INSO
17113

1st. Edition

Mar.2014

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

استاندارد ملی ایران
۱۷۱۱۳
چاپ اول
اسفند ۱۳۹۲

الزامات ساختار نحوی پیام‌های رمزنگاشتی در زیرساخت کلید عمومی ایران

Cryptographic Messages Syntax Requirements in Iranian Public Key Infrastructure

ICS: 35.040

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 می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود. بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[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 می‌کند. 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 می‌تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و 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 صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها 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 می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است .

---

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

کمیسیون فنی تدوین استاندارد

« الزامات ساختار نحوی پیامهای رمزنگاشتی در زیرساخت کلید عمومی ایران »

رئیس :	**سمت و/ یا نمایندگی**
فیاضی، اسماعیل (فوق لیسانس مهندسی نرم‌افزار و حقوق)	جانشین مدیرعامل شرکت ره آورد سامانه های امن
دبیر:	
فلاح چای، سیدمهدی (فوق لیسانس مهندسی مخابرات رمز)	کارشناس مسؤول مرکز دولتی صدور گواهی الکترونیکی ریشه
اعضاء : (اسامی به ترتیب حروف الفبا)	
امین مقدم، عماد (فوق لیسانس مهندسی مخابرات رمز)	کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه
بداغی، امیرحسین (فوق لیسانس مهندسی برق- الکترونیک)	کارشناس IT سازمان فناوری اطلاعات ایران
بهربگی، مهدی (فوق لیسانس مهندسی کامپیوتر)	مشاور PKI شرکت ره آورد سامانه های امن
پوربابایی، هادی (لیسانس مهندسی کامپیوتر- نرم‌افزار)	مدیر طرح و برنامه شرکت خدمات انفورماتیک راهبر
تیمورنژاد، علی (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس PKI شرکت پیام پرداز
جامی، سارا (لیسانس مهندسی علوم کامپیوتر)	کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه
جلالی، امیر (فوق لیسانس مهندسی کامپیوتر- نرم‌افزار)	برنامه نویس PKI شرکت امن افزار گستر شریف
جوادی، مصطفی (لیسانس مهندسی کامپیوتر سخت‌افزار)	کارشناس شرکت پیام پرداز
جوادی نیا، رضا (لیسانس مهندسی کامپیوتر)	کارشناس PKI مرکز میانی عام
حسینی، ریحانه (لیسانس مهندسی کامپیوتر)	کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه، دانشجوی فوق لیسانس مهندسی IT
خواجوی، هادی (لیسانس مهندسی کامپیوتر – نرم‌افزار)	مدیرفروش شرکت پیام پرداز
راستی، رامبد (لیسانس مهندسی برق- الکترونیک)	نماینده سازمان نظام صنفی کمیسیون افتا و مدیرگروه امنیت شرکت گام الکترونیک
سبزی نژاد، محمد (دکترای مهندسی رمز)	کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه

شادمان، مهدی (لیسانس مهندسی کامپیوتر – نرم‌افزار)	رییس گروه شبکه و سخت افزار سازمان ثبت اسناد و املاک کشور
شاه حسینی، علیرضا (فوق لیسانس مهندسی ICT)	کارشناس امنیت اطلاعات شرکت نوین ۵۲
شاهی، فرید (لیسانس مهندسی کامپیوتر- نرم‌افزار)	سرپرست آزمایشگاه PKI ی مرکز تحقیقات صنایع انفورماتیک ایران
صفرعلی نجار، میثم (فوق لیسانس مهندسی ICT)	کارشناس امنیت اطلاعات شرکت نوین ۵۲
عابدی، اسماعیل (لیسانس مهندسی کامپیوتر)	کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه، دانشجوی فوق لیسانس مدیریت تکنولوژی
علیزاده، جواد (دکترای مهندسی رمز)	کارشناس طراحی، تحلیل و ارزیابی الگوریتم مرکز تحقیقات فتح
قرایی، حسین (فوق لیسانس مهندسی مخابرات)	مدیرعامل شرکت نوین
کریمی، داود (فوق لیسانس مهندسی IT)	مدیرامنیت سازمان امور مالیاتی کشور
گوکی، رضا (لیسانس مهندسی کامپیوتر- نرم‌افزار)	کارشناس امنیت اطلاعات شرکت ره آورد سامانه های امن
محلوجی، نرگس (لیسانس مهندسی کامپیوتر- نرم‌افزار)	کارشناس نرم‌افزار سازمان امور مالیاتی کشور
نیک آذین، حسین (لیسانس مهندسی کامپیوتر)	رئیس گروه تدوین استاندارد سازمان تنظیم مقررات رادیوئی
هایراپطیان، کارین (فوق لیسانس مهندسی معماری کامپیوتر)	کارشناس PKI شرکت داده پردازی ایران
هولکیان، مهدی (لیسانس مهندسی کامپیوتر- نرم‌افزار)	کارشناس آزمایشگاه PKI مرکز تحقیقات صنایع انفورماتیک

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « الزامات ساختار نحوی پیام‌های رمزنگاشتی در زیرساخت کلید عمومی ایران » که پیش نویس آن در کمیسیون های مربوط توسط مرکز دولتی صدور گواهی الکترونیکی ریشهِ مرکز توسعه تجارت الکترونیکیِ وزارت صنعت، معدن و تجارت، تهیه و تدوین شده است و در سیصدمین اجلاس کمیته ملی استاندارد رایانه و فرآوری دادهمورخ ۱۳۹۲/۱۰/۰۹ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه 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 تجدید نظر استانداردهای ملی استفاده کرد .

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

PKCS#7:1998, CMS: Cryptographic Message Syntax Standard, Version 1.5

RFC 5652:2009, Cryptographic Message Syntax Standard (CMS), R. Housley

مقدمه

پیام رمزنگاشتی به داده‌ای گفته می‌شود که حاوی اطلاعات رمزنگاشتی است (به عنوان مثال داده امضا شده، رمز شده و چکیده شده). پیام‌های رمزنگاشتی به عنوان یکی از ارکان انواع نرم‌افزارهای مجهز بـه زیرسـاخت کلید عمومی محسوب می‌شوند که تبادل و نگهداری اطلاعات حساس در قالب این داده‌ها صورت می‌پـذیرد. لذا به منظور تعامل پذیری، آزمون‌پذیری و امنیت نـرم‌افزارهـای اشـاره شـده لازم اسـت سـاختار پیـام‌هـای رمزنگاشتی از یک الگوی استاندارد تبعیت نمایند و الزامات و ملاحظات این الگو در آن‌ها اعمال شـده باشـد. این استاندارد در بردارنده الزامات مرتبط با سـاختار نحـوی انـواع پیـام‌هـای رمزنگاشـتی مـورد اسـتفاده در زیرساخت کلید عمومی ایران است.

الزامات ساختار نحوی پیام‌های رمزنگاشتی در زیرساخت کلید عمومی ایران

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین الزامات ساختار نحوی پیام‌های رمزنگاشتی مورد استفاده در زیرساخت کلید عمومی ایران است. این ساختارها جهت نگهداری و تبادل پیام‌های رمزنگاشتی در نرم‌افزارهایی که مجهز به زیرساخت کلید عمومی ایران می‌باشند، مورد استفاده قرار می‌گیرد.

۲ مراجع الزامی

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

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

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ مستند جامع پروفایل‌های زیرساخت کلید عمومی کشور، نسخه دوم، ۱۳۹۱

2-2 PKCS #1:1993, RSA Encryption Standard. Version 1.5, RSA Laboratories.

2-3 PKCS #6:1993, Extended-Certificate Syntax Standard. Version 1.5, RSA Laboratories.

2-4 PKCS #9:1993, Selected Attribute Types. Version 1.1, RSA Laboratories.

2-5 RFC 1421:1993, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, J. Linn.

2-6 RFC 1422: 1993, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, S. Kent.

2-7 RFC 1423: 1993, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, D. Balenson.

2-8 RFC 1424: 1993, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, B. Kaliski.

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

2-10 CCITT. Recommendation X.209: 1988, Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).

2-11 CCITT. Recommendation X.500: 1988, The Directory—Overview of Concepts, Models and Services.

2-12 CCITT. Recommendation X.501: 1988, The Directory—Models.

2-13 CCITT. Recommendation X.509: 1988, The Directory—Authentication Framework.

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود:

۳-۱
AlgorithmIdentifier

از انواع داده تعریف شده در استاندارد X.509 می‌باشد که در حالت کلی، مشخص‌کننده یک الگوریتم (با یک شناسه شیء[1] مشخص می‌شود) و پارامترهای آن است.

۳-۲
نشانه‌گذاری نحو انتزاعی یک

ASN.1[2]

روش استاندارد تعریف شده در X.690 به جهت توصیف ساختارهای داده می‌باشد.

۳-۳
صفت[3]

داده‌ای مرکب از یک صفت (با یک شناسه مشخص می‌شود) و یک یا چند مقدار برای آن صفت می‌باشد که در استاندارد X.501 تعریف شده است.

۳-۴
قواعد کدبندی‌شده پایه

BER[4]

قواعد کدبندی‌شده پایه که در استاندارد X.690 تعریف شده است.

۳-۵
گواهی[5]

از انواع داده تعریف شده در استاندارد X.509 می‌باشد که در آن از یک امضای دیجیتال برای برقراری تناظر یک به یک بین شناسه منحصر به فرد[6] یک هستار و کلید عمومی آن استفاده شده است. شناسه منحصر به

1 - Object identifier
2 - Abstract Syntax Notation One
3 - Attribute
4 - Basic Encoded Rules
5 - Certificate
6 - Distinguished Name

فرد صادرکننده (امضا کننده) گواهی، شماره ترتیب[1] خاص صادرکننده گواهی، شناسه الگوریتم استفاده شده توسط صادر کننده گواهی به جهت امضاء، دوره اعتبار گواهی و الحاقیه‌های[2] مختلف، بخش‌های دیگر این نوع داده هستند.

۶-۳
CertificateSerialNumber
از انواع داده تعریف شده در استاندارد X.509 بوده و مشخص‌کننده یک گواهی (و به تبع آن یک موجودیت و کلید عمومی آن) است که از میان گواهی‌های امضاءشده توسط یک صادرکننده گواهی، خاص است.

۷-۳
فهرست گواهی‌های باطل شده[3]
CRL
گواهی‌های الکترونیکی که باطل شده‌اند و دیگر نباید آن‌ها را معتبر به حساب آورد، فهرست می‌کند. این ساختار داده که توسط صادرکننده CRL امضاء می‌گردد، دربرگیرنده اطلاعاتی مشتمل بر نام صادرکننده CRL، زمان انتشار CRL، زمانی که بر طبق برنامه[4] قرار است CRL بعدی منتشر گردد و فهرستی از شماره سریال گواهی‌های باطل‌شده و زمان ابطال هریک است. این ساختار داده، همان ساختار داده تعریف شده در RFC 1422 است.

۸-۳
قواعد کدبندی‌شده منحصر به فرد[5]
DER
قواعد کدبندی است که در X.690 تعریف شده و در آن، براساس X.509 محدویت‌هایی بر روش کدبندی پایه اعمال شده است. این روش کدبندی که زیرمجموعه‌ای از روش کدبندی BER است، روشی یکتا برای تفسیر مقادیر ASN.1 فراهم می‌آورد.

۹-۳
استاندارد رمزبندی داده[6]
DES
استاندارد رمزبندی داده در FIPS PUB 46-3[7] تعریف شده است. همچنین 3DES الگوریتمی است که در آن الگوریتم DES، ۳ بار بر روی بستک[8] داده اعمال می‌شود.

---

1 - Serial Number
2 - Extension
3 - Certificate Revocation List
4 - Scheduled
5 - Distinguished Encoding Rules
6 - Data Encryption Standard
7 - Federal Information Processing Standards Publications
8 - Block

۱۰-۳
desCBC
شناسه شیء الگوریتم DES در روش زنجیره‌ای بستک‌های رمز(CBC)[1] است که در استاندارد NIST[2] SP 500-202 تعریف شده است.

۱۱-۳
ExtendedCertificate
ساختار داده‌ای حاوی یک گواهی کلید عمومی X.509 و مجموعه‌ای از صفت‌ها است که (در مجموع) توسط صادر کننده گواهی کلید عمومی X.509 امضا شده است. این ساختار داده در PKCS#6 [3]تعریف شده است.

۱۲-۳
SHA-1
نوعی الگوریتم تولید چکیده پیام است.

۱۳-۳
SHA-2
نوعی الگوریتم تولید چکیده پیام است که شامل چهار نوع تابع چکیده پیام، با طول چکیده ۲۲۴، ۲۵۶، ۳۸۴ و ۵۱۲ بیت است.

۱۴-۳
رایانامه ارتقاء یافته حریم خصوصی[4]
PEM
رایانامه ارتقاء یافته حریم‌خصوصی که در استانداردهای RFC 1421 تا RFC 1424 تعریف شده است.

۱۵-۳
RSA
یک الگوریتم رمزنگاشتی کلید عمومی براساس تعریف PKCS#1 [5] است.

۱۶-۳
rsaEncryption
شناسه الگوریتم رمزنگاشتی RSA که در PKCS#1 تعریف شده است.

1 - Cipher Block Chaining
2 - National Institute of Standard Technology
3 - PKCS #6v1.5: Extended-Certificate Syntax Standard
4 - Privacy Enhanced Mail
5 - PKCS#1v2.1:RSA Cryptography Standard

۱۷-۳
Name

از انواع داده تعریف شده در X.501 است که به طریقی یکتا موجب مشخص‌شدن و یا متمایزشدن شیء داده[۱] از فهرست X.500 می‌گردد. در گواهی X.509، برای مشخص کردن صادر کننده گواهی و هستاری که برایش گواهی صادر شده است، از این نوع داده استفاده می‌گردد.

۱۸-۳
X.509

استاندارد X.509 یکی از استانداردهای اتحادیه بین‌المللی مخابرات – بخش استانداردسازی مخابرات (ITU-T)[۲] برای زیرساخت کلید عمومی است که ساختار گواهی الکترونیکی و فهرست گواهی‌های باطل شده را تعیین می‌کند.

۴ مرورکلی

در این استاندارد به تبیین انواع داده مورد استفاده در ساختار پیام‌های رمزنگاشتی، ساختار کلی یک پیام رمزنگاشتی، ساختارهای داده هفت‌گانه‌ای که می‌تواند به عنوان محتوا مورد استفاده قرارگیرد و شناسه‌ها پرداخته شده است.

ساختار کلی تعریف شده برای یک پیام رمزنگاشتی در این استاندارد، از جامعیت کافی برخوردار بوده و از انواع مختلفی از داده‌ها به عنوان محتوا پشتیبانی می‌کند. ساختارهای داده‌ای که بر اساس این استاندارد می‌تواند به عنوان محتوا مورد استفاده قرار گیرد، در حال حاضر شامل انواع هفت‌گانه «داده»[۳]، « داده امضا شده»[۴]، «داده پوشیده»[۵]، « داده امضا شده و پوشیده»[۶]، « داده چکیده شده»[۷] ، « داده رمزشده»[۸] و « داده احرازهویت شده»[۹] می‌باشد. با این وجود، ممکن است که در آینده ساختارهای داده دیگری نیز بدین مجموعه اضافه گردد.

در حالت کلی، ساختارهای داده‌ای که می‌تواند به عنوان محتوا مورد استفاده قرار گیرد، به دو دسته کلی «پایه»[۱۰] و «توسعه‌یافته»[۱۱] قابل طبقه‌بندی است. ساختارهای داده «پایه»، فقط دربردارنده داده بوده و فاقد هرگونه بخش رمزنگاشتی شده‌ی توسعه‌یافته[۱۲] است. مشخصات، ساختار داده از نوع «داده» را می‌توان

1 - Data Object
2 - International Telecommunication Union-Telecommunication
3 - Data
4 - Signed-data
5 - Enveloped-data
6 - Signed-and-enveloped-data
7 - Digested-data
8 - Encrypted-data
9 - Authenticated-data
10 - Base
11 - Extended
12 - Cryptographic Enhanced

در این دسته قرار داد. ساختارهای حاوی چند نوع داده (به طور احتمالی رمز شده) و یا ساختارهای داده‌ای که دارای بخش رمزنگاشتی شده است، در دسته «توسعه‌یافته» قرار می‌گیرند. به عنوان مثال، یک داده از نوع «پوشیده» می‌تواند حاوی یک داده از نوع«امضاشده» (رمزشده) باشد که به نوبه خود حاوی داده‌ای از نوع «داده» است. در حالت کلی، شش نوع داده «امضا شده»، «پوشیده»، «امضا شده و پوشیده»، «چکیده شده»، «رمزشده» و «احرازهویت شده» که فقط دربردارنده داده نبوده و حاوی بخش رمزنگاشتی شده می‌باشند و به دسته «توسعه‌یافته» تعلق دارند.

بر اساس این استاندارد، می‌توان یک ساختار داده «توسعه‌یافته» را به صورت یک مرحله‌ای[1] تولید کرد (با استفاده از کدگذاری BER با طول نامشخص) و آن‌را به صورت یک مرحله‌ای (با هر نوع کدگذاری BER) پردازش کرد. این امر به ویژه در ذخیره‌سازی بر روی نوارهای مغناطیسی اهمیت می‌یابد. یکی از چالش‌های عملیات تک مرحله‌ای، دشوار بودن پردازش ساختارداده کدبندی شده به صورت DER در یک مرحله است، زیرا ممکن است از قبل طول اجزای مختلف مشخص نباشد. از آنجایی که کدبندی DER برای انواع داده‌ای «امضا شده»، «امضا شده و پوشیده» و «چکیده شده»، مورد نیاز است، ممکن است عملیات چند مرحله-ای[2] لازم باشد (به عنوان مثال برای حالتی که یک نوع داده‌ای متفاوت با داده‌ای که محتوای داخلی آن نوع داده‌ای است، مد نظر باشد).

٤-١ انواع داده مورد استفاده

در این قسمت به توصیف برخی از انواع داده‌ای که در قسمت‌های دیگر استاندارد مورد نیاز است، پرداخته شده است.

٤-١-١ نوع داده‌ای CertificateRevocationLists

ساختارداده‌ای مرکب از تعدادی فهرست گواهی‌های باطل شده است. بر مبنای اطلاعات موجود در این ساختار، باید بتوان وضعیت دقیق یک گواهی (ابطال یا عدم ابطال) موجود در فهرست را تعیین کرد. البته ممکن است که تعداد فهرست‌های گواهی باطل شده، بیشتر و یا کمتر از حد نیاز باشد.

CertificateRevocationLists ::=
SET OF CertificateRevocationList

٤-١-٢ نوع داده‌ای ContentEncryptionAlgorithmIdentifier

شناسه شیء الگوریتم استفاده شده در رمزبندی محتویات ساختار داده (به عنوان مثال 3DES) است. از این الگوریتم می‌توان در عملیات رمزبندی و نیز در عملیات رمزگشایی استفاده کرد. عملیات رمزبندی، نگاشت مبتنی بر کلید رمزبندی یک رشته بایتی (پیام) به یک رشته بایتی دیگر (متن رمز شده) است. در عملیات رمزگشایی، عکس عملیات فوق صورت می‌گیرد.

ContentEncryptionAlgorithmIdentifier ::=

---

1 - Single pass
2 - Extra Pass

AlgorithmIdentifier

٤-١-٣ نوع داده‌ای DigestAlgorithmIdentifier

شناسه الگوریتم استفاده شده در تولید چکیده‌پیام (به طور مثال SHA-1) است. مراد از الگوریتم چکیده‌پیام در این‌جا، الگوریتمی است که یک رشته بایتی (پیام) را به یک رشته بایتی دیگر (چکیده‌پیام) نگاشت می کند.

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

٤-١-٤ نوع داده‌ای DigestEncryptionAlgorithmIdentifier

شناسه الگوریتم رمزبندی است که به منظور رمزبندی چکیده‌پیام مورد استفاده قرار گرفته است. الگوریتم rsaEncryption معرفی شده در استاندارد PKCS#1 از جمله این الگوریتم‌ها است. درحالت کلی، یک الگوریتم رمزبندی چکیده می‌تواند هم در رمزبندی و هم در رمزگشایی مورد استفاده قرار گیرد. در عملیات رمزبندی، از یک کلید رمزبندی برای نگاشت یک رشته بایتی (چکیده پیام) به یک رشته بایتی دیگر (چکیده پیام رمزشده) استفاده می‌شود. عملیات رمزگشایی عکس عملیات رمزبندی است.

.DigestEncryptionAlgorithmIdentifier ::=
AlgorithmIdentifier

٤-١-٥ نوع داده‌ای ExtendedCertificateOrCertificate

ساختار داده‌ای حاوی یگ گواهی توسعه‌یافته یا یک گواهی X.509 می‌باشد که از ساختار توصیه شده در این استاندارد پیروی می‌کند.

```
ExtendedCertificateOrCertificate := CHOISE{
        Certificate Certificate -- X.509
        ExtendedCertificate [0] IMPLICIT ExtendedCertificate}
```

٤-١-٦ نوع داده‌ای ExtendedCertificatesAndCertificates

این ساختار داده، حاوی مجموعه‌ای از گواهی‌های الکترونیکی است. این مجموعه باید بتواند زنجیره اتصالی بین یک مرکز صدور گواهی ریشه یا بالادستی و همه امضاکننده‌های موجود در مجموعه برقرار کند. البته ممکن است که گواهی‌های موجود در این مجموعه، بیشتر یا کمتر از حد لازم باشد.

```
Extended Certificates And Certificates :=
        SET OF Extended Certificate Or Certificate
```

٤-١-٧ نوع داده‌ای IssuerAndSerialNumber

ساختار داده‌ای مرکب از شناسه منحصر به فرد صادرکننده گواهی و شماره ترتیب تخصیص داده شده به گواهی (توسط صادرکننده‌گواهی) است که یک گواهی (و در نتیجه یک هستار و کلید عمومی او) را مشخص می‌کند.

```
IssuerAndSerialNumber ::= SEQUENCE {
        Issuer Name,
        SerialNumber CertificateSerialNumber}
```

٤-١-٨ نوع داده‌ای KeyEncryptionAlgorithmIdentifier

شناسه الگوریتم رمزبندی است که در رمزبندی کلیدی که بر اساس آن فرایند رمزبندی انجام شده، مورد استفاده قرار گرفته است. به عنوان نمونه می‌توان به الگوریتم rsaEncryption معرفی شده در استاندارد PKCS#1 اشاره کرد. در حالت کلی، از این الگوریتم می‌توان در عملیات رمزبندی و نیز در عملیات رمزگشایی استفاده کرد. عملیات رمزبندی کلید، عملیاتی است که طی آن، یک رشته بایتی (کلید) به رشته بایتی دیگری (کلید رمزشده) نگاشت می‌یابد. عملیات رمزگشایی عکس عملیات رمزبندی است.

```
KeyEncryptionAlgorithmIdentifier ::=
        AlgorithmIdentifier
```

٤-١-٩ نوع داده‌ای Version

این عدد بیانگر شماره نسخه استانداردی است که درتنظیم ساختار داده ملاک عمل قرار گرفته است. وجود چنین فیلدی[1]، میزان سازگاری با استانداردهای آتی را افزایش می‌دهد.

```
Version=INTEGER
```

٥ ساختار کلی

ساختار کلی برای محتوایی که بر اساس این استاندارد بین موجودیت‌های مختلف مبادله می‌گردد، ساختار داده‌ای از نوع ContentInfo است که از یک بخش محتوا[2] و یک بخش مشخص‌کننده نوع محتوا یا نوع داده تشکیل شده است. نمایش ASN.1 این ساختار داده به قرار زیر است:

1 - Field
2 - content

```
ContentInfo ::= SEQUENCE {
 contentType ContentType,
 content
  [0] EXPLICIT ANY DEFINED BY contentType OPTIONAL }

ContentType ::= OBJECT IDENTIFIER
```

در زیر به تبیین فیلدهای یک ساختار داده از نوع contentInfo پرداخته شده است:

- contentType : شناسه‌ای است که نوع داده (نوع ساختار داده فیلد content) را مشخص می‌کند. این شناسه، در واقع رشته‌ای منحصر به فرد از اعداد صحیح است که توسط همان مرجعی که نوع داده را تعریف می‌کند، تخصیص داده می‌شود. براساس این استاندارد، فیلد contentType می‌تواند یکی از هفت مقدار data، SignedData ، envelopedData ، signedAndEnvelopedData ، digestedData ، authenticatedData و یا encryptedData را داشته باشد.
- content : بخش محتوایی یک ساختار داده از نوع contentInfo است. شناسه‌ای که در فیلد contentType قرار گرفته است، نوع این ساختار داده را مشخص می‌کند. در حالت کلی، این فیلد اختیاری است. البته بدیهی است در حالتی که این فیلد وجود ندارد، اطلاعات آن باید به طریقی دیگر منتقل گردد.

یادآوری۱-روش‌هایی که در ادامه آمده است، مفروض بر این است که فیلد contentType، نوع فیلد content را به‌صورت یکتایی مشخص می‌کند. بنابراین هر شناسه‌ای که بر یک نوع داده مشخص دلالت می‌کند، نمی‌تواند از نوع *CHOICE*[1] باشد.

یادآوری۲-درحالتی‌که محتوای داخلی ساختارهای داده از نوع «امضا شده»، «امضا شده و پوشیده» یا «چکیده شده» یک ساختار داده از نوع ContentInfo است، الگوریتم تولید چکیده پیام بر محتویات بایتی فیلد content که به‌صورت DER کدبندی شده است، اعمال می‌گردد. در حالتی‌که محتوای داخلی ساختارهای داده از نوع «پوشیده» یا «امضا شده و پوشیده» یک ساختار داده از نوع ContentInfo است، الگوریتم رمزبندی محتوا بر محتویات بایتی فیلد content که به صورت BER با طول معلوم[2] کدبندی شده اعمال می‌گردد.

یادآوری۳-اختیاری بودن فیلد content این امکان را فراهم می‌آورد که به طور مثال بدون نیاز به تغییر و یا تکرار محتوایی که قرار است امضا شود، امضای خارجی[3] تولید گردد. در تولید امضای خارجی محتوایی که قرار است امضاء شود از محتوای داخلی ساختار داده ContentInfo که درون یک نوع داده از نوع «امضا شده» مورد استفاده قرار گرفته، حذف می‌گردد.

۶ نوع داده‌ای «داده»

این نوع داده را می‌توان فقط یک رشته‌بایتی دانست. در حالت کلی، نمایش ASN.1 یک نوع داده از نوع «داده» به‌صورت زیر است:

```
Data ::= OCTET STRING
```

---

۱ - یکی از انواع داده‌ای پایه که در ساختار ASN.1 تعریف می‌شود.

2 - Definite-length BER

3 - External signature

تفسیر این رشته بایتی که رشته‌ای دلخواه از حروف و فایلهای متنی کد استاندارد آمریکایی برای تبادل اطلاعات (ASCII)[1] است، برعهده برنامه کاربردی[2] است. در حالت کلی، لزومی بر وجود ساختار داخلی خاص در این رشته‌های بایتی نیست (البته چنین امری غیرممکن نیز نمی‌باشد. حتی ممکن است این رشته‌های بایتی به صورت DER کدبندی شده باشند).

۷ نوع داده‌ای «امضاء شده»

نوع داده‌ای متشکل از یک بخش محتوایی (که هر نوع ساختار داده‌ای می‌تواند داشته باشد) و مقدار رمزشده چکیده‌پیام این بخش محتوایی است که متناظر با امضاءکننده‌های[3] مختلف است (تعداد امضا کننده در این ساختار ممکن است صفر یا بیشتر باشد). هر چکیده‌پیام رمز شده مرتبط با بخش محتوایی متناظر با یک امضاءکننده را در واقع می‌توان «امضای دیجیتالی (رقمی)»[4] بخش محتوایی برای آن امضاءکننده دانست. در حالت کلی هر تعداد امضا کننده می‌توانند به موازات هم، هر نوع محتوا را امضا کنند. به علاوه یک حالت خاص برای این ساختار حالتی است که هیچ امضاءکننده‌ای وجود ندارد. چنین ساختار داده‌ای (یک ساختار داده از نوع «امضاءشده» که فاقد امضاءکننده است) در انتشار گواهی و فهرست گواهی باطل شده کاربرد دارد.

از متداول‌ترین کاربردهای یک نوع داده از نوع «امضاءشده»، قراردادن امضای دیجیتالی یک امضاءکننده، بر محتوای یک نوع داده از نوع «داده» است. از دیگر کاربردهای چنین نوع داده‌ای می‌توان به کاربرد آن در انتشار گواهی و فهرست گواهی باطل شده اشاره کرد.

فرایند تولید یک داده از نوع «امضاء شده» به قرار زیر است:

۱- به ازای هر یک از امضاءکنندگان، از الگوریتم تولید چکیده‌پیام خاص آن موجودیت برای محاسبه چکیده پیام بخش محتوایی استفاده می‌شود. (البته در حالتی که دو امضاءکننده از الگوریتم تولید چکیده‌پیام یکسانی استفاده می‌کنند، دیگر نیازی به دوبار محاسبه چکیده‌پیام نبوده و کافی است که چکیده‌پیام فقط به ازای یکی از امضاءکنندگان محاسبه گردد) در بعضی مواقع نیاز است که اصالت اطلاعات دیگری غیر از محتوا نیز توسط یک امضاءکننده احراز گردد (طبق بند ۷-۴). در این حالت با اعمال الگوریتم تولید چکیده‌پیام خاص امضاءکننده بر رشته حاوی چکیده‌پیام بخش محتوایی و این اطلاعات اضافی، چکیده پیام محاسبه می‌شود.

۲- به ازای هر یک از امضاءکنندگان، از کلید خصوصی آن امضاءکننده برای رمزبندی چکیده‌پیام اشاره شده و اطلاعات مربوطه استفاده می‌گردد.

---

1 - American Standard Code for Information Interchange
2 - application
3 - Signer
4 - Digital signature

۳- به ازای هریک از امضاءکنندگان، با استفاده از چکیده‌پیام رمزشده و دیگر اطلاعات آن امضاءکننده، یک نوع داده از نوع SignerInfo (به بند ۷-۲ مراجعه شود) تولید می‌گردد. جمع‌آوری گواهی‌ها و فهرست های گواهی باطل‌شده هریک از امضاءکنندگان و حتی گواهی‌ها و فهرست‌های گواهی باطل‌شده‌ای که به هیچ امضا کننده‌ای تعلق ندارند، از دیگر اقداماتی است که در این مرحله انجام می‌شود.

۴- از ترکیب بخش محتوایی، شناسه الگوریتم‌های تولید چکیده‌ای که امضاکنندگان استفاده کرده‌اند و انواع داده از نوع SignerInfo که به ازای هریک از امضاءکنندگان تولید شده است، یک نوع داده از نوع SignedData (به بند ۷-۱ مراجعه شود) تولید می‌گردد.

گیرنده برای وارسی امضاهای دیجیتالی موجود در یک نوع داده از نوع «امضاءشده»، ابتدا با استفاده از کلید عمومی هر امضاءکننده، چکیده‌پیام رمزشده متناظر با آن امضاءکننده را رمزگشایی و سپس با چکیده‌پیامی که به طور مستقیم و به صورت مستقل محاسبه شده، مقایسه می‌کند. اطلاع از کلید عمومی یک امضاءکننده، نیازمند رجوع به گواهی آن امضاءکننده است. این گواهی، یا جزء اطلاعات موجود آن امضاکننده است و یا با استفاده از شناسه منحصر به فرد صادرکننده گواهی و شماره ترتیب خاصی که توسط صادرکننده گواهی به آن اختصاص داده شده، قابل بازیابی است.

در این قسمت ابتدا به بررسی کلی و سطح بالای یک نوع داده از نوع SignedData پرداخته شده است. در ادامه به بررسی ساختار داده از نوع SignerInfo که دربردارنده اطلاعات یکی از امضاءکنندگان است، پرداخته شده است. در قسمت‌های بعدی به ترتیب به بررسی فرایندهای تولید چکیده‌پیام و رمزبندی چکیده‌پیام اختصاص پرداخته شده است.

۷-۱ SignedData

نمایش ASN.1 یک داده از نوع «امضاء شده» به‌صورت زیر است:

```
SignedData ::= SEQUENCE {
  version Version,
  digestAlgorithms DigestAlgorithmIdentifiers,
  contentInfo ContentInfo,
  certificates
    [0] IMPLICIT ExtendedCertificatesAndCertificates   OPTIONAL,
  crls
    [1] IMPLICIT CertificateRevocationLists   OPTIONAL,
  signerInfos SignerInfos }

DigestAlgorithmIdentifiers ::=

  SET OF DigestAlgorithmIdentifier

SignerInfos ::= SET OF SignerInfo
```

در ادامه این قسمت به توصیف فیلدهای این نوع داده پرداخته شده است:

- version : مشخص می‌کند که در تنظیم فیلدهای ساختار داده بر مبنای کدام ویرایش از استاندارد عمل شده است. در صورتی که از ویرایش حاضر استاندارد استفاده شده باشد، این فیلد با مقدار 1 پر می‌شود.

- digestAlgorithms: در بردارنده شناسه‌های متعلق به الگوریتم‌های تولید چکیده‌پیام است. این فیلد می‌تواند یک فیلد تهی و یا حاوی یک یا چند شناسه باشد. در حالت کلی، محدودیتی از این حیث وجود ندارد. هر یک از شناسه‌هایی که در این فیلد قرار می‌گیرد، مشخص‌کننده یکی از الگوریتم‌های تولید چکیده‌پیام استفاده‌شده توسط امضاءکنندگان (و همه پارامترهای آن) برای محاسبه چکیده محتوا است. در مجموع، این فیلد باید مشخص کند که چه الگوریتم‌های تولیدچکیده‌پیامی توسط همه امضاءکنندگان مورد استفاده قرار گرفته است تا بدین وسیله وارسی یک مرحله‌ای امضاء تسهیل شود.(به بند ۷-۳ برای تبیین فرایند تولید چکیده‌پیام مراجعه شود).

- contentInfo : بخشی از نوع داده است که امضاء شده است. در حالت کلی، محدودیتی در مورد نوع داده این بخش وجود ندارد و این بخش می‌تواند داده‌ای از نوع «داده»، «امضا شده»، «پوشیده»، «امضا شده و پوشیده»، «چکیده شده» یا «رمزشده» باشد.

- certificates : حاوی تعدادی گواهی X.509 می‌باشد. در کل با استفاده از این مجموعه گواهی باید بتوان زنجیره اتصالی بین کلیه امضاءکنندگانی که در فیلد signerInfos از آن‌ها نام برده شده و یک مرکز صدور گواهی ریشه یا بالادستی که مورد اعتماد می‌باشد، برقرار کرد. با این وجود، ممکن است که تعداد گواهی های موجود در این فیلد بیشتر از حد نیاز باشد و یا حتی یک امضاءکننده را بتوان در زنجیره‌های اعتماد منتهی به مراکز صدور گواهی سطح بالای متعددی قرار داد. البته کمتر از تعداد مورد نیاز بودن گواهی‌هایی که در این فیلد قرار می‌گیرند نیز امری محتمل است. فقط در حالتی که این امکان برای وارسی‌کننده امضاهای دیجیتالی وجود دارد که از طریق دیگری به گواهی‌های مورد نیاز خود دست یابد (به طور مثال با استفاده از مجموعه گواهی‌های قبلی) شاهد چنین امری هستیم.

- crls : حاوی مجموعه‌ای از فهرست‌های گواهی باطل‌شده است که بر مبنای آن می‌توان وضعیت دقیق (باطل بودن یا نبودن) گواهی‌های موجود در فیلد certificates را تعیین کرد. البته این فیلد نباید حتما وضعیت تمام گواهی‌های موجود در فیلد certificates را مشخص کند. ممکن است که تعداد فهرست‌های گواهی باطل‌شده، بیشتر و یا کمتر از حد نیاز باشد.

- signerInfos : حاوی اطلاعات کلیه امضاءکنندگان است. در حالت کلی، محدودیتی در مورد تعداد عناصر این فیلد وجود ندارد و حتی ممکن است هیچ مقداری در آن قرار نگیرد.

یادآوری۱–قرارگرفتن فیلد digestAlgorithms در قبل از فیلد contentInfo و قرارگرفتن فیلد SignerInfos در بعد از آن، پردازش یک‌مرحله‌ای یک ساختار داده از نوع SignedData را ممکن کرده است.

یادآوری۲-در حالت خاصی که هیچ امضاءکننده‌ای وجود ندارد، چندان مناسب نیست که ContentInfo ، داده‌ای از نوع «امضاء شده» باشد. در این حالت توصیه می‌شود ContentInfo که امضاء شده است از نوع «داده» بوده و فیلد content آن حذف گردد.

۲-۷ SignerInfo

این ساختار داده، دربردارنده اطلاعات یک امضاءکننده بوده و نمایش ASN.1 آن به صورت زیر است:

```
SignerInfo ::= SEQUENCE {
  version Version,
  issuerAndSerialNumber IssuerAndSerialNumber,
  digestAlgorithm DigestAlgorithmIdentifier,
  authenticatedAttributes
    [0] IMPLICIT Attributes   OPTIONAL,
  digestEncryptionAlgorithm
    DigestEncryptionAlgorithmIdentifier,
  encryptedDigest EncryptedDigest,
  unauthenticatedAttributes
    [1] IMPLICIT Attributes   OPTIONAL }

EncryptedDigest ::= OCTET STRING
```

در ادامه این بخش به تبیین فیلدهای یک ساختار داده از نوع SignerInfo پرداخته شده است:

- version : بیانگر آن است که کدام ویرایش از استاندارد، ملاک عمل قرار گرفته است. در صورتی که از ویرایش حاضر استاندارد استفاده شده باشد، این فیلد با مقدار 1 پر می‌شود.
- issuerAndSerialNumber : گواهی امضاءکننده (و در نتیجه شناسه منحصر به فرد امضاءکننده و کلید عمومی او) را مشخص می‌کند و این کار را با استفاده از شناسه منحصر به فرد صادرکننده گواهی و شماره ترتیبی که این صادرکننده‌گواهی به گواهی اختصاص داده انجام می‌دهد.
- digestAlgorithm : شناسه (و دیگر پارامترهای وابسته) الگوریتمی است که در محاسبه چکیده‌پیام بخش محتوایی (فیلد contentInfo از ساختارداده از نوع SignedData) و اطلاعات موجود در فیلد authenticatedAttributes مورد استفاده قرار گرفته است. مقداری که در این فیلد قرار می‌گیرد، باید یکی از مقادیر موجود در فیلد digestAlgorithms از ساختار داده از نوع SignedData بالادستی‌اش باشد. (به بند ۷-۳ برای تبیین فرایند تولید چکیده‌پیام مراجعه شود).
- authenticatedAttributes : دربردارنده مجموعه صفت‌هایی است که توسط امضاءکننده، امضا (تایید) شده است. در حالت کلی، این فیلد را می‌توان یک فیلد اختیاری دانست اما درحالتی که ContentInfo (از ساختار داده از نوع SignedData فوق) نوع داده‌ای غیر از نوع «داده» داشته باشد، وجود این فیلد الزامی می‌گردد. این فیلد، در صورت وجود، حداقل حاوی دو صفت خواهد بود:

- یک صفت از نوع «content-type» کـه در اسـتاندارد PKCS#9 تعریـف شـده و حـاوی نـوع داده ContentInfo است که امضا می‌شود.
- یک صفت از نوع «message-digest» که در PKCS#9 تعریف شده اسـت و حـاوی چکیـده‌پیـام محتوای استفاده شده می‌باشد.

از دیگر صفت‌های قابل استفاده در این فیلد می‌تـوان بـه صـفت «زمـان‌امضـاء»[1] کـه آن هـم در اسـتاندارد PKCS#9 تعریف شده است اشاره کرد.

- digestEncryptionAlgorithm : شناسه الگوریتمی است که از آن به جهت رمزبندی چکیده‌پیام و دیگـر اطلاعات وابسته با استفاده از کلیدخصوصی امضاءکننده استفاده شده است. (بـه بنـد ۷-۴ بـرای تبیـین فرایند رمزبندی چکیده‌پیام مراجعه شود).
- encryptedDigest : رشـته حاصـل از رمزبنـدی چکیـده‌پیـام و دیگـر اطلاعـات مربوطـه بـا اسـتفاده از کلیدخصوصی امضاءکننده است.
- unauthenticatedAttributes : فیلدی اختیاری بوده و دربردارنده مجموعه صـفت‌هـایی اسـت کـه مـورد تأیید امضاءکننده نیست، یعنی امضاءشده و مستند نیستند. صفت «امضاء چندگانـه»[2] کـه در PKCS#9 تعریف شده است، از جمله مقادیر قابل استفاده در این فیلد است.

یادآوری- به جهت سـازگاری بـا PEM، توصـیه مـی‌گـردد درحـالتی کـه نـوع داده ContentInfo (از سـاختار داده از نـوع SignedData مـافوق) کـه امضـا مـی شـود از نـوع «داده» بـوده و صـفت احـراز هویـت شـده دیگـری وجـود نـدارد، فیلـد authenticatedAttributes حذف گردد.

۷-۳ فرآیند تولید چکیده‌پیام

فرآیندی است که طی آن، چکیده‌پیام نوع داده که قرار است امضاء شود و یـا چکیـده پیـام داده، بـه همـراه صفت‌های احراز هویت شده، محاسبه شود. به هر حال، ورودی اولیه فرایند تولید چکیده‌پیام در هر یک از دو حالت فوق، همان بخشی از نوع داده است که قرار است امضاء شود. این بخش، در واقع همـان رشـته بایـت حاصل از کدبندی به صورت DER اطلاعات موجود در فیلد content از ساختار داده ContentInfo که بایـد امضاء گردد، است. تابع محاسبه چکیده‌پیام، فقط بر همین رشته بایتی (که به صورت DER کدبنـدی شـده است) اعمال شده و رشته بایت‌های دیگری مانند رشته بایت معرف طول[3] یا رشته‌بایت متعلق به شناسه‌هـا[4] در این محاسبه لحاظ نمی‌گردد.

بسته به این‌که فیلد authenticatedAttributes وجود دارد یا خیـر، فراینـد تولیـد چکیـده‌پیـام بـه برونـداد متفاوتی منتهی می‌گردد (از این خروجی، تحت عنوان «چکیده‌پیام» نیز یاد مـی‌گـردد). در صـورت عـدم

1 - signing time
2 - Counter signature
3 - Length octets
4 - Identifier octets

وجود این فیلد، فقط چکیده‌پیام نوع داده‌ای که قرار است امضاء شود، محاسبه می‌گردد. این در حالی است که در صورت وجود این فیلد، چکیده‌پیام انواع داده از نوع Attributes موجود در فیلد authenticatedAttributes که به صورت DER کدبندی شده‌اند، نیز محاسبه می‌گردند. با توجه به این‌که این فیلد در صورت وجود، حداقل حاوی یک صفت از نوع «نوع‌داده» و یک صفت از نوع «چکیده‌پیام» خواهد بود، این انواع داده را می‌توان به طور غیرمستقیم در تولید خروجی دخیل دانست.

اگر بخش محتوایی که قرار است امضا شود، نوع داده‌ای از نوع «داده» داشته باشد و فیلد authenticatedAttributes نیز وجود نداشته باشد، الگوریتم تولید چکیده‌پیام فقط بر داده موجود (به طور مثال محتویات یک فایل) اعمال می‌شود. از مزایای این امر می‌توان به عدم نیاز به اطلاع از طول بخش محتوایی تا پیش از انجام فرایند رمزبندی اشاره کرد. در این‌جا شاهد سازگاری کاملی با PEM هستیم.

لحاظ نکردن رشته‌بایت معرف طول یا رشته‌بایت متعلق به شناسه‌ها در محاسبه چکیده‌پیام، به معنای عدم حفاظت از این داده‌ها نیست. حفاظت از این داده‌ها به گونه‌ای دیگر و با توجه به ویژگی ذاتی الگوریتم چکیده‌پیام است. در حالت کلی، از بایدهای یک الگوریتم تولیدچکیده پیام این است که پیداکردن دو پیام (با هر طولی) که به چکیده‌پیام یکسانی منتهی شود، از لحاظ محاسباتی غیرممکن باشد. این امر در واقع به معنای محافظت از رشته‌بایت معرف طول است. با توجه به این‌که نوع داده بخش محتوایی به طرز یکتایی مبین رشته‌بایت متعلق به شناسه‌ها است، می‌توان گفت که محافظت از رشته‌بایت متعلق به شناسه‌ها به یکی از دو طریق زیر است:

۱- در نظر گرفتن «نوع داده» به عنوان یکی از صفت‌های احراز هویت شده

۲- استفاده از روش جایگزین سازگار با PEM تبیین شده در بخش ۷-۴ که به معنای از نوع data بودن نوع داده بخش محتوایی می‌باشد.

یادآوری- این‌که گفته می‌شود، الگوریتم تولید چکیده‌پیام بر یک ساختار کدبندی شده به صورت DER اعمال می‌گردد، به معنای الزام بر استفاده از DER در کدبندی داده‌ای که قرار است منتقل شود نیست. در پیاده‌سازی‌هایی که بر اساس این استاندارد انجام می‌شوند و از روش کدبندی دیگری، متفاوت از DER، به جهت ذخیره‌سازی استفاده می‌کنند این امر خللی در محاسبه چکیده‌پیام ایجاد نمی‌کند.

۷-٤ فرآیند رمزبندی چکیده

فرایندی است که یک نوع داده از نوع DigestInfo را که به روش BER کدبندی شده به همراه برونداد فرایند تولید چکیده‌پیام (که از آن تحت عنوان «چکیده‌پیام» نیز یاد می‌شود) و شناسه الگوریتم تولید چکیده‌پیام (یا همان «شناسه») به عنوان درونداد دریافت کرده و آن‌را با استفاده از کلید خصوصی امضاءکننده رمز می‌کند. نمایش BER یک ساختار داده از نوع DigestInfo به صورت زیر است:

```
DigestInfo ::= SEQUENCE {
  digestAlgorithm DigestAlgorithmIdentifier,
```

digest Digest }

Digest ::= OCTET STRING

در ادامه این بخش به تشریح فیلدهای این ساختار داده پرداخته شده است:

- digestAlgorithm : مشخص‌کننده الگوریتم تولید چکیده‌پیام استفاده شده (به جهت تولید چکیده‌پیام از محتویات نوع داده و صفت‌های احراز هویت شده) و همه پارامترهای آن است. این فیلد به طور دقیق همان مقداری را دارد که در فیلد digestAlgorithm از ساختار داده از نوع SinerInfo مافوق درج شده است.
- digest : برونداد فرآیند تولید چکیده‌پیام است.

یادآوری۱–ورودی فرایند رمزبندی چکیده، به طور معمول رشته‌ای متشکل از حداکثر ۳۰ بایت است. با توجه به این‌که طول پیمانه در RSA حداقل برابر ۱۰۲۴ بیت است، در صورتی که فیلد digestEncryptionAlgorithm حاوی شناسه rsaEncryption تعریف شده در PKCS#1 باشد، این رشته را می‌توان فقط در یک بستک رمز کرد. این امر، امری منطقی و سازگار با توصیه‌نامه‌های امنیتی است.

یادآوری۲–وجود شناسه الگوریتم تولید چکیده‌پیام در یک ساختار داده از نوع DigestInfo را می‌توان به عنوان اقدامی مناسب در جهت جلوگیری از عواقب ناشی از لو رفتن یا افشاء یک الگوریتم تولید چکیده‌پیام ارزیابی کرد. به عنوان مثال، مهاجمی را درنظر بگیرید که به ازای یک چکیده‌پیام الگوریتم SHA-1 موجود می‌تواند پیام‌هایی تولید نماید که اعمال الگوریتم SHA-1 بر آن‌ها به برونداد مشابهی منتهی می‌گردد. بدیهی است که این مهاجم به راحتی می‌تواند با یافتن پیامی که چکیده‌پیام SHA-1 مشابهی دارد و در قبل توسط یک امضاءکننده، امضاء شده است و جایگزین کردن این امضای جعلی با امضاء موجود، یک حمله موفق را انجام دهد. در چنین شرایطی، وجود شناسه الگوریتم تولید چکیده‌پیام در ساختار داده از نوع DigestInfo مورد بحث، سبب می‌گردد تا موفقیت مهاجم فقط در حالتی که امضاءکننده در قبل از الگوریتم SHA-1 استفاده کرده است، قابل تصور باشد. افشاء الگوریتم SHA-1 در این‌حالت، هیچ‌گونه مشکلی را برای امضاءکننده‌ای که هیچ‌گاه از الگوریتم SHA-1 استفاده نکرده و همواره از الگوریتم SHA-2 استفاده کرده است در پی نخواهد داشت. در صورت عدم درج شناسه الگوریتم تولید چکیده‌پیام در ساختار داده از نوع DigestInfo مورد بحث، افشای یک الگوریتم تولید چکیده‌پیام (به طور مثال SHA-1)، امنیت تمام امضاءکنندگان (از هر الگوریتم تولید چکیده‌پیامی که استفاده کرده باشد) را در معرض خطر قرار خواهد داد.

یادآوری۲–در یک ساختار داده از نوع DigestInfo مشخص نشده است که آیا فیلد digest فقط حاوی چکیده‌پیام بخش محتوایی است یا این‌که چکیده‌پیام فیلد authenticatedAttributes (که به صورت DER کدبندی شده است) را نیز در بر می‌گیرد و این می‌تواند منجر به ابهام گردد. در این‌حالت مهاجم می‌تواند با تغییر بخش محتوایی (به گونه‌ای که در بردارنده نمایش DER فیلد authenticatedAttributes باشد) و حذف فیلد authenticatedAttributes، وانمود کند که امضاء فقط از روی بخش محتوایی محاسبه شده است. (در حالت کلی، عکس قضیه نیز ممکن است. لازمه این قضیه، امکان تبدیل بخش محتوایی به نمایش DER یک صفت احراز هویت شده است. بدیهی است که این امر، امری غیرمحتمل می‌باشد.) ابهام اشاره شده، مشکل جدیدی نیست. در واقع، در اصل مشکل خاصی نمی‌باشد. چرا که با توجه به قرائن موجود به راحتی می‌توان به وقوع سوءاستفاده‌ای از این دست پی برد. در حالت کلی، یک مهاجم می‌تواند وانمود کرد که امضای موجود بر یک گواهی یا فهرست گواهی باطل شده، فقط به یک نوع داده از نوع امضاءشده تعلق دارد.

۸ نوع داده‌ای «پوشیده»

ساختار داده‌ای مرکب از یک بخش محتوایی رمزشده و کلیدهای مورد نیاز برای رمزبندی آن بخش محتوایی برای یک یا چند گیرنده است. « پاکت دیجیتال»[1] هر دریافت‌کننده، ترکیبی از بخش محتوایی رمز شده اشاره شده در بالا و نسخه رمزشده‌ای از کلید رمزبندی محتوا[2] خواهد بود. هر محتوایی می‌تواند به صورت موازی و برای چند گیرنده پوشیده شود.

به طور معمول یک ساختار داده از نوع پوشیده حاوی پاکت‌های دیجیتال بر روی یک ساختار داده از نوع «داده»، «داده چکیده شده» یا «داده امضاءشده» متعلق به یک یا چند دریافت‌کننده می‌باشد. فرایند ایجاد یک ساختار داده از نوع پوشیده، از مراحل زیر تشکیل شده است:

۱- تولید تصادفی یک کلید رمزبندی محتوا به جهت استفاده در الگوریتمی که قرار است از آن در رمزبندی بخش محتوایی استفاده گردد.

۲- رمزبندی کلید اشاره شده در بند۱ با استفاده از کلید عمومی یکایک دریافت‌کنندگان (در نتیجه به ازای هریک از دریافت‌کنندگان، یک نسخه رمزشده از کلید رمزبندی محتوا خواهیم داشت).

۳- تولید یک ساختار داده از نوع RecipientInfo (به بند ۸-۲ مراجعه شود) به ازای هریک از دریافت کنندگان. (حاوی یکی از نسخه‌های رمزشده کلید رمزبندی محتوا که در مرحله ۲ تولید شده است و اطلاعات مربوط به دریافت‌کننده متناظر با آن)

۴- رمزبندی بخش محتوایی با استفاده از کلید رمزبندی محتوا (همانطور که در بند ۸-۳ نیز بیان شده است، انجام این کار در برخی موارد مستلزم لایه‌گذاری[3] در بخش محتوایی و تبدیل آن به چندین بستک با اندازه خاص خواهد بود)

۵- ایجاد یک ساختار داده از نوع EnvelopedData (به بند ۸-۱ مراجعه شود) که دربردارنده محتوای رمز شده و ساختارهای داده از نوع RecipientInfo برای کلیه دریافت کنندگان است.

گیرنده برای باز کردن پاکت با استفاده از کلید خصوصی خود یکی از کلیدهای رمزبندی محتوا را رمزگشایی کرده و با استفاده از آن محتوای رمز شده را رمزگشایی می‌کند. کلید خصوصی گیرنده شامل شناسه منحصر به فرد صادرکننده و یک شماره ترتیب مختص صادر کننده است که به طور انحصاری گواهی مربوط به کلید عمومی متناظر با آن کلید خصوصی را مشخص می‌کند.

---

1 - Digital Envelope

2 - content-encryption key

۲- همان کلیدی است که از آن برای رمزبندی بخش محتوایی استفاده شده است. یک دریافت‌کننده مجاز می‌تواند با استفاده از کلید خصوصی خود نسبت به رمزگشایی یکی از نسخه‌های رمزشده موجود از کلید رمزبندی محتوا و بازیابی آن اقدام کند.

3 - Padding

این بخش از چهار قسمت تشکیل شده است. در ابتدا به بررسی یک ساختار داده سطح بالا از نوع EnvelopedData پرداخته شده است. در ادامه به بررسی ساختارهای داده از نوع RecipientInfo که هر یک دربردارنده اطلاعات یکی از دریافت‌کنندگان پیام می‌باشند، پرداخته شده است. قسمت‌های سوم و چهارم این بخش نیز به ترتیب به بررسی فرایندهای رمزبندی بخش محتوایی و رمزبندی کلید رمز، اختصاص یافته است.

علی‌رغم این‌که سازگاری کاملی بین برخی از فرایندهای تعریف شده در این بخش و فرایندهای معادل در PEM وجود دارد، ساختار داده تعریف‌شده در این بخش فاقد سازگاری لازم با PEM است. این امر از آن رو است که در PEM همواره از امضای دیجیتالی استفاده شده و هیچگاه به تنهایی از پاکت دیجیتال استفاده نمی‌گردد.

۱-۸ EnvelopedData

نمایش ASN.1 یک داده از نوع «پوشیده‌شده» به صورت زیر است:

```
EnvelopedData ::= SEQUENCE {
  Version Version,
  recipientInfos RecipientInfos,
  encryptedContentInfo EncryptedContentInfo }

RecipientInfos ::= SET OF RecipientInfo

EncryptedContentInfo ::= SEQUENCE {
  contentType ContentType,
  contentEncryptionAlgorithm
    ContentEncryptionAlgorithmIdentifier,
encryptedContent
   [0] IMPLICIT EncryptedContentOPTIONAL }

EncryptedContent ::= OCTET STRING
```

در زیر به تبیین فیلدهای این ساختار داده پرداخته شده است:

- version : مشخص می‌کند که در تنظیم فیلدهای ساختار داده بر مبنای کدام ویرایش از استاندارد عمل شده است. در صورتی که از ویرایش حاضر استاندارد استفاده شده باشد، این فیلد با مقدار 0 پر می‌شود.

- recipientInfos : یک مجموعه از اطلاعات یکایک دریافت‌کنندگان پیام است. در حالت کلی این مجموعه باید دربردارنده نام حداقل یکی از دریافت‌کنندگان باشد.

- encryptedContentInfo : حاوی اطلاعاتی در مورد بخش محتوایی است (که رمز شده است). در زیر به تبیین فیلدهای این ساختارداده پرداخته شده است:

- contentType : نوع ساختارداده بخش محتوایی است (ساختارداده‌ای که رمز شده) را مشخص می‌کند.
- contentEncryptionAlgorithm : الگوریتم استفاده شده در رمزبندی بخش محتوایی (و پارامترهای آن) را مشخص می‌کند. فرایند رمزبندی بخش محتوایی در بخش ۸-۳ شرح داده شده است.
- encryptedContent : فیلدی اختیاری است که دربردارنده رشته حاصله از رمزبندی بخش محتوایی است. بدیهی است درحالتی‌که این فیلد وجود ندارد، اطلاعات آن باید به طریقی دیگر منتقل گردد.

یادآوری- قرارگرفتن فیلد recipientInfos در قبل از فیلد encryptedContentInfo، پردازش یک‌مرحله‌ای یک ساختار داده از نوع EnvelopedData را به امری ممکن تبدیل کرده است.

۸-۲ RecipientInfo

این ساختار داده، دربردارنده اطلاعات یکی از دریافت‌کنندگان پیام بوده و نمایش ASN.1 آن به صورت زیر است:

```
RecipientInfo ::= SEQUENCE {
  version Version,
  issuerAndSerialNumber IssuerAndSerialNumber,
  keyEncryptionAlgorithm
    KeyEncryptionAlgorithmIdentifier,
  encryptedKey EncryptedKey }

EncryptedKey ::= OCTET STRING
```

در ادامه این بخش به تبیین فیلدهای این ساختار داده پرداخته شده است:

- version : مشخص می‌کند که در تنظیم فیلدهای ساختار داده بر مبنای کدام ویرایش از استاندارد عمل شده است. در صورتی که از ویرایش حاضر استاندارد استفاده شده باشد، این فیلد با مقدار 0 پر می‌شود.
- issuerAndSerialNumber: گواهی دریافت‌کننده (و در نتیجه شناسه منحصر به فرد دریافت‌کننده و کلید عمومی او) را مشخص می‌کند، این کار را با استفاده از شناسه منحصر به فرد صادرکننده گواهی و شماره ترتیب مختص صادر کننده گواهی انجام می‌دهد.
- KeyEncryptionAlgorithm: شناسه (و دیگر پارامترهای وابسته) الگوریتم رمزبندی است که از آن به جهت رمزبندی کلید رمزبندی محتوا (با استفاده از کلید عمومی دریافت‌کننده) استفاده شده است. در بخش ۸-۴ به تبیین فرایند رمزبندی کلید رمزبندی پرداخته شده است.
- encryptedKey: رشته حاصل از رمزبندی کلید رمزبندی بخش محتوایی با استفاده از کلید عمومی دریافت‌کننده است.

۳-۸ فرآیند رمزبندی بخش محتوایی

ورودی این فرایند، همان مقداریست که قرار است در یک ساختار داده از نوع پوشیده جاسازی گردد. در یک بیان دقیق‌تر ورودی، رشته بایت‌های حاصل از کدبندی به صورت BER با طول مشخص اطلاعات موجود در فیلد content از ساختار داده از نوع ContentInfo (که قرار است در یک ساختار داده از نوع پوشیده جاسازی گردد) است. فقط رشته بایتی (که به صورت BER کدبندی شده است) رمزبندی می‌شود و رشته بایت‌های دیگری مانند رشته بایت معرف طول یا رشته‌بایت متعلق به شناسه‌ها رمز نمی‌شوند.

در حالتی که بخش محتوایی (که قرار است در یک ساختار داده از نوع «پوشیده» جاسازی گردد) دارای ساختار داده‌ای از نوع «داده» می‌باشد، الگوریتم رمزبندی اشاره شده فقط بر داده موجود (به طور مثال محتویات یک فایل) اعمال می‌شود. از مزایای این امر عدم نیاز به اطلاع از طول بخش محتوایی است که قرار است رمز شود تا پیش از انجام فرایند رمزبندی شود. این روش سازگاری کاملی با PEM دارد.

در حالت کلی، رشته‌های بایتی معرف طول و رشته‌های بایتی متعلق به شناسه‌ها رمز نمی‌شوند. بسته به الگوریتم رمزبندی ممکن است از سازوکار خاصی برای محافظت از رشته‌های بایتی معرف طول استفاده شود. از رشته‌های بایتی متعلق به شناسه‌ها نیز محافظت نمی‌شود اما با فرض این‌که ساختار داده می‌تواند به طرز یکتایی مبین رشته‌های بایتی متعلق به شناسه‌ها باشد، می‌توان از ساختار داده آن‌ها را بازیابی کرد. حفاظت کامل رشته‌های بایتی معرف طول و رشته‌های بایتی متعلق به شناسه‌ها، مستلزم استفاده از یک ساختار داده از نوع امضاء و پوشیده‌شده و یا استفاده هم‌زمان از یک ساختار داده از نوع پوشیده‌شده و یک ساختار داده از نوع چکیده‌شده خواهد بود.

یادآوری۱–در یک ساختار داده از نوع «پوشیده»، بیتی که برای مشخص کردن نوع کدبندی به کار می‌رود (این‌که از کدبندی با طول شخص یا کدبندی با طول نامشخص استفاده شده است) در جایی ذخیره نمی‌شود و در نتیجه برای جلوگیری از ابهام، از کدبندی BER با طول مشخص استفاده می‌شود. در این‌جا با توجه به این‌که برای ساختارهای داده ساده‌ای مانند رشته‌های بایتی استفاده از کدبندی با طول مشخص مناسب‌تر می‌باشد، بر استفاده از کدبندی BER با طول مشخص تاکید شده است.

یادآوری۲–در برخی از الگوریتم‌های رمزبندی محتوا فرض می‌شود که طول ورودی مضربی از k بایت (k>1) است و ورودی که طول آن مضرب صحیحی از k بایت نمی‌باشد به نوعی اصلاح می‌گردد. برای استفاده از این الگوریتم‌ها برای یک رشته ورودی به طول ℓ، باید k-(ℓ mod k) بایت حاوی مقدار k-(ℓ mod k) به انتهای آخرین بلوک ورودی اضافه گردد. این امر بدین معناست که از یکی از رشته‌های زیر برای لایه‌گذاری بلوک آخر ورودی استفاده می‌شود:

01 — if $l \bmod k = k\text{-}1$
02 02 — if $l \bmod k = k\text{-}2$
.
.
.
$k\ k \ldots k\ k$ — if $l \bmod k = 0$

با توجه به این‌که تمام ورودی‌ها لایه‌گذاری شده‌اند و هیچیک از رشته‌هایی که بدین منظـور اسـتفاده شـده است پیشوند دیگری نمی‌باشند، می‌توان به راحتی و بدون هیچگونه ابهامی نسبت به حذف بایت‌های الحاقی اقدام کرد. از این روش لایه‌گذاری فقط می‌توان در حالتی که $k<256$ می‌باشد استفاده کرد. بـه ازای مقـادیر بزرگتر k نیازمند استفاده از روش‌های دیگری می‌باشیم که باید در مطالعات آینده به آن پرداخته شود.

٤-٨ فرایند رمزبندی کلید رمز

کلید رمزبندی محتوا را می‌توان تنها مقدار ورودی یک فرایند رمزبندی کلید رمز دانست (الگوریتمی که یک دریافت‌کننده از آن برای رمزبندی کلید استفاده می‌کند).

۹ نوع داده‌ای «امضاءشده و پوشیده»

در این بند از استاندارد، به تبیین یک ساختار داده از نوع «امضاءشده و پوشیده» پرداخته شـده اسـت. یـک ساختار داده از نوع امضاءشده و پوشیده، ساختار داده‌ای مرکب از یک بخش محتوایی رمزشده، چکیـده‌پیـام رمز شده (که دو بار رمزبندی شده) برای یک یا چند امضاءکننده و نسخه رمزشـده از کلیـدهای رمزبنـدی محتوا برای یک یا چند دریافت‌کننده است. کلید خصوصی امضاءکننـده و کلیـد رمزبنـدی محتـوا دو کلیـد رمزبندی هستند که به ترتیب در این عملیات «رمزبندی دوگانه»[1] مورد استفاده قرار می‌گیرند.

ترکیب بخش محتوایی رمز شده و نسخه رمزشده‌ای از کلید رمزبندی محتوا که توسـط یـک دریافـت‌کننـده قابل رمزگشایی می‌باشد، «پاکت دیجیتال» آن دریافت‌کننده را تشکیل می‌دهد. چکیده‌پیام رمزشده‌ای که به ازای یک امضاءکننده بازیابی می‌گردد، «امضاء دیجیتالی» آن امضاءکننده بر روی محتوای بازیابی شده است. هر محتوایی می‌تواند به صورت موازی توسط هر تعداد امضاکننده، امضا و برای هـر تعـداد گیرنـده، پوشـیده شود.

کاربرد یک ساختار داده از نوع امضاءشده و پوشیده، نمایش امضاء دیجیتالی (متعلق به یک امضاءکننـده) و پاکت‌های دیجیتال (متعلق به یک یا چند دریافت‌کننده) بوده که به بخش محتوایی با ساختار داده از نـوع «داده» اعمال می‌شود.

فرایند ایجاد یک ساختار داده از نوع امضاءشده و پوشیده، از مراحل زیر تشکیل می‌گردد:

۱- تولید تصادفی یک کلید رمزبندی محتوا به جهت استفاده در الگوریتمی که قرار است از آن در رمزبندی بخش محتوایی استفاده گردد(کلید رمزبندی محتوا).

۲- رمزبندی کلید رمزبندی اشاره شده، با استفاده از کلید عمومی یکایک دریافت‌کنندگان (در نتیجه به ازای هریک از دریافت‌کنندگان، یک نسخه رمزشده از کلید رمزبندی محتوا خواهیم داشت).

1 - Double Encryption

۳- تولید یک ساختار داده از نوع RecipientInfo (به بند ۸-۲ مراجعه شود) به ازای هریک از دریافت کنندگان (حاوی یکی از نسخه‌های رمزشده کلید رمزبندی محتوا که در مرحله ۲ تولید شده است و اطلاعات مربوط به دریافت‌کننده متناظر با آن).

۴- محاسبه چکیده‌پیام بخش محتوایی با استفاده از الگوریتم چکیده پیام خاص هریک از امضاءکنندگان (البته در حالتی که دو امضاءکننده از الگوریتم تولید چکیده‌پیام یکسانی استفاده می‌کنند، دیگر نیازی به دوبار محاسبه چکیده‌پیام نبوده و کافی است که چکیده‌پیام فقط به ازای یکی از امضاءکنندگان محاسبه گردد).

۵- رمزبندی چکیده‌پیام اشاره شده و دیگر اطلاعات مربوط به آن با استفاده از کلید خصوصی یکایک امضاء-کنندگان و رمزبندی هریک از رشته‌های حاصله با استفاده از کلید رمزبندی محتوا که در مرحله ۱ تولید شده است (همانطور که در بخش ۸-۳ نیز تشریح شده است، یکی از الزامات احتمالی در انجام این رمزبندی ثانویه، لایه‌گذاری رشته حاصل از رمزگذاری اولیه و تبدیل آن به تعدادی بستک با طول مشخص می‌باشد).

۶- تولید یک ساختار داده از نوع signerInfo (به بند ۷-۲ مراجعه شود) به ازای هریک از امضاءکنندگان (حاوی چکیده‌پیامی که دو بار رمز شده و در مرحله ۵ تولید شده است و اطلاعات مربوط به امضاءکننده متناظر با آن).

۷- رمزبندی بخش محتوایی با استفاده از کلید رمزبندی محتوا (فرایند رمزبندی بخش محتوایی، در بخش ۸-۳ شرح داده شده است).

۸- ایجاد یک ساختار داده از نوع SignedAndEnvelopedData (به بند ۹-۱ مراجعه شود) که دربردارنده الگوریتم‌های تولید چکیده‌پیام متناظر با تمام امضاءکنندگان، ساختارهای داده از نوع SignerInfo متناظر با یکایک امضاءکنندگان، ساختارهای داده از نوع RecipientInfo متناظر با یکایک دریافت‌کنندگان و نسخه رمزشده بخش محتوایی است.

دریافت یک پاکت دیجیتال و بررسی امضاءهای موجود در آن توسط گیرنده، فرایندی دو مرحله‌ای دارد:

- استفاده از کلید خصوصی دریافت‌کننده برای رمزگشایی مقدار رمزشده یکی از کلیدهای رمزبندی محتوا ، محاسبه کلید رمزبندی محتوا و استفاده از آن در رمزگشایی بخش محتوایی رمزشده
- چکیده پیام‌هایی که برای هر امضاکننده بصورت دو مرحله‌ای رمزبندی شده‌اند با کلید رمزبندی محتوی (حاصل از مرحله قبل)، رمزگشایی شده و نتیجه با استفاده از کلید عمومی امضاکننده رمزگشایی می-گردد. در نهایت چکیده پیام حاصله با چکیده‌پیامی که به طورمستقل از روی پیام محاسبه شده، مقایسه می‌گردد.

.

این بخش از دو قسمت تشکیل شده است. در ابتدا به بررسی کلی و سطح بالای یک ساختار داده از نوع SignedAndEnvelopedData و سپس به بررسی فرایند رمزبندی چکیده‌پیام پرداخته شده است. به جهت رعایت اختصار، از بررسی مجدد ساختارهای داده و فرایندهایی که در قبل تشریح شده‌اند خودداری شده است.

یادآوری- از بعد رمزنگشاتی، یک ساختار داده از نوع امضاءشده و پوشیده را می‌توان متناظر با استفاده متوالی از یک ساختار داده از نوع امضاء شده و یک ساختار داده از نوع پوشیده دانست. اما از آنجا که یک ساختار داده از نوع امضاءشده و پوشیده فاقد صفت‌های احراز هویت شده و صفت‌های احراز هویت نشده بوده و در آن فقط به رمزبندی (به معنای لحاظ کردن در تولید پوشیده دیجیتال) امضای دیجیتالی یک امضاءکننده بسنده می‌گردد (دیگر اطلاعات امضاءکننده در تولید پاکت دیجیتال لحاظ نمی‌گردد) در نتیجه استفاده ترتیبی از یک ساختار داده از نوع امضاء شده و یک ساختار داده از نوع پوشیده، مزایای بیشتری نسبت به استفاده از یک ساختار داده از نوع امضاءشده و پوشیده خواهد داشت مگر این‌که هدف، سازگاری با فرایند رمزبندی براساس PEM باشد.

۱-۹ SignedAndEnvelopedData

نمایشASN.1 یک داده از نوع «رمزشده و پوشیده» به صورت زیر است:

```
SignedAndEnvelopedData ::= SEQUENCE {
  version Version,
  recipientInfos RecipientInfos,
  digestAlgorithms DigestAlgorithmIdentifiers,
  encryptedContentInfo EncryptedContentInfo,
  certificates
    [0] IMPLICIT ExtendedCertificatesAndCertificates

OPTIONAL,
  crls
    [1] IMPLICIT CertificateRevocationLists OPTIONAL,
  signerInfos SignerInfos }
```

در زیر به تبیین فیلدهای این ساختار داده پرداخته شده است:

- version : مشخص می‌کند که در تنظیم فیلدهای ساختار داده بر مبنای کدام ویرایش از استاندارد عمل شده است. در صورتی که از ویرایش حاضر استاندارد استفاده شده باشد، این فیلد با مقدار 1 پر می‌شود.
- recipientInfos : حاوی اطلاعات یکایک دریافت‌کنندگان پیام می‌باشد. در حالت کلی، این فیلد باید دربردارنده نام حداقل یکی از دریافت‌کنندگان باشد.
- digestAlgorithms: در بردارنده شناسه‌های متعلق به الگوریتم‌های تولید چکیده‌پیام است. فرایند تولید چکیده‌پیام مورد بحث در این‌جا را می‌توان متناظر با فرایند تولید چکیده‌پیام معرفی شده در بخش ۷ در حالتی‌که هیچ صفت احراز هویت شده‌ای وجود ندارد دانست.

- encryptedContentInfo: طبق بند ۸، حاوی نسخه رمزشده بخش محتوایی است(که هر نوع ساختار داده‌ای می‌تواند داشته باشد).
- certificates: طبق بند ۷، حاوی تعدادی گواهی X.509 و گواهی PKCS#6 توسعه‌یافته است.
- crls : طبق بند ۷، حاوی مجموعه‌ای از فهرست‌های گواهی باطل‌شده است.
- signerInfos : حاوی اطلاعات یکایک امضاءکنندگان است. در حالت کلی باید حداقل یک عنصر در این فیلد وجود داشته باشد. مقادیر SignerInfo به استثنای فیلد encryptedDigesst مشابه بخش ۷ می باشند.

یادآوری-قرارگرفتن فیلدهای recipientInfos و digestAlgorithms در قبل از فیلد contentInfo و قرارگرفتن فیلد SignerInfos در بعد از آن، پردازش یک‌مرحله‌ای یک ساختار داده از نوع SignedAndEnvelopedData را ممکن کرده است.

۹-۲ فرایند رمزبندی چکیده

علی‌رغم شباهتی که بین ورودی این فرایند و فرایند رمزبندی چکیده بیان شده در بند ۷ وجود دارد، روند کار کاملا متفاوت است. فرایند رمزبندی چکیده مورد بحث در این‌جا، فرایندی دو مرحله‌ای است. ابتدا طبق بند ۷، ورودی فرایند به الگوریتم رمزبندی چکیده متعلق به امضاکننده اعمال می‌شود. در ادامه، از کلید رمزبندی محتوا برای رمزبندی برونداد مرحله اول استفاده می‌گردد. درونداد مرحله دوم فرایند، همان مقدار برونداد مرحله اول فرایند بوده و هیچگونه کدبندی DER (طبق بند ۸-۳) مجددی نیاز نیست. درحالت کلی، سازگاری کاملی بین این فرایند و فرایند رمزبندی براساس PEM وجود دارد.

یادآوری- پوشاندن چکیده‌پیام بخش محتوایی از دید مهاجم را می‌توان نتیجه مستقیم مرحله دوم رمزبندی اشاره شده دانست. عدم استفاده از چنین رمزبندی موجب می‌گردد که مهاجم بتواند با مقایسه چکیده پیام موجود و چکیده‌پیام واقعی، از صحت بخش محتوایی (به طور مثال به صورت «بله» یا «خیر») مطلع گردد.

۱۰ نوع داده‌ای «چکیده شده»

ساختار داده‌ای متشکل از یک بخش محتوایی (که هر نوع ساختار داده‌ای می‌تواند داشته باشد) و چکیده پیام آن بخش محتوایی است. از متداول‌ترین کاربردهای یک ساختار داده از نوع «چکیده شده»، می‌توان به کاربرد آن در افزودن یکپارچگی به یک ساختار داده از نوع «داده» به منظور استفاده (به عنوان بخش محتوایی) در یک ساختار داده از نوع پوشیده اشاره کرد. فرایند ایجاد یک ساختار داده از نوع چکیده‌شده، شامل مراحل زیر است:

۱- محاسبه چکیده‌پیام بخش محتوایی با استفاده از یک الگوریتم تولید چکیده‌پیام.

۲- تولید یک ساختار داده از نوع DigestedData (حاوی بخش محتوایی، چکیده‌پیام و الگوریتم تولید چکیده پیام)

گیرنده با مقایسه چکیده‌پیام دریافتی و چکیده‌پیامی که به‌طورمستقل از روی پیام دریافتی متناظر محاسبه می‌گردد، صحت و سقم چکیده‌پیام دریافتی را وارسی می‌کند.
نمایشASN.1 یک داده از نوع " چکیده شده" به صورت زیر است:

```
DigestedData ::= SEQUENCE {
  version Version,
  digestAlgorithm DigestAlgorithmIdentifier,
  contentInfo ContentInfo,
  digest Digest }

Digest ::= OCTET STRING
```

در زیر به تبیین فیلدهای این ساختار داده پرداخته شده است:

- version: مشخص می‌کند که در تنظیم فیلدهای ساختار داده بر مبنای کدام ویرایش از استاندارد عمل شده است. در صورتی که از ویرایش حاضر استاندارد استفاده شده باشد، این فیلد با مقدار 0 پر می‌شود.
- digestAlgorithm: شناسه (و دیگر پارامترهای آن) الگوریتمی است که در محاسبه چکیده‌پیام بخش محتوایی مورد استفاده قرار گرفته است. (فرایند تولید چکیده‌پیام مورد بحث در این‌جا را می‌توان متناظر با فرایند تولید چکیده‌پیام معرفی شده در بخش ۷ در حالتی‌که هیچ صفت احراز هویت شده‌ای وجود ندارد دانست.)
- contentInfo: چکیده‌پیام از روی این بخش از ساختار داده محاسبه می‌گردد. در حالت کلی، محدودیتی در مورد نوع ساختار داده این بخش وجود ندارد و این بخش می‌تواند داده‌ای از نوع «داده»، «امضا شده»، «پوشیده»، «امضاءشده و پوشیده»، «چکیده شده»، و یا «رمزشده» باشد.
- digest: برونداد فرایند تولید چکیده‌پیام است.

یادآوری- قرارگرفتن فیلد digestAlgorithms در قبل از فیلد contentInfo و قرارگرفتن فیلد digest در بعد از آن، پردازش یک‌مرحله‌ای یک ساختار داده از نوع DigestedData را ممکن کرده است.

۱۱ نوع داده‌ای «رمزشده»

ساختار داده‌ای متشکل از یک بخش محتوایی (با هر نوع ساختار داده) رمزشده است. برخلاف یک ساختار داده از نوع پوشیده‌شده، در این‌جا از هیچ دریافت‌کننده‌ای نام برده نشده و هیچ نسخه رمزشده‌ای از کلید رمزبندی محتوا نیز موجود نیست. بنابراین مدیریت کلید در این‌جا مستلزم استفاده از یک مجموعه روش‌های دیگر خواهد بود.

از متداول‌ترین کاربردهای یک ساختار داده از نوع «رمزشده» می‌توان به کاربرد آن (در مواقعی که کلید رمزبندی یک کلمه عبور است) در رمزبندی ساختار داده از نوع داده برای ذخیره‌سازی محلی اشاره کرد.
نمایشASN.1 یک داده از نوع «رمزشده» به صورت زیر است:

```
EncryptedData ::= SEQUENCE {
  version Version,
  encryptedContentInfo EncryptedContentInfo }
```

در زیر به تبیین فیلدهای این ساختار داده پرداخته شده است:

- version: مشخص می‌کند که در تنظیم فیلدهای ساختار داده بر مبنای کدام ویرایش از استاندارد عمل شده است. در صورتی که از ویرایش حاضر استاندارد استفاده شده باشد، این فیلد با مقدار 0 پر می‌شود.
- encryptedContentInfo: طبق بند ۸، حاوی نسخه رمزشده بخش محتوایی است (که هر نوع ساختار داده‌ای می‌تواند داشته باشد).

۱۲ نوع داده‌ای «احرازهویت شده»

نوع داده‌ای AuthenticatedData شامل هر نوع محتوا، یک کد احرازهویت پیام (MAC)[1] و کلیدهای احرازهویت رمز شده برای یک یا چند گیرنده است. ترکیب MAC و یک کلید احرازهویت رمز شده، جهت بررسی تمامیت محتوای احرازهویت شده برای یک گیرنده ضروری است. محافظت از یکپارچگی هر نوع محتوایی برای هر تعداد گیرنده امکان‌پذیر است.

فرایند ایجاد ساختار احرازهویت شده شامل مراحل زیر است:

۱- یک کلید احرازهویت پیام برای یک الگوریتم احرازهویت پیام به طور تصادفی تولید می‌شود.

۲- کلید احرازهویت پیام برای هر گیرنده رمز می‌شود.

۳- کلید احرازهویت پیام رمز شده و سایر اطلاعات مختص به گیرنده، برای هر گیرنده در ساختار RecipientInfo (طبق بند ۸-۲) قرار داده می‌شود.

۴- مبدأ پیام با استفاده از کلید احرازهویت پیام، مقدار MAC را بر روی محتوا محاسبه می‌کند. اگر مبدأ پیام علاوه بر محتوا بخواهد از یکپارچگی اطلاعات دیگری نیز محافظت کند، ابتدا چکیده پیام محتوا را محاسبه کرده سپس چکیده محتوا را در کنار سایر اطلاعات قرار داده و مقدار MAC را با استفاده از کلید احراز اصالت پیام به دست می‌آورد.

برای بررسی یکپارچگی پیام ارسالی، مقدار MAC محاسبه شده در سمت گیرنده باید برابر با مقدار فیلد mac از ساختار داده AuthenticatedData باشد.

نمایش ASN.1 یک داده از نوع « احرازهویت شده» به صورت زیر است:

1 - Message authentication code

```
AuthenticatedData ::= SEQUENCE {
version                                 CMSVersion,
originatorInfo              [0]         IMPLICIT OriginatorInfo OPTIONAL,
recipientInfos                          RecipientInfos,
macAlgorithm                            MessageAuthenticationCodeAlgorithm,
digestAlgorithm             [1]         DigestAlgorithmIdentifier OPTIONAL,
ContentInfo                             ContentInfo,
authAttrs                   [2]         IMPLICIT AuthAttributes OPTIONAL,
mac                                             MessageAuthenticationCode,
unauthAttrs                 [3]         IMPLICIT UnauthAttributes OPTIONAL }

AuthAttributes ::= SET SIZE (1..MAX) OF Attribute
UnauthAttributes ::= SET SIZE (1..MAX) OF Attribute
MessageAuthenticationCode ::= OCTET STRING
```

در زیر به تبیین فیلدهای این ساختار داده پرداخته شده است:

- version: مشخص می‌کند که در تنظیم فیلدهای ساختار داده بر مبنای کدام ویرایش از استاندارد عمل شده است.
- originatorInfo: یک فیلد اختیاری است که اطلاعاتی در مورد منبع پیام در اختیار قرار می‌دهد. این فیلد ممکن است حاوی گواهی‌ها و فهرست گواهی‌های باطل شده باشد.
- recipientInfos: این فیلد مجموعه‌ای از اطلاعات هر گیرنده است. حداقل باید اطلاعات یک گیرنده در این فیلد وجود داشته باشد.
- macAlgorithm: یک شناسه الگوریتم کد احرازهویت پیام (MAC) است. این فیلد الگوریتم MAC و پارامترهای مربوط به آن را که توسط مبدأ مورد استفاده قرار گرفته است، مشخص می‌کند. قرارگیری این فیلد پردازش یک مرحله‌ای توسط گیرنده را تسهیل می‌کند.
- digestAlgorithm: شناسه (و دیگر پارامترهای وابسته) الگوریتمی است که در محاسبه چکیده‌پیام بخش محتوایی (فیلد contentInfo) و اطلاعات موجود در فیلد authenticatedAttributes مورد استفاده قرار گرفته است. در بخش ۷-۳ به تبیین فرایند تولید چکیده‌پیام پرداخته شده است.
- contentInfo: مقداری است که احراز اصالت می‌شود.
- authAttrs: دربردارنده مجموعه صفت‌هایی می‌باشد که توسط احرازهویت کننده، تایید شده است. در حالت کلی، این فیلد را می‌توان یک فیلد اختیاری دانست اما درحالتی که ContentInfo (از ساختار داده از نوع AuthenticatedData فوق) نوع داده‌ای غیر از نوع «داده» داشته باشد، وجود این فیلد الزامی می‌گردد. این فیلد، در صورت وجود، حداقل حاوی دو صفت خواهد بود:
  - یک صفت از نوع «content-type» که در استاندارد PKCS#9 تعریف شده و حاوی نوع داده ContentInfo است که احرازاصالت می‌شود.

- یک صفت از نوع «message-digest» که در PKCS#9 تعریف شده است و حاوی چکیده‌پیام محتوای استفاده شده است.

– mac: کد احراز اصالت پیام است.

– unauthAttrs : فیلدی اختیاری بوده و دربردارنده مجموعه صفت‌هایی است که احرازهویت شده نمی-باشند یعنی امضاءشده و مستند نیستند.

۱۳ شناسانه‌ها

شناسانه‌های data، signedData، envelopedData، signedAndEnvelopedData، digestedData، encryptedData و authenticatedData، شناسانه‌های هفت‌گانه‌ای هستند که بر اساس استاندارد حاضر می-توان از آن‌ها استفاده کرد.
شناسه pkcs-7، مشخص‌کننده استاندارد حاضر است:

```
pkcs-7 OBJECT IDENTIFIER ::=
{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 7 }
```

شناسانه‌های data، signedData، envelopedData، signedAndEnvelopedData، digestedData، encryptedData و authenticatedData نیز به ترتیب مبین ساختارهای داده از نوع «داده»، «امضا شده»، «پاکت شده»، «امضا و پاکت شده»، « چکیده شده» و «رمزشده» است(که در بندهای قبلی به آن‌ها اشاره شد):

```
data OBJECT IDENTIFIER ::= { pkcs-7 1 }
signedData OBJECT IDENTIFIER ::= { pkcs-7 2 }
envelopedData OBJECT IDENTIFIER ::= { pkcs-7 3 }
signedAndEnvelopedData OBJECT IDENTIFIER ::= { pkcs-7 4 }
digestedData OBJECT IDENTIFIER ::= { pkcs-7 5 }
encryptedData OBJECT IDENTIFIER ::= { pkcs-7 6 }
authenticatedData OBJECT IDENTIFIER ::= {id-pkcs 9 16 1 2}
```

فیلد contentType از یک ساختار داده از نوع ContentInfo است باید همواره حاوی یکی از شش شناسانه فوق باشد. شناسانه‌ای که در این فیلد قرار می‌گیرد، ساختار ASN.1 داده‌ای که در فیلد content قرار گرفته است (از ساختار داده از نوع ContentInfo اشاره شده) را به طوردقیق مشخص می‌کند. این شناسانه در واقع مشخص می‌کند که فیلد content حاوی کدامیک از انواع داده Data، SignedData، EnvelopedData، SignedAndEnvelopedData، EncryptedData،DigestedData یا authenticatedData است. از دیگر موارد کاربرد این شناسانه‌ها، می‌توان به کاربرد آن‌ها در صفت‌های از نوع «نوع‌محتوا» در PKCS#9 اشاره کرد.