Watch

สำหรับข้อมูลเกี่ยวกับการควบคุมอุปกรณ์ที่กำกับดูแลเพิ่มเติม โปรดดู การอ้างอิงโปรไฟล์กำหนดค่า

การลบข้อมูลระยะไกล

ผู้ดูแลระบบหรือผู้ใช้สามารถลบอุปกรณ์ iOS จากระยะไกลได้ สามารถทำการลบข้อมูลระยะไกลโดยอัตโนมัติได้โดยการทิ้งกุญแจเข้ารหัสบล็อคเก็บข้อมูลออกจากพื้นที่จัดเก็บที่ลบได้ ซึ่งจะทำให้อ่านข้อมูลทั้งหมดไม่ได้ สามารถเริ่มคำสั่งลบข้อมูลระยะไกลได้โดย MDM, Exchange หรือ iCloud

เมื่อ MDM หรือ iCloud ใช้คำสั่งลบข้อมูลระยะไกล อุปกรณ์จะส่งข้อมูลการรับรู้แล้วทำการลบข้อมูล สำหรับการลบข้อมูลระยะไกลผ่าน Exchange อุปกรณ์จะเช็คอินกับเซิร์ฟเวอร์ Exchange ก่อนที่จะทำการลบข้อมูล

ผู้ใช้ยังสามารถลบข้อมูลในอุปกรณ์ที่ครอบครองอยู่ได้โดยใช้แอพการตั้งค่า และตามที่ได้กล่าวไปแล้ว คุณสามารถตั้งค่าให้อุปกรณ์ทำการลบข้อมูลโดยอัตโนมัติหลังจากที่ป้อนรหัสผ่านตัวเลขผิดหลายครั้งติดต่อกัน

โหมดสูญหาย

หากอุปกรณ์สูญหายหรือถูกขโมย ผู้ดูแลระบบ MDM สามารถเปิดใช้งานโหมดสูญหายบนอุปกรณ์ที่ได้รับการกำกับดูแลที่ใช้ iOS 9.3 ขึ้นไปจากระยะไกลได้ เมื่อเปิดใช้งานโหมดสูญหาย ผู้ใช้ปัจจุบันจะออกจากระบบและจะปลดล็อคอุปกรณ์ไม่ได้ หน้าจอจะแสดงข้อความที่สามารถผู้ดูแลระบบสามารถกำหนดเองได้ เช่น แสดงหมายเลขโทรศัพท์ให้โทรติดต่อเมื่อมีคนพบอุปกรณ์ เมื่ออุปกรณ์ถูกทำให้อยู่ในโหมดสูญหาย ผู้ดูแลระบบจะสามารถร้องขอให้อุปกรณ์ส่งตำแหน่งที่ตั้งปัจจุบันได้ เมื่อผู้ดูแลระบบปิดใช้โหมดสูญหาย ซึ่งเป็นวิธีเดียวที่จะสามารถออกจากโหมดนี้ได้ ผู้ใช้จะได้รับแจ้งเกี่ยวกับเรื่องนี้ผ่านทางข้อความบนหน้าจอล็อคและการแจ้งเตือนบนหน้าจอโฮม

การล็อคการเข้าใช้งานเครื่อง

เมื่อเปิดใช้ค้นหา iPhone ของฉันอยู่ จะไม่สามารถทำการเปิดใช้งานอุปกรณ์อีกครั้งโดยไม่ป้อนข้อมูลประจำตัว Apple ID ของเจ้าของ

อุปกรณ์ที่องค์กรเป็นเจ้าของควรได้รับการกำกับดูแลเพื่อให้องค์กรสามารถจัดการการล็อคการเข้าใช้งานเครื่องแทนที่จะต้องให้ผู้ใช้แต่ละคนป้อนข้อมูลประจำตัวของ Apple ID ของตัวเองเพื่อเปิดใช้งานอุปกรณ์อีกครั้ง

บนอุปกรณ์ที่ได้รับการกำกับดูแล โซลูชั่น MDM ที่เข้ากันได้จะสามารถจัดเก็บรหัสบายพาสเมื่อเปิดใช้งานการล็อคการเข้าใช้งานเครื่องอยู่ แล้วใช้รหัสนี้เพื่อล้างการล็อคการเข้าใช้งานเครื่องโดยอัตโนมัติเมื่อจำเป็นต้องลบอุปกรณ์และมอบให้กับผู้ใช้คนใหม่ โปรดดูรายละเอียดในเอกสารประกอบโซลูชั่น MDM ของคุณ

ตามค่าเริ่มต้นแล้ว อุปกรณ์ที่ถูกกำกับดูแลจะไม่สามารถเปิดใช้งานการล็อคการเข้าใช้งานเครื่อง ถึงแม้ว่าผู้ใช้จะเปิดใช้ค้นหา iPhone ของฉัน อย่างไรก็ตาม เซิร์ฟเวอร์ MDM อาจรับรหัสบายพาสแล้วอนุญาตให้เปิดใช้งานการล็อคการเข้าใช้งานเครื่องบนอุปกรณ์ก็ได้ หากเปิดใช้ค้นหา iPhone ของฉันอยู่ในขณะที่เซิร์ฟเวอร์ MDM เปิดใช้งานการล็อคการเข้าใช้งานเครื่อง ค้นหา iPhone ของฉันจะเปิดใช้งานตอนนั้น หากปิดใช้ค้นหา iPhone ของฉันอยู่ในขณะที่เซิร์ฟเวอร์ MDM เปิดใช้งานการล็อคการเข้าใช้งานเครื่อง ค้นหา iPhone ของฉันจะเปิดใช้งานเมื่อผู้ใช้เปิดใช้งานในครั้งถัดไป

สำหรับอุปกรณ์ที่ใช้ในบริบทด้านการศึกษากับ Apple ID ที่ได้รับการจัดการที่สร้างผ่าน Apple School Manager จะสามารถผูกการล็อคการเข้าใช้งานเครื่องเข้ากับ Apple ID ของผู้ดูแลระบบแทน Apple ID ของผู้ใช้ หรือเปิดใช้งานการใช้รหัสบายพาสของอุปกรณ์ได้

การควบคุมความเป็นส่วนตัว

Apple ให้ความสำคัญกับความเป็นส่วนตัวของลูกค้าอย่างยิ่งยวด และมีการควบคุมและตัวเลือกในตัวจำนวนมากที่ทำให้ผู้ใช้ iOS สามารถเลือกได้ว่าจะให้แอพใช้ข้อมูลของลูกค้าเมื่อใด และจะให้ใช้ข้อมูลใดได้บ้าง

บริการหาตำแหน่งที่ตั้ง

บริการหาตำแหน่งที่ตั้งจะใช้ GPS, บลูทูธ และ ตำแหน่งที่ตั้งของฮอตสปอต Wi-Fi จากฐานข้อมูลที่รวบรวมไว้ และตำแหน่งที่ตั้งของเสาสูงส่งสัญญาณเพื่อกำหนดตำแหน่งที่ตั้งโดยประมาณของผู้ใช้ บริการหาตำแหน่งที่ตั้งสามารถปิดได้โดยใช้สวิตช์เดียวในการตั้งค่า หรือผู้ใช้สามารถรับรองการเข้าถึงของแต่ละแอพที่ใช้บริการนี้ก็ได้ แอพต่างๆ อาจร้องขอข้อมูลตำแหน่งที่ตั้งเมื่อใช้แอพอยู่เท่านั้น หรืออาจร้องขอเมื่อใดก็ได้ ผู้ใช้สามารถเลือกไม่อนุญาตการเข้าถึงนี้ได้ และสามารถเปลี่ยนตัวเลือกได้ตลอดเวลาในการตั้งค่า จากการตั้งค่า คุณสามารถตั้งค่าเป็น ไม่อนุญาตเลย อนุญาตเมื่อใช้งานอยู่ หรือตลอดเวลา โดยขึ้นอยู่กับแอพที่ขอใช้ตำแหน่งที่ตั้ง และหากแอพที่ได้รับอนุญาตให้ใช้ตำแหน่งที่ตั้งได้ตลอดเวลาได้ใช้คำอนุญาตนี้ขณะที่อยู่ในโหมดเบื้องหลัง ผู้ใช้จะได้รับการเตือนเกี่ยวกับคำอนุญาตนี้และสามารถเปลี่ยนการเข้าถึงของแอพได้

นอกจากนี้ ผู้ใช้ยังสามารถควบคุมการใช้งานข้อมูลตำแหน่งที่ตั้งโดยบริการของระบบได้อย่างละเอียดอีกด้วย ซึ่งรวมถึงสามารถเปิดหรือปิดการรวมข้อมูลตำแหน่งที่ตั้งไว้ในข้อมูลที่รวบรวมโดยบริการวินิจฉัยและการใช้งานที่ Apple ใช้เพื่อปรับปรุง iOS, ข้อมูลของ Siri แบบอิงตามตำแหน่งที่ตั้ง, บริบทที่อิงตามตำแหน่งที่ตั้งสำหรับการค้นหาคำแนะนำโดย Spotlight, สภาพการจราจรในท้องถิ่น และสถานที่ที่ไปบ่อยที่ใช้เพื่อประมาณเวลาเดินทาง

การเข้าถึงข้อมูลส่วนตัว

iOS ช่วยป้องกันไม่ให้แอพต่างๆ เข้าถึงข้อมูลส่วนตัวของผู้ใช้โดยไม่ได้รับอนุญาต นอกจากนี้ในการตั้งค่า ผู้ใช้สามารถดูได้ว่าได้อนุญาตให้แอพใดบ้างเข้าถึงข้อมูลบางอย่าง เช่นเดียวกับการมอบหรือถอนสิทธิ์การเข้าถึงในอนาคตทั้งหมด ซึ่งรวมถึงการเข้าถึง:

- รายชื่อ
- ปฏิทิน
- เตือนความจำ
- รูปภาพ
- กิจกรรมเคลื่อนไหวบน iPhone 5s ขึ้นไป
- คลังสื่อ
- บัญชีสื่อสังคม เช่น ทวิตเตอร์และ Facebook
- ไมโครโฟน
- กล้อง
- HomeKit
- HealthKit
- การแชร์ผ่านบลูทูธ

หากผู้ใช้ลงชื่อเข้าสู่ iCloud อยู่ แอพต่างๆ จะได้รับสิทธิ์เข้าถึง iCloud Drive ตามค่าเริ่มต้น ผู้ใช้สามารถควบคุมสิทธิ์เข้าถึงของแต่ละแอพได้ที่ใต้ iCloud ในการตั้งค่า นอกจากนี้ iOS ยังมอบการจำกัดที่ป้องกันไม่ให้มีการเคลื่อนย้ายข้อมูลระหว่างแอพและบัญชีที่ติดตั้งโดย MDM กับแอพและบัญชีที่ผู้ใช้ติดตั้งเอง

นโยบายความเป็นส่วนตัว

สามารถดูนโยบายความเป็นส่วนตัวของ Apple แบบออนไลน์ได้ที่ www.apple.com/th/legal/privacy

บทสรุป

ความมุ่งมั่นทุ่มเทเพื่อความปลอดภัย

Apple มุ่งมั่นทุ่มเทเพื่อช่วยปกป้องลูกค้าด้วยเทคโนโลยีด้านความเป็นส่วนตัวและการรักษาความปลอดภัยชั้นนำที่ออกแบบมาเพื่อปกป้องข้อมูลส่วนบุคคล และวิธีการอันครอบคลุมเพื่อช่วยปกป้องข้อมูลขององค์กรในสภาพแวดล้อมแบบองค์กร

การรักษาความปลอดภัยในตัว iOS ตั้งแต่แพลตฟอร์มไปจนถึงเครือข่ายไปจนถึงแอพแพลตฟอร์ม iOS มีทุกสิ่งที่ธุรกิจต้องการให้ใช้งาน เมื่อทำงานร่วมกัน องค์ประกอบเหล่านี้จะมอบการรักษาความปลอดภัยชั้นนำให้กับ iOS โดยไม่ลดทอนประสบการณ์การใช้งานของผู้ใช้

Apple ใช้โครงสร้างพื้นฐานการรักษาความปลอดภัยที่สม่ำเสมอและรวมอยู่ในตัวทั้ง iOS และระบบแอพของ iOS การเข้ารหัสเนื้อที่เก็บข้อมูลด้วยฮาร์ดแวร์ทำให้สามารถลบข้อมูลจากระยะไกลได้เมื่ออุปกรณ์สูญหาย และทำให้ผู้ใช้สามารถเอาข้อมูลขององค์กรและข้อมูลส่วนตัวออกได้เมื่อขายหรือมอบอุปกรณ์ให้กับผู้อื่น และรวบรวมยังข้อมูลการวินิจฉัยโดยไม่ระบุตัวตนอีกด้วย

แอพ iOS ที่ออกแบบโดย Apple ได้สร้างขึ้นโดยคำนึงถึงการรักษาความปลอดภัย Safari มีการเลือกดูแบบปลอดภัยที่รองรับโปรโตคอลสถานะใบรับรองออนไลน์ (OCSP) ใบรับรอง EV และคำเตือนให้ยืนยันความถูกต้องของใบรับรอง แอพเมลจะใช้ประโยชน์จากใบรับรองของเมลที่ได้รับการรับรองความถูกต้องและเข้ารหัสโดยการรองรับ S/MIME ซึ่งทำให้สามารถใช้ S/MIME รายข้อความได้ ผู้ใช้ S/MIME จึงสามารถเลือกค่าเริ่มต้นให้ลงชื่อและเข้ารหัสเสมอ หรือเลือกวิธีการควบคุมปกป้องข้อความแต่ละข้อความก็ได้ iMessage และ FaceTime ยังมอบการเข้ารหัสแบบไคลเอนต์ทูไคลเอนต์อีกด้วย

สำหรับแอพของบริษัทอื่น การใช้การลงชื่อรหัส, Sandbox และสิทธิ์ร่วมกันจะทำให้ผู้ใช้ได้รับการปกป้องที่ไว้ใจได้จากไวรัส มัลแวร์ และการใช้ประโยชน์จากช่อโหว่อื่นๆ ที่จะลดทอนความปลอดภัยของแพลตฟอร์มอื่นๆ กระบวนการส่งให้พิจารณาของ App Store จะช่วยปกป้องผู้ใช้จากความเสี่ยงเหล่านี้โดยการตรวจสอบแอพ iOS ทุกแอพก่อนที่จะวางขายได้

เพื่อให้ได้ประโยชน์สูงสุดจากคุณสมบัติด้านความปลอดภัยในตัว iOS ขอแนะนำให้ธุรกิจต่างๆ ตรวจทานนโยบายด้าน IT และด้านความปลอดภัยของตัวเองเพื่อให้มั่นใจได้ว่ากำลังใช้ประโยชน์สูงสุดจากเทคโนโลยีรักษาความปลอดภัยหลายชั้นที่แพลตฟอร์มนี้นำเสนอ

Apple มีทีมงานด้านการรักษาความปลอดภัยเพื่อให้การสนับสนุนผลิตภัณฑ์ทั้งหมดของ Apple โดยเฉพาะ ทีมงานนี้จะช่วยตรวจสอบการรักษาความปลอดภัยและทดสอบผลิตภัณฑ์ที่กำลังพัฒนา รวมถึงผลิตภัณฑ์ที่วางจำหน่ายแล้ว ทีมงานของ Apple ยังมอบเครื่องมือรักษาความปลอดภัยและการฝึกอบรม และตรวจสอบรายงานปัญหาด้านความปลอดภัยและอันตรายอยู่ตลอดเวลาอีกด้วย Apple เป็นสมาชิกของ Forum of Incident Response and Security Teams (FIRST) หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการรายงานปัญหาให้กับ Apple และการสมัครใช้งานการแจ้งเตือนความปลอดภัย โปรดไปที่ apple.com/th/support/security.

อภิธานศัพท์

การสุ่มเค้าโครงพื้นที่ที่อยู่ (ASLR)	เทคนิคที่ iOS ใช้เพื่อทำให้การใช้ประโยชน์จากช่องโหว่ของข้อผิดพลาดของซอฟต์แวร์ยากขึ้นมาก โดยการทำให้แน่ใจว่าไม่สามารถคาดเดาที่อยู่หน่วยความจำและออฟเซ็ตได้ จึงทำให้ไม่สามารถเขียนโค้ดเพื่อเจาะช่องโหว่แบบตายตัว ใน iOS 5 ขึ้นไป ตำแหน่งของแอพระบบและคลังทั้งหมดจะเป็นแบบสุ่ม รวมถึงแอพของบริษัทอื่นทั้งหมดที่คอมไพล์เป็นโปรแกรมปฏิบัติงานแบบไม่ยึดกับตำแหน่ง
บริการการแจ้งเตือนแบบผลักข้อมูลของ Apple (APN)	บริการของ Apple ที่ครอบคลุมทั่วโลก ซึ่งจะนำส่งการแจ้งเตือนแบบผลักข้อมูลไปที่อุปกรณ์ iOS
Boot ROM	โค้ดแรกสุดที่หน่วยประมวลผลของอุปกรณ์จะดำเนินการเมื่อบูตเป็นครั้งแรก เนื่องจากเป็นส่วนสำคัญของหน่วยประมวลผล จึงไม่สามารถดัดแปลงได้ทั้งโดย Apple และผู้โจมตี
คลาส	กลไกป้องกันไฟล์และพวงกุญแจสำหรับ iOS และอาจหมายถึง API ที่ Apple ใช้เพื่อปกป้องไฟล์และรายการในพวงกุญแจ
อัพเกรดเฟิร์มแวร์อุปกรณ์ (DFU)	โหมดที่โค้ด Boot ROM ของอุปกรณ์จะรอให้กู้คืนผ่าน USB หน้าจอ จะเป็นสีดำเมื่ออยู่ในโหมด DFU แต่เมื่อเชื่อมต่อกับคอมพิวเตอร์ที่ใช้งาน iTunes จะแจ้งข้อความต่อไปนี้: “iTunes ตรวจพบ iPad ในโหมดการกู้คืน คุณต้องกู้คืน iPad ก่อนจึงจะใช้กับ iTunes ได้”
ECID	ตัวระบุแบบ 64 บิตที่เป็นเอกลักษณ์เฉพาะประจำหน่วยประมวลผลในอุปกรณ์ iOS แต่ละเครื่อง โดยจะใช้เป็นส่วนหนึ่งของกระบวนการทำให้เป็นเฉพาะบุคคล และไม่ถือว่าเป็นความลับ
พื้นที่จัดเก็บที่ลบได้	พื้นที่หนึ่งในเนื้อที่เก็บข้อมูล NAND ที่ใช้จัดเก็บกุญแจเข้ารหัสโดยเฉพาะ ซึ่งสามารถจัดการได้โดยตรงและสามารถลบข้อมูลได้อย่างปลอดภัย ถึงแม้ว่าพื้นที่นี้จะไม่สามารถปกป้องข้อมูลหากผู้โจมตีสามารถเข้าถึงตัวอุปกรณ์ได้ แต่กุญแจที่เก็บอยู่ในพื้นที่จัดเก็บที่ลบได้จะสามารถใช้เป็นส่วนหนึ่งของลำดับชั้นกุญแจเพื่อทำการลบข้อมูลอย่างรวดเร็วและส่งต่อการรักษาความปลอดภัย
กุญแจระบบไฟล์	กุญแจที่เข้ารหัส Metadata ของแต่ละไฟล์ รวมถึงคลาสกุญแจ โดยจะเก็บอยู่ในพื้นที่จัดเก็บที่ลบได้เพื่อทำการลบข้อมูลอย่างรวดเร็ว แทนที่จะเก็บเป็นความลับ
ID กลุ่ม (GID)	เหมือน UID แต่จะเป็นข้อมูลทั่วไปของหน่วยประมวลผลทั้งหมดในคลาส
โมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM)	คอมพิวเตอร์ที่ทนต่อการแทรกแซงเป็นพิเศษซึ่งจะปกป้องและจัดการกุญแจดิจิตอล
iBoot	โค้ดที่โหลดโดย LLB ดังนั้นจึงโหลด XNU ด้วย เพื่อเป็นส่วนหนึ่งของลำดับการบูตอย่างปลอดภัย
บริการข้อมูลประจำตัว (IDS)	ไดเร็กเทอรี่กุญแจสาธารณะ iMessage ที่อยู่ APN และหมายเลขโทรศัพท์และที่อยู่อีเมลของ Apple ที่ใช้เพื่อค้นหากุญแจและที่อยู่อุปกรณ์
วงจรรวม (IC)	มีอีกชื่อหนึ่งว่าไมโครชิป
Joint Test Action Group (JTAG)	เครื่องมือแก้ไขข้อผิดพลาดฮาร์ดแวร์มาตรฐานที่โปรแกรมเมอร์และผู้พัฒนาวงจรใช้
Keybag	โครงสร้างข้อมูลที่ใช้เพื่อจัดเก็บคอลเลกชั่นคลาสกุญแจ แต่ละประเภท (ผู้ใช้ อุปกรณ์ ระบบ ข้อมูลสำรอง การรับฝาก หรือข้อมูลสำรอง iCloud) จะมีรูปแบบเดียวกัน: • ส่วนหัวประกอบด้วย: – เวอร์ชั่น (ตั้งเป็น 3 ใน iOS 5) – ประเภท (ระบบ ข้อมูลสำรอง การรับฝาก หรือข้อมูลสำรอง iCloud) – Keybag UUID – HMAC หาก Keybag มีการลงชื่อ – วิธีการที่ใช้สำหรับห่อคลาสกุญแจ: พันด้วย UID หรือ PBKDF2 พร้อมด้วยจำนวน salt และ iteration • รายการคลาสกุญแจ: – UUID ของกุญแจ – คลาส (คลาสการป้องกันข้อมูลของไฟล์หรือพวงกุญแจนี้) – ประเภทการห่อ (กุญแจที่ได้จาก UID เท่านั้น กุญแจที่ได้จาก UID และกุญแจที่ได้จากรหัสผ่านตัวเลข) – คลาสกุญแจที่ถูกห่อ – กุญแจสาธารณะสำหรับคลาสแบบอสมมาตร

พวงกุญแจ	โครงสร้างพื้นฐานและชุด API ที่แอพ iOS และแอพของบริษัทอื่นใช้เพื่อจัดเก็บและดึงข้อมูลรหัสผ่าน กุญแจ และข้อมูลประจำตัวที่เป็นความลับอื่นๆ
การห่อกุญแจ	การเข้ารหัสกุญแจหนึ่งด้วยอีกกุญแจหนึ่ง โดย iOS ใช้การห่อกุญแจแบบ NIST AES ตาม RFC 3394
Low-Level Bootloader (LLB)	โค้ดที่ใช้งานโดย Boot ROM ดังนั้นจึงโหลด iBoot ด้วย เพื่อเป็นส่วนหนึ่งของลำดับการบูตอย่างปลอดภัย
กุญแจรายไฟล์	กุญแจ AES แบบ 256 บิตที่ใช้เพื่อเข้ารหัสไฟล์ในระบบไฟล์ กุญแจรายไฟล์จะถูกห่อด้วยคลาสกุญแจและจัดเก็บไว้ใน Metadata ของไฟล์
โปรไฟล์การกำหนดสิทธิ์	ไฟล์ plist ที่ลงชื่อโดย Apple ซึ่งมีชุดเอนทิตี้และสิทธิ์ที่ทำให้สามารถติดตั้งและทดสอบแอพต่างๆ บนอุปกรณ์ iOS ได้ โปรไฟล์การกำหนดสิทธิ์การพัฒนาจะแสดงรายการอุปกรณ์ที่ผู้พัฒนาเลือกเพื่อแจกจ่ายเป็นการเฉพาะกิจ และโปรไฟล์การกำหนดสิทธิ์การแจกจ่ายจะมี ID แอพของแอพที่องค์กรพัฒนา
การเทียบผังมุมรอยเส้นใต้ผิวหนัง	การแสดงเชิงคณิตศาสตร์ของทิศทางและความกว้างของรอยที่ได้มาจากส่วนหนึ่งของลายนิ้วมือ
สมาร์ทการ์ด	วงจรที่รวมและฝังอยู่ซึ่งมอบการยืนยันตัวตน การรับรองความถูกต้อง และเนื้อที่เก็บข้อมูลที่ปลอดภัย
System on a chip (SoC)	วงจรรวม (IC) ที่รวมองค์ประกอบหลายส่วนไว้ในชิปชิ้นเดียว Secure Enclave คือ SoC ภายในหน่วยประมวลผลกลางของ Apple รุ่น A7 ขึ้นไป
การพัน	กระบวนการเปลี่ยนรหัสผ่านตัวเลขของผู้ใช้เป็นกุญแจเข้ารหัสและเสริมด้วย UID ของอุปกรณ์ ซึ่งจะทำให้แน่ใจได้ว่าจะต้องทำการโจมตีด้วยการเดารหัสผ่านบนตัวอุปกรณ์เท่านั้น จึงเป็นไปได้ยากและไม่สามารถโจมตีแบบคู่ขนาน อัลกอริธึมการพันคือ PBKDF2 ซึ่งใช้ AES ที่ใส่กุญแจด้วย UID ของอุปกรณ์เป็นฟังก์ชันแบบกึ่งสุ่ม (PRF) สำหรับการทำซ้ำแต่ละครั้ง
Uniform Resource Identifier (URI)	สตริงอักขระที่ระบุแหล่งข้อมูลบนเว็บ
ID เฉพาะ (UID)	กุญแจ AES แบบ 256 บิตที่ผู้ผลิตเขียนลงบนหน่วยประมวลผลแต่ละตัว ซึ่งเฟิร์มแวร์หรือซอฟต์แวร์จะอ่านไม่ได้ และจะใช้โดยกลไก AES ของฮาร์ดแวร์ของหน่วยประมวลผลเท่านั้น หากต้องการรับกุญแจของจริง ผู้โจมตีจะต้องทำการโจมตีซิลิคอนของหน่วยประมวลผลด้วยวิธีการทางกายภาพที่ซับซ้อนและมีราคาแพง UID ไม่เกี่ยวข้องกับตัวระบุอื่นใดบนอุปกรณ์ รวมถึงแต่ไม่จำกัดเพียง UDID
XNU	Kernel ที่เป็นหัวใจสำคัญของระบบปฏิบัติการ iOS และ OS X ซึ่งจะถูกอนุมานว่าเชื่อถือได้ และบังคับใช้มาตรการรักษาความปลอดภัยต่างๆ เช่น การลงชื่อรหัส, Sandbox, การตรวจสอบสิทธิ์ และ ASLR

ประวัติการแก้ไขเอกสาร

วันที่	เนื้อหาสรุป
พฤษภาคม 2016	**อัพเดทสำหรับ iOS 9.3** • iPad ที่ใช้ร่วมกัน • Apple ID ที่ได้รับการจัดการ • การรับรองความถูกต้องแบบสองปัจจัยสำหรับ Apple ID • Keybag • ใบรับรองความปลอดภัย • การล็อคการเข้าใช้งานเครื่อง • โน้ตที่ปลอดภัย • Apple School Manager • โหมดสูญหาย • สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเนื้อหาด้านความปลอดภัยของ iOS 9.3 โปรดดู: support.apple.com/th-th/HT206166
กันยายน 2015	**อัพเดทสำหรับ iOS 9** • การล็อคการเข้าใช้งานเครื่อง Apple Watch • นโยบายเกี่ยวกับรหัสผ่านตัวเลข • รองรับ Touch ID API • การป้องกันข้อมูลบน A8 จะใช้ AES-XTS • Keybag สำหรับการอัพเดทซอฟต์แวร์ที่ไม่ต้องจัดการ • อัพเดทใบรับรอง • โมเดลการเชื่อถือแอพขององค์กร • การป้องกันข้อมูลสำหรับที่คั่นหน้า Safari • ความปลอดภัยของการส่งข้อมูลแอพ • ข้อมูลจำเพาะของ VPN • การเข้าถึงระยะไกล iCloud สำหรับ HomeKit • บัตรสะสมแต้ม Apple Pay • แอพของผู้ออกบัตร Apple Pay • การทำดัชนีบนอุปกรณ์ของ Spotlight • โมเดลการจับคู่ iOS • Apple Configurator • การจำกัด • สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเนื้อหาด้านความปลอดภัยของ iOS 9 โปรดดู: support.apple.com/th-th/HT205212

© 2016 Apple Inc. สงวนลิขสิทธิ์ Apple, โลโก้ Apple, AirDrop, AirPlay, Apple TV, Apple Watch, Bonjour, FaceTime, iBooks, iMessage, iPad, iPhone, iPod, iPod touch, iTunes, พวงกุญแจ, Mac, OS X, Safari, Siri, Spotlight และ Xcode เป็นเครื่องหมายการค้าของ Apple Inc. ที่จดทะเบียนในสหรัฐอเมริกาและในประเทศอื่นๆ Apple Pay, CarPlay, Lightning, และ Touch ID เป็นเครื่องหมายการค้าของ Apple Inc. ขณะที่ iCloud และ iTunes Store เป็นเครื่องหมายบริการของ Apple Inc. ที่จดทะเบียนในสหรัฐอเมริกาและในประเทศอื่นๆ App Store และ iBooks Store เป็นเครื่องหมายบริการของ Apple Inc. ขณะที่ IOS เป็นเครื่องหมายการค้าหรือเครื่องหมายการค้าจดทะเบียนของ Cisco ในสหรัฐอเมริกาและในประเทศอื่นๆ และใช้โดยได้รับอนุญาต เครื่องหมายการค้าและโลโก้ Bluetooth® เป็นเครื่องหมายการค้าจดทะเบียนซึ่งเป็นเจ้าของโดย Bluetooth SIG Inc. และ Apple ใช้เครื่องหมายนี้โดยได้รับอนุญาต Java เป็นเครื่องหมายการค้าของ Oracle และบริษัทในเครือ ชื่อผลิตภัณฑ์และชื่อบริษัทอื่นๆ ที่อ้างถึงในที่นี้อาจเป็นเครื่องหมายการค้าของบริษัทที่เป็นเจ้าของ ข้อมูลจำเพาะของผลิตภัณฑ์สามารถเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบ