INSO
10822-1
1st. Edition
Feb.2013

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

استاندارد ملی ایران
۱-۱۰۸۲۲
چاپ اول
اسفند ۱۳۹۲

فناوری اطلاعات - فنون امنیتی - مدیریت کلید - قسمت ۱: چارچوب

Information technology — Security techniques — Key management — Part 1: Framework

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

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

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

1- International Organization for Standardization

2 - International Electrotechnical Commission

3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)

4 - Contact point

5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات – فنون امنیتی – مدیریت کلید – قسمت ۱: چارچوب»

رئیس :	**سمت و/ یا نمایندگی**
کمرخانی، حبیب (فوق لیسانس فناوری اطلاعات- امنیت)	رئیس امور اداری بنادر و کشتیرانی ایران
دبیر:	
بی مانند، هدی (لیسانس مهندسی کامپیوتر)	کارشناس رایانه و آمار اداره کل استاندارد استان ایلام
اعضاء : (اسامی به ترتیب حروف الفبا)	
اکبری، علی (لیسانس مهندسی برق،الکترونیک)	کارشناس مسؤول فناوری اطلاعات هلال احمر استان ایلام
بشارتی، یاسر (لیسانس مهندسی کامپیوتر)	کارشناس رایانه جهاد دانشگاهی استان ایلام
جستجو، صفورا (لیسانس مهندسی کامپیوتر)	کارشناس فنی سامانه الکترونیک ارتباط مردمی(سامد) استان ایلام
حیدری، نرگس (فوق لیسانس مهندسی کامپیوتر)	عضو هیأت علمی دانشگاه آزاد اسلامی ایلام
عبدی، اسرا (لیسانس مترجمی زبان اتگلیسی)	مدرس جهاد دانشگاهی استان ایلام
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر- نرم‌افزار)	کارشناس استاندارد
مرادی، افسانه (لیسانس مهندسی کامپیوتر)	کارشناس آموزش و پرورش استان البرز

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات – فنون امنیتی - مدیریت کلید - قسمت ۱: چارچوب » که پیش نـویس آن در کمیسیون های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده است ودر سیصد و دوازدهمـین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۲/۱۱/۲ 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 ایـن 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 .

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

ISO/IEC 11770-1:2010, Information technology - Security techniques - Key management- Part 1: Framework

فناوری اطلاعات ـ فنون امنیتی ـ مدیریت کلید ـ قسمت ۱: چارچوب

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین موارد زیر است:

الف- ایجاد مدل کلی که سازوکارهای مدیریت کلید بر آن استوار است،

ب- تعریف مفاهیم مبنا مدیریت کلید را که برای تمام قسمت‌های این مجموعه استاندارد مشترک است،

پ– تعیین مشخص سازی خدمات مدیریت کلید ،

ت- اصول کلی را درباره مدیریت مورد کلیدگذاری[1] در طی چرخه حیات آن تعیین می‌کند و

ث- مدل مفهومی از توزیع کلید، ایجاد می‌کند.

۲ اصطلاحات و تعاریف

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

۲-۱
فن رمزنگاشتی نامتقارن[2]

رمزنگاشتی روش است که از دو تبدیل مرتبط، تبدیل عمومی (تعریف شده توسط کلید عمومی) و تبدیل خصوصی (تعریف شده توسط کلید خصوصی) استفاده می‌کند.

یادآوری- این دو تبدیل‌ها دارای ویژگی‌هایی هستند که، با توجه به تبدیل عمومی، محاسبات غیرممکنی را به تبدیل خصوصی مشتق می‌کنند.

۲-۲
زوج کلید نامتقارن[3]

زوجی از کلیدهای مرتبط که در آن کلید خصوصی، تبدیل خصوصی را تعریف کرده و کلید عمومی، تبدیل عمومی را تعریف می‌کند.

1 - keying Material
2 - asymmetric cryptographic technique
3 - asymmetric key pair

[قسمت سوم این مجموعه استاندارد[1]]

۳-۲

مرجع صدور گواهی[2]

هستار مورد اعتمادی به منظور ایجاد و تخصیص گواهی‌های کلید عمومی است.

٤-۲

یکپارچگی داده[3]

خاصیتی است که در آن داده تغییری نداشته یا در روشی غیرمجاز از بین نرفته باشد.

[استاندارد ملی ایران به شماره ۱۶۲۷۴-۲: سال ۱۳۹۱]

٥-۲

اصالت‌سنجی مبدأ داده[4]

تأیید این که منبع داده دریافت شده همانی است که ادعا می‌کند.

[استاندارد ملی ایران به شماره ۱۶۲۷۴-۲: سال ۱۳۹۱]

٦-۲

رمزگشایی[5]

معکوس رمزبندی متناظر آن است.

یادآوری-رمزگشایی [ISO/IEC 18033-1] و پوشیده‌خوانی[6] [ISO/IEC 9798-1[7]] اصطلاحات معادلی هستند.

۷-۲

امضای دیجیتال(امضای رقمی)

داده‌ی الحاقی یا تبدیل رمزنگاشتی، یک واحد داده است که به گیرنده واحد داده اجازه می‌دهد تا منبع و یکپارچگی واحد داده را اثبات کند و در مقابل جعل امضا به طور مثال توسط گیرنده حافظت کند.

[ISO/IEC 9798-1:1997]

۸-۲

مرجع نگهداری فهرست راهنما[8]

هستار مسؤولی برای در دسترس‌سازی برخط گواهی‌های کلید عمومی جهت آماده مصرف بودن توسط هستارهای کاربر است.

---

۱ - استاندارد بین‌المللی ISO/IEC 11770-3:2008 با شماره ملی ۱۱۸۸۰-۳ در سال ۱۳۸۷منتشر شده است.

2 - certification authority

3 - data integrity

4 - data origin authentication

5 - decryption

6 - Decipherment

۷ - استاندارد بین‌المللی ISO/IEC 9798-1:2010 با شماره ملی ۱۰۸۲۵-۱ در سال ۱۳۸۷منتشر شده است.

1 - directory maintenance authority

۹-۲
شناسانه متمایز
اطلاعاتی که بدون ابهام هستاری را متمایز می‌سازد.

۱۰-۲
رمزبندی[1]
تبدیل داده(برگشت‌پذیر) توسط یک الگوریتم رمزنگاشتی برای تولید متن رمزی شده[2] است، یعنی، برای مخفی کردن محتوای اطلاعات از داده است.

یادآوری- رمزبندی [ISO/IEC 18033-1] و رمزگذاری [ISO/IEC 9798-1] اصطلاحات معادلی هستند.

۱۱-۲
اصالت‌سنجی هستار[3]
تأییدی است که هستار آن را ادعا می‌کند

[ISO/IEC 9798-1:1997]

۱۲-۲
کلید[4]
دنباله‌ای از نمادها که عملیات تبدیل رمزنگاشتی را کنترل می‌کنند(به عنوان مثال، رمزبندی، رمزگشایی، محاسبه تابع وارسی رمزنگاشتی، تولید امضا یا درستی‌سنجی امضا)

۱۳-۲
توافق کلید[5]
فرآیند تعیین یک کلید مخفی اشتراکی بین هستارها است، به گونه‌ای که هیچ‌یک از آن‌ها نمی‌توانند ارزش این کلیدها را از قبل تعیین کنند.

۱۴-۲
بایگانی کلید
خدمتی است که ذخیره‌سازی امن، طولانی مدت از کلیدها را بعد از استفاده عادی، فراهم می‌سازد.

۱۵-۲
صدور گواهی کلید
خدمتی که همبستگی یک کلید عمومی با هستار را تضمین می‌کند.

۱۶-۲
تأیید کلید
تضمینی است برای هستاری که هستار شناسایی شده دیگر در تصرف کلید درستی است.

---

2 - encryption
2 - ciphertext
4 - entity authentication
5 - key
6 - key agreement

۲-۱۷
کنترل کلید
توانایی انتخاب کلید یا پارامترهای مورد استفاده در محاسبه کلید است.

۲-۱۸
ابطال کلید
رویه ارائه شده توسط مرجع ثبت کلید است که همبستگی کلید با هستار را حذف می‌کند.

۲-۱۹
اشتقاق کلید[1]
خدمتی است که به طور بالقوه با استفاده از یک کلید اصلی مخفی که کلید اشتقاق نامیده می‌شود، داده متغیر غیرمخفی و فرآیند تبدیل امن، تعداد زیادی از کلیدها را شکل می‌دهد.

۲-۲۰
تخریب کلید[2]
خدمتی است برای تخریب امن کلیدهایی که بیش از این مورد نیاز نیستند.

۲-۲۱
توزیع کلید
خدمتی است که اشیاء اطلاعات مدیریت کلید را به هستارهای مجاز به طور امن فراهم می‌کند.

۲-۲۲
مرکز توزیع کلید
هستار مورد اعتمادی است برای تولید یا اکتساب کلیدها و برای توزیع کلید در طرف‌های ارتباطی که آن کلید متقارن منحصر به فردی با هر یک از طرفین، به اشتراک می‌گذارد.

۲-۲۳
برقراری کلید
فرآیندی است که یک کلید به اشتراک گذاشته شده را برای یک یا چند هستار در دسترس قرار می‌دهد، که فرآیند شامل توافق کلید یا انتقال کلید است.

[قسمت سوم این مجموعه استاندارد]

۲-۲۴
تولید کلید
فرآیند تولید یک کلید است.

1 - key derivation
2 - key destruction

۲۵_۲
مولد کلید
هستار مسؤولی برای تولید یک زوج کلید نامتقارن است.

۲۶_۲
نصب کلید
خدمتی است که یک کلید را در داخل افزارگان مدیریت کلید[1] را به طور امن برقرار کرده، به روشی که آن را از به خطر انداختن[2] حافظت می‌کند .

۲۷_۲
موارد کلیدگذاری
داده‌ی لازم برای برقراری و نگهداری ارتباطات کلیدگذاری رمزنگاشتی است.

مثال‌ها: کلیدها، مقادیر اولیه

۲۸_۲
مدیریت کلید
سرپرستی و استفاده از تولید، ثبت، صدور گواهی، ابطال، توزیع، نصب، ذخیره‌سازی، بایگانی، ابطال، اشتقاق و تخریب موارد کلیدگذاری مطابق با خط‌مش‌های امنیتی است.

۲۹_۲
ثبت کلید
خدمتی است که یک کلید را با هستار همبسته می‌کند.

۳۰_۲
ابطال کلید
خدمتی است که غیر فعال کردن امن یک کلید را تضمین می‌کند.

۳۱_۲
ذخیره‌ساز کلید
خدمتی است که ذخیره‌سازی امن از کلیدهای در نظر گرفته شده برای استفاده جاری یا کوتاه مدت یا برای پشتیبانی را فراهم می‌کند.

۳۲_۲
مرکز ترجمه کلید
هستار مورد اعتمادی است برای رمزگشایی کلیدی که توسط یک طرف تولید و رمزبندی‌شده و برای طرف دیگر مجدد رمزبندی‌شده است.

---

۱ - استاندارد زیرساخت کلید عمومی برای برقراری ارتباطات امن است.

2 - Compromise

۳۳-۲
انتقال کلید
فرآیند انتقال کلید از یک هستار به هستار دیگر است که به طور مناسبی حافظت می‌شود.

[قسمت سوم این مجموعه استاندارد]

۳٤-۲
شماره شناسایی شخصی
دنباله شماره مخفی به کار رفته برای اصالت‌سنجی هستار که اطلاعات مخفی ضعیفی را حفظ کرده است.

۳٥-۲
کلید خصوصی
کلیدی از زوج کلید نامتقارن هستار است که خصوصی حفظ می‌شود.

یادآوری- امنیت سامانه نامتقارن به محرمانگی این کلید بستگی دارد.

۳٦-۲
کلید عمومی
کلیدی از زوج کلید نامتقارن هستار است که می‌تواند به طور معمول بدون به خطراندازی امنیت، عمومی شود.

۳۷-۲
گواهی کلید عمومی
اطلاعات کلید عمومی از هستاری است که توسط صادرکننده گواهی، امضاء می‌شود.

۳۸-۲
اطلاعات کلید عمومی
اطلاعات دربردارنده کمینه شناسانه متمایزکننده هستار و کلید عمومی است که می‌تواند شامل اطلاعات ثابت دیگری در مورد مرجع صدور گواهی، هستار، محدودیت‌ها در کاربرد کلید، دوره اعتبار یا الگوریتم‌های پیچیده باشد.

[قسمت سوم این مجموعه استاندارد]

۳۹-۲
عدد تصادفی
بیت تصادفی
پارامتر متغیر زمانی که مقدار آن غیر قابل پیش‌بینی است.

٤۰-۲
مرجع ثبت
هستار مسؤولی برای ارائه هویت‌های تضمینی کاربر به صادرکننده گواهی است.

۴۱-۲
کلید امنیتی
کلید به کار رفته برای فنون رمزنگاشتی متقارن است و فقط قابل استفاده توسط مجموعه‌ای از هستارهای مشخصی است.

۴۲-۲
مرجع امنیتی
هستاری که مسؤول تعریف، پیاده‌سازی یا اجرای خط‌مشی امنیتی است.

[استاندارد ملی ایران به شماره ۱۶۳۰۰-۱: سال ۱۳۹۱]

۴۳-۲
دامنه امنیتی
مجموعه عناصر، خط‌مشی امنیتی، مرجع امنیتی و مجموعه فعالیت‌های مرتبط با امنیت است که در آن‌ها مجموعه عناصر تابع خط‌مشی امنیتی برای فعالیت‌های مشخص می‌باشد و خط‌مشی امنیتی به توسط مرجع امنیتی برای دامنه امنیتی، سرپرستی می‌شود.

[استاندارد ملی ایران به شماره ۱۶۳۰۰-۱: سال ۱۳۹۱]

۴۴-۲
شماره ردیف
پارامتر متغیر زمانی است که مقدار آن از دنباله مشخص شده‌ای که در دوره زمانی معین، تکرار نمی‌شوند، به‌دست می‌آید.

۴۵-۲
فن رمزنگاشتی متقارن
فن رمزنگاشتی است که از کلید مخفی مشابهی برای هر دو تبدیل مبدأ و گیرنده استفاده می‌کند.

یادآوری- بدون دانش از کلید مخفی، از لحاظ محاسباتی امکان پذیر نیست که هریک از تبدیل مبدأ یا گیرنده را محاسبه کرد.

۴۶-۲
مُهر زمانی[1]
قلم داده است که نقطه زمانی را نسبت به مرجع زمانی مشترک نشان می‌دهد.

[قسمت سوم این مجموعه استاندارد]

۴۷-۲
پارامتر متغیر زمانی
قلم داده‌ای از قبیل عدد تصادفی، عدد ترتیبی یا مُهر زمانی است.

1-Time -stamp

[قسمت سوم این مجموعه استاندارد]

۲-۴۸
شخص سوم مورد اعتماد
مرجع امنیتی یا عامل آن که نسبت به برخی فعالیت‌های مرتبط با امنیت مورد اعتماد است.

[استاندارد ملی ایران به شماره ۱۶۳۰۰-۱: سال ۱۳۹۱]

۳ نمادها و کوته‌نوشت‌ها

۳-۱ نمادها

A,B	شناسانه‌های متمایزکننده هستارها
CA	مرجع صدور گواهی
DIR	مرجع نگهداری فهرست راهنما
KDC	مرکز توزیع کلید
KG	مولد کلید
KTC	مرکز ترجمه کلید
RA	مرجع ثبت
S_A	کلید امضای هستار A
V_A	کلید درستی‌سنجی هستار A
X	شناسانه متمایزکننده مرجع

۳-۲ کوته‌نوشت‌ها

CA	مرجع صدور گواهی
MAC	کد اصالت‌سنجی پیام
PIN	شماره شناسایی شخصی
RA	مرجع ثبت
TTP	شخص سوم مورد اعتماد
TVP	پارامتر متغیر زمانی

۴ مدل کلی مدیریت کلید

۴-۱ کلیات

هدف مدیریت کلید، اداره ایمن و استفاده از خدمت مدیریت کلید است و از این رو حفاظت از کلیدها بسیار مهم است.

رویه‌های مدیریت کلید بستگی به اصول سازوکارهای رمزنگاشتی، استفاده موردنظر از کلید وخط‌مشی امنیتی مورداستفاده دارند. مدیریت کلید نیز شامل تابع‌هایی است که در افزاره‌های رمزنگاشتی انجام می‌شوند.

٤-٢ حفاظت از کلیدها

٤-٢-١ جنبه‌های کلی مدیریت کلید

کلیدها قسمت حیاتی از هر سامانه امنیتی هستند که متکی بر فنون رمزنگاشتی هستند. حفاظت مناسب کلیدها بستگی به تعدادی عوامل از قبیل نوع کاربردی که کلیدها برای آن استفاده می‌شوند، تهدیدهای که با آن مواجه می‌شوند، حالت‌های مختلفی که کلیدها ممکن است به خود بگیرند و غیره دارد. در ابتدا بسته به فن رمزنگاشتی باید در مقابل افشا، اصلاح، تخریب و بازپخش حفاظت شوند. مثال‌هایی از تهدیدهای احتمالی برای کلیدها در پیوست الف ارائه می‌شود. بیش از یکی از فنون حفاظتی زیر ممکن است برای حفاظت در مقابل این تهدیدها موردنیاز باشد. اعتبار کلید باید از لحاظ زمانی و تعداد استفاده، محدود باشد. این محدودیت‌ها به وسیله زمان و تعداد داده‌ی موردنیاز برای انجام حمله بازیابی کلید و ارزش راهبردی اطلاعات ایمن در طول زمان کنترل می‌شود. کلیدهایی که برای تولید کلیدها به کار می‌روند، به حفاظت بیشتری نسبت به کلیدهای تولید شده نیاز دارند. جنبه مهم دیگری از حفاظت از کلیدها اجتناب از سوءاستفاده از آن‌ها می‌باشد. به طور مثال: استفاده از رمزبندی کلید برای رمزبندی داده.

٤-٢-٢ حفاظت به وسیله فنون رمزنگاشتی

با برخی تهدیدها موارد کلیدگذاری می‌توان با استفاده از فنون رمزنگاشتی مقابله کرد. به عنوان مثال، رمزبندی، با افشاسازی کلید و استفاده غیرمجاز مقابله می‌کند؛ سازوکارهای یکپارچگی داده با اصلاح مقابله می‌کنند؛ سازوکارهای اصالت‌سنجی مبدأ داده، امضاهای رقمی و سازوکارهای اصالت‌سنجی هستار، با تغییرشکل مقابله می‌کنند.

برای استانداردهای الگوریتم رمزبندی به ISO/IEC 18033 مراجعه شود. برای سازوکارهای یکپارچگی داده به ISO/IEC 9796، ISO/IEC 9797، ISO/IEC 10118 و ISO/IEC 14888 مراجعه شود. برای امضاهای رقمی به ISO/IEC 9796 و ISO/IEC 14888 مراجعه شود. برای سازوکارهای اصالت‌سنجی هستار، به ISO/IEC 9798 مراجعه شود.

سازوکارهای تفکیک رمزنگاشتی، با سوءاستفاده مقابله می‌کنند. چنین تفکیکی از کاربرد تابعی ممکن است با انقیاد اطلاعات به کلید، صورت پذیرد. به عنوان مثال: انقیاد اطلاعات کنترلی به کلید، تضمین می‌کند که کلیدهای مشخصی برای وظایف مشخصی به کار روند(برای مثال: رمزبندی کلید، یکپارچگی داده)؛ کنترل کلید برای انکارناپذیری با استفاده از فنون متقارن، موردنیاز می‌باشد. برای انکارناپذیری با استفاده از فنون متقارن، به ISO/IEC 13888-2[1] مراجعه شود.

---

۱ - استاندارد بین‌المللی ISO/IEC 13888-2:2010 در سال ۱۳۹۰ با شماره ملی ۲-۱۳۸۸۸ منتشر شده است.

٤-٢-٣ حفاظت به وسیله فنون غیررمزنگاشتی

مُهرهای زمانی ممکن است برای محدودسازی استفاده از کلیدها به دوره‌های زمانی معتبر معینی به کار روند. آن‌ها همراه با شماره ردیف‌ها ممکن است در مقابل بازپخش اطلاعات توافق کلید ثبت شده، حفاظت شوند. برای مُهرهای زمانی، به ISO/IEC 18014 مراجعه شود.

٤-٢-٤ حفاظت با ابزارهای فیزیکی

افزاره رمزنگاشتی در سامانه ایمن، به طور معمول نیاز به حفاظت از موارد کلیدگذاری دارد که از آن در مقابل تهدیدها اصلاح، حذف و افشاسازی به جز کلید عمومی، استفاده می‌کند. افزاره به طور معمول حوزه ایمنی برای ذخیره‌سازی کلید، استفاده کلید و پیاده‌سازی الگوریتم رمزنگاشتی ارائه می‌کند. همچنین ممکن است ابزاری برای موارد زیر ارائه کند:

- بارگذاری موارد کلیدگذاری از افزاره مجزا ذخیره‌سازی کلید ایمن
- تعامل با الگوریتم‌های رمزنگاشتی پیاده‌سازی شده در تسهیلات مجزا امنیتی (برای مثال، کارت‌های هوشمند)، یا
- ذخیره‌سازی موارد کلیدگذاری به صورت برون‌خط

قسمت‌های ایمن به طور معمول به وسیله سازوکارهای امنیت فیزیکی حافظت می‌شوند. سازوکارهای امنیت فیزیکی ممکن است شامل سازوکارهای غیرفعال باشند که از دسترسی مستقیم به حوزه ایمن ممانعت کنند همانند سازوکارهای تشخیص مداخله فعال که موارد کلیدگذاری را در رویداد حمله احتمالی به حوزه ایمن تخریب می‌کنند. سازوکارهای امنیت فیزیکی به کار گرفته شده، بستگی به ارزش راهبردی کلیدهای ایمن شده در طول زمان خواهند داشت. حفاظت امنیتی برای افزاره‌های رمزنگاشتی در ISO/IEC 19790 استانداردسازی می‌شود.

٤-٢-٥ حفاظت با ابزار سازمانی

یک ابزار حافظت از کلیدها، سازمان‌دهی آن‌ها در سلسله مراتب کلید می‌باشد. به جز در پایین‌ترین سطح سلسله مراتب، کلیدها فقط در یک سطح از سلسله مراتب برای حفاظت کلیدها در سطح پایینی بعدی به کار می‌روند. تنها کلیدها در پایین‌ترین سطح سلسله مراتب به صورت مستقیم برای ارائه خدمت امنیت داده به کار می‌روند. این رویکرد سلسله مراتبی اجازه محدودسازی استفاده از هر کلید را می‌دهد، از این رو افشاسازی و ایجاد حمله را مشکل می‌کند. به عنوان مثال، اثر به خطراندازی کلید تکی نشست تنها جهت خطراندازی اطلاعات پشتیبانی شده توسط آن کلید، محدود می‌شود.

اجازه دادن به افراد برای داشتن دسترسی به کلیدها می‌تواند برحسب داشتن توانایی جهت ممانعت از افشاسازی(به طور خاص برای انکارناپذیری) و جهت اثبات این که آن کلید نمی‌تواند مورد سوءاستفاده قرار گرفته باشد، منجر به مشکلات عمده‌ای می‌شود. توصیه می‌شود کلیدها تنها در متن بدون رمز هنگامی که درون افزاره‌های ایمن هستند، در دسترس قرار بگیرند. اگر آن‌ها باید صادر شوند، توصیه می‌شود در این

صورت سنجه‌های ویژه‌ای از قبیل تقسیم کلید به اجزا و اجازه ندادن به یک شخص جهت دسترسی به تمام اجزا، به کار روند.

استفاده از کلید، جهت ممانعت از استفاده از آن به روشی که خواهان افشای کلید یا داده‌ای باشد که حفاظت می‌کند، نیز باید کنترل شود.

٤-٣ مدل چرخه حیات کلید عمومی

٤-٣-١ تعاریف چرخه حیات کلید

یک کلید رمزنگاشتی از طریق مجموعه حالاتی پیشرفت می‌کند که چرخه حیات آن را تعریف می‌کند . سه حالت اصولی عبارتند از:

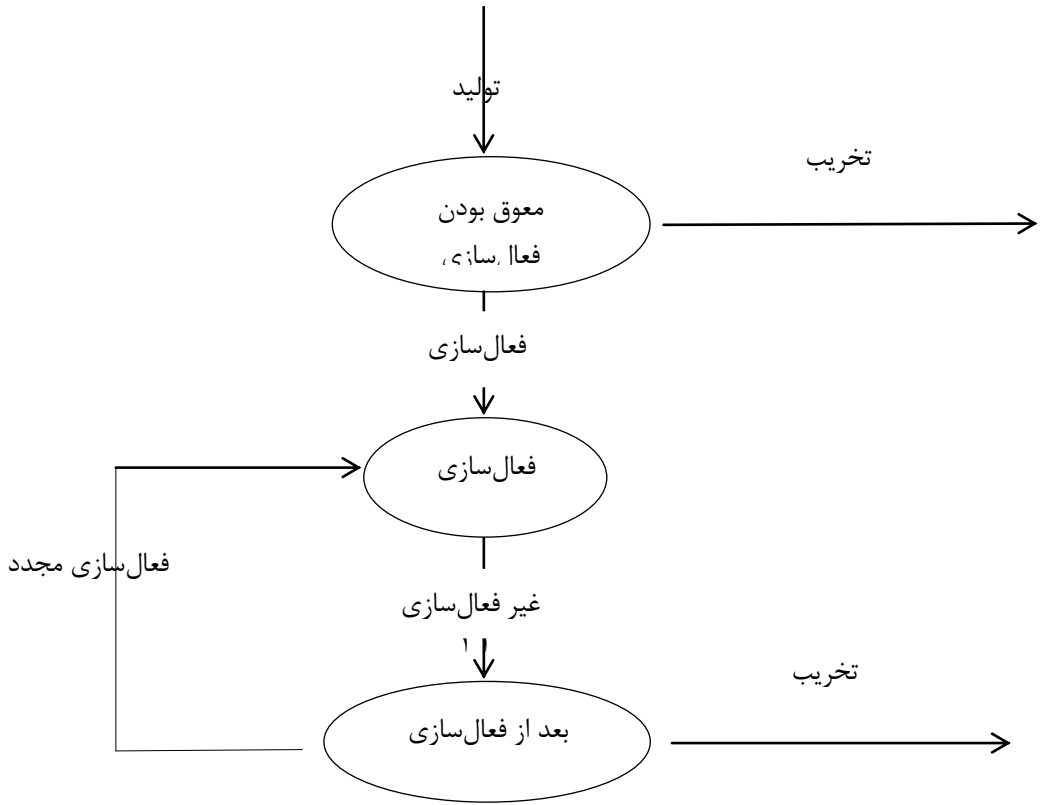
- **معلق بودن فعال** : در حالت معلق بودن فعال‌سازی، کلید تولید شده اما هنوز برای استفاده فعال‌سازی نشده است.

- **فعال‌سازی**: در حالت فعال‌سازی، کلید برای پردازش داده به صورت رمزنگاشتی یا جهت رمزگشایی یا درستی‌سنجی داده‌ی پردازش شده، به کار می‌رود.

- **بعد از فعال‌سازی**: در این حالت، کلید باید تنها برای رمزگشایی یا درستی‌سنجی به کار رود.

کلیدی که جهت به خطراندازی، آشکار می‌شود، باید سریع به حالت بعد از فعال‌سازی برود و برای هر هدف دیگری به جای رمزگشایی یا درستی‌سنجی داده‌ای که قبل از به خطراندازی پردازش شده نباید مورداطمینان قرار گیرد. به ویژه کلید به خطرافتاده نباید مجدد فعال شود.زمانی‌که تعیین می‌شود کلید در معرض دسترسی یا کنترل غیرمجاز قرار گرفته باشد، به خطراندازی گفته می‌شود.

شکل ۱، این حالت‌ها و گذارهای متناظر را نشان می‌دهد. همچنین شکل ۱، مدل کلی چرخه حیات را نشان می‌دهد. مدل‌های دیگر چرخه حیات ممکن است جزییات بیشتری داشته باشند که ممکن است حالت‌های



فرعی از سه حالت ارائه شده باشند. اکثر چرخه‌های حیات به فعالیت بایگانی نیاز دارند. این فعالیت ممکن است همبسته با هر یک از حالت‌ها بسته به جزییات ویژه چرخه حیات باشد.

شکل ۱-چرخه حیات کلید

٤-۳-۲ گذارهای بین حالت‌های کلید[1]

هنگامی که کلید از یک حالت به حالت دیگر حرکت می‌کند، این امر دستخوش یکی از گذارهای زیر می‌شود که در شکل ۱ نشان داده شده است:

- **تولید**: فرآیند تولید کلید می‌باشد. توصیه می‌شود تولید کلید مطابق با قواعد تولید کلید تعیین شده، انجام شود؛ این فرآیند ممکن است شامل رویه آزمایشی برای درستی‌سنجی این امر باشد که آیا از این قواعد پیروی شده است یا خیر. باید اشاره کرد که در طول تولید کلید، منبعی از اعداد تصادفی غیرقابل‌پیش‌بینی، دارای بیشترین اهمیت باشد در غیر این صورت، حتی قوی‌ترین الگوریتم‌ها را نمی‌توانند حفاظت کافی ارائه کنند. برای راهنمایی در مورد تولید عدد تصادفی به ISO/IEC 18031 مراجعه شود.

- **فعال‌سازی**: کلید را برای عملیات رمزنگاشتی، معتبر می‌کند.

- **غیرفعال‌سازی**: استفاده از کلید را محدود می‌کند. این امر به دلیل این رخ می‌دهد که کلید منقضی یا باطل شده است.

- **فعال‌سازی مجدد**: به کلید پس از فعال‌سازی اجازه می‌دهد تا مجدد برای عملیات رمزنگاشتی به کار رود.

- **تخریب**:چرخه حیات کلید را پایان می‌دهد. این امر، تخریب منطقی کلید را پوشش داده و ممکن است شامل تخریب فیزیکی آن نیز باشد.

گذارها ممکن است توسط رویدادهایی از قبیل نیاز برای کلیدهای جدید، به خطراندازی کلید، انقضاء کلید و تکمیل چرخه حیات کلید، راه‌اندازی شوند. تمام این گذارها شامل تعدادی خدمت برای مدیریت کلید می‌باشند.

٤-۳-۳ گذارها، خدمت و کلیدها

کلیدها برای فنون رمزنگاشتی خاص، ترکیب مختلفی از خدمات در طول چرخه حیات خود استفاده خواهند کرد. دو مثال در زیر ارائه می‌شود.

برای فنون رمزنگاری متقارن، در ادامه تولید کلید، گذار از حالت معوق بودن فعال‌سازی به حالت فعال‌سازی شامل نصب کلید است و ممکن است شامل ثبت و توزیع کلید نیز باشد. در برخی موارد، نصب ممکن است

1-Transitions between key states

شامل اشتقاق کلید ویژه باشد. توصیه می‌شود دوره حیات کلید محدود به دوره‌ای ثابت باشد. غیرفعال‌سازی به حالت فعال‌سازی پایان می‌دهد که به طور معمول به محض انقضاء است. اگر به خطر اندازی کلید درحالت فعال‌سازی، موردشک یا آشکار باشد، ابطال نیز منجر به ورود به حالت بعد از فعال‌سازی می‌شود. کلید در حالت بعد از فعال‌سازی ممکن است بایگانی شود. اگر کلید بایگانی شده مجدد موردنیاز باشد، مجدد فعال‌سازی خواهد شد و ممکن است یک بار دیگر معوق بودن فعال‌سازی شدن کامل، نصب یا توزیع شود. در غیر این صورت، در ادامه غیرفعال‌سازی، کلید ممکن از حالت ثبت خارج شده و تخریب شود.

برای فنون رمزنگاشتی غیرمتقارن، یک زوج از کلیدها (عمومی و خصوصی) تولید می‌شود و هردو کلید وارد حالت معوق بودن فعال‌سازی می‌شوند. یادآوری می‌شود که چرخه‌های حیات این دو کلید مرتبط هستند ولی یکسان نمی‌باشند. کلید خصوصی قبل از این‌که وارد حالت فعال‌سازی شود، ممکن است به طور اختیاری ثبت شود، ممکن است به طور اختیاری برای کاربران خود توزیع شود و همیشه نصب می‌شود. گذارها بین حالت‌های فعال و بعد از حالت فعال‌سازی برای کلید خصوصی شامل غیرفعال‌سازی، فعال‌سازی مجدد و تخریب مشابه با موارد توصیف شده بالا برای کلیدهای متقارن می‌باشند. هنگامی که یک کلید عمومی صادر می‌شود، به طور معمول این گواهی دربردارنده کلید عمومی است که توسط مرجع صدورگواهی (CA)[1] ایجاد می‌شود تا اعتبار و مالکیت کلید عمومی را تضمین کند. این گواهی کلید عمومی ممکن است در فهرست راهنما یا خدمت مشابه دیگری برای توزیع قرار گیرد یا ممکن است به مالک برای توزیع به عقب برود. هنگامی که مالک، داده‌ی امضا شده با کلید خصوصی خود را ارسال می‌کند، ممکن است گواهی خود را اضافه کند. زوج کلید زمانی که کلید عمومی صادر شود، فعال می‌شود. هنگامی که زوج کلید برای مقاصد امضای رقمی به کار می‌رود، کلید عمومی ممکن است برای زمان نامحدودی بعد از این که کلید خصوصی‌اش غیرفعال شده یا تخریب شده باشد، درحالت فعال‌سازی یا حالت بعد از فعال‌سازی باقی بماند. دسترسی به کلید عمومی ممکن است برای درستی‌سنجی امضاهای رقمی ایجاد شده قبل از تاریخ انقضای اصلی کلید خصوصی همبسته، ضروری باشد. هنگامی که فنون نامتقارن برای پیاده‌سازی خدمات محرمانگی به کار می‌روند و کلید به کار رفته برای رمزبندی، غیرفعال یا تخریب شده باشد، کلید متناظر از زوج کلید ممکن است در حالت فعال‌سازی یا حالت بعد از فعال‌سازی برای رمزگشایی بعدی باقی بماند.

از این رو برای کلیدهای امضا، قسمت عمومی کلید در حالت فعال‌سازی یا حالت بعد از فعال‌سازی باقی می‌ماند و برای کلیدهای رمزبندی، قسمت کلید خصوصی در حالت فعال‌سازی یا حالت بعد از فعال‌سازی باقی می‌ماند.

استفاده یا به کاربردن یک کلید ممکن است، خدمت آن کلید را تعیین کند. به عنوان مثال، یک سامانه از آن‌جا که ممکن است فرآیند ثبت طولانی‌تر از دوره حیات آن‌ها باشد، تصمیم بگیرد که کلیدهای نشست را

1 - Certification Authority

ثبت نکند . در مقابل، ضروری است تا هنگامی که فنون متقارن برای امضای رقمی استفاده مـی‌شـود، کلیـد مخفی را ثبت کرد.

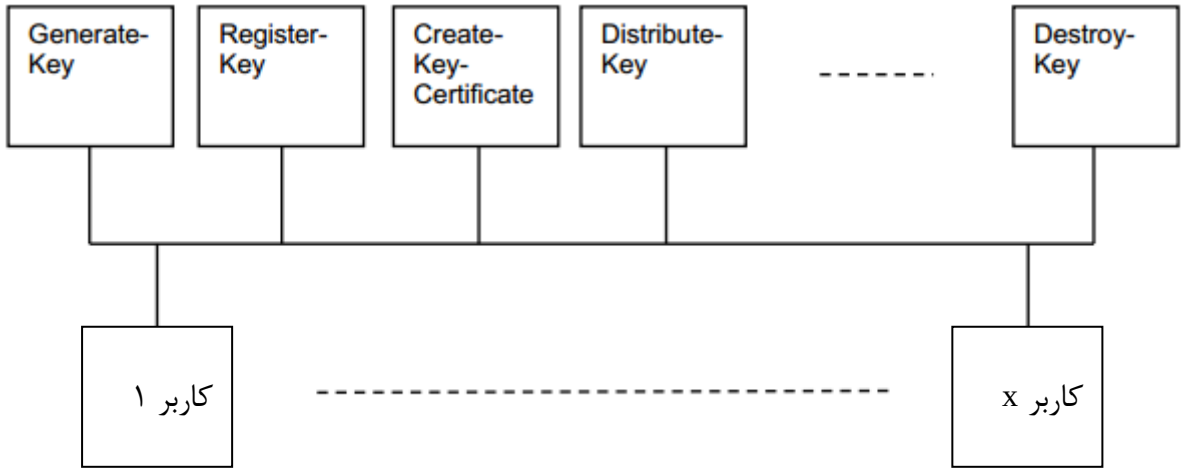
۵ مفاهیم مبنای پایه مدیریت کلید

۵-۱ خدمات مدیریت کلید

۵-۱-۱ چکیده خدمات مدیریت کلید

مدیریت کلید، سرپرستی و استفاده از خدمات تولید، ثبت، صدور گواهی، لغوثبت، توزیع، نصب، ذخیره‌سازی، بایگانی، ابطال، اشتقاق و تخریب موارد کلیدگذاری می‌باشد.

مدیریت کلید متکی بر خدمات پایه تولید، ثبت، صدور گواهی، توزیع، نصب، ذخیره‌سازی، اشـتقاق، بایگـانی، ابطال، لغو ثبت و تخریب است. این خدمات ممکن است قسمتی از مـدیریت سـامانه کلیـد بـوده یـا توسـط تأمین‌کنندگان دیگر خدمت ارائه شوند. بسته به نوع خدمت، تأمین‌کننده خدمت باید کمینه الزامات امنیتـی (برای مثال، تبادل امن) را جهت اطمینان توسط تمام هستارهای مشمول، بـرآورده کنـد. بـه عنـوان مثـال، تأمین‌کننده خدمت ممکن است طرف سوم مورداطمینان(TTP)[1] باشد. شکل ۲، نشان می‌دهد کـه خـدمات مدیریت کلید در سطح مشابهی قرار داشته و ممکن است توسط انواع کاربرهای مختلف(افراد یا فرآیندها) به کار روند. این کاربران ممکن است از تسهیلات مختلف مدیریت کلید با به کارگرفتن خدمت مشخصـی بـرای نیازهایشان در کاربردهای مختلف، بهره‌برداری کنند. خدمت مدیریت کلید در جدول ۱ فهرست می‌شود.



شکل ۲- خدمات مدیریت کلید

1 - Trusted Third Party

روابط بین گذارها[1] و خدمات در جدول ۱ نشان داده می‌شود. این خدمات در زیر توضیح داده می‌شوند. هر رویکرد رمزنگاشتی ویژه تنها به زیرمجموعه‌ای از خدمت ارائه شده در جدول ۱ نیاز دارد.

جدول ۱- گذارها و خدمات

گذارها (به شکل ۱ مراجعه شود)	خدمات	نکات
تولید	Generate-Key	الزامی
	Derive-Key	اختیاری
	Register-Key	اختیاری یا در این‌گذار یا در فعال سازی
	Create-Key-Certificate	اختیاری
	Distribute-Key	اختیاری
	Store-Key	اختیاری
فعال‌سازی	Create-Key-Certificate	اختیاری
	Distribute-Key	اختیاری
	Derive-Key	اختیاری
	Install-Key	اجباری
	Store-Key	اختیاری
	Register-Key	اختیاری یا در این‌گذار یا در تولید
غیرفعال‌سازی	Store-Key	اختیاری
	Archive-Key	اختیاری یا در این‌جا یا در تخریب
	Revoke-Key	اختیاری
فعالیت مجدد	Create-Key-Certificate	اختیاری
	Distribute-Key	اختیاری
	Derive-Key	اختیاری
	Install-Key	اجباری
	Install-Key	اختیاری
تخریب	Store-Key	اجباری، در صورت ثبت شدن
	Deregister-Key	اجباری
	Destroy-Key	
	Archive-Key	اختیاری یا در این‌گذار یا در غیرفعال‌سازی

۱ -**یادآوری**- روابط بین گذارها و خدمات، برچسب‌گذاری شده است.

۵-۱-۲ Generate-Key (تولید کلید)

خدمت Generate-Key، خدمتی است که برای تولید کلیدها به روشی ایمن برای الگوریتم رمزنگاشتی ویژه بدان استناد می‌شود. این امر دلالت بر این دارد که تولید کلید را نمی‌توان دستکاری کرد و این‌که کلیدها به روشی غیرقابل‌پیش‌بینی مطابق با توزیع تعیین شده، تولید می‌شوند. این توزیع به وسیله الگوریتم رمزنگاشتی صورت می‌گیرد که برای آن، مورداستفاده قرار خواهد گرفت و موردنیاز سطح حفاظت رمزنگاشتی خواهدشد. تولید برخی کلیدها به عنوان مثال شاه‌کلیدها، مراقبت ویژه‌ای را خواستارهستند زیرا که دانش این کلیدها، دسترسی به تمام کلیدهای مرتبط یا مشتق شده را می‌دهد.

تولید کلید همیشه شامل مولدهای عدد تصادفی است. این امر ضروری است تا مولدهای عدد تصادفی نه تنها اعداد تصادفی غیرقابل‌پیش‌بینی تولید کنند، بلکه اعداد تصادفی تولید بکنند که در سرتاسر فضای کلید الگوریتم به روشی یکنواخت گسترده شوند. به عنوان نمونه، اگر ورودی مولد عدد تصادفی، به طور موثر تنها در روال‌های تولید کلید، ۳۲ بیت انتروپی[1] تولید کند حال آن‌که کلیدهایی را برای الگوریتم متقارن ۱۲۸ بیتی تولید کند، فرآیند تولید کلید دچار کاستی می‌شود.

۵-۱-۳ Register-Key (ثبت کلید)

خدمت Register-Key، کلید را با هستار همبسته می‌کند. این امر توسط مرجع ثبت ارائه می‌شود و به طور معمول‌هنگام استفاده از فنون رمزنگاشتی نامتقارن، اعمال می‌شود. هنگامی که هستار تمایل به ثبت کلید دارد باید با مرجع ثبت تماس برقرار کند. ثبت کلید شامل درخواست برای ثبت و تأیید آن ثبت است.

مرجع ثبت، از ثبت کلیدها و اطلاعات مرتبط را به روشی ایمن و مناسب نگهداری می‌کند. پیوست ب جزییات اطلاعات مدیریت کلید را ارائه می‌کند.

عملیات ارائه شده توسط مرجع ثبت کلید، ثبت و لغو ثبت می‌باشند.

۵-۱-۴ Create-Key-Certificate (صدور گواهی کلید)

خدمت صدور گواهی کلید، همبستگی کلید عمومی با هستار را تضمین می‌کند که این امر توسط صادرکننده گواهی ارائه می‌شود. هنگامی که درخواست صدور گواهی کلید پذیرفته می‌شود، صادرکننده گواهی، گواهی کلید را صادر می‌کند. گواهی‌های کلید عمومی با جزییات بیشتری در قسمت سوم این مجموعه استاندارد[2] بحث می‌شوند.

۵-۱-۵ Distribute-Key (توزیع کلید)

توزیع کلید، مجموعه رویه‌هایی را به طور امن برای تأمین اشیاء اطلاعاتی مدیریت کلید به هستارهای مجاز می‌دهد. مورد ویژه توزیع کلید، ترجمه کلید در جایی است که موارد کلیدگذاری بین موجودیت‌های استفاده‌کننده از مرکز ترجمه کلید ایجاد می‌شود(طبق زیربند ۶-۳). قسمت دوم این مجموعه استاندارد، سازوکارهای مختلفی در ایجاد کلیدها بین هستارها ارائه می‌کند. قسمت سوم این مجموعه استاندارد شامل

۱- سنجه عدم قطعیت اعداد تصادفی است یا سنجه قابلیت غیرقابل‌پیش‌بینی محتوای اطلاعات است.

۲ - استاندارد بین‌المللی ISO/IEC 11770-3:1999 در سال با شماره ملی ۱۰۸۲۲-۳ منتشر شده است.

سازوکارهایی برای توافق کلید از کلیدهای مخفی است و سازوکارها را برای کلیدهای عمومی و مخفی انتقال می‌دهد.

۵-۱-۶ Install-Key (نصب کلید)

خدمت Install-Key، همیشه قبل از استفاده از کلید موردنیاز است. نصب کلید به معنای ایجاد کلید در تسهیل مدیریت کلید است به روشی که از آن در مقابل خطر، حفاظت کند. در کمترین حالت، تنها تابع نصب کلید برای نشان دادن کلید همان «در حال استفاده» است.

۵-۱-۷ Store-Key (ذخیره‌سازی کلید)

خدمت Store-Key، ذخیره‌سازی ایمنی از کلیدها را تأمین می‌کند که برای استفاده کوتاه مدت یا برای پشتیبانی گرفتن در نظر گرفته شده است. این امر به طور معمول به طور فیزیکی برای تأمین ذخیره‌سازی کلید مجزا مفید است. به عنوان مثال، محرمانگی و یکپارچگی برای موارد کلیدگذاری یا یکپارچگی برای کلیدهای عمومی را تضمین می‌کند. ذخیره‌سازی ممکن است در تمام حالت‌های کلید(یعنی معوق بودن فعال‌سازی، فعال‌سازی و بعد از فعال‌سازی) از چرخه حیات کلید رخ دهد. بسته به اهمیت کلیدها، آن‌ها می‌توانند با استفاده از یکی از سازوکارهای زیر حفاظت شوند.

- امنیت فیزیکی(برای مثال، توسط ذخیره‌سازیشان با افزاره مقاوم در برابر دست‌کاری یا توسط ابزار خارجی از قبیل کارت حافظه)،
- رمزبندی با کلیدهایی که خودشان با امنیت فیزیکی حفاظت می‌شوند، یا
- حفاظت از دسترسی به آن‌ها با اسم رمز[1] یا شماره شناسایی شخصی(PIN)[2]

برای تمام موارد کلیدگذاری، توصیه می‌شود، هرگونه تلاش جهت به خطراندازی قابل تشخیص باشد. این امر هنگامی‌که حفاظت به طور کامل مبتنی بر اسم رمز/PIN ذخیره شده در نرم‌افزار باشد، به طور کلی تشخیص به خطراندازی کلید تلاش شده، دشوار می‌شود. در چنین موردی، کلیدهای حفاظت شده را می‌توان کپی کرد و قفل‌شکنی اسم رمز/PIN می‌تواند به صورت برون‌خط رخ دهد که به معنای واقعای تشخیص غیرممکن است. برای چنین مواردی، بسته به کاربرد، سنجش‌های رویه‌ای امنیت دیگر باید در نظر گرفته شوند.

۵-۱-۸ Derive-Key (اشتقاق کلید)

خدمت Derive-Key، تعداد زیادی از کلیدها را به طور بالقوه با استفاده از کلید اصلی مخفی که کلید اشتقاق نامیده می‌شود، با استفاده از داده متغیر و با استفاده از فرآیند تبدیل، شکل می‌دهد. اشتقاق کلید به حفاظت ویژه‌ای نیاز دارد. توصیه می‌شود، فرآیند اشتقاق جهت تضمین این که به خطراندازی کلید اشتقاق، کلید اشتقاق یا هر کلید مشتق شده دیگری را افشا نمی‌کند، بازگشت‌ناپذیر و غیرقابل‌پیش‌بینی باشد.

---

1 - Password
2 - Personal Identification Number

۵-۱-۹ Archive-Key (بایگانی کلید)

بایگانی کلید، فرآیندی برای ذخیره‌سازی ایمن و بلندمدت از کلیدها بعد از استفاده عادی، ارائه می‌کند. این امر ممکن است از خدمت ذخیره‌سازی کلید استفاده کند، اما اجازه پیاده‌سازی مختلفی از قبیل ذخیره‌سازی برون‌خط می‌دهد. کلیدهای بایگانی شده ممکن است جهت اثبات یا عدم اثبات ادعاهای قطعی بعد از توقف استفاده عادی، نیاز به بازیابی در تاریخی به مراتب دیرتر داشته باشند.

۵-۱-۱۰ Revoke-Key (ابطال کلید)

هنگامی که به خطراندازی کلید، مظنون بوده یا آشکار می‌شود، خدمت Revoke-Key ، غیرفعال‌سازی ایمن کلید را تضمین می‌کند. این خدمت همچنین برای کلیدهایی که به تاریخ انقضای خود رسیده‌اند، ضروری است. ابطال کلیدها ممکن است زمانی رخ دهد که شرایط مالک، تغییر می‌کند. بعد از ابطال کلید باید تنها برای رمزگشایی و درستی‌سنجی به کار رود. در مورد کلید در حال ابطال، به دلیل به خطراندازی، تنها داده‌ی پردازش شده قبل از به خطراندازی ممکن است رمزگشایی یا درستی‌سنجی شود.

یادآوری- برخی کاربردها از اصطلاح Delete-Key برای این خدمت استفاده می‌کنند.

۵-۱-۱۱ Deregister-Key (لغو ثبت کلید)

خدمت Deregister-Key، رویه ارائه شده توسط مرجع ثبت کلید است که همبستگی کلید با هستار را حذف می‌کند که قسمتی از فرآیند تخریب است(به زیربند ۵-۱-۱۲ Destroy-Key مراجعه شود).

۵-۱-۱۲ Destroy-Key (تخریب کلید)

خدمت Destroy-Key، فرآیندی را برای تخریب ایمن کلیدهایی که دیگر موردنیاز نیستند، ارائه می‌کند. تخریب کلید به معنای حذف تمام رکوردهای[1] این شیء اطلاعاتی مدیریت کلید است به گونه‌ای که هیچ اطلاعاتی بعد از تخریب باقی نماند تا هرگونه ابزار ترمیم کلید تخریب شده را ارائه کند. این امر جهت دربرداشتن تخریب تمامی کپی‌های بایگانی شده، رخ می‌دهد. با این حال قبل از این‌که کلیدهای بایگانی شده تخریب شوند، باید جهت تضمین این که هیچ حفاظتی از موارد لازم بایگانی شده توسط کلیدهایی که هرگز موردنیاز نخواهد بود، نشده است، وارسی صورت گیرد.

برخی کلیدها ممکن است خارج از افزاره یا سامانه الکترونیکی ذخیره شوند. تخریب آن کلیدها نیاز به اقدامات افزوده‌ی سرپرستی دارد.

۵-۲ خدمات پشتیبانی

۵-۲-۱ خدمات تسهیلات مدیریت کلید

خدمت مدیریت کلید می‌تواند از خدمات دیگری استفاده کنند که مرتبط با امنیت هستند. این خدمات شامل:

- کنترل دسترسی

1 - Records

این خدمت جهت تضمین این است که به منابع سامانه مدیریت کلید را تنها می‌توان توسط هستارهای مجاز به روشی مجاز دسترسی یافت.

- ممیزی

این خدمت برای ممیزی اقدامات مرتبط با امنیت است که در سامانه مدیریت کلید پیدا می‌شوند. سلسله ممیزی[1] می‌تواند به شناسایی مخاطرات امنیتی و نشت‌های امنیتی کمک کنند.

- اصالت‌سنجی

این خدمت برای ایجاد هستار به عنوان عضو مجاز دامنه امنیتی است.

- خدمات رمزنگاشتی

این خدمات توسط خدمات مدیریت کلید برای تأمین یکپارچگی، محرمانگی، اصالت‌سنجی و انکارناپذیری به کار می‌روند.

- خدمت زمانی

این خدمت برای تولید پارامترهای متغیر زمانی(TVPs)[2] از قبیل طول مدت اعتبار است.

۵-۲-۲ خدمت کاربرگرا

خدماتی وجود دارند مثل خدمات ثبت کاربر که برای کارکرد مناسب، ضروری هستند. این خدمات، به طور مشخص پیاده‌سازی شده و فراتر از دامنه این استاندارد ملی است.

٦ مدل‌های مفهومی برای توزیع کلید برای دو هستار

٦-١ مقدمه‌ای بر توزیع کلید

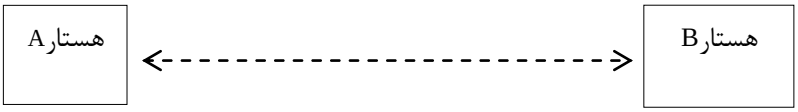
توزیع کلیدها بین هستار می‌تواند پیچیده باشد. توسط طبیعت پیوندهای ارتباطاتی، روابط مورد اعتماد مشمول و فنون رمزنگاشتی به کار رفته، تحت تاثیر قرار می‌گیرند. هستارها ممکن است یا به صورت مستقیم یا غیرمستقیم ارتباط برقرار کنند یا ممکن است متعلق به دامنه‌های امنیتی مشابه یا مختلفی باشند.

٦-٢ توزیع کلید بین دو هستار ارتباطی

ارتباط میان هستارها، توسط پیوند میان این هستارها، اعتماد بین این هستارها و فنون رمزنگاشتی به کار رفته،تحت تاثیر قرار می‌گیرد.

اتصالی بین هستارهای A و B وجود دارد که تمایل به تبادل اطلاعات با استفاده از فنون رمزنگاشتی دارند. این اتصال ارتباطی در شکل ۳ نشان داده می‌شود.

1 - Audit trail
2 - time variant parameters



شکل ۳- پیوند ارتباطات بین دو هستار

مواردی که در آن‌ها هستارهای ارتباط مستقیم موجود می‌باشند شامل توافق کلید، کنترل و تایید کلید می‌باشند.

۳-۶ توزیع کلید در یک دامنه

مدل زیر مبتنی بر مفهوم دامنه امنیتی با مرجع امنیتی مطابق با ISO/IEC 10181-1 است.

این مرجع ممکن است خدمات مدیریت کلید از قبیل ترجمه کلیدها را ارائه کند. هنگامی که هستارها از فن نامتقارن برای تبادل ایمن اطلاعات استفاده می‌کنند. موارد زیر را می‌توان متمایز کرد:

برای یکپارچگی داده یا اصالت‌سنجی اصلی داده، گیرنده به گواهی کلید عمومی متناظر فرستنده نیاز دارد.

برای محرمانگی، فرستنده به گواهی کلید عمومی معتبری از گیرنده نیاز دارد.

برای اصالت‌سنجی، محرمانگی و یکپارچگی، هر طرف به گواهی کلید عمومی دیگری نیاز دارد. این امر ابزاری برای انکارناپذیری متقابل ارائه می‌کند. هر هستار ممکن است نیاز به برقراری تماس با مرجع خود داشته باشد تا گواهی کلید عمومی مناسبی به دست آورد. اگر شرکای ارتباطی به یکدیگر اعتماد کنند و بتوانند به طور متقابل گواهی‌های کلید عمومی خود را اصالت‌سنجی کنند، آن‌گاه هیچ مرجعی موردنیاز نیست.

درخواست‌های رمزنگاشتی وجود دارد که هیچ مرجعی در آن وجود ندارد. دراین وضعیت، شرکای ارتباطی ممکن است تنها به صورت ایمن، اطلاعات عمومی ویژه‌ای را به جای گواهی‌های کلید عمومی خود، تبادل کنند.

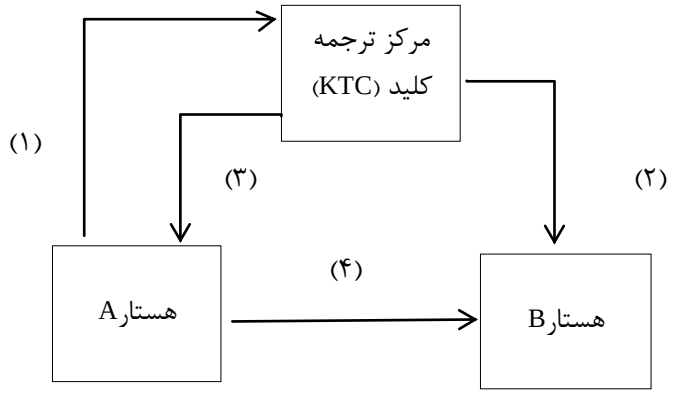
هنگامی که از رمزنگاری متقارن بین دو شریک استفاده می‌شود، تولید کلید به یکی از دو روش زیر ایجاد می‌شود:
الف– توسط یک هستار تولیدکننده کلید و ارسال آن به مرکز ترجمه کلید(KTC)؛

ب– توسط یک هستار درخواست‌کننده از مرکز توزیع کلید(KDC)جهت تولید کلید برای توزیع بعد؛

اگر تولید کلید توسط یکی از هستارها انجام شود، توزیع ایمن کلید می‌تواند توسط مرکز ترجمه کلید، ساماندهی شود، که در شکل ۴ نشان داده شده است. شماره‌ها، نشان دهنده مراحل تبادل می‌باشند. مرکز ترجمه کلید(KTC)، کلید رمزبندی شده را از هستار A، (۱) دریافت می‌کند، بازگشایی کرده و آن را با

استفاده از کلید به اشتراک گذاشته شده بین خود و هستار B، رمزبندی مجدد می‌کند. در این صورت ممکن است:

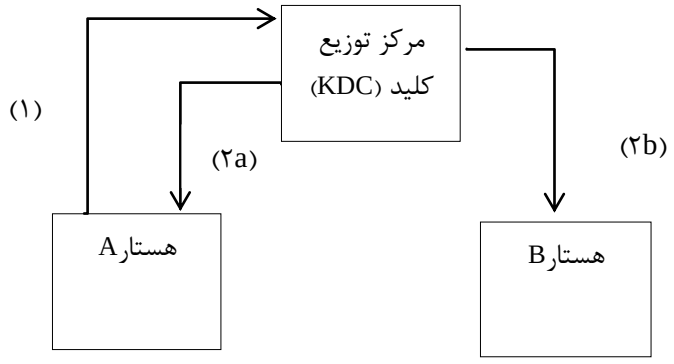
- یا به کلید رمزبندی شده در هستار B، (۲) هدایت کند، یا
- آن را به هستار A، (۳) ارسال کند که آن را به هستار B، (۴) هدایت می‌کند.



شکل ۴- مرکز ترجمه کلید

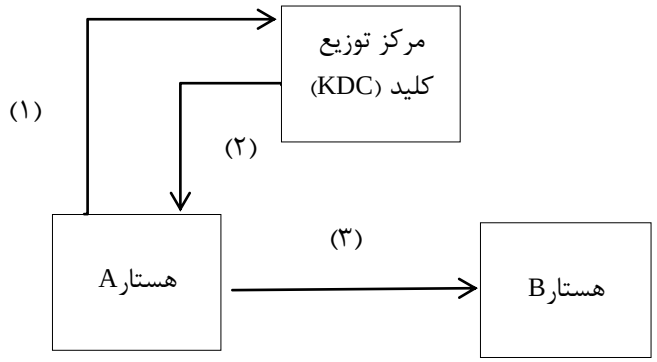
اگر تولید کلید توسط طرف سوم مورداعتماد(TTP)، انجام شود، دو گزینه برای توزیع بعدی کلید جهت ارتباط‌دهی شرکا وجود داد؛ این موارد در شکل ۵ - مدل مفهومی مرکز توزیع کلید(KDC) و شکل ۶ – توزیع کلید توسط هدایت کلید از هستارA به هستارB، نشان داده می‌شوند.

شکل ۵ موردی را نشان می‌دهد که در آن مرکز توزیع کلید قادر به برقراری ارتباط به طور ایمن با هردو هستار است. در این مورد، هنگامی که کلید بر مبنای درخواست یکی از هستارها تولید شده باشد، مرکز توزیع کلید مسؤول توزیع ایمن کلید به هردو هستار است. درخواست کلید به اشتراک گذاشته شده، در زیر با (۱) و توزیع کلید به شرکای ارتباطی با (۲a) و (۲b) نمایش داده می‌شود.



شکل ۵- مدل مفهومی مرکز توزیع کلید

هنگامی که تنها هستارA درخواست کلید مخفی به اشتراک گذاشته شده بین هستارهای A و B می‌کند، مرجع ممکن است به دو روش مختلف عمل کند. اگر مرجع بتواند با هر دو هستار، ارتباطی ایمن برقرار کند، ممکن است کلید مخفی را به هردوی آن‌ها همانطور که در بالا توصیف شد، توزیع کند. اگر مرجع تنها بتواند با هستار A ارتباط برقرار کند، هستار A مسؤول توزیع کلید به هستار B است. شکل ۶ این نوع توزیع کلید را نشان می‌دهد. درخواست برای کلید به اشتراک گذاشته شد، با (۱) و توزیع به هستارA با (۲) نمایش داده می‌شود. هدایت این کلید از A به B با (۳) نمایش داده می‌شود.



شکل ۶- توزیع کلید توسط هدایت کلید از هستارA به هستارB

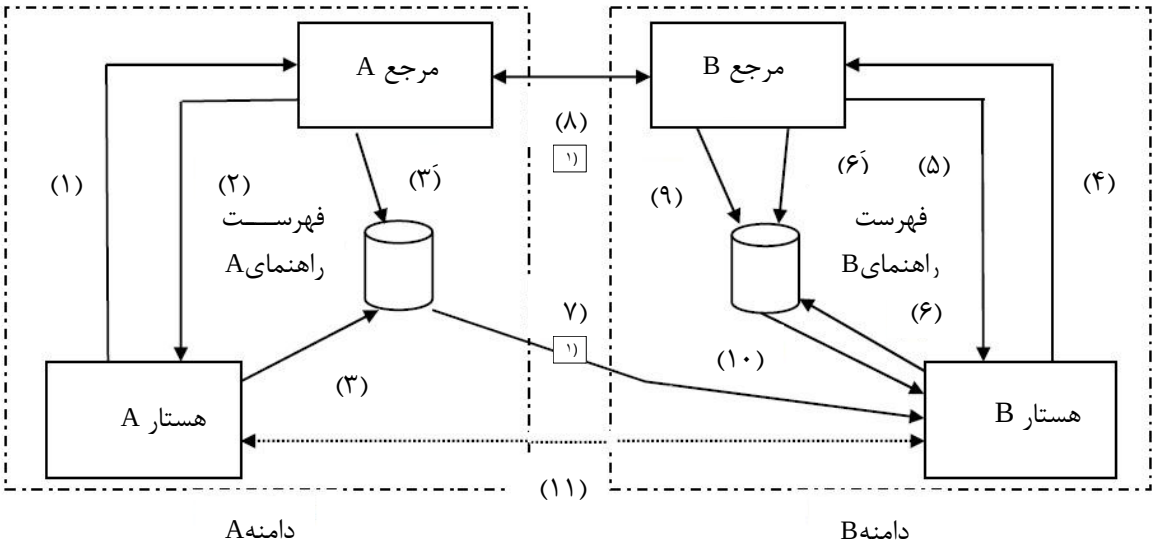
٤-٦ توزیع کلید بین دو دامنه

مدل اینجا شامل دو هستار به نام‌های A و B است که متعلق به دو دامنه امنیتی مختلف هستند که کمینه یک فن رمزنگاشتی(یعنی متقارن یا نامتقارن) را به اشتراک می‌گذارند. به شکل ۷ برای مورد نامتقارن و به شکل ۸ برای مورد متقارن مراجعه شود. هر دامنه امنیتی، مرجع امنیت خود را دارا است: یکی مورداعتماد توسط A و دیگری مورداعتماد توسط B است. اگر A و B یا به یکدیگر اعتماد داشته باشند، یا هر یک به مرجع دامنه دیگری اعتماد داشته باشد، در این صورت کلیدها مطابق زیربند ۶-۲ یا ۶-۳ توزیع می‌شوند.
دو مورد را می‌توان برای ایجاد کلید بین A و B متمایز کرد:

- به دست آوردن گواهی کلید عمومی B (وقتی کاربردپذیر است) و
- ایجاد کلید مخفی به اشتراک گذاشته شده بین A و B .

روابط کلیدی مختلفی بین این اجزاء امکان‌پذیر است. این روابط کلیدی، طبیعت اطمینان بین اجزاء را بازتاب می‌دهند.
هنگامی که هستارها از فن نامتقارن برای تبادل اطلاعات استفاده می‌کنند، هر یک نیاز به دسترسی به گواهی دیگری دارد(به شکل ۷ مراجعه شود). هنگامی که مرجع A، مطابق با درخواست A (۱)، گواهی برای A صادر می‌کند(۲)، این گواهی به طور کلی به فهرست راهنما یا با A (۳) یا مرجع آن (۳َ) ارسال می‌شود. فهرست راهنما ممکن است باز باشد، که در آن، مورد B، ممکن است به طور مستقیم به گواهی A از فهرست راهنمای A (۷) دست یابد. اگر هر دو مرجع A و B دارای توافق ارسال متقابل باشند (۸)، B ممکن

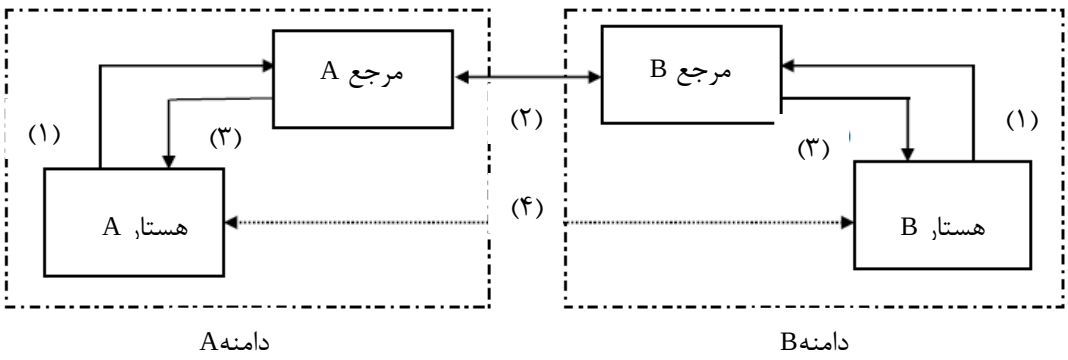
است گواهی A را در فهرست راهنمای خود پیدا کند (۱۰). با شکست آن، A گواهی خود را به B همراه با تبادل یا به عنوان قسمتی از قرارداد ایجاد کلید، ارسال می‌کند.



شکل ۷-توزیع کلید بین دو دامنه با استفاده از فنون نامتقارن

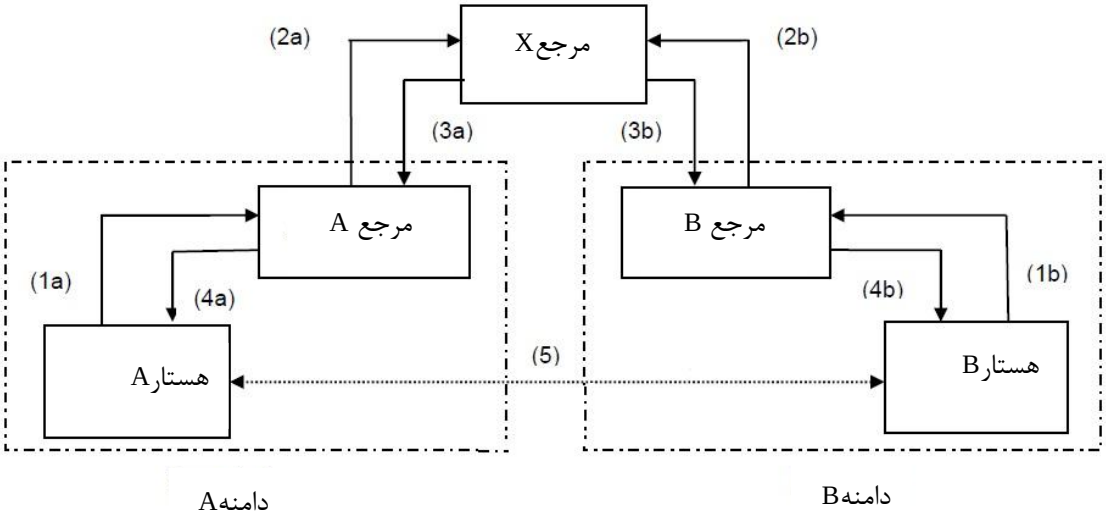
هنگامی که هستارها با استفاده از فن متقارن ارتباط برقرار می‌کنند، هر هستار همچنین باید به صورت ایمن با مرجع مربوطه خود تماس برقرار کند (۱) (به شکل ۸ مراجعه شود) تا رمز مخفی بگیرد که به آن‌ها اجازه ارتباط می‌دهد. مراجع بر روی کلید مخفی مشترک جهت استفاده توسط هستارها، توافق دارند (۲) . یک مرجع، کلید مخفی را به هر دو هستار با استفاده از مرجع دیگر به عنوان مرکز توزیع، توزیع می‌کند. مرجع دیگر نیز ممکن است ترجمه کلید را ارائه کند (۲) و (۳) .

هنگامی که تنها هستار A درخواست کلید مخفی جهت ارتباط با هستار B می‌کند، مرجع ممکن است به دو روش عمل کند. اگر مرجع بتواند با هر دو هستار ارتباط برقرار کند، ممکن است کلید مخفی را به هر دوی آن‌ها همانطور که در بالا توصیف شد، توزیع کند. اگر مرجع بتواند تنها با یک هستار ارتباط برقرار کند،هستاری که کلید را دریافت می‌کند، مسؤول هدایت کلید به هستار دیگر می‌شود.



شکل ۸-توزیع کلید بین دو دامنه با استفاده از فنون متقارن

بعضی وقت‌ها، مراجع A و B، نه رابطه اعتماد متقابل داشته و نه مسیر ارتباط مستقیمی دارند. در این صورت آن‌ها باید شامل مرجع X باشند که همان‌طور که در شکل ۹ نشان داده شده است، هردو اعتماد کنند [به (۲a) و (۲b) مراجعه شود]. مرجع X ممکن است کلیدی را تولید کند و آن را به مراجع A و B در شکل ۹ توزیع کند [به (۳a) و (۳b) مراجعه شود]. به طور متناوب، مرجع X ممکن است گواهی کلید مخفی یا گواهی کلید عمومی دریافتی[برای مثال (۲a)] را از مرجع A به مرجع B (۳b) هدایت کند. سپس مراجع باید کلید دریافتی را به هستارهای مربوطه خود هدایت کنند[به (۴a) و (۴b) در شکل ۹ مراجعه شود] که آن‌گاه ممکن است اطلاعات را به طور ایمن تبادل کنند (۵) . این امر ممکن است ضروری باشد که به دنبال مرجع‌های مردیف بود تا زنجیره اعتماد، ایجاد شود.



شکل ۹- زنجیره اطمینان بین مراجع

۷ تأمین‌کنندگان خدمت خاص

برخی از خدماتی که موردنیاز سامانه مدیریت کلید است، ممکن است توسط تأمین‌کنندگان خدمت خارجی، تأمین شوند. هستارهای محتمل برای این خدمت عبارتند از:

- مرجع ثبت کلید یا صادرکننده گواهی کلید
- مرکز توزیع کلید
- مرکز ترجمه کلید

پیوست الف
(اطلاعاتی)
تهدیدها برای مدیریت کلید

مدیریت کلید در معرض تعدادی تهدید است که عبارتند از:

- **افشای موارد کلیدگذاری:**

یا موارد کلیدگذاری در متن بدون رمز است که حفاظت نشده و قابل دسترسی است یا رمزبندی شده است و می‌تواند رمزگشایی شود.

- **اصلاح موارد کلیدگذاری:**

تغییر موارد کلیدگذاری به نحوی که به خوبی که مورد نظر است، عمل نکند.

- **حذف غیرمجاز موارد کلیدگذاری:**

حذف کلید یا داده‌ای مرتبط با کلید است.

- **تخریب ناقص موارد کلیدگذاری:**

این امر ممکن است منجر به خطراندازی کلیدهای کنونی یا آینده شود.

- **ابطال غیرمجاز:**

حذف مستقیم یا غیرمستقیم کلید معتبر یا موارد کلیدگذاری است.

- **تغییرشکل:**

جعل هویت کاربر یا هستار مجاز است.

- **تأخیر در اجرای توابع مدیریت کلید:**

این امر ممکن است منجر به شکست در تولید، توزیع، ابطال یا ثبت کلید شود یا منجر به شکستی در به‌روزرسانی مخزن کلید به شیوه‌ای به جا شود با منجر به شکست در نگهداری سطوح اجازه کاربر شود. تهدید تأخیر ممکن است ناشی از هرگونه تهدید ذکر شده در قبل باشد یا ناشی از شکست فیزیکی تجهیزات مرتبط با کلید باشد.

- **سوءاستفاده از کلیدها:**

- استفاده از کلید برای هدفی که کلید مجاز نیست، برای مثال، استفاده از کلید رمزبندی کلید برای رمزبندی داده.

- استفاده از تسهیلات مدیریت کلید برای هدفی که کلید مجاز نیست، برای مثال، رمزبندی غیرمجاز داده یا رمزگشایی داده.

- استفاده از کلید بعد از انقضای آن است.
- استفاده بیش از حد از کلید است.
- فراهم کردن کلیدهایی برای گیرنده غیرمجاز است.

پیوست ب
(اطلاعاتی)
اشیاء اطلاعاتی مدیریت کلید

شیء اطلاعاتی مدیریت کلید شامل کلید یا کلیدهایی به طور اختیاری با اطلاعات دیگری همراه است که چگونگی استفاده از کلیدها را کنترل می‌کنند. اطلاعات کنترلی ممکن است به جای این‌که صریح باشند، توسط قراردادهای کنترل‌کننده استفاده از شیء اطلاعاتی مدیریت کلید، ضمنی باشند. (برای مثال، استفاده از یک کلید از زوج کلید نامتقارن، توسط استفاده توافق شده دیگری، کنترل می‌شود که یکی برای رمزبندی و دیگری برای رمزگشایی است.

اطلاعات کنترلی ممکن است موارد زیر را کنترل کنند:

- نوع شیء که کلید ممکن است از آن حفاظت کند(برای مثال، شیء اطلاعاتی مدیریت داده یا کلید)؛
- عملیات معتبر (برای مثال، رمزبندی، رمزگشایی)؛
- کاربر مجاز؛
- محیطی که در آن کلید به کار می‌رود؛
- جنبه‌های خاص دیگری که در فن کنترلی مشخص یا کاربردی که از شیء اطلاعاتی مدیریت کلید استفاده می‌کند.

برای اهداف بهینه‌سازی، شیء اطلاعاتی مدیریت کلید ممکن است جزیی یا کامل در فرآیند تولید کلید، ایجاد شود.

مثال خاصی از شیء اطلاعاتی مدیریت کلید، گواهی کلید است. این امر ممکن است دربردارنده کمینه موارد امضاء شده زیر توسط صادرکننده گواهی باشد:

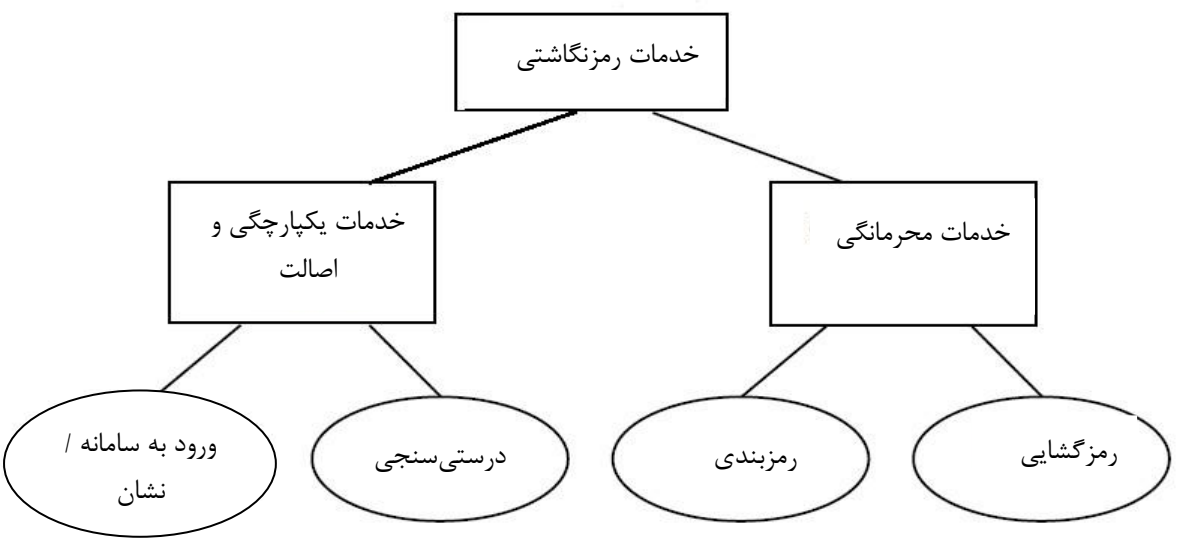
- موارد کلیدگذاری عمومی؛
- هویت کاربری که قادر به استفاده از شیء اطلاعاتی مدیریت کلید متناظر است؛
- عملیاتی که شیء اطلاعاتی مدیریت کلید متناظر، انجام می‌دهد(ممکن است ضمنی باشد)؛
- دوره اعتبار؛
- هویت مرجع صدور گواهی؛

پیوست پ
(اطلاعاتی)
رده‌های کاربردهای رمزنگاشتی

پ-۱ رده‌بندی متداول سامانه‌های رمزنگاشتی

رده‌بندی متداول سامانه‌های رمزنگاشتی توسط دو فن به کاررفته اصلی رمزنگاشتی، یعنی متقارن و غیرمتقارن، تعریف می‌شوند. به دلیل این که توصیه می‌شود مدیریت کلید هردو فن را فراهم کند، رویکرد دیگری موردنیاز است. از این رو بخش زیر، سامانه‌های رمزنگاشتی را مطابق با کارکرد ارائه شده توسط فن، رده‌بندی می‌کند.

به طور کلی، سامانه رمزنگاشتی دو نوع مختلف خدمت رمزنگاشتی را ارائه می‌کند: خدمات یکپارچگی و اصالت و خدمات محرمانگی. خدمات محرمانگی برای حفاظت رمزگونه از اطلاعات به کار می‌رود؛ یعنی، آن‌ها محرمانه بودن داده را تأمین می‌کنند. خدمات یکپارچگی و اصالت در ابتدا برای اصالت‌سنجی هستار، اصالت‌سنجی مبدأ داده، یکپارچگی و انکارناپذیری به کار می‌رود. انواع سامانه‌های رمزنگاشتی و عملیات متناظر آن‌ها در شکل پ-۱ نشان داده می‌شود.



شکل پ-۱-خدمات رمزنگاشتی و سازوکارهای متناظر آن‌ها

پ-۲ خدمات و کلیدهای یکپارچگی و اصالت:

خدمات یکپارچگی و اصالت، برای اصالت‌سنجی هستارهای ارتباطی(اصالت‌سنجی هستار)، برای اصالت‌سنجی منبع داده(اصالت‌سنجی مبدأ داده)، برای انکارناپذیری و برای یکپارچگی داده ارائه می‌شوند. این خدمات از سازوکارهای زیر استفاده می‌کنند:

- **مُهر و موم یک واحد داده:**

که شامل تولید ارزش وارسی رمزنگاشتی از داده برای یکپارچگی داده است، برای مثال تولید کد اصالت‌سنجی پیام(MAC) با الگوریتم متقارن. برای کدهای اصالت‌سنجی پیام(MAC)، به ISO/IEC 9797 مراجعه شود.

- **امضای یک واحد داده:**

که شامل تولید امضای رقمی برای اصالت‌سنجی مبدأ داده، یکپارچگی داده و یا انکارناپذیری است.

- **درستی‌سنجی یک واحد داده مُهر موم شده:**

که شامل محاسبه ارزش وارسی رمزنگاشتی داده و مقایسه آن با ارزش وارسی مرجع است.

- **درستی‌سنجی یک واحد داده امضاء شده**

که شامل درستی‌سنجی امضای رقمی برای تعیین این که آیا توسط صادرکننده پیام مدعی و یا توسط اثبات یکپارچگی داده، تولید شده است یا خیر.

در خدمات یکپارچگی و اصالت، فرآیندهای امضاء شده و مهر و موم شده، از اطلاعاتی استفاده می‌کنند که یا برای صادرکننده پیام خصوصی است(یعنی، منحصر به فرد و محرمانه) یا مخفی است و تنها توسط صادرکننده پیام و گیرنده آشکار می‌شود؛ فرآیند درستی‌سنجی یا از رویه‌ها و اطلاعاتی که به طور عمومی در دسترس هستند ولی از آن اطلاعات خصوصی صادرکننده پیام نمی‌تواند کسر شود، استفاده می‌کند یا از مخفی به اشتراک گذاشته صادرکننده پیام و گیرنده استفاده می‌کند. خصیصه لازم امضاء، امضایی است که می‌تواند تنها با استفاده از اطلاعات خصوصی صادرکننده پیام، *کلید مخفی* آن تولید شود. بنابراین وقتی که امضاء با استفاده از *کلید عمومی* صادرکننده پیام، درستی‌سنجی شود، سپس می‌تواند در طرف سوم اثبات شود(برای مثال، اصالت‌سنجی ثبت رسمی[1]) که تنها دارنده منحصر به فرد اطلاعات خصوصی است که می‌تواند امضاء تولید کند.

خدمات یکپارچگی و اصالت، دو تا از سه نوع کلید زیر استفاده می‌کنند:

- **کلید مهر و موم**: *کلید مخفی* به اشتراک گذاشته شده است.

- **کلید امضا**: *کلید خصوصی* و منحصر به فردی است که همبسته با صادرکننده پیام است.

- **کلید درستی‌سنجی**: یا *کلید عمومی* یا *کلید مخفی* است.

برای فنون متقارن، خدمات یکپارچگی و اصالت، از کلید مهر و موم و کلید درستی‌سنجی استفاده می‌کنند که توسط کلید مخفی مشابهی نمایش داده می‌شوند، برای فنون نامتقارن، از کلید امضاء و کلید

1 - notarisation authority

درستی‌سنجی استفاده می‌کنند که توسط زوج کلیدی شامل *کلید عمومی* و *کلید خصوصی* نمایش داده می‌شوند.

پ-۳ خدمات و کلیدهای محرمانگی

خدمات محرمانگی در ابتدا محرمانگی اطلاعات را تأمین می‌کنند. آن‌ها از دو سازوکار مبنا استفاده می‌کنند:
رمزبندی که متن رمز شده را از داده مفروض، تولید می‌کند.

رمزگشایی که متن رمز نشده را از متن رمز شده متناظر، تولید می‌کند.

خدمات محرمانگی ممکن است توسط فن رمزنگاشتی به کار رفته، یعنی متقارن یا نامتقارن، توصیف شوند. هنگام استفاده از فنون متقارن، عملیات رمزبندی و رمزگشایی توسط کلید مشابهی(کلید مخفی به اشتراک گذاشته شده) ساماندهی می‌شود. هنگام استفاده از فنون نامتقارن، عملیات رمزبندی و رمزگشایی توسط دو کلید مجزا ولی مرتبط یعنی، *کلید عمومی* و *کلید خصوصی* ساماندهی می‌شوند.

پ-۴ خدمت ترکیبی

برخی طرح‌های رمزبندی نیز ممکن است محرمانگی، یکپارچگی داده و یا اصالت‌سنجی مبدأ داده را تأمین کنند. به خصوص، طرح‌های رمزبندی اصالت‌سنجی شده توصیفی در ISO/IEC 19772 و نحوه عمل MULTI-SO1 از رمز جریان توصیفی در ISO/IEC 18033-4، محرمانگی، یکپارچگی داده و اصالت‌سنجی صادرکننده پیام را با استفاده از فنون رمزنگاشتی متقارن، تأمین می‌کند. طرح امضاءرمز توصیفی در ISO/IEC 29150، محرمانگی، یکپارچگی داده و اصالت‌سنجی پیام را با استفاده از فنون رمزنگاشتی نامتقارن، تأمین می‌کند. بسته یه فنون به کار رفته، توابع امنیتی از قبیل اصالت‌سنجی و انکارناپذیری ممکن است موجود باشد.

پیوست ت
(اطلاعاتی)
مدیریت چرخه حیات گواهی

ت-۱ کلیات

در جایی که صادرکننده گواهی به کار می‌رود، درخواست‌هایی از الزامات و رویه‌های زیر که آن‌ها در مدیریت چرخه‌های حیات گواهی کلید عمومی استفاده می‌شوند، توصیه می‌شوند:

ت-۲ مرجع صدور گواهی (CA)

ت-۲-۱ مسؤولیت‌های CA:

مرجع صدور گواهی (CA) توسط مشترکین خود مورد اعتماد قرار می‌گیرند. این‌گونه اعتماد مبتنی بر استفاده از سازوکارها و تجهیزات رمزنگاشتی مناسب و شیوه‌های مدیریت و کنترل حرفه‌ای می‌باشد. توصیه می‌شود این اعتماد توسط تابع ممیزی مستقلی(داخلی، خارجی یا هردو) تأیید شود که باید نتایج ممیزی را برای مشترکین، در دسترس قرار بدهند.

CA باید مسؤول موارد زیر باشد:

الف- شناسایی هستارهایی که اطلاعات کلید عمومی را برای صدور گواهی ارائه می‌کند.

ب- ایمن‌سازی فرآیند صدور گواهی و کلید خصوصی به کار رفته برای امضای اطلاعات کلید عمومی است.

پ- مدیریت داده مشخص برای سامانه است که باید در اطلاعات کلید عمومی موجود باشد، از قبیل شماره ردیف صدور گواهی کلید عمومی، شناسایی مرجع صدور گواهی، غیره.

ت- تخصیص و وارسی دوره‌های معتبر است.

ث- آگاه کردن هستار شناسایی شده در اطلاعات کلید عمومی،از این که گواهی کلید عمومی صادر شده است. توصیه می‌شود ابزار به کار رفته برای انتقال این آگاهی، مستقل از روش به کار رفته برای انتقال اطلاعات کلید عمومی در CA باشد.

ج- تضمین این‌که دو هستار مختلف، به هویت یکسانی تخصیص داده نمی‌شوند بدین صورت که آن‌ها را می‌توان به درستی متمایز کرد.

چ- نگهداری و صدور فهرست‌های ابطال است.

ح- رویدادنگاری تمام مراحل موجود در فرآیند تولید گواهی کلید عمومی است

یک CA می‌تواند اطلاعات کلید عمومی CA دیگر را گواهی کند تا گواهی کلید عمومی ارائه کند. از این رو اصالت‌سنجی ممکن است شامل زنجیره‌ای از گواهی‌های کلید عمومی باشد. توصیه می‌شود اولین گواهی

کلید عمومی در چنین زنجیره‌ای، توسط بعضی ابزار به جای گواهی‌های کلید عمومی، دست‌یابی و اصالت‌سنجی شود.

ت-۲-۲ زوج کلید نامتقارن CA

توصیه می‌شود، CA دارای دسترسی به تسهیلات مدیریت ایمن داشته باشد تا بتواند زوج کلید نامتقارن را برای استفاده توسط CA آن، تولید کند. فرآیند تولید باید غیرقابل‌پیش‌بینی موارد کلیدگذاری را تضمین کند. هیچ طرفی نباید با دانش فرآیند تولید، مزیتی به دست آورد.

کلید خصوصی CA برای امضای اطلاعات کلید عمومی هستار به کار می‌رود. از آن‌جایی که مالکیت آن، یک طرف را قادر به تغییرشکل به عنوان CA کرده و گواهی‌های کلید عمومی جعلی را تولید می‌کند، این امر باید سطح بالایی از حفاظت را ارائه شود. از این رو کلید خصوصی CA باید هنگام استفاده درون تسهیل مدیریت کلید به شدت حافظت شود.

یکپارچگی کلید درستی‌سنجی عمومی CA، برای امنیت سامانه گواهی کلید عمومی، ضروری است. اگر کلید عمومی CA در گواهی کلید عمومی موجود نباشد، در این صورت احتیاطات ویژه‌ای باید صورت گیرد تا توزیع اصالت‌سنجی شده آن را تضمین کند. در مقر جایگاه‌های کاربر، باید رخ دهد تا اصالت رونوشت ذخیره شده از کلید عمومی CA را تضمین کند.

کلید درستی‌سنجی عمومی CA، برای اعتبارسنجی گواهی‌های کلید عمومی کاربران دیگر به کار می‌رود. قبل از هر استفاده از کلید عمومی CA، کاربر باید تضمین کند که کلید درستی‌سنجی در حال حاضر معتبر است.

ت-۳ فرآیند صدور گواهی

ت-۳-۱ مدل صدور گواهی کلید عمومی

ت-۳-۱-۱ مدل مبنا

این بند فرعی، مدل مبنایی برای صدور گواهی کلیدهای عمومی تعیین می‌کند. این مدل، تابع‌های اصلی را از هستارهای منطقی تفکیک می‌کند(به زیربند ت-۱ مراجعه شود).

- **صادرکننده گواهی (CA):**

هستار مسؤول گواهی اطلاعات کلید عمومی هستار کاربر است.

- **مرجع نگهداری فهرست راهنما (DIR):**

هستار مسؤول در دسترس قرار دادن برخط گواهی‌های کلید عمومی برای آماده بودن جهت استفاده توسط هستارهای کاربر است

- **مولد کلید (KG):**

هستار مسؤول تولید زوج کلید نامتقارن است.

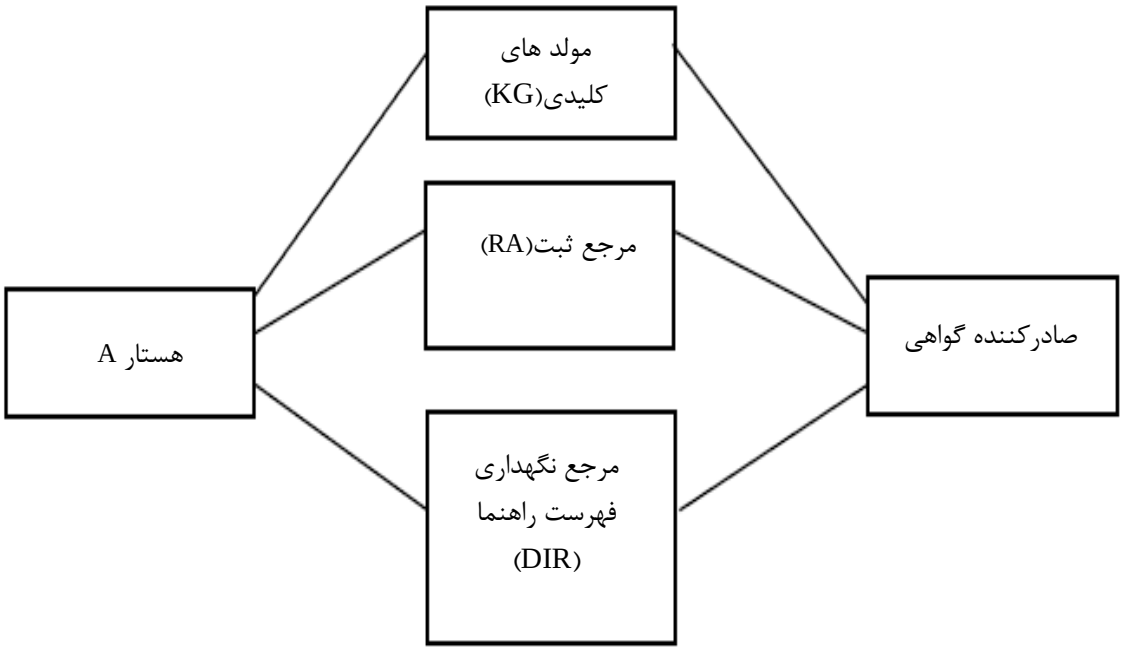
- **مرجع ثبت (RA):**

هستار مسؤول ارائه هویت‌های تضمین شده کاربر به CA است.

- **هستار کاربر(A):**

روابط بین هستارهای منطقی مدل و الزامات امنیتی متناظر در مورد این روابط، مورد بحث قرار می‌گیرند. هستارهای منطقی ممکن است ترکیب شوند. به عنوان مثال، A و KG ممکن است هنگامی که هستار کاربر زوج کلید نامتقارن را خود تولید کند، ترکیب شوند یا CA و KG ممکن است در صورتی کهCA ، زوج کلید از طرف هستارهای کاربر تولید کند، ترکیب شوند.

باید مراقبت شود تا گواهی تولید شده توسط RA و CA همانی باشد که توسط RA و CA که از هم مجزا و متمایز هستند، تولید شده است.



شکل ت-۱- مدل مبنا برای صدور گواهی کلید عمومی

ت-۳-۱-۲ روابط صدورگواهی

این بند فرعی بعضی از روابط صدور گواهی مدل مبنا و الزامات امنیتی متناظر را توصیف می‌کند. نیازی نیست که تمام این روابط در پیاده‌سازی سامانه ویژه، فعال باشند. برای نمونه، وظایف RA، CA و KG ممکن است ترکیب شوند.

- ***A-KG*:**

هستار A مولد کلید KG را برای تولید زوج کلید متقارن، درخواست می‌کند. KG برای تولید زوج کلید نامتقارن با کیفیت مناسب، مورداعتماد است. KG زوج کلید (S_A,V_A) را تولید می‌کند، بدین صورت که S_A کلید امضاء و V_A کلید درستی‌سنجی است و آن را به A دوباره انتقال می‌دهد. این انتقال باید به روشی اصالت‌سنجی شده و محرمانه شده صورت گیرد. KG و A باید به طور کامل مطمئن باشند که هیچ گونه طرف سومی نه می‌تواند زوج کلید نامتقارن را اصلاح کند و نه می‌تواند آن را در طول انتقال بخواند.

- ***R-RA*:**

هستار A، ثبت را توسط مرجع ثبت درخواست می‌کند. A باید اطلاعات هویتی خود را به RA ارائه کند. RA، اصالت اطلاعات A را درستی‌سنجی می‌کند و به طور احتمالی داده مشخص در سامانه را اضافه می‌کند. اطلاعات سپس به روشی ایمن، به CA هدایت می‌شود.

- ***A-CA*:**

هستار A، از صادرکننده گواهی، CA را درخواست می‌کند تا اطلاعات کلید عمومی خود (یا زیرممجموعه وابسته به آن) را از جمله کلید عمومی خود و نام متمایز خود را گواهی کند. ارائه اطلاعات کلید عمومی به CA باید به روشی صورت پذیرد که اصالت و یکپارچگی آن را تضمین کند. CA، اصالت اطلاعات کلید عمومی A را درستی‌سنجی می‌کند و به طور احتمالی، داده مشخص سامانه را اضافه می‌کند و سپس اطلاعات کلید عمومی تکمیلی را امضاء می‌کند تا گواهی کلید عمومی A تولید کند. گواهی کلید عمومی ممکن است در بعد به A دوباره انتقال داده شود.

پس از دریافت کلید عمومی صادرشده، A صحت خود را با استفاده از کلید درستی‌سنجی عمومی V_{CA}، از صادرکننده گواهی، درستی‌سنجی می‌کند. این کلید درستی‌سنجی عمومی V_{CA}، باید برای A به روشی اصالت‌شده در دسترس قرار بگیرد. از آن نقطه به بعد، کلید عمومی A می‌تواند به عنوان یک گواهی کلید عمومی، توزیع شود و توسط هر کسی که به کلید درستی‌سنجی عمومی CA دسترسی دارد، به کار رود.

با این حال اگر صادرکننده گواهی CA از KG درخواست کند تا زوج کلید نامتقارنی از طرف هستار A تولید کند، سپس زوج کلید A بایداز KG به A انتقال یابد. الزامات امنیتی برای انتقال، محرمانگی، یکپارچگی و اصالت می‌باشند. علاوه بر این، CA برای حفظ محرمانگی، یکپارچگی و اصالت تمام زوج کلیدهای نامتقارن در طی پردازش و ذخیره‌سازی، مورداعتماد است.

در نهایت، CA باید کلید خصوصی A را به A انتقال دهد و به طور کامل مطمئن باشد که هیچ گونه طرف سومی نمی‌تواند ارزش انتقال یافته را اصلاح کرده یا بخواند.

- ***A-DIR*:**

هستار A گواهی کلید عمومی خود را به مرجع نگهداری فهرست راهنما (DIR) انتقال می‌دهد و آن را در فهرست راهنما ثبت می‌کند. اصالت‌سنجی و کنترل دسترسی هستار برای ثبت گواهی کلید عمومی در فهرست راهنما موردنیاز است. باید توافقی بین A و DIR باشد به عنوان کسی‌که جهت مدیریت ورودی فهرست راهنمای هستار، مجاز است. در اولین فرانامه درخواست، DIR تمام ورودی‌های فهرست راهنما را مدیریت می‌کند. در دومین فرانامه درخواست، هر هستار X مسؤول ورودی فهرست راهنما خود بوده و آن را مدیریت می‌کند.

- ***RA-CA*:**

RA از CA درخواست می‌کند تا اطلاعات کلید عمومی A را گواهی کند. انتقال اطلاعات کلید عمومی A از RA به CA باید به روشی اصالت‌سنجی شده صورت گیرد. CA، اصالت اطلاعات کلید عمومی A را درستی‌سنجی می‌کند و به طور احتمالی داده‌ی مشخص سامانه را اضافه کرده و سپس اطلاعات گواهی کلید عمومی تکمیلی A را جهت تولید گواهی کلید عمومی A، امضاء می‌کند. CA به RA صدور گواهی را آگاهی می‌دهد.

- ***CA-KG*:**

صادرکننده گواهی CA از تولیدکننده کلید KG درخواست می‌کند تا زوج کلید نامتقارنی را از طرف هستار A، تولید کند. KG برای تولید زوج کلیدهای نامتقارن با کیفیت مناسب، مورداعتماد است. KG زوج کلید را تولید کرده و آن را به CA دوباره انتقال می‌دهد. این انتقال باید به روشی اصالت‌سنجی شده و محرمانه صورت گیرد. KG و CA باید به طور کامل مطمئن باشند هیچ گونه طرف سومی نه می‌تواند زوج کلید نامتقارن را اصلاح کند و نه می‌تواند آن را در طول انتقال بخواند. CA برای حفظ محرمانگی و اصالت تمام زوج‌های کلید نامتقارن در طی پردازش و ذخیره‌سازی مورداعتماد است.

- ***CA-DIR*.**

CA گواهی‌های کلید عمومی تولید شده را به طور مستقیم مرجع نگهداری فهرست راهنما(DIR) انتقال می‌دهد و آن‌ها را در فهرست راهنما ثبت می‌کند. اصالت‌سنجی و کنترل دسترسی هستار برای ثبت گواهی‌های کلید عمومی در فهرست راهنما موردنیاز می‌باشند

.

ت-۳-۲ ثبت

ت-۳-۲-۱ الزامات ثبت

ثبت کلید هستار، شامل ارائه درخواست گواهی هستار و اعتبارسنجی آن توسط RA یا CA می‌باشد. زیربندهای زیر، الزامات را همانطور که در ارائه درخواست گواهی هستار اعمال می‌کنند، نشان می‌دهند. درخواست گواهی ممکن است شامل ارزش کلید عمومی باشد یا که نباشد.

ت-۳-۲-۲ ارائه درخواست گواهی فردی

برای درخواست‌های کم‌مخاطره، پذیرش درخواست گواهی باید بر مبنای شناسایی فرد درخواست کننده برای گواهی کلید عمومی باشد. درخواست‌های گواهی نیاز به ارائه به صورت شخصی ندارند اما شیوه‌های کسب‌وکار قابل قبولی باید برای شناسایی فرد به کار روند.

برای درخواست‌های پُرمخاطره، پذیرش درخواست گواهی باید بر مبنای حضور شخصی(یا توسط نمایند مجاز) فرد درخواست کننده برای گواهی کلید عمومی باشد و استفاده از استانداردهای تجاری قابل قبول برای شناسایی فرد(و نماینده فرد در صورت لزوم) باشد. این امر ممکن است شامل درستی‌سنجی هویت توسط هستار طرف سوم مورداعتماد(TTP) باشد.

ت-۳-۲-۳ ارائه درخواست گواهی هستار حقوقی

پذیرش درخواست گواهی باید بر مبنای تحویل دستی اطلاعات درخواست گواهی توسط کمینه یک نماینده از هستار باشد و:

الف- امضاء و مهر و موم(در جایی که کاربردپذیر است) روی سربرگ مجوزدهی درخواست‌نامه، برای گواهی کلید عمومی.

ب- استفاده از شیوه‌های تجاری قابل قبول برای شناسایی امضاء و مهر وموم(در جایی که کاربردپذیر است) هستار و

پ- استفاده از شیوه‌های تجاری قابل قبول برای شناسایی نمایندگان تحویل‌دهنده اطلاعات درخواست گواهی.

ت-۳-۳ روابط بین هستارهای حقوقی

الزامی برای هستارهای حقوقی برای ورود به روابط قراردادی با هستارهای حقوقی دیگر وجود دارد. این امر ممکن است به روش‌های مختلفی انجام شود:

الف- کارمندان شرکت دارای زوج کلیدهای نامتقارن شخصی هستند. هستار حقوقی تنها به عنوان CA برای کارمندان شرکت خود عمل می‌کند. تراکنش‌ها توسط افراد با استفاده از کلیدهای شخص گواهی شده توسط CA شرکت، مجاز می‌شوند. گیرندگان وارسی می‌کنند که صادرکننده پیام توسط شرکت گواهی می‌شود که کلید عمومی به نوبه خود، توسط CA بالاتری گواهی می‌شود.

ب- کارمندان شرکت دارای زوج کلید نامتقارن شخصی نیستند. تنها هستار حقوقی دارای یک یـا چنـد زوج کلید نامتقارن است. گیرندگان وارسی می‌کنند که تراکنش‌ها سازگار با کلید عمومی شرکت باشد. گیرندگان نیازی به نگرانی برای خود با حقوق ویژه و خطوط‌مشی اجازه شرکت صادرکننده پیام ندارند.

ت-۳-۴ تولید گواهی

فرایند تولید گواهی کلید عمومی باید قبل از هر استفاده از زوج کلید نامتقارن صورت گیرد. مراحـل زیـر در فرایند تولید گواهی، موردنیاز است:

الف- وارسی اطلاعات کلید عمومی برای خطاها.

ب– پذیرش اطلاعات کلید عمومی: الزاماتی برای پذیرش اطلاعات کلید عمومی در زیربند ثبت در بالا تعیین می‌شوند.

پ- آماده‌سازی و افزودن داده‌ی موردنیاز برای مدیریت گواهی کلید عمومی؛ به طـور اختیـاری CA ممکـن است زوج کلید نامتقارن هستار را تولید کند.

ت- محاسبه امضاء برای گواهی کلید عمومی. این امرممکن است شامل تابع «چکیده‌ساز» باشد.

ث- ورودی رویدادنگاری ممیزی. اقدامات CA در فرایند تولید گواهی کلید عمومی باید رویدادنگاری شوند.

برای درخواست‌های با مخاطره بالا، ممکن است موارد زیر مطلوب باشـد ۱- بـا امضـاهای در حـال انجـام در تسهیلات رمزنگاشتی مستقل، نیاز به چند امضاء روی گواهی کلید عمومی توسط CA داشته باشد یا ۲- نیاز به چند امضاء روی اطلاعات کلید عمومی توسط CAهای مختلف داشته باشد.

ت-۳-۵ تجدیدنظر/ طول عمر

گواهی کلید عمومی دارای طول عمری است که توسط دوره اعتبار بیان شده در گواهی کلید عمومی، نشـان داده می‌شود یا در غیر این صورت توسط مدیریت CA، تعریف می‌شود.

ت-۴ توزیع و استفاده از گواهی کلید عمومی

ت-۴-۱ الزامات و رویه‌ها

این بند، الزامات و رویه‌هایی را توصیف می‌کند همانطور که برتوزیع و استفاده از گواهی‌هـای کلیـد عمـومی اعمال می‌شوند.

ت-۴-۲ توزیع و ذخیره‌سازی گواهی‌های کلید عمومی

هنگامی که گواهی کلید عمومی تولید می‌شود، هیچ گونـه سـنجش خاصـی نیـاز نـدارد تـا محرمـانگی یـا یکپارچگی خود را تضمین کند. گواهی‌های کلیـد عمـومی ممکـن اسـت در فهرسـت راهنمـا عمـومی بـرای دسترسی ساده کاربرها ذخیره‌سازی شود.

ت-۴-۳ درستی‌سنجی گواهی‌های کلید عمومی

به منظور اعتبارسنجی گواهی کلید عمومی، هستار درستی‌سنجی B، باید حداقل امضای CA را بر روی گواهی کلید عمومی درستی‌سنجی کند. اگر گواهی کلید عمومی یک دوره اعتبار تخصیص داده باشد، B باید تضمین کند که اطلاعات کلید عمومی هستار A در حال حاضر معتبر است(همچنین به ابطال گواهی، زیربند ت-۶ مراجعه شود). برای درستی‌سنجی گواهی کلید عمومی، ارزیاب باید دارای رونوشت معتبری از کلید درستی‌سنجی عمومی CA باشد.

ت-۵ مسیرهای گواهی

تمام CAها نیاز به دانستن و گواهی یکدیگر ندارند و نه نیازی به سلسله مراتب محکمی از CAها ندارند. احتمال می‌رود که CAها یکدیگر را (گواهی متقابل) گواهی کنند تا اجازه استفاده و تبادل انعطاف‌پذیری از گواهی‌های کلید عمومی را دهند. این گواهی متقابل باید با استفاده از سطوح تضمین بالا و بهترین روش دقیق انجام شود. هنگامی که شبکه‌ی متقابل گواهی‌های کلید عمومی وجود دارد، مسیرهای اعتبارسنجی گواهی‌های کلید عمومی را می‌توان ساخت. کاربر تنها نیاز به داشتن اعتماد در مورد کلید درستی‌سنجی یک CA دارد. این اعتماد در بعد از طریق مسیر گواهی به کلید عمومی صادر شده شرکای توسط CA نامعلومی، بسط می‌یابد.

ت-۶ ابطال گواهی

ت-۶-۱ الزامات ابطال

گواهی‌ها باید قبل از انقضای زمان‌بندی شده خود توسط صادرکننده CA، ابطال شوند. این امر ممکن است برای دلایلی از جمله موارد زیر رخ دهد:

الف- به خطر انداختن کلید عمومی هستار،

ب- درخواست برای حذف توسط هستار،

پ- تغییر وابستگی هستار،

ت— پایان‌دهی هستار،

ث- شناسایی غلط هستار،

ج- به خطر انداختن کلید خصوصی CA،

چ- پایان‌دهی CA

در پی آن، رویه و ابزار ارتباطات سریع باید ایجاد شوند تا حذفی ایمن و اصالت‌سنجی شده موارد زیر را تسهیل بخشد:

- یک یا چند گواهی کلید عمومی از یک یا چند هستار،

- مجموعه گواهی‌های کلید عمومی صادر شده توسط CA مبتنی بر زوج کلید نامتقارن به کار رفته توسط CA برای امضاء اطلاعات کلید عمومی،

- تمام گواهی‌های کلید عمومی صادر شده توسط CA، صرف‌نظر از تابع زوج کلید نامتقارن به کار رفته.

دو الزام آخر را برای ابطال گواهی‌های کلیدی، هنگامی که به خطر اندازی یا به خطر اندازی مشکوکی از کلید خصوصی CA رخ می‌دهد یا هنگامی که زوج کلید نامتقارن استفاده شده در گواهی‌های کلید عمومی تغییر می‌کند، ارائه می‌کند. خواه اینکه گواهی‌های کلید عمومی منقضی یا ابطال شوند، رونوشت‌های گواهی‌های کلید عمومی قدیمی باید توسط طرف سوم مورداعتماد(TTP) برای زمان موردنیاز توسط شیوه، قانون و تنشیم مقررات کسب‌وکار محتاط، حفظ شوند.

هنگامی که کلید خصوصی هستار یا CA به هر دلیلی حذف می‌شود، CA صادر کننده آن گواهی کلید عمومی، باید با اقدام سریعی به تمام هستارها در سامانه طلاع‌دهی کند که هر گونه گواهی کلید عمومی ابطال شده باشند. این امر ممکن است برای مثال پیام اصالت‌سنجی شده توسط CA را شکل دهد و به تمام هستارها ارسال کند.

هنگامی که گواهی کلید عمومی به خاطر به خطر انداختن واقعی یا مشکوک کلید خصوصی، ابطال می‌شود، کلید خصوصی نباید دیگر به کار رود. گواهی کلید عمومی باید تنها برای اهداف درستی‌سنجی به کار رود مشروط بر اینکه داده قبل از زمان ابطال‌سازی، امضاء شده است. علاوه بر این، هرگونه موارد کلیدگذاری رمزبندی‌شده توسط آن گواهی کلید عمومی(بدون توجه به نوع)، باید فوری متوقف شود.

هنگامی که گواهی کلید عمومی، برای دلایلی غیر از به خطر انداختن واقعی یا مشکوک، منقضی یا ابطال می‌شود، کلید خصوصی نباید دیگر به کار رود. گواهی کلید عمومی ممکن است هنوز برای مقاصد درستی‌سنجی یا رمزگشایی به کار رود. تمام موارد کلیدگذاری ارسالی و حفاظت شده توسط آن گواهی کلید عمومی(بدون توجه به نوع) باید به محض مناسب بودن، جایگزین شود.

ت-۶-۲ فهرست‌های ابطال

فهرست ابطال دربردارنده فهرست دارای مُهرزمانی از شماره‌های ردیف یا شناسانه‌های گواهی کلید معتبر برای آن دسته از گواهی‌های کلید عمومی است که توسط CA ابطال شده باشند. دو نوع مُهر زمانی را می‌توان برای فهرست ابطال به کار برد:

الف- تاریخ و زمانی که در آن CA، ابطال را صادر می‌کند؛

ب- تاریخ و زمان به خطراندازی آشکار یا مشکوک.

تاریخ بعدی، هنگامی که آشکار شد، ممیزی پیام‌های مشکوک را ساده‌تر در می‌آورد. گواهی کلید عمومی بـر روی فهرست ابطال تا تاریخ انقضای خود باقی می‌ماند. مُهر زمانی بسیار مهم است زیرا که باید مشخص باشد که چه زمانی انقیاد بین کلید عمومی هستار و هویت منحل شده است.

هنگامی که ابطال برای به خطراندازی مشخص یا مشکوک رخ داد، در صورتی که امضاء بعد از تاریخ مشکوک به خطراندازی پردازش شود یا در صورتی که تاریخ امضاء را نتوان به طور قابل اعتماد تعیین کـرد، اطلاعـات امضاء شده با استفاده از کلید خصوصی همبسته، نباید دیگر معتبر شناخته شوند. اطلاعات نباید با استفاده از کلید عمومی ابطال شده، رمزبندی شود.

فهرست ابطال باید:

- توسط CA تاریخ‌گذاری و امضاء شود بدین صورت که هستارها بتوانند یکپارچگی فهرست و تاریخ توزیع را اعتبارسنجی کنند.
- توسط CA در فواصل منظم صادر شوند حتی اگر هیچ گونه تغییری از زمان صدور آخر رخ نداده باشد
- برای تمام هستارهای سامانه به جز هنگام مسدود بودن، در دسترس باشد. برای مثال، توسط قانون، تنظیم مقررات یا قرار صادره از دادگاه

انواع سازوکارهای توزیع برای فهرست‌های ابطال امکان‌پذیر است که عبارتند از:

- تحویل به هر کاربر به عنوان پیام/ تراکنش توسط طرف سوم مورداعتماد (TTP)،
- درخواست‌ها به طرف سوم مورداعتماد(TTP) توسط کاربر برای وضعیت فعلی گواهی کلید عمومی مفروض،
- جستجوها برای CA برای فهرست ابطال فعلی خود،

CA باید به طور دوره‌ای فهرست ابطال جدیدی را منتشر و توزیع کند.

کتاب‌نامه

[۱] استاندارد ملی ایران به شماره ۱۰۸۲۲-۳: سال۱۳۸۷، فناوری اطلاعات -فنون امنیتی-مدیریت کلید -قسمت ۳-ساز و کارهای مبتنی بر فنون نامتقارن

[۲] استاندارد ملی ایران به شماره ۱۰۸۲۲-٤: سال۱۳۸۷، فن آوری اطلاعات -فنون امنیتی - مدیریت کلید-قسمت چهارم -مکانیزم مبتنی بر رازهای ضعیف

[3] ISO 7498-2, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

[4] ISO/IEC 9594-8, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks

[5] ISO/IEC 9796 (all parts), Information technology — Security techniques — Digital signature schemes giving message recovery

[6] ISO/IEC 9797 (all parts), Information technology — Security techniques — Message Authentication Codes (MACs)

[7] ISO/IEC 9798 (all parts), Information technology — Security techniques — Entity authentication

[8] ISO/IEC 10118 (all parts), Information technology — Security techniques — Hash-functions

[9] ISO/IEC 10181 (all parts), Information technology — Open Systems Interconnection — Security frameworks for open systems

[10] ISO 11568 (all parts), Banking — Key management (retail)

[11] ISO/IEC 11770-2, Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques

[12] ISO/IEC 11770-5, Information technology — Security techniques — Key management — Part 5: Group key management

[13] ISO/IEC 13888 (all parts), Information technology — Security techniques — Non-repudiation

[14] ISO/IEC 14888 (all parts), Information technology — Security techniques — Digital signatures with appendix

[15] ISO/IEC 18014 (all parts), Information technology — Security techniques — Time-stamping services

[16] ISO/IEC 18031, Information technology — Security techniques — Random bit generation

[17] ISO/IEC 18033 (all parts), Information technology — Security techniques — Encryption algorithms

[18] ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules

[19] ISO/IEC 19772, Information technology — Security techniques — Authenticated encryption

[20] ISO/IEC 29150, Information technology — Security techniques — Signcryption