INSO
21949-1
1st.Edition
2017
Identical with
ISO/IEC 25185-1:2016

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران
۲۱۹۴۹-۱
چاپ اول
۱۳۹۶

کارت‌های شناسایی- پروتکل (قرارداد)های اصالت‌سنجی کارت مدار یکپارچه- قسمت ۱: پروتکل اصالت‌سنجیِ سبُک برای شناسه

Identification cards — Integrated circuit card authentication protocols — Part 1: Protocol for Lightweight Authentication of Identity

ICS: 35.240.15

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.gov.ir

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 .gov.ir

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 توجه 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

«کارت‌های شناسایی- پروتکل (قرارداد)های اصالت‌سنجی کارت مدار یکپارچه- قسمت ۱: پروتکل اصالت‌سنجیِ سبُک برای شناسه»

رئیس:	سمت و/ یا محل اشتغال:
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات- سیستم‌های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون مدیر کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
تهرانی، محمد (کارشناسی ارشد فناوری اطلاعات)	مدیر کارت و خدمات نوین– بانک قوامین
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
عباسپور، مقصود (دکتری مهندسی کامپیوتر- معماری)	دانشیار– معاون مرکز فناوری دانشگاه شهید بهشتی
طی نیا، رضا (کارشناسی ارشد فناوری اطلاعات)	مدیر عامل– شرکت مهندسی کاربرد سیستم (کاسیس)
مطلق، کامبیز (کارشناسی ارشد فناوری اطلاعات)	معاون فناوری اطلاعات– بانک قوامین
مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران
ناظمی، اسلام (دکتری مهندسی کامپیوتر)	دانشیار- دانشگاه شهید بهشتی

اعضاء : (اسامی به ترتیب حروف الفبا)

	سمت و/ یا محل اشتغال:
نصیری آسایش، حمیدرضا (کارشناسی ارشد فناوری اطلاعات- معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات- معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی

ویراستار:	**سمت و/ یا محل اشتغال:**
معروف، سینا (لیسانس مهندسی کامپیوتر، سخت‌افزار)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «کارت‌های شناسایی- پروتکل (قرارداد)های اصالت‌سنجی کارت مدار یکپارچه- قسمت ۱: پروتکل اصالت‌سنجیِ سبُک برای شناسه» که پیش نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شمارهٔ ۵ تهیه و تدوین شده، در چهارصد و نود و سومین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۶/۰۲/۱۱ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 25185-1: 2016, Identification cards — Integrated circuit card authentication protocols: — Part 1: Protocol for Lightweight Authentication of Identity

کارت‌های شناسایی- پروتکل (قرارداد)های اصالت‌سنجی کارت مدار یکپارچه- قسمت ۱: پروتکل اصالت‌سنجیِ سبُک برای شناسه

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین قرارداد اصالت‌سنجی مناسب برای استفاده در سامانه‌های واپایش دسترسی فیزیکی و منطقی بر اساس کارت‌های مدار یکپارچه (ICCs)[1] و سامانه‌های مرتبط با آن‌ها است که از استانداردهای مبتنی بر رمزهای AES-128 و RSA-2048 و الگوریتم چکیده‌ساز SHA-256 پشتیبانی می‌کنند.

این استاندارد، قرارداد اصالت‌سنجی سبُک برای شناسه (PLAID) و پیاده‌سازی آن را با جزئیات کافی مشخص می‌کند، تا این امکان را فراهم سازد که دو یا چند پیاده‌سازی، قابلیت همکاری داشته باشند.

این استاندارد، به چگونگیِ به اشتراک‌گذاریِ کلیدهای رمزنگاشتی[2]، سوابق اعتباری سامانه‌های واپایش دسترسی (ازجمله ابطال) یا مدیریت هستارهای پایه‌بار[3] مانند PIN، PINHash و یا الگوهای زیست‌سنجشی[4] یا دیگر اشیاء پایه‌بار، در پیاده‌سازی‌ها نمی‌پردازد.

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 محسوب می‌شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

3-1 ISO/IEC 7816-4, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange

3-2 ISO/IEC 7816-5, Identification cards — Integrated circuit cards — Part 5: Registration of application providers

1- Integrated Circuit Card
2- Cryptographic keys
3- Payload
4- Biometric

یادآوری- استاندارد ملی ایران شماره ۵-۸۲۳۲: سال ۱۳۸۷، کارت‌های شناسایی- کارت‌های مدار مجتمع– قسمت ۵: ثبت فراهم کنندگان برنامه‌کاربردی، با استفاده از استاندارد ISO/IEC 7816-5:2004 تدوین شده است.

3-3 ISO/IEC 8824-1, Information technology — Abstract Syntax Notation One (ASN.1) — Part 1: Specification of basic notation

یادآوری- استاندارد ملی ایران شماره ۱-۸۸۲۴: سال ۱۳۹۰، فناوری اطلاعات- نشانه‌گذاری قاعده‌ی نحوی انتزاعی یک (ASN.1) – قسمت ۱: ویژگی نشانه‌گذاری پایه، با استفاده از استاندارد ISO/IEC 8824-1:2008 تدوین شده است.

3-4 ISO/IEC 9797-1, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher

یادآوری- استاندارد ملی ایران شماره ۱-۹۷۹۷: سال ۱۳۹۰، فناوری اطلاعات- فنون امنیتی- کدهای احراز هویت پیام (MACs) – قسمت ۱: سازوکارهای استفاده از رمزگذاری بستکی، با استفاده از استاندارد ISO/IEC 9797-1:2011 تدوین شده است.

3-5 ISO/IEC 10116, Information technology — Security techniques — Modes of operation for an n-bit block cipher

یادآوری- استاندارد ملی ایران شماره ۹۶۰۰: سال ۱۳۸۶، فناوری اطلاعات- روش‌های امنیتی- حالت‌های عملیاتی یک الگوریتم رمزنگاری قطعه‌ای n بیتی، با استفاده از استاندارد ISO/IEC 10116:2006 تدوین شده است.

3-6 ISO/IEC 10118-3, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions

یادآوری- استاندارد ملی ایران شماره ۳-۹۵۹۸: سال ۱۳۹۱، فناوری اطلاعات- فنون امنیتی- توابع درهم ساز -قسمت ۳: توابع درهم ساز اختصاصی، با استفاده از استاندارد ISO/IEC 10118-3:2004 تدوین شده است.

3-7 ISO/IEC 18033-2, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers

3-8 ISO/IEC 18033-3, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers

یادآوری- استاندارد ملی ایران شماره ۳-۱۰۸۲۴: سال ۱۳۸۷، فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمز نگاری- قسمت ۳: رمزهای بستکی، با استفاده از استاندارد ISO/IEC 18033-3:2005 تدوین شده است.

3-9 IETF RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

۳ اصطلاحات وتعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در استانداردهای ISO/IEC 7816-4، ISO/IEC 7816-5، ISO/IEC 8824-1، ISO/IEC 10116، ISO/IEC 10118-3، ISO/IEC 18033-2،

ISO/IEC 18033-3 و IETF RFC 3447 اصطلاحات و تعاریف زیر نیز به‌کار می‌رود.

۴ نمادها و کوته‌نوشت‌ها

||	Logical concatenation of bit strings	الحاق منطقی رشته‌های بیتی
ACS	Access Control System	سامانه واپایش دسترسی
AES	Advanced Encryption Standard (as defined in ISO/IEC 18033-3)	استاندارد رمزگذاری پیشرفته (مطابق تعریف استاندارد ISO / IEC 18033-3)
AES $_{\text{Decrypt}}^{\text{Key}}$	Perform AES Decryption using Key	انجام رمزگشایی AES با استفاده از کلید
AES $_{\text{Encrypt}}^{\text{Key}}$	Perform AES Encryption using Key	انجام رمزگذاری AES با استفاده از کلید
AID	Application IDentifier (as defined in ISO/IEC 7816-4)	شناسانه نرم‌افزار (مطابق تعریف استاندارد ISO / IEC 7816-4)
AP	Authentication Protocol (as defined in ISO/IEC 24727-3)	قرارداد اصالت‌سنجی (مطابق تعریف استاندارد ISO/IEC 24727-3)
APDU	Application Protocol Data Unit (as defined is ISO/IEC 7816-4)	واحد داده‌های قرارداد کاربرد (مطابق تعریف استاندارد ISO / IEC 7816-4)
ASN.1	Abstract Syntax Notation Number 1 (as defined in ISO/IEC 8824-1)	نشانه‌گذاری نحوی انتزاعی، شماره ۱
BER	Basic Encoding Rules of ASN.1 (as defined in ISO/IEC 8825-1)	قواعد کدبندی عمومیASN.1 (مطابق تعریف ا مطابق تعریف استاندارد ISO/IEC 8825-1)
CBC	Cipher Block Chaining (as defined in ISO/IEC 10116)	سَبک زنجیره‌ایِ بستک‌های رمز (مطابق تعریف استاندارد ISO/IEC 10116)
CLA	Class Byte (as defined in ISO/IEC 7816-4)	بایت رده (مطابق تعریف استاندارد ISO/IEC 7816-4)
CRT	Chinese Remainder Theorem	قضیه باقیمانده چینی
DivData	Diversification Data — Seed data used in cryptographic operations	داده‌های تنوع‌بخشی ـــ داده‌های مورد استفاده در عملیات رمزنگاشتی
eSTR	Encrypted version of data object (STR in this case)	نسخه رمزگذاری‌شده داده‌ها (در این مورد STR)
FA	Final Authenticate	اصالت‌سنجی نهایی

IA	Initial Authenticate	اصالت‌سنجی اولیه
ICC	Integrated Circuit Card, logically equivalent in this International Standard to PICC	کارت مدار یکپارچه، در این استاندارد از لحاظ منطقی، معادل باPICC
IFD	InterFace Device	افزاره واسط
INS	Instruction Byte (as defined in ISO/IEC 7816-4)	بایت دستورالعمل (مطابق تعریف استاندارد ISO/IEC 7816-4)
IV	Initialisation Vector	بردار اولیه
Key(DIV)	Diversified version of key	نسخه متنوع کلید
KeySetID	A 2 byte value specifying which keyset the protocol will negotiate or use	یک مقدار ۲ بایتی مشخص‌کننده اینکه کدام مجموعه کلید را قرارداد استفاده خواهد کرد
LACS	Logical Access Control System	سامانه واپایش دسترسی منطقی
OpModeID	A 2 byte value specifying which operational mode the protocol will use	یک مقدار ۲ بایتی مشخص‌کننده اینکه کدام حالت عملیاتی را قرارداد استفاده خواهد کرد.
PACS	Physical Access Control System	سامانه واپایش دسترسی فیزیکی
PICC	Proximity Integrated Circuit Card, logically equivalent to ICC in this International Standard	مجاورت کارت مدار یکپارچه، به لحاظ منطقی معادل با ICC در این استاندارد
PIN	Personal Identification Number	شماره شناسایی شخصی
PKI	Public-Key Infrastructure	زیرساخت کلید عمومی
PKCS1.5	RSA padding method (as defined in IETF RFC 3447)	روشPadding RSA (مطابق تعریف IETF RFC 3447)
PLAID	Protocol for Lightweight Authentication of IDentity	قرارداد اصالت‌سنجی سبُک برای شناسه
RNG	Random Number Generator	مولد عدد تصادفی
RSA	Asymmetric cryptographic cipher (as defined in ISO/IEC 18033-2)	رمزنگاری نامتقارن (مطابق تعریف استاندارد ISO/IEC 18033-2)
$RSA_{Decrypt}^{Key}$	Perform RSA Decryption using Key	انجام رمزگشایی RSA با استفاده از کلید
$RSA_{Encrypt}^{Key}$	Perform RSA Encryption using Key	انجام رمزگذاری RSA با استفاده از کلید
SHA	Secure Hash Algorithm (as defined in ISO/IEC 10118-3)	الگوریتم چکیده‌ساز امن (مطابق تعریف استاندارد ISO/IEC 10118-3)
SW1-SW2	Status Bytes (as defined in ISO/IEC 7816-4)	بایت‌های وضعیت (مطابق تعریف استاندارد ISO/IEC 7816-4)

TLV	Tag, Length, Value
UID	Unique IDentifier
UUID	Open credential numbering system (as defined in IETF RFC 4122)
Wiegand	PACS credential numbering system based on Wiegand effect card readers from the 1980s

برچسب، طول، مقدار

شناسانه منحصربه‌فرد

سامانه شماره‌گذاری اعتبارنامه باز (مطابق تعریف IETF RFC 4122)

سامانه شماره‌گذاری اعتبارنامه PACS بر اساس کارت‌خوان‌های اثر Wiegand از سال ۱۹۸۰

۵ فرهنگ لغات داده‌ها

جدول ۱، اندازه و جزئیات اشیاء داده‌های PLAID را تعریف می‌کند.

جدول ۱- فرهنگ لغات داده‌ها

نام شی	هدف	اندازه	نوع داده	توضیحات
ACSRecord	سابقه سامانه واپایش دسترسی	متغیر یادآوری- توصیه می‌شود ACSRecord به علاوه پایه‌بار از ۶۴ بیت تجاوز نکند مگر اینکه بازبینی خطای انتقال ثانویه مانند CMAC پیاده‌سازی شود	باز	سابقه سامانه واپایش دسترسی برای هر شناسانه حالت عملیاتی پشتیبانی شده به‌منظور اجازه و ابطال توسط سامانه‌های ستادی واپایش دسترسی PACS یا LACS.. این سابقه توسط OpModeID به سامانه شماره‌گذاری ستادی خاص که قرارداد پشتیبانی می‌کند، نگاشت می‌شود. این سابقه توسط پاسخ فرمان اصالت‌سنجی نهایی بازگشت داده می‌شود.
DivData	داده‌های تنوع‌بخشی کلید متقارن	۱۲۸ بیت	دودویی	یک مقدار اولیه که در طول توانمندسازی PLAID برای استفاده در الگوریتم تنوع‌بخشی کلید برای حصول اطمینان نسبت به از دست دادن کلید متقارن ICCخاص نمی‌تواند به نقض کلیدهای اصلی سامانه منجر شود. این مقدار اولیه توسط مالک کلید تعیین می‌شود و توصیه می‌شود این مقدار اولیه ترجیحا در هر PLAID ICC و

نام شی	هدف	اندازه	نوع داده	توضیحات
				در هر سامانه، تصادفی یا منحصربه‌فرد باشد.
FAKey	کلید اصالت‌سنجی نهایی غیر متنوع	۱۲۸ بیت	دودویی	کلید اصلی AES غیر متنوع
$FAKey^{(DIV)}$	کلید اصالت‌سنجی نهایی متنوع (AES-128)	۱۲۸ بیت	دودویی	کلید مشتق‌شده از FAKey توسط فرایند مشخص تنوع‌بخشی
IV	بردار مقداردهی اولیه	۱۶ بایت	دودویی	تمام بیت‌های بردار IV باید به بیت صفر(۰) تنظیم شود.
IAKey	کلید اصالت‌سنجی اولیه (RSA-2048)	۲۰۴۸ بیت	دودویی	نمونه‌ای از جفت کلید اصالت‌سنجی RSA اولیه.
KeySetID	به صورت منحصربه‌فرد شناسایی می‌کند keysetکه شامل می‌شود FAKey(div)و جفت IAKey	۲ بایت	دودویی	یک یا دو شناسانه بایت اضافی فرستاده شده در فهرست به ICC در فرمان اصالت‌سنجی اولیه طوری که برای تعیین و / یا مذاکره keyset برای اصالت‌سنجی استفاده می‌شود.
OpModeID	شناسانه حالت	۲ بایت	دودویی	شناسانه فرستاده شده به ICC در فرمان اصالت‌سنجی نهایی که تعیین می‌کند کدام ACSRecord و پایه‌بار در پاسخ

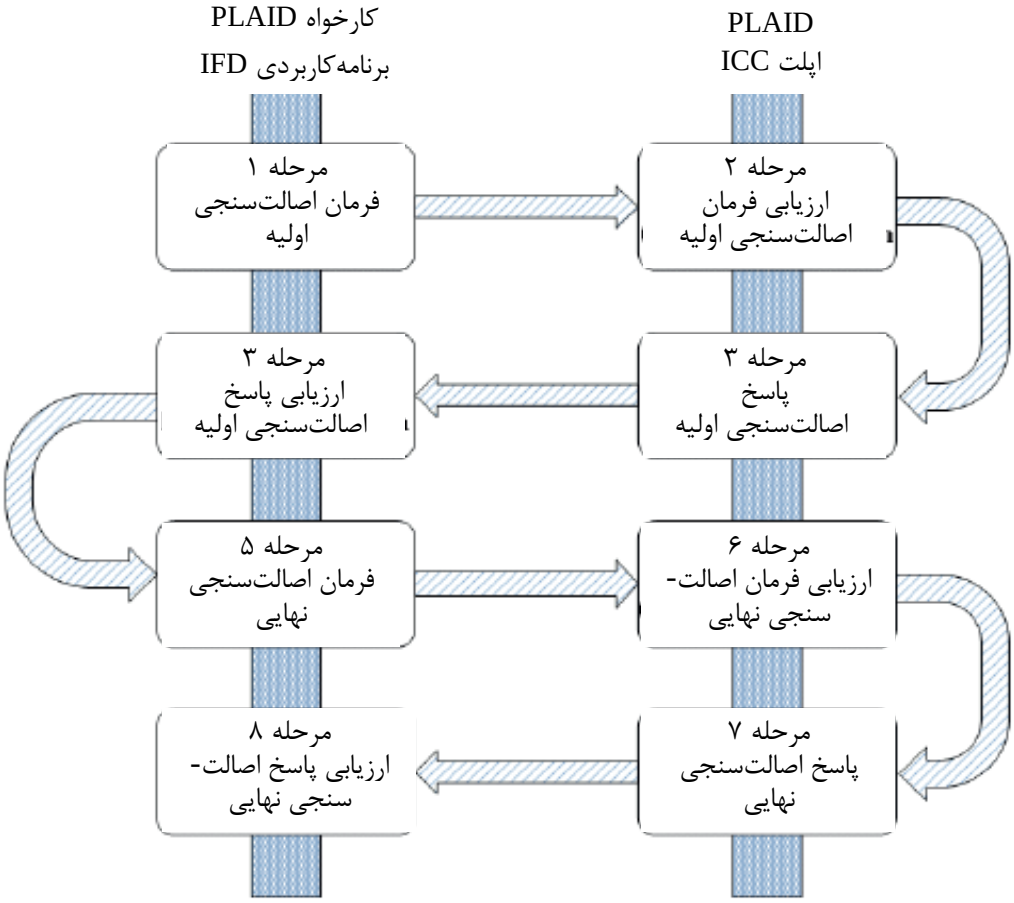
نام شی	هدف	اندازه	نوع داده	توضیحات
	عملیاتی			اصالت‌سنجی نهایی از ICC عبور داده می-شود.
Payload	انتقال داده‌های توسعه‌پذیر مربوط به کاربر	متغیر **یادآوری**- توصیه می‌شود در نمونه پاسخ نهایی اصالت‌سنجی، سابقه ACSRecord به علاوه پایه‌بار از ۶۴ بیت تجاوز نکند مگر اینکه انتقال بازبینی خطاهایی مانند CMAC پیاده‌سازی شده باشد.	باز	ظرفی برای حمل داده‌های اختیاری .پایه‌بار همیشه به مقدار OpModeID مرتبط است.
RND1	عدد تصادفی ۱	۱۶ بایت	دودویی	عدد تصادفی تولید شده توسط ICC با استفاده ازRNG
RND2	عدد تصادفی ۲	۱۶ بایت	دودویی	عدد تصادفی تولید شده توسط IFDیا سامانه back officeبا استفاده از RNG
STR1	اولین شی بدنه APDU	۵۰ بایت	دودویی	درونی فقط برایICC
^{e}STR1	نسخه RSA-2048 رمزنگاری‌شد ه اولین رشته APDU	۲۵۶ بایت	RSA-2048 رمزنگاری شده دودویی	RSAمنتقل شده، رمزنگاری می‌شود.

نام شی	هدف	اندازه	نوع داده	توضیحات
STR(2,3)	دومین و سومین شی APDU	متغیر	دودویی	درونی فقط برایICC/IFD
^{e}STR(2,3)	نسخه AES رمزنگاری‌شد ه دومین و سومین شی APDU	متغیر	AES رمزنگاری شده دودویی	AES منتقل شده، رمزنگاری می‌شود.
KeysHash	چکیده کلید	۱۲۸ بیت	دودویی	رشته تولید شده توسط IFD و ICC به‌طور جداگانه محاسبه می‌کند SHA-256[RND1|RND2]. بیت‌های خروجی اضافی انتهایی باید به طول مورد نیاز کوتاه شود.
SessionKey	کلید جلسه	۱۲۸ بیت	دودویی	کلید ایجاد شده توسط IFD و ICC که به صورت جداگانه KeysHash را محاسبه می‌کند.
ShillKey	Shill key (RSA/ AES)	به ترتیب RSA، ۲۰۴۸ بیت و AES، ۱۲۸ بیت)	دودویی	کلید Shill به‌طور تصادفی توسط ICC ایجاد شده و تنها برای برنامهICC شناخته شده است. کلید shill ایجاد می‌شود هم برای فرمان‌های اصالت‌سنجی اولیه (RSA) و هم برای فرمان‌های اصالت‌سنجی نهایی(AES) تولید می‌شود. کلید Shill توسط ICC در محل کلید واقعی استفاده می‌شود زمانی که خطا در پاسخ شناسایی شده باشد، در نتیجه هرگونه نشانه برای مهاجم بالقوه که خطا تشخیص داده شده است را از بین می‌برد.

یادآوری– ترتیب جریان بایت در تمام اشیای داده‌ای big-endian است.

۶ توصیف قرارداد اصالت‌سنجی

این بند، مراحل مربوط به اصالت‌سنجی دوجانبه PLAID شامل موارد استفاده واپایش دسترسی فیزیکی یا منطقی را مورد بحث قرار می‌دهد. شکل ۱ این فرایند را نشان می‌دهد.



شکل ۱- مرور کلی قرارداد اصالت‌سنجی PLAID

مراحل لازم برای انجام اصالت‌سنجی دوجانبه با استفاده از PLAID باید به شرح زیر باشد:

۱-۶ مرحله ۱ - فرمان اصالت‌سنجی اولیه

الف) افزارهٔ IFD، درخواست اولیه اصالت‌سنجی APDU، جهت حصول داده‌های تنوع‌بخشی (DivData)، را به ICC می‌فرستد.

ب) بدنه APDU شامل فهرست کامل مقادیر مجاز KeySetID (کدبندی به‌صورت BER-TLV) که توسط IFD شناخته شده‌اند می‌شود.

پ) این فهرست ابتدا باید توسط KeySet بیشتر ترجیح داده‌شده و سپس توسط مقادیر KeySetID ترجیح داده‌شده، مرتب شده باشد.

ت) نمایش رسمی ASN.1 از بدنه اصالت‌سنجی اولیه APDU به صورت زیر است:

```
PLAID {iso(1) standard(1) iccap(25185) part1(1) plaid(1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

KeySetID ::= OCTET STRING (SIZE (2))

KeySetIDSequence ::= SEQUENCE OF

KeySetID

END
```

یادآوری ۱- کدبندی BER-TLV تنها در مورد فرمان اصالت‌سنجی اولیه استفاده می‌شود.

یادآوری ۲- مقادیر KeySetID به‌وضوح توسط IFS تصویب شده و توصیه می‌شود امن در نظر گرفته نشود.

۶-۲ مرحله ۲ - ارزشیابی فرمان اصالت‌سنجی اولیه

الف) کارت ICC فهرست BER-TLV از مقادیر KeySetID را جدا[1] کرده و اولین IAKey یافت شده را که منطبق بر KeySetID است و توسط ICC پشتیبانی می‌شود، بازیابی می‌کند.

ب) کارت ICC باید فهرست کامل مقادیر KeySetID را صرف نظر از هنگامی که تطابق با keyset یافت می‌شود، بررسی کند. این امر منجر به جلوگیری از حملات بالقوه زمان‌بندی می‌شود.

پ) اگر هیچ یک از مقادیر KeySetID مشخص شده با کلید ذخیره شده توسط ICC منطبق نشوند، آنگاه ICC، مشابه مرحله ۳، با استفاده از رشته بایت تصادفی با ShillKey رمزگذاری شده، پاسخ می‌دهد، در نتیجه از هرگونه نشانه‌ای که به معنای بروز خطا باشد، جلوگیری می‌کند.

۶-۳ مرحله ۳ - پاسخ اصالت‌سنجی اولیه

الف) کارت ICC، مقدار تصادفی (RND1) با استفاده از RNG خودش تولید می‌کند. اندازه RND1 با اندازه کلیدِ رمز AES-128 انتخاب شده (۱۶ بایت) یکسان است.

ب) کارت ICC، داده‌های متنوع (DivData) منحصربه‌فرد را بازیابی می‌کند.

پ) کارت ICC، رشته بیتی STR1: RND1 || RND1 || DivData || KeySetID را ایجاد می‌کند.

1- Parse

ت) کارت ICC، رشته بیتی $^{e}STR1$ که در آن $^{e}STR1 = RSA_{Encrypt}^{IAKey}(STR1)$ را محاسبه می‌کند. این رمزگذاری تنها از پیمانه و نمای عمومی IAKey استفاده می‌کند. کدهای ساختگی PKCS1.5 باید در رمزگذاری گنجانده شوند.

ث) کارت ICC، رشته $^{e}STR1$ را به IFD انتقال می‌دهد.

۶-۴ مرحله ۴ - ارزیابی پاسخ اصالت‌سنجی اولیه

الف) افزارهٔ IFD، رشته $^{e}STR1$ را دریافت کرده و STR1 که در آن $STR1 = RSA_{Decrypt}^{IAKey}(^{e}STR1)$ را با استفاده از مقادیر KeySetID مشخص شده در فهرست، محاسبه می‌کند.

ب) افزارهٔ IFD دو نسخه RND1 را برای تمام مقدار مقایسه می‌کند تا تایید شود که رمزگشایی موفق بوده است.

پ) توصیه می‌شود IFD، فهرست کامل KeySetID را، صرف نظر از زمانی که اولین رمزگشایی موفق انجام شده، بررسی کرده و مقادیر KeySetID موفق را ذخیره کند. این به‌منظور جلوگیری از حملات بالقوه زمان-بندی به کار می‌رود.

ت) اگر تمام مقادیر KeySetID استفاده شده و رمزگشایی انجام نشود، اصالت‌سنجی شکست خورده است. توجه داشته باشید که ممکن است همان کلیدهای نامتقارن در مجموعه چند کلید برای پیاده‌سازی‌های بزرگ استفاده شوند.

ث) افزارهٔ IFD، ICC داده‌های تنوع‌بخشی DivData و مقدار KeySetID را از اولین رمزگشایی STR1 موفق استخراج می‌کند.

۶-۵ مرحله ۵ - فرمان اصالت‌سنجی نهایی

الف) افزارهٔ IFD مقداری تصادفی (RND2) با استفاده از RNG تولید می‌کند. اندازه RND2 با اندازه کلید رمز AES-128 انتخاب شده (۱۶ بایت) یکسان است.

ب) افزارهٔ IFD، SHA-256 [RND1||RND2] را محاسبه کرده و نتیجه به‌عنوان KeysHash مشخص می‌شود.

پ) افزارهٔ IFD داده‌های تنوع‌بخشی (DivData) را استفاده کرده و کلید اصالت‌سنجی نهایی متنوع را که در آن $FAKey^{(Div)} = AES_{Encrypt}^{FAKey}(DivData)$ محاسبه می‌کند. FAKey مورد استفاده، توسط KeySetID شناسایی شده به‌عنوان موفقیت در ارزیابی اولیه پاسخ IA اشاره می‌شود.

ت) افزارهٔ IFD، رشته بیتی STR2 را ایجاد می‌کند: OpModeID || RND2 || <Payload> || KeysHash

ث) در صورت نیاز، padding باید شامل مجموعه بایت اجباری 0x80، در صورت لزوم به دنبال مجموعه ۰ تا K-1 بایت تا 0x00، باشد تا زمانی که بستک داده‌های مربوطه، مطابق با استاندارد ISO/IEC 9797-1 روش padding ۲ ، تا k بایت پر شود.

ج) افزارهٔ IFD، $^{e}STR2$ را که در آن (STR2) $eSTR2 = AES_{Encrypt}^{FAKey(Div)}$ محاسبه می‌کند. حالت رمزنگاری برای این عملیات CBC است.

چ) افزارهٔ IFD رشته نهایی اصالت‌سنجی $^{e}STR2$ را به ICC انتقال می‌دهد.

۶-۶ مرحله ۶ - ارزیابی فرمان اصالت‌سنجی نهایی

الف) کارت ICC، STR2 که در آن: $(^{e}STR2)$ $STR2 = AES_{Decrypt}^{FAKey(Div)}$ است، محاسبه می‌کند. FAKey(Div) مورد استفاده توسط KeySetID در پاسخ IA اولیه اشاره می‌شود.

ب) کارت ICC، KeysHash را به صورت SHA-256 [RND1 || RND2] با استفاده از RND1 ایجاد شده در مرحله فرمان قبلی IA و RND2 استخراج شده از STR2 محاسبه می‌کند.

پ) کارت ICC، KeysHash را با KeysHash استخراج شده از STR2 مقایسه می‌کند. اگر عدم تطابق مشاهده شود آنگاه ICC، با استفاده از رشته بایت تصادفی رمز شده با ShilKey پاسخ داده و در نتیجه از هرگونه نشانه‌ای که بیان کننده خطا باشد، جلوگیری می‌کند.

ت) اگر پایه‌بار اختیاری ارسال شود، آنگاه رمزگشایی‌شده و در صورت نیاز بر اساس مقررات پیاده‌سازی، پردازش می‌شود.

۶-۷ مرحله ۷ - پاسخ اصالت‌سنجی نهایی

الف) کارت ICC، زمینه‌های مناسب را بر اساس OpModeID استخراج شده از STR2 بازیابی می‌کند. این امر به‌طور معمول Wiegand مناسب، شماره‌های ID و یا UUID خواهد بود.

ب) کارت ICC، رشته بیتی STR3 را ایجاد می‌کند: ACSRecord || <Payload>|| DivData

پ) در صورت نیاز، padding باید شامل مجموعه بایت اجباری 0x80 و در صورت لزوم، سپس مجموعه ۰ تا K-1 بایت تا 0x00 باشد، تا زمانی که بستک داده‌های مربوطه، مطابق با استاندارد ISO/IEC 9797-1 روش padding ۲، تا k بایت پر شود.

ت) کارت ICC، $^{e}STR3$ را که در آن: (STR3) $^{e}STR3 = AES_{Encrypt}^{KeysHash}$ است، محاسبه می‌کند. حالت رمزنگاری برای این عملیات باید CBC باشد.

ث) کارت ICC، رشته نهایی اصالت‌سنجی $^{e}STR3$ را به IFD انتقال می‌دهد.

۸-۶ مرحله ۸ - ارزشیابی پاسخ اصالت‌سنجی نهایی

الف) افزارهٔ IFD، STR3 را که در آن: $STR3 = AES_{Decrypt}^{KeysHash}(^{e}STR3)$ است، محاسبه می‌کند.

ب) افزارهٔ IFD، DivData منتقل شده را با نسخه IFD دریافت شده در پاسخ IA مقایسه می‌کند. اگر آن‌ها با هم مطابقت نداشته باشند، اصالت‌سنجی شکست می‌خورد.

پ) اکنون ACSRecord و Payload از STR3 استخراج شده و اکنون می‌توانند تایید شده در نظر گرفته شوند.

ت) اکنون Payload اختیاری ممکن است در صورت نیاز بر اساس مقررات پیاده‌سازی پردازش شود.

ث) اکنون ACSRecord ممکن است به هر کجا که سامانه back office مناسب باشد برای بازبینی بازگشت و سپس باز کردن درب و یا بخشی از فرایند بیشتر، منتقل شود. معنی دقیق تامین امنیت سابقه فراتر از این نقطه، خارج از محدوده این استاندارد است.

ج) قراردادهای اصالت‌سنجی و یا قراردادهای دسترسی کارت بیشتر ممکن است KeysHash تولید شده را به صورت اختیاری به‌عنوان پیام‌رسانی امن، جلسه یا کلید رمزنگاری در جلسات بعدی، استفاده کنند. حالت رمزنگاری برای این عملیات باید CBC باشد.

۷ شناسایی برنامه‌کاربردی

برنامه PLAID باید توسط موارد زیر انتخاب شود:

الف) فراخوانی PLAID عمومی AID پیش‌فرض به‌طور مستقیم در "E0 28 81 C4 61 01"، و یا

ب) تنظیم PLAID به‌عنوان برنامه پیش‌فرض، یا

پ) ثبت مدیریت طرح AID خاص برای طرح خاص با توجه به استاندارد ISO/IEC 7816-5 با استفاده از استاندارد ثبت صلاحیت ISO / IEC ذکر شده در:

standards_development/maintenance_agencies.htm.http://www.iso.org/iso/

اگرچه تنها یک نرم‌افزار پیش‌فرض در ICC می‌تواند وجود داشته باشد، تا زمانی که AID مناسب به صراحت فراخوانی شود، ممکن است بیش از پیاده‌سازی در هر کارت یا کارت‌خوان پشتیبانی شود.

۸ مجموعه فرمان‌ها

در زیر، فرمان‌های خاص استاندارد ISO / IEC 7816-4، که مطابق با این استاندارد هستند، مورد نیاز هستند. این فرمان‌های، فرمان عمومی اصالت‌سنجی را در دو حالت استفاده می‌کنند. فرمان‌های IA و FA، مقادیر INS مربوطه را که به ترتیب نشان دهنده رمزهای RSA و AES موجود در عملیات عمومی اصالت‌سنجی ISO / IEC 7816-4 هستند، مشخص می‌کنند.

جدول ۲- مجموعه فرمان استاندارد ISO/IEC 7816-4

عملیات	CLA	INS	مقدار P1	مقدار P2	مقدار LC	SL
اصالت‌سنجی اولیه	0x00	0x87	0x00	0x00	0x00	BER-TLV
اصالت‌سنجی نهایی	0x00	0x86	0x00	0x00	متغیر	داده‌های دودویی رمزگذاری

یادآوری- طول پاسخ APDU استاندارد ۲۵۶ بایت، توسط مقدار 0x00 برای LC با طول کوتاه، تحت استاندارد ISO / IEC 7816-4 پشتیبانی می‌شود. یادآوری‌های جدول ۱ را ملاحظه نمایید. این امر، نیاز به APDU اضافی را حذف می‌کند.

۹ بایت‌های وضعیت و سامان‌دهی خطا

کدهای خطا باید مطابق با استاندارد ISO / IEC 7816-4 باشند. به‌منظور حفاظت از فاش شدن هویت و به کمینه رساندن اطلاعات مفید موجود برای مهاجم، در جریان عملیات PLAID، بر اساس استاندارد ISO / IEC 7816-4، نباید کدهای خطای وضعیت بایت ایجاد شوند. چنین بایت‌های وضعیتی نشان می‌دهند که تناقض یا تلاش ناموفق رخ داده است. در عوض، ICC باید برای تکمیل عملیات و بازگشت بایت وضعیت SW_OK، از کلید ShillKey استفاده کند.

جدول ۳- بایت‌های وضعیت

نام کد خطا	مقدار SW1-SW2	توضیحات
SW_OK	0x9000	به استاندارد ISO/IEC 7816-4 مراجعه شود.

۱۰ تنوع‌بخشی کلید

قرارداد PLAID برای اطمینان از اینکه سامانه امن باقی خواهد ماند، از تنوع‌بخشی کلیدهای متقارن AES بهره می‌گیرد، توصیه می‌شود ICC مشخص در خطر کشف رمز قرار گرفته و کلیدهای مخفی آن تعیین

شوند. الگوریتم مورد استفاده برای تنوع‌بخشیدن به FAKey به شرح زیر است:

$$FAKey^{(DIV)} = AES_{Encrypt}^{FAKey}(DivData)$$

۱۱ ایجاد کلید جلسه

قرارداد PLAID منجر به ایجاد کلید نشست AES می‌شود که ممکن است به صورت اختیاری برای ارتباطات بعدی با ICC استفاده شود. اندازه این کلید نشست توسط اندازه کلید رمز AES انتخاب شده، تعیین می‌شود. در حال حاضر تنها سه اندازه کلید مجاز پشتیبانی شده توسط AES (۱۶، ۲۴ یا ۳۲ بایتی) وجود دارند. ازآنجا که AES از بستک‌های ۱۲۸ بیتی (۱۶ بایتی) برای رمزگذاری / رمزگشایی استفاده می‌کند، padding ممکن است در بستک بعدی لازم باشد. روند مورد استفاده برای ایجاد کلید جلسه به شرح زیر است:

$$SessionKey\ (KeysHash) = SHA\text{-}256\ [RND1 \parallel RND2]$$

الگوریتم چکیده‌ساز پیش‌فرض، SHA-256 است. الگوریتم چکیده‌ساز مورد استفاده به تولید پیامی که منطبق بر اندازه کلید رمز AES انتخاب شده باشد، نیاز دارد. جایی که این امر امکان‌پذیر نباشد، الگوریتم چکیده‌ساز تولیدکننده پیامی بزرگ‌تر از اندازه کلید AES، با بایت‌های خروجی اضافی کوتاه شده به‌اندازه طول مورد نیاز، استفاده می‌شود.

۱۲ حالت پیش‌فرض

ممکن است PLAID با تعدادی از گزینه‌های مربوط به تفاوت رمزها و حالت‌های رمزها یا الگوریتم‌های چکیده‌ساز پیاده‌سازی شود.

جدول ۴ حالت پیش‌فرض عملیات و رمزهایی که توصیه می‌شود توسط پیاده‌سازی با استفاده از AID ‘E0 28 81 C4 61 01’ پیش‌فرض و ایجاد قابلیت همکاری، استفاده شود، نشان می‌دهد.

جدول ۴- حالت پیش‌فرض

رمزگذاری متقارن	طول کلید (بیت)	AES Padding	حالت AES	رمزگذاری متقارن	طول کلید (بیت)	RSA padding	گزینه RSA	الگوریتم چکیده-ساز
AES	128	ISO/IEC 9797-1 padding method 2	CBC (به یادآوری مراجعه شود)	RSA	2048	PKCS 1.5	CRT	SHA-256

یادآوری- تنوع‌بخشی کلید DivData تحت AES از بستک داده استفاده می‌کند و در نتیجه هیچ حالتی لازم نیست.

پیوست الف

(الزامی)

بردارهای آزمون

این پیوست، با استفاده از حالت‌های پیش‌فرض بحث شده در بند ۱۲، و بر اساس مراحل شماره‌گذاری شده در شکل ۱، بردارهای آزمون برای PLAID را تعریف می‌کند.

با توجه به حجم زیاد بردارهای دودویی آزمون RSA-2048، AES-128 و SHA-256، و احتمال اشتباهات جابجایی در انتشار و جابجایی آن‌ها برای استفاده‌های بعدی، محتوای این پیوست در پرونده rtf. جداگانه در آدرس زیر ارائه شده است: http://standards.iso.org/iso/25185/-1/.

پیوست ب

(آگاهی‌دهنده)

خط‌مشی مدیریت کلید

درحالی‌که روش‌های خاص برای مدیریت کلید، خارج از دامنه کاربرد این استاندارد است، هر پیاده‌سازی بدون خط‌مشی مدیریت کلید کافی می‌تواند به خطر بیافتد.

قرارداد PLAID، با اغلب APهای دیگر تفاوت دارد، زیرا ترکیبی از رمزنگاری متقارن و نامتقارن بوده و اصالت‌سنجی را به صورت متقابل انجام می‌دهد نه فقط اصالت‌سنجی «خارجی» (از نقطه نظر کارت).

به‌منظور محافظت از حملات مستقیم و پنهان، پس از اولین IFD APDU، هیچ داده‌ای عبور نکرده و تنها داده قابل حصول آزادانه، فهرست IFDهای مقادیر KeySetID (داده‌هایی که برای بسیاری از پیاده‌سازی‌ها می‌شود آشکار از محل reader در هر مورد) است.

مراحل اولیه اصالت‌سنجی از رمز نامتقارن و یا یک طرفه استفاده می‌کنند. این امر تنوع ICC (DivData) و اولین عدد تصادفی (RND1) را از قرار گرفتن نمایان شدن، حفاظت می‌کند. اصالت‌سنجی نهایی، اصالت‌سنجی کلید متقارن شبیه به دیگر قراردادهای اصالت‌سنجی بدون تماس رایج است.

از این رو این قرارداد اصالت‌سنجی ترکیبی، از اصالت‌سنجی PKI معمول‌تر، بسیار متفاوت است حتی اگر هر دو از رمزهای نامتقارن استفاده کنند. نقش کلیدهای RSA عمومی و خصوصی در PLAID متفاوت از PKI است.

به این دلیل که اصالت‌سنجی اولیه برای PLAID (برای اولین بار)، ثابت می‌کند که ICC، تنها اطلاعات شناخته شده برای IFD را می‌شناسد تا اطلاعات شناخته شده توسط ICC. در بار دوم (اصالت‌سنجی نهایی) این مشاهده معکوس می‌شود.

در اثر کلیدهای عمومی و خصوصی RSA، به اندازه کلیدهای AES، به امن بودن توسط هم on-card applet و هم reader نیاز است. بنابراین توصیه می‌شود این کلیدها همان‌طور که کلید متقارن مشترک هستند، مدیریت شوند.

بنابراین توصیه می‌شود خط‌مشی مدیریت کلید، از ذخیره‌سازیِ تمامی کلیدها در پیمانه‌های رمزنگاشتی امن، از قبیل ICCهای تایید شده، پیمانه‌های واپایش امنیت، یا متخصص پیمانه‌های امنیت اطمینان سخت‌افزار و هم‌چنین در قسمت ستاد، با سامانه‌های قدرتمند مدیریت کلید که ترجیحا دارای پشتیبانی رمزنگاشتی سخت‌افزاری هستند، حاصل نماید.

یادآوری- دستیابی به این سطح از امنیت در پیمانه‌های سخت‌افزاری به‌تازگی با ICC کم‌هزینه بسیار ساده‌تر شده و تراشه-های SAM و IFD در دسترس قرار می‌گیرند که تایید شده است هر دو به صورت محلی می‌توانند PLAID و مدیریت کلید آن را حمایت کنند. نمونه‌هایی از کد مورد نیاز برای این ابزارها می‌توانند از پیاده‌سازی مرجع PLAID بارگیری شوند (به پیوست ت مراجعه شود).

پیوست پ

(آگاهی‌دهنده)

مدیریت مجموعه کلید

این استاندارد اجازه بیش از ۶۵۵۳۵ مجموعه کلید تعیین شده توسط سابقه ۲ بایتی KeySetID را می‌دهد. در نتیجه، با توجه به حافظه ICC، ممکن است ICC، کمینه تعداد دو و در صورت عملی بودن تعداد بیشتری از مجموعه کلید پشتیبانی کند. این استاندارد همچنین از مذاکرات مجموعه کلیدها پشتیبانی می‌کند، که در آن IFD، در فرمان اصالت‌سنجی اولیه، در ترتیب ترجیحی، فهرست مجموعه کلیدها به ICC داده شده و ICC، ارجح‌ترین Keyset را از مجموعه یا مجموعه‌هایی که بارگذاری کرده است، به کار می‌برد. این امر امکان می‌دهد که سطوح مختلف اعتماد و قابلیت همکاری، بسته به نیازهای کسب‌وکار پیاده‌سازی، به دست آیند. این امر ممکن است ساخت‌وساز، ساختار مبتنی بر نقش یا کارکرد مجموعه کلیدها و یا ترکیبی از این-ها و یا سایر عوامل باشد. به‌عنوان مثال، پیاده‌سازی ممکن است مجموعه کلیدهای زیر را استفاده کند:

جدول ۵- مدیریت مجموعه کلیدها

راهبری	Keyset = 0	فقط برای راهبریِ برنامه کاربردیِ PLAID
مشترک	Keyset = 1	برای اصالت‌سنجی نواحی عمومی مشترک محدوده‌ای از ساختمان‌ها که فقط افراد مورد اعتماد می‌توانند به محیط بیرونی وارد شوند.
دسترسی فیزیکی	Keyset = 2	برای اصالت‌سنجی سامانه‌های PACS در محیط بیرونی
اتاق رایانه	Keyset = 3	برای اصالت‌سنجی برای دسترسی به اتاق رایانه و مناطق بسیار امن با سامانه PACS جداگانه
سایر دسترسی‌ها	Keyset = 4	برای اصالت‌سنجی برای دسترسی به چاپگر، و غیره

پیوست ت

(آگاهی‌دهنده)

پیاده‌سازی مرجع

یک پیاده‌سازی مرجع برای PLAID و PLAID SAM، برای کمک به درک جامع چگونگی پیاده‌سازی این استاندارد، موجود است.

پیاده‌سازی مرجع، بردارهای آزمون و دیگر ابزارهای مفید برای توسعه‌دهندگان ممکن است از نشانی زیر دریافت شوند:

https://www.plaid.gov.au

پیوست ث

(آگاهی‌دهنده)

ملاحظات فاش شدن هویت

ث-۱ عمومی

فاش شدن ID ممکن است به اشکال منفعل یا فعال رخ دهد. فاش شدن منفعل ID در مواقعی است که داده‌های منحصربه‌فرد هر کارت یا هر طرح‌واره به سادگی توسط ثبت کردن جلسات بین IFD و ICC در دسترس باشند. فاش شدن فعال، مواقعی است که ابزارها یا ویروس‌های خاص، ICC را برای شناسایی مفید و یا اطلاعات خصوصی در آدرس‌های پرکاربردتر در کارت، پویش می‌کنند.

حملات منفعل با استفاده از روش استفاده شده حذف توسط PLAID و مقداردهی اولیه مناسب ICC نسبتا راحت‌تر هستند، همان‌طور که در زیر شرح داده شده است.

از بین بردن کامل حملات فعال ممکن است غیرعملی باشد، ازآنجا که بیشتر استانداردهای موجود به اطلاعات آزادانه در دسترس نیاز دارند که در آدرس‌های ICC قابل پیش‌بینی موجود باشد و حل این امر، فراتر از دامنه کاربرد این استاندارد است. بحث زیر برخی از گزینه‌های در نظر گرفته به‌منظور به کمینه رساندن تاثیر فاش شدن ID را فراهم می‌کند.

ث-۲ فاش شدن منفعل ID

به‌منظور حذف فاش شدن منفعل احتمالی ID هنگام پیاده‌سازی PLAID، توصیه می‌شود بازبینی‌های اضافی زیر به‌عنوان بخشی از راه‌اندازی شخصی شده PLAID ICC در نظر گرفته شود.

- توصیه می‌شود در مورد PICC غیر تماسی، UID تولید شده توسط PICC برای روش اجراییِ ضدتصادم[1] در استاندارد ISO / IEC 14443-3، برای استفاده گزینه «تصادفی» بر اساس استاندارد ISO / IEC 14443-3 مشخص شود. این امر به‌طور کلی نیاز دارد که قبل از شخصی‌سازی کارت و یا در برخی موارد در تولید، تنظیم شود.

- در پیاده‌سازی‌هایی که در آن‌ها فاش شدن ID از هر نوعی نمی‌تواند تحمل شود، ممکن است برای اطمینان از این که پاسخ ATR / ATQ شامل داده‌های شناسایی منحصربه‌فرد در هر کارت یا هر طرح نشود، نیاز به مراقبت باشد، به‌ویژه در بایت‌های تاریخی یافت شده در استاندارد ISO / IEC 7816 -3 و ISO / IEC 7816-4. تمام چنین داده‌هایی که باید تنظیم شوند، ممکن است به صورت بهترین مقدار NULL تنظیم شوند. به‌طور کلی این امر نیاز به تنظیم قبل شخصی‌سازی کارت و یا در برخی موارد، تولید دارد.

1- Anti-collision

- هر جلسه گفت‌وگوی ممکن با برنامه‌های کاربردی دیگر در ICC، به‌ویژه آن‌ها که به‌عنوان برنامه پیش‌فرض تنظیم شده‌اند باید بازبینی شوند.

ث-۳ فاش شدن فعال ID

- وضعیت و جلسه گفت‌وگوی تمام برنامه‌های کاربردی بر روی کارت، به‌خصوص برنامه‌های کاربردی عمومی یا تشخیصی تولیدکننده که ممکن است در ROM مخفی شده باشند و ممکن است به‌طور رسمی مستند شده یا به‌طور معمول توسط تولیدکننده فاش شده باشند را بازبینی کنید.

- به‌طور کلی فعالیت‌های پیاده‌سازی مانند مدیریت کارت با استفاده از reader تماس انجام می‌شوند. بسیاری از ICCها می‌توانند به صورت برنامه‌ای بین رابط‌های تماسی و غیرتماسی، تمایز قائل شوند و می‌توانند از دسترسی به برنامه‌های کاربردی رابط تماسی جلوگیری کنند. دسترسی در حالت خاموش به برنامه‌های کاربردی پیاده‌سازی رابط‌های غیرتماسی، به‌خصوص آن‌هایی که اطلاعات کارت شناسایی منحصربه‌فرد مانند داده‌های چرخه عمر تولید کارت بسترِ جهانی (CPLC) [1] را ذخیره می‌کنند، را در نظر بگیرید.

1 - GlobalPlatform Card Production Life Cycle

پیوست ج

(آگاهی‌دهنده)

مدیریت حالت عملیاتی

این استاندارد امکان بیش از ۶۵۵۳۵ حالت عملیاتی تعیین شده توسط سابقهٔ ۲ بایتی ACS فرستاده شده به ICC در فرمان نهایی اصالت‌سنجی را فراهم می‌کند. سپس مقادیر مختلف ACSRecord تایید شده و توسط پاسخ نهایی اصالت‌سنجی، بازگشت داده می‌شوند. این امکان، اجازه می‌دهد که سابقهٔ مختلف و متمایز ACS، بسته به نیازهای کاری اصالت‌سنجی برای پیاده‌سازی، بتواند به IFD و سامانه‌های back-end عبور کند. به‌عنوان مثال، پیاده‌سازی ممکن است از حالت عملیاتی زیر استفاده کند:

جدول ۶- مدیریت حالت عملیاتی

ساختمان‌های جدید	ACSRecord = 1	به‌عنوان مثال RFC 4122 مبتنی بر رشته، UUID برای اصالت‌سنجی در سامانه‌های ساختمانی جدید برمی‌گردد.
ساختمان‌های قدیمی	ACSRecord = 2	به‌عنوان مثال رشته ۲۶ بیتی Wiegand برای اصالت‌سنجی در سامانه‌های ساختمانی قدیمی‌تر، برمی‌گردد.
دسترسی منطقی	ACSRecord = 3	به‌عنوان مثال FIPS 201 بر اساس رشته CHUID / FASC N برای اصالت‌سنجی ورود به سامانه، دسترسی به چاپگر، و غیره برمی-گردد.
اتاق رایانه	ACSRecord = 4	به‌عنوان مثال RFC 4122 .مبتنی بر رشته UUID برای اجازه دسترسی به اتاق رایانه و نواحی با امنیت بالا، برمی‌گردد.

یادآوری- ممکن است تناظر یک‌به‌یک بین OpModeID و KeySetID در هر پیاده‌سازی، وجود داشته یا نداشته باشد. به‌عنوان مثال ممکن است در طول انتقال، KeySetID مورد استفاده فقط برای دسترسی ساختمان باشد، ساختمان‌های جدید ممکن است یک OpModeID استفاده کنند درحالی‌که OpModeID دیگری توسط ساختمان‌های قدیمی‌تر، به‌منظور انتقال استفاده آن‌ها از شماره‌گذاری قدیمی‌تر بر اساس Wiegand، استفاده شود.

پیوست چ

(آگاهی‌دهنده)

ویژگی‌های امنیتی PLAID

این پیوست، منطق و هدف هر مرحله از قرارداد را تعریف کرده و مورد بحث قرار می‌دهد. در این قرارداد، به ترتیب و ساختار نشان داده شده در شکل ۱ توضیح داده می‌شود، که توصیه می‌شود به ملاحظات شرح داده شده در زیر، اشاره شود.

چ-۱ اصالت‌سنجی اولیه - عمومی

- هدف اصلی فرمان IA، محافظت از حریم خصوصی و مقادیر داده تنوع‌بخشی (DivData) است که برای تنوع بخشیدن به کلیدهای درگیر در عملیات بعدی FA مورد نیاز هستند تا اطمینان حاصل شود که آن‌ها در معرض افشا نیستند.

- قراردادهای اصالت‌سنجی دیگری شناخته شده‌اند که مقادیر این داده‌های تنوع‌بخشی را به صورت شماره‌سریال کارت و یا UID، در معرض افشا قرار می‌دهند که به صورت بالقوه برای منجر به حملات می‌شود. با استفاده از این مرحله PLAID، AP اجازه می‌دهد تا کلیه اطلاعات هویتی منحصربه‌فرد به غیر اطلاعات در دسترس ICC، مسدود شده و یا توسط کلید ایمن باشند.

- هدف ثانویه این مرحله، جلوگیری از افشای مقادیر RND1 (که توسط ICC برای جلسه خاص تولید می‌شود) است.

- هیچ‌کدام از نقض شدن‌های مرحله‌ی IA، برای مرحله بعدی FA مهلک نیستند، زیرا تنها نقض واقعی، برای مقدار RND1 و DivData است.

- این مرحله از رمزگذاری نامتقارن (RSA) استفاده می‌کند.

- کارت ICC با استفاده از نمای عمومی و پیمانه کلید RSA رمزگذاری می‌کند، طوری که بیشینه کارایی در رمزگذاری on-card به دست آید.

- فقط IFD ها با دسترسی به مواد کلید RSA خصوصی قادر به رمزگشایی پاسخ ICC هستند.

- با این حال هر دو کلید محافظت می‌شوند؛ آن‌ها مشابه کلیدهای متقارن مشترک، مدیریت می‌شوند.

- این مرحله باید بسیار سریع باشد. انتخاب رمز نامتقارن و طول کلید نیاز به در نظر گرفتن قابلیت ICC ها و IFDهای عملیاتی برای رسیدن به این سرعت دارد و همچنین این واقعیت که نقض این مرحله تنها بر

امنیت DivData و RND1، اثر می‌گذارد و بر کل معامله AP اثر نمی‌گذارد.

چ-۱-۱ مرحله ۱ - فرمان اصالت‌سنجی اولیه

- قرارداد AP آغاز می‌کند.

- در شرایط عدم حضور هیچ مهاجمی، همه داده‌ها واضح هستند.

- فهرستی از Keyset های پشتیبانی شده از IFD به ICC در اولویت عبور قرار می‌گیرند.

- فهرست Keyset به‌ندرت توسط مهاجم استفاده می‌شود، زیرا شامل هیچ مقدار کلید نیست، و فهرست واقعی در هر مورد بر اساس محل و یا مورد استفاده، معمولا آشکار است.

- روش کدبندی BER-TLV برای بیشینه توسعه‌پذیری استفاده می‌شود.

- داده‌ها بسیار کوچک بوده و بنابراین سرعت زیاد است.

چ-۱-۲ مرحله ۲ - ارزیابی فرمان اصالت‌سنجی اولیه

- فهرست Keyset ها تجزیه شده و Keyset برای باقی مانده جلسه AP انتخاب می‌شود.

چ-۱-۳ مرحله ۳ - پاسخ اصالت‌سنجی اولیه

- داده‌های DivData در هر ICC منحصربه‌فرد بوده و در نمونه ICC ترجیحا به‌عنوان عدد تصادفی، اما منحصربه‌فرد تولید می‌شود. داده DivData برای تنوع بخشیدن به کلید AES مورد استفاده در مراحل FA استفاده می‌شود.

- داده‌های DivData از حافظه محافظت شده، بازیابی شده و RND1 با استفاده از ICC RNG تولید می‌شود. توجه داشته باشید که قدرت RNG مهم است در غیر این صورت، ممکن است حمله رخ دهد.

- رشته 'KeySetID||DivData||RND1||RND1'، تولید می‌شود و با استفاده از رمز نامتقارن انتخاب شده، رمزگذاری شده و به IFD بازگشت داده می‌شود.

- تکرار RND1 به‌عنوان مجموع مقابله‌ای استفاده می‌شود.

- رمز نامتقارن برای حصول اطمینان از این که در رویداد ICC در خطر فاش شدن، دشمن قادر به رمزگشایی ترافیک هوایی از هیچ ICC نخواهد بود، استفاده می‌شود.

- با استفاده از رمز نامتقارن، مهاجمی که به‌طور کامل ICC را به خطر انداخته، حتی نمی‌تواند پاسخ‌های ICC IA را رمزگشایی کند زیرا آن‌ها تنها کلید عمومی و مواد کلید خصوصی مربوط را دارند که برای

رمزگشایی هر کارتی که در ابزارهایback office یا در SAM وجود دارد، لازم است.

چ-۱-۴ مرحله ۴ - ارزیابی پاسخ اصالت‌سنجی اولیه

- افزارهٔ IFD رشته پاسخ را با استفاده از IAKey رمزگشایی کرده و بازبینی می‌کند تا RND1 تکرار شده باشد.

- اگر IFD با موفقیت بتواند رمزگشایی کرده و فرمان IA را معتبر سازد، آنگاه ICC مقدار کلید IA تایید شده را ثابت خواهد کرد. ICC نشان‌دهنده تنوع‌بخشی داده‌ها برای اعتبار دادن به فرمان FA استفاده می‌شود.

چ-۲ اصالت‌سنجی نهایی- عمومی

- فرمان FA، RND2 تولید شده توسط IFD و KeysHash ترکیبی را به IFD عبور می‌دهد.

- وجود KeysHash به‌منظور پیوند مراحل مورد نیاز بوده و در نتیجه تضمین می‌کند که دستگاه نتواند خود را در وسط ارتباطات بین مراحل IA و FA قرار دهد.

- فرمان FA از رمز متقارن AES-128 استفاده می‌کند. این کار به‌منظور به دست آوردن عملکردی با طول کلید کافی است. این امر با AES-128، دست‌یافتنی است.

- همچنین فرمان FA، OpModeID را طوری عبور می‌دهد که ICC، بتواند نوع سامانه IFD را تعیین کرده و سوابق واپایش دسترسی درست و یا پایه‌بار را برای آن ارسال کند.

چ-۲-۱ مرحله ۵ - فرمان اصالت‌سنجی نهایی

- عدد RND2 تولید شده و KeysHash بر اساس RND1 تولید شده توسط ICC، محاسبه می‌شود. بنابراین KeysHash، ترکیبی از اعداد تصادفی تولید شده توسط IFD و ICC است و به اندازه برتری RNG، مهم خواهد بود.

- شناسه OpModeID در ICC تصویب می‌شود طوری که ICC تنها به داده‌های اعتباری مورد نیاز برای موارد استفاده خاص پاسخ می‌دهد. این مسئله موجب کاهش داده‌های غیرضروری تصویب شده در رابط شده و امکان فاش شدن اطلاعات خصوصی را کاهش می‌دهد. همچنین باعث انتقال آسان‌تر می‌شود زیرا ICC می‌تواند بسیاری از انواع مختلف سابقه PACS را پشتیبانی کند.

- ارتباطات AES-128 با استفاده از کلید محاسبه شده برای ICC بر اساس DivData به دست آمده در مرحله قبل، رمزگذاری می‌شوند.

چ-۲-۲ مرحله ۶ - ارزشیابی فرمان اصالت‌سنجی نهایی

- اگر ICC بتواند با موفقیت رمزگشایی کرده و فرمان FA را معتبر سازد، آنگاه ICC اصالت‌سنجی IFD را در نظر خواهد گرفت. رمزگشایی موفق با ویژگی‌های زیر تعیین می‌شود.

- محاسبه ICC برای KeysHash با محاسبه IFD برای KeysHash. مطابقت دارد. این نشان می‌دهد به ICC که در مرحله قبل، IFD با موفقیت از فرمان IA برای بازیابی مقدار داده تنوع‌بخشی شده و RND1، رمزگشایی کرده است.

- رمزگشایی ICC از فرمان FA (با مقایسه‌های KeysHash) معتبر است. این به ICC نشان می‌دهد که IFD، کلید AES درست و منحصربه‌فرد را در هر ICC استفاده کرده است.

چ-۲-۳ مرحله ۷ - پاسخ اصالت‌سنجی نهایی

- الگوریتم AES، اطلاعات گواهی‌نامه پایه‌بار را رمزگذاری می‌کند (ACSRecord, < Payload >).

- همچنین AES، DivData را رمزگذاری می‌کند که به‌عنوان تایید ارتباط بین پاسخ IA و پاسخ FA به صورت روش پشتیبان KeysHash برای جلوگیری از ربودن جلسه[1]، تصویب می‌شود.

- پاسخ، از ترکیب KeysHash به‌عنوان کلید برای رمزگذاری AES رشته استفاده می‌کند. این امر، تداوم اصالت‌سنجی پاسخ IA اول را تضمین می‌کند.

چ-۲-۴ مرحله ۸ - ارزیابی پاسخ اصالت‌سنجی نهایی

- اگر IFD بتواند با موفقیت فرمان FA را آشکار کند، آنگاه ICC، ICC اصالت‌سنجی شده و داده‌های ارائه شده و تصدیق شده را در نظر خواهد گرفت. رمزگشایی موفق با تایید این که داده‌های تنوع‌بخشی موجود در فرمان FA با داده‌های تنوع‌بخشی ارائه شده در فرمان IA قبلی انطباق دارد، تعیین می‌شود. انطباق موارد زیر را تایید می‌کند:

- رمزگشایی موفق بوده است.

- جلسه ربوده نشده است.

1 - Session Hijacking

کتاب‌نامه

[1] ISO/IEC 8824-2, Information technology — Abstract Syntax Notation One (ASN.1): — Part 2: Information object specification

[2] ISO/IEC 14443-3, Identification cards — Contactless integrated circuit cards — Proximity cards — Part 3: Initialization and anti-collision