INSO
16302
1st. Edition
May.2013

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

استاندارد ملی ایران
۱۶۳۰۲
چاپ اول
اردیبهشت ۱۳۹۲

فناوری اطلاعات – مخابرات و تبادل اطلاعات بین سامانه‌ها – پروتکل امنیت لایه انتقال

Information technology – Telecommunications and information exchange between systems – Transport layer security protocol

ICS: 35.100.40

به‌نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

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

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

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

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

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

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

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- مخابرات و تبادل اطلاعات بین سامانه‌ها - پروتکل امنیت لایه انتقال»

رئیس:	**سمت و/ یا نمایندگی**
فرهاد شیخ احمد، لیلا (کارشناسی‌ارشد مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (کارشناسی مهندسی کامپیوتر نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (کارشناسی مهندسی برق کنترل)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
جمیل پناه، ناصر (کارشناسی‌ارشد مدیریت)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سعیدی، عذرا (کارشناسی‌ارشد مهندسی برق-مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سلطانی حقیقت، الهه (کارشناسی مهندسی برق مخابرات)	کارشناس سازمان فناوری اطلاعات ایران
عبداللهی ازگمی، محمد (دکترای مهندسی کامپیوتر-نرم‌افزار)	استادیار دانشگاه علم و صنعت ایران
عسکرزاده، مجید (کارشناسی‌ارشد مهندسی کامپیوتر)	نماینده دانشگاه آزاد – واحد علوم و تحقیقات
فولادیان، مجید (کارشناسی‌ارشد مهندسی برق-مخابرات)	مشاور سازمان فناوری اطلاعات ایران
فیاضی، مهدی (کارشناسی مهندسی برق الکترونیک)	کارشناس سازمان فناوری اطلاعات ایران
قسمتی، سیمین (کارشناسی‌ارشد فناوری اطلاعات)	کارشناس سازمان فناوری اطلاعات ایران

مجاهدی، الناز (کارشناسی مهندسی کامپیوتر نرم‌افزار)	نماینده دانشگاه علم و صنعت ایران
معروف، سینا (کارشناسی مهندسی کامپیوتر سخت‌افزار)	کارشناس سازمان فناوری اطلاعات ایران
میرزایی رضایی، طیبه (کارشناسی‌ارشد فیزیک)	رییس اداره تدوین استانداردها و نظارت بر فرآیند سرویس‌ها سازمان فناوری اطلاعات

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات- مخابرات و تبادل اطلاعات بین سامانه‌ها - پروتکل امنیت لایه انتقال» که پیش‌نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و در دویست و شصتمین اجلاس کمیته‌ی ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۱/۱۱/۸ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

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

منبع و ماخذی که برای تهیه‌ی این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 10736:1995, Information technology – Telecommunications and information exchange between systems – Transport layer security protocol.

مقدمه

این استاندارد ملی، پروتکل انتقال مشخص‌شده در ISO/IEC 8073 | ITU-T Rec. X.224 خدمت انتقال اتصال‌گرای توصیف شده در ISO/IEC 8072 | ITU-T Rec. 234 را تعریف می‌کند. پروتکل انتقال مشخص‌شده در ISO/IEC 8602 | ITU-T Rec. 234 خدمت انتقال حالت بی‌اتصال توصیف شده در استاندارد ISO/IEC 8072 را فراهم می‌سازد. این استاندارد ملی کارکردهای افزونه اختیاری را برای ISO/IEC 8073 | ITU-T Rec. X.224 و ISO/IEC 8602 | ITU-T Rec. X.234 مشخص می‌کند تا به آن‌ها اجازه دهد از فنون رمزنگاری به‌منظور فراهم کردن محافظت از داده‌ها در اتصالات انتقال یا در ارسال[1] واحد داده پروتکل انتقال (TPDU)[2] حالت بی‌اتصال استفاده کنند.

1 - Transmission
2 - Transport Protocol Data Unit (TPDU)

فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها - پروتکل امنیت لایه انتقال

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، مشخص کردن رویه‌هایی است که به‌عنوان گسترشی بر رویه‌های تعریف‌شده در ISO/IEC 8073| ITU-T Rec. X.224 و ISO/IEC 8602 | ITU-T Rec. X.234 عمل می‌کنند و از اتصال محافظت‌نشده بین هستارهای انتقال پیاده‌سازی‌کننده ISO/IEC 8073 | ITU-T Rec. X.224 یا ISO/IEC 8602 | ITU-T Rec. X.234 جلوگیری نمی‌کنند.

محافظتی که با پروتکل امنیتی تعریف‌شده در این استاندارد ملی به‌دست می‌آید به عملکرد مناسب مدیریت امنیتی شامل مدیریت کلید[1] بستگی دارد. اگر چه این استاندارد ملی کارکردهای مدیریتی و پروتکل‌های مورد نیاز برای پشتیبانی این پروتکل امنیتی را مشخص نمی‌کند.

این پروتکل می‌تواند از خدمات یکپارچگی[2]، محرمانگی[3]، احراز هویت[4] و کنترل دسترسی[5] مربوط به لایه‌ی انتقال شناسایی‌شده در ISO 7498-2 | CCITT Rec. X.800[6] پشتیبانی کند. این پشتیبانی از طریق به‌کارگیری سازوکارهای رمزنگاشتی[7]، صفات و برچسب‌زنی[8] امنیتی مانند کلیدها و شناسه‌های احراز هویت‌شده که به‌وسیله مدیریت امنیت از قبل ایجاد شده‌اند یا از طریق استفاده از پروتکل همبستگی امنیتی (SA-P)[9] ایجاد می‌شوند، صورت می‌گیرد.

محافظت تنها می‌تواند در بستر یک خط‌مشی امنیتی فراهم شود.

این پروتکل احراز هویت، هستار همتا را در لحظه برقراری اتصال پشتیبانی می‌کند. به علاوه کلیددهی مجدد[10] نیز از طریق استفاده از SA-P یا ابزارهای خارج از پروتکل پشتیبانی می‌شود.

همبستگی‌های امنیتی را می‌توان فقط در بستر یک خط‌مشی امنیتی تعیین کرد. تعیین خط‌مشی‌های امنیتی که ممکن است به‌وسیله‌ی رویه‌های مشخص‌شده در این استاندارد ملی محدود شده باشد، یک مسأله برای کاربران است.

خط‌مشی امنیتی می‌تواند شامل موارد زیر باشد:

الف- روش برقراری/رهاسازی SA[11]، طول عمر SA؛

1 - Key management
2 - Integrity
3 - Confidentiality
4 - Authentication
5 - Access control
6 - Comité Consultatif International Téléphonique et Télégraphique
7 - Cryptographic mechanisms
8 - Labelling
9 - Security Association-Protocol
10 - Rekeying
11 - Security Association

ب- سازوکارهای احراز هویت/کنترل دسترسی؛
پ- سازوکار برچسب‌زنی؛
ت- رویه دریافت یک TPDU نامعتبر در طی رویه برقراری SA یا ارسال PDU محافظت‌شده؛
ث- طول عمر کلید؛
ج- فاصله زمانی رویه کلیددهی مجدد جهت به‌روزرسانی کلید و رویه تبادل اطلاعات کنترل امنیت (SCI)[1]؛
چ- مهلت تبادل SCI و رویه کلیددهی مجدد؛
ح- تعداد تلاش مجدد جهت تبادل SCI و کلیددهی مجدد.

این استاندارد ملی پروتکلی را تعریف می‌کند که می‌تواند برای برقراری همبستگی امنیتی مورد استفاده قرار گیرد. هستارهایی که می‌خواهند یک SA را برقرار کنند باید سازوکارهای مشترکی را برای احراز هویت و توزیع کلید به اشتراک بگذارند. این استاندارد ملی الگوریتمی جهت احراز هویت و توزیع کلید مشخص می‌کند که مبتنی بر سامانه‌های رمزنگاری کلید عمومی است.

پیاده‌سازی این الگوریتم اجباری نیست، با این وجود زمانی که یک سازوکار جایگزین استفاده می‌شود باید بتواند شرایط زیر را برآورده کند:

الف- همه صفات SA معرفی‌شده در زیربند ۵-۲ استخراج شوند.
ب- کلیدهای استخراج‌شده احراز هویت شوند.

۲ مراجع الزامی

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

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

استفاده از مراجع زیر برای این استاندارد الزامی است:[2]

2-1 ITU-T Recommendation X.214 (1993) | ISO 8072:1994, Information technology - Open Systems Interconnection - Transport Service definition.

2-1ITU-T Recommendation X.234 (1993) | ISO/IEC 8602:1995, Information technology - Protocol for providing the OSI connectionless - mode transport Service.

2-3 CCITT Recommendation X.200 (1988), Reference Model of Open Systems Interconnection for CCITT applications.

---

1 - Security control information (SCI)

۲ – مراجع الزامی ردیف‌های ۲-۱ و ۲-۲ مربوط به توصیه‌نامه‌ها||استانداردهای بین‌المللی مشابه، مراجع الزامی مندرج در ردیف‌های ۲-۳ الی ۲-۱۴ مربوط به توصیه‌نامه‌ها||استانداردهای بین‌المللی معادل با محتوای فنی و مراجع الزامی ردیف‌های ۲-۱۵ و ۲-۱۶ مربوط به سایر مراجع است.

2-4 ISO/IEC 7498- 1: 1994, Information technology - Open Systems Interconnection - Basic Reference Model - Part 1: The Basic Model.

2-5 CCITT Recommendation X.800 (1991), Security architecture for Open Systems Interconnection for KITT applications.

2-6 ISO 7498-2: 1989, Information processing Systems - Open Systems Interconnection – Basic Reference Model - Part 2: Security Architecture.

2-7 ITU-T Recommendation X.224 (1993), Protocol for providing the OSI connection-mode transport Service.

2-8 ISO/IEC 8073: 1992, Information technology - Telecommunications and information exchange between Systems - Open Systems Interconnection - Protocol for providing the connection-mode transport Service.

2-9 CCITT Recommendation X.208 (1988), Specification of Abstract Syntax Notation One (ASN. 1).

2-10 ISO/IEC 8824: 1990, Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1).

2-11 CCITT Recommendation X.209 (1988), Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN. 1).

2-12 ISO 8825: 1990, Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN. 1).

2-13 ITU-T Recommendation X.264 (1993), Transport protocol identification mechanism.

2-14 ISO/IEC 11570: 1992, Information technology - Telecommunications and information exchange between Systems - Open Systems Interconnection - Transport protocol identification mechanism.

2-15 ISO/IEC 9834- 1: 1993, Information technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities: General Procedures.

2-16 ISOIIEC 9834-3: 1990, Information technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities - Part 3: Registration of Object identifier component values for joint ISO-CCITT use.

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود:

این استاندارد ملی بر پایه مفاهیمی است که در مدل مرجعِ اتصال متقابل سامانه‌های باز (ISO 7498-1 | CCITT Rec. X.200) و ISO 7498-2 | CCITT Rec. X.800 در معماری امنیت، تدوین شده‌اند.

۳-۱ تعاریف مدل مرجع امنیت

در این استاندارد، اصطلاحات و تعاریف زیر همان‌گونه که در ISO 7498-2 | CCITT Rec. X.800 تعریف شده‌اند، به‌کار می‌روند:

الف- کنترل دسترسی؛

ب- نامتقارن[1]؛
پ- متن رمزشده[2]؛
ت- متن واضح[3]؛
ث- محرمانگی؛
ج- یکپارچگی داده‌ها[4]؛
چ- احراز هویت مبدأ داده؛
ح- انکار خدمت[5]؛
خ- رمزگذاری انتها به انتها؛
د- کلید؛
ذ- مدیریت کلید؛
ر- خط‌مشی امنیتی؛
ز- متقارن؛

۳-۲ سایر تعاریف

این استاندارد ملی از تعاریف زیر استفاده می‌کند:

۳-۲-۱

طول عمر کلید رمز[6]

مدت زمان مجازی که امکان استفاده از کلید رمزنگاشتی وجود دارد. بعد از این مدت زمان، کلید منقضی باید جایگزین شود.

۳-۲-۲

سازوکار پروتکل درون باند[7]

سازوکار پروتکلی که در این استاندارد ملی تعریف‌شده است.

۳-۲-۳

سازوکار پروتکل برون باند[8]

سازوکار پروتکلی که در این استاندارد ملی تعریف نشده است.

1 - Asymmetric
2 - Ciphertext
3 - Cleartext
4 - Data Integrity
5 - Denial of Service
6 - Cryptoperiod
7 - In-band protocol mechanism
8 - Out-band protocol mechanism

۴-۲-۳

جفت کلید[1]

یک زوج از مقادیر کلید مرتبط (کلید عمومی) یا همسان (کلید سرّی)[2] که برای استفاده بین دو طرف ارتباطی خاص، تولید می‌شود.

۵-۲-۳

محافظت بازتابی[3]

سازوکار محافظتی برای تشخیص مواقعی که واحد داده پروتکل، به مبدأ باز گردانده شده است.

۶-۲-۳

همبستگی امنیتی[4]

رابطه‌ی بین هستارهای در حال ارتباط که برای آن‌ها صفات SA متناظر وجود دارد.

۷-۲-۳

صفات[5] **همبستگی امنیتی**

مجموعه اطلاعاتی که برای کنترل امنیت ارتباطات بین یک هستار و همتا(ها)ی راه دور آن، الزامی است.

۸-۲-۳

کپسوله‌سازی واحد داده‌ی پروتکل انتقال (SE TPDU)[6]

واحد داده‌ی پروتکل انتقال (TPDU) کپسوله‌شده برای امنیت، تا ارسال TPDU تعریف‌شده در ITU-T Rec. X,2241 | ISO/IEC 8073 یا ITU-T Rec. X.234 | ISO 8602 پس از امن کردن آن صورت پذیرد.

۴ نمادها و کوته‌نوشت‌ها

این استاندارد ملی از کوته‌نوشت‌های بند ۴ در ITU-T Rec. X.224 | ISO/IEC 8073 به شرح زیر استفاده می‌کند:

درخواست اتصال TPDU	Connection Request TPDU	CR TPDU
تایید قطع اتصال TPDU	Disconnect Conformation TPDU	DC TPDU
درخواست قطع اتصال TPDU	Disconnect Request TPDU	DR TPDU

1 - Pairwise key
2 - Secret key
3 - Reflection protection
4 - Security association
5 - Attributes
6 - Security Encapsulation Transport Protocol Data Unit

DST-REF	Destination Reference (field)	مرجع مقصد (فیلد)
DT TPDU	Data TPDU	TPDU داده‌ای
ED TPDU	Expedited Data TPDU	TPDU داده‌ای پیشتاز
ED-TPDU-NR	Expedited Data TPDU number (field)	شماره‌ی TPDU داده‌ای پیشتاز (فیلد)
ER TPDU	Error TPDU	TPDU خطا
LI	Length Indicator (field)	نشانگر طول (فیلد)
NC	Network Connection	اتصال شبکه
SN	Sequence Number	شماره دنباله
SRC-REF	Source Reference (field)	مرجع مبدأ (فیلد)
TC	Transport Connection	اتصال انتقال
TPDU	Transport protocol data unit	واحد داده‌ی پروتکل انتقال
TPDU-NR	DT TPDU number (field)	شماره‌ی DT TPDU (فیلد)

به علاوه کوته‌نوشت‌های زیر نیز در این استاندارد ملی استفاده می‌شوند:

CBTSS	Connection Based Transport Security Service	خدمت امنیتی انتقال مبتنی بر اتصال
Conf_no	Confidentiality is not to be provided	محرمانگی فراهم نشده است.
Conf_yes	Confidentiality is to be provided	محرمانگی فراهم شده است.
DEK	Data Encipherment Key	کلید رمزگذاری داده
GTSS	General Transport Security Service	خدمت امنیتی انتقال عمومی
ICV	Integrity Check Value	مقدار وارسی یکپارچگی
Integ – no	Integrity is not to be provided	یکپارچگی ارائه نشده است.
Ineteg_yes	Integrity is to be provided	یکپارچگی ارائه شده است.
KEK	Key Encipherment Key	کلید رمزگذاری کلید
KEY-ID	Key Identifier	شناسه‌ی کلید
Kg-esp	A separate cryptographic key is used for each end System pair	یک کلید رمزنگاشتی مجزا برای هر زوج سامانه پایانی استفاده می‌شود.
Kg-esp-sr	A separate cryptographic key is used for each end System pair and security level set	یک کلید رمزنگاشتی مجزا برای هر زوج

		سامانه پایانی و مجموعه سطح امنیتی استفاده می‌شود.
Kg_tc	A separate cryptographic key is used for each Transport connection	یک کلید رمزنگاشتی مجزا برای هر اتصال انتقال استفاده می‌شود.
LABEL	Security Label	برچسب امنیتی
LLSG	Lower Layer Security Guidelines	راهنماهای امنیتی لایه پایین‌تر
LME	Layer Management Entity	هستار مدیریت لایه
MAC	Message Authentication Code	کد احراز هویت پیام
MDC	Manipulation Detection Code	کد تشخیص فرابری
NLSP	Network Layer Security Protocol	پروتکل امنیتی لایه‌ی شبکه
NSAP	Network Service Access Point	نقطه دسترسی خدمت شبکه
NSDU	Network Service Data Unit	واحد داده‌ی خدمت شبکه
PAD	Padding (field)	لت‌گذاری (فیلد)
Pp1- abs	Security Label never used on TPDUs	برچسب امنیتی که هیچ وقت روی TPDUها استفاده نمی‌شود.
Ppl_pres	Security Label used on every TPDU	برچسب امنیتی که بر روی هر TPDU استفاده می‌شود.
SA-P	Security Association - Protocol	همبستگی امنیتی – پروتکل
SE TPDU	Security Encapsulation TPDU	کپسوله‌سازی امنیتی TPDU
TLSP	Transport Layer Security Protocol	پروتکل امنیتی لایه‌ی انتقال

۵ مروری کلی بر پروتکل

۵-۱ مقدمه

توصیه‌نامه‌ی CCITT Rec. X.800 | ISO 7498-2 خدمات امنیتی زیر مربوط به لایه‌ی انتقال را شناسایی می‌کند:

- احراز هویت هستار همتا[1]؛
- احراز هویت مبدأ داده[2]؛
- خدمت کنترل دسترسی[1]؛

1 - Peer entity authentication
2 - Data origin authentication

- محرمانگی اتصال[۲]؛
- محرمانگی بی‌اتصال[۳]؛
- یکپارچگی اتصال با بازیافت[۴]؛
- یکپارچگی اتصال بدون بازیافت؛
- یکپارچگی بی‌اتصال[۵].

یادآوری ۱– ITU-T Rec. X.214 | ISO 8072 در حال حاضر تنها چهار سطح از کیفیت محافظت را تعریف می‌کند:
الف- بدون ویژگی‌های محافظت؛
ب- محافظت در برابر پایش[۶] غیرفعال[۷]؛
پ- محافظت در برابر تغییرات، بازارسال[۸]، اضافه کردن و حذف‌کردن؛
ت- دو مورد ب و پ،
این موارد معادل خدمات امنیتی زیر هستند.
CCITT Rec. X.800 | ISO 7498-2 از اصطلاحات زیر برای خدمات امنیتی بر روی معماری امنیتی OSI استفاده می‌کند:
الف- بدون خدمات امنیتی؛
ب- محرمانگی با اتصال/بی‌اتصال؛
پ- یکپارچگی با اتصال/بی‌اتصال (با یا بدون بازیافت)؛ و
ت- هر دو یکپارچگی و محرمانگی با اتصال/بی‌اتصال.
یک گزارش نقص برای ITU-T Rec. X.214 | ISO 8072 داده شد تا از این انواع و سایر انواع محافظت پشتیبانی کند.

یادآوری ۲- یکپارچگی بی‌اتصال از اضافه یا حذف کردن SDUهای بی‌اتصال محافظت نمی‌کند و فقط به‌صورت محدود محافظت بازارسال را فراهم می‌کند.

پروتکل امنیتی لایه انتقالی که به‌وسیله ISO/IEC 8073 | ITU-T Rec. X.224 استفاده می‌شود می‌تواند از یکپارچگی اتصال با بازیافت یا بدون بازیافت، محرمانگی اتصال، خدمت کنترل دسترسی و احراز هویت هستار همتا در حالی که هر اتصال به‌طور مجزا محافظت می‌شود، پشتیبانی کند. اگر چه یک کلید ممکن است بین چندین اتصال به اشتراک گذاشته شود.

پروتکل امنیتی لایه انتقال که با ISO/IEC 8602 | ITU-T Rec. X.234 استفاده می‌شود، می‌تواند از یکپارچگی بی‌اتصال، محرمانگی بی‌اتصال، خدمت کنترل دسترسی و احراز هویت مبدأ داده، پشتیبانی کند.

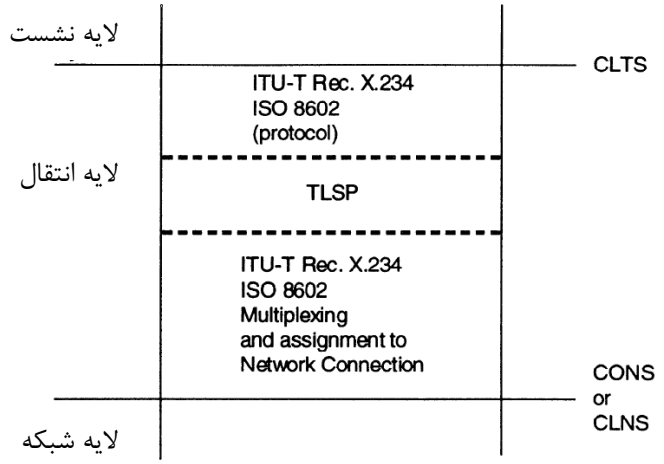
این استاندارد ملی گسترش‌های پروتکل برای ارائه محرمانگی و یکپارچگی محافظت داده‌ها را مشخص می‌کندکه شامل موارد زیر است:

الف- رویه‌هایی که فنون رمزنگاشتی را در پردازش پروتکل به‌کار می‌گیرند؛

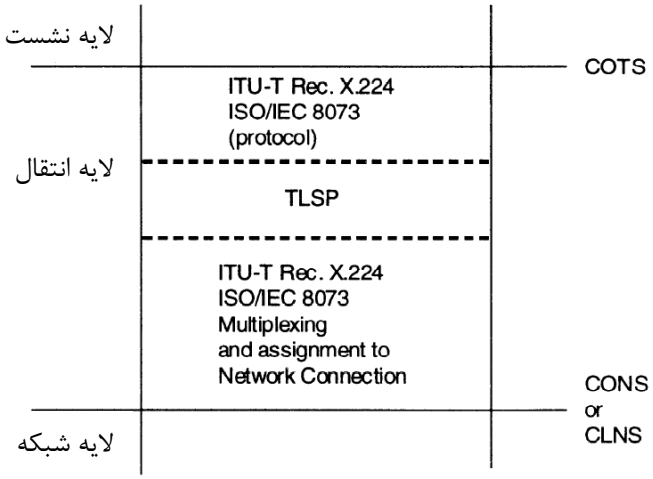
---

1 - Access control service
2 - Connection confidentiality
3 - Connectionless confidentiality
4 - Connection integrity with recovery
5 - Connectionless integrity
6 - Monitoring
7 - Passive
8 - Replay

ب- حداقل مشخصات الگوریتم‌های رمزنگاشتی که این رویه‌ها می‌توانند با آن‌ها استفاده شوند؛
پ- ساختار و کدبندی واحدهای داده که برای دستیابی به تعامل‌پذیری[1] ضروری هستند.
شکل‌های ۱ و ۲ محل TLSP را در هفت لایه مدل OSI نشان می‌دهند.



شکل ۱ – TLSP با توصیه‌نامه‌ی ITU-T Rec. X.234| ISO 8602



شکل ۲ – TLSP با توصیه‌نامه‌ی ITU-T Rec. X.224| ISO 8073

۲-۵ صفات و همبستگی‌های امنیتی[2]

گزینه‌های پردازش TLSP خاص که در یک نمونه ارتباطات به‌کار می‌رود، با یک مجموعه از صفات امنیتی شامل کلیدهای محافظت دوگانه تعیین می‌شوند. پروتکل امنیتی لایه انتقال فرض می‌کند که دو هستار انتقال، مجموعه‌ی صفات متناظری را بین هم به اشتراک می‌گذارند. شناسه همبستگی امنیتی (SA-ID)[3]، مجموعه‌ای از صفاتی که ممکن است برای محافظت یک نمونه ارتباط به‌کار رود، را مشخص می‌کند.

1 - Interoperability
2 - Security associations and attributes
3 - Security Association identifier

هر همبستگی امنیتی به‌وسیله مجموعه‌ای از صفات در هر سامانه‌ی پایانی تعریف می‌شود. ابزارهای ایجاد همه‌ی این صفاتی که قرار است در یک پیوند استفاده شوند در حال حاضر خارج از محدوده‌ی این مشخصات است. برخی از آن‌ها می‌توانند به‌وسیله‌ی تبادل دستی[1] صفات برقرار شوند و برخی دیگر از آن‌ها می‌توانند از طریق به‌کارگیری یک مجموعه توافق شده از قواعد امنیتی (ASSR)[2] برقرار شوند. یک ASSR مجموعه‌ای مشترک از قواعدی است که سازوکارهای امنیتی را که باید استفاده شوند مشخص می‌کند. این سازوکارها شامل همه پارامترهای مورد نیاز برای تعریف عملکرد سازوکارِ خدمت(های) محافظتی مفروض است. قواعد امنیتی و شناسه‌های آن‌ها ممکن است به‌وسیله طرف‌های سوم[3] ثبت شوند. برای دیدن یک نمونه‌ی ترسیمی از ASSR به پیوست ب مراجعه شود.

سایر صفات از قبیل طول عمر[4] و مهلت زمانی[5] رویه کلیددهی مجدد می‌توانند تحت خط‌مشی امنیتی تعریف شوند.

پروتکل امنیتی لایه‌ی انتقال با استفاده از این صفات همبستگی امنیتی خصوصیات پردازشی داده‌های کاربر را تعیین می‌کند. در ادامه، صفاتِ TLSP توضیح داده می‌شود و علایم کوته‌نوشتی را که برای ارجاع به این صفات در این مشخصات استفاده می‌شود فهرست می‌کند. یک مجموعه از صفات مناسب برای ارتباط بین دو سامانه پایانی به سازوکارهای استفاده‌شده و خط‌مشی امنیتی وابسته است.

الف- شناسایی SA

۱- Local_SAID: رشته‌ی هشت‌تایی شناسه‌ی محلی SA.

۲- Peer_SAID: رشته‌ی هشت‌تایی – شناسه‌ی همتای راه دور SA.

۳- SAID_Len: عدد صحیح – طول SAID تعریف‌شده به‌وسیله‌ی ASSR، عدد صحیح در محدوده ۲ تا ۱۲۶.

Local_SAID و Peer_SAID در هنگام برقراری SA مقداردهی می‌شوند. مقدار SAID_Len برای ASSR مفروض تعریف می‌شود.

زمانی که یک هستار TLSP تشخیص می‌دهد که یک SA به‌خصوص قطع شده است، باید SA-ID که اختصاص داده بود را به حالت بی‌حرکت[6] ببرد. زمانی که SA-ID بی‌حرکت است، نباید استفاده مجدد شود. دوره‌ی زمانی که SA-ID در آن بی حرکت است باید بزرگتر از طول عمر PDU (های) شبکه زیرین باشد.

ب- شاخص این‌که کدام هستار TLSP نقش آغازکننده و کدام هستار نقش پاسخ‌دهنده را دارد. این صفت نشان می‌دهد که چگونه نشانگر جهت باید برای تشخیص TPDUهای بازتاب‌شده تنظیم شود.

آغازکننده: بولی[7].

1 - Mannual exchange
2 - Agreed Set of Security Rules
3 - Third parties
4 - Lifetime
5 - Timeout
6 - Frozen
7 - Boolean

مقدار این صفت در هنگام برقراری SA تنظیم می‌شود.

پ- آدرس هستار (هستارهای) TLSP همتا

Peer_Adr: رشته‌ی هشت‌تایی

مقدار این صفت در هنگام برقراری SA تنظیم می‌شود که یا بیانگر آدرس NSAP هستار انتقال است (اگر کلیدی یکسان بین چندین اتصال به اشتراک گذاشته شده باشد.)، یا شناسه‌ی اتصال را به‌وسیله شماره‌های مرجع انتقال محلی یا راه دور نشان می‌دهد، که این امر در صورتی امکان‌پذیر است که کلید تنها برای یک اتصال باشد.

ت– شناسه‌ی مجموعه قواعد امنیتی توافق‌شده جهت اعمال بر این همبستگی

ASSR_ID: شناسه‌ی شئ همان‌گونه‌که در ASN.1 CCITT Rec. X.208| ISO 8824 تعریف شده است.

مقدار این صفت در هنگام برقراری یا پیش از برقراری SA تنظیم می‌شود.

ث- QOS محافظت انتخاب شده برای SA

QOS_Label: قالب تعریف‌شده به‌وسیله ASSR

AC: (سطح کنترل دسترسی) عدد صحیحی در محدوده تعریف‌شده به‌وسیله ASSR

پارامترهای کیفیت خدمت (QoS) زیر تنها مربوط به TLSP به‌کار برده شده توام با ITU-T Rec. X.234 | ISO/IEC 8602 هستند:

- DOAuth: (سطح احراز هویت مبدأ داده) عدد صحیح در محدوده تعریف‌شده به‌وسیله ASSR
- CLConf: (سطح محرمانگی بی‌اتصال) عدد صحیح در محدوده تعریف‌شده به‌وسیله ASSR
- CLInt: (سطح یکپارچگی بی‌اتصال) عدد صحیح در محدوده تعریف‌شده به‌وسیله ASSR

پارامترهای QOS زیر تنها مربوط به TLSP به‌کار برده شده توام با ITU-T Rec. X.224 | ISO/IEC 8073 هستند:

- Auth: (سطح احراز هویت هستار همتا) عدد صحیح در محدوده تعریف‌شده به‌وسیله ASSR
- CO Conf: (سطح محرمانگی اتصال) عدد صحیح در محدوده تعریف‌شده به‌وسیله ASSR
- CO Int: (یکپارچگی اتصال بدون بازیافت) عدد صحیح در محدوده تعریف‌شده به‌وسیله ASSR
- CO Intr: (یکپارچگی اتصال با بازیافت) عدد صحیح در محدوده تعریف‌شده به‌وسیله ASSR
- CLConf: (سطح محرمانگی بی‌اتصال) عدد صحیح در محدوده تعریف‌شده به‌وسیله ASSR
- CLInt: (سطح یکپارچگی بی‌اتصال) عدد صحیح در محدوده تعریف‌شده به‌وسیله ASSR

مقدار این صفات در هنگام برقرارسازی یا پیش از برقرارسازی SA تنظیم می‌شوند.

ج- سازوکارهای انتخاب شده برای SA

- برچسب: بولی – برچسب زدن صریح TPDUها.

Conf-: بولی - محرمانگی یک انتقال داده امن به‌وسیله‌ی رمزگذاری.

- ICV check: بولی – یکپارچگی محتوای یک انتقال داده امن با استفاده از یک مقدار یکپارچگی.
- SN: بولی – رویه شماره دنباله‌ی یکپارچگی اتصال مورد استفاده.
- PE-Authentication: بولی – احراز هویت هستار همتا با استفاده از تبادل PDU های درخواست اتصال/ پاسخ اتصال کپسوله‌شده.
- UNProt: بولی - TPDUهای محافظت‌نشده

چ– صفات سازوکار برچسب

مقادیر این صفات در هنگام برقرارسازی یا پیش از برقرارسازی SA تنظیم می‌شوند. این صفت مجموعه‌ی مجاز برچسب‌های امنیتی را برای همبستگی امنیتی مشخص می‌کند.

Label-Set: Set of {
Label_Ref: Integer
Label_Defining_Auth: Object Identifier
Label_Content: Format defined by Label_Defining_Auth
}

ح– صفات سازوکار ICV

- ICV_Alg: شناسه‌ی شئ
- ICV_Len: عدد صحیح
- ICV_Blk: اندازه‌ی عدد صحیح بستک لت‌گذاری[1] برای الگوریتم ICV

صفات زیر تنها در صورتی که الگوریتم، رمزنگاشتی باشد، وجود دارند:

- ICV_Kg: عدد صحیح مقدار Kg_tc یا Kg_esp یا Kg_esp_sr

دانه‌بندی کلید یکی از موارد زیر است:

- Kg_tc کلید رمزنگاشتی مجزایی که برای هر اتصال انتقال استفاده می‌شود.
- Kg_esp کلید رمزنگاشتی مجزایی که برای هر زوج سامانه پایانی استفاده می‌شود.
- Kg_esp_sr کلید رمزنگاشتی مجزایی که برای هر زوج سامانه پایانی و مجموعه امنیتی استفاده می‌شود.

مقادیر صفات فوق به‌وسیله ASSRای که QOS محافظت را برآورده می‌کند، تعریف می‌شوند.

- ICV_Gen_key: مرجع کلید تولید ICV - قالب آن به‌وسیله ASSR تعریف می‌شود.
- ICV_Check_Key: مرجع کلید وارسی ICV – قالب آن به‌وسیله ASSR تعریف می‌شود.

خ- صفات سازوکار SN

صفات زیر تنها مربوط به آن TLSP است که توام با ISO/IEC 8073 | ITU-T Rec. X.224 استفاده می‌شود:

- Data_Local_SN: SN برای آخرین داده‌ی عادی ارسال‌شده
- Data_Peer_SN: SN برای آخرین داده‌ی عادی دریافت‌شده

1 - Padding

مقادیر اولیه‌ی این صفات به‌عنوان بخشی از اتصال عادی تنظیم می‌شوند. SN، شماره‌ی دنباله‌ی استفاده شده در ISO/IEC 8073 | ITU-T Rec. X.224 است.

د- صفات سازوکار شماره دنباله‌ی پیشتاز (EXSN)[1]

صفات زیر تنها مربوط به آن TLSP است که توام با ISO/IEC 8073 | ITU-T Rec. X.224 استفاده می‌شود:

- Data_Local_EXSN: EXSN آخرین داده‌ی پیشتاز ارسال شده
- Data_Peer_EXSN: EXSN آخرین داده‌ی پیشتاز دریافت شده

مقادیر اولیه‌ی این صفات به‌عنوان بخشی از رویه پیشتاز تنظیم می‌شوند. EXSN، شماره دنباله‌ی استفاده شده به‌وسیله ISO/IEC 8073 | ITU-T Rec. X.224 است.

ذ- صفات سازوکار رمزگذاری

- Enc_Alg: شناسه‌ی شئ (به‌عنوان مثال تخصیص‌داده‌شده تحت استاندارد ISO 9979)
- Enc_Blk: اندازه‌ی عدد صحیح بستک لت‌گذاری برای الگوریتم رمزگذاری
- Enc_Kg: عدد صحیحِ مقدار Kg-tc یا Kg_esp یا Kg_esp_sr

صفات دانه‌بندی کلید در بند ح تعریف‌شده‌اند.

مقدار این صفت به‌وسیله ASSR ای که QOS محافظت را برآورده می‌کند، تعریف می‌شود:

- Enc_Key: مرجع کلید رمزگذاری – قالب آن به‌وسیله‌ی ASSR تعریف‌شده است.
- Dec_Key: مرجع کلید رمزگشایی- قالب آن به‌وسیله‌ی ASSR تعریف‌شده است.

یادآوری– ممکن است در نسخه‌های بعدی این استاندارد ملی یا برای سازوکارهای خصوصی، سازوکارها و صفات اضافی دیگری تشخیص داده شوند.

۵-۲-۱ خدمات امنیتی برای پروتکل انتقال اتصال‌گرا

زمانی که TLSP برای ارائه خدمات امنیتی اتصال‌گرا استفاده می‌شود، هستار انتقال باید یک SA-ID به هر اتصال انتقال محافظت‌شده (Kg_tc)، هر زوج سامانه‌ی پایانی انتقال (Kg_esp) یا هر سامانه پایانی انتقال و مجموعه سطح امنیتی (Kg_esp_sr) اختصاص دهد. SA-ID باید به‌طور صریح برای اتصال(های) انتقال محافظت‌شده ساخته شود. خدمات امنیتی که باید برای اتصال ارائه شوند، خدماتی هستند که به‌وسیله همبستگی امنیتی تعریف شده‌اند. تمام TPDUهایی که بر روی اتصال(های) انتقال محافظت‌شده دریافت یا ارسال می‌شوند باید براساس خدمات مربوط به همبستگی امنیتی محافظت شوند. اگر Kg_tc برقرار باشد، یک تناظر نظیر به نظیر بین اتصال انتقال و همبستگی امنیتی وجود خواهد داشت.

اگر یکپارچگی اتصال‌گرا مطلوب باشد، خدمات امنیتی مرتبط با همبستگی امنیتی باید شامل پردازش مقدار وارسی یکپارچگی (ICV) باشند (ICV=True). باید از دریافت TPDUهایی که به‌طور نامناسب محافظت شده‌اند صرف‌نظر کرد. این دریافت TPDUهای به‌طور نامناسب محافظت‌شده یک رویداد[2] مرتبط با امنیت

1 - Expedited Sequence Number
2 - Event

است؛ به هر حال اقدام بیشتر در این مورد خارج از محدوده‌ی این استاندارد ملی است. (به‌عنوان مثال پرکردن گزارش‌های ممیزی)

۵-۲-۲ خدمت امنیتی برای پروتکل انتقال بی‌اتصال

زمانی که TLSP برای ارائه خدمات امنیتی در خدمت انتقال حالت بی‌اتصال استفاده می‌شود، هستار انتقال باید یک SA-ID را به یکی از موارد زیر اختصاص دهد:

- هر زوج هستار انتقال (Kg_esp)؛
- هر هستار انتقال و زوج مجموعه سطح امنیتی (Kg_esp_sr).

هستار انتقال ارسالی باید هر TPDU را براساس صفاتی مرتبط با SA-ID محافظت کند و باید شناسه‌ی همتا (SA-ID) را در پارامتر SA-ID در SE TPDU قرار دهد. در لحظه‌ی دریافت SE TPDU، کلیدی که با پارامتر SA-ID مشخص شده است باید برای رمزگشایی TPDU یا برای درستی‌سنجی ICV آن استفاده شود. باید از دریافت هر TPDU که به‌طور نامناسب محافظت‌شده است صرف‌نظر شود. دریافت TPDUهای به درستی محافظت‌نشده یک رویداد امنیتی است، به هر حال اقدام بیشتر در این مورد خارج از محدوده‌ی این استاندارد ملی است (به‌عنوان مثال پر کردن گزارش‌های ممیزی).

۵-۳ خدمت مفروض برای لایه شبکه

خدمات امنیتی که به‌وسیله‌ی پروتکل TLSP ارائه شده‌اند مستقل از هر خدمت امنیتی هستند که به‌وسیله‌ی لایه‌ی شبکه ممکن است استفاده شود.

۵-۴ الزامات مدیریت امنیت[1]

این پروتکل امنیتی نیاز دارد که صفات همبستگی امنیتی پیش از یک تقاضای ارتباط محافظت‌شده‌ی داده‌ی کاربر برقرار شده باشند. این صفات ممکن است از طریق استفاده از کارکردهای مدیریت امنیت (که خارج از محدوده‌ی این استاندارد ملی است) یا از طریق استفاده از SA-P برقرار شوند.

درجه‌ی محافظتی که به‌دست می‌آید به مدیریت مناسب امنیت که شامل مدیریت کلید نیز می‌شود، بستگی خواهد داشت. رویه‌های این استاندارد ملی فرض می‌کنند که:

الف- فضای ذخیره‌سازی کلیدهای رمزنگاشتی موجود است؛

ب- در صورتی که از کلید متقارن استفاده شود، هر دو هستار انتقال دریافتی و ارسال، یک کلید رمزنگاشتی یکسان دارند. برای کلیدسازی نامتقارن، کلیدهای رمزنگاشتی یکسان برای هستارهای TLSP ارسالی و دریافتی موجود نیست. هردو کلیدسازی متقارن و نامتقارن در این استاندارد ملی مجاز هستند.

پ- کلیدهای رمزنگاشتی دوگانه هستند. به زیربند ۳-۲-۴ مراجعه شود.

این استاندارد ملی چگونگی ایجاد، به‌روزرسانی و سایر مدیریت‌های کلیدهای رمزنگاشتی را تعریف نمی‌کند.

1 - Security management requirements

۵-۵ حداقل مشخصات الگوریتم

هر دوی هستارهای انتقال ارسالی و دریافتی باید از الگوریتم یا الگوریتم‌های رمزنگاشتی یکسان استفاده کنند. مفروضات مربوط به الگوریتم‌های رمزنگاشتی به شرح زیر است:

الف- یک الگوریتم یکسان یا یک الگوریتم متفاوت باید برای ارائه خدمات محرمانگی و یکپارچگی استفاده شود؛

ب- رمزگذاری و رمزگشایی در چندین هشت‌تایی انجام می‌پذیرد؛

پ- همگام‌سازی رمزنگاشتی یا مقداردهی اولیه بر مبنای هر TPDU مجزا تحقق می‌یابد.

مشخص کردن یک الگوریتم ویژه یا ارزیابی نقاط ضعف و قوت امنیتی الگوریتم‌ها خارج از محدوده‌ی این استاندارد ملی است.

۵-۶ کارکرد کپسوله‌سازی امنیتی

کپسوله‌سازی توأم با رمزگذاری و/یا کارکرد وارسی یکپارچگی، به‌منظور ارائه خدمات محرمانگی و یکپارچگی اتصال‌گرا یا بی‌اتصال استفاده می‌شود. کارکرد رمزگذاری همیشه بر اساس رمزنگاری است، در حالی که کارکردهای وارسی یکپارچگی ممکن است براساس رمزنگاشتی باشند یا نباشند. این امر به الزامات کاربر بستگی دارد. زمانی که کپسوله‌سازی به‌وسیله هستار ارسال‌کننده استفاده می‌شود، همان‌طورکه در ITU-T | ISO/IEC 8073 Rec. X.224 و ISO/IEC 8602 | ITU-T Rec. X.234 توضیح داده شده است، پس از تمام کارکردهای پردازش پروتکل اعمال می‌شود (اما پیش از هم‌تافتگری[1] و انتساب[2] اتصال شبکه). واکپسوله‌سازی[3] به‌وسیله هستار دریافت‌کننده پس از واتافتگری[4] و پیش از دیگر کارکردهای پردازش پروتکل اعمال می‌شود.

۵-۶-۱ کارکرد رمزگذاری داده[5]

یک سازوکار رمزگذاری، محرمانگی داده را فراهم می‌کند. هر SE TPDU شامل اطلاعات کافی برای رمزگشایی مستقل از اطلاعات دیگر SE TPDUها است. این امر شامل تشخیص صفات همبستگی امنیتی (SA-ID) برای رمزگشایی و همگام‌سازی رمزنگاشتی یا دنباله‌های مقداردهی اولیه الگوریتم است.

۵-۶-۲ کارکرد یکپارچگی[6]

این کارکرد از یکپارچگی اتصال یا بی‌اتصال و همچنین احراز هویت مبدأ داده‌ها پشتیبانی می‌کند. عناصر یکپارچگی و سازوکارهای استفاده شده جهت ارائه آن‌ها عبارتند از:

---

1 - Multiplexing
2 - Assignment
3 - Decapsulation
4 - Demultiplexing
5 - Data encipherment function
6 - Integrity function

محافظت در برابر	سازوکار	CBTSS (CO)	GTSS (CL)
تغییر	ICV محاسبه شده بر روی سرآیند محافظت‌شده و PDU کپسوله‌شده	*	*
درج	ICV و شماره‌های دنباله‌ی انتقال	*	
حذف	ICV و شماره‌های دنباله‌ی انتقال	*	
بازارسال اتصال	کلید مجزا برای هر اتصال انتقال (Kg_tc) یا شناسه‌ی اتصال یکتا تحت هر کلید	*	
بازارسال PDU	کلید مجزا برای هر اتصال انتقال (Kg_tc) و استفاده از شماره‌های دنباله یکتا تحت هر کلید یا شناسه اتصال یکتا و شماره دنباله تحت هر کلید	*	
بازتاب[1]	نشانگر جهت (فیلد پرچم‌ها) در هر SE TPDU	*	*
دگرنمایی[2]	ICV و کلید یکپارچگی یا رمزگذاری، یکتا برای آدرس انتقال	*	

۵-۶-۳ کارکرد برچسب امنیت

برچسب‌گذاری امنیتی یک کارکرد اختیاری است که می‌تواند یک برچسب امنیتی را به هر مجموعه TPDU کپسوله‌شده مربوط کند. برچسب، حساسیت داده را نشان می‌دهد. برچسب امنیتی از سازوکارهای کنترل دسترسی پشتیبانی می‌کند.

ساختار و تفسیر محتویات برچسب به‌وسیله مراجع تعریف[3] گوناگون تشریح می‌شوند. مرجع تعریف با یک شناسه‌ی شئ مشخص می‌شود و مانند تعریف محتوی مشخص‌شده در CCITT Rec. X.209 | ISO/IEC 8825 کدبندی می‌شوند.

۵-۶-۴ کارکرد لت‌گذاری امنیتی[4]

لت‌گذاری امنیتی یک کارکرد اختیاری است که می‌تواند در مواقع نیاز برای افزایش طول یک مجموعه TPDU کپسوله‌شده به‌کار رود. این امر از الزامات الگوریتم رمزنگاشتی برای محرمانگی و یکپارچگی پشتیبانی می‌کند.

۵-۶-۵ کارکرد احراز هویت هستار همتا

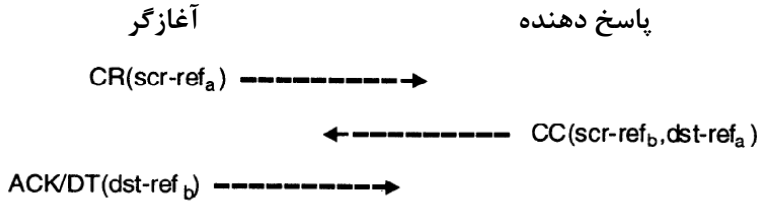
این کارکرد، احراز هویت هستار همتا را از طریق تبادل PDUهای برقراری اتصال کپسوله‌شده‌ی حاوی یک شناسه‌ی اتصال انجام می‌دهد. این رویه درشکل ۳ نمایش داده شده است.

مراجع مبدأ و مقصد باید:

- محافظت یکپارچگی داشته باشند؛ و

1 - Reflection
2 - Masquerade
3 - Defining Authorities
4 - Security padding function

- در طول عمر کلید یکپارچگی، یکتا باشند؛



شکل ۳- تصویر تبادلات برای پشتیبانی احراز هویت هستار همتا

۶-۶-۵ کارکرد SA با استفاده از SA-P ورودی

این پروتکل برای پشتیبانی از انتقال SA-P PDUها می‌تواند با استفاده از رویه‌های تعریف‌شده در ISO/IEC 8073 | ITU-T Rec. X.224 مقداردهی اولیه شود، اما این مقداردهی اولیه باید قبل از برقراری اتصال انتقال صورت پذیرد، یا از طریق کانال‌های مدیریت محلی انجام شود. در صورتی که از رویه‌های تعریف‌شده در ISO/IEC 8073 | ITU-T Rec. X.224 استفاده شده باشد، باید از یک شماره‌ی مرجع محلی استفاده کرد تا بتوان به‌صورت یکتا تشخیص داد که این امر در لایه‌ی انتقال برای برقرارسازی، نگهداری و رهاسازی SA است.

یادآوری– اگر سامانه‌هایی که ISO/IEC 8602 | ITU-T Rec. X.234 را پیاده‌سازی می‌کنند، باور داشته باشند که سطح اتکاپذیری مرتبط با برقراری یک همبستگی امنیتی در دسترس نیست، ممکن است تصمیم بگیرند که از روش SA-P ورودی در برقرارسازی یک همبستگی امنیتی استفاده نکنند.

۶ عناصر رویه[1]

عناصر رویه همان مشخصاتی هستند که در پروتکل انتقال اتصال‌گرا در (ISO/IEC 8073 | ITU-T X.224) و پروتکل ارائه خدمت انتقال حالت بی‌اتصال در (ISO/IEC 8602 | ITU-T X.234) مشخص شده است، به علاوه موارد زیر نیز مدنظر قرار گیرد:

سازوکارهای پروتکلی که در زیر توصیف شده‌اند آن‌هایی هستند که برای کپسوله‌سازی داده استفاده شده‌اند.

یک SE TPDU شامل موارد زیر است:

الف- یک سرآیند متن واضح؛

ب- یک محتوا، طول و پرچم محافظت‌شده؛ اگر محرمانگی استفاده نشده باشد، این سرآیند نیز متن واضح خواهد بود؛

پ- یک TPDU تک یا یک مجموعه از TPDUهای متصل‌شده براساس قواعد ITU-T Rec. X.224 | ISO/IEC 8073؛

ت- یک فیلد پارامتر ICV، در صورتی که محافظت یکپارچگی استفاده شود.

ث- مکان‌های درج لت‌گذاری مناسب برای محرمانگی و یکپارچگی.

1 - Elements of procedure

ج- یک برچسب امنیتی، اگر سازوکار برچسب‌گذاری انتخاب شده باشد.
یک TPDU باید براساس صفات همبستگی امنیتی محافظت شود و در SE TPDU کپسوله شود. در لحظه‌ی دریافت یک SE TPDU، هستار انتقال باید تایید کند که تمام محافظت‌های مشخص‌شده به‌وسیله‌ی صفات کلید همبستگی امنیتی ارائه شده‌اند. باید از TPDUای که به‌طور مناسب محافظت‌نشده است، (براساس صفات SA محافظت‌نشده است) صرف‌نظر شود.

یادآوری– دریافت TPDUهای به درستی محافظت‌نشده یک رویداد امنیتی است؛ به هر حال اقدام بیشتر در این مورد خارج از محدوده‌ی این استاندارد ملی است. (به‌عنوان مثال پر کردن گزارش‌های ممیزی)

اگر کارکرد کپسوله‌سازی امنیتی برای یک TPDU که برای آن یک SA مناسب موجود نیست فراخوانی شود، TLSP ممکن است یا یک پروتکل برقرارسازی SA (همان‌طورکه در این استاندارد ملی مشخص شده است) را فراخوانی کند یا عمل مناسب دیگری را انجام دهد.

۶-۱ الحاق و جداسازی[1]

رویه الحاق و جداسازی مانند خصوصیات توصیف‌شده در زیربند ۶-۴ برای پروتکل انتقال اتصال‌گرا است (به ITU-T Rec. X.224 | ISO/IEC 8073 مراجعه شود) که در آن تغییرات زیر صورت گرفته است:
الف- الحاق باید فقط قبل از کپسوله‌سازی انجام پذیرد. هر TPDUای که در ITU-T Rec. X.224 | ISO/IEC 8073 تعریف‌شده است، می‌تواند پس از کپسوله شدن در یک SE TPDU، انتقال داده شود. فقط TPDUهایی که قرار است تحت کلید همبستگی امنیتی یکسانی محافظت شوند، ممکن است به هم ملحق شوند.
ب- یک SE TPDU هرگز نباید در داخل یک SE TPDU دیگر کپسوله شود.

یادآوری– این رویه با پروتکل انتقال بی‌اتصال استفاده نمی‌شود (ITU-T Rec. X.234 | ISO 8602).

۶-۲ محرمانگی

۶-۲-۱ هدف

محرمانگی ممکن است به‌وسیله‌ی یک پروتکل انتقال در حالت اتصال و بی‌اتصال برای محافظت انتها به انتهای TPDU و عبور اطلاعات کنترل امنیت بین هستارهای انتقال ارتباط، استفاده شود.

۶-۲-۲ TPDU ها و پارامترهای استفاده شده

این رویه از TPDU و پارامترهای زیر استفاده می‌کند:
- واحد داده پروتکل انتقال کپسوله‌شده (SE-TPDU)؛
- شناسه‌ی همبستگی امنیتی (SA-ID)؛
- فیلد Crypto-synch؛
- لت رمزگذاری (Encipherment Pad).

1 - Concatenation and separation

۶-۲-۳ رویه

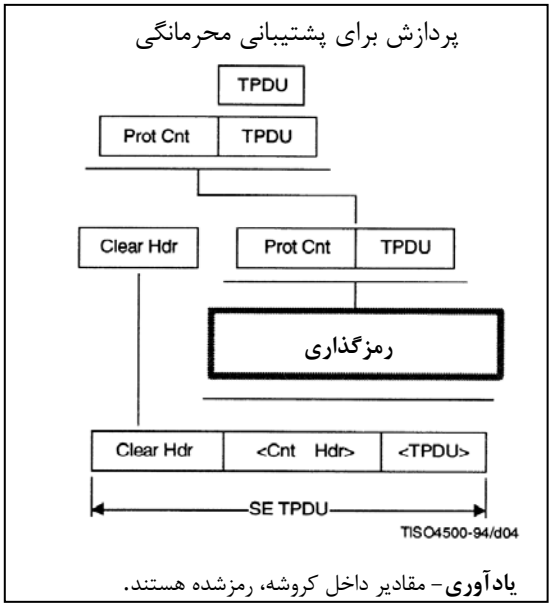
اگر محرمانگی برای یک همبستگی امنیتی مشخص شده باشد (Conf = true)، آنگاه تمامی TPDUها باید به‌وسیله کپسوله شدن در یک SE TPDU محافظت شوند. تمام هشت‌تایی‌ها که در ادامه‌ی SA-ID می‌آیند (سرآیندهای محافظت‌شده و TPDU) باید رمزگذاری شوند. شکل ۴ ملاحظه شود. اگر یک فیلد crypto-synch در الگوریتم رمزگذاری مورد نیاز باشد، باید پیش از محتوای محافظت‌شده و بعد از سرآیند واضح بیاید.

در صورت لزوم، قبل از رمزگذاری باید یک لت رمزگذاری در انتهای SE-TPDU قرار داده شود؛ به نحوی که طول محتویات محافظت‌شده (شامل فیلد طول محتوای محافظت‌شده)، به‌علاوه‌ی طول ICV و فیلد لت ICV (اگر یکپارچگی درخواست شده باشد)، به‌علاوه‌ی طول لت رمزگذاری، مضرب صحیح اندازه‌ی بستک[1] شود. به‌محض دریافت فیلد، crypto-synch در صورت وجود، برای همگام‌سازی استفاده می‌شود.

الگوریتم رمزنگاشتی به‌وسیله‌ی صفت همبستگی امنیتی مشخص می‌شود که با شناسه‌ی همبستگی امنیتی (SA-ID) شناسایی می‌شود.

به‌محض دریافت یک SE TPDU، هستار انتقال از کلید مشخص شده به‌وسیله‌ی SA-ID در SE TPDU برای شناسایی خدمت امنیتی و رمزگشایی SE TPDU استفاده می‌کند. در هنگام دریافت، محتویات فیلد لت رمزگذاری باید نادیده گرفته شود. اگر کلید در دسترس نباشد از SE TPDU صرف‌نظر می‌شود.

یادآوری - دریافت یک SE-TPDU با SA-ID نامعتبر یک رویداد امنیتی است؛ به هر حال اقدام بیشتر در این مورد خارج از محدوده‌ی این توصیه نامه|استاندارد ملی است (به عنوان مثال پر کردن گزارش‌های ممیزی).



یادآوری– مقادیر داخل کروشه، رمزشده هستند.

شکل ۴ – روش‌های کپسوله‌سازی TLSP (روش کپسوله‌سازی و رمزگذاری برای پشتیبانی از محرمانگی نشان داده شده در زیربند ۶-۲)

1 - Block

۶-۳ پردازش یکپارچگی[1]

رویه‌های زیر برای ارائه خدمات یکپارچگی اتصال‌گرا و بی‌اتصال استفاده می‌شوند.

۶-۳-۱ پردازش مقدار وارسی یکپارچگی (ICV)[2]

۶-۳-۱-۱ هدف

پردازش ICV ممکن است به‌وسیله TLSP، هم برای حالت اتصال پروتکل انتقال (| ITU-T Rec. X.224 ISO/IEC 8073) و هم برای حالت بی‌اتصال (ISO/IEC 8602 | ITU-T Rec. X.234) به‌منظور شناسایی تغییرات غیرمجاز داده‌های کاربر و اطلاعات کنترل امنیت در حین گذر بین هستارهای انتقال در حال ارتباط با یکدیگر، استفاده شود.

۶-۳-۱-۲ TPDUها و پارامترهای استفاده شده

رویه، از TPDU و پارامترهای زیر استفاده می‌کند:

- واحد داده پروتکل انتقال کپسوله‌شده (SE TPDU)؛
- شناسه‌ی همبستگی امنیتی (SA-ID)؛
- لت یکپارچگی (Integrity PAD)؛
- پردازش مقدار وارسی یکپارچگی (ICV).

۶-۳-۱-۳ رویه

دو نوع پردازش ICV وجود دارد: کد احراز هویت پیام[3] (MAC) و کد تشخیص فرابری[4] (MDC). تفاوت بین استفاده از MAC یا MDC به‌طور مستقیم وابسته به آن چیزی است که مشخص شده، یعنی وابسته به «یکپارچگی» یا «یکپارچگی و محرمانگی» است. اگر تنها یکپارچگی انتخاب شده باشد آنگاه یک MAC مبتنی بر رمز استفاده خواهد شد. در صورتی که یکپارچگی و محرمانگی انتخاب شده باشد، ICV ممکن است یک کد تشخیص فرابری (MDC) که مبتنی بر رمز نیست (مثل XOR یا checksum) ، یا یک روش مبتنی بر رمز مثل MAC باشد. از آنجایی که با انتخاب محرمانگی کل محتوای محافظت‌شده رمزنگاری خواهد شد نیازی به روش مبتنی بر رمز برای پردازش ICV نیست. اگر فقط محرمانگی انتخاب شود آنگاه فیلد ICV وجود نخواهد داشت.

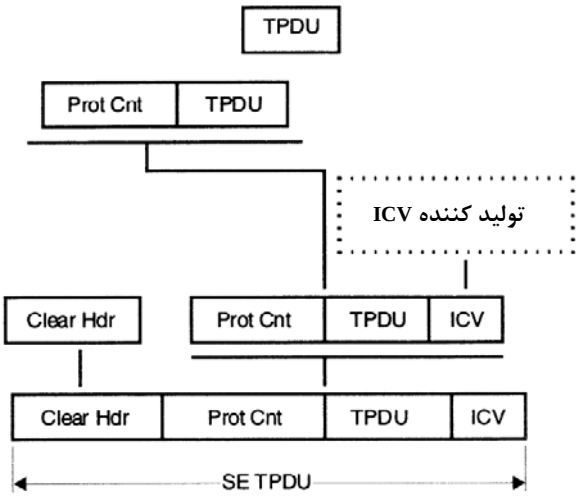
اگر یکپارچگی داده برای یک همبستگی رمزنگاشتی مشخص شود (Integ = True)، آنگاه یک ICV باید از هر SE TPDU محافظت کنـد. کد احراز هویت پیام (MAC) در پارامتر ICV حمل شده و در آخرین فیلد SE TPDU واقع می‌شود. پردازش مقدار وارسی یکپارچگی بر روی محتویات محافظت‌شده و TPDU کپسوله‌شده محاسبه می‌شود. اگر محرمانگی مشخص شود (Conf = True)، علاوه بر یکپارچگی، کد تشخیص فرابری (MDC) یا MAC مبتنی بر رمز، قبل از رمزگذاری محاسبه خواهد شد. در صورت نیاز ، لت

1 - Integrity processing
2 - Integrity Check Value (ICV) processing
3 - Message authentication code
4 - Manipulation detection code

یکپـارچگـی در محتـویات محافظت‌شـده به‌گونه‌ای قرار می‌گیـرد که طول محتـوای محافظت‌شـده (که شـامل فیلد محتـوای محافظت‌شـده نیز می‌شـود) مضرب صحیحی از انـدازه بسـتک ICV (SA Attribute ICV_Blk) شود. هنگام دریافت، باید محتوای فیلد لت‌گذاری یکپارچگی نادیده گرفته شود. شکل ۵ ملاحظه شود.

کارکرد وارسی یکپارچگی و طول فیلد ICV، صفت‌های همبستگی امنیتی هستند.

در هنگام دریافت SE TPDU در یک همبستگی امنیتی با محافظت یکپارچگی، صحت فیلد ICV باید به‌وسیله محاسبه یک آزمایش مقدار وارسی یکپارچگی بر روی محتویات محافظت‌شده و مجموعه TPDU کپسوله‌شده ارزیابی شود.



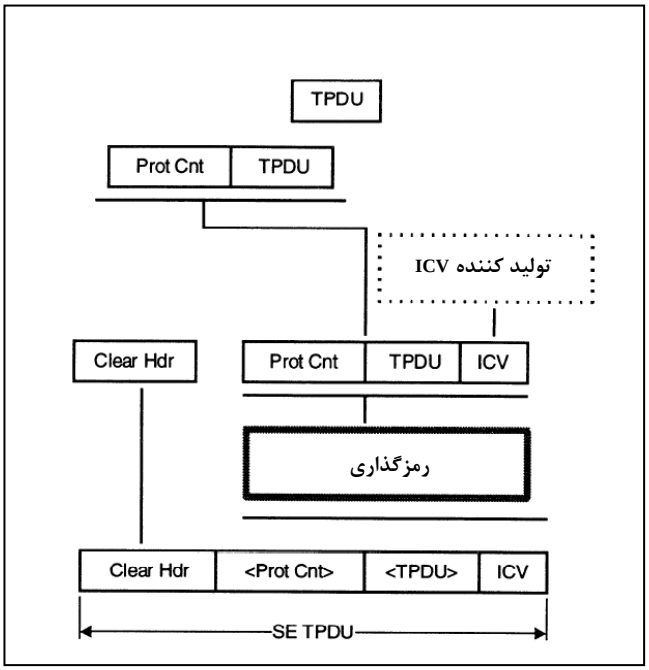
شکل ۵ – روش‌های کپسوله‌سازی TLSP (روش TLSP برای کپسوله‌سازی و تولید ICV در پشتیبانی از یکپارچگی نشان داده شده در زیربند ۶-۳)

اگر همبستگی امنیتی مشخص‌شده به‌وسیله SA-ID در دسترس نباشد یا آزمایش مقدار وارسی یکپارچگی برابر با فیلد ICV نباشد، آن‌گاه از کل SE TPDU صرف‌نظر خواهد شد.

یادآوری– شکست بررسی ICV، یک رویداد مرتبط با امنیت است؛ به هر حال اقدام بیشتر در این مورد خارج از محدوده‌ی این استاندارد ملی است (به‌عنوان مثال پر کردن گزارش‌های ممیزی).

اگر رمزگشایی نیز مورد نیاز باشد، آزمایش مقدار وارسی یکپارچگی باید پس از رمزگشایی صورت پذیرد.

شکل ۶ یکپارچگی و محرمانگی را با هم نمایش می‌دهد.



یادآوری- مقادیر درون کروشه رمزشده هستند.

شکل ۶ – روش کپسوله‌سازی TLSP (روش TLSP برای کپسوله‌سازی و تولید ICV در پشتیبانی از یکپارچگی و محرمانگی آورده شده در زیربندهای ۶-۲ و ۶-۳)

۶-۳-۲ پردازش نشانگر جهت[1]

۶-۳-۲-۱ هدف

هدف از نشانگر جهت، ارائه محافظت از بازتاب است.

۶-۳-۲-۲ TPDU ها و پارامترهای استفاده‌شده

رویه، از TPDU و پارامترهای زیر استفاده می‌کند:

- پارامتر SE TPDU؛
- پارامتر FLAGS.

۶-۳-۲-۳ رویه

هر SE TPDU باید حاوی بیت نشانگر جهتی باشد (فیلد FLAGS) که فرستنده‌ی TPDU را نشان می‌دهد. طرف‌های دخیل در همبستگی امنیتی بر روی اینکه کدام یک پاسخ‌دهنده و کدام یک آغازگر اتصال هستند توافق کرده‌اند. زمانی که یک SE TPDU به‌وسیله‌ی آغاز کننده‌ی همبستگی امنیتی ارسال می‌شود ، بیت نشانگر جهت به ۱ تنظیم می‌شود. زمانی که یک SE TPDU به‌وسیله‌ی پاسخ‌دهنده‌ی همبستگی امنیتی ارسال می‌شود ، بیت نشانگر جهت به صفر تنظیم می‌شود. در زمان دریافت یک SE TPDU، هستار انتقال باید درستی بیت نشانگر جهت را تأیید کند. اگر یک SE TPDU با نشانگر جهت نادرست دریافت شود، از آن TPDU صرف‌نظر می‌شود.

1 - Direction indicator processing

یادآوری– دریافت یک SE TPDU با نشانگر جهت نادرست یک رویداد امنیتی است. به هر حال اقدام بیشتر در این مورد خارج از محدوده‌ی این استاندارد ملی است (به‌عنوان مثال پر کردن گزارش‌های ممیزی).

۶-۳-۳ پردازش شماره‌ی دنباله‌ی یکپارچگی اتصال[1]

تشخیص بازارسال، درج و حذف نیازمند این است که هر TPDU در یک همبستگی امنیتی شماره‌ی دنباله یکتا داشته باشد. زمانی که یکپارچگی اتصال‌گرا برای یک اتصال تعیین شود (Kg_tc and Integ_yes)، این امر به‌وسیله‌ی یک کلید به ازای هر اتصال توأم با رویه شماره دنباله‌ی یکتا ارائه می‌شود. (به زیربند ۶-۳-۳-۱ مراجعه شود.) این رویه با ISO 8602 | ITU-T Rec. X.234 استفاده نمی‌شود.

۶-۳-۳-۱ شماره‌های دنباله‌ی یکتا[2]

شماره‌های دنباله‌ی یکتا، شماره‌های دنباله یکسانی هستند که در ISO/IEC 8073 | ITU-T Rec. X.224 بیان شده‌اند (به زیربندهای ۶-۱۰ و ۶-۱۱ مراجعه شود.).

۶-۳-۳-۲ هدف

شماره‌های دنباله‌ی یکتا یک رویه اختیاری برای شناسایی یکتای هر DT و ED TPDU (داده‌ی انتقال پیشتاز و عادی) در یک اتصال است. این رویه تنها به ISO/IEC 8073 | ITU-T Rec. X.224 قابل اعمال است (کلاس‌های ۲، ۳ و ۴).

۶-۳-۳-۳ رویه

اگر خدمت یکپارچگی اتصال‌گرا برای اتصال انتقال (Kg_tc و Integ = true) مشخص شود، هر TPDU در یک همبستگی امنیتی شماره دنباله‌ی یکتا خواهد داشت. هیچکدام از هستارهای انتقال نباید یک DT یا ED TPDU جدید حاوی شماره دنباله‌ای (TPDU NR یا ED TPDU NR) که از پیش با آن کلید استفاده شده است را ارسال کند. ارسال‌های مجدد[3] به‌عنوان بخشی از کنترل خطا و بازیافت عادی ممکن است شماره دنباله را تحت کلید اصلی تکرار کنند یا از یک کلید جدید استفاده کنند. زمانی که فضای شماره دنباله‌ی ED یا DT در یک اتصال به‌خصوص تمام شود، ممکن است برای ارسال TPDUهای داده‌ای بیشتر از کلید رمزنگاشتی که متفاوت از سایر کلیدهای قبلی است و برای محافظت داده به‌وسیله آن شناسه‌ی اتصال (DST-REF) به‌کار رفته بود، استفاده کند. رویه جایگزینی کلید (به زیربند ۶-۷ مراجعه شود) باید فراخوانی شود. اگر چنین کلیدی موجود نباشد ممکن است اتصال رها شود. در هنگام دریافت DT یا ED TPDUای که از رونوشت شماره دنباله‌ی دریافتی قبلی بر روی کلید رمزنگاشتی جاری استفاده کرده باشد، هستار انتقال باید از TPDU صرف‌نظر کند.

یادآوری– دریافت یک DT یا ED TPDU با یک شماره دنباله استفاده شده قبلی یک رویداد امنیتی است؛ به هر حال اقدام بیشتر در این مورد خارج از محدوده‌ی این استاندارد ملی است (به‌عنوان مثال پر کردن گزارش‌های ممیزی).

---

1 - Connection integrity sequence number processing
2 - Unique sequence numbers
1 - Retransmitions

شماره دنباله‌ی یکتا، شماره دنباله‌ی انتقال استفاده شده در کلاس‌های ۲، ۳ و ۴ است. پیشنهاد می‌شود که برای جلوگیری از کلیددهی مجدد از شماره دنباله‌های گسترش‌داده‌شده استفاده شود.

۶-۴ پردازش وارسی آدرس همتا[1]

۶-۴-۱ هدف

این رویه برای مقابله با حملات دگرنمایی و پشتیبانی از احراز هویت مبدأ داده‌ها است.

۶-۴-۲ رویه

به محض دریافت TPDU، نشانی همتای مرتبط با کلید رمزنگاشتی باید با آدرس مبدأ TPDU مقایسه شود. اگر آدرس‌ها مطابقت[2] نداشته باشند از SE TPDU صرف‌نظر خواهد شد.

یادآوری– دریافت یک SE TPDU با یک آدرس نامعتبر یک رویداد امنیتی است؛ به هر حال اقدام بیشتر در این مورد خارج از محدوده‌ی این استاندارد ملی است (به‌عنوان مثال پر کردن گزارش‌های ممیزی).

برای هر نوع از دانه‌بندی[3] کلید، یک درجه‌ی متناظر با اطلاعات آدرس همتا وجود دارد که باید درستی آن بررسی شود. زمانی که کلیددهی به ازای هر سامانه پایانی (Kg_esp) استفاده می‌شود، آدرس NSAP هستار انتقال همتا با آدرس همتای مورد گفتگوی آن بررسی می‌شود. زمانی که از کلیددهی به ازای هر سامانه‌ی پایانی و سطح امنیتی (Kg-esp-sr) استفاده می‌شود، علاوه بر بررسی آدرس NSAP هستار انتقال، برچسب امنیتی SE TPDU با مجموعه‌ی سطح امنیتی مورد گفتگو بررسی می‌شود. از آن‌جایی که برچسب امنیتی همیشه اطلاعات آدرس نیست و ممکن است به‌طور اختیاری با همبستگی‌های امنیتی تک سطحی استفاده شود، همان‌طورکه قبلاً نیز بحث شد، وارسی برچسب امنیتی به‌طور مستقل انجام می‌گیرد (به زیربند ۶-۵، برچسب امنیتی برای همبستگی‌های امنیتی، مراجعه شود.).

وقتی که برای هر اتصال (Kg-tc) کلیددهی استفاده می‌شود، رویه اندکی پیچیده‌تر می‌شود زیرا علاوه بر آدرس NSAP هستار انتقال همتا، درستی شناسه‌های اتصال انتقال (SCR-REF, DST-REF) که در TPDUهای مجزا حمل می‌شوند نیز باید بررسی شود. SCR-REF با بخش شماره‌ی مرجع انتقال راه دور صفت امنیتی آدرس همتا بررسی شده و DST-REF با مرجع محلی اتصال بررسی می‌شود. توجه شود که هستار انتقالی که یک اتصال را آغاز می‌کند ممکن است از مرجع محلی که به‌وسیله‌ی همتای آن استفاده می‌شود آگاه نباشد و ممکن است نتواند درستی SRC-REF یک CC TPDU وارده را بررسی کند. این حالت زمانی رخ می‌دهد که همتا به‌صورت پویا و براساس پردازش یک CR TPDU مرجع محلی را تعیین می‌کند و برای مدیرکلید، در زمان برقرارسازی صفات امنیتی هیچ مقداری برای حمل در دسترس نباشد. TPDU ممکن است مشروط بر این‌که ارائه فیلد DST-REF از CC TPDU با مرجع محلی اتصال یکسان باشد، پذیرفته شده و مقدار فیلد SCR-REF ابقا شود.

1 - Peer address check processing
2 - Match
3 - Granularity

۶-۵ برچسب‌های امنیتی برای همبستگی‌های امنیتی[1]

۶-۵-۱ هدف

برچسب‌های امنیتی برای ارائه پشتیبانی از کنترل دسترسی و تفکیک داده‌ها براساس حساسیت استفاده می‌شوند.

۶-۵-۲ TPDU و پارامترهای استفاده شده

رویه از TPDUها و پارامترهای زیر استفاده می‌کند:

- کپسوله‌سازی امنیتی واحد داده‌ی پروتکل انتقال (SE TPDU)؛
- شناسه‌ی همبستگی امنیتی (SA-ID)؛
- برچسب (LABEL).

۶-۵-۳ رویه

زمانی که یک همبستگی امنیتی استفاده از یک برچسب امنیتی صریح را روی هر TPDU مشخص می‌کند، برچسب باید در فیلد برچسب سرآیند محافظت‌شده‌ی هر SE TPDU ارسال شود. به‌محض دریافت یک SE TPDU حاوی پارامتر برچسب، هستار انتقال باید بررسی کند که پارامتر LABEL در مجموعه‌ی سطوح امنیتی قابل قبول برای همبستگی امنیتی قرار داشته باشد. اگر یک SE TPDU با LABEL نامناسب دریافت شود ، از TPDU صرف‌نظر خواهد شد.

یادآوری– دریافت یک SE TPDU که در بررسی برچسب رد می‌شود یک رویداد امنیتی است؛ به هر حال اقدام بیشتر در این مورد خارج از محدوده‌ی این استاندارد ملی است (به‌عنوان مثال پر کردن گزارش‌های ممیزی).

۶-۶ رهاسازی اتصال[2]

در صورتی که از خدمت اتصال‌گرا (Kg_tc) استفاده شود، کلید مرتبط با یک اتصال باید به‌عنوان بخشی از رویه رهاسازی اتصال رها شود.

۶-۷ جایگزینی کلید[3]

رویه جایگزینی کلید وقتی استفاده می‌شود که طول عمر رمز کلید منقضی شود. زمانی که از خدمت اتصال‌گرا (Kg_tc) استفاده می‌شود جایگزینی کلید در مواقعی که فضاهای شماره‌ی دنباله کاملاً پر شده باشد، به‌کار می‌رود. (به زیربند ۶-۳-۳-۱ مراجعه شود.)

جایگزینی کلید، یک کلید رمزنگاشتی جدید را به اتصالات انتقال پیش‌رو مرتبط می‌کند. همبستگی امنیتی جدید باید صفاتی مشابه همبستگی‌های امنیتی قبلی داشته باشد (به استثناء کلید جدید). اگر چنین کلیدی وجود نداشته باشد، باید هستار مدیریت امنیت باخبر شود و کلید رمزنگاشتی اصلی نباید برای ارسال‌ها استفاده شود. بعد از اینکه رویه جایگزینی کلید اجرا شد، از کلید رمزنگاشتی قدیمی صرف‌نظر می‌شود. این

1 - Security labels for Security Associations
2 - Connection release
3 - Key replacement

مورد که کلید جدید مناسب دیگری موجود نیست یک رویداد امنیتی است، در هر صورت اقدامات دیگر مثل پر کردن گزارش‌های ممیزی به‌عنوان یک موضوع محلی تلقی می‌شود.

یادآوری– کلید جدید باید در زمان فعالیت انتقال (برای کلاس ۴) یا زمان TWR (کلاس ۳) در دسترس باشد، در غیر این صورت اتصال ممکن است به‌وسیله‌ی پروتکل انتقال پایان یابد.

در ادامه‌ی جایگزینی کلید، DT و ED TPDUهای تصدیق نشده که نیازمند ارسال مجدد هستند باید تحت یک کلید جدید ارسال شوند.

۸-۶ واحدهای داده پروتکل انتقال محافظت‌نشده[1]

ممکن است خط‌مشی امنیتی، اتصالات انتقال امن و اتصالات ناامن را بین هستارهای در حال ارتباط مجاز بداند. ابزاری که به واسطه‌ی آن‌ها این امر محقق می‌شود یک موضوع محلی است.

اگر مقدار SA-Attribute UNProt در زمان ارسال درست (true) باشد، آنگاه TPDU بدون اضافه کردن پردازش PCI تحت TLSP به‌صورت ناامن عبور داده می‌شود.

اگر مقدار SA-Attribute UNProt در هنگام دریافت درست (true) باشد، TPDU دریافتی بدون هیچگونه پردازش تحت رویه‌های TLSP عبور داده می‌شود.

۹-۶ شناسایی پروتکل[2]

اگر این پروتکل بر روی اتصال شبکه به‌کار رود، باید به‌طور صریح با استفاده از رویه‌های شناسایی تعریف‌شده در ISO/IEC 11570 شناسایی شود. یک UN TPDU که عمل شناسایی را انجام می‌دهد؛ ممکن است خودش به‌وسیله‌ی پروتکل مشخص‌شده در این استاندارد ملی محافظت‌شده باشد. اگر UN TPDU محافظت‌نشده باشد و این استاندارد ملی را توأم با ISO/IEC 8073 | ITU-T Rec. X.224 یا ITU-T Rec. X.234 | ISO 8602 مشخص کرده باشد، آنگاه TPDUها پس از اتمام موفق برقراری اتصال شبکه براساس صفات SA محافظت خواهند شد. اگر UN TPDU محافظت‌شده باشد و فقط ITU-T Rec. X.224 | ISO/IEC 8073 یا ITU-T Rec. X.234 | ISO 8602 را مشخص کرده باشد، آنگاه آن تک پروتکل مشخص‌شده پس از اتمام موفق برقراری اتصال شبکه استفاده خواهد شد.

یادآوری ۱– این‌که از ارتباط محافظت‌نشده پشتیبانی می‌شود یا خیر، به صفات SA بستگی دارد.

یادآوری ۲– اگر TCهای محافظت‌نشده پشتیبانی شوند، این‌که آیا آن‌ها به‌وسیله‌ی TCهای محافظت‌شده بر روی NC یکسان هم‌تافته شده‌اند یا خیر، به صفات SA و خط‌مشی امنیتی هستار بستگی دارد.

اگر همان‌طورکه در ISO 8384 تعریف‌شده است ITU-T Rec. X.224 | ISO/IEC 8073 (کلاس ۴) بر روی خدمت شبکه بی‌اتصال OSI در حال اجرا باشد، رویه شناسایی صریح تعریف‌شده در ISO/IEC 11570 به‌کار نمی‌رود.

1 - Unprotected TPDUs
2 - Protocol identication

۶-۱۰ همبستگی امنیتی- پروتکل[1]

یک همبستگی امنیتی-پروتکل (SA-P) با تبادل SA PDUها انجام می‌شود و برای فعال‌سازی برقراری و سفارشی‌سازی یک SA طراحی شده است.

فیلدهای دقیقی که در SA PDU برای تبادل اطلاعات امنیتی به‌کار رفته‌اند، برای این‌که از SA پشتیبانی کنند، به استفاده از سازوکارهای مشخصی وابسته هستند. هر سازوکاری که برای SA-P به‌کار رفته باشد، موارد زیر را فراهم می‌کند:

الف- استخراج همه صفات SA که برای نوع محافظت انتخاب شده نیاز هستند؛

ب- احراز هویت کلیدهای استخراج شده؛

پ- برقرارسازی اطلاعات اولیه به‌منظور احراز هویت و یکپارچگی در صورت نیاز؛

ت- کلیددهی مجدد؛ و

ث- رهاسازی همبستگی امنیتی.

یک الگوریتم متقارن یا نامتقارن می‌تواند برای این منظور استفاده شود. توصیه می‌شود که یک الگوریتم نامتقارن استفاده شود. پیوست ب شامل یک مثال از چنین سازوکاری است.

در طی بخشی از فرآیند برپاسازی SA که نیازمند تبادل محافظت‌نشده اطلاعات است باید از SA-PDUها استفاده شود. تبادل محافظت‌شده‌ی اطلاعات (که برای برقرارسازی SA نیاز است)، می‌تواند در SA-PDUها یا SE-TPDUها حمل شود.

بلافاصله بعد از دریافت SA PDU نهایی در پروتکل SA-P، اگر یک TPDU در انتظار کپسوله‌سازی امنیتی باشد، پردازش شده و ارسال می‌شود.

یادآوری– آخرین SA PDU با اطلاعات کنترل امنیت باید پرچم را در SA-P از پاسخ‌دهنده به آغازگر تنظیم کند. در صورت لزوم یک SA PDU با SA-ID محلی و SA-ID همتا به‌عنوان تنها محتوا باید ارسال شود.

اگر دنباله‌ی مورد انتظار PDUها در یک مهلت زمانی مشخص رخ ندهد، یک SA PDU برای تبادل اطلاعات کنترل امنیت (SCI) ممکن است چندین بار تکرار شود. دریافت یک SA PDU که SCI آن از پیش دریافت شده است، منجر به ارسال مجدد SA PDUهایی می‌شود که از پیش در پاسخ ارسال شده بودند. SA PDUها با SCIهای خارج از دنباله‌ی مورد انتظار نادیده گرفته خواهد شد.

یک هستار TLSP در صورتی که هر کدام از بررسی‌ها به شکست منجر شود ممکن است که از رویه برقرارسازی SA صرف‌نظر کند و SA PDUهای بعدی همراه با SCI را نادیده بگیرد.

۷ استفاده از عناصر رویه

جدول ۱ مروری برعناصر رویه‌ای دارد که در هر کلاس از ITU-T Rec. X.224 | ISO/IEC 8073 و در ITU-T Rec. X.234 | ISO 8602 وجود دارد.

1 - Security Association-Protocol

جدول ۱ – عناصر TLSP رویه

سازوکار پروتکل	مرجع (زیربند)	ISO/IEC 8073, class ITU-T X.224					ISO 8602 ITU-T X.234
محرمانگی رمزنگاشتی شده	۲-۶	m	m	m	m	m	m
پردازش ICV	۱-۳-۶	m	m	m	m	m	m
پردازش نشانگر جهت	۲-۳-۶	*	*	*	*	*	*
دنباله‌ی یکتای. شماره‌ها	۱-۳-۳-۶	NA	NA	o	o	o	NA
پردازش وارسی آدرس همتا	۴-۶	*	*	*	*	*	*
برچسب‌های امنیتی برای همبستگی رمزنگاشتی	۵-۶	o	o	o	o	o	o
رهاسازی اتصال	۶-۶	o	o	o	o	o	NA
جایگزینی کلید	۷-۶	o	o	o	o	o	o

* رویه همیشه در کلاس وجود دارد.

NA کاربرد ندارد.

o رویه‌های قابل مذاکره که پیاده‌سازی آن‌ها در تجهیزات اختیاری است.

m رویه‌های قابل مذاکره که پیاده‌سازی آن‌ها در تجهیزات اجباری است.

یادآوری– همه‌ی مذاکرات یا خارج از محدوده‌ی این استاندارد ملی هستند یا از طریق رویه SA-P توصیف‌شده در زیربند ۶-۱۰ که اجازه می‌دهد مذاکرات به‌عنوان بخشی از TLSP در هر زمانی قبل از اتصال انجام گیرند، ارائه می‌شوند.

۸ ساختار و کدبندی TPDUها[1]

۸-۱ ساختار TPDU

ساختار TPDU یا TPDUهای ملحق‌شده، قبل از کپسوله‌سازی (یعنی در فیلد داده‌ی محافظت شده‌ی TPDU جاسازی شده باشند، به زیربند ۸-۲ مراجعه شود) در زیربند ۱۳-۲ از ITU-T Rec. X.224 | ISO/IEC 8073 تعریف‌شده است.

۸-۲ کپسوله‌سازی امنیتی TPDU

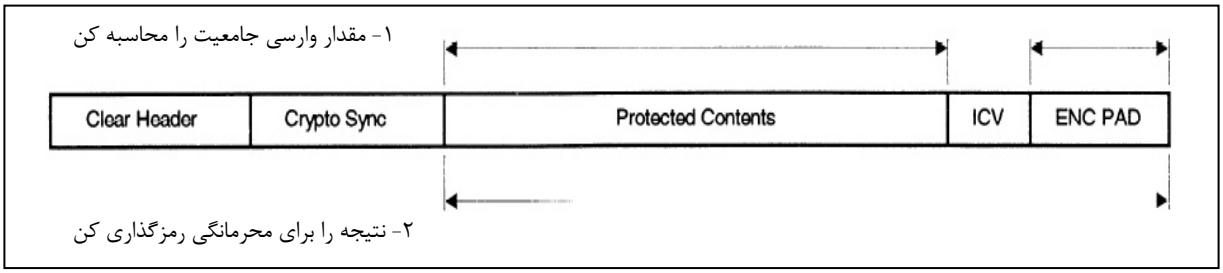
همه‌ی واحدهای داده پروتکل انتقال (SE TPDUها) باید شامل تعداد صحیحی هشت‌تایی باشند. هشت‌تایی‌ها در یک SE TPDU براساس ترتیب قرار گرفتن در یک NSDU از عدد یک شماره‌گذاری می‌شوند. بیت‌ها در یک هشت‌تایی از ۱ تا ۸ شماره‌گذاری می‌شوند (بیت ۱ کم‌اهمیت‌ترین بیت است.).

وقتی که هشت‌تایی‌های متوالی در SE TPDU برای نمایش یک عدد دودویی استفاده می‌شوند، کم‌ترین عدد هشت‌تایی پرارزش‌ترین مقدار را خواهد داشت.

برای هر فیلد با طول ثابت SE TPDU، تعداد هشت‌تایی‌های فیلد در زیرِ فیلد در شکل ۷ فهرست شده‌اند.

ساختار TPDU باید به شکل زیر باشد:

1 - Structure and encoding of TPDUs

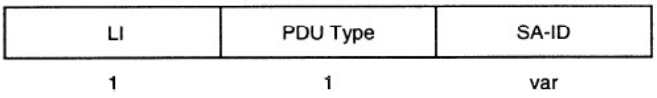


*این فیلد بستگی به این دارد که آیا الگوریتم رمزگذاری انتخاب‌شده به لت رمزگذاری مستقل نیاز دارد یا خیر.

شکل ۷ – ساختار TPDU

۸-۲-۱ سرآیند صریح[1]

شکل ۸ ملاحظه شود.



شکل ۸ – قالب سرآیند صریح

۸-۲-۱-۱ طول سرآیند صریح PDU

فیلد نشانگر طول سرآیند صریح PDU (LI) شامل طول هشت‌تایی PUD Type و SA-ID (به‌غیر از خود فیلد نشانگر طول) است.

۸-۲-۱-۲ نوع PDU[2]

این فیلد حاوی کد PDU TYPE است که برای تعریف ساختار سرآیند باقیمانده استفاده می‌شود. مقدار کد PDU TYPE برابر است با: 1000 0100.

۸-۲-۱-۳ شناسه‌ی همبستگی امنیتی

فیلد شناسه‌ی همبستگی امنیتی (SA-ID) حاوی شناسه‌ی راه دور کلید رمزنگاشتی به‌کار رفته برای محافظت TPDU است.

۸-۲-۲ فیلد Crypto sync

این یک فیلد اختیاری است که ممکن است حاوی داده‌های همگام‌سازی باشد که برای شناسه‌ی یک الگوریتم رمزگذاری مشخص در صفات همبستگی امنیتی آمده است.

یادآوری– اندازه این فیلد برای هستارهای شرکت‌کننده مشخص خواهد شد و جزیی از صفات همبستگی امنیتی است.

1 - Clear header
2 - PDU type

۸-۲-۳ محتویات محافظت‌شده [1]

شکل ۹ قالب محتویات محافظت‌شده برای یک PDU امن را نشان می‌دهد.

Content Length	Flag/type	Label	Protected Data	INT PAD
1-3	1	(tlv)	(tlv)	(tlv)[a)]

[a)] ممکن است یک لت تک هشت‌تایی باشد.

شکل ۹- محتویات محافظت‌شده

۸-۲-۳-۱ ساختار فیلد محتویات محافظت‌شده [2]

فیلدهای محتوای محافظت‌شده، نوع، طول و مقدار (tlv) کدبندی شده هستند.
نوع فیلد محتوا شامل تخصیص‌های زیر می‌شود:

نوع فیلد محتویات	مقدار
ذخیره‌شده برای استفاده خصوصی	00-7F
ذخیره‌شده	80-BF
داده‌ی محافظت‌شده	C0
ذخیره‌شده	C1-C5
برچسب	C6
ذخیره‌شده	C7-CF
ذخیره‌شده	D0
لت هشت‌تایی منفرد	D1
ذخیره‌شده	D2
لت یکپارچگی	D3
لت رمزگذاری	D4
ذخیره‌شده برای استفاده در آینده	D5-FF

اگر یک فیلد لت دو هشت‌تایی برای لت رمزگذاری یا یکپارچگی نیاز باشد، فیلد طول باید مقدار صفر و نوع فیلد محتوی مناسب داشته باشد.

1 - Protected contents
2 - Structure of protected contents field

طول فیلد محتوا، حاوی مقدار طول فیلد محتوی به‌صورت هشت‌تایی است. طول فیلد محتوا می‌تواند یک، دو یا سه هشت‌تایی باشد.

الف- اگر یک هشت‌تایی طول داشته باشد، آنگاه بیت ۸، مقدار صفر و ۷ بیت باقیمانده مقدار طولی تا حداکثر ۱۲۷ هشت‌تایی را تعریف می‌کند؛

ب- اگر دو هشت‌تایی طول داشته باشد، آنگاه هشت‌تایی اول با مقدار 1000 0001 کدبندی خواهد شد و هشت‌تایی‌های باقیمانده طول فیلدهایی تا حداکثر ۲۵۵ هشت‌تایی را تعریف می‌کند؛

پ- اگر سه هشت‌تایی طول داشته باشد، آنگاه هشت‌تایی اول با 1000 0010 کدبندی خواهد شد و دو هشت‌تایی‌های باقیمانده طول فیلد تا حداکثر ۶۵۵۳۵ هشت‌تایی را تعریف می‌کنند.

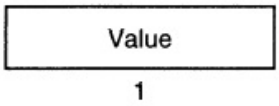
سایر مقادیر هشت‌تایی اول برای استفاده در آینده ذخیره شده‌اند.

۸-۲-۳-۲ طول محتوی[1]

فیلد طول حاوی طول محتویات محافظت‌شده به‌صورت هشت‌تایی است، اما فیلد طول محتوی را شامل نمی‌شود. (یعنی: پرچم، برچسب، داده محافظت‌شده و لت ICV) حداکثر مقدار این فیلد ۶۵۵۳۵ است.

۸-۲-۳-۳ پرچم‌ها[2]

به شکل ۱۰ مراجعه شود.



شکل ۱۰ – فیلد پرچم‌ها

بیت‌های تعریف‌شده فعلی در این فیلد عبارتند از:

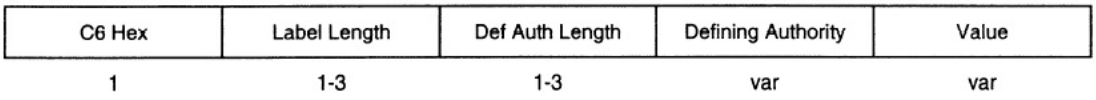
- بیت ۱ نشانگر جهت
  - 0 = از پاسخ‌دهنده به آغازگر
  - 1 = از آغازگر به پاسخ‌دهنده
- بیت ۴، به سمت خارج / پاسخ
  - 0 = به سمت خارج
  - 1 = پاسخ

بیت‌های ۲،۳ و ۵ تا ۸ که بیت‌های بدون استفاده پرچم هستند در ارسال با مقدار صفر تنظیم می‌شوند.

۸-۲-۳-۴ برچسب

شکل ۱۱ ملاحظه شود.

1 - Content length
2 - Flags



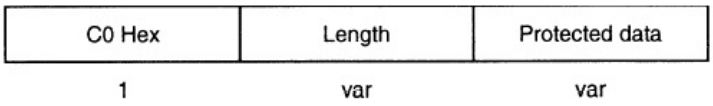
شکل ۱۱ – قالب فیلد برچسب

قالب فیلد مقدار به‌وسیله مراجع تعریف مشخص می‌شود.

یادآوری– انتظار می‌رود که این برچسب‌ها تحت رویه‌های تعریف‌شده در ISO و CCITT ثبت شوند. یک مرجع تعریف به‌عنوان مقدار شناسه‌ی شئ مطابق با استاندارد ISO 8824 ثبت خواهد شد، بر طبق استاندارد ISO 8825 و با استفاده از رویه‌های تعریف‌شده در استاندارد ISO/IEC 9834 کدبندی خواهد شد.

۸-۲-۳-۵ داده‌ی محافظت‌شده

فیلد داده حاوی یک TPDU یا یک مجموعه از TPDUهای به‌هم الحاق‌شده بر طبق ITU-T Rec. X.224 | ISO/IEC 8073 یا ITU-T Rec. X.234 | ISO/IEC 8602 است. (شکل ۱۲ ملاحظه شود.)



شکل ۱۲ – قالب فیلد داده‌ی محافظت‌شده

۸-۲-۳-۶ لت یکپارچگی[1]

فیلد مقدار، حاوی داده‌های اختیاری مورد نیاز برای سازوکارهای یکپارچگی است.

طول لت‌گذاری به‌وسیله‌ی موارد زیر تعریف می‌شود:

الف– لت‌گذاری که برای سازوکار یکپارچگی نیاز است.

سازوکار یکپارچگی که استفاده می‌شود صفات شناخته شده‌ای دارد که شامل طول بستک تعریف‌شده برای استفاده در همبستگی امنیتی است (اگر سازوکار در حالت بستک استفاده شود.). نقطه‌ی شروع پردازش یکپارچگی تا انتهای لت یکپارچگی باید مضرب صحیحی از طول بستک باشد.

ب- برای سازوکار رمزگذاری بستک که انتهای ICV را به‌میزان اندازه بستک افزایش دهد، لت‌گذاری مورد نیاز است (در صورتی که لت رمزگذاری جداگانه‌ای نیاز نباشد.).

انتخاب مقدار لت، یک موضوع محلی است. اگر یک لت هشت‌تایی منفرد مورد نیاز باشد، یک Single Octet Pad (Type برابر است با D1 بدون طول یا مقدار) به جای لت یکپارچگی به‌کار می‌رود.

۸-۲-۴ فیلد ICV

فیلد ICV حاوی مقدار وارسی یکپارچگی است. طول این فیلد به‌طور ضمنی به‌وسیله‌ی شناسه‌ی الگوریتم ICV که در صفات همبستگی امنیتی موجود است، تعیین می‌شود.

1 - Integrity PAD

۸-۲-۵ لت رمزگذاری[1]

اندازه‌ی بستک رمزگذاری یک ویژگی شناخته‌شده از الگوریتم رمزگذاری است. نقطه‌ی آغاز پردازش محرمانگی تا انتهای ICV باید مضرب صحیحی از طول بستک باشد. وجود لت رمزگذاری که در ادامه ICV می‌آید بستگی به این دارد که آیا الگوریتم رمزگذاری انتخاب‌شده نیازمند یک لت رمزگذاری مستقل است یا خیر.

انتخاب مقدار لت، یک موضوع محلی است. اگر یک لت هشت‌تایی منفرد نیاز باشد، یک Single Octet Pad (Type = D1 – بدون طول یا مقدار) به جای لت رمزگذاری استفاده می‌شود.

۸-۳ همبستگی امنیتی PDU

قالب SA PDU در شکل ۱۳ نمایش داده شده است.

LI	PDU Type	SA-ID	SA-P-Type	SA PDU Contents
1	1	var	lv	var

شکل ۱۳ – ساختار SA PDU

۸-۳-۱ شناسه‌ی طول (فیلد LI)

این فیلد حاوی طول فیلد نوع PDU به اضافه‌ی SA-ID است. اگر SA-ID نیاز به فرستادن سیگنال به همتایش مبنی بر این‌که SA-ID آن را نمی‌شناسد (برای مثال در زمان برقرارسازی یک SA جدید) داشته باشد، فیلد طول باید به شکلی تنظیم شود که نشان دهد فیلد SA-ID موجود نیست (یعنی مقدار آن ۱ است.).

۸-۳-۲ نوع PDU

این فیلد حاوی مقدار نوع PDU 0100 1001 برای نشان دادن یک همبستگی امنیتی PDU است.

۸-۳-۳ شناسه همبستگی امنیتی

فیلد SA-ID حاوی شناسه‌ی همبستگی امنیتی دریافت‌کننده است (صفت Peer_SAID SA). این فیلد زمانی که SA-P برای برقرارسازی یک SA جدید به‌کار می‌رود، نیاز نیست (به این معنی که دریافت‌کننده هنوز یک SA-ID تخصیص نداده است.).

۸-۳-۴ نوع SA-P

این فیلد حاوی شناسه‌ی شئ‌ای است که سازوکارهای مجموعه‌ای را که برای ارائه پروتکل SA استفاده می‌شوند، (مطابق آن‌چه در ادامه آمده است.) مشخص می‌کند.

شناسه‌ی شئ برای تبادل کلید نمایی اختصاص داده شده است (همان‌طورکه در پیوست ت تعریف‌شده است (joint-ccitt-iso (2) tlsp (21) sa-p-kte (1) eke (1).

1 - Encipherment PAD

استفاده از سایر الگوریتم‌ها با SA-P ممکن است با شناسه‌های شئ بیشتر که طبق استاندارد ISO 9834-1 تعیین می‌شوند، نشان داده شوند (رویه‌های ثبت).

۸-۳-۵ محتویات SA PDU

ساختار داخلی این فیلد همان‌طورکه در زیربند ۸-۳-۴ مشخص شد بستگی به سازوکار ارائه پروتکل SA دارد. پیوست ب، چنین پروتکل SAای را که از تبادل کلید نشانه و سازوکارهای امضای رقمی استفاده می‌کند تعریف می‌نماید.

۹ انطباق[1]

۹-۱ عمومی

بیانیه‌ی انطباق پیاده‌سازی پروتکل (PICS) باید با در نظر گرفتن هر ادعایی مبنی بر انطباق با پیاده‌سازی این استاندارد ملی تکمیل شود. PICS باید بر طبق پیش‌نویس PICS مربوطه تولید شود.

۹-۲ الزامات انطباق ایستای مشترک[2]

الف- یک پیاده‌سازی دارای انطباق حداقل باید با ISO/IEC 8073 | ITU-T Rec. X.224 یا ITU-T Rec. | ISO/IEC 8602 X.234 از TLSP پشتیبانی کند.

ب- یک پیاده‌سازی منطبق باید از پیاده‌سازی در یک سامانه نهایی پشتیبانی کند.

پ- هر سامانه‌ای که ادعای انطباق با TLSP را دارد باید بتواند داده‌های کاربر را در یک PDU انتقال داده امن، کپسوله کرده و استخراج کند.

ت- هر سامانه‌ای که ادعای ارائه خدمات امنیتی محرمانگی را دارد باید حداقل از سازوکار رمزگذاری پشتیبانی کند.

ث- هر سامانه‌ای که ادعای ارائه خدمات امنیتی یکپارچگی را دارد باید حداقل از سازوکار ICV پشتیبانی کند.

۹-۳ پروتکل امنیتی لایه انتقال با الزامات انطباق ایستای ISO 8602 | ITU-T Rec. X.234

هر سامانه‌ای که ادعای انطباق با پروتکل TLSP را داشته باشد باید حداقل یکی از خدمات امنیتی زیر را ارائه کند:

الف- محرمانگی بی‌اتصال؛ و

ب- یکپارچگی بی‌اتصال.

۹-۴ پروتکل امنیتی لایه انتقال با الزامات انطباق ایستای ISO 8073 | ITU-T Rec. X. 224

هر سامانه‌ای که ادعای انطباق با پروتکل TLSP را داشته باشد باید حداقل یکی از خدمات امنیتی زیر را ارائه کند:

الف- محرمانگی اتصال

1 - Conformance

2 - Common static conformance requirements

ب- یکپارچگی اتصال بدون بازیافت
پ- احراز هویت هستار همتا.

۹-۵ الزامات انطباق پویای مشترک[1]

هر سامانه‌ای که ادعای انطباق با این استاندارد ملی را داشته باشد، باید مطابق زیر رفتار کند:
الف- تشخیص همه‌ی فیلدهای اجباری و اختیاری در یک PDU انتقال داده‌ی امن در یک دنباله.
ب- با فیلدهای تشخیص‌داده نشده در یک PDU انتقال داده‌ی امن باید مانند یک خطا برخورد شود (همان‌طورکه در بند ۶ توضیح داده شد.).

۹-۶ پروتکل امنیتی لایه انتقال با الزامات انطباق پویای ISO 8602 | ITU-T Rec. X.234

هر سامانه‌ای که ادعای انطباق با پروتکل TLSP را دارد باید مطابق زیر رفتار کند:
- زمانی که احراز هویت مبدأ داده‌ها ارائه می‌شود، باید یا سازوکار رمزگذاری یا یک سازوکار رمزنگاشتی ICV فراخوانی شود.

۹-۷ پروتکل امنیتی لایه انتقال با الزامات انطباق پویای ISO 8073 | ITU-T Rec. X.224

هر سامانه‌ای که ادعای انطباق با پروتکل TLSP را دارد باید مطابق زیر رفتار کند:
- زمانی که هستار همتا یا احراز هویت مبدأ داده‌ها ارائه می‌شود باید یا سازوکار رمزگذاری یا یک سازوکار رمزنگاشتی ICV فراخوانی شود.

۱۰ بیانیه‌ی انطباق پیاده‌سازی پروتکل PICS[2]

تأمین‌کننده یک پیاده‌سازی پروتکل که ادعای انطباق با این استاندارد ملی را دارد باید رونوشتی از پیش‌نویس PICS ارائه شده در پیوست الف (که شامل اطلاعات لازم جهت شناسایی کامل تأمین‌کننده و پیاده‌سازی می‌شود) را تکمیل کند.

1 - Common dynamic conformance requirements
2 - Protocol implementation conformance statement

پیوست الف

(الزامی)

پیش‌برگ (مقدماتی)[1] PICS[2]

الف-۱ مقدمه

الف-۱-۱ پیش‌زمینه

تأمین‌کننده پیاده‌سازی پروتکل که ادعای انطباق با این استاندارد را دارد، باید پروتکل امنیتی لایه‌ی انتقال (TLSP) و پیش‌نویس بیانیه‌ی انطباق پیاده‌سازی پروتکل (PICS) را تکمیل کند. پیش‌نویس تکمیل‌شده‌ی PICS تبدیل به PICS برای پیاده‌سازی می‌شود. PICS بیانیه‌ای است که قابلیت‌ها و گزینه‌های پروتکل پیاده‌سازی‌شده را مشخص می‌کند. PICS می‌تواند کاربردهای مختلفی داشته باشد، از جمله:

- به‌وسیله‌ی پیاده‌ساز پروتکل، به‌عنوان یک فهرست بررسی برای کاهش خطر تخطی از استاندارد ناشی از خطاهای سهوی، استفاده شود.
- به‌وسیله‌ی تأمین‌کننده و دریافت‌کننده‌ی پیاده‌سازی، حاکی از توانایی‌های آن به‌طور تفصیلی، که مرتبط با اساس مشترک از درک ارائه شده به‌وسیله‌ی پیش‌نویس PICS ارائه استاندارد است، بیان می‌شود.
- به‌وسیله‌ی کاربر پیاده‌ساز به‌عنوان پایه‌ای برای وارسی امکان کار و تبادل با یک پیاده‌سازی دیگر استفاده شود.
- به‌وسیله‌ی یک آزمون‌گر پروتکل، به‌عنوان اساس انتخاب آزمون‌های مناسب برای بررسی ادعای انطباق با پیاده‌سازی استفاده شود.

الف-۱-۲ رویکرد

اولین بخش پیش‌نویس PICS، شناسایی پیاده‌سازی و خلاصه‌ی پروتکل، باید همان‌طورکه نشان داده شد با اطلاعات ضروری برای شناسایی کامل تأمین‌کننده و پیاده‌سازی کامل شود. بخش اصلی پیش‌نویس PICS یک پرسش‌نامه با قالب ثابت است که به چند زیربند (که هر کدام حاوی چندین مورد مجزا هستند) تقسیم می‌شود. سوالات این پرسش‌نامه در آخرین ستون سمت راست یا با علامت‌گذاری جواب در مواردی که انتخاب محدود شده است (به‌طور معمول «بله» یا «خیر») یا وارد کردن یک مقدار یا یک مجموعه یا گستره‌ای[3] از مقادیر، پاسخ داده می‌شوند. توجه شود که در بعضی موارد می‌توان دو یا چند جواب از میان جواب‌های ممکن را انتخاب کرد. بنابراین همه‌ی انتخاب‌های مرتبط باید علامت‌گذاری شوند.

---

1 - Proforma

۲ - رهاسازی حقوق مؤلف برای پیش‌نویس PICS : کاربران این استاندارد ملی می‌توانند آزادانه پیش‌نویس PICS موجود در این پیوست را بازتولید کنند، تا بتوانند از این پیش‌نویس برای اهداف موردنظر خود استفاده کنند و می‌توانند PICS تکمیل شده را انتشار دهند.

3 - Range

هر مورد با یک شاخص مرجع در ستون اول مشخص می‌شود؛ ستون دوم حاوی موردی است که آدرس‌دهی می‌شود و ستون سوم حاوی محل مرجع (مراجع) مورد اشاره در بدنه‌ی اصلی استاندارد است. برای موردهای اختیاری، ستون‌های اضافی، نشان‌دهنده‌ی وضعیت مورد هستند (یعنی بیان می‌کنند که آیا پشتیبانی اجباری، اختیاری یا مشروط است) و فضا یا انتخاب یا موردها را برای پاسخ پشتیبانی‌شده در پیاده‌سازی فراهم می‌کنند.

نشان‌گذاری‌های ستون وضعیت زیر که در ISO/IEC JTC1 | SC6 N6233 توصیف شده‌اند. فهرست نشان‌گذاری‌های پیش‌نویس PICS، برای این پیش‌نویس PICS استفاده می‌شوند.

نماد	معنی
M	اجباری
O	اختیاری
-	غیر کاربردی (N/A)
o.<n>	اختیاری، اما پشتیبانی از حداقل یکی از گروه اختیارات برچسب‌زده شده به‌وسیله‌ی عدد یکسان <n> الزامی است.
<cid>:	الزامات مشروط، منطبق بر شاخص شرط یا مورد مشخص‌شده به‌وسیله‌ی <cid>
<item>::	شرط گزاره‌ی ساده، وابسته به پشتیبانی علامت‌گذاری‌شده برای <item>

الف-۲ شناسایی پیاده‌سازی

به جدول الف-۱ مراجعه شود.

جدول الف-۱ شناسایی پیاده‌سازی TLSP

مورد	اطلاعات
تأمین‌کننده	
نقطه‌ی تماس برای درخواست‌های مرتبط با این PICS	
نام(ها) و نسخه(های) پیاده‌سازی	
اطلاعات ضروری دیگر برای شناسایی کامل (به‌عنوان مثال نام‌ها و نسخه(های) ماشین‌ها و سامانه‌های عامل، نام(های) سامانه	
یادآوری ۱- تنها سه مورد اول برای هر پیاده‌سازی ضروری هستند. سایر اطلاعات ممکن است برای برآورده کردن الزامات در راستای شناسایی کامل تکمیل شوند. **یادآوری ۲**- اصطلاحات «نام» و «نسخه» باید متناسب با واژگان فنی تأمین‌کننده به‌طور مناسب تفسیر شوند. (به‌عنوان مثال با استفاده از نوع، سری و مدل)	

الف-۳ بیانیه‌ی انطباق عمومی

جدول الف-۲ بیانیه‌ی انطباق عمومی را برای پیاده‌سازی تدوین می‌کند.

جدول الف-۲– بیانیه انطباق عمومی

نشانه مورد		پشتیبانی	
SP	آیا پیاده‌سازی ادعای انطباق با ISO/IEC 10736 را دارد؟	بله	خیر
SPMAN	آیا همه صفات اجباری ISO/IEC 10736 پیاده‌سازی شده‌اند؟	بله	خیر

الف-۴ پیاده‌سازی پروتکل

جدول الف-۳ کوته‌نوشت‌های معمول به‌کار رفته در PICSها را مشخص می‌کند، همین کوته‌نوشت‌ها در استاندارد ISO/IEC 8073 | ITU-T Rec. X.224 نیز وجود دارند اما در اینجا نیز برای کمک در انطباق با این PICS آمده‌اند.

جدول الف-۳ CO و CL پیاده‌سازی‌شده در انتقال

خدمت شبکه کلاس انتقال شاخص	
C0	کلاس ۰ بر روی cons
C1	کلاس ۱ بر روی cons
C2	کلاس ۲ بر روی cons
C3	کلاس ۳ بر روی cons
C4	کلاس ۴ بر روی cons
C4L	کلاس ۴ بر روی clns
CLTP	پروتکل انتقال بی‌اتصال

الف-۵ خدمات امنیتی پشتیبانی‌شده

جدول الف-۴ تا الف-۷ برای هر کلاس انتقال (COTP::) خدمات امنیتی در دسترس از طریق TLSP و سطح پشتیبانی آن‌ها در پیاده‌سازی را مشخص می‌کنند. خدمات امنیتی فهرست شده از استاندارد CCITT Rec. X.800 | ISO 7498-2 گرفته شده‌اند.

جدول الف-۴ – پیش‌نویس عنصر خدمت برای C0

عنصر خدمت شاخص	وضعیت	پشتیبانی	
محرمانگی TOSE0	0.1	بله	خیر
محرمانگی اتصال TOSE1	TOSE0:m	بله	خیر
محرمانگی بی‌اتصال TOSE2	-		
یکپارچگی TOSE3	0.1	بله	خیر
یکپارچگی اتصال TOSE4 با قابلیت بازیافت	-		
یکپارچگی اتصال TOSE5 بدون قابلیت بازیافت		بله	خیر
یکپارچگی بی‌اتصال TOSE6	TOSE3:m		
احراز هویت هستار همتا TOSE7	0	بله	خیر
کنترل دسترسی TOSE8	0	بله	خیر
TOSE9 ورودی SA-P	0	بله	خیر

جدول الف-۵ – پیش‌نویس عنصر خدمت برای C1، C2، C3

عنصر خدمت شاخص	وضعیت	پشتیبانی	
محرمانگی T3SE0	0.1	بله	خیر
محرمانگی اتصال T3SE1	T3SE0:m	بله	خیر
محرمانگی بی‌اتصال T3SE2	-		
یکپارچگی T3SE3	0.1	بله	خیر
یکپارچگی اتصال T3SE4 با قابلیت بازیافت	-		
یکپارچگی اتصال T3SE5 بدون قابلیت بازیافت	T3SE3:0.2	بله	خیر
یکپارچگی بی‌اتصال T3SE6	T3SE3:0.2	بله	خیر
احراز هویت هستار همتا T3SE7	0	بله	خیر
کنترل دسترسی T3SE8	0	بله	خیر

جدول الف-۶ – پیش‌نویس عنصر خدمت برای C4

عنصر خدمت شاخص	وضعیت	پشتیبانی	
محرمانگی T4SE0	0.1	بله	خیر
محرمانگی اتصال T4SE1	T4SE0:m	بله	خیر
محرمانگی بی‌اتصال T4SE2	-		
یکپارچگی T4SE3	0.1	بله	خیر
یکپارچگی اتصال T4SE4 با قابلیت بازیافت	T4SE3:0.2	بله	خیر
یکپارچگی اتصال T4SE5 بدون قابلیت بازیافت	-	بله	خیر
یکپارچگی بی‌اتصال T4SE6	T3SE3:0.2	بله	خیر
احراز هویت هستار همتا T4SE7	0	بله	خیر
کنترل دسترسی T4SE8	0	بله	خیر

جدول الف-۷ – پیش‌نویس عنصر خدمت برای C4L

عنصر خدمت شاخص	وضعیت	پشتیبانی	
محرمانگی TLSE0	0.1	بله	خیر
محرمانگی بی‌اتصال TLSE2	TLSE0:m	بله	خیر
محرمانگی اتصال TLSE1	-		
یکپارچگی TLSE3	0.1	بله	خیر
یکپارچگی اتصال TLSE4 با قابلیت بازیافت	TLSE3:0.2		
یکپارچگی اتصال TLSE5 بدون قابلیت بازیافت	-		
یکپارچگی بی‌اتصال TLSE6	T3SE3:0.2	بله	خیر
احراز هویت هستار همتا TLSE7	0	بله	خیر
کنترل دسترسی TLSE8	0	بله	خیر

جدول الف-۸ برای هر کلاس انتقال بی‌اتصال (COTP::)[1] خدمات امنیتی در دسترس از طریق TLSP و سطح پشتیبانی آن‌ها در پیاده‌سازی را مشخص می‌کنند.

۱- علامت :: برای مشخص‌کردن کلاس‌ها استفاده می‌شود.

جدول الف-۸ – پیش‌نویس عنصر خدمت برای CLTP

عنصر خدمت شاخص	وضعیت	پشتیبانی	
محرمانگی TCSE0	0.1	بله	خیر
محرمانگی اتصال TCSE1	-		
محرمانگی بی‌اتصال TCSE2	TCSE0:m	بله	خیر
یکپارچگی TCSE3	0.1	بله	خیر
یکپارچگی اتصال TCSE4 با قابلیت بازیافت	-		
یکپارچگی اتصال TCSE5 بدون قابلیت بازیافت	-		
یکپارچگی بی‌اتصال TCSE6	TCSE3:m	بله	خیر
احراز هویت مبدأ داده TCSE7	0	بله	خیر
کنترل دسترسی TCSE8	0	بله	خیر

الف-۶ کارکردهای پشتیبانی‌شده

جداول الف-۹ تا الف-۱۶ کارکردهای پیاده‌سازی‌شده‌ی اجباری و اختیاری برای هر کلاس انتقال (COTP::) پشتبیانی‌شده را مشخص می‌کنند.

جدول الف-۹ – کارکردهای اجباری برای C0

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
T0SF1	تأیید آدرس همتا	۵-۶-۲، ۶-۴	m	بله	
T0SF2	تشخیص بازتاب	۵-۶-۲، ۶-۳-۲	m	بله	
T0SF3	کپسوله‌سازی امنیتی	۶-۵	m	بله	
T0SF4	گزارش رویدادهای امنیتی	یادآوری‌ها	m	بله	

جدول الف-۱۰ – کارکردهای اختیاری برای C0

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
T0SF5	رمزگذاری داده	۶-۲	0.1	بله	خیر
T0SF6	محافظت یکپارچگی	۶-۳	0.1	بله	خیر
T0SF7	لت‌گذاری یکپارچگی	۶-۳-۱-۳	0	بله	خیر
T0SF8	برچسب‌زنی امنیتی صریح	۶-۵	0	بله	خیر
T0SF9	لت‌گذاری رمزگذاری	۶-۲-۲	0	بله	خیر

جدول الف-۱۱ – کارکردهای اجباری برای C1

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
T1SF1	تأیید آدرس همتا	۵-۶-۲، ۶-۴	m	بله	
T1SF2	تشخیص بازتاب	۵-۶-۲، ۶-۳-۲	m	بله	
T1SF3	تفکیک پس از واکپسوله‌سازی	۶-۱	m	بله	
T1SF4	کپسوله‌سازی امنیتی	۶-۵	m	بله	
T1SF5	گزارش رویدادهای امنیتی	یادآوری‌ها	m	بله	

جدول الف-۱۲ – کارکردهای اختیاری برای C1

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
T1SF6	رمزگذاری داده	۶-۲	0.1	بله	خیر
T1SF7	محافظت یکپارچگی	۶-۳	0.1	بله	خیر
T1SF8	الحاق پیش از کپسوله‌سازی	۶-۱	0	بله	خیر
T1SF9	لت‌گذاری یکپارچگی	۶-۳-۱-۳	0	بله	خیر
T1SF10	برچسب‌زنی امنیتی صریح	۶-۵	0	بله	خیر
T1SF11	لت‌گذاری رمزگذاری	۶-۲-۲	0	بله	خیر

جدول الف-۱۳ – کارکردهای اجباری برای C2، C3

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
T3SF1	تأیید آدرس همتا	۵-۶-۲، ۶-۴	m	بله	
T3SF2	تشخیص بازتاب	۵-۶-۲، ۶-۳-۲	m	بله	
T3SF3	تفکیک پس از واکپسوله‌سازی	۶-۱	m	بله	
T3SF4	هم‌تافتگری امن	ضمنی	m	بله	
T3SF5	کپسوله‌سازی امنیتی	۶-۵	m	بله	
T3SF6	گزارش رویدادهای امنیتی	یادآوری‌ها	m	بله	

جدول الف-۱۴ – کارکردهای اختیاری برای C2، C3

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
T3SF7	رمزگذاری داده	۶-۲	0.1	بله	خیر
T3SF8	محافظت یکپارچگی	۶-۳	0.1	بله	خیر
T3SF9	فضای شماره دنباله‌ی یکپارچگی	۶-۳-۳	0	بله	خیر
T3SF10	الحاق قبل از کپسوله‌سازی	۶-۱	0	بله	خیر
T3SF11	لت‌گذاری یکپارچگی	۶-۳-۱-۳	0	بله	خیر
T3SF12	برچسب‌زنی امنیتی صریح	۶-۵	0	بله	خیر
T3SF13	لت‌گذاری رمزگذاری	۶-۲-۲	0	بله	خیر

جدول الف-۱۵ – کارکردهای اجباری برای C4، C4L

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
T4SF1	تأیید آدرس همتا	۶-۵-۲-۶، ۶-۴	m	بله	
T4SF2	تشخیص بازتاب	۶-۵-۲-۶، ۶-۳-۲	m	بله	
T4SF3	تفکیک پس از واکپسوله‌سازی	۶-۱	m	بله	
T4SF4	هم‌تافتگری امن	ضمنی	m	بله	
T4SF5	کپسوله‌سازی امنیتی	۶-۵	m	بله	
T4SF6	گزارش رویدادهای امنیتی	یادآوری‌ها	m	بله	

جدول الف-۱۶ – کارکردهای اختیاری برای C4، C4L

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
T4SF7	رمزگذاری داده	۶-۲	0.1	بله	خیر
T4SF8	محافظت یکپارچگی	۶-۳	0.1	بله	خیر
T4SF9	فضای شماره دنباله‌ی یکپارچگی	۶-۳-۳	0	بله	خیر
T4SF10	الحاق کپسوله‌سازی اولیه	۶-۱	0	بله	خیر
T4SF11	لت‌گذاری یکپارچگی	۶-۳-۱-۳	0	بله	خیر
T4SF12	برچسب‌زنی امنیتی صریح	۶-۵	0	بله	خیر
T4SF13	لت‌گذاری رمزگذاری	۶-۲-۲	0	بله	خیر

جداول الف-۱۷ و الف-۱۸ کارکردهای اجباری و اختیاری پیاده‌سازی شده برای انتقال بی‌اتصال (CLTP::) را شناسایی می‌کنند.

جدول الف-۱۷ – کارکردهای اجباری برای CLTP

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
TLF1	تأیید آدرس همتا	۵-۶-۲، ۶-۴	m	بله	
TLF2	تشخیص بازتاب	۵-۶-۲، ۶-۳-۲	m	بله	
TLF3	کپسوله‌سازی امنیتی	۵-۶	m	بله	
TLF4	گزارش رویدادهای امنیتی	۵-۲-۱، ۶	m	بله	

جدول الف-۱۸ – کارکردهای اختیاری برای CLTP

شاخص	عملکرد	مرجع (زیربند)	وضعیت	پشتیبانی	
TLF5	رمزگذاری داده	۶-۲	0.1	بله	خیر
TLF6	محافظت یکپارچگی	۶-۳	0.1	بله	خیر
TLF7	لت‌گذاری یکپارچگی	۶-۳-۱-۳	0	بله	خیر
TLF8	برچسب‌زنی امنیتی صریح	۶-۵	0	بله	خیر
TLF9	لت‌گذاری رمزگذاری	۶-۲-۲	0	بله	خیر

الف-۷ واحدهای داده‌ی پروتکل (PDUs) پشتیبانی‌شده

الف-۷-۱ PUDهای انتقال پشتیبانی‌شده

همان‌طورکه در جدول الف-۱۹ نشان داده شده است، از SE TPDU هم برای ارسال و هم برای دریافت در پروتکل اتصال‌گرا (COTP::) و پروتکل انتقال بی‌اتصال (CLTP::) پشتیبانی می‌شود.

جدول الف-۱۹ – TPDUهای پشتیبانی‌شده

شاخص	TPDU	مورد	وضعیت	پشتیبانی	
STS1	SE	ارسال COTP یا CLTP	m	بله	
STS2	SE	دریافت COTP یا CLTP	m	بله	

الف-۷-۲ پارامترهای پشتیبانی TPDUهای صادر شده

جدول الف-۲۰ و الف-۲۱ مشخص می‌کنند که کدام پارامترها، وقتی که یک SE TPDU به‌وسیله انتقال صادر می‌شود اجباری یا اختیاری هستند (COTP:: یا CLTP::).

جدول الف-۲۰ – پارامترهای اجباری برای COTP، CLTP

شاخص	پارامتر	مرجع (زیربند)	وضعیت	پشتیبانی	
SPI1	شناسه‌ی کلید باید ارائه شده باشد.	۶-۲، ۶-۳	m	بله	
SPI2	بیت اول پرچم سرآیند محافظت‌شده باید به عنوان نشانگر جهت تنظیم شود.	۸-۲-۳-۳	m	بله	

جدول الف-۲۱ – پارامترهای اختیاری برای COTP، CLTP

شاخص	پارامتر	مرجع (زیربند)	وضعیت	پشتیبانی	
SPI3	برچسب	۸-۲-۳-۴	0	بله	خیر
SPI4	لت یکپارچگی	۸-۲-۳-۶	0	بله	خیر
SPI5	ICV	۸-۲-۴	0	بله	خیر
SPI6	لت رمزگذاری	۸-۲-۵	0	بله	خیر

الف-۷-۳ پارامترهای پشتیبانی‌شده برای TPDUهای دریافتی

پیاده‌سازی‌ها باید قابلیت دریافت و پردازش همه‌ی پارامترهای ممکن SE TPDU نشان داده شده در جدول الف-۲۲ را داشته باشند.

جدول الف-۲۲ – پارامترهای اجباری برای COTP، CLTP

شاخص	پارامتر	مرجع (زیربند)	وضعیت	پشتیبانی	
SPR1	شناسه‌ی کلید باید ارائه شود	۶-۲، ۶-۳	m	بله	
SPR2	بیت اول پرچم سرآیند محافظت‌شده	۸-۲-۳-۳	m	بله	
SPR3	برچسب	۸-۲-۳-۴	m	بله	
SPR4	لت یکپارچگی	۸-۲-۳-۶	m	بله	
SPR5	ICV	۸-۲-۴	m	بله	
SPR6	لت رمزگذاری	۸-۲-۵	m	بله	

مقادیر مجاز پارامترهای TPDU صادر شده در جدول الف-۲۳ آورده شده است.

جدول الف-۲۳ – مقادیر پارامترهای TPDUهای صادر شده برای COTP، CLTP

شاخص	پارامتر	مقادیر	
		مجاز	پشتیبانی‌شده
AVI1	SA-ID	۲ تا ۱۲۶ هشت‌تایی‌ها	
AVI2	پرچم‌های سرآیند محافظت‌شده	۰ یا ۱	
	برچسب		
AVI3	مرجع تعریف	۱ تا n هشت‌تایی‌ها	
AVI4	مقدار	۱تا m هشت‌تایی‌ها	
	لت ICV		
AVI5	طول	۱-۲۵۴	
AVI6	مقدار	۱-۲۵۴ هشت‌تایی‌ها	
AVI7		indef-۱ ICV هشت‌تایی‌ها	
	ENC PADDING		
AVI8	طول	۱-۲۵۴	
AVI9	مقدار	۱-۲۵۴ هشت‌تایی‌ها	

الف-۷-۴ مقادیر مجاز پارامترهای TPDU صادر شده

به جدول الف-۲۴ مراجعه شود.

جدول الف-۲۴ – مقادیر برای پارامترهای TPDUهای دریافت‌شده برای COTP، CLTP

شاخص	پارامتر	مقادیر	
		مجاز	پشتیبانی شده
AVR1	SA-ID	۲-۱۲۶ هشت‌تایی‌ها	
AVR2	پرچم‌های سرآیند محافظت‌شده	۰ یا ۱	
	برچسب		
AVR3	مرجع تعریف‌شده	۱-n هشت‌تایی‌ها	
AVR4	مقدار	۱-m هشت‌تایی‌ها	
	لت‌گذاری ICV		
AVR5	طول	۱-۲۵۴	
AVR6	مقدار	۱-۲۵۴ هشت‌تایی‌ها	
AVR7	ICV	۱-indef هشت‌تایی‌ها	
	ENC PADDING		
AVR8	طول	۱-۲۵۴	
AVR9	مقدار	۱-۲۵۴ هشت‌تایی‌ها	

الف-۸ روابط خدمت، کارکرد و پروتکل

الف-۸-۱ رابطه‌ی بین خدمات و کارکردها

جدول الف-۲۵ یک نگاشت بین خدمات امنیتی OSI ارائه‌شده به‌وسیله TLSP و کارکردهای مرتبط مورد نیاز در یک پیاده‌سازی را نشان می‌دهد. سازگاری بین کارکردهای پشتیبانی‌شده و خدمات امنیتی باید طبق این جدول نگهداری شود.

جدول الف-۲۵ – نگاشت خدمات امنیتی به کارکردهای پشتیبانی‌شده

خدمت امنیتی	کارکردها
محرمانگی	لت‌گذاری رمزگذاری داده
یکپارچگی اتصال	فضای شماره دنباله‌ی یکپارچگی محافظت یکپارچگی لت‌گذاری تشخیص بازتاب
یکپارچگی بی‌اتصال	محافظت یکپارچگی لت‌گذاری تشخیص بازتاب
هستار همتا	تایید آدرس همتا
احراز هویت مبدأ داده	کپسوله‌سازی امنیتی استفاده از: محافظت یکپارچگی یا رمزگذاری داده
کنترل دسترسی	برچسب‌گذاری امنیتی صریح هم‌تافتگری امن کپسوله‌سازی امنیتی

الف-۸-۲ رابطه بین خدمات و پروتکل

جدول الف-۲۶ یک نگاشت بین خدمات امنیتی OSI ارائه شده به‌وسیله‌ی TLSP و اطلاعات کنترل پروتکل SE TPDU (PCI) و فیلدهای پارامتر به‌کارگرفته‌شده را به‌وسیله‌ی سازوکارهای امنیتی زیرین می‌دهد. سازگاری بین پارامترهای امنیتی پشتیبانی‌شده و فیلدهای پارامتر SE TPDU باید طبق این جدول ابقاء شود.

جدول الف-۲۶ – نگاشت خدمات امنیتی به پارامترهای SE TPDU

خدمت امنیتی	پارامترهای PCI/TPDU
محرمانگی	داده‌های رمزنگاری شده لت‌گذاری محرمانگی
یکپارچگی بی‌اتصال	مقدار وارسی یکپارچگی نشانگر جهت لت‌گذاری یکپارچگی
یکپارچگی اتصال	مقدار وارسی یکپارچگی نشانگر جهت لت‌گذاری یکپارچگی شماره دنباله ارسالی DT/ED (شماره دنباله نهایی)
احراز هویت مبدأ داده	آدرس همتا
احراز هویت هستار همتا	شناسه‌ی کلید شناسه‌ی کلید به‌کار رفته در مقدار وارسی یکپارچگی یا داده‌ی رمزنگاری شده
کنترل دسترسی	برچسب‌های امنیتی شناسه‌ی کلید شناسه کلید به‌کار رفته در مقدار وارسی یکپارچگی یا داده‌ی رمزنگاری شده

الف-۹ الگوریتم‌های پشتیبانی‌شده

جدول الف-۲۷ مجموعه الگوریتم‌های یکپارچگی و محرمانگی پشتیبانی‌شده به‌وسیله این پیاده‌سازی را مشخص می‌کند.

جدول الف-۲۷ – الگوریتم‌های پشتیبانی‌شده

شاخص	مورد	مرجع (زیربند)	شناسه‌ی الگوریتم*
ALG1	رمزنگاری داده	۶-۲-۳	
ALG2	رمزنگاشتی ICV	۶-۳-۱-۳	
ALG3	فاقد رمزنگاشتی ICV	۶-۳-۱-۳	
* الگوریتم‌های پشتیبانی‌شده تحت طرح ثبت تعریف‌شده در ISO/IEC 9979 یا ISO/IEC 9834.			

الف-۱۰ سامان‌دهی خطا

الف-۱۰-۱ خطاهای امنیتی

جدول الف-۲۸ حاوی اقدامات خطای امنیتی اجباری است که باید در هنگام دریافت یک SE TPDU متناظر با توصیف رویداد انجام شوند.

جدول الف-۲۸ - اقدامات خطای امنیتی اجباری برای COTP، CLTP

شاخص	رویداد	مرجع (زیربند)
SEA1	از یک TPDU دریافت‌شده که به شکل نامناسب محافظت‌شده است باید صرف نظر شود.	۶-۰
SEA2	از یک TPDU با مقدار نامعتبر شناسایی شده در SA-ID باید صرف نظر شود.	۶-۲-۳
SEA3	از یک TPDU با ICV نامعتبر باید صرف نظر شود.	۶-۳-۱-۳
SEA4	از یک TPDU با نشانگر جهت نامعتبر باید صرف نظر شود.	۶-۳-۲-۳
SEA5	از یک TPDU با برچسب نامناسب باید صرف نظر شود.	۶-۵-۳
SEA6	از یک TPDU با لت یکپارچگی نامناسب باید صرف نظر شود.	۶-۳-۱-۳
SEA7	از یک TPDU با شماره دنباله تکراری باید صرف نظر شود.	۶-۳-۳-۳
SEA8	از یک TPDU با آدرس همتای نامعتبر باید صرف نظر شود.	۶-۴
SEA9	از یک TPDU با یک لت رمزگذاری نامناسب باید صرف نظر شود.	۶-۲-۲
یادآوری ۱- در مورد SEA1، یک TPDU که به شکل مناسبی محافظت‌نشده است هم شامل SE TPDUهایی است که از گزینه‌های مذاکره‌نشده در آن‌ها استفاده شده و هم شامل آن‌هایی است که گزینه‌های مذاکره‌شده در آن‌ها استفاده نشده است. **یادآوری ۲**- مورد SEA7 تنها به پروتکل انتقال اتصال‌گرا (::COTP) (زمانی که فضای شماره دنباله‌ی یکپارچگی و محافظت کوتاه‌سازی برای C2-C4 و C4L مذاکره شده باشد) اعمال می‌شود.		

الف-۱۰-۲ خطاهای پروتکل

جدول الف-۲۹ اقدامات خطای پروتکل که به محض دریافت یک SE TPDU متناظر با توصیف رویداد انجام می‌گیرند را مشخص می‌کند.

جدول الف-۲۹ – اقدامات خطای پروتکل برای COTP، CLTP

شاخص	رویداد	مرجع (زیربند)	اقدام	
			مجاز	پشتیبانی‌شده
PEA1	یک پارامتر تعریف‌نشده که در محتوای محافظت‌شده رخ می‌دهد.	۸-۲-۳		
PEA2	پارامترهای خارج از دنباله که در محتوی محافظت‌شده کشف می‌شوند.	۸-۲-۳		

الف-۱۱ همبستگی امنیتی

الف-۱۱-۱ فیلدهای عمومی SA

به جدول الف-۳۰ مراجعه شود.

جدول الف-۳۰

مورد	سؤال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی در ارسال	پشتیبانی در دریافت
SaLI	فیلد شناسه‌ی طول ارسال‌شده در هر SA PDU؟	۸-۳-۱	SA:M	بله N/A	بله N/A
SaPDUType	فیلد نوع PDU با مقدار 01001001 در هر SA PDU	۸-۳-۲	SA:M	بله N/A	بله N/A
SaSAID	فیلد SA-ID	۸-۳-۳	SA:M	بله N/A	بله N/A
SA-PType	فیلدنوع SA-P TYPE	۸-۳-۴	SA:M	بله N/A	بله N/A
SA-RK	آیا از SA REKEY پشتیبانی می‌شود؟	ب-۵-۳	SA:O	بله خیر N/A	بله خیر N/A
SSLYR*	آیا از پروتکل SA نمونه که از تبادل نشانه‌ی کلید استفاده می‌کند، پشتیبانی می‌شود؟	پیوست ب	SA:O	بله خیر N/A	بله خیر N/A

الف-۱۱-۲ فیلدهای محتوای مشخص شده برای تبادل کلید SA-P

به جدول الف-۳۱ مراجعه شود.

جدول الف-۳۱

مورد	سؤال‌ها/ویژگی‌ها	مرجع(زیربند)	وضعیت	پشتیبانی در ارسال	پشتیبانی در دریافت
SAExchId	ExchangeID	ب-۶-۱	SAKTE:M	بله N/A	بله N/A
ContLen	آیا فیلد نشانگر طول در هر SA PDU ارسال می‌شود؟	ب-۶-۲	SAKTE:M	بله N/A	بله N/A
MySAID	فیلد محتوی My SAID	ب-۶-۳-۱	SAKTE:M	بله N/A	بله N/A
OldYrSAID	فیلد محتوی Old Your SAID	ب-۶-۳-۲	SAKTE:M	بله N/A	بله N/A
KeyTokens	فیلـدهای محتوی Key Token 1 و Key Token 2	ب-۶-۳-۳	SAKTE:M	بله N/A	بله N/A
AuthFields	امضای دیجیتالی احراز هویت و فیلدهای محتوی گواهی احراز هویت	ب-۶-۳-۴	SAKTE:M	بله N/A	بله N/A
ServSel	فیلد محتوی انتخاب خدمت	ب-۶-۳-۵	SAKTE:O	بله خیر	بله خیر

					N/A
SARejReas	فیلد محتوی دلیل ردشدن SA	ب-۶-۳-۶	SAKTE:O	بله خیر N/A	بله خیر N/A
SAAbReas	فیلد محتوی دلیل رهاسازی/صرف‌نظر SA	ب-۶-۳-۷	SAKTE: M	بله خیر N/A	بله خیر N/A
LabDef	فیلد محتوی تعریف برچسب	ب-۶-۳-۸	SAKTE:O	بله خیر N/A	بله خیر N/A
KeySel	فیلد محتوی انتخاب کلید	ب-۶-۳-۹	SAKTE:O	بله خیر N/A	بله خیر N/A
KeyUse	زیرفیلد پرچم‌های کاربرد	ب-۶-۳-۹	KeySel:M	بله خیر N/A	بله خیر N/A
KeySelInfo	زیرفیلد اطلاعات انتخاب کلید	ب-۶-۳-۹	KeySel:M	بله خیر N/A	بله خیر N/A
KeyRefx	زیرفیلد مرجع کلید	ب-۶-۳-۹	KeySel:O	بله خیر N/A	بله خیر N/A
SaFlags	فیلد محتوی پرچم‌های SA	ب-۶-۳-۱۰	SAKTE:O	بله خیر N/A	بله خیر N/A
ASSR	فیلد محتوی ASSR	ب-۶-۳-۱۱	ServSel:M	بله خیر N/A	بله خیر N/A

پیوست ب

(الزامی)

پروتکل همبستگی امنیتی با استفاده از تبادل نشانه‌ی کلید و امضاهای دیجیتالی

ب-۱ مرور کلی

این پیوست معرف یک پروتکل برای استفاده از سازوکاری نامتقارن جهت عملی ساختن برقراری، نگهداری و پایان‌دهی/ رهاسازی SA است. این پروتکل به هستارهای در حال ارتباط TSLP اجازه می‌دهد تا:

الف- اعتبار دو هستار را برای هم احراز هویت کنند.

ب- به صفات SA از جمله کلیدها مقدار اولیه بدهند؛ و

پ- اطلاعات اولیه را برای استفاده در ارائه یکپارچگی برقرار کنند.

این پیوست یک پروتکل SA را توصیف می‌کند که به‌طور منطقی عملکردهای مجزای زیر را انجام می‌دهد:

الف- تبادل نشانه‌ی کلید (KTE)، برای برقراری رمز مشترک مورد استفاده قرار می‌گیرد. این سازوکار از تبادل نشانه‌های کلید پشتیبانی می‌کند. قالب این نشانه‌ها به‌وسیله سازوکار مشخص می‌شود. نمونه‌ای از نشانه‌های کلید مشخص‌شده به‌وسیله سازوکار (که از تبادل کلیدهای نمایی پشتیبانی می‌کنند)، و تحت نام تبادل دیفی-هلمن[1] هم شناخته می‌شود، در پیوست پ آورده شده است.

ب- گواهی‌نامه‌ها، امضاهای دیجیتالی و عناصر KTE برای احراز هویت مورد استفاده قرار می‌گیرند.

پ- تبادلات پروتکل برای مذاکره در مورد صفات SA به‌کار برده می‌شوند.

ت- تبادلات پروتکل برای نشان‌دادن رهاسازی SA به‌کار برده می‌شوند.

پیش از برقرارسازی SA با استفاده از پروتکل SA هر کدام از هستارهای TLSP باید اطلاعات زیر را پیشاپیش فراهم کنند:

الف- سازوکارهایی که مورد پشتیبانی هستند و به شکل زیر بیان می‌شوند:

۱ - فهرستی از ASSRهای مورد پشتیبانی؛ و

۲ – مجموعه‌ی خدمات امنیتی پشتیبانی‌شده برای هر کدام از ASSRهای مشخص‌شده در بالا.

ب- یک زوج کلید نامتقارن برای هر کدام از الگوریتم‌های نامتقارن مورد پشتیبانی که می‌تواند به‌وسیله هستار TLSP برای ارائه امضاء داده در راستای احراز هویت به‌کار گرفته شود.

پ- گواهینامه‌ای از طرف یک مقام مورد اعتماد برای هر کدام از الگوریتم‌های نامتقارن مورد پشتیبانی که هویت هستار TLSP و کلید نامتقارن عمومی آن را برای اهداف احراز هویت مشخص می‌کند.

ت- کلیدهای عمومی و الگوریتم‌های نامتقارن ضمنی هر مقام تأییدکننده‌ی اعتبار مورد اعتمادی که گواهینامه‌ها را برای هستارهای TLSPای که هستار TLSP فعلی با آن در حال ارتباط است، صادر می‌کند.

1- Diffie-Hellman

این پروتکل SA، به‌طور پویا اطلاعات امنیتی زیر را که برای امن‌سازی ارتباط خود نیاز دارد، انجام می‌دهد:
الف- مذاکره در رابطه با الگوریتم رمزگذاری برای محافظت از ارتباط پروتکل SA.
ب– مذاکره در مورد الگوریتم نامتقارن و طرح امضای دیجیتالی مورد استفاده برای فراهم کردن احراز هویت پروتکل SA.
ج- تولید اطلاعات کلیدسازی مورد نیاز برای الگوریتم رمزگذاری به‌منظور محافظت از ارتباطات پروتکل SA.
این پروتکل SA اطلاعات به اشتراک گذاشته‌شده‌ی زیر را بین دو هستار TLSP برقرار می‌سازد:
الف- SA-IDهای محلی و راه دور.
ب- خدمات امنیتی که میان هستارهای مرتبط برای نمونه‌های ارتباط مورد استفاده قرار می‌گیرند.
پ- سازوکارها و پارامترهای آن‌ها که از طریق خدمت امنیتی انتخاب‌شده به‌صورت ضمنی بیان می‌شوند.
ت- کلیدهای اشتراکی اولیه برای یکپارچگی، سازوکارهای رمزگذاری و احراز هویت نمونه‌ی ارتباط
ث– مجموعه‌ی برچسب‌های امنیتی که ممکن است برای کنترل دسترسی این همبستگی مورد استفاده قرار بگیرند.
یک SA می‌تواند با استفاده از خدمات امنیتی انتخاب‌شده‌ی یکسان، سازوکارها و پارامترهای آن‌ها و مجموعه‌ی برچسب‌های امنیتی از SAای که از پیش برقرار شده بود، برقرار شود. در این مورد، فقط SA-ID و کلیدها تغییر می‌کنند و بقیه‌ی صفات همان‌طور باقی می‌مانند.
هر زمان که یک SA جدید برقرار می‌شود، مقادیر کلید جدید نیز باید برقرار شوند.
در مورد حالت TLSP بی‌اتصال، بعد از این که یک SA رها شد، SA-ID نباید دوباره مورد استفاده قرار گیرد.
در دوره‌ای که SA-ID بدون تغییر است باید از حداکثر طول عمر یک PDU در شبکه زیرین بیشتر باشد.
صفت SA adr-served با ابزاری خارج از این پروتکل برقرار می‌شود.
صفت آغازگر (Initiator) SA برای آغازگر تبادل پروتکل SA درست (true) و برای پاسخ‌دهنده، نادرست (false) تنظیم می‌شود.
تبادلات پروتکل برای برقرارسازی SA در شکل د-۱ نمایش داده شده است.

ب-۲ تبادل نشانه‌ی کلید (KTE)

هستارهای TLSP پروتکل SA خود را برای تولید یک رمز مشترک (به‌عنوان مثال یک رشته بیتی) بین هستارها، با یک KTE شروع می‌کنند. هستارهای TLSP سپس از یک زیرمجموعه از این رشته بیتی سری به همراه یک الگوریتم کلید خصوصی برای رمزگذاری ادامه‌ی ارتباطات میان آن‌ها استفاده می‌کنند، و به این ترتیب قابلیت محرمانگی را برای مابقی تبادلات پروتکل SA فراهم می‌کنند.
KTE شامل تبادل دو مقدار می‌شود: نشانه کلید ۱ و نشانه کلید ۲ که از پارامترهای مختص سازوکار و اعداد تولید شده‌ی محلی به‌وسیله الگوریتم‌های مختص سازوکار (مانند آن‌هایی که در پیوست د آورده شده‌اند) محاسبه می‌شوند. سپس مقادیر تبادل‌شده به‌وسیله‌ی هستارهای ارتباط برای تولید رشته بیت سری به اشتراک گذاشته شده استفاده می‌شوند.

زیرمجموعه‌ای از این رشته بیتی در کنار یک الگوریتم کلید خصوصی برای رمزگذاری مابقی تبادل پروتکل SA مورد استفاده قرار می‌گیرد و در عین حال از احراز هویت پروتکل SA و مذاکره‌ی صفت SA نیز پشتیبانی می‌شود. به‌علاوه، زیرمجموعه‌ای از این رشته بیتی نیز برای استفاده به‌عنوان کلید و صفات ISN همبستگی امنیتی در حال برقرار شدن، مورد ارجاع قرار می‌گیرد. این رشته بیتی به یکی از دو روش زیر مورد ارجاع قرار داده می‌شود:

۱- با تبادل اطلاعات موقعیت در مذاکره‌ی صفت SA؛ یا

۲- از طریق دانش استقرایی[1].

ب-۳ احراز هویت پروتکل SA

برای این‌که یک هستار TLSP بتواند اصالت هستار دیگر را در طی برقرارسازی SA تأیید کند، به یک گواهی احراز هویت و یک زوج کلید عمومی نیاز دارد.

هستارهای TLSP برای تصدیق هویت یکدیگر، گواهی‌نامه و امضای دیجیتالی (از قبیل آن‌هایی که در استاندارد ISO 9594-8 تعریف‌شده است) را تبادل می‌کنند. یک گواهی‌نامه حداقل حاوی اطلاعات شناسایی برای یک TLSPE به‌علاوه کلید عمومی هستار است (شکل د-۱ ملاحظه شود.).

گواهی‌نامه به‌وسیله یک مقام مورد اعتماد تأیید و با استفاده از رویه‌ای خارج از محدوده پروتکل TLSP، برای TLSP ارائه می‌شود. گواهی‌نامه شامل امضای احراز هویت مقام مورد اعتماد است. یک هستار TLSP که در این پروتکل SA شرکت می‌کند باید کلید عمومی مقام مورد اعتماد مرجع صدور گواهی‌نامه را داشته باشد. روش به‌کار رفته برای به‌دست آوردن کلید عمومی مقام مورد اعتماد خارج از محدوده‌ی این استاندارد ملی است. یک هستار TLSP برای این‌که نشان دهد که یک گواهی‌نامه خاص را دارا است، باید اثبات کند که کلید سری مرتبط با کلید عمومی گواهی‌نامه را دارد.

اثبات به‌هنگام‌بودن[2] و جلوگیری از حملات بازارسال، به‌وسیله‌ی داده‌های علامت‌گذاری شده‌ای صورت می‌گیرد که حاوی اعداد مشخصی هستند که به‌صورت مشترک تعیین شده و مختص عملکرد این پروتکل هستند. این امر مطابق رویه زیر برای دو هستار در حال ارتباط A (آغازگر SA) و B (پاسخ‌دهنده) انجام می‌گیرد:

الف- محتویات SA ساخته می‌شوند، این محتویات شامل فیلدهای کدبندی شده‌ی TLV:

A'Certificate،

مذاکره‌ی صفت SA (بند ب-۴ ملاحظه شود) یا دلایل پایان‌دهی/رهاسازی (بند ب-۶ مراجعه شود)، Key Token 3 که به‌وسیله‌ی یک الگوریتم (مانند آن‌چه که در پیوست د آورده شده است) محاسبه می‌شود،

و سپس (به جز ID تبادل و طول محتوا) امضاء می‌شوند (به‌عنوان مثال به‌وسیله‌ی امضای احراز هویت تعریف‌شده در ISO 9594-8). سپس محتویات SA، (که شامل امضاء نیز می‌شود و به‌عنوان یک TLV

1 - A priori knowledge

2 - Timeliness

کدبندی شده است) و طول محتوا رمزگذاری خواهند شد. کلید رمزگذاری، n بیت اول رشته بیتی تولیدشده به‌وسیله‌ی تبادل KTE است که n تعداد بیت‌های مورد نیاز در الگوریتم به‌کار رفته است.
ب- محتویات SA به‌وسیله‌ی اطلاعات معادل مرتبط با B و Key Token 4 به جای Key Token 3 ساخته، امضاء و رمزگذاری می‌شوند.
هر هستار امضای احراز هویت هستار همتا را به‌وسیله‌ی رمزگشایی تبادل دریافتی و تایید امضاء و وارسی نشانه‌ی کلید برای مقابله در برابر حمله‌ی بازارسال درستی‌سنجی می‌کند. درستی‌سنجی به به‌کارگیری کلید عمومی هستار و پردازش توافق‌شده برای ارزیابی امضاء، نیاز دارد.

ب-۴ مذاکره‌ی صفت SA

ب-۴-۱ مذاکره‌ی خدمت

هستار TLSP آغازگر، براساس خط‌مشی امنیتی خود ، مجموعه‌ای از یک یا چند انتخاب خدمت امنیتی مجاز را صادر می‌کند. هر عنصر در مجموعه حاوی موارد زیر است:
الف- ASSR_ID که معناشناسی خدمات امنیتی انتخاب‌شده (که در زیر فهرست شده است) برای این عنصر در مجموعه را تعریف می‌کند؛ و
ب- مقادیر انتخاب خدمت (معناشناسی تعریف‌شده به‌وسیله ASSR_ID) برای: محرمانگی، احراز هویت، کنترل دسترسی، یکپارچگی و محرمانگی جریان ترافیک.
هستار TLSP دریافت‌کننده براساس خط‌مشی امنیتی محلی، PCI زیر را به آغازگر برمی‌گرداند:
الف- اگر خدمتی از مجموعه خدمات پیشنهادشده مورد قبول باشد، دریافت‌کننده عنصر تک خدمت انتخاب‌شده را بازمی‌گرداند.
ب- اگر هیچ یک از خدمات مجموعه خدمات پیشنهادشده مورد قبول نباشند، دریافت‌کننده SA را با بازگرداندن وضعیتی که دلیل پذیرفته نشدن SA را نشان می‌دهد، رد می‌کند.

یادآوری– این مذاکره به هر دو هستار TLSP اجازه می‌دهد، خدمات امنیتی که با خط‌مشی امنیتی محلی آن سازگار است را انتخاب کنند.

ب-۴-۲ مذاکره‌ی مجموعه برچسب

هستار TLSP آغازگر، براساس خط‌مشی امنیتی محلی، یک مجموعه از برچسب‌های امنیتی و مراجعی که می‌خواهد تحت محافظت این SA انتقال داده شود را صادر می‌کند. هر عنصر در مجموعه حاوی معناشناسی کامل برچسب است.
هستار TLSP دریافت‌کننده، براساس خط‌مشی امنیتی محلی مجموعه برچسب‌های پیشنهادی را که می‌خواهد تحت محافظت این SA انتقال داده شود، تعیین می‌کند. هستار TLSP دریافت‌کننده، PCI زیر را به آغازگر برمی‌گرداند:
الف- اگر یک یا تعداد بیشتری برچسب از مجموعه پیشنهادی قابل قبول باشد، دریافت‌کننده یک زیرمجموعه از مجموعه پیشنهادی مراجع را برمی‌گرداند.

ب- اگر هیچ برچسبی در مجموعه پیشنهادی قابل قبول نباشد، دریافت‌کننده SA را رد کرده و یک وضعیت نشان‌دهنده‌ی دلیل رد شدن SA را بازمی‌گرداند.

یادآوری– این مذاکره به دو هستار TLSP اجازه می‌دهد یک مجموعه برچسب را که با خط‌مشی امنیتی محلی آن سازگار است انتخاب کنند. البته این موضوع تنها در مواردی کاربرد دارد که صفت برچسب انتخاب شده باشد.

ب-۴-۳ انتخاب ISN و کلید

هستار TLSP آغازگر، براساس خط‌مشی امنیتی محلی، قسمت‌هایی از رشته بیتی حاصله از KTP را برای استفاده به‌عنوان کلیدها و/ یا ISNها در طی ارتباطات (ارتباطات TLSP و نه ارتباطات پروتکل SA) با هستار دریافت‌کننده‌ی TLSP انتخاب می‌کند. کلید/ISN با تبادل موقعیت بیت آغازین در رشته بیتی حاصله از KTE مشخص می‌شود. طول کلید/ISN با استفاده از پارامترهای مرتبط با خدمت انتخابی مشخص می‌شود.
یک مجموعه اشاره‌گر برای موارد زیر به هستار TLSP دریافت‌کننده ارسال می‌شود:

الف- کلید رمزگذاری داده‌ی عادی؛

ب- کلید رمزگذاری داده‌ی پیشتاز؛

پ- کلید تولید وارسی یکپارچگی داده‌ی عادی؛

ت- کلید تولید وارسی یکپارچگی داده‌ی پیشتاز؛

ث- My ISN برای داده‌ی عادی؛

ج- My ISN برای داده‌ی پیشتاز؛ و

چ- کلید تولید احراز هویت.

به‌طور مشابه، هستار TLSP دریافت‌کننده از طریق خط‌مشی امنیتی محلی خود مشخص می‌کند که کدام‌یک از بخش‌های رشته بیتی حاصله از KTE را برای کلیدها/ISNها استفاده خواهد کرد. هستار TLSP دریافت‌کننده PCI زیر را به آغازگر برمی‌گرداند:

الف- اگر دریافت‌کننده همان موقعیت بیت پیشنهاد شده به‌وسیله‌ی آغازگر را انتخاب کند هیچ PCI صریحی برگشت داده نمی‌شود.

ب- اگر دریافت‌کننده SA را به‌دلیل سایر شکست‌های مذاکره رد کند، هیچ PCI صریحی برگشت داده نمی‌شود.

پ- اگر دریافت‌کننده موقعیت‌های بیتی متفاوت را برای کلید/ISNهایش انتخاب کند، یک مجموعه اشاره‌گر را برگشت خواهد داد.

یادآوری– یک مقدار کلید یکسان می‌تواند جهت اهداف متعددی با استفاده از ارائه اشاره‌گر یکسان برای بیشتر از یک کلید/ISN به‌کار رود.

ب-۴-۴ انواع گوناگون مذاکره صفت SA

هستار TLSP آغازگر، براساس خط‌مشی امنیتی محلی، مقدار صفات SA زیر را برای برقراری SA تعیین می‌کند، مانند حفظ کردن این صفات SA در صورت قطع اتصال (ITU-T X.224 | ISO/IEC 8073 انتخاب شده است.)

هستار TLSP آغازگر، این مجموعه صفات SA پیشنهادی را در قالب فیلد پرچم‌های گوناگون به هستار TLSP دریافت‌کننده ارسال می‌کند.

دریافت‌کننده‌ی TLSP براساس خط‌مشی امنیتی خود، PCI زیر را به آغازگر برمی‌گرداند:

الف- اگر دریافت‌کننده همه‌ی صفات SA پیشنهادی را بپذیرد، هیچ PCI صریحی برگشت داده نمی‌شود. اگر دریافت‌کننده SA را رد نکند، دلالت بر این دارد که صفات SA برای هستار TLSP دریافتی قابل قبول هستند.

ب- اگر هر یک از صفات قابل قبول نباشند، دریافت‌کننده SA را نمی‌پذیرد و وضعیتی را برمی‌گرداند که نشان‌دهنده‌ی صفاتی است که سبب رد شدن SA شده‌اند.

ب-۴-۵ مرور کلی کلیددهی مجدد

اگر یک SA برای کلیددهی مجدد یک SA قدیمی در حال برقرار شدن است، آنگاه فقط انتخاب کلید و ISN انجام می‌شود. به‌جای مذاکره‌ی خدمت، مجموعه برچسب و انواع گوناگون صفت SA، ارجاع به SA قدیمی که این صفات از آن به ارث رسیده‌اند در Old_Your_SA-ID قرار داده می‌شود.

ب-۴-۶ مرور کلی پایان‌دهی/رهاسازی SA

یک همبستگی امنیتی به‌وسیله‌ی روش‌های زیر رهاسازی می‌شود:

الف- از طریق تبادل واحدهای داده پروتکل همبستگی امنیتی؛

ب- استفاده از سازوکارهای خارج ازمحدوده‌ی پروتکل لایه پایین‌تر؛

پ- به‌صورت ضمنی با بستن یک اتصال؛

ت- به‌صورت ضمنی زمانی که کلیدی در SA منقضی می‌شود.

روش‌های رهاسازی همبستگی امنیتی به دو دسته تقسیم می‌شوند، روش‌های داخلی و روش‌های خارجی. در مورد روش داخلی ممکن است رهاسازی SA به‌وسیله‌ی درخواست قطع اتصال انتقال یا صادر کردن رهاسازی SA انجام شود (SA PDU با یک نوع فیلد محتوی دلیل پایان‌دهی/رهاسازی SA. برای جزئیات بیشتر به زیربند ب-۶-۳ مراجعه شود).

ب-۵ نگاشت عملکردهای پروتکل SA به تبادلات پروتکل

این پروتکل SA سه عملکرد توصیف‌شده در بالا را در طی دو تبادل پروتکل مجزا اجرا می‌کند:

الف- اولین تبادل شامل KTE و تبادل گواهی‌نامه است و هیچ رمزگذاری در آن استفاده نمی‌شود؛

ب- دومین تبادل شامل یک مذاکره امنیتی محافظت‌شده برای ارائه احراز هویت تعریف‌شده در بند ب-۳ است؛

پ- یک تبادل جداگانه زمانی آغاز می‌شود که دیگر SA نیاز نیست و شامل کد دلیل محافظت‌شده برای ارائه احراز هویت تعریف‌شده در بند ب-۳ است.

ب-۵-۱ (اولین) تبادل KTE

ب-۵-۱-۱ درخواست برای آغاز پروتکل SA

هستار TLSP یا مدیریت امنیت محلی، پروتکل SA را آغاز می‌کنند.

هستار TLSP آغازگر، عملکردهای زیر را انجام می‌دهد و اطلاعات زیر را به دریافت‌کننده ارسال می‌کند:

الف- یک SA-ID موجود انتخاب می‌شود و به‌عنوان My_SA-ID آغازگر ارسال می‌شود.

ب- KTE آغاز شده و Key Token 1 فرستاده می‌شود.

پ- یک فهرست از سازوکارهای محرمانگی پیشنهادی که می‌توانند برای محافظت از تبادل دومین پروتکل SA استفاده شود. این فهرست به‌صورت یک مجموعه از یک یا چند عنصر که شامل ASSR_ID و خدمت امنیتی محرمانگی انتخاب‌شده است، بیان می‌شود. در صورتی که سازوکار از پیش توافق شده باشد نیاز نیست که این فهرست ارسال شود.

ت- یک فهرست از سازوکارهای یکپارچگی پیشنهادی که یکی از آن‌ها برای امضای دیجیتالی دومین تبادل پروتکل SA به‌کار می‌رود. این فهرست به‌صورت مجموعه‌ای از یک یا چند عنصر که شامل ASSR_ID و خدمات امنیتی یکپارچگی انتخاب‌شده هستند، بیان می‌شود. در صورتی که سازوکار از پیش توافق شده باشد نیاز نیست که این فهرست ارسال شود.

یادآوری– خدمات امنیتی محرمانگی انتخاب‌شده باید تنها یک الگوریتم رمزگذاری متقارن و حالت کاری آن را شناسایی کنند. خدمات امنیتی یکپارچگی انتخاب‌شده باید تنها یک الگوریتم نامتقارن و طرح امضای دیجیتالی مربوطه‌ی آن را شناسایی کنند. موارد پ و ت ممکن است به صورت استنتاجی شناخته شوند.

در مورد CO، اگر هیچ PDU برای اولین تبادل پس از گذشت یک مهلت زمانی بازنگردد، SA برقرار نمی‌شود و تلاش بیشتری نیز انجام نخواهد گرفت.

در مورد CL، اگر هیچ PDU برای اولین تبادل پس از گذشت یک مهلت زمانی بازنگردد، TLSP آغازگر دوباره اولین PDU تبادل خود را ارسال می‌کند. تعداد ارسال‌های مجدد به تعداد متناهی تعریف‌شده به‌صورت محلی محدود شده است.

ب-۵-۱-۲ دریافت اولین PDU تبادل به‌وسیله دریافت‌کننده

به‌محض دریافت اولین PDU تبادل، هستار TLSP دریافت‌کننده عملکردهای زیر را انجام می‌دهد و اطلاعات زیر را به آغازگر می‌فرستد:

الف- My_SAID دریافتی در فیلد Your-SAID سرآیند عمومی قرار داده می‌شود (همان‌گونه‌که در زیربند ۸-۳ توضیح داده شد).

ب- یک SAID موجود انتخاب شده و به‌عنوان My_SAID آغازگر ارسال می‌شود.

پ- هستار TLSP دریافت‌کننده براساس خط‌مشی امنیتی محلی خود، PCI زیر را به آغازگر برمی‌گرداند:

۱- اگر دریافت‌کننده یکی از سازوکارهای محرمانگی پیشنهادی را بپذیرد، سازوکار انتخاب‌شده را برمی‌گرداند. اگر آغازگر یک سازوکار را پیشنهاد داده باشد هیچ PCI صریحی برگشت داده نمی‌شود.
۲- اگر هیچ‌یک از سازوکارهای محرمانگی قابل قبول نباشند، دریافت‌کننده SA را نمی‌پذیرد و دلیل رد شدن را برمی‌گرداند.
ت- اگر هم سازوکار محرمانگی و هم یکپارچگی انتخاب شده باشند، محاسبه‌ی KTE آغاز شده و Key Token 2 ارسال می‌شود.
در مورد CO، اگر هیچ PDUای از دومین تبادل، پس از گذشت یک مهلت زمانی برنگردد، SA برقرار نشده و هیچ تلاش بیشتری صورت نمی‌پذیرد.
در مورد CL، اگر هیچ PDUای از دومین تبادل، پس از گذشت یک مهلت زمانی برنگردد، هستار TLSP آغازگر، دوباره اولین PDU تبادل خود را ارسال می‌کند. تعداد ارسال‌های مجدد به یک تعداد متناهی که به‌صورت محلی تعریف‌شده، محدود شده است.
در مورد CL، اگر PDU از اولین تبادل دوباره دریافت شود، PUD بازگشتی دوباره ارسال می‌شود.

ب-۵-۲ احراز هویت و مذاکره‌ی امنیتی (دومین) تبادل

ب-۵-۲-۱ دریافت اولین PDU تبادل به‌وسیله آغازگر

به‌محض دریافت اولین SA PDU تبادل، هستار TLSP آغازگر عملکردهای زیر را انجام می‌دهد و اطلاعات زیر را به دریافت‌کننده می‌فرستد:
الف- MY_SAID دریافتی در فیلد Your_SAID سرآیند عمومی قرار می‌گیرد. (همان‌طورکه در زیربند ۸-۲ توضیح داده شد.)
ب- گواهی‌نامه آغازگر مربوط به سازوکار یکپارچگی انتخاب‌شده در گواهی فیلد محتوی قرار داده می‌شود.
پ- آغازگر، Key Token 3 را تولید می‌کند.
ت- یک فهرست از خدمات امنیتی پیشنهادی که می‌تواند برای محافظت ارتباط TLSP به‌کار رود در فیلد محتوی انتخاب خدمت قرار داده می‌شود.
ث- یک مجموعه از برچسب‌های پیشنهادی که می‌توانند به‌وسیله‌ی SA در طی ارتباط TLSP محافظت شوند در Label_Def قرار داده می‌شوند.
ج- یک مجموعه از اشاره‌گرهای کلید/ISN در انتخاب کلید قرار داده می‌شوند.
چ- انواع گوناگون صفات SA برای این SA در پرچم‌های SA قرار داده می‌شوند.
ح- اگر برقرارسازی SA، یک SA قدیمی را کلیددهی مجدد کند آنگاه Old Your SA-ID به SA SA-ID قدیمی تنظیم می‌شود. اگر این رویه انجام پذیرد موارد ت، ث و چ نباید اجرا شوند.
خ- محتویات SA همان‌طورکه در بند ب-۳ توضیح داده شد محافظت شوند.
در مورد CO، اگر هیچ PDUای از دومین تبادل، پس از گذشت یک مهلت زمانی برنگردد، SA برقرار نشده و هیچ تلاش بیشتری صورت نمی‌پذیرد. در مورد CL، اگر هیچ PDUای از دومین تبادل، پس از گذشت یک

مهلت زمانی برنگردد، هستار TLSP آغازگر، دوباره دومین PDU تبادل خود را ارسال می‌کند. تعداد ارسال‌های مجدد به تعداد متناهی تعریف‌شده به‌صورت محلی محدود شده است.
در مورد CL، اگر PDU از اولین تبادل دوباره دریافت شود، PUD تبادل دوم دوباره فرستاده می‌شود.

ب-۵-۲-۲ دریافت دومین PDU تبادل به‌وسیله دریافت‌کننده

به‌محض دریافت دومین PDU تبادل، هستار TLSP دریافت‌کننده عملکردهای زیر را انجام می‌دهد و اطلاعات زیر را به آغازگر می‌فرستد:
الف- MY_SAID دریافتی در فیلد Your_SAID سرآیند عمومی همان‌طورکه در زیربند ۸-۳ توصیف شده است، قرار می‌گیرد.
ب- موارد زیر بررسی می‌شوند. اگر بررسی یکی از موردها با شکست مواجه شود، آنگاه SA رد شده و دلیل رد شدن SA برگردانده می‌شود:
۱- اعتبار امضای دیجیتالی دریافتی بررسی می‌شود.
۲- اعتبار Key Token 3 دریافتی بررسی می‌شود.
۳- مجموعه خدمات امنیتی پیشنهادی بررسی می‌شوند تا مشخص شود که آیا موردی قابل پذیرش است یا خیر. تنها یکی از خدمات امنیتی پیشنهادی می‌تواند انتخاب شود.
۴- مجموعه برچسب‌های پیشنهادی بررسی می‌شوند تا مشخص شود که آیا موردی قابل قبول است یا خیر.
۵– انواع گوناگون صفات SA بررسی می‌شوند تا مشخص شود که آیا همه‌ی آن‌ها مورد قبول هستند یا خیر.
پ- اگر Old Your SA-ID در PDU دریافتی باشد، آنگاه SA مناسب از SA-ID مرجع رونوشت می‌شود. در این مورد فیلدهای استفاده‌شده که در پ و ث در زیر توصیف شده‌اند نمی‌توانند ارسال شوند.
در صورتی که همه بررسی‌ها موفقیت‌آمیز باشند ، موارد زیر ارسال می‌شوند:
الف- گواهی‌نامه آغازگر مربوط به سازوکار یکپارچگی انتخابی ارسال می‌شود.
ب- خدمات امنیتی انتخابی مورد استفاده برای محافظت از ارتباطات TLSP، ارسال می‌شوند. اگر مجموعه‌ی خدمات پیشنهادی حاوی یک عنصر باشند هیچ PCIای برگشت داده نمی‌شود.
پ- دریافت‌کننده Key Token 4 را تولید می‌کند.
ت- زیرمجموعه انتخابی از برچسب‌های پیشنهادی که با استفاده از این SA می‌توانند در طی ارتباط TLSP محافظت شوند، ارسال می‌شوند.
ث- یک مجموعه از اشاره‌گرهای کلید/ISN ارسال می‌شود. اگر اشاره‌گرهای آغازگر برای دریافت‌کننده قابل قبول باشند، هیچ PCIای فرستاده نمی‌شود.
ج- همان‌طورکه در بند ب-۳ توضیح داده شد، از محتویات SA محافظت شود.
در مورد CL، اگر PDU دومین تبادل دوباره دریافت شود، دریافت‌کننده، PDU تبادل دوم خود را دوباره ارسال می‌کند.

ب-۵-۳ رویه کلیددهی مجدد

هستارهای TLSP ممکن است کلیدها را در هر زمانی طی همبستگی امنیتی به‌روزرسانی کنند. این امر از طریق تبادل SCI انجام می‌پذیرد. این تبادل از دید کاربر TLSP سری است و هیچ خدمت TLSP برای به‌کارگیری آن تعریف نشده است.

یک حالت ممکن از عملیات، تبادل SCI در بازه‌های زمانی منظم است (به‌عنوان مثال هر ساعت یا هر ۱۰۰۰۰ SE-TPDU). کلیددهی مجدد باعث می‌شود یک SA-ID جدید انتخاب شود ؛ با این وجود صفات SA جاری می‌توانند به ارث برده شوند.

اطلاعات کلیددهی مجدد می‌تواند شامل یکی از موارد زیر باشد:

الف- یک کلید رمزگذاری جدید با KEK دوطرفه؛

ب- یک کلید جدید که با کلید عمومی دریافت‌کننده رمزگذاری شده است؛

پ- یک مرجع به کلید توزیع‌شده قبلی؛

ت- اطلاعات کلیددهی مجدد که به‌وسیله یک روش توزیع کلید از پیش توافق شده، استفاده می‌شود.

رویه‌های کلیددهی مجدد براساس تبادل دو SA PDU با اطلاعات کلیددهی مجدد (که به سمت بیرون و پاسخ نامیده می‌شود) و SE-TPDUهای عادی به شکل زیر است:

یک SA PDU حاوی اطلاعات کلیددهی مجدد به سمت بیرون با موارد زیر آماده می‌شود:

الف- پرچم به سمت بیرون/ پاسخ در هشت‌تایی پرچم به صفر تنظیم می‌شود.

ب- اگر سازوکار برچسب انتخاب شود آنگاه Label-Ref به مرجع برچسب مناسب تنظیم می‌شود.

پ- اطلاعات کلید به‌محض نیاز به‌وسیله‌ی سازوکار توزیع کلید تنظیم می‌شوند.

ت- ISN اولیه‌ی محافظت‌شده، شماره دنباله‌ی SE TPDUای که باید به‌وسیله‌ی کلید به‌روزرسانی‌شده رمز شود را تنظیم می‌کند.

ث- فیلد SA Flag Rekey سه، به ۱ تنظیم می‌شود.

به‌محض دریافت یک SA TPD حاوی اطلاعات کلیددهی مجدد به سمت بیرون:

الف- اگر سازوکار برچسب انتخاب شده باشد، آنگاه بررسی می‌شود که فیلد label-ref یک مقدار مجاز برای این SA داشته باشد.

ب - در صورت نیاز اطلاعات کلید به‌وسیله‌ی سازوکار توزیع کلید، پردازش می‌شوند.

پ- بررسی شود که ISN اولیه مناسب است یا خیر.

ت- فیلد Check Flag Rekey سه، به۱ تنظیم شود.

آنگاه یک SA PDU حاوی اطلاعات کلیددهی مجدد پاسخ با موارد زیر آماده می‌شود:

الف- پرچم به سمت بیرون/ پاسخ از پرچم هشت‌تایی، به ۱ تنظیم می‌شود.

ب- اگر سازوکار برچسب انتخاب شده باشد آنگاه Label-Ref به مرجع برچسب مناسب تنظیم می‌شود.

پ- اطلاعات کلید در موقع نیاز به‌وسیله‌ی سازوکار توزیع کلید تنظیم می‌شود.

ت- ISN اولیه‌ی محافظت‌شده، شماره دنباله‌ی SE TPDUای که باید به‌وسیله‌ی کلید به‌روزرسانی‌شده رمز شود را تنظیم می‌کند.

ث- فیلد SA Flag Rekey سه، به ۱ تنظیم می‌شود.
به‌محض دریافت یک SA TPD حاوی اطلاعات کلیددهی مجدد پاسخ:
الف- اگر سازوکار برچسب انتخاب شده باشد، آنگاه بررسی می‌شود که فیلد label-ref یک مقدار مجاز برای این SA داشته باشد.
ب- در صورت نیاز اطلاعات کلید به‌وسیله‌ی سازوکار توزیع کلید، پردازش می‌شوند.
پ- بررسی شود که ISN اولیه مناسب است یا خیر.
ت- فیلد Check Flag Rekey سه، به ۱ تنظیم شود.
بعد از بررسی موفقیت‌آمیز پاسخ اگر هستار TLSP هیچ TPDU منتظر کپسوله‌سازی نداشته باشد، یک SA PDU خالی از داده برای تکمیل رویه کلیددهی مجدد، ارسال می‌شود.
زمانی که یک هستار TLSP یک SE-TPDU حاوی اطلاعات کلیددهی مجدد به سمت بیرون را ارسال می‌کند، یک SE-TPDU کپسوله‌شده را با استفاده از کلید قبلی دریافت می‌کند، هستار TLSP نباید از SE-TPDU کلید قبلی صرف‌نظر کند، مگر اینکه خط‌مشی امنیتی تعیین کند که از این SE-TPDUها باید صرف نظر شود.
اگر رویه کلیددهی مجدد با شکست روبه‌رو شود، آنگاه همبستگی یا با به‌کارگیری SA-P یا با یک ابزار مناسب دیگر، دوباره برقرار می‌شود.

ب-۵-۴ تبادل پایان‌دهی/رهاسازی SA

ب-۵-۴-۱ درخواست برای آغاز رهاسازی/پایان‌دهی SA

هستار TLSP یا مدیریت امنیت محلی ، رهاسازی/پایان‌دهی SA را شروع می‌کنند. نیازی نیست که آغازگر یک رهاسازی/پایان‌دهی SA همان آغازگر برقرارسازی SA باشد.
الف- اگر هستار محلی آغازگر برقرارسازی SA باشد، آنگاه Key Token 3 تولید می‌شود در غیر این‌صورت Key Token 4 تولید می‌شود. در هر دو مورد، نشانه‌ی تولیدشده در محتوی SA قرار داده می‌شود.
ب- کد دلیل مناسب در فیلد دلیل رهاسازی/پایان‌دهی محتوی SA قرار داده می‌شود.
پ- از محتوی SA همان‌طورکه در بند ب-۳ توصیف شده است محافظت شود.
در مورد CO، اگر یک PDU تصدیق از درخواست رهاسازی/پایان‌دهی بعد از یک مهلت زمانی بازنگردد، SA برقرار نشده و هیچ تلاش دیگری صورت نمی‌گیرد.
در مورد CL، اگر یک PDU از تبادل رهاسازی/پایان‌دهی بعد از یک مهلت زمانی بازنگردد، هستار TLSP آغازگر، PDU درخواست رهاسازی/پایان‌دهی SA خودش را دوباره ارسال می‌کند. ارسال‌های مجدد به یک تعداد متناهی تعریف‌شده به‌صورت محلی، محدود شده است.

ب-۵-۴-۲ دریافت درخواست‌های رهاسازی/پایان‌دهی SA

به‌محض دریافت PDU تصدیق رهاسازی/ پایان‌دهی SA، هستار TLSP دریافت‌کننده عملکردهای زیر را انجام خواهد داد و اطلاعات زیر را به آغازگر ارسال می‌کند:

الف- اگر هستار محلی آغازگر برقرارسازی SA باشد، آنگاه Key Token 3 تولید می‌شود در غیر این‌صورت Key Token 4 تولید می‌شود. در هر دو حالت نشانه‌ی تولیدشده در محتوی SA قرار داده می‌شود.
ب- کد دلیل مناسب در فیلد دلیل رهاسازی/پایان‌دهی محتوی SA قرار داده می‌شود.
پ- از محتوی SA همان‌طورکه در بند ب-۳ توصیف شده است محافظت شود.
در مورد CL، اگر PDU از درخواست رهاسازی/ پایان‌دهی دوباره دریافت شود، دریافت‌کننده دومین PDU تبادل خودش را به تعداد محدود مفروض مجدداً ارسال می‌کند.

ب-۶ SA PDU – محتویات SA

برای یک پروتکل SA خاص، قالب فیلد محتویات SA از SA PDU تعریف‌شده در زیربند ۸-۴ در شکل ب-۲ نمایش داده شده است.

Exchange Id	Content Length	Content Field	Content . . . . Field
1	2	var	var

شکل ب-۲ – محتویات SA

ب-۶-۱ ID تبادل

اگر PDU مربوط به اولین تبادل KTE باشد این فیلد مقدار 00000000 را خواهد داشت و اگر PDU مربوط به دومین تبادل مذاکره/احراز هویت باشد، مقدار 00000001 را خواهد داشت. اگر PDU مربوط به درخواست رهاسازی/پایان‌دهی SA باشد مقدار، 10000000 و اگر PDU مربوط به تصدیق رهاسازی/ پایان‌دهی SA باشد، مقدار 10000001 را خواهد داشت.

ب-۶-۲ طول محتوا

طول هشت‌تایی‌ها در همه‌ی فیلدهای محتوا (به‌غیر از فیلد طول محتوا).

ب-۶-۳ فیلدهای محتوی

کدبندی نوع فیلد محتوا در زیربند ۸-۲ تعریف‌شده است. فیلدهای محتوای SA (یعنی 00-BF) که به‌وسیله‌ی رویه‌های این پیوست استفاده می‌شوند، در زیر آمده‌اند:

نوع فیلد محتوی	مقدار
MY SA-ID	A0
Old Your SA-ID	A1
Key Token 1	A2
Key Token 2	A3
امضای دیجیتالی احراز هویت	A4

گواهی‌نامه احراز هویت	A5
انتخاب خدمت	A6
دلیل رد شدن SA	A7
دلیل رهاسازی/پایان‌دهی SA	A8
پرچم‌های SA	A9
انتخاب کلید	AA
ASSR	AB
آغازگر	AC
الگوریتم یکپارچگی	AD
الگوریتم محرمانگی	AE
طول ICV	AF
کلید رمزگذاری	B1
کلید رمزگشایی	B2
سازوکار احراز هویت	B3
سازوکار کنترل دسترسی	B4
Key Token 3	B5
Key Token 4	B6
ذخیره‌شده برای استفاده آینده	B7-BF

یادآوری– کدهای بیشتر برای استفاده خصوصی در زیربند ۸-۲ در متن اصلی این استاندارد ملی رزرو[1] شده‌اند.

انتخاب خدمت، دلیل رد شدن SA، Label-Def، پرچم‌های SA و فیلدهای انتخاب کلید در این تعریف محتوی پروتکل SA، اختیاری هستند.

1 - Reserve

ب-۶-۳-۱ My SA-ID

این فیلد اجباری تنها در اولین تبادل مورد استفاده قرار می‌گیرد. این پارامتر شناسه‌ی محلی برای یک همبستگی امنیتی است.

ب-۶-۳-۲ Old Your SA-ID

اگر صفت‌هایی (غیر از کلیدها) قرار باشد از SA قدیمی به ارث برده شوند، این فیلد در دومین تبادل مورد استفاده قرار می‌گیرد.

ب-۶-۳-۳ Key Token 1، Key Token 2، Key Token 3 و Key Token 4

این فیلدهای اجباری همان‌طورکه پیش‌تر در این پیوست توضیح داده شد، برای پشتیبانی KTE مورد استفاده قرار می‌گیرند.

ب-۶-۳-۴ احراز هویت امضای دیجیتالی، گواهینامه

این فیلدهای اجباری برای پشتیبانی از احراز هویت همان‌طورکه پیش‌تر در این پیوست شرح داده شده است به‌کار می‌روند.

ب-۶-۳-۵ انتخاب خدمت

این فیلد اختیاری برای اولین و دومین تبادل، مورد استفاده قرار می‌گیرد:

الف- اگر در طی اولین تبادل مورد استفاده قرار گیرد، جهت تشخیص سازوکارهای محرمانگی و/یا یکپارچگی پیشنهادی برای دومین تبادل پروتکل SA به‌کار می‌رود. در این مورد، تنها دو هشت‌تایی اول ارائه می‌شوند.

ب- اگر در طی دومین تبادل مورد استفاده قرار گیرد، جهت پیشنهاد همه‌ی سازوکارها برای استفاده در طی ارتباطات TLSP محافظت‌شده به‌وسیله‌ی SAای که در حال برقرار شدن است، به‌کار می‌رود.

این فیلد ممکن است یک یا چند بار در تبادل اول یا دوم PDU برای تشکیل یک مجموعه پیشنهادی از خدمات امنیتی جهت مذاکره، حضور داشته باشد.

این پارامتر حاوی یک دنباله از هشت‌تایی‌ها است که سطوح خدمات امنیتی انتخاب‌شده را نشان می‌دهند. معناشناسی سطوح به‌عنوان بخشی از خط‌مشی امنیتی تعریف شده است. هشت‌تایی‌ها برای هر یک از خدمات امنیتی به ترتیب مشخص‌شده در زیر، ظاهر می‌شوند. اگر هشت‌تایی‌های کوتاه‌سازی‌شده همگی مربوط به خدماتی باشند که مقدار QOS آن‌ها صفر است، آنگاه دنباله‌ی هشت‌تایی‌ها می‌تواند کوتاه شوند. یک تک هشت‌تایی با مقدار ۲۵۵ مشخص می‌کند که خدمات امنیتی انتخابی از قبل برقرار شده‌اند.

هشت‌تایی	معنی
۱	محرمانگی بی‌اتصال/ محرمانگی اتصال
۲	یکپارچگی بی‌اتصال/ یکپارچگی اتصال با یا بدون بازیافت
۳	احراز هویت مبدأ داده/ احراز هویت هستار همتا
۴	کنترل دسترسی
۵	محافظت سامانه پایانی

۶	محافظت به ازای هر اتصال

ب-۶-۳-۶ دلیل رد شدن SA

این فیلد اختیاری ممکن است در اولین یا دومین PDU تبادل حاضر باشد. این فیلد برای نشان دادن ردشدن یک SA در طی برقرارسازی آن، ارائه می‌شود. این فیلد حاوی دلیل رد شدن به‌صورت زیر است:

مقدار	معنی
۱	سازوکار محرمانگی پشتیبانی نمی‌شود.
۲	سازوکار یکپارچگی پشتیبانی نمی‌شود.
۳	سازوکار کنترل دسترسی پشتیبانی نمی‌شود.
۴	سازوکار احراز هویت پشتیبانی نمی‌شود.
۵	سامانه پایانی پشتیبانی نمی‌شود.
۶	به ازای هر اتصال پشتیبانی نمی‌شود.
۷	سازوکار محرمانگی رد شده است.
۸	سازوکار یکپارچگی رد شده است.
۹	سازوکار کنترل دسترسی رد شده است.
۱۰	سازوکار احراز هویت رد شده است.
۱۱	امضای احراز هویت نامعتبر است.
۱۲	گواهی‌نامه نامعتبر است.
۱۳	مجموعه برچسب پیشنهادی رد شده است.
۱۴	Retain_on_Disconnect رد شده است.
۱۵	Param_Prot رد شده است.
۱۶	سامانه پایانی رد شده است.
۱۷	Per Connection رد شده است.

ب-۶-۳-۷ دلیل رهاسازی/پایان‌دهی SA

این فیلد اجباری در نشان‌دادن و درخواست رهاسازی/پایان‌دهی SA موجود است. این فیلد برای مشخص کردن دلیل رهاسازی/پایان‌دهی SA استفاده می‌شود.

این فیلد، برای پایان‌دهی به صفر و برای رهاسازی عادی به ۱ تنظیم می‌شود. مقادیر ۲ تا ۱۲۷ برای استفاده در آینده ذخیره شده‌اند. از مقادیر دیگر می‌توان برای کدهای دلیل تعریف‌شده خصوصی استفاده کرد.

ب-۶-۳-۸ برچسب

این فیلد اختیاری تنها برای استفاده در دومین PDU تبادل همان‌طورکه در زیربند ۸-۲-۳-۴ تعریف‌شده است، به‌کار می‌رود. آغازگر یک مجموعه برچسب امنیتی، پیشنهاد می‌دهد و دریافت‌کننده ممکن است یا کل مجموعه یا یک زیرمجموعه از آن را انتخاب کند. اگر مجموعه‌ی اصلی قابل قبول نباشد، دریافت‌کننده ممکن است یک مجموعه برچسب متفاوت را پیشنهاد بدهد.

ب-۶-۳-۹ انتخاب کلید

این فیلد اختیاری تنها برای استفاده در دومین PDU تبادل است. این فیلد ممکن است به هر تعداد در محتویات SA رخ بدهد.

این فیلد به سه زیرفیلد تقسیم می‌شود:

الف- پرچم‌های کاربرد[1]

ب- اطلاعات انتخاب کلید

پ- مرجع کلید

ب-۶-۳-۹-۱ پرچم‌های کاربرد

این فیلد حاوی حداکثر هفت مقدار است و مکانی در رشته بیتی حاصله از KTE را نشان می‌دهد که از آن‌جا قرار است کلیدهای مشخصی مقدار خود را اختیار کنند. طول کلید از طریق خدمت امنیتی مرتبط انتخاب‌شده‌ای تعیین می‌شود که الگوریتم مربوطه را مشخص می‌کند. چندین کلید ممکن است از یک موقعیت بیت یکسان (یعنی کلید یکسان) استفاده کنند. ترکیب‌های مجاز بستگی به خط‌مشی امنیتی محلی دارند.

هشت‌تایی	مکان کلید/ISN مرتبط در رشته بیتی EKE
۲-۱	کلید رمزگذاری داده‌ی عادی
۴-۳	کلید رمزگذاری داده‌ی پیشتاز
۶-۵	کلید تولید بررسی یکپارچگی داده‌ی عادی
۸-۷	کلید تولید بررسی یکپارچگی داده‌ی پیشتاز
۱۰-۹	My ISN برای داده‌ی عادی
۱۲-۱۱	My ISN برای داده‌ی پیشتاز
۱۴-۱۳	کلید تولید احراز هویت

اگر دریافت‌کننده بخواهد کلیدهای یکسان با ارسال‌کننده پیام را استفاده کند، این فیلد در دومین PDU تبادل دریافت‌کننده نباید ارائه شود.

1- Usage Flags

ب-۶-۳-۹-۲ اطلاعات انتخاب کلید

این فیلد، مکان رشته بیتی حاصله از KTE را مشخص می‌کند که کلیدهای انتخاب‌شده از آن مقدار می‌گیرند. طول کلید از طریق خدمت امنیتی مرتبط انتخابی که الگوریتم مربوطه را مشخص می‌کند، تعیین می‌شود. چندین کلید ممکن است از یک موقعیت بیت یکسان (یعنی کلید یکسان) استفاده کنند. ترکیب‌های مجاز بستگی به خط‌مشی امنیتی محلی دارند.

ب-۶-۳-۹-۳ مرجع کلید

از این زیرفیلد اختیاری می‌توان برای فعال‌سازی ارجاع بعدی به کلید استفاده کرد. این امر به‌عنوان مثال می‌تواند برای اهداف ممیزی یا انتخاب یک کلید جدید برای یک اتصال با به‌کارگیری SA PDU، استفاده شود. مقدار این مرجع برای همبستگی امنیتی باید یکتا باشد.

ب-۶-۳-۱۰ پرچم‌های SA

مکان‌های بیتی زیر برای اعلام صفات SA به‌کار می‌روند. مقدار صفر به معنی نادرست (false) و مقدار یک به معنی درست (true) است.

بیت	صفت SA
۱	Retain-on-Disconnect
۲	Param_Protect
۳	Rekey
۴	Outward/Response
۸-۵	ذخیره‌شده برای استفاده در آینده

بیت‌های ۵ تا ۸ در زمان انتقال به صفر تنظیم می‌شوند و در هنگام دریافت از آن‌ها صرف‌نظر می‌شود.

ب-۶-۳-۱۱ ASSR

این فیلد در صورتی که فیلد انتخاب خدمت ارائه شود، باید حضور داشته باشد. این فیلد شناسه‌ی شئ‌ای است (همان‌طورکه در ISO/IEC 9834 تعریف‌شده است) که مجموعه قواعد امنیتی را شناسایی می‌کند؛ این قواعد با داشتن QOS محافظتی انتخاب شده، سازوکارهایی که باید اعمال شوند را تعریف می‌کنند.

پیوست پ

(الزامی)

مثالی از یک مجموعه توافق‌شده از قواعد امنیتی (ASSR)

یک مجموعه توافق‌شده از قواعد امنیتی (ASSR)، سازوکارهای امنیتی را برای استفاده برقرار می‌سازدکه شامل همه‌ی پارامترهای مورد نیاز برای تعریف عملکرد سازوکار در یک QOS محافظت مفروض است.

ASSR-ID {joint-iso-ccitt (2) identified organization (3) oiw (14) secsig (3) oiwsecsigassrobjectidentifier (5) rule (1)} (شناسه شئ)

طول SA-ID چهار هشت‌تایی

پیمانه تعریف QOS محافظت

PE Auth: low

AC: none

Confid: high

Integ: high

Security Lable: none

محافظت تمامی پارامترهای خدمت

For Protection QOS: Integ=high Confid = high

پیمانه سازوکار – برچسب‌های امنیتی برای کنترل دسترسی

For Protection QOS: AC=high or Conf = high

Label_Def_Auth XYZ

نشان صریح: بله

پیمانه سازوکار – مقدار وارسی یکپارچگی

برای QOS محافظت: Integ .none or Auth = High یا سازوکار برای برچسب‌های امنیتی

ICV_Alg_ID XYZ

ICV_Block_size ۸ هشت‌تایی

Rekey after PDU ۱۵۰۰۰

Key Distribution mech نامتقارن

پیمانه سازوکار – شماره دنباله‌ی یکپارچگی

برای QOS محافظت: Integ=high Auth = high

ISN_Len ۴ هشت‌تایی

پیمانه سازوکار – رمزگذاری

برای QOS محافظت:	Conf > low
Enc_Alg_ID	XYZ
Mode	Chained
Enc_Block_Size	۸ هشت‌تایی
Rekey after	PDU ۱۰۰۰۰
Key Distribution mech	نامتقارن

پیمانه سازوکار – احراز هویت اتصال

For Protection QOS:	AC > low or PE Auth > Low
Enc_Alg_ID	XYZ

پیمانه سازوکار – توزیع کلید نامتقارن

برای سازوکار رمزگذاری یا مقدار وارسی یکپارچگی

PKC_Alg_ID	RSA

پیمانه سازوکار – توزیع کلید متقارن

برای رمزگذاری سازوکار یا مقدار وارسی یکپارچگی

PKC_Alg_ID	DES (X9.17)

پیوست ت

(اطلاعاتی)

مرور کلی الگوریتم EKE

دو پارامتر برای EKE نیاز است: یکی یک عدد اول p بزرگ است (به‌نحوی که p-1 یک فاکتور اول بزرگ دارد) و دیگری یک عدد «a» که در محدوده ۱, a, p-۱ قرار دارد.

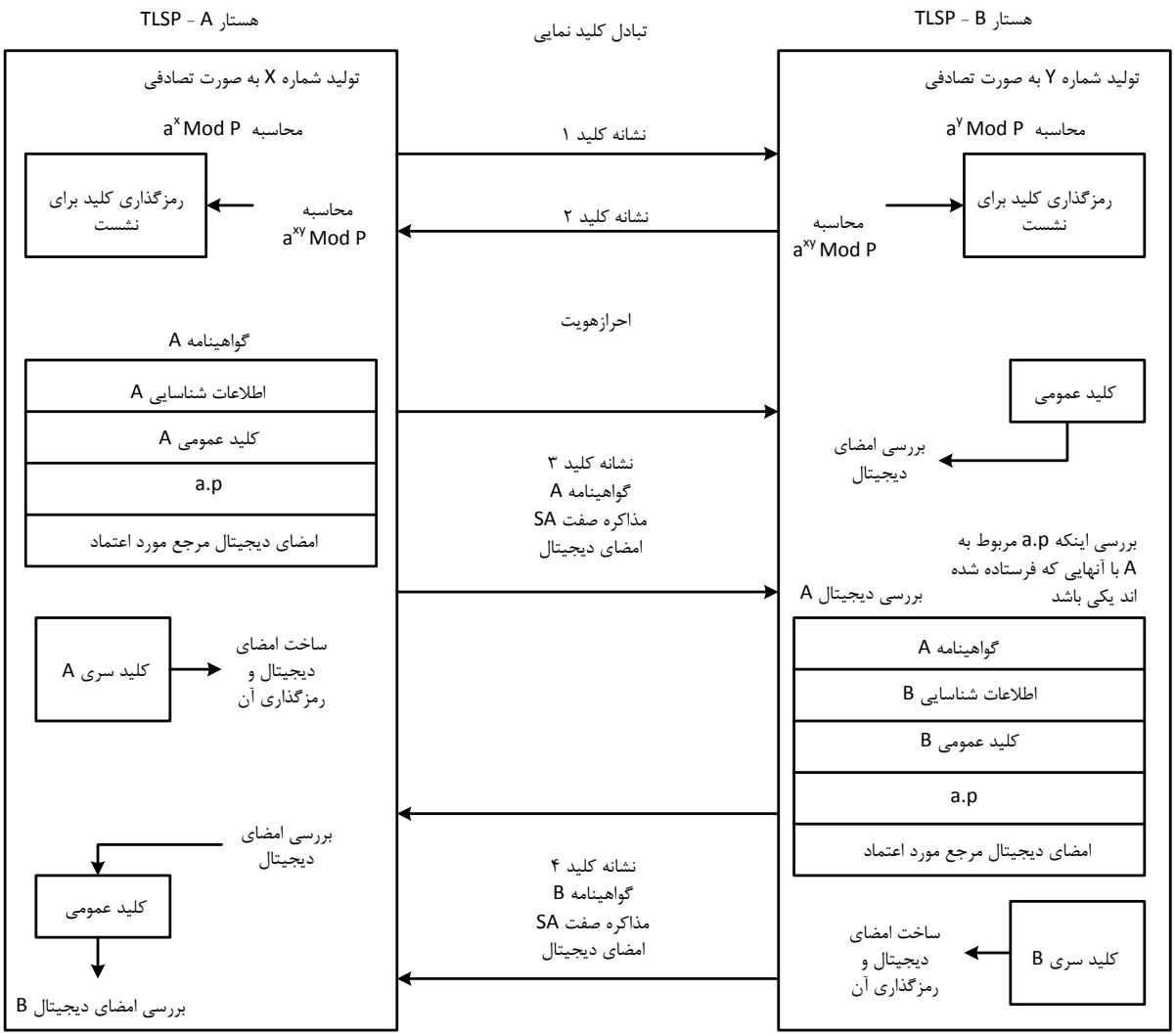
A و B دو طرف یک اتصال فرض می‌شوند (شکل د-۱ ملاحظه شود.). EKE با انتخاب یک عدد تصادفی بزرگ X به‌وسیله‌ی A و انتخاب یک عدد تصادفی بزرگ Y به‌وسیله‌ی B آغاز می‌شود. A مقدار (a**X mod p)[1] را محاسبه کرده و a، p و (a**X mod p) را برای B ارسال می‌کند، و B مقدار (a**XY mod p) را محاسبه کرده و آن را به A ارسال می‌کند. هر دوی A و B مقدار (a**XY mod p) را محاسبه می‌کنند. یک شنودگر تنها می‌تواند مقادیر (a**X mod p) و (a**Y mod p) را ببیند و نمی‌تواند مقادیر X و Y را تشخیص دهد، بنابراین نمی‌تواند (a**XY mod p) را محاسبه کند.

در نتیجه A و B می‌توانند زیرمجموعه‌هایی از بیت‌های (a**XY mod p) را به‌عنوان کلید استفاده کنند.

مقادیر پروتکل SA تعریف‌شده در پیوست ب عبارتند از:

- رشته بیتی EKE مشترک برابر (a**XY mod p) است.
- Key Token 1 a، p، (a**X mod p) است که در آن «a»، «p» و (a**X mod p) در قالب یک رشته بیتی الحاق‌شده کدبندی می‌شوند.
- Key Token 2 (a**Y mod p) است.
- Key Token 3 اطلاعات استخراج‌شده از رشته بیتی KTE مشترک (a**XY mod p) برای مقابله با حملات بازارسال است.
- Key Token 4 اطلاعات استخراج‌شده از رشته بیتی KTE مشترک (a**XY mod p) برای مقابله با حملات replay است.

۱- علامت ** برای به «نما رساندن» یا «به توان رساندن» استفاده شده است.



شکل ت-۱ – نمایش استخراج کلید برخط و امضای دیجیتالی با استفاده از EKE