INSO
14634
1st. Edition

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

استاندارد ملی ایران
۱۴۶۳۴
چاپ اول

بررسی موضوعات الگوریتم احراز هویت و یکپارچگی

AUTHENTICATION/INTEGRITY ALGORITHM ISSUES SURVEY

ICS: 33

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 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

"بررسی موضوعات الگوریتم احراز هویت و یکپارچگی"

رئیس:	**سمت و/ یا نمایندگی**
راعی، جلال (دکترای مدیریت)	کارشناس استاندارد
دبیر:	
نجاتی جهرمی، منصور (دکتری برق مخابرات)	عضو هیات علمی دانشگاه علوم و فنون هوایی شهید ستاری – کارشناس استاندارد
اعضاء: (اسامی به ترتیب حروف الفبا)	
اکبر زاده، هومن (کارشناس ارشد برق-الکترونیک)	عضو هیات علمی دانشگاه علوم و فنون هوایی شهید ستاری
ذره، مهدی (کارشناس ارشد برق)	کارشناس استاندارد
سازدار، امیرمهدی (کارشناس ارشد برق مخابرات)	عضو هیات علمی دانشگاه علوم و فنون هوایی شهید ستاری
سلکی، سعید (کارشناس ارشد برق الکترونیک)	مدیر مطالعات راهبردی دفتر تحقیقات و مطالعات نظری نهاجا
علیمحمدی، علیرضا (کارشناس ارشد مدیریت)	مرکز تحقیقات و جهادخودکفائی دانشگاه علوم و فنون هوایی شهید ستاری
مردیان، ساسان (کارشناس ارشد مهندسی پزشکی)	مدرس دانشگاه علوم و فنون هوایی شهید ستاری
نفری، منا (کارشناس ارشد برق-الکترونیک)	کارشناس شرکت کیمیا پخش شرق

فهرست مندرجات

عنوان		صفحه
آشنایی با سازمان ملی استاندارد ایران		ب
کمیسیون فنی تدوین استاندارد		ج
پیش گفتار		ه
۱	هدف و دامنهٔ کاربرد	۱
۲	مراجع الزامی	۱
۳	کوته نوشته‌ها، اصطلاحات و تعاریف	۲
۴	الگوریتم‌های مناسب مورد پذیرش CCSDS (بر اساس دسته‌بندی)	۴
۴-۱	الگوریتم‌های امضای دیجیتال	۵
۴-۲	کدهای احرازهویت پیام مبتنی بر توابع درهم‌ساز(HMAC)	۶
۴-۳	کدهای احرازهویت پیام مبتنی بر رمزنگاری	۷
۵	خلاصه و نتیجه‌گیری	۸

پیش گفتار

استاندارد "بررسی موضوعات الگوریتم احراز هویت و یکپارچگی" که پیش نویس آن درکمیسیون‌های مربوط توسط مرکز تحقیقات و جهاد دانشگاه علوم و فنون هوایی شهید ستاری تهیه و تدوین شده و در صد و پانزدهمین اجلاس کمیتهٔ ملی استاندارد مخابرات مورخ ۱۳۹۱/۰۳/۲۳ مورد تصویب قرار گرفته است ، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی 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 زمینهٔ 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 تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

[1] Authentication/Integrity Algorithm Issues Survey. Report Concerning Space Data System Standards, CCSDS 350.3-G-1. Green Book, Washington, DC, USA. March 2008.

بررسی موضوعات الگوریتم احراز هویت و یکپارچگی

۱ هدف و دامنهٔ کاربرد

این استاندارد بیانگر بررسی‌های انجام شده توسط "گروه کاری امنیتی[1] (SecWG)" در "کمیته‌ی مشاوره‌ای سامانه‌ی داده‌ی فضایی[2] (CCSDS)" است، که برای تدوین استانداردهای الگوریتم‌های مطرح استاندارد CCSDS در احراز هویت و یکپارچگی، فعالیت‌های گسترده‌ای داشته است. این الگوریتم می‌تواند توسط تمام اعضای آژانس‌های هوافضایی برای احرازهویت و یکپارچگی در فرمان از دور (لینک یا پیوند بالا رونده) مانند آماده سازی داده یا اطلاعات ماموریت در سنجش از دور (لینک یا پیوند پایین رونده) استفاده شوند.

یک الگوریتم برای تامین هر دو عامل احراز هویت و یکپارچگی ارائه می‌شود، در این صورت الگوریتم یکپارچگی به سادگی به عنوان یک اثر جانبی از الگوریتم احراز هویت حاصل می‌شود.

احرازهویت خدمتی را فراهم می‌کند که به وسیله‌ی آن گیرنده بتواند منبع ارسال اطلاعات را تایید و یقین حاصل کند که داده‌ها از منبع ادعا کننده ارسال شده‌اند. یکپارچگی نیز خدمتی را فراهم می‌کند که باعث می‌شود گیرنده یقین کند، داده‌های دریافتی همان داده‌های ارسالی از سوی فرستنده است و هیچ نوع تغییری (تصادفی یا عمدی) در آن رخ نداده است.

اطلاعات موجود در این استاندارد بخشی از استاندارد CCSDS نمی‌باشد. در مواردی که بین اطلاعات ارائه شده در این سند و استاندارد CCSDS تداخلی مشاهده شود، اولویت با موارد مطرح شده در استاندارد CCSDS است.

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.

درصورتی‌که 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:

2-1 ANSI X9.31:1998. New York: ANSI, 1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).

2-2 ANSI X9.62:2005. New York: ANSI, 2005. Public Key Cryptography for the Financial Services Industry, the Elliptic Curve Digital Signature Algorithm (ECDSA).

1 - Security Working Group (SecWG)

2 - Consultative Committee For Space Data System(CCSDS)

2-3 Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-2. Gaithersburg, Maryland: NIST, January 2000.
2-4 H. Krawczyk, M. Bellar, and M. Bellar. HMAC: Keyed-Hashing for Message Authentication. RFC 2104. Reston, Virginia: ISOC, February 1997.
2-5 The Keyed-Hash Message Authentication Code (HMAC). Federal Information Processing Standards Publication 198. Gaithersburg, Maryland: NIST, March 2002.
2-6 T. Krovetz, ed. UMAC: Message Authentication Code using Universal Hashing. RFC 4418. Reston, Virginia: ISOC, March 2006.
2-7 P. Metzger and W. Simpson. IP Authentication using Keyed MD5. RFC 1828. Reston, Virginia: ISOC, August 1995.
2-8 Computer Data Authentication. Federal Information Processing Standards Publication 113.Gaithersburg, Maryland: NIST, May 1985.
2-9 Morris Dworkin. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. National Institute of Standards and Technology Special Publication 800-38B (Draft). Gaithersburg, Maryland: NIST, March 9, 2005.
2-10 Morris Dworkin. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. National Institute of Standards and Technology Special Publication 800-38C. Gaithersburg, Maryland: NIST, May 2004.
2-11 Secure Hash Standard. Federal Information Processing Standards Publication 180-2. Gaithersburg, Maryland: NIST, August 2002.

۳ کوته نوشته‌ها، اصطلاحات و تعاریف

کوته نوشته‌ها و کلمات اختصاری استفاده شده در این استاندارد به ترتیب عبارتند از:

کوته نوشته	معادل لاتین	معادل فارسی
AES	Advance Encryption Standard	نام نوعی الگوریتم رمزنگاری است
CBC	Cipher Block Chaining	زنجیره بلوک رمزی
CCM	Counter with Cipher Block Chaining MAC	شمارنده با MAC زنجیره بلوک رمزی
CMAC	Digital Signature Standard	امضای دیجیتال استاندارد
DES	Data Encryption Algorithm	نام نوعی الگوریتم رمزنگاری است
DSA	Digital Signature Algorithm	الگوریتم امضای دیجیتال استاندارد
DSS	Digital Signature Standard	امضای دیجیتال استاندارد
EC	Elliptic Curve	خم بیضوی
ECC	Elliptic Curve Cryptography	رمزنگاری مبتنی بر خم بیضوی
ECDSA	Elliptic Curve Digital Signature	امضای دیجیتال مبتنی بر خم بیضوی
HMAC	Hash Base Message Authentication Code	کد احرازهویت پیام مبتنی بر درهم‌سازی
IETF	International Engineering Task Force	کارگروه مهندسی بین‌المللی

کوته نوشته	معادل لاتین	معادل فارسی
MAC	Message Authentication Code	کد احرازهویت پیام
MD	Message Digest	خلاصه پیام
NIST	National Institute of Standards and Technology	موسسه بین‌المللی استاندارد و تکنولوژی
PKI	Public Key Infrastructure	زیرساخت کلید عمومی
RACE	Research and Development in Advanced Communications Technologies in Europe	تحقیق و توسعه در تکنولوژی ارتباطات پیشرفته‌ی اروپا
RSA	Revest-Shamir-Adleman	نام نوعی الگوریتم رمزنگاری است
SHA	Secure Hash Algorithm	الگوریتم درهم‌ساز امن
SHS	Secure Hash Standard	درهم‌ساز امن استاندارد
TDES	Triple Data Encryption Algorithm	(نام نوعی الگوریتم رمزنگاری است) سه گانهDES
UMAC	Universal Message Authentication Code	کد احرازهویت جهانی پیام

الگوریتم‌های پیشنهادی یکپارچگی و احراز هویت بر پایه تکنولوژی امضای دیجیتال بنا شده است. حداقل دو روش کلی برای پیاده سازی سازوکار یکپارچگی و احراز هویت وجود دارد، که یکی از آن‌ها دارای دو زیر روش مطرح است، که در ادامه به بررسی آن‌ها پرداخته می‌شود.

۳-۱
امضای دیجیتال[1]

فناوری امضای دیجیتال نیازمند استفاده از رمزنگاری کلید عمومی و استفاده از زوج کلید عمومی و خصوصی را است. فرستنده پیام را با محاسبه‌ی مقدار درهم‌ساز (سرجمع[2]) برای تولید کلمه‌ی کنترل به صورت دیجیتال امضا می‌کند. سپس کلمه‌ی کنترل را با کلید خصوصی خود رمز می‌نماید. کلمه‌ی کنترل رمزشده به همراه داده‌ها برای گیرنده ارسال می‌شود. گیرنده باید هویت پیام را با محاسبه‌ی مجدد کلمه‌ی کنترل و مقایسه‌ی آن با کلمه‌ی کنترل رمزگشای شده توسط کلید عمومی فرستنده که از قبل در اختیار دارد، تایید نماید. اگر این دو کلمه مشابه بودند پیام معتبر است و از طرف فرستنده صحیح آمده است.

۳-۲
کدهای احرازهویت پیام (MAC)

هرچند امضای دیجیتال به عنوان روشی برای بررسی یکپارچگی و احراز هویت به کار می‌رود، اما روش دیگری نیز به نام کدهای احراز هویت پیام (MAC) برای این منظور وجود دارد. در امضای دیجیتال از زوج کلید عمومی و خصوصی استفاده می‌شود، در حالیکه MAC از کلید رمزی اشتراکی استفاده می‌کند. جالبتر آنکه MAC می‌تواند از یک کلید خصوصی برای یکپارچگی و احراز هویت از طرق مختلف استفاده نماید. در

1 - Digital Signature
2 - Checksum

یک روش کلمه کنترل می‌تواند، روی داده‌ها با یک کلید رمزی جاسازشده، ایجاد شود و در روش دیگر، با الگوریتم درهم ساز تولید و سپس با به کارگیری کلید خصوصی رمز می‌شود.

۳-۳

کدهای احرازهویت پیام مبتنی بر توابع درهم‌ساز (HMAC)

یکی از انواع MAC ها کدهای احراز هویت بر اساس توابع درهم‌ساز می‌باشد. این نوع از MAC ها از انواع قویتری از الگوریتم‌های درهم‌ساز (نظیر MD5، SHA1، SHA256) برای تولید یک کلمه کنترل روی داده‌ها و کلید جاسازی شده استفاده می‌کنند. به عنوان مثال اگر داده‌ها شامل جمله "Mary Had a Little Lamb" و کلید خصوصی "01234567890000" باشد، الگوریتم درهم ساز کلمه کنترل را با اعمال درهم‌سازی روی رشته ترکیبی "Mary Had a Little Lamb 01234567890000" تولید می‌نماید. این رشته می‌تواند به صورت رشته ترکیبی"01234567890000 Mary Had a Little Lamb" یا "Mary Had a Little Lamb 01234567890000" نیز باشد. تعداد متنوعی از الگوریتم‌های HMAC وجود دارد که دقیقاً نحوه ترکیب داده و کلید را قبل از درهم‌سازی مشخص کرده‌اند.

گیرنده با داشتن کلید رمزی بااعمال تابع درهم‌ساز مشابه روی ترکیب کلید و داده می‌تواند، کلمه کنترل را باز تولید نماید. در صورت مشابه بودن این کلمه کنترل تولید شده با کلمه کنترل دریافتی یکپارچگی و احرازهویت پیام را تایید می‌نماید.

۴-۳

کدهای احرازهویت پیام مبتنی بر رمزنگاری

پرکاربردترین MAC ها عموماً بر اساس ترکیب درهم‌سازی و رمزنگاری می‌باشد (به طور نمونه زنجیره بلوک رمزی یا CBC). این نوع MAC یک کلمه کنترل روی داده با کمک الگوریتم درهم‌ساز ایجاد می‌نماید. سپس الگوریتم رمزنگاری با کلید رمز کلمه کنترل را رمز می‌کند.
گیرنده با داشتن کلید خصوصی کلمه کنترل را مجددا تولید می‌نماید و کلمه کنترل رسیده را رمزگشایی می‌کند. با مقایسه کلمه کنترل تولید شده و رمزگشایی شده و مشابه بودن آن‌ها یکپارچگی و احرازهویت پیام تایید می‌شود.

۴ الگوریتم‌های مناسب مورد پذیرش CCSDS (بر اساس دسته‌بندی)

با توجه به شرح بالا سه نوع دسته بندی

۱- امضای دیجیتال،
۲- کدهای احرازهویت پیام بر اساس توابع درهم‌ساز،
۳- کدهای احرازهویت پیام بر اساس رمزنگاری

از الگوریتم‌ها در این استاندارد وجود دارد که در جدول ۱ شرح داده شده است.

جدول ۱- الگوریتم‌های امضای دیجیتال

نام	نوع	مشخصات	حداقل طول کلید (بیت)
امضای دیجیتال استاندارد (DSS)	امضای دیجیتال FIPS 186-2	امضای دیجیتال مبتنی بر SHA1 (بدون نیاز به مجوز و امتیازنامه)	۱۰۲۴
امضای دیجیتال RSA	امضای‌دیجیتال RSA (مصوبFIPS)	امضای دیجیتال قدیمی (انقضا سال ۲۰۰۰)	۱۰۲۴
امضای دیجیتال مبتنی بر خم بیضوی (ECDSA)	امضای دیجیتال مبتنی بر خم بیضوی	امضای دیجیتال بر اساس خم بیضوی که از کلیدهای با طول کمتر نسبت به سایر روش‌های کلید عمومی استفاده می‌کند. اما ممکن است توسط گواهینامه‌ها، امتیازنامه‌ها و خصوصیات سرتیکام[1] پیچیده شده باشد. ظاهرا ECDSA توسط امتیازنامه‌های سرتیکام پوشش داده نمی‌شود و دارای کتابخانه‌های با منابع عمومی[2] ECC هستند. اما سرتیکام بیش از ۳۰۰ امتیازنامه در مورد انواع ECC شامل پیاده‌سازی‌های کارآمد نرم‌افزاری و سخت‌افزاری، توافقِ کلید و غیره دارد.	۱۶۰

۴-۱ الگوریتم‌های امضای دیجیتال

سه نوع امضای دیجیتال توسط CCSDS مطرح شده است:

۱- الگوریتم امضای دیجیتال DSA،

۲- الگوریتم RSA (در ANSI با X9.31 تعریف شده)،

۳- الگوریتم امضای دیجیتال مبتنی بر خم بیضوی.

تمام این سه نوع امضای دیجیتال در FIPS شماره ۲-۱۸۶ آمده است (با تغییرات ذکر شده در پنجم اکتبر سال ۲۰۰۱).

رمزنگاری خم بیضوی (ECC) با توجه به طول کلید مورد استفاده به مراتب پرکاربردتر و موثرتر از سایر روش‌ها می‌باشد. به‌هرحال بسیاری از روش‌های خم بیضوی (بیش از ۳۰۰ مورد) توسط سرتیکام مستند شده است و گواهینامه‌های آن‌ها موجود می‌باشد. به هر حال همه‌ی آن‌ها از مطالب ECDSA ی پایه که رایگان و در دسترس است، گرفته شده است. موسسه‌ی سرتیکام امتیازنامه‌های انواع مختلف و کارآمد در پیاده‌سازی بسترهای سخت‌افزاری و نرم‌افزاری ECC و همچنین امتیازنامه‌های توافق کلید ECC و غیره را در اختیار دارد. کتابخانه‌های خم بیضوی در دسترس است و بدون مجوز و حق تالیف می‌باشد.(مانند

1 - Certicom (www.certicom.com)
2 - Open Source

کتابخانه *libecc* در زبان C++ که یک کتابخانه رمز ECC است و در وبگاه http://libecc.sourceforge.net/ وجود دارد).

الگوریتم RSA توسط RSA ثبت شده، اما امتیازنامه‌ی آن منقضی شده است. الگوریتم DSA نیز تدوین شده و بدون نیاز به مجوز و امتیازنامه به صورت رایگان قابل استفاده است.

۴-۲ کدهای احرازهویت پیام مبتنی بر توابع درهم‌ساز (HMAC)

در فضای MAC مبتنی بر درهم‌سازی الگوریتم‌های بسیاری برای CCSDS وجود دارد. در این زمینه دو بخش عمده‌ی "خصوصیات الگوریتم HMAC" و "الگوریتم‌های درهم‌ساز واقعی[1]" وجود دارد. از آنجا که الگوریتم HMAC متکی بر به کارگیری الگوریتم درهم‌ساز و الگوریتم درهم‌ساز متکی بر خصوصیات HMAC به کارگرفته شده در کد احراز هویت پیام است، در این بخش هر دو مورد بحث می‌شوند.

برجسته‌ترین الگوریتم HMAC مدل استاندارد IETF (RFC 2104) است، که دارای استاندارد FIPS PUB 198 نیز می‌باشد. الگوریتم HMAC می‌تواند از الگوریتم‌های درهم‌ساز MD5 یا SHA1 (انواع دیگر SHAها) استفاده نماید. علاوه بر این FIPS شماره ۱۹۸ می‌تواند از سایر الگوریتم‌های درهم‌ساز نظیر RIPEMD-160 و Tiger نیز بهره بگیرد.

واضح‌ترین الگوریتم مبتنی بر درهم‌سازی به نام کد احراز هویت جهانی پیام UMAC[2] (RFC 4418) شناخته می‌شود، که با معیارها و ضوابط سریع‌ترین الگوریتم مبتنی بر درهم‌سازی طراحی شده است.

با وجود این که الگوریتم سریع است، اما معمولا الگوریتم پرقدرتی نسبت به سایر الگوریتم‌های مبتنی بر خم بیضوی نیست. همچنین ساده‌ترین الگوریتم MAC مبتنی بر درهم‌سازی الگوریتم MD5 است (مانند مثال "Mary Had a Little Lamb" در مثال بالا) که در IETF RFC 1828 توصیف شده است.

این MD5 ساده به صورت زیر به کار می‌رود.

MD5 {key, keyfill, entire IP datagram, key, MD5fill}

پارامترهای بالا برای پیام‌های تا ۵۱۲ بیتی به کار می‌رود.

1 - Actual Hash Algorithm
2 - Universal MAC

جدول۲ - کدهای احراز هویت پیام براساس توابع درهم ساز

نام	نوع	مشخصات	طول خروجی درهم (بیت)
الگوریتم SHA1	الگوریتم درهم‌ساز	مصوب FIPS، سایر نسخه‌ها (نظیر SHA256, SHA384, SHA512) خروجی‌های طولانی تر تولید می‌کنند	۱۶۰ بیت
الگوریتم MD5	الگوریتم درهم‌ساز	ضعف‌های بالقوه : می‌تواند به عنوان درهم‌ساز مبتنی بر کلید استفاده شود	۱۲۸ بیت
الگوریتم UMAC	MAC مبتنی بر درهم‌ساز	طراحی شده بر اساس سریع ترین توابع درهم‌ساز کنونی	۳۲، ۶۴ یا ۹۶ بیت (۶۴ بیت توصیه می‌شود)
الگوریتم RIPEMD-160	الگوریتم درهم‌ساز	تدوین شده در بخش RACE	۱۶۰ بیت
الگوریتم TIGER	الگوریتم درهم‌ساز	طراحی شده برای کارایی بهتر در بسترهای ۶۴ بیتی	۱۹۲ بیت
الگوریتم HMAC-SHA1-96	MAC مبتنی بر درهم‌ساز	استفاده از SHA1 برای درهم‌سازی	۹۶ بیت (برش خروجی ۱۶۰ بیتی SHA1)
الگوریتم HMAC-MD5-96	MAC مبتنی بر درهم‌ساز	استفاده از MD5 برای درهم‌سازی	۹۶ بیت (برش خروجی ۱۶۰ بیتی SHA1)

۴-۳ کدهای احرازهویت پیام مبتنی بر رمزنگاری

آخرین بخش از الگوریتم‌های ممکن MAC در این استاندارد، کدهای احراز هویت پیام براساس رمزنگاری است. الگوریتم‌های این فضا براساس الگوریتم‌های رمز قالبی کلید عمومی (نظیر DES[1]، AES[2]، CAST و غیره) است. ممکن است MAC به جای MAC مبتنی بر درهم‌ساز استفاده شود، چون امکان دارد سامانه‌ای الگوریتم‌های رمز قالبی متقارن را تایید و الگوریتم‌های درهم‌ساز را رد کند.

تعدادی از الگوریتم‌های اولیه که توسط CCSDS باید در نظر گرفته شود عبارتند از : DES-CBC-MAC، MAC مبتنی بر رمز(CMAC) و MAC با شمارنده زنجیره بلوک رمزی (CCM). DES-CBC-MAC در FIPS شماره ۱۱۳ شرح داده شده است، CMAC در NIST ویژه‌نامه 800-38B آمده است و CCM در NIST ویژه‌نامه 800-38C آمده است.

علیرغم ضعف بدیهی الگوریتم رمزنگاری DES در رایانه‌های امروزی با پردازشگر قوی (که بطور ذاتی قادر به انجام حمله جستجوی کامل هستند)، الگوریتم MAC مبتنی بر DES ممکن است در برخی شرایط هنوز موثر باشد. ولی با توجه به بی میلی جهانی در استفاده از DES این الگوریتم در سطح وسیعی مورد استفاده قرار نگرفته است و به سادگی قابل استفاده در MAC نیست. اگر سامانه‌ای از الگوریتم DES برای اهداف

1 - Data Encryption Algorithm
2 - Advanced Encryption Standard

دیگری استفاده می‌کند، می‌تواند به سادگی از آن برای احرازهویت نیز بهره بگیرد. اما در سامانه‌های جدید چنین حالتی مطرح نیست.

الگوریتم CMAC بر اساس کاربرد رمزنگاری متقارن در حالت زنجیره بلوک رمزی (CBC) (همانند DES-CBC) برای تولید MAC می‌باشد. بهرحال CMAC (در ویژه‌نامه 800-38B) اجباراً الگوریتم رمز قالبی با کلید عمومی را برای استفاده اختصاص نمی‌دهد. ترجیحاً در فراهم سازی آن از الگوریتم‌های نظیر AES (128,196,256) و TDEA (3DES) استفاده می‌شود.

CCM ترکیبی از CBC-MAC در ساخت MAC یا حالت شمارنده رمزنگاری در ایجاد موجودیت مستقل داده که دارای MAC و رمز در کنار هم هستند، بهره می‌گیرند (هم سندیت و هم محرمانگی). در تولید رمزنگاری، زنجیره‌ی بلوک رمزی (CBC) بر محموله، داده‌ی همراه و در حال حاضر برای تولید یک کد احراز هویت پیام (MAC)، اعمال شده است، سپس رمزنگاری در مد شمارشی بر MAC و محموله برای تبدیل آن‌ها به شکل ناخوانا که متن رمزی نامیده می‌شود، اعمال شده است. در تایید رمزگشایی حالت رمزگشایی شمارنده‌ای، به متن رمزی اعمال می‌شود، تا MAC و متن متناظر آن پوشش داده شود. سپس زنجیره قالبی رمز در محموله، داده انجمنی دریافتی و دریافت کنونی به منظور صحت MAC به کار می‌رود. تصدیق موفقیت آمیز، اطمینان از اصلی بودن محموله و داده‌ی همراه، از منبع با دسترسی به کلید را فراهم می‌کند. حالت CCM تنها روی الگوریتم‌های با طول کلید ۱۲۸ بیت یا بیشتر کاربرد دارد، که با الگوریتم TDEA/3DES که از کلیدهای ۶۴ بیتی (چندین کلید ۶۴ بیتی) بهره می‌گیرند، سازگار نیست.

جدول۳ – کدهای احراز هویت پیام براساس رمزنگاری

نام	نوع	مشخصات	طول خروجی درهم (برحسب بیت)
DES-CBC-MAC	MAC رمزشده	بر اساس الگوریتم DES (انتشار ۱۱۳ توسط FIPS تاریخ ۳۰ می ۱۹۸۵)	۶۴
CMAC	MAC رمزشده	MAC رمز شده، با استفاده از الگوریتم رمزنگاری قالبی کلید متقارن	۶۴، ۱۲۸، ۱۹۲، ۲۵۶ (بر اساس الگوریتم رمز قالبی مورد استفاده)
CCM	MAC رمزشده	استفاده از CBC با حالت شمارنده‌ای رمزنگاری برای پوشش هر دو حالت سندیت و محرمانگی، استفاده از رمزقالبی با طول کلید حداقل ۱۲۸ بیت	۱۲۸، ۱۹۲، ۲۵۶

۵ خلاصه و نتیجه‌گیری

این استاندارد سعی در تهیه اطلاعاتی در خصوص احراز هویت و یکپارچگی در CCSDS دارد، در این راستا سه نوع از کدهای احراز هویت پیام (MAC) که مورد قبول CCSDS است به همراه جزییات مربوط به چندین MAC در هر کدام از آن‌ها مطرح گردید.

امضای دیجیتال جدیدترین تکنولوژی مناسب، برای CCSDS است که نیازمند زوج کلید عمومی و خصوصی می‌باشد. بنابراین برای به کارگیری امضای دیجیتال مبتنی بر احراز هویت، توانایی تولید زوج کلید عمومی و خصوصی و توزیع کلید عمومی بین طرفین درگیر نیز باید لحاظ شود. این امر مستلزم تهیه‌ی ساختار زیر ساخت کلید عمومی (PKI) با مولد کلید و یک سرویس دهنده امن کلید است، تا کلیدهای عمومی رسمیت داده شده و قابل بازیابی باشند. (مانند پیش‌بارگذاری و ذخیره نمودن کلید عمومی و غیره). بنابراین کلیدهای عمومی معمول (بجز کلیدهای خم‌های بیضوی) به مراتب بزرگتر از کلیدهای متقارن هستند. تمام این موارد ممکن است منجر به مسایلی در به کارگیری، با حذف ماموریت[1] استانداردهای توصیه شده در CCSDS باشد.

به این دلیل، CCSDS به تشریح چندین روش استاندارد برای احرازهویت به منظور پوشش دادن بیش از یک جنبه از احراز هویت پیام پرداخته است. روش MAC های مبتنی بر کلید متقارن، کلیدهای کوتاه را به کار می‌برند و نیازی به تولید و توزیع کلیدهای عمومی و خصوصی ندارند. بنابراین نیازی به PKI (و یا مفاهیم مشابه) نیست. اما همچنان نیاز به تولید امن، توزیع و مدیریت کلیدهای مشترک متقارن، وجود دارد. این کلیدهای مشترک تنها بخشی از اندازه کلیدهای عمومی را دارند (مانند ۱۲۸ بیت در مقابل ۱۰۲۴ بیت، هرچند که این مقدار ممکن است با توجه به الگوریتم مورد استفاده طولانی تر نیز باشد). اگر زیرساخت کلید عمومی (PKI) برخط به کار نرود، آنگاه هر دو کلید عمومی مبتنی بر روش امضای دیجیتال و کلید متقارن، بر اساس راه حل‌ها، نیازمند توزیع کلیدها به سامانه‌های نهایی هستند. تفاوت اصلی، در این است که در توزیع کلید عمومی، نیازی به امن بودن رسانه‌ی توزیع نیست. در حالی که برای کلید متقارن این موارد باید امن باشند.(و یا اینکه خود کلید برای محافظت در هنگام تبادل رمز شده و پیچیده‌تر شود)

به عنوان یک نتیجه حاصل از گردآوری اطلاعات و دانش برای ارائه این استاندارد، این استاندارد، الگوریتم امضای دیجیتال (DSA) را به عنوان استاندارد امضای دیجیتال CCSDS و هم‌چنین الگوریتم HMAC را به عنوان الگوریتم MAC مبتنی بر توابع در هم ساز پذیرفته است.

الگوریتم امضای دیجیتال در FIPS انتشار۲-۱۸۶ و الگوریتم استاندارد درهم‌ساز امن (SHS) نیز در FIPS انتشار ۲-۱۸۰ مشخص شده است. الگوریتم درهم‌ساز امن باید حداقل SHA-1 را به کار گیرد. الگوریتم HMAC در FIPS شماره ۱۹۸ مشخص شده است.

به این ترتیب، هر دو الگوریتم کلید عمومی و نوع متقارن برای استفاده در CCSDS به نیازهای ماموریت و پشتیبانی از زیرساخت‌های آماده بستگی دارد.

1 - Missions Hopping