بسمه تعالی

دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن

Pendar Kooshk Imen's Private Intermediate CA CPS

طبقه‌بندی: عادی

شماره ویرایش: ۰۴

شرکت پندار کوشک ایمن

مرداد ماه ۱۴۰۱

فهرست مطالب

فهرست جداول

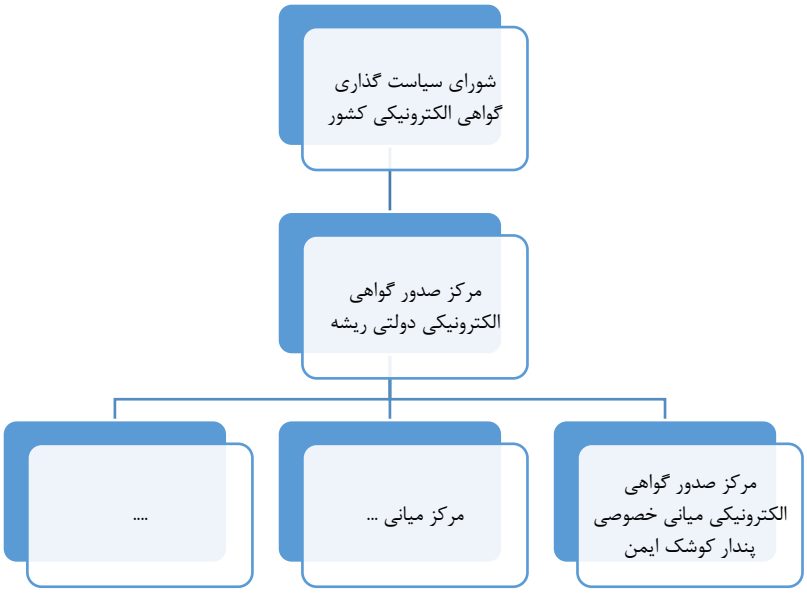
۱. مقدمه

شرکت پندار کوشک ایمن یک شرکت دانش بنیان عضو پارک علم و فناوری دانشگاه تهران می‌باشد. این شرکت در سال ۱۳۹۰ با هدف بومی‌سازی صنعت امنیت فناوری اطلاعات تاسیس شد. حوزه فعالیت شرکت پندار کوشک ایمن بطور تخصصی مرتبط با اعتماد دیجیتال و استناد پذیری اسناد و عملیات الکترونیک می‌باشد و در این حوزه محصولات تخصصی تولید، اختراعات مختلفی ثبت و پروژه‌های بسیاری در ابعاد ملی کشور انجام شده است. شرکت پندار کوشک ایمن در حوزه استناد پذیری اسناد و عملیات الکترونیک، در پروژه‌های کوچک و بزرگ مربوط به بخش دولتی و خصوصی حضور داشته است.

دستورالعمل اجرایی **"مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن"** که در این مستند به اختصار با عنوان **"مرکزمیانی"** شناخته می‌شود مبتنی بر سند **سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور** (که در این سند به اختصار سند سیاست‌های گواهی الکترونیکی نامیده می‌شود) در راستای فراهم کردن سرویس‌های گواهی الکترونیکی در حوزه‌های مختلف تولید شده است. این دستورالعمل بر پایه استاندارد X.509 و مطابق با RFC3647 تنظیم شده است.

لازم به ذکر است عنوان **مرکز دولتی صدور گواهی الکترونیکی دولتی ریشه**، زین پس در این مستند، به اختصار **مرکز دولتی ریشه** لحاظ می‌گردد.

سند پیشرو، رویه‌های عملیاتی و امنیتی صدور و مدیریت گواهی‌هایی که در سطوح اطمینان مختلف توسط این مرکز (به عنوان مرکز صدور گواهی الکترونیکی میانی خصوصی) صادر می‌شود را مشخص می‌کند. در شکل زیر جایگاه این مرکز در ساختار سلسله مراتبی زیرساخت کلید عمومی کشور آمده است.



برنامه‌هایی که قابلیت ارائه خدمات امنیتی مبتنی بر زیرساخت کلید عمومی را دارا می‌باشند، سرویس‌هایی مانند احراز هویت، محرمانگی[1]، تمامیت[2] و انکارناپذیری[3] را با استفاده از رمزنگاری کلید عمومی فراهم می‌کنند. قابلیت اطمینان رمزنگاری کلید عمومی نتیجه مستقیم عملکرد مطمئن زیرساخت کلید عمومی است که با طراحی و پیاده‌سازی مطمئن مرکز صدور گواهی الکترونیکی شامل تجهیزات، تأسیسات، کارکنان و فرایندها، حاصل می‌شود.

کلیه امور فوق با اخذ گواهی الکترونیکی و استفاده از آن انجام‌پذیر است. گواهی عبارت است از ساختاری از داده‌ها براساس استاندارد X.509 که به‌صورت دیجیتال امضا شده و صادر می‌گردد. این گواهی‌ها در مراکزی صادر می‌شوند که مورد اعتماد طرفین تبادل بوده و به نام «مرکز صدورگواهی الکترونیکی میانی» شناخته می‌شوند.

کلیه عملیات این مرکز مبتنی بر دو سند اصلی می باشد:

سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور(CP)» که اساسی‌ترین سند حاکم بر سیاست‌های کلی مراکز صدور گواهی الکترونیکی به شمار می‌رود. این سند ضوابط و الزامات عملیاتی، حقوقی و فنی جهت تأیید، صدور، مدیریت، نحوه استفاده، ابطال و تمدید گواهی در مراکز صدورگواهی الکترونیکی میانی را تشریح نموده و صاحبان گواهی می‌توانند با اطمینان، از خدمات مراکز مذکور استفاده نمایند. وجود یک مجموعه مقرراتی واحد، حافظ امنیت و یکپارچگی مراکز صدور گواهی الکترونیکی می‌باشد.

سند «دستورالعمل اجرایی مرکز صدورگواهی الکترونیکی میانی خصوصی پندار کوشک ایمن» که به تشریح دستورالعمل‌ها و روش‌های اجرایی برای صدور، نگهداشت و استفاده از گواهی‌های صادر شده توسط این مرکز بر اساس سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور» می‌پردازد.

سند حاضر «دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن» می‌باشد. این سند مطابق با RFC3647 تدوین‌گردیده است.

۱-۱ خلاصه

در این سند به ارائه مطالبی در حوزه گواهی الکترونیکی پرداخته شده است. با توجه به بخش‌های سند در بخش اول به توضیح مواردی چون دفتر ثبت‌نام، مالکان گواهی ، طرف‌های اعتماد کننده و کاربردهای گواهی، همچنین انواع کاربردهای مناسب گواهی کاربردهای غیرمجاز گواهی پرداخته شده است. در ادامه راهبری سیاست‌ها مانند اطلاعات تماس و سازمان راهبری بیان شده است. انتشار و وظایف مخزن به همراه مطالبی پیرامون کنترل دسترسی به آن و شناسایی و احراز هویت در ادامه توضیح داده شده است و انواع نام‌ها و قواعد تفسیر آن‌ها به همراه تائید شناسایی اولیه و روش اثبات تصرف کلید خصوصی و احراز هویت سازمان‌ها و افراد به تفصیل بیان شده است.

برای تکمیل این فرایندها به بیان نحوه ابطال و روال ابطال گواهی‌ها نیز اشاره شده است. روال‌های مربوط به صدور، پذیرش، تجدید، اصلاح، ابطال و تعلیق گواهی به همراه شرایط آن‌ها در ادامه سند با جزئیات ارائه شده ومحدودیت‌های دوره تعلیق و خدمات وضعیت گواهی نیز بیان شده است.

[1] Confidentiality
[2] Integrity
[3] Non Repudation

در ادامه به کنترل‌های عملیاتی، مدیریتی و تجهیزاتی و کنترل کارکنان پرداخته، بایگانی اطلاعات و بازیابی آن‌ها و کنترل‌های امنیتی فنی نیز بیان گشته است. تولید و نصب زوج کلید و محافظت از کلیدهای خصوصی وکنترل‌ها و استانداردهای دستگاه رمزنگاری در بخشی جداگانه توضیح داده شده است. مشخصات گواهی، CRL[4] و OCSP[5] و نحوه بازرسی لیست ابطال گواهی و شرایط بازرسی به همراه مطالبی پیرامون هویت و صلاحیت ارزیاب در ادامه مطالب ذکر شده است.

برای تکمیل کردن سند در انتهای آن به بیان الزامات حقوقی مانند تعرفه‌ها، اعم از تعرفه‌های صدور یا تجدید گواهی و نیز تعرفه‌های ابطال یا دسترسی و تعهدات مالی به همراه محافظت از اطلاعات شخصی اشاره شده است. همچنین حق مالکیت معنوی و محدودیت‌ها، مسئولیت‌ها و خسارت‌ها و مطالب مرتبط با آن‌ها عنوان شده است.

این مستند دو سیاست گواهی را برای صدور گواهی‌های الکترونیکی که در زیرساخت کلید عمومی کشور مورد استفاده قرار خواهند گرفت، و در سند سیاست‌های گواهی الکترونیکی کشور تعریف شده است، بیان می‌کند که این سیاست‌ها در سطوح اطمینان زیر تعریف شده‌اند.

سطح ۱ یا برنز

سطح ۲ یا نقره

در جدول زیر برای هر سطح اطمینان، گواهی‌هایی که تحت این سیاست‌ها صادر می‌شوند و موارد کاربرد هر سطح تعریف شده است.

جدول ۱ انواع گواهی با توجه به سطوح اطمینان

سطح اطمینان	نام گواهی	کاربرد
سطح ۱	برنز[6]	این سطح از گواهی می‌بایست در محیط‌هایی که ریسک و خسارات ناشی از سوءاستفاده، جعل و افشای اطلاعات پایین است، مورد استفاده قرار گیرد. از این سطح می‌توان برای تراکنش‌هایی که حاوی ارزش مالی پایین هستند و در آن‌ها امکان جعل و سوء استفاده پایین است، استفاده نمود. از گواهی‌های این سطح با در نظر گرفتن بند اول و دوم ، می‌توان برای تراکنش‌هایی که نیاز به احراز هویت، انکارناپذیری و یا محرمانگی دارند استفاده نمود. این سطح پایین‌ترین درجه اعتماد به هویت مالک گواهی را فراهم می‌نماید. یکی از کاربردهای اولیه سطح یک، فراهم کردن سرویس امنیتی تمامیت یا اطمینان از دست‌نخوردگی برای اطلاعاتی که امضا شده است، می‌باشد.

[4] Certificate Revokation List
[5] Online Certificate Status Protocol
[6] Bronze

سطح ۲	نقره[۷]	این سطح برای محیط‌هایی که در آن ریسک و خسارات ناشی از سوءاستفاده، جعل و افشای اطلاعات چندان زیاد نمی‌باشد (حد متوسط) مورد استفاده قرار گیرد. از این سطح می‌توان برای تراکنش‌هایی که حاوی ارزش مالی متوسط هستند و در آن‌ها امکان جعل و سوء استفاده چندان زیاد نمی‌باشد (حد متوسط)، استفاده نمود. از گواهی‌های این سطح با در نظر گرفتن بند اول و دوم، می‌توان برای تراکنش‌هایی که نیاز به احراز هویت، انکارناپذیری و یا محرمانگی دارند استفاده نمود.

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن دارای مجوز صدور گواهی الکترونیکی برای دو سطح اول و دوم می‌باشد.

۱-۲ نام و شناسه سند

این سند با عنوان "دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن" جهت ارائه دستورالعمل‌های اجرایی در راه‌اندازی و راهبری مرکز میانی نام‌گذاری و تدوین گردیده است. آخرین نسخه این سند از طریق وب سایت اینترنتی این مرکز به آدرس https://ica.pki.co.ir/download/ca/pkicps.pdf با جزئیات ذیل قابل دسترسی است.

این سند برای مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن قابل استفاده خواهد بود و مورد تایید و تصویب مرکز دولتی ریشه می‌باشد.

شناسه OID مطابق سند "سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور" برای دو سطح امنیتی عبارت است از:

سطح یک:	۲,۱۶,۳۶۴,۱۰۱,۱,۱,۱
سطح دو:	۲,۱۶,۳۶۴,۱۰۱,۱,۱,۲

۱-۳ اجزای زیر ساخت کلید عمومی

۱-۳-۱ مراکز صدور گواهی الکترونیکی

مرکز صدورگواهی الکترونیکی موجودیتی است که وظیفه صدور، انتشار، ابطال گواهی و تجدید کلید را بر عهده دارد. مراکز صدور گواهی الکترونیکی در زیر ساخت عمومی کشور از مرکز دولتی ریشه و مراکز صدور گواهی الکترونیکی میانی تشکیل شده است. مرکز دولتی ریشه طبق قانون وظیفه ایجاد، امضا، صدور و ابطال گواهی الکترونیکی مراکزصدور گواهی

[7] Silver

میانی را دارد. مرکز دولتی ریشه مسئول تمام ابعاد صدور و مدیریت مراکز صدورگواهی میانی، شامل نظارت بر فرآیندهای ثبت‌نام، احراز هویت، صدور گواهی‌های میانی، انتشار و ابطال گواهی و تجدید کلید می‌باشد.

به مراکزی که مجوز فعالیت و همچنین گواهی خود را از مرکز دولتی ریشه دریافت نموده باشند، مراکز صدور گواهی الکترونیکی میانی گفته می‌شود. این مراکز، صلاحیت صدور و ابطال گواهی مالکان گواهی را دارا هستند. مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن موجودیتی است که توسط مرکز دولتی ریشه مورد تأیید قرار گرفته و مجوز ایجاد، امضا و صدور گواهی الکترونیکی را برای موجودیت‌های نهایی دریافت کرده است. این مرکز براساس مصوبات شورای سیاست‌گذاری گواهی الکترونیکی کشور در کلاس ۲ مراکز گواهی میانی قراردارد و قابلیت صدور گواهی برای هر ۲ سطح اطمینان ۱و ۲ را خواهد داشت.

۱-۳-۲ دفاتر ثبت نام

دفتر ثبت‌نام موجودیتی است اختیاری که برای شناسایی، جمع‌آوری و بررسی صحت اطلاعات مربوط به هویت مالکان گواهی، با مرکز صدور گواهی الکترونیکی میانی همکاری می‌نماید، دفتر ثبت نام مورد تأیید مرکز صدور گواهی الکترونیکی میانی می‌باشد و پس از انعقاد قرارداد فی‌مابین، یک گواهی الکترونیکی توسط مرکز صدور گواهی الکترونیکی میانی (که در اینجا منظور مرکز صدور گواهی الکترونیکی میانی خصوصی شرکت پندار کوشک ایمن است) جهت امضای درخواست‌ها برای آن صادر می‌شود. دفتر ثبت‌نام مطابق با سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و این دستورالعمل فعالیت می‌کنند.

این دفتر مسئولیت ثبت اطلاعات درخواست‌دهنده گواهی الکترونیکی و صحت‌سنجی آن‌ها را دارد و انتقال درخواست به مرکز صدور گواهی الکترونیکی میانی و همچنین گرفتن پاسخ از مرکز را انجام می‌دهند و همچنین ثبت و صحت‌سنجی درخواست ابطال گواهی را نیز از مراجع ذیصلاح انجام می‌دهند.

در حال حاضر تنها یک دفتر ثبت نام درنظر گرفته شده است و درصورت توسعه دفاتر با عقد قرارداد جدید این دفاتر تاسیس خواهند شد.

۱-۳-۳ مالکان گواهی

مالک گواهی به موجودیتی گفته می‌شود که از مرکز صدور گواهی الکترونیکی میانی، گواهی الکترونیکی دریافت کرده و نام او به‌عنوان نام مالک گواهی ثبت شود و همچنین متعهد استفاده از کلید و گواهی بر طبق سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و این دستورالعمل باشد. هویت مالک گواهی قبل از صدور گواهی توسط دفتر ثبت‌نام احراز می‌شود.

انواع مالکان گواهی عبارتند از:

یک شخص، یک سازمان یا کارمندان یک سازمان، اجزای زیرساختی مثل فایروال یا سرویس‌دهنده و یا ابزار دیگری که در یک سازمان جهت برقراری ارتباط امن مورد استفاده قرار می‌گیرند.

۱-۳-۴ طرف های اعتماد کننده

طرف اعتمادکننده موجودیتی است که به صحت پیوند میان مشخصات مالک گواهی با کلید عمومی‌اش اعتماد کرده و گواهی الکترونیکی او را مورد استناد قرار می‌دهد.

براساس این اعتماد (به عبارت دیگر مطمئن بودن از صحت هویت مالک گواهی با کلید عمومی ذکر شده در گواهی و بررسی اعتبار گواهی مذکور) طرف اعتمادکننده می‌تواند به گواهی الکترونیکی اعتماد کند و از گواهی الکترونیکی با اطمینان در برنامه‌هایی که قابلیت ارائه خدمات امنیتی مبتنی بر زیرساخت کلید عمومی را دارا می‌باشند، سرویس‌هایی مانند احراز هویت، تمامیت و انکارناپذیری با استفاده از رمزنگاری کلید عمومی، استفاده کند.

۱-۳-۵ اجزای دیگر

وجود ندارد.

۱-۴ کاربردهای گواهی

۱-۴-۱ مصارف مناسب گواهی

کلیه گواهی‌های الکترونیکی صادر شده توسط این مرکز منطبق با سند پروفایل‌های زیرساخت کلید عمومی کشورقابل استفاده می‌باشد. کلیه گواهی‌های صادر شده توسط این مرکز تحت این دستورالعمل اجرایی می‌باشند و گواهی‌های صادر شده تحت این دستورالعمل مطابق با استاندارد X.509V3 می‌باشند. در این مرکز انواع گواهی در سطوح اطمینان ۱ و ۲ مطابق سند "سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور" صادر می‌شود.

جدول ۲ انواع کاربردهای گواهی

کاربرد/نوع گواهی	توضیحات
گواهی امضا	این گواهی جهت امضای اسناد و تراکنش‌های الکترونیکی و همچنین می‌تواند جهت احراز هویت کاربران[8] مورد استفاده قرار گیرد.
گواهی پست الکترونیکی امن	این گواهی از طریق پروتکل S/MIME امکان محرمانگی و امن کردن ایمیل را به واسطه رمزگذاری محتوای پیام و همچنین امضا نمودن آن فراهم می‌سازد.
گواهی احراز هویت	این گواهی جهت احراز هویت مالکان گواهی به منظور اعمال کنترل دسترسی جهت ورود به سیستم‌ها مورد استفاده قرار می‌گیرد. به عنوان مثال از این گواهی می‌توان برای ورود به سیستم از طریق احراز هویت دو عاملی[9] مبتنی بر کلید عمومی، در سیستم عامل‌های متعلق به مایکروسافت استفاده نمود. از طریق این گواهی می‌توان با استفاده از یک کارت هوشمند عملیات ورود به سیستم (Logon) را انجام داد.
گواهی مهر سازمانی	این گواهی به عنوان گواهی امضای یک شرکت یا سازمان تلقی شده و می‌تواند به عنوان مهرسازمانی آن شرکت یا سازمان در قالب امضای دیجیتال مورد استفاده قرار گیرد.
گواهی سرور	این گواهی جهت استفاده در سمت سرورهای مختلف در نظر گرفته شده است. دو نمونه از کاربردهای رایج این گواهی عبارتند از گواهی SSL/TLS و گواهی Domain Controller؛ **گواهی SSL/TLS** مختص یک نشانی اینترنتی (URL) صادر شده و به منظور تضمین اصالت یک سرور و به عبارتی تضمین ارتباط بین نشانی و وب سایتی که به آن مراجعه

[8] Client Authentication
[9] Two Factor Authentication

کاربرد/نوع گواهی	توضیحات
	می‌شود، به کار می‌رود. همچنین با استفاده از این گواهی ایجاد یک ارتباط امن و رمزنگاری شده بین برنامه مرورگر و وب سایت صورت می‌گیرد. **گواهی Domain Controller** نیز جهت ورود به سیستم در یک Domain و در سمت سرور (Domain Controller) مورد استفاده قرار می‌گیرد و متناظر با گواهی MS SmartCard Logon در سمت کاربر می‌باشد. گواهی اشیا: این گواهی جهت اشیا از قبیل دیواره آتش، سوییچ یا وسایل الکترونیکی به کار می‌رود.
گواهی CodeSigning	این گواهی جهت اطمینان از اصالت و حفظ جامعیت نرم‌افزارهای مختلف به ویژه نرم‌افزارهایی که از طریق اینترنت منتشر می‌شوند نظیر ActiveX و Java Applet به کار می‌رود. بنابراین زمانی که کاربران، نرم‌افزار امضا شده را دانلود می‌نمایند، می‌توانند نسبت به صحت محتوای کد منبع و نیز جامعیت آن از طریق این گواهی مطمئن شوند.
گواهی دفاتر ثبت نام (RA)	گواهی متعلق به دفاتر ثبت نام وابسته به یک مرکز صدور گواهی که جهت امضای درخواست‌ها در سمت RA مورد استفاده قرار می‌گیرد.
گواهی OCSP Signing[10]	گواهی متعلق به سرور پاسخگوی OCSP[11] که جهت امضای پاسخ‌های OCSP تنظیم شده توسط این سرور، مورد استفاده قرار می‌گیرد.
گواهی مراکز مهر زمانی[12]	اصولاً مهر زمانی جهت ثبت دقیق زمان در هنگام امضای اسناد مختلف از جمله قراردادها و یا توافق‌نامه‌ها و بایگانی آن ها مورد استفاده قرار می‌گیرد. با استفاده از مهر زمانی، می‌توان به طور شفاف اثبات نمود که داده‌های متناظر با یک مهر زمانی، از زمان مورد اشاره در مهر زمانی، تغییر داده نشده است. گواهی مهر زمانی جهت انجام عملیات امضا در فرایند مهر زمانی توسط مرکز مهر زمانی مورد استفاده قرار می‌گیرد.

۱-۴-۲ مصارف غیرمجاز گواهی

گواهی‌های صادره توسط مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن فقط در چارچوب کاربردهای مشخص شده برای آنها (طبق جدول ۲) قابل استفاده‌اند و استفاده از آنها در هر نوع کاربرد دیگری مجاز نیست.

مصارف غیر مجاز گواهی به شرح زیر است:

- گواهی‌ها نباید در موارد غیرقانونی و مخالف با نظم عمومی استفاده شوند.
- هر گواهی صرفاً باید برای کاربردهای در نظر گرفته شده برای همان گواهی، آنگونه که در جدول ۲ قید شده است، مورد استفاده قرار گیرد.
- گواهی‌های اشخاص و سرویس‌گیرندگان، برای استفاده در برنامه‌های کاربردی سرویس‌گیرنده صادر شده‌اند و نباید به عنوان گواهی سرویس‌دهنده و یا گواهی سازمانی مورد استفاده قرار گیرند.
- گواهی مالکان گواهی نباید به عنوان گواهی مراکز صدور گواهی اعم از ریشه یا میانی به کار رود.

[10] Online Certificate Status Protocol
[11] OCSP Responder
[12] Time Stamping Authority

۱-۵ راهبری سیاست ها

۱-۵-۱ سازمان راهبری سند

مسئولیت تدوین، اصلاح و بازنگری و انتشار این سند بر عهده مرکز صدور گواهی الکترونیکی میانی خصوصی شرکت پندار کوشک ایمن می‌باشد و مسئولیت تطبیق این سند با سیاست‌های گواهی الکترونیکی بر عهده مرکز دولتی ریشه می‌باشد و در صورت تایید، تصویب آن نیز بر عهده ی مرکز دولتی ریشه است.

۱-۵-۲ طرف تماس

سؤالات مربوط به دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن بر عهده این مرکز می‌باشد. اطلاعات تماس این مرکز به شرح زیر است:

نشانی پست الکترونیکی: info@pki.co.ir

نشانی پایگاه وب: https://pki.co.ir

شماره تلفن: 021-88220715 – 021-88220690

شماره فاکس: 021-88220690-1

نشانی: خیابان ولیعصر – خیابان فاطمی – نرسیده به میدان جهاد (فاطمی) – ساختمان اداری تجاری ۳۷ – پلاک ۴۹ – طبقه ۳ – واحد ۷

۱-۵-۳ مسئول تطبیق دستورالعمل اجرایی با سیاست‌های مرکز دولتی ریشه

مرکز دولتی ریشه مسئولیت تأیید، تطبیق و تصویب سند حاضر را با سند "سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور" برعهده دارد.

۱-۵-۴ فرایند تأیید دستورالعمل اجرایی

لازم است متقاضی تأسیس مرکز میانی، دستورالعمل اجرایی گواهی الکترونیکی (دستورالعمل اجرایی) خود را بر اساس RFC3647 و منطبق با سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور تدوین نموده و به همراه اسناد و مدارک مرتبط به مرکز دولتی ریشه ارائه نماید. دستورالعمل ارائه شده به همراه اسناد مرتبط در مرکز دولتی ریشه مورد ارزیابی، تایید و تصویب قرار می‌گیرد.

۱-۶ تعاریف و اختصارات

اختصارات و تعاریف مورد استفاده در سند به شرح زیر است:

- اختصارات

جدول ۳ اختصارات

مخفف	معادل	معنی

CA	**Certificate Authority**	موجودیتی که مجاز به صدور و مدیریت گواهی های الکترونیکی می‌باشد.
CP	**Certificate Policies**	مجموعه‌ای از قوانین که الزامات سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور را مشخص می‌نماید.
CPS	**Certificate Practice Statement**	دستورالعمل اجرایی که مرکز میانی برای صدور گواهی الکترونیکی از آن استفاده می‌نماید.
CRL	**Certificate Revocation List**	ساختمان داده‌ای که گواهی های الکترونیکی را که پیش از تاریخ انقضا، دیگر توسط صادرکننده گواهی معتبر به حساب نمی‌آیند، لیست می‌نماید.
CSR	**Certificate Signing Request**	قالب تراکنشی تعریف شده‌ای توسط استاندارد **PKCS#10**، حاوی نام متمایز و تعدادی مشخصه اختیاری می‌باشد که توسط موجودیت درخواست‌کننده گواهی الکترونیکی، امضا شده و به مرکز صدور گواهی فرستاده شده است و مرکز آن را به گواهی الکترونیکی **X.509** تبدیل می‌نماید.
DN	**Distinguished Name**	شناسه منحصر به فردی که شی موجود در درخت اطلاعاتی دایرکتوری قالب **X.500** را ارائه می‌نماید.
DNS	**Domain Name System**	**DNS** یا سیستم نام‌گذاری دامنه، روشی سلسله مراتبی است که بانک اطلاعاتی مربوط به نام‌های نمادین و معادل **IP** آن ها را بر روی کل شبکه اینترنت توزیع کرده است. هر ایستگاه می‌تواند در یک روال منظم و سلسله مراتبی نشانی **IP** معادل با ایستگاه مورد نظرش را در نقطه‌ای از شبکه پیدا نماید. این سیستم در سال ۱۹۸۴ معرفی شده است.
FIPS	**Federal Information Processing Standard**	راهنمایی‌های تخصصی که **NIST** برای تهیه تجهیزات سیستم و سرویس پردازشگر اطلاعاتی تهیه کرده است.
IETF	**Internet Engineering Task Force**	**IETF** جامعه بین‌المللی بزرگی از طراحان شبکه، اپراتورها، فروشندگان و محققان مرتبط با سیر تکاملی معماری اینترنت و کارکرد روان و دقیق اینترنت است.
OCSP	**Online Certificate Status Protocol**	پروتکلی است که جهت اعلام برخط وضعیت ابطال یا عدم ابطال گواهی **X.509** به کار می‌رود. ماهیت پروتکل**OCSP** مبتنی بر درخواست و پاسخ است.
OID	**Object Identifier**	شناسه‌ای منحصر به فرد و رسمی، تشکیل شده از مجموعه‌ای از اعداد (تعریف شده در استاندارد **ASN.1**) که برای اشاره به اشیا با ویژگی‌های مشخص استفاده می‌شود.
PKCS #10	**Public Key Cryptography Standard**	استاندارد رمزنگاری کلید عمومی شماره **10** که ساختاری را برای درخواست گواهی تعریف می‌نماید.
PKI	**Public Key Infrastructure**	مجموعه‌ای از خدمات، محصولات، سیاست ها، فرایندها و سیستم‌های نرم‌افزاری و سخت‌افزاری که جهت مدیریت و بکارگیری گواهی های

		الکترونیکی **X.509** و به منظور ارائه سرویس‌های امنیتی مختلف مبتنی بر رمزنگاری کلید عمومی مورد استفاده قرار می‌گیرند.
PKIX	**Public Key Infrastructure (X.509)**	گروه **PKIX** در سال ۱۹۹۵ با هدف توسعه استانداردهای اینترنت برای پشتیبانی از زیرساخت‌های کلید عمومی مبتنی بر **X.509**، تأسیس شد.
RA	**Registration Authority**	موجودیتی اختیاری در زیرساخت کلید عمومی می‌باشد که گواهی های الکترونیکی یا لیست گواهی های باطل شده را امضا نمی‌نماید ولی مسئولیت ثبت و شناسایی اطلاعات مورد نیاز مرکز صدور گواهی برای صدور گواهی الکترونیکی یا لیست گواهی های باطل شده و اجرای وظایف مدیریت گواهی را دارد.
RFC	**Request For Comment**	توافق‌نامه منتشر شده توسط **IETF** در توصیف روش، رفتار، پژوهش و یا نوآوری برای کار با اینترنت و سیستم‌های متصل به اینترنت است.
RSA	**Rivest-Shamir-Adelman**	االگوریتم رمزنگاری کلید عمومی که در سال ۱۹۷۸ توسط سه نفر به نام‌های ران ریوست، ادی شامیر و لئونارد آدلمن اختراع شده است.
URL	**Uniform Resource Locator**	رشته‌ای از کاراکترها که مکان منبعی که در اینترنت قابل دسترس است را مشخص می‌نماید.
X.500	**X.500**	مجموعه‌ای از استانداردهای ارائه شده توسط **ITU-T** و سازمان جهانی **ISO** که «سرویس دایرکتوری» را به دقت توصیف می‌نماید.
X.501	**X.501**	استانداردی در مجموعه استانداردهای سری **X.500** است. یک موجودیت شبکه مانند مسیریاب، ممکن است به شناسه **X.501** برای استفاده از سرویس دایرکتوری **LDAP** و یا تولید درخواست‌های گواهی **PKCS** نیاز داشته باشد.
X.509	**X.509**	استانداردی در مجموعه استانداردهای سری **X.500** که برای احراز هویت در مجموعه سیستم دایرکتوری تعریف شده است، در حال حاضر رایج‌ترین استاندارد برای صدور گواهی الکترونیکی به شمار می‌رود.

تعاریف

جدول ۴ تعاریف

لغت	معادل	معنی
ابطال گواهی	Certificate Revocation	اعلام عدم اعتبار گواهی الکترونیکی که توسط یک مرکز صدور گواهی صادر شده و دارای مهلت اعتبار نیز می‌باشد.
احراز هویت	Authentication	فرایند شناسایی هویتی که توسط یک شخص یا برای یک موجودیت سیستمی ادعا شده است.

احراز هویت بایومتریک	Biometric Authentication	شیوه تولید اطلاعات احراز هویت اشخاص از طریق الکترونیکی کردن مشخصات فیزیکی مانند اثر انگشت.
اختیارات	Authorization	مکانیزمی که بر اساس آن مشخص می‌شود موجودیتی که هویت واقعی آن احراز شده، مجوز انجام چه کارها و عملیاتی را دارد.
اطلاعات فعال‌ساز	Activation Data	اطلاعاتی خصوصی (غیر از کلیدها) که برای دسترسی به کلید خصوصی، مورد نیاز هستند.
اطمینان	Assurance	مشخصه‌ای از سیستم اطلاعاتی که اطمینان می‌دهد سیستم مطابق با سیاست‌های امنیتی کار می‌نماید.
اعتبار	Authenticity	اصل، قابل اطمینان و قابل تشخیص بودن.
اعتبار گواهی	Validity of Certificate	یک واحد داده در گواهی الکترونیکی که دوره زمانی اعتبار پیوند بین اطلاعات گواهی و کلید موجود در گواهی را مشخص می‌نماید (مگر زمانی که گواهی در لیست گواهی‌های باطل شده قرار بگیرد).
امحا	Zeroize	روشی برای پاک کردن الکترونیکی اطلاعات ذخیره‌شده با تغییر محتویات مخزن اطلاعات است به طوری که از بازیابی اطلاعات جلوگیری شود.
امضای الکترونیکی	Digital Signature	یک رشته عددی که به روش پیچیده‌ای از متن یک سند استخراج و پس از رمزنگاری با کلید خصوصی صاحب سند، به اصل سند ضمیمه و ارسال می‌شود به گونه‌ای که هر گیرنده اطلاعات بتواند منبع و تمامیت اطلاعات را تشخیص دهد.
امنیت	Security	اقداماتی که برای حفاظت از یک سیستم انجام می‌شوند مثل: پیشگیری یا کاهش احتمال وقوع رخدادهای خطرناک و احیای سیستم هنگام وقوع این رخدادها
انقضا گواهی	Certificate Expiration	عدم اعتبار گواهی به دلیل پایان طول عمر اختصاص یافته به گواهی.
انکارناپذیری	Non- Repudiation	مجموعه مکانیزم‌هایی که به پیام‌ها و تراکنش‌ها، پشتوانه حقوقی می‌بخشد و اجازه نمی‌دهد که فرستنده به هر طریق ارسال پیام خود را انکار نماید و یا گیرنده منکر دریافت آن شود.
بازرسی	Compliance Audit	بررسی و بازبینی مستقل اسناد و فعالیت‌های سیستم برای تشخیص کفایت کنترل‌های سیستم، اطمینان از مطابقت با دستورالعمل اجرایی، شناسایی نقص در سرویس صدور گواهی و پیشنهاد تغییرات به منظور اقدام متقابل.

بازیابی کلید	Key Recovery	فرایند به دست آوردن مقدار یک کلید رمزنگاری که قبلاً برای انجام عملیات رمزنگاری به کار می‌رفت.
بایگانی	Archive	مجموعه‌ای از اطلاعات که برای مدت زمان طولانی برای مقاصدی مانند پشتیبانی سرویس ثبت رویدادها و سرویس تمامیت سیستم ذخیره می‌شوند.
بررسی صحت هویت	Identity Verification	ارائه اطلاعاتی برای اثبات اینکه هویت ادعا شده، واقعی است.
به‌روز رسانی گواهی	Certificate Renewal	تولید یک گواهی جدید همسان با گواهی قبلی است به جز آنکه گواهی جدید دارای یک مدت اعتبار متفاوت و یک شماره سریال متفاوت می‌باشد.
پاسخگوی OCSP	OCSP Responder	سرویس‌دهنده‌ای که وضعیت ابطال یا اعتبار گواهی X.509 را به صورت برخط اعلام می‌نماید. ماهیت پروتکل OCSP مبتنی بر درخواست و پاسخ است.
پروتکل اعلام بر خط وضعیت گواهی‌ها	Online Certificate Status Protocol	یک پروتکل اینترنتی برای به دست آوردن وضعیت اعتبار گواهی الکترونیکی و اطلاعات مرتبط با آن توسط مشتری از سرویس‌دهنده.
پیکربندی	Configuration	تنظیمات نرم‌افزاری و سخت‌افزاری سیستم‌های رایانه‌ای.
پیمانه	Modulus	مقدار ثابت تعریف شده در حساب پیمانه‌ای که معمولاً بخشی از کلید عمومی سیستم رمزنگاری RSA بر اساس حساب پیمانه‌ای می‌باشد.
تجدید کلید گواهی	Certificate Rekey	فرایند تجدید کلید عمومی گواهی الکترونیکی موجود با صدور گواهی جدیدی که دارای کلید متفاوت جدیدی است.
ترمیم خرابی	Disaster Recovery	فرایندی که کلیه اطلاعات از دست رفته را در زمان وقوع آتش، تخریب، حوادث طبیعی، یا خرابی سیستم بازیابی می‌نماید.
تعلیق گواهی	Certificate Suspension	عدم اعتبار موقت گواهی الکترونیکی.
تمامیت	Integrity	مجموعه مکانیزم‌هایی که از هرگونه تغییر، دست‌کاری، تکرار یا حذف غیرمجاز اطلاعات پیشگیری می‌کنند یا حداقل باعث کشف چنین اقداماتی می‌شوند.
تمدید گواهی	Certificate Renewal	فرایند تمدید اعتبار اطلاعات گواهی الکترونیکی با صدور گواهی جدید.
توکن	Token	یک رسانه الکترونیکی قابل حمل جهت نگه‌داری ایمن زوج کلید رمزنگاری و مقادیر مربوط به شناسایی و انجام محاسبات

		مرتبط به آن‌ها (به عنوان مثال عملیات رمزنگاری مختلف) می‌باشد. همچنین از این وسیله می‌توان برای اعمال کنترل دسترسی استفاده کرد.
تولید کلید	Key Generation	فرایند تولید کلیدهای رمزنگاری
ثبت نام	Registration	یک اقدام یا فرایند اجرایی برای ثبت اولیه نام و مشخصه‌های دیگر یک موجودیت در مرکز صدور گواهی یا دفتر ثبت نام (پیش از صدور گواهی الکترونیکی).
الحاقیه‌های گواهی	Certificate Extensions	اطلاعاتی که برای افزودن مشخصات اضافی به گواهی X.509V3 تعریف شده‌اند.
حق مالکیت معنوی	Intellectual Property Right	حق کنترل و ایجاد مزایا نسبت به آنچه اختراع، اکتشاف یا ایجاد شده است.
در خطر افشا قرار گرفتن	To be Compromised	یک حادثه امنیتی که تحت آن اطلاعات در معرض دسترسی غیرمجاز قرار می‌گیرند.
درخواست گواهی	Certificate Request	پیامی مبتنی بر درخواست داشتن یک گواهی امضا از سوی متقاضی به دفتر ثبت نام.
دسترسی	Access	فراهم بودن امکان ارتباط با سیستم به منظور استفاده از منابع سیستم جهت کنترل یا به دست آوردن اطلاعات موجود در سیستم.
قابلیت دسترسی	Availability	تحویل دادن اطلاعات به شخص درست، در زمان مناسب.
دستورالعمل اجرایی گواهی الکترونیکی	Certificate Practice Statement	دستورالعمل اجرایی که مرکز صدور گواهی برای صدور گواهی از آن استفاده می‌نماید.
دستیابی قانونی به کلید	Key Escrow	تکنیک بازیابی کلید به منظور ذخیره اطلاعات کلید رمزنگاری با مسئولیت شخص سومی (مسئول دستیابی قانونی) به منظور بازیابی کلید و استفاده از آن در شرایط خاص.
دفتر ثبت نام	Registration Authority	یک موجودیت اختیاری در زیرساخت کلید عمومی می‌باشد که گواهی‌های الکترونیکی یا لیست گواهی‌های باطل شده را امضا نمی‌نماید ولی مسئولیت ثبت و شناسایی اطلاعات مورد نیاز مرکز صدور گواهی برای صدور گواهی یا لیست گواهی‌های باطل شده و اجرای وظایف مدیریت گواهی را دارد.
رمزنگاری	Cryptography	جستجو به دنبال راه‌حل‌هایی امن برای مجموعه‌ای از دو (یا چند) کاربر که می‌خواهند روی یک کانال عمومی که در معرض حمله یک مهاجم خارجی قرار دارد، با هم ارتباط برقرار کنند.

		به عبارت دیگر حوزه‌ای از دانش و تکنیک برای انتقال داده به منظور: • مخفی کردن محتوی آن • جلوگیری از تغییرات ناخواسته • جلوگیری از دسترسی‌های غیر مجاز
زنجیره گواهی	Certification Path	زنجیره منظم گواهی‌های الکترونیکی که به طرف اعتماد کننده توانایی ارزیابی صحت امضا و جعلی نبودن آخرین گواهی این زنجیره را می‌دهد.
زوج کلید	Key Pair	مجموعه‌ای از کلیدهای مرتبط ریاضیاتی (کلید خصوصی و کلید عمومی) که برای رمزنگاری نامتقارن استفاده می‌شوند و به گونه‌ای تولید می‌شوند که امکان به دست آوردن کلید خصوصی از کلید عمومی وجود نداشته باشد.
زیرساخت کلید عمومی	Public Key Infrastructure (PKI)	مجموعه‌ای از خدمات، محصولات، سیاست‌ها، فرایندها و سیستم‌های نرم‌افزاری و سخت‌افزاری گفته می‌شود که جهت مدیریت و بکارگیری گواهی‌های الکترونیکی X.509 و به منظور ارائه سرویس‌های امنیتی مختلف مبتنی بر رمزنگاری کلید عمومی مورد استفاده قرار می‌گیرد.
سخت‌افزار	Hardware	اجزا فیزیکی سیستم رایانه‌ای.
ماژول رمزنگاری سخت‌افزاری	Hardware Security Module (HSM)	نوعی ماژول سخت‌افزاری امن که از طریق واسط‌های نرم‌افزاری، امکان نگهداری امن کلیدهای رمزنگاری و اجرای ایمن مکانیزم‌های رمزنگاری را با کارایی مطلوب فراهم می‌آورد.
سرویس‌دهنده	Server	یک موجودیت سیستمی که در جواب درخواست‌های موجودیت‌های سیستمی دیگر به نام مشتری یا سرویس‌گیرنده، سرویس فراهم می‌نماید.
سطح اطمینان	Assurance Level	یک سطح به خصوص در مقیاس مرتبه‌ای که نشان‌دهنده اطمینان به مطابقت هدف مورد بررسی با نیازها می‌باشد.
سیاست‌های گواهی الکترونیکی	Certificate Policy	مجموعه‌ای از قوانین که سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور را مشخص می‌نماید.
سیستم عامل	Operating System	برنامه رایانه که عملیات اساسی سیستم (مانند مدیریت منابع رایانه، اجرای برنامه‌های کاربردی، فراهم آوردن سیستم فایل) را انجام می‌دهد.

شبکه	Network	مجموعه‌ای از رایانه‌های میزبان که با شبکه‌های دیگر یا شبکه اینترنت اطلاعات مبادله می‌کنند.
شماره سریال- شماره نسخه	Serial Number	یک مقدار عددی که توسط صادرکننده گواهی به گواهی داده می‌شود و بین تمام گواهی‌های تولید شده توسط صادر کننده گواهی، منحصر به فرد می‌باشد.
شناسه	Object Identifier	شناسه‌ای منحصر به فرد و رسمی، تشکیل شده از مجموعه‌ای از اعداد (تخصیص یافته توسط استاندارد ASN.1) که برای اشاره به اشیا با ویژگی‌های مشخص (مانند الگوریتم‌های رمزنگاری، سیاست‌های گواهی الکترونیکی و ...) استفاده می‌شود.
شناسه سیاست گواهی	Policy Object Identifier (POID)	شناسه‌ای منحصر به فرد و رسمی، تشکیل شده از مجموعه‌ای از اعداد (تخصیص یافته توسط استانداردASN.1) که جهت اشاره به سیاست‌های گواهی الکترونیکی متعلق به یک مرکز صدور گواهی الکترونیکی به کار می‌رود.
مالک گواهی	Subscriber	شخصی که برای وی گواهی الکترونیکی صادر شده است و می‌تواند از کلید خصوصی مرتبط با کلید عمومی درون گواهی استفاده نماید.
طرف اعتماد کننده	Relying Party	شخصی که به اعتبار اطلاعات گواهی الکترونیکی اعتماد می‌نماید.
دیواره آتش	Firewall	یک اتصال بین شبکه‌ای که ترافیک اطلاعاتی بین شبکه‌های متصل را محدود می‌نماید و منابع سیستمی شبکه را در مقابل مخاطرات شبکه‌ای دیگر محافظت می‌نماید.
فیلد	Field	بخشی از گواهی که محتوای آن نوع خاصی از داده‌ها (از پیش تعریف شده توسط استاندارد X.509) می‌باشد.
گذرواژه	Password	اطلاعات احراز هویت محرمانه که معمولاً از رشته‌ای از حروف تشکیل می‌شود.
گواهی الکترونیکی	Digital Certificate	یک ساختار داده‌ای الکترونیکی که به آن یک امضای الکترونیکی بر اساس آن ساختار داده‌ای اضافه می‌شود و جهت ارتباط دادن نام و مشخصات یک موجودیت با کلید عمومی او مورد استفاده قرار می‌گیرد.
گواهی امضا	Signature Certificate	یک گواهی الکترونیکی، محتوی یک کلید عمومی که از آن جهت تصدیق امضای دیجیتال استفاده می‌شود.

گواهی مورد اطمینان	Trusted Certificate	یک گواهی که طرف‌های اعتماد کننده به اعتبار آن، بدون نیاز به ارزیابی صحت گواهی مذکور، اطمینان می‌کنند. به خصوص گواهی الکترونیکی که برای فراهم کردن اولین کلید عمومی گواهی در زنجیره گواهی استفاده می‌شود.
گواهی میانی	Intermediate Certificate	گواهی مرکز صدور گواهی میانی که توسط مرکز دولتی ریشه امضا می‌شود و به مرکز صدور گواهی میانی اجازه صدور گواهی برای مالکان گواهی را می‌دهد.
الگوریتم	Algorithm	مجموعه‌ای محدود از دستورالعمل‌های گام به گام برای حل کردن مسائل و روال‌های محاسباتی، به خصوص روال‌هایی که توسط رایانه اجرا می‌شوند.
الگوریتم متقارن	Symmetric Algorithm	یک الگوریتم رمزنگاری که در آن کلیدهای رمزنگاری و رمزگشایی یکی هستند.
لیست گواهی‌های باطله	Certificate Revocation List	یک ساختمان داده که گواهی‌های الکترونیکی را که پیش از تاریخ انقضا، توسط صادرکننده گواهی معتبر به حساب نمی‌آیند، لیست می‌نماید.
مأمور امنیتی PKI	PKI Security Officer	فردی که مسئولیت اداره مدیران PKI را همراه با دیگر مأموران امنیتی PKI بر عهده دارد. همچنین پیکربندی سیاست‌های امنیتی مرکز صدور گواهی بر عهده مأموران امنیتی می‌باشد.
محرمانگی	Confidentiality	پوشاندن اطلاعات محرمانه برای اشخاص، موجودیت‌ها و یا روال‌های غیرمجاز.
مخزن	Repository	یک سیستم ذخیره و پخش گواهی‌های الکترونیکی و اطلاعات مربوط به آن‌ها (مانند لیست گواهی‌های باطل شده) برای طرف‌های اعتماد کننده.
مرکز دولتی صدور گواهی الکترونیکی ریشه	IR Governmental Root CA	یک مرکز صدور گواهی که مستقیماً مورد اطمینان موجودیت نهایی می‌باشد. مرکز دولتی صدور گواهی الکترونیکی ریشه، نقطه اطمینان در زیرساخت کلید عمومی کشور می‌باشد. این مرکز بر اساس مفاد بند الف از ماده ۴ آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و طی اولین جلسه شورای سیاست‌گذاری گواهی الکترونیکی کشور در مورخ ۱۳۸۶/۰۷/۳۰ مجوز ایجاد، امضا، صدور و ابطال گواهی الکترونیکی مراکز صدور گواهی میانی را دریافت کرده است.

مرکز صدور گواهی	Certificate Authority	موجودیتی که وظیفه صدور و مدیریت گواهی‌های الکترونیکی را بر عهده دارد و پیوند بین اطلاعات گواهی را ضمانت می‌نماید.
مرکز صدور گواهی میانی	Subordinate CA	یک مرکز صدور گواهی که گواهی خود را از مرکز دولتی صدور گواهی ریشه دریافت می‌نماید و می‌تواند برای مالکان گواهی، گواهی صادر نماید.
مسیریاب	Router	یک رایانه شبکه‌ای که بسته‌های پروتکل اینترنت را که مقصدشان خود رایانه نیست به خارج هدایت می‌نماید.
مشتری (سرویس‌گیرنده)	Client	یک موجودیت سیستمی که از موجودیت سیستمی دیگری که سرویس‌دهنده نامیده می‌شود درخواست سرویس کرده و از این سرویس استفاده می‌نماید.
مقداردهی اولیه	Initialization	یک پارامتر ورودی که الگوریتم رمزنگاری را مقداردهی اولیه می‌نماید.
مکانیزم M از N	M out of N Mechanism	تقسیم یک وظیفه بین n موجودیت به گونه‌ای که هر تعداد کمتر از m نفر نتوانند کل وظیفه را انجام دهند و برای انجام وظیفه حداقل حضور m نفر از آن n نفر لازم می‌باشد.
موجودیت نهایی	End Entity	موجودیتی که از کلیدها و گواهی‌ها برای ایجاد یا تشخیص صحت امضا یا محرمانگی آن استفاده می‌نماید. موجودیت‌های نهایی مالک گواهی، سازمان‌ها یا طرف‌های اعتماد کننده می‌باشند.
مهر زمانی	Time Stamp	امضای الکترونیکی که دارای تاریخ و ساعت می‌باشد و گواهی می‌نماید که محتویات آن در زمان مشخصی امضا شده‌اند.
نام ترکیبی	Distinguished Name	یک شناسه منحصر به فرد که شی موجود در درخت اطلاعاتی دایرکتوری (DIT) قالب X.500 را ارائه می‌نماید.
نام/ مشخصات مالک گواهی	Subject Name	نامی که به دارنده کلید خصوصی متناظر با کلید عمومی اختصاص داده شده است. در رابطه با گواهی‌های سازمانی، نامی که توصیف کننده سازمان می‌باشد و یا توصیف کننده وسایل یا تجهیزاتی است کلید خصوصی را مورد استفاده قرار می‌دهند.
نسخه پشتیبان	Backup	گرفتن کپی از فایل‌ها، اطلاعات و برنامه‌هایی که بازیابی اطلاعات را تسهیل می‌نماید.
ورود به سیستم	Login/Logon	حصول دسترسی یک موجودیت سیستمی به منابع سیستم که معمولاً از طریق فراهم کردن اسم کاربر و اسم رمز برای سیستم کنترل دسترسی که کاربران را احراز هویت می‌نماید و یا احراز هویت دو عاملی، انجام می‌شود.

ورودی	Entry	اطلاعات وارد شده در مستندات، نرم‌افزارهای کاربردی و پایگاه داده‌ها.
ویروس	Virus	یک قسمت مخفی و خودتکرار نرم‌افزاری دارای مناطق مخرب که با آلوده کردن منتشر می‌شود. برای مثال خود را به برنامه‌های دیگر کپی کرده و بخشی از آن‌ها می‌شود. ویروس نمی‌تواند به تنهایی اجرا شود و برنامه میزبان می‌بایست برای فعال شدن ویروس اجرا شود.
هویت	Identity	مجموعه‌ای از مشخصات محسوس و نامحسوس شخصی که اشخاص را از یکدیگر متمایز می‌نماید.
شناسایی (هویت‌شناسی)	Identification	شناسایی و تشخیص یک موجودیت از موجودیت‌های دیگر، از طریق بررسی مدارک شناسایی اشخاص و اطلاعات شناسایی دیگر از قبیل گذرواژه‌ها، اطلاعات بایومتریک و ...

۲. انتشار و وظایف مخزن

۲-۱ مخزن

مخزن مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، با آدرس ldap://pkd.pki.co.ir:389/c=ir جهت مشاهده گواهی‌های منتشر شده، مشاهده لیست گواهی‌های باطله و اطلاعات مرتبط دیگر به صورت بر خط در دسترس کاربران قرار دارد. لازم به ذکر است سایر موارد مطرح شده در بخش ۲-۲ از طریق آدرس https://ica.pki.co.ir قابل ارائه می‌باشد.

۲-۲ انتشار اطلاعات گواهی

نحوه برقراری ارتباط با مخزن در این مرکز، مطابق با بخش ۲-۱ است. این مرکز علاوه بر مسئولیت نگهداری مخزن گواهی‌ها، ارائه اطلاعات مربوط به وضعیت گواهی‌ها از هر لحاظ از جمله وضعیت ابطال را به صورت برخط برای درخواست کننده فراهم می‌سازد که نحوه‌ی ارتباط با کنترل برخط وضعیت گواهی[۱۳] مطابق با بخش ۶-۹-۴ می‌باشد. همچنین این مرکز وظیفه انتشار کلیه گواهی‌های صادر شده را بر عهده دارند. لازم به ذکر است مخزن، به صورت دائمی و ۲۴ ساعت هر روز هفته در دسترس می‌باشد.

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن حداقل اطلاعات زیر را از طریق مخزن منتشر می‌کند تا در دسترس مالکان گواهی و طرف‌های اعتمادکننده قرار گیرد.

- گواهی‌های صادر شده توسط این مرکز؛

[13] Online Certificate Status Protocol(OCSP)

- آخرین نسخهٔ منتشر شدهٔ CRL؛
- گواهی(های) صادر شده برای مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن؛
- آخرین نسخهٔ سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور» (CP)؛
- آخرین نسخهٔ سند «دستورالعمل اجرایی گواهی الکترونیکی مرکز صدور گواهی میانی» (CPS)؛
- نحوهٔ دسترسی به سرویس‌دهندهٔ OCSP؛
- توافق‌نامهٔ طرف اعتمادکننده[14]؛
- توافق‌نامهٔ مالک گواهی[15].
- گواهی مرکز دولتی ریشه؛

همچنین مرکز دولتی ریشه اطلاعات زیر را از طریق وب‌سایت خود منتشر می‌نماید:

- گواهی(های) مرکز دولتی ریشه؛
- گواهی‌های صادر شده برای مراکز میانی؛
- فهرست گواهی‌های باطله (CRL)؛
- آخرین نسخهٔ سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور»؛
- آخرین نسخهٔ سند جامع پروفایل‌های زیرساخت کلید عمومی کشور؛
- سند نرخ خدمات و محصولات مرکز صدور گواهی؛
- فهرست ماژول‌های رمزنگاری و نرم‌افزارهای صدور و مدیریت گواهی مورد تأیید مرکز دولتی ریشه؛
- کلیهٔ مصوبات شورای سیاست‌گذاری گواهی الکترونیکی و اسناد مرتبط دیگر که مرکز دولتی ریشه لزوم به انتشار آنها را احراز نماید.

۲-۳ زمان یا تناوب انتشار

زمان‌بندی و تناوب انتشار گواهی‌های مالکان گواهی، فهرست گواهی‌های باطله، و نسخه‌های به‌روز شده مستند جاری توسط مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن به صورت زیر می‌باشد:

گواهی‌های صادره پس از پذیرش گواهی توسط مالکان گواهی که طبق بخش ۱-۴-۴ صورت می‌گیرد، منتشر می‌شوند.

زمان و تناوب انتشار فهرست گواهی‌های باطله در بخش ۷-۹-۴ ذکر شده است.

سرور پاسخگوی OCSP وضعیت گواهی را به صورت بلادرنگ[16] به سرویس‌گیرندهٔ OCSP ارائه می‌نماید.

[14] Relying Party Agreement
[15] Subscriber Agreement
[16] Real-time

سند پیش رو با عنوان «دستورالعمل اجرایی گواهی الکترونیکی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن» پس از تأیید و تصویب توسط مرکز دولتی ریشه کشور منتشر می‌گردد و در صورت نیاز به اعمال تغییر، به صورت سالیانه مورد بازنگری قرار می‌گیرد و مجددا جهت تایید و تصویب نسخه‌ی بازنگری شده، به مرکز دولتی ریشه ارائه می‌شود.

۲-۴ کنترل دسترسی به مخازن

مرکز میانی از کلیه اطلاعات مخزن در برابر تغییرات غیرمجاز محافظت می‌نمایند. هرگونه تغییر و به‌روزرسانی در مخزن، تنها توسط نقش‌های مورد اطمینان صورت می‌گیرد. مرکز میانی سیستم‌عامل و مخزن خود را طوری پیکربندی می‌نمایند که تنها نقش‌های مجاز بتوانند، نسخه برخط اسناد را جایگزین نمایند. تغییر و به‌روزرسانی مخزن مرکز تنها توسط پرسنل مجاز مرکز میانی پندار کوشک ایمن و پس از اعمال فرایند کنترل دسترسی چند لایه امکان‌پذیر می‌باشد.

۳. شناسائی و احراز هویت

۳-۱ نام گذاری

هر موجودیت مالک گواهی، می‌بایست مطابق PKIX Part1، یک نام کاملاً متمایز و یکتا به فرم استاندارد X.501 در فیلدهای نام مالک گواهی و نام صادرکننده گواهی داشته باشد. در این بخش به نحوه نام‌گذاری و شناسایی مالکان گواهی پرداخته شده است. الزامات نام‌گذاری برای تمامی انواع/کاربردهای گواهی الکترونیکی به طور کامل در سند جامع پروفایل‌های زیرساخت کلید عمومی کشور تشریح شده است.

۳-۱-۱ انواع نام‌ها

نام‌های گواهی‌های الکترونیکی صادر شده توسط این مرکز منطبق با الزامات مشخص شده در سند "سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور" می‌باشد.

۳-۱-۲ نیاز به نام‌های بامعنی

منطبق با الزامات مشخص شده در سند "سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور" می‌باشد.

۳-۱-۳استفاده از نامهای مستعار و غیرواقعی برای مالکان گواهی

برای هیچ کدام از سطوح مورد اطمینان امکان استفاده از نام‌های مستعار و غیرواقعی برای مالکان گواهی وجود ندارد.

۳-۱-۴ قواعد تفسیر قالب های مختلف نام‌ها

تعریف نشده است.

۳-۱-۵ یکتایی نام ها

یکتایی نام در این مرکز رعایت می‌شود. مرکز صدور گواهی الکترونیکی میانی از نام‌های متمایز X.501 مورد تایید شورای سیاستگذاری گواهی الکترونیکی استفاده می‌نماید. تخصیص نام‌های متمایز به مالکان گواهی، وظیفه مرکز صدور گواهی الکترونیکی میانی می‌باشد. که می‌تواند از شماره سریال یا اطلاعات دیگری برای حفظ یکتایی نام متمایز استفاده کند که

چگونگی اعمال یکتایی در نام‌گذاری گواهی‌های الکترونیکی مطابق، "سند جامع پروفایل‌های زیرساخت کلید عمومی کشور" می‌باشد.

۳-۱-۶ تشخیص، احراز هویت و نقش نام‌های تجاری

از آنجایی که به کارگیری نام‌هایی که باعث نقض حقوق قانونی اشخاص ثالث گردد (به عنوان مثال استفاده از نام‌های تجاری ثبت شده، نام‌های دستگاه های دولتی و حقوق مالکیت معنوی) برای متقاضیان گواهی ممنوع می‌باشد، مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن در صورت اطلاع، هرگز برای نامی که مراجع قانونی آن را سوء استفاده از علامت تجاری سازمان دیگر تشخیص داده اند، گواهی صادر نمی‌کند.

۳-۲ هویت‌شناسی اولیه

۳-۲-۱ روش اثبات مالکیت کلید خصوصی

در صورتی که زوج کلیدها توسط دفتر ثبت‌نام به نمایندگی مالک گواهی تولید گردد، لزومی به اثبات مالکیت کلید خصوصی توسط شخص مالک گواهی نمی باشد. در هر صورت اثبات مالکیت کلید خصوصی براساس استاندارد PKCS#10 صورت می‌پذیرد.

۳-۲-۲ شناسایی سازمان/شرکت‌ها

سازمان‌ها (یا شرکت‌های خصوصی) جهت دریافت گواهی سازمانی (که به یک شخص به نیابت از سازمان داده می‌شود) درخواستی شامل نام، نشانی اقامتگاه، اسناد حقوقی و رسمی مانند اوراق ثبت شرکت (برای اثبات وجود سازمان یا شرکت) به همراه معرفی نامه رسمی و معتبر را به نماینده شرکت (برای اثبات مجاز بودن فرد مذکور به نمایندگی سازمان) ارایه می‌نمایند و نماینده شرکت با به‌همراه داشتن اوراق هویتی برای خود و معرفی نامه شرکت به‌صورت حضوری به دفتر ثبت‌نام، مراجعه می‌نماید و احراز هویت شخص نماینده مطابق با بخش ۳-۲-۳ و ۳-۲-۵ انجام می‌گیرد.

دفتر ثبت‌نام مرکز میانی نسخه‌ای از نوع و جزئیات شناسایی مورد استفاده در احرازهویت سازمان و تاریخ احرازهویت را مطابق با بخش ۲-۵-۵ بایگانی می‌نمایند.

۳-۲-۳ احراز هویت افراد

۳-۲-۳-۱ فردی شخصاً درخواست گواهی نماید

چنانچه فردی درخواست گواهی خود را شخصاً ارائه دهد دفتر ثبت‌نام مرکز میانی منطبق با نظام شناسایی توصیف شده در زیر، هویت فرد را شناسایی می‌نماید.

جهت صدور گواهی در کلیه سطوح اطمینان، در هر دو حالت احراز هویت حضوری و غیرحضوری، موارد زیر توسط این مرکز میانی رعایت می شود:

صحت اطلاعات هویتی ارائه شده (به ویژه نام، نام خانوادگی و کد ملی) با استفاده از پایگاه های اطلاعاتی معتبر مربوطه بررس می شود.

صحت اطلاعات هویتی شخص حقوقی با استفاده از پایگاه های اطلاعاتی معتبر مربوطه بررسی می شود.

استعلام های لازم جهت اطمینان از در قید حیات بودن متقاضی از پایگاه های اطلاعاتی معتبر مربوطه انجام می گیرد.

با استفاده از پایگاه های اطلاعاتی معتبر از مالکیت سیم کارت متناظر با شماره همراه ارائه شده توسط متقاضی اطمینان حاصل می شود.

جدول ۵ نحوه شناسایی افراد

سطح اطمینان	نحوه‌ی شناسایی
سطح ۱	احراز هویت بصورت غیر حضوری صورت می پذیرد و به روش مناسب اطمینان حاصل می شود که اطلاعات هویتی از طرف شخص غیر مجاز ارائه نمی گردد. برای این منظور از مشخصات بایومتریک چهره و کنترل زنده بودن و حاضر بودن فرد با روشهایی مانند ویدئو و الگوریتمهای هوش مصنوعی با درصد اطمینان بالا انجام می پذیرد. تصویر الکترونیکی یک نوع مدرک شناسایی معتبر عکس دار دریافت می شود.
سطح ۲	به صورت حضوری و ارائه کارت ملی و شناسنامه صورت می گیرد و در صورت نیاز مدارک لازم دیگربا توجه به نوع فعالیت در حوزه‌های متفاوت استفاده می شود. چنانچه قبلاً برای یک متقاضی، گواهی سطح دوم و یا گواهی سطح بالاتر صادر شده و گواهی او معتبر باشد و کلید خصوصی متناظر با گواهی در خطر افشا قرار نگرفته باشد، عملیات درخواست گواهی همراه با امضای الکترونیکی یک فرم درخواست گواهی که برای این منظور طراحی شده است، از طریق کلید متناظر با گواهی قبلی و به صورت غیرحضوری صورت می پذیرد و در این حالت اطلاعات هویتی فرد از گواهی الکترونیکی قبلی استخراج می شود.

جدول ۶ مدارک شناسایی معتبر

سطح اطمینان	مدارک شناسایی معتبر
سطح ۲	• اصل و کپی کارت ملی • اصل و کپی شناسنامه

• اصل و کپی گذرنامه • اصل و کپی گواهی‌نامه	

دفتر ثبت‌نام مرکز میانی نسخه‌ای از نوع و جزئیات شناسایی مورد استفاده در احرازهویت شخص و تاریخ احرازهویت را حداقل در طول دوره عمر گواهی صادر شده برای او نگه‌داری می‌نمایند.

فرآیند احرازهویت برای شخص درخواست کننده گواهی به صورت زیر می‌باشد:

- شخص درخواست کننده گواهی به دفتر ثبت‌نام مرکز میانی مراجعه و مدارک مربوط به سطح گواهی مورد درخواست را به متصدی ثبت‌نام ارائه می‌نماید.
- متصدی دفتر ثبت‌نام صحت مدارک ارائه شده از طرف شخص درخواست‌کننده را بررسی می‌نماید.
- شخص درخواست‌کننده، فرم مربوط به درخواست گواهی را تکمیل نموده و در حضور متصدی دفتر ثبت‌نام آن را با امضای خود تایید می‌نماید.
- متصدی دفتر ثبت‌نام اطلاعات وارد شده در فرم را با مدارک ارائه شده تطبیق می‌دهد.

۳-۲-۳-۲ شخصی به نمایندگی از شخص دیگری درخواست گواهی کند

یک فرد می‌تواند درخواست گواهی خود را از طریق فرد دیگری با اعطای وکالتنامه رسمی به وی ارائه دهد. فرآیند هویت‌شناسی برای حالتی که ارائه درخواست گواهی از سوی نماینده شخص متقاضی صورت می‌گیرد به صورت زیر می‌باشد:

- نماینده شخص درخواست‌کننده گواهی به دفتر ثبت‌نام مرکز میانی مراجعه می‌نماید و وکالتنامه مربوط به نمایندگی از طرف شخص درخواست‌کننده گواهی، مدارک مربوط به خود و متقاضی را باتوجه به سطح گواهی مورد درخواست مطابق با بخش ۱-۳-۲-۳ به متصدی دفتر ثبت‌نام ارائه می‌نماید.
- متصدی دفتر ثبت‌نام صحت وکالتنامه و مدارک ارائه شده از طرف نماینده شخص درخواست‌کننده گواهی را بررسی می‌نماید.
- نماینده شخص درخواست‌کننده گواهی، فرم درخواست گواهی را تکمیل نموده و در حضور متصدی دفتر ثبت‌نام آن را با امضای خود تایید می‌نماید.
- متصدی دفتر ثبت‌نام اطلاعات مربوط به نماینده را ثبت نموده و اطلاعات وارد شده در فرم را با مدارک ارائه شده تطبیق می‌دهد.

دفتر ثبت‌نام مرکز میانی نسخه‌ای از نوع و جزئیات شناسایی مورد استفاده در احرازهویت شخص درخواست‌کننده گواهی و نماینده و تاریخ احرازهویت را نگه‌داری می‌نماید.

۳-۲-۳-۳ شخصی برای یک نقش سازمانی درخواست گواهی کند

قبل از ثبت و ارسال درخواست به مرکز، دفتر ثبت‌نام مطابق با بخش ۱-۳-۲-۳ هویت فردی که درخواست صدور گواهی برای نقش سازمانی خود دارد را شناسایی می‌کند. علاوه بر این، دفتر ثبت‌نام از اینکه فرد برای این نقش سازمانی مجاز

می‌باشد، اطمینان حاصل می‌نماید مدارک مورد نیاز جهت احراز نقش سازمانی درخواست‌کننده گواهی علاوه بر مدارک ذکر شده ۱-۳-۲-۳ شامل موارد زیر نیز می‌باشد:

۱. کپی آگهی تاسیس (ممهور به مهر سازمان)
۲. کپی آگهی آخرین تغییرات روزنامه رسمی (ممهور به مهر سازمان)
۳. معرفی‌نامه متقاضی گواهی در سربرگ سازمان که نقش سازمانی در آن قید شده باشد (ممهور به مهر سازمان، با امضای بالاترین مقام سازمان)

مدارک مربوط به احراز نقش سازمانی درخواست‌کننده گواهی مطابق با بخش ۲-۵-۵، توسط دفتر ثبت‌نام مرکز میانی نگهداری می‌گردند.

۳-۲-۱۴اطلاعات تصدیق نشده مالکان گواهی

اطلاعاتی که از طرف درخواست‌کننده گواهی به دفتر ثبت‌نام ارائه می‌گردد و احتیاج به بررسی و تصدیق ندارد، عبارتند از:

- واحد سازمانی (OU) دوم به بعد: سطح اطمینان اول و دوم؛
- اطلاعات دیگری که براساس بخش ۳-۲-۴ از سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور نیازی به تصدیق ندارد.

۳-۲-۱۵اعتبارسنجی مرجع ذی‌صلاح

هرگاه نام درخواستی برای گواهی یک شخص، با یک سازمان خاص مرتبط باشد تا وابستگی شخص درخواست‌کننده را به سازمان نشان دهد و یا زمانی که شخصی از طرف یک سازمان مأمور ارائه درخواست گواهی برای سازمان باشد، دفتر ثبت‌نام:

- موجودیت سازمان را به عنوان شخص حقوقی از طریق سازمان ثبت اسناد و املاک کشور استعلام و پیگیری می‌نماید.
- برای سطح اطمینان دو حداقل با استعلام تلفنی یا کتبی از سازمان مربوطه صلاحیت شخص درخواست‌کننده را احراز می‌نماید.
- برای تمامی سطوح، متناسب با نوع گواهی، استعلام هویتی و حیات شخص حقیقی از سازمان ثبت احوال کشور، اطلاعات هویتی شخص حقوقی از سازمان ثبت اسناد و املاک کشور، استعلام مالکیت سیم کارت از وزارت ارتباطات و فناوری اطلاعات و سایر خصوصیات از پایگاه داده‌های معتبر را انجام می‌نماید.

۳-۲-۶ شرایط تعامل با سایر نهادها

در حال حاضر کاربرد ندارد.

۳-۳ شناسائی و احرازهویت برای درخواست های تجدید کلید

تجدید کلید یک گواهی به معنای تولید یک گواهی جدید همسان با گواهی قبلی است، به جز آن که گواهی جدید دارای یک کلید عمومی جدید و متفاوت (مطابق با یک کلید خصوصی متفاوت) و یک شماره سریال متفاوت و احتمالا یک مدت اعتبار متفاوت باشد.

اشخاص و سازمان‌هایی که قصد تجدید کلید عمومی را دارند می‌بایست درخواست گواهی جدید خود را به دفتر ثبت‌نام تحویل دهند، دفتر ثبت‌نام پس از احراز هویت درخواست‌کننده مطابق با بخش‌های ۱-۳-۳ و ۲-۳-۳ عملیات لازم را انجام می‌دهد. سپس گواهی توسط دفتر ثبت‌نام، ثبت و نگه داری می‌شود. لازم به ذکر است درخواست‌های تجدید کلید در مرکز میانی ثبت و نگه‌داری می‌شوند.

۳-۳-۱ فرایند عادی شناسایی و احراز هویت برای تجدید کلید (عادی)

شناسایی و احراز هویت برای تجدید کلید عبارت است از بررسی و تصدیق این‌که شخص یا سازمانی که درخواست تجدید کلید را داده، مالک گواهی و یا یک نماینده‌ی مجاز برای مالک گواهی باشد.

روال درخواست تجدید کلید و شناسایی مالک گواهی یا نماینده ی ایشان مطابق با بخش ۲-۳ می‌باشد با این تفاوت که دفتر ثبت‌نام اطلاعات و مدارک ارائه شده توسط درخواست‌کننده را با مدارک موجود در بایگانی خود که هنگام درخواست صدور گواهی برای شخص یا سازمان مربوطه ثبت گردیده، مقایسه می‌کند. درصورت تطابق دفتر ثبت‌نام درخواست تجدید کلید را تأیید نموده و جهت پردازش به مرکز صدور گواهی ارسال می‌کند.

۳-۳-۲ شناسایی و احراز هویت برای تجدید کلید پس از ابطال گواهی

تعریف نشده است.

۳-۴ شناسایی و احراز هویت برای درخواست ابطال

شناسایی و احراز هویت برای درخواست ابطال عبارت است از بررسی و تصدیق این‌که شخص یا سازمانی که درخواست ابطال گواهی را داده، مالک واقعی گواهی و یا یک نماینده مجاز برای مالک گواهی می‌باشد. فرایند درخواست ابطال گواهی و شناسایی مالک گواهی یا نماینده وی مطابق با بخش‌های ۲-۲-۳ و ۳-۲-۳ صورت می‌گیرد با این تفاوت که دفتر ثبت نام اطلاعات و مدارک ارائه‌شده توسط درخواست‌کننده را با اطلاعات و مدارک موجود در پایگاه‌داده و بایگانی خود که هنگام درخواست صدور گواهی برای شخص یا سازمان مربوطه ثبت گردیده، مقایسه می‌نماید. در صورت تطابق، دفتر ثبت‌نام درخواست ابطال گواهی را تأیید نموده و جهت پردازش، به مرکز میانی ارسال می‌نماید. درخواست‌های ابطال گواهی ثبت و نگهداری می‌شوند.

۴. الزامات عملی چرخه حیات گواهی الکترونیکی

۴-۱ درخواست گواهی

درخواست‌کنندهٔ گواهی و دفتر ثبت‌نام باید مراحل زیر را هنگام ارائهٔ درخواست گواهی انجام دهند:

- شناسایی مالک گواهی توسط دفتر ثبت‌نام (طبق بخش ۲-۳)؛
- ثبت اطلاعات درخواست‌کنندهٔ گواهی مطابق با دستورالعمل اجرایی گواهی الکترونیکی توسط دفتر ثبت‌نام؛
- تولید زوج کلید و ارائه کلید عمومی به همراه هر درخواست گواهی (طبق ۳-۱-۱-۶) توسط درخواست کننده گواهی یا دفتر ثبت‌نام به نمایندگی از درخواست کننده گواهی؛
- حصول اطمینان از ارتباط کلید عمومی ارائه شده با کلید خصوصی موجود نزد مالک گواهی (طبق بخش ۱-۲-۳) توسط دفتر ثبت‌نام؛

همه‌ی موارد مذکور باید قبل از صدور گواهی و با همین ترتیب قید شده به صورت کامل انجام شوند.

۴-۱-۱ موجودیت‌های مجاز جهت ارائه درخواست گواهی

افرادی که می‌توانند یک درخواست گواهی را ارائه نمایند عبارتند از:

- شخصی که قرار است مالک گواهی شود یا وکیل قانونی وی؛
- نمایندهٔ مجاز یک سازمان یا موجودیت (جهت ارائهٔ درخواست گواهی برای نقش سازمانی، یک دستگاه یا یک برنامهٔ کاربردی و یا ارائهٔ درخواست گواهی سازمانی).

۴-۱-۲ فرایند ثبت نام و مسئولیت‌ها

در صورتی که شخص یا سازمانی قصد درخواست صدور گواهی داشته باشد، می‌بایست مراحل زیر را انجام دهد:

- درخواست‌کنندهٔ گواهی باید پس از تولید زوج کلید، یک فایل درخواست امضای گواهی[17] مطابق با استاندارد PKCS#10 ایجاد کند و همراه با اثبات مالکیت کلید خصوصی منطبق با بخش ۱-۲-۳، فایل درخواست امضای گواهی را به دفتر

[17] Certificate Signing Request (CSR)

ثبت‌نام تحویل دهد. به جای این کار، درخواست‌کنندهٔ گواهی می‌تواند فرایند تولید کلید و فایل درخواست امضای گواهی را به دفتر ثبت‌نام واگذار نماید.

- اطلاعات و مدارک لازم جهت ارائهٔ درخواست گواهی را مطابق با بخش ۲-۳ به دفتر ثبت‌نام ارائه نماید.
- توافقنامهٔ مربوط به شرایط حاکم بر استفاده از گواهی را امضا کند.

۴-۲ بررسی درخواست گواهی

این بخش به تشریح روال‌ها و رویه‌های بررسی درخواست گواهی می‌پردازد.

۴-۲-۱ اجرای فرایندهای شناسایی و احراز هویت

دفتر ثبت‌نام کلیه اطلاعات موردنیاز ارائه شده توسط درخواست‌کننده گواهی جهت صدور یک گواهی توسط مرکز میانی را مطابق با بخش ۲-۳ شناسایی و احراز هویت می‌نماید.

۴-۲-۲ تأیید و یا رد درخواست گواهی

مرکز گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن و یا دفاتر ثبت‌نام گواهی درصورتی‌که مفاد درخواست‌ها با معیارهای ذیل انطباق داشته باشند باید نسبت به تأیید آنها اقدام نمایند:

- احراز هویت کلیه مشترکین و متقاضیان گواهی بر اساس شرایط مندرج در بخش ۲-۳ با موفقیت انجام پذیرفته باشد.

دفتر ثبت‌نام در موارد ذیل اقدام به رد درخواست گواهی می‌نماید:

- احراز هویت و انطباق اطلاعات مشترک و یا درخواست کننده گواهی مطابق با بخش ۲-۳ نبوده و تأیید وی امکان پذیر نباشد.
- فایل درخواست امضای گواهی (CSR) تحویل داده شده توسط درخواست‌کننده در قالب استاندارد PKCS#10 نباشد و یا عملیات اثبات مالکیت کلید خصوصی با موفقیت صورت نگیرد.
- درخواست‌کننده‌ی گواهی توافق‌نامه شرایط حاکم بر استفاده از گواهی را نپذیرد.
- درخواست‌کننده‌ی گواهی به تذکرات دفتر ثبت‌نام در زمان تعیین شده پاسخ ندهد.
- وجه صدور گواهی پرداخت نشده باشد.

۴-۲-۳ مدت رسیدگی به درخواست گواهی

حداکثر فاصله زمانی بین دریافت و تأیید درخواست و صدور گواهی مورد نظر مطابق با فاصله تعیین شده در جدول زیر برای هر سطح اطمینان باشد.

جدول ۷ مدت رسیدگی به درخواست گواهی

سطح اطمینان	حداکثر فاصله بین درخواست و صدور گواهی
سطح ۱	گواهی‌های کاربران نهایی حداکثر در طی مدت هفت روز از زمان درخواست دفتر ثبت نام صادر می‌شوند.
سطح ۲	گواهی‌های کاربران نهایی حداکثر در طی مدت پنج روز از زمان درخواست دفتر ثبت نام صادر می‌شوند.

۴-۳ صدور گواهی

۴-۳-۱ اقدامات مرکز در طول صدور گواهی

هر گواهی پس از تأیید درخواست توسط دفتر ثبت‌نام و دریافت درخواست صدور گواهی توسط مرکز صدور گواهی پردازش و صادر می‌گردد.

این مرکز براساس اطلاعاتی که در درخواست گواهی درج گردیده و بعد از استعلام صحت آن‌ها از مراجع مختلف جهت تأیید، اقدام به صدور گواهی برای درخواست کننده می‌نماید.

۴-۳-۲اطلاع‌رسانی به متقاضی توسط مرکز صدور گواهی

پس از صدور گواهی، دفتر ثبت‌نام از طریق پست الکترونیکی به مالک گواهی صدور موفقیت آمیز یا عدم آن را (با ذکر دلایل) اطلاع رسانی می‌کند. چنانچه گواهی در حضور شخص صادر شود گواهی در توکن ارائه شده توسط متقاضی درج شده و امضای رسید تحویل گواهی توسط متقاضی در فرم درخواست گواهی به منزله اطلاع از صدور گواهی و پذیرش آن می‌باشد.

۴-۴ پذیرش گواهی

۴-۴-۱ چگونگی پذیرش گواهی

ازآنجایی که پذیرش گواهی توسط درخواست‌کننده جهت استفاده از گواهی الکترونیکی الزامی می‌باشد، مالک گواهی ملزم به پذیرش گواهی می‌باشد.

روال پذیرش بدین صورت می‌باشد که مالک گواهی یا متقاضی گواهی پس از حضور در دفتر ثبت‌نام تصدیق می‌نماید تمامی اطلاعاتی که در گواهی الکترونیکی قید شده است صحت دارد. سپس برگه رسید گواهی را امضا می نماید و در صورت عدم پذیرش گواهی از سوی درخواست‌کننده‌ی گواهی، درخواست‌کننده‌ی گواهی می‌بایست حداکثر ظرف مدت ۲۴ ساعت دلایل عدم پذیرش خود را به‌صورت کتبی جهت ابطال و یا تجدید صدور گواهی به مرکز اعلام کند. همچنین فرآیند پذیرش گواهی در توافق نامه ما بین مرکز میانی و مالک گواهی تشریح می‌شود.

۴-۴-۲انتشار گواهی توسط مرکز صدور گواهی

این مرکز گواهی‌های صادر شده که توسط مالک گواهی مورد پذیرش قرار گرفته اند را از طریق مخزن منتشر می‌نماید.

۴-۴-۳ اطلاع‌رسانی صدور گواهی به سایر موجودیت‌ها توسط مرکز

این مرکز، دفتر ثبت‌نام را از صدور گواهی که درخواست آن را تأیید و ثبت نموده بود، مطلع می‌کند.

۴-۵ کاربرد گواهی و زوج کلید

۴-۵-۱ کاربرد گواهی و کلید خصوصی مالک گواهی

استفاده از کلید خصوصی که با کلید عمومی در گواهی صادره متناظر می‌باشد صرفا زمانی امکان پذیر است که مالک گواهی توافق نامه شرایط حاکم بر استفاده از گواهی و گواهی صادر شده را پذیرفته و فرم درخواست گواهی را امضا نماید. مالک گواهی می‌بایست گواهی را مطابق با قانون و مفاد توافق‌نامه شرایط حاکم بر استفاده از گواهی، سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور(CP) و دستورالعمل اجرایی این مرکز(CPS) مورد استفاده قراردهد. استفاده از گواهی نباید متناقض با فیلدهای KeyUsage و Extended Key Usage از الحاقیه‌های گواهی باشد.

مالک گواهی نباید از کلید خصوصی خود در کاربردهای غیرمجاز و به قصد ضرر رساندن به غیر، استفاده کند. مالک گواهی نباید با منقضی شدن یا باطل شدن گواهی از کلید خصوصی متناظر با آن گواهی استفاده نماید.

۴-۵-۲کاربرد گواهی و کلید عمومی برای طرف اعتماد کننده

در زیرساخت کلید عمومی مشخصات یک موجودیت از طریق گواهی‌هایX.509 به کلید عمومی او پیوند داده می‌شود. یکی از مهمترین قابلیت‌هایی که یک نرم افزار مجهز به زیرساخت کلید عمومی(PKE) می‌بایست از آن پشتیبانی کند، فرآیند اعتبارسنجی زنجیره‌ی گواهی می‌باشد. از طریق این فرآیند می‌توان دریافت که به یک گواهی الکترونیکی جهت استفاده در یک نرم‌افزار خاص و یا جهت استفاده در سخت افزار مناسب به منظور انجام عمل تصدیق امضا ، می‌توان اعتماد نمود یا خیر.

در یک زنجیره‌ی گواهی هر گواهی توسط صادرکننده‌ی این گواهی امضا شده است و این زنجیره، از گواهی کاربر تا گواهی متعلق به مرکز دولتی ریشه صدور گواهی امتداد دارد.

کلیه نرم‌افزارهای PKE باید در آزمایشگاه زیرساخت کلید عمومی کشور ارزیابی و مورد تایید باشند، طرف‌های اعتمادکننده می‌بایست همواره به تناسب استفاده از گواهی با اهداف و کاربردهای تعیین شده و عدم استفاده از گواهی در کاربردهای

منع شده توسط سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و دستورالعمل اجرایی این مرکز توجه داشته باشند و قبل از اعتماد به یک گواهی جهت اعتبارسنجی زنجیره گواهی، حداقل به موارد زیر توجه نمایند:

- وجود یا عدم وجود گواهی متعلق به صادرکننده گواهی مورد نظر در زنجیره گواهی باید بررسی شود.
- امضای کلیه گواهی‌های موجود در زنجیره گواهی می‌بایست اعتبارسنجی شود.
- از گواهی می‌بایست در کاربردهای متناسب با کاربردهای تعیین شده در الحاقیه‌های گواهی مانند Extended Key Usage و KeyUsage استفاده شود.
- وضعیت ابطال یا عدم ابطال گواهی مالک گواهی و کلیه گواهی‌های متعلق به مراکز صدور گواهی موجود در زنجیره گواهی می‌بایست بررسی شود. اگر هر یک از گواهی‌های موجود در زنجیره گواهی باطل شده باشد، طرف اعتمادکننده منحصراً مسئول اعتماد به گواهی مالک گواهی و امضای تصدیق شده توسط این گواهی می‌باشد.
- اعتبار کلیه لیست‌های گواهی‌های باطله مرتبط با زنجیره گواهی می‌بایست بررسی شود.

۴-۶ تمدید گواهی

منظور از تمدید گواهی، تولید یک گواهی جدید، همسان با گواهی قبلی است به جز آنکه گواهی جدید دارای یک مدت اعتبار متفاوت و یک شماره سریال متفاوت می‌باشد.

تمدید گواهی زمانی انجام می‌گیرد که تمام اطلاعات مربوط به هویت و کلید عمومی از گواهی قبلی به گواهی جدید انتقال یافته و سریال گواهی و دوره اعتبار آن تغییر نموده و مدت آن افزایش یافته باشد. در این مرکز تمدید گواهی فقط برای یک دوره انجام خواهد شد.

۴-۶-۱ شرایط تمدید گواهی

در صورتی تمدید امکان پذیر است که:

۱- گواهی منقضی یا باطل نشده باشد

۲- مجموع دوره اعتبار گواهی‌های صادر شده در زمان تمدید از الزامات بخش ۶-۳-۲ سند سیاست‌های گواهی الکترونیکی پیروی می‌کند.

۳- مالک گواهی برای بار اول درخواست تمدید داده باشد.

در این مرکز تمدید گواهی فقط برای یک دوره انجام خواهد شد. مالک گواهی باید حداکثر تا یک ماه قبل از انقضای گواهی درخواست تمدید را داده باشد.

۴-۶-۲ متقاضیان تمدید گواهی

تنها مالکان گواهی و یا نمایندگان مجاز آن‌ها می‌توانند درخواست تمدید گواهی نمایند.

۴-۶-۳ بررسی درخواست های تمدید گواهی

فرایند بررسی درخواست تمدید مطابق با بخش ۶-۴ انجام می‌گیرد.

۴-۶-۴ اعلام صدور گواهی جدید به مالک گواهی

اطلاع‌رسانی صدور یک گواهی تمدید شده به مالک گواهی مطابق با بخش ۲-۳-۴ می‌باشد.

۴-۶-۵ چگونگی پذیرش گواهی تمدید شده

چگونگی پذیرش تمدید یک گواهی مطابق با بخش ۱-۴-۴ می‌باشد.

۴-۶-۶انتشار گواهی تمدید شده توسط مرکز

گواهی‌های جدید صادر شده که توسط مالک گواهی مورد پذیرش قرار گرفته اند و مدت اعتبار آنها تمدید شده است، از طریق مخزن منتشر می‌گردند.

۴-۶-۷ اطلاع‌رسانی صدور گواهی توسط مرکز صدور گواهی به سایر موجودیت‌ها

این مرکز، دفتر ثبت‌نام را از صدور گواهی که درخواست آن را تأیید و ثبت نموده بود، مطلع می‌کند.

۴-۷ تجدید کلید گواهی

تجدید کلید یک گواهی به معنای تولید یک گواهی جدید همسان با گواهی قبلی است، به جز آنکه گواهی جدید دارای یک کلید عمومی جدید و متفاوت (متناظر با یک کلید خصوصی متفاوت) و یک شماره سریال متفاوت و احتمالاً یک مدت اعتبار متفاوت می‌باشد.

۴-۷-۱ شرایط تجدید کلید گواهی

مالک گواهی قبل از رسیدن به موعد زمان انقضای گواهی اقدام به تجدید کلید گواهی می‌نماید. تجدید کلید گواهی ممکن است بخاطر دلایل زیر نیاز باشد:

- دوره اعتبار گواهی در آستانه به پایان رسیدن باشد.
- گواهی بدلیل خطر افشای کلید خصوصی باطل گردد.

عمل تجدید کلید گواهی همراه با ابطال گواهی صورت می‌گیرد.

مالک گواهی باید حداکثر تا یک ماه قبل از انقضای گواهی درخواست تجدید کلید را داده باشد.

۴-۷-۲متقاضیان گواهی با کلید عمومی جدید

فقط مالک گواهی یا نمایندهٔ مجاز وی و یا نمایندهٔ مجاز برای گواهی سازمانی می‌تواند درخواست تجدید کلید گواهی نماید.

۴-۷-۳ بررسی درخواست‌های تجدید کلید گواهی

فرایند بررسی درخواست تجدید کلید یک گواهی مطابق با بخش ۱-۳-۳ می‌باشد.

۴-۷-۴ اعلام صدور گواهی جدید به مالک گواهی

اطلاع‌رسانی صدور یک گواهی با کلید عمومی جدید به مالک گواهی مطابق با بخش ۲-۳-۴ می‌باشد.

۴-۷-۵ چگونگی پذیرش گواهی با کلید جدید

چگونگی پذیرش یک گواهی تجدید کلید شده مطابق با بخش ۱-۴-۴ می‌باشد.

۴-۷-۶ انتشار گواهی تجدید کلید شده توسط مرکز صدور گواهی

گواهی‌های جدیدی که کلید عمومی آنها تجدید شده است و از سوی مالک گواهی پذیرفته شده‌اند از طریق مخزن منتشر می‌شوند.

۴-۷-۷ اطلاع‌رسانی صدور گواهی توسط مرکز صدور گواهی به سایر موجودیت‌ها

این مرکز، دفتر ثبت‌نام را از صدور گواهی‌ای که درخواست آن را تأیید و ثبت نموده بود، مطلع می‌کند.

۴-۸ اصلاح گواهی

این سرویس در این مرکز ارائه نمی‌شود.

۴-۸-۱ شرایط اصلاح گواهی

تعریف نشده است.

۴-۸-۲متقاضیان اصلاح گواهی

تعریف نشده است.

۴-۸-۳ بررسی درخواست‌های اصلاح گواهی

تعریف نشده است.

۴-۸-۴ اعلام صدور گواهی جدید به مالک گواهی

تعریف نشده است.

۴-۸-۵ چگونگی پذیرش گواهی اصلاح شده

تعریف نشده است.

۴-۸-۶ انتشار گواهی اصلاح شده توسط مرکز صدور گواهی

تعریف نشده است.

۴-۸-۷ اطلاع‌رسانی صدور گواهی توسط مرکز صدور گواهی به سایر موجودیت‌ها

تعریف نشده است.

۴-۹ ابطال و تعلیق گواهی

۴-۹-۱ شرایط ابطال

ابطال گواهی زمانی انجام می‌شود که پیوند بین مشخصات مالک گواهی و کلید عمومی وی اعتبار خود را از دست بدهد.

۴-۹-۱-۱ شرایط ابطال گواهی الکترونیکی مراکز میانی

در موارد زیر، مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، ابطال گواهی خود را از مرکز دولتی ریشه درخواست می‌کند:

- کلید خصوصی مرکز میانی احتمالاً یا مطمئناً در خطر افشا باشد؛
- دیگر نیازی به گواهی مرکز میانی نباشد. این امر ممکن است به علت خاتمهٔ خدمات ارائه شده توسط مرکز میانی یا انقضای قرارداد بین مرکز میانی و مرکز دولتی ریشه باشد.

همچنین در موارد زیر، مرکز دولتی ریشه اقدام به ابطال گواهی مرکز میانی می‌نماید:

- در صورت ابطال گواهی مرکز دولتی ریشه، کلیهٔ گواهی‌های متعلق به مرکز میانی زیرین باطل می‌شوند؛
- در صورت احراز تخلف مرکز میانی یا دفتر ثبت‌نام وابسته به مرکز میانی از مندرجات سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و تأیید این تخلف توسط شورای سیاستگذاری گواهی الکترونیکی کشور؛

- محرز شدن صدور گواهی مبتنی بر اظهارات خلاف واقع اعم از عمدی و غیرعمدی توسط مرکز میانی و تأیید آن توسط شورای سیاستگذاری گواهی الکترونیکی کشور؛
- دستور ابطال گواهی مرکز میانی از سوی مراجع قضایی ذیصلاح؛
- پایان فعالیت مرکز دولتی ریشه.

مرکز دولتی ریشه به محض قطع عملیات مرکز میانی و زمانی که فعالیت این مرکز به موجب حکم مراجع قضایی و یا دلیل دیگری متوقف شود و همچنین در صورت لغو مجوز مرکز میانی به روش مندرج در بند (خ) ماده (۵) آیین نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و درج در روزنامه رسمی جمهوری اسلامی ایران فهرست گواهی‌های باطله را منتشر نماید. مسئولیت جبران خسارت ناشی از ابطال گواهی مرکز میانی به مالکان گواهی صادر شده از این مرکز در توافق‌نامه منعقد شده بین طرفین (مرکز میانی و مالک گواهی) ذکر خواهد شد.

۴-۹-۱-۲ شرایط ابطال گواهی الکترونیکی موجودیت نهایی

در موارد زیر، مالک گواهی و یا وکیل قانونی وی باید ابطال گواهی مالک گواهی را از این مرکز درخواست کند:

- کلید خصوصی مالک گواهی احتمالاً یا مطمئناً در خطر افشا باشد؛
- اطلاعات موجود در گواهی (نظیر مشخصات مالک گواهی) به هر دلیلی تغییر کند؛
- دیگر نیازی به گواهی نباشد؛ این امر ممکن است به علت توقف فعالیت یک سازمان و یا توقف فعالیت یک شخص در یک سازمان، تغییر جایگاه سازمانی و نزول درجهٔ سازمانی مالک گواهی باشد.

در صورت بروز هر یک از شرایط زیر، مرکز میانی، گواهی مالک گواهی را بدون تأیید وی باطل می‌کند:

- در صورت استفادهٔ غیرمجاز، جعل و در خطر افشا قرار گرفتن کلید خصوصی مرکز میانی و یا در صورت باطل شدن گواهی مرکز دولتی ریشه، کلیهٔ گواهی‌های امضا شده توسط مرکز میانی باطل می‌شوند؛
- دستور ابطال از سوی مراجع قضایی ذیصلاح صادر شود؛
- مالک گواهی از تعهداتش تخطی کند؛
- مرکز میانی به فعالیت خود پایان دهد؛
- مرکز دولتی ریشه به فعالیت خود پایان دهد؛
- مالک گواهی فوت کند.

لازم به ذکر است طبق توافق‌نامه‌ای که بین مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن و مالکان گواهی صورت می‌گیرد، مالکان گواهی ملزم هستند که در صورت به خطر افتادن یا احتمال به خطر افتادن کلید خصوصی خود، در اسرع وقت در یک روز کاری بعد از مفقود شدن کلید خصوصی مربوط به گواهی و یا مشخص شدن اینکه داده های گواهی دیگر اعتبار ندارد، این موضوع را به این مرکز اطلاع دهند و جهت ابطال گواهی اقدام کنند.

۴-۹-۲ متقاضیان درخواست ابطال

۴-۹-۲-۱ موجودیت‌های نهایی

درخواست ابطال گواهی الکترونیکی باید توسط افراد زیر ارائه شود:

- مالک گواهی؛
- وکیل قانونی از سوی مالک گواهی (بخش ۳-۲-۳)؛
- نمایندهٔ مجاز سازمان جهت ارائه درخواست ابطال گواهی‌های سازمانی و یا گواهی یکی از پرسنل سازمان؛

- نمایندهٔ مجاز برای ابطال گواهی دفتر ثبت‌نام؛
- مراجع قضایی ذیصلاح.

۴-۹-۲-۲ مراکز صدور گواهی الکترونیکی

موجودیت‌های مجاز جهت ارائهٔ درخواست ابطال گواهی متعلق به مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن عبارتند از:

- نمایندهٔ مجاز مرکز میانی برای ابطال گواهی(های) این مرکز؛
- مراجع قضایی ذیصلاح؛
- شورای سیاست‌گذاری گواهی الکترونیکی کشور؛
- مرکز دولتی ریشه.

۴-۹-۳ فرایند رسیدگی به درخواست ابطال

با دریافت درخواست ابطال در دفترثبت‌نام، احراز هویت درخواست‌کننده مطابق با بخش ۴-۳ انجام می‌گردد. سپس دفتر از مرکز میانی درخواست ابطال گواهی را می‌نماید. مرکز صدور گواهی الکترونیکی براساس سطوح گواهی پس از دریافت درخواست ابطال نسبت به ابطال گواهی اقدام می نماید. مرکز از طریق مخزن اقدام به انتشار لیست گواهی‌های باطل شده می‌نماید. اطلاع‌رسانی ابطال گواهی به متقاضی از طریق دفاتر ثبت‌نام انجام می‌گردد.

الزامات مربوط به روال رسیدگی به درخواست ابطال عبارت است از:

- شناسایی و احراز هویت درخواست ابطال گواهی
- ثبت و نگه‌داری تمام اطلاعات مربوط به درخواست
- بروز نمودن لیست گواهی‌های باطله و سرور ocsp بعد از ابطال گواهی

۴-۹-۴ مهلت اعلام درخواست ابطال

پس از تحقق هر یک از موارد بند ۱-۹-۴ درخواست ابطال گواهی در کمترین زمان ممکن به این مرکز ارائه می‌گردد.

۴-۹-۵ مدت رسیدگی به درخواست ابطال توسط مرکز گواهی

حداکثر زمان مجاز جهت رسیدگی به درخواست ابطال گواهی (مخصوصا در صورت افشای کلید خصوصی) توسط دفتر ثبت‌نام و مرکز میانی، در جداول زیر تعیین شده است.

جدول ۸ مدت رسیدگی به درخواست ابطال توسط دفتر ثبت‌نام

سطح اطمینان	مدت رسیدگی به درخواست ابطال توسط دفتر ثبت‌نام
سطح ۱و ۲	چنانچه درخواست ابطال در ساعات کاری دریافت گردد، در کمتر از ۲ ساعت پس از دریافت آن، پردازش می گردد. چنانچه درخواست ابطال خارج از ساعات کاری دریافت گردد، بلافاصله در شروع روز کاری بعد، پردازش می گردد چنانچه درخواست ابطال خارج از ساعات کاری دریافت گردد و روز بعدی نیز یک روز کاری نباشد، پردازش درخواست بیشتر از ۲۴ ساعت طول نخواهد کشید.

لازم به ذکر است که الزامات مدت زمان رسیدگی به درخواست تایید شده ابطال دریافتی از دفتر ثبت‌نام توسط مرکز صدور گواهی طبق جدول زیر می‌باشد.

جدول ۹ مدت رسیدگی به درخواست ابطال توسط مرکز صدور گواهی

سطح اطمینان	مدت رسیدگی به درخواست ابطال توسط مرکز
سطح ۱ و ۲	چنانچه درخواست ابطال در ساعات کاری توسط مرکز صدور گواهی دریافت گردد، در کمتر از ۲ ساعت پس از دریافت آن، پردازش می گردد. چنانچه درخواست ابطال خارج از ساعات کاری توسط مرکز صدور گواهی دریافت گردد، بلافاصله در شروع روز کاری بعد، پردازش می گردد چنانچه درخواست ابطال خارج از ساعات کاری توسط مرکز صدور گواهی دریافت گردد و روز بعدی نیز یک روز کاری نباشد، پردازش درخواست بیشتر از ۲۴ ساعت طول نخواهد کشید.

۴-۹-۶ الزامات بررسی ابطال توسط طرف های اعتماد کننده

طرف‌های اعتماد کننده باید پیش از استفاده از گواهی با مراجعه به مخزن یا با کمک سرویس OCSP از عدم وجود گواهی در لیست گواهی‌های باطل شده اطمینان حاصل نمایند.

الزامات مربوط به کنترل وضعیت ابطال گواهی، مطابق با بخش ۴-۹-۶ سند "سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور" می‌باشد.

آدرس سرویس OCSP این مرکز https://va.ica.pki.co.ir/ocsp و آدرس دسترسی به آخرین نسخه CRL، ldap://pkd.pki.co.ir:389/c=ir/pkiica.crl می‌باشد.

۴-۹-۷ تناوب صدور فهرست گواهی های باطله

لیست (های) گواهی‌های باطل شده، حتی اگر هیچ تغییر یا به‌روزرسانی در آن‌ها انجام نشده باشد، برای تایید اطلاعات، به صورت دوره‌ای صادر و به مخزن ارسال می‌شوند. مرکز میانی از این که لیست گواهی‌های باطل شده قبلی پس از ارسال آخرین نسخه این لیست از مخزن برداشته شده‌اند، مطمئن می‌شود. تناوب صدور لیست گواهی‌های باطله توسط این مرکز در جدول زیر قید شده است:

جدول ۱۰ تناوب صدور لیست گواهی‌های باطل‌شده

سطح اطمینان	تناوب صدور لیست گواهی‌های باطل شده
سطح ۱	• نسخه به‌روز شده CRL هر ۷ روز صادر می‌شود. • در صورتی که دلیل ابطال یک گواهی افشای کلید خصوصی باشد، حداکثر ۱ روز پس از دریافت و پردازش درخواست ابطال گواهی توسط مرکز میانی، یک نسخه به‌روز شده CRL صادر می‌شود.
سطح ۲	• نسخه به‌روز شده CRL هر ۲۴ ساعت صادر می‌شود.

سطح اطمینان	تناوب صدور لیست گواهی‌های باطل شده
	• در صورتی که دلیل ابطال یک گواهی افشای کلید خصوصی باشد، بلافاصله پس از دریافت و پردازش درخواست ابطال گواهی توسط مرکز میانی، یک نسخه به‌روز شده CRL صادر می‌شود.

۴-۹-۸ حداکثر تاخیر انتشار لیست گواهی های باطل شده

به طور معمول لیست گواهی‌های باطله به صورت خودکار و بلافاصله پس از ابطال گواهی، در مخزن منتشر می‌شود؛ در غیر این صورت حداکثر تأخیر مجاز بین ابطال یک گواهی (صدور لیست گواهی‌های باطل شده) و انتشار CRL در مخزن ۲ ساعت می‌باشد.

۴-۹-۹ دسترسی برخط به کنترل وضعیت/ابطال

این مرکز از پروتکل OCSP پشتیبانی می‌نماید و دسترسی به سرور پاسخ‌گوی OCSP را برای طرف‌های اعتمادکننده فراهم می‌آورد تا آن‌ها بتوانند برای اطلاع از وضعیت گواهی به صورت برخط به پاسخگوی OCSP مراجعه نمایند.

۴-۹-۱۰ الزامات کنترل برخط وضعیت ابطال

طرف اعتمادکننده می‌بایست قبل از استفاده از گواهی، وضعیت ابطال یا عدم ابطال آن را بررسی کند. این مرکز علاوه بر پشتیبانی از پروتکلOCSP، جهت اطمینان از دسترس‌پذیری دائمی سرویس اعلام وضعیت گواهی، از CRL نیز پشتیبانی می‌نماید. چنانچه نرم افزار سرویس گیرندگان این مرکز از پروتکل OCSP جهت اطلاع از وضعیت ابطال یک گواهی استفاده نمایند این نرم افزار نیازی به دریافت CRL و پردازش آن به منظور کنترل وضعیت ابطال آن گواهی ندارد.

۴-۹-۱۱ سایر روش‌های ممکن اعلان ابطال

در حال حاضر پشتیبانی نمی‌گردد.

۴-۹-۱۲الزامات خاص در صورت افشای کلید

در صورت افشای کلید خصوصی، بعد از ابطال گواهی، مرکز صدور گواهی، لیست گواهی‌های باطله به‌روز شده را مطابق با بخش ۴-۹-۷ منتشر می‌نماید و سرویس‌دهنده پاسخگوی OCSP منطبق با بخش ۴-۹-۹ در دسترس قرار می‌گیرد.

۴-۹-۱۳ شرایط تعلیق

این سرویس ارائه نمی‌گردد.

۴-۹-۱۴متقاضیان درخواست تعلیق گواهی

این سرویس ارائه نمی‌گردد.

۴-۹-۱۵فرایند رسیدگی به درخواست تعلیق

این سرویس ارائه نمی‌گردد.

۴-۹-۱۶محدودیت های دوره تعلیق

این سرویس ارائه نمی‌گردد.

۴-۱۰ خدمات وضعیت گواهی

۴-۱۰-۱ویژگی های عملیاتی

همیشه آخرین نسخه بروز شده لیست گواهی‌های باطله از طریق مخزن قابل دریافت می‌باشد و همچنین طرف‌های اعتماد کننده می‌توانند ازطریق نرم‌افزارهایی که تولید و ارسال یک درخواست OCSP و همچنین دریافت و اعتبارسنجی یک پاسخ OCSP را مطابق با RFC2560 پشتیبانی می‌کنند، از خدمات اعلام برخط وضعیت گواهی استفاده نمایند. ویژگی-های عملیاتی لیست گواهی‌های باطله در بخش ۲-۷ و ویژگی‌های عملیاتی خدمات اعلام برخط وضعیت گواهی در بخش ۳-۷ قید شده است.

۴-۱۰-۲ دسترسی‌پذیری خدمت (سرویس)

سرویس‌های ارائه وضعیت گواهی در طول عمر آن، بدون هیچ محدودیتی همواره در دسترس می‌باشند.

۴-۱۰-۳ ویژگی های اختیاری

خدمات اعلام برخط وضعیت گواهی(OCSP) و (TSA) از ویژگی‌های اختیاری بوده که در دسترس و قابل استفاده می‌باشند.

۴-۱۱ پایان اشتراک

این مرکز در صورت وقوع یکی از شرایط زیر می‌تواند به ارائه خدمات گواهی الکترونیکی برای مالک گواهی پایان دهد:

- با منقضی شدن گواهی بدون اینکه مجددا درخواست صدور گواهی نماید.
- با ابطال گواهی بدون اینکه درخواست تجدید کلید و یا درخواست صدور گواهی جدید نماید.

۴-۱۲ امانت‌گذاری و بازیابی کلید

پشتیبانی نمی‌گردد.

۴-۱۲-۱سیاست‌ها و دستورالعمل اجرایی امانت‌گذاری و بازیابی کلید

پشتیبانی نمی‌گردد.

۴-۱۲-۲ سیاست و دستورالعمل اجرایی بازیابی و اطلاعات مورد نیاز دسترسی به کلید

پشتیبانی نمی‌گردد.

۵. تجهیزات، مدیریت، و کنترل های عملیاتی

۵-۱ کنترل های فیزیکی

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن دارای تجهیزاتی مختص به فعالیت‌های این مرکز می‌باشد که از آنها در فعالیت‌های غیرمرتبط با وظایف مرکز استفاده نمی‌شود. همچنین کنترل‌های امنیت فیزیکی مورد نیاز به منظور حفاظت از نرم افزارها و سخت افزارهای این مرکز از دسترسی غیرمجاز، سرقت و خسارت، اجرا می‌شوند.

۵-۱-۱ ساختمان و محل سایت

این مرکز در محیطی عملیات خود را انجام می‌دهد که از لحاظ فیزیکی محافظت شده است، به طوریکه از هرگونه استفاده، دسترسی، افشای غیرمجاز اطلاعات حساس جلوگیری بعمل می‌آورد. ساختمان این مرکز براساس ملزومات امنیتی خاص طراحی شده است که دسترسی به تجهیزات مرکز مستلزم عبور از لایه‌های امنیتی فیزیکی مختلف با سطوح امنیتی مختلف (مطابق الزامات مندرج در سند سیاست های گواهی الکترونیکی زیرساخت کلید عمومی کشور) است و به این ترتیب دسترسی محدودتر شده و امنیت فیزیکی بیشتری در مقابل ورود و دسترسی غیرمجاز فراهم می‌آورد. هر لایه امنیتی فیزیکی لایه‌ی داخلی بعدی را در خود محصور می‌نماید و هر لایه امنیتی درونی به صورت کامل در لایه‌ی امنیتی بیرونی خود قرار می‌گیرد و نمی‌تواند با سطح خارجی لایه امنیتی بیرونی دیوار مشترک داشته باشد.

۵-۱-۲ دسترسی فیزیکی

دسترسی به سیستم‌های مرکز صدور گواهی الکترونیکی میانی خصوصی شرکت پندار کوشک ایمن توسط لایه های امنیتی مختلف کنترل می‌شود. ورود به سایت مرکز تنها با صدور مجوز توسط مدیر مرکز میانی و به همراه یکی از نقش‌های مجاز تعریف شده در مرکز میانی میسر می‌باشد. دسترسی به لایه‌های فیزیکی بعدی نیز توسط دستگاه‌های کنترل تردد و با استفاده از کارت‌های مخصوص و یا به صورت بایومتریک می‌باشد. دسترسی به لایه‌های امنیت فیزیکی قابل ثبت، بازرسی

و کنترل می‌باشد و هر لایه امنیتی تنها توسط پرسنل مجاز قابل دسترس می‌باشد، افراد و کارکنان غیرمجاز اجازه ورود به اماکن حساس و حافظت شده را ندارند.

اطلاعات فعال ساز که برای دسترسی و فعال کردن تجهیزات و ماژول‌های رمزنگاری مورد استفاده در مرکز به کار می‌روند، در زمانی که استفاده نمی‌شوند، به صورت امن و همراه با کنترل دسترسی نگه داری می‌شود.

هر متصدی پیش از خروج از سایت، یک بازرسی امنیتی شامل موارد زیر در قالب فرم گزارش اقدامات و کنترل‌ها، انجام داده و فرم مذکور را بایگانی می‌نماید.

- تجهیزات در وضعیتی متناسب با حالت عملکرد عادی قرار دارند؛
- تمام محفظه‌های حاوی اطلاعات امنیتی کاملاً در وضعیت ایمن قرار داشته باشند؛
- سیستم‌های امنیت فیزیکی (مانند قفل درها و سیستم‌های کنترل دسترسی) درست کار می‌کنند؛

سایت تجهیزات مرکز با سیستم‌های تشخیص نفوذ محافظت شود. علاوه بر این، حداقل هر ۲۴ ساعت یک بررسی صورت می‌گیرد تا اطمینان حاصل شود که هیچ تلاشی مبنی بر مقابله با مکانیزم‌های امنیتی صورت نگرفته است.

۵-۱-۳ تهویه هوا و منبع تغذیه

تجهیزات و محیط مرکز گواهی مجهز به نیروی برق و تهویه مطبوع کافی می‌باشد و این امر باعث می‌گردد که یک محیط قابل اطمینان جهت انجام عملیات ایجاد گردد.

مرکز صدور گواهی الکترونیکی میانی خصوصی شرکت پندار کوشک ایمن مجهز به تجهیزات امن اصلی و پشتیبان به شرح زیر می‌باشد:

- سیستم‌های تأمین نیروی برق به منظور دسترسی مداوم و بدون وقفه به نیروی برق
- سیستم‌های گرمایشی - سرمایشی و تهویهٔ هوا جهت کنترل درجهٔ حرارت و رطوبت نسبی.
- سیستم‌ها بصورت مداوم تحت نظارت قرار داشته و براساس دستورات تولیدکننده بصورت منظم مورد رسیدگی قرار می‌گیرند.

۵-۱-۴ جلوگیری از آبگرفتگی

مرکز میانی اقدامات کافی را به‌منظور به حداقل رساندن تأثیر نفوذ آب به سیستم‌های مربوطه اتخاذ می‌نماید نحوه‌ی نصب تجهیزات به گونه‌ای است که در معرض آبگرفتگی نباشند. سیستم جلوگیری از نفوذ آب که در مکان‌های آسیب‌پذیر و غیرمقاوم در برابر سیل نصب می‌گردد بر اساس دستورالعمل تولیدکننده آنها بطور منظم مورد کنترل و حفاظت قرار می‌گیرند.

۵-۱-۵ پیشگیری و محافظت در مقابل آتش

مرکز میانی اقدامات لازم برای پیشگیری و اطفاءحریق یا سایر صدمات ناشی از آتش یا دود را پیش‌بینی نموده است. اقدامات پیشگیری و جلوگیری از آتش سوزی براساس ضوابط آتش‌نشانی طراحی شده است. سیستم اطفای حریق به صورتی طراحی شده است که به محض بالا رفتن درجه حرارت محیط، به‌صورت اتوماتیک فعال می‌گردد.

۵-۱-۶ حفاظت از رسانه‌های ذخیره سازی

کلیهٔ ابزارهای نگهداری اطلاعات که دارای نرم افزار و داده‌های عملیاتی، اطلاعات ممیزی، آرشیو، یا پشتیبانی است و در داخل و یا خارج از این مرکز نگهداری می‌شوند به گونه‌ای محافظت می‌گردند که مکانیسم‌های کنترل دسترسی فیزیکی

و منطقی به آن‌ها محدود گردیده تا دسترسی اشخاص غیرمجاز به آنها امکان ناپذیر گردد. این امر از بروز خطرات (نظیر آب، آتش و الکترومغناطیس) جلوگیری می‌نماید. رسانه‌های حاوی اطلاعات بازرسی امنیتی، بایگانی‌ها یا اطلاعات پشتیبانی در مکانی جدا از تجهیزات مرکز میانی نگه‌داری می‌شوند.

به‌منظور کنترل و ذخیره اطلاعات، رویه‌هائی تدوین گردیده که جهت حفظ و حراست و عدم افشاء و یا سوء استفاده افراد غیر مجاز به کار برده می‌شوند.

۵-۱-۷ انهدام ضایعات

کلیهٔ وسایل حاوی اطلاعات حساس مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، در صورت عدم استفاده، به صورتی که اطلاعات موجود در آن‌ها غیرقابل بازیابی باشد، منهدم می‌شوند. ضمن این که سخت‌افزارهای رمزنگاری بلااستفاده یا غیر قابل استفاده در مرکز، شامل توکن‌ها و HSM قبل از امحاء سخت‌افزاری، جهت اطمینان و در صورت امکان امحاء نرم‌افزاری (همراه با بازنویسی فضای حافظه) می‌گردند. کارکنان این مرکز قبل از تخریب این وسایل دلیل آن را ذکر می‌کنند.

۵-۱-۸ نسخهٔ پشتیبان خارج از سایت

مرکز میانی به طور منظم از داده‌های حیاتی سیستم، داده‌های ممیزی، و سایر اطلاعات محرمانه مطابق با ۲-۵-۵ نسخه پشتیبان تهیه می‌کنند. نسخه پشتیبان خارج از سایت به شیوه‌ای که به لحاظ فیزیکی امن باشد و به لحاظ الزامات، همانند مرکز داده اصلی باشد، نگهداری می‌شود.

۵-۲ کنترل‌های فرایندی

۵-۲-۱ نقش‌های مورد اطمینان

کلیه فعالیت‌های مرکز میانی در قالب وظایف تدوین شده برای نقش‌های تعریف شده‌ای که به کارکنان مرکز منتسب شده‌اند، صورت می‌پذیرند. افرادی که برای این نقش‌ها انتخاب می‌شوند همانگونه که در بخش ۳-۵ ذکر شده قابل اطمینان می‌باشند. نقش‌های مورد اطمینان در مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن شامل کلیهٔ کارکنانی در مرکز می‌باشد که به فرایندهای احراز هویت و عملیات اجرایی اصلی مرکز دسترسی و یا کنترل دارند و در رده‌های مختلف فعالیت می‌نمایند. برای افزایش امنیت، انجام فعالیت‌های مرکز میانی، مستلزم حضور بیش از یک نقش مورد اطمینان است. این امر از فعالیت‌های مخرب که احتیاج به تبانی دارند، جلوگیری می‌نماید.

نقش‌های اصلی مورد اطمینان برای اداره و راهبری مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن به شرح زیر است:

- **مدیر مرکز میانی**

مدیر مرکز میانی کلیه هماهنگی‌های موردنیاز، جهت پیش‌برد اهداف مرکز را انجام می‌دهد. وی از دانش، اطلاعات و تجربیات لازم و کافی مدیریتی و توانایی و تجربه کافی در زمینه دانش زیرساخت کلید عمومی برخوردار می‌باشد. همچنین با کلیه فعالیت‌هایی که جهت صدور گواهی در دفتر ثبت‌نام و مرکز میانی انجام می‌پذیرد، روند اجرای امور و کلیه کارکنان مرکز به تفکیک وظایف آشنا می‌باشد.

بازرسی داخلی مرکز میانی بعهده این نقش می باشد.

- **مدیر دفتر ثبت‌نام**

مدیر دفتر ثبت‌نام مرکز میانی زیرنظر مدیر مرکز میانی، فعالیت‌های دفتر ثبت‌نام را کنترل و نظارت می‌نماید. کلیهٔ عملیات احراز هویت و تنظیم درخواست متقاضیان گواهی که به دفتر ثبت‌نام این مرکز مراجعه می‌کنند در این دفتر صورت می‌گیرد عمده وظایفی که وی در مرکز میانی برعهده دارد عبارتند از:

- بازرسی و بررسی تطابق عملیات صورت گرفته در دفتر ثبت‌نام با دستورالعمل اجرایی مرکز میانی و سایر اسناد مربوط به دفتر ثبت‌نام؛
- نظارت بر کلیه فعالیت‌های کارکنان دفتر ثبت‌نام و ارائه راهنمایی‌های لازم به آنها؛
- ارائه گزارش‌های مربوط به دفتر ثبت‌نام به مدیر مرکز میانی؛
- تایید، رد یا بازگشت درخواست متقاضی.

- **متصدی دفتر ثبت‌نام**

متصدی دفتر ثبت‌نام فردی است که در دفتر ثبت‌نام فعالیت می‌کند و مسئولیت احراز هویت درخواست‌کنندگان گواهی و یا نمایندگان آنها را بر عهده دارد. این فرد باید بر روند اجرای عملیات احراز هویت تسلط کافی داشته باشد. وی باید از مطالب مندرج در توافق‌نامه سطح ارائه خدمات آگاهی داشته و از تعداد و نوع مدارک مورد نیاز برای هر موجودیت و برای هر نوع گواهی مطلع باشد.

در دفتر ثبت‌نام این مرکز، متصدی دفتر ثبت‌نام وظایف زیر را بر عهده دارد:

- دریافت و کنترل مدارک شناسایی متقاضی و نمایندگان او (در صورت ارائه درخواست توسط نماینده متقاضی) جهت احراز هویت موجودیت با توجه به نوع گواهی مورد درخواست و این که گواهی برای چه موجودیتی درخواست شده است؛
- بررسی انطباق توکن ارائه شده توسط متقاضی صدور گواهی با لیست توکن‌های معتبر و قابل اطمینانی که در وب‌سایت مرکز دولتی ریشه قرار داده شده است؛
- دریافت اصل قبض واریزی مطابق با مبالغ تعیین شده برای هر نوع درخواست، طبق تعرفه‌های مصوب هیات وزیران.
- بایگانی مطمئن اطلاعات شامل مدارک شناسایی متقاضی و نمایندگان او (در صورت ارائهٔ درخواست توسط نماینده)، توافق‌نامه سطح ارائه خدمات امضا شده توسط متقاضی، اصل قبض واریزی، و دیگر اسناد.

- **اپراتور دفتر ثبت‌نام**

اپراتور دفتر ثبت‌نام فردی است که در دفتر ثبت‌نام فعالیت می‌کند و مسئولیت ثبت کامپیوتری درخواست‌های صدور، تمدید، و ابطال گواهی را بر عهده دارد. اپراتور دفتر ثبت‌نام باید با سرویس‌های ارائه شده در نرم‌افزار دفتر ثبت‌نام آشنایی کافی داشته باشد و از نحوه کار با آن نرم‌افزار مطلع باشد. وظایف اپراتور دفتر ثبت‌نام از این قرارند:

- انجام عملیات کامپیوتری مربوط به ثبت درخواست‌های صدور، تمدید، و ابطال گواهی و امضای آن‌ها؛
- کنترل تطابق کلید خصوصی با کلید عمومی متقاضی با بررسی صحت امضای روی درخواست گواهی که با استفاده از استاندارد PKCS#10 تنظیم شده است (در صورتی که تولید کلید از سوی متقاضی انجام شده باشد)؛
- تولید کلید بر روی توکن متقاضی و نیز ایجاد CSR (در صورتی که قرار باشد تولید کلید به نمایندگی از متقاضی توسط دفتر ثبت‌نام انجام شود)؛
- ارسال درخواست به مرکز صدور گواهی؛

- دریافت نتیجه درخواست ارسالی از سمت مرکز صدور گواهی؛
- تحویل گواهی به مالک آن؛
- پشتیبان‌گیری دوره‌ای از سرویس‌دهنده دفتر ثبت‌نام.

- **مدیر صدور گواهی الکترونیکی**

در مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن کلیهٔ عملیات مربوط به مدیریت گواهی الکترونیکی موجودیت‌های نهایی شامل صدور، ابطال، انتشار، تمدید و تجدید کلید گواهی صورت می‌گیرد. مدیر صدور گواهی الکترونیکی میانی باید با روند اجرای فعالیت‌ها و کلیهٔ فرایندهایی که در مرکز میانی انجام می‌گیرد آشنا باشد. به علاوه، وی باید آشنایی کافی با دانش زیرساخت کلید عمومی داشته باشد.

مدیر صدور گواهی الکترونیکی میانی بصورت مستقیم زیرنظر مدیر مرکز میانی فعالیت‌های خود را انجام می‌دهد و در ارتباط مستقیم با اپراتورهای صدور گواهی مرکز میانی است.

مدیر صدور گواهی الکترونیکی میانی مسئولیت‌های زیر را بر عهده دارد:

- بررسی تطابق عملیات صورت گرفته در مرکز میانی با «دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن»؛
- اطمینان از آگاهی اپراتورهای صدور گواهی میانی در مورد مسئولیت‌های محول شده به وی؛
- اطمینان از مسئولیت‌پذیری اپراتورهای صدور گواهی میانی؛
- ارائه راهنمایی‌های لازم به اپراتورهای صدور گواهی میانی.

- **اپراتور اول صدور گواهی میانی**

اپراتور اول صدور گواهی میانی شخصی است که زیر نظر مدیر مرکز صدور گواهی الکترونیکی میانی فعالیت می‌کند و مسئولیت مدیریت درخواست‌های مرتبط با گواهی را بر عهده دارد. اپراتور اول صدور گواهی میانی باید به نرم‌افزار مرکز میانی تسلط کافی داشته باشد و با همهٔ امکانات و قابلیت‌های این نرم‌افزار آشنا باشد.

وظایف عمدهٔ اپراتور اول صدور گواهی میانی عبارتند از:

- رسیدگی به درخواست‌های امضا شده توسط دفتر ثبت‌نام (صدور، ابطال، تجدید، و تمدید گواهی)؛
- اعلام صدور گواهی به مالک گواهی جهت پذیرش آن؛
- قرار دادن گواهی صادر شده در مخزن گواهی پس از پذیرش گواهی توسط متقاضی[۱۸]؛
- صدور دوره‌ای فهرست گواهی‌های باطله و قرار دادن آن در مخزن.

- **اپراتور دوم صدور گواهی میانی**

اپراتور دوم صدور گواهی میانی شخصی است که زیر نظر مدیر صدورگواهی الکترونیکی میانی فعالیت می‌کند و مسئولیت‌هایی مانند مدیریت پشتیبان‌گیری/ بازیابی، برپایی مرکز صدور، و توقف سیستم را برعهده دارد.

اپراتور دوم صدور گواهی میانی باید به نرم‌افزار صدور گواهی مرکز میانی تسلط کافی داشته باشد و با همهٔ امکانات و قابلیت‌های این نرم‌افزار آشنا باشد.

وظایف عمدهٔ اپراتور دوم صدور گواهی میانی عبارتند از:

[۱۸] شرایط پذیرش گواهی در بخش ۴-۴ سند «دستورالعمل اجرایی گواهی الکترونیکی پندار کوشک ایمن» آمده است.

- پشتیبان‌گیری از مرکز صدور گواهی (Backup CA)،
- بازگردانی مرکز صدور گواهی (Restore CA)،
- برپایی مرکز صدور گواهی (Build Server)،
- گزارش‌گیری رویدادهای نگهداری (Export Maintenance Logs)،
- توقف سیستم (Stop System).

- **کارشناس امنیت اطلاعات**

کارشناس امنیت اطلاعات، فردی است که دارای دانش، اطلاعات و تجربیات کافی در زمینه سیستم مدیریت امنیت اطلاعات می‌باشد و با استانداردهای امنیت فضای تبادل اطلاعات، مفاهیم ارزیابی امنیتی و تست نفوذ، آشنایی کافی دارد.

وظایف عمدهٔ کارشناس امنیت اطلاعات به شرح زیر می‌باشد:

- نظارت بر اجرای درست استانداردهای امنیتی فناوری اطلاعات در کلیهٔ فعالیت‌های انجام شده در مرکز میانی
- پیاده‌سازی و نگهداری سیستم مدیریت امنیت اطلاعات؛
- نظارت بر امنیت شبکه و اطلاعات زیرساخت؛
- تحلیل ریسک‌های امنیتی زیرساخت؛
- تعریف پروژه‌ها و ارائه سیاست‌هایی در راستای بهبود امنیت زیرساخت؛
- ارزیابی امنیتی زیرساخت کلید عمومی به صورت دوره‌ای؛
- انجام بازنگری رویدادهای بازرسی و تهیه خلاصه از آنها؛
- برقراری امنیت در منابع انسانی (منابع انسانی شامل کلیهٔ افرادی است که مرکز میانی فعالیت می‌کنند).

- **مدیر نگهداری و پشتیبانی**

نگهداری و پشتیبانی مرکز میانی دربرگیرنده کلیهٔ فعالیت‌هایی است که به منظور نگهداری و پشتیبانی از شبکه، نرم‌افزارها، سخت‌افزارها و مرکز دادهٔ زیرساخت انجام می‌شود. مدیر نگهداری و پشتیبانی، باید از دانش و اطلاعات کافی در مورد شبکه و امنیت شبکه برخوردار باشد. همچنین، این شخص جهت مدیریت کارشناسان بخش نگهداری و پشتیبانی سخت‌افزارها و نرم‌افزارها، باید با نرم‌افزارها و سخت‌افزارهای مورد استفاده در مرکز میانی و نحوه پیکربندی آن‌ها آشنایی کافی داشته باشد.

مدیر نگهداری و پشتیبانی مرکز، وظایف زیر را بر عهده دارد:

- مدیریت و نظارت بر کارکرد مطمئن مرکز داده؛
- مدیریت و نظارت بر عملکرد کارشناسان نرم‌افزار، سخت‌افزار، شبکه و مرکز داده؛
- پشتیبانی فنی تجهیزات و سیستم های دفتر های ثبت نام

- **کارشناس نگهداری و پشتیبانی مرکز داده**

کارشناس نگهداری و پشتیبانی مرکز داده باید دانش کاملی درباره نحوه پشتیبانی، نگهداری، و عملکرد مرکز داده داشته باشد.

وظایف عمدهٔ کارشناس نگهداری مرکز داده عبارتند از:

- نظارت بر عملیات مرکز داده؛
- مدیریت دسترسی فیزیکی به تجهیزات مرکز داده؛

- نظارت و کنترل سیستم‌های تهویه و خنک‌کننده؛
- نظارت و کنترل سیستم‌های اطفای حریق؛
- نظارت و کنترل سیستم دوربین‌های مداربسته؛
- نظارت و کنترل سیستم برق مرکز داده از جمله UPS و ژنراتور؛
- همکاری با کارشناسان دیگر در صورت لزوم به منظور رفع مشکلات یا بهبود سرویس‌دهی مرکز داده؛
- مطلع کردن مدیر نگهداری و پشتیبانی از هرگونه تغییری که در مرکز داده صورت می‌گیرد؛
- مستندسازی فعالیت‌ها و سرویس‌های ارائه شده و تهیه گزارش‌ها و آمارهای درخواستی در حوزه وظایف.

- **کارشناس نگهداری و پشتیبانی شبکه**

کارشناس نگهداری و پشتیبانی شبکه باید دانش و اطلاعات کاملی از تجهیزات شبکه و نحوه عملکرد آنها داشته باشد. وظایف عمدهٔ کارشناس نگهداری شبکه عبارتند از:

- نگهداری از کلیهٔ تجهیزات شبکه بر اساس استانداردهای فناوری اطلاعات و ارتباطات؛
- مطلع کردن مدیر نگهداری و پشتیبانی از هر گونه تغییری که در شبکه صورت می‌گیرد؛
- نظارت بر کلیهٔ عملیات و رویدادهای شبکه؛
- نظارت و بازرسی کلیهٔ عملیات و رویدادهای امنیتی فایروال‌ها و سیستم‌های تشخیص و جلوگیری از نفوذ در تناوب حداکثر ۲۴ ساعت؛
- شناسایی و رفع مشکلات شبکه‌ای هر یک از اجزای شبکه زیرساخت مثل فایروال‌ها، سوئیچ‌ها و غیره؛
- نصب و پیکربندی سیستم‌عامل و نرم‌افزارهای امنیتی مثل آنتی‌ویروس و فایروال‌ها بر روی سیستم‌ها مرکز میانی و دفاتر ثبت نام؛
- مستندسازی فعالیت‌ها و سرویس‌های ارائه شده و تهیه گزارش‌ها و آمارهای درخواستی در حوزه وظایف؛

- **کارشناس نگهداری و پشتیبانی نرم‌افزار**

نگهداری و پشتیبانی نرم‌افزار شامل کلیهٔ عملیاتی است که جهت توسعه و بهبود عملکرد نرم‌افزارهای موجود در زیرساخت و رفع مشکلات آن‌ها انجام می‌گیرد. کارشناس نگهداری و پشتیبانی نرم‌افزار باید با نرم‌افزارهای زیرساخت و سخت‌افزارهایی که این نرم‌افزارها روی آن‌ها نصب شده‌اند، آشنایی فنی کافی داشته باشد. این شخص باید توانایی و تجربه کافی در زمینه برنامه‌نویسی و سیستم‌عامل لینوکس داشته باشد. وظایف عمدهٔ کارشناس نگهداری و پشتیبانی نرم‌افزار عبارتند از:

- نصب و پیکربندی نرم‌افزارهای مرکز صدور گواهی و دفتر ثبت‌نام؛
- نصب و پیکربندی کلیهٔ نرم‌افزارهای مرتبط با صدور گواهی؛
- شناسایی و رفع مشکلات پیش‌آمده در نرم‌افزارها؛
- ارائه راهکارهای مناسب در جهت توسعه و بهبود نرم‌افزارها؛
- نظارت و پیگیری نگهداری نرم‌افزارها (مثلاً نظارت بر روند تهیه نسخهٔ پشتیبان از پیکربندی نرم‌افزارها به صورت دوره‌ای و بایگانی آن‌ها)؛
- پاسخگویی و راهنمایی کاربران در حوزه وظایف؛
- مستندسازی فعالیت‌ها و سرویس‌های ارائه شده و تهیه گزارش‌ها و آمارهای درخواستی در حوزه وظایف.
- بایگانی مطمئن اطلاعات.

- **کارشناس نگهداری و پشتیبانی سخت‌افزار**

نگهداری و پشتیبانی سخت‌افزار شامل کلیهٔ عملیاتی است که جهت رفع مشکلات و بهبود عملکرد سخت‌افزارهای موجود در زیرساخت کلید عمومی صورت می‌گیرد. وظایف عمدهٔ کارشناس نگهداری و پشتیبانی سخت‌افزار عبارتند از:

- نصب و پیکربندی ملزومات سخت‌افزاری مرکز میانی و دفاتر ثبت نام؛
- تولید کلید و نگهداری از پودمان رمزنگاشتی؛
- ارائه مشاوره فنی، کنترل و نظارت در امر تهیه تجهیزات سخت‌افزاری موردنیاز زیرساخت؛
- بررسی فنی قطعات و سخت‌افزارهای خریداری شده؛
- تشخیص و رفع مشکلات سخت‌افزاری سیستم‌ها؛
- نظارت بر فرایند ارسال تجهیزاتی که نیاز به تعمیر دارند و کنترل کیفیت تعمیر تجهیزات؛

مستندسازی فعالیت‌ها و سرویس‌های ارائه شده و تهیه گزارش‌ها و آمارهای درخواستی در حوزه وظایف.

۵-۲-۲ تعداد افراد مورد نیاز برای هر نقش

مرکز میانی به منظور حصول اطمینان از تفکیک وظائف براساس مسئولیت‌ها و حضور بیش از یک شخص مورد اطمینان برای انجام فعالیت‌های حساس، روش‌های کنترلی مجدانه‌ای را تدوین، به روزآوری و اعمال نموده است. به منظور حصول اطمینان از تفکیک وظائف براساس مسئولیت‌ها، روش‌های کنترلی اجرا می‌شوند. انجام فعالیت‌های حساس از قبیل مدیریت و دسترسی به سخت‌افزارهای رمزنگاری مرکز گواهی و تجهیزات مربوط به کلیدها، به بیش از یک شخص مورد اطمینان نیاز دارد بشکلی که کلیه امور در حضور تمامی افراد مورد اطمینان مجاز صورت پذیرد. به طورکلی در موارد که دسترسی به اطلاعات حساس مرکز میانی مانند کلیدهای خصوصی مورد نیاز است برای سطح ۱، حداقل ۱ نفر و برای سطح ۲، حداقل دو نفر مورد نیاز است و برای سایر وظایف ۱ نفر کافی است.

۵-۲-۳شناسائی و احراز هویت برای هر نقش

هر یک از کارکنان مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن که به عنوان نقش مورد اطمینان در مرکز فعالیت می‌کنند، پیش از اینکه در موقعیت های زیر قرار گیرند باید شناسایی و احرازهویت شوند.

- قرار گرفتن در لیست دسترسی به سایت مرکز میانی؛
- قرار گرفتن در لیست دسترسی فیزیکی به سیستم مرکز میانی؛
- دریافت حکم برای برعهده گرفتن یک نقش مورد اطمینان در مرکز میانی؛
- ایجاد حساب کاربری در سیستم‌های مرتبط با زیرساخت کلید عمومی (PKI). اگر حساب کاربری نیاز باشد؛
- حکم یا حساب کاربری در دو بند بالا:
  - تنها به یک شخص به طور مستقیم منتسب می‌شود؛
  - اشتراکی نیست؛
  - با استفاده از کنترل‌های فرایندی برای هیچ منظور دیگری غیر از اجرای وظایف تخصیص داده شده به نقش مربوطه، استفاده نمی‌شود.

۵-۲-۴ نقش‌های مستلزم تفکیک وظایف

در مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، نقش‌های مورد اطمینان به صورت تفکیک شده، تعریف شده است. این نقش‌ها به همراه وظایف تعریف شده برای آن‌ها در بخش ۵-۲-۱ آمده است.

۵-۳ کنترل کارکنان

کارهایی که مرکز میانی به کارکنان واگذار می‌نماید، با وظایف تعریف‌شده برای آن‌ها و حدود اختیاراتشان تناقضی ندارد. علاوه بر آن کارکنان موارد زیر را انجام می‌دهند:

- تعهد کتبی به منظور رعایت مقررات و عدم افشای اطلاعات حساس و امنیتی مرکز را امضا می‌کنند.
- به وسیله قرارداد یا حکم، به شرایط و ضوابط موقعیتی که در آن قرار می‌گیرند، پایبند می‌باشند.
- آموزش‌های لازم متناظر با وظایفی که بر عهده دارند را دریافت می‌کنند.

۵-۳-۱ الزامات مربوط به قابلیت‌ها، سابقه و عدم سوء پیشینه

اشخاصی که برای انجام فعالیت‌های مرکز میانی در نظر گرفته می‌شوند براساس معیارهایی از قبیل قابلیت‌های فنی، مورد اطمینان بودن و امانت‌داری انتخاب می‌شوند. علاوه بر این تمام کارکنان مرکز دارای تابعیت ایرانی بوده و دارای گواهی عدم سوء پیشینه از نیروی انتظامی جمهوری اسلامی ایران می‌باشند. افرادی که برای کار با تجهیزات مرکز میانی انتخاب شده‌اند دارای مشخصات زیر می‌باشند:

- با موفقیت یک دوره مناسب آموزش را به پایان رسانده باشند.
- توانایی خود را برای انجام وظایفی که به ایشان محول شده به اثبات رسانند.
- مورد اطمینان باشند.
- دارای هیچ‌گونه شغل یا وظیفه دیگری که روی انجام وظایف محوله به آن ها مداخله یا تأثیر داشته باشد، نباشند.
- ارائه گواهی حسن انجام کار (در صورت داشتن سابقه کاری مرتبط)
- دارای سوء پیشینه نبوده و یا گواهی عدم سوء پیشینه‌شان با اطلاع قبلی باطل نشده باشد.
- دارای محکومیت کیفری نبوده باشند.

۵-۳-۲ رویه بررسی سابقه افراد

این فرایند تحت قوانین جاری کشور صورت می‌گیرد. مرکز میانی، پیش از آغاز استخدام فرد، در مورد سوابق فردی وی کنترل‌های زیر را انجام می‌دهد:

- تأیید سوابق شغلی
- بررسی مدارک و سوابق حرفه‌ای
- تأیید آخرین مدرک تحصیلی مرتبط
- احراز عدم سوء پیشینه بررسی سوابق مالی/ اعتباری

- بررسی سوابق تخلفات

اطلاعاتی که از بررسی سوابق مشخص می‌شود و احتمالاً موجب عدم پذیرش شخص برای تصدی یک نقش مورد اطمینان می‌شود و یا موجب سلب اطمینان از فرد شاغل می‌گردد، حداقل شامل موارد زیر می‌باشد:

- ارائه اطلاعات غیر واقعی توسط نامزد تصدی نقش مورد اطمینان
- سوابق حرفه‌ای نامعتبر یا غیر قابل اعتماد
- سابقه جرم در برخی تخلفات معین
- هرگونه نشانه ای از تخلفات مالی

۵-۳-۳ الزامات آموزشی

مرکز میانی، آموزش‌های مورد نیاز پرسنل را در آغاز کار و یا حین خدمت جهت ایفای مطلوب و رضایت بخش مسئولیت‌های محوله ارائه می‌دهد. همچنین سوابق این گونه آموزش‌ها را ثبت و نگهداری می‌نماید. شرکت پندار کوشک ایمن برنامه‌های آموزشی را به صورت دوره ای بازنگری نموده و در صورت نیاز آن را بهبود می‌بخشد.

برنامه‌های آموزشی، متناسب با مسئولیت‌های محوله تنظیم شده که می‌تواند شامل موارد زیر باشد:

- مفاهیم پایه‌ای زیرساخت کلید عمومی
- مسئولیت‌های شغلی
- دستورالعمل‌ها، خط مشی ها، قوانین، و رویه های امنیتی و اجرائی
- نحوه به کارگیری و اجرای سخت‌افزار و نرم‌افزار مورد استفاده
- نحوه گزارش‌دهی و مواجهه با اتفاقات و افشای اطلاعات
- رویه‌های بازیابی از بحران و تداوم عملیات

۵-۳-۴ الزامات آموزش مکرر و متناوب

مرکز میانی آموزش‌های حین خدمت را جهت به روزآوری دانش کارکنان به صورت سالانه ارائه می‌نماید به ترتیبی که کارکنان در سطح کیفی و حرفه‌ای به روز باقی مانده و وظائف خود را به طور مطلوب و رضایت بخش انجام دهند. این مرکز پیش از تغییر در عملکرد مرکز صدور گواهی دارای برنامه آموزشی لازم می‌باشد و پس از برگزاری هر آموزشی، آن را به صورت مستند شده در اختیار کارکنان مرکز قرار می‌دهد. در صورت هرگونه تغییر در نقش مورد اطمینان برای کارکنان مرکز میانی آموزش‌های مرتبط به کارکنان ارائه خواهد شد. اجرای برنامه های آموزشی مستند می شود.

۵-۳-۵ دوره زمانی و ترتیب چرخش کار

در حال حاضر سیاستی برای چرخش مشاغل تعریف نگردیده است.

۵-۳-۶ جریمه‌های اقدامات خارج از محدوده اختیارات

در قبال رفتارهای غیر مجاز و هر گونه نقض دستورالعمل‌ها، خط مشی‌ها، قوانین و رویه‌های مرکز میانی، مدیریت مرکز می‌تواند ضمن در نظر گرفتن جریمهٔ متناسب برای شخص خاطی، به همکاری وی با مرکز میانی پایان دهد. اقدامات مربوط به این موضوع در چارچوب مقرارت و با رعایت الزامات زیرساخت کلید عمومی صورت می‌گیرد.

۵-۳-۷ الزامات پیمانکاران مستقل

مرکز میانی با دریافت ضمانت‌نامه‌های متناسب، مراحل عقد قرارداد و شرایط و ضوابط همکاری را مشخص می‌کند تا اطمینان حاصل شود که کلیهٔ پیمانکاران طرف قرارداد بر طبق مفاد سیاست‌های گواهی الکترونیکی و دستورالعمل اجرایی گواهی الکترونیکی این مرکز عمل می‌کنند.

۵-۳-۸ مستندات فراهم شده برای کارکنان

مرکز میانی برای انجام مطلوب و رضایت‌بخش وظائف، آموزش و مستندات لازم را به کارکنان ارائه می‌نماید.

۵-۴ فرایندهای ثبت رویدادهای بازرسی

۵-۴-۱ انواع رویدادهای قابل ثبت

مرکز میانی ظرفیت ثبت همه‌ی رویدادهای مربوط به امنیت سیستم مرکز صدور گواهی شامل فایروال‌ها، دایرکتوری و سرورهای میزبان نرم افزار CA و RA را در فایل‌های ثبت رویدادهای بازرسی امنیتی دارد. همچنین قابلیت ثبت رویدادهای امنیتی در سیستم عامل‌های تجهیزات مرکز میانی در زمان شروع به کار سیستم، به طور خودکار فعال می‌باشند.

رویدادهای زیر در سیستم‌های مرکز میانی توسط سیستم یا به صورت دستی ثبت می‌گردد:

- ورود و خروج به برنامه‌های کاربردی مرکز میانی
- تلاش برای تعیین و حذف گذرواژه یا تغییر مجوزهای ورود به سیستم
- تعریف، حذف یا اضافه کردن کاربران و نقش‌ها
- هر تغییری در پیکربندی سیستم‌های مرکز میانی
- پشتیبان‌گیری و بازیابی پایگاه داده
- تولید کلیدهای مرکز میانی
- صدور و ابطال گواهی‌ها
- امضای لیست گواهی‌های باطل شده

- تولید درخواست‌های تنظیم و تایید شده در دفتر ثبت‌نام
- ارسال هر داده‌ای به مخزن
- خطاهای رخ داده شده در سیستم

کلیه موارد ثبت‌شده، چه الکترونیکی و چه دستی، دارای تاریخ و زمان رویداد و موجودیتی که باعث وقوع رویداد شده است می‌باشند. ضمنا جهت اطمینان از تمامیت و دست نخوردگی اطلاعات مرتبط با رویدادهای ثبت شده، این اطلاعات امضا می‌شود.

همچنین مرکز میانی به صورت الکترونیکی یا دستی، اطلاعات امنیتی که توسط سیستم مرکز میانی تولید نشده است را جمع آوری می‌نماید. این اطلاعات شامل موارد زیر است:

- رویدادهای مربوط به دسترسی‌های فیزیکی
- تغییرات مربوط به پیکربندی سیستم
- تغییرات مربوط به کارکنان مرکز میانی
- گزارش‌های مربوط به اختلافات و تفاهم‌ها
- گزارش‌های مربوط به از بین رفتن اطلاعات حساس
- نسخه‌های قبلی و نسخه‌های جاری دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن
- گزارش‌های مربوط به ارزیابی آسیب‌پذیری
- گزارش‌های مربوط به ارزیابی تهدیدات و خطرها
- خرابی تجهیزات
- زمان و مدت قطع جریان برق
- گزارشات مربوط به قبول بازدید و سرکشی
- نسخه‌های قبلی و نسخه‌های جاری توافق‌نامه شرایط حاکم بر استفاده از گواهی و دیگر اطلاعاتی که مالک گواهی با آنها موافقت کرده است
- انتصاب کارکنان مرکز
- آموزش کارکنان مرکز.

۵-۴-۲تناوب پردازش اطلاعات رویدادهای ثبت شده

سوابق ممیزی رخدادهای مهم امنیتی و عملیاتی مطابق جدول تناوب زمانی بررسی می‌گردند. علاوه بر مورد مذکور، سوابق ممیزی به منظور شناسایی هرگونه فعالیت غیرمعمول یا مشکوک در پاسخ به هشدارهای اعلام شده توسط سیستم‌های مرکز میانی و دفاتر ثبت‌نام گواهی مورد بررسی قرار می‌گیرند. پردازش سوابق ممیزی شامل بررسی سوابق و مستندات کلیه رخدادهای موجود در گزارش جمع بندی سوابق است. بررسی سوابق ممیزی دربرگیرنده تأییدیه عدم دستکاری، بازرسی کلیه موارد ثبت شده، و بررسی هرگونه هشدار و موارد غیرمعمول می‌باشد. در این مرکز کارشناس امنیت اطلاعات مسئول انجام بازنگری رویدادهای بازرسی و تهیه خلاصه رویدادهای بازرسی می‌باشد. کلیه عملیات انجام شده جهت بررسی سوابق مستند می‌گردند.

جدول ۱۱ تناوب پردازش اطلاعات رویدادهای ثبت‌شده

سطح اطمینان	تناوب پردازش اطلاعات رویدادهای ثبت شده
سطح ۱	پردازش و بازنگری رویدادها حداقل هر شش ماه یک بار صورت می‌گیرد.
سطح ۲	پردازش و بازنگری رویدادها حداقل هر دو ماه یک بار صورت می‌گیرد.

۵-۴-۳ دوره نگهداری از اطلاعات رویدادهای ثبت شده

سوابق ممیزی لازم است حداقل به مدت شش ماه پس از پردازش، در همان محل سایت نگهداری شده و پس از آن مطابق بخش ۲-۵-۵ بایگانی می‌گردند.

۵-۴-۴ محافظت از اطلاعات رویدادهای ثبت شده

سوابق ممیزی توسط سیستم الکترونیکی رخدادنگاری محافظت می‌شوند که شامل: مکانیسم‌هایی جهت جلوگیری از هرگونه مشاهده، تغییر، حذف، یا دستکاری غیرمجاز در فایل‌های سوابق می‌باشد. نتایج بدست آمده از ممیزی وقایع ثبت شده به صورتی محافظت می‌گردند که افراد غیر مجاز قادر به تغییر و یا حذف آنها نباشند. هیچ کس مجاز به تغییر محتوای وقایع ثبت شده نیست.

نسخه ای از ثبت وقایع ممیزی، در مکانی امن (مطابق الزامات مرکز دولتی ریشه) می‌باشد و جدا از تجهیزات مرکز میانی است، نگه داری می‌شود. هیچ فردی حق حذف و یا از بین بردن وقایع ثبت شده را نخواهد داشت.

۵-۴-۵فرایندهای پشتیبان‌گیری از رویدادهای بازرسی

نسخه پشتیبان افزایشی به صورت روزانه، و نسخه پشتیبان کامل به صورت هفتگی تهیه می‌گردند.

۵-۴-۶سامانه جمع‌آوری اطلاعات بازرسی

داده‌های ممیزی در سطوح برنامه کاربردی، شبکه، و سیستم عامل به صورت خودکار تولید و ثبت می‌گردند. داده‌های ممیزی دستی توسط کارکنان مرکز میانی ثبت می‌شوند.

فرآیند ثبت وقایع هنگام راه اندازی سیستم شروع به کار می‌نماید و فقط هنگام خاموش شدن سیستم متوقف می‌شود. در صورتی که مشخص شود سیستم ثبت وقایع خودکار از کار افتاده است و یا در این سیستم اشکالی وجود دارد و تمامیت سیستم و محرمانگی اطلاعات در خطر است، مرکز کلیه فعالیت‌های خود را به غیر از فرآیند باطل کردن گواهی‌ها متوقف می‌نماید تا وقتی که سیستم مجددا به کار افتد.

۵-۴-۷ تذکر به مسبب رویداد

هنگامی که رخداد به وسیله سیستم جمع‌آوری اطلاعات ممیزی ثبت می‌گردد، ارسال اعلامیه به شخص، سازمان، دستگاه، یا برنامه کاربردی ایجاد کننده رخداد الزامی نمی‌باشد.

۵-۴-۸ ارزیابی آسیب‌پذیری

کارکنان مراکز میانی باید مراقب اقداماتی که برای ایجاد اختلال در تمامیت سیستم مدیریت گواهی‌ها انجام می‌شوند (مانند تجهیزات، مکان فیزیکی و کارکنان) باشند. کارشناس امنیت اطلاعات ثبت وقایع امنیتی را برای وقایعی مانند فعالیت‌های ناموفق تکراری برای دسترسی به سیستم، اقدام برای به دست‌آوردن اطلاعات محرمانه، تلاش برای دسترسی به فایل‌های سیستمی و پاسخ‌های تأیید نشده، بازبینی می‌نماید. خلاصه نتایج مرور اطلاعات بازرسی امنیتی مستند می‌شود. یکی از دلایل ثبت رخدادها در فرایند ممیزی، کاهش آسیب‌پذیری سیستم می‌باشد. متعاقب بررسی رخدادهای رویدادنگاری شده، فرایندهای ارزیابی منطقی آسیب‌پذیری امنیتی اجرا، مرور و بازبینی می‌شوند. ارزیابی‌های منطقی آسیب‌پذیری امنیتی بر پایه داده‌های رخدادنگاری خودکار و بلادرنگ استوار بوده و به صورت روزانه، ماهانه، و سالانه انجام می‌گردد. ارزیابی منطقی آسیب‌پذیری امنیتی به عنوان ورودی برای ممیزی سالانه انطباق رویه ها تلقی می‌گردد.

۵-۵ بایگانی اطلاعات

۵-۵-۱ انواع اطلاعات قابل بایگانی

اطلاعات زیر در مورد عملیات مرکز میانی و دفاتر ثبت‌نام بایگانی می‌شوند:

- کلیه رخدادهای ثبت شده
- درخواست‌های تنظیم شده توسط RA شامل ابطال و به‌روزرسانی گواهی و تجدید کلید
  فایل‌های درخواست امضای گواهی(CSR)
- کلیه گواهی‌های صادر شده و CRL تولید شده توسط CA

- وضعیت گواهی‌ها (ابطال یا عدم ابطال)
- کلیه اطلاعات مربوط به چرخه حیات گواهی
- تاریخ و دلیل ابطال گواهی‌های باطل شده
- توافق‌نامه‌های بین مالک گواهی یا درخواست‌کننده و مرکز میانی
- توافق‌نامه یا قراردادهای منعقد شده بین مرکز میانی و دفاتر ثبت‌نام
- مستندات و مدارک مربوط به هویت‌شناسی درخواست‌کننده گواهی
- مستندات مربوط به دریافت و پذیرش گواهی
- کلیه گزارشات مربوط به بازرسی داخلی
- سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و دستورالعمل اجرایی گواهی الکترونیکی این مرکز
- هر توافق‌نامه پیمانی که مرکز میانی به آن مقید است
- پیکربندی تجهیزات سیستم
- نسخه پشتیبان پایگاه داده سیستم صدور و مدیریت گواهی الکترونیکی
- کلیه مکاتبات با دبیرخانه شورای سیاستگذاری گواهی الکترونیکی، مراکز دیگر و بازرسان ثبت وقایع

نرم افزار و سخت‌افزار مورد لزوم چه به صورت عملیاتی و چه پس از خارج شدن از رده، باید به منزلهٔ ابزار بازیابی اطلاعات بایگانی حفظ گردند تا طی دوره کلی تعیین شده برای بایگانی بتوان از آنها جهت تفسیر اطلاعات استفاده نمود. داده های مربوط به ممیزی امنیتی نیز بایگانی می‌گردند.

۵-۵-۲ دوره نگهداری اطلاعات بایگانی شده

اطلاعات ثبت‌شده در بایگانی مرکز میانی برای هر سطح اطمینان مطابق با جدول زیر نگه‌داری می‌شود.

جدول ۱۲ دوره نگهداری اطلاعات ثبت‌شده در بایگانی

سطح اطمینان	دوره نگهداری اطلاعات ثبت‌شده در بایگانی
سطح ۱	اطلاعات ثبت‌شده در بایگانی حداقل برای ۵ سال نگهداری می‌شود.
سطح ۲	اطلاعات ثبت‌شده در بایگانی حداقل برای ۱۶ سال نگهداری می‌شود.

۵-۵-۳ محافظت از بایگانی

مرکز میانی به گونه‌ای از بایگانی محافظت می‌نماید که فقط اشخاص قابل اطمینان مجاز بتوانند به آن دسترسی یابند. بایگانی، با استفاده از اعمال کنترل‌های فیزیکی و منطقی مناسب، در مقابل هرگونه مشاهده، تغییر، حذف ویا دستکاری‌های غیرمجاز محافظت می‌گردد. ابزارهای نگهداری داده‌های بایگانی و برنامه‌های کاربردی مورد نیاز برای پردازش این داده‌ها، به گونه‌ای نگهداری می‌شوند که حتماً در دوره زمانی‌ذکر شده در این دستورالعمل اجرایی قابل دسترسی خواهند بود.

هیچ فردی قادر به تغییر و یا حذف داده‌های موجود در بایگانی نمی‌باشد.

۵-۵-۴فرایندهای پشتیبان‌گیری از بایگانی

مراکز گواهی از بایگانی‌های الکترونیکی اطلاعات گواهی‌های صادر شده، نسخ پشتیبان الحاقی به صورت روزانه، و نسخ پشتیبان کامل به صورت هفتگی تهیه می‌نمایند. کپی سوابق کاغذی در مکان های امن خارج از سایت اصلی، نگهداری می‌شوند.

۵-۵-۵الزامات مهر زمانی اطلاعات بایگانی

گواهی‌ها، فهرست‌های گواهی‌های ابطال شده، و سایر اقلام بانک اطلاعاتی گواهی‌های ابطال شده، حاوی اطلاعات زمان و تاریخ می‌باشند. اطلاعات زمانی فوق، نیازی به رمزنگاری ندارند. کلیهٔ اطلاعات بایگانی شده در فرم‌های کاغذی نیز باید دارای تاریخ باشند.

۵-۵-۶سامانه جمع‌آوری بایگانی (درونی یا بیرونی)

بایگانی اطلاعات مربوط به گواهی‌ها و سایر موارد مربوط به صدور گواهی در نرم افزار CA به صورت اتوماتیک انجام می‌شود و سایر اطلاعات مربوط به درخواست کننده گواهی مانند مدارک شناسایی و فرم درخواست به صورت فیزیکی و سازمان‌دهی شده بایگانی می‌شوند. پایگاه داده مرکز میانی که اطلاعات الکترونیکی بایگانی در آن ذخیره می‌گردد، روی یک سرور به صورت امن و مطمئن نگه‌داری می‌شوند. مستندات کاغذی در محفظه‌های امن ضد حریق نگه‌داری می‌شوند.

۵-۵-۷فرایندهای به دست آوردن و بررسی اطلاعات بایگانی

در این مرکز فقط افراد مورد اطمینان مجاز می‌توانند به اطلاعات بایگانی شده دسترسی پیدا کنند. تمامیت اطلاعات بایگانی شده دو بار در سال بررسی می‌شود. تمامیت کپی‌های کاغذی خارج از سایت یک بار در سال بررسی می‌شود. برای اطمینان از تمامیت داده‌های الکترونیکی، این داده ها امضای دیجیتال می‌شوند.

۵-۶ تغییر کلید

مرکز میانی از کلید خصوصی برای امضای گواهی‌ها استفاده می‌کند. از آنجایی که طرف‌های اعتماد کننده از گواهی مرکز میانی برای اعتبارسنجی گواهی مالکان گواهی استفاده می‌کنند، بنابراین گواهی مالک گواهی دوره اعتبار کوتاه‌تری از دوره اعتبار گواهی مرکز میانی و کلید عمومی آن دارد.

مرکز میانی در صورت افشای کلید خصوصی و یا در معرض افشا قرار گرفتن کلید خصوصی و یا بروز سایر مشکلات که نیاز به تجدید کلید باشد، ابتدا درخواست ابطال گواهی خود را برای مرکز دولتی ریشه ارسال می‌کند پس از اجرای فرآیند ابطال گواهی، مرکز میانی درخواست تجدید کلید خود را به همراه فایل CSR، به مرکز دولتی ریشه ارائه می‌دهد که در

صورت تایید درخواست و صدور گواهی جدید و پس از پذیرش آن امکان دریافت آن از طریق مخزن مرکز میانی وجود خواهد داشت.

مالکان گواهی مطابق با بخش‌های ۲-۱-۴ و ۱-۷-۴ اقدام به صدور گواهی جدید خود می‌نمایند.

۵-۷ بازیابی به علت سوانح غیرمترقبه و در خطر افشا بودن

۵-۷-۱ فرایندهای مقابله با افشای کلید و حوادث

اگر مشخص شود که تلاشی برای هک کردن مرکز میانی صورت گرفته و یا اطلاعات به شکل پنهانی دیگری در معرض افشا شدن قرار دارند، به منظور تعیین نوع و میزان آسیب وارد شده، این تلاش‌ها بررسی می‌شوند. اگر احتمال رود که کلید مرکز میانی افشا شده است، روال هایی که در بخش ۳-۷-۵ آمده است انجام می‌شود. در غیر این صورت دامنه آسیب وارد شده ارزیابی می‌گردد تا معین شود که آیا مرکز میانی می‌بایست بازسازی شود، تنها بعضی از گواهی‌ها می‌بایست باطل شوند، و یا این‌که اعلام شود کلید مرکز میانی در خطر افشا قرار گرفته است.

در حالتی که کلید پاسخگوی OCSP مرکز میانی در خطر افشا قرار گرفته باشد، مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن گواهی آن را باطل می‌نماید و اطلاعات باطل‌شده به سرعت در مخزن منتشر می‌شوند. سپس، پاسخگوی OCSP کلید جدیدی را دریافت می‌نماید.

۵-۷-۲از بین رفتن تجهیزات کامپیوتری، نرم‌افزار و داده‌ها

مرکز میانی، کپی‌هایی از نسخه‌های پشتیبان سیستم، پایگاه‌داده‌ها و کلیدهای خصوصی نگه‌داری می‌نماید تا در صورت بروز خرابی در نرم افزار یا از بین رفتن داده‌ها، بتواند عملیات مرکز را از سر بگیرد. مرکز میانی پس از از بین رفتن سیستم‌ها یا داده‌ها به مرکز دولتی ریشه اطلاع رسانی نموده و مطابق با بخش ۴-۷-۵ عملیات بازیابی سیستم‌ها و اطلاعات را انجام می‌دهد.

استراتژی بازیابی خرابی مرکز، بر سه اصل زیر بنا نهاده شده است:

- بازیابی خدمات حیاتی مرکز در کوتاه‌ترین فاصله زمانی ممکن
- انجام عملیات بازیابی خرابی مرکز تا حد امکان به صورت خودکار
- بازیابی مرکز به پایدارترین وضعیت قبلی ممکن

بدین منظور اقدامات زیر هنگام پوشش حوادث در نظر گرفته می‌شوند:

- ارزیابی میزان خرابی

- انجام اقدامات ضروری تا برقراری سرویس‌های مرکز
- تامین تجهیزات و جایگزینی تجهیزات سخت افزاری آسیب دیده
- ترمیم و یا نصب مجدد سیستم‌عامل و نرم افزارهای آسیب دیده
- بازیابی کلیدهای خصوصی، اطلاعات و پایگاه‌های داده با استفاده از بروزترین نسخ پشتیبان تهیه شده
- انجام تست ارزیابی عملکرد سرویس‌های مرکز

۵-۷-۳ فرایندهای در خطر افشا قرار گرفتن کلید خصوصی موجودیت

در صورت در خطر افشا قرار گرفتن کلید خصوصی مرکز میانی و یا افشا شدن آن، اقدامات زیر توسط مرکز صورت می‌گیرد:

- صدور و انتشار گواهی‌ها و لیست ابطال را متوقف می‌کند؛
- درخواست ابطال گواهی خود را به مرکز دولتی ریشه ارائه می‌نماید؛
- یک زوج کلید جدید تولید کرده و درخواست صدور گواهی جدید را به مرکز دولتی ریشه ارائه می‌نماید؛
- با ابطال گواهی افشا شده و صدور گواهی جدید، کلیهٔ گواهی‌های معتبری که قبلاً توسط کلید افشا شده، امضا شده بود را باطل می‌نماید؛
- CRL جدید را از طریق مخزن منتشر می‌کند.

اگر کلید خصوصی مالک گواهی افشا شود و یا در خطر افشا قرار بگیرد، مالک گواهی باید فوراً به دفتر ثبت‌نام جهت ارائه درخواست ابطال گواهی مراجعه نماید. با ابطال گواهی، تمام طرف‌های اعتمادکننده از طریق فهرست گواهی‌های باطله که توسط مرکز منتشر می‌شود و پاسخگوی OCSP،از ابطال گواهی مذکور اطلاع می‌یابند.

اگر کلید خصوصی دفتر ثبت‌نام افشا شود و یا در خطر افشا قرار بگیرد، دفتر ثبت‌نام فوراً به مرکز میانی اطلاع‌رسانی می‌کند. مرکز میانی، گواهی متناظر با کلید خصوصی دفتر ثبت‌نام را باطل می‌نماید و اطلاعات گواهی باطل شده در مخزن منتشر می‌شود. سپس در صورت لزوم، زوج کلید و گواهی جدیدی برای دفتر ثبت‌نام تولید می‌شود.

۵-۷-۴ تداوم ارائه خدمت بعد از وقوع حوادث

مرکز میانی دارای یک طرح تداوم کار شامل روش امنی برای اجرای مجدد فعالیت‌ها در صورت وقوع بلایای طبیعی و یا هرگونه حادثهٔ دیگر می‌باشد. این طرح شامل موارد زیر است:

- تعریف نقش‌ها و مسئولیت کسانی که مسئول اجرای اجزای مختلف این طرح هستند؛
- شرایط برای فعال کردن طرح، که روندی را که قبل از فعال شدن طرح باید دنبال نمود، بیان کند؛

- شیوهٔ عمل در شرایط اضطراری که به عملیات کسب و کار و یا زندگی انسان خدشه وارد می‌کند؛
- روش جایگزین، که روند انتقال فعالیت‌های کسب و کار ضروری و یا خدمات پشتیبانی به مکان‌های جایگزین و بازگرداندن فرایندهای کسب و کار به حالت قبل در زمان مورد نیاز را بیان کند؛
- روش از سرگیری، که فعالیت‌های لازم برای بازگشت به عملیات کسب و کار عادی را بیان کند؛
- برنامهٔ تعمیر و نگهداری، که چگونگی و زمانی که این طرح آزمایش خواهد شود و همچنین فرایند حفظ طرح را مشخص نماید؛
- فعالیت‌های آگاهی و آموزش، طراحی شده برای درک فرایندهای تداوم کسب و کار و حصول اطمینان از این که فرایندها مؤثر ادامه می‌یابند.

۵-۸ توقف فعالیت مرکز صدور گواهی یا دفتر ثبت‌نام

در حالتی که عملیات مرکز میانی متوقف شود یا تغییرات عمده‌ای در عملیات صورت گیرد، این توقف و یا تغییر در عملیات به مرکز دولتی ریشه و کلیه موجودیت‌هایی که برای آن‌ها گواهی صادر شده است، اعلام می‌شود. ضمن اینکه قبل از خاتمه یافتن عملیات یا تغییرات عمده در عملیات این مسئله اعلام می‌شود.

به محض توقف مرکز میانی، همه کلیدهای خصوصی که وجود داشته‌اند یا ممکن است برای عملیات رمزنگاری مرکز میانی استفاده شوند، مطابق با بخش ۶-۲-۱۰ باطل (به دلیل ابطال متوقف شدن سرویس[19]) و نابود می‌شوند. همچنین لیست گواهی‌های باطل شده تولید و منتشر می‌شوند. مراحل پایان فعالیت مراکز میانی به شرح زیر است:

- اطلاع‌رسانی به مرکز دولتی ریشه و طرح مسئله در شورای سیاست‌گذاری گواهی الکترونیکی حداقل ۴ ماه قبل از پایان فعالیت مرکز صدور گواهی؛
- اطلاع‌رسانی به موجودیت‌هایی که تحت تأثیر قرار می‌گیرند، از جمله مالکان گواهی، طرف‌های اعتماد کننده، دفتر ثبت نام و مشتریان؛
- ابطال گواهی‌های صادر شده برای مرکز میانی توسط مرکز دولتی ریشه؛
- حفاظت و ارائه بایگانی و سوابق مرکز میانی برای مدت زمان تعیین شده توسط این سند و ارائه آن به یک مرجع معتبر که توسط شورای سیاست‌گذاری گواهی الکترونیکی تعیین می‌شود؛

[19] Cessation of Service

در حین توقف عملیات، مرکز میانی پندار کوشک ایمن، اطلاعات مرکز را توسط متولی مجاز که توسط شورای سیاست-گذاری گواهی الکترونیکی تعیین می‌گردد و طبق الزامات بایگانی تعیین‌شده در این سند نگهداری می‌نماید. این اطلاعات شامل موارد زیر می‌باشد:

- گواهی‌های مرکز میانی؛
- گواهی‌های صادره؛
- لیست گواهی‌های باطل شده؛
- اطلاعات بازرسی امنیتی که در بخش فرآیندهای ۴-۵ آمده است؛
- دیگر اطلاعات بایگانی شده همان‌طور که در بخش ۵-۵ آمده است.

مرکز میانی برای نگه داری هر داده‌ای (مثل گذرواژه) اطمینان حاصل می‌کند که آن داده قابل استفاده است (به عنوان مثال داده‌های رمز شده در زمان نیاز قابل رمزگشایی می‌باشند.) اطلاعات به صورت امن به مکان‌هایی که در آنجا نگه داری خواهند شد، مطابق با بخش ۸-۱-۵ منتقل می‌شوند.

۶. کنترل‌های امنیتی فنی

۶-۱ تولید و نصب زوج کلید

۶-۱-۱ تولید زوج کلید

۶-۱-۱-۱ تولید زوج کلید مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن

انجام عملیات تولید کلید برای مرکز میانی در مراسم KGC (مراسم تولید کلید) و از طریق یک HSM مورد تایید و ارزیابی شده توسط مرکز دولتی ریشه که در آن ملزومات امنیتی مطابق استاندارد FIPS 140-2 در سطح سوم رعایت شده است، صورت می‌پذیرد. این مرکز از زوج کلید الگوریتم RSA جهت صدور گواهی، پشتیبانی می‌نماید. الزامات امنیتی درنظر گرفته شده توسط مرکز میانی برای تولید زوج کلید این مرکز، به شرح زیر است:

- توسط متصدیانی با نقش مورد اطمینان و مجاز برای تولید کلید صورت می‌پذیرد.
- در داخل ماژول سخت‌افزاری رمزنگاری انجام می‌پذیرد که حداقل الزامات بخش ۱-۲-۶ را در بر می‌گیرد.
- با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت می‌پذیرد.

این مرکز، فرایند تولید کلید را مستند می‌کند و دلایل و شواهد لازم را برای اثبات اینکه مراحل مستند شده انجام گرفته‌اند، ارائه می‌کند.

۶-۱-۱-۲ تولید زوج کلید دفاتر ثبت‌نام

تولید زوج کلید دفتر ثبت‌نام در داخل ماژول رمزنگاری سخت‌افزاری انجام می‌پذیرد که حداقل الزامات بخش ۱-۲-۶ را در بردارد. این کار با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت می‌پذیرد.

۶-۱-۱-۳ تولید زوج کلید مالک گواهی

چگونگی انجام عملیات تولید کلید برای مالکان گواهی به شرح زیر است:

برای گواهی‌های سطح ۱: تولید زوج کلید مالکان گواهی با استفاده از الگوریتم های پذیرفته شده در زیر ساخت کلید عمومی کشور می پذیرد.

برای گواهی‌های سطح ۲:

- تولید کلید داخل ماژول رمزنگاری سخت افزاری صورت می‌پذیرد که حداقل الزامات بخش ۱-۲-۶ را در برگیرد. (تولید کلید به صورت نرم افزاری صرفا توسط مالک گواهی انجام می‌شود و کلید عمومی متناظر به صورت pkcs#10 به دفتر ثبت نام تحویل داده می‌شود.)
- تولید زوج کلید برای مالکان گواهی با استفاده از الگوریتم های پذیرفته شده در زیرساخت کلید عمومی کشور صورت می‌پذیرد. لازم به توضیح است که تولید کلید برای مالک گواهی در دفتر ثبت‌نام، به نمایندگی از متقاضی صورت می‌گیرد و در این حالت این موضوع در توافق‌نامه مرکز صدور گواهی با متقاضی ذکر می‌شود.

۶-۱-۲ تحویل کلید خصوصی به موجودیت نهایی

- تولید زوج کلید به صورت نرم‌افزاری صرفاً توسط مالک گواهی صورت می گیرد و تحویل کلید عمومی متناظر به مرکز میانی یا دفتر ثبت نام همراه با اثبات مالکیت کلید خصوصی انجام می شود.
- برای گواهی‌های سطح دو، چنانچه عملیات تولید کلید توسط دفتر ثبت‌نام به نمایندگی از متقاضی صورت گیرد، این عملیات به صورت داخلی توسط یک ماژول رمزنگاری سخت افزاری مورد تایید مرکز دولتی ریشه، که دارای حداقل الزامات بخش ۱-۲-۶ است، مطابق با بخش ۱-۱-۶ انجام می‌شود و کلید خصوصی از طریق سخت افزار در اختیار مالک قرار داده می‌شود. در این حالت این موضوع در توافق نامه‌ی مرکز صدور گواهی با متقاضی ذکر می گردد.

تولید کلید به صورت نرم‌افزاری صرفا توسط مالک گواهی انجام می‌شود و کلید عمومی متناظر به صورت pkcs#10 به دفتر ثبت‌نام تحویل داده می‌شود.

۶-۱-۳ تحویل کلید عمومی به مرکز صدور گواهی الکترونیکی

مالکان گواهی کلید عمومی خود را در یک فایل امضای درخواست گواهی (CSR)، طبق استاندارد PKCS#10 به مرکز تحویل می‌دهند. چنانچه عملیات تولید کلید توسط مالک گواهی و یا دفتر ثبت‌نام صورت گیرد، تحویل کلید عمومی به مرکز میانی به گونه‌ای می باشد، که تناظر بین کلید عمومی ارائه شده و کلید خصوصی مالک گواهی و همچنین حفظ تمامیت آن با استفاده از امضای دیجیتال دفتر ثبت نام توسط مرکز صدور گواهی قابل بررسی باشد.

۶-۱-۴ تحویل کلید عمومی مرکزصدور گواهی به طرف های اعتمادکننده

گواهی‌های مرکز میانی از طریق انتشاردر مخزن بصورت امن در دسترس طرف‌های اعتماد کننده قرار می‌گیرند.

۶-۱-۵ طول کلید

کلید مرکز میانی مطابق با ساختار G3 در سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور دارای طول ۴۰۹۶ بیت RSA می‌باشد و برای دفاتر ثبت‌نام، سرویس‌دهندهٔ OCSP و سرویس‌دهندهٔ مهر زمانی ۲۰۴۸ بیت RSA می‌باشد. همچنین طول کلید در نظر گرفته شده برای موجودیت‌های نهایی برای سطح یک ۱۰۲۴ و برای سطح دو ۲۰۴۸ می‌باشد.

۶-۱-۶ تولید پارامترهای کلید عمومی و کنترل کیفیت

تولید پارامترهای کلید عمومی برای الگوریتم های امضا و همچنین بررسی کیفیت پارامترها مطابق با استاندارد FIPS 186 انجام می شود.

۶-۱-۷ موارد کاربرد کلید (طبق فیلد کاربرد کلید در X.509 v3)

مالکان گواهی و طرف‌های اعتماد کننده ملزم به رعایت کاربردهای اشاره شده در فیلدهای الحاقی KeyUsage و ExtendedKeyUsage در گواهی به هنگام استفاده می‌باشند. کاربردهای در نظر گرفته شده برای گواهی الکترونیکی در بخش ۱-۴-۱ توصیف شده است. ضمن این که فیلد کاربرد کلید گواهی باید مطابق با سند جامع پروفایل‌های زیرساخت کلید عمومی کشور به کار رود.

۶-۲ محافظت از کلید خصوصی و کنترل‌های مهندسی ماژول رمزنگاری

۶-۲-۱ کنترل‌ها و استانداردهای ماژول رمزنگاری

کلید خصوصی مرکز میانی در یک ماژول سخت‌افزاری امنیتی (HSM) ذخیره می‌گردد که در آن الزامات استاندارد FIPS 140-2 در سطح سوم رعایت شده است.

همچنین انجام عملیات تولید کلید برای مرکز میانی و امضای کلیهٔ گواهی‌های صادرشده توسط این مرکز از طریق این HSM و به صورت داخلی[20] صورت می‌گیرد.

الزامات مربوط به کنترل‌ها و استانداردهای ماژول‌های امنیتی در زیرساخت کلید عمومی کشور مطابق با بخش ۶-۲-۱ سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور می‌باشد.

۶-۲-۲ کنترل ترکیبی چند نفره (n نفر از m نفر) کلید خصوصی

پشتیبانی نمی‌گردد.

۶-۲-۳دستیابی قانونی به کلید خصوصی

قابل اعمال نیست.

[20] On-board

۶-۲-۴پشتیبان‌گیری از کلید خصوصی

مرکز میانی زوج کلید خود را بر روی ماژول امنیتی سخت افزاری (HSM) تولید و نگه‌داری می‌کند. برای جلوگیری از خسارت‌های ناشی از خرابی HSM و عدم دسترسی به کلید خصوصی، از زوج کلید مرکز میانی پشتیبان تهیه می‌گردد تا در مواقع خرابی بتوان کلیدها را بازگردانی نمود.

زوج کلیدها بر روی پارتیشن HSM ذخیره می‌شوند بنابراین می‌بایست از زوج کلیدهای موجود در پارتیشن‌های HSM پشتیبان تهیه نمود. پشتیبان‌گیری از زوج کلیدهای موجود در پارتیشن‌های HSM در روز مراسم تولید کلید انجام می‌شود. (الزامات تهیه نسخه پشتیبان از کلید خصوصی، مطابق با بخش ۶-۲-۴ سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور می‌باشد.) جهت تهیه نسخه پشتیبان پس از انجام مراسم تولید کلید از محتوای هر یک از این پارتیشن‌ها به صورت مجزا بر روی یک ماژول رمزنگاری سخت افزاری (کارت هوشمند) پشتیبان مجزا با اتصال آن به HSM از طریق دستگاه کارتخوان و اجرای دستورات موردنیاز، عملیات پشتیبان‌گیری انجام می‌گیرد سپس این ماژول رمزنگاری سخت افزاری به سایت پشتیبان انتقال یافته و به شکل امن و با اعمال کنترل دسترسی نگه داری می‌شود، طوری که تنها نقش‌های مورد اطمینان مجاز امکان دسترسی به آن را دارند. لازم به ذکر است که اطلاعات فعالسازی ماژول رمزنگاری بصورت امن و در محلی جداگانه از ماژول رمزنگاری نگهداری خواهد شد.

۶-۲-۵بایگانی کلید خصوصی

قابل اعمال نیست.

۶-۲-۶انتقال کلید خصوصی به / از ماژول رمز نگاری

مرکز میانی، زوج کلیدهای مربوط به خود را بر روی ماژول امنیتی سخت افزاری (HSM) تولید و نگه‌داری می‌نماید. در هنگام کپی زوج کلیدهای مرکز میانی از روی ماژول امنیتی سخت‌افزاری، این زوج کلیدها به صورت رمز شده، به ماژول رمزنگاری سخت افزاری (کارت هوشمند) پشتیبان منتقل می‌شوند. سپس این ماژول رمزنگاری سخت افزاری به سایت پشتیبان انتقال یافته و به شکل امن و با اعمال کنترل دسترسی نگه داری می‌شود، طوری که تنها نقش‌های مورد اطمینان مجاز امکان دسترسی به آن را دارند.

۶-۲-۷ذخیره‌سازی کلیدهای خصوصی بر روی ماژول رمزنگاری

کلیدهای خصوصی مرکز میانی در یک ماژول امنیتی که الزامات قید شده در بخش ۶-۲-۱ در آن رعایت شده است، ذخیره می‌شوند. کلیدهای خصوصی مالکان گواهی در توکن‌هایی که توسط مرکز دولتی ریشه تأیید شده‌اند، ذخیره می‌شوند.

۶-۲-۸روش فعال‌سازی کلید خصوصی

جدول ۱۳فعال سازی کلید خصوصی

سطح اطمینان	فعال سازی کلید خصوصی
سطح ۱	از طریق گذرواژه صورت می‌گیرد.

سطح اطمینان	فعال سازی کلید خصوصی
سطح ۲	استفاده از رمز یا گذرواژه، داده‌های مورد نیاز برای کنترل چند نفره، اطلاعات بایومتریکی و شیوه‌های دیگر احراز هویت برای فعال کردن کلید خصوصی در دستگاه رمزنگاری قابل استفاده می‌باشند. (الزامات تولید اطلاعات فعال‌ساز در بخش ۱-۴-۶ آمده است). اطلاعات فعال‌ساز توسط مالک گواهی تولید و یا به روشی امن در اختیار مالکان گواهی قرار می‌گیرد تا هنگام ورود اطلاعات فعال‌ساز از افشاء آن‌ها جلوگیری شود. (چنانچه کلید خصوصی از طریق دفتر ثبت‌نام و یا مرکز صدور گواهی در اختیار مالک گواهی قرار داده شود، به وی اعلام می‌گردد که گذرواژه سخت‌افزار رمزنگاری خود را در اسرع وقت تغییر دهد).

۶-۲-۹ روش غیرفعال نمودن کلید خصوصی

جدول ۱۴ غیرفعال نمودن کلید خصوصی

سطح اطمینان	غیرفعال نمودن کلید خصوصی
سطح ۱ و ۲	ماژول‌های رمزنگاری در حالت فعال بدون استفاده باقی نمی‌مانند. این ماژول‌ها پس از استفاده به روش دستی خروج از سیستم، یا پس از گذشت زمان معینی ارتباط به طور خودکار قطع یا غیرفعال می‌شود. وقتی کلیدهای خصوصی غیرفعال می‌شوند، قبل از آزادسازی فضای حافظه از حافظه پاک می‌شوند و فقط به شکل رمز شده نگهداری می‌شوند.

۶-۲-۱۰ روش انهدام کلید خصوصی

مرکز میانی در هنگامی که دیگر نیازی به کلیدهای خصوصی خود وجود نداشته باشد تضمین می نمایند که کلیدها را به گونه‌ای از بین ببرد که هیچ اثری از کلید که بتواند منجر به بازسازی آن شود باقی نماند. برای این منظور مرکز میانی برای از بین بردن کلیدهای خود از روی ماژول های رمزنگاری سخت‌افزاری از طریق فرآیند صفر کردن[۲۱] در حافظه به همراه بازنویسی حافظه عمل می‌نماید. این رویه را برای کلیدهای موجودیت‌های نهایی که بر روی توکن‌های سخت‌افزاری ذخیره شده است نیز قابل انجام می‌باشد. در صورت نیاز به از بین بردن کلیدهایی که بصورت نرم‌افزاری ذخیره شده باشند، صرفاً از طریق بازنویسی مقادیر کلید با اطلاعات تصادفی صورت می‌پذیرد. پس از اجرای عملیات فوق، مراحل امحای کلید ثبت می‌گردند.

۶-۲-۱۱ رده‌بندی ماژول رمزنگاری

به بخش ۱-۲-۶ مراجعه شود.

۶-۳ سایر ابعاد مدیریت زوج کلید

[21] Zeroize

۶-۳-۱ بایگانی کلید عمومی

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، کلیدهای عمومی متناظر با گواهی‌های خود و همچنین کلیدهای عمومی متناظر با گواهی‌های صادر شده را مطابق با بخش ۲-۵-۵ بایگانی می‌کند.

۶-۳-۲ دوره‌های عملیاتی گواهی و دوره‌های استفاده از زوج کلید

طول کلید RSA برای کلید عمومی و خصوصی متناسب با سطح گواهی می‌باشد. حداقل طول ۱۰۲۴ بیت و حداکثر آن ۲۰۴۸ بیت می‌باشد. الزامات مربوط به دوره اعتبار گواهی‌های صادر شده توسط این مرکز در جدول زیر آورده شده است.

جدول ۱۵ دوره عملیاتی گواهی‌ها و دوره‌های استفاده از زوج کلید موجودیت‌نهایی

سطح اطمینان	طول کلید	حداکثر دوره اعتبار گواهی
سطح یک	۱۰۲۴	۲ سال
سطح دو	۲۰۴۸	۳ سال

۶-۴ اطلاعات فعال‌ساز

۶-۴-۱ تولید و بکارگیری اطلاعات فعال‌ساز

به منظور تولید و استفاده از داده‌های فعال‌سازی کلید خصوصی، روش‌هایی بکار گرفته می‌شود تا در حد لزوم داده‌های فعال‌سازی را از مفقود شدن، سرقت، تغییر، افشای غیرمجاز، و استفاده غیرمجاز محافظت نمایند. به عنوان مثال گذرواژه‌هایی تولید می‌گردند که به آسانی قابل حدس و پیش‌بینی، افشاء و یا سو استفاده نباشند و به صورت تصادفی تولید شوند. الزامات انتخاب گذرواژه به شرح زیر می‌باشد:

- حداقل از ۸ کاراکتر تشکیل شده است؛
- از ترکیب حروف، اعداد، و کاراکترهای قابل چاپ (غیر از حروف و اعداد) استفاده شده است؛
- در آن‌ها از تعداد زیادی کاراکترهای یکسان استفاده نشده است؛
- گذرواژه‌های انتخابی برای مالکان گواهی با اطلاعات شناسایی شخصی آن‌ها مرتبط نیست؛
- گذرواژه‌های انتخابی بامعنا و قابل حدس زدن نیستند.

چنانچه از اعداد تصادفی به عنوان اطلاعات فعال‌ساز بکار گرفته شود، کلیهٔ الزامات مربوط به اعداد تصادفی منطبق با استانداردهای معرفی شده توسط مرکز دولتی ریشه، در آنها رعایت می‌گردد.

۶-۴-۲ محافظت از اطلاعات فعال‌ساز

اطلاعات فعال‌ساز دستگاه رمزنگاری به حافظه سپرده می‌شوند و به صورت نوشته نگه‌داری نمی‌شوند اگر نوشته شوند، نوشته در سطحی از امنیت، معادل با امنیت داده‌های دستگاه رمزنگاری، نگه داری می‌شوند. بطور کلی اطلاعات فعالساز

در یک مدیا به صورت آفلاین، جدا از کلید خصوصی رمز شده و در یک محل امن نگه داری می‌شود، به گونه ای که تنها افراد مجاز حق دسترسی به آنجا را دارند. این رویه برای موارد مشابه نیز به کار می‌رود. اطلاعات فعال‌ساز کلیدهای خصوصی منحصرا نزد مالک گواهی محفوظ می‌ماند.

۶-۴-۳ سایر ابعاد اطلاعات فعال‌ساز

تعریف نشده است.

۶-۵ کنترل‌های امنیتی رایانه

۶-۵-۱ الزامات فنی ویژه امنیت رایانه

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، موارد زیر را در سیستم عامل‌های خود فعال می‌نماید:

- امکان ورود به سیستم صرفاً پس از احراز هویت متمرکز؛
- ایجاد دسترسی کنترل شده به اطلاعات و برنامه‌ها بر اساس هویت تعریف شده در سیستم؛
- راه‌اندازی سیستم ثبت وقایع و بازبینی آنها.
- همچنین سیستم‌های این مرکز مجهز به سیستم‌های شناسایی و پاکسازی ویروس با مشخصات زیر می‌باشند:
- امکان بروزرسانی با آخرین فهرست ویروس‌های شناسایی شده؛
- امکان جستجو در تمام فایل‌های سیستمی و غیرسیستمی به صورت خودکار؛
- ثبت وقایع مرتبط به بررسی سیستم و وجود ویروس‌های احتمالی و نتیجهٔ عملکرد برنامه روی آنها.

۶-۵-۲ رتبه‌بندی امنیت رایانه

تمامی تجهیزات نرم‌افزاری و سخت‌افزاری مورد استفاده در مرکز میانی در آزمایشگاه‌های مورد تایید مرکز دولتی ریشه ارزیابی و تایید شدند.

۶-۶ کنترل‌های فنی چرخه حیات

۶-۶-۱ کنترل‌های توسعه سامانه

کنترل‌های توسعهٔ سامانه که توسط مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن در نظر گرفته شده است به صورت زیر می‌باشند:

- مرکز صدور گواهی از یک سامانه صدور و مدیریت گواهی که مورد تایید مرکز دولتی ریشه است و تحت یک روش ساخت‌یافته طراحی و توسعه یافته است، استفاده می‌کند. این سامانه و سایر نرم افزارهای مربوط و فرآیند طراحی و توسعه سامانه مورد استفاده در مرکز میانی، توسط آزمایشگاه زیرساخت کلید عمومی کشور ارزیابی و تایید شده‌اند.

- سخت‌افزار یا نرم‌افزار خریداری شده در یک بستهٔ مهر و موم شده و یا به روش مطمئن دیگری حمل و تحویل داده می‌شود و توسط پرسنل آموزش دیده نصب می‌شود. لازم به ذکر است این مرکز میانی تنها پس از تایید مرکز دولتی ریشه نسبت به توسعه و عملیاتی نمودن سامانه‌های سخت افزاری و نرم افزاری اقدام خواهد نمود.

۶-۶-۲ کنترل‌های مدیریت امنیت

سخت‌افزارها و نرم‌افزارهای مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن به‌طور اختصاصی برای انجام وظایف مربوط به این مرکز مورد استفاده قرار می‌گیرند. این مرکز حاوی هیچ برنامه کاربردی، وسایل سخت‌افزاری، اتصالات شبکه، و مؤلفه‌های نرم‌افزاری که به عملیات این مرکز مربوط نیستند، نمی‌باشد.

در مرکز میانی نصب و پیکربندی کلیهٔ نرم‌افزارها، و سرویس‌دهنده‌ها به صورت کاملاً کنترل شده و تنها توسط نقش‌های مجاز انجام می‌شود. این نقش‌ها پس از احراز هویت وظایف خود را انجام می‌دهند. نصب و پیکربندی کلیهٔ نرم‌افزارها پس از بررسی تمامیت بسته‌های نرم‌افزاری جهت اطمینان از دست‌نخوردگی آن‌ها صورت می‌گیرد. ضمن این که تمام رویدادهای مرتبط با تغییرات صورت گرفته در پیکربندی سرویس‌دهنده‌های مرکز، ثبت و بایگانی می‌گردد.

این مرکز اطمینان حاصل می‌کند که نرم‌افزار دفتر ثبت‌نام و مرکز صدور گواهی که بر روی سیستم نصب می‌شوند:

- نرم‌افزارهایی هستند که توسط توسعه‌دهنده نرم‌افزار ارائه شده است؛
- قبل از نصب تغییر داده نشده است؛
- نسخه موردنظر برای استفاده است.

مرکز میانی مکانیسم‌ها و سیاست‌هایی برای کنترل و نظارت پیکربندی سیستم مرکز دارد به طوری که می‌توان از صحت پیکربندی سیستم اطمینان حاصل نمود. همچنین، برای پیشگیری از آلوده شدن و انتشار نرم‌افزارهای مخرب در تجهیزات مرکز، از نرم‌افزارها و سخت‌افزارهای مناسب مثل ضدویروس، فایروال‌ها و سیستم‌های تشخیص و جلوگیری از نفوذ برای جلوگیری و مقابله با نرم‌افزارهای مخرب و نفوذگران استفاده می‌کند.

بررسی دوره‌ای تمامیت پایگاه داده این مرکز برای سطح یک و دو هرماه یکبار انجام می‌گردد.

۶-۶-۳ کنترل‌های امنیتی چرخه حیات

پیاده سازی نشده است.

۶-۷ کنترل‌های امنیتی شبکه

در مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، جهت اطمینان از امنیت سرویس‌دهنده‌ها و جلوگیری از تهدیدات شبکه، از فایروال‌ها و UTM به عنوان لایه‌های امنیتی استفاده شده است.

- برخی از سرویس‌های امنیتی پشتیبانی شده توسط UTM مورد استفاده در این مرکز عبارتند از:
- بازرسی حالتمند (Stateful Inspection)
- ترجمه آدرس شبکه[۲۲] (NAT)
- سیستم تشخیص و جلوگیری از حملات[۲۳] (IDPS)

[22] Network Address Translation
[23] Intrusion Detection and Prevention System

- مدیریت پهنای باند و یا Traffic Shaping
- آنتی‌ویروس تحت شبکه بر اساس پروتکل ICAP
- آنتی‌اسپم و آنتی ویروس ترافیک پست الکترونیکی (SMTP، IMAP و POP3)
- قابلیت High Availability
- جلوگیری از حملات DOS
- حفظ تمامیت در انتقال داده

کلیهٔ پیکربندی‌های امنیتی لازم در فایروال‌ها و سایر تجهیزات شبکه تنظیم شده است، به طوری که تنها سرویس‌های مشخصی برای سیستم‌ها و کاربران مشخصی قابل دسترسی می‌باشند.

۸-۶ مهر زمانی

این مرکز میانی قابلیت مهر زمانی را برای تراکنش‌های مالکان گواهی فراهم می‌کند.

۷. پروفایل گواهی، فهرست گواهی های باطله و ocsp

۷-۱ پروفایل گواهی

پروفایل گواهی‌های صادره توسط این مرکز با RFC5280 و سند جامع پروفایل‌های زیرساخت کلید عمومی کشور سازگار می‌باشد. هر گواهی X.509 حداقل شامل فیلدهای اصلی و مقداردهی فیلدها باید با توجه به قیودی که برای مقادیر آنها تعیین شده است، مطابق جدول زیر انجام شود.

جدول ۱۶ الزامات مربوط به فیلدهای گواهی

فیلد	الزامات
Serial Number	شمارهٔ سریال گواهی که برای هر گواهی صادره توسط مرکز صدور گواهی مقداری منحصربفرد دارد.
Signature Algorithm	شناسهٔ الگوریتم بکار رفته جهت امضای گواهی (بخش ۳-۱-۷)
Issuer DN	در بخش ۴-۱-۷ توضیح داده شده است.
Validity	دورهٔ اعتبار گواهی.
Subject DN	در بخش ۴-۱-۷ توضیح داده شده است.

Subject Public Key	کلید عمومی مالک گواهی که مطابق با RFC5280 کدگذاری می‌گردد.
Signature	امضای گواهی که مطابق با RFC5280 تولید و کدگذاری می‌گردد.

۷-۱-۱ شماره نسخه

صدور گواهی‌ها بر اساس نسخهٔ سوم استاندارد X.509 انجام می‌شود.

۷-۱-۲ الحاقیه‌های گواهی

الزامات مربوط به الحاقیه‌های گواهی شامل مقداردهی و پردازش آنها در سند جامع پروفایل‌های زیرساخت کلید عمومی کشور بیان شده است.

۷-۱-۳ شناسه های الگوریتم

شناسه الگوریتم ها مطابق با بخش ۷-۱-۳ سند "سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور" می باشد.

۷-۱-۴ قالب نام‌ها

حوه مقداردهی نام متمایز مربوط به مالک و صادرکننده گواهی مطابق با بخش ۱-۳ می باشد

۷-۱-۵ محدویت های نامگذاری

فیلد الحاقی Name Constraints طبق سند جامع پروفایل‌های زیرساخت کلید عمومی کشور در گواهی قید می‌شود.

۷-۱-۶ شناسهٔ سیاست‌های گواهی

مرکز میانی شناسه‌های سیاست گواهی را مطابق با شناسه مختص هر سطح گواهی که در بخش ۲-۱ مقدار آن مشخص شده است، در گواهی قرار می‌دهد.

۷-۱-۷ کاربرد الحاقیه Policy Constraints

مطابق با سند جامع پروفایل‌های زیرساخت کلید عمومی کشور، استفاده از فیلد الحاقی Policy constraints در گواهی ممنوع می‌باشد.

۷-۱-۸ ساختار و معنای الحاقیه Policy Qualifier

گواهی‌های نسخه سوم X.509 حاوی یک توصیف اعتماد کننده سیاست در فیلد الحاقی Certificate Policies می‌باشند. در این توصیف کننده نشانی دسترسی به این سند آورده می‌شود.

۷-۱-۹ پردازش معنایی برای الحاقیه حیاتی Certificate Policies[۲۴]

بر اساس سند جامع پروفایل‌های زیرساخت کلید عمومی کشور برای فیلد الحاقی Certificate Policy وضعیت غیرحیاتی در نظر گرفته شده است.

۷-۲ پروفایل فهرست گواهیهای باطله (CRL)

پروفایل فهرست گواهی‌های باطله مطابق با استاندارد RFC5280 می‌باشد. فهرست گواهی‌های باطله حداقل شامل فیلدهای اصلی (مطابق جدول زیر) می‌باشد و مقداردهی آنها بر اساس قیود مشخص شده صورت می‌پذیرد.

جدول ۱۷ الزامات مربوط به خصوصیات فهرست گواهی‌های باطله

فیلد	الزامات
Version	در بخش ۷-۲-۱ توضیح داده شده است.
Signature Algorithm	شناسهٔ الگوریتم بکار رفته جهت امضای CRL (بخش ۷-۱-۳)
Issuer	نام متمایز موجودیتی که CRL را امضا و تولید می‌نماید.
Effective Date	تاریخ صدور CRL.
Next Update	تاریخی که CRL بعدی صادر خواهد شد. الزامات مربوط به تناوب صدور فهرست گواهی‌های باطله در بخش ۷-۹-۴ بیان شده است.
Revoked Certificates	فهرست گواهی‌های باطله شامل شماره سریال گواهی‌های باطله و تاریخ ابطال.

۷-۲-۱ شماره نسخه

مرکز صدور گواهی از نسخهٔ دوم X.509 فهرست گواهی‌های باطله منطبق با RFC5280 پشتیبانی می‌کند.

۷-۲-۲ الحاقیه CRL و CRL Entry

الزامات مربوط به الحاقیه‌های CRL و CRL Entry به همراه مقداردهی و پردازش آنها در سند جامع پروفایل‌های زیرساخت کلید عمومی کشور بیان شده است.

۷-۳ پروفایل OCSP

۷-۳-۱ شماره نسخه

مرکز صدور گواهی از نسخهٔ اول OCSP تعریف شده در RFC2560 و بروز رسانی های بعدی آن پشتیبانی می‌نماید.

[24] Critical Certificate Policy Extension

۷-۳-۲ الحاقیه‌های ocsp

الحاقیه‌های OCSP آنگونه که در سند جامع پروفایل‌های زیرساخت کلید عمومی کشور ذکر شده است، به کار می‌روند. سرویس‌دهندهٔ پاسخگوی OCSP جهت مقابله با حملات تکرار و اطمینان سرویس‌گیرندهٔ OCSP از تازگی پاسخ OCSP، از الحاقیهٔ Nonce استفاده می‌کند. این الحاقیه با مقدار الحاقیهٔ Nonce موجود در درخواست OCSP که از سوی سرویس‌گیرندهٔ OCSP ارسال می‌شود، مقداردهی می‌گردد.

۸. بازرسی تطابق و سایر ارزیابی‌ها

بازرسی تطابق به معنای بررسی تطابق عملیات مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن با الزامات و فرایندهای بیان شده در سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و دستورالعمل اجرایی این مرکز می‌باشد. بازرسی تطابق با هدف حصول اطمینان از عملکرد مرکز میانی انجام می‌شود. این نوع بازرسی به سه صورت می‌باشد:

- بازرسی شورا: بر اساس آیین‌نامهٔ شورای سیاست‌گذاری گواهی الکترونیکی کشور، یکی از مسئولیت‌های شورا نظارت بر عملکرد مراکز ریشه و میانی می‌باشد. بر این اساس، به منظور اعمال نظارت بر عملکرد مرکز میانی، لازم است بازرسی دوره‌ای از این مرکز زیر نظر شورا و توسط بازرس یا بازرسین مورد تأیید شورا صورت گیرد.
- بازرسی مرکز دولتی ریشه: یکی از مسئولیت‌های اصلی مرکز دولتی ریشه، حصول اطمینان از عملکرد صحیح مرکز میانی می‌باشد. بر این اساس و به منظور حصول اطمینان از عملکرد صحیح مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، مرکز دولتی ریشه از این مرکز بازرسی به عمل می‌آورد.
- بازرسی داخلی: به منظور حصول اطمینان از عملکرد صحیح، مرکز میانی هر ۶ ماه یک بار بازرسی داخلی انجام می‌دهد. نتایج بازرسی داخلی انجام شده توسط مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن به مدیر بخش مورد بازرسی، مدیر مرکز میانی و مرکز دولتی ریشه ارائه می‌شود.

۸-۱ تناوب و شرایط ارزیابی

بازرسی تطابق حداقل یک بار و ترجیحاً دو بار در سال انجام می‌گیرد. بازرسی داخلی از مرکز حداقل هر ۶ ماه یکبار انجام می‌شود. توضیح این که، زمان و تناوب بازرسی به میزان کارکرد مرکز میانی وابسته است.

۸-۲ هویت و صلاحیت ارزیاب

بازرسی مرکز دولتی ریشه از مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن توسط یک یا چند تن از کارشناسان واجد شرایط مرکز دولتی ریشه در حوزه‌های تعیین شده در بخش ۸-۴ انجام می‌گیرد و بازرسی شورای سیاست‌گذاری گواهی الکترونیکی توسط یک یا چند شخص حقیقی یا حقوقی مورد تایید شورا انجام می‌پذیرد. بازرسی داخلی مرکز توسط پرسنل مجاز مرکز میانی انجام می‌شود.

بازرس می‌بایست با زیرساخت کلید عمومی و استانداردهای آن، سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن و مصوبات شورا کاملا آشنا باشد. بازرسانی که بازرسی داخلی از مرکز میانی را اجرا می‌کنند نیز واجد این شرایط هستند.

۸-۳ ارتباط ارزیاب با مرکز مورد ارزیابی

بازرسی از مرکز میانی صرفاً توسط اشخاص واجد شرایط مندرج در بخش ۸-۲ انجام می‌گیرد.

۸-۴ موضوعات مورد ارزیابی

فرایند بازرسی تطابق مرکز میانی حداقل شامل موارد زیر می‌باشد:

- دستورالعمل اجرایی گواهی الکترونیکی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، دستورالعمل‌های فنی، فرایندی و پرسنلی مرکز و طرح فنی تجهیزات و ساختمان مرکز؛
- بررسی تطابق این مرکز، شامل ساختمان، تجهیزات و همچنین کلیهٔ سخت‌افزارها، نرم‌افزارها، نیروی انسانی و فرایندهای بکار گرفته شده در مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، با دستورالعمل‌ها و مستندات قید شده در بند اول؛
- بررسی تطابق تجهیزات، نرم‌افزارها و عملکرد دفتر ثبت‌نام با دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن.
- در بازرسی داخلی حداقل، عملکرد دفتر ثبت‌نام با دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن ارزیابی می‌شود.

۸-۵ اقدامات اتخاذ شده در برخورد با نقایص

در صورتی که فرایند بازرسی هرگونه مغایرت با سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور یا دستورالعمل اجرایی این مرکز را مشخص کند و یا هرگونه نقص و یا مشکل امنیتی در مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن هنگام انجام عملیات فرایند بازرسی آشکار شود، اقدامات زیر صورت می‌گیرد:

- نقص و یا ناهمخوانی ثبت می‌شود؛
- به طرف‌های تعیین شده در بخش ۶-۸ اعلام ناهمخوانی و یا نقص ثبت شده، اعلام می‌شود؛
- مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن در مدت زمان تعیین شده توسط مرجع بازرسی‌کننده، نسبت به رفع نواقص و ناهمخوانی‌ها اقدام می‌نماید؛
- در صورت عدم اصلاح نقص یا ناهمخوانی توسط این مرکز در زمان پیش‌بینی شده، گزارش مغایرت به اطلاع شورای سیاستگذاری گواهی الکترونیکی کشور می‌رسد؛
- شورای سیاستگذاری گواهی الکترونیکی کشور می‌تواند راهکار مناسبی مانند تمدید مدت زمان اصلاح نواقص، جلوگیری از فعالیت مرکز میانی و یا در صورت لزوم ابطال گواهی‌های مرکز را انتخاب نماید.

در مورد بازرسی داخلی در صورت آشکار شدن هرگونه نقص یا مغایرت در عملکرد دفتر ثبت‌نام موارد به ایشان اطلاع داده می‌شود. دفتر ثبت‌نام مربوطه در سریع ترین زمان ممکن اقدام به رفع مشکل می‌نماید. در صورت عدم اصلاح نواقص توسط دفتر ثبت‌نام، مرکز میانی می‌تواند نسبت به ابطال مجوز فعالیت دفتر ثبت‌نام اقدام نماید.

۸-۶ گزارش نتایج

مرکز دولتی ریشه نتایج بازرسی خود از مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن را به شورای سیاستگذاری گواهی الکترونیکی کشور ارائه می‌نماید. این نتایج به عنوان اطلاعات محرمانه تلقی شده و فقط در صورت لزوم و با موافقت مراجع قضایی ذیصلاح یا پیرو دستور آنها افشا می‌شوند. نتایج بازرسی داخلی به مدیر مرکز میانی ارائه می‌شود.

۹. سایر موارد حقوقی و مربوط به کسب و کار

۹-۱ تعرفه‌ها

تعرفه‌های مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن برای خدمات گواهی طبق تعرفه‌های ابلاغیهٔ هیأت دولت و یا سایر مراجع ذی صلاح است.

۹-۱-۱ تعرفه‌های صدور یا تمدید گواهی

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن و دفاتر ثبت نام وابسته به این مرکز از تعرفه‌های ابلاغیهٔ هیأت دولت و یا سایر مراجع ذی صلاح تبعیت می‌کنند.

۹-۱-۲ تعرفه های دسترسی به گواهی

دسترسی به گواهی برای کلیهٔ طرف‌های اعتمادکننده به صورت رایگان است.

۹-۱-۳ تعرفه‌های ابطال یا دسترسی به اطلاعات وضعیت گواهی

برای هیچ‌کدام از خدمات مربوط به ابطال و اعلام وضعیت گواهی تعرفه‌ای دریافت نمی‌شود.

۹-۱-۴ تعرفه سایرخدمات

برای سایر خدمات مانند دسترسی به سند «دستورالعمل اجرایی گواهی الکترونیکی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن» (CPS) تعرفه‌ای دریافت نمی‌شود.

۹-۱-۵ سیاست استرداد

پس از پذیرش گواهی از سوی متقاضی، مطابق با آنچه که در بخش ۱-۴-۴ آمده است، امکان استرداد گواهی وجود ندارد.

۹-۲ مسئولیت های مالی

۹-۲-۱ پوشش بیمه

در حال حاضر، این مرکز از هیچ نوع پوشش بیمه‌ای پشتیبانی نمی‌کند.

۹-۲-۲ دیگر دارائی ها

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن منابع مالی کافی به منظور ادامهٔ عملکرد، انجام وظایف و پذیرش مسئولیت‌های خود را دارا می‌باشد. دارایی‌های این مرکز به حدی است که می‌تواند با استفاده از آنها خطرات مسئولیت نسبت به مالکان گواهی و طرف‌های اعتمادکننده را تا میزان قابل توجهی پوشش دهد.

۹-۲-۳ پوشش بیمه‌ای و گارانتی برای موجودیت‌های نهایی

در صورتی که گواهی صادر شده با ارائه دلایل منطقی که نشان‌دهندهٔ قصور مرکز میانی باشد، مورد قبول متقاضی گواهی قرار نگیرد (به عنوان مثال، عدم تطابق اطلاعات داخل گواهی با اطلاعات ارائه شده توسط متقاضی)، مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن مجدداً برای وی گواهی صادر می‌نماید و گواهی قبلی که پذیرش نشده بود را ابطال می‌نماید.

۹-۳ محرمانگی اطلاعات کسب و کار

۹-۳-۱ محدوده اطلاعات محرمانه

اطلاعات زیر محرمانه تلقی می‌شوند، و دفتر ثبت‌نام و مرکز میانی از آنها در مقابل افشا محافظت می‌نمایند:

- آن بخش از اطلاعات مربوط به درخواست گواهی که توسط مرکز میانی نگهداری می‌شود و در گواهی‌های صادره وجود ندارد.
- تمامی کلیدهای خصوصی و داده‌های فعال‌ساز که در مرکز میانی و دفتر ثبت‌نام بکار گرفته می‌شود.
- اطلاعات تجاری دریافتی از متقاضیان گواهی مانند طرح تجاری، اطلاعات فروش، اسرار بازرگانی و سایر اطلاعات دریافتی از شخص ثالث تحت قرارداد عدم انتشار اطلاعات.
- سوابق مربوط به کاربردهای گواهی الکترونیکی.
- کلیه اطلاعات مربوط پیگیری ثبت وقایع که توسط مرکز میانی ایجاد و نگه داری می‌شوند.
- تمهیدات امنیتی که برای طرح فنی تجهیزات، ساختمان، نرم‌افزارها و اجرای خدمات گواهی تخصیص یافته است.

۹-۳-۲ اطلاعاتی که در محدوده اطلاعات محرمانه نمی‌باشند

اطلاعات زیر محرمانه محسوب نمی‌شوند و نیاز به تمهیدات محافظتی خاصی از جانب این مرکز ندارند:

- کلیهٔ اطلاعات موجود در مخزن مرکز؛
- اطلاعات شناسایی و سایر اطلاعات مندرج در گواهی‌ها، مگر آنکه در توافق‌نامه‌های منعقده خلاف آن تصریح شده باشد.

۹-۳-۳ مسئولیت محافظت از اطلاعات محرمانه

مرکز میانی و دفتر ثبت‌نام، مسئولیت حفظ محرمانگی اطلاعات خصوصی و عدم افشای آن اطلاعات را به عهده دارد.

۹-۴ محافظت از اطلاعات خصوصی

بخشی از اطلاعات درخواست گواهی که توسط این مرکز نگهداری می‌شود ولی در گواهی‌های صادر شده وجود ندارد، به عنوان اطلاعات خصوصی مالک گواهی تلقی می‌شود. مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن مسئول محافظت از این اطلاعات می‌باشد.

۹-۴-۱ طرح حریم خصوصی

طرح حریم خصوصی مالکان گواهی الکترونیکی براساس قوانین موضوعه جمهوری اسلامی ایران از جمله قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۲۴ فصل سوم از باب سوم (مواد ۶۱-۵۸) و فصل دوم از باب چهارم (مواد ۷۳-۷۱) تعریف می‌شود. مرکز میانی در چارچوب قوانین جمهوری اسلامی ایران، حریم خصوصی مالکان گواهی را حفظ می‌نماید.

۹-۴-۲ اطلاعاتی که خصوصی محسوب می‌شوند

کلیهٔ اطلاعات مربوط به متقاضیان گواهی که جهت صدور گواهی به دفتر ثبت‌نام و مرکز میانی داده شده‌اند، و به صورت عمومی از طریق خود گواهی یا مخزن قابل دسترسی نمی‌باشد، خصوصی محسوب می‌شود.

۹-۴-۳ اطلاعاتی که خصوصی محسوب نمی‌شوند

کلیهٔ اطلاعات موجود در گواهی‌های منتشر شده و یا اطلاعات موجود در مخزن، خصوصی محسوب نمی‌شوند.

۹-۴-۴ مسئولیت محافظت از اطلاعات

مرکز میانی و دفتر ثبت‌نام، مسئول محافظت از کلیه اطلاعات شخصی و خصوصی مالکان گواهی می‌باشد.

۹-۴-۵ آگاهی و رضایت برای استفاده از اطلاعات خصوصی

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن اطلاعات خصوصی مالکان گواهی را در اختیار دیگران قرار نمی‌دهد. در صورتی که مالک گواهی قصد داشته باشد اطلاعات خصوصی او در اختیار شخص ثالثی قرار بگیرد، این مرکز تنها در صورت دریافت نامهٔ رسمی و کتبی مبنی بر رضایت مالک گواهی، اطلاعات وی را در اختیار شخص ثالث قرار می‌دهد.

۹-۴-۶ افشا مطابق با فرآیندهای اداری و قضایی

در شرایطی که به موجب قوانین موضوعه کشور در راستای حفظ امنیت و نظم عمومی و حمایت از حقوق شهروندان، کشف جرم و تعقیب مجرم، مرکز میانی موظف به ارائه اطلاعات خصوصی مالکان گواهی به مراجع قضایی و یا ضابطین قضایی باشد، همکاری مذکور صرفا با دریافت حکم قضایی رسمی، تنظیم شده توسط مرجع ذی صلاح خطاب به مرکز میانی انجام خواهد شد.

۹-۴-۷ سایر شرایط افشای اطلاعات

قابل اعمال نیست.

۹-۵ حق مالکیت معنوی

- **حق مالکیت معنوی گواهی‌ها و اطلاعات ابطال گواهی‌ها**

مالکیت معنوی کلیهٔ گواهی‌ها و اطلاعات ابطال آنها به مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن تعلق دارد. مالکان گواهی و طرف‌های اعتمادکننده می‌توانند از گواهی‌ها در کاربردهای مجاز مطابق با دستورالعمل تدوین شدهٔ این مرکز و توافق‌نامه‌های منعقده استفاده کنند.

- **حق مالکیت معنوی اسناد**

حق مالکیت معنوی کلیهٔ اسناد تنظیم شده در مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن، از جمله دستورالعمل اجرایی صدور گواهی (CPS) در انحصار این مرکز می‌باشد.

- **حق مالکیت معنوی نام‌ها**

هر گواهی الکترونیکی که توسط مراکز صدور گواهی الکترونیکی براساس ضوابط صادر می‌شود، در برگیرنده مالکیت معنوی آن نام برای مالک گواهی خواهد بود. این نام در مالکیت انحصاری مالک گواهی می‌باشد و هیچ شخص دیگری حق ثبت مجدد آن نام را برای خود ندارد.

- **حق مالکیت معنوی کلیدها**

حق مالکیت معنوی زوج کلید متناظر با هر گواهی، متعلق به مالک همان گواهی می‌باشد.

- **سایر موارد**

حق مالکیت معنوی کلیهٔ اطلاعات منتشر شده در مخزن متعلق به مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن می‌باشد.

۹-۶ مسئولیت‌ها و التزامات

۹-۶-۱ مسئولیت‌ها و التزامات مراکز صدور گواهی

۹-۶-۱-۱ التزامات مرکز صدور گواهی ریشه

در سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور» این التزامات بیان شده است، لذا برای اطلاعات بیشتر به این سند مراجعه شود.

۹-۶-۱-۲ مسئولیت‌ها و التزامات مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن موارد زیر را تضمین می‌کند:

- تدوین «سند دستورالعمل اجرایی گواهی الکترونیکی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن» (CPS) مطابق با سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور» و اخذ تأییدیه از مرکز دولتی ریشه؛
- مسئولیت ایجاد و امضای گواهی برای مالکان گواهی با اثبات مالکیت کلید خصوصی؛
- تضمین امنیت داده‌های مربوط به امضا در فرایند ایجاد این داده‌ها برای جلوگیری از شبیه سازی گواهی‌ها؛
- تضمین ارائه خدمات اعلام وضعیت گواهی‌ها به صورت سریع و مطمئن؛
- تضمین دسترسی دائم به مخزن منطبق با دستورالعمل اجرایی مرکز میانی (سند پیش رو)؛
- انطباق و بروزرسانی سند «دستورالعمل اجرایی گواهی الکترونیکی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن» (CPS) مطابق با سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور» و اخذ تأییدیه از مرکز دولتی ریشه؛
- بررسی صلاحیت و صدور مجوز برای دفاتر ثبت‌نام متعلق به خود؛
- تضمین ارایهٔ خدمات مدیریت گواهی الکترونیکی شامل صدور، ابطال، انتشار گواهی و اعلام وضعیت (ابطال یا عدم ابطال) گواهی به صورت مطمئن؛
- انجام بازرسی‌های دوره‌ای و مقطعی از دفاتر ثبت‌نام متعلق به خود؛
- انجام عملیات تولید زوج کلید به روش امن و منطبق با بخش ۳-۱-۱-۶ در صورت انجام این عملیات به نمایندگی از متقاضی؛
- حصول اطمینان از تولید زوج کلید تحت کنترل انحصاری مالک گواهی؛
- عدم نسخه برداری از زوج کلید تولید شده توسط مرکز میانی و دفاتر ثبت نام وابسته
- مطابقت فعالیت‌های مرکز میانی با سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور»، استانداردهای ارائه شده توسط مرکز دولتی ریشه، دستورالعمل اجرایی گواهی الکترونیکی و قرارداد بین مرکز مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن با مرکز دولتی ریشه؛
- اعمال استانداردهای زیرساخت کلید عمومی کشور؛
- اعلام پذیرش یا رد گواهی صادر شده توسط مرکز دولتی ریشه برای این مرکز، پس از دریافت ابلاغیه صدور گواهی (پذیرش گواهی میانی صادر شده توسط مرکز دولتی ریشه، بدین معناست که مرکز میانی صحت اطلاعات آن گواهی را تأیید می‌نماید)؛

- صدور گواهی الکترونیکی با استفاده از کلید خصوصی فقط در زمانی که گواهی صادر شده از سوی مرکز دولتی ریشه اعتبار داشته باشد؛
- اطلاع‌رسانی سریع به مرکز دولتی ریشه در موقع بروز هرگونه حادثه مانند گم شدن یا در خطر افشا قرار گرفتن کلید و درخواست ابطال گواهی؛
- التزام به قوانین حاکم موضوعه؛
- رعایت موارد امنیتی فیزیکی و منطقی؛
- آگاهی از این مطلب که مرکز میانی مسئول هرگونه خسارت وارده ناشی از تخطی موارد فوق می‌باشد.

۹-۶-۲ مسئولیت‌ها و التزامات دفاتر ثبت‌نام

دفاتر ثبت‌نام مرکز میانی باید موارد زیر را تضمین نمایند:

- انجام عملیات مطابق با دستورالعمل اجرایی مرکز میانی، استانداردهای ارائه شده توسط مرکز دولتی ریشه و نیز قراردادهای بین دفتر ثبت‌نام و مرکز میانی؛
- دریافت درخواست صدور، تجدید کلید، تمدید و ابطال گواهی و تحویل به مرکز میانی؛
- انجام عملیات احراز هویت متقاضی و اطمینان از صحت اطلاعات تحویل داده شده به مرکز میانی؛
- التزام به قوانین حاکم موضوعه؛
- رعایت موارد امنیتی فیزیکی و منطقی.

۹-۶-۳ مسئولیت‌ها و التزامات مالکان گواهی

مالک گواهی باید موارد زیر را تضمین نماید:

- تولید زوج کلید به روش امن و مطابق با بخش ۳-۱-۱-۶؛
- نگهداری کلید خصوصی به‌گونه‌ای که اشخاص غیرمجاز هیچ‌گونه دسترسی به آن نداشته باشند؛
- ارائه اطلاعات صحیح مرتبط با تقاضا و اعلام تغییر این اطلاعات در دوره اعتبار گواهی؛
- استفاده از گواهی فقط در کاربردهای مجاز و قانونی مطابق با کاربردهای مندرج در گواهی؛
- اعتبارسنجی گواهی هنگام استفاده از گواهی مطابق با بخش ۲-۵-۴ این سند؛
- ارائه درخواست ابطال گواهی در شرایط ذکر شده در بخش ۲-۱-۹-۴؛
- حصول اطمینان از این که نرم‌افزار استفاده شده، مورد تأیید مرکز دولتی ریشه می‌باشد. منظور از نرم‌افزار، نرم‌افزارهایی است که برای تولید زوج کلید و استفاده از گواهی (مثلاً نرم‌افزار امضاکننده با استفاده از کلید خصوصی) استفاده می‌شوند؛
- اطمینان از ایمن بودن محیط رایانه‌ای مورد استفاده به ویژه در هنگام تولید زوج کلید؛
- پایبندی به قراردادهای منعقد شده بین متقاضی و مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن؛
- به‌کارگیری گواهی در سطح اطمینان متناسب با سطوح اطمینان تعریف شده در بخش ۱-۱.

۹-۶-۴ مسئولیت‌ها و التزامات طرف‌های اعتمادکننده

طرف اعتمادکننده باید شرایط زیر را قبل از اعتماد به گواهی در نظر داشته باشد:

- استفاده از مخزن معتبر اعلام شده توسط مرکز صدور گواهی الکترونیکی پندار کوشک ایمن؛
- اعتبارسنجی گواهی هنگام استفاده از گواهی مطابق با بخش ۲-۵-۴ این سند؛

- دریافت گواهی خودامضای مرکز دولتی ریشه و همچنین گواهی مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن از طریق کانال توزیع مطمئن؛
- اطمینان از این که گواهی فقط در کاربردهای مجاز و قانونی مطابق با کاربردهای مندرج در گواهی به‌کار گرفته شده است؛
- حصول اطمینان از این که نرم‌افزار به‌کار گرفته شده مورد تأیید مرکز دولتی ریشه می‌باشد. منظور از نرم‌افزار، نرم‌افزاری است که عملیات بررسی صحت و اعتبار گواهی، تصدیق امضا، احراز هویت، و تمامیت داده‌های امضاشده را انجام می‌دهد؛
- حصول اطمینان از این که گواهی در سطح اطمینان متناسب با سطوح اطمینان تعریف شده در بخش ۱-۱ به‌کار گرفته شده باشد؛
- اطمینان از ایمن بودن محیط رایانه‌ای طرف‌های اعتمادکننده؛
- نگهداری اطلاعات امضاشده و نیز اطلاعات مربوط به امضا، گواهی و فرایندهای مرتبط با عملیات رمزنگاری تا زمان مقتضی.

۹-۶-۵ مسئولیت‌ها و التزامات سایر موجودیت‌ها

تعریف نشده است.

۹-۷ عدم پذیرش مسئولیت‌ها و التزامات

به جز مسئولیت‌ها و التزامات مورد اشاره در این سند، مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن هیچ‌گونه مسئولیتی در قبال خسارات مستقیم، غیرمستقیم، تصادفی، استنتاجی، خاص یا کیفری در مورد گواهی‌هایی صادرشده توسط این مرکز نمی‌پذیرد.

۹-۸ محدودیت مسئولیت‌ها

در مورد خسارت‌های ناشی از پذیرش گواهی‌های صادر شده از سوی طرف‌های اعتمادکننده و یا عدم پذیرش یک گواهی معتبر و یا پذیرش یک گواهی باطل شده توسط طرف‌های اعتمادکننده، هیچگونه مسئولیتی متوجه مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن نخواهد بود.

۹-۹ خسارت‌ها

مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن در صورت اعمال درست سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و ارائه خدمات در راستای قوانین تجارت الکترونیکی و این دستورالعمل اجرایی، هیچ‌گونه پرداختی جهت جبران خسارت ناشی از پذیرش و یا عدم پذیرش گواهی‌های صادر شده را به عهده نمی‌گیرد.

۹-۱۰ دوره و خاتمه

۹-۱۰-۱دوره

تا زمانی که نسخه جدید این سند تصویب و منتشر نشده است، این سند معتبر می‌باشد. این سند و هرگونه اصلاحات مصوب آن در مرکز دولتی ریشه ، برای مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن لازم‌الاجرا می‌باشد.

۹-۱۰-۲ خاتمه

به محض تایید و تصویب نسخه جدید این سند، از طریق وب‌سایت مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن منتشر می‌گردد و اعتبار نسخهٔ قبلی خاتمه خواهد یافت. همچنین با خاتمهٔ فعالیت مرکز صدور گواهی، اعتبار این سند به پایان می‌رسد.

۹-۱۰-۳ اثرات خاتمه و ابقا

تعریف نشده است.

۹-۱۱ اعلان‌های خاص و ارتباط بین موجودیت‌ها

ارتباط بین مرکز صدور گواهی و دفتر ثبت‌نام به صورت برخط از طریق نرم افزار دفتر ثبت‌نام انجام می‌شود. ارتباط بین این مرکز و مالکان گواهی می‌تواند از طریق ایمیل، فکس، صفحات وب، و سایر روش‌های اعلام شده توسط این مرکز باشد. مرکز میانی و دفاتر ثبت نام در زمینه اقداماتی که بر روابط آنها تاثیر گذار است به یکدیگر اطلاع رسانی می کنند.

۹-۱۲ تغییرات

۹-۱۲-۱فرایند تغییر

هر گونه تغییر در این سند به اطلاع مرکز دولتی ریشه می‌رسد. این تغییرات در مرکز دولتی ریشه ارزیابی می‌شود و پس از تایید و تصویب آن مرکز نسخه‌ی جدید به صورت عمومی در وب سایت مرکز منتشر می‌شود.

۹-۱۲-۲ دوره و مکانیزم اطلاع‌رسانی

این مرکز هرگونه تغییر در سند را به اطلاع مرکز دولتی ریشه می‌رساند، اگر توسط آن مرکز مورد تایید و تصویب واقع شد حداکثر تا ۵ روز کاری از طریق وب سایت مرکز منتشر می‌شود.

۹-۱۲-۳ شرایطی که OID باید تغییر نماید

کاربرد ندارد.

۹-۱۳ فرایندهای حل اختلاف

هر گونه اختلاف میان مرکز دولتی ریشه، مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن ابتدا از طریق کمیتهٔ نظارتی شورای سیاست‌گذاری گواهی الکترونیکی مورد رسیدگی قرار می‌گیرد؛ در صورت عدم حل اختلاف، مسأله به شورای سیاست‌گذاری گواهی الکترونیکی ارجاع می‌شود.

هرگونه اختلاف میان مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن و مالکان گواهی یا طرف‌های اعتمادکننده از طریق هیأت حل اختلاف در مرکز میانی برطرف می شود؛ و چنانچه اختلاف حادث شده از این طریق حل نشود و به تشخیص مرکز دولتی ریشه قابلیت حل و فصل در این مرکز را هم نداشته باشد، مسأله با طرح دعوا در مراجع قضایی ذیصلاح خاتمه می‌یابد. فرآیند حل اختلاف با دفتر ثبت‌نام مطابق قرارداد و توافق‌نامه منعقد شده میان طرفین است.

۹-۱۴ قوانین حاکم

کلیه قوانین موضوعه جمهوری اسلامی ایران از جمله قانون تجارت الکترونیکی (مصوب ۱۳۸۲/۱۰/۲۴)، آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی (مصوب در جلسه مورخ ۱۳۸۶/۰۶/۱۱ هیئت وزیران) و همچنین مصوبات شورای سیاست‌گذاری گواهی الکترونیکی کشور، حاکم بر کلیه فعالیت‌ها و قراردادهای بین مراکز صدور گواهی با مالکان گواهی و طرف‌های اعتماد کننده می‌باشد.

۹-۱۵ تطابق با قوانین اجرایی

این سند منطبق با قوانین اجرایی بخش ۹-۱۴ می‌باشد.

۹-۱۶ ملاحظات متفرقه

تعریف نشده است.

۹-۱۶-۱توافق‌نامه کلی

تعریف نشده است.

۹-۱۶-۲ تخصیص

تعریف نشده است.

۹-۱۶-۳ عدم وابستگی

در صورتی که مراجع ذیصلاح یکی از مفاد این سند را نادرست، نامعتبر یا غیر قابل اعمال بدانند، سایر مفاد آن تا زمان اصلاح سند، معتبر و لازم‌الاجرا خواهند بود.

۹-۱۶-۴ اجرای تعرفه‌های وکالت و فسخ مالکیت

تعریف نشده است.

۹-۱۶-۵ فورس ماژور

موارد فورس ماژور همان است که در قوانین عام جمهوری اسلامی ایران تدوین شده است. مرکز صدور گواهی الکترونیکی میانی خصوصی پندار کوشک ایمن می‌تواند گسترهٔ شمول موارد فورس ماژور را تا حدی که قوانین اجازه می‌دهند، بسط دهد.

۹-۱۷ سایر قیود

تعریف نشده است.