

« תקנים ביומטריים - על מפת התקינה הבין-לאומית



מאת: גבי קטי טילטון, סמנכ"ל לתקנים ולטכנולוגיות מתהוות בחברת Daon שבארה"ב, ראש המשלחת האמריקנית לוועדת המשנה ISO/IEC/JTC1/SC 37 לביומטריה, יו"ר ה-BioAPI Consortium ויו"ר קבוצה האד-הוק לביומטריה בתחום ה-e-Authentication. עורכת טכנית של תקן ה-BioAPI ב- SC37/WG2 והיו"ר הנוכחית של הוועדה הטכנית BIAS Integration ב-OASIS

קודם לאירועי האחד עשר בספטמבר, מרבית תקני הביומטריה עסקו בתחום של טביעת אצבעות למטרות אכיפת החוק. התקן הראשון בנושא העברה ממוחשבת של נתונים הנוגעים לזיהוי פלילי, "Data Format for the Interchange of - ANSI/NIST ITL1-2000 Fingerprint, Facial & Scar Mark & Tattoo Information (SMT)" פורסם בשנת 1986. בעקבותיו הוכן ופורסם תקן של ה-FBI העוסק אף הוא בהעברת מידע בתחום זה - "Electronic Fingerprint Transmission Specification (EFTS)". נוסף על שני התקנים האלה (ותקנים בנושאים קרובים), המהווים את הבסיס לחילופי נתונים הנוגעים לטביעת אצבעות בין רשויות אכיפת החוק בעולם כולו, פורסמו בסוף שנות ה-90 של המאה הקודמת התקנים המסחריים הראשונים בתחום הביומטריה. אולם רק בעקבות אירועי האחד עשר בספטמבר נוכחה הקהילה הבין-לאומית בצורך בתקנים ספציפיים בתחום הביומטריה ונעשתה מעורבת בהכנתם. בחודש יוני 2002 אישר ISO את התקנתה של ועדת משנה להכנת תקנים ביומטריים "נגריים" - SC37 JTC1 ISO/IEC. מפגש הפתיחה של ועדת משנה זו התקיים בחודש דצמבר 2002, ונכחו בו נציגים מ-17 מדינות. במעמד זה הקימה ועדת המשנה 6 קבוצות עבודה (WGs), ואלה מפורטות בטבלה שלהלן:

רבים בעולם טכנולוגיית המידע ובקהילה הביטחונית רואים בביומטריה תופעה שראשיתה בתקופה האחרונה - גורם חדש בזירה שזה עתה הצטרף למירוץ הטכנולוגי המואץ. אחרים טוענים שהביומטריה התפתחה בעקבות אירועי האחד עשר בספטמבר, במסגרת המאמץ להגן על הגבולות ולחזק את הביטחון הלאומי. רשויות אכיפת החוק רואות בביומטריה כלי בדוק ומונסה לזיהוי פלילי ולחקירות רקע. אלה גם אלה צודקים במידה רבה, כל אחד מנקודת המבט שלו. אולם ככל שהדבר נוגע לתקינה בתחום זה של הטכנולוגיה, הרי שמרבית התקנים העוסקים בביומטריה פורסמו רק בשנים האחרונות.

קנדה	Harmonized Biometric Vocabulary and Definitions	WG1
קוריאה הדרומית [הרפובליקה של קוריאה]	Biometric Technical Interfaces	WG2
גרמניה	Biometric Data Interchange Formats	WG3
ארצות הברית	Profiles for Biometric Applications	WG4
הממלכה המאוחדת [של בריטניה הגדולה וצפון אירלנד]	Biometric Testing and Reporting	WG5
איטליה	Cross Jurisdictional and Societal Aspects	WG6

ועדת המשנה. כיום מונה ועדת המשנה SC37 24 חברים משתתפים [P-members], 6 חברים משקיפים [O-members] ו-15 משתתפים נלווים. המדינות החברות ב-ISO המשתתפות בוועדת המשנה, בין אם במעמד של חבר משתתף ובין אם במעמד של חבר משקיף, מפורטות להלן:

בעמודה השמאלית בטבלה מצוינות המדינות שנציגיהן יושבים בראש קבוצות העבודה, ואשר בתוקף תפקידם זה מכנסים את קבוצות העבודה לדיונים. ארצות הברית מיוצגת בוועדת המשנה SC37 על ידי מכון התקנים הלאומי האמריקני [American National Standards Institute (ANSI)], הממלא את תפקידי מזכירות ועדת המשנה וראשות

חברים משקיפים [O-members]

פולניה	אוסטריה
פינלנד	דנמרק
שווייץ	הונגריה

במסמך המפרט את סמכויות ועדת המשנה SC37 ותפקידיה מתואר תחום הפעולה של ועדת המשנה כך: "תקינה של טכנולוגיות ביומטריות גנריות הרלוונטיות לבני אדם במטרה לתמוך ביכולת של מערכות שונות ויישומים שונים לתקשר ביניהם, להחליף נתונים ולעבוד בשיתוף פעולה."

ההתקדמות בעבודת ועדת המשנה SC37, והמצב נכון להיום

ובכן, מה עשתה ועדת המשנה SC37 במשך שלוש שנים וחצי של פעילות?

לזכותה של ועדת המשנה נזקפת שורה ארוכה של תקנים - תקנים מאושרים, תקנים בשלבי הכנה מתקדמים ויוזמות תקינה חדשות. אמנם, לעתים נשמעת ביקורת כי תהליך התקינה ב-ISO "איטי" מדי, אך מסתבר כי במקרה זה הביקורת אינה מוצדקת.

חברים משתתפים [P-members]

אוסטרליה	ישראל
אוקראינה	מלזיה
איטליה	נורווגיה
אירלנד	ניו זילנד
ארצות הברית	סין
גרמניה	סינגפור
דרום אפריקה	ספרד
הולנד	פורטוגל
הממלכה המאוחדת (של בריטניה הגדולה וצפון אירלנד)	צרפת
הפדרציה הרוסית (רוסיה)	קוריאה הדרומית (הרפובליקה של קוריאה)
הרפובליקה הצ'כית	קנדה
יפן	שוודיה

זיהוי ימאים

ארגון העבודה הבין-לאומי (International Labour Organization (ILO)), הפועל במסגרת ארגון האומות המאוחדות, הכין תוכנית להנפקת תעודות מזהות מאובטחות³ עבור ימאים. בהתאם לתוכנית זו נדרש, כי תבניות של פרטי טביעות האצבעות המאוחסנות על גבי תעודות הזרות של ימאים יעמדו בדרישות התקן הבין-לאומי ISO/IEC 19794-2.

● תוכניות לניהול מעברי גבול בין-לאומיים

מדינות רבות החלו לאחרונה ביישום תוכניות לניהול מעברי גבול, למעבר בטוח בין מדינות ולהנפקת תעודות זהות לאומיות. מסתבר כי לצורך מימוש תוכניות אלה, מספר רב של מדינות מסתייעות במערכת התקנים שהכניח ועדת המשנה SC37.



● המשרד לביטחון האומה של ארצות הברית

המשרד לביטחון האומה של ארצות הברית (US Department of Homeland Security (DHS)) דורש שימוש בתקני הביومترית הלאומיים של ארצות הברית בכמה מן הפרויקטים הביומטריים הגדולים שלו, ובהם:

- פרויקט לרישום ולזיהוי ביומטרי של אזרחים זרים המבקרים בארצות הברית ושל מהגרים אליה [US Visitor and Immigration Status Indicator Technology (US-VISIT)], הנערך במסגרת התוכנית הלאומית לניהול מעברי גבול;
- הפרויקט להנפקת תעודות מזהות מאובטחות עבור עובדי ענף התחבורה [Transportation Worker Identification Credential (TWIC)];
- תוכנית ה-Registered Traveler (RT)⁵ של המנהל לבטיחות בתחבורה [Administration (TSA) Transportation Security], הפועל במסגרת המשרד לביטחון האומה של ארצות הברית.

● משרד ההגנה של ארצות הברית

כמה מתקני הביומרית הלאומיים של ארצות הברית אומצו במסגרת ה-Joint Technical Architecture⁶ של משרד ההגנה של ארצות הברית [US Department of Defense (DoD) Defense Information Standards Registry].

לא מדובר כאן באוסף סתמי של תקנים שאין כל קשר ביניהם. למעשה, התרשים מייצג מערכת רב-שכבתית של תקנים שניתן לארגן אותם באופן היררכי, כשהאחד משמש בסיס למשנהו, ואשר ניתן להשתמש בהם גם במקביל, תוך התייחסות לכמה תקנים יחדיו. כך, למשל, יישום נתון (תוכנה המשמשת לביצוע מטלה מסוימת), שקיימת לגבי דרישה לתפעוליות בינית [interoperability]¹ והמבוסס על ארכיטקטורה פתוחה, עשוי להשתמש בתקן אחד או יותר של פורמט חילופי נתונים עבור הנתונים שהוא אוסף או/וגם מעבד (19794). לאחר מכן, יישום זה עשוי "לארוז" נתונים אלה ב"חבילה" אחת עם מטא-נתונים הקשורים במבנה CBEFF [Common Biometric Exchange File Format] (19785). ייתכן גם כי הנתונים עצמם יידרשו לעמוד בדרישות סף מסוימות הנוגעות לאיכות (24794), כאשר ערך האיכות נכלל ב־מֶטָא-נתונים. כמו כן, ליישום זה עשוי להיות ממשק [interface] לטכנולוגיה האוספת או המעבדת את הנתונים באמצעות ממשק תכנות תקני, כגון BioAPI² (19784), אשר מחזיר בתורו את הנתונים בפורמטים או ב"חבילות" המוגדרים. היישום עצמו עשוי להיות מפותח בהתאם לדרישות פרופיל יישום (24713), ולהיבדק כדי להבטיח שהוא עומד בדרישות ביצועים (19795). נוסף על כך, ייתכן כי היישום יידרש לפעול בסביבה שבה יש להביא בחשבון שיקולים הנוגעים לתחומים צולבים של סמכות שיפוטית או שיקולים הנוגעים לחברה כהילה מאורגנת הנושאת באחריות (24714). לפיכך, הכנת התקנים על ידי ועדת המשנה SC37 נעשית באופן המבטיח תואמות בין התקנים, כך שניתן יהיה להשתמש בהם יחדיו בהקשר מערכת.

אימוץ תקנים

לתקנים יש ערך מעשי רק אם מאמצים אותם, דהיינו: רק אם הם נדרשים על ידי לקוחות ומשמשים ספקים לצורך פיתוח ושיווק של מוצרים העומדים בדרישות התקנים. בדרך כלל קיים פער זמנים בין מועד זמינותם של תקנים לבין מועד זמינותם של מוצרים העומדים בדרישות התקנים. יתרה מזו, לעתים קרובות ספקים מעכבים מימוש של תקנים עד אשר מתעוררת דרישה בקרב ציבור הלקוחות להתאמת המוצרים לדרישות התקנים. להלן מובאות כמה דוגמות לאימוץ תקנים (הן תקנים לאומיים של ארצות הברית והן תקנים בין-לאומיים) על ידי משתמשי קצה.

דרכונים אלקטרוניים [e-passports]



הארגון הבין-לאומי לתעופה אזרחית [International Civil Aviation Organization (ICAO)], הפועל במסגרת ארגון האומות המאוחדות, קובע את הדרישות למסמכי מעבר קריאים על ידי מחשב [readable travel documents (MRTDs)], לרבות דרכונים ואשרות אלקטרוניים. הארגון הבין-לאומי לתעופה אזרחית דורש שנתונים ביומטריים המאוחסנים על גבי דרכונים אלקטרוניים יעמדו בדרישות הפורמט לחילופי נתונים ביומטריים שקבעה ועדת המשנה SC37 לגבי נתוני תווי הפנים, טביעות האצבעות וקשתית העין.

¹ היכולת לתקשר עם יישומים אחרים, להחליף אתם מידע ולעבוד אתם בשיתוף ובהרמוניה.
² ממשק תכנות יישומים המשרת טכנולוגיות ביומטריות שונות.
³ תעודות המזהות את נושא התעודה כבעל עיסוק או מעמד מקצועי מסוים, כאשר נתוני הזיהוי מוצפנים באופן הקריא על ידי מחשב.
⁴ פרויקט זה מהווה חלק מתוכנית ביטחונית כוללת למעקב אחר הכניסות לארצות הברית והיציאות ממנה.
⁵ תוכנית חלוץ זו של המנהל לבטיחות בתחבורה מאפשרת לנוסעים מתמידים לקבל הרשאת מעבר מהירה, מבוססת זיהוי ביומטרי, דרך ביקורת הגבולות בנמלי תעופה בארצות הברית ומחוצה לה. זכאים להשתתף בה אזרחי ארצות הברית ותושבים זרים בעלי מעמד של תושבי קבע העומדים בדרישות המנהל לבטיחות בתחבורה.
⁶ מטרת ה-Joint Technical Architecture (JTA) היא לאפשר למערכות נשק שונות לתקשר ביניהן, להחליף נתונים ולעבוד בשיתוף פעולה, וכן לקדם תכנון של מערכות של כלי נשק על בסיס ארכיטקטורת מערכות פתוחות.



לפיכך, נוסף על בדיקות התאמה לדרישות התקן, לעתים יש צורך לערוך בדיקות של התפעוליות הבינית. (יש לציין כי ניתן לצמצם את השפעתו של הגורם הראשון על ידי שימוש בתקני "פרופיל", המטילים הגבלות נוספות על מימוש האופציות שבמסגרת התקן - למשל, על ידי הגדרת האופציות שבהן ניתן להשתמש והאופציות שבהן לא ניתן להשתמש, על ידי הגבלת טווחי הערכים, וכדומה.)

התועלת שבתקנים

לא אחת נשאלת השאלה, מדוע אנו מייחסים חשיבות כה רבה לתקנים. ובכן, באופן כללי, תקנים טכניים תומכים בחליפות [interchangeability]⁷ ובתפעוליות בינית. הדבר מקטין את הסיכון הן עבור האינטגרטור⁸ והן עבור משתמש הקצה. זאת, בראש ובראשונה, משום שהדבר מפשט את האינטגרציה, מאפשר החלפה ושדרוג של טכנולוגיות, ומקטין את התלות בסק בלעדי אחד, על כל המשתמע מכך. יתרה מזו, הדבר עשוי להוביל להגדלת טווח המוצרים וזמינותם, ולחולל מגמה של הפיכת מצרכים או מוצרים, אשר בדרך כלל אינם נסחרים בשוק, לפריטים מסחריים⁹.

מן התועלת שבתקנים נהנה לא רק משתמש הקצה - יתרונותיהם באים לידי ביטוי לאורך שרשרת ההספקה כולה, כפי שממחיש התרשים שלהלן:

תחרות חופשית, שווקים חדשים, שימוש חוזר	ספקים
אפשרויות בחירה מרובות, קלות הביצוע של האינטגרציה	אינטגרטורים
גמישות, תפעוליות בינית, הקטנת הסיכונים	משתמשי קצה
רענון של טכנולוגיות, סביבות עבודה מגוונות	יזמים
בשלות, תחרות, נוכחות נרחבת בשווקים	התעשייה

על אף כל האמור לעיל, מפעם לפעם אנו נשאלים: "מדוע פתרונות המבוססים על תקנים טובים יותר מפתרונות שמספקים מוצרים בלעדיים?"

ובכן, אם להודות על האמת, התשובה אינה תמיד חד-משמעית לטובת מימוש התקן. השימוש בתקן הוא, כמעט תמיד, סוג מסוים של פשרה, של "קח ותן". אמנם המשתמש בתקן מרוויח תפעוליות בינית וחליפות [interchangeability], אך לעתים הוא מפסיד משהו אחר או נאלץ להשלים עם ירידה ברמה, באיכות או בערך של משהו אחר (כגון איכות הביצועים, רמת הבקרה). הגמישות שמעניק התקן למשתמש על ידי תמיכה במגוון של ספקים בא, לעתים קרובות, על חשבון ביצועים אופטימליים שמבטיח פתרון המוצע על ידי הבעלים של מוצר. הברירה היא, אם כן, בידי המשתמש, ועליו לשקול בכל מקרה את העלות לעומת התועלת שבמימוש התקן או שבדרישה להשתמש בו.

אימות נתוני הזהות האישיים של עובדי הממשל הפדרלי של ארצות הברית

בהתאם לצו הנשיאותי Homeland Security Presidential Directive 12 (HSPD), המכון הלאומי לתקנים ולטכנולוגיה של ארצות הברית, NIST [US National Institute of Standards and Technology], הכין מפרטים טכניים עבור המערכת הנלווית של הנפקת תעודות מזהות מאובטחות, המבוססת על זיהוי ביומטרי. במפרטים אלה נכללות דרישות להתאמה לפורמט הנתונים הביומטריים הנדרש בתקני הביומטריה הלאומיים של ארצות הברית העוסקים בטביעת אצבעות דיגיטלית, בתבניות של פרטי טביעות האצבעות ובסריקה ממוחשבת של תווי הפנים.

במקביל להתקדמות בהכנת תקני הביומטריה, חלה התקדמות מואצת גם בזמינותם של מוצרים בתחום זה. דוגמה לכך מספקים המוצרים המתאימים למנשק תכנות היישומים BioAPI, המשרת טכנולוגיות ביומטריות שונות. תקן BioAPI פורסם לראשונה בשנת 2001, ובשנת 2002 הפך לתקן ANSI רשמי. באותו מועד כבר הוכרז על פיתוחם של כ-40 מוצרים תואמים.

התאמה לתקן

לסוגיית אימוץ התקנים נלווית סוגיה חשובה לא פחות - זו של בדיקות התאמה לתקן. כיצד נדע האם מוצר מסוים אכן מתאים לתקן נתון? לשם כך יהיה עלינו לערוך בדיקה או הערכה ברמה כלשהי. אך מה הם הקריטריונים להתאמה לתקן? אמנם תקני ועדת המשנה SC37 כוללים כולם סעיף התאמה לתקן, המגדיר את הקבוצה המינימלית של דרישות שיש לקיים קודם שניתן יהיה להצהיר הצהרת התאמה לתקן (לעתים מוגדרות כמה קבוצות של דרישות, שעבור כל אחת מהן נבדקת ההתאמה לתקן בנפרד), אך לא בכל מקרה הדבר מספיק. על רקע זה מתעורר הצורך בתקן התאמה ספציפי ובמערך של בדיקות התאמה, כמפורט להלן:

● תקן הכולל הגדרת בדיקות התאמה לדרישות (דוגמת התקן שהוכן עבור מנשק תכנות היישומים BioAPI), אשר קובע מתודולוגיה של בדיקות והגדרה של מערך בדיקות נדרשות;

● תקן ספציפי המגדיר מערך של בדיקות.

במקרים מסוימים נקבעת תוכנית בדיקות התאמה לתקן, המנוהלת בדרך כלל על ידי גוף ממשלתי, ארגון תקינה או מעבדה הפועלת במעמד של צד שלישי, במטרה לבצע בדיקות התאמה של מוצר או מוצרים, ובדיקות אלה עשויות להוביל לסוג מסוים של התעדה או לפרסום רשימת מוצרים שנמצאו עומדים בדרישות.

בהקשר זה מתעוררת השאלה באשר לקשר שבין התאמה לדרישות לבין תפעוליות בינית [interoperability]. באופן כללי, התאמה לדרישות התקן נדרשת כדי לאפשר תפעוליות בינית; יחד עם זאת, התאמה לדרישות התקן אינה מהווה ערובה לתפעוליות בינית. הסיבה לכך נעוצה בשני גורמים עיקריים:

1. מימוש האופציות שבמסגרת התקן;

2. תנאים שמחוץ לתחום התקן או לטווח הבקרה של התקן.

⁷ היכולת להחליף את הרכיבים, החלקים או הציוד של יצרן מסוים באלה של יצרן אחר מבלי לפגוע בתפקוד או בהתאמה של המערכת בכללותה.
⁸ אינטגרטור [integrator] הוא אדם או ארגון המתמחה באינטגרציה של מערכות, בעיקר בתחומי טכנולוגיית המידע [IT], התעשייה הצבאית והתקשורת. בתחום טכנולוגיית המידע, אינטגרטור הוא בית מערכות [systems house].
⁹ מגמה זו מכונה באנגלית commoditization.

ד

אם נמשיך ונבחן את נושא המנשקים, הרי שפעמים רבות נשמעות טענות כגון: "אני יכול לבנות / בניתי משהו [מנשק] הרבה יותר טוב מזה הנדרש לפי תקן X". האמת היא שטענות אלה, בדרך כלל, נכונות. אולם משמעות הדבר היא, שאחת מן השתיים - או ספק היישום / התוכנה המתוכנת יצר שכבת מנשק משלו כדי לבודד את (יתרת) היישום מהטכנולוגיה, או שהספק הגדיר מנשק בעל זהות מותגית משלו, המחייב את ספקי המוצר להתאים את עצמם אליו (דהיינו, עליהם ליצור את שכבת הבידוד סביב המוצר שלהם). התוצאה היא, בדרך כלל, מנשק 'תפור לפי מידה', במיוחד בהתאם ליישום הספציפי (מה שאינו בהכרח דבר רע כשלעצמו). אך מה שקורה בפועל הוא שעדיין יש צורך לבנות שכבת מנשק ואת ניהול התצורה [ה-CM] המשיך אליה. כך, למשל, ספק עשוי להכריז על "תקן" מנשקים משלו - דהיינו, מנשק שהוא עצמו הגדיר, ואשר על שותפיו להתאים עצמם אליו. (זוהי דרך פעולה הרווחת בקרב חברות תוכנה - אם ברצונך לשלב את הטכנולוגיה שלך בטכנולוגיה או במוצר של חברה א', למשל, עליך להשתמש במנשקי תכנות היישומים [APIs] של אותה חברה. אם אותה חברה גדולה דיה או שולטת בנתח שוק גדול מספיק, ביכולתה להפעיל טקטיקות כאלה באין מפריע, מבלי שתיתן את הדין על כך.) כל זאת מוביל לשפע של יישומים תקינים כביכול, הצצים בשטח כפטריות אחר הגשם. הדבר מאלץ את הזכיינים המפיצים את מוצרי אותן חברות לבנות "מעטפת" שונה עבור כל "שותף" (או עבור כל לקוח גדול) שהגדירו מנשקי תכנות יישומים [APIs] "תקינים" משל עצמם. לחלופין, היישום או התוכנה המתוכנת בין יישומים מגדירים מנשקים אינדוידואליים עבור כל טכנולוגיה או בונים "מעטפות" משלהם סביב כל טכנולוגיה - ומתחזקים כל אחד מאלה.

האלטרנטיבה היא לבחור במנשק תקני תעשייתי יחיד (על יתרונו וחסרונו), המאפשר שימוש בכל טכנולוגיה המתאימה לדרישות התקן המחייב בלא שיתעורר הצורך בשינויים ובהתאמות ליישומים אלה או אחרים או לתכנות המתוכנת בין יישומים כל אימת שחלים שינויים במוצרי הספקים וככל שאלה מפותחים ומשודרגים.

מנקודת מבטו של הספק, שיקולים אלה הם חלק בלתי נפרד מהמאבק המתמיד בין ה'המוני' (הזמין ממקורות מרובים) לבין 'הטוב ביותר' (כמעט תמיד רכיב מותאם אישית, המיוצר לפי דרישה והמשווק כמוצר בעל זהות מותגית). ספקים משקיעים, לעתים קרובות, סכומים ניכרים במחקר ובפיתוח, מתוך שאיפה להשיג יתרון תחרותי (במילים אחרות: במטרה להשיג משהו שהוא 'הטוב ביותר'), אך בה בעת אינם פוסלים תמיכה ברכיבים ה'המוניים'. בדרך כלל אכן קיימת תועלת ממשית בפתרון המוצע על ידי הבעלים של מוצר. התשובה לשאלה, האם ה'עלות' של פתרון זה אכן כדאית, תלויה בצורכי המשתמש ובמידת האמון שיש למשתמש בספק. ('עלות' הפתרון עשויה לבוא לידי ביטוי, בין היתר, באפשרויות רכש מועטות יותר הפתוחות בפני המשתמש, בכך שהמשתמש 'שם את כל הביצים בסל אחד' - זה של ספק בלעדי - וכך נעשה תלוי בהיענותו של ספק יחיד ובמאמצים שזה משקיע בפיתוחים חדשים, בצורך להשתמש במנשקי יישומים 'תפורים לפי מידה', שאינם ניתנים להתאמה בקלות לשימוש חוזר, וכדומה. צורכי המשתמש הם, למשל, הקצב הצפוי של שינויים עתידיים, המשאבים הזמינים כדי לתחזק את ההתאמה האישית של המוצר לדרישות המשתמש, וכדומה.)

לעומת זאת, כאשר מכינים תקן שכל הנוגעים בדבר מסכימים עליו (דהיינו: תקן המבוסס על הסכמה כללית), התוצאה עשויה להיות במקרים מסוימים פחות מאופטימלית, ולעתים אף לייצג את המכנה המשותף הנמוך ביותר. ייתכן בהחלט, אם כן, שפתרון אופטימלי המוצע על ידי הבעלים של מוצר ייחשב מועיל פי כמה מהפתרון שמשפק התקן, שכן כמעט תמיד ניתן לבנות יישום 'תפור לפי מידה', בהתאם לדרישות ספציפיות מוגדרות, שאינו ניתן לשינוי ולהתאמה, והוא יהיה מהיר ויעיל יותר מיישום סטנדרטי כלשהו בעל יכולת להחליף נתונים ולעבוד בשיתוף פעולה עם יישומים אחרים.

נבחן, לשם דוגמה, את תחום התקנים הטכניים העוסקים במנשקי יישומים. הטבלה שלהלן משווה בין מנשקי יישומים סטנדרטיים לבין מנשקי יישומים (ביומטריים) מותאמים אישית:

מנשקי יישומים מותאמים אישית	מנשקי יישומים סטנדרטיים
<ul style="list-style-type: none"> ■ הספקים דואגים להביא את המנשקים למצב אופטימלי עבור המוצר שלהם וביצועיו, מה שעשוי להבטיח ביצועים טובים יותר של המערכת בכללותה (למשל, במונחים של זמני תגובה); ■ הספקים עשויים לספק פקודות ובקורות בסיסיות עבור המוצר שלהם, מה שמאפשר ליישומים גישה לפונקציות בקרה וכך הופך אותם למתוחכמים או למפורטים יותר. 	<ul style="list-style-type: none"> ■ מקטינים את מורכבות היישומים; ■ מאפשרים שימוש באותו מנשק עבור מגוון של מוצרים תואמים (מנשק גנרי יחיד, המוגדר באופן חד-פעמי); ■ מספקים הגנה מפני שינויים עתידיים; ■ מבטיחים אי-תלות בספק; ■ מאפשרים מסלול שדרוג קל ופשוט; ■ מפשטים ניהול תצורה [CM]; ■ ניתן להשתמש באותו מנשק עבור מספר רב של טכנולוגיות (כגון זיהוי ביומטרי של טביעות האצבעות, תווי הפנים וקשתיית העין).
<ul style="list-style-type: none"> ■ מנשקים מותאמים אישית חייבים להיות מוגדרים במסגרת כל יישום בנפרד עבור כל מוצר בעל זהות מותגית שיש לקשרו באמצעות מנשק, מה שעלול להגדיל את העלויות והמורכבות של היישום והתמיכה בו; ■ שינויים במנשק המותאם אישית או תוספות למנשק כזה עשויים לחייב שינויים בכל אחד מן היישומים (או בכל אחת מהתוכנות המתוכנות בין יישומים); ■ מנשקים מותאמים אישית עלולים להביא לתלות בספק בלעדי אחד. 	<ul style="list-style-type: none"> ■ עשויים לגרום לתקורה נוספת; ■ עלולים להיות חסרי יכולת לנצל את היכולות הייחודיות שמאפשר הספק; ■ המנשקים גנריים ומבוססים על הסכמה כללית, ומשום כך לא ניתן להביא אותם למצב אופטימלי לשימוש מיוחד.



מגמות בתקינה הביומטרית

בשלוש-ארבע השנים האחרונות חלה התקדמות ניכרת בתחום התקינה הביומטרית - התקדמות כה מרשימה עד כי ניתן לשאול: "מה עוד נותר לעשות שלא נעשה?" אם לענות בקצרה על שאלה זו, הרי שהתשובה היא: הרבה מאוד. כמה מן המגמות הצפויות בשנים הקרובות בתחום התקינה הביומטרית מפורטות להלן:

- פיתוח של תקני התאמה לדרישות. עתה, לאחר שכבר פורסמו תקנים בסיסיים רבים בתחום הביומטריה, הצורך לתמוך בבדיקות ובהערכות התאמה לדרישות מניע יוזמות להכנת תקני התאמה לדרישות. בשלב זה נמצאים בתכנון תקני התאמה עבור כל אחד מתקני תבניות חילוף הנתונים שבתוקף כיום.

- גיליונות תיקון ורוויזיות. ככל שאימוץ תקני ביומטריה בסיסיים והשימוש בהם נעשים רווחים יותר ויותר, מתעורר הצורך בעריכת שינויים בהם, בהרחבתם ובשיפורם. צורך זה נענה בהצעות לשינויים, לשיפורים ולהרחבת תחום החלות של תקנים אלה.

- גישור על פני פערים. הסבב הראשון של תקני ביומטריה עוסק בטכנולוגיות הביומטריות הרווחות ביותר בשימוש ובדרישה למתן מענה מהיר לצורך הדחוק בתפעוליות בינתי. הסבב השני של תקני ביומטריה צפוי להתמקד בתחומים שלא טופלו עד כה, בצרכים בולטים פחות אך חשובים לא פחות, ובטכנולוגיות חדשות יותר.

- השתתפות נרחבת יותר בתקינה. בשלב הראשון, מדינות מעטות בלבד היו מעורבות בתקינה הביומטרית - מדינות אלה העלו הצעות לפרויקטים של תקינה, הציעו עורכים לעריכת התקנים שבהכנה, ואף תרמו תרומה טכנית משמעותית לתהליך התקינה. לאחרונה החלו מדינות נוספות לגלות עניין בתהליך זה ולקחת חלק פעיל בו. מעורבות זו מחזקת את פעילות התקינה הביומטרית בכללה, ומאפשרת הכנת אוסף תקנים מפותח, מגוון ומקיף יותר מקודמו בסבב התקינה הבא.

לסיכום

התקינה הביומטרית עברה דרך ארוכה מאז עשתה את צעדיה המהוססים הראשונים בשנת 1986 - השנה שבה פורסם התקן הראשון בתחום טביעת אצבעות למטרות זיהוי פלילי. כיום עומדים לרשות כל הנוגעים בדבר תקנים רבים העוסקים בטכנולוגיות זיהוי ביומטרי, ורבים אחרים נמצאים בשלבי הכנה. שוב לא ניתן להשתמש בתירוצים כגון: "אין בנמצא תקנים העוסקים בביומטריה", או: "התקנים שבתוקף קשים מדי לשימוש". התקנים הנדרשים עומדים לרשות המשתמשים הפוטנציאליים, ויתרונות השימוש בהם רבים. תקינה כזו קריטית להתרחבות שוק הביומטריה ולשימוש האפקטיבי בטכנולוגיה מבטיחה.