INSO

8232-11

1st. Edition

2015

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران

۸۲۳۲-۱۱

چاپ اول

۱۳۹۳

کارت‌های شناسایی --
کارت‌های مدار مجتمع —
قسمت ۱۱: درستی‌سنجی افراد از طریق روش‌های زیست‌سنجی (بیومتریک)

Identification cards —
Integrated circuit cards —
Part 11: Personal verification through biometric methods

ICS: 35.240.15

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی 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 وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی 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 می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (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 of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«کارت‌های شناسایی- کارت‌های مدار مجتمع- قسمت ۱۱: درستی‌سنجی افراد از طریق روش‌های زیست‌سنجی (بیومتریک)»

رئیس:	**سمت و/یا نمایندگی**
یزدیان ورجانی، علی (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس و مسئول مرکز آپا دانشگاه تربیت مدرس
دبیر:	
قسمتی، سیمین (لیسانس برق الکترونیک، فوق لیسانس مهندسی فناوری اطلاعات)	مشاور مرکز آپا دانشگاه تربیت مدرس
اعضا: (اسامی به ترتیب حروف الفبا)	
اسدی پویا، سمیرا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیر عامل شرکت مهندسی پویا دانش و کیفیت آوا
شیخ‌الاسلامی، محمد کاظم (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس
صادقی، مریم (لیسانس مهندسی کامپیوتر)	کارشناس نظام صنفی رایانه‌ای
عبداله پور، امید (لیسانس مهندسی کامپیوتر)	کارشناس پژوهشگاه استاندارد سازمان ملی استاندارد ایران
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس حقیقی تدوین استاندارد سازمان ملی استاندارد ایران
قندهاری، آزاده (فوق لیسانس هوش مصنوعی)	عضو هیات علمی دانشگاه آزاد اسلام واحد ساوه و کارشناس مرکز تحقیقات مخابرات ایران
محمدیان، مصطفی (دکتری، برق)	عضو هیات علمی و معاون پژوهشی دانشکده برق و کامپیوتر دانشگاه تربیت مدرس

معروف، سینا
(لیسانس مهندسی کامپیوتر، سخت‌افزار)
کارشناس سازمان فناوری اطلاعات ایران و کارشناس حقیقی تدوین استاندارد سازمان ملی استاندارد ایران

فهرست مندرجات

عنوان **صفحه**

آشنایی با سازمان ملی استاندارد ایران **Error! Bookmark not defined.**
کمیسیون فنی تدوین استاندارد ج
پیش‌گفتار ح
۱ هدف و دامنه کاربرد ۱
۱-۱ کلیات ۱
۲ مراجع الزامی ۱
۳ اصطلاحات و تعاریف ۱
۴ اصطلاحات کوته‌نوشت ۲
۵ دستورها برای فرآیندهای درستی‌سنجی زیست‌سنجی ۳
۵-۱ دستورها برای بازیابی اطلاعات زیست‌سنجی ۴
۵-۲ دستور برای فرآیند درستی‌سنجی زیست‌سنجی ایستا ۴
۵-۳ دستورها برای فرآیند درستی‌سنجی زیست‌سنجی پویا ۴
۶ عناصر داده ۴
۶-۱ اطلاعات زیست‌سنجی ۴
۶-۲ داده‌های زیست‌سنجی ۶
۶-۳ اطلاعات الزامات درستی‌سنجی ۷
پیوست الف (اطلاعاتی) فرآیند درستی‌سنجی زیست‌سنجی ۱۰
پیوست ب (اطلاعاتی) مثال‌های ثبت‌نام و درستی‌سنجی ۱۶
پیوست پ (اطلاعاتی) اشیاء داده اطلاعات زیست‌سنجی ۲۳
پیوست ت (اطلاعاتی) استفاده از الگوهای پیام دادن امن ۳۵
کتاب‌نامه ۴۰

پیش‌گفتار

استاندارد «کارت‌های شناسایی- کارت‌های مدار مجتمع- قسمت ۱۱: درستی‌سنجی افراد از طریق روش‌های زیست‌سنجی (بیومتریک)» که پیش‌نویس آن در کمیسیون‌های مربوط توسط مرکز آپا (آگاهی‌رسانی، امداد و پشتیبانی رخدادهای رایانه‌ای) دانشگاه تربیت مدرس تهیه و تدوین شده است و در سیصد و پنجاه و ششمین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۹۳/۱۰/۲۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه 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 زمینه 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 تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 7816-11:2004, Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods

کارت‌های شناسایی- کارت‌های مدار مجتمع - قسمت ۱۱: درستی‌سنجی افراد از طریق روش‌های زیست‌سنجی (بیومتریک)

۱ هدف و دامنه کاربرد

۱-۱ کلیات

هدف از تدوین این استاندارد، تعیین دستورات امنیتی بین صنعت‌ها است تا برای درستی‌سنجی افراد توسط روش‌های زیست‌سنجی در کارت‌های مدار(های) مجتمع استفاده شود. همچنین این استاندارد، ساختار داده و روش‌های دسترسی به داده را تعریف می‌کند تا از کارت به عنوان حامل داده‌های مرجع زیست‌سنجی و/ یا به عنوان افزاره‌ای برای درستی‌سنجی (تطبیق درکارت)[1] زیست‌سنجی شخصی استفاده شود. شناسایی اشخاص با استفاده از روش‌های زیست‌سنجی، خارج از دامنه کاربرد این استاندارد است.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

در صورتی که به آگاهی با ذکر تاریخ انتشار آن ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نمی‌باشد و در غیر این صورت همواره تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 7816-4:2003, Identification cards — Integrated circuit cards with contacts — Part 4: Organization, security and commands for interchange

2-2 ISO/IEC CD 19785:2003, Information technology — Common Biometric Exchange Framework Format (CBEFF)

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می‌رود:

۳-۱

داده‌های زیست‌سنجی

داده‌هایی که یک ویژگی یا ویژگی‌های مورد استفاده در درستی‌سنجی زیست‌سنجی را کدگذاری می‌کند.

1 - on-card matching

۲-۳

اطلاعات زیست‌سنجی

اطلاعات مورد نیاز دنیای بیرون برای ساخت داده‌های درستی‌سنجی است.

۳-۳

داده‌های مرجع زیست‌سنجی

داده‌های ذخیره‌شده در کارت به منظور مقایسه با داده‌های درستی‌سنجی زیست‌سنجی است.

۴-۳

درستی‌سنجی زیست‌سنجی

فرآیند درستی‌سنجی توسط مقایسه یک به یک داده‌های درستی‌سنجی زیست‌سنجی در برابر داده‌های مرجع زیست‌سنجی است.

۵-۳

داده‌های درستی‌سنجی زیست‌سنجی

داده‌های به دست آمده در طول فرآیند درستی‌سنجی برای مقایسه با داده‌های مرجع زیست‌سنجی است.

۶-۳

الگو

مشابه آنچه در استاندارد ISO/IEC 7816-4 تعریف شده است.

هشدار - اصطلاح «الگو[1]» به معنای فیلد حاوی مقدار شی داده ساختاریافته[2] است. این واژه نباید با نمونه داده زیست‌سنجی پردازش‌شده اشتباه گرفته شود.

۴ اصطلاحات کوته‌نوشت

در این استاندارد کوته‌نوشت‌های زیر به کار می‌رود:

AID	Application Identifier
AT	Authentication Template
BER	Basic Encoding Rules
BIT	Biometric Information Template
BD	Biometric Data
BDP	BD in proprietary format
BDS	BD in standardized format
BDT	Biometric Data Template

شناسانه کاربرد
الگوی اصالت‌سنجی
قواعد کدگذاری عمومی
الگوی اطلاعات زیست‌سنجی
داده زیست‌سنجی
داده زیست‌سنجی در قالب اختصاصی
داده زیست‌سنجی در قالب استاندارد
الگوی داده زیست‌سنجی

1 - Template
2 - Constructed data object

CCT	Cryptographic Checksum Template	الگوی جمع‌آزمای رمزنگاشتی
CRT	Control Reference Template	الگوی مرجع کنترل
CT	Confidentiality Template	الگوی محرمانگی
DE	Data Element	عنصر داده
DF	Dedicated File	پرونده اختصاصی
DO	Data Object	شی داده
DST	Digital Signature Template	الگوی امضای دیجیتال (رقمی)
EFIDID	Elementary File ID	شناسانه پرونده ابتدایی
FCI	File Control Information	اطلاعات کنترلی پرونده
ID	Identifier	شناسانه
L	Length	طول
OID	Object Identifier	شناسانه شی
RD	Reference Data	داده مرجع
SE	Security Environment	محیط امنیتی
SM	Secure Messaging	پیام دادن امن
TLV	Tag-Length-Value	برچسب - طول- مقدار
UQ	Usage Qualifier	توصیف‌کننده کاربرد
VIDO	Verification requirement Information Data Object	شی داده اطلاعات الزامات درستی‌سنجی
VIT	Verification requirement Information Template	الگوی اطلاعات الزامات درستی‌سنجی

۵ دستورهای فرآیندهای درستی‌سنجی زیست‌سنجی

دستورهای بازیابی، درستی‌سنجی و اصالت‌سنجی تعریف‌شده در استاندارد ISO/IEC7816-4 برای درستی‌سنجی زیست‌سنجی به کار می‌رود. داده‌های زیست‌سنجی (به طور مثال ویژگی‌های صورت، شکل گوش، اثر انگشت، الگوی گفتار، الگوی صدا[1]، ضربه زدن به کلید[2]) ممکن است به محافظت در برابر بازپخش یا ارائه داده درستی‌سنجی به دست آمده از داده‌های اصلی زیست‌سنجی نیاز داشته باشد (به طور مثال اثر انگشت، عکس چهره). ارسال داده‌های درستی‌سنجی همراه با جمع‌آزمای رمزنگاشتی یا امضای رقمی حاوی پیام دادن امن به کارت، طبق تعریف استاندارد ISO/IEC 7816-4 ، روشی برای پیشگیری از این نوع حمله است. به همین ترتیب، برای تضمین اصالت داده‌های زیست‌سنجی بازیابی‌شده از کارت، ممکن است از پیام دادن امن استفاده شود.

1 - Voice Print
2 - Key stroke

۵-۱ دستورهای بازیابی اطلاعات زیست‌سنجی

دستورها همان طور که در بند مربوط به مرجع داده در استاندارد ISO/IEC 7816-4 مشخص شده باید برای بازیابی اطلاعات زیست‌سنجی استفاده شود.

۵-۲ دستور برای فرآیند درستی‌سنجی زیست‌سنجی ایستا

دستوری که باید برای فرآیند درستی‌سنجی ایستا استفاده شود (به پیوست الف مراجعه شود) همان طور که در ISO/IEC 7816-4 مشخص شده، دستور VERIFY است. اطلاعاتی که باید منتقل شوند:

— شناسانه داده مرجع زیست‌سنجی (به طور مثال توصیف‌کننده داده مرجع)؛

— داده درستی‌سنجی زیست‌سنجی.

داده درستی‌سنجی زیست‌سنجی ممکن است به عنوان اشیا داده BER-TLV (به جدول ۲ مراجعه شود) کدگذاری شود. همچنین بایت CLA ممکن است نشان دهد که فیلد داده دستور با BER-TLV کد شده است (به ISO/IEC 7816-4 مراجعه شود).

برای طرح‌های ترکیبی زیست‌سنجی، ممکن است طبق تعریف ISO/IEC 7816-8 از زنجیره دستور، استفاده شود.

۵-۳ دستورهای فرآیند درستی‌سنجی زیست‌سنجی پویا

برای دریافت چالش، پاسخ کاربر مورد نیاز است (به پیوست الف مراجعه شود) که باید از دستور GET CHALLENGE استفاده شود.

نوع چالش در فرآیند درستی‌سنجی زیست‌سنجی، به طور مثال عبارتی برای الگوی صدا یا عبارتی برای ضربه زدن به کلید، بستگی به الگوریتم زیست‌سنجی دارد که می‌تواند در P1 دستور GET CHALLENGE مشخص شود (به ISO/IEC 7816-4 مراجعه شود). الگوریتم مرتبط ممکن است یک در میان با استفاده از دستور MANAGE SECURITY ENVIRONMENT انتخاب شود. (به طور مثال گزینه SET با CRT AT و توصیف‌کننده کاربرد شی داده و شناسانه الگوریتم شی داده در فیلد داده).

پس از دستور موفقیت‌آمیز GET CHALLENGE، دستور EXTERNAL AUTHENTICATE به کارت ارسال می‌شود. فیلد داده دستور، داده درستی‌سنجی زیست‌سنجی مرتبط را انتقال می‌دهد. برای کدگذاری داده درستی‌سنجی زیست‌سنجی، اصول مشابهی مانند دستورVERIFY اعمال می‌شود، به بند ۵-۱ مراجعه شود.

۶ عناصر داده

۶-۱ اطلاعات زیست‌سنجی

الگوی اطلاعات زیست‌سنجی (BIT)، اطلاعات توصیفی در مورد داده زیست‌سنجی مرتبط را ارائه می‌کند. این موضوع توسط کارت در پاسخ به دستور بازیابی، قبل از فرآیند درستی‌سنجی ارائه می‌شود. جدول ۱ اشیا داده اطلاعات زیست‌سنجی را تعریف می‌کند.

جدول۱- اشیا داده اطلاعات زیست‌سنجی

برچسب	طول	مقدار			وجود
‘7F60’	متغیر	الگوی اطلاعات زیست‌سنجی (BIT)			
		برچسب	**طول**	**مقدار**	
		‘80’	۱	الگوریتم مرجع برای استفاده در VERIFY / EXT. دستور AUTHENTICATE /MANAGE SE	اختیاری
		‘83’	۱	توصیف‌کننده داده مرجع برای استفاده در VERIFY / EXT. AUTH. دستور MANAGE SE	اختیاری
		‘A0’	متغیر	اشیا داده اطلاعات زیست‌سنجی تعریف‌شده در این استاندارد	اختیاری
		‘06’ ‘41’ ‘42’ ‘4F’	متغیر متغیر متغیر متغیر	مرجع دارای اختیار تخصیص برچسب (به ISO/IEC 7816-6 مراجعه شود): - شناسانه شی (OID) - مرجع دارای اختیار کشور (به ISO/IEC 7816-4 مراجعه شود) - صادرکننده (به ISO/IEC 7816-4 مراجعه شود) - شناسانه کاربرد (AID)، کاربرد و ارائه دهنده آن را شناسایی می‌کند (به ISO/IEC 7816-4 مراجعه شود) مرجع دارای اختیار تخصیص برچسب پیش‌فرض ISO/IEC JTC1 / SC37 است.	اگر ‘A1’ وجود داشته باشد، یکی از این اشیا داده اجباری است
	‘A1’			اشیا داده اطلاعات زیست‌سنجی با مرجع دارای اختیار تخصیص برچسب مشخص شده است (به اجباری بودن اشاره دارد، به قسمت بالا مراجعه شود). همچنین به مثال پیوست پ مراجعه شود.	اگر ‘A0’ وجود داشته باشد، اجباری است
		برچسب	**طول**	**مقدار**	
		‘8x’/’Ax’ ‘9x’/’Bx’	متغیر متغیر	اشیا داده تعریف‌شده با مرجع دارای اختیار تخصیص برچسب ...(اولیه / ساخته‌شده) ...(اولیه / ساخته‌شده)	شی داده وابسته

یادآوری- در موردی که کارت، فرآیند درستی‌سنجی را انجام نمی‌دهد، الگوی اطلاعات زیست‌سنجی، ممکن است داده‌های مرجع زیست‌سنجی (به جدول ۳ مراجعه شود) و احتمالا داده‌های احتیاطی (برچسب ’53‘یا’73‘) را شامل شود، به طور مثال برای داده‌هایی که در صورت مثبت شدن درستی‌سنجی باید به سامانه خدمت تحویل داده شود (به پیوست پ مراجعه شود).

اگر چندین BIT در همان کاربرد وجود داشته باشد، باید طبق جدول ۲، گروه‌بندی صورت گیرد.

جدول ۲ – الگوی گروه BIT

برچسب	طول	مقدار			وجود
'7F61'	متغیر	الگوی گروه BIT			
		برچسب	طول	مقدار	
		'02'	متغیر	تعداد BITهـا در گروه	اجباری
		'7F60'	متغیر	BIT 1	شرطی
				…	
				BIT n	شرطی

به طور مثال الگوی گروه BIT می‌تواند توسط موارد زیر بازیابی شود.

— دستور GET DATA

— خواندن پرونده در DF مرتبط و یافتن EFID در FCI، یا

— خواندن الگوی SE (به ISO/IEC 7816-4 مراجعه شود)، که در آن الگوی گروه BIT ذخیره شده است.

۶-۲ داده‌های زیست‌سنجی

داده‌های زیست‌سنجی (داده‌های درستی‌سنجی زیست‌سنجی، داده‌های مرجع زیست‌سنجی) ممکن است به صورت موارد زیر ارائه شود.

— به عنوان الحاق عناصر داده،

— در داخل شی دادهٔ داده‌های زیست‌سنجی طبق تعریف استاندارد ISO/IEC 7816-6

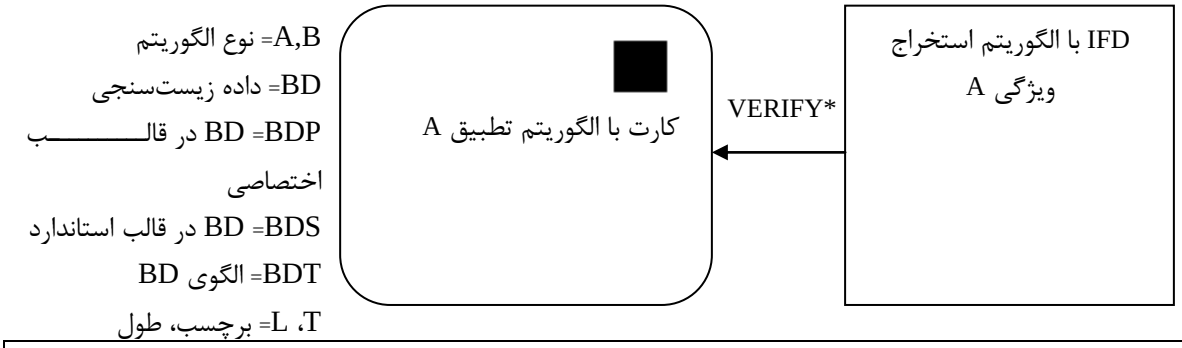
— یا به عنوان الحاق اشیا داده در الگوی داده زیست‌سنجی، به جدول ۳ مراجعه شود.

جدول ۳ – اشیا داده داده‌های زیست‌سنجی

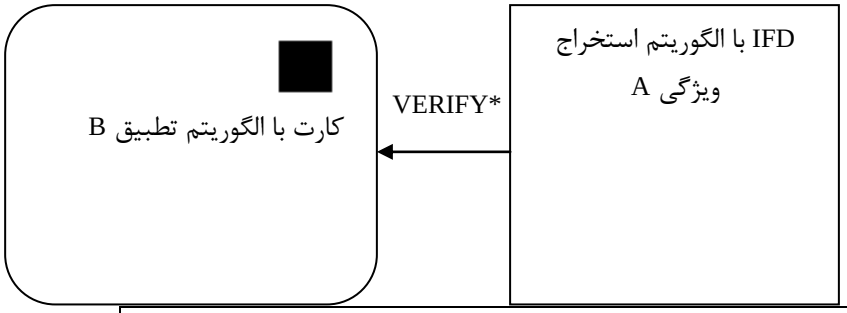
برچسب	طول	مقدار			وجود
'5F2E'	متغیر	داده زیست‌سنجی			
'7F2E'	متغیر	الگوی داده زیست‌سنجی			
		برچسب	طول	مقدار	
		'5F2E'	متغیر	داده زیست‌سنجی	
		'81'/'A1'	متغیر	داده زیست‌سنجی با الگوی استاندارد (اولیه/ساخته‌شده)	
		'82'/'A2'	متغیر	داده زیست‌سنجی با الگوی اختصاصی (اولیه/ساخته‌شده)	در صورتی که الگو استفاده شود، دست کم یکی از این اشیا داده وجود دارد

همان طور که در جدول ۳ نشان داده شده است، داده‌های زیست‌سنجی ممکن است در یک قسمت با قالب استاندارد و در یک قسمت با قالب اختصاصی تقسیم شود که به طور مثال ممکن است استفاده از قسمت

الگوی اختصاصی، برای دستیابی به عملکرد بهتر باشد. استفاده از داده‌های زیست‌سنجی با قالب‌های استاندارد و اختصاصی در شکل ۱ نشان داده شده است.
ساختار و کدگذاری داده‌های زیست‌سنجی، وابسته به نوع زیست‌سنجی (به طور مثال ویژگی‌های صورت، اثر انگشت) است و خارج از دامنه کاربرد این استاندارد است.



*= داده درستی‌سنجی:							
BD در قالب اختصاصی A	L	T.BDP	BD در قالب استاندارد	L	T.BDS	L	T.BDT



الگوریتم‌های تطبیق A و B متعلق به یک نوع یکسان زیست‌سنجی است، اما از داده‌های زیست‌سنجی اختصاصی مختلف به طور مثال برای ارتقا کارایی، استفاده می‌کند. با این حال، هر دو قادر به محاسبه نتیجه درستی‌سنجی، تنها با استفاده از BD در قالب استاندارد هستند.

***= داده درستی‌سنجی:**				
BD در قالب استاندارد	L	T.BDS	L	T.BDT

شکل ۱ - استفاده از داده‌های زیست‌سنجی با ساختار استاندارد و اختصاصی

۶-۳ اطلاعات الزامات درستی‌سنجی

۶-۳-۱ هدف

الزامات درستی‌سنجی کنونی توسط هریک از موارد زیر ارائه می‌شود:
- VIDO شی داده اطلاعات الزامات درستی‌سنجی (برچسب '96'، قالب کوتاه)، یا
- VIT الگوی اطلاعات الزامات درستی‌سنجی (برچسب 'A6' و قالب طولانی).

VIDO یا VIT در صورت وجود، بخشی از اطلاعات پارامتر کنترلی پرونده DF مرتبط هستند یا در پرونده پسوند FCI طبق تعریف ISO/IEC 7816-4 ذخیره شده است. VIDO و VIT حاوی اطلاعاتی هستند که

نشان می‌دهد آیا داده‌های مرجع برای درستی‌سنجی کاربر (به طور مثال کلمه‌های عبور و/ یا داده‌های زیست‌سنجی):

— فعال یا غیرفعال و

— قابل استفاده یا غیر قابل استفاده است.

یادآوری- معمولا پرچم فعال/غیرفعال تحت کنترل دارنده کارت است و پرچم قابل استفاده/ غیر قابل استفاده تحت کنترل ارائه‌دهنده برنامه کاربردی است.

۶-۳-۲ VIDO- قالب کوتاه

اولین بایت VIDO (به جدول ۴ مراجعه شود) نقشه بیتی نشان می‌دهد که کدام کلید (به طور مثال داده‌های مرجع برای درستی‌سنجی کاربر) فعال (بیت را ۱ قرار دهید) یا غیرفعال (بیت را ۰ قرار دهید) است. بایت دوم نقشه بیتی نشان می‌دهد که کدام کلید قابل استفاده (بیت را ۱ قرار دهید) یا غیر قابل استفاده (بیت را ۰ قرار دهید) است. هر یک از بایت‌های زیر، کلیدهای مرجع هستند. اولین کلید مرجع مربوط به بیت b8 نقشه‌های بیتی، دومین کلید مرجع مربوط به بیت b7 و به همین ترتیب است. به طور ضمنی تعداد کلیدهای مرجع توسط طول VIDO ارائه می‌شود، به طور مثال هنگامی که L کمتر یا برابر با ۱۰ است، همواره تعداد کلیدهای مرجع L-2 است.

جدول ۴ - ساختار VIDO

...	کلید مرجع	کلید مرجع	پرچم قابل استفاده/ غیر قابل استفاده[1]	پرچم فعال/ غیرفعال[2]	L	برچسب VIDO
...	'xx'	'xx'	'xx'	'xx'	متغیر	'96'

۶-۳-۳ VIT - قالب طولانی

VIT اطلاعات را در قالب‌های طولانی ارائه می‌کند که می‌تواند اطلاعات افزوده‌ای در مورد توصیف‌کننده کاربرد شی داده ارائه دهد. اشیا داده‌ای که ممکن است در یک VIT رخ دهد، در جدول ۵ نشان داده شده است.

جدول ۵ - الگوی اطلاعات الزامات درستی‌سنجی (VIT) و اشیا داده تعبیه‌شده

برچسب	طول	مقدار		
'A6'	متغیر	الگوی اطلاعات الزامات درستی‌سنجی		
		برچسب	طول	مقدار
		'90'	۱	پرچم‌های فعال / غیرفعال (شی داده DO)
		'95'	۱	توصیف‌کننده کاربرد طبق تعریف ISO/IEC 7816

1 - Usable / unusable

2 - Enabled / disabled

		‘83’	۱	کلید مرجع

پرچم فعال/ غیر فعال شی داده الزامی است. دست کم یک کلید مرجع شی داده باید ارائه شود. هر کلید مرجع شی داده ممکن است به دنبال شی داده توصیف‌کننده کاربرد مرتبط بیاید. اگر هیچ توصیف‌کننده کاربردی به کلید مربوط نشود، آنگاه استفاده، ضمنی تلقی خواهد شد. در این زمینه، توصیف‌کننده کاربرد صفر تنظیم می‌شود و به معنی آن است که کلید مرتبط نباید استفاده شود.

یادآوری- نیازی به معرفی VIT با برچسب برنامه جهت بازیابی توسط GET DATA نیست، چرا که FCI یا پرونده پسوند FCI می‌تواند همیشه خوانده شود.

پیوست الف

(اطلاعاتی)

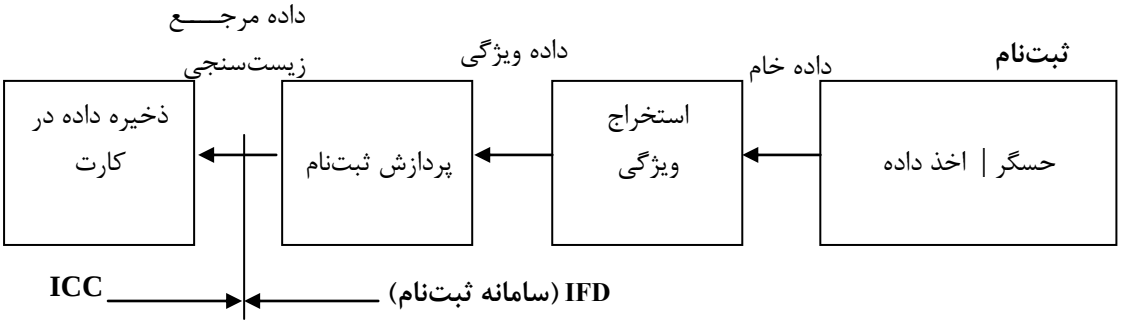
فرآیند درستی‌سنجی زیست‌سنجی

الف-۱ کوته‌نوشت‌ها

کارت مدار(های) مجتمع	Integrated Circuit(s) Card	ICC
افزاره واسط	Interface Device	IFD
شناسانه شی	Object Identifier	OID
پیام دادن امن	Secure Messaging	SM

الف-۲ فرآیند ثبت‌نام و فرآیند درستی‌سنجی

طرح فرآیند ثبت‌نام به طور کلی (ساده‌شده) در شکل الف-۱ نشان داده شده است.



شکل الف-۱ طرح کلی فرآیند ثبت‌نام

حسگر و پودمان (ماژول)[1] به دست آوردن داده به عنوان یک واحد منطقی در نظر گرفته می‌شود، اگر چه ممکن است پودمان‌های جداگانه باشند. داده‌های خام معمولاً خارج از کارت با توجه به اندازه این داده‌ها پردازش می‌شود. در طی این پردازش، ویژگی‌های زیست‌سنجی استخراج و برای استفاده‌های بعدی قالب‌بندی می‌شود. در پردازش ثبت‌نام یا در مرحله بعد، داده مرجع زیست‌سنجی احتمالاً همراه با اطلاعات افزوده به روشی امن برای ذخیره‌سازی و استفاده‌های بعدی به کارت ارسال می‌شود.

درمورد تطبیق در کارت، این داده‌ها نمی‌تواند پس از ذخیره‌سازی بازیابی شود. در مورد تطبیق خارج از کارت، داده‌های مرجع زیست‌سنجی ممکن است به عنوان بخشی از BIT بازیابی شود. داده‌های مرجع زیست‌سنجی یا احتمالاً کل BIT به طور مثال توسط امضای رقمی، ممکن است امن شود. همچنین دسترسی به BIT ممکن است محدود شود، به طور مثال دسترسی تنها پس از عملکرد موفقیت‌آمیز رویه اصالت‌سنجی امکان‌پذیر خواهد بود.

داده‌های مرجع زیست‌سنجی ممکن است در کارت ذخیره شود:

— در طول مرحله شخصی‌سازی کارت، یا

1 - Module

— پس از صدور کارت به دارنده کارت.

ذخیره داده‌های مرجع پس از صدور کارت به دارنده کارت یا هنگام تحویل کارت به دارنده کارت در پیوست ب ارائه شده است.

شکل الف-۲ طرحی ساده‌شده برای درستی‌سنجی را نشان می‌دهد که پیکربندی‌های زیر را تحت پوشش قرار می‌دهد:

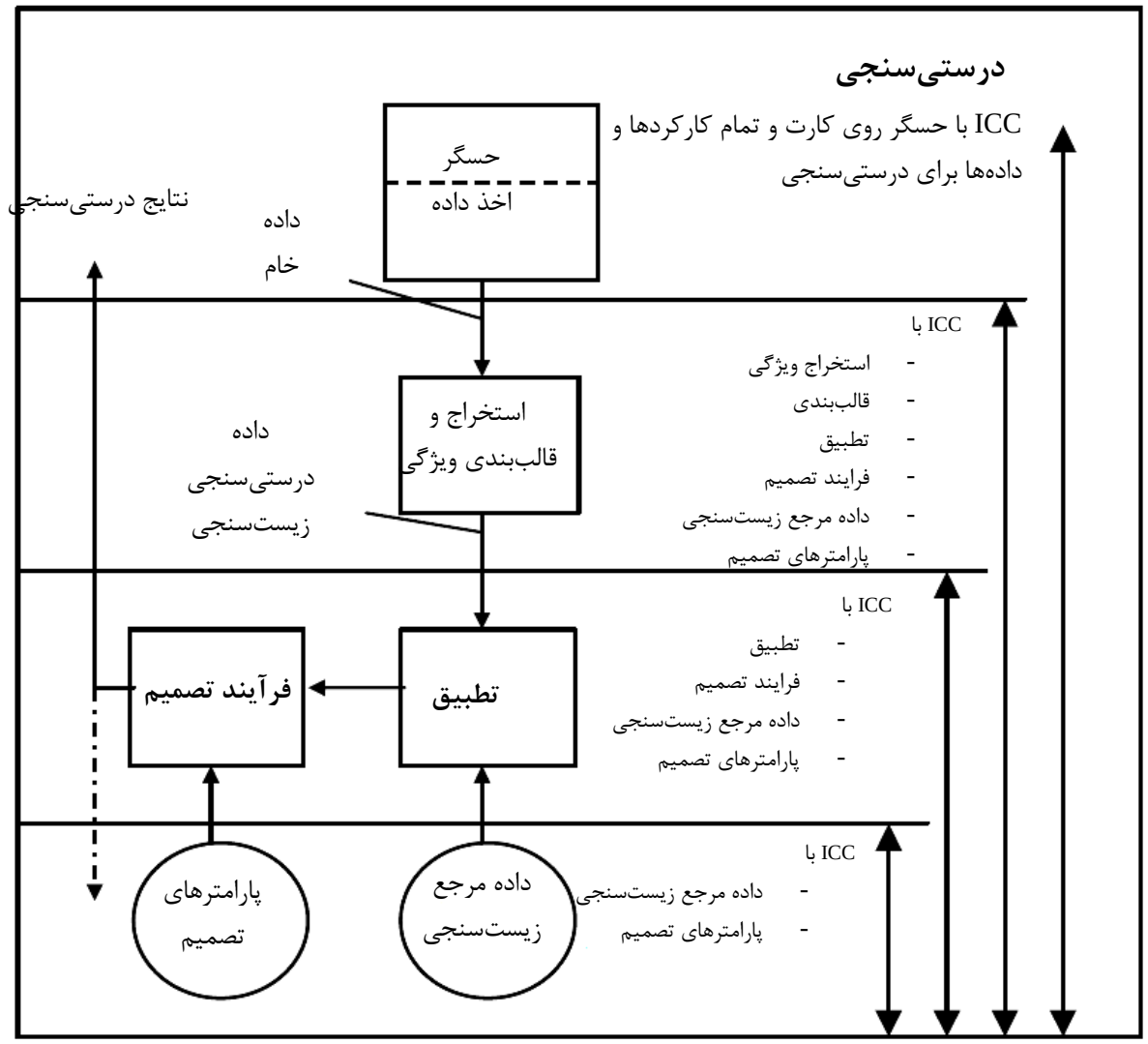
—داده‌های مرجع زیست‌سنجی و احتمالا پارامترهای ذخیره‌شده در کارت

—پردازش تطبیق و تصمیم در کارت

—پردازش استخراج ویژگی، قالب‌بندی، تطبیق و تصمیم در کارت

—حسگر بر روی کارت و عملکرد کل فرآیند درستی‌سنجی در کارت.

سایر پیکربندی‌ها نیز امکان پذیر است.



شکل الف-۲ - طرح کلی فرآیند درستی‌سنجی

یادآوری- پارامترهای تصمیم‌گیری معمولاً به پردازش تصمیم محدود می‌شود. هنگامی که کارت، برای تطبیق خارجی (پایین‌ترین مورد در شکل الف-۲)، داده‌های مرجع زیست‌سنجی را ارائه می‌کند (که احتمالا توسط رمزنگاشتی محافظت شده است) پارامترهای تصمیم‌گیری ممکن است تنها در صورتی که حاوی مولفه‌های خاص کاربر باشند، موجود و قابل بازیابی (به روشی امن) باشد.

الف-۳ رده‌بندی روش‌های درستی‌سنجی زیست‌سنجی

با در نظر گرفتن تبادل پیام‌های مختلف بین کارت و IFD، رده‌بندی زیر استفاده می‌شود:

— روش درستی‌سنجی زیست‌سنجی ایستا:

روش درستی‌سنجی زیست‌سنجی که به ارائه ویژگی (به طور مثال ایستا) فیزیولوژیکی شخص برای اصالت‌سنجی (به نوع A مراجعه شود) یا به عملکرد اقدام ثبت‌نام‌شده از پیش تعیین‌شده (به نوع B مراجعه شود) نیاز دارد.

— روش درستی‌سنجی زیست‌سنجی پویا:

روش درستی‌سنجی زیست‌سنجی که به اقدام پویا از شخصی که باید اصالت‌سنجی شود، نیاز دارد (به طور مثال پاسخ کاربر به چالش زیست‌سنجی، به نوع B مراجعه شود).

مثال‌های زیست‌سنجی نوع A:

شکل گوش

ویژگی‌های صورت

شکل هندسی انگشت

اثر انگشت

شکل هندسی دست

عنبیه

شکل هندسی کف دست

شبکیه چشم

الگوی رگ‌ها[1]

یادآوری- این انواع زیست‌سنجی تنها می‌تواند برای درستی‌سنجی ایستا استفاده شود.

مثال‌های زیست‌سنجی نوع B:

پویایی ضربه زدن به کلید

حرکات لب

تصویر امضا

الگوی گفتار (رد صدا)

پویایی نوشتن (پویایی امضا)

1 - Vein pattern

یادآوری- این انواع زیست‌سنجی ممکن است بسته به مورد استفاده، هم برای درستی‌سنجی ایستا و هم برای درستی‌سنجی پویای انواع مرتبط، استفاده شود.

خصوصیات اصلی زیست‌سنجی ویژگی‌های نوع A عبارتند از:

— منحصر به فرد، تغییرناپذیر

— قابل انتخاب، اگر نمونه‌های متعددی از همان نوع وجود داشته باشد (به طور مثال شست، انگشت اشاره)

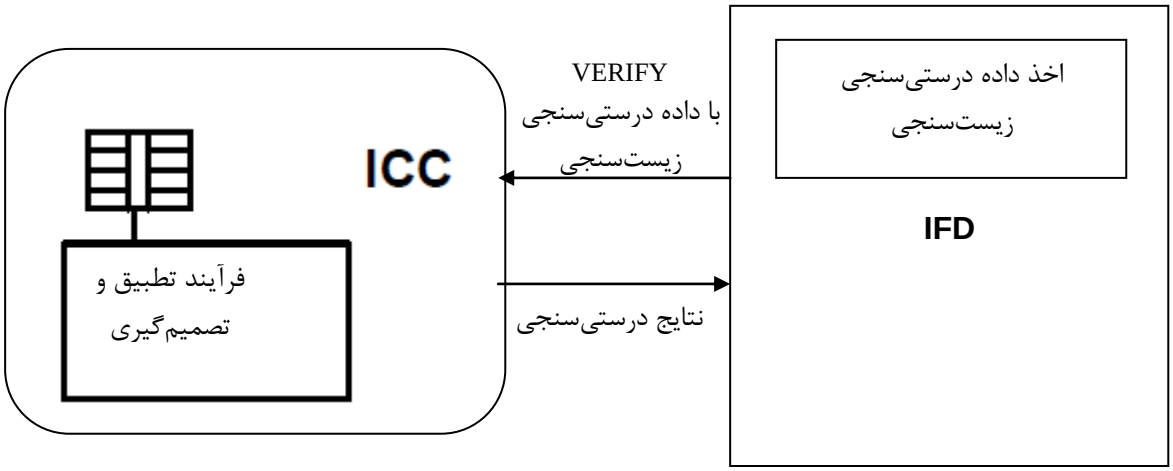
— عمومی، در صورتی که ویژگی‌های مرتبط (به طور مثال صورت، گوش، اثر انگشت) بتواند توسط هر فردی گرفته یا سنجش شود، به طور مثال داده‌های درستی‌سنجی زیست‌سنجی مرتبط باید از یک مسیر معتبر به کارت ارائه شود (به شکل ب-۴ پیوست ب مراجعه شود).

مشخصه‌های اصلی ویژگی‌های زیست‌سنجی نوع B عبارتند از:

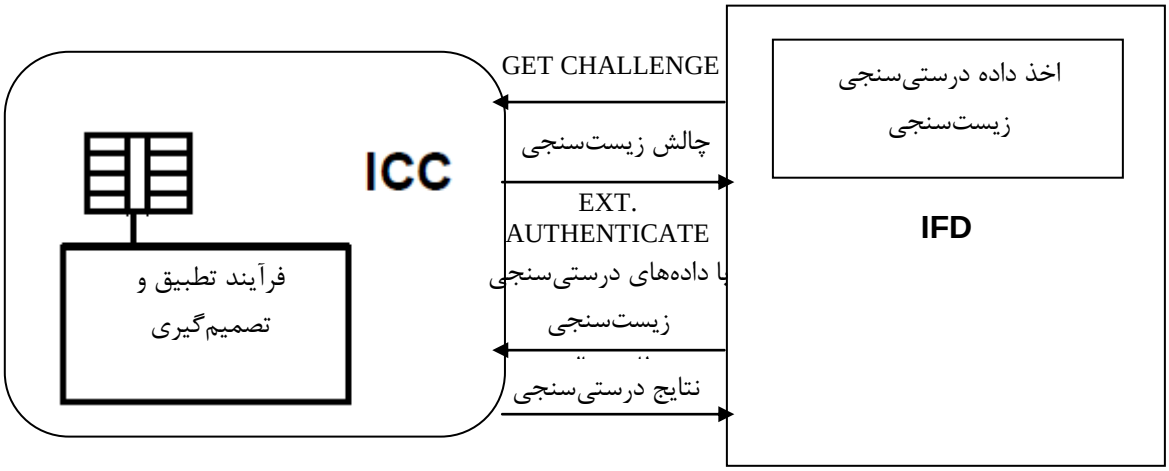
— منحصر به فرد، اما تغییرپذیر

— وابسته به چالش، اگر درستی‌سنجی پویا استفاده شود.

شکل الف-۳ و الف-۴ تفاوت بین درستی‌سنجی زیست‌سنجی ایستا و پویا در واسط کارت را در حالت تطبیق و پردازش تصمیم در کارت، نشان می‌دهد.



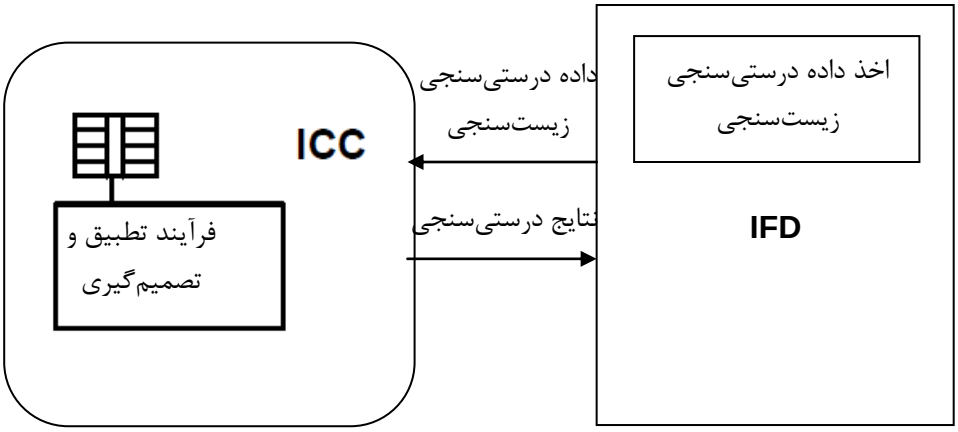
شکل الف-۳ - دستورها برای درستی‌سنجی زیست‌سنجی ایستا



شکل الف-۴ - دستورها برای درستی‌سنجی زیست‌سنجی پویا

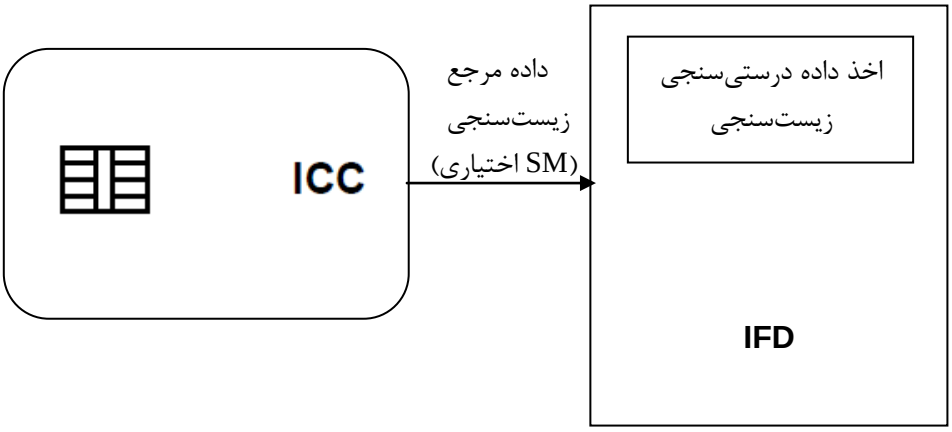
الف-۴ فرانامه‌ها

شکل الف-۵ و الف-۶ برخی فرانامه‌های مربوط به درستی‌سنجی کاربر زیست‌سنجی را نشان می‌دهد.



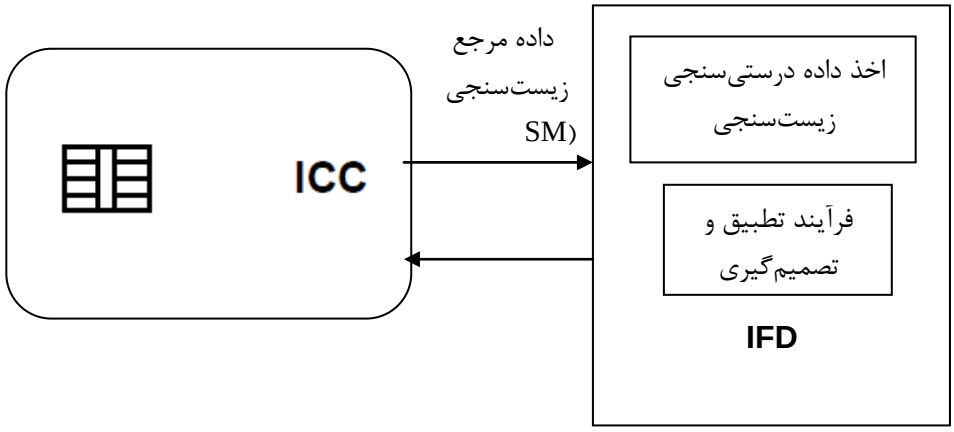
نتیجه فرآیند درستی‌سنجی زیست‌سنجی، وضعیت امنیتی کارت را تغییر می‌دهد. اگر همچنین وضعیت امنیتی IFD را اصلاح کند، باید با پیام‌نگاری امن محافظت شود.

شکل الف-۵ - فرانامه با فرایند تطبیق و تصمیم‌گیری در داخل کارت



.

ممکن است شرایط دسترسی به داده‌های مرجع زیست‌سنجی ضمیمه شود.



اگر نتیجه فرآیند درستی‌سنجی زیست‌سنجی، وضعیت امنیتی کارت را تغییر دهد، باید توسط پیام‌نگاری امن محافظت شود.

شکل الف-۶- فرانامه‌ها با فرایند تطبیق و تصمیم‌گیری در خارج از کارت

الف-۵ بازیابی اطلاعات مرتبط برای فرآیند درستی‌سنجی زیست‌سنجی

ممکن است IFD به اطلاعات مربوط به فرآیند درستی‌سنجی نیاز داشته باشد. فهرست زیر شامل اقلام اطلاعاتی است که ممکن است توسط IFD مورد نیاز باشد:

— نوع زیست‌سنجی (به طور مثال اثر انگشت، ویژگی‌های صورت، ...)

— زیرنوع زیست‌سنجی، اگر مناسب باشد (به طور مثال انگشت اشاره چپ)

— مالک قالب و نوع قالب داده‌های زیست‌سنجی

— الگوریتم مرجع، اگر باشد، همان طور که به طور مثال در دستور MANAGE SECURITY ENVIRONMENT استفاده شده است.

— شناسانه داده‌های مرجع زیست‌سنجی (توصیف‌کننده داده‌های مرجع در دستور VERIFY یا دستور EXTERNAL AUTHENTICATE)

— داده احتیاطی، در صورت وجود.

پیوست ب

(اطلاعاتی)

مثال‌هایی برای ثبت‌نام و درستی‌سنجی

ب-۱ کوته‌نوشت‌ها

AID	Application Identifier	شناسانه برنامه کاربردی
AT	Authentication Template	الگوی اصالت‌سنجی
BIT	Biometric Information Template	الگوی اطلاعات زیست‌سنجی
BT	Biometric Type	نوع زیست‌سنجی
CRT	Control Reference Template	الگوی کنترل مرجع
DO	Data Object	شی داده
DST	Digital Signature Template	الگوی امضای رقمی
FCI	File Control Information	اطلاعات کنترلی پرونده
FO	Format Owner	مالک قالب
FT	Format Type	نوع قالب
ID	Identifier	شناسانه
IFD	Interface Device	افزاره واسط
OID	Object Identifier	شناسانه شی
RD	Reference Data	داده مرجع
SM	Secure Messaging	پیام دادن امن
TAT	Tag allocation Authority Template	الگوی مرجع دارای اختیار تخصیص برچسب
UQ	Usage Qualifier	توصیف‌کننده کاربرد
VIT	Verification Requirement Information Template	الگوی اطلاعات الزامات درستی‌سنجی
||	Concatenation	الحاق

ب-۲ ثبت‌نام

در این مثال، فرض بر این است، که:

— کارت به جز ذخیره داده‌های مرجع زیست‌سنجی و الگوی اطلاعات زیست‌سنجی مربوط، کاملا شخصی‌سازی شده، (همچنین این موضوع شامل وجود سوابق زیست‌سنجی در پرونده کلید با صفت‌های مرتبط برای داده‌های مرجع زیست‌سنجی است، به طور مثال تعداد تلاش مجدد با مقدار اولیه، بازنشانی کد با تعداد تلاش مجدد و مقدار اولیه، پرچم‌هایی برای فعال‌سازی/ غیرفعال‌سازی الزامات درستی‌سنجی و تغییرپذیری، ...)

— کارت علاوه بر زیست‌سنجی، دارای رمز عبور درستی‌سنجی است.

با دستور CHANGE REFERENCE DATA، داده‌های مرجع خالی با داده‌های مرجع کاربر در فرآیند ثبت‌نام جایگزین می‌شود. اجرای دستور CHANGE REFERENCE DATA باید به شرایط امنیتی به طور مثال تنظیم وضعیت امنیتی مورد نیاز پس از تکمیل موفقیت‌آمیز رمزنگاشتی مبتنی بر رویه اصالت‌سنجی یا ارائه موفقیت‌آمیز رمز عبور، محدود شود.

یادآوری- شرایط امنیتی برای دستور CHANGE REFERENCE DATA، که پس از ثبت‌نام صورت می‌گیرد، ممکن است با توجه به خط‌مشی امنیتی ارائه‌دهنده برنامه کاربردی (به طور مثال تغییر داده مرجع پس از ثبت‌نام مجاز نیست) متفاوت باشد.

پس از ذخیره داده‌های مرجع زیست‌سنجی، الگوی اطلاعات زیست‌سنجی BIT که توسط IFD در فرآیند درستی‌سنجی این مثال استفاده می‌شود، باید ذخیره شود. BIT بعد از تمام انواع و زیر انواع مرجع زیست‌سنجی ثبت‌نام‌شده، ذخیره می‌شود.

معمولاً IFD (به طور مثال رایانه شخصی، پایانه (ترمینال) اینترنت عمومی یا پایانه صندوق) نمی‌داند که کارت ارائه‌شده:

— متعلق به کاربری است که زیست‌سنجی را اعمال می‌کند
— دارای الگوریتم زیست‌سنجی پشتیبانی‌شده توسط IFD است
— چه نوع زیست‌سنجی برای آن چه باید انجام شود، استفاده شده است
— کلید مرجع مرتبط (به طور مثال توصیف‌کننده داده‌های مرجع) چه مقداری دارد
— چه پارامترهای خاص پیاده‌سازی‌شده الگوریتم تطبیق باید مشاهده شود (به طور مثال محدودیت تعداد مینوشیاهایی[1] که باید به عنوان داده‌های تایید ارسال شود).

بنابراین الگوی اطلاعات زیست‌سنجی BIT باید اطلاعاتی همچون موارد زیر را ارائه کند:

— توصیف‌کننده داده‌های مرجع زیست‌سنجی
— OID مرجع دارای اختیار تخصیص برچسب و اشاره به قالب داده‌های درستی‌سنجی
— نوع زیست‌سنجی و احتمالا زیرنوع زیست‌سنجی ثبت‌نام‌شده (به طور مثال انگشت شست راست)
— اشیا داده بیشتر، در صورت وجود
— تکرار اشیای داده مرتبط، اگر به طور مثال نوع دوم زیست‌سنجی نیز ثبت‌نام شده باشد.

شکل ب-۱ دستورهایی که ممکن است در این مسیر در فرآیند ثبت‌نام انجام شود را نشان می‌دهد.

۱- مینوشیا (minutiae)، ویژگی‌ای است که از اثرانگشت اسخراج می شود.

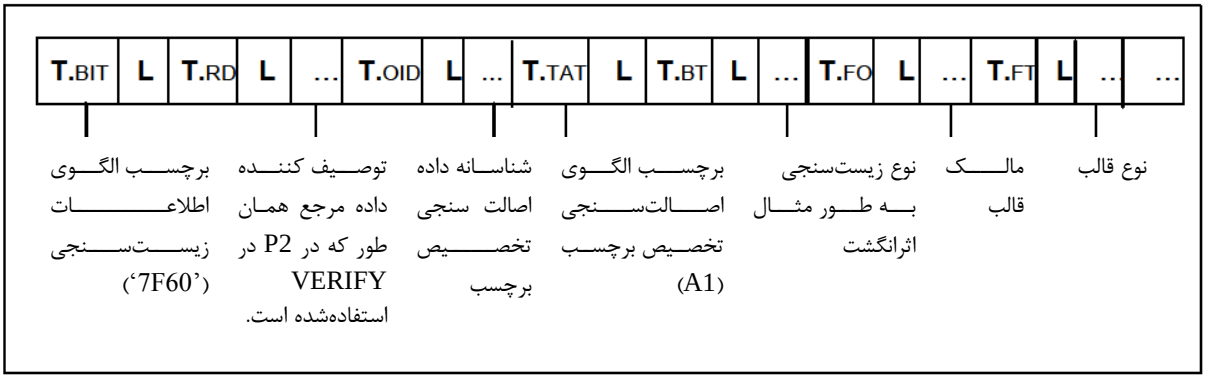
مفهوم	دستور/پاسخ
VERIFY <Password> OK	تنظیم وضعیت امنیتی برای ذخیره‌سازی داده مرجع زیست‌سنجی
CHANGE RD <Biometric Reference Data> OK	جایگزینی داده مرجع خالی با داده مرجع زیست‌سنجی ثبت‌نام‌شده
SELECT <File ID> OK	انتخاب پرونده اولیه برای ذخیره‌سازی الگوی اطلاعات زیست‌سنجی BIT (که با GET DATA بازیابی می‌شود)
UPDATE BINARY <BIT> OK	ذخیره‌سازی الگوی اطلاعات زیست‌سنجی BIT

شکل ب-۱ - دستورهایی برای ثبت‌نام (مثال)

یادآوری ۱- ممکن است به حفاظت از ثبت‌نام با پیام دادن امن نیاز باشد.

یادآوری ۲- برای ذخیره و بازیابی اطلاعات، ممکن است دستورهای دیگر شرح داده شده در ISO/IEC 7816-4 نیز مورد استفاده قرار گیرد. این موضوع برای شکل‌های ب-۴، ب-۶ و ب-۷ نیز معتبر است.

شکل ب-۲، BIT و اشیا داده آن را نشان می‌دهد.



شکل ب-۲ - مثال الگوی اطلاعات زیست‌سنجی (BIT)، برچسب‌های تخصیص یافته توسط مرجع مشخص تخصیص برچسب

یادآوری- برچسب‌های داخل الگوی "A1" مرجع دارای اختیار تخصیص برچسب استفاده‌شده را تعریف می‌کند.

ب-۳ درستی‌سنجی با روش زیست‌سنجی واحد

فرآیند درستی‌سنجی با بازیابی الگوی اطلاعات زیست‌سنجی به طور مثال با استفاده از دستور GET DATA شروع می‌شود. اگر IFD از قالب مورد نیاز برای داده‌های درستی‌سنجی زیست‌سنجی که در BIT نشان‌داده‌شده، پشتیبانی کند و کاربر شی زیست‌سنجی مرتبط را ارائه دهد، داده‌های درستی‌سنجی محاسبه می‌شود و با استفاده از دستور VERIFY به کارت تحویل داده می‌شود (به شکل ب-۳ مراجعه شود).

دستور/پاسخ	مفهوم
انتخاب برنامه کاربردی با شناسانه برنامه کاربردی (AID)	**SELECT** <AID> OK
بازیابی الگوی اطلاعات زیست‌سنجی (BIT)	**GET DATA** <Tag BIT> Bio. Information Template
درستی‌سنجی کاربر	**VERIFY** <Biometric Verification Data> OK

شکل ب-۳ - دستورهایی برای درستی‌سنجی بدون پیام دادن امن (مثال)

یادآوری- اگر الگوی اطلاعات زیست‌سنجی وجود نداشته باشد، به معنی آن است که در این مثال کاربر مرتبط از زیست‌سنجی استفاده نمی‌کند.

اگر داده‌های درستی‌سنجی زیست‌سنجی عمومی باشد (به طور مثال چهره، اثر انگشت، شکل گوش)، نیاز به حفاظت از آن‌ها با پیام دادن امن وجود دارد (به شکل ب-۴ مراجعه شود).

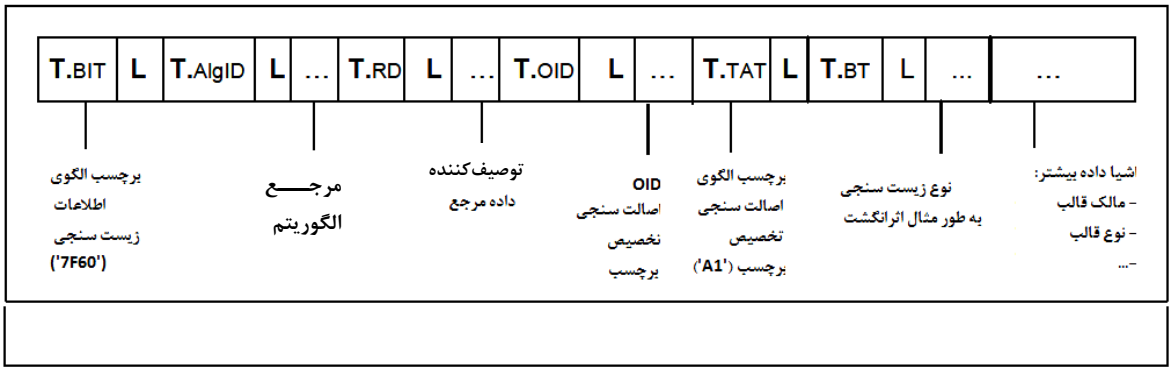
دستور/پاسخ	مفهوم
انتخاب برنامه کاربردی با شناسانه برنامه کاربردی (AID)	**SELECT** <AID> OK
بازیابی الگوی اطلاعات زیست‌سنجی (BIT)	**GET DATA** <Tag BIT> Bio. Information Template
تنظیم CTR DST با کلید عمومی برای گواهی درستی‌سنجی	**MANAGE SE** <DO Key Ref> OK

VERIFY CERTIFICATE <certificate> → OK ←	درستی‌سنجی گواهی متعلق به واحد زیست‌سنجی
GET CHALLENGE → Random Number ←	درخواست چالش برای استفاده در پیام دادن امن
EXTERNAL AUTHENTICATE <authentication related data> → authentication related data ←	اصالت‌سنجی خارجی با استقرار کلیدهای SM
VERIFY <Biom. Verification Data, SM protected> → OK ←	درستی‌سنجی کاربر با داده‌های درستی‌سنجی حفاظت‌شده SM؛ پاسخ‌ها نیز می‌تواند با SM حفاظت شود

شکل ب- ۴- دستورات برای درستی‌سنجی با پیام دادن امن (مثال)

یادآوری- پیام دادن امن (SM) در ISO/IEC 7816-4 مطرح شده است.

در این مثال، فرآیند درستی‌سنجی با بازیابی الگو اطلاعات الزامات درستی‌سنجی (VIT) و الگوی اطلاعات زیست‌سنجی مرتبط (BIT)، شروع می‌شود که ممکن است به طور مثال در پرونده پسوند FCI (پرونده ID به طور ضمنی شناخته‌شده) ذخیره شده باشد. VIT حاوی اطلاعاتی است، که آیا درستی‌سنجی زیست‌سنجی و/ یا رمز عبور در دسترس و فعال است یا غیر فعال است و این که کدام توصیف‌کننده مربوط به داده‌های مرجع (KeyRef) در واسط کارت باید استفاده شود. BIT که در این مثال (به شکل ب-۵ مراجعه شود) اطلاعات مربوط به الگوریتم مرجع خاص کارت (AIgID)، توصیف‌کننده داده‌ی مرجع (KeyRef) و اطلاعات بیشتری از قبیل نوع زیست‌سنجی، مالک قالب و نوع قالب را در برمی‌گیرد.



شکل ب-۵- مثال الگوی اطلاعات زیست‌سنجی (BIT)

اگر IFD و کارت ارائه‌شده، سازوکار مشابهی را پشتیبانی کند و کاربر ویژگی‌های زیست‌سنجی مرتبط را ارائه دهد، داده‌های درستی‌سنجی باید محاسبه شود و با استفاده از دستور VERIFY که پس از دستور MANAGE SECURITY ENVIRONMENT آمده است، برای انتخاب روش درستی‌سنجی خاص تحویل داده شود (به شکل ب-۶ مراجعه شود)

دستور/پاسخ	مفهوم
انتخاب پرونده پسوند FCI	**SELECT** <File ID> OK
بازیابی الگوی اطلاعات الزامات درستی‌سنجی VIT و الگوی اطلاعات زیست‌سنجی BIT	**READ BINARY** VIT || BIT
تنظیم CRT AT با توصیف‌کننده کاربرد UQ، الگوریتم مرجع و کلید مرجع	**MANAGE SE** <DO UQ || DO Alg. Reference || DO Key Reference> OK
درستی‌سنجی کاربر	**VERIFY** <Biometric Verification Data> OK

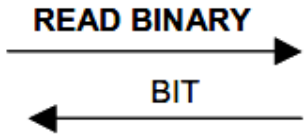
شکل ب-۶ – دستورهای درستی‌سنجی بدون پیام دادن (مثال)

هنگامی که درستی‌سنجی زیست‌سنجی ایستا پیش از درستی‌سنجی به اطلاعات از سوی کارت نیاز دارد، این اطلاعات ممکن است در قالب اطلاعات زیست‌سنجی ارائه شود.

ب-۴ دسترسی به BIT در مورد تطبیق خارج از کارت

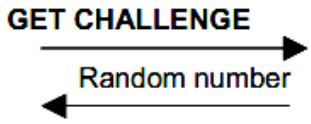
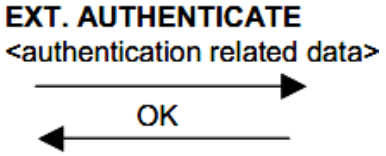
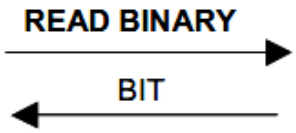
BIT احتمالاً در ترکیب با داده‌های دیگر (به طور مثال داده‌های گواهینامه راننده) ممکن است به طور مثال با امضا مرجع صادرکننده (برای مثال‌های مربوط به حفاظت داده به پیوست ت مراجعه شود) محافظت شود. بنابراین ممکن است BIT با استفاده از دستور READ BINARY ساده بازیابی شود، به شکل ب-۷ مراجعه شود.

دستور/پاسخ	مفهوم
انتخاب پرونده حاوی الگوی اطلاعات زیست‌سنجی	**SELECT** <File ID> OK

شی داده BIT ممکن است حاوی الگوی پیام دادن امن باشد؛ به طور مثال برای تضمین اصالت داده مرجع زیست‌سنجی	

شکل ب-۷ - دستورهای بازیابی BIT (مثال)

دسترسی به BIT ممکن است محدود شده باشد، بدین معنی که قبل از خواندن رویه اصالت‌سنجی باید طبق شکل ب-۸ انجام شود.

دستور/پاسخ	مفهوم
دریافت عدد تصادفی	
اصالت‌سنجی هستاری که حق دسترسی به BIT دارد	
خواندن BIT	

شکل ب-۸ - دستورهای بازیابی BIT پس از انجام رویه اصالت‌سنجی (مثال)

اگر BIT به طور مثال با اینترنت منتقل شود، ممکن است به منظور ارائه محرمانگی و اصالت‌سنجی، همان طور که در شکل ب-۴ نشان داده شده نیاز به پیام دادن امن داشته باشد.

پیوست پ

(اطلاعاتی)

اشیاء داده اطلاعات زیست‌سنجی

این پیوست، اشیا داده اطلاعات زیست‌سنجی را بر اساس چارچوب CBEFF ارائه می‌دهد، به ISO/IEC 19785 مراجعه شود.

پ-۱ کوته‌نوشت‌ها

BDB	Biometric Data Block	بلوک داده زیست‌سنجی
BHT	Biometric Header Template	الگوی سرآیند زیست‌سنجی
BIT	Biometric Information Template	الگوی اطلاعات زیست‌سنجی
CBEFF	Common Biometric Exchange Formats Framework	چارچوب قالب‌های متداول تبادل زیست‌سنجی
DO	Data Object	شی داده
IBIA	International Biometric Industry Association	انجمن بین‌المللی صنایع زیست‌سنجی
IC	Integrated Circuit(s)	مدار(های) مجتمع
MAC	Message Authentication Code	کد اصالت‌سنجی پیام
OID	Object Identifier	شناسانه شی
PID	Product Identifier	شناسانه محصول
SE	Security Environment	محیط امنیتی
SMT	Secure Messaging Template	الگوی پیام دادن امن
TLV	Tag-Length-Value	برچسب- طول- مقدار

پ-۲ اشیا داده اطلاعات زیست‌سنجی به‌کاررفته در حالت تطبیق در کارت

پ-۲-۱ کاربرد نوع زیست‌سنجی واحد یا زیرنوع زیست‌سنجی

قبل از فرآیند درستی‌سنجی، ممکن است که اطلاعاتی از کارت، بازیابی شود که جزییاتی را توسط دنیای خارج در هنگام فرآیند درستی‌سنجی نشان خواهد داد. اشیا داده مرتبط در جدول پ-۱ نشان داده شده است.

جدول پ-۱- اشیا داده اطلاعات زیست‌سنجی در حالت تطبیق در کارت

برچسب	طول	مقدار				وجود
'7F60'	متغیر	الگوی اطلاعات زیست‌سنجی (BIT)				
		برچسب	**طول**	**مقدار**		
		'80'	۱	الگوریتم مرجع برای استفاده در VERIFY / EXT. دستور AUTHENTICATE / MANAGE SE همان طور که در استاندارد ISO/IEC 7816-4 تعریف شده است؛ به یادآوری ۵ مراجعه شود.		اختیاری
		'83'	۱	توصیف‌کننده داده مرجع برای استفاده در VERIFY / EXT. دستور AUTHENTICATE / MANAGE SE همان طور که در استاندارد ISO/IEC 7816-4 تعریف شده است.		اختیاری
		'06'	متغیر	OID در نهاد استاندارد CBEFF		در صورت عدم استفاده از پیش‌فرض اجباری است.
		'A1'	متغیر	الگوی سرآیند زیست‌سنجی (BHT) در تطابق با CBEFF		اجباری
				برچسب	**طول**	**مقدار**
				'80'	۲	نسخه سرآیند پاترون[1] (پیش فرض '0101')	در صورت عدم استفاده از پیش‌فرض اجباری است.
				'90'	متغیر	شاخص، شناسانه منحصر به فرد به کار رفته برای مرجع این مجموعه داده‌های زیست‌سنجی در خارج زمینه برنامه کاربردی کارت	اختیاری
				'81'	۳-۱	نوع زیست‌سنجی، به جدول پ-۲ مراجعه شود.	اختیاری
				'82'	۱	زیرنوع زیست‌سنجی، به جدول پ-۳ مراجعه شود.	اختیاری، فقط استفاده با نوع زیست‌سنجی
				'83'	۷	تاریخ و زمان ایجاد داده زیست‌سنجی (CCYYMMDDhhmmss)	اختیاری
				'84'	متغیر	ایجادکننده	اختیاری
				'85'	۸	دوره اعتبار (از CCYYMMDD تا CCYYMMDD)	اختیاری

1 - Patron

ادامه جدول پ-۱

					‘86’	۲	شناسانه محصول (PID) که داده مرجع زیست‌سنجی را ایجاد کرده است، مقدار توسط IBIA تخصیص یافته است، به www.ibia.org مراجعه شود.	اختیاری
					‘87’	۲	مالک قالب داده درستی‌سنجی زیست‌سنجی، مقدار توسط IBIA تخصیص یافته است، به www.ibia.org مراجعه شود. زیست‌سنجی	اجباری
					‘88’	۲	نوع قالب داده درستی‌سنجی زیست‌سنجی، مشخص‌شده توسط مالک قالب	اجباری
					‘91’ /’B1’	متغیر	پارامترهای الگوریتم تطبیق زیست‌سنجی (اولیه / ساخته‌شده)، به یادآوری ۲ و ۷ مراجعه شود.	اختیاری

یادآوری ۱- فقط آن دسته از اشیا داده CBEFF ای وجود دارند که مربوط به تطبیق در کارت هستند.

یادآوری ۲- شی داده اضافی در ساختار CBEFF اصلی ارائه نشده است.

یادآوری ۳- در جدول پ-۱، بلوک داده‌های زیست‌سنجی طبق تعریف استاندارد ISO/IEC 19785، وجود ندارند، داده‌های مرجع زیست‌سنجی به طور جداگانه در کارت ذخیره شده است و در این BIT نیست و داده‌های درستی‌سنجی زیست‌سنجی باید به طور مثال با استفاده از دستور VERIFY ارائه شود.

یادآوری ۴- در جدول پ-۱ هیچ پایه‌باری[1] وجود ندارد، معمولاً دسترسی به پایه‌بار، در صورتی که توسط برنامه کاربردی استفاده شود، پس از اتمام موفقیت‌آمیز درستی‌سنجی زیست‌سنجی، تضمین می‌شود. ممکن است پایه‌بار با استفاده از دستورهای دسترسی مانند GET DATA یا READ BINARY بازیابی شود.

یادآوری ۵- دنیای بیرون (یعنی IFD) از مالک قالب / نوع قالب برای شناسایی ساختار مورد نیاز برای داده‌های درستی‌سنجی استفاده می‌کند. الگوریتم تطبیق در کارت توسط الگوریتم مرجع ارائه می‌شود.

یادآوری ۶- اگر نسخه ISO استاندارد CBEFF (ISO/IEC 19785) استفاده شود، OID نهاد استاندارد ISO مرتبط (ISO/IEC JTC1/SC37) مقدار پیش فرض است، یعنی ممکن است DO با برچسب '06' وجود نداشته باشد. اگر OID به NISTIR 6529 اشاره کند، OID ثبات اشیای امنیت رایانه (CSOR)[2] در NIST {joint-iso-itu-t (2) country (16) us (840) organization {(3) csor (101) gov (1) استفاده می‌شود (کدگذاری هگزادسیمال OID: ’608648016503‘).

1 - Payload
2 - Computer Security Objects Register

یادآوری ۷- این شی داده هرگونه پارامترهای خاص پیاده‌سازی الگوریتم تطبیق در کارت را ارئه می‌کند، به عنوان مثال بیشینه تعداد مینوشیای مورد انتظار در داده‌های درستی‌سنجی زیست‌سنجی. محتوای این شی داده توسط مالک قالب تعریف می‌شود.

جدول پ-۲- نوع زیست‌سنجی طبق تعریف ISO/IEC 19785

نام نوع زیست‌سنجی	مقدار
اطلاعاتی ارائه نشده است	'00'
زیست‌سنجی چندگانه استفاده شده است	'01'
ویژگی‌های صورت	'02'
صدا	'04'
اثر انگشت	'08'
عنبیه	'10'
شبکیه چشم	'20'
شکل هندسی دست	'40'
پویایی امضا	'80'
پویایی ضربه زدن به کلید	'0100'
حرکت لب	'0200'
تصویر حرارتی صورت	'0400'
تصویر حرارتی دستی	'0800'
طرز راه رفتن	'1000'
بوی بدن	'2000'
DNA	'4000'
شکل گوش	'8000'
هندسه انگشت	'010000'
اثر کف دست	'020000'
الگوی رگ‌ها	'040000'
اثر پا	'080000'
سایر مقادیر RFU	

یادآوری- ممکن است برخی انواع زیست‌سنجی غیر مرتبط با برنامه‌های کاربردی مورداستفاده در کارت باشد.

جدول پ-۳- زیرنوع زیست‌سنجی طبق تعریف ISO/IEC 19785

زیرنوع زیست‌سنجی	b1	b2	b3	b4	b5	b6	b7	b8
اطلاعاتی ارائه نشده است	۰	۰	۰	۰	۰	۰	۰	۰
راست	۱	۰						
چپ	۰	۱						
بدون معنی			۰	۰	۰			
انگشت شست			۱	۰	۰			
انگشت اشاره			۰	۱	۰			

انگشت وسط			۱	۱	۰			

ادامه جدول پ-۳

انگشت حلقه			۰	۰	۱			
انگشت کوچک			۱	۰	۱			
سایر مقادیر RFU								

پ-۲-۲ کاربرد قالب‌های داده‌های زیست‌سنجی استاندارد و اختصاصی

در مواردی که داده‌های درستی‌سنجی زیست‌سنجی، داده‌های درستی‌سنجی زیست‌سنجی با ساختار استاندارد که به دنبال داده‌های درستی‌سنجی زیست‌سنجی با ساختار خاص سازنده می‌آید را شامل شود، ساختار BHT تودرتو باید طبق جدول پ-۴ به کار گرفته شود.

جدول پ-۴ - BIT با BHT های تودرتو برای قالب داده‌های زیست‌سنجی استاندارد و اختصاصی (مثال)

برچسب	طول	مقدار
'7F60'	متغیر	BIT

	برچسب	طول	مقدار
	'80'	۱	الگوریتم مرجع
	'83'	۱	توصیف‌کننده داده مرجع
	'06'	متغیر	OID نهاد استاندارد CBEFF، به یادآوری ۶ جدول پ-۱ مراجعه شود.
	'A1'	متغیر	BHT (سطح ۱)

			برچسب	طول	مقدار
			...		اشیا داده معمول، به جدول پ-۱ مراجعه شود
			'A1'	متغیر	BHT 1 (سطح ۲)

				برچسب	طول	مقدار
				'87'	۲	مالک قالب داده درستی‌سنجی زیست‌سنجی، به طور مثال شناسانه مالک قالب ISO/IEC JTC1/SC37
				'88'	۲	نوع قالب داده درستی‌سنجی زیست‌سنجی، مشخص‌شده توسط مالک قالب
			'A2'	متغیر	BHT 2 (سطح ۲)	
				برچسب	طول	مقدار
				'87'	۲	مالک قالب داده درستی‌سنجی زیست‌سنجی، به طور مثال سازنده کارت
				'88'	۲	نوع قالب داده درستی‌سنجی زیست‌سنجی، مشخص‌شده توسط مالک قالب

پ-۲-۳ کاربرد چندین نوع زیست‌سنجی یا زیرانواع زیست‌سنجی

اگر در داخل یک برنامه کاربردی، از چندین نوع زیست‌سنجی یا زیرانواع زیست‌سنجی به طور مستقل استفاده شود و توسط توصیف‌کننده مختلف داده‌های مرجع (مشابه رمزعبور برای امضا و رمز عبور جداگانه برای اصالت‌سنجی) به آن ارجاع شود، ساختار BIT گروهی با BITهای تودرتو به کار گرفته می‌شود، به جدول پ-۵ مراجعه شود.

جدول پ-۵ – الگوی گروه BITها با بیت‌های تودرتو برای برنامه‌های کاربردی با چندین داده مرجع که دارای توصیف‌کننده داده‌های مرجع خود هستند (مثال)

برچسب	طول	مقدار								
'7F61'	متغیر	قالب گروهی اطلاعات زیست‌سنجی								
		برچسب	طول	مقدار						
		'02'	۱	'02' = تعداد BITها						
		'7F60'	متغیر	BIT 1						
				برچسب	طول	مقدار				
				'80'	۱	الگوریتم مرجع				
				'83'	۱	توصیف‌کننده داده مرجع				
				'06'	متغیر	OID نهاد استاندارد CBEFF، به یادآوری ۶ جدول پ-۱ مراجعه شود.				
				'A1'	متغیر	BHT				
						برچسب	طول	مقدار		
						...				
						'81'	۱-۳	نوع زیست‌سنجی، به طور مثال اثرانگشت		
						'82'	۱	زیرنوع زیست‌سنجی، به طور مثال انگشت اشاره راست		
						'87'	۲	مالک قالب داده درستی‌سنجی زیست‌سنجی		
						'88'	۲	نوع قالب داده درستی‌سنجی زیست‌سنجی، مشخص‌شده توسط مالک قالب		
		'7F60'	متغیر	BIT 2						
				برچسب	طول	مقدار				
				'80'	۱	الگوریتم مرجع				
				'83'	۱	توصیف‌کننده داده مرجع				
				'06'	متغیر	OID نهاد استاندارد CBEFF، به یادآوری ۶ جدول پ-۱ مراجعه شود.				

				'A1'		متغیر	BHT	

ادامه جدول پ-۵

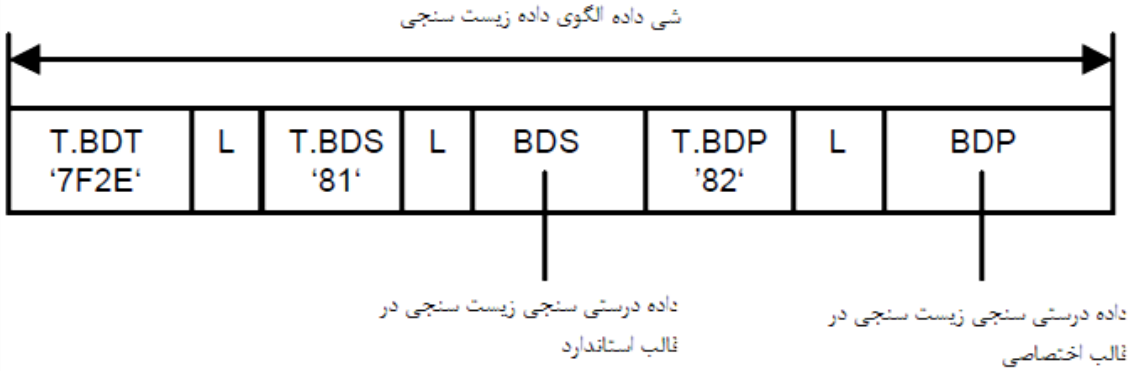
							برچسب	طول	مقدار
							...		
							'81'	۳-۱	نوع زیست‌سنجی، به طور مثال اثرانگشت
							'82'	۱	زیرنوع زیست‌سنجی، به طور مثال انگشت اشاره راست
							'87'	۲	مالک قالب داده درستی‌سنجی زیست‌سنجی
							'88'	۲	نوع قالب داده درستی‌سنجی زیست‌سنجی، مشخص‌شده توسط مالک قالب

پ-۲-۴ کاربرد زیست‌سنجی‌های چندگانه

در مواردی که چندین ویژگی زیست‌سنجی (از جهت زیست‌سنجی چندگانه یا ترکیبی) باید درستی‌سنجی شود، به طور مثال به منظور دسترسی به داده‌های معین یا کلید خاص، BIT گروهی با BITهای تودرتو به کار گرفته می‌شود و درستی‌سنجی با ارسال به عنوان مثال چندین دستور VERIFY انجام می‌شود. شرایط دسترسی متصل به شی محافظت‌شده مرتبط تعریف می‌کند که ترکیبی از ویژگی‌های زیست‌سنجی باید با موفقیت درستی‌سنجی شود.

پ-۲-۵ ارائه داده‌های درستی‌سنجی زیست‌سنجی

کدگذاری و قالب دستورها برای درستی‌سنجی زیست‌سنجی که داده‌های درستی‌سنجی زیست‌سنجی را به کارت منتقل می‌کند در ISO/IEC 7816-4 بیان شده است. امکانات کدگذاری برای فیلد داده دستور در بند ۶-۲ استاندارد ISO/IEC 7816-11 بیان شده است. شکل پ-۱ مثالی از فیلد داده دستور مربوط به مثال ارائه‌شده در جدول پ-۴ را نشان می‌دهد.



شکل پ-۱ - الگوی داده زیست‌سنجی در فیلد داده دستور (مثال)

پ-۳ اشیا داده اطلاعات زیست‌سنجی به کار رفته در مورد تطبیق خارج از کارت

پ-۳-۱ ساختار و کاربرد کلی

اشیا داده برای تطبیق خارج از کارت که به عنوان BIT ارائه شده، شامل موارد زیر است:

— الگوی سرآیند زیست‌سنجی BHT،

— بلوک داده زیست‌سنجی BDB شامل داده‌های مرجع زیست‌سنجی که احتمالاً به دنبال پایه‌بار می‌آید و

— اشیا داده احتیاطی مربوط به امنیت، به بند ۳-۴ مراجعه شود.

استفاده از ساختارهای داده ارائه‌شده در بندهای بعدی به کارت‌های IC محدود نمی‌شود، یعنی ممکن است ساختار داده‌ها در انواع دیگر کارت، به عنوان مثال کارت‌های نوار مغناطیسی، کارت‌های حافظه نوری یا کارت‌های دارای رمزینه ۲ بعدی مورد استفاده قرار گیرد.

پ-۳-۲ کاربرد نوع زیست‌سنجی واحد یا نوع فرعی زیست‌سنجی

در جدول پ-۷، اشیا داده مربوط به تطبیق در خارج از کارت، در صورت استفاده از نوع واحد یا زیرنوع زیست‌سنجی مشخص شده است.

جدول پ-۷ - اشیا داده اطلاعات زیست‌سنجی مورد استفاده در تطبیق خارج از کارت

<table>
<tr><th>برچسب</th><th>طول</th><th colspan="4">مقدار</th><th>وجود</th></tr>
<tr><td>‘7F60’</td><td>متغیر</td><td colspan="4">الگوی اطلاعات زیست‌سنجی (BIT)</td><td></td></tr>
<tr><td></td><td></td><td>برچسب</td><td>طول</td><td colspan="2">مقدار</td><td></td></tr>
<tr><td></td><td></td><td>‘06’</td><td>متغیر</td><td colspan="2">OID نهاد استاندارد CBEFF، به یادآوری ۶ جدول پ-۱ مراجعه شود.</td><td>در صورت عدم استفاده از پیش‌فرض اجباری است.</td></tr>
<tr><td></td><td></td><td>‘A1’</td><td>متغیر</td><td colspan="2">الگوی سرآیند زیست‌سنجی (BHT) در تطابق با CBEFF</td><td>اجباری</td></tr>
<tr><td></td><td></td><td></td><td>برچسب</td><td>طول</td><td>مقدار</td><td></td></tr>
<tr><td></td><td></td><td></td><td>’80’</td><td>۲</td><td>شماره نسخه سرآیند پاترون (پیش‌فرض ‘0101’)</td><td>در صورت عدم استفاده از پیش‌فرض اجباری است.</td></tr>
<tr><td></td><td></td><td></td><td>‘90’</td><td>متغیر</td><td>زیست‌سنجی شاخص، شناسانه منحصر به فرد به کار رفته برای مرجع این مجموعه داده‌های زیست‌سنجی در خارج زمینه برنامه کاربردی کارت</td><td>اختیاری</td></tr>
<tr><td></td><td></td><td></td><td>‘81’</td><td>۱-۳</td><td>نوع زیست‌سنجی، به جدول پ-۲ مراجعه شود.</td><td>اختیاری</td></tr>
</table>

ادامه جدول پ-۷

			‘82’			۱	زیر نوع زیست‌سنجی، به جدول پ-۳ مراجعه شود.	اختیاری، فقط با نوع زیست سنجی استفاده می‌شود.
			‘83’			۷	تاریخ و زمان ایجاد داده زیست‌سنجی (CCYYMMDDhhmmss)	اختیاری
			‘84’			متغیر	ایجادکننده	اختیاری
			‘85’			۸	طول دوره اعتبار (از CCYYMMDD به CCYYMMDD)	اختیاری
			‘86’			۲	شناسانه محصول (PID) که داده مرجع زیست‌سنجی را ایجاد می‌کند، مقدار توسط IBIA تخصیص داده می‌شود، به www.ibia.org مراجعه شود.	اختیاری
			‘87’			۲	مالک قالب داده درستی‌سنجی زیست‌سنجی، مقدار توسط IBIA تخصیص داده می‌شود، به www.ibia.org مراجعه شود.	اجباری
			‘88’			۲	نوع قالب داده درستی‌سنجی زیست‌سنجی، مشخص‌شده توسط مالک قالب	اجباری
		'5F2E' /'7F2E'	متغیر	داده مرجع زیست‌سنجی (اولیه/ساخته‌شده، به جدول پ-۸ مراجعه شود)				اجباری
		'53' / '73'	متغیر	داده احتیاطی برای پایه‌بار (اولیه/ساخته‌شده، به یادآوری ۲ و ۳ مراجعه شود)				اختیاری

یادآوری ۱- فقط آن اشیا داده از CBEFF ارائه‌شده که مربوط به تطبیق خارج از کارت هستند.

یادآوری ۲- شی داده اضافی در حال حاضر در ساختار CBEFF اصلی نیست.

یادآوری ۳- پایه‌بار در صورت موفقیت درستی‌سنجی برای دنیای بیرون در دسترس خواهد بود (به مشخصات BioAPI مراجعه شود).

تفاوت اصلی در جدول پ-۱ این است که اشیا داده برای الگوریتم مرجع و توصیف‌کننده داده مرجع (کلید مرجع که توسط کارت استفاده می‌شود) وجود ندارد و به جای آن بلوک داده زیست‌سنجی (BDB)، شامل داده مرجع زیست‌سنجی و احتمالاً یک پایه‌بار متصل، به دنبال الگوی سرآیند زیست‌سنجی (BHT) می‌آید.

همچنین ممکن است بلوک امضا (SB) نیز وجود داشته شود، امـا در تطـابق بـا ISO/IEC 7816 کدگـذاری می‌شود، به بند پ-۳-۴ مراجعه شود.

جدول پ-۸ – الگوی داده زیست‌سنجی

برچسب	طول	مقدار		
'7F2E'	متغیر	الگوی داده زیست‌سنجی		
		اشیا داده‌ای که ممکن است در الگوی داده زیست‌سنجی تعبیه شود.		
		برچسب	طول	مقدار
		'80'/ 'A0'	متغیر	چالش برای عکس‌العمل کاربر (اولیه/ساخته‌شده، به جدول پ-۹ مراجعه شود) این شی داده فقط به نوع زیست‌سنجی پویا مربوط است.
		'81'/ 'A1'	متغیر	داده زیست‌سنجی با ساختار استاندارد (اولیه/ساخته‌شده)
		'82' / 'A2'	متغیر	داده زیست‌سنجی با ساختار اختصاصی (اولیه/ساخته‌شده)

جدول پ-۹ - الگوی چالش

برچسب	طول	مقدار		
'A0'	متغیر	الگوی چالش		
		اشیای داده‌ای که ممکن است در الگوی چالش، تعبیه شود.		
		برچسب	طول	مقدار
		'90'	متغیر	توصیف‌کننده چالش '00'= اطلاعاتی ارائه نشده است (نا مشخص) '01'= کدگذاری UTF8 (پیش‌فرض) RFU سایر مقادیر
		'80'	متغیر	چالش

پ-۳-۳ کاربرد ساختارهای تودرتو

در جدول پ-۱۰، مثالی از کاربرد ساختارهای تودرتو بیان شده است. تفاوت اصلی با جدول پ-۵ ایـن اسـت که اشاره‌گر به داده‌های مرجع زیست‌سنجی (به عنوان مثال توصیف‌کننده داده‌های مرجع) با خود داده‌هـای مرجع زیست‌سنجی جایگزین شده است.

جدول پ-۱۰ - الگوی گروهی BIT با BIT های تودرتو برای برنامه‌های کاربردی با داده‌های مرجع زیست‌سنجی از چندین نوع زیست‌سنجی (مثال)

برچسب	طول	مقدار				
'7F61'	متغیر	الگوی گروهی اطلاعات زیست‌سنجی				
		برچسب	طول	مقدار		
		'02'	۱	تعداد BITها در الگوی گروهی		
		'7F60'	متغیر	BIT 1		
				برچسب	طول	مقدار

ادامه جدول پ-۱۰

					متغیر	OID نهاد استاندارد CBEFF، به یادآوری ۶ جدول پ-۱ مراجعه شود.
					متغیر	BHT
				برچسب	**طول**	**مقدار**
				'81'	۳-۱	نوع زیست‌سنجی، به طور مثال ویژگی‌های صورت
				'87'	۲	مالک قالب داده مرجع زیست‌سنجی
				'88'	۲	نوع قالب داده مرجع زیست‌سنجی، مشخص‌شده با مالک قالب
				'5F2E'	متغیر	داده مرجع زیست‌سنجی
			'7F60'	BIT 2	متغیر	
				برچسب	**طول**	**مقدار**
				'06'	متغیر	OID نهاد استاندارد CBEFF، به یادآوری ۶ جدول پ-۱ مراجعه شود.
				'A1'	متغیر	BHT
				برچسب	**طول**	**مقدار**
				'81'	۳-۱	نوع زیست‌سنجی، به طور مثال اثرانگشت
				'82'	۱	زیرنوع زیست‌سنجی، به طور مثال انگشت اشاره چپ
				'87'	۲	مالک قالب داده مرجع زیست‌سنجی
				'88'	۲	نوع قالب داده مرجع زیست‌سنجی، مشخص‌شده توسط مالک قالب
				'5F2E'	متغیر	داده مرجع زیست‌سنجی

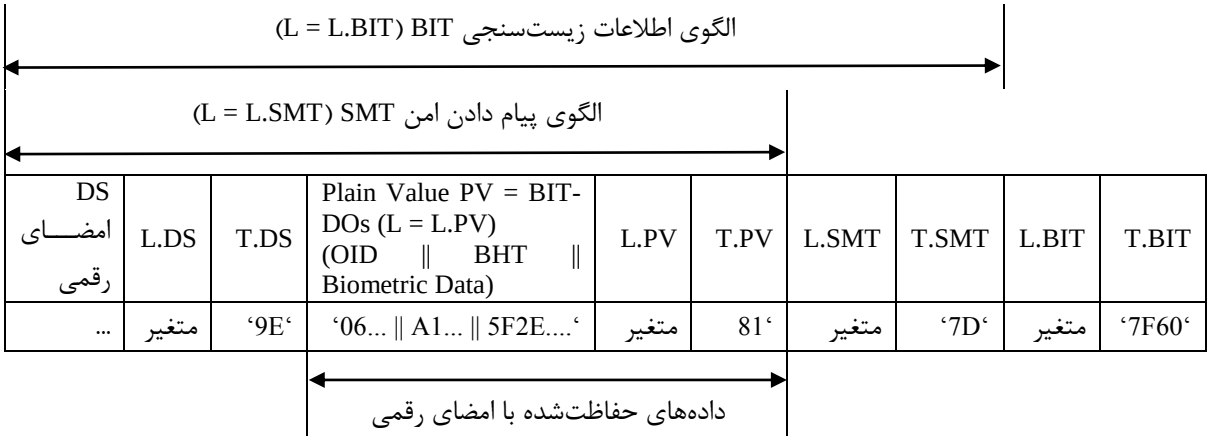
پ-۳-۴ موضوعات امنیتی

برخی احتمالات، از جمله چگونگی امن‌سازی BIT یا چگونگی اجازه دسترسی به BIT و انتقال آن به روشی امن در پیوست ب و پیوست ت بیان شده است. ویژگی‌های امنیتی توضیح داده شده در ISO/IEC 19785 با توجه به:

— اشاره به گزینه‌های امنیتی

— اشاره به گزینه‌های یکپارچگی
— ارائه فیلدی برای امضا یا MAC

به طور کامل با استفاده از الگوی پیام دادن امن (SMT)[1] و اشیای داده مرتبط (به پیوست ت مراجعه شود) پشتیبانی می‌شود. نیازی به اشاره به گزینه‌های امنیتی و یکپارچگی در دو فیلد خاص در BHT نیست چون وجود رمزنگاشت، امضای رقمی یا MAC با برچسب‌های مرتبط نشان داده شده است. مثالی ساده از استفاده SMT در شکل پ-۲ نشان داده شده است. علاوه بر این، مثال‌های پیچیده‌تر در پیوست ت ارائه شده است.



شکل پ-۲ - الگوی اطلاعات زیست‌سنجی امن (مثال)

پ-۴ اطلاعات ثبت‌نام IBIA

تطابق با CBEFF، نیازمند ثبت‌نام مالکان قالب با IBIA برای تخصیص شناسانه منحصر به فرد به مالک قالب است. انواع قالب توسط مالک قالب تخصیص داده می‌شود و قالب داده‌های زیست‌سنجی خاص همان طور که توسط مالک قالب مشخص شده، نشان داده می‌شود. توصیه می‌شود که مالکان قالب، انواع قالب را برای مقاصد بایگانی و نشر در استفاده با IBIA ثبت کنند. همچنین IBIA مقادیر ID محصول را ثبت‌نام می‌کند (به جدول پ-۱ و پ-۷ مراجعه شود). منحصر به فرد بودن شماره‌ها تضمین شده است.

IBIA مقادیر بین 'FFF0' تا 'FFFE' را برای مالکان قالب و شناسانه‌های محصول تخصیص نمی‌دهد. این مقادیر برای آزمون هستند.

برای اطلاعات ثبت‌نام به www.ibia.org مراجعه شود.

1 - Secure Messaging Template

پیوست ت

(اطلاعاتی)

کاربرد الگوهای پیام دادن امن

ت-۱ کوته‌نوشت‌ها

BD	Biometric Data	داده زیست‌سنجی
BER	Basic Encoding Rules	قواعد کدگذاری پایه
BHT	Biometric Header Template	الگوی سرآیند زیست‌سنجی
BIT	Biometric Information Template	الگوی اطلاعات زیست‌سنجی
CC	Cryptographic Checksum	جمع‌آزمای رمزنگاشتی
CCT	Cryptographic Checksum Template	الگوی جمع‌آزمای رمزنگاشتی
CT	Confidentiality Template	الگوی محرمانه
CG	Cryptogram	رمزنگاشت
DE	Data Element	عنصر داده
DO	Data Object	شی داده
DS	Digital Signature	امضای رقمی
DST	Digital Signature Template	الگوی امضای رقمی
KR	Key Reference	کلید مرجع
L	Length	طول
MAC	Message Authentication Code	کد اصالت‌سنجی پیام
PD	Personal Data	داده شخصی
PDT	Personal Data Template	الگوی داده شخصی
PV	Plain Value	مقدار داده آشکار
SM	Secure Messaging	پیام دادن امن
SMT	Secure Messaging Template	الگوی پیام دادن امن
T	Tag	برچسب
TLV	Tag-Length-Value	برچسب- طول- مقدار
||	Concatenation	الحاق

ت-۲ پیام دادن امن مرتبط با اشیا داده و کاربرد آن‌ها

در صورت استفاده کارت به عنوان حامل BIT ممکن است نیاز به حفاظت از الگوی اطلاعات زیست‌سنجی BIT باشد. (همچنین به NISTIR 6529 و ANSI X9.84 مراجعه شود):

— BIT با حریم خصوصی (رمزگذاری)

— BIT با یکپارچگی (امضاشده یا MACed)

— BIT با حریم خصوصی و یکپارچگی.

ابزار حریم خصوصی و یکپارچگی در زمینه کارت با پیام دادن امن (SM) طبق تعریف ISO/IEC 7816-4 ارائه می‌شود. ۲ روش وجود دارد:

۱) قبل از خواندن BIT، کلیدهای SM برای بایگانی حریم خصوصی و یکپارچگی به صورت پویا با انتقال کلید یا سازوکارهای توافق کلید، مستقر می‌شود.

۲) BIT به خودی خود به روشی ایستا، امن می‌شود، به طور مثال با به کارگیری فن الگوی SM همان طور که در زیر شرح داده شده است.

اگر فیلد مقدار BIT باید به روشی ایستا امن شود، فیلد مقدار در یک الگو SM تعبیه می‌شود، که در آن:

— تمام اشیا داده‌ای که به عنوان متن آشکار باقی مانده‌اند در الگوی مقادیر آشکار قرار داده می‌شود.

— تمام اشیا داده‌ای که باید رمز شود در رمزنگاشتی گذاشته می‌شود.

و در صورتی که یکپارچگی لازم باشد، شی داده جمع‌آزمای رمزنگاشتی یا شی داده امضای رقمی وجود دارند. اگر اشیا داده مانند الگوریتم مرجع و کلید مرجع سامانه خدمت را برای درستی‌سنجی یکپارچگی قادر سازد و بازیابی مقدار آشکار داده رمزشده مورد نیاز باشد، این موارد در الگوهای مرجع کنترل معرفی خواهند شد (به شکل ت-۱ مراجعه شود).

شکل ت-۱ - الگوی اطلاعات زیست‌سنجی در ترکیب با SMT

کدگذاری اشیا داده مرتبط با الگو پیام دادن امن SMT در جدول ت-۱ نشان داده شده است.

جدول ت-۱ - اشیا دادهSMT (زیر مجموعه)

برچسب	طول	مقدار		
'7D'	متغیر	الگوی پیام دادن امن SMT		
		برچسب	طول	مقدار
		'xx'	متغیر	الگوی مرجع کنترل، به جدول ت-۲ مراجعه شود (اصالت‌سنجی حفاظت‌شده)
		'81'	متغیر	مقدار آشکار (PV)، شامل ترتیب DEها یا BER-TLV کدشده با اشیا داده، بدون SM مربوط به اشیا داده، به یادآوری مراجعه شود (اصالت‌سنجی حفاظت‌شده)
		'85'	متغیر	رمزنگاشتی (CG)، مقدار آشکار)، شامل ترتیب DEها یا BER-TLV کدشده با اشیا داده، بدون SM مربوط به اشیا داده، (اصالت‌سنجی حفاظت‌شده)
		'8E'	متغیر	جمع‌آزمای رمزنگاشتی(CC)، مثال کد اصالت‌سنجی پیام (MAC)
		'9E'	متغیر	امضای رقمی (DS)

یادآوری- از دیدگاه SM، مقدار آشکار، همیشه مقدار اولیه است.

الگوی پیام دادن امن ممکن است الگوهای مرجع کنترل زیر را شامل شود:

— الگوی جمع‌آزمای رمزنگاشتی (CCT)

— الگوی امضای رقمی (DST)

— الگوی محرمانگی (CT).

الگوهای مرجع کنترل حاوی اشیا داده بیشتر هستند، به طور مثال برای مشخص کردن الگوریتم و کلید مرجع (به جدول ت-۲ مراجعه شود).

جدول ت-۲ - الگوهای مرجع کنترل و اشیا داده مرتبط (زیر مجموعه)

برچسب	طول	مقدار		
'B5'	متغیر	الگوی جمع‌آزمای رمزنگاشتی (CCT)		
'B7'	متغیر	الگوی امضای رقمی (DST)		
'B9'	متغیر	الگوی محرمانگی (CT)		
		اشیا داده مرتبط با CCT، DST و CT		
		برچسب	طول	مقدار
		'80'	متغیر	الگوریتم مرجع
		'83'	متغیر	- ارجاع به کلید مخفی برای استفاده مستقیم - ارجاع به کلید عمومی (مرتبط با الگوریتم‌های نامتقارن)
		'84'	متغیر	- ارجاع به کلید مخفی برای اقتباس کلید - ارجاع به کلید خصوصی (مرتبط با الگوریتم‌های نامتقارن)

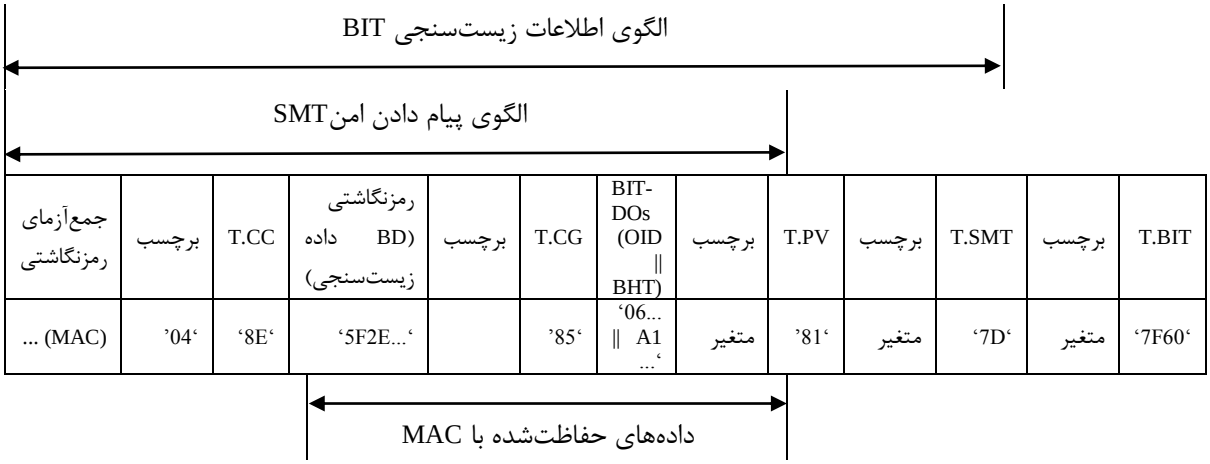
یادآوری- اشیا داده بیشتر در ISO/IEC 7816-4 مشخص شده است.

ت-۳ مثال‌های رمزگذاری

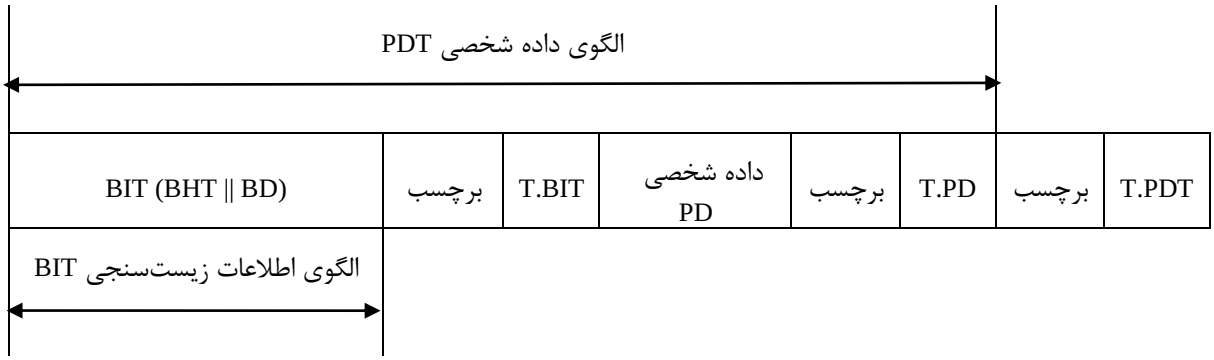
مثال‌های رمزگذاری موارد زیر را نشان می‌دهد:

— الگوی اطلاعات زیست‌سنجی که در آن اشیا داده اطلاعات زیست‌سنجی (سرآیند زیست‌سنجی) به دنبال یک رمزنگاشتی حاوی داده‌های زیست‌سنجی می‌آیند و هر دو توسط MAC حفاظت می‌شود (به شکل ت-۲ مراجعه شود) و

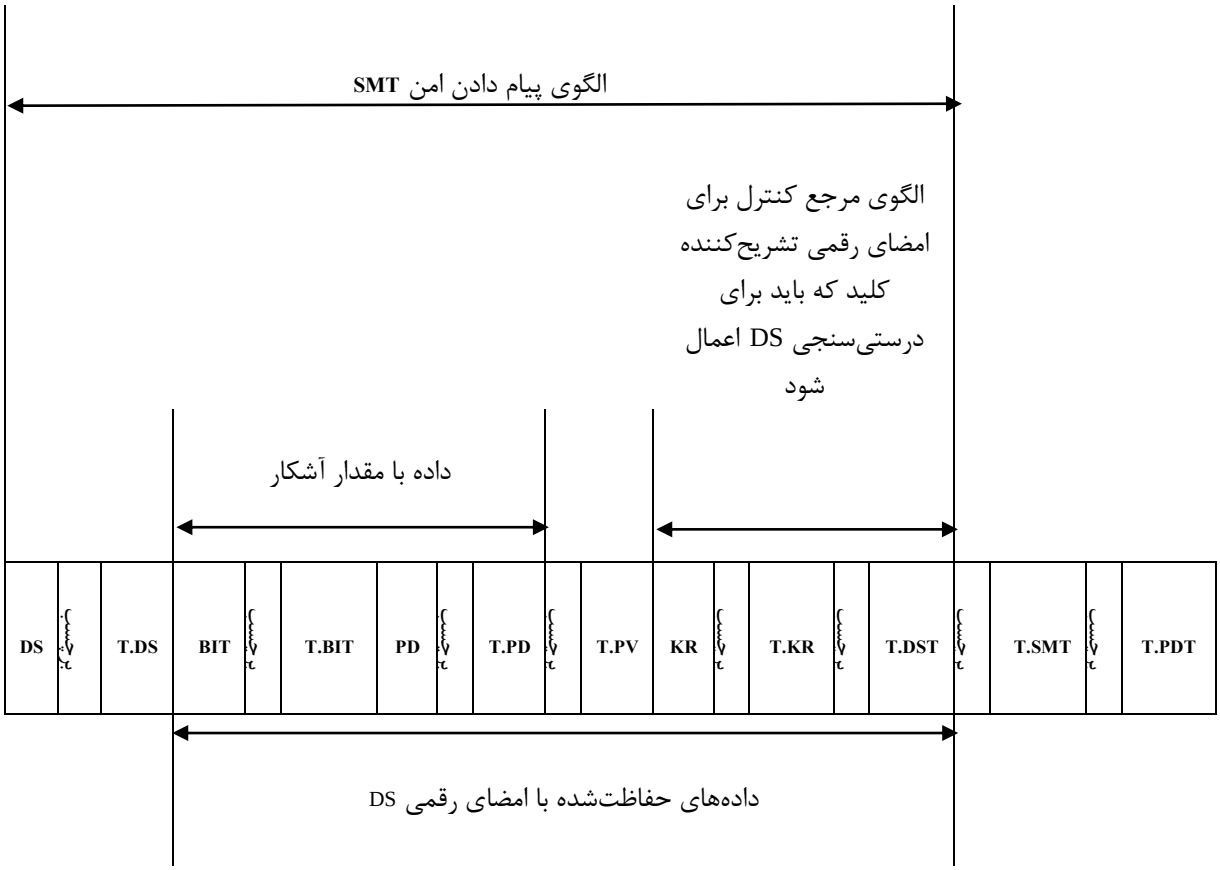
— برخی انواع داده‌های برنامه‌های کاربردی (به طور مثال داده‌های فردی برای شناسایی) با الگوی اطلاعات زیست‌سنجی ترکیب شده و با روش‌های دیگر امن شده است (به شکل‌های ت-۳ تا ت-۵ مراجعه شود).



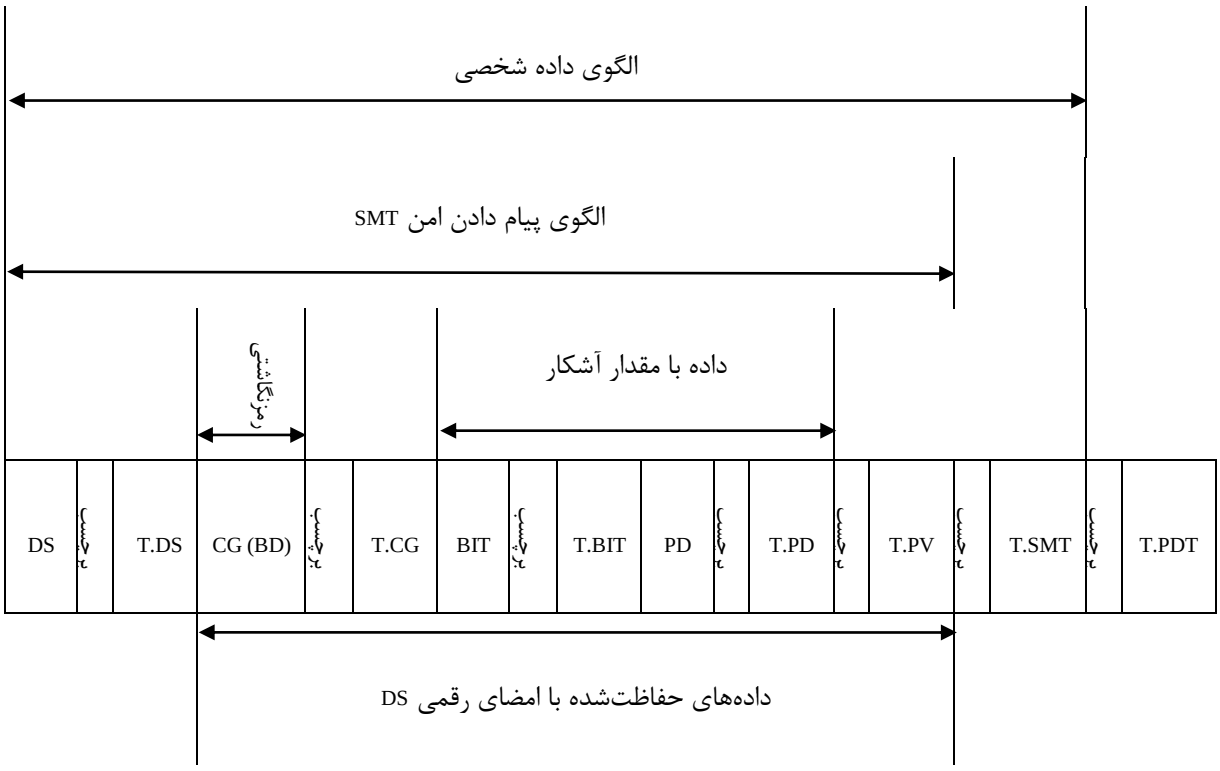
شکل ت-۲ – الگوی BIT با SMT تعبیه‌شده (مثال)



شکل ت-۳ – الگوی داده شخصی با BIT (مثال)



شکل ت-۴ - الگوی داده شخصی با BIT حفاظت شده توسط امضای رقمی (مثال)



شکل ت-۵ - الگوی داده‌های فردی حفاظت‌شده با امضای رقمی و حاوی رمزنگاشتی کنار سایر اشیا داده برای داده‌های زیست‌سنجی (مثال)

کتاب‌نامه

[1] ISO/IEC 7816 Identification cards – Integrated circuit cards – All parts

[2] ISOIEC 19784 BioAPI Specification

[3] ANSI X9.84-2001 Biometric Information Management and Security

[4] NISTIR 6529-A Common Biometric Exchange Format Framework