INSO
18477-2
1st. Edition
2015

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۸۴۷۷-۲
چاپ اول
۱۳۹۳

فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها - امنیت ارتباط میدان نزدیک (NFC)- قسمت ۲: استاندارد رمزنگاری ارتباط میدان نزدیک امن (NFC-SEC) با به‌کارگیری منحنی‌های بیضوی دیفی-هلمن (ECDH) و استاندارد رمزبندی پیشرفته (AES)

Information technology - Telecommunications and information exchange between systems – NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES

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 اولیه 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 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 افزاره 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 ۲: استاندارد رمزنگاری ارتباط میدان نزدیک امن (NFC-SEC) با به‌کارگیری منحنی‌های بیضوی دیفی-هلمن (ECDH) و استاندارد رمزبندی پیشرفته (AES) »

رئیس:	**سمت و/ یا نمایندگی**
کشاورزی ، فرزاد (لیسانس مهندسی کامپیوتر نرم‌افزار)	کارشناس رایانه شرکت پیشاهنگان آمایش
دبیر:	
امیری ، حسین (لیسانس مهندسی کامپیوتر نرم‌افزار)	مدیر عامل شرکت نوآوران مبانی پرداز
اعضاء: (اسامی به ترتیب حروف الفبا)	
خندزاد ، بهزاد (لیسانس مهندسی کامپیوتر نرم‌افزار)	کارشناس رایانه شرکت نوآوران مبانی پرداز
خندزاد ، بیتا (فوق‌لیسانس هوش مصنوعی و رباتیک)	کارشناس ارشد ادارات مرکزی هواپیمائی جمهوری اسلامی ایران هما
درفشی ، رکسانا (لیسانس زبان انگلیسی)	کارشناس تایید صلاحیت سازمان استاندارد
سروشیان ، سپیده (لیسانس مهندسی کامپیوتر نرم‌افزار)	کارشناس رایانه شرکت پیشتازان پردازش اطلاعات
قاسمی ، رضا (فوق‌لیسانس ارتباطات – تحقیق در ارتباطات)	کارشناس رایانه دفتر پژوهشی صدا و سیما
موجبی ، محمود (فوق‌لیسانس مخابرات رمز)	کارشناس استاندارد
ندائی فرخد ، الهام (لیسانس مهندسی کامپیوتر نرم‌افزار)	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 ۲: استاندارد رمزنگاری ارتباط میدان نزدیک امن (NFC-SEC) با به‌کارگیری منحنی‌های بیضوی دیفی- هلمن (ECDH) و استاندارد رمزبندی پیشرفته (AES) » که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده و در سیصد و چهل و دومین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۱۳۹۳/۱۱/۱۵ 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 13157-2:2010, Information technology - Telecommunications and information exchange between systems – NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES

مقدمه

سری استانداردهای امنیت ارتباط میدان نزدیک (NFC)[1]، خدمات مشترک و استاندارد پروتکل و استانداردهای رمزنگاری ارتباط میدان نزدیک – امن (NFC_SEC)[2] را در برمی‌گیرند.

این استاندارد رمزنگاری NFC-SEC سازوکارهای رمزنگاری را مشخص می‌کند که از پروتکل منحنی‌های بیضوی دیفی-هلمن (ECDH)[3] برای توافق کلیدی و الگوریتم استاندارد رمزبندی پیشرفته (AES) [4] برای رمزبندی داده و یکپارچگی استفاده می‌کند.

این استاندارد ارتباط امن دو افزاره NFC را نشان می‌دهد که هیچگونه داده کلید مخفی مشترک (‹‹کلیدها››) را به اشتراک نمی‌گذارند پیش از اینکه شروع به ارتباط با یکدیگر کنند.

1- Near Field Communication
2- Near Field Communication - Secure
3- Elliptic Curves Diffie-Hellman
4- Advanced Encryption Standard

فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها- امنیت ارتباط میدان نزدیک (NFC)- قسمت ۲: استاندارد رمزنگاری ارتباط میدان نزدیک امن (NFC-SEC) با به‌کارگیری منحنی‌های بیضوی دیفی-هلمن (ECDH) و استاندارد رمزبندی پیشرفته (AES)

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین محتوای پیام و روش‌های رمزنگاری برای شناسانه پروتکل (۰۱) (PID 01) [1] است.

این استاندارد سازوکارهای رمزنگاری که پروتکل منحنی‌های بیضوی دیفی-هلمن را برای توافق کلید و الگوریتم AES را برای رمزبندی و یکپارچگی داده به‌کار می‌گیرد، مشخص می‌کند.

۲ انطباق

پیاده‌سازی‌های منطبق، سازوکارهای امنیتی مشخص شده در این استاندارد رمزنگاری NFC-SEC (با PID 01 شناسائی شده) و مطابق با استاندارد ISO / IEC 13157-1 را به خدمت می‌گیرد.

خدمات امنیتی NFC-SEC باید از طریق پروتکل مشخص شده در استاندارد ISO/IEC 13157-1 و سازوکارهای مشخص شده در این استاندارد بر پا گردند.

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 10116:2006, Information technology — Security techniques — Modes of operation for an n-bit block cipher

3-2 ISO/IEC 11770-3:2008, Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques

3-3 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 (also published by Ecma as Standard ECMA-385)

3-4 ISO/IEC 15946-1:2008, Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General

3-5 ISO/IEC 18031:2005, Information technology — Security techniques — Random bit generation

---

1- Protocol Identifier

3-6 ISO/IEC 18033-3:2005, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers
3-7 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)
3-8 IEEE 1363, IEEE Standard Specifications for Public-Key Cryptography
3-9 FIPS 186-2, Digital Signature Standard (DSS)

۴ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف به‌کار رفته در استاندارد بین‌المللی ISO/IEC 13157-1 به‌کار می‌رود

۵ نمادها و قراردادها

نمادها و قراردادهای استاندارد ISO / IEC 13157-1 و همچنین موارد زیر در این استاندارد اعمال می‌شود، مگر اینکه غیر این بیان شود.

۵-۱ الحاق[1]

A || B نشان دهنده الحاق فیلدهای A و B می‌باشد: محتوای A پس از محتوای B است.

۵-۲ اعداد مبنای ۱۶

(XY) نشان دهنده یک عدد مبنای شانزده XY (یعنی با مبنای ۱۶) و هر زوج نویسه در یک هشتایی کدبندی شده است.

۶ کوته‌نوشت‌ها

در این استاندارد کوته‌نوشت‌های به‌کار رفته در استاندارد بین‌المللی ISO/IEC 13157-1 و موارد ذیل به‌کار می‌رود:

A	Sender, as specified in ISO/IEC 13157-1 — فرستنده، همانگونه که در استاندارد بین‌المللی ISO/IEC 13157-1 مشخص شده است
AES	Advanced Encryption Standard — استاندارد رمزبندی پیشرفته
B	Receiver, as specified in ISO/IEC 13157-1 — دریافت کننده، همانگونه که در استاندارد بین‌المللی ISO/IEC 13157-1 مشخص شده است
d_A	Sender’s private EC key — کلید EC خصوصی فرستنده
d_B	Recipient’s private EC key — کلید EC خصوصی دریافت کننده
DataLen	Length of the UserData — طول داده کاربر
EC	Elliptic Curve — منحنی بیضوی
ECDH	Elliptic Curve Diffie-Hellman — منحنی بیضوی دیفی-هلمن
EncData	Encrypted data — داده رمزبندی شده

1- Concatenation

G	The base point on EC	نقطه پایه در EC
ID_A	Sender nfcid3	فرستنده nfcid3
ID_B	Recipient nfcid3	دریافت کننده nfcid3
ID_R	Any Recipient identification number (e.g. IDB)	شماره شناسایی هر دریافت کننده (به عنوان مثال ID_B)
ID_S	Any Sender identification number (e.g. IDA)	شماره شناسایی هر فرستنده(به عنوان مثال ID_A)
IV	Initial Value	مقدار آغازین
K	Key	کلید
KDF	Key Derivation Function	تابع اشتقاق کلید
KE	Encryption Key	کلید رمزبندی
KI	Integrity Key	یکپارچگی کلید
MAC	Message Authentication Code	کد اصالت سنجی پیام
Mac_A /Mac_B	Integrity protection value of Sender/ Recipient	مقدار حفاظت از یکپارچگی فرستنده/دریافت کننده
$MacTag_A$	Key confirmation tag from Sender	برچسب تایید کلید از فرستنده
$MacTag_B$	Key confirmation tag from Recipient	برچسب تایید کلید از دریافت کننده
MK	Master Key	کلید اصلی
NA / NB	Nonce generated by Sender/Recipient	نانس[1] تولید شده توسط فرستنده/دریافت کننده
NAA / NBB	Nonce generated by the pair of NFC-SEC entities	نانس تولید شده توسط جفت هستارهای NFC-SEC
$Nonce_S$	Sender’s nonce	نانس فرستنده
$Nonce_R$	Recipient’s nonce	نانس دریافت کننده
PK	Public Key	کلید عمومی
PK_R	Recipient’s Public Key	کلید عمومی دریافت کننده
PK_S	Sender’s Public Key	کلید عمومی فرستنده
PRNG	Pseudo Random Number Generator	مولد شماره شبه تصادفی
QA / QB	Compressed EC public key of Sender / Recipient	کلید عمومی EC فشرده شده فرستنده / دریافت کننده
Q_A / Q_B	Decompressed EC public key of Sender / Recipient	کلید عمومی EC غیر فشرده شده فرستنده / دریافت کننده

۱- (nounce): در مهندسی امنیت، هر نانس، عددی اختیاری است که تنها یکبار در ارتباط پنهانی استفاده می‌شود.

RNG	Random Number Generator	مولد شماره تصادفی
SharedSecret	Shared secret	کلید مخفی به اشتراک گذاشته‌شده
UserData	NFC-SEC User data	داده کاربر NFC-SEC
z	Unsigned integer representation of the Shared Secret	نمایش عدد صحیح بدون برچسب کلید مخفی به اشتراک گذاشته‌شده
Z	Octet string representation of z	نمایش رشته هشتایی از z

کوته‌نوشت‌هایی که در بند ۹ و ۱۰ استفاده شده‌اند و در بالا فهرست نشدند، پارامترهای رسمی هستند.

۷ کلیات

این استاندارد سازوکارهایی برای خدمت کلید مخفی به اشتراک گذاشته‌شده (SSE)[1] و خدمت کانال ایمن (SCH)[2] در استاندارد بین‌المللی ISO/IEC 13157-1 مشخص می‌کند.

جهت فعال کردن ارتباطی امن بین افزاره‌های NFC که هیچ داده کلید مخفی به اشتراک گذاشته‌شده‌ی («کلیدها») را پیش از اینکه شروع به برقراری ارتباط با یکدیگر کنند به اشتراک نمی‌گذارند، رمزنگاری کلید عمومی جهت برپاسازی یک کلید مخفی به اشتراک گذاشته‌شده بین این افزاره‌ها ایجاد می‌شود و بطور خاص بیشتر طرحواره تبادل کلید منحنی بیضوی دیفی-هلمن. این کلید مخفی به اشتراک گذاشته‌شده جهت برپاسازی SSE و SCH استفاده شده است.

۸ شناسانه پروتکل (PID)

این استاندارد باید از یک شناسانه پروتکل هشتایی PID با مقدار ۱ استفاده کند.

۹ نخستینه‌ها

این بند نخستینه‌های رمزنگاری را مشخص می‌کند. بند ۱۱ و ۱۲ کاربرد واقعی این عناصر اولیه را مشخص می‌کند.

جدول ۱ بطور خلاصه این ویژگی‌ها را بیان می‌کند.

جدول ۱ - خلاصه ویژگی‌ها

خدمات پشتیبانی	SSE (به استاندارد بین‌المللی ISO/IEC 13157-1 مراجعه شود) SCH (به استاندارد بین‌المللی ISO/IEC 13157-1 مراجعه شود)
توافق‌نامه کلید	ECDH P-192
KDF[3]	AES-XCBC-PRF-128
تایید کلیدی	AES-XCBC-MAC-96
رمزبندی داده	AES128-CTR

1- Shared Secret Service
2- Secure Channel Service
3- Key Derivation Function

	IV Init: AES-XCBC-PRF-128
یکپارچگی داده	AES-XCBC-MAC-96
یکپارچگی ترتیب	SN (به استاندارد بین‌المللی ISO/IEC 13157-1 مراجعه شود)
ترتیب رمزبندی	رمزبندی (بند ۹-۵) پیش از محاسبه MAC (بند ۹-۶)

۹-۱ توافق‌نامه کلید

هستارها باید نظیر NFC-SEC بر یک کلید مخفی به اشتراک گذاشته‌شده که سازوکار ۴ توافق‌نامه کلید از استاندارد ISO/IEC 11770-3 و عناصر اولیه منحنی‌های بیضوی دیفی-هلمن از استاندارد IEEE 1363 استفاده می‌کنند همانگونه که در زیر بیشتر مشخص شده موافقت کنند.

۹-۱-۱ منحنی P-192

منحنی P-192 باید همانگونه که در FIPS 186-2 مشخص شده استفاده شود.

۹-۱-۲ نخستینه تولید جفت کلید EC

کلید خصوصی d باید از یک فرآیند تصادفی یا شبه تصادفی مطابق با استاندارد ISO/IEC 18031 بدست آورده شود.

۱- کلید خصوصی d را از یک فرآیند تصادفی یا شبه تصادفی مطابق با استاندارد بین‌المللی ISO/IEC 18031 بدست آورید.

۲- کلید عمومی PK را بعنوان نقطه‌ای بر روی EC، PK=dG محاسبه کنید.

۹-۱-۳ اعتبارسنجی کلید عمومی EC

کلید عمومی EC باید همانگونه که در اعتبارسنجی کلید عمومی استاندارد بین‌المللی ISO/IEC 15946-1 مشخص شده، اعتبارسنجی شود.

۹-۱-۴ نخستینه اشتقاق مقدار مخفی ECDH

عناصر اولیه ECDH همانگونه که در بند ۷-۲-۱ ECSVDP-DH of IEEE 1363 مشخص شده باید کلید مخفی به اشتراک گذاشته‌شدهی «معتبر» z و در غیر اینصورت «نامعتبر» را خروجی دهد.

۹-۱-۵ نانس‌های تصادفی

هر هستار نظیر NFC-SEC باید نانس‌های تصادفی تازه‌ای را با کلید عمومی EC هستار ارسال کند.

نانس‌ها به منظور فراهم نمودن آنتروپی بیشتری جهت اشتقاق کلیدها از کلید مخفی به اشتراک گذاشته‌شده (z) و آسان کردن مدیریت جفت کلید EC به‌کار برده می‌شوند.

تولید صحیح این نانس‌ها تحت مسئولیت هستار است.

هستار باید تضمین کند برای نانس‌هایی که تولید می‌کند دارای ۹۶ بیت از آنتروپی معتبر برای طی دوره پروتکل باشد. نانس‌های استفاده شده در یک تراکنش NFC-SEC باید بطور ناهمبسته با نانس‌های تراکنش قبلی، رمزنگاری شوند.

جهت توصیه‌های بیشتر در خصوص تولید شماره تصادفی به استاندارد بین‌المللی ISO/IEC 18031 مراجعه شود.

۹-۲ توابع اشتقاق کلید

دو تابع اشتقاق کلید (KDF) مشخص شده است؛ یکی برای SSE و یکی برای SCH.

باید که KDFها از SCH در حالت XCBC-PRF-128 استفاده کنند، همانگونه که در پیوست الف-۱ مشخص شده است.

برای قسمت‌های زیر KDF بدین شرح است:

$KDF\ (K, S) = AES\text{-}XCBC\text{-}PRF\text{-}128_K\ (S)$

باید که منبع تصادفی (نانس‌ها + کلید مخفی به اشتراک گذاشته‌شده z بدست آمده از بند ۹-۱-۴) استفاده شده برای SCH متفاوت از منبع تصادفی استفاده شده برای SSE باشد.

۹-۲-۱ KDF برای SSE

KDF برای SSE بدین شرح است:

$MK_{SSE} = KDF\text{-}SSE\ (Nonce_S, Nonce_R, SharedSecret, ID_S, ID_R)$

جزئیات تابع KDF-SSE بدین شرح است:

$S = (Nonce_S\ [0..63] \| Nonce_R\ [0..63])$
$SKEYSEED = KDF\ (S, SharedSecret)$
$MK_{SSE} = KDF\ (SKEYSEED, S \| ID_S \| ID_R \| (01))$

۹-۲-۲ KDF برای SCH

KDF برای SCH بدین شرح است:

$\{MK_{SCH}, KE_{SCH}, KI_{SCH}\} = KDF\text{-}SCH\ (Nonce_S, Nonce_R, SharedSecret, ID_S, ID_R)$

جزئیات تابع KDF-SCH بدین شرح است:

$S = (Nonce_S\ [0..63] \| Nonce_R\ [0..63])$
$SKEYSEED = KDF(S, SharedSecret)$
$MK_{SCH} = KDF\ (SKEYSEED, S \| ID_S \| ID_R \| (01))$
$KE_{SCH} = KDF\ (SKEYSEED, MK_{SCH} \| S \| ID_S \| ID_R \| (02))$
$KI_{SCH} = KDF\ (SKEYSEED, KE_{SCH} \| S \| ID_S \| ID_R \| (03))$

۹-۳ کاربرد کلید

هرکدام از کلیدهای مشتق شده MK_{SCH}، KE_{SCH}، KI_{SCH} و MK_{SSE} باید که فقط به منظور مشخص شده در جدول ۲ استفاده شوند.

کلیدهای MK_{SCH}، KE_{SCH}، KI_{SCH} و MK_{SSE} باید که برای هر کدام از تراکنش‌های NFC-SEC متفاوت باشد.

جدول ۲ - کاربرد کلید

کلید	شرح کلید	کاربرد کلید
MK_{SCH}	شاه کلید برای SCH	درستی‌سنجی کلید برای کلیدهای کانال امن
KE_{SCH}	کلید رمزبندی برای SCH	رمزبندی بستک‌های داده‌های ارسالی از طریق SCH
KI_{SCH}	کلید حفاظت یکپارچگی برای SCH	حفاظت یکپارچگی بستک‌های داده‌های ارسالی از طریق SCH
MK_{SSE}	شاه کلید برای SSE	شاه کلید برای SSE به عنوان کلید مخفی به اشتراک گذاشته‌شده جهت گذر دادن به لایه بالاتر و درستی‌سنجی کلید استفاده شده است.

۹-۴ تایید کلید

زمانی که کلید مشتق شده‌ای یکی از پردازش‌های KDF توصیف شده در بند ۹-۲ را استفاده می‌کند، هر دو هستار NFC-SEC بررسی می‌کنند که آنها براستی کلید مشابهی داشته باشند. هر هستار باید که برچسب تایید کلیدی را همانگونه که در بند ۹-۴-۱ مشخص شده، تولید و به هستار نظیر خود ارسال کند. هستارها باید که برچسب تایید روی رسید دریافتی را همانگونه که در بند ۹-۴-۲ مشخص شده، بازبینی کنند.
ساز و کار این تایید کلید مطابق با تایید کلید ۹ استاندارد بین‌المللی ISO/IEC 11770-3 است.
MAC بکارگرفته شده برای تایید کلید (MacTag) باید AES در حالت XCBC-MAC-96 همانگونه که در پیوست الف-۲ مشخص شده است باشد.

۹-۴-۱ تولید برچسب تایید کلید

برچسب تایید کلید MacTag برابر است با
MAC-KC (K, MsgID, IDS, IDR, PKS, PKR) و باید با بکارگیری
AES-XCBC-MAC-96$_K$ ($MsgID \parallel ID_S \parallel ID_R \parallel PK_S \parallel PK_R$) که در پیوست الف-۲ با کلید K مشخص شده است، محاسبه شود.

۹-۴-۲ درستی‌سنجی برچسب تایید کلید

اگر MacTag' برابر با MAC-KC (K, MsgID, IDS, IDR, PKS, PKR) باشد، مقدار برگشتی MAC-KC-VER (K, MsgID, ID_S, ID_R, PK_S, PK_R, MacTag') برای وضعیت درست است.

۹-۵ رمزبندی داده‌ها

الگوریتم بکارگرفته شده جهت رمزبندی داده‌ها همان AESای است که در بند ۵-۱ AES از استاندارد بین‌المللی ISO/IEC 18033-3 مشخص شده است.
حالت رمزبندی داده‌ها باید همان CRTای باشد که در حالت ۱۰ شمارشگر (CRT) از استاندارد بین‌المللی ISO/IEC 10116 مشخص شده است.

۹-۵-۱ مقدار آغازین شمارشگر (IV)

برای جلوگیری از نیاز به ارسال مقدار آغازین شمارشگر، باید که توسط هر دو هستار نانس محاسبه شوند.
IV، مقدار آغازین شمارشگر برابر است با

MAC-IV (MK, KI, NonceS, NonceR) و باید با بکارگیری

AES-XCBC-PRF-128MK (KI || NonceS || NonceR || (04)) که در پیوست الف-۱ با کلید MK مشخص شده است، محاسبه شود.

۹-۵-۲ رمزبندی

داده‌ها باید با استفاده از همان کلید رمزبندی KE که در بند ۱۰-۲ رمزبندی از استاندارد بین‌المللی ISO/IEC 10116 مشخص شده است، رمزبندی شوند:

$EncData = ENC_{KE} (Data)$

از آنجا که حالت CRT است، هیچگونه لایه‌گذاری[1] از داده‌ها نباید اعمال شود.

۹-۵-۳ رمزگشایی

داده‌های رمزبندی شده باید با بکارگیری همان کلید رمزبندی KE که در بند ۱۰-۳ رمزگشایی از استاندارد بین‌المللی ISO/IEC 10116 مشخص شده است، رمزگشایی شوند:

$Data' = DEC_{KE} (EncData)$

۹-۶ یکپارچگی داده‌ها

یکپارچگی تمامی داده‌های انتقال یافته بر روی SCH باید که از طریق یک MAC نگه داشته شود.

MAC به‌کار گرفته شده برای یکپارچگی داده‌ها باید که همان AES در حالت XCBC-MAC-96 باشد که در پیوست الف-۲ مشخص شده است.

۹-۶-۱ یکپارچگی داده‌های حفاظت شده

Mac، کد اصالت سنجی پیام برابر است با

MAC-DI (KI, SN, DataLen, EncData) و باید با بکارگیری

$AES\text{-}XCBC\text{-}MAC\text{-}96_{KI}$ (SN || DataLen || EncData) که در پیوست الف-۲ با کلید KI مشخص شده است، محاسبه شود.

۹-۶-۲ یکپارچگی داده‌های بررسی شده

اگر Mac' برابر با MAC-DI (KI, SN || DataLen || EncData) باشد، مقدار برگشتی MAC-DI-VER (KI, SN, DataLen, EncData, Mac') برای وضعیت درست است.

۹-۷ یکپارچگی توالی پیام

باید که یکپارچگی توالی پیام به همانگونه که در بند ۱۲-۳ از استاندارد بین‌المللی ISO/IEC 13157-1 مشخص شده است، بکارگرفته شود.

باید که مقدار SNV در دامنه صفر تا ۱-۲^۲۴ باشد؛ با مقدار آغازین صفر.

هستارها باید زمانی که SNV به ۱-۲^۲۴ می رسد، SCH را به پایان رسانند.

1- Padding

۱۰ تبدیل داده‌ها

۱۰-۱ تبدیل عدد صحیح به رشته هشتایی

ورودی: عدد صحیحی غیر منفی X، و طول مورد نظر k از رشته هشتایی مورد قبول: $X<2^{8k}$.

خروجی: یک رشته هشتایی M به طول k هشتایی.

M_1، M_2، ...، M_k هشتایی‌های M از سمت چپ‌ترین به سمت راست‌ترین قرار می‌گیرند.

هشتایی‌های M باید بدین صورت ایفا گردند:

$$x = \sum_{i=1}^{k} 2^{8(k-1)} M_i$$

۱۰-۲ تبدیل رشته هشتایی به عدد صحیح

ورودی: یک رشته هشتایی M به طول k هشتایی.

خروجی: یک عدد صحیح X.

M_1، M_2، ...، M_k هشتایی‌های M از سمت چپ‌ترین به سمت راست‌ترین قرار می‌گیرند.

M باید به یک عدد صحیح X مورد قبولی تبدیل گردد:

$$x = \sum_{i=1}^{k} 2^{8(k-1)} M_i$$

۱۰-۳ تبدیل نقطه به رشته هشتایی

نقطه روی منحنی بیضوی باید به طریق ذیل به یک رشته هشتایی تبدیل شود:

ورودی: یک نقطه روی منحنی بیضوی $P = (X_P, Y_P)$.

خروجی: یک رشته هشتایی PO با مختصات Y در سمت چپ‌ترین هشتایی و مختصات X در باقیمانده رشته هشتایی.

۱- تبدیل عنصر مشخصه X_P به یک رشته هشتایی X همانگونه که در بند ۱۰-۱ مشخص شده است.

۲- محاسبه بیت $\tilde{Y}_P$ همانگونه که در بند ۶-۶ مشخص شده است: نقطه منحنی بیضوی / تبدیل رشته هشتایی: EC2OSPE و OS2ECPE از استاندارد بین‌المللی ISO/IEC 15946-1.

۳- نشاندن مقدار (۰۲) به واحد هشتایی PC اگر $\tilde{Y}_P$ صفر باشد، یا مقدار (۰۳) اگر $\tilde{Y}_P$ برابر با یک باشد.

۴- نتیجه یک رشته هشتایی است $PO = PC \parallel X$.

۱۰-۴ تبدیل رشته هشتایی به نقطه

یک رشته هشتایی باید به طریق ذیل به نقطه روی منحنی بیضوی تبدیل شود:

ورودی: یک رشته هشتایی PO با مختصات Y در سمت چپ‌ترین هشتایی و مختصات X در باقیمانده رشته هشتایی.

خروجی: یک نقطه روی منحنی بیضوی $P = (X_P, Y_P)$

۱- PO بدین شرح تجزیه می‌شود: PO = PC || X ،درجایی که PC یک واحد هشتایی و X یک رشته هشتایی با طول K هشتایی است.

۲- تبدیل X به عنصر مشخصه xP همانگونه که در بند ۱۰-۲ مشخص شده است.

۳- درستی‌سنجی PC از این لحاظ که مقدار آن (۰۲) یا (۰۳) است. غیر از این حالت این یک خطا است.

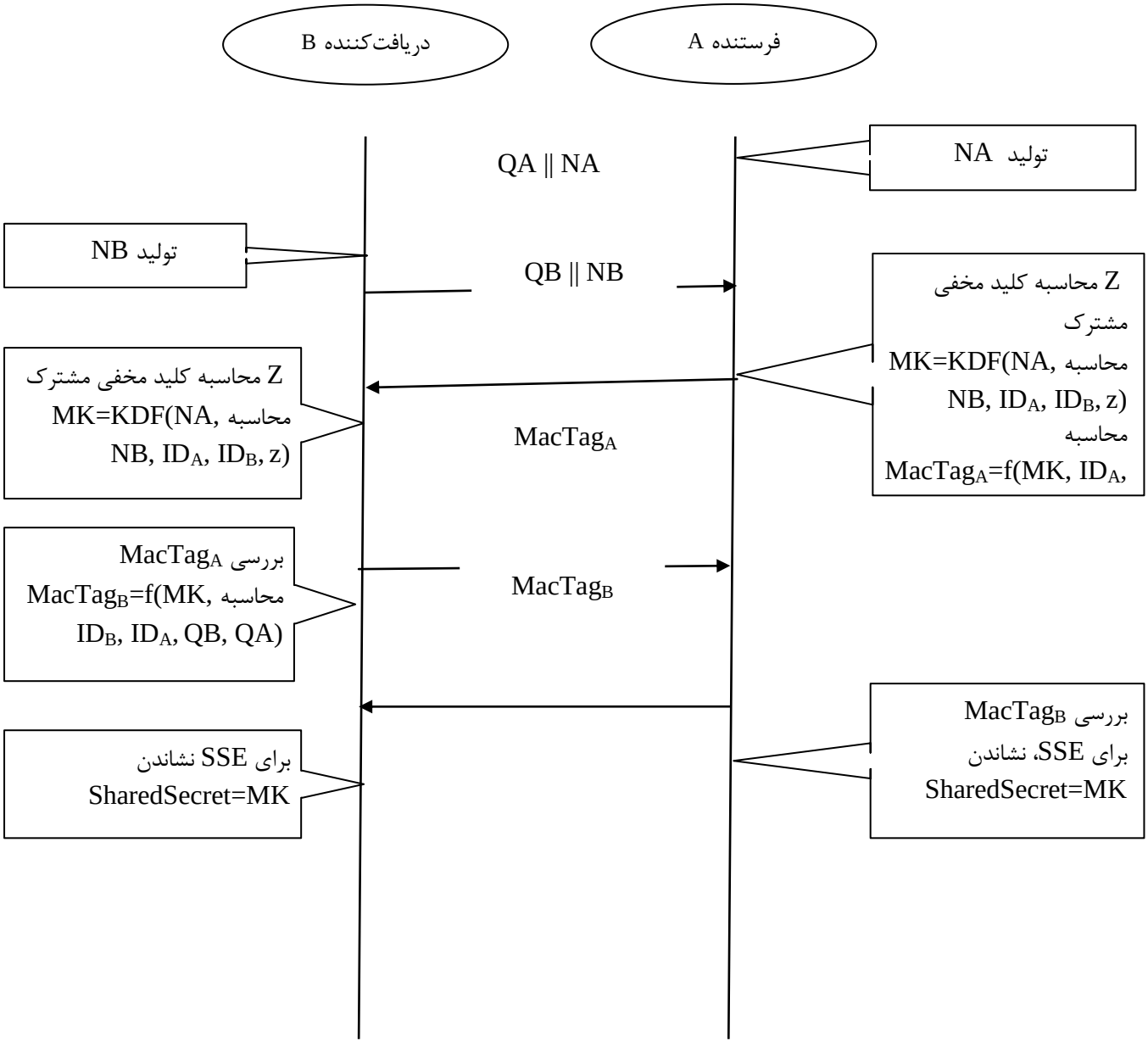
۴- نشاندن بیت $\tilde{Y}P$ به مقدار صفر اگر (۰۲) = PC باشد و یا ۱ اگر (۰۳) = PC باشد.

۵- تبدیل $(X_P, \tilde{Y}_P)$ به یک نقطه روی منحنی بیضوی (X_P, Y_P) همانگونه که در بند ۶-۶ مشخص شده است: نقطه منحنی بیضوی / تبدیل رشته هشتایی: EC2OSPE و OS2ECPE از استاندارد بین‌المللی ISO/IEC 15946-1.

۶- نتیجه $P=(X_P, Y_P)$ است.

۱۱ فراخوانی خدمت SSE و SCH

SSE و SCH با استقرار یک کلید مخفی به اشتراک گذاشته‌شده بین دو هستار NFC-SEC با استفاده توافق‌نامه کلید و پروتکل تایید کلیدکه در ISO/IEC 13157-1 مشخص شده‌اند، در مسیری که در شکل ۱ مصور گردیده و در ادامه آن در این بند مشخص شده است، فراخوانده می‌شوند.



شکل ۱ - نمای کلی تایید و توافق‌نامه کلید

۱۱-۱ پیش‌نیازها

پیش از شروع خدمت، باید موارد زیرین برای هر هستار NFC-SEC در دسترس باشند:

- تولید کلید عمومی و خصوصی خود منحنی بیضوی، همانگونه که در بند ۹-۱-۲ مشخص شده است.

یادآوری: زمانی که (و در آن بسامد) این جفت کلید منحنی بیضوی تولید می‌شوند، خارج از حوزه این استاندارد ملی است.

- خود nfcid3 و سایر nfcid3های هستار NFC-SEC، همانگونه که در استاندارد بین‌المللی ISO/IEC 18092 مشخص شده است.

۱۱-۲ توافق‌نامه کلید

فرستنده (A)	واحد داده‌های پروتکل(PDU) [1] جهت ارتباط با نویسه جهت‌نما[2] نشان داده شده است. پایه مفید[3] بین () است.	دریافت‌کننده (B)
تولید نانس NA		
فشرده‌سازی Q_A		
ارسال به B	A→B: ACT_REQ (QA || NA)	
		تولید نانس NB
		فشرده‌سازی Q_B
	A←B: ACT_RES (QB || NB)	ارسال به A
نوسازی Q_B' از QB'		نوسازی Q_A' از QA'
بررسی Q_B'		بررسی Q_A'
محاسبه کلید مخفی به اشتراک گذاشته‌شده Z		محاسبه کلید مخفی به اشتراک گذاشته‌شده Z

۱۱-۲-۱ تبدیل فرستنده (A)

۱- تولید نانس NA همانگونه که در بند ۹-۱-۵ مشخص شده است.

۲- اطمینان از اینکه QA برابر با همان رشته هشتایی QA یاشد که در بند ۱۰-۳ مشخص شده است.

۳- فرستاندن NA || QA به عنوان ACT_REQ PDU.

۴- دریافت NB' || QB' به عنوان پایه بار ACT_RES PDU.

۵- نوسازی Q_B' از QB' همانگونه که در بند ۱۰-۴ مشخص شده است.

الف- اگر در حال حاضر کلیدهای عمومی دریافت شده بودند، مقدار محاسبه و ذخیره شده Q_B' ممکن است دوباره مورد استفاده قرار گیرد و مراحل زیرین کنار گذاشته شوند.

۶- درستی‌سنجی آن QB' کلید معتبری برای پارمترهای منحنی بیضوی است همانگونه که در بند ۹-۱-۳ مشخص شده است. اگر نامعتبر باشد، «محتویات معتبر PDU» به مقدار نادرست در ماشین پروتکل نشانده می‌شود و مراحل ۷ و ۸ کنار می‌روند.

۷- استفاده از عناصر اولیه دیفی-هلمن در بند ۹-۱-۴. اگر خروجی z نامعتبر باشد، «محتویات معتبر PDU» به مقدار نادرست در ماشین پروتکل نشانده می‌شود و مرحله ۸ کنار می‌رود.

۸- تبدیل z به رشته هشتایی Z با استفاده از تبدیلی که در بند ۱۰-۱ مشخص شده است.

۱۱-۲-۲ تبدیل دریافت‌کننده (B)

۱- دریافت NA' || QA' از پایه بار ACT_REQ PDU.

1- Protocol Data Unit
2- Arrow Character
3- Payload

۲- تولید نانس NB همانگونه که در بند ۹-۱-۵ مشخص شده است.
۳- اطمینان از اینکه QB برابر با همان رشته هشتایی QB یاشد که در بند ۱۰-۳ مشخص شده است.
۴- ارسال NB || QB به عنوان پایه بار ACT_RES PDU.
۵- نوسازی Q_A' از QA' همانگونه که در بند ۱۰-۴ مشخص شده است.
الف- اگر در حال حاضر کلیدهای عمومی دریافت‌شده بودند، مقدار محاسبه و ذخیره شده Q_A' ممکن است دوباره مورد استفاده قرار گیرد و مراحل زیرین کنار روند.
۶- درستی‌سنجی آن QA' کلید معتبری برای پارمترهای منحنی بیضوی است همانگونه که در بند ۹-۱-۳ مشخص شده است. اگر نامعتبر باشد، «محتویات معتبر PDU» به مقدار نادرست در ماشین پروتکل نشانده می‌شود و مراحل ۷ و ۸ کنار می‌روند.
۷- استفاده از عناصر اولیه دیفی-هلمن در بند ۹-۱-۴. اگر خروجی z نامعتبر باشد، «محتویات معتبر PDU» به مقدار نادرست در ماشین پروتکل نشانده می‌شود و مرحله ۸ کنار می‌رود.
۸- تبدیل z به رشته هشتایی Z با استفاده از تبدیلی که در بند ۱۰-۱ مشخص شده است.

۱۱-۳ اشتقاق کلید

۱۱-۳-۱ تبدیل فرستنده (A)

برای خدمت SSE، MK_{SSE} = KDF-SSE (NA, NB', Z, ID_A, ID_B) مشتق می‌شود، همانگونه که در بند ۹-۲-۱ مشخص شده است.

برای خدمت SCH، {MK_{SCH}, KE_{SCH}, KI_{SCH}} = KDF-SCH (NA, NB', Z, ID_A, ID_B) مشتق می‌شود، همانگونه که در بند ۹-۲-۲ مشخص شده است.

۱۱-۳-۲ تبدیل دریافت‌کننده (B)

برای خدمت SSE، MK_{SSE} = KDF-SSE (NA', NB, Z, ID_A, ID_B) مشتق می‌شود، همانگونه که در بند ۹-۲-۱ مشخص شده است.

برای خدمت SCH، {MK_{SCH}, KE_{SCH}, KI_{SCH}} = KDF-SCH (NA', NB, Z, ID_A, ID_B) مشتق می‌شود، همانگونه که در بند ۹-۲-۲ مشخص شده است.

۱۱-۴ تایید کلید

فرستنده (A)	واحد داده‌های پروتکل جهت ارتباط با برچسب جهت‌نما نشان داده شده است. پایه بار بین () است.	دریافت‌کننده (B)
محاسبه برچسب تایید کلید: $MacTag_A$(MK)		
ارسال به B	A→B: VFY_REQ ($MacTag_A$)	
		بررسی برچسب تایید کلید دریافت شده از A: $MacTag_A$'(MK)

		محاسبه برچسب تایید کلید: $MacTag_B(MK)$
	A←B: VFY_RES ($MacTag_B$)	ارسال به A
بررسی برچسب تایید کلید دریافت شده از B: $MacTag_B'(MK)$		
برای SSE، مقدار کلید مخفی به اشتراک گذاشته‌شده به MK نشانده می‌شود.		برای SSE، مقدار کلید مخفی به اشتراک گذاشته‌شده به MK نشانده می‌شود.

۱۱-۴-۱ تبدیل فرستنده (A)

۱- برچسب تایید کلید از A به B به صورت MacTagA = MAC-KC(MK , (03), IDA, IDB, QA, QB') محاسبه می شود، همانگونه که در بند ۹-۴-۱ مشخص شده است.

۲- ارسال MacTagA به عنوان پایه بار VFY_REQ PDU.

۳- دریافت کردن MacTagB' از پایه بار VFY_RES PDU.

۴- بررسی کردن برچسب تایید کلید از B به A. نشاندن ‹‹محتویات معتبر PDU›› در ماشین پروتکل به خروجی MAC-KC-VER(MK, (02), IDB, IDA, QB', QA, MacTagB')، همانگونه که در بند ۹-۴-۲ مشخص شده است. اگر نامعتبر باشد مرحله ۵ کنار می‌رود.

۵- برای خدمت SSE، $SharedSecret = MK_{SSE}$ نشانده می‌شود.

۱۱-۴-۲ تبدیل دریافت‌کننده (B)

۱- دریافت کردن MacTagA' از پایه بار VFY_REQ PDU.

۲- بررسی کردن برچسب تایید کلید از A به B. نشاندن ‹‹محتویات معتبر PDU›› در ماشین پروتکل به خروجی MAC-KC-VER(MK, (03), IDA, IDB, QA', QB, MacTagA')، همانگونه که در بند ۹-۴-۲ مشخص شده است. اگر نامعتبر باشد مراحل ۳، ۴ و ۵ کنار می‌روند.

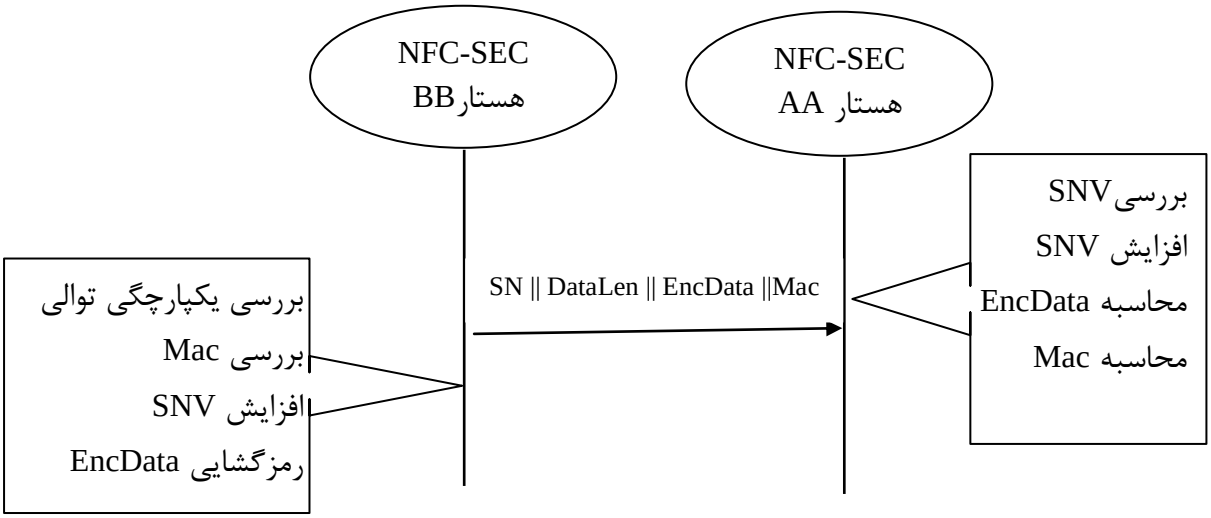
۳- برچسب تایید کلید از B به A به صورت MacTagB = MAC-KC(MK , (02), IDB, IDA, QB, QA') محاسبه می شود، همانگونه که در بند ۹-۴-۱مشخص شده است.

۴- ارسال MacTagB به عنوان پایه بار VFY_RES PDU.

۵- برای خدمت SSE، $SharedSecret = MK_{SSE}$ نشانده می‌شود.

۱۲ تبادل داده‌های SCH

بعد از فراخوانی SCH همانگونه که در بند ۱۱ مشخص شده است، تبادل داده‌ها بین دو هستار NFC-SEC، پروتکل مشخص شده در استاندارد بین‌المللی ISO/IEC 13157-1 را همانگونه که در شکل ۲ مصور گردیده و در ادامه آن در این بند مشخص شده است، استفاده می‌کند.



شکل ۲ – SCH: نمای کلی پروتکل

۱-۱۲ آماده‌سازی

هستار NFC-SEC (AA و BB) باید مراحل آماده‌سازی زیرین را انجام دهد:

۱ - تولید مقدار آغازین شمارشگر CTR بدین صورت که IV = MAC-IV (MK, KI, NAA, NBB)، همانگونه که در بند ۹-۵-۱ مشخص شده است.

۲- مقداردهی اولیه به متغیر شماره توالی (SNV)، همانگونه که در بند ۹-۷ مشخص شده است.

۲-۱۲ تبادل داده‌ها

ارسال هستار نظیرAA (A یا B)	واحد داده‌های پروتکل فرستاده‌شده جهت ارتباط با برچسب جهت‌نما نشان داده شده است. پایه بار بین () است.	دریافت هستار نظیرBB (A یا B)
• دریافت داده‌های کاربر از داده‌های ارسالی واحد داده‌های ارسالی (SDU) [1] • بررسیSNV • افزایش SNV • رمزبندی داده‌ها: EncData • اعمال MAC: Mac		
	ENC (SNV || DataLen || EncData || Mac)	
		دریافت: • بررسی یکپارچگی توالی

1- Send Data Unit

		• بررسی یکپارچگی داده‌ها • رمزگشایی داده‌ها

۱-۲-۱۲ ارسال

جهت ارسال داده‌ها، ارسال AA (A یا B) هستار نظیرNFC-SEC باید مراحل زیرین انجام شوند:

۱- دریافت داده‌های کاربر از داده‌های ارسالی SDU.

۲- اگر ۲^۲۴-۱ = SNV باشد، «محتویات معتبر PDU» در ماشین پروتکل به مقدار نادرست نشانده می‌شود، در غیر اینصورت برای مرحله بعدی اقدام می‌شود.

۳- افزایش SNV همانگونه که در بند ۱۲-۳ از استاندارد بین‌المللی ISO/IEC 13157-1 مشخص شده است.

۴- محاسبه داده‌های رمزبندی شده، EncData از داده‌های کاربر، همانگونه که در بند ۹-۵-۲ مشخص شده است.

۵- محاسبه MAC، Mac روی EncData || DateLen || SNV ،همانگونه که در بند ۹-۶-۱ مشخص شده است.

۶- ارسال Mac || EncData || DataLen || SNV به عنوان پایه بار ENC PDU.

۲-۲-۱۲ دریافت

جهت دریاف داده‌ها، دریافت BB (A یا B) هستار نظیرNFC-SEC باید مراحل زیرین انجام شوند:

۱- دریافت Mac || EncData || DataLen || SNV به عنوان پایه بار ENC PDU.

۲- اگر ۲^۲۴-۱ = SNV باشد، «محتویات معتبر PDU» در ماشین پروتکل به مقدار نادرست نشانده می‌شود، در غیر اینصورت برای مرحله بعدی اقدام می‌شود.

۳- بررسی یکپارچگی توالی، همانگونه که در بند ۱۲-۳ از استاندارد بین‌المللی ISO/IEC 13157-1 مشخص شده است.

۴- بررسی یکپارچگی داده‌های EncData || DataLen || SNV، همانگونه که در بند ۹-۶-۲ مشخص شده است. اگر نامعتبر باشد، «محتویات معتبر PDU» در ماشین پروتکل به مقدار نادرست نشانده می‌شود، در غیر اینصورت برای مرحله بعدی اقدام می‌شود.

۵- محاسبه داده‌های رمزگشایی شده، داده‌های کاربر از EncData، همانگونه که در بند ۹-۵-۳ مشخص شده است.

پیوست الف

(الزامی)

الگوریتم‌های AES-XCBC-PRF-128 و AES-XCBC-MAC-96

الف-۱ AES-XCBC-PRF-128

الگوریتم AES-XCBC-PRF-128 نوع دیگری از CBC-MAC پایه با ‹‹۱۰*لایه گذاری›› الزامی است که پیام‌های با طول اختیاری را امن می‌سازد.

عملیات رمزبندی باید با بکارگیری AES همراه با یک کلید ۱۲۸ بیتی انجام شود.

K، کلید مخفی ۱۲۸ بیتی مفروض است، الگوریتم AES-XCBC-PRF-128 به شرح زیرین برای یک پیام M که حاوی n بلاک، M[n] ... M[1]، است که در آن اندازه بستکهای M[n-1] ... M[1]، ۱۲۸ بیت و اندازه بلاک M[n] بین ۱ و ۱۲۸ بیت است، محاسبه می‌شود:

۱- مشتق شدن ۳ کلید ۱۲۸ بیتی (K1، K2 و K3) از کلید مخفی ۱۲۸ بیتی K به شرح زیر:

K1 = (01010101010101010101010101010101) رمزبندی شده با کلید K.

K2 = (02020202020202020202020202020202) رمزبندی شده با کلید K.

K3 = (03030303030303030303030303030303) رمزبندی شده با کلید K.

۲- تعریف E[0] = 0x00000000000000000000000000000000

۳- برای هر بلاک M[i]، جایی که i=1 ... n-1 است:

M[i] با E[i-1]، XOR شده،

سپس نتیجه با کلید K1 رمزبندی شده و حاصل E[i] می‌شود.

۴- برای بلاک M[n]:

الف- اگر اندازه بلاک M[n]، ۱۲۸ بیت باشد:

M[n] با E[n-1] و کلید K2، XOR شده،

سپس نتیجه با کلید K1 رمزبندی شده و حاصل E[n] می‌شود.

ب- اگر اندازه بلاک M[n] کمتر از ۱۲۸ بیت باشد:

۱. M[n] با یک بیت واحد ‹‹یک››، بدنبال تعدادی بیت ‹‹صفر›› (محتمل هیچکدام) مورد نیاز جهت افزایش اندازه بلوک M[n] به ۱۲۸ بیت لایه‌گذاری می‌شود (این ‹‹۱۰*لایه‌گذاری›› است).

۲. M[n] با E[n-1] و کلید K3، XOR شده،

سپس نتیجه با کلید K1 رمزبندی شده و حاصل E[n] می‌شود.

۵- خروجی آخرین بلاک ۱۲۸ بیتی E[n] است.

الف-۲ AES-XCBC-MAC-96

الگوریتم AES-XCBC-MAC-96 همان الگوریتم AES-XCBC-PRF-128 است، بدنبال یک مرحله کوتاه‌سازی:

۱- برداشتن ۹۶ بیت اول از E[n].

به محض ارسال، مقدار کوتاه شده در مشخصه تاییدکننده اعتبار (Mac) ذخیره می‌شود.

به محض دریافت کردن، مقدار ۱۲۸ بیتی وارد شده محاسبه می شود و ۹۶ بیت اول با مقدار ذخیره شده در مشخصه تاییدکننده اعتبار (Mac) مقایسه می‌شود.

پیوست ب

(الزامی)

اندازه‌های فیلدها

جدول ب-۱ اندازه‌های فیلدها

فیلد	اندازه
NA	۹۶ بیتی
NB	۹۶ بیتی
d_A	۱۹۲ بیتی
d_B	۱۹۲ بیتی
DataLen	۲۴ بیتی
Q_A	۳۸۴ بیتی
Q_B	۳۸۴ بیتی
QA	۲۰۰ بیتی
QB	۲۰۰ بیتی
Z	۱۹۲ بیتی
MK	۱۲۸ بیتی
KE	۱۲۸ بیتی
KI	۱۲۸ بیتی
$MacTag_A$	۹۶ بیتی
$MacTag_B$	۹۶ بیتی
IV	۱۲۸ بیتی
SNV	۲۴ بیتی
Mac	۹۶ بیتی

پیوست پ

(اطلاعاتی)

مراجع اطلاعاتی

درخواست فرمان (RFC)[1] ۴۳۰۳	پایه بار امنیت پوشینه‌دارسازی (ESP)[2] IP
درخواست فرمان (RFC) ۴۳۰۶	پروتکل تبادل کلید اینترنت (IKEv2)
درخواست فرمان (RFC) ۴۴۳۴	الگوریتم AES-XCBC-PRF-128 برای پروتکل تبادل کلید اینترنت(IKE)[3]
درخواست فرمان (RFC) ۳۵۶۶	الگوریتم AES-XCBC-MAC-96 و کاربردش با IPSec

الگوریتم AES-XCBC-PRF-128 در (IPSEC v2) RFC 4434 مشخص شده است.

الگوریتم AES-XCBC-MAC-96 در (IPSEC v2) RFC 3566 مشخص شده است.

KDF در (IPSEC v2) RFC 4306 مشخص شده است.

سازوکار حفاظت ENC و MAC در (IPSEC v2) RFC 4303 مشخص شده است.

1- Request For Comment
2 Encapsulating Security Payload
3- Internet Key Exchange