INSO
20126-1
1st.Edition
2016

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران

۲۰۱۲۶-۱
چاپ اول
۱۳۹۴

فناوری اطلاعات

راهنمای استانداردها و کاربردهای مقایسه ای زیست‌سنجی روی کارت

, Information technology — Guide to on-card biometric comparison standards and applications

ICS: 35.080

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن تـوجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات – راهنمای استانداردها و کاربردهای مقایسه ای زیست‌سنجی روی کارت »

رئیس :	**سمت و/ یا نمایندگی**
جلالت، بهنام (کارشناس ارشد مهندسی صنایع)	کارشناس برنامه ریزی صنایع دفاع
دبیر:	
مرادی، فریبا (کارشناسی فناوری اطلاعات)	کارشناس فناوری اطلاعات و آمار اداره کل استاندارد ایلام
اعضاء : (اسامی به ترتیب حروف الفبا)	
آذرکار، علی (کارشناسی ارشد مهندسی نرم‌افزار)	مدیرعامل شرکت مهندسی پدیدپرداز تهران
بای، مهیا (کارشناسی مهندسی کامپیوتر)	کارشناس فناوری اطلاعات آموزش و پرورش البرز
بشارتی، رضا (کارشناسی مهندسی کامپیوتر)	کارشناس فناوری‌اطلاعات جهاد دانشگاهی استان ایلام
بهادری، فاطمه (کارشناسی مهندسی کامپیوتر)	کارشناس فناوری اطلاعات آموزش و پرورش استان البرز
پدرام، سعیده (کارشناسی مهندسی کامپیوتر)	کارشناس فناوری اطلاعات آموزش و پرورش استان البرز
خلیلی فر، نوید (کارشناسی ارشد هوش مصنوعی)	معاونت نرم افزار شرکت مهندسی بهین پژوهش خاور تهران
فرخی، ستاره (کارشناس ادبیات زبان انگلیسی)	کارشناس آموزش جهاد دانشگاهی استان ایلام

فهرست مندرجات

پیش‌گفتار

استاندارد « فناوری اطلاعات– راهنمای استانداردها و کاربردهای مقایسه ای زیست‌سنجی روی کارت » که پیش نویس آن درکمیسیون فنی مربوط، توسط سازمان ملی استاندارد ایران تهیه و تدوین شده ودر چهارصد و سومین اجلاسیه کمیته ملی فناوری اطلاعات مورخ۹۴/۱۲/۸ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادۀ ۳ قانون اصلاح قوانین و مقررات مؤسسۀ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ ، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینۀ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و مآخذی که برای تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC TR, 30117-1: 2014, Information technology — Guide to on-card biometric comparison standards and application

فناوری اطلاعات- راهنمای استانداردها و کاربردهای مقایسه ای زیست‌سنجی روی کارت

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین خلاصه ای از چگونگی استانداردهای ملی، ارتباطات، گزارش فنی مرتبط با کارت‌های شناسایی، زیست‌سنج‌ها و یا امنیت اطلاعاتی مرتبط با یکدیگر، در استفاده مشترک زیست‌سنج‌ها و کارت‌های مداری یکپارچه است. این استاندارد هم چنین برای خط‌مشی‌های مورد نیاز برای تدوین کنندگان یکپارچه‌سازی برنامه‌های کاربردی مرتبط با مقایسه زیست‌سنجی روی- کارت کاربرد دارد.

۲

اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می رود:

۲-۱ پروب زیست‌سنجی،

پرسمان زیست‌سنجی

نمونه زیست‌سنجی یا مجموعه ویژگی زیست‌سنجی، که ورودی الگوریتمی را برای استفاده به عنوان موضوع مقایسه زیست‌سنجی با مرجع(مراجع) زیست‌سنجی تنظیم می‌کند.

یادآوری ۱- اصطلاح مقایسه، به مقایسه در دریافت های زیست سنجی اشاره می کند.

یادآوری ۲- ممکن است، برچسب‌گذاری تحت عناوین موضوع شیء در یک مقایسه دلخواه باشد. در برخی مقایسه‌ها، ممکن است یک مرجع زیست‌سنجی به عنوان موضوع مقایسه با دیگر مراجع زیست‌سنجی، یا نمونه‌های ورودی استفاده شده به عنوان اشیاء مقایسه‌ها، به کار گرفته شود. به عنوان مثال، در بررسی ثبت تکراری، یک مرجع زیست‌سنجی به عنوان موضوعی برای مقایسه در برابر تمام مراجع زیست‌سنجی در دادگان ، به کار خواهد رفت.

یادآوری ۳- بطور نوعی در یک فرآیند مقایسه زیست‌سنجی، نمونه‌های ورودی آن به عنوان موضوع مقایسه زیست‌سنجی در مقابل مراجع آن در دادگان به کار گرفته خواهند شد.

[منبع : ISO/IEC 2382-37:2012]

یادآوری ۴- در هدف و دامنه کاربرد استانداردISO/IEC7816-11، [به مرجع ۶ کتاب نامه مراجعه شود] این دو اصطلاح تحت اصطلاح کلی‌تر «داده‌های تصدیق زیست‌سنجی» استفاده شده است.

۲-۲ مرجع زیست سنجی

یک یا چند نمونه از زیست‌سنجی ذخیره شده، الگو ها یا مدل‌های زیست‌سنجی منتسب شده به یک موضوع داده‌ای زیست‌سنجی است، و به عنوان هدف مقایسه آن به کار گرفته شده است.

مثال : تصویر صورت که روی گذرنامه به صورت رقمی ذخیره شده؛ الگوی جزئیات اثر انگشت روی کارت شناسایی ملی ؛ مدل ترکیبی گاوسی[1] برای تشخیص صدای سخنگو در یک دادگان است.

یادآوری ۱- ممکن است، یک مرجع زیست‌سنجی با کاربرد صریح و یا ضمنی داده‌های کمکی مثل مدل‌های پس زمینه جامع ایجاد شود.

یادآوری ۲- ممکن است ، برچسب‌گذاری موضوع/ شیء در یک مقایسه، اختیاری باشد. در برخی مقایسه‌ها، ممکن است مرجع زیست‌سنجی به عنوان موضوعی برای مقایسه با دیگر منابع آن یا نمونه‌های ورودی به کار رفته به عنوان اشیاء مقایسه، به کار رود. به طور مثال، در یک بررسی ثبت تکراری، یک مرجع زیست‌سنجی، به عنوان موضوعی برای مقایسه در برابر تمام منابع زیست‌سنجی دیگر موجود در پایگاه‌داده به کار گرفته می‌شود.

[منبع:ISO/IEC 2382-37: 2012]

یادآوری ۳- در هدف و دامنه کاربرد استاندارد11- ISO/IEC7816، [به منبع ۶ کتاب نامه مراجعه شود] این اصطلاح، تحت اصطلاح کلی‌تر «داده‌های مرجع زیست‌سنجی» استفاده می‌شود.

۲-۳ ویژگی زیست‌سنجی

به اعداد یا برچسب‌های استخراج شده از نمونه‌های زیست‌سنجی و مورد استفاده برای مقایسه گفته می شود.

یادآوری ۱- ویژگی‌ها زیست‌سنجی، خروجی یک استخراج کامل ویژگی‌های زیست‌سنجی است.

یادآوری ۲- بهتر است، استفاده از این اصطلاح سازگار با کاربرد آن توسط جوامع تشخیص الگو و ریاضیات باشد.

یادآوری ۳- هم‌چنین یک مجموعه ویژگی زیست‌سنجی می‌تواند به عنوان یک نمونه‌پردازش شده آن درنظر گرفته شود.

یادآوری ۴- ممکن است، ویژگی‌های زیست‌سنجی از یک نمونه میانی آن استخراج شده باشد.

یادآوری ۵- خود پالایه های به کار برده شده برای نمونه‌های زیست‌سنجی، از ویژگی‌های آن به شمار نمی‌آیند، با این حال، خروجی پالایه به کار رفته برای این نمونه‌ها، ممکن است خود، ویژگی آن محسوب شود. بنابراین مثلاً الگوهای اولیه چهره[2] زیست‌سنجی نیست.

[منبع ISO/IEC 2382-37:2012]

۲-۴ نمونه زیست‌سنجی

نمایش قیاسی یا رقمی مشخصه های زیست‌سنجی قبل از انجام استخراج ویژگی آن است.

مثال: یک رکورد، شامل تصویر یک انگشت، یک نمونه زیست‌سنجی است.

[منبع ISO/IEC 2382-37:2012]

1- Gaussian Mixture
2- Eigenfaces

۲-۵ الگوی زیست سنجی

مجموعه‌ای از ویژگی‌های زیست سنجی ذخیره شده و قابل مقایسه مستقیم با ویژگی‌های زیست‌سنجی مورد بررسی است.

یادآوری ۱- در هدف و دامنه کاربرد استانداردبه منبع ISO/IEC 7816، اصطلاح الگو معنای به طور کامل متفاوتی دارد، و بدین صورت تعریف می‌شود: « فیلد مقدار یک شی داده‌ای ایجاد شده» و اگر شی داده مورد نظر مرتبط با زیست سنجی باشد یا نه، اهمیتی ندارد.

۲-۶ نمونه میانی زیست سنجی / پروب

نمونه‌ی زیست سنجی یا پروب منتج شده از پردازش واسط نمونه‌ی آن است.

مثال: نمونه‌های زیست سنجی که برش داده شده، مختصر شده، فشرده یا ارتقاء داده شده اند، مثال‌هایی از نمونه‌های میانی زیست سنجی هستند.

[منبع ISO/IEC 2382-37:2012]

۲-۷ پردازش نمونه‌ی میانی زیست‌سنجی

هرگونه دستکاری یک نمونه زیست‌سنجی که ویژگی‌های آن را تولید نمی کند.

مثال: مثال‌هایی از پردازش نمونه زیست‌سنجی میانی شامل برش دادن، مختصر کردن، فشرده سازی، تبدیل به قالب های استانداردهای تبادل داده و ارتقاء تصویری می باشند.

[منبع ISO/IEC 2382-37:2012]

۲-۸ نمونه پردازش شده / پروب

نمونه زیست‌سنجی/ پروب منتج از پردازش نمونه‌ی زیست‌سنجی است، که آماده استفاده برای ذخیره به عنوان یک مرجع زیست‌سنجی بوده، یا قابل مقایسه با مرجع قبلی آن باشد.

مثال: جزئیات اثرانگشت یا کدهای عنبیه چشم، نمونه‌هایی از نمونه‌های زیست‌سنجی پردازش شده است.

۲-۹ نمونه زیست‌سنجی اخذ شده

نمونه خام زیست‌سنجی است. (منسوخ)

نمونه‌ی زیست‌سنجی منتج از یک فرآیند اخذ زیست‌سنجی است.

[منبع ISO/IEC 2382-37: 2012].

۳ نمادها و کوته نوشت ها

API [۱] واسط برنامه‌ی کاربردی

BIR [۲] رکورد اطلاعات زیست‌سنجی

CBEFF [۳] چارچوب قالب مشترک تبادل زیست‌سنجی

ICC [۴] کارت مداری یکپارچه

IFD [۵] افزاره واسط

SB [۶] بستک امنیتی، به گونه‌ای که در استاندارد ISO/IE 19785-1، برای CBEFF تعریف شده است

COS [۷] سامانه عامل کارت

۴ روابط میان زیست‌سنج‌ها وICCsها

استاندارد ISO/IEC 24787، [به مرجع ۱۶ کتاب نامه مراجعه شود] مقدمه جامعی را در مورد روش‌های متفاوتی بیان می کند، که در آنها زیست‌سنجی وICCsها می‌توانند در یک برنامه کاربردی نهایی یکپارچه شوند. این بخش به صورتی خلاصه در ادامه آمده، تا مقدمه مختصری را برای خواننده این استاندارد فراهم - آورد. هنگام یکپارچه‌سازی زیست‌سنج‌ها با ICCها، چهار رویکرد مختلف می‌تواند دنبال شود:

- ذخیره روی - کارت: در این مورد، از ICC برای ذخیره مرجع زیست‌سنجی استفاده می‌شود. برنامه کاربردی، در صورت نیاز، از روی ICC، مرجع زیست‌سنجی را خوانده و تمام فرآیندهای احراز هویت را در IFD یا مابقی سامانه اجرا می‌کند. سامانه عامل کارت (COS) واپایش بیشتری را روی داده‌های زیست‌سنجی، جدا از استفاده از همان سازوکارهای موجود در هنگام ذخیره‌سازی هر نوع دیگر از داده‌ها در ICC، ندارد.
- مقایسه زیست‌سنجی روی کارت: در این رویکرد، ICC نه تنها مرجع زیست‌سنجی را ذخیره کرده، بلکه همچنین مقایسه زیست‌سنجی درون کارت را به محض دریافت پروب زیست‌سنجی خارجی توسط ICC، انجام می‌دهد. با این رویکرد، COS می‌تواند واپایش مشابه مرجع زیست‌سنجی را برای همان کلیدهای اجرایی ذخیره شده در کارت، استفاده کند (به عنوان مثال، عدم اجازه خوانش مرجع زیست‌سنجی، واپایش تعداد مقایسه‌های ناموفق متوالی انجام شده، مسدود کردن سازوکار احراز هویت در صورت رسیدن به تعداد معینی از مقایسه‌های ناموفق متوالی و مانند آن). همچنین COS می‌تواند دسترسی به اطلاعات دیگری در کارت و یا فرامین موجود در کارت، را با در نظر گرفتن نتیجه زیست‌سنجی قبلی روی- کارت، واپایش کند. در این فناوری، پروب زیست‌سنجی معمولاً، به جای یک نمونه خام، یک مجموعه ویژگی زیست‌سنجی در نظر گرفته می‌شود.

1- Application Program Interface
2- Biometric Information Record
3-Common Biometric Exchange Format Framework
4-Integrated Circuit Card
5-Interface Device
6-Security Block
7-Card Operating System

- سازوکار به اشتراک‌گذاری کار برای مقایسه زیست‌سنجی روی - کارت: رویکرد قبلی ممکن است به دلایل مختلف قادر به یکپارچگی کامل با ICC نباشد، که رایج‌ترین آنها فقدان قابلیت‌های پردازشی ICC است. درچنین موردی، ممکن است، این امکان وجود داشته باشد که قسمتی در فرآیند در IFD یا سامانه اجرا شده، و نتایج به منظور اتمام فرآیند مقایسه، به ICC منتقل شود. اگر چه این امر در ابتدا برای به اشتراک‌گذاری‌کار روی الگوریتم‌های مقایسه تعریف شده، ولی طرح‌واره (شمای) مشابهی را می-توان برای پیش پردازش و مراحل استخراج ویژگی فرآیند زیست‌سنجی به کار گرفت. در مورد اولی، پروب زیست‌سنجی که برای کارت ارسال شود، بهتر است، یک مجموعه ویژگی زیست‌سنجی باشد، در حالی‌که در مورد دوم، پروب زیست‌سنجی می‌تواند یک مجموعه خام، یک نمونه میانی یا یک نمونه پردازش شده باشد.
- سامانه‌های روی- کارت[1]: این رویکرد مبتنی بر مشمول بودن تمام گام‌های فرآیند زیست‌سنجی در ICC ، شامل تحصیل نمونه، یعنی حسگر درون ICC جای دارد. به واسطه این تعریف، صرفاً شرایط خاصی را می‌توان با فناوری روز موجود در نظر قرار داد، که به آن مواردی محدود می‌شود که در آنها حسگر به قدری کوچک و منعطف است که به ICC اجازه می‌دهد که روش‌های آزمون مکانیکی و فیزیکی تعریف شده دراستاندارد ISO/IEC10373-1، را با موفقیت طی کند. اگر محدودیت‌های فیزیکی برداشته و انواع دیگری از ترکیب ها انتخاب شود (با حفظ انطباق با دیگر استانداردهای کاربردی ICC)، آنگاه می‌توان تعداد شرایط زیست‌سنجی را افزایش داد.

با وجود این مفاهیم اولیه، طراح یا تدوین کننده برنامه کاربردی، ناچار است، چندین تصمیم، برای تعریف سامانه کلی و ارتباط میان زیست‌سنج‌ها و ICCها اتخاذ کند. درخت تصمیم زیر به منظور شفاف سازی ارائه شده است، جایی که در آن بندهای بعدی این استاندارد به آنها ارجاع شده است:

الف) آیا سامانه قصد دارد تا یک طرح واره احراز هویت را پیاده‌سازی کند (یعنی کاربر هویت خود را ادعا کرده و مقایسه تنها بین نمونه ارائه شده و مرجع زیست‌سنجی کاربر مدعی صورت گرفته است) یا یک طرح‌واره شناسایی (یعنی نمونه زیست‌سنجی بهتر است، با کل پایگاه داده کاربران ثبت شده مقایسه شود)؟

۱) اگر یک طرح واره شناسایی استفاده شده است، دیگر هیچ نیازی به ارتباط بیشتری میان زیست‌سنج‌ها و ICCها وجود نخواهد داشت، در چنین حالتی، این استاندارد قابل کاربرد نخواهد بود.

ب) آیا سامانه، استفاده از یک پایگاه‌داده‌ای متمرکز را مد نظر قرار داده، یا قصد دارد آن را به شکل توزیع‌شده پیاده‌سازی کند؟

۱) اگر قصد بر استفاده از یک پایگاه‌داده متمرکز است و این چنین پایگاه‌داده‌ای، برای هر مورد منفرد احراز هویت مرتبط شود، پس نیاز به ارتباط بیشتر بین اطلاعات زیست‌سنجی و ICCها مورد نیاز نیست. بنابراین، این استاندارد قابل کاربرد نخواهد بود. در این صورت، ICC تنها به عنوان ابزاری برای ادعای هویت کاربر عمل خواهد کرد.

1- System-on-card

پ) آیا الزام اولیه‌ای برای تأئیدیه زیست‌سنجی استفاده شده است؟

۱) در صورت وجود یک الزام اولیه، مجموعه‌ای از تصمیم‌های بیشتر، ممکن است تا اکنون اتخاذ شده باشد؛ مانند تصمیم‌هایی همچون امکان استفاده از مقایسه زیست‌سنجی روی کارت، به اشتراک‌گذاری- کار یا سامانه های روی- کارت.

۱) چنانچه الزام اولیه‌ای وجود نداشته باشد، تصمیم در مورد شرایط را می‌توان، آن‌گونه که دیگر الزام ها برآورده شوند، اتخاذ کرد.

۲) زمانی که رویه انتخاب شد، قالب‌های داده‌ای هم کنش پذیری باید بررسی شوند (به بند ۵ مراجعه شود).

ت) الزامات هزینه اولیه چه مواردی هستند؟

۱) در صورت وجود الزام استفاده از ICCهایی کم‌هزینه، جایگزین‌هایی همچون مقایسه زیست‌سنجی روی -کارت، به اشتراک‌گذاری کار یا سامانه روی- کارت می‌تواند مورد توافق قرار گیرد.

۲) به علاوه، اگر ظرفیت ذخیره روی هزینه‌ی ICC اثرگذار باشد، تعداد ارجاعاتی که باید روی کارت ذخیره شود، یا شرایط بهتر استفاده را می‌توان محدود کرد و/ یا استفاده از قالب‌های داده‌ای فشرده، ممکن است به یک الزام اصلی تبدیل شود. (به بند ۵ مراجعه شود).

ث) نیازهای هم‌کنش پذیری با یکدیگر کدام موارد هستند؟

۱) در صورت عدم نیاز، طراح ممکن است، بدون تبعیت از هیچ استانداردی تصمیم به خلق راه‌حل خود بگیرد. بنابراین، ممکن است این استاندارد، قابل اجرا نباشد. این گزینه به عنوان نیازی برای ایجاد قابلیت همکاری که ممکن است در هر زمان در طول پروژه به وجود آید، یا هنگام کاربرد تدوین انجام شده برای پروژه جاری به پروژهای بعدی توصیه نمی شود.

۲) چنانچه قابلیت همکاری برای تبادل داده‌ها مورد نیاز باشد، به بند ۵ مراجعه شود. همان‌طور که مشاهده خواهد شد، ممکن است، برای دستیابی به قابلیت همکاری جهانی، استفاده از قالب‌های داده‌ای نمونه‌ی خام مستقل از الگوریتم به کار گرفته شده ممکن است، تنها راه عملی باشد.

۳) چنانچه قابلیت همکاری برای داشتن چندین تأمین‌کننده فناوری مورد نیاز باشد، آنگاه نه تنها قابلیت هم کنش پذیری داده‌ها، بلکه قابلیت هم کنش پذیری در سطح API و از سازوکارهای امنیتی نیز مورد نیاز است. (به بندهای ۶ و ۷ مراجعه شود).

۴) استفاده از محصولات بسیار پیچیده‌تر، مثل موارد مقایسه‌ای زیست‌سنجی روی- کارت یا سامانه روی- کارت برای دستیابی به قابلیت هم کنش پذیری نقش دارد، به مثابه اینکه فقط نیاز به تمرکز بر قابلیت هم کنش پذیری داده‌ها (و شاید سازوکارهای امنیتی) با دوری از تمام تفاوت‌های فن آوری حاصل از راه حل‌های فن آوری در سطح الگوریتم، وجود خواهد داشت.

ج) در بسیاری از نقاط دنیا، داده‌های زیست‌سنجی در بسیاری از نقاط دنیا به عنوان داده‌های شخصی در نظر گرفته می شوند و بنابراین برای حصول اطمینان از حریم شخصی شهروندان، از آنها محافظت می شود. بسته به محیط استقرار برنامه کاربردی، استفاده از سازوکارهای امنیتی، تبدیل به یک الزام عمده می‌شود. برای مشاهده کارهای قبلا انجام شده دراین زمینه، به بند ۶ مراجعه شود

چ) معمول‌ترین فرانامه برای طراحی و توسعه یک پروژه جدید شامل ICCها و زیست‌سنج‌ها، یکپارچه‌سازی پودمان های فناورانه از چندین تأمین‌کننده است. به علاوه، بسیاری از طراحان پروژه برای یکپارچه سازی به بیش از یک تأمین‌کننده برای هر پودمان فناورانه نیاز دارند. در این نوع فرانامه ها، بهتر است برای تسهیل یکپارچه سازی APIهای استاندارد شده به کار گرفته شوند. برای جزئیات بیشتربه بند ۷ مراجعه شود.

ح) برای برنامه‌های کاربردی معین، نیاز به پیگیری ویژگی های تعریف شده تاکنون، وجوددارد. (بند ۸، ویژگی های قابل دسترس در حال حاضر را توصیف خواهد کرد.)

خ) آخرین مورد که کم اهمیت‌ترین نیست، برای انتخاب پودمان های فناورانه یکپارچه شده یا تأمین نتایج نهایی برای کاربر نهایی درباره رفتار کل پروژه، روش شناسی ارزیابی مورد نیاز است. بند۹، استانداردهای مرتبط ارزیابی ارتباط با ICC، زیست‌سنج‌ها و امنیت را توصیف می‌کند

علاوه بر تمام این اطلاعات، بند ۹ راهنمایی برای پیاده‌سازی راه‌حل‌های مقایسه‌ای زیست‌سنجی روی-کارت، مبتنی بر استاندارد ISO/IEC 24787، [به مرجع ۱۶ کتاب نامه مراجعه شود] است.

۵ قالب‌های داده‌ای

استانداردهای مرتبط با ICC، محدودیت‌های جدی در مورد قالب داده‌هایی که بهتر است مبادله یا ذخیره شود، تامین نمی کند. مادامی‌که این داده‌ها در پروتکل ICC و ویژگی ها COS (یعنی پیروی از استانداردهای ISO/7816-4، [به مرجع ۲ کتاب نامه مراجعه شود] ISO/IEC7816-6، [به مرجع۳ کتاب نامه مراجعه شود] ISO/IEC7816-6، [به منبع ۴ کتاب نامه مراجعه شود] ISO/IEC7816-8، ISO/IEC7816-9، [به مرجع ۵ کتاب نامه مراجعه شود] و محدودیت‌های سازندگان نسبت به COS پیاده‌سازی شده درICC) پوشینه دار می‌شود، تنها استانداردهایی که مرتبط با زیست‌سنج‌ها می باشند، برای قالب‌های داده‌ای در نظر گرفته می شوند.

مجموعه استانداردهای ISO/IEC19794 [به مرجع ۱۱ کتاب نامه مراجعه شود] روش‌های هم کنش-پذیری برای کدگذاری داده‌های زیست‌سنجی، بسته به شرایط، را تامین می کند. این استاندارد چند قسمتی، چارچوبی قابل کاربرد برای تمام قسمت‌ها، مثل قالب‌های داده‌ای برای داده‌های خام نمونه (مثلاً تصاویر نمونه)، و برخی موارد برای داده‌های پردازش شده نمونه (مثلاً جزئیات اثرانگشت) تامین می کند. این خانواده از استانداردها در حال حاضر دارای دو نسل متفاوت تعریف شده هستند، که هر دوی آنها پذیرفته شده است. نسل نخست، استانداردهایی است که در سال‌های ۲۰۰۷- ۲۰۰۵ منتشر شد و درخواست شده، این نسل توسط دو سازمان ISO/IEC، برای حفظ انطباق با برخی استانداردهای برنامه‌های کاربردی جهانی مثل گذرنامه الکترونیکی (ePass porT)، در دسترس، باشد. امّا برای پروژه جدید، توصیه شده نسل دوم این استانداردها دنبال شود. این نسل تشکیل شده از استانداردهای منتشر شده در سال ۲۰۱۱ و سال‌های پس از آن، است.

نسل دوم استانداردISO/IEC19794، [به مرجع ۱۱ کتاب نامه مراجعه شود] یک استاندارد چند بخشی با ساختار زیر است:

- قسمت ۱ یک چارچوب کلی قابل کاربرد برای تمام قسمت‌ها را ارائه می کند. این قسمت ساختار عمومی برای سوابق زیست‌سنجی و عناصر مشترک چنین ساختاری را تعریف می‌کند. این قسمت هرکدام از سابقه اطلاعات زیست سنجی (BIR) شامل یک سرایند عمومی، معرفی کننده اطلاعات دنباله آن و یک یا چند نمایش(یعنی، نمونه های زیست سنجی) که در قالب یک سرایند نمایش و دادهای نمایش ساختاربندی شده را تعریف می کند. قسمت۱عناصر مشترک هر کدام از این سرآیند ها را تعریف می‌کند. این مورد برای کدگذاری دودویی و هم برای کدگذاری XML، تعریف شده است. علاوه بر آن، چارچوبی را نیز برای آزمون انطباق BIR هایی تعریف شده در این خانواده از استانداردها بیان می کند.
- قسمت ۲-n اطلاعاتی تکمیلی اضافه شده به سرایندهای مختلف و نیز روش کد گذاری دادهای نمایش شده، ارائه می دهد، این مورد برای تمام شرایط تعریف شده، انجام شده است. تا به امروز، سری مجموعه استانداردهای SO/IEC19794، [به مرجع ۱۱ کتاب نامه مراجعه شود] شرط های زیر را تعریف کرده است:
  - قسمت ۲: جزئیات اثر انگشت
  - قسمت ۴: تصویر اثر انگشت
  - قسمت ۵: تصویر صورت
  - قسمت ۶: تصویر عنبیه چشم
  - قسمت ۷:سری های زمانی امضاهای دست نوشته
  - قسمت ۸: دادهای اسکلتی اثر انگشت
  - قسمت ۹: تصویر عروق و رگ
  - قسمت ۱۱: داده‌های پردازش شده امضاهای دست‌نوشته[۱]
  - قسمت ۱۳: داده‌های صدا
  - قسمت ۱۴: داده‌های DNA

برای برخی از این شرط ها، بیش از یک قالب تعریف شده و شامل یک بازنمایش است که به عنوان قالب کارت هم شناخته می‌شود. چنین قالب کارتی برای کاهش فضای ذخیره سازی و نیازهای ارتباطی برای کاربردهایی معین مانند کارت‌های مقایسه زیست‌سنجی روی- کارت، در نظر گرفته شده است. تفکر اصلی پس زمینه‌آن قالب‌های‌کارتی،کاهش اندازه با حذف بسیاری‌از فیلدها در سرآیند اصلی یا سرآیند بازنمایش است. اگر انتقال یک رکورددادهٔ به یک IEC ، دارای شرایط محیطی برنامه کاربردی ثابت باشد و به بسیاری از آن فیلدها نیازی نباشد، این موضوع امکان‌پذیر است

علاوه بر سوابق و قالب‌های کارت، در نسل دوم استانداردهای ISO/IEC19794، [به مرجع۱۱ کتاب نامه مراجعه شود] یک مجموعه جدید از اصلاحات تعریف شده برای ایجاد امکان کدگذاری XML اطلاعات، نیز وجود دارند. در حال‌حاضر، بیشتر قسمت‌ها کدگذاری XML را تعریف می‌کنند وحتی‌دو قسمت دیگر وجود

[۱]

دارد (یعنی استاندارد ISO/IEC19794-13 و ISO/IEC19794-14) که از ابتدا به صورت XML مشخص شده اند.

علاوه بر قالب‌های داده‌ای که دراستاندارد ISO/IEC19794، [به مرجع ۱۱ کتاب نامه مراجعه شود] تعریف شده که برای شمول اطلاعات از یک کاربر واحد و یک شرط واحد تعریف شده اند، استاندارد ISO/IEC JTC1 SC37 نیز یک فراساختار به نام CBEFF (یعنی مجموعه استانداردهای سری ISO/IEC 19785، [به مرجع ۹ کتاب نامه مراجعه شود] را امکانات زیر، تعریف کرده است:

- کدگذاری اطلاعات زیست‌سنجی از بیش از یک کاربر واحد؛
- کدگذاری اطلاعات زیست‌سنجی از بیش از یک شرط واحد؛ و
- حفاظت از داده‌های زیست‌سنجی با استفاده از سازوکارهای امنیتی که ممکن است داده‌های موجود در سوابق را رمزگذاری و احراز هویت کند.

یک رکورد CBEFF شامل موارد زیر است:

- سرآیندی که اطلاعات تلفیق شده در رکورد را معرفی می‌کند؛
- داده‌های زیست‌سنجی که می‌تواند آن‌گونه که در ISO/IEC1979 ، تعریف شده، یک BIR باشد؛ و
- یک بستک امنیتی اختیاری (SB) که داده‌های مورد نیاز برای حفاظت از اطلاعات زیست‌سنجی را تلفیق می‌کند.

هم چنینCBEFF، امکان وجود یک رویکرد سلسه مراتبی را فراهم می‌آورد که قادر است رکوردهای CBEFF ساده‌ی چندگانه را، که به عنوان یک رکورد CBEFF پیچیده نامیده می شود، شامل شود.

شیوه‌ای را که بتوان در آن رکوردهای CBEFF، کدگذاری کرد، می‌تواند از یک ساختار به یک ساختار دیگر متغیر باشد. این موضوع بدین دلیل است که استاندارد ISO/IEC19785-3، چندین روش برای کدگذاری رکوردهای CBEFF، تعریف می‌کند، که با قالب‌های پشتیبان[1] نامیده می شود، این قالب‌های پشتیبان برای کدگذاری دودویی با طول‌های کلمات در سامانه متفاوت، کدگذاری XML یا ASN طراحی شده است. یکی از کدگذاری‌های دودویی به گونه‌ای تعریف شده که بهترین گزینه مناسب برای ICCها باشد، به ویژه زمانی‌که از رویکردهای مقایسه‌ای زیست‌سنجی روی- کارت استفاده می‌شود.

استاندارد ISO/IEC7816-11 [به مرجع ۶ کتاب نامه مراجعه شود] چگونگی استفاده از اطلاعات زیست‌سنجی را درICCها، از طریق تعریف یک «قاب الگو اطلاعات زیست‌سنجی» (به بند ۵ و پیوست C را در ISO/IEC 7816-11 مراجعه شود) تعریف می‌کند. کدگذاری درون قاب در بند ۱۱ استاندارد ISO/IEC 19785-3، تعریف شده است.

۶ سازوکارهای امنیتی

داده‌های زیست‌سنجی در بسیاری از فرانامه ها، به عنوان داده‌های شخصی در نظر گرفته شده، و حفاظت از این داده‌ها لازم است. همان‌گونه که قبلاً ذکر شد، CBEFF (یعنی در استاندارد ISO/IEC 19785) [به مرجع ۹ کتاب نامه مراجعه شود]یک بستک امنیتی (SB) را برای نگهداری اطلاعات به منظور حفاظت از

1- Patron

داده‌های زیست‌سنجی تعریف می‌کند (به عنوان مثال، پیام‌های رمزی که تأمین‌کننده سازوکارهای یکپارچگی و احراز هویت است). اما به برای رسیدن به هم کنش پذیری، استانداردها واسناد ملی مطابق با استاندارد در ISO/IEC JTC1/SC27، را در نظر می گیرد. امنیت و حریم شخصی در تمام زمینه‌های فناوری اطلاعات در دامنه کاربرد کمیته فرعیSC27 می باشد، امّا کارهای عمده انجام شده مرتبط با زیست‌سنج‌ها عبارت است از:

- در خصوص فرانامه های طراحی برنامه‌های کاربردی و امنیتی و حریم شخصی، کارهای زیر آغاز شده، که در ادامه در بند ۸ به آنها ارجاع داده شده است:
  - استاندارد ISO/IEC 29100، [به مرجع ۱۷ کتاب نامه مراجعه شود] در مورد چارچوب حریم خصوصی
  - استانداردISO/IEC 29101، [به مرجع ۱۸ کتاب نامه مراجعه شود] در مورد ساختار مرجع حریم خصوصی
  - استاندارد ISO/IEC 29146، [به مرجع ۲۰ کتاب نامه مراجعه شود] در چارچوبی برای مدیریت دسترسی
  - استاندارد ISO/IEC 24760 در مورد چارچوبی برای مدیریت هویت
  - استاندارد ISO/IEC 29115، [به مرجع ۱۹ کتاب نامه مراجعه شود] در چارچوب اطمینان از احراز هویت هستار[1]
  - استانداردISO/IEC29191، [به مرجع ۲۴ کتاب نامه مراجعه شود] در مورد الزامات ناشناسی نسبی با وثیقه هویتی [2]
  - استاندارد ISO/IEC 29190، [به مرجع۲۳ کتاب نامه مراجعه شود] در مورد مدل بلوغ قابلیت حریم خصوصی
- استاندارد ISO/IEC19792، [به مرجع استاندارد ۱۰ کتاب نامه مراجعه شود] در ارزیابی امنیت زیست‌سنج‌ها، که در بند ۹ به آن ارجاع داده شده است.
- استاندارد ISO/IEC 2476، [به مرجع ۱۵ کتاب نامه مراجعه شود] در شرایط دسترسی به زیست‌سنج-ها[3]. این استاندارد روش استفاده از سازوکارهای امنیتی را مشخص می کند، و چگونگی کدگذاری اطلاعات به SB، مشخص می شود
- استاندارد ISO/IEC 24745، [به مرجع ۱۳ کتاب نامه مراجعه شود] در مورد حفاظت اطلاعات زیست‌سنجی است، که روش استفاده برای دستیابی به مراجع زیست‌سنجی لغو پذیر را مشخص می کند، یعنی آنچه که در صنعت به عنوان «حفاظت الگو زیست‌سنجی» از آن یاد می‌شود.

1- Assurance Framework
2- Identity Escrow
3- Access Conditions for Biometrics

علاوه بر این کارها، در کمیته های فرعی استانداردهای SC37 دو پروژه مرتبط با امنیت در زیست‌سنج‌ها وجود دارد. اولین پروژه در استاندارد ISO/IECTR 29156 [به مرجع ۲۱ کتاب نامه مراجعه شود] هست، که در مورد الزامات دستیابی به امنیت و قابلیت استفاده در زیست‌سنج‌ها است. دومین پروژه ISO/IEC30107 در استاندارد [به مرجع ۲۶ کتاب نامه مراجعه شود] 30107 است که در مورد «نمایش سازوکارهای کشف حمله» است. این پروژه‌ها، یک مکمل عالی برای کارهای صورت گرفته درکمیته فرعی SC27، است.
با کاهش به سطح ICC،کمیته فرعیSC17، سازوکارهای امنیتی مورد استفاده درICCها، همچون پیام‌رسانی امن و یا شیوه مدیریت که کلیدهای مخفی توسط COS، تعریف می‌شود. استاندارد [به مرجع۲کتاب نامه مراجعه شود4-ISO/IEC 7816] و [به مرجع ۵ کتاب نامه مراجعه شود] 8-ISO/IEC 7816، این‌گونه ویژگی ها را تعریف می‌کند. درخصوص مقایسه زیست‌سنجی روی- کارت، استاندارد ISO/IE 24787، [به مرجع ۱۶ کتاب نامه مراجعه شود] برخی الزامات امنیتی را برای این فناوری تعریف می‌کند.
روش‌هایی که در این بند به شکل کلی بیان شد، با روش‌های گوناگون می تواند پیاده‌سازی شود. تعریف پیاده‌سازی آنها، خارج از هدف و دامنه کاربرد این‌استاندارد است. بهتر است، اینگونه پیاده سازی ها در رخ نمون های خاص مرتبط با کاربرد نهایی هدف، تعریف شود.
تدوین کننده یک برنامه کاربردی مرتبط با مقایسه زیست‌سنجی روی- کارت، ممکن است، علاقه‌مند به در نظر گرفتن دیگر استانداردهای مربوط به امنیت، مطابق با استانداردهای ISO/IEC JTC1/SC 27 باشد.

۷ تدوین برنامه کاربردی

تدوین برنامه کاربردی شامل ICCsها و زیست‌سنج‌ها، به طور معمول نیاز به یکپارچه‌سازی چندین پودمان دارد. برای تسهیل در یکپارچه‌سازی، استفاده از واسط‌های برنامه کاربردی (API) استاندارد، توصیه می شود. برنامه‌ها وپودمان های کاربردی زیست‌سنجی، با استفاده ازBioAPI تدوین شده، مطابق استاندارد چند قسمتیISO/IEC 19784، [به مرجع ۸ کتاب نامه مراجعه شود] مشخص شده، است و مطابق با تعریف اصلی API دراستاندارد 1-ISO/IEC 19784، ممکن است. واسط BioAPI در تعریف اولیه آن، مبتنی بر چارچوبی است‌که پودمان های مختلفی را به یکدیگر مرتبط می کند که به عنوان تامین‌کنندگان خدمات زیست‌سنجی (BSPs) ها تدوین شده اند و ممکن است، شامل واحدها (الگوریتم ها، حسگر یا واحد بایگانی) و/یا تامین کنندگان کارکردهای زیست سنجی باشد (BFP) ها که واحدها را گروه بندی می کنند. در استاندارد1-ISO/IEC 19784، همچنین امکان پیاده‌سازی یک نسخه رایگان چارچوب BioAPI نیز وجود دارد، که استقرار آن را در افزاره‌هایی با سامانه عامل را با قابلیت‌های محدود پردازش، ممکن می‌سازد.
واسط BioAPI با زبان برنامه‌نویسی C مشخص شده که باعث فقدان یک رویکرد شی‌گرایی به پیاده‌سازی آن می باشد. برای غلبه بر این ناسازگاری، استاندارد[به مرجع ۲۵ کتاب نامه مراجعه شود] ISO/IE 30106 ، ویژگی از یک BipAPI شی‌گرا، ارائه می‌دهد. که از یک چارچوب عمومی با توصیف UML (ISO/IEC30160-1)، یک مرجع پیاده‌سازی زبان جاوا (ISO/IEC 30106-2) و یک مرجع پیاده‌سازی زبان C# (ISO/IEC 30106-3) تشکیل شده است.

در یک محصول دارای ساختار BioAPI، یک مقایسه زیست‌سنجی روی- کارت ICC، خدمت زیست‌سنجی دیگری درقالب یک BSPبه سامانه ارائه خواهد شد. در این حالت، BSP دو قابلیت کارکردی عمده ذخیره سازی و مقایسه ارائه می‌کند هر چند از قابلیت کارکردی ذخیره‌سازی، فقط ذخیره اطلاعات مجاز خواهد بود و خواندن اطلاعات مجاز نمی باشد. در آن دسته از موارد که از یک ICC مقایسه زیست‌سنجی بیرون از کارت استفاده می‌شود، ICC با استفاده از یک BSP دیگر تأمین خواهد شد، امّا در چنین موردی، BSP تنها ارائه‌کننده پشتیبانی برای قابلیت‌های ذخیره‌سازی (خواندن) خواهد بود.

اگر پیاده سازی که برنامه کاربردی مورد نظر با استفاده از یک معماری خدمت گرا SOA[1]مورد انتظار است، بهتر است ISO/IEC 30108، [به مرجع ۲۷ کتاب نامه مراجعه شود] باشد، زیرا خدمات تضمین هویت زیست سنجی BIAS [2]را تعریف می‌کند.
در زمان تدوین برنامه کاربردی مورد نظر با هزینه کم، افزاره های هایی با عملکرد پایین، مانند سامانه‌های تلفیق شده پیاده‌سازی شود، نسخه ساده‌تری از BioAPI درمطابق با استاندارد [به مرجع ۲۲ کتاب نامه مراجعه شود] ISO/IEC 29164، تعریف شده،که BioAPI تلفیق شده نام دارد.

۸ رخ نماهای کاربردی

بهتر است، استانداردها و متعدد انتشار یافته برای طراح و/یا تدوین کننده به هنگام تعریف برنامه‌های کاربردی معین، مرجع باشد. یکی از آن موارد استانداردهای تدوین شده در دامنه کاربرد استاندارد WG6 ISO/IEC JTC1/ SC3 است، که مسئول تدوین ویژگی ها برای آن دسته از پی آمدهای اجتماعی و قضایی پیرامون استفاده از زیست‌سنج‌ها است، مورد دیگر ممکن است، کارهای انجام شده توسط کمیته فنی کار گروه CEN TC224 WG6، باشد، که به تعریف واسط کاربر در برنامه‌های کاربردی ID در اروپا اختصاص داده شده است.

به طور مشخص، با در نظر گرفتن فناوری مقایسه زیست‌سنجی روی- کارت، برخی ویژگی‌های چند ملیتی، ملی و یا حتی محدودشده- بخشی وجود دارد که به این فناوری ارجاع داده می‌شود. نمونه‌هایی از این نوع مشخصه‌ها عبارت است از:

- کارت شهروندی اروپایی (CEN/TS 15480) که توسط کمیته فنی CEN TC224، تدوین شده، الزامات مربوط به یک کارت شهروندی را مشخص می کند که نه تنها شامل تصدیق هویت فیزیکی بلکه هویت الکترونیکی شهروند را نیز شامل می‌شود. در ویژگی های خود، امکان پیاده‌سازی کارت شهروندی را با استفاده از محصولات مقایسه زیست‌سنجی روی- کارت را فراهم می‌آورد. این ویژگی ها توسط چندین کشور اروپایی برای صدور کارت‌های شناسایی (ID) ملی آنها هم اکنون دنبال شده، و برخی از آنها (از جمله اسپانیا) مقایسه زیست‌سنجی روی- کارت را در نظر گرفته اند.

1-Service Oriented Architecture
2-Biometric Identity Assurance Services

۹ ارزیابی فناوری

علاوه بر تمام اسنادی که در بندهای بالا قبلا ذکر شده، اطلاع از تدوین استانداردها و گزارش‌ها برای آزمون فناوری شامل ICCها و زیست‌سنج‌ها، اهمیت شایانی دارد. شروع با روش‌های آزمون مبتنی بر ICCها، خانواده استانداردهای [به مرجع ۷ کتاب نامه مراجعه شود] ISO/IEC 10373، روش‌های آزمون برای تمام ویژگی های فناورانه کارت‌های شناسایی، شامل کارت‌های ICC، تماسی و غیر تماسی، تعریف می شود.

کمیته فرعی استاندارد ISO/IEC JTC1/SC37، دارای یک گروه کاری کامل برای تدوین استانداردها و گزارش‌های مرتبط با ارزش یابی زیست‌سنج‌ها در کارگروه (WG5) است، و در میان تمام پروژه‌های مختلف انجام شده در چنین گروه کاری، استاندارد چند قسمتی ISO/IEC 19795، دارای اهمیت عمده‌ای است و اصول ارزیابی زیست‌سنج‌ها و نیز برخی کاربردهای خاص این اصول را برای فرانامه های معین، تعریف می-کند. یکی از این فرانامه ها، مقایسه زیست‌سنجی روی- کارت است. در استاندارد [به مرجع ۱۲ کتاب نامه مراجعه شود] ISO/IEC 19795-7 روش شناسی برای ارزیابی چگونگی متفاوت عمل کردن یک راه‌حل زیست‌سنجی هنگام پیاده سازی درون کارت ویا هنگام پیاده سازی روی یک رایانه متداول است. این استاندارد نتیجه ارزیابی MINEX-II است، که NIST آن را برای ارزیابی سطح عملکرد مقایسه زیست‌سنجی روی- کارت، با اندیشه تصمیم‌گیری در مورد مناسب بودن این‌گونه فناوری برای پیاده‌سازی در یک سامانه کارت هویت، یا نامناسب بودن، آغاز کرد. تاکید بر این نکته دارای اهمیت است که استاندارد ISO/IEC19795-7، عملکرد الگوریتم را ارزیابی نمی‌کند. استاندارد ISO/IEC 19795-7 در جستجوی انطباق درستی الگوریتم اجرا شده درون ICC به اندازه درستی الگوریتم اجرا شده در رایانه است. علاوه بر این‌گونه ارزیابی، می تواند یک ارزیابی فناوری در مورد نسخه الگوریتم بر روی یک رایانه شخصی، اجرا شود (با مطالق با استاندارد ISO/IEC 19795-1 و ISO/IEC 19795-2). توجه به این نکته نیز دارای اهمیت است که برای تسهیل فرآیند ارزیابی‌کارت‌ها بهتر است، اطلاعاتی در مورد نتیجه مقایسه اطلاعاتی، که به طور معمول در محصولات تجاری در دسترس نیست، برای پرهیز از حملات خزنده[1]، فراهم شود.

برای ارزیابی سطح امنیتی به دست آمده با استفاده از راه حل تدوین شده، معیارهای عمومی، مرجع اصلی است. کارهای انجام شده در معیارهای عمومی به طور متناوب مطابق با استاندارد ISO/IEC 15408 استاندارد سازی شده است. برای پرداختن به زیست‌سنج‌ها کمیته فرعی استاندارد، ISO/IEC JTC1/SC27، [به مرجع ۱۰ کتاب نامه مراجعه شود] ISO/IEC 19792، را تدوین کرده است، این استاندارد روش شناسی برای ارزیابی امنیت در سامانه‌های زیست‌سنجی را تعیین می‌کند. در درگاه معیارهای عمومی (http://www.commoncriteriaPortal.org) برخی رخ‌نماهای حفاظتی (PPs)[2]ها و اهداف امنیتی (STs)[3] ها وجود دارد که برای محصولات مقایسه ای زیست‌سنجی بر روی- کارت قابل کاربرد است، و در آینده برخی PPsها و/یا STsها ممکن است نسبت به این فناوری، خاص به نظر برسند.

1- Hill Climbing Attacks
2- Protection Profiles
3- Security Targets

۱۰ پیاده‌سازی راه‌حل‌های مقایسه زیست‌سنجی روی کارت

۱۰-۱ کارت شناسایی ملی اسپانیایی (DNIe)

۱۰-۱-۱ مقدمه

اسپانیا قدمتی طولانی در استفاده از کارت‌های شناسایی ملی دارد، این قدمت به نیمه نخست قرن بیستم برمی‌گردد. این کارت (که به عنوان DNI شناخته می شود) یک سند کاغذی دارای پوشش فیلم با سازوکار-های امنیتی فیزیکی بود. ممکن بود این کارت در هر زمان برای فراهم کردن هویت فرد دارنده کارت استفاده شود و حتی به عنوان اسناد سفر در منطقه شینگن[۱] هم پذیرفته شده است.

بر این اساس، دولت اسپانیا برتصمیم گرفت با افزودن قابلیت‌های ID الکترونیکی، از طریق ترکیب جفت کلیدهای مبتنی بر PKI، به این سند کارت را ارتقاء دهد. بنابراین تصمیم به تغییر فناوری به یک سند مبتنی بر ICC با حفاظت فیزیکی و الکترونیکی گرفته شد تا امکان شناسایی هویت چهره صاحب کارت و سازوکارهای احراز هویت الکترونیکی و امضاء برای شناسایی هویت ازراه دور را نیز فراهم شود.

هنگام تعریف نسل جدید کارت ID ملی اسپانیایی (که تحت عنوان DNIe برای نسخه الکترونیک DNI سنتی نیز شناخته می‌شود) تصمیم گرفته شد تا قابلیت‌های مقایسه زیست‌سنجی روی کارت به کارت اضافه شود.

در زیر بندهای زیر، جزئیات چنین پیاده‌سازی آمده است:

۱۰-۱-۲ خدمات زیست‌سنجی ارائه شده

مقایسه زیست‌سنجی بر روی- کارت، دسترسی امن به منابع مشخص تعبیه شده در ICC مربوط به DNIe را تکمیل می‌کند. این منابع عبارت است از:

- کلیدهای امضاء الکترونیک
- کلیدهای احراز هویت
- گواهی امضاء الکترونیک
- گواهی احراز هویت
- گواهی‌هایی برای مراجع میانی گواهی دهند CA[۲]
- داده‌های نسبی دارنده کارت
- تصویری از امضاء دست‌نوشته دارنده کارت
- تصویر چهره دارنده کارت.

به دلیل دستیابی به شرایط تعریف شده، در حال حاضر سازوکار مقایسه زیست‌سنجی روی- کارت فقط برای شهروندان در ایستگاه‌های پلیس در دسترس است تا بتوانند اقدامات زیر را انجام دهند:

- تصدیق هویت
- باز کردن کد PIN
- تغییر کد PIN

4- Schengen

1- Certification Authority

۱۰-۱-۳ شرایط زیست سنجی و قالب های داده‌ای

شرط زیست‌سنجی منتخب برای DNIe، اثر انگشت است. کارت DNIe قادر به تصدیق هویت از طریق استفاده از هر کدام از دو انگشت سبابه شخص دارنده‌ی کارت است. بنابراین ویژگی‌های زیر برای سامانه جایگذاری شده است:

- در حین ثبت نام، اثر انگشت‌های غلطان هر دو انگشت سبابه اخذ شده، و پذیرش آنها پس از گذر موفقیت‌آمیز از حد آستانه‌ی کیفیت، صورت می‌گیرد.

- در مرحله تصدیق، دارنده کارت، کارت را وارد کرده و در این هنگام برنامه از وی می خواهد، که بلافاصله انگشت اشاره مورد نظر را روی حسگر اثر انگشت بگذارد. جزئیات اثر انگشت استخراج شده و بر اساس قالب کارت مطابق استاندارد ISO/IEC19794-2: 2011 رمزگذاری شده، و به روشی امن به ICC ارسال می‌شود. پس از آن ICC، جزئیات مربوط را با جزئیات ذخیره شده در ICC مقایسه کرده و تصمیم گرفته می‌شود. اگر مقایسه موفقیت‌آمیز باشد، یک بازخورد تأیید به صورت OK ارائه خواهد شد. و در غیر اینصورت، یک بازخورد عدم تأیید به صورت NO-OK خواهد بود. برای دوری از حملات خزنده، اطلاعات بیشتری از مقایسه، ارائه نمی‌شود.

۱۰-۱-۴ سازوکارها و عملیات امنیتی

برای استفاده از سازوکار تصدیق هویت زیست‌سنجی، شرایط دسترسی برمبنای تاسیس از پیش یک مجرای سازمانی امن[1] است. دلیل این موضوع، این واقعیت است که نهادهای گواهی کننده در حال حاضر، زیست‌سنج‌های اثرانگشت را به عنوان یک سازوکار احراز هویت قوی، نمی‌پذیرند. استفاده از سازوکارهای امنیتی قوی، برای دستیابی به گواهینامه EAL4 + تحت شرایط معیارهای عمومی، یک الزام است. در همان زمان، برای DNIe نیز یک الزام وجود دارد، زیرا بهتر است، یک افزاره ایجاد امضاء امن، تحت قانون، در نظر گرفته شود.

بنابراین راه‌حل، حفاظت از کاربرد سازوکار مقایسه‌ای زیست‌سنجی روی- کارت، با استفاده قبلی از تصدیق کلید(های) دیگری بود تا الگوریتم اعتبارسنجی بتواند قوی در نظر گرفته شود.

عملیات متعددی درکارت، در تصدیق زیست‌سنجی دخالت دارد:

- تجدید کلیدهای RSA: زیست‌سنجی + PIN + مجرای اجرایی امن
- تجدید گواهی‌ها: زیست‌سنج‌ها + PIN + مجرای اجرایی امن
- بازکردن رمز PIN: سازوکار کلید بازکننده PIN (PUK) وجود ندارد، بلکه رمزگشایی با ترکیبی از موارد زیر صورت می‌گیرد:
  - زیست‌سنج‌ها
  - مجرای اجرایی امن و
  - یک کلید متنوع اجرایی کاربردی که از واپایش کل فرآیند در یک محیط کنترل شده و امن

1- Secure Administrative Channel

که توسط پلیس تعریف شده، اطمینان حاصل کند.

- تغییر کد PIN: اگر PIN مسدود نشده باشد، می‌تواند با یکی از ترکیب‌های شروط دستیابی تغییر کند:
  - کد PIN موجود + مجرای اجرایی امن، یا
  - زیست‌سنج‌ها + مجرای اجرایی امن + کلید متنوع اجرایی کاربردی

مقایسه زیست‌سنجی روی- کارت با استفاده از دستور VERIFY، مطابق با استاندارد در-ISO/IEC7816 11، [به مرجع ۶ در کتاب نامه مراجعه شود] و با استفاده از قالب کارت استاندارد2011 :ISO/IEC19794-2 انجام می‌شود.

۱۰-۱-۵ ارزشیابی‌ها و نتایج

کارت DNIe اسپانیا گواهینامه معیارهای عمومی + EAL4 را دریافت کرده است.

پیوست

(اطلاعاتی)

کتابنامه

[1] Li S.Z. *Encyclopedia of Biometrics*, Springer, 2009

[2] ISO/IEC 7816-4, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

[3] ISO/IEC 7816-6, *Identification cards — Integrated circuit cards — Part 6: Inter industry data elements for interchange*

[4] ISO/IEC 7816-8, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

[5] ISO/IEC 7816-9, *Identification cards — Integrated circuit cards — Part 9: Commands for card management*

[6] ISO/IEC 7816-11, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

[7] ISO/IEC 10373 (all parts), *Identification cards — Test methods*

[8] ISO/IEC 19784 (all parts), *Information technology — Biometric application programming interface*

[9] ISO/IEC 19785 (all parts), *Information technology — Common Biometric Exchange Formats Framework*

[10] ISO/IEC 19792, *Information technology — Security techniques — Security evaluation of biometrics*

[11] ISO/IEC 19794 (all parts), *Information technology — Biometric data interchange formats*

[12] ISO/IEC 19795-7, *Information technology — Biometric performance testing and reporting — Part 7: Testing of on-card biometric comparison algorithms*

[13] ISO/IEC 24745, *Information technology — Security techniques — Biometric information protection*

[14] ISO/IEC 24760-1, *Information technology — Security techniques — a framework for identity management — Part 1: Terminology and concepts*

[15] ISO/IEC 24761, *Information technology — Security techniques — Authentication context for biometrics*

[16] ISO/IEC 24787, *Information technology — Identification cards — On-card biometric comparison*

[17] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[18] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[19] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[20] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*[1]

[21] ISO/IEC TR 29156, *Guidance for specifying performance requirements to meet security & usability needs in applications using biometrics*[2]

[22] ISO/IEC 29164, Information technology — Biometrics — Embedded BioAPI

[23] ISO/IEC 29190, Proposal on Privacy capability assessment model[3]

[24] ISO/IEC 29191, *Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication*

[25] ISO/IEC 30106 (all parts), *BioAPI for object oriented programming languages*[4]

[26] ISO/IEC 30107, *Anti-Spoofing and Liveness Detection Techniques*[5]

[27] ISO/IEC 30108 (all parts), *Information technology — Biometric identity assurance service (BIAS)*[6]

۱ در دست آماده‌سازی

۲ در دست آماده‌سازی

۳ در دست آماده‌سازی

۴ در دست آماده‌سازی

۵ در دست آماده‌سازی

۶ در دست آماده‌سازی