استاندارد ملی ایران

۱۸۴۷۷-۱

چاپ اول

۱۳۹۳

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

INSO

18477-1

1st. Edition

2014

فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها- امنیت ارتباط میدان نزدیک (NFC)- قسمت ۱: پروتکل و خدمات امنیتی ارتباط میدان نزدیک_ امن (NFC-SEC) پروتکل و واسط ارتباط میدان نزدیک ۱ (NFCIP-1)

Information technology - Telecommunications and information exchange between systems – NFC Security – Part 1: NFC-SEC NFCIP-1 security services and protocol

ICS : 35.110

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 حوزه‌های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود 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 واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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 می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند 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)[۱]،کمیسیون بین المللی الکتروتکنیک (IEC)[۲] و سازمان بین المللی اندازه شناسی قانونی (OIML)[۳] است و به عنوان تنها رابط[۴] کمیسیون کدکس غذایی (CAC)[۵] 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 می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه 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 آن ها نظارت می‌کند. ترویج دستگاه بین‌المللی 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

« فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها- امنیت ارتباط میدان نزدیک (NFC)- قسمت ۱: پروتکل و خدمات امنیتی ارتباط میدان نزدیک_امن (NFC-SEC) پروتکل و واسط ارتباط میدان نزدیک ۱ (NFCIP-1) »

رئیس:	**سمت و/ یا نمایندگی**
کشاورزی ، فرزاد (لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس رایانه شرکت پیشاهنگان آمایش
دبیر:	
امیری ، حسین (لیسانس مهندسی کامپیوتر نرم افزار)	مدیر عامل شرکت نوآوران مبانی پرداز
اعضاء: (اسامی به ترتیب حروف الفبا)	
خندزاد ، بهزاد (لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس رایانه شرکت نوآوران مبانی پرداز
خندزاد ، بیتا (فوق لیسانس هوش مصنوعی و رباتیک)	کارشناس ارشد ادارات مرکزی هواپیمائی جمهوری اسلامی ایران هما
درفشی ، رکسانا (لیسانس زبان انگلیسی)	کارشناس تایید صلاحیت سازمان استاندارد
ستاری ، آناهیتا (لیسانس مهندسی متالوژی)	مترجم ارشد شرکت پیشاهنگان آمایش
سروشیان ، سپیده (لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس رایانه شرکت پیشتازان پردازش اطلاعات
ندائی فرخد ، الهام (لیسانس مهندسی کامپیوتر نرم افزار)	رئیس تحلیل و طراحی گروه کارخانجات پارت لاستیک

فهرست مندرجات

پیش گفتار

استاندارد « فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها- امنیت ارتباط میدان نزدیک (NFC)- قسمت ۱: پروتکل و خدمات امنیتی ارتباط میدان نزدیک_امن (NFC-SEC) پروتکل و واسط ارتباط میدان نزدیک ۱ (NFCIP-1) » که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران/شرکت نوآوران مبانی پرداز تهیه و تدوین شده و در سیصدوچهل‌ودومین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۱۳۹۳/۰۳/۱۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد 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 متن صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC 13157-1: 2010, Information technology - Telecommunications and information exchange between systems – NFC Security - Part 1: NFC-SEC NFCIP-1 security services and protocol

مقدمه

این استاندارد ملی، خدمات امنیتی مشترک ارتباط میدان نزدیک (NFC)[1] و یک پروتکل را مشخص می‌کند. این استاندارد قسمتی از سری استانداردهای امنیتی NFC می‌باشد.

ارتباط میدان نزدیک – امن (NFC-SEC)[2] استانداردهای سری رمزنگاری را تکمیل می‌کند و خدمات پروتکل مشخص‌شده در این استاندارد ملی را استفاده می‌کند.

1- Near Field Communication
2- Near Field Communication -Secure

فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها- امنیت ارتباط میدان نزدیک (NFC)- قسمت ۱: پروتکل و خدمات امنیتی ارتباط میدان نزدیک_امن (NFC-SEC) پروتکل و واسط ارتباط میدان نزدیک ۱ (NFCIP-1)

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین کانال امن NFC_SEC و خدمات محرمانه به اشتراک گذارده شده برای پروتکل و واسط ارتباط نزدیک ۱ (NFCIP-1)[1] و PDU و پروتکل برای این خدمات است.

یادآوری ۱: NFC-SEC بصورت انحصاری برای پروتکل تبادل داده از استاندارد بین‌المللی ISO/IEC 18092 طراحی شده است.

یادآوری ۲: این استاندارد سازوکارهای امنیتی کاربرد خاصی را نشانی‌دهی نمی‌کند (به طور نمونه برای موارد مورد نیاز مربوط به استفاده از کارت هوشمند و استاندارد بین‌المللی سری ISO / IEC 781). NFC-SEC ممکن است تکمیل‌کننده پروتکل‌های امنیتی کاربردی خاص از استاندارد بین‌المللی ISO/IEC 7816 باشد.

۲ انطباق

پیاده‌سازی‌های منطبق، سازوکارهای امنیتی در قسمت رمزنگاری NFC-SEC را بکار می‌گیرند که تعیین می‌کند PID انتخاب شده از یک یا بیشتر خدمات مشخص شده در این استاندارد ملی استفاده می‌کند.

پیاده‌سازی‌های منطبق که از NFCIP-1 استفاده می‌کنند نیز بهتر است که مطابق با الزامات پیوست ب باشد.

۳ 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 مدرکی با ذکر تاریخ انتشار ارجاع داده شده است، اصلاحیه‌ها و تجدیدنظرهای 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 تجدیدنظر و اصلاحیه‌های بعدی آنها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

3-1 ISO/IEC 7498-1:1994, Information technology — Open Systems Interconnection — Basic Reference Model:The Basic Model

3-2 ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

3-3 ISO/IEC 10731:1994, Information technology — Open Systems Interconnection — Basic Reference Model — Conventions for the definition of OSI services

1- Near Field Communication Interface and Protocol

3-4 ISO/IEC 11770-1:1996, Information technology — Security techniques — Key management — Part 1: Framework
3-5 ISO/IEC 13157-2:2010, Information technology — Telecommunications and information exchange between systems — NFC Security — Part 2: NFC-SEC cryptography standard using ECDH and AES (also published by Ecma as Standard ECMA-386)
3-6 ISO/IEC 18092:2004, Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1) (also published by Ecma as Standard ECMA-340)

۴ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف بکار رفته در استانداردهای بین‌المللی ISO/IEC 18092، ISO/IEC 7498-1، ISO 7498-2، ISO/IEC 10731، ISO/IEC 11770-1 و اصطلاحات و تعاریف زیر بکار می‌روند:

۴-۱
اتصال
(N)- اتصال همانطور که در استاندارد بین‌المللی ISO / IEC 7498-1 مشخص شده است.

۴-۲
هستار
(N)- هستار همانطور که در استاندارد بین‌المللی ISO / IEC 7498-1 مشخص شده است.

۴-۳
کلید اتصال
کلید محرمانه امن‌کننده ارتباطات در سراسر یک کانال امن است.

۴-۴
کاربر NFC-SEC
هستار با استفاده‌کننده از خدمت NFC-SEC است.

۴-۵
پروتکل
(N)- پروتکل همانطور که در استاندارد بین‌المللی ISO/IEC 7498-1 مشخص شده است

۴-۶
گیرنده
هستار NFC-SEC که ACT_REQ را دریافت می‌کند

۴-۷
کانال امن

۸-۴

فرستنده

هستار NFC-SEC که ACT_REQ را ارسال می‌کند.

۹-۴

خدمت

(N)- خدمت همانطور که در استاندارد بین‌المللی ISO/IEC 7498-1 مشخص شده است.

۱۰-۴

راز به اشتراک گذارده شده

راز به اشتراک گذارده شده بین دو کاربر NFC-SEC است.

۵ نمادها و قراردادها

نمادها و قراردادهای زیر در این سند اعمال می شود مگر اینکه غیر آن اعلام گردد:

۵-۱ نمایش اعداد

نمادها و قراردادهای زیر در این سند اعمال می شود مگر اینکه غیر آن اعلام گردد:

- حروف و ارقام در پرانتز و اعداد در مبنای شانزده نشان داده می‌شوند.
- تنظیم بیت با صفر یا یک نشان داده شده است.
- شماره‌ها در نماد دودویی و الگوهای بیتی با رشته‌ای از بیت‌های ۰ و ۱ نمایش داده می‌شوند که با ترتیب پر ارزشترین بیت از چپ نشان داده می‌شوند.
- در هشتایی کم ارزش‌ترین بیت شماره ۱ و پر ارزش‌ترین بیت ۸ است.

۵-۲ نام‌ها

نام هستارهای اصلی، به عنوان مثال فیلدهای خاص، با حرف بزرگ در ابتدا نوشته می‌شود.

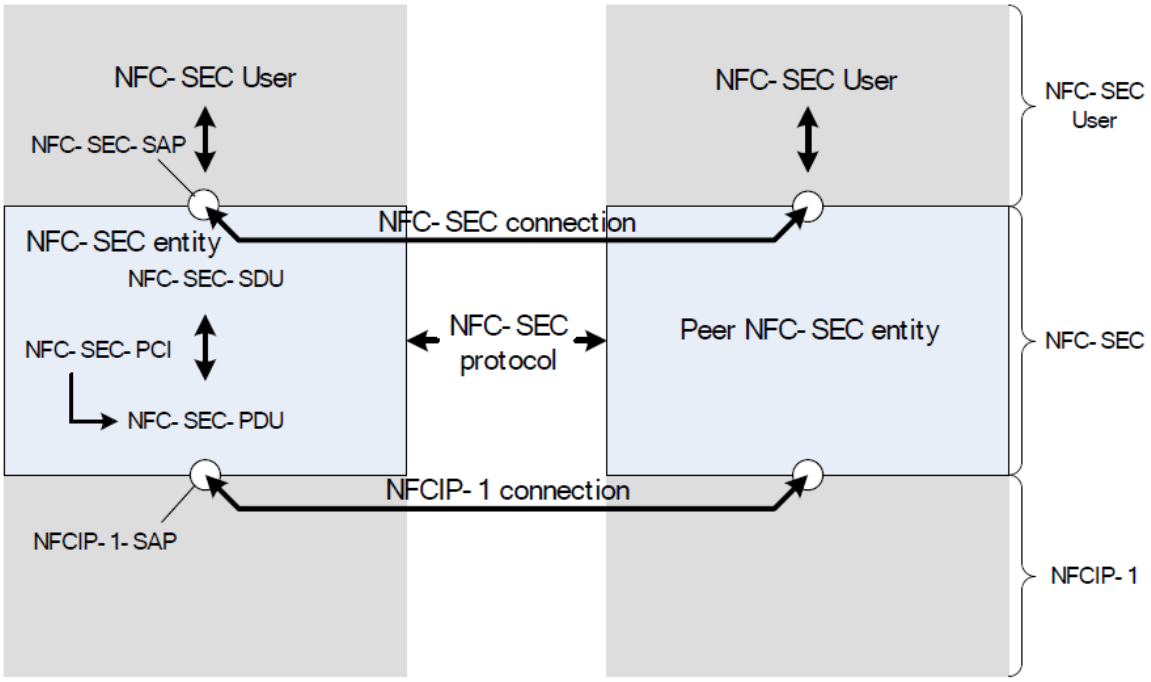
۶ کوته‌نوشت‌ها

برای اهداف این استاندارد، کلمات اختصاری داده شده در استاندارد بین‌المللی ISO/IEC 18092 و موارد زیر اعمال می شود.

درخواست فعال سازی PDU	ACT_REQ
فعال سازی پاسخ PDU	ACT_RES
بسته های رمزگذاری شده PDU	ENC
خطای PDU	ERROR
کم ارزش‌ترین بیت	Lsb
کم ارزش‌ترین بایت	LSB
پر ارزش‌ترین بیت	Msb
پر ارزش‌ترین بایت	MSB
کد پیام	MSG
اطلاعات کنترل پروتکل (به استاندارد بین‌المللی ISO/IEC 7498-1 مراجعه شود)	PCI
پروتکل واحد داده (به استاندارد بین‌المللی ISO/IEC 7498-1 مراجعه شود)	PDU
شناسه پروتکل	PID
برای استفاده در آینده رزرو شده است	RFU
خدمت کانال امن	SCH
مشخصات و توضیحات زبان (به استاندارد بین‌المللی ITU-T Z.100 مراجعه شود)	SDL
خدمات واحد اطلاعات (به استاندارد بین‌المللی ISO/IEC 7498-1 مراجعه شود)	SDU
پارامتر پروتکل تبادل امنیت	SEP
اعداد متوالی	SN
متغیرSN	SNV
خدمات راز به اشتراک گذاشته شده	SSE
کد خدمات	SVC
خاتمه دادن PDU	TMN
تأیید درخواست PDU	VFY_REQ
تائید پاسخ PDU	VFY_RES

۷ کلیات

همانطور که در شکل شرح داده شده، NFC-SEC مدل مرجع OSI ،مشخص شده در استاندارد بین‌المللی ISO/IEC 7498-1 را استفاده می‌کند.



شکل ۱ – معماری **NFC-SEC**

کاربران NFC-SEC درخواست می‌کنند و به خدمات NFC-SEC از طریق خدمت نقطه دسترسی، دسترسی می‌یابند. هستارهای NFC-SEC از کاربران NFC-SEC، NFC-SEC-SDU (درخواست‌ها) را بدست می‌آورند و به آنها NFC-SEC-SDU (تائیدیه) را باز می‌گردانند.

این استاندارد خدمات کانال امن (SCH) و خدمات مخفی به اشتراک گذاشته شده (SSE) را مشخص می‌کند.

به منظور ارائه خدمات NFC-SEC، نظیر هستارهای NFC-SEC، NFC-SEC-PDU ها مطابق با پروتکل NFC-SEC از اتصالات NFC-SEC تغییر می‌یابند.

یک جفت هستار NFC-SEC برای دسترسی به خدمات داده NFCIP-1 از طریق خدمت نقطه دسترسی NFCIP-1 (NFCIP-1-SAP)، ارسال و دریافت NFC-SEC-PDU ها، با یکدیگر ارتباط برقرار می‌کنند.

۸ خدمات

این بند دو خدمت SSE و SCH را که NFC-SEC برای کاربران NFC-SEC فراهم می‌کند را مشخص می‌کند. در زمان فراخوانی، این خدمت‌ها انتقال حفاظت شده و رمزنگاری شده، پیام‌های کاربر NFC-SEC بین یک جفت NFC-SEC را با استفاده از یک پروتکل شرح داده شده در بند ۹ را فراهم می‌کنند.

۸-۱ خدمت محرمانه به اشتراک گذاشته شده (SSE)

SSE اشتراک مخفیانه بین کاربران یک جفت NFC-SEC را فراهم می‌کند تا بتوانند به اختیار خود از آن استفاده کنند.

درخواست از SSE باید یک راز به اشتراک گذاشته شده را توسط توافق‌های کلیدی ایجاد و سازوکارهای تائید مطابق با بخش رمز نگاری NFC-SEC که PID را تعریف می‌کند را ایجاد کند.

۸-۲ خدمت مسیر امن (SCH)

SCH یک کانال امن را ایجاد می‌کند.

درخواستار SCH باید یک کلید پیوند را به وسیله اشتقاق از یک راز مشترک ایجاد شده توسط مورد کلید و سازوکارهای تأیید کلید ایجاد کند و پس از آن باید از تمام ارتباطات در هر دو جهت در سراسر کانال مطابق با بخش رمز نگاری NFC-SEC که PID را تعریف می‌کند، حفاظت کند.

۹ سازوکارهای پروتکل

پروتکل NFC-SEC شامل سازوکارهای زیراست. شکل ۲ توالی از سازوکارهای پروتکل را مشخص می‌کند.

۹-۱ مطابقت کلید

یک جفت هستار NFC-SEC باید یک راز مشترک را با استفاده از ACT_REQ و ACT_RES و مطابق با بخش رمز نگاری NFC-SEC که PID را تعریف می‌کند، ایجاد کنند.

۹-۲ پذیرش کلید

یک جفت هستار NFC-SEC باید راز مشترک توافق‌شان را توسط VFY_REQ و VFY_RES و مطابق با بخش رمز نگاری NFC-SEC که PID را تعریف می‌کند را بازبینی کنند.

۹-۳ امنیت PDU

امنیت PDU فقط یک مکانیزم از خدمت SCH می‌باشد.

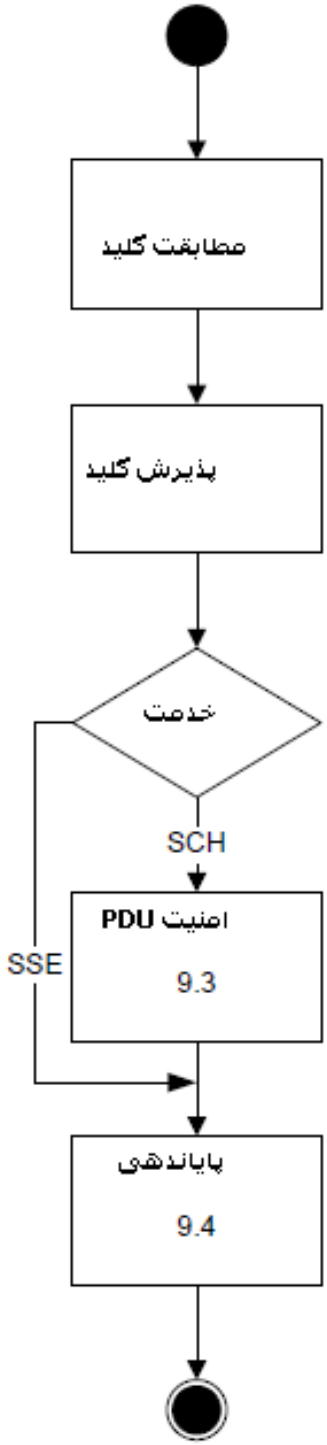
یک جفت هستار NFC-SEC باید از تبادل داده با استفاده از ENC و مطابق با بخش رمز نگاری NFC-SEC که PID را تعریف می‌کند حمایت کنند.

این مکانیزم همانطور که در استاندارد مربوطه رمزنگاری NFC-SEC مشخص شده است، باید شامل یک یا چند مورد از موارد زیر باشد:

- توالی جامعیت، منطبق با الزامات بند ۱۲-۳
- محرمانه بودن
- جامعیت داده
- احراز هویت مبدا

۹-۴ پایان‌دهی

یک جفت هستار NFC-SEC باید SSE و SCH را توسط TMN خاتمه دهند. پس از انتشار یا عدم انتخاب از NFCIP-1 ، یا وقتی که NFCIP-1 دستگاه خاموش شده است، موارد SSE و SCH باید خاتمه یابند. به محض انتقال به حالت IDLE راز مشترک مرتبط و کلید اتصال باید از بین بروند.



شکل ۲- جریان عمومی از خدمات NFC-SEC

۱۰ حالات و زیرحالات

دستگاه پروتکل NFC-SEC در ضمیمه الف حالت انتقال برای حالات و زیرحالات در جدول ۱ را مشخص می‌کند.

جدول ۱ – حالت

حالت	توضیحات
بیکار	NFC-SEC آماده برای شروع یک خدمت جدید بر اساس درخواست از کاربر NFC-SEC و یا همکار NFC-SEC هستار است
انتخاب	NFC-SEC در انتظار ACT_RES
ایجاد	خدمات NFC-SEC درخواست شده است. حالت ایجاد شده شامل دو زیرحالت است که در زیرحالت Established_Sender در انتظار VFY_RES و در زیرحالت Established_Recipient در انتظار VFY_REQ است.
تائید شده	یک خدمت NFC-SEC ایجاد شده است .حالت تائید شده شامل دو زیرحالت است که در زیرحالت Confirmed _SSE راز مشترک آماده به بازیابی است ودر زیرحالت Confirmed _SCH تبادل داده امن آماده است.

۱۱ NFC-SEC-PDU ها:

NFC-SEC-PDU ها باید در NFCIP-1 DEP داده محرمانه را حمل کنند. PDU ها بایت SEP را در بایت صفر بایت‌های اطلاعات حمل ونقل قرار می‌دهد. بایت اطلاعات حمل و نقل DEP باید دقیقا شامل یک NFC-SEC-PDU باشد.

ساختار NFC-SEC-PDU در شکل ۳ مشخص شده است.

شکل ۳– ساختار NFC-SEC-PDU

جدول ۲ مشخصه‌های NFC-SEC-PDUها را به عنوان گزینه های اجباری (m)، ممنوع (p) ، مشروط (C) مشخص می کند. مشروط (C) بعدا در بند ۱۱-۳ مشخص می‌شود.

جدول ۲ – مشخصه‌های **NFC-SEC-PDU**

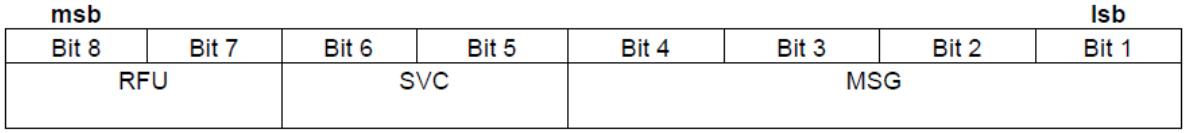
NFC-SEC-PDU	SEP	PID	NFC-SEC Payload
ACT_REQ	m	m	c
ACT_RES	m	p	c
VFY_REQ	m	p	c
VFY_RES	m	p	c
ENC	m	p	c
TMN	m	p	p
ERROR	m	p	c

۱۱-۱ پروتکل تبادل امن (SEP)

پروتکل تبادل (SEP) امن ۱ بایتی به شرح زیر مشخص شده است:

- مقدار 00b در SVC نشان می دهد که PDU بخشی از تبادل SSE است. مقدار 01b در SVC نشان می‌دهد که PDU بخشی از تبادل SCH است.
- کد MSG نوع PDU را همانطور که در جدول ۳ مشخص شده، شناسایی می‌کند. تمام کدهای دیگر RFU هستند.
- بیت‌های RFU باید ZERO تنظیم شوند.

شکل ۴ انتساب بیت را مشخص می‌کند.



شکل ۴ – انتساب بیت‌های SEP

جدول ۳ – انواع PDU و کدهای MSG

کد	نام	شرح
0000	ACT_REQ	درخواست فعال سازی به درخواست یک خدمت جدید
0001	ACT_RES	پاسخ فعال سازی، به قبول درخواست خدمات
0010	VFY_REQ	درخواست بازبینی برای ارائه نتیجه بررسی مقادیر برایارزیابیراز به اشتراک گذاشته فرستندگان
0011	VFY_RES	پاسخ ارزیابی به ارائه نتیجه بررسی برای ارزیابی گیرندگان راز به اشتراک گذاشته
0100	ENC	رمز نگاری بسته برای تبادل امن داده
0110	TMN	درخواست Terminate برای پایاندهی به خدمت
1111	ERROR	خطا و نشانه یک خطا
سایر		RFU

۱۱-۲ شناسه پروتکل (PID)

هر بخش رمزنگاری NFC-SEC از این استاندارد یک PID هشت بیتی منحصر به فرد را که فقط ACT_REQ موجود می‌باشد را تعریف می‌کند.

۱۱-۳ بارمفید[1] NFC-SEC

TMN PDU بهتر است شامل مشخصه بارمفید NFC-SEC نباشد. مشخصه بارمفید باید از عدد صحیح مبنای هشت تشکیل شده باشد. استفاده از آن در PDU ERROR در زیر بند خطا در زیر مشخص شده است. استفاده از آن، ساختار و کدبندی در سایر تمامی PDUها در قسمت رمزنگاری NFC-SEC که PID را تعیین می‌کند، مشخص شده است.

۱۱-۴ پایان دادن (TMN)

همانطور که در جدول ۲ مشخص شده است TMN PDU فقط شامل مشخصه SEP است.

۱۱-۵ خطا (ERROR)

ERROR PDU با مشخصه SEP شروع می‌شود و اگر شامل بارمفید باشد، باید شامل یک رشته مبنای هشت خاتمه یافته با صفر در مشخصه بارمفید NFC-SEC باشد.

۱۲ قاعده پروتکل

این بخش قاعده پروتکل NFC-SEC را مشخص می‌کند.

۱۲-۱ پروتکل و خطاهای خدمت

– هنگامی که یک هستار NFC-SEC در یک حالت که در آن مجاز نیست، PDUی را دریافت می‌کند، آن را باید با ERROR PDU پاسخ دهد.

1- Payload

- هنگامی که یک هستار NFC-SEC، PDU ی که آن را پشتیبانی نمی‌کند یا با محتوای نامعتبر که در استاندارد رمزنگاری NFC-SEC مشخص شده است را دریافت می‌کند، آن را باید با ERROR PDU پاسخ دهد.
- هنگامی که یک هستار NFC-SEC، ERROR PDU را ارسال و یا دریافت می‌کند باید حالت پروتکل به بیکار (Idle) تنظیم کند.
- هنگامی که یک هستار NFC-SEC، ERROR PDU را ارسال و یا دریافت می‌کند باید یک ERROR SDU را به کاربر NFC-SEC ارسال کند.
- هنگامی که یک هستار NFC-SEC در حالتی دریافت می‌کند که مجاز نیست و یا محتوای نامعتبری دارد، باید با ERROR SDU آنرا پاسخ دهد و بدون تغییر از آن حالت خارج شود.

۱۲-۲ قواعد تعامل داخلی[1]

- اجرای NFC-SEC ممکن است یک حد بالا روی طول NFC-SEC-SDU تنظیم کند. ارسال درخواست داده مشخص شده در پیوست الف-۲ با SDU های طولانی‌تر باید برگشت شوند.
- یک NFC-SEC-PDU باید دقیقا یک NFC-SEC-SDU را شامل شود.
- هستارهای NFC-SEC باید هر NFC-SEC-PDU تکراری را دور بیندازند همانطور که در بند یکپارچگی توالی مشخص شده است.

۱۲-۳ یکپارچگی توالی

استاندارد رمز نگاری NFC-SEC در صورت یکپارچگی توالی باید ساز و کار یکپارچگی توالی مطابق با موارد ذیل مشخص نماید:

- هر هستار NFC-SEC باید SNV خود را حفظ کند.
- پس از استقرار SCH ، دریافت کننده باید SNV را مقدار دهی اولیه کند و مقدار آنرا همان مقدار اولیه SNV ارسال کننده، مطابق با بخش رمز نگاری NFC-SEC که PID را تعریف می‌کند، قرار دهد.
- بخش رمز نگاری NFC-SEC که PID را تعریف می‌کند یک محدوده از مقادیر SNV را مشخص می‌کند.
- پس از ارسال از ENC ، NFC-SEC هستار باید SNV خود را با ۱ افزایش می‌دهد، و سپس آنرا در مشخصه SN قرار دهد.
- مشخصه SN باید توسط مکانیزم امنیتی PDU برای ایجاد هر گونه تغییر قابل تشخیص، محافظت شود.

1- Interworking

- پس از دریافت ENC، هستار NFC-SEC باید مشخصه SN را استخراج کرده آنرا با SNVاش مقایسه کند. اگر SN مساوی SNV بود PDU نباید به کاربر NFC-SEC ارسال شود و حالت و SNV باید بدون تغییر همانطور که در پیوست الف-۴-۴ مشخص شده، باقی بمانند.
- هستار NFC-SECباید SNV خود را با ۱ افزایش دهد.

شرط 'مقدار PDU معتبر است؟ ' در پیوست الف-۴-۴، در صورتی که SN وSNV یکسان باشند صحیح و در غیر اینصورت غلط می‌باشد.

یادآوری – در مورد خطاهای یکپارچگی توالی، NFC-SEC ،SCH و اطلاع رسانی به کاربران جفت هستار NFC-SEC را صرفنظر می‌کند. برای برقرار مجدد یک SCH با کلیدهای جدید یا صرفنظر از تراکنش.

۴-۱۲ پردازش رمزنگاری

پرازش رمزنگاری مطابق با بخش رمز نگاری NFC-SEC که PID را تعریف می‌کند، پیش از ارسال و پس از دریافت PDUها به غیر از TMN و ERROR، رخ می‌دهد. اگر نتیجه پردازش رمزنگاری از PDU های ورودی منفی است، پس از آن 'محتوای معتبر PDU ' تصمیم‌گیری در پیوست الف نادرست است.

پیوست الف

(الزامی)

مشخصات ماشین پروتکل

دستگاه پروتکل NFC-SEC در این ضمیمه دنباله‌ای از PDU ها برای ایجاد و پایان دادن به SSE، و برای ایجاد، استفاده و پایان دادن به SCH مشخص می‌کند.

علاوه بر این دستگاه پروتکل مشخص می‌کند که کدام یک از PDU ها ممکن است ارسال و یا دریافت که در آن حالت را داشته باشند.

الف – ۱ علائم SDL

NFC-SEC-PDU دریافت شده از هستار همکار NFC-SEC، توسط هستار NFCIP-1 محلی تحویل داده می‌شود.

NFC-SEC-PDU،ارسال شده به هستار NFCIP-1 محلی، به هستار همکار NFC-SEC ارائه می‌شود.

NFC-SEC-SDU بدست آمده از کاربر NFC-SEC، از هستار NFC-SEC درخواست اعمال واکنش را می‌کند.

NFC-SEC-SDU یا در پاسخ به درخواست قبلی یا نشان دادن یک رویداد، به کاربر NFC-SEC ارائه می‌شود.

حالت. در یک حالت ماشین پروتکل در انتظار یک رویداد است.

رویدادها در دیاگرام‌هایی که خطاهای پروتکل را تشکیل می‌دهند پیش‌بینی نشده‌اند.

یک شرط شاخه‌ای در پردازش رویدادها.

الف-۲ درخواست SDUها

درخواست SDUها توسط کاربران NFC-SEC برای درخواست خدمت NFC-SEC، ارائه می‌شود.
پارامترها در داخل پرانتز داده می‌شوند. الزامات بر روی مقادیر پارامترها در استانداردهای رمزنگاری NFC-SEC مشخص شده‌اند.

یادآوری- روش اجرای واقعی از شکل‌های هندسی اولیه درخواست (به عنوان مثال: فراخوانی روش، فرایند درونی PDUها) خارج ار محدوده این استاندارد است.

درخواست خدمت	درخواست یک خدمت جدید (نوع خدمت،PID)
ارسال اطلاعات	درخواست ارسال داده،قابل قبول فقط برای SCH (داده)
بازیابی داده	درخواست بازیابی داده دریافت شده، قابل قبول فقط برایSCH
بازیابی راز	درخواست برای بازیابی راز مشترک ایجاد شده، قابل قبول فقط برای SSE
پایاندهی	درخواست پایاندهی خدمت (نوع خدمت)

الف- ۳ تصدیق SDUها:

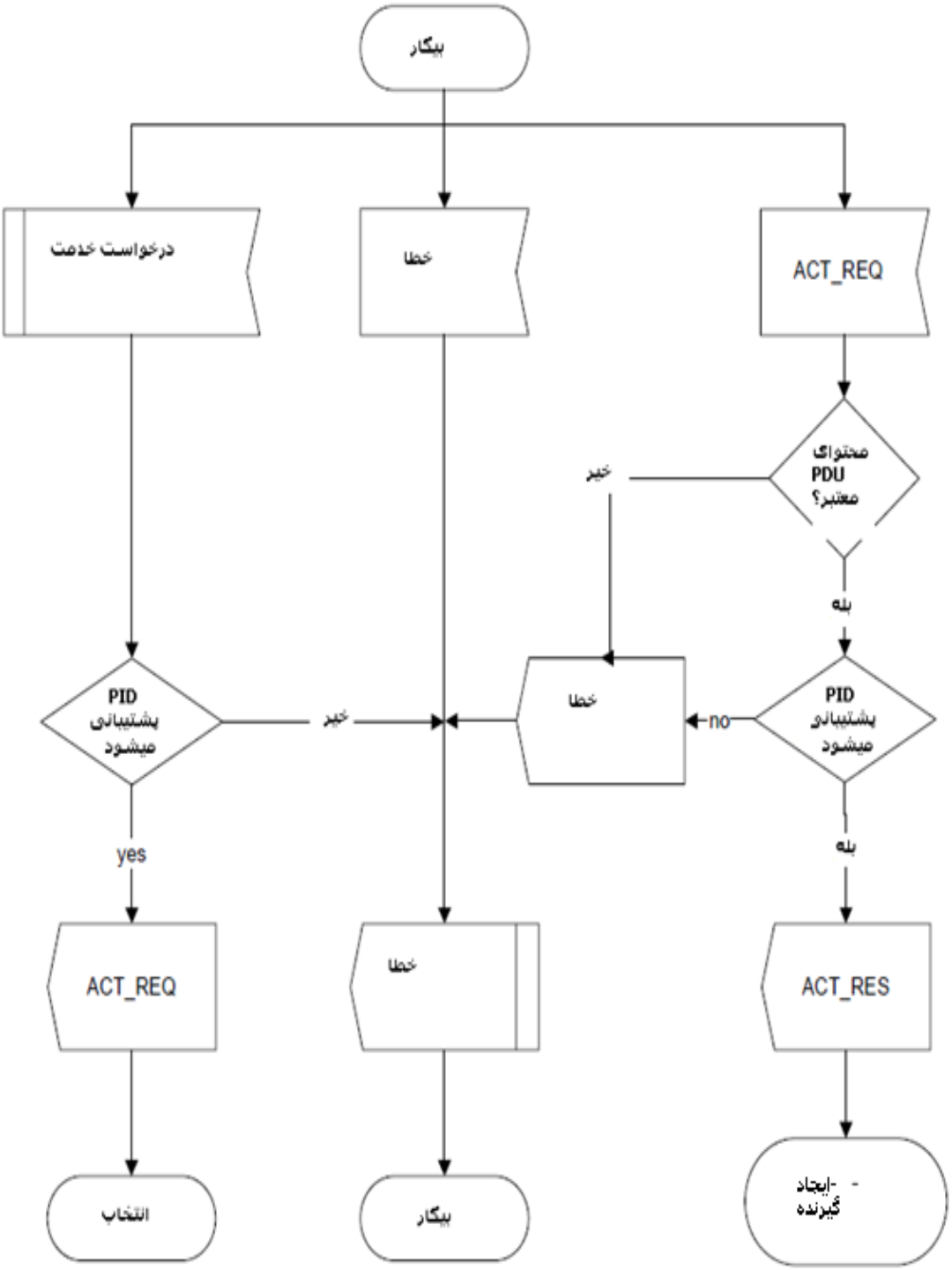
تصدیق SDUهای ارسال شده توسط هستارهای NFC-SEC به کاربران NFC-SEC. پارامترها در داخل پرانتز داده می‌شوند. الزامات بر روی مقادیر پارامترها در استانداردهای رمزنگاری NFC-SEC مشخص شده‌اند.

یادآوری- روش اجرای واقعی از شکل‌های هندسی اولیه تصدیق (به عنوان مثال: فراخوانی روش، فرایند درونی PDUها) خارج از محدوده این استاندارد است.

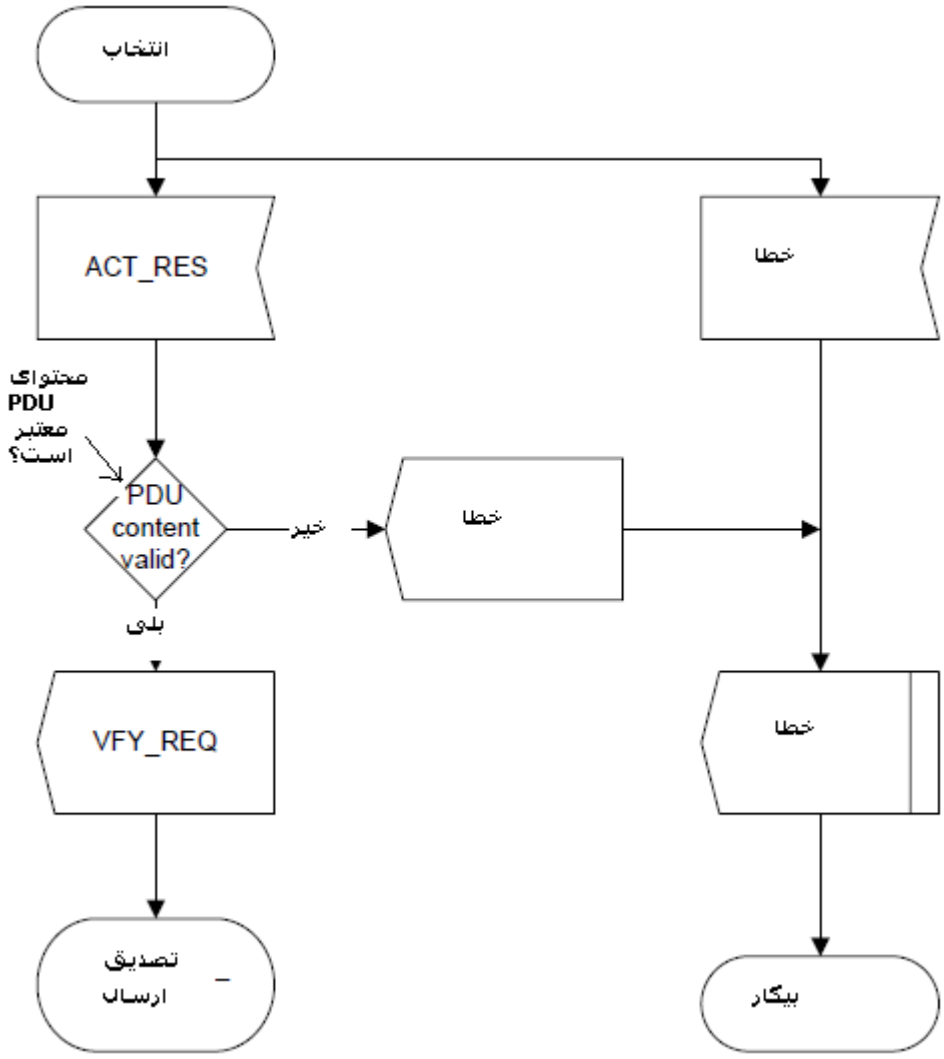
ایجاد	مشخص کننده موفقیت آمیز بودن ایجاد یک خدمت است (نوع خدمت)
داده‌های ارسال شده	مشحص کننده نتیجه درخواست ارسال داده است (حالت). این نتیجه ممکن است مثبت یا منفی باشدکه به علت وقوع خطا در ارسال و یا آماده نبودن هستار NFC-SEC برای ارسال داده باشد.
داده در دسترس	مشخص کننده رسید داده می‌باشد.
داده بازگشتی	پاسخ به درخواست بازیابی داده (داده)
راز بازگشتی	پاسخ به درخواست بازیابی راز (راز مشترک)
پایاندهی	به یک کاربر پایان خدمات را نشان می‌دهد .(نوع خدمت)
خطا	خطای ایجاد شده در طی پردازش درخواست و یا یک PDU ، و یا هر گونه خطا را نشان می‌دهد. پارامترها ممکن است دلیل خطا یا جزئیات آنرا منعکس کنند. (جزئیات)

الف-۴ دیاگرام‌های SDL

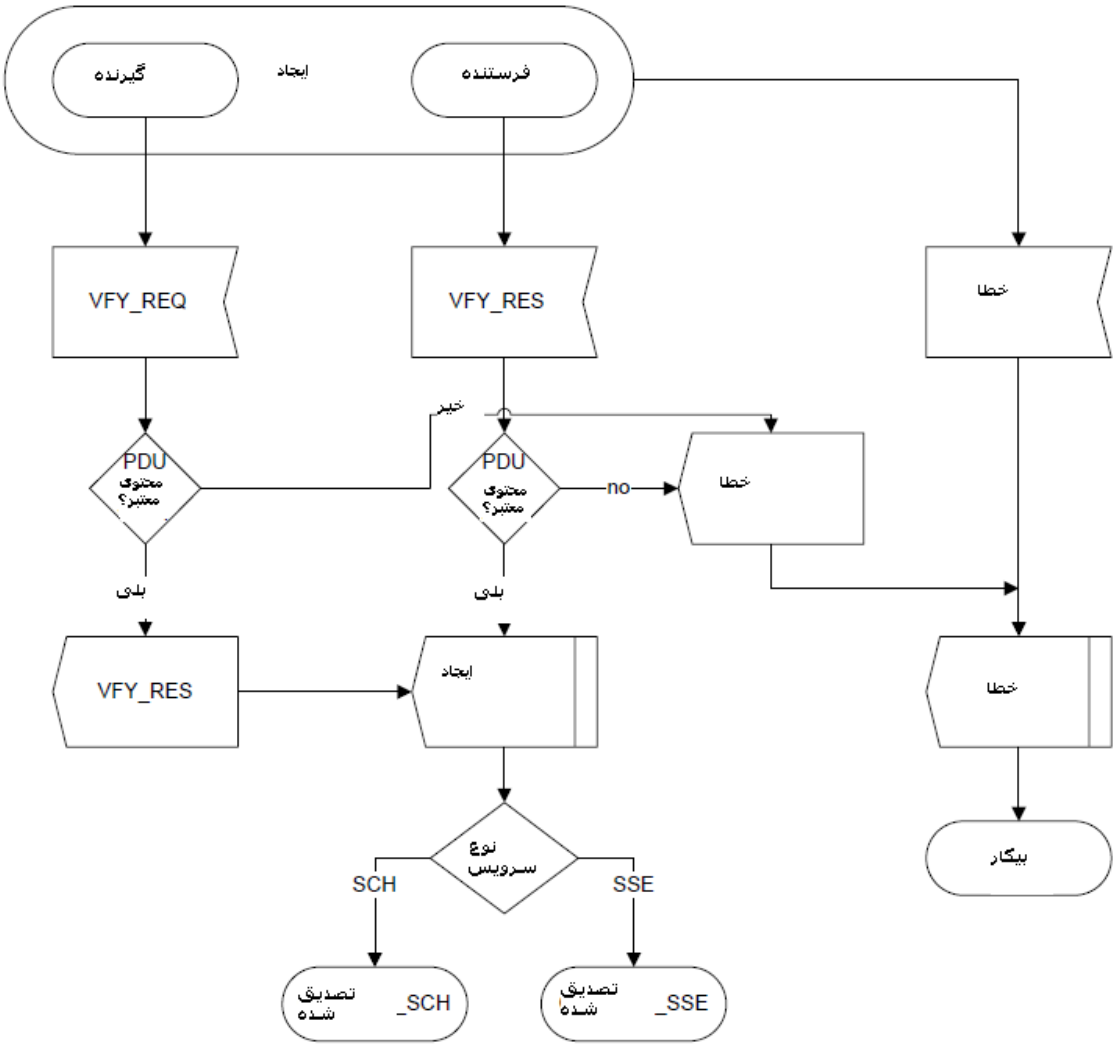
الف-۴-۱ حالت بیکار



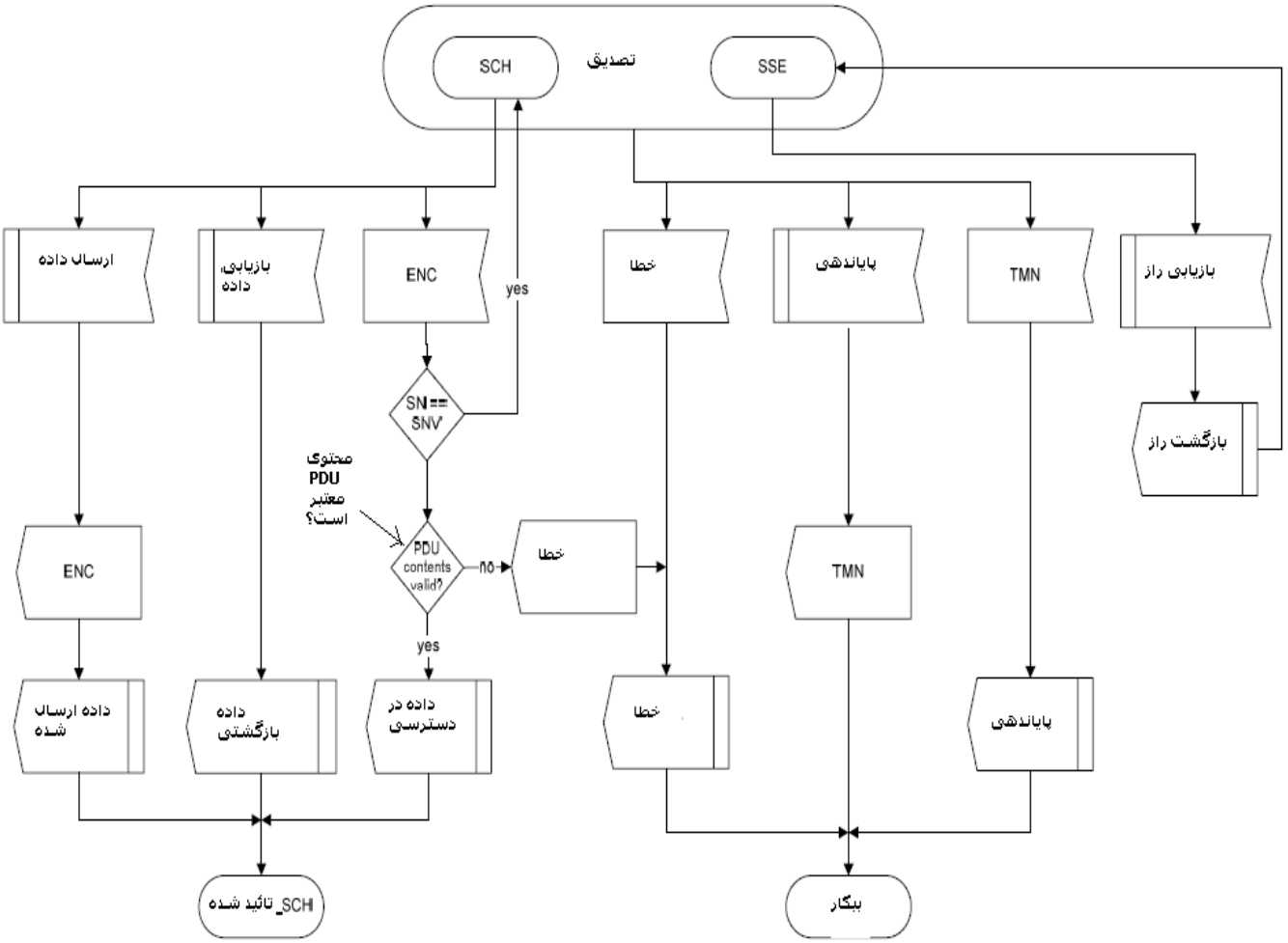
الف-۴-۲ حالت انتخاب



الف-۴-۳ حالت ایجاد



الف-۴-۴ حالت تصدیق



پیوست ب

(الزامی)

الزامات اضافی در هنگام استفاده از NFC-SEC با استاندارد بین‌المللی ISO/IEC 18092:2004 (NFCIP-1)

هنگام استفاده از این استاندارد با پیاده‌سازی استاندارد بین‌المللی ISO/IEC 18092:2004، الزامات اضافی زیر باید اعمال شود:

ب-۱ روش‌های که دستگاه NFCIP-1 ، حمایت خود را از NFC-SEC نشان می‌دهد

یک آغازگر حمایت خود را از NFC-SEC با مشخصه SECi در ATR_REQ نشان می‌دهد.
یک هدف حمایت خود را از NFC-SEC با مشخصه SECt در ATR_RES نشان می‌دهد.
برای تعریف مشخصههای SECi و SECt، به پیوست ب-۴ مراجعه شود.

ب-۲ مقدمه‌ای بر PDU حفاظت شده

PDU های اضافی حفاظت شده، همانطور که در بند ب-۴ مشخص شده، در پروتکل تبادل داده استفاده می‌شوند.

ب-۳ تعمیم قوانین شماره گذاری PDU ها برای PDU محافظت شده

PDU حفاظت شده در قوانین برای شماره گذاری PDU ها، همانطور که در بند ب-۴ مشخص شده، شامل هستند.

ب-۴ اصلاحات NFCIP-1

اصلاحات زیر به استاندارد بین‌المللی ISO/IEC 18092:2004 باید اعمال شوند:
در بند ۱۲-۵-۱-۱-۱ تعریف بیت ۷ از PPi با مورد زیر جایگزین شود:
بیت ۷: SECi. آغاز گر باید مقدار SECi را در صورتی که NFC-SEC را حمایت می‌کند ۱ و در صورتی که حمایت نمی‌کند ۰ قرار دهد.
در بند ۱۲-۵-۱-۲-۱ تعریف بیت ۷ از PPt با مورد زیر جایگزین شود:
بیت ۷: SECt. هدف باید مقدار SECt را در صورتیکه NFC-SEC را حمایت می‌کند ۱ و در صورتی که حمایت نمی‌کند ۰ قرار دهد.
به جای بند ۱۲-۶-۱-۱-۱ تعریف بایت FEB:0 ، جدول ۲۴ موارد زیر را قرار دهید:

بایت FEB:0

بایت PFB باید بیت برای کنترل انتقال داده‌ها و بازیابی خطا داشته باشد.
بایت PFB برای انتقال اطلاعات مورد نیاز کنترل انتقال استفاده می‌شود.
پروتکل تبادل اطلاعات این نوع اساسی از PDU ها را تعریف می‌کند:

- PDUهای اطلاعاتی برای انتقال اطلاعات برای لایه کاربردی
- PDUهای حفاظت شده برای انتقال اطلاعات حفاظت شده
- Acknowledge PDU'sPDUهای تصدیق برای انتقال تصدیق مثبت یامنفی. یک PDU تصدیق هرگز شامل مشخصه داده نیست و آخین بلوک دریافت شده را گزارش می‌دهند.
- PDUهای نظارت جهت تبادل داده های کنترلی بین آغازگر و هدف. دونوع PDU ی نظارتی تعریف شده‌اند:
  - پسوند اتمام مهلت زمان حاوی ۱ بایت مشخصه داده طولانی
  - توجه شامل مشخصه داده‌ای نیست

کدگذاری PFB بستگی به نوع آن و در جدول ب-۳ تعریف شده است.

جدول ب-۳ کد گذاریPFB بیت‌های ۷ تا ۵

FEB	بیت ۵	بیت ۶	بیت ۷
PDU های اطلاعاتی	۰	۰	۰
PDUهای حفاظت شده	۱	۰	۰
PDUهای تصدیقAcknowledge PDU's	۰	۱	۰
PDUهای نظارت	۰	۰	۱
سایر تنظیمات RFU			

اضافه کردن تعریف PDU حفاظت شده در بند ۱۲-۶-۱-۱-۱ و اضافه کردن شکل ب-۳ به شرح زیر است:

تعریف PDU حفاظت شده:

بیت ۰	بیت ۱	بیت ۲	بیت ۳	بیت ۴	بیت ۵	بیت ۶	بیت ۷
PNI	PNI	DID	NAD	MI	۱(ONE)	RFU	RFU

شکل ب-۳ کد گذاری PDU حفاظت شده

- بیت ۷ تا بیت ۶: RFU. آغازگر باید آن را صفر (ZERO) تنظیم کند. هدف باید آن را نادیده بگیرد.
- بیت ۵: باید به یک تنظیم شود.
- بیت ۴: اگر با یک تنظیم شوداطلاعات چند زنجیری فعال را نشان می‌دهد.
- بیت ۳: اگر به یک تنظیم شود در دسترس بودن NAD را نشان می‌دهد.
- بیت ۲: اگر به یک تنظیم شود در دسترس بودن DID را نشان می‌دهد.
- بیت ۱: PNI بسته شماره اطلاعات

بسته شماره اطلاعات (PNI) تعداد بسته ارسال شده توسط آغازگر را به مقصد و بلعکس که با صفر شروع می‌شود را می شمارد. این بایت‌ها برای تشخیص خطا در حیت بررسی پروتکل بکار می‌روند.

به جای بند ۱۲-۶-۱-۲ موارد زیر را قرار دهید:

بند ۱۲-۶-۱-۲ رسیدگی به اطلاعات تعداد PDU

بند ۱۲-۶-۱-۲-۱ قوانین آغازگر

PNI آغازگر باید برای هر هدف با تمام صفر مقدار دهی اولیه شود.

هنگامی که یک اطلاعات، PDU حفاظت شده یا تائید شده با PNI برابر دریافت شود، آغازگر باید مقدار PNI جاری را قبل از ارسال اختیاری یک قالب جدید افزایش دهد.

بند ۱۲-۶-۱-۲-۲ قوانین مقصد

PNI مقصد باید با تمام صفر مقدار دهی اولیه شود.

هنگامی که یک اطلاعات، PDU حفاظت شده یا تائید شده با PNI برابر دریافت شود، مقصد باید پاسخ خود را با این PNI ارسال و باید PNI را پس از آن افزایش دهد.

به جای بند ۱۲-۶-۱-۳-۱ موارد زیر را قرار دهید:

بند ۱۲-۶-۱-۳-۱ قوانین کلی

اولین PDU باید توسط آغازگر ارسال شود.

هنگامی که اطلاعات و یا PDU حفاظت شده نشان می‌دهد که اطلاعات بیشتری دریافت کرده است PDU باید توسط PDU تصدیق (ACK)، تصدیق شود.

PDUهای نظارت تنها به صورت جفت مورد استفاده قرار می‌گیرند. درخواست نظارت همیشه باید توسط یک پاسخ نظارت دنبال شود.

به جای بند ۱۲-۶-۱-۳-۳ موارد زیر را قرار دهید:

بند ۱۲-۶-۱-۳-۳ قوانین مقصد

هدف مجاز به ارسال PDU نظارت (RTO) به جای یک PDU اطلاعات است.

هنگامی که یک PDU اطلاعات یا حفاظت شده که شامل زنجیری نمی‌باشد دریافت شد باید توسط بک PDU اطلاعات یا حفاظت شده تصدیق شود.

وقتی یک PDU تصدیق(NACK) دریافت شد اگر PNI با PNI از PDU ارسالی قبلی برابر است، بلوک‌های قبلی باید دوباره انتقال یابند.

هنگامی که یک PDUی اشتباه دریافت کرده است مقصد نباید پاسخی بدهد اما در همان حالت باقی بماند.

هنگامی که یک PDUی نظارت(توجه) دریافت کرده است، مقصد باید پاسخ ارسال PDUی نظارت (توجه) پاسخ را بدهد.