INSO
18224-6

1st. Edition

2013

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

استاندارد ملی ایران
۱۸۲۲۴-۶
چاپ اول
۱۳۹۱

فناوری‌اطلاعات – اتصال‌متقابل سامانه‌های باز – امنیت لایه‌های بالایی عام: پیش‌برگ بیانیه انطباق پیاده‌سازی پروتکل قاعده نحوی انتقال حفاظت (PICS)

Information technology-Open System Interconnection-Generic Upper layers security :protecting transfer syntax Protocol Implementation Conformance Statement (PICS) Performa

ICS:35.100.01

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

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

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

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

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

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه-بندی 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

«فناوری‌اطلاعات – اتصال‌متقابل سامانه‌های باز – امنیت لایه‌های بالایی عام: پیش نویس بیانیه انطباق پیاده‌سازی پروتکل قواعد نحوی انتقال حفاظت‌کننده (PICS)»

رئیس:	**سمت و/ یا نمایندگی**
رضایی، رامین (لیسانس الکترونیک)	معاون طرح و توسعه مرکز تحقیقات صنایع انفورماتیک
دبیر:	
یحیایی، مهری (لیسانس کامپیوتر)	سرپرست آزمایشگاه فناوری اطلاعات مرکز تحقیقات صنایع انفورماتیک
اعضاء: (اسامی به ترتیب حروف الفبا)	
افکار، علی (دکتری الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت
ترابی، سعید (لیسانس مدیریت صنعتی)	مدیر فنی شرکت بازرسی کالای تجاری
حنیفه، فرشته (لیسانس اقتصاد)	کارشناس مرکز تحقیقات صنایع انفورماتیک
زندباف، عباس (لیسانس مخابرات)	کارشناس شرکت ارتباطات زیرساخت
فرج‌پور، مهیار (فوق‌لیسانس الکترونیک)	عضو هیات مدیره شرکت سیماوا
نادری، مجید (دکتری الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری‌اطلاعات – اتصال متقابل سامانه‌های باز – امنیت لایه‌های بالایی عام: پیش‌برگ بیانیه انطباق پیاده‌سازی پروتکل قاعده نحوی انتقال حفاظت (PICS) » که پیش‌برگ آن در کمیسیون فنی مربـوط، توسـط مرکـز تحقیقات صنایع انفورماتیک، تهیه شده و تدوین شده و در دویست و چهل و هشتمین اجلاسیه‌ی کمیته‌ی ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۹۱/۱۱/۰۹ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

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

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

ISO/IEC 11586-6:1997: Information Technology-Open System Interconnection-Generic Upper Layers security: protecting transfer syntax Protocol Implementation Conformance Statement (PICS) Performa

مقدمه

این استاندارد خدمت‌های فناوری‌اطلاعات – اتصال متقابل سامانه‌های باز – امنیت لایه‌های بالایی عام: پیش‌برگ بیانیه انطباق پیاده‌سازی پروتکل قاعده نحوی انتقال حفاظت (PICS) امنیتی لایه‌های بالایی عمومی را فراهم می‌کنند. این قسمت‌ها به عبارت زیر هستند:

نمای کلی، مدل و نشانه‌گذاری

تعریف سرویس عنصر سرویس تبادل امنیت

مشخصات پروتکل عنصر سرویس تبادل امنیت

مشخصات قواعد نحوی انتقال حفاظت‌کننده

پیش‌برگ PICS تعریف سرویس عنصر سرویس تبادل امنیت

پیش‌برگ PICS قواعد نحوی انتقال حفاظت‌کننده

این توصیه‌نامه|استاندارد قسمت ۶ از این مجموعه را تشکیل می‌دهد.

قسمت چهارم قواعد نحوی انتقال حفاظت‌کننده برای انتقال ارتباطات بین سامانه‌های باز، به عنوان قسمتی از عملیات یک مکانیزم امنیتی را تعیین می‌کند. برای ارزیابی انطباق یک پیاده‌سازی خاص، داشتن یک توصیف از توانایی‌ها و گزینه‌هایی که پیاده‌سازی شده‌اند، ضروری‌است.چنین توصیفی یک عبارت انطباق پیاده‌سازی پروتکل (PICS) نامیده می‌شود.

این استاندارد شامل پیش‌برگ PICS برای قواعد نحوی انتقال حفاظت‌کننده در قسمت ۴ و تبدیلات امنیت تعریف شده در قسمت ۱، پیوست دال می‌باشد[۱].

۱- ISIRI ISO/IEC 11586-11 : فناوری اطلاعات- اتصال متقابل سامانه های باز- امنیت لایه های بالا به طور عام: نگرش کلی، مدل ها و نمادگذاری

فناوری‌اطلاعات – اتصال‌متقابل سامانه‌های باز – امنیت لایه‌های بالایی عام: پیش‌برگ بیانیه انطباق پیاده‌سازی پروتکل قاعده نحوی انتقال حفاظت (PICS)

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین یک پیش‌برگ بیانیه مطابقت پیاده‌سازی پروتکل، برای بیان تفصیلی الزامات مطابقت با ITU-T Rec. X.832| ISO/IEC 11586-4 و پیوست C از ITU-T Rec. X.830|ISO/IEC 11586-1، تعریف می‌کند. این پیش‌برگ پروتکل اجرا بیانیه انطباق (PICS)[1]، در توصیه قاعده نحوی انتقال حفاظت (PICS) انطباق با الزامات مرتبط می‌باشد و با راهنمای مربوطه برای یک پیش‌برگ PICS مندرج در ITU-T Rec.X.291 و ISO/IEC 9646-2 مطابقت می‌دارد. جزئیات استفاده از این پیش‌برگ در این استاندارد ارائه شده‌است. پیاده‌سازی‌هایی که مدعی مطابقت با ITU-T Rec. X.832|ISO/IEC 11586-3 یا پیوست D از ITU-T Rec. X.830|ISO/IEC 11586-1 هستند باید پیش‌برگ را به عنوان قسمتی از الزامات مطابقت، انجام دهند. سطح جزئیات مورد نیاز در پیش‌برگ، از سطح مشخصه‌های پروتکل، در الزام کردن جزئیاتی که برای تعیین هویت منحصر بفرد پیاده‌سازی و فراهم‌کننده است.

یادآوری– PICSها به استانداردهای پایه مرتبط می‌شوند، فقط به توصیه‌نامه‌ها و استانداردهای پایه. ساختار PICS ممکن‌است برای سایر مدارکی که از استانداردهای پایه استفاده می‌کنند گسترش پیدا کرده و اصلاح شود.

۲ مراجع الزامی

مدارک الزامی‌زیر 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 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 آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

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

2-1 ITU-T Recommendation X.830 (1995) | ISO/IEC 11586-1:1996, Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation.

2-2 ITU-T Recommendation X.833 (1995) | ISO/IEC 11586-4:1996, Information technology- Open Systems Interconnection – Generic upper layers security Protecting transfer syntax specification.

1- Protocol Implementation Conformance Statement

۲ - از شماره ۲-۱ الی ۲-۳ مربوط به توصیه‌نامه و استانداردهای بین‌المللی یکسان و از شماره ۲-۴ الی ۲-۶ مربوط به جفت‌هایی از توصیه‌نامه‌ها استانداردهای بین‌المللی که در محتوای فنی معادلند می‌باشد.

2-3 ITU-T Recommendation X.210 (1993) | ISO/IEC 10731:1994, Information technology - Open Systems Interconnection – Basic Reference Model: Conventions for the definition of OSI services.

2-4 ITU-T Recommendation X.290 (1995), OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – General concepts.

2-5ISO/IEC 9646-1:1994, Information technology- Open Systems Interconnection - Conformance testing methodology and framework – Part 1: General concepts.

2-6 ITU-T Recommendation X.291 (1995), OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – Abstract test suite specification.

2-7 ISO/IEC 9646-2:1994, Information technology- Open Systems Interconnection - Conformance testing methodology and framework – Part 2: Abstract test suite specification.

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر که در ITU-T Rec. X.290|ISO/IEC 9646-1 استفاده شده است بکار می‌رود:

الف) بیانیه انطباق پیاده‌سازی پروتکل (PICS)

ب) پیش نویس PICS

پ) اطلاعات اضافی پیاده‌سازی پروتکل برای آزمون (PIXIT)[1]

۴ کوته نوشت‌ها

کوته‌نوشت‌های زیر که در این استاندارد استفاده شده‌اند در ITU-T Rec. X.290 و ISO/IEC 9646-1 تعریف شده‌اند:

الف) PICS

ب) PIXIT

۵ قراردادها

این توصیه‌نامه|استاندارد از قراردادهای توصیفی در قراردادهای خدمات OSI ITU-T Rec. X.210|ISO/IEC 10731، استفاده می‌کند. پیوست الف پیش‌برگ PICS به گونه‌ای طراحی شده‌است که یک بخش خودکفای این توصیه‌نامه|استاندارد برای استفاده در آزمون و تدارک کردن باشد .

۶ انطباق

یک پیش‌برگPICS منطبق باید از نظر فنی معادل پیش‌برگ PICS منتشرشده ITU-T | ISO/IEC باشد و باید شماره‌گذاری و ترتیب موضوعات داخل پیش‌برگ PICS ITU-T | ISO/IEC را ادامه دهد.

یک PICS منطبق با این توصیه‌نامه| استاندارد باید:

الف- یک PICS که بر این توصیه‌نامه|استاندارد منطبق باشد باید:

1- Protocol Implementation extra Information for Testing

ب- یک پیاده‌سازی منطبق با ITU-T Rec. X.833|ISO/IEC 11586-4 را توصیف کند
یک پیش‌برگ PICS منطبقی باشد که به طبق دستور العمل تکمیل ارائه شده در بندهای ۱-الف و ۳-الف از پیوست الف کامل شده باشد. و
پ- شامل اطلاعات ضروری برای تشخیص هویت منحصر بفرد هر دوی پیاده‌سازی و فراهم‌کننده، باشد.

پیوست الف

بیانیه انطباق پیاده‌سازی پروتکل (PICS)

پیش‌برگ برای انتقال قاعده حفاظت

(پیوست الزامی)

الف-۱ نشانه‌گذاری‌های به‌کار رفته برای پیش‌برگ

برای کاهش اندازه جداول در پیش‌برگ PICS، نشانه‌گذاری‌هایی معرفی شده‌اند که اجازه استفاده از یک صفحه‌آرایی با چند ستون را داده‌اند، که در آن‌ها عنوان ستون‌ها "وضعیت" و "پشتیبانی" هستند. تعریف هر یک از این ستون‌ها به شرح زیر است.

الف-۱-۱ ستون وضعیت

این ستون سطح پشتیبانی لازم برای انطباق با ITU-T Rec.X.833|ISO/IEC 11586-4 را نشان می‌دهد. این مقادیر به شرح زیر می‌باشند:

M پشتیبانی اجباری، الزامی است.

O پشتیبانی اختیاری برای مطابقت با ITU-T Rec.X.833|ISO/IEC 11586-4 مجاز است.
در صورتی که پیاده‌سازی شود باید با مشخصات و محدودیت‌های مندرج در
ITU-Rec.X.833|ISO/IEC 11586-4 مطابقت نماید. این محدودیت‌ها ممکن است بر انتخابی بودن سایر اقلام تاثیر بگذارد.

n/a قابل کاربرد نیست.

cn مورد شرطی است (که در آن n عددی است که وضعیت قابل کاربرد را نشان می‌دهد.) تعاریف برای عبارات شرطی استفاده‌شده در این پیوست، زیر جداولی که اولین بار در نمایان می‌شوند، نوشته شده‌است.

o.n مورد اختیاری است اما اختیاری بودنش مشروط است(آنها که در آن n عددی است که شرطی را نشان می‌دهد که واجد شرایط بودن کاربرد است.) تعاریف برای عبارات اختیاری مشروط استفاده‌شده در این پیوست، زیر جداولی که در ابتدا و در انتها نمایان می‌شوند، نوشته شده‌است.

الف-۱-۲ ستون پشتیبانی

ستون پشتیبانی باید توسط فراهم‌کننده یا اجراکننده به منظور نشان دادن سطح پیاده‌سازی هر ویژگی، تکمیل شود. پیش‌برگ طوری طراحی شده‌است که تنها ورودی‌های مورد نیاز در ستون پشتیبانی شامل موارد زیر است:

Y بلی، این ویژگی پیاده‌سازی شده است.

N خیر، این ویژگی پیاده‌سازی نشده است.

- کاربرد ندارد.

الف-۲ اعداد PICS

هر خط در پیش‌برگ PICS که نیازمند وارد کردن جزئیات پیاده‌سازی باشد، در حاشیه سمت چپ خط، عددگذاری شده است. این عددگذاری به عنوان یک وسیله تعیین هویت منحصربفرد، همه جزئیات ممکن پیاده‌سازی ممکن در پیش‌برگ PICS است. نیاز به چنین ارجاع منحصربفرد، توسط نهادهای آزمون‌کننده تشخیص داده شده است.

وسیله ارجاع پاسخ‌های جداگانه بهتر است با مشخص کردن زنجیره زیر نشان داده شود:

۱- یک ارجاع به کوچکترین زیرفرعی که مورد مربوطه را فراگرفته است.

۲- یک کاراکتر خط مورب،"/"

۳- عدد نشان‌دهنده ردیفی که پاسخ در آن نمایان شده‌است.

۴- اگر و فقط اگر، بیش از یک پاسخ در یک ردیف رخ دهد که توسط عدد ارجاع مشخص شده است، در این صورت هر ورودی احتمالی به‌طور قطعی از راست به چپ الف، ب، پ و الی آخر، برچسب‌گذاری شوند و این حرف به زنجیره مزبور الحاق می‌شود.

الف-۳ تکمیل‌کردن PICS

اجراکننده باید همه ورودی‌های سطر با عنوان "پشتیبانی" را کامل کند. در بندهای خاصی از پیش‌برگ PICS، احتمال دارد راهنمایی بیشتری برای کامل‌کردن، لازم باشد. چنین راهنمایی باید مکمل راهنمایی داده‌شده در این بند باشد و باید شامل یک دامنه کاربرد محدودشده به ماده‌ای باشد که در آن ظاهر می‌شود. علاوه بر آن، سایر اطلاعاتی که به گونه‌ای خاص مشخص شده‌اند باید در زمان درخواست، توسط اجراکننده ارائه شوند.

هیچ تغییری به‌جز تکمیل‌کردن به گونه‌ای که الزام شده است، نباید روی پیش‌برگ اعمال شود.

با تشخیص اینکه سطح جزئیات مورد نیاز ممکن است در بعضی موارد، از فضای موجود برای پاسخ‌ها فراتر رود، تعدادی از پاسخ‌ها اجازه اضافه نمودن پیوست‌هایی را به PICS، می‌دهند.

الف-۴ تاریخ بیانیه

تاریخ بیانیه (ر ر- م م- س س)

الف-۵ جزئیات پیاده‌سازی

فراهم‌کننده پیاده‌سازی پروتکل باید اطلاعات ضروری برای شناسایی هویت منحصربفرد پیاده‌سازی و سامانه‌ای که ممکن است در آن قرار داشته باشد را ذکر کند. این ممکن است شامل جزئیات زیر باشد:

الف- فراهم‌کننده، نام پیاده‌سازی، سامانه‌عامل، سخت‌افزار مناسب

ب- فراهم‌کننده سامانه و/یا مشتری آن آزمایشگاه آزمونی که پیاده‌سازی را آزمون می‌کند.

پ- اطلاعاتی درباره این‌که اگر پرسش‌هایی مربوط به محتوای PICSها مجود داشته باشد، با چه کسی تماس گرفته شود.

ت- ارتباط بین این PICS و بیانیه مطابعت سامانه برای سامانه مورد نظر(به یادآوری مراجعه شود).

یادآوری- بیانیه مطالقت سامانه در ITU-T Rec.X.290 | ISO/IEC 11586-1 مشاهده می‌شود. این بیانیه شامل اعلام لایه‌های مدل مرجع مرجعی است که توسط پیاده‌سازی است که قرار است آزمون شود پوشش داده‌شده است.

الف-۶ جزئیات پروتکل ITU-T Rec.X.833 | ISO/IEC 11586-4

الف-۶-۱ اشتباهات فنی پیاده‌سازی شده در ITU-T Rec.X.833 | ISO/IEC 11586-4

الف-۷ بیانیه جهانی انطباق

آیا همه ویژگی های اجباری پیاده سازی شده اند؟(بلی یا خیر)

یادآوری- اگر جواب مثبت به این جعبه داده نشده باشد، در آن صورت پیاده سازی منطبق با ITU-T Rec.X.833 | ISO/IEC 11586-4 نیست.

الف-۸ ساختارهای قاعده نحو پشتیبانی‌شده

	ساختار نحو	فرستادن		دریافت کردن		مرجع	توضیحات
		وضعیت	پشتیبانی	وضعیت	پشتیبانی		
الف- ۱/۸	اولین (PDV) صریح	O		O		قسمت۴ ۵-۴و۶	
الف- ۲/۸	اولینPDVخارجی	O		O		قسمت۴ ۵-۴و۶	
الف- ۳/۸	PDV بعدی	O		O		قسمت۴ ۵- ۴و۶	

الف-۹ فیلدهای PDV پشتیبانی‌شده

الف-۹-۱ اولین PDV صریح

	فیلد	فرستادن		دریافت کردن	
		وضعیت	پشتیبانی	وضعیت	پشتیبانی
الف-۹-۱/۱	شناسانه[1] تبدیل	c1		c1	
الف-۹-۱/۲	پارامترهای حفاظت‌نشده ثابت	c2		c2	
الف-۹-۱/۳	پارامترهای حفاظت‌نشده پویا	c2		c2	
الف-۹-۱/۴	داده‌های با قالب X	c1		c1	
	c1: اگر الف-۱/۸ باشد، آن‌گاه M است و در غیراین‌صورت n/a می‌باشد. c2: اگر الف-۱/۸ باشد، آن‌گاه O است و در غیراین‌صورت n/a می‌باشد.				

1-Identifier

الف-۹-۲ اولین PDV خارجی

	فیلد	فرستادن		دریافت کردن	
		وضعیت	پشتیبانی	وضعیت	پشتیبانی
الف-۹-۱/۲	شناسانه شرایط خارجی	c3		c3	
الف-۹-۲/۲	پارامترهای حفاظت‌نشده پویا	c4		c4	
الف-۹-۳/۲	داده‌های با قالب X	c3		c3	
	c3: اگر الف-۲/۸ باشد، آن‌گاه M است و در غیراین‌صورت n/a می‌باشد. c4: اگر الف-۲/۸ باشد، آن‌گاه O است و در غیراین‌صورت n/a می‌باشد.				

الف-۹-۳ PDV بعدی

	فیلد	فرستادن		دریافت کردن	
		وضعیت	پشتیبانی	وضعیت	پشتیبانی
الف-۹-۱/۳	پارامترهای حفاظت شده پویا	c6		c6	
الف-۹-۲/۳	داده‌های با قالب X	c5		c5	
	c5: اگر الف-۳/۸ باشد، آن‌گاه M است و در غیراین‌صورت n/a می‌باشد. c6: اگر الف-۳/۸ باشد، آن‌گاه O است و در غیراین‌صورت n/a می‌باشد.				

الف-۱۰ مقرر کردن کدگذاری برای قواعد نحو انتقال حفاظت کننده

		مرجع	وضعیت	پشتیبانی
الف-۱/۱۰	کدگذاری خاص/ به قوانین رمزگشایی اشاره شده است.	قسمت ۴ ۵-۲ الف	O	
الف-۲/۱۰	کدگذاری خاص/ به قوانین رمزگشایی اشاره نشده است.	قسمت ۴ ۵-۲ ب	O	

الف-۱۱ تبدیلات امنیتی

الف-۱۱-۱ تبدیلات امنیتی پشتیبانی‌شده

		مرجع	وضعیت	پشتیبانی
الف-۱۱-۲/۱	تبدیلات رمزشده فهرست‌راهنما	قسمت ۱ پیوست د-۱	O	
الف-۱۱-۳/۱	تبدیلات امضاشده فهرست‌راهنما	قسمت ۱ پیوست د-۲	O	
الف-۱۱-۴/۱	تبدیلات امضای فهرست‌راهنما	قسمت ۱ پیوست د-۳	O	
الف-۱۱-۵/۱	تبدیلات امضاشده GULS	قسمت ۱ پیوست د-۴	O	
الف-۱۱-۶/۱	تبدیلات امضای GULS	قسمت ۱ پیوست د-۵	O	

الف-۱۱-۲ تبدیلات رمزشده فهرست راهنما

الف-۱۱-۲-۱ پارامترها

هیچ پارامتری تعریف نشده است.

الف-۱۱-۲-۲ سایر اطلاعات

		وضعیت	پشتیبانی	
الف-۱۱-۲-۱/۲	نگاشت حفاظت وابسته	c7	اسمASN.1	
الف-۱۱-۲-۲/۲	قوانین کدگذاری اولیه	c7	BER/ DER/ متعارف سایر	
c7 :اگر الف-۱۱-۱/۱ باشد، آن‌گاه O است و در غیر این‌صورت n/a می‌باشد.				

الف-۱۱-۳ تبدیلات امضاشده فهرست راهنما

الف-۱۱-۳-۱ پارامترها

		فرستادن		دریافت‌کردن	
		وضعیت	پشتیبانی	وضعیت	پشتیبانی
الف-۱۱-۳-۱/۱	(داده) برای امضاشدن	c8		c8	
الف-۱۱-۳-۲/۱	الگوریتم	c9		c9	
الف-۱۱-۳-۳/۱	سایر پارامترهای خاص الگوریتم	c9		c9	
الف-۱۱-۳-۴/۱	Hash کدگذاری‌شده	c8		c8	
c8 : اگر الف-۹-۲/۱ باشد، آن‌گاه M است و در غیر این‌صورت n/a می‌باشد. c9 : اگر الف-۹-۲/۱ باشد، آن‌گاه O است و در غیر این‌صورت n/a می‌باشد.					

الف-۱۱-۳-۲ سایر اطلاعات

		وضعیت	پشتیبانی	
الف-۱۱-۳-۱/۲	نگاشت حفاظت‌شده وابسته	c9	اسمASN.1	
الف-۱۱-۳-۲/۲	قوانین کدگذاری اولیه	c9	DER	

الف-۱۱-۴ تبدیلات امضا فهرست راهنما

الف-۱۱-۴-۱ پارامترها

		فرستادن		دریافت‌کردن	
		وضعیت	پشتیبانی	وضعیت	پشتیبانی
الف-۱۱-۴-۱/۱	الگوریتم	c10		c10	
الف-۱۱-۴-۲/۱	سایر الگوریتم‌ها با پارامترهای خاص	c10		c10	
الف-۱۱-۴-۳/۱	hash کدگذاری‌شده	c11		c11	

c10: اگر الف-۱۱-۳/۱ آن‌گاه O در غیر این‌صورت n/a c11: اگر الف-۱۱-۳/۱ آن‌گاه M در غیر این‌صورت n/a

الف-۱۱-۴-۲ سایر اطلاعات

	وضعیت	پشتیبانی	
نگاشت حفاظت‌شده وابسته	c10	اسم ASN.1	
قوانین کدگذاری اولیه	c10	DER	

الف-۱۱-۵ تبدیلات امضاشده GULS

الف-۱۱-۵-۱ پارامترها

		فرستادن		دریافت‌کردن	
		وضعیت	پشتیبانی	وضعیت	پشتیبانی
الف-۱۱-۵-۱/۱	مورد حفاظت‌نشده	c12		c12	
الف-۱۱-۵-۲/۱	قوانین کدگذاری اولیه	c13		c13	
الف-۱۱-۵-۳/۱	الگوریتم مهر یا امضا	c13		c13	
الف-۱۱-۵-۴/۱	الگوریتم Hash	c13		c13	
الف-۱۱-۵-۵/۱	اطلاعات کلیدی	c13		c13	
الف-۱۱-۵-۶/۱	پیوست	c12		c12	
c12: اگر الف-۱۱-۴/۱ باشد، آن‌گاه M است و در غیر این‌صورت n/a می‌باشد. c13 اگر الف-۱۱-۴/۱ باشد، آن‌گاه O است و در غیر این‌صورت n/a می‌باشد.					

الف-۱۱-۵-۲ سایر اطلاعات

		وضعیت	پشتیبانی	
الف-۱۱-۵-۱/۲	نگاشت حفاظت‌شده وابسته	c13	اسم ASN.1	
الف-۱۱-۵-۲/۲	قوانین کدگذاری اولیه	c13	استاندارد اگر N است،مشخص نمایید	
الف-۱۱-۵-۳/۲	کدگذاری مستقیم(به زیربند۸-۱ در قسمت ۱ مراجعه‌شود).	c14	پشتیبانی شده	
الف-۱۱-۵-۴/۲	کدگذاری جاسازی‌شده(به زیربند ۸-۱ در قسمت ۱ مراجعه	c14	پشتیبانی شده	
الف-۱۱-۵-۵/۲	کنید).			
	نحو انتقال حفاظتکننده(ماده ۹ در قسمت ۴ را ببینید).	c15	GLUS کلی اگر N است، مشخص نمایید	
c14: اگر الف-۱۱-۴/۱ نبود آن‌گاه n/a است. در غیر این‌صورت کدگذاری مستقیم یا جاسازی شده باید انتخاب شوند. c15: اگر الف-۱۱-۱ نبود آن‌گاه n/a است. در غیر این‌صورت اگر الف-۱۱-۵-۳/۲ آن‌گاه GULS کلی m است و در غیر این‌صورت O می‌باشد.				

الف-۱۱-۶ تبدیلات امضاGULS

الف-۱۱-۶-۱ پارامترها

		فرستادن		دریافت‌کردن	
		وضعیت	پشتیبانی	وضعیت	پشتیبانی
الف-۱۱-۶-۱/۱	قوانین کدگذاری اولیه	c16		c16	
الف-۱۱-۶-۱/۲	الگوریتم مهر یا امضا	c16		c16	
الف-۱۱-۶-۱/۳	الگوریتم Hash	c16		c16	
الف-۱۱-۶-۱/۴	اطلاعات کلیدی	c16		c16	
الف-۱۱-۶-۱/۵	پیوست	c17		c17	
c16: اگر الف-۱۱-۶-۱/۵ باشدآن‌گاه O است ودر غیر این‌صورت n/a می‌باشد. c17 اگر الف-۱۱-۶-۱/۵ باشد، آن‌گاه M است ودر غیر این‌صورت n/a می‌باشد.					

الف-۱۱-۶-۲ سایر اطلاعات

		وضعیت	پشتیبانی	
الف-۱۱-۶-۲/۱	نگاشت حفاظت‌شده وابسته	c16	اسمASN.1	
الف-۱۱-۶-۲/۲	قوانین کدگذاری اولیه	c16	استاندارد اگر اسN است،شرح دهید	
الف-۱۱-۶-۲/۳	کدگذاری مستقیم(زیر بند ۸-۱ در قسمت ۱ را ببینید)	c18	پشتیبانی شده	
الف-۱۱-۶-۲/۴	کدگذاری جاسازی‌شده(زیر بند ۸-۱ در قسمت ۱ را ببینید)	c18	پشتیبانی شده	
الف-۱۱-۶-۲/۵	قواعد نحو انتقال حفاظت‌کننده	c19	GLUSکلی اگرN است،شرح دهید	
c18: اگر الف-۱۱-۶-۱/۵ نبود آن‌گاه n/a است. در غیر این‌صورت کدگذاری مستقیم یا جاسازی شده باید انتخاب شوند. c19: اگر الف-۱۱-۶-۱/۵ نبود آن‌گاه n/a است. در غیر این‌صورت اگر الف-۱۱-۶-۲/۵ باشد، آن‌گاه GULS کلی m است و در غیر این‌صورت O می‌باشد.				