מאפייני אבטחה בהתקן הביומטרי הנייד SMUFS

	• אין מידע רגיש במכשיר – בשימוש הרגיל שלו, המכשיר לא אוגר מידע, אלא רק אוסף את טביעת האצבע ומשדר ל-Host. באופן זה, אם המכשיר נפרץ, לא ניתן לעשות בו שימוש זדוני מכל סוג. • נעילה רכה – מכשיר הSMUFS ניתן לנעילה ושחרור באמצעות טביעת האצבע של המפעיל המורשה. • מתג מחיקה פיזי – כל פתיחה של המכשיר גוררת מחיקה של כל המידע הרגיש מהמכשיר. • כל פתיחה פיזית של המכשיר משאירה סימנים – הקופסא של ה SMUFS מולחמת כך שלא ניתן לפתוח את המכשיר ללא השארת סימנים. • זיהוי טביעת אצבע חיה בלבד, טביעת אצבע מלאכותית תידחה • Fusing – מכשיר הSMUFS בלתי ניתן לפיצוח, כל ניסיון לבצע שינוי קושחה יגרור להרס בלתי הפיך של המכשיר • מארז חתום – שיברת הקופסא היא הדרך היחידה לפתוח את המכשיר. כל ניסיון לפתיחה פיזית יותיר ראיות.
	• מידע המועבר על גבי ה Bluetooth מוצפן – 256-bit AES • אפשרות הצפנה נוספת על גבי קישוריות הBluetooth (אופציונאלי) • שליחת קובץ templet, בלתי ניתן לשחזור, בלבד (אופציונלי)– שיחזור ו"גנבה" של טביעת אצבע, אינה אפשרית • רשימת כתובות MAC – ניהול רשימה של מכשירים ניידים המורשים לעבוד עם מכשיר הSMUFS • שימוש בתקשורת Bluetooth2 בעל רדיוס שידור מוגבל, וכתוצאה מכך מופחת הסיכון לפריצה או "האזנה" • קוד אבטחה נוסף – חסימת טלפונים שאינם מורשים
	• רשימת כתובות MAC – ניהול רשימה של מכשירים סורקי SMUFS מורשים • שימוש בתקשורת Bluetooth2 בעל רדיוס שידור מוגבל, וכתוצאה מכך מופחת הסיכון לפריצה או "האזנה"
	• שימוש בפרוטוקול SSL לתקשורת עם השרת • Low-friction – ניתן להשתמש ברשת מאובטחת של הלקוח • שידור על גבי רשתות WiFi ו GPRS בעלי פרוטוקולי אבטחה מחמירים • שליחת קובץ templet, בלתי ניתן לשחזור, בלבד (אופציונלי)– שיחזור ו"גנבה" של טביעת אצבע, אינה אפשרית
	• שימוש בפרוטוקול SSL לתקשורת עם השרת • Low fraction – ניתן להשתמש בשרת מאובטח של הלקוח • נעילה והגנת הגישה לקבוצת זהויות באמצעות טביעות אצבע מורשות • ניהול והגבלת המידע המתקבל מהשרת (תמונה בלבד, מזוהה/לא מזוהה וכד')