استاندارد ملی ایران

INSO

...

1st.Edition

May.2015

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standard Organization

چاپ اول

اردیبهشت ماه ۱۳۹۴

فناوری اطلاعات – الزامات تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی

Information Technology - Requirements of Digital Certificate Path Building and Validation

ICS: 35.240.01

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه 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 حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیته ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته 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 شماره ۵ تدوین و در کمیته 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 درزمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی 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، گواهینامه 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
«الزامات تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی»

رئیس:	**سمت و/ یا نمایندگی**
فیاضی، اسماعیل (فوق لیسانس نرم‌افزار)	قائم مقام مدیرعامل شرکت ره آورد سامانه‌های امن
دبیر:	
عابدی، اسماعیل (کارشناس ارشد مدیریت فناوری)	کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه
اعضاء: (اسامی به ترتیب حروف الفبا)	
امین مقدم، عماد (فوق لیسانس مهندسی مخابرات رمز)	کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه
ایزدپناه، سحرسادات (فوق لیسانس فناوری اطلاعات)	سرپرست اداره تدوین استاندارد سازمان فناوری اطلاعات ایران
تختایی، بهامین (فوق لیسانس MBA)	کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه
تیمورنژاد، علی (فوق لیسانس فناوری اطلاعات)	کارشناس زیرساخت کلید عمومی شرکت پیام پرداز
جان نثار، نرگس (لیسانس مهندسی کامپیوتر)	کارشناس زیرساخت کلید عمومی شرکت ره آورد سامانه‌های امن
جعفرپور، مریم (فوق لیسانس نرم‌افزار)	کارشناس تحقیق و توسعه دفتر آمار و فناوری وزارت بهداشت
جامی، سارا	کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه

(کارشناس کامپیوتر)

حسینی، ریحانه — کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه

(لیسانس مهندسی کامپیوتر)

شادمان، مهدی — رییس گروه شبکه و سخت‌افزار سازمان ثبت اسناد و املاک کشور

(لیسانس سخت‌افزار)

فروزنده دوست، محمدرضا — سرپرست معاونت سیاست‌گذاری و اعتباربخشی فناوری اطلاعات ایران

(فوق لیسانس MBA)

فخرعطار، رضا — مدیر پروژه مرکز میانی نفت شرکت فاوانفت صباکیش

(کارشناس نرم‌افزار)

فلاح چای، سید مهدی — کارشناس مسئول مرکز دولتی صدور گواهی الکترونیکی ریشه

(فوق لیسانس مخابرات رمز)

فیروزیان، علیرضا — کارشناس سامانه‌های مبتنی بر کارت هوشمند شرکت فاوانفت صبا کیش

(کارشناس نرم‌افزار)

قسمتی، سیمین — کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

(فوق لیسانس فناوری اطلاعات)

کریمی، قدسیه — مسئول بخش PKE شرکت امن افزار گستر شریف

(کارشناس ارشد سخت‌افزار)

یارمحمدی، معصومه — مدیر دفتر ثبت‌نام شرکت امن افزار گستر شریف

(فوق لیسانس مخابرات رمز)

فهرست مندرجات

عنوان **صفحه**

پیشگفتار

استاندارد «الزامات تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی» که پیش‌نویس آن در کمیسیون‌های مربوط توسط مرکز دولتی صدور گواهی الکترونیکی ریشه تهیه و تدوین‌شده و در سیصد و هفتاد و پنجمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۹۴/۲/۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

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

منابع و مأخذی که برای تهیه این استاندارد مورداستفاده قرار گرفته به شرح زیر است:

۱- سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور

۲- سند جامع پروفایل‌های زیرساخت کلید عمومی کشور

۳- استاندارد ملی ایران به شماره ...، الزامات برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی ایران

4- RFC 5280: 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

5- RFC 5055: 2007, Server-Based Certificate Validation Protocol

6- NIST Recommendation for X.509 Path Validation, Version 0.5, May 3, 2004

مقدمه

در زیرساخت کلید عمومی از طریق گواهی‌های X509، مشخصات یا هویتِ یک هستار[۱] به کلید عمومی رمزنگاشتی[۲] آن پیوند داده می‌شود. یکی از مهم‌ترین قابلیت‌هایی که یک نرم‌افزار مجهز به زیرساخت کلید عمومی (PKE)[۳] باید به‌صورت مستقیم یا غیرمستقیم پشتیبانی نماید، فرآیند تشکیل و اعتبارسنجی مسیر گواهی است. از طریق این فرآیند می‌توان دریافت که به یک گواهی دیجیتال جهت استفاده در یک نرم‌افزار خاص می‌توان اعتماد نمود یا خیر؛ به عبارت دیگر در این فرآیند درستی پیوند بین هویت مالک گواهی و کلید عمومی او و همچنین کاربردی که گواهی دیجیتال جهت استفاده در این کاربرد صادر شده است، بررسی می‌گردد.

مسیر گواهی به دنباله‌ای از گواهی‌ها گفته می‌شود که از گواهی هستار نهایی[۴] شروع شده و به گواهی نقطه اعتماد[۵] زیرساخت کلید عمومی (گواهی مرکز ریشه) ختم می‌گردد و در آن هر گواهی دیجیتال توسط مرکز صدور این گواهی (CA)[۶]، امضاشده است. به‌عنوان‌مثال یک مسیر گواهی ممکن است شامل گواهی کاربر ($Cert_{User}$) که توسط CA امضاشده، گواهی CA($Cert_{CA}$) که توسط مرکز صدور گواهی ریشه[۷] امضاشده و گواهی متعلق به مرکز صدور گواهی ریشه ($Cert_{rootCA}$) که توسط خودش امضاشده است، باشد.

$$Cert_{(User)} \rightarrow Cert_{(CA)} \rightarrow Cert_{(rootCA)}$$

پردازش مسیر گواهی، مستلزم تشکیل این مسیر و اعتبار سنجی آن است و هدف آن بررسی اعتبار گواهی برای استفاده در یک برنامه کاربردی است. برای مثال باید بررسی شود که گواهی، متعلق به مالک گواهی است و نیز برای یک کاربرد خاص نظیر امضای دیجیتالیِ اسناد مناسب است یا خیر. در این استاندارد ملی به الزامات تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی در زیرساخت کلید عمومی کشور پرداخته شده است.

۱- Entity
۲- Cryptographic
۳- Public Key-Enabled
۴- End Entity
۵- Trust Point
۶- Certificate Authority (CA)
۷- Root CA

«الزامات تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی»

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین الزامات تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی جهت اطمینان از اعتبار گواهی‌های دیجیتال در نرم‌افزارهای به‌کارگیرنده قابلیت‌های گواهی دیجیتال است. این استاندارد برای کلیه نرم‌افزارهایی (مانند سامانه‌های صدور و مدیریت گواهی دیجیتالی و نرم‌افزارهای PKE) که فرآیند تشکیل و اعتبارسنجی مسیر گواهی را انجام می‌دهند، کاربردپذیر است.

لازم به ذکر است که توصیف الگوریتم اعتبارسنجی مسیر، خارج از قلمروی این استاندارد بوده و لازم است الگوریتم بکار گرفته‌شده جهت پیاده‌سازی، از الزامات این استاندارد پیروی نماید.

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 موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها موردنظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱- سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور

۲-۲- سند جامع پروفایل‌های زیرساخت کلید عمومی کشور

۲-۳- استاندارد ملی ایران به شماره ....، الزامات برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی ایران

۲-۴- استاندارد ملی ایران به شماره ....، الزامات امنیتی پودمان‌های رمزنگاشتی PKI

۲-۵- استاندارد ملی ایران به شماره ۱۷۱۱۳: سال ۱۳۹۲، الزامات ساختار نحوی پیام‌های رمزنگاشتی در زیرساخت کلید عمومی ایران

2-6- RFC 5280: 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

2-7- RFC 5055: 2007, Server-Based Certificate Validation Protocol

۳ اصطلاحات و تعاریف

در این استاندارد ملی اصطلاحات و تعاریف زیر بکار می‌رود:

۱-۳

مسیر گواهی

مسیری از گواهی‌ها که از یک طرف با گواهی هستار نهایی شروع شده و به گواهی نقطه اعتماد (گواهی مرکز ریشه) ختم می‌شود.

۲-۳

طول مسیر گواهی

تعداد گواهی‌های موجود در یک مسیر است.

۳-۳

شماره ردیف گواهی[۱]

فیلدی[۲] از گواهی، حاوی عددی که توسط مرکز صدور گواهی به هر گواهی اختصاص داده می‌شود. مقدار این فیلد برای هر گواهی صادرشده توسط یک مرکز صدور گواهی باید یکتا باشد.

۴-۳

گواهی دیجیتال

از انواع داده تعریف‌شده در استاندارد X.509 می‌باشد که در آن از یک امضای دیجیتالی برای برقراری تناظر یک‌به‌یک بین نام متمایزشده[۳] یک هستار و کلید عمومی او استفاده می‌شود. نام متمایزشده مرکز صدور (امضاکننده) گواهی، شماره ردیف گواهی، شناسانه الگوریتم استفاده‌شده توسط مرکز صدور گواهی به جهت امضا، دوره اعتبار گواهی و الحاقیه‌های[۴] مختلف، بخش‌های دیگر این نوع داده می‌باشند.

۵-۳

فهرست گواهی‌های باطل‌شده (CRL)[۵]

گواهی‌های دیجیتال که باطل شده‌اند و دیگر نباید آن‌ها را معتبر به‌حساب آورد را فهرست می‌نماید. این ساختار داده که توسط مرکز صدور CRL امضا می‌گردد، دربرگیرنده اطلاعاتی مشتمل بر نام متمایزشده مرکز صدور CRL، زمان انتشار CRL، زمانی که قرار است CRL بعدی منتشر گردد و فهرستی از شماره ردیف گواهی‌های باطل‌شده و زمان ابطال هر یک می‌باشد. این ساختار داده، همان ساختار داده تعریف‌شده در RFC1422 می‌باشد.

۶-۳

شناسه شئ (OID)[۱]

۱- Certificate Serial Number
2- Field
3- Distinguished Name
۴- Extension
۵- Certificate Revocation List

یکی از انواع اولیه در ساختار ASN.1 است.

۷-۳

X.509

استاندارد X.509 یکی از استانداردهای بخش استانداردسازی اتحادیه بین‌المللی مخابرات (ITU-T) برای زیرساخت کلید عمومی است که ساختار گواهی دیجیتال و CRL را تعیین می‌کند.

۸-۳

مرکز صدور گواهی (CA)

هستاری که مجاز به صدور و مدیریت گواهی‌های دیجیتال می‌باشد.

۹-۳

نام متمایزشده (DN)[۲]

نامی یکتا که یک هستار را مشخص می‌کند و در استاندارد X500 تعریف می‌گردد.

۱۰-۳

هستار نهایی (EE)[۳]

هستاری که یک زوج کلید در اختیار دارد و گواهی برای او صادر می‌شود. هستار نهایی به‌عنوان مالک گواهی دیجیتال از قابلیت‌های مختلف گواهی دیجیتال بهره می‌گیرد.

۱۱-۳

زیرساخت کلید عمومی (PKI)[۴]

به مجموعه‌ای از خدمات، محصولات، خط‌مشی‌ها، فرآیندها، سامانه‌های نرم‌افزاری و سخت‌افزاری گفته می‌شود که جهت مدیریت و به‌کارگیری گواهی‌های X.509 و به‌منظور ارائه خدمات امنیتی مختلف مبتنی بر رمزنگاری کلید عمومی[۵] مورداستفاده قرار می‌گیرد.

۱۲-۳

کارساز[۶]

سامانه‌ای که در جواب درخواست‌های سامانه‌ای دیگر به نام مشتری یا کارخواه[۷]، خدمت فراهم می‌کند.

۱۳-۳

کارخواه

۱- Object Identifier
۲- Distinguished Name
۳- End Entity
۴- Public Key Infrastructure
۵- Public Key Cryptography
۶- Server
۷- Client

سامانه‌ای که از سامانه‌ای دیگری که کارساز نامیده می‌شود، درخواست خدمت کرده و از این خدمت استفاده می‌کند.

۱۴-۳

notAfter

فیلدی در گواهی که حاوی تاریخ و زمانی است که بعد از آن گواهی قابل‌استفاده نیست.

۱۵-۳

notBefore

فیلدی در گواهی که حاوی تاریخ و زمانی است که قبل از آن گواهی قابل‌استفاده نیست.

۱۶-۳

پروتکل اعلام بر خط وضعیت گواهی‌ها (OCSP)[1]

پروتکلی است جهت اعلام و به دست آوردن برخط وضعیت اعتبار گواهی (ابطال یا عدم ابطال گواهی) که توسط یک کارسازِ متعلق به مرکز صدور گواهی، وضعیت ابطال یا عدم ابطال گواهی دیجیتال به نرم‌افزاری که نقش کارخواه OCSP را ایفا می‌کند، اعلام می‌گردد.

۴ کلمات کلیدی برای تعریف الزامات

در این استاندارد ملی الزامات ارائه‌شده، به سه نوع **الزام مشروط، الزام وابسته و الزام قطعی** تقسیم می‌شوند. الزام مشروط، الزامی است که در آن به‌طور مستقیم یا غیرمستقیم از قیدهای شرطی استفاده‌شده است. الزام وابسته به الزاماتی گفته می‌شود که وابسته به سطوح اطمینان[2] می‌باشند و برای کلیه سطوح کاربردپذیر نیستند. در این نوع الزامات از عبارت «بهتر است» استفاده‌شده است. همچنین الزام قطعی به الزامی گفته می‌شود که برای کلیه سطوح اطمینان، کاربردپذیر باشد و در آن از واژه «باید» به‌جای عبارت «بهتر است» استفاده‌شده است. ***جدول ۱***، انواع و مشخصات الزام به همراه واژه مورداستفاده در این استاندارد را نشان می‌دهد.

۱- Online Certificate Status Protocol

۲- سطوح اطمینان زیرساخت کلید عمومی کشور در مستند «سیاست‌های گواهی الکترونیکی در زیرساخت کلید عمومی کشور» از طریق تارنمای مرکز دولتی صدور گواهی الکترونیکی ریشه به آدرس www.rca.gov.ir منتشر شده است.

جدول ۱- انواع و مشخصات الزامات نرم‌افزارهای PKE

ردیف	انواع الزامات نرم‌افزارهای PKE	مشخصات الزام	واژه مورداستفاده
۱	مشروط	بسته به نوع نرم‌افزار و پشتیبانی نرم‌افزار از قابلیت‌های مختلف	«اگر»، «درصورتی‌که» و قیدهای شرطی دیگر
۲	وابسته	- وابسته به سطوح اطمینان - عدم کاربردپذیری برای کلیه سطوح اطمینان	«بهتر است»
۳	قطعی	کاربردپذیر برای کلیه سطوح اطمینان	«باید»، «نباید»، «لازم است»

یادآوری - کلیه الزامات یا احکام مرتبط با اعتبارسنجی مسیر گواهی دارای یک شناسانه منحصربه‌فرد می‌باشند که با الگوی AS[۱]-x-y-z به شرح جدول ۲ نمایش داده می‌شود (x: نوع الزام، y: حوزه الزام، z: شناسانه الزام در هر حوزه).

جدول ۲- اجزای شناسانه الزام

X	Y	Z
نوع الزام ۱: الزامات مربوط به اعتبارسنجی گواهی دیجیتال ۲: الزامات مربوط به پردازش وضعیت ابطال	حوزه الزام	شناسانه الزام در هر حوزه

۵ مفروضات

در این استاندارد ملی از مفروضات زیر در تدوین الزامات استفاده می‌شود:

۱. گواهی‌ها و CRL ها توسط یک CA و یک کلید خصوصی مشترک امضا می‌شوند؛ بنابراین نام ترکیبی موجود در گواهی CA با نام مرکز صدور CRL تطابق دارد. به‌علاوه نیازی به تشکیل مسیر کامل گواهی برای اعتبارسنجی امضای CRL وجود ندارد. درواقع همان کلید عمومی موجود برای اعتبارسنجی امضای گواهی باید برای امضای CRL نیز مورداستفاده قرار گیرد.

۱- AS کوته نوشت واژه Assertion است.

۲. الحاقیه "basic constraints" باید در تمام گواهی‌های CA وجود داشته باشد و در گواهی‌های هستارهای نهایی نیازی به وجود این الحاقیه نیست. در صورت عدم وجود الحاقیه مزبور در گواهی‌های هستار نهایی، نرم‌افزار نباید اعتبارسنجی گواهی را مردود نماید.

۳. در این استاندارد ملی فرض بر این است که برای انجام عملیات رمزنگاشتی از یک پودمان رمزنگاشتی منطبق با استاندارد ملی «الزامات امنیتی پودمان‌های رمزنگاشتی PKI» به شماره .... استفاده می‌شود.

۴. فرض بر آن است که پودمان تشکیل و اعتبارسنجی مسیر گواهی توصیف‌شده در این استاندارد ملی، در یک برنامه کاربردی مطابق با استاندارد ملی «الزامات برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی ایران» به شماره .... مورداستفاده قرار می‌گیرد.

۶ مشخصات پودمان تشکیل و اعتبارسنجی مسیر گواهی

شکل ۱، مؤلفه‌های عملیاتی اصلی یک «سامانه اعتبارسنجی مسیر[۱]» گواهی را نشان می‌دهد. مؤلفه اصلی سامانه اعتبارسنجی مسیر، پودمان اعتبارسنجی مسیر (PVM)[۲] است که وابسته به پودمان رمزنگاشتی به‌منظور اعتبارسنجی امضای دیجیتالی و پودمان تشکیل مسیر گواهی به‌منظور تشکیل مجموعه‌ای از گواهی‌ها و CRL ها می‌باشد. درواقع برای اینکه پودمان اعتبارسنجی مسیر به‌درستی عمل نماید، باید قابلیت‌های عملیاتی دیگری از طریق مؤلفه‌های عملیاتی دیگر به آن اضافه شود که این مؤلفه‌های عملیاتی همان پودمان رمزنگاشتی و پودمان تشکیل مسیر گواهی هستند. پودمان رمزنگاشتی، امضای گواهی‌ها و CRL ها را اعتبارسنجی می‌نماید. پودمان تشکیل مسیر نیز از طریق بازیابی گواهی‌ها و CRL ها یک مسیر بین گواهی هستار نهایی تا گواهی نقطه اعتماد، ایجاد می‌نماید. در برخی از نرم‌افزارها، مسیر گواهی از طریق یک کارساز بیرونی تشکیل و اعتبارسنجی مسیر گواهی منطبق با بخش ۹، ایجاد و پردازش می‌گردد که در این حالت نیازی به پیاده‌سازی پودمان PVM در این نرم‌افزارها نخواهد بود.

۱- Path Validation System

۲- Path Validation Module

شکل ۱- پودمان اعتبارسنجی مسیر

۷ تشکیل مسیر گواهی

قبل از اینکه یک گواهی مورد اعتماد قرار گیرد، باید اعتبار آن موردبررسی قرار گیرد. برای اعتبارسنجی یک گواهی باید مسیری از گواهی‌ها، بین آن گواهی تا گواهی نقطه اعتماد ایجاد شود. تشکیل مسیر گواهی با ایجاد یک یا چند مسیر گواهی منتخب همراه است، بدین معنی که ممکن است برخی از مسیرها با توجه به مواردی مانند طول، نام یا محدودیت‌های خط‌مشی معتبر نباشند؛ بنابراین ممکن است چندین مسیر انتخاب شوند اما تنها یک مسیر معتبر باشد.

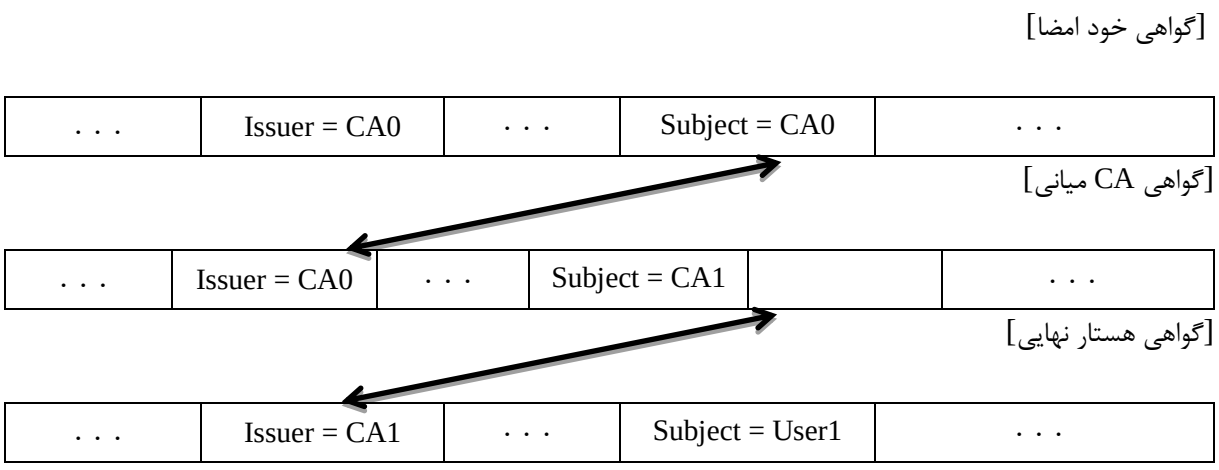
فرآیند تشکیل مسیر گواهی می‌تواند پیچیده باشد و تا حدودی ممکن است از طریق سعی و خطا انجام شود. برای انجام این فرآیند تاکنون استانداردی ارائه نشده است؛ بنابراین هدف در این استاندارد ملی بیان برخی روش‌های پایه برای تشکیل مسیر گواهی است که توسعه‌دهندگان نرم‌افزار می‌توانند از طریق این روش‌ها، پودمان تشکیل مسیر گواهی را پیاده‌سازی نمایند.

همان‌طور که اشاره شد تشکیل مسیر گواهی عبارت است از ایجاد مسیری از گواهی‌ها بین گواهی هستار نهایی تا گواهی نقطه اعتماد (گواهی مرکز ریشه) که به دو صورت قابل تشکیل است. درصورتی‌که فرآیند تشکیل مسیر گواهی از سمت گواهی هستار نهایی آغازشده و به گواهی نقطه اعتماد ختم شود آنگاه مسیر در جهت مستقیم ایجادشده است و برعکس اگر فرآیند تشکیل مسیر گواهی از سمت گواهی نقطه اعتماد آغازشده و به گواهی هستار نهایی ختم شود آنگاه مسیر در جهت معکوس ایجادشده است. استفاده از هر یک از این دو روش برای تشکیل مسیر گواهی امری اختیاری است اما برای ساختار سلسله مراتبی زیرساخت

کلید عمومی کشور، استفاده از روش مستقیم توصیه می‌شود. در ادامه به تشریح فرآیند تشکیل مسیر گواهی می‌پردازیم.

۱-۷ زنجیره‌سازی نام[۱]

مسیر گواهی برگزیده باید به‌گونه‌ای باشد که ارتباط و اتصالی بین نام گواهی نقطه اعتماد و گواهی هدف وجود داشته باشد. اگر بخواهیم مسیر را از گواهی نقطه اعتماد به گواهی هدف در نظر بگیریم باید نام مالک[۲] گواهی در یک گواهی با نام صادرکننده[۳] گواهی در گواهی بعدی موجود در مسیر برابر باشد. شکل ۲ به درک بهتر این مطلب کمک می‌کند. در این شکل مسیر گواهی، با یک گواهیِ خود امضا[۴] که حاوی کلید عمومی نقطه اعتماد است آغاز می‌شود و با گواهی هستار نهایی پایان می‌پذیرد. گواهی دیگری که در مسیر وجود دارد گواهی مرکز صدور میانی است. لازم به ذکر است که غیر از گواهی هستار نهایی، کلیه گواهی‌های موجود در مسیر، گواهی مرکز صدور میانی می‌باشند.



شکل ۲– مفهوم زنجیره‌سازی نام

در هنگام تشکیل مسیر گواهی در جهت مستقیم، می‌توان از نام صادرکننده گواهی هستار نهایی که در گواهی آن موجود است برای بازیابی گواهی متعلق به مرکزِ صدور گواهیِ هستارِ نهایی استفاده نمود. همان‌طور که در شکل ۲ ملاحظه می‌شود، فیلد Issuer = CA1 موجود در گواهیِ هستارِ نهایی، ما را به سمت گواهی CA1 هدایت می‌کند. پس از بازیابی گواهی CA1 می‌توان با استفاده از نام صادرکننده گواهی

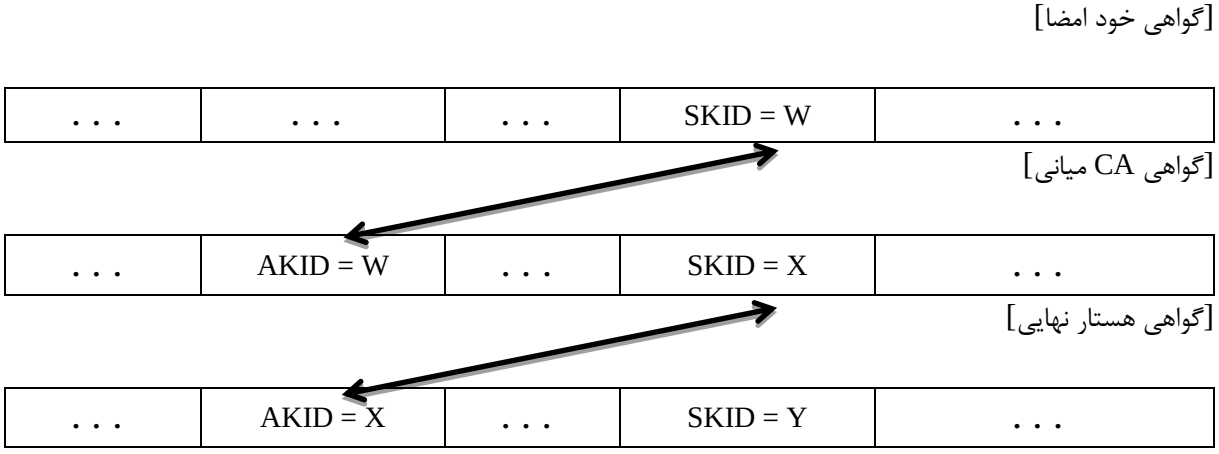
۱- Name Chaining
۲- Subject Name
۳- Issuer Name
۴- Self Signed Certificate

CA1، به گواهی نقطه اعتماد یعنی CA0 رسید. همین منطق برای زمانی که از روش معکوس برای تشکیل مسیر گواهی استفاده می‌شود نیز وجود دارد.

اگر CA ها تنها یک زوج کلید عمومی و خصوصی فعال در هرلحظه داشته باشند، استفاده از الزامات اتصال نام برای تشکیل مسیرهای گواهیِ برگزیده کافی است؛ اما گاهی ممکن است یک CA، بیش از یک زوج‌کلید فعال، با یک نام خاص و در یک دوره زمانی خاص داشته باشد. به‌عنوان‌مثال، زمانی که عملیات تجدید کلید برای گواهی نقطه اعتماد صورت گرفته باشد، این حالت رخ می‌دهد. این بدین معنی است که استفاده از اتصال نام گواهی‌ها به‌تنهایی برای تشکیل مسیر گواهی معتبر، کافی نیست. لذا نیازمند روش دیگری نیز برای تشکیل مسیر گواهی است که از طریق مفهوم زنجیره‌سازی شناسانه کلید[1] انجام می‌شود.

۲-۷ زنجیره‌سازی شناسانه کلید

شناسانه کلید مرکز صدور (AKID)[2] گواهی و شناسانه کلید مالک (SKID)[3] گواهی، در زمره الحاقیه‌های یک گواهی هستند که می‌توانند به‌منظور آسانی در فرآیند تشکیل مسیر گواهی مورداستفاده قرار گیرند. همان‌طور که در RFC5280 اشاره شده است AKID برای تشخیص یک کلید عمومی از کلید عمومی دیگر، در حالتی که یک CA دارای چندین کلید امضا است و نیز SKID برای شناسایی گواهی‌ها از روی کلید عمومی مالک گواهی، بکار می‌رود. به‌منظور تشکیل مسیر گواهی در جهت مستقیم، مشابه زنجیره‌سازی نام، AKID گواهی اول باید با SKID گواهی بعدی در مسیر برابر باشد. شکل ۳ مفهوم زنجیره‌سازی شناسانه کلید را نشان می‌دهد.



شکل ۳ – مفهوم زنجیره‌سازی شناسانه کلید

۱- Key Identifier Chaining
۲- Authority Key Identifier
۳- Subject Key Identifier

۸ الزامات اعتبارسنجی مسیر گواهی

در این بخش الزامات موردنیاز در یک برنامه کاربردی برای اعتبارسنجی مسیر گواهی آورده شده است. این الزامات در دو بخش اعتبارسنجی گواهی و اعتبارسنجی وضعیت ابطال، بیان می‌شود.

۸-۱ اعتبارسنجی گواهی

در این بخش الزامات اعتبارسنجی گواهی‌های موجود در مسیر گواهی در سه بخش با عنوان‌های الزامات عمومی پردازش گواهی، الزامات پردازش گواهی CA و پردازش خط‌مشی‌ها، بیان می‌شود.

۸-۱-۱ الزامات عمومی پردازش گواهی

در این بخش الزامات عمومی پردازش مسیر گواهی شامل گواهی‌های CA و گواهیِ هستارِ نهایی آورده شده است.

جدول ۳- الزامات پردازش گواهی

شناسانه[۱]	شرح الزام
AS-۱-۱-۱	پودمان اعتبارسنجی مسیر باید صحیح بودن ساختار نحوی[۲] گواهی‌های موجود در مسیر را بر اساس استاندارد X.509 و RFC5280 بررسی کرده و در صورت ناصحیح بودن ساختار نحوی باید اعتبارسنجی مسیر گواهی را با اعلام عدم موفقیت، متوقف نماید.
AS-۲-۱-۱	امضای کلیه گواهی‌های موجود در مسیر گواهی (به‌جز گواهی نقطه اعتماد) باید با کلید عمومی موجود در گواهی بالادستی، اعتبارسنجی گردد. امضای گواهی نقطه اعتماد را می‌توان از طریق کلید عمومی موجود در همان گواهی اعتبارسنجی نمود، لازم به ذکر است چگونگی تعیین یک گواهی دیجیتالی به‌عنوان نقطه اعتماد در مسیر گواهی، خارج از قلمروی این استاندارد است.
AS-۳-۱-۱	پودمان اعتبارسنجی مسیر باید اطمینان حاصل نماید که زمان موجود در فیلد notBefore هر گواهی، قبل از زمان فعلی باشد.
AS-۴-۱-۱	پودمان اعتبارسنجی مسیر باید اطمینان حاصل نماید که زمان موجود در فیلد notAfter هر گواهی، بعد از زمان فعلی باشد.
AS-۵-۱-۱	پودمان اعتبارسنجی مسیر، باید زنجیره‌سازی نام‌های گواهی‌ها و ارتباط بین آن‌ها را بررسی کند. اگر نام صادرکننده هر گواهی موجود در مسیر گواهی با نام مالک گواهی بالادستی آن برابر باشد آنگاه زنجیره‌سازی نام، صحیح است. (به‌طور مثال برای اولین CA میانی موجود در مسیر باید نام صادرکننده گواهی آن همان نام نقطه اعتماد باشد).

۱- Identifier

۲-Syntax

ادامه جدول ۳- الزامات پردازش گواهی

شناسانه	شرح الزام
AS-۱-۱-۶	پودمان اعتبارسنجی مسیر، باید وضعیت ابطال یا عدم ابطال گواهی هستار نهایی و هریک از گواهی‌های مراکز میانی را بررسی نموده و مسیری که شامل گواهی باطل‌شده باشد را نامعتبر اعلام نماید. همچنین چنانچه به هر دلیلی امکان تعیین وضعیت ابطال وجود نداشته باشد، باید مسیر نامعتبر اعلام شود یا هشدار[۱] مناسب بازگردانده شود.
AS-۱-۱-۷	پودمان اعتبارسنجی مسیر، بهتر است کاربرد گواهی را از طریق الحاقیه‌های Key Usage و Extended Key Usage موردبررسی قرار دهد. به‌عنوان‌مثال از یک گواهی که کاربرد آن منحصراً Key Encipherment قیدشده باشد، نباید برای امضا یا احراز هویت استفاده کرد یا یک گواهی با کاربرد امضا یا احراز هویت که فاقد مقدار Key Encipherment در الحاقیه Key Usage باشد، نباید به‌عنوان گواهی با کاربرد محرمانگی مورداستفاده قرار گیرد. درصورتی‌که گواهی‌های موجود در مسیر، دارای کاربرد مناسب نباشد، مسیر باید نامعتبر اعلام گردد.
AS- ۱-۱-۸	پودمان اعتبارسنجی مسیر، باید الحاقیه‌های بحرانی[۲] گواهی را (در صورت کاربردپذیری این الحاقیه‌ها) پردازش نموده و در صورت نامفهوم بودن آن‌ها یا درصورتی‌که شامل یک فیلد نامفهوم باشند، با اعلام عدم موفقیت، اعتبارسنجی مسیر گواهی را متوقف نماید.
AS- ۱-۱-۱۰	در صورت پشتیبانی یک برنامه کاربردی از پروتکل OCSP، باید الحاقیه Authority Information Access در گواهی‌هایی که مرکز صدور آن‌ها خدمات OCSP ارائه می‌دهد، قابل‌پردازش باشد.
AS-۱-۱-۱۱	پودمان اعتبارسنجی مسیر باید تطابق کاربرد گواهی را بین الحاقیهKey Usage و Extended Key Usage بررسی کند و در صورت عدم تطابق کاربردها با یکدیگر مطابق با RFC5280 بهتر است، مسیر نامعتبر اعلام شود یا هشدار مناسب بازگردانده شود.

۸-۱-۲ الزامات پردازش گواهی CA

در این بخش الزامات خاص مربوط به پردازش گواهی CA های موجود در مسیر گواهی بیان می‌شود.

جدول ۴- الزامات پردازش گواهی CA

شناسانه	شرح الزام
AS-۱-۲-۱	پودمان اعتبارسنجی مسیر بهتر است بررسی کند که کلیه گواهی‌های CA موجود در مسیر گواهی دارای الحاقیه Basic Constraints باشند. در صورت وجود این الحاقیه، باید باارزش "CA" مقداردهی شده باشد. اگر این الحاقیه در یک گواهی وجود نداشته باشد یا به‌صورت غیر بحرانی بوده و قابل‌شناسایی توسط نرم‌افزار نباشد آنگاه آن گواهی به‌عنوان گواهی هستار نهایی در نظر گرفته می‌شود و برای اعتبارسنجی امضای

۱- Warning
۲- Critical

شناسانه	شرح الزام
	گواهی‌ها بکار نمی‌رود.

ادامه جدول ۴- الزامات پردازش گواهی CA

شناسانه	شرح الزام
AS-۱-۲-۲	در صورت وجود یک گواهی دارای الحاقیه KeyUsage با مقدار KeyCertSign و نیز شامل الحاقیه Basic Constraints، پودمان اعتبارسنجی مسیر بهتر است اطمینان حاصل نماید که الحاقیه Basic Constraints گواهی دارای مقدار CA = True باشد.
AS-۱-۲-۳	پودمان اعتبارسنجی مسیر بهتر است اطمینان حاصل نماید که گواهی هر CA موجود در مسیر، دارای الحاقیه KeyUsage با مقدار KeyCertSign باشد. لازم به ذکر است در صورت نیاز به بررسی الحاقیه KeyUsage در گواهی CA، با توجه به بحرانی بودن این الحاقیه در پروفایل گواهی CA، پودمان باید قابلیت پردازش الحاقیه مزبور را داشته باشد. در غیر این صورت مسیر گواهی نامعتبر اعلام می‌شود.
AS-۱-۲-۴	پودمان اعتبارسنجی مسیر بهتر است اطمینان حاصل نماید که گواهی هر CA موجود در مسیر که شامل کلید عمومی امضاکننده CRL است، دارای الحاقیه KeyUsage با مقدار CRLSign باشد. لازم به ذکر است در صورت نیاز به بررسی الحاقیه KeyUsage در گواهی CA، با توجه به بحرانی بودن این الحاقیه، نرم‌افزار باید قابلیت پردازش الحاقیه مزبور را داشته باشد. در غیر این صورت مسیر گواهی نامعتبر اعلام شود.
AS-۱-۲-۵	پودمان اعتبارسنجی مسیر بهتر است، حداکثر طول مجاز مسیر را پردازش نماید. به‌طور مثال اگر اولین گواهی موجود در مسیر (از سمت نقطه اعتماد) دارای فیلد path length constraint در الحاقیه Basic Constraint با مقدار صفر باشد، آنگاه بعدازآن در مسیر گواهی نباید گواهی CA وجود داشته باشد.

۸-۱-۳ الزامات پردازش خط‌مشی‌ها

با توجه به الزامات خط‌مشی گواهی الکترونیکی زیرساخت کلید عمومی کشور[۱]، این استاندارد به بیان چند الزام در این حوزه می‌پردازد.

جدول ۵- الزامات پردازش خط‌مشی‌ها

شناسانه	شرح الزام
AS-۱-۳-۱	در زیرساخت کلید عمومی کشور وجود الحاقیه‌های Policy Mapping، Policy Constraints و Inhibit Any Policy در کلیه گواهی‌ها ممنوع شده است. لذا پودمان اعتبارسنجی مسیر نباید این الحاقیه‌ها را حتی در صورت وجود در گواهی، پردازش نماید.
AS-۱-۳-۲	به‌منظور تعیین خط‌مشی‌ها و سطوح اطمینان متناظر که تحت آن مسیر گواهی معتبر است، بهتر است

۱- آخرین نسخه مصوب سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور از طریق تارنمای مرکز دولتی صدور گواهی الکترونیکی ریشه به آدرس www.rca.gov.ir، قابل دسترسی می‌باشد.

شناسانه	شرح الزام
	پودمان اعتبارسنجی مسیر، قابلیت پردازش الحاقیه CertificatePolicies را داشته باشد.

ادامه جدول ۵- الزامات پردازش خط‌مشی‌ها

شناسانه	شرح الزام
۳-۳-۱-AS	بهتر است پودمان اعتبارسنجی مسیر، قابلیت تعیین مجموعه‌ای از خط‌مشی‌های پذیرفته‌شده (سطوح اطمینان پذیرفته‌شده) که تحت آن‌ها مسیر گواهی معتبر شناخته می‌شود را داشته باشد. **توجه:** این قابلیت می‌تواند از طریق تنظیمات پیکربندی یا از طریق یک پارامتر در فراخوانی توابع پودمان اعتبارسنجی مسیر، فراهم گردد.
۴-۳-۱-AS	در صورت پردازش الحاقیه Certificate Policy در گواهی و وجود مقدار ویژه anyPolicy با مقدار { ۰ ۳۲ ۲۹ ۵ ۲ } در این الحاقیه، برنامه کاربردی باید اعتبارسنجی مسیر گواهی را با اعلام عدم موفقیت، متوقف نماید.

۸-۲ اعتبارسنجی وضعیت ابطال گواهی

یکی از مراحل اعتبارسنجی مسیر گواهی دیجیتال در یک نرم‌افزار PKE، بررسی وضعیت ابطال یا عدم ابطال گواهی‌های موجود در مسیر است. بررسی وضعیت گواهی‌های دیجیتال به دو روش برون‌خط و برخط امکان‌پذیر است. روش برون‌خط از طریق فهرست گواهی‌های باطل‌شده (CRL) صورت می‌پذیرد که بر اساس استاندارد ملی «الزامات برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی ایران» به شماره .....، پشتیبانی از این روش در کلیه نرم‌افزارهای PKE الزامی است. در روش دوم بررسی وضعیت گواهی دیجیتال از طریق پروتکل OCSP و به‌صورت برخط صورت می‌پذیرد که در صورت پشتیبانی یک نرم‌افزار PKE از این روش، باید الزامات مربوطه منطبق با استاندارد مزبور در نظر گرفته شود. در ادامه این بخش، الزامات مرتبط با پردازش CRL، آورده شده است.

۸-۲-۱ الزامات مربوط به پردازش CRL

الزامات این بخش مربوط به پردازش CRL در هنگام اعتبارسنجی مسیر گواهی است.

جدول ۶- الزامات پردازش CRL

شناسانه	شرح الزام
۱-۱-۲-AS	پودمان اعتبارسنجی مسیر، باید قادر باشد تا CRL های معتبر برای هر گواهی را شناسایی نماید. درصورتی‌که CRL متناظر با هر یک از گواهی‌های موجود در مسیر شناسایی نشود، باید مسیر نامعتبر اعلام شود یا هشدار مناسب بازگردانده شود.
۲-۱-۲-AS	پودمان اعتبارسنجی مسیر، باید امضای هر فهرست گواهی باطل‌شده در مسیر گواهی را با استفاده از همان

شناسانه	شرح الزام
	کلید عمومی که برای امضای گواهی‌ها استفاده شده است، اعتبارسنجی نماید.
AS-۱-۲-۳	در هنگام بررسی وجود یک گواهی در CRL، پودمان اعتبارسنجی مسیر باید تطابق نام صادرکننده گواهی و نام مرکز صدور CRL را بررسی نماید.

ادامه جدول ۶- الزامات پردازش CRL

شناسانه	شرح الزام
AS-۱-۲-۴	درصورتی‌که هر یک از گواهی‌های موجود در مسیر باطل شده باشند، پودمان اعتبارسنجی مسیر باید مسیر را نامعتبر اعلام نماید. گواهی‌های باطل‌شده از طریق شماره ردیف گواهی در CRL مشخص می‌شوند.
AS-۱-۲-۵	درصورتی‌که هر یک از گواهی‌های موجود در مسیر باطل شده باشند، پودمان اعتبارسنجی مسیر باید بدون توجه به وجود الحاقیه‌های غیرقابل‌پردازش در CRL در بخش crlExtensions، مسیر گواهی را نامعتبر اعلام نماید.
AS-۱-۲-۶	درصورتی‌که زمان nextUpdate موجود در CRL قبل از زمان فعلی باشد، پودمان اعتبارسنجی مسیر نباید از آن CRL در عملیات اعتبارسنجی مسیر گواهی استفاده نماید. زمان nextUpdate درواقع مشخص‌کننده زمان و تاریخی است که CRL بعدی صادر خواهد شد.

۹ پروتکل اعتبارسنجی گواهی مبتنی بر کارساز (SCVP)[۱]

SCVP این امکان را به یک نرم‌افزار PKE می‌دهد که فرآیند تشکیل و اعتبارسنجی مسیر گواهی را به یک کارساز بیرونی واگذار نماید. مزایای استفاده از این پروتکل عبارت است از:

۱- به‌کارگیری SCVP برای پایانه‌هایی که دارای محدودیت‌های پردازشی هستند نظیر تلفن‌های همراه، بسیار مناسب است، زیرا این پایانه‌ها به‌عنوان کارخواه SCVP، متحمل بار پردازشی زیاد و پیچیدگی‌های عملیات تشکیل و اعتبارسنجی گواهی نمی‌شود و این عملیات را به کارساز SCVP واگذار می‌نمایند.

۲- اگر نرم‌افزار PKE یا کارخواه SCVP، در یک سازمان یا مجموعه‌ای قرارگرفته باشد که در آن لازم باشد خط‌مشی‌ها و الزامات اعتبارسنجی مسیر گواهی به‌صورت متمرکز مدیریت شود، استفاده از یک کارساز SCVP می‌تواند بسیار مفید باشد. این کارساز امکان اعمال الزامات و خط‌مشی‌های ابلاغ‌شده از سوی مرجع اعتماد (مرکز ریشه) را به‌صورت متمرکز فراهم می‌کند و از پیچیدگی‌های توسعه نرم‌افزارهای PKE می‌کاهد.

۱- Server-Based Certificate Validation Protocol

در این استاندارد ملی، واگذاری عملیات تشکیل و اعتبارسنجی مسیر گواهی به کارساز SCVP در دو حالت ذیل مجاز شمرده شده است:

۱- کارخواه SCVP می‌تواند به‌طور کامل تشکیل و اعتبارسنجی گواهی را به یک کارساز واگذار نماید که به این روش DPV[۱] گفته می‌شود.

۲- کارخواه SCVP می‌تواند فقط عملیات تشکیل مسیر را به یک کارساز واگذار کند که به این روش DPD[۲] گفته می‌شود.

۹-۱ الزامات پروتکل SCVP

با در نظر گرفتن ملاحظات ذیل، الزامات مرتبط با پروتکل SCVP منطبق با RFC5055 است:

۱- لازم است الزامات مربوط به خط‌مشی‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور در پیاده‌سازی و اجرای پروتکل SCVP در نظر گرفته شود.

۲- در پیاده‌سازی و اجرای پروتکل SCVP باید الزامات اعتبارسنجی مسیر گواهی منطبق با بخش ۸ این استاندارد ملی، در نظر گرفته شود.

۳- لازم است الزامات مرتبط با استاندارد ملی «الزامات برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی کشور» به شماره ..... در پیاده‌سازی و نگهداشت کارخواه و کارساز SCVP در نظر گرفته شود.

۴- ساختار پیام‌های رمزنگاشتی مورداستفاده در پروتکل SCVP باید از الزامات استاندارد ملی «ساختار نحوی پیام‌های رمزنگاشتی در زیرساخت کلید عمومی ایران» به شماره ۱۷۱۱۳، سال ۱۳۹۲ پیروی نماید.

۵- درخواست‌ها و پاسخ‌های پروتکل SCVP باید در حالت محافظت‌شده[۳] منطبق با RFC5055 مورداستفاده قرار گیرد.

۱- Delegated Path Validation

۲- Delegated Path Discovery

۳- Protected

کتاب‌نامه

[1] Public Key Interoperability Test Suite (PKITS) Certification Path Validation, Version 1.0, September 2004