سیاست‌های گواهی الکترونیکی

زیرساخت کلید عمومی کشور

طبقه‌بندی: عادی

ویرایش: ۵،۰

تاریخ تصویب: ۱۳۹۹/۱۲/۲۰

Digitally signed by Reza Javadinia [Sign]
DN: c=IR, st=تهران, l=تهران, o=Governmental, ou=مرکز توسعه تجارت الکترونیکي, title=معاون زیرساخت کلید عمومی و امنیت اطلاعات تجاری, 2.5.4.97=14000405500, serialNumber=0074333607, givenName=رضا, sn=جوادي نیا, cn=Reza Javadinia [Sign]
Date: 2022.04.16 14:22:38 +04'30'

Digitally signed by Ali Rahbari [Sign]
DN: c=IR, st=تهران, l=تهران, o=Governmental, ou=مرکز توسعه تجارت الکترونیکي, title=MANAGER, 2.5.4.97=14000405500, serialNumber=4579352343, givenName=علي, sn=رهبري, cn=Ali Rahbari [Sign]
Date: 2022.04.18 11:44:13 +04'30'

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست جداول

۱ مقدمه

سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور دربردارنده مجموعه‌ای از ضوابط و الزامات عملیاتی و امنیتی حاکم بر زیرساخت کلید عمومی کشور می‌باشد. زیرساخت کلید عمومی یا PKI[1] به مجموعه‌ای از خدمات، محصولات، سیاست‌ها، فرایندها و سیستم‌های نرم‌افزاری و سخت‌افزاری گفته می‌شود که جهت مدیریت و به‌کارگیری گواهی‌های الکترونیکی X.509 و به منظور ارائه سرویس‌های امنیتی مختلف مبتنی بر رمزنگاری کلید عمومی[2] مورد استفاده قرار می‌گیرد.

تعاملات الکترونیکی امن در ایران تحت نظارت قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۲۴ مجلس شورای اسلامی و آیین نامه اجرایی ماده ۳۲ آن، مصوب ۱۳۸۶/۰۶/۱۱ هیئت دولت صورت می‌پذیرد. بر اساس آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیک، به منظور رسمیت بخشیدن به امضای الکترونیکی در کشور، مدل سلسله مراتبی[3] متشکل از شورای سیاست‌گذاری گواهی الکترونیکی کشور، مرکز دولتی صدور گواهی الکترونیکی ریشه به عنوان نقطه اعتماد[4] و مراکز صدور گواهی الکترونیکی میانی زیرین، به عنوان معماری زیرساخت کلید عمومی کشور به تصویب رسیده است.

مراکز صدور گواهی الکترونیکی میانی می‌توانند مجموعه‌ای از سازمان‌ها یا شرکت‌های دولتی یا خصوصی باشند که پس از طی مراحل لازم و تأیید مرکز دولتی صدور گواهی الکترونیکی ریشه و همچنین کسب مجوز از مرکز دولتی صدور گواهی الکترونیکی ریشه، شروع به ارائه خدمات گواهی الکترونیکی در ساختار سلسله مراتبی زیرساخت کلید عمومی کشور می‌نمایند.

در یک ساختار سلسله مراتبی PKI، مرکز دولتی صدور گواهی الکترونیکی ریشه، ملزم به تعیین سیاست‌های گواهی الکترونیکی منطبق با نیازمندی‌های عملیاتی و امنیتی کشور در حوزه‌های مختلف می‌باشد؛ بر این اساس، سند پیش رو دربردارنده سیاست‌های گواهی الکترونیکی در زیرساخت کلید عمومی کشور مشتمل بر الزامات و فرآیندهای مرکز دولتی صدور گواهی الکترونیکی ریشه و همچنین سیاست‌ها و الزامات مورد نیاز برای اعتمادسازی و ایجاد یکپارچگی و تعامل در اجزای مختلف زیرساخت کلید عمومی کشور می‌باشد.

سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور، سند یکپارچه‌ای است که مراکز صدور گواهی الکترونیکی مورد تأیید، در چارچوب آن تأسیس شده و آغاز به کار می‌کنند. تمام شرایط مذکور در این

---

1 Public Key Infrastructure

2 Public Key Cryptography

3 Hierarchical Model

4 Trust Point

سند برای انواع مراکز صدور گواهی الکترونیکی موضوع این سند صدق می‌نماید، مگر اینکه خلاف آن صریحاً بیان شود.

برنامه‌هایی که قابلیت ارائه خدمات امنیتی مبتنی بر زیرساخت کلید عمومی را دارا می‌باشند، سرویس‌هایی مانند احراز هویت، محرمانگی[۱]، تمامیت[۲] و انکارناپذیری[۳] 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 مراکز صدور گواهی الکترونیکی شامل تجهیزات، تأسیسات، کارکنان و فرایندها، حاصل می‌شود. عملکرد مطمئن یک مرکز صدور گواهی الکترونیکی نیز تنها در صورت وجود و اعمال سیاست‌های گواهی الکترونیکی نقطه اعتماد در ساختار سلسله مراتبی - که همان مرکز دولتی صدور گواهی الکترونیکی ریشه - می‌باشد، محقق خواهد شد. بنابراین طراحی یک زیرساخت کلید عمومی با امنیت مناسب بسیار حیاتی است تا طرف‌های اعتماد کننده بتوانند به گواهی‌های الکترونیکی اعتماد نمایند. این اعتماد به معنی اعتماد به پیوند میان مالک گواهی و کلید عمومی او می‌باشد.

سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور بر اساس استاندارد X.509 و منطبق با RFC3647[۴] تهیه و تنظیم شده است.

۱-۱ خلاصه

مستند پیش رو دربردارنده سیاست‌ها و فرایندهای مرکز دولتی صدور گواهی الکترونیکی ریشه و همچنین سیاست‌ها و الزامات کلیه مراکز صدور گواهی میانی موجود در ساختار سلسله مراتبی زیر ساخت کلید عمومی کشور است؛ ضمن اینکه توسط کلیه موجودیت‌های نهایی شامل مالکان گواهی، طرف‌های اعتماد کننده و دفاتر ثبت نام نیز قابل استفاده می‌باشد.

این مستند چهار سیاست گواهی را برای صدور گواهی‌های الکترونیکی که در زیرساخت کلید عمومی کشور مورد استفاده قرار خواهند گرفت، تعریف می‌نماید. این سیاست‌ها در سطوح اطمینان[۵] زیر تعریف شده‌اند:

- سطح ۱ یا برنز
- سطح ۲ یا نقره
- سطح ۳ یا طلا
- سطح ۴ یا پلاتین

---

1 Confidentially

2 Integrity

3 Non Repudiation

4 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

5 Assurance Level

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[1]	• 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.
سطح ۲	نقره[2]	• 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.
سطح ۳	طلا[3]	• این سطح برای محیط‌هایی که در آن ریسک و خسارات ناشی از سوءاستفاده، جعل و افشای اطلاعات زیاد است، مورد استفاده قرار می‌گیرد. • از این سطح می‌توان برای تراکنش‌هایی که حاوی ارزش مالی بالا هستند و در آن‌ها امکان جعل و سوء استفاده بالاست، استفاده نمود. • گواهی‌های این سطح با در نظر گرفتن بند اول و دوم، می‌توانند برای تراکنش‌هایی که نیاز به احراز هویت، انکارناپذیری و یا محرمانگی دارند مورد استفاده قرار گیرند.
سطح ۴	پلاتین[4]	• این سطح برای محیط‌هایی که تهدیدات روی منابع اطلاعاتی یا خسارات ناشی از ناکارایی و شکست سرویس‌های امنیتی خیلی زیاد است، مورد استفاده قرار می‌گیرد. • از این سطح می‌توان برای تراکنش‌هایی که حاوی ارزش مالی بسیار بالا هستند و در آن‌ها امکان جعل و سوءاستفاده بسیار بالاست، استفاده نمود. • گواهی‌های این سطح با در نظر گرفتن بند اول و دوم، می‌توانند برای تراکنش‌هایی که نیاز به احراز هویت، انکارناپذیری و یا محرمانگی دارند مورد استفاده قرار گیرند.

[1] Bronze
[2] Silver
[3] Gold
[4] Platinum

افراد یا سازمان‌های درخواست‌کننده گواهی مسئول انتخاب سطح اطمینان مورد نیاز خود می‌باشند و می‌بایست با توجه به طبقه‌بندی اطلاعات و میزان حساسیت و اهمیت سیستم‌های استفاده کننده از گواهی الکترونیکی، درخواست گواهی الکترونیکی در سطح اطمینان مناسب و مطلوب نمایند.

مراکز صدور گواهی الکترونیکی مختلف با توجه به سطح گواهی قابل ارائه، به چهار کلاس مختلف تقسیم‌بندی می‌شوند. یک مرکز صدور گواهی الکترونیکی می‌تواند سیاست‌های گواهی را برای بیش از یک سطح اطمینان پیاده‌سازی نماید؛ به عنوان مثال یک مرکز صدور گواهی کلاس ۳ می‌تواند برای سه سطح اطمینان ۱، ۲ و ۳ گواهی صادر نماید. در جدول زیر سطوح گواهی قابل ارائه برای کلاس‌های مختلف مراکز صدور گواهی آورده شده است.

جدول ۲ سطوح مراکز میانی و سطوح گواهی‌های قابل ارائه آن‌ها

کلاس مرکز صدور گواهی الکترونیکی میانی	سطح گواهی قابل ارائه
کلاس ۱	سطح ۱
کلاس ۲	سطوح ۱ و ۲
کلاس ۳	سطوح ۱، ۲ و ۳
کلاس ۴	سطوح ۱، ۲، ۳ و ۴

۲-۱ نام و شناسه سند

این سند به نام «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور» نام‌گذاری شده و در بیست و هفتمین جلسه شورای سیاست‌گذاری گواهی الکترونیکی کشور مورخ ۱۳۹۹/۱۲/۲۰ به تصویب رسید. تاریخ انتشار سند ۱۴۰۱/۰۱/۲۵ و آخرین نسخه این سند در سایت مرکز دولتی صدور گواهی الکترونیکی ریشه به نشانی http://www.rca.gov.ir قابل دسترسی است. شناسه (OID[1]) سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور بر اساس چهار سطح امنیتی در جدول زیر آورده شده است.

جدول ۳ شناسه سیاست‌های سطوح اطمینان

سطح اطمینان	شناسه
سطح ۱	2.16.364.101.1.1.1
سطح ۲	2.16.364.101.1.1.2
سطح ۳	2.16.364.101.1.1.3
سطح ۴	2.16.364.101.1.1.4

[1] Object Identifier

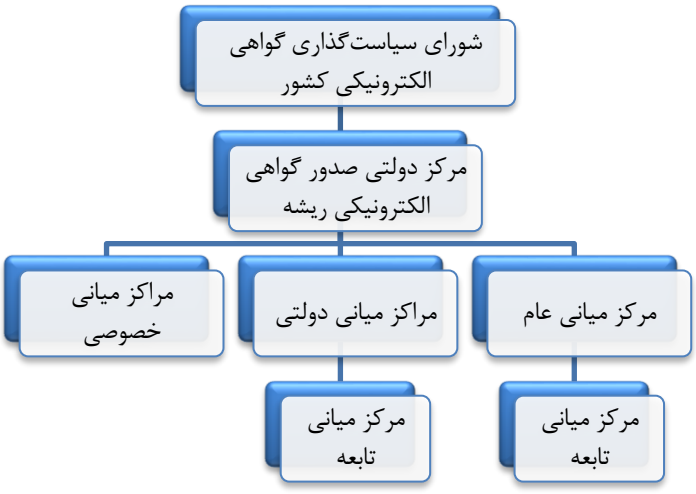
۳-۱ اجزای زیرساخت کلید عمومی

۱-۳-۱ مراکز صدور گواهی الکترونیکی[1]

مراکز صدور گواهی الکترونیکی در زیرساخت کلید عمومی کشور از مرکز دولتی صدور گواهی الکترونیکی ریشه و مراکز صدور گواهی الکترونیکی میانی تشکیل شده است که در این بخش به تشریح انواع مراکز صدور گواهی و معماری سلسله مراتبی زیرساخت کلید عمومی کشور پرداخته شده است.

مرکز دولتی صدور گواهی الکترونیکی ریشه: مرکز دولتی صدور گواهی الکترونیکی ریشه که از این پس در این سند به اختصار به آن «مرکز دولتی ریشه» نامیده می‌شود، 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 مورخ ۱۳۸۶/۰۷/۳۰ مجوز ایجاد، امضا، صدور و ابطال گواهی الکترونیکی مراکز صدور گواهی الکترونیکی میانی را دریافت کرده است. مرکز دولتی ریشه مسئول تمام ابعاد صدور و مدیریت مراکز صدور گواهی الکترونیکی میانی، شامل نظارت بر فرایندهای ثبت نام، احراز هویت، صدور گواهی‌های میانی، انتشار و ابطال گواهی‌ها و تجدید کلید[2] می‌باشد.

ساختار معماری سلسله مراتبی زیر ساخت کلید عمومی کشور بدون در نظر گرفتن سطوح اطمینان، به صورت اجمالی در شکل زیر نشان داده شده است.



شکل ۱ ساختار سلسله مراتبی زیرساخت کلید عمومی کشور

[1] Certificate Authorities (CA)

[2] Re-Key

همان‌طور که در شکل بالا نشان داده شده است، مرکز دولتی ریشه تحت نظر شورای سیاست‌گذاری گواهی الکترونیکی کشور (توضیحات مربوط به شورای سیاست‌گذاری در بخش ۱-۳-۵ آورده شده است)، در سطح اول زیرساخت قرار دارد و در سطح بعدی مراکز صدور گواهی میانی وجود دارند.

مراکزی که مجوز فعالیت‌ها و همچنین گواهی خود را از مرکز دولتی ریشه دریافت نموده باشند، مراکز صدور گواهی الکترونیکی میانی گفته می‌شوند که از این پس در این سند به اختصار «مرکز میانی» نامیده می‌شوند. این مراکز، صلاحیت صدور و ابطال گواهی الکترونیکی مالکان گواهی را دارا هستند. مراکز میانی می‌بایست به منظور دریافت گواهی خود مطابق با شرایط این سند عمل نمایند. انواع مراکز میانی بر اساس «سند دستورالعمل اجرایی ساماندهی مراکز صدور گواهی الکترونیکی میانی» مصوبه مورخ ۱۳۸۸/۰۲/۱۹ شورای سیاست‌گذاری و اصلاحات بعدی آن، عبارتند از:

- **مرکز میانی دولتی عام**

مرکز منحصر به فردی است که به طور عام مبادرت به ارائه خدمات گواهی الکترونیکی برای تمامی کاربردهای مختلف به متقاضیان می‌نماید.

تبصره- تا زمان راه‌اندازی مرکز میانی خصوصی، این مرکز مجاز است به مشتریان بخش خصوصی برای کاربردهای غیر دولتی، خدمات گواهی الکترونیکی ارائه نماید.

- **مراکز میانی دولتی**

هر یک از دستگاه‌های اجرایی می‌توانند با کسب مجوز و اخذ گواهی از مرکز دولتی ریشه، در حوزه فعالیت خود، مبادرت به تاسیس مرکز میانی دولتی نمایند.

تبصره – مرکز میانی دولتی می‌تواند، با ائتلاف چند دستگاه اجرایی جهت ارائه خدمات گواهی الکترونیکی در حوزه‌های مشترک با مسئولیت یکی از دستگاه‌های موتلفه مزبور و ارائه سند دستورالعمل گواهی واحد، تاسیس شود.

- **مراکز میانی تابعه**

مراکز میانی دولتی تا یک سطح بعدی دستگاه یا دستگاه‌های متبوع خود در صورت داشتن شرایط مربوط، می‌توانند صرفاً در حوزه فعالیت خود اقدام به ایجاد مراکز میانی تابعه و صدور گواهی برای آن‌ها نمایند.

تبصره ۱- تا زمانی که دستگاه‌های بالا دستی متقاضیان تاسیس مرکز میانی تابعه، اقدام به تاسیس مرکز میانی دولتی نکرده‌اند، این مراکز می‌تواند زیر مرکز میانی عام تاسیس شوند.

تبصره ۲- در صورت عدم تطابق دستورالعمل گواهی متقاضی تاسیس مرکز میانی تابعه با دستورالعمل گواهی دستگاه بالادستی و احراز وجود شرایط ویژه برای متقاضی می‌تواند در حوزه فعالیت خود در مرتبه اول مجوز تاسیس مرکز میانی تابعه زیر مرکز میانی عام و در مرتبه بعدی مجوز تاسیس مرکز میانی دولتی دریافت نماید.

- **مراکز میانی خصوصی**

این مراکز برای صدور گواهی الکترونیکی مورد استفاده در بخش خصوصی برای کاربردهای تعریف شده آن‌ها پس از احراز صلاحیت‌های کیفی، کمی و حقوقی، مجوز تاسیس از مرکز دولتی ریشه خواهند گرفت. آیین‌نامه شرایط احراز صلاحیت مراکز میانی خصوصی توسط مرکز دولتی ریشه تهیه و در جلسه بیست و چهارم شورا مورخ ۱۳۹۷/۰۲/۱۱به تصویب رسیده است.

مجوز تاسیس مراکز میانی اعم از دولتی، عام، خصوصی و تابعه، پس از تأیید و تصویب دستورالعمل‌های اجرایی مربوطه توسط مرکز دولتی ریشه صادر می‌شود. ضمن اینکه بازرسی‌های دوره‌ای از تمامی مراکز میانی نام‌برده، بر عهده مرکز دولتی ریشه بوده و مراکز مزبور موظف به ارائه کلیه تمهیدات لازم می‌باشند.

همان‌طور که در بخش ۱-۱ اشاره شد، مراکز صدور گواهی مختلف با توجه به سطوح گواهی قابل ارائه، به ۴ کلاس مختلف تقسیم می‌شوند و این مراکز می‌توانند سیاست‌های گواهی را برای یک یا چند سطح اطمینان پیاده‌سازی نمایند. تقسیم‌بندی مرکز دولتی ریشه و مراکز میانی به شرح زیر می‌باشد:

جدول ۴ سطوح مختلف مراکز صدور گواهی الکترونیکی

نوع مرکز صدور گواهی	کلاس مرکز صدور گواهی
مرکز دولتی ریشه	کلاس ۴
مرکز میانی دولتی عام	کلاس ۴
مراکز میانی دولتی	کلاس ۳ یا ۴
مراکز میانی خصوصی	کلاس ۲ یا ۳
مراکز میانی تابعه	کلاس ۲ تا کلاس مرکز میانی بالادستی

همان طور که در شکل ۱ مشهود است، ساختار سلسله مراتبی زیرساخت کلید عمومی کشور حداکثر از ۳ لایه تشکیل شده است که می‌تواند متناظر با زنجیره‌ای متشکل از سه گواهی باشد (به عنوان مثال گواهی مرکز دولتی ریشه، گواهی مرکز میانی عام و گواهی مرکز میانی تابعه).

لازم به ذکر است که مرکز میانی عام و مراکز میانی دولتی تنها در صورت تایید مرکز دولتی ریشه مجاز به ایجاد لایه سوم (مرکز تابعه)، می‌باشند؛ ضمن اینکه مراکز میانی خصوصی مجاز به ایجاد این لایه نیستند.

بر اساس جدول ۴ مرکز دولتی ریشه امکان صدور گواهی در چهار سطح امنیتی پلاتین، طلا، نقره و برنز را دارد. این گواهی‌ها بسته به کلاس مرکز میانی در اختیار آن‌ها قرار می‌گیرد. به عنوان مثال برای یک مرکز میانی دولتی از کلاس ۳، گواهی‌هایی در ۳ سطح برنز، نقره و طلا صادر شده تا این مرکز امکان ارائه خدمات گواهی الکترونیکی در سطوح امنیتی ۱، ۲ و ۳ را متناسب با سیاست‌های هر سطح داشته باشد.

۱-۳-۲ دفاتر ثبت نام[1]

دفتر ثبت نام موجودیتی است اختیاری که وظیفه شناسایی و بررسی صحت اطلاعات دریافت شده از سوی درخواست‌کنندگان گواهی الکترونیکی را بر عهده دارد. در واقع دفتر ثبت نام با بررسی هویت درخواست کننده، وظیفه تنظیم درخواست صدور، تعلیق/ رفع تعلیق، ابطال و به‌روزرسانی گواهی و همچنین درخواست تجدید کلید را بر عهده دارد. دفتر ثبت نام می‌بایست مورد تایید مرکز صدور گواهی باشد و توافق‌نامه یا قراردادی بین این دو جهت متعهد شدن دفتر ثبت نام بر ارائه خدمات منطبق با دستورالعمل اجرایی مرکز میانی، منعقد گردد. دفتر ثبت نام می‌بایست فعالیت‌های خود را با دستورالعمل اجرایی مرکز میانی مربوطه، تطابق دهد.

۱-۳-۳ مالکان گواهی[2]

مالک گواهی به موجودیتی گفته می‌شود که از مرکز صدور گواهی، گواهی دریافت کرده و نام او به عنوان نام مالک گواهی[3] در گواهی الکترونیکی، ثبت می‌شود. هویت مالک گواهی قبل از صدور گواهی، توسط مرکز صدور گواهی یا دفتر ثبت نام بررسی و احراز می‌شود.

مالک گواهی ممکن است یک مرکز صدور گواهی، شخص، یک سازمان، کارمندان یک سازمان و یا سایر موجودیت‌های مثل دیواره آتش[4]، سرویس‌دهنده مورد اعتماد[5] و ... باشد که در یک سازمان جهت برقراری ارتباط امن مورد استفاده قرار می‌گیرند.

۱-۳-۴ طرف‌های اعتماد کننده[6]

طرف اعتماد کننده موجودیتی است که به صحت تطابق میان مشخصات و کلید عمومی مالک گواهی الکترونیکی اعتماد کرده و گواهی الکترونیکی او را مورد استناد قرار می‌دهد.

۱-۳-۵ اجزای دیگر

۱-۳-۵-۱ شورای سیاست‌گذاری گواهی الکترونیکی کشور

به منظور حفظ یکپارچگی و جلوگیری از تفکیک راهکارها و استانداردهای به‌کار گرفته شده در مراکز صدور گواهی، سیاست‌گذاری در زمینه فعالیت‌های مرکز دولتی ریشه و به‌روزرسانی سیاست‌های گواهی این مرکز

---

1 Registration Authorities (RA)

2 Subscriber

3 SubjectName

4 Firewall

5 Trusted Server

6 Relying Parties

شورایی به نام شورای سیاست‌گذاری گواهی الکترونیکی تشکیل شده است که از این پس در این سند به اختصار «شورا» نامیده می‌شود. اعضای شورا مطابق با ماده ۲ آئین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی مصوب هیأت محترم وزیران و اصلاحات بعدی آن تعیین می‌گردد.

۱-۳-۵-۲ کمیته نظارتی شورا

به منظور انجام فعالیت‌های نظارتی، شورا کمیته‌ای با نام کمیته نظارتی را با عضویت ۵ نفر (ترجیحاً از اعضای شورا) به مدت یک سال انتخاب می‌نماید. حضور ۳ نفر از اعضا برای فعال کردن پودمان امنیتی سخت‌افزاری[1] مرکز دولتی ریشه ضروری است.

۱-۴ کاربردهای گواهی[2]

۱-۴-۱ مصارف مناسب گواهی

زیرساخت کلید عمومی کشور به منظور تأمین سرویس‌های امنیتی تمامیت، احراز هویت، انکارناپذیری و محرمانگی طراحی شده است. مراکز میانی در صورت استفاده از سطوح اطمینان مختلف، می‌بایست تعریف این سطوح اطمینان و کاربرد پذیری و شناسه هر سطح اطمینان را در دستورالعمل اجرایی گواهی[3] خود قید کنند. جدول زیر کاربردها/انواع گواهی تعریف شده و مورد استفاده در زیرساخت کلید عمومی کشور را نمایش می‌دهد.

جدول ۵ انواع مقاصد مورد استفاده گواهی

کاربرد/نوع گواهی	توضیحات
گواهی امضا	این گواهی جهت امضای اسناد و تراکنش‌های الکترونیکی و همچنین می‌تواند جهت احراز هویت کاربران[4] مورد استفاده قرار می‌گیرد.
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[5] مبتنی بر کلید عمومی، در سیستم عامل‌های

1 Hardware Security Module (HSM)

2 Certificate Usage

3 Certificate Practice Statemen (CPS)

4 Client Authentication

5 Two Factor Authentication

کاربرد/نوع گواهی	توضیحات
	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 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 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 مرکز دولتی ریشه	گواهی خودامضایی[1] که متعلق به مرکز دولتی صدور گواهی الکترونیکی ریشه می‌باشد.
گواهی مراکز میانی	گواهی متعلق به مراکز صدور گواهی میانی موجود در ساختار سلسله مراتبی زیرساخت کلید عمومی کشور، که توسط مرکز صدور گواهی بالا دستی صادر می‌شود.
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[2]	گواهی متعلق به سرور پاسخگوی OCSP[3] که جهت امضای پاسخ‌های OCSP تنظیم شده توسط این سرور، مورد استفاده قرار می‌گیرد.
گواهی مراکز مهر زمانی[4]	اصولاً مهر زمانی جهت ثبت دقیق زمان در هنگام امضای اسناد مختلف از جمله قراردادها و یا توافق‌نامه‌ها و بایگانی آن‌ها 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.

1 Self Signed Certificate

2 Online Certificate Status Protocol

3 OCSP Responder

4 Time Stamping Authority

۱-۴-۲ مصارف غیرمجاز گواهی

مصارف غیر مجاز گواهی به شرح زیر می‌باشد:

- گواهی‌ها نباید در مصارف غیر قانونی و مخالف با نظم عمومی، مورد استفاده قرار گیرند.
- از گواهی الکترونیکی صرفاً می‌بایست در کاربرد (های) در نظر گرفته شده برای همان گواهی که در بخش ۱-۴-۱ قید شده است، استفاده گردد.
- گواهی‌های صادر شده برای اشخاص و سرویس‌گیرندگان، جهت استفاده در برنامه‌های کاربردی سرویس‌گیرنده بوده و نباید به عنوان گواهی سرویس‌دهنده و یا گواهی سازمانی مورد استفاده قرار گیرد.
- گواهی مرکز صدور گواهی نباید برای کاربردی غیر از حوزه عملیات مرکز صدور گواهی به‌کار رود.
- گواهی موجودیت‌های نهایی نباید به عنوان گواهی مراکز صدور گواهی به‌کار روند.

۱-۵ راهبری سیاست‌ها[1]

۱-۵-۱ سازمان راهبری سند

مسئولیت تدوین، اصلاح و بازنگری و انتشار این سند بر عهده مرکز دولتی ریشه بوده و همچنین مسئولیت تأیید و تصویب این سند بر عهده شورا می‌باشد. تنها مرجع مجاز برای تفسیر این سند مرکز دولتی ریشه بوده و این مرکز پاسخگوی هرگونه سؤال و ابهام در ارتباط با این سند منطبق با بخش ۱-۵-۲ خواهد بود.

۱-۵-۲ اطلاعات تماس

سؤالات مربوط به سیاست‌های گواهی، توسط مرکز دولتی ریشه پاسخ داده می‌شود:

- نشانی پست الکترونیکی: rca@ecommerce.gov.ir
- نشانی پایگاه وب: http://www.rca.gov.ir/
- شماره تلفن: ۰۲۱-۴۱۰۳۱۰۰۰
- شماره فاکس: ۰۲۱-۸۸۹۵۵۹۵۳
- نشانی: تهران، بلوار کشاورز، خیابان شهید نادری، پلاک ۱۱، ساختمان شماره یک وزارت صنعت، معدن و تجارت، مرکز توسعه تجارت الکترونیکی

[1] Policy Administration

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

مرکز دولتی ریشه مسئولیت تأیید تطبیق دستورالعمل‌های اجرایی مراکز میانی با سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور را بر عهده دارد و در صورت تطبیق، ضمن تصویب دستورالعمل‌های اجرایی مراکز میانی، مجوز راه‌اندازی مراکز میانی را صادر می‌نماید.

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 کشورتدوین نموده و به همراه اسناد و مدارک مرتبط[1] به مرکز دولتی ریشه ارائه نمایند. دستورالعمل اجرایی ارائه شده به همراه اسناد مرتبط در مرکز دولتی ریشه مورد ارزیابی، تأیید و تصویب قرار می‌گیرد.

۱-۶ تعاریف و اختصارات

اختصارات

جدول ۶ اختصارات

مخفف	معادل	معنی
CA	Certificate Authority	موجودیتی که مجاز به صدور و مدیریت گواهی‌های الکترونیکی می‌باشد.
CP	Certificate Policies	مجموعه‌ای از قوانین که الزامات سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشوررا 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 گواهی‌های 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 ترکیبی 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 آن‌ها را بر روی کل شبکه اینترنت توزیع

[1] روال ارائه دستورالعمل اجرایی گواهی الکترونیکی مراکز میانی و اسناد مرتبط دیگر در مستند «راهنمای درخواست تاسیس مراکز میانی» به‌طور کامل تشریح شده است و از طریق وب سایت مرکز دولتی ریشه، قابل دریافت می‌باشد.

مخفف	معادل	معنی
		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 ۱۰ که ساختاری را برای درخواست گواهی تعریف می‌نماید.
PKI	Public Key Infrastructure	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[1] مورد استفاده قرار می‌گیرد.
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 گواهی‌های الکترونیکی یا لیست گواهی‌های باطل شده را امضا نمی‌نماید ولی مسئولیت ثبت و شناسایی اطلاعات مورد نیاز مرکز صدور گواهی برای صدور گواهی الکترونیکی یا لیست گواهی‌های 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	الگوریتم رمزنگاری کلید عمومی که در سال ۱۹۷۸ توسط سه نفر به نام‌های ران ریوست[2]، ادی شامیر[3] و لئونارد آدلمن[4] اختراع شده است.
URL	Uniform Resource Locator	رشته‌ای از کاراکترها است که مکان منبعی که در اینترنت قابل دسترس است را مشخص می‌نماید.

1 Public Key Cryptography

2 Rivest

3 Shamir

4 Adleman

مخفف	معادل	معنی
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 ۷ 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.

لغت	معادل	معنی
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.
پودمان رمزنگاشتی سخت‌افزاری	Hardware Security Module (HSM)	نوعی پودمان سخت‌افزاری امن که از طریق واسطهای نرم‌افزاری، امکان نگهداری امن کلیدهای رمزنگاری و اجرای ایمن مکانیزم‌های رمزنگاری را با کارایی مطلوب فراهم می‌آورد.
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

لغت	معادل	معنی
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.509,V3 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.
امانت‌گذاری 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.

لغت	معادل	معنی
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[1] مورد استفاده قرار می‌گیرد.
سخت‌افزار	Hardware	اجزا فیزیکی سیستم رایانه‌ای.
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 کشوررا 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 استاندارد ASN.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.

[1] Public Key Cryptography

لغت	معادل	معنی
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، تعلیق/رفع تعلیق 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.

لغت	معادل	معنی
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

کلیه مراکز میانی ملزم به ایجاد و نگهداری یک مخزن عمومی جهت انتشار گواهی‌ها، لیست گواهی‌های باطله و اطلاعات مرتبط دیگر هستند که به صورت برخط در دسترس کاربران مختلف قرار می‌گیرد. حداقل اطلاعاتی که می‌بایست در مخزن منتشر شود در بخش ۲-۲ معرفی شده است. مراکز صدور گواهی می‌بایست مالکان گواهی را از محل انتشار گواهی‌ها و لیست گواهی‌های باطله و یا سرویس‌دهنده پاسخگوی OCSP مطلع نمایند. سند دستورالعمل اجرایی مراکز میانی می‌بایست پس از تصویب توسط مرکز دولتی ریشه، در مخزن قرار گیرد.

مرکز دولتی ریشه، گواهی(های) خودامضا و لیست گواهی‌های باطله، گواهی‌های صادر شده برای مراکز میانی، این سند و کلیه اسناد مرتبط دیگر را از طریق وب‌سایت خود به نشانی http://www.rca.gov.ir منتشر می‌نماید.

۲-۲ انتشار اطلاعات گواهی

کلیه مراکز صدور گواهی میانی می‌بایست حداقل اطلاعات زیر را از طریق مخزن منتشر کنند تا در دسترس مالکان گواهی و طرف‌های اعتماد کننده قرار گیرد:

- کلیه گواهی‌های صادرشده توسط مرکز میانی؛
- آخرین نسخه منتشرشده CRL؛
- گواهی‌های صادره برای مرکز میانی؛
- سند دستورالعمل اجرایی گواهی الکترونیکی مرکز صدور گواهی (CPS)؛
- سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور(CP)؛
- سرویس OCSP در صورتی که مرکز میانی از پروتکل OCSP پشتیبانی نماید؛
- توافقنامه با طرف اعتماد کننده؛
- توافقنامه با مالک گواهی؛

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

- گواهی (های) مرکز دولتی ریشه؛
- گواهی‌های صادر شده برای مراکز میانی؛

- لیست گواهی‌های باطل شده (CRL)؛
- سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور؛
- سند جامع پروفایل‌های زیرساخت کلید عمومی کشور؛
- راهنمای درخواست تأسیس مراکز میانی؛
- سند نرخ خدمات و محصولات مراکز صدور گواهی؛
- استانداردهای زیرساخت کلید عمومی کشور.
- فهرست پودمان‌های رمزنگاشتی و نرم‌افزارهای صدور و مدیریت گواهی مورد تایید مرکز دولتی ریشه؛
- کلیه مصوبات شورا و اسناد مرتبط دیگر که مرکز دولتی ریشه لزوم به انتشار آن‌ها را احراز نماید.

۲-۳ زمان یا تناوب انتشار

الزامات زمان‌بندی و تناوب انتشار برای کلیه مراکز صدور گواهی به شرح زیر می‌باشد:

- گواهی‌های صادر شده می‌بایست پس از پذیرش گواهی توسط مالکان گواهی که منطبق با بخش ۴-۴ صورت می‌گیرد، منتشر شوند.
- زمان یا تناوب انتشار لیست گواهی‌های باطله با توجه به سطح اطمینان در بخش ۴-۹-۷ تعیین شده است.
- در صورت پشتیبانی از پروتکل OCSP توسط مرکز صدور گواهی، سرور پاسخگوی OCSP می‌بایست به صورت بلادرنگ[1] وضعیت گواهی را به سرویس‌گیرنده OCSP ارائه نماید.
- این سند پس از تأیید و تصویب توسط شورا منتشر می‌گردد و به صورت سالیانه در صورت نیاز به اعمال تغییر مورد بازنگری قرار می‌گیرد.

۲-۴ کنترل دسترسی به مخازن

مراکز صدور گواهی می‌بایست از کلیه اطلاعات مخزن در برابر تغییرات غیرمجاز محافظت نمایند. هرگونه تغییر و به‌روزرسانی در مخزن، تنها می‌بایست توسط نقش‌های مورد اطمینان مندرج در بخش ۵-۲-۱، صورت گیرد. مراکز میانی می‌بایست سیستم عامل و مخزن خود را طوری پیکربندی نمایند که تنها نقش‌های مجاز مرکز میانی بتوانند پس از تایید مرکز دولتی ریشه، نسخه برخط سند دستورالعمل اجرایی را جایگزین نمایند.

تغییر و به‌روزرسانی مخزن مرکز دولتی ریشه تنها توسط پرسنل مجاز مرکز دولتی ریشه و پس از اعمال فرایند کنترل دسترسی چند لایه امکان‌پذیر می‌باشد؛ همچنین آخرین نسخه مصوب این سند در شورا در

[1] Real Time

قالب یک فایل PDF و پس از امضای الکترونیکی توسط دبیر شورا در مخزن مرکز دولتی ریشه منتشر خواهد شد و تنها در صورتی معتبر است که شامل این امضای الکترونیکی باشد.

۳ شناسایی و احراز هویت

۳-۱ نام‌گذاری

هر موجودیت مالک گواهی، می‌بایست مطابق PKIX Part1، یک نام کاملاً متمایز و یکتا به فرم استاندارد X.501 در فیلدهای «نام مالک گواهی[1]» و «نام صادرکننده گواهی[2]» 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

جدول ۸ الزامات نام‌گذاری

سطح اطمینان	الزامات
سطح ۱	هر موجودیت می‌بایست: • یک نام کاملاً متمایز و یکتا به فرم استاندارد X.501 در فیلدهای «نام مالک گواهی» و «نام صادرکننده گواهی» داشته باشد. • ممکن است با استفاده از فیلد الحاقی 'subjectAltName' نام اختیاری در قالب دیگری برای موجودیت تعیین شود. • نام ترکیبی (DN) می‌بایست به فرم یک رشته قابل چاپ X.501 در گواهی ثبت گردد و حتماً می‌بایست مقدار داشته باشد.
سطح ۲	
سطح ۳	
سطح ۴	

۳-۱-۲ نیاز به نام‌های با معنی

جدول ۹ نیاز به نام‌های با معنی

سطح اطمینان	الزامات
سطح ۱	محتوای هر کدام از فیلدهای صادرکننده (Issuer) و مالک (Subject) گواهی می‌بایست با نام شناسایی موجودیت مرتبط باشد. ضمن اینکه فیلدهای مذکور می‌بایست منطبق با سند جامع پروفایل‌های زیرساخت کلید عمومی کشور مقداردهی گردد.
سطح ۲	
سطح ۳	
سطح ۴	

۳-۱-۳ استفاده از نام‌های مستعار و غیر واقعی برای مالکان گواهی

برای گواهی‌های صادرشده در سطوح مختلف اطمینان نمی‌توان از نام‌های مستعار و غیر واقعی استفاده نمود.

---

[1] Subject Name

[2] Issuer Name

۳-۱-۴ قواعد تفسیر قالب‌های مختلف نام‌ها

تعریف نشده است.

۳-۱-۵ یکتایی نام‌ها

یکتایی نام در مراکز صدور گواهی می‌بایست رعایت شود. کلیه مراکز صدور گواهی می‌بایست از نام‌های ترکیبی X.501 مورد تایید شورا، استفاده نمایند. تخصیص نام‌های ترکیبی به مالکان گواهی، وظیفه مراکز صدور گواهی می‌باشد. مراکز صدور گواهی می‌توانند از شماره سریال یا اطلاعات دیگری برای حفظ یکتایی نام ترکیبی استفاده کنند. چگونگی اعمال یکتایی در نام‌گذاری گواهی‌های الکترونیکی در «سند جامع پروفایل‌های زیرساخت کلید عمومی کشور» توصیف شده است.

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

مراکز صدور گواهی نباید برای نامی که مراجع قانونی آن را سوء استفاده از علامت تجاری سازمان دیگر تشخیص داده است، گواهی صادر نمایند.

۳-۲ هویت‌شناسی اولیه

۳-۲-۱ روش اثبات مالکیت کلید خصوصی

از آنجایی که در زیرساخت کلید عمومی کشور به طور معمول عملیات تولید کلید توسط درخواست‌کننده گواهی صورت می‌گیرد، درخواست‌کننده می‌بایست ثابت نماید که آیا کلید خصوصی او متناظر با کلید عمومی ارائه شده برای دفتر ثبت نام و یا مرکز صدور گواهی است یا خیر. چنانچه عملیات تولید کلید توسط دفتر ثبت نام صورت گیرد، در این حالت نیز می‌بایست تناظر بین کلید عمومی موجود در درخواست با کلید خصوصی تولید شده، برای مرکز صدور گواهی احراز گردد.

جدول ۱۰ روش اثبات مالکیت کلید خصوصی

سطح اطمینان	الزامات
سطح ۱	قبل از صدور گواهی، کاربران نهایی (جهت ارائه درخواست صدور گواهی به مراکز میانی) و مراکز صدور گواهی میانی (جهت ارائه در خواست صدور گواهی مراکز میانی به مرکز صدور گواهی بالادستی) می‌بایست مالکیت کلید خصوصی خود را اثبات نمایند. فرآیند اثبات مالکیت کلید خصوصی مراکز میانی و احراز آن توسط مرکز دولتی ریشه، باید منطبق با استاندارد PKCS#10 صورت پذیرد. کلیه مراکز میانی در دستورالعمل اجرایی خود باید روش اثبات مالکیت کلید خصوصی متقاضیان گواهی را تعیین نمایند.
سطح ۲	
سطح ۳	
سطح ۴	

۳-۳ شناسایی سازمان‌ها

سازمان‌ها جهت دریافت گواهی سازمانی که به یک شخص به نیابت از سازمان داده می‌شود، می‌بایست درخواست گواهی را از طریق فرد نماینده و به صورت حضوری به دفتر ثبت نام ارائه نمایند. بر اساس بخش ۱-۴-۱ و سند جامع پروفایل‌های زیرساخت کلید عمومی کشور، گواهی‌هایی که در حال حاضر می‌تواند برای سازمان‌ها صادر شود عبارتند از گواهی‌های مهر سازمانی، گواهی Code Signing، گواهی سرور، گواهی رمزنگاری و گواهی‌های وابسته به مراکز صدور گواهی.

درخواست گواهی بنام یک سازمان می‌بایست شامل نام، نشانی اقامتگاه و اسناد حقوقی و رسمی سازمان برای اثبات وجود سازمان باشد. دفتر ثبت نام علاوه بر بررسی صحت این موارد، هویت فرد نماینده سازمان، مجاز بودن فرد مذکور به نمایندگی سازمان و مدارک اثبات وابستگی او به سازمان را نیز می‌بایست بررسی نمایند؛ همچنین احراز هویت شخص نماینده می‌بایست مطابق بخش ۳-۳-۱ و ۳-۳-۳ انجام گیرد.

دفاتر ثبت نام یا مراکز میانی می‌بایست نسخه‌ای از نوع و جزئیات شناسایی مورد استفاده در احراز هویت سازمان و تاریخ احراز هویت را مطابق با بخش ۵-۵-۲ بایگانی نمایند.

۳-۳-۱ احراز هویت افراد

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

قبل از ثبت و ارسال درخواست به مرکز میانی، مراکز میانی یا دفاتر ثبت نام می‌بایست منطبق با نظام شناسایی که در ادامه توصیف می‌شود، هویت فرد را شناسایی نمایند.

جهت صدور گواهی در کلیه سطوح اطمینان، در هر دو حالت احراز هویت حضوری و غیرحضوری، رعایت موارد زیر توسط مراکز میانی الزامی است:

- می‌بایست صحت اطلاعات هویتی ارائه شده (به‌ویژه نام، نام خانوادگی و کد ملی) با استفاده از پایگاه‌های اطلاعاتی معتبر مربوطه بررسی شود.
- می‌بایست صحت اطلاعات هویتی شخص حقوقی با استفاده از پایگاه‌های اطلاعاتی معتبر مربوطه بررسی شود.
- می‌بایست استعلام‌های لازم جهت اطمینان از در قید حیات بودن متقاضی از پایگاه‌های اطلاعاتی معتبر مربوطه انجام گیرد.
- می‌بایست با استفاده از پایگاه‌های اطلاعاتی معتبر از مالکیت سیم‌کارت متناظر با شماره همراه ارائه شده توسط متقاضی اطمینان حاصل نماید.

- در صورت استفاده از سایر خصوصیات و اقلام اطلاعاتی در احراز هویت افراد، که با توجه به نوع فعالیت در حوزه‌های متفاوت قابل تعریف خواهد بود، لازم است صحت این اطلاعات نیز با استفاده از پایگاه‌های اطلاعاتی معتبر مربوطه بررسی شوند.

سایر الزامات مربوط به نحوه شناسایی افراد در سطوح مختلف اطمینان به تفکیک هر سطح در جدول ۱۱ توصیف شده است.

جدول ۱۱ نحوه شناسایی افراد

سطح اطمینان	نحوه شناسایی
سطح ۱	الزامات هویت‌شناسی جهت درخواست گواهی سطح اول، برای اشخاص وابسته[۱] و غیر وابسته[۲] به شرح زیر می‌باشد: • نیازی به احراز هویت حضوری وجود ندارد ولی می‌بایست به روش مناسب اطمینان حاصل نمایند که اطلاعات هویتی از طرف شخص غیر مجاز ارائه نمی‌گردد. برای این منظور استفاده از مشخصات بایومتریک و کنترل زنده بودن[۳] و حاضر بودن فرد[۴] با روشهایی مانند کنترل کاربر میز امداد[۵] یا استفاده از الگوریتمهای هوش مصنوعی با درصد اطمینان بالا الزامی است؛ • ارائه تصویر الکترونیکی یک نوع مدرک شناسایی معتبر عکس‌دار.
سطح ۲	الزامات هویت‌شناسی جهت درخواست گواهی سطح دوم، برای اشخاص وابسته و غیر وابسته به شرح زیر می‌باشد: • به‌صورت حضوری و ارائه ۲ نوع مدرک شناسایی معتبر که حداقل یکی از آنها عکس‌دار باشد به اضافه مدارک لازم دیگر که با توجه به نوع فعالیت در حوزه‌های متفاوت قابل تعریف خواهد بود. • 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 می‌تواند همراه با امضای الکترونیکی یک فرم درخواست گواهی، از طریق کلید متناظر با گواهی قبلی و به صورت غیرحضوری صورت پذیرد؛ در این حالت فرآیند شناسایی درخواست‌کننده گواهی، در دستورالعمل اجرایی مرکز میانی باید توصیف گردد.
سطح ۳	اشخاص وابسته: به صورت حضوری و ارائه ۲ نوع مدرک شناسایی معتبر و حداقل کسب امتیاز ۱۰۰
	اشخاص غیر وابسته: به صورت حضوری و ارائه ۲ نوع مدرک شناسایی معتبر عکس‌دار به همراه شناسایی بایومتریک[۶] صرفاً توسط شخص حقیقی اصیل (مشخصات بایومتریک اشخاصی که به نمایندگی اقدام می‌کنند قابل استناد نمی‌باشد.)

[۱] اشخاص وابسته به یک سازمان (Affiliated Individuals)

[۲] اشخاص حقیقی مستقل (Non-Affiliated Individuals)

[3] Liveness Detection

[4] Proof of Presense

[5] Help Desck

[۶] فرآیند شناسایی بایومتریک به‌کارگرفته شده توسط مراکز صدور گواهی می‌بایست در دستورالعمل اجرایی این مراکز تشریح شده و مورد تأیید مرکز ریشه قرار گیرد.

سطح اطمینان	نحوه شناسایی
سطح ۴	اشخاص وابسته: به صورت حضوری و ارائه ۲ نوع مدرک شناسایی معتبر و حداقل کسب امتیاز ۱۵۰

جدول ۱۲ نحوه امتیازدهی به افراد

شاخص		امتیاز	مثال
سابقه کار مورد قبول دستگاه		۱ تا ۲ سال ۱۰ امتیاز	۱۰۰ امتیاز = دو مدرک (۸۰) + ۲ سال سابقه (۲۰)
		۲ تا ۴ سال ۲۰ امتیاز	
		۴ تا ۷ سال ۴۰ امتیاز	۱۰۰ امتیاز= دو مدرک (۸۰) + نوع قرارداد (۱۰) + ۱ سال سابقه (۱۰)
		۷ تا ۱۰ سال ۶۰ امتیاز	
		۱۰ سال به بالا: ۷۰ امتیاز	۱۵۰ امتیاز= دو مدرک (۸۰) + عنوان شغلی: مدیر (۵۰) + ۳ سال سابقه (۲۰)
عنوان شغلی		مدیرکل/ مدیر عامل به بالا ۵۰ امتیاز	
نوع قرارداد		رسمی و پیمانی ۱۰ امتیاز (این شاخص فقط برای ارگان‌های دولتی قابل اعمال می‌باشد)	۱۵۰ امتیاز= دو مدرک (۸۰) + احراز هویت بایومتریک (۲۰) + ۵ سال سابقه (۴۰) + نوع قرارداد (۱۰)
حداکثر ۲ مدرک	شناسنامه	۴۰ امتیاز	
	کارت ملی	۴۰ امتیاز	۱۵۰ امتیاز= دو مدرک (۸۰) +۱۰ سال سابقه (۷۰)
	گذرنامه	۲۰ امتیاز	
	گواهینامه	۲۰ امتیاز	
شناسایی بایومتریک		۲۰ امتیاز	

دفاتر ثبت نام یا مراکز میانی می‌بایست نسخه‌ای از نوع و جزئیات شناسایی مورد استفاده در احراز هویت شخص و شواهد دال بر صحت این اطلاعات را به همراه تاریخ احراز هویت را مطابق با الزامات بخش ۵-۵-۲ برای او نگهداری نمایند.

کلیه مراکز میانی می‌بایست به طور دقیق و شفاف فرایند احراز هویت اشخاص و مدارک مورد نیاز جهت شناسایی آن‌ها را به تفکیک سطوح در دستورالعمل اجرایی گواهی الکترونیکی خود، تشریح نمایند.

۳-۳-۱-۲ شخصی به نمایندگی از شخص دیگر درخواست گواهی نماید

یک فرد می‌تواند درخواست گواهی خود را از طریق فرد دیگری با اعطای نمایندگی رسمی ارائه نماید. قبل از ثبت و ارسال درخواست به مرکز میانی، دفتر ثبت نام می‌بایست مطابق با بخش ۳-۳-۱-۱، هویت شخص اصیل و نماینده را شناسایی نماید. علاوه بر این، دفتر ثبت نام می‌بایست اطمینان حاصل نماید که فرد نماینده از سوی فرد درخواست‌کننده، مجاز به ارائه درخواست گواهی به نیابت از وی می‌باشد. برای این منظور، مجوزی که به فرد نماینده از سوی شخص درخواست کننده گواهی اعطا می‌شود، می‌بایست بررسی و تصدیق شود.

اطلاعات مربوط به روش و جزئیات شناسایی مورد استفاده در تأیید هویت شخص اصیل و نماینده، می‌بایست توسط مرکز میانی یا دفتر ثبت نام ثبت و نگه‌داری شوند. همچنین مراکز میانی می‌بایست در دستورالعمل اجرایی گواهی الکترونیکی خود به طور دقیق و شفاف، فرایند شناسایی برای حالتی که ارائه درخواست گواهی از سوی نماینده شخص متقاضی صورت می‌گیرد را شرح و مدارک شناسایی مورد نیاز را تعیین نمایند.

۳-۳-۱-۳ *شخصی برای نقش سازمانی خود درخواست گواهی نماید*

قبل از ثبت و ارسال درخواست به مرکز میانی، دفتر ثبت نام می‌بایست مطابق با بخش ۳-۳-۱-۱، هویت فردی که درخواست صدور گواهی برای نقش سازمانی خود دارد را شناسایی نماید. علاوه بر این، دفتر ثبت نام می‌بایست از اینکه فرد برای این نقش سازمانی مجاز می‌باشد، اطمینان حاصل نماید.

مدارک مربوط به احراز نقش سازمانی درخواست کننده گواهی می‌بایست مطابق با بخش ۵-۵-۲، توسط دفتر ثبت نام یا مرکز صدور گواهی میانی نگهداری گردند.

کلیه مراکز میانی می‌بایست در دستورالعمل اجرایی گواهی الکترونیکی خود به طور دقیق و شفاف مدارک مورد نیاز جهت احراز نقش سازمانی درخواست کننده گواهی را تعیین نمایند.

۳-۳-۲ اطلاعات تصدیق نشده مالکان گواهی

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

- واحد سازمانی (OU): سطح اطمینان اول و دوم؛
- اطلاعات دیگری که به عنوان اطلاعات تصدیق نشده در گواهی تعیین شده باشند.

۳-۳-۳ اعتبارسنجی مرجع ذیصلاح

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

- موجودیت سازمان را از طریق پایگاه‌داده یا اسناد و مدارک رسمی و قانونی ارائه‌شده پیگیری نماید؛
- برای سطح اطمینان ۲ حداقل با استعلام تلفنی از سازمان مربوطه صلاحیت شخص درخواست کننده را احراز نماید.
- برای سطوح اطمینان ۳ و ۴ با استعلام کتبی از سازمان مربوطه، صلاحیت شخص درخواست کننده را احراز نماید.

۳-۳-۴ شرایط تعامل با سایر نهادها

در حال حاضر تعریف نشده است.

۳-۴ شناسایی و احراز هویت برای درخواست‌های تجدید کلید[1]

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، متناظر با کلید خصوصی، شماره سریال و احتمالاً یک مدت اعتبار متفاوت می‌باشد.

اشخاص و سازمان‌هایی که قصد تجدید کلید دارند، می‌بایست درخواست گواهی جدید خود را به دفتر ثبت نام تحویل دهند و دفتر ثبت نام احراز هویت درخواست‌کننده را مطابق با بخش‌های ۳-۴-۱ و ۳-۴-۲ انجام می‌دهد. درخواست‌های تجدید کلید می‌بایست ثبت و نگهداری گردند.

۳-۴-۱ فرایند عادی شناسایی و احراز هویت برای تجدید کلید

شناسایی و احراز هویت برای تجدید کلید عبارت است از بررسی و تصدیق اینکه شخص یا سازمانی که درخواست تجدید کلید گواهی را داده، مالک واقعی گواهی و یا یک نماینده مجاز برای مالک گواهی می‌باشد. فرایند درخواست تجدید کلید و شناسایی مالک گواهی یا نماینده وی مطابق با بخش ۳-۲ می‌باشد با این تفاوت که دفتر ثبت نام می‌بایست 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 نماید. در صورت تطابق، دفتر ثبت نام می‌بایست درخواست تجدید کلید را تأیید نموده و جهت پردازش، به مرکز میانی ارسال نماید.

۳-۴-۲ شناسایی و احراز هویت برای تجدید کلید پس از ابطال گواهی

تعریف نشده است.

۳-۵ 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 ۳-۳ و ۳-۳-۱ صورت می‌گیرد با این تفاوت که دفتر ثبت نام می‌بایست اطلاعات و مدارک ارائه‌شده توسط درخواست‌کننده

---

[1] Re-Key

را با اطلاعات و مدارک موجود در پایگاه‌داده و بایگانی خود که هنگام درخواست صدور گواهی برای شخص یا سازمان مربوطه ثبت گردیده، مقایسه نماید. در صورت تطابق، دفتر ثبت نام می‌بایست درخواست ابطال گواهی را تأیید نموده و جهت پردازش، به مرکز میانی ارسال نماید. درخواست‌های ابطال گواهی می‌بایست ثبت و نگهداری شوند.

۴ الزامات عملیاتی چرخه حیات گواهی

۴-۱ درخواست گواهی

درخواست کننده گواهی و دفتر ثبت نام می‌بایست مراحل زیر را هنگام ارائه درخواست گواهی، انجام دهند:

- شناسایی مالک گواهی (طبق بخش ۳-۲)
- ثبت اطلاعات اساسی درخواست‌کننده گواهی مطابق با دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی؛
- تولید زوج کلید و ارائه کلید عمومی به همراه هر درخواست گواهی؛
- حصول اطمینان از ارتباط کلید عمومی ارائه شده با کلید خصوصی نزد مالک گواهی (طبق بخش ۳-۲-۱)

مراحل فوق ممکن است با هر ترتیبی که مناسب است و امنیت را مختل نمی‌نماید انجام شود، اما همه آن‌ها می‌بایست قبل از صدور گواهی الکترونیکی کامل شود. فرایند درخواست گواهی مالکان گواهی در دستورالعمل اجرایی گواهی الکترونیکی مراکز میانی مربوطه می‌بایست ارائه شود.

درخواست مراکز میانی برای گواهی خود می‌بایست از طریق اطلاعات تماس مندرج در بخش ۱-۵-۲ و بر اساس مستند «راهنمای درخواست تأسیس مراکز میانی» منتشر شده در سایت مرکز دولتی ریشه صورت گیرد. متقاضیان تأسیس مراکز میانی می‌بایست دستورالعمل اجرایی گواهی الکترونیکی خود را بر مبنای سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و چارچوب دستورالعمل اجرایی (RFC3647)، به مرکز دولتی ریشه ارائه نمایند. دستورالعمل اجرایی ارائه شده به همراه اسناد مرتبط در مرکز دولتی ریشه مورد ارزیابی، تأیید و تصویب قرار می‌گیرد. در صورت تأیید و تصویب دستورالعمل اجرایی گواهی الکترونیکی مراحل تأسیس مرکز میانی ادامه خواهد یافت. مراکز میانی تنها با مجوز کتبی مرکز دولتی ریشه و بعد از صدور گواهی توسط مرکز صدور گواهی بالادستی، مجاز به صدور گواهی‌هایی حاوی شناسه سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور می‌باشند.

۴-۱-۱ موجودیت‌های مجاز جهت ارائه درخواست گواهی

افرادی که ممکن است یک درخواست گواهی را ارائه نمایند عبارتند از:

- شخصی که می‌خواهد مالک گواهی شود؛

- نماینده مجاز برای یک سازمان یا موجودیت (جهت ارائه درخواست گواهی برای شخص دیگر، نقش سازمانی، تجهیزات یا برنامه کاربردی و یا ارائه درخواست گواهی‌های سازمانی)؛
- نماینده مجاز برای مرکز میانی جهت ارائه درخواست گواهی از مرکز صدور گواهی بالادستی.

۴-۱-۲ فرایند ثبت نام و مسئولیت‌ها

هر شخص یا سازمانی که قصد درخواست صدور یک گواهی از یک مرکز صدور گواهی را دارد، می‌بایست حداقل مراحل زیر را طی نماید:

- درخواست کننده گواهی می‌بایست پس از تولید زوج کلید، درخواست گواهی را همراه با اثبات مالکیت کلید خصوصی منطبق با بخش ۳-۲-۱ به مرکز صدور گواهی یا دفتر ثبت نام تحویل دهد و یا فرایند تولید کلید را به مرکز صدور گواهی یا دفتر ثبت نام مربوطه واگذار نماید؛
- مدارک و اطلاعات لازم جهت ارائه یک درخواست گواهی را مطابق با بخش ۳-۲ به دفتر ثبت نام ارائه نماید؛
- امضای یک توافق‌نامه در مورد شرایط حاکم بر استفاده از گواهی.

۴-۲ بررسی درخواست گواهی

مراکز میانی می‌بایست در دستورالعمل اجرایی گواهی، فرایندها و الزامات درخواست صدور گواهی را بیان نمایند. همین‌طور می‌بایست اطلاعات مورد نیاز برای ثبت درخواست و فرایند درخواست گواهی را به اطلاع درخواست کنندگان برسانند.

۴-۲-۱ اجرای فرایندهای شناسایی و احراز هویت

دفتر ثبت نام یا مرکز صدور گواهی می‌بایست کلیه اطلاعات مورد نیاز ارائه‌شده توسط درخواست کننده گواهی جهت صدور یک گواهی توسط مرکز صدور گواهی را مطابق با بخش ۳-۲، شناسایی و احراز هویت نماید.

۴-۲-۲ تأیید یا رد درخواست‌های گواهی

چنانچه احراز هویت درخواست‌کننده گواهی منطبق با بخش ۳-۲ با موفقیت و به طور کامل انجام گیرد، دفتر ثبت نام می‌بایست درخواست گواهی را تأیید نماید. ضمناً دفتر ثبت نام می‌بایست در صورت وقوع حداقل یکی از شرایط ذیل درخواست گواهی را رد نماید:

- هویت‌شناسی درخواست‌کننده گواهی بر اساس مدارک تحویل داده شده و اطلاعات احراز هویت دیگر و منطبق با بخش ۳-۲ با موفقیت و به طور کامل صورت نگیرد؛

- عملیات اثبات مالکیت کلید خصوصی با موفقیت صورت نگیرد؛
- درخواست کننده گواهی توافق‌نامه شرایط حاکم بر استفاده از گواهی را نپذیرد؛
- درخواست کننده گواهی به تذکرات دفتر ثبت نام در زمان تعیین‌شده پاسخ ندهد؛

کلیه مراکز میانی می‌بایست فرایند تایید یا عدم تایید درخواست‌های گواهی را در دستورالعمل اجرایی گواهی الکترونیکی خود به طور کامل تشریح نمایند.

۴-۲-۳ مدت رسیدگی به درخواست گواهی

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

جدول ۱۳ 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.
سطح ۳	گواهی‌های کاربران نهایی حداکثر در طی مدت دو روز از زمان درخواست دفتر ثبت نام صادر می‌شوند.
سطح ۴	گواهی‌های کاربران نهایی به محض درخواست دفتر ثبت نام صادر می‌شوند.

۴-۳ صدور گواهی

۴-۳-۱ اقدامات مرکز در طول صدور گواهی

گواهی پس از تأیید نهایی درخواست گواهی از سوی مرکز صدور گواهی و یا پس از دریافت درخواست صدور گواهی از سوی دفتر ثبت نام و تصدیق امضای درخواست گواهی، صادر می‌شود.

مرکز صدور گواهی می‌بایست برای درخواست‌کننده گواهی بر اساس اطلاعات موجود در درخواست گواهی تصدیق شده، گواهی صادر نماید.

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

کلیه مراکز صدور گواهی می‌بایست پس از صدور گواهی به روشی که در دستورالعمل اجرایی آن‌ها قید می‌گردد، مالک گواهی را از صادر شدن گواهی مطلع نمایند.

مرکز دولتی ریشه پس از صدور گواهی برای یک مرکز میانی، از طریق ارسال نامه اطلاع‌رسانی، به آن مرکز اطلاع می‌دهد که گواهی او صادر شده است.

۴-۴ پذیرش گواهی

۴-۴-۱ چگونگی پذیرش گواهی

پذیرش گواهی توسط درخواست کننده گواهی به عنوان یک پیش شرط جهت استفاده از گواهی الکترونیکی است. مراکز میانی می‌بایست در دستورالعمل اجرایی گواهی الکترونیکی خود و توافق نامه تنظیم شده با درخواست کننده گواهی، فرایند پذیرش گواهی توسط درخواست‌کننده گواهی را شرح دهند. فرایند صدور، اطلاع رسانی و پذیرش بستگی به عواملی مانند مکانی که زوج کلید ایجاد می‌شود و چگونگی در دسترس قرار گرفتن گواهی برای موجودیت‌های نهایی دارد. با پذیرش یک گواهی، موجودیت نهایی تصدیق می‌نماید تمام اطلاعاتی که در گواهی الکترونیکی قید شده است، صحت دارد.

اگر گواهی به هر دلیل (مثلاً عدم انطباق اطلاعات موجود در گواهی با اطلاعات درخواستی) پذیرفته نشود، عدم پذیرش گواهی و دلایل آن می‌بایست از سوی مالک گواهی به روشی که در توافق‌نامه قید شده است، به مرکز صدور گواهی اطلاع داده شود و گواهی مذکور توسط مرکز صدور گواهی باطل گردد.

مرکز دولتی ریشه پس از صدور گواهی برای یک مرکز میانی، گواهی مذکور را به صورت حضوری و از طریق یک CD در اختیار نماینده مجاز مرکز میانی قرار می‌دهد و پذیرش این گواهی با امضای فرم پذیرش گواهی توسط نماینده مجاز مذکور صورت می‌گیرد. مرکز دولتی ریشه تنها پس از انجام فرایند پذیرش گواهی، گواهی مرکز میانی را در مخزن خود منتشر خواهد نمود.

۴-۴-۲ انتشار گواهی توسط مرکز صدور گواهی

مرکز صدور گواهی می‌بایست گواهی‌های صادر شده و پذیرفته شده از سوی مالک گواهی را از طریق مخزن منتشر نماید.

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

دفتر ثبت نام ممکن است از صدور گواهی که درخواست آن را تأیید و ثبت نموده بود، مطلع شود.

۴-۵ کاربرد گواهی و زوج کلید

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

استفاده از کلید خصوصی متناظر با کلید عمومی موجود در گواهی تنها در صورتی مجاز می‌باشد که مالک گواهی توافق‌نامه شرایط حاکم بر استفاده از گواهی و گواهی صادر شده را بپذیرد.

مالک گواهی می‌بایست گواهی را مطابق با قانون و مفاد توافق‌نامه بین مالک گواهی و مرکز صدور گواهی، سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور(CP) و دستورالعمل اجرایی مرکز میانی مربوطه (CPS) مورد استفاده قرار دهد. استفاده از گواهی نباید متناقض با فیلد KeyUsage از الحاقیه‌های[1] گواهی باشد.

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

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

در یک زیرساخت کلید عمومی از طریق گواهی‌های X.509، مشخصات یک موجودیت به کلید عمومی او پیوند داده می‌شود. یکی از مهم‌ترین قابلیت‌هایی که یک نرم‌افزار مجهز به زیرساخت کلید عمومی (PKE[2]) می‌بایست پشتیبانی نماید، فرایند اعتبارسنجی زنجیره گواهی می‌باشد. از طریق این فرایند می‌توان دریافت که به یک گواهی الکترونیکی جهت استفاده در یک نرم‌افزار خاص می‌توان اعتماد نمود یا خیر. به عبارت دیگر در این فرایند درستی پیوند بین مشخصات مالک گواهی و کلید عمومی او بررسی می‌گردد.

در یک زنجیره گواهی، هر گواهی توسط صادر کننده این گواهی امضا شده است و این زنجیره، از گواهی موجودیت نهایی تا گواهی متعلق به مرکز دولتی ریشه امتداد دارد. به عنوان مثال یک زنجیره گواهی ممکن است شامل گواهی کاربر (User) که توسط صادر کننده این گواهی (CA) امضا شده، گواهی CA که توسط صادر کننده این گواهی (Root CA) امضا شده و گواهی متعلق به مرکز دولتی ریشه صدور گواهی (Root CA) که توسط خودش امضا شده است، باشد.

Root CA $\rightarrow$ CA $\rightarrow$ User

طرف‌های اعتماد کننده می‌بایست همواره به تناسب استفاده از گواهی با اهداف و کاربردهای تعیین‌شده و عدم استفاده از گواهی در کاربردهای منع شده توسط سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و دستورالعمل اجرایی مرکز میانی توجه داشته باشند و قبل از اعتماد به یک گواهی، جهت اعتبارسنجی زنجیره گواهی می‌بایست حداقل موارد زیر را در نظر داشته باشند:

- وجود یا عدم وجود گواهی متعلق به صادر کننده گواهی مورد نظر در زنجیره گواهی می‌بایست بررسی گردد[3]؛

---

1 Extension

2 PK-Enabled

3 Name Chaning

- امضای کلیه گواهی‌های موجود در زنجیره گواهی می‌بایست اعتبارسنجی گردد[1]؛
- از گواهی می‌بایست در کاربردهای متناسب با کاربردهای تعیین‌شده در الحاقیه‌های گواهی (مثل الحاقیه KeyUsage) استفاده شود. (به عنوان مثال اگر کاربرد امضای الکترونیکی برای گواهی فعال نشده باشد، از این گواهی نباید برای تصدیق امضای مالک گواهی استفاده نمود)؛
- وضعیت (ابطال یا عدم ابطال) گواهی مالک گواهی و کلیه گواهی‌های متعلق به مراکز صدور گواهی موجود در زنجیره گواهی می‌بایست بررسی گردد. اگر هر یک از گواهی‌های موجود در زنجیره گواهی باطل شده باشد، طرف اعتماد کننده 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 گردد.

با فرض اینکه از گواهی در کاربرد مناسب استفاده می‌شود، طرف‌های اعتماد کننده می‌بایست از نرم‌افزار و یا سخت‌افزار مناسب جهت انجام عمل تصدیق امضا، اعتبارسنجی زنجیره گواهی و یا دیگر عملیات رمزنگاری وابسته به کلید عمومی استفاده کنند. این عملیات یکی از شرایط اعتماد به گواهی می‌باشد که شامل شناسایی یک زنجیره گواهی و تصدیق امضای تمام گواهی‌های موجود در زنجیره گواهی نیز می‌باشد. کلیه نرم‌افزارهای مجهز به زیرساخت کلید عمومی کشور (نرم‌افزارهای PKE) می‌بایست مورد تأیید مرکز دولتی ریشه بوده و در آزمایشگاه زیرساخت کلید عمومی کشور آزمون و ارزیابی شده باشند.

۴-۶ تمدید گواهی[2]

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.

۴-۶-۱ شرایط تمدید گواهی

تمدید یک گواهی در صورتی امکان‌پذیر است که زمان انقضای گواهی فرا نرسیده باشد، گواهی باطل نشده باشد و مجموع دوره اعتبار گواهی‌های صادر شده (مجموع دوره اعتبار گواهی جدید و قدیم) از الزامات قید شده در بخش ۶-۳-۲ پیروی نماید.

۴-۶-۲ متقاضیان تمدید گواهی

در زیرساخت کلید عمومی کشور متقاضیان تمدید گواهی می‌تواند شامل موارد زیر باشند:

---

1 Signature Chaning

2 Certificate Renewal

- مالک گواهی و یا نماینده مجاز برای او می‌تواند درخواست تمدید گواهی نماید.
- دفاتر ثبت نام (فرایند تمدید گواهی باید در دستورالعمل اجرایی مراکز میانی قید شود)

۴-۶-۳ بررسی درخواست‌های تمدید گواهی

فرایند بررسی درخواست تمدید یک گواهی مطابق با بخش ۳-۴-۱ می‌باشد.

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

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

۴-۶-۵ چگونگی پذیرش گواهی تمدید شده

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

۴-۶-۶ انتشار گواهی تمدید شده توسط مرکز

گواهی‌های جدید صادر شده که مدت اعتبار آن‌ها تمدید شده است و از سوی مالک گواهی پذیرفته شده‌اند می‌بایست از طریق مخزن منتشر شوند.

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

دفتر ثبت نام ممکن است از صدور گواهی که درخواست آن را تأیید و ثبت نموده، مطلع شود.

۴-۷ تجدید کلید گواهی[1]

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 می‌بایست قبل از فرا رسیدن زمان انقضای گواهی اقدام به تجدید کلید گواهی نماید تا استمرار استفاده از کاربردهای گواهی حفظ شود. در صورت وقوع یکی از حالت‌های زیر ممکن است یک گواهی تجدید کلید گردد:

---

[1] Certificate Re-Key

- دوره اعتبار گواهی در آستانه به پایان رسیدن باشد و بر اساس شرایط بخش ۴-۶-۱ امکان تمدید وجود نداشته باشد؛
- کلید خصوصی متناظر با گواهی الکترونیکی در خطر افشا باشد.

ارایه خدمات تجدید کلید در مراکز میانی، وابسته به امکانات مرکز میانی ذی‌ربط بوده و فرایند ارایه آن‌ها می‌بایست در دستورالعمل اجرایی گواهی الکترونیکی مربوطه درج گردد.

در فرایند تجدید کلید یک گواهی الکترونیکی متعلق به موجودیت‌های نهایی، اعمال این فرایند می‌بایست همراه با ابطال گواهی قبلی باشد. فرایند تجدید کلید برای مراکز صدور گواهی نیز در صورتی که دلیل تجدید کلید، در خطر افشا قرار گرفتن کلید باشد، باید همراه با ابطال گواهی قبلی صورت پذیرد.

۴-۷-۲ متقاضیان گواهی با کلید عمومی جدید

فقط مالک گواهی یا نماینده مجاز وی و یا نماینده 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 ۳-۴-۱ 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 ۴-۳-۲ می‌باشد.

۴-۷-۵ چگونگی پذیرش گواهی با کلید جدید

چگونگی پذیرش تجدید کلید یک گواهی مطابق با بخش ۴-۴-۱ 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 می‌بایست از طریق مخزن منتشر شوند.

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

دفتر ثبت نام ممکن است از صدور گواهی که درخواست آن را تأیید و ثبت نموده بود، مطلع شود.

۴-۸ اصلاح گواهی[1]

در حال حاضر قابل اعمال نیست.

۴-۸-۱ شرایط اصلاح گواهی

در حال حاضر قابل اعمال نیست.

۴-۸-۲ متقاضیان اصلاح گواهی

در حال حاضر قابل اعمال نیست.

۴-۸-۳ بررسی درخواست‌های اصلاح گواهی

در حال حاضر قابل اعمال نیست.

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

در حال حاضر قابل اعمال نیست.

۴-۸-۵ چگونگی پذیرش گواهی اصلاح شده

در حال حاضر قابل اعمال نیست.

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

در حال حاضر قابل اعمال نیست.

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

در حال حاضر قابل اعمال نیست.

۴-۹ ابطال و تعلیق گواهی

۴-۹-۱ شرایط ابطال

ابطال گواهی زمانی که پیوند بین مشخصات مالک گواهی و کلید عمومی گواهی اعتباری نداشته باشد، انجام می‌گردد.

---

[1] Certficate Modification

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

در صورت وقوع هر یک از موارد زیر می‌بایست مرکز میانی، ابطال گواهی خود را از مرکز دولتی ریشه و یا از مرکز صدور گواهی بالادستی خود درخواست نماید:

- کلید خصوصی مرکز میانی احتمالاً یا مطمئناً در خطر افشا باشد؛
- دیگر نیازی به گواهی نباشد. این امر ممکن است به علت خاتمه خدمات ارائه‌شده توسط مرکز میانی یا انقضای قرارداد بین مرکز میانی و مرکز میانی بالادستی باشد.

حداقل در صورت وقوع هر یک از موارد زیر مرکز دولتی ریشه و یا مرکز میانی می‌بایست اقدام به ابطال گواهی مرکز میانی زیرین خود بدون تأیید او نماید:

- در صورت ابطال گواهی مرکز دولتی ریشه و یا مرکز میانی بالادستی، کلیه گواهی‌های متعلق به مراکز میانی زیرین می‌بایست باطل شوند؛
- در صورت احراز تخلف مرکز میانی یا دفاتر ثبت نام وابسته به آن مرکز میانی از مندرجات این سند و تایید این تخلف توسط شورا؛
- محرز شدن صدور گواهی مبتنی بر اظهارات خلاف واقع اعم از عمدی و غیر عمدی مرکز میانی و تأیید آن توسط شورا؛
- درخواست ابطال از سوی مراجع قضائی ذیصلاح؛
- مرکز دولتی ریشه و یا مرکز صدور گواهی بالادستی، به فعالیت خود پایان دهد.

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 و در صورت لغو مجوز مرکز میانی می‌بایست به روش مندرج در بند (خ) ماده (۵) آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و درج در روزنامه رسمی جمهوری اسلامی ایران فهرست گواهی‌های باطله را منتشر نماید. مسئولیت جبران خسارات ناشی از ابطال گواهی مرکز میانی به مالکان گواهی صادرشده از این مرکز باید در دستورالعمل اجرایی یا در توافقنامه منعقد شده بین طرفین قید شود.

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

در صورت وقوع هر یک از موارد زیر مالک گواهی و یا نماینده مجاز وی می‌بایست ابطال گواهی را از مرکز میانی درخواست نماید:

- کلید خصوصی مالک گواهی احتمالاً یا مطمئناً در خطر افشا باشد؛

- اطلاعات موجود در گواهی (نظیر مشخصات مالک گواهی) به هر دلیلی تغییر نماید؛
- دیگر نیازی به گواهی نباشد؛ این امر ممکن است به علت توقف فعالیت یک سازمان و یا توقف فعالیت یک شخص در یک سازمان و تغییر جایگاه سازمانی مالک گواهی باشد.

مرکز صدور گواهی، گواهی مالکان گواهی را می‌بایست بدون تأیید آن‌ها در صورت بروز هر یک از شرایط زیر باطل نماید:

- در صورت استفاده غیرمجاز، جعل و در خطر افشا قرار گرفتن کلید خصوصی مرکز میانی و یا باطل شدن گواهی الکترونیکی مرکز دولتی ریشه، کلیه گواهی‌های امضاشده توسط مرکز صدور گواهی می‌بایست باطل شوند؛
- درخواست ابطال از سوی مراجع قضائی ذیصلاح؛
- تخطی مالک گواهی الکترونیکی از تعهداتش؛
- مرکز صدور گواهی به فعالیت خود پایان دهد؛
- مرکز دولتی ریشه به فعالیت خود پایان دهد؛
- در صورت فوت مالک گواهی.

کلیه مراکز صدور گواهی می‌بایست در توافق‌نامه فی‌مابین خود و مالکان گواهی، مالکان گواهی را ملزم نمایند که در صورت اطلاع یا احتمال به خطر افتادن کلید خصوصی خود در اسرع وقت مرکز مربوطه را مطلع کنند و جهت ابطال گواهی اقدام کنند.

۴-۹-۲ متقاضیان درخواست ابطال

۴-۹-۲-۱ موجودیت‌های نهایی

جدول ۱۴ موجودیت‌های مجاز به ارائه درخواست ابطال گواهی الکترونیکی

سطح اطمینان	موجودیت‌های مجاز به ارائه درخواست ابطال گواهی الکترونیکی
سطح ۱ سطح ۲ سطح ۳ سطح ۴	درخواست ابطال گواهی الکترونیکی توسط افراد زیر ارائه شود: • مالک گواهی؛ • نماینده مجاز از سوی مالک گواهی (بخش ۳-۳-۱)؛ • نماینده مجاز از یک سازمان جهت ارائه درخواست ابطال گواهی‌های سازمانی و یا گواهی یکی از پرسنل سازمان؛ • نماینده مجاز برای ابطال گواهی دفاتر ثبت نام. • مراجع قضائی ذیصلاح

۴-۹-۲-۲ *مراکز صدور گواهی الکترونیکی میانی*

موجودیت‌های مجاز جهت ارائه درخواست ابطال گواهی متعلق به مراکز میانی عبارتند از:

- نماینده مجاز مراکز میانی برای ابطال گواهی (های) این مراکز؛
- مراجع قضائی ذیصلاح؛
- شورا؛
- مرکز دولتی ریشه.

تمامی درخواست‌ها با تصویب در شورای سیاست‌گذاری قابل اجرا خواهند بود.

۴-۹-۳ فرایند رسیدگی به درخواست ابطال

هر درخواست ابطال گواهی می‌بایست منحصراً برای یک گواهی باشد و دلیل ابطال گواهی را شرح دهد ضمن اینکه این درخواست می‌بایست منطبق با بخش ۳-۵ تعیین هویت شود.

چنانچه درخواست ابطال معتبر باشد، مرکز صدور گواهی می‌بایست از طریق قرار دادن شماره سریال گواهی مورد نظر در لیست گواهی‌های باطله، اقدام به ابطال گواهی نماید. الزامات مربوط به فرایند رسیدگی به درخواست ابطال عبارت است از:

- شناسایی و احراز هویت درخواست ابطال گواهی (مطابق با بخش ۳-۵)؛
- ثبت و نگه‌داری تمام اطلاعات مربوط به درخواست؛
- به‌روز نمودن لیست گواهی‌های باطله و سرور پاسخگوی OCSP بعد از ابطال گواهی

۴-۹-۴ مهلت اعلام درخواست ابطال

چنانچه کلید خصوصی مالک گواهی احتمالاً و یا مطمئناً در خطر افشا (به عنوان مثال افشای گذرواژه پودمان رمزنگاشتی) باشد، درخواست ابطال گواهی می‌بایست در کمترین زمان ممکن ارائه گردد.

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

حداکثر زمان مجاز جهت رسیدگی به درخواست ابطال گواهی (مخصوصاً در صورت افشای کلید خصوصی) توسط مراکز صدور گواهی، در جدول زیر تعیین شده است همچنین کلیه مراکز صدور گواهی میانی می‌بایست در دستورالعمل اجرایی خود الزامات مدت زمان لازم جهت ارائه درخواست تایید شده ابطال از سمت دفتر ثبت نام به مرکز میانی را تعیین نمایند.

جدول ۱۵ مدت رسیدگی به درخواست ابطال توسط مرکز صدور گواهی

سطح اطمینان	مدت رسیدگی به درخواست ابطال توسط مرکز
سطح ۱	• چنانچه درخواست ابطال در ساعات کاری توسط مرکز صدور گواهی دریافت گردد، می‌بایست در کمتر از ۲ ساعت پس از دریافت آن، پردازش گردد. • چنانچه درخواست ابطال خارج از ساعات کاری توسط مرکز صدور گواهی دریافت گردد، می‌بایست بلافاصله در شروع روز کاری بعد، پردازش گردد.
سطح ۲	• چنانچه درخواست ابطال خارج از ساعات کاری توسط مرکز صدور گواهی دریافت گردد و روز بعدی نیز یک روز کاری نباشد، پردازش درخواست نباید بیشتر از ۲۴ ساعت طول بکشد.
سطح ۳	درخواست ابطال می‌بایست در کمتر از یک ساعت پس از دریافت آن توسط مرکز صدور گواهی پردازش گردد.
سطح ۴	درخواست ابطال می‌بایست بلافاصله پس از دریافت آن توسط مرکز صدور گواهی، پردازش گردد.

۴-۹-۶ الزامات بررسی ابطال توسط طرف‌های اعتماد کننده

طرف اعتماد کننده قبل از استفاده از گواهی می‌بایست وضعیت (ابطال یا عدم ابطال) آن را بررسی نماید. چنانچه در شرایط خاص دسترسی به اطلاعات وضعیت گواهی امکان‌پذیر نباشد، مسئولت اعتماد به گواهی بر عهده طرف اعتماد کننده می‌باشد. الزامات بررسی ابطال برای طرف اعتماد در ذیل آورده شده است.

- در فرایند اعتبارسنجی زنجیره گواهی می‌بایست وضعیت ابطال یا عدم ابطال کلیه گواهی‌های موجود در زنجیره، از طریق لیست گواهی‌های باطله متناظر با گواهی و یا از طریق پروتکل OCSP، بررسی گردد.
- صحت و تمامیت لیست (های) گواهی‌های باطله را نیز می‌بایست بررسی نماید.
- برای سطح ۴ اطلاعات مربوط به ابطال نباید جهت استفاده در دفعات بعدی ذخیره گردد[1].

مراکز صدور گواهی می‌بایست محل دریافت آخرین CRL منتشر شده (CDP[2])، و محل دسترسی به سرور پاسخگوی OCSP[3] را (در صورت پشتیبانی) جهت بررسی وضعیت گواهی در اختیار طرف اعتماد کننده قرار دهند.

۴-۹-۷ تناوب صدور لیست گواهی‌های باطل‌شده

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. اگر تحت شرایط خاصی، مرکز میانی، به‌روزرسانی

1 Cache

2 CRL Distribution Point

3 OCSP Responder

لیست گواهی‌های باطل‌شده را زودتر انجام دهد، شرایط خاص مذکور می‌بایست در دستورالعمل اجرایی ذکر شود. مرکز میانی می‌بایست از این که لیست گواهی‌های باطل شده قبلی پس از ارسال آخرین نسخه این لیست از مخزن برداشته شده‌اند، مطمئن شود.

مرکز دولتی ریشه هر ۶ ماه یک‌بار، یک لیست گواهی‌های باطله را صادر و منتشر می‌نماید. الزامات مربوط به تناوب صدور لیست گواهی‌های باطله توسط مراکز میانی در جدول زیر قید شده است:

جدول ۱۶ تناوب صدور لیست گواهی‌های باطل‌شده

سطح اطمینان	تناوب صدور لیست گواهی‌های باطل شده
سطح ۱	• نسخه به‌روز شده CRL می‌بایست حداقل هر ۷ روز صادر شود. • در صورتی که دلیل ابطال یک گواهی افشای کلید خصوصی باشد، می‌بایست حداکثر ۱ روز پس از دریافت و پردازش درخواست ابطال گواهی توسط مرکز میانی، یک نسخه به‌روز شده CRL صادر شود.
سطح ۲	• نسخه به‌روز شده CRL می‌بایست حداقل هر ۲۴ ساعت صادر شود. • در صورتی که دلیل ابطال یک گواهی افشای کلید خصوصی باشد، می‌بایست بلافاصله پس از دریافت و پردازش درخواست ابطال گواهی توسط مرکز میانی، یک نسخه به‌روز شده CRL صادر شود.
سطح ۳	• نسخه به‌روز شده CRL می‌بایست حداقل هر ۱۲ ساعت صادر شود. • در صورتی که دلیل ابطال یک گواهی افشای کلید خصوصی باشد، می‌بایست بلافاصله پس از دریافت و پردازش درخواست ابطال گواهی توسط مرکز میانی، یک نسخه به‌روز شده CRL صادر شود.
سطح ۴	• نسخه به‌روز شده CRL می‌بایست حداقل هر ۴ ساعت صادر شود. • در صورتی که دلیل ابطال یک گواهی افشای کلید خصوصی باشد، می‌بایست بلافاصله پس از دریافت و پردازش درخواست ابطال گواهی توسط مرکز میانی، یک نسخه به‌روز شده CRL صادر شود.

۴-۹-۸ حداکثر تأخیر انتشار لیست گواهی‌های باطله

به طور معمول لیست گواهی‌های باطله می‌بایست به صورت خودکار و بلافاصله پس از ابطال، تعلیق/ رفع تعلیق گواهی، در مخزن منتشر شود؛ در غیر این صورت حداکثر تأخیر مجاز بین ابطال، تعلیق/ رفع تعلیق یک گواهی (صدور لیست گواهی‌های باطل شده) و انتشار CRL در مخزن می‌بایست ۱ ساعت باشد.

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

مراکز صدور گواهی در صورت پشتیبانی از پروتکل OCSP می‌بایست دسترسی به یک سرور پاسخگوی OCSP مبتنی بر وب را برای طرف‌های اعتماد کننده فراهم آورند تا آن‌ها بتوانند برای اطلاع از وضعیت گواهی و یا جزئیات دیگر وضعیت گواهی به صورت برخط به پاسخگوی OCSP مراجعه نمایند. نشانی و نحوه دسترسی به آن نیز می‌بایست در اختیار طرف‌های اعتماد کننده قرار داده شود. چنانچه نرم‌افزار سرویس‌گیرندگان از

پروتکل OCSP جهت اطلاع از وضعیت ابطال یک گواهی استفاده می‌نماید، این نرم‌افزار نیازی به دریافت CRL و پردازش آن به‌منظور کنترل وضعیت ابطال آن گواهی ندارد.

۴-۹-۱۰ الزامات کنترل برخط وضعیت ابطال

طرف اعتماد کننده می‌بایست قبل از استفاده از گواهی، وضعیت ابطال یا عدم ابطال آن را بررسی نماید. کلیه مراکز صدور گواهی و نرم‌افزارهای PKE، در صورت پشتیبانی از پروتکل OCSP، می‌بایست جهت اطمینان از دسترس‌پذیری دائمی سرویس اعلام وضعیت گواهی، از CRL نیز پشتیبانی نمایند. چنانچه نرم‌افزار سرویس‌گیرندگان از پروتکل OCSP جهت اطلاع از وضعیت ابطال یک گواهی استفاده نماید، این نرم‌افزار نیازی به دریافت CRL و پردازش آن به منظور کنترل وضعیت ابطال آن گواهی ندارد.

۴-۹-۱۱ سایر روش‌های ممکن اعلان ابطال

چنانچه یک مرکز صدور گواهی از روش دیگری غیر از CRL و OCSP جهت اعلام وضعیت گواهی استفاده نماید، می‌بایست در دستورالعمل اجرایی خود روش مذکور را توصیف نماید.

۴-۹-۱۲ الزامات خاص در صورت افشای کلید

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

۴-۹-۱۳ شرایط تعلیق

تعلیق یک گواهی زمانی انجام می‌شود که پیوند بین مشخصات مالک گواهی و کلید عمومی گواهی در مقطعی از زمان معتبر نبوده و یا ابهامی پیرامون صحت پیوند بین اطلاعات گواهی و مالک گواهی وجود داشته باشد که تصمیم‌گیری درخصوص آن نیازمند بررسی‌های دقیق‌تر باشد، همچنین ممکن است تعلیق گواهی یک مرکز صدور گواهی به‌دلیل ضرورت توقف فعالیت‌های آن انجام شود.

تعلیق گواهی از طریق ابطال گواهی با دلیل ابطال «در انتظار»[1] انجام می‌شود.

پس از تعلیق یک گواهی این گواهی باید به لیست گواهی‌های باطل شده مرکز صدور گواهی الکترونیکی اضافه شده و تا زمان رفع تعلیق گواهی و یا منقضی شدن گواهی در لیست گواهی‌های باطل شده باقی بماند.

---

[1] On Hold

رفع تعلیق گواهی به محض رفع ابهام و اطمینان از اعتبار پیوند بین اطلاعات گواهی و مالک گواهی انجام می‌گردد. فعال‌سازی مجدد گواهی‌هایی که با دلایل دیگری باطل شده‌اند امکان‌پذیر نبوده و مراکز صدور گواهی می‌بایست سازوکارهای فنی لازم را در این خصوص فراهم نمایند.

۴-۹-۱۳-۱ شرایط تعلیق گواهی موجودیت نهایی

درصورتی‌که گواهی مشمول شرایط ابطال گواهی نباشد، گواهی موجودیت نهایی می‌تواند تعلیق شود. مسئولیت عواقب ناشی از عدم رفع تعلیق گواهی باید در دستورالعمل اجرایی مرکز صدور گواهی و توافق‌نامه با مالک گواهی مشخص شود. درصورت درخواست تعلیق گواهی توسط مراجع ذی‌صلاح قضایی و شورا، تعلیق گواهی می‌تواند بدون تأیید مالک آن انجام شود. هم‌چنین برای گواهی سازمانی در صورت درخواست سازمان مربوط به آن، تعلیق گواهی می‌تواند بدون تأیید مالک آن صورت گیرد. مراکز صدور گواهی الکترونیکی باید در دستورالعمل اجرایی خود شرایطی را که منجر به تعلیق گواهی موجودیت نهایی می‌گردد تشریح نمایند.

۴-۹-۱۳-۲ شرایط تعلیق گواهی مراکز صدور گواهی

گواهی مراکز صدور گواهی در شرایط زیر بدون درخوا ست آنها، تو سط مرکز دولتی ری شه یا مرکز صدور گواهی بالادستی تعلیق می‌شود. در این شرایط اطلاع‌رسانی لازم به مرکز صدور گواهی صورت می‌گیرد.

- در شرایطی که بنا به تشخیص مرکز دولتی ریشه، شورا و یا کمیته نظارتی شورا نیاز به توقف و جلوگیری از فعالیت مرکز میانی بدون نیاز به ابطال گواهی آن باشد؛
- در شرایطی که در آیین‌نامهٔ انضباطی مراکز صدور گواهی الکترونیکی میانی تعیین می‌شود؛
- درصورت درخواست مراجع ذی‌صلاح قضایی.

مراکز صدور گواهی می‌توانند درخواست تعلیق گواهی خود را در شرایطی به‌جز شرایط ذکر شده در بخش ۴-۹-۱ (که به ابطال گواهی منجر می‌شود) با تشریح ضرورت آن به مرکز دولتی ریشه یا مرکز گواهی بالادستی ارائه کنند. مسئولیت جبران خسارت ناشی از تعلیق گواهی مرکز صدور گواهی برای مالکان گواهی‌های صادر شده توسط مرکز صدور گواهی باید در دستورالعمل اجرایی آن مرکز و در توافق‌نامهٔ منعقد شده بین دو طرف قید شود. مرکز دولتی ریشه به محض تعلیق/رفع تعلیق گواهی مراکز صدور گواهی فهرست گواهی‌های باطله را منتشر می‌نماید. تعلیق گواهی برای گواهی مرکز دولتی ریشه اعمال نمی‌شود.

۴-۹-۱۴ متقاضیان درخواست تعلیق گواهی

۴-۹-۱۴-۱ متقاضیان تعلیق گواهی موجودیت نهایی

جدول ۱۷ موجودیت‌های مجاز به ارائه درخواست تعلیق گواهی الکترونیکی

سطح اطمینان	موجودیت‌های مجاز به ارائه درخواست تعلیق گواهی الکترونیکی
سطح ۱	درخواست تعلیق گواهی الکترونیکی میبایست توسط افراد زیر ارائه شود: • مالک گواهی؛ • نماینده مجاز از سوی مالک گواهی (بخش ۳-۳-۱)؛ • نماینده مجاز سازمان جهت ارائه درخواست تعلیق گواهی‌های سازمانی و یا گواهی یکی از پرسنل سازمان؛ • نماینده مجاز برای تعلیق گواهی دفاتر ثبت نام؛ • مراجع قضائی ذیصلاح
سطح ۲	
سطح ۳	
سطح ۴	

۴-۹-۱۴-۲ متقاضیان تعلیق گواهی مراکز صدور گواهی

تنها موجودیت‌های زیر مجاز به ارائه درخواست تعلیق گواهی مراکز صدور گواهی هستند.

- نماینده مجاز مرکز صدور گواهی؛
- مراجع قضائی ذی‌صلاح؛
- مرکز دولتی ریشه؛
- کمیتهٔ نظارتی شورا؛
- شورا.

۴-۹-۱۵ فرایند رسیدگی به درخواست تعلیق

درصورت تصمیم شورا و یا کمیته نظارتی شورا به تعلیق گواهی مرکز صدور گواهی، تعلیق اجرا می‌شود. درصورتی‌که درخواست تعلیق گواهی توسط مراجع ذی‌صلاح قضایی ارائه شود، این درخواست در کمیتهٔ نظارتی شورا بررسی شده و در صورت تأیید، تعلیق اجرا می‌شود.در صورت ارائه درخواست تعلیق گواهی توسط مرکز صدور گواهی، مرکز دولتی ریشه آن را بررسی کرده و چنانچه مورد تأیید باشد و در صورت تأیید کمیتهٔ نظارتی شورا، تعلیق گواهی اجرا می‌شود.

مراکز صدور گواهی باید شرایط و مقتضیات درخواست تعلیق گواهی و فرایند رسیدگی به آن را در دستورالعمل اجرایی خود ذکر کنند. دفاتر ثبت‌نام و موجودیت‌های نهایی می‌بایست به شیوه‌ای که در دستورالعمل اجرایی

مرکز صدور گواهی تعیین می‌شود، درخواست تعلیق گواهی خود را به مرکز صدور گواهی ارائه کند. مرکز صدور گواهی در صورت تأیید درخواست تعلیق گواهی دفتر ثبت‌نام، باید در فاصلهٔ زمانی ذکر شده در دستورالعمل اجرایی صدور گواهی خود، تعلیق گواهی را اجرا کند.

ارائه درخواست رفع تعلیق باید به شیوه‌ای که در دستورالعمل اجرایی صدور گواهی مرکز صدور گواهی تعیین می‌شود، صورت گیرد. مرکز صدور گواهی در صورت تأیید درخواست رفع تعلیق گواهی، باید در فاصلهٔ زمانی ذکر شده در دستورالعمل اجرایی صدور گواهی خود تعلیق گواهی را اجرا کند.

اطلاع‌رسانی دربارهٔ تعلیق/ رفع تعلیق گواهی باید منطبق با دستورالعمل اجرایی مرکز صدور گواهی صورت گیرد.

۴-۹-۱۶ محدودیت‌های دوره تعلیق

گواهی مراکز صدور گواهی حداکثر تا زمانی‌که در زمان تأیید تعلیق گواهی توسط کمیتهٔ نظارتی شورا تعیین می‌شود، معلق می‌ماند و درصورتی‌که درخواست رفع تعلیق تا پیش از فرا رسیدن زمان تعیین شده ارائه نشود گواهی باطل می‌گردد.

درصورت ارائه درخواست رفع تعلیق تا پیش از فرا رسیدن زمان تعیین شده، و در صورت تأیید این درخواست تو سط مرکز دولتی ری شه و کمیته نظارتی شورا رفع تعلیق اجرا می شود. در صورت عدم تأیید درخوا ست، گواهی باطل می‌شود.

در صورتی که درخوا ست رفع تعلیق دریافت نشود، مراکز صدور گواهی می‌توانند گواهی را تا زمان انق ضای آن در حالت معلق نگه دارند یا پس از بازهٔ زمانی مشخصی که در دستورالعمل اجرایی و توافق‌نامه با مالک گواهی/دفاتر ثبت‌نام ذکر می‌شود، آن را باطل کند. ابطال گواهی در این رویه می‌بایست به‌گونه‌ای صورت گیرد که مرکز صدور گواهی اطمینان حا صل نماید که گواهی بین حالت معلق و باطل شده در حالت معتبر قرار نگیرد. رویه مورد استفاده توسط مرکز صدور گواهی باید در دستورالعمل اجرایی آن مشخص شود.

۴-۱۰ خدمات وضعیت گواهی

مراکز صدور گواهی حداقل موظف به اعلام و انتشار وضعیت گواهی‌ها از طریق لیست گواهی‌های باطله می‌باشند.

۴-۱۰-۱ ویژگی‌های عملیاتی

آخرین نسخه به‌روز شده لیست گواهی‌های باطله می‌بایست از طریق مخزن مراکز صدور گواهی قابل دریافت باشد؛ همچنین طرف‌های اعتماد کننده می‌توانند از طریق نرم‌افزارهایی که تولید و ارسال یک درخواست

OCSP[1] و همچنین دریافت و اعتبارسنجی یک پاسخ OCSP[2] را مطابق با RFC2560[3] و به‌روزرسانی‌های بعدی آن پشتیبانی می‌نمایند، از خدمات اعلام برخط وضعیت گواهی استفاده نمایند.
ویژگی‌های عملیاتی لیست گواهی‌های باطله در بخش ۷-۲ قید شده است؛ همچنین ویژگی‌های عملیاتی خدمات اعلام برخط وضعیت گواهی در بخش ۷-۳ قید شده است.

۴-۱۰-۲ دسترس‌پذیری خدمت

سرویس‌های ارائه وضعیت گواهی در طول عمر آن گواهی می‌بایست همواره در دسترس باشند.

۴-۱۰-۳ ویژگی‌های اختیاری

خدمات اعلام برخط وضعیت گواهی (OCSP) یک مشخصه اختیاری در ارائه خدمات اعلام وضعیت گواهی می‌باشد که فقط توسط نرم‌افزارهایی که از OCSP (منطبق با RFC2560 و به‌روزرسانی‌های بعدی آن) پشتیبانی می‌نمایند، قابل استفاده است.

۴-۱۱ پایان اشتراک

کلیه مراکز صدور گواهی تنها در صورت وقوع یکی از شرایط زیر می‌توانند به ارائه خدمات گواهی الکترونیکی برای مالک گواهی پایان دهند:

- با منقضی شدن گواهی بدون اینکه مجدداً 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[4]

در حال حاضر قابل اعمال نیست.

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

تعریف نشده است.

---

1 OCSP Request

2 OCSP Response

3 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

4 Key escrow and recovery

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

قابل اعمال نیست.

۵ کنترل‌های امکانات، تجهیزات، مدیریتی و عملیاتی

۵-۱ کنترل‌های فیزیکی

تأسیسات مرکز صدور گواهی می‌بایست دارای تجهیزاتی مختص به فعالیت‌های مرکز صدور گواهی باشند و نباید فعالیت‌های غیر مرتبط با وظایف مرکز صدور گواهی انجام دهند.

استفاده غیرمجاز از تجهیزات مرکز صدور گواهی و دفتر ثبت نام ممنوع می‌باشد. کنترل‌های امنیت فیزیکی می‌بایست به منظور حفاظت از نرم‌افزارها و سخت‌افزارهای این مراکز از دسترسی غیرمجاز، سرقت و خسارت اجرا شوند.

۵-۱-۱ ساختمان و محل سایت

عملیات مرکز صدور گواهی و دفتر ثبت نام می‌بایست در محیطی انجام شود که از لحاظ فیزیکی محافظت‌شده باشد، طوری که از هرگونه استفاده، دسترسی، افشای غیرمجاز اطلاعات حساس جلوگیری و در صورت بروز، شناسایی شود. برای این منظور، مکان سایت می‌بایست بر اساس یک سری ملزومات امنیتی انتخاب شود. چنین ملزوماتی بر پایه تفکیک برقراری لایه‌های امنیتی فیزیکی می‌باشد. منظور از لایه امنیتی فیزیکی یک درب یا مدخل قفل شده همراه با کنترل دسترسی می‌باشد که موجب اعمال کنترل دسترسی اجباری برای اشخاص می‌شود.

لایه‌های امنیتی متوالی به ترتیب دسترسی محدودتر و امنیت فیزیکی بیشتری در مقابل ورود و دسترسی غیرمجاز فراهم می‌آورند. هر لایه امنیتی فیزیکی لایه داخلی بعدی را در خود محصور می‌نماید و هر لایه امنیتی درونی می‌بایست به صورت کامل در لایه امنیتی بیرونی خود قرار گیرد و نمی‌تواند با سطح خارجی لایه امنیتی بیرونی (محیط) دیوار مشترک داشته باشد. بیرونی‌ترین لایه امنیتی، دیوار بیرونی، کف و سقف ساختمان می‌باشد. حداقل لایه‌های امنیتی فیزیکی مورد نیاز برای مرکز داده CA، سه تا چهار لایه امنیتی بسته به معماری سایت آن مرکز می‌باشد.

مراکز میانی می‌بایست در دستورالعمل اجرایی گواهی خود، رویه اعمال شده در ساختمان و مکان سایت خود را جهت برآورده سازی الزامات این بخش، به تفصیل شرح دهند.

۵-۱-۲ دسترسی فیزیکی

دسترسی به لایه‌های امنیت فیزیکی می‌بایست قابل ثبت، بازرسی و کنترل بوده تا هر لایه امنیتی تنها توسط پرسنل مجاز قابل دسترس باشد.

تجهیزات دفتر ثبت نام نیز می‌بایست زمانی که پودمان رمزنگاشتی نصب و فعال می‌شود از دسترسی غیرمجاز محافظت شوند.

اطلاعات فعال‌ساز که برای دسترسی و فعال کردن تجهیزات و پودمان‌های رمزنگاشتی مورد استفاده در مرکز صدور گواهی و دفاتر ثبت نام، بکار می‌روند، می‌بایست زمانی که استفاده نمی‌شوند، به صورت امن و همراه با کنترل دسترسی نگهداری شود.

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

- 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؛

لازم به ذکر است که در فرم مذکور، می‌بایست شرحی از اقدامات انجام شده آورده شود؛ در ضمن هر تغییر اعمال شده در سیستم‌ها و تجهیزات توسط متصدی می‌بایست به حالت پایدار باز گردد.

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

۵-۱-۳ تهویه هوا و منبع تغذیه برق

دستگاه‌های الکترونیکی تجهیزات امنیتی مراکز صدور گواهی و دفاتر ثبت نام، می‌بایست به صورت پیوسته تغذیه شوند تا دسترسی مداوم به آن‌ها تضمین شود. همچنین، این تجهیزات امنیتی می‌بایست به سیستم‌های تهویه مطبوع، جهت کنترل دما و رطوبت مجهز باشند.

۵-۱-۴ جلوگیری از آب‌گرفتگی

تجهیزات مراکز صدور گواهی می‌بایست طوری نصب شوند که در معرض خطر آب‌گرفتگی نباشند. برای مثال، این تجهیزات می‌توانند روی میزها و یا در مکان‌های مرتفع دیگر قرار گیرند. همچنین می‌بایست در نواحی مشکوک به نشت آب، حسگرهای رطوبتی نصب شود. اشخاصی که در مراکز صدور گواهی مسئولیت وسایل کنترل آتش را دارند نیز می‌بایست دقت کنند که این وسایل درست عمل کنند و از نفوذ آب به نواحی خارج از محدوده آتش پیش‌گیری کنند.

۵-۱-۵ پیش‌گیری و محافظت در مقابل آتش

مراکز صدور گواهی می‌بایست جهت پیشگیری از آتش‌سوزی و مقابله با آن، اقدامات لازم را به عمل آورند و تجهیزات لازم فراهم شود.

دستورالعملی در مورد شیوه ترمیم آتش‌سوزی می‌بایست به طرح ترمیم خرابی مراکز صدور گواهی الکترونیکی اضافه شود.

۵-۱-۶ حفاظت از رسانه‌های ذخیره‌سازی

رسانه‌های ذخیره‌سازی می‌بایست در برابر آب، آتش سوزی، الکترومغناطیس و دیگر عوامل محیطی محافظت شوند.

مراکز صدور گواهی و دفاتر ثبت نام می‌بایست از اقدامات حفاظتی برای کشف و جلوگیری از دسترسی، افشا یا استفاده غیرمجاز از رسانه‌های ذخیره سازی، استفاده کنند. رسانه‌های حاوی اطلاعات بازرسی امنیتی، بایگانی‌ها یا اطلاعات پشتیبانی می‌بایست در مکانی جدا از تجهیزات مرکز صدور گواهی نگهداری شوند.

۵-۱-۷ انهدام ضایعات

مرکز صدور گواهی می‌بایست مطمئن باشد که کلیه وسایل حاوی اطلاعات حساس در صورت عدم استفاده، می‌بایست طوری از بین بروند که بازیابی اطلاعات آن‌ها ممکن نباشد. کارکنان مرکز صدور گواهی می‌بایست دلیل تخریب اطلاعات حساس را ذکر کنند.

۵-۱-۸ نسخه پشتیبان خارج از سایت

نسخه‌های پشتیبان که برای ترمیم خرابی سیستم تهیه می‌شوند و شامل اطلاعات حساس می‌باشند، می‌بایست طبق برنامه منظمی مطابق با بخش ۵-۵-۲ ایجاد شوند و حداقل یک نسخه پشتیبان می‌بایست در مکانی خارج از سایت (جدا از تجهیزات مرکز صدور گواهی) نگهداری شود. نسخه پشتیبان می‌بایست در مکانی با کنترل‌های فیزیکی و رویه‌ای که در سطح امنیتی سیستم عملیاتی مرکز صدور گواهی می‌باشد، نگهداری شود.

مراکز صدور گواهی می‌بایست اطمینان حاصل نمایند که تجهیزات به کار رفته در سایت پشتیبان دارای سطح امنیتی برابر با سایت اصلی هستند.

۵-۲ کنترل‌های فرایندی

۵-۲-۱ نقش‌های مورد اطمینان

کلیه فعالیت‌های مرکز صدور گواهی در قالب وظایف تدوین شده برای نقش‌های تعریف شده‌ای که به کارکنان مرکز منتسب شده‌اند، صورت می‌پذیرند. افرادی که برای این نقش‌ها انتخاب می‌شوند می‌بایست همان‌گونه که در بخش ۵-۳ ذکر شده قابل اطمینان باشند. برای افزایش امنیت، انجام فعالیت‌های مرکز صدور گواهی مستلزم حضور بیش از یک نقش مورد اطمینان است. این امر از فعالیت‌های مخرب که احتیاج به تبانی دارند، جلوگیری می‌نماید.

مرکز میانی می‌بایست در دستورالعمل اجرایی گواهی الکترونیکی خود، نقش‌های مورد اطمینانی که مسئول انجام عملیات و روال‌های زیر می‌باشند را، تعریف نموده و شرح وظایف هر نقش را به تفکیک تعیین نماید.

عملیات اجرایی در مرکز صدور گواهی:

- صدور و مدیریت گواهی؛
- انتشار گواهی‌ها و لیست گواهی‌های باطل شده؛
- تهیه نسخه پشتیبان؛
- فعالیت‌های راهبری مانند تولید کلید، مدیریت پودمان‌های رمزنگاشتی و عملیات کنترلی و نظارتی
- بازرسی تطابق
- توسعه نرم‌افزارها (در صورت لزوم)

عملیات اجرایی در دفتر ثبت نام:

- هویت شناسی متقاضی و تایید صحت اطلاعات؛
- تنظیم و تایید درخواست نهایی[۱]
- ارسال درخواست‌ها به مراکز صدور گواهی و دریافت نتیجه به صورت ایمن؛
- تحویل گواهی به مالک گواهی.

عملیات اجرایی مشترک در مراکز صدور گواهی و دفاتر ثبت نام:

- نصب، راه اندازی و پیکربندی اولیه سیستم
- بازرسی داخلی؛
- پشتیبانی فنی تجهیزات و سیستم‌ها؛

[۱] شامل درخواست صدور، ابطال، تمدید گواهی و تجدید کلید

- بایگانی مطمئن اطلاعات؛
- بازیابی خرابی در راستای طرح تداوم خدمات (بخش ۵-۷-۴)

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

جدول ۱۸ افراد مورد نیاز برای هر نقش

سطح اطمینان	افراد مورد نیاز برای هر نقش
سطح ۱	حداقل توسط ۱ نفر انجام گیرد.
سطح ۲	برای نقش‌هایی که انجام وظایف آن‌ها مستلزم دسترسی به اطلاعات حساس مرکز صدور گواهی مانند کلید خصوصی می‌باشند، حداقل ۲ نفر مورد نیاز است. برای انجام وظایف سایر نقش‌ها، ۱ نفر کافی است.
سطح ۳	
سطح ۴	

۵-۲-۳ شناسایی و احراز هویت برای هر نقش

پیش از آنکه هر یک از کارکنان مراکز صدور گواهی در موقعیت‌های زیر قرار گیرند، می‌بایست شناسایی و احراز هویت شوند:

- قرار گرفتن در لیست دسترسی به سایت مرکز صدور گواهی؛
- قرار گرفتن در لیست دسترسی فیزیکی به سیستم مرکز صدور گواهی؛
- دریافت حکم برای بر عهده گرفتن یک نقش مورد اعتماد در مرکز صدور گواهی و یا دفتر ثبت نام؛
- ایجاد حساب کاربری در سیستم‌های مرتبط با زیرساخت کلید عمومی، اگر حساب کاربری نیاز باشد.
- این حکم یا حساب کاربری:

الف) می‌بایست تنها به یک شخص به طور مستقیم قابل انتساب باشد؛

ب) اشتراکی نباشد؛

پ) می‌بایست از طریق استفاده از نرم‌افزار CA، سیستم عامل و کنترل‌های رویه‌ای، محدود به فعالیت‌های مجاز برای آن نقش باشد.

مرکز صدور گواهی می‌بایست این الزامات را از طریق استفاده از نرم‌افزار صدور گواهی، سیستم عامل و کنترل‌های رویه‌ای اجرا نماید.

۵-۲-۴ نقش‌های مستلزم تفکیک وظایف

مرکز صدور گواهی می‌بایست تفکیک وظایف را برای وظایف بحرانی مرکز مربوطه مطابق با بخش ۵-۲-۱، در

دستورالعمل اجرایی خود شرح دهد.

۵-۳ کنترل کارکنان

کارهایی که مرکز صدور گواهی به کارکنان واگذار می‌نماید، نباید با وظایف تعریف‌شده برای آن‌ها و حدود اختیاراتشان تناقضی داشته باشد. علاوه بر آن کارکنان می‌بایست:

۱. تعهد کتبی به منظور رعایت مقررات امضا کنند؛

۲. به وسیله قرارداد یا حکم، به شرایط و ضوابط موقعیتی که در آن قرار می‌گیرند، پایبند باشند؛

۳. طبق قرارداد یا حکم، ملزم به عدم افشای اطلاعات حساس و امنیتی مرکز صدور گواهی یا اطلاعات کاربر باشند؛

۴. آموزش‌های لازم متناظر با وظایفی که بر عهده دارند را دیده باشند؛

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

اشخاصی که برای انجام فعالیت‌های مرکز صدور گواهی در نظر گرفته می‌شوند می‌بایست بر اساس قابلیت فنی، مورد اطمینان بودن و امانت‌داری انتخاب شوند. علاوه بر این تمام کارکنان مرکز می‌بایست دارای تابعیت ایرانی بوده و دارای گواهی عدم سوء پیشینه از نیروی انتظامی جمهوری اسلامی ایران باشند.

افرادی که برای کار با تجهیزات مرکز صدور گواهی انتخاب شده‌اند می‌بایست دارای مشخصات زیر باشند:

- 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 آن‌ها 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 می‌بایست تحت قوانین جاری کشور صورت گیرد. فرایند بررسی سوابق افراد می‌بایست در دستورالعمل اجرایی مرکز صدور گواهی بیان شود.

مرکز دولتی ریشه، رویه بررسی سابقه کارکنان خود را مطابق با قوانین استخدامی دولت اعمال می‌نماید.

۵-۳-۳ الزامات آموزشی

کلیه کارکنانی که در مرکز صدور گواهی فعالیت می‌کنند می‌بایست آموزش متناسب با فعالیتشان را ببینند. همچنین آن‌ها می‌بایست به طور دوره‌ای این برنامه‌های آموزشی را مرور کنند. موضوع این آموزش‌ها می‌بایست شامل موارد آشنایی با اصول امنیتی و ساختار مرکز صدور گواهی، کار با نرم‌افزارها و سخت‌افزارهای در حال استفاده، گزارش دهی و رسیدگی به حوادث، فرایندهای ترمیم خرابی و تداوم کسب و کار، به‌کارگیری و اجرای اقدامات امنیتی و اطلاعات لازم برای اعمال شرایط سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور باشد. لزوم آموزش‌های خاص بستگی به تجهیزات استفاده شده و کارکنان انتخاب شده دارد. یک طرح آموزش برای نصب و برپاسازی مرکز صدور گواهی می‌بایست تهیه شده و همچنین موارد آموزشی تکمیل شده توسط کارکنان مستندسازی شوند.

۵-۳-۴ الزامات آموزش مکرر و متناوب

مراکز صدور گواهی می‌بایست حداقل یک بار در سال برنامه‌های آموزشی جدید را فراهم کنند و کارکنان خود را به‌روزرسانی کنند تا مطمئن باشند که این افراد سطح مهارت مورد نیاز برای انجام مسئولیت‌های شغلیشان را به خوبی احراز می‌کنند. همچنین هرگونه تغییر در عملکرد مرکز صدور گواهی مستلزم داشتن یک برنامه آموزشی است و اجرای این برنامه می‌بایست مستند شود.

۵-۳-۵ دوره زمانی و ترتیب چرخش کار

تعریف نشده است.

۵-۳-۶ جریمه‌های اقدامات خارج از محدوده اختیارات

در صورت انجام عملی غیرمجاز یا مشکوک به غیرمجاز توسط کارکنان، مدیریت می‌تواند دسترسی او به سیستم را تعلیق نماید.

۵-۳-۷ الزامات پیمانکاران مستقل

مرکز صدور گواهی می‌بایست با ایجاد رویه‌هایی مراحل عقد قرارداد و شرایط و ضوابط همکاری را مشخص نماید تا بتوان اطمینان حاصل کرد که کلیه مراکز طرف قرارداد بر طبق مفاد این سیاست‌ها و دستورالعمل اجرایی گواهی الکترونیکی، عمل می‌کنند.

۵-۳-۸ مستندات فراهم‌شده برای کارکنان

مرکز صدور گواهی می‌بایست مستندات کافی و مورد نیاز را برای تعریف خدمات و وظایف هر نقش فراهم نماید تا کارکنان مسئولیت‌هایشان را به خوبی انجام دهند.

۵-۴ فرایندهای ثبت رویدادهای بازرسی

این بخش ملزومات بازرسی امنیتی برای مراکز صدور گواهی را تشریح می‌نماید.

۵-۴-۱ انواع رویدادهای قابل ثبت

مرکز صدور گواهی می‌بایست مطمئن باشد که ظرفیت ثبت همه رویدادهای مربوط به امنیت سیستم مرکز صدور گواهی -شامل ، فایروال‌ها، دایرکتوری و سرویس دهنده‌های میزبان نرم‌افزار CA و RA- را در فایل‌های ثبت رویدادهای بازرسی امنیتی دارد. قابلیت ثبت رویدادهای امنیتی در سیستم عامل‌های تجهیزات مراکز صدور گواهی می‌بایست در زمان شروع به کار سیستم، به طور خودکار فعال باشند. مراکز صدور گواهی می‌بایست از مکانیزم‌های مناسب جهت اطمینان از تمامیت و دست‌نخوردگی رویدادهای ثبت شده بهره گیرند.

حداقل رویدادهای زیر می‌بایست در سیستم‌های مرتبط با مرکز صدور گواهی یا دفتر ثبت نام ثبت گردد:

- روشن و خاموش شدن سیستم؛
- ورود و خروج به برنامه‌های کاربردی مرکز صدور گواهی و دفاتر ثبت نام؛
- تلاش برای تولید، حذف، تعیین گذرواژه یا تغییر مجوزهای ورود به سیستم؛
- تعریف، حذف یا اضافه کردن کاربران و نقش‌ها؛
- هر تغییری در جزئیات مرکز صدور گواهی و یا کلیدها؛
- هر تغییری در تنظیمات مرتبط با صدور گواهی (مثل: دوره اعتبار)؛
- هر تلاش مربوط به ورود و خروج همراه با Login و Logout به/از برنامه‌های کاربردی مرکز صدور گواهی یا دفاتر ثبت نام؛
- هر تلاش غیر مجاز در دسترسی به سیستم مرکز صدور گواهی یا دفتر ثبت نام ؛
- هر تلاش مربوط به عدم احراز هویت برای دسترسی به فایل‌های سیستمی؛
- اعمال تغییر در پیکربندی سیستم‌ها؛
- پشتیبان گیری و بازیابی پایگاه داده؛
- تولید و پشتیبان گیری کلیدهای مرکز صدور گواهی و کلیدهای فرعی؛

- صدور، ابطال، تعلیق/رفع تعلیق، به‌روزرسانی و تجدید کلید گواهی‌ها؛
- امضای لیست گواهی‌های باطل شده؛
- تولید و ارسال درخواست‌های تنظیم و تایید شده در دفاتر ثبت نام؛
- انجام عملیات اثبات مالکیت کلید خصوصی منطبق با بخش ۳-۲-۱؛
- ارسال هر داده‌ای به مخزن؛
- عملیات خواندن و نوشتن ناموفق در مخزن گواهی‌ها و لیست گواهی‌های باطل‌شده؛
- خطاهای رخ داده شده در سیستم و شرایط رخداد آن‌ها.

کلیه موارد ثبت‌شده، چه الکترونیکی و چه دستی، می‌بایست دارای تاریخ و زمان رویداد و شناسه موجودیتی که باعث وقوع رویداد شده است، باشند.

همچنین مرکز صدور گواهی می‌بایست به صورت الکترونیکی یا دستی، اطلاعات امنیتی که توسط سیستم مرکز صدور گواهی تولید نشده است را جمع‌آوری نماید. این اطلاعات می‌تواند شامل موارد زیر باشد:

- رویدادهای مربوط به دسترسی‌های فیزیکی؛
- تغییرات مربوط به پیکربندی سیستم، همان‌طور که در دستورالعمل اجرایی گواهی تعریف شده است؛
- تغییرات مربوط به کارکنان مرکز صدور گواهی؛
- گزارشات مربوط به اختلافات و تفاهم‌ها؛
- گزارشات مربوط به از بین رفتن اطلاعات حساس؛
- نسخه‌های قبلی و نسخه‌های جاری سیاست‌های گواهی الکترونیکی؛
- نسخه‌های قبلی و نسخه‌های جاری دستورالعمل‌های اجرایی گواهی الکترونیکی؛
- گزارشات مربوط به ارزیابی آسیب‌پذیری؛
- گزارشات مربوط به ارزیابی تهدیدات و خطرها؛
- خرابی تجهیزات؛
- زمان و مدت قطع جریان برق؛
- گزارشات مربوط به صدور گواهی؛
- گزارشات مربوط به قبول بازدید و سرکشی؛
- نسخه‌های قبلی و نسخه‌های جاری توافق‌نامه کاربر و دیگر اطلاعاتی که مالک گواهی با آن‌ها موافقت کرده است؛

- انتصاب کارکنان مرکز؛
- آموزش کارکنان مرکز.

مراکز صدور گواهی می‌بایست در دستورالعمل‌های اجرایی خود انواع رویدادهای قابل ثبت را به تفکیک تعیین نمایند و رویه اعمال شده جهت اطمینان از تمامیت و دست‌نخوردگی اطلاعات مرتبط با رویدادهای ثبت شده را بیان نمایند.

۵-۴-۲ تناوب پردازش اطلاعات رویدادهای ثبت‌شده

مرکز صدور گواهی می‌بایست اطمینان حاصل نماید که رویدادهای مهم در چکیده رویدادهای بازرسی شرح داده شده باشند و کارکنان مرکز صدور گواهی رویدادها را برای هر سطح اطمینان مطابق با جدول ۱۹ بازنگری می‌کنند.

این بازنگری‌ها شامل اعمالی از قبیل بررسی رویدادهای ثبت شده جهت اطمینان از عدم دست‌کاری آن‌ها و بازرسی از تمام ورودی‌ها می‌باشد. هر جا که یک اخطار یا ناهماهنگی مشاهده شود، کارکنان مرکز صدور گواهی می‌بایست تحقیق کامل‌تر و بیشتری انجام دهند. مرکز صدور گواهی می‌بایست فردی را که مسئول انجام بازنگری رویدادهای بازرسی و تهیه خلاصه رویدادهای بازرسی می‌باشد را در دستورالعمل اجرایی معین نماید.

در صورتی که مورد مشکوکی مشاهده شود، مرکز صدور گواهی می‌بایست رویدادها را به صورت الکترونیکی و دستی، شامل رویدادهای سمت دفتر ثبت نام، بررسی نماید.

مرکز صدور گواهی می‌بایست هر فعالیتی را که در آن این بازنگری‌ها صورت می‌گیرد، مستند نماید.

جدول ۱۹ تناوب پردازش اطلاعات رویدادهای ثبت شده

سطح اطمینان	تناوب پردازش اطلاعات رویدادهای ثبت شده
سطح ۱	پردازش و بازنگری رویدادها حداقل هر شش ماه یک بار می‌بایست صورت گیرد.
سطح ۲	پردازش و بازنگری رویدادها حداقل هر دو ماه یک بار می‌بایست صورت گیرد.
سطح ۳	پردازش و بازنگری رویدادها حداقل هر یک ماه یک بار می‌بایست صورت گیرد.
سطح ۴	

۵-۴-۳ دوره نگهداری از اطلاعات رویدادهای ثبت‌شده

مرکز صدور گواهی می‌بایست اطلاعات ثبت شده را حداقل دو ماه در سایت نگه‌داری نماید و سپس این اطلاعات به روشی که در بخش ۵-۵-۲ آورده شده است، حفظ و نگه‌داری شوند.

۵-۴-۴ محافظت از اطلاعات رویدادهای ثبت‌شده

مرکز صدور گواهی می‌بایست به وسیله یک سیستم الکترونیکی از اطلاعات رویدادهای ثبت‌شده محافظت نماید. اطلاعات رویدادهای ثبت‌شده می‌بایست از معرض دید افراد غیرمجاز محافظت شوند. همچنین این افراد نباید تا قبل از پایان دوره نگهداری قادر به اصلاح، حذف و یا تخریب این اطلاعات باشند. فردی که موظف به بایگانی اطلاعات رویدادهای ثبت شده است نیز نباید قادر به تغییر اطلاعات باشد. اطلاعات رویدادهای ثبت شده می‌بایست در مکانی جدا از تجهیزات مرکز صدور گواهی نگهداری شوند. مراکز صدور گواهی می‌بایست روال‌ها و مکانیزم بکار گرفته شده جهت محافظت از رویدادهای ثبت شده را در دستورالعمل اجرایی خود تشریح نمایند.

۵-۴-۵ فرآیندهای پشتیبان گیری از رویدادهای بازرسی

گرفتن نسخه پشتیبان از رویدادهای ثبت‌شده باید به صورت افزایشی، به طور کامل و ماهانه صورت گیرد.

۵-۴-۶ سامانه جمع‌آوری اطلاعات بازرسی

فرایند ثبت وقایع می‌بایست هنگام راه‌اندازی سیستم شروع به‌کار نماید و فقط هنگام خاموش شدن سیستم متوقف شود. 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 صدور گواهی می‌بایست کلیه فعالیت‌های خود را به غیر از فرآیند باطل کردن و تعلیق گواهی‌ها را متوقف نماید تا وقتی که سیستم مجدداً به‌کار افتد. در چنین شرایطی مرکز صدور گواهی می‌بایست از مکانیزم‌هایی برای ممانعت از ادامه فعالیت‌های غیرمجاز این مرکز استفاده نماید. این مکانیزم‌ها می‌بایست در دستورالعمل اجرایی گواهی الکترونیکی توضیح داده شوند.

۵-۴-۷ تذکر به مسبب رویداد

با توجه به ثبت یک رویداد توسط سیستم رویدادنگار، نیاز به اطلاع‌رسانی به شخص، سازمان، وسیله یا نرم‌افزاری که مسبب رویداد بوده، نمی‌باشد.

۵-۴-۸ ارزیابی آسیب‌پذیری

کارکنان مراکز صدور گواهی می‌بایست مراقب اقداماتی که برای ایجاد اختلال در تمامیت سیستم مدیریت گواهی‌ها انجام می‌شوند (مانند تجهیزات، مکان فیزیکی و کارکنان) باشند. بازرس می‌بایست اطلاعات ثبت وقایع امنیتی را برای وقایعی مانند فعالیت‌های ناموفق تکراری برای دسترسی به سیستم، اقدام برای به دست

آوردن اطلاعات محرمانه، تلاش برای دسترسی به فایل‌های سیستمی و پاسخ‌های تأیید نشده، بازبینی نماید. خلاصه نتایج مرور اطلاعات بازرسی امنیتی می‌بایست مستند شود.

۵-۵ بایگانی اطلاعات

۵-۵-۱ انواع اطلاعات قابل بایگانی

اطلاعات زیر می‌بایست در مورد عملیات مراکز صدور گواهی و دفاتر ثبت نام بایگانی شوند:

- کلیه رویدادهای ثبت شده مطابق با بخش ۵-۴؛
- درخواست‌های تنظیم شده توسط RA (صدور، ابطال، تعلیق/رفع تعلیق، به‌روزرسانی گواهی و تجدید کلید)؛
- فایل‌های درخواست امضای گواهی (CSR)؛
- کلیه گواهی‌ها صادر شده و CRLتولید شده توسط CA؛
- وضعیت گواهی‌ها (ابطال/معلق یا عدم ابطال)؛
- تاریخ و دلیل ابطال گواهی‌های باطل شده؛
- تاریخ و دلیل تعلیق/ رفع تعلیق گواهی‌ها؛
- توافق‌نامه‌های بین مالک گواهی یا درخواست‌کننده و مرکز صدور گواهی؛
- توافق‌نامه یا قراردادهای منعقد شده بین مرکز صدور گواهی و دفاتر ثبت نام؛
- مستندات و مدارک مربوط به هویت‌شناسی درخواست‌کننده گواهی منطبق با بخش ۳-۳-۱؛
- مستندات مربوط به دریافت و پذیرش گواهی منطبق با بخش ۴-۴؛
- کلیه گزارشات مربوط به بازرسی داخلی؛
- سیاست‌ها و دستورالعمل اجرایی گواهی؛
- هر توافق‌نامه پیمانی که مرکز صدور گواهی الکترونیکی به آن مقید است؛
- پیکربندی تجهیزات سیستم؛
- نسخه پشتیبان پایگاه داده سیستم صدور و مدیریت گواهی الکترونیکی؛
- کلیه مکاتبات با شورا، مراکز دیگر و بازرسان ثبت وقایع.

۵-۵-۲ دوره نگهداری اطلاعات بایگانی‌شده

اطلاعات ثبت‌شده در بایگانی مرکز صدور گواهی می‌بایست برای هر سطح اطمینان مطابق با جدول زیر

نگه‌داری گردند.

جدول ۲۰ دوره نگهداری اطلاعات ثبت‌شده در بایگانی

سطح اطمینان	دوره نگهداری اطلاعات ثبت‌شده در بایگانی
سطح ۱	اطلاعات ثبت‌شده در بایگانی می‌بایست حداقل برای ۵ سال نگهداری شود.
سطح ۲	اطلاعات ثبت‌شده در بایگانی می‌بایست حداقل برای ۱۶ سال نگهداری شود.
سطح ۳	اطلاعات ثبت‌شده در بایگانی می‌بایست حداقل برای ۲۴ سال نگهداری شود.
سطح ۴	اطلاعات ثبت‌شده در بایگانی می‌بایست حداقل برای ۳۰ سال نگهداری شود.

۵-۵-۳ محافظت از بایگانی

از بایگانی اطلاعات می‌بایست طوری محافظت شود که فقط افراد مجاز بتوانند به آن دسترسی داشته باشند. بایگانی اطلاعات می‌بایست در یک سیستم امن ذخیره‌سازی شود تا از معرض دید افراد غیرمجاز، تغییر، حذف یا عملیات پنهانی دیگر محفوظ بماند.

همچنین سخت‌افزار نگه‌دارنده اطلاعات بایگانی و نرم‌افزارهایی که این اطلاعات را پردازش می‌کنند می‌بایست به گونه‌ای محافظت شوند که در طول دوره نگهداری، اطلاعات بایگانی قابل دسترسی باشند.

مراکز صدور گواهی می‌بایست در دستورالعمل اجرایی خود روال‌ها و مکانیزم‌های به کار گرفته شده جهت محافظت از بایگانی را بیان نمایند.

۵-۵-۴ فرایندهای پشتیبان گیری از بایگانی

جدول ۲۱ روال تهیه نسخه پشتیبان از بایگانی

سطح اطمینان	روال تهیه نسخه پشتیبان از بایگانی
سطح ۱	از بایگانی اطلاعات الکترونیکی می‌بایست به صورت افزایشی و به طور کامل و ماهیانه نسخه پشتیبان تهیه شود.
سطح ۲	
سطح ۳	
سطح ۴	

۵-۵-۵ الزامات مهر زمانی[1] اطلاعات بایگانی

گواهی‌ها، لیست گواهی‌های باطل‌شده و کلیه اطلاعات مربوط به ابطال، تعلیق/ رفع تعلیق گواهی می‌بایست دارای زمان و تاریخ ثبت اطلاعات باشد. ضمن اینکه کلیه فرم‌ها و اسناد کاغذی نیز باید دارای تاریخ باشد.

[1] Time Stamp

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

اطلاعات بایگانی می‌تواند با استفاده از هر روش مناسبی جمع‌آوری شود. مراکز صدور گواهی باید در دستورالعمل اجرایی خود سامانه جمع‌آوری بایگانی را توصیف نمایند.

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

جدول ۲۲ روال به دست آوردن و بررسی اطلاعات بایگانی

سطح اطمینان	روال به دست آوردن و بررسی اطلاعات بایگانی
سطح ۱	• تنها افراد مورد اطمینان مجاز می‌توانند به اطلاعات بایگانی شده دسترسی پیدا کنند. • تمامیت اطلاعات بایگانی‌شده هر ۶ ماه می‌بایست بررسی شود. همین‌طور تمامیت کپی‌های کاغذی خارج از سایت می‌بایست یک بار در سال بررسی شود. • مرکز صدور گواهی می‌بایست فرایندی را که طی آن تمامیت اطلاعات بررسی می‌شود، در دستورالعمل اجرایی خود تعیین نماید.
سطح ۲	
سطح ۳	
سطح ۴	

۵-۶ تغییر کلید

مراکز صدور گواهی از کلید خصوصی برای امضای گواهی‌ها استفاده می‌کنند. از آنجایی که طرف‌های اعتماد کننده از گواهی مراکز صدور گواهی برای اعتبارسنجی گواهی مالک گواهی استفاده می‌کنند، بنابراین گواهی مالک گواهی نمی‌بایست دوره اعتبار طولانی‌تری از دوره اعتبار گواهی مراکز صدور گواهی و کلیدهای عمومی آن‌ها داشته باشند.

مراکز صدور گواهی برای به حداقل رساندن ریسک زیرساخت کلید عمومی (در خطر افشا قرار گرفتن کلید مرکز) می‌توانند کلید خصوصی امضا را در بازه‌های زمانی مشخص تجدید نمایند. در این صورت، کلید خصوصی قبلی می‌بایست تا زمان انقضای تمامی گواهی‌های امضا شده توسط آن، محافظت شود. گواهی مرتبط با کلید خصوصی سابق مرکز نیز -برای تعیین اعتبار گواهی‌هایی که توسط آن صادر شده‌اند- تا زمانی که تمامی گواهی‌های امضا شده با آن کلید خصوصی منقضی شوند، معتبر خواهد بود. روال انجام این کار و جزئیات آن می‌بایست در دستورالعمل اجرایی گواهی الکترونیکی مراکز صدور گواهی مربوطه تشریح شود.

مرکز دولتی ریشه در صورت تجدید کلید، مقدار درهم شده کلید عمومی مربوط به گواهی قدیم را در گواهی جدید خود می‌گنجاند و گواهی جدید را از طریق مخزن منتشر می‌نماید. گواهی قدیم تا زمان منقضی یا باطل شدن گواهی‌های مراکز میانی زیرین، معتبر باقی مانده و از طریق مخزن قابل دسترسی خواهد بود. مرکز صدور گواهی می‌بایست در دستورالعمل اجرایی خود موارد زیر را تعیین نماید:

۱. بازه زمانی قبل از فرا رسیدن زمان انقضای گواهی، که در طول آن امکان تجدید کلید خصوصی مالکان گواهی به شرط باطل نشدن آن وجود دارد.
۲. روالی که طی آن مراکز صدور گواهی و مالکان گواهی اقدام به تجدید کلید می‌کنند.

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

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

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

در حالتی که کلید پاسخگوی OCSP در خطر افشا قرار گرفته باشد، مرکز صدور گواهی که برای پاسخگوی OCSP گواهی صادر کرده است می‌بایست آن را باطل نماید و اطلاعات باطل‌شده می‌بایست به سرعت در مخزن منتشر شود. سپس، پاسخگوی OCSP می‌بایست کلید جدیدی را دریافت نماید.

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

مرکز صدور گواهی می‌بایست کپی‌هایی از نسخه‌های پشتیبان سیستم، پایگاه داده‌ها و کلیدهای خصوصی نگهداری نماید تا در صورت بروز خرابی در نرم‌افزار یا از بین رفتن داده‌ها، بتواند عملیات مرکز را از سر بگیرد. مرکز صدور گواهی همچنین باید در صورت از بین رفتن سیستم‌ها یا داده‌ها، پس از اطلاع‌رسانی به مرکز دولتی ریشه منطبق با الزامات بیان شده در بخش ۵-۷-۴ عملیات بازیابی سیستم‌ها و اطلاعات را انجام دهند، ضمن اینکه در دستورالعمل اجرایی گواهی خود، در صورت از بین رفتن تجهیزات کامپیوتری، نرم‌افزار و داده‌ها باید روالی را تعیین کنند.

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

در صورت در خطر افشا قرار گرفتن کلید یک مرکز صدور گواهی، مرکز صدور گواهی بالادستی می‌بایست گواهی آن مرکز را باطل نماید و اطلاعات باطل‌شده می‌بایست به سرعت در مخزن منتشر شود. سپس سیستم‌های مرکز صدور گواهی همان‌طور که در بخش ۵-۷-۴ آمده است، می‌بایست بازسازی شود. گواهی

خودامضای مرکز دولتی ریشه نیز (در صورت در خطر افشا قرار گرفتن کلید خصوصی متناظر و پس از اطلاع رسانی) می‌بایست از برنامه‌های کاربردی طرف‌های اعتماد کننده برداشته شود و به جای آن گواهی جدید که توسط این مرکز منتشر می‌شود باید جایگزین گردد.

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

مرکز صدور گواهی می‌بایست یک نقشه تداوم کار داشته باشد که در آن، در صورت وقوع بلایای طبیعی و یا هرگونه حادثه دیگر روش امنی برای اجرای مجدد فعالیت‌ها وجود داشته باشد.

طرح تداوم کار می‌بایست شامل موارد زیر باشد:

۱. تعریف نقش‌ها و مسئولیت کسانی که مسئول اجرای اجزای مختلف این طرح هستند؛
۲. شرایط برای فعال کردن طرح، که روندی را که قبل از فعال شدن طرح می‌بایست دنبال نمود، بیان نماید؛
۳. شیوه عمل در شرایط اضطراری که به عملیات کسب و کار و/ یا زندگی انسان خدشه وارد می‌نماید؛
۴. روش از سر گیری، که فعالیت‌های لازم برای بازگشت به عملیات کسب و کار عادی را بیان نماید؛
۵. برنامه تعمیر و نگهداری، که چگونگی و زمانی که این طرح آزمایش خواهد شد و همچنین فرآیند حفظ طرح را مشخص نماید؛
۶. فعالیت‌های آگاهی و آموزش، طراحی شده برای درک فرآیندهای تداوم کسب و کار و حصول اطمینان از این که فرایندها موثر ادامه می‌یابند.

۵-۸ توقف فعالیت مرکز صدور گواهی یا دفتر ثبت نام

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

به محض توقف مرکز میانی، همه کلیدهای خصوصی که وجود داشته‌اند یا ممکن است برای عملیات رمزنگاری مرکز میانی استفاده شوند، می‌بایست باطل (با دلیل ابطال متوقف شدن سرویس[1]) و نابود شوند مطابق با بخش ۶-۲-۱۰ (روش نابود کردن کلید خصوصی). لیست گواهی‌های باطل شده می‌بایست تولید و منتشر شوند. مراحل پایان فعالیت مراکز میانی به شرح زیر است:

---

[1] Cessation of Service

- اطلاع‌رسانی به مرکز دولتی ریشه و طرح مسئله در شورا 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، دفاتر ثبت نام و مشتریان؛
- ابطال گواهی مرکز میانی توسط مرجع صدور گواهی بالادستی،
- حفظ و ارائه بایگانی و سوابق مرکز میانی برای مدت زمان تعیین شده توسط این سند به یک مرجع معتبر که توسط شورا تعیین خواهد شد،

در حین توقف عملیات مرکز میانی، مرکز میانی می‌بایست اطلاعات مرکز را توسط متولی مجاز که توسط شورا تعیین می‌گردد و طبق الزامات بایگانی تعیین‌شده در این سیاست‌های گواهی نگهداری نماید. این اطلاعات شامل موارد زیر می‌باشد:

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

مرکز میانی همچنین می‌بایست برای نگهداری هر داده‌ای (مثل گذرواژه) مطمئن باشد که اطلاعات مرکز میانی قابل استفاده هستند (مثل داده‌های رمز شده‌ای که می‌تواند در زمانی که نیاز است رمزگشایی شود). اطلاعات می‌بایست به صورت امن و مطابق با بخش ۵-۱-۸ منتقل شوند.

۶ کنترل‌های امنیتی فنی

۶-۱ تولید و نصب زوج کلید

۶-۱-۱ تولید زوج کلید

۶-۱-۱-۱ تولید زوج‌کلید مراکز صدور گواهی

مرکز دولتی ریشه از زوج کلید الگوریتم RSA جهت صدور گواهی، پشتیبانی می‌نماید. انجام عملیات تولید کلید در این مرکز از طریق یک HSM مورد تأیید مرکز دولتی ریشه که در آن ملزومات امنیتی مطابق استاندارد FIPS 140-2 درسطح سوم رعایت شده است و به روش کنترل چند نفره ۳ از ۵ صورت می‌پذیرد. الزامات مربوط به عملیات تولید کلید برای مراکز میانی در جدول زیر قید شده است.

جدول ۲۳ تولید زوج‌کلید مرکز میانی

سطح اطمینان	تولید زوج‌کلید مرکز میانی
سطح ۱	مرکز میانی می‌بایست اطمینان حاصل نماید که تولید کلید مرکز با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور و توسط نقش مورد اعتماد و مجاز صورت می‌پذیرد.
سطح ۲	تولید زوج کلید مرکز میانی: • می‌بایست توسط متصدیانی با نقش مورد اعتماد و مجاز برای تولید کلید صورت پذیرد. • می‌بایست در داخل پودمان رمزنگاشتی سخت‌افزاری انجام پذیرد که حداقل الزامات بخش ۶-۱-۲ را در بر گیرد
سطح ۳	• می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد. • در سطح سوم و چهارم می‌بایست انجام عملیات تولید کلید از طریق کنترل چند نفره مطابق با بخش ۶-۲-۲ صورت گیرد.
سطح ۴	• مرکز میانی می‌بایست فرایند تولید کلید را مستند نماید و دلایل و شواهد لازم را برای اثبات اینکه مراحل مستند شده انجام گرفته‌اند، ارائه نماید.

۶-۱-۱-۲ تولید زوج‌کلید دفاتر ثبت نام

جدول ۲۴ تولید زوج‌کلید دفتر ثبت نام

سطح اطمینان	تولید زوج‌کلید دفتر ثبت نام
سطح ۱	مرکز میانی می‌بایست اطمینان حاصل نماید که تولید کلید دفتر ثبت نام با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور انجام گیرد.
سطح ۲	می‌بایست در داخل پودمان رمزنگاشتی سخت‌افزاری انجام پذیرد که حداقل الزامات بخش ۶-۲-۱ را در بر گیرد و نیز می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد.
سطح ۳	
سطح ۴	

۶-۱-۱-۳ تولید زوج‌کلید مالک گواهی

جدول ۲۵ تولید زوج‌کلید مالک گواهی

سطح اطمینان	تولید زوج‌کلید مالک گواهی
سطح ۱	• تولید زوج کلید برای مالکان گواهی می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد.
سطح ۲	• تولید زوج کلید برای مالک گواهی می‌بایست در یک پودمان رمزنگاشتی نرم‌افزاری و ترجیحاً سخت‌افزاری که در آن حداقل الزامات بخش ۶-۲-۱ رعایت شده است، صورت پذیرد (تولید کلید به صورت نرم‌افزاری صرفاً می‌بایست توسط مالک گواهی صورت گیرد و تحویل کلید عمومی متناظر، به دفتر ثبت نام یا مرکز میانی باید همراه با اثبات مالکیت کلید خصوصی باشد). • تولید زوج کلید برای مالکان گواهی می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد.
سطح ۳	• تولید زوج کلید برای مالک گواهی می‌بایست در داخل یک پودمان رمزنگاشتی سخت‌افزاری که در آن حداقل الزامات بخش ۶-۲-۱ رعایت شده است، صورت پذیرد.
سطح ۴	• تولید زوج کلید برای مالکان گواهی می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد.

لازم به ذکر است چنانچه مرکز صدور گواهی میانی به نمایندگی از متقاضی اقدام به تولید زوج کلید نمود، می‌بایست این موضوع در توافقنامه طرفین ذکر شود. مرکز میانی می‌بایست فرایند این عملیات را در دستورالعمل اجرایی خود تشریح نماید.

۶-۱-۲ تحویل کلید خصوصی به موجودیت نهایی

جدول ۲۶ تحویل کلید خصوصی به موجودیت نهایی

سطح اطمینان	تحویل کلید خصوصی به موجودیت نهایی
سطح ۱	تولید زوج کلید به صورت نرم‌افزاری صرفاً می‌بایست توسط مالک گواهی صورت گیرد و تحویل کلید عمومی متناظر به مرکز میانی یا دفتر ثبت نام باید همراه با اثبات مالکیت کلید خصوصی باشد.
سطح ۲	چنانچه عملیات تولید کلید توسط دفتر ثبت نام و یا مرکز میانی به نمایندگی از مالک گواهی صورت گیرد، می‌بایست این عملیات به صورت داخلی توسط یک سخت‌افزار رمزنگاشتی مورد تأیید (منطبق با بخش ۶-۱-۱) انجام گیرد و کلید خصوصی از طریق این سخت‌افزار در اختیار مالک گواهی قرار داده شود. تولید زوج کلید به صورت نرم‌افزاری صرفاً می‌بایست توسط مالک گواهی صورت گیرد و تحویل کلید عمومی متناظر به مرکز میانی یا دفتر ثبت نام باید همراه با اثبات مالکیت کلید خصوصی باشد.
سطح ۳	چنانچه عملیات تولید کلید توسط دفتر ثبت نام و یا مرکز میانی به نمایندگی از مالک گواهی صورت گیرد، می‌بایست این عملیات به صورت داخلی توسط یک سخت‌افزار رمزنگاشتی مورد تأیید (منطبق با بخش ۶-۱-۱) انجام گیرد و کلید خصوصی از طریق این سخت‌افزار در اختیار مالک گواهی قرار داده شود.
سطح ۴	

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

چنانچه عملیات تولید کلید توسط مالک گواهی و یا دفتر ثبت نام صورت گیرد، تحویل کلید عمومی به مرکز صدور گواهی می‌بایست به گونه‌ای باشد، که تناظر بین کلید عمومی ارائه شده و کلید خصوصی مالک گواهی و همچنین حفظ تمامیت آن توسط مرکز صدور گواهی قابل بررسی باشد.

کلیه مراکز میانی جهت ارائه درخواست صدور گواهی به مرکز دولتی ریشه می‌بایست کلید عمومی خود را در قالب استاندارد PKCS#10 در اختیار مرکز دولتی ریشه قرار دهند.

۶-۱-۴ تحویل کلید عمومی مرکز صدور گواهی به طرف‌های اعتماد کننده

مرکز دولتی ریشه از طریق مخزن خود که دسترسی و اعمال تغییر در آن فقط توسط نقش‌های مجاز مرکز دولتی ریشه امکان‌پذیر است، کلید عمومی خود را در اختیار طرف‌های اعتماد کننده قرار می‌دهد. الزامات مربوط به مراکز میانی در جدول زیر قید شده است:

جدول ۲۷ تحویل کلید عمومی مرکز میانی به طرف‌های اعتماد کننده

سطح اطمینان	تحویل کلید عمومی مرکز میانی به طرف‌های اعتماد کننده
سطح ۱	کلید عمومی مرکز میانی می‌بایست به صورت امن به طرف‌های اعتماد کننده منتقل شود، به طوری که صحت و اعتبار آن تضمین شود. روش تحویل کلید عمومی می‌بایست در دستورالعمل اجرایی مراکز میانی تشریح شود.
سطح ۲	
سطح ۳	
سطح ۴	

۶-۱-۵ طول کلید

مرکز دولتی ریشه از طول کلید ۲۰۴۸ بیت RSA برای ساختار سلسله مراتبی G2 و از طول کلید ۴۰۹۶ بیت RSA برای ساختار سلسله مراتبی G3 استفاده می‌نماید. لازم به ذکر است ساختارهای G2 و G3 در بخش ۷-۱-۳ معرفی شده است. از تاریخ ۱۳۹۸/۰۲/۱۷ تمدید و صدور گواهی الکترونیکی مراکز میانی توسط مرکز دولتی ریشه در ساختار سلسله‌مرتبی G2 متوقف شده‌است. الزامات مربوط به طول کلید برای مراکز میانی در جدول زیر قید شده است.

جدول ۲۸ الزامات طول کلید

سطح اطمینان	الزامات طول کلید
سطح ۱	حداقل طول کلید برای مراکز میانی، ۲۰۴۸ بیت RSA می‌باشد. حداقل طول کلید برای موجودیت‌های نهایی، ۱۰۲۴ بیت RSA ،یا ۲۲۴ بیت برای الگوریتم ECC یا ۲۵۶ بیت (معادل ۳۲ بایت) برای الگوریتم Ed25519 می‌باشد.
سطح ۲	
سطح ۳	حداقل طول کلید برای مراکز میانی ۲۰۴۸ بیت RSA می‌باشد. حداقل طول کلید برای موجودیت‌های نهایی، ۲۰۴۸ بیت RSA ،یا ۳۸۴ بیت برای الگوریتم ECC یا ۴۵۶ بیت (معادل ۵۷ بایت) برای الگوریتم Ed25519 می‌باشد.
سطح ۴	حداقل طول کلید برای مراکز میانی ۴۰۹۶ بیت RSA می‌باشد. حداقل طول کلید برای موجودیت‌های نهایی، ۲۰۴۸ بیت RSA، یا ۵۱۲ بیت برای الگوریتم ECC یا ۴۵۶ بیت (معادل ۵۷ بایت) برای الگوریتم Ed25519 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[1] انجام می‌شوند.

۶-۱-۷ موارد کاربرد کلید (طبق فیلد کاربرد کلید[2] در X.۵۰۹ v۳)

جدول ۲۹ موارد کاربرد کلید

سطح اطمینان	موارد کاربرد کلید
سطح ۱	کلید خصوصی متناظر با گواهی الکترونیکی می‌بایست صرفاً منطبق با کاربردهای در نظر گرفته شده در فیلد KeyUsage و ExtendedKeyUsage گواهی مورد استفاده قرار گیرد. کاربردهای در نظر گرفته شده برای گواهی الکترونیکی در بخش ۱-۴-۱ توصیف شده است. ضمن اینکه فیلد کاربرد کلید گواهی می‌بایست مطابق با سند جامع پروفایل‌های زیرساخت کلید عمومی کشور به‌کار رود.
سطح ۲	
سطح ۳	
سطح ۴	

[1] FIPS PUB 186: “Digital Signature Standard (DSS)”

[2] Key Usage

۶-۲ محافظت از کلیدهای خصوصی و کنترل‌های مهندسی پودمان رمزنگاشتی

۶-۲-۱ کنترل‌ها و استانداردهای پودمان‌های رمزنگاشتی

در کلیه پودمان‌های رمزنگاشتی مورد استفاده در زیرساخت کلید عمومی کشور (به عنوان مثال توکن‌های امنیتی، کارت‌های هوشمند و HSM) می‌بایست الزامات مرکز دولتی ریشه شامل:

- الزامات امنیتی[۱] (استاندارد FIPS 140[۲] و یا استاندارد Common Criteria[۳])
- الزامات عملیاتی[۴] (استاندارد PKCS#11[۵])
- الزامات کارایی[۶]

مورد ارزیابی قرار گرفته و به تأیید آزمایشگاه زیرساخت کلید عمومی رسیده باشد. کلید خصوصی مرکز دولتی ریشه در یک دستگاه سخت‌افزاری امن (HSM) نگهداری می‌شود که در آن الزامات استاندارد FIPS 140-2 در سطح سوم ارزیابی شده است؛ همچنین انجام عملیات تولید کلید برای مرکز دولتی ریشه و امضای کلیه گواهی‌های صادر شده توسط این مرکز از طریق این HSM و به صورت on-board[۷] صورت می‌گیرد.

الزامات مربوط به کنترل‌ها و استانداردهای پودمان‌های رمزنگاشتی در زیرساخت کلید عمومی کشور در جدول ۳۰ خلاصه شده است.

---

1 Security Requirements

2 FIPS PUB 140: Security Requirements for Cryptographic Modules

3 ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation

4 Functionality Requirements

5 11th of the Public Key Cryptography Standards group

6 Performance Requirements

۷ به‌صورت داخلی و توسط تراشه

جدول ۳۰ الزامات پودمان‌های رمزنگاشتی

سطح اطمینان	آخرین نسخه استاندارد سری FIPS 140 یا Common Criteria	مراکز صدور گواهی	دفاتر ثبت نام	مالکان گواهی
سطح ۱	مورد نیاز نیست.	حداقل الزامات سطح دوم FIPS 140 اعمال شده باشد.	حداقل الزامات سطح اول FIPS 140 اعمال شده باشد.	مورد نیاز نیست.
سطح ۲	مورد نیاز است.	حداقل الزامات سطح سوم FIPS 140 اعمال شده باشد.	حداقل الزامات سطح دوم FIPS 140 اعمال شده باشد.	حداقل الزامات سطح اول و ترجیحاً سطح دوم FIPS 140 و یا +EAL4 اعمال شده باشد.
سطح ۳	مورد نیاز است.	حداقل الزامات سطح سوم FIPS 140 اعمال شده باشد.	حداقل الزامات سطح دوم FIPS 140 اعمال شده باشد.	حداقل الزامات سطح دوم FIPS 140 و یا +EAL5 اعمال شده باشد.
سطح ۴	مورد نیاز است.	حداقل الزامات سطح سوم FIPS 140 اعمال شده باشد.	حداقل الزامات سطح سوم FIPS 140 اعمال شده باشد.	حداقل الزامات سطح سوم FIPS 140 و یا +EAL6 اعمال شده باشد.

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

در مرکز دولتی ریشه عملیات تولید کلید و مدیریت طول عمر کلیدها به صورت کنترل چند نفره ۳ از ۵ و از طریق HSM صورت می‌گیرد. الزامات مربوط به کنترل چند نفره برای مراکز میانی در جدول زیر آورده شده است.

جدول ۳۱ کنترل چندنفره به کلید خصوصی

سطح اطمینان	کنترل چندنفره به کلید خصوصی
سطح ۱	مورد نیاز نیست.
سطح ۲	
سطح ۳	برای عملیات تولید و استفاده از کلید خصوصی مرکز میانی می‌بایست کنترل چندنفره از طریق حداقل دو نقش مجاز وجود داشته باشد.
سطح ۴	

۶-۲-۳ امانت‌گذاری کلید خصوصی[1]

قابل اعمال نیست.

[1] Key Escrow

۶-۲-۴ پشتیبان گیری از کلید خصوصی

مرکز دولتی ریشه یک نسخه پشتیبان از کلید خصوصی خود را از طریق توکن پشتیبان با استفاده از کنترل چند نفره و به صورت کاملاً محافظت شده و در مکانی امن به منظور استفاده در سایت پشتیبان مرکز دولتی ریشه، نگهداری می‌نماید. الزامات تهیه نسخه پشتیبان کلید خصوصی برای مراکز میانی در جدول زیر قید شده است.

جدول ۳۲ تهیه نسخه پشتیبان از کلید خصوصی

سطح اطمینان	تهیه نسخه پشتیبان از کلید خصوصی
سطح ۱	مرکز میانی می‌بایست جهت امکان‌پذیر بودن بازیابی تجهیزات و داده‌های خود در صورت وقوع حوادث غیرمترقبه از کلید خصوصی خود نسخه پشتیبان تهیه نماید. پشتیبان گیری می‌بایست با کپی گرفتن از کلید خصوصی و انتقال آن به پودمان پشتیبان به صورت رمز شده مطابق با بخش‌های ۶-۲-۶ و ۶-۲-۷ انجام بگیرد و می‌بایست از آن در سایت پشتیبان به صورت کاملاً محافظت‌شده نگهداری شود.
سطح ۲	
سطح ۳	
سطح ۴	

مراکز میانی می‌بایست در دستورالعمل اجرایی گواهی الکترونیکی خود فرایندهای پشتیبان گیری از کلید خصوصی CA را تعیین نمایند.

۶-۲-۵ بایگانی کلید خصوصی

قابل اعمال نیست.

۶-۲-۶ انتقال کلید خصوصی به/از یک پودمان رمزنگاشتی

جدول ۳۳ انتقال کلید خصوصی به/از یک پودمان رمزنگاشتی

سطح اطمینان	انتقال کلید خصوصی به یا از یک دستگاه رمزنگاری
سطح ۱	کلیه مراکز صدور گواهی می‌بایست کلید (های) خصوصی خود را توسط پودمان (های) رمزنگاشتی امن تولید کرده و آن را در این پودمان (ها) نگهداری نمایند. در هنگام تهیه نسخه پشتیبان از کلید خصوصی مرکز صدور گواهی، می‌بایست این کلید به صورت رمزگذاری شده به پودمان پشتیبان انتقال داده شود و به صورت کاملاً محافظت شده از این پودمان در سایت پشتیبان مرکز صدور گواهی نگهداری گردد.
سطح ۲	
سطح ۳	
سطح ۴	

۶-۲-۷ ذخیره‌سازی کلیدهای خصوصی در پودمان رمزنگاشتی

ذخیره‌سازی کلیدهای خصوصی می‌بایست در یک پودمان رمزنگاشتی منطبق با الزامات قید شده در بخش ۶-۲-۱ صورت گیرد.

۶-۲-۸ روش فعال‌سازی کلید خصوصی

جدول ۳۴ فعال‌سازی کلید خصوصی

سطح اطمینان	فعال‌سازی کلید خصوصی
سطح ۱	می‌تواند از طریق گذرواژه صورت گیرد.
سطح ۲	شیوه‌هایی مانند 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 رمزنگاشتی قابل استفاده هستند. (الزامات تولید اطلاعات فعال‌ساز در بخش ۶-۴-۱ آمده است). اطلاعات فعال‌ساز را می‌بایست به روشی امن که در دستورالعمل اجرایی مراکز میانی باید توصیف گردد، در اختیار مالکان گواهی قرار داد (چنانچه کلید خصوصی از طریق دفتر ثبت نام و یا مرکز صدور گواهی در اختیار مالک گواهی قرار داده شود، حتماً می‌بایست به وی اعلام گردد که گذرواژه سخت‌افزار رمزنگاشتی خود را در اسرع وقت تغییر دهد).
سطح ۳	
سطح ۴	هنگام ورود اطلاعات فعال‌ساز می‌بایست از افشاء آن‌ها جلوگیری شود (مثلاً هنگام ورود، اطلاعات نباید روی صفحه نمایش ظاهر شوند).

۶-۲-۹ روش غیر فعال نمودن کلید خصوصی

جدول ۳۵ غیر فعال نمودن کلید خصوصی

سطح اطمینان	غیر فعال نمودن کلید خصوصی
سطح ۱	پودمان‌های رمزنگاشتی در حالت فعال نباید بدون استفاده باقی بمانند. این پودمان‌ها پس از استفاده می‌بایست به روشی غیرفعال شوند؛ برای مثال، از طریق روش دستی خروج از سیستم، یا پس از گذشت زمان معینی ارتباط به طور خودکار قطع شود. وقتی کلیدهای خصوصی غیرفعال می‌شوند، می‌بایست قبل از آزادسازی فضای حافظه از حافظه پاک شوند و می‌بایست فقط به شکل رمز شده نگهداری شوند.
سطح ۲	
سطح ۳	
سطح ۴	

۶-۲-۱۰ روش انهدام کلید خصوصی

جدول ۳۶ انهدام کلید خصوصی

سطح اطمینان	انهدام کلید خصوصی
سطح ۱	کلیدهای خصوصی زمانی که دیگر به آن‌ها نیازی نیست یا زمانی که گواهی‌های مرتبط با آن‌ها منقضی یا باطل شده‌اند، می‌بایست نابود شوند. برای پودمان‌های رمزنگاشتی نرم‌افزاری، این امر می‌تواند از طریق بازنویسی بر روی اطلاعات قبلی انجام شود. برای پودمان‌های رمزنگاشتی سخت‌افزاری، این کار از طریق اجرای دستور امحا[1] که می‌بایست همراه با عملیات بازنویسی حافظه باشد، انجام می‌گیرد.
سطح ۲	
سطح ۳	
سطح ۴	

[1] Zeroize

۶-۲-۱۱ رده‌بندی پودمان رمزنگاشتی

به بخش ۶-۲-۱ را مراجعه شود.

۶-۳ سایر ابعاد مدیریت زوج کلید

۶-۳-۱ بایگانی کلید عمومی

مراکز صدور گواهی می‌بایست کلید (های) عمومی متناظر با گواهی‌های خود و همچنین کلیدهای عمومی متناظر با گواهی‌های صادر شده را مطابق با بخش ۵-۵-۲ بایگانی کنند.

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

گواهی مرکز دولتی ریشه دارای دوره اعتبار ۲۰ ساله می‌باشد. الزامات مربوط به دوره اعتبار گواهی‌های مراکز میانی و همچنین گواهی‌های صادر شده توسط این مراکز در جدول زیر آورده شده است.

جدول ۳۷ دوره‌های عملیاتی گواهی و دوره‌های استفاده از زوج کلید

سطح اطمینان	نوع مالک گواهی	الگوریتم	طول کلید	حداکثر دوره اعتبار
سطح ۱	مرکز میانی	RSA	۲۰۴۸	۱۰ سال
			۴۰۹۶	۱۲ سال
	موجودیت نهایی	RSA	۱۰۲۴	۳ سال
			۲۰۴۸	۸ سال
		ECC	۲۲۴	۳ سال
			۲۵۶	۴ سال
			۳۸۴	۶ سال
			۵۱۲	۸ سال
		Ed25519	۲۵۶	۴ سال
			۴۵۶	۶ سال
سطح ۲	مرکز میانی	RSA	۲۰۴۸	۱۰ سال
			۴۰۹۶	۱۲ سال
	موجودیت نهایی	RSA	۱۰۲۴	۲ سال
			۲۰۴۸	۶ سال
		ECC	۲۲۴	۲ سال
			۲۵۶	۳ سال
			۳۸۴	۴ سال
			۵۱۲	۶ سال
		Ed25519	۲۵۶	۳ سال

سطح اطمینان	نوع مالک گواهی	الگوریتم	طول کلید	حداکثر دوره اعتبار
			۴۵۶	۵ سال
سطح ۳	مرکز میانی	RSA	۲۰۴۸	۱۰ سال
			۴۰۹۶	۱۲ سال
	موجودیت نهایی	RSA	۲۰۴۸	۵ سال
		ECC	۳۸۴	۳ سال
			۵۱۲	۵ سال
		Ed25519	۴۵۶	۴ سال
سطح ۴	مرکز میانی	RSA	۴۰۹۶	۱۲ سال
	موجودیت نهایی	RSA	۲۰۴۸	۴ سال
		ECC	۵۱۲	۴ سال
		Ed25519	۴۵۶	۳ سال

۶-۴ اطلاعات فعال‌ساز

۶-۴-۱ تولید و به‌کارگیری اطلاعات فعال‌ساز

کلیه اطلاعات فعال‌ساز می‌بایست یکتا و غیر قابل پیش‌بینی باشند. گذرواژه بکار رفته جهت فعال‌سازی کلید خصوصی حداقل می‌بایست ۸ کاراکتر باشند و در صورت امکان به صورت تصادفی تولید گردند ضمن اینکه می‌بایست کاراکترهای انتخابی ترکیبی از کاراکترهای قابل چاپ باشد. در صورتی که تولید گذرواژه‌ها به صورت تصادفی توسط مالکان گواهی امکان‌پذیر نباشد، می‌بایست دقت شود که گذرواژه انتخابی غیر قابل حدس بوده و به عنوان مثال با اطلاعات شناسایی شخصی او مرتبط نباشد. همچنین دنباله‌های تکراری کاراکترها، اعداد تکراری، اعداد مرتبط با تاریخ و یا دیگر اعدادی که به راحتی قابل حدس هستند نباید بکار روند. اطلاعات فعال‌ساز هرگز نباید به لغات با معنا شباهتی داشته باشند.

چنانچه از اعداد تصادفی جهت استفاده به عنوان اطلاعات فعال‌ساز به کار گرفته شود، می‌بایست کلیه الزامات مربوط به اعداد تصادفی منطبق با استانداردهای معرفی شده توسط مرکز دولتی ریشه، در آن‌ها رعایت شده باشد.

۶-۴-۲ محافظت از اطلاعات فعال‌ساز

جدول ۳۸ محافظت از اطلاعات فعال‌ساز

سطح اطمینان	محافظت از اطلاعات فعال‌ساز
سطح ۱	اطلاعات فعال‌ساز پودمان رمزنگاشتی می‌بایست به حافظه سپرده شوند و نباید به صورت نوشته نگهداری شود. اگر نوشته شوند، نوشته می‌بایست در سطحی از امنیت، معادل با امنیت داده‌های دستگاه رمزنگاری، نگهداری شوند. اطلاعات فعال‌ساز کلیدهای خصوصی می‌بایست منحصراً نزد مالک گواهی محفوظ باشد.
سطح ۲	
سطح ۳	
سطح ۴	

۶-۴-۳ سایر ابعاد اطلاعات فعال‌ساز

تعریف نشده است.

۶-۵ کنترل‌های امنیتی رایانه

۶-۵-۱ الزامات فنی ویژه امنیت رایانه

مراکز صدور گواهی می‌بایست موارد زیر را در سیستم عامل‌های خود فعال سازند:

- 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؛
- توانایی تنظیم و راه‌اندازی سیستم ثبت وقایع و بازبینی آن‌ها
- مراکز صدور گواهی می‌بایست مجهز به سیستم‌های شناسایی و تخریب ویروس با مشخصات زیر باشند:
- امکان به‌روزرسانی با آخرین لیست ویروس‌های شناسایی شده؛
- امکان جستجو در تمام فایل‌های سیستمی و غیر سیستمی به صورت خودکار؛
- ثبت وقایع مرتبط به بررسی سیستم و وجود ویروس‌های احتمالی و نتیجه عملکرد برنامه روی آن‌ها.

۶-۵-۲ رده‌بندی امنیت رایانه

جدول ۳۹ رده‌بندی امنیت رایانه

سطح اطمینان	رده‌بندی امنیت رایانه
سطح ۱	الزامی در نظر گرفته نشده است.
سطح ۲	آزمایشگاه شخص ثالث معتبر می‌بایست امنیت عناصر حیاتی مرکز صدور گواهی را ارزیابی نماید.
سطح ۳	
سطح ۴	

۶-۶ کنترل‌های فنی چرخه حیات

۶-۶-۱ کنترل‌های توسعه سامانه

مرکز صدور گواهی می‌بایست از نرم‌افزار صدور گواهی که تحت یک روش توسعه ساخت‌یافته طراحی و توسعه یافته است، استفاده نماید.

کلیه مراکز صدور گواهی می‌بایست از سامانه‌های صدور و مدیریت گواهی الکترونیکی مورد تایید مرکز دولتی ریشه استفاده نمایند و این سامانه‌ها و نرم‌افزارهای متناظر می‌بایست در آزمایشگاه زیرساخت کلید عمومی کشور ارزیابی شده و مورد تایید قرار گرفته شده باشند؛

کلیه مراکز میانی تنها پس از اطلاع‌رسانی به مرکز دولتی ریشه مجاز به توسعه سامانه‌های سخت‌افزاری و نرم‌افزاری خود خواهند بود و سامانه‌های توسعه یافته تنها پس از ارزیابی مجدد و تایید مرکز دولتی ریشه، قابلیت عملیاتی شدن خواهند داشت.

سخت‌افزار یا نرم‌افزار خریداری شده می‌بایست در یک بسته مهر و موم شده و یا به‌روش مطمئن دیگری حمل و تحویل داده شود و توسط پرسنل آموزش‌دیده نصب گردد.

۶-۶-۲ کنترل‌های مدیریت امنیت

سخت‌افزار و نرم‌افزار مرکز صدور گواهی می‌بایست به طور اختصاصی برای انجام وظایف مربوط به مرکز صدور گواهی مورد استفاده قرار گیرد. سیستم مرکز صدور گواهی نباید حاوی برنامه‌های کاربردی، وسایل سخت‌افزاری، اتصالات شبکه یا اجزاء نرم‌افزاری که مربوط به عملیات مرکز صدور گواهی نیستند، باشد. امنیت سیستم‌های سخت‌افزاری و نرم‌افزاری مراکز صدور گواهی می‌بایست در آزمایشگاه زیرساخت کلید عمومی کشور ارزیابی شده و مورد تایید قرار گرفته شده باشند.

مرکز صدور گواهی می‌بایست در دستورالعمل اجرایی گواهی، به سیاست‌ها و فرایندهایی که از قرار گرفتن نرم‌افزارهای مخرب در تجهیزات مرکز صدور گواهی پیشگیری می‌کند، اشاره نماید. سیستم‌های مراکز صدور گواهی و دفاتر ثبت نام می‌بایست برای یافتن کدهای مخرب احتمالی در اولین استفاده و بعد از آن به صورت دوره‌ای، بررسی شوند.

مرکز صدور گواهی می‌بایست از یک فرایند مدیریت پیکربندی برای نصب و نگهداری مداوم سیستم مرکز صدور گواهی استفاده نماید. نرم‌افزار مرکز صدور گواهی، زمانی که برای بار اول بر روی سیستم قرار می‌گیرد، می‌بایست روشی برای مرکز صدور گواهی فراهم نماید که تأیید کند نرم‌افزار روی سیستم:

۱) از توسعه‌دهنده نرم‌افزار نشئت گرفته؛

۲) قبل از نصب تغییر داده نشده است؛

۳) نسخه مورد نظر برای استفاده است.

مرکز صدور گواهی می‌بایست مکانیزمی برای بررسی دوره‌ای تمامیت پایگاه‌داده مرکز صدور گواهی فراهم نماید. مرکز صدور گواهی همچنین مکانیزم‌ها و سیاست‌هایی برای کنترل و نظارت بر پیکربندی سیستم مرکز صدور گواهی باید داشته باشد؛ کلیه این مکانیزم‌ها می‌بایست در دستورالعمل اجرایی مرکز صدور گواهی توصیف گردد.

جدول ۴۰ بررسی دوره‌ای تمامیت پایگاه‌داده

سطح اطمینان	بررسی دوره‌ای تمامیت پایگاه‌داده
سطح ۱	به محض نصب و حداقل هر ماه یک‌بار، تمامیت پایگاه‌داده مرکز صدور گواهی می‌بایست رسیدگی شود.
سطح ۲	
سطح ۳	به محض نصب و حداقل هفته‌ای یک‌بار، تمامیت پایگاه‌داده مرکز صدور گواهی می‌بایست رسیدگی شود.
سطح ۴	به محض نصب و حداقل روزی یک‌بار، تمامیت پایگاه‌داده مرکز صدور گواهی می‌بایست رسیدگی شود.

۶-۶-۳ کنترل‌های امنیتی چرخه حیات

پیاده‌سازی نشده است.

۶-۷ کنترل‌های امنیتی شبکه

جدول ۴۱ کنترل‌های امنیتی شبکه

سطح اطمینان	کنترل‌های امنیتی شبکه
سطح ۱	مرکز صدور گواهی می‌بایست مطمئن شود که کنترل‌های امنیتی برای فراهم کردن تمامیت مرکز صدور گواهی و قابل دسترس بودن آن از طریق هر شبکه سراسری یا باز، که به آن متصل است، انجام می‌گیرد. چنین محافظتی می‌بایست شامل نصب یک یا چند دستگاه پیکربندی شده باشد به طوری که تنها پروتکل‌ها و دستورات مورد نیاز عملیات اجرایی مرکز صدور گواهی پذیرفته شود. مرکز صدور گواهی در دستورالعمل اجرایی گواهی خود، چنین پروتکل‌هایی و همچنین مکانیزم‌ها و روال‌های در نظر گرفته شده برای اعمال کنترل‌های امنیت شبکه را می‌بایست توصیف نماید.
سطح ۲	
سطح ۳	
سطح ۴	

۸-۶ مهر زمانی

جدول ۴۲ مهر زمانی

سطح اطمینان	مهر زمانی
سطح ۱	الزامی در نظر گرفته نشده است.
سطح ۲	مرکز صدور گواهی می‌توانند برای مالکان گواهی قابلیت افزودن مهر زمانی در تراکنش‌های خود را فراهم نماید یا باعث فراهم شدن آن شود.
سطح ۳	
سطح ۴	

۷ پروفایل‌های[1] گواهی، لیست گواهی‌های باطله و OCSP

۷-۱ پروفایل گواهی

پروفایل گواهی‌های صادر شده توسط مراکز صدور گواهی می‌بایست با RFC5280[2] و سند جامع پروفایل‌های زیرساخت کلید عمومی کشور منطبق باشد و صدور هر نوع گواهی متفاوت با پروفایل‌های تعریف شده در سند مذکور، مجاز نمی‌باشد. هر گواهی X.509 حداقل می‌بایست شامل فیلدهای اصلی باشد و هر کدام از فیلدها می‌بایست با توجه به قیودی که برای مقادیر آن‌ها تعیین شده است، مقداردهی شوند. در جدول زیر فیلدهای گواهی X.509 قید شده است. تشریح کامل پروفایل‌های گواهی الکترونیکی در سند جامع پروفایل‌های زیرساخت کلید عمومی کشور آورده شده است.

جدول ۴۳ الزامات خصوصیات گواهی

فیلد	الزامات خصوصیات گواهی
Serial Number	شماره سریال گواهی که برای هر گواهی صادر شده توسط مرکز صدور گواهی مقداری منحصر به فرد می‌باشد.
Signature Algorithm	شناسه الگوریتم ۷-۱-۴ بکار رفته جهت امضای گواهی (بخش ۷-۱-۳)
Issuer DN	در بخش ۷-۱-۴ توضیح داده شده است.
Validity	دوره اعتبار گواهی
Subject DN	در بخش ۷-۱-۴ 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

گواهی‌ها می‌بایست منطبق با نسخه سوم استاندارد X.509 صادر شوند.

۷-۱-۲ الحاقیه‌های گواهی[3]

الزامات مربوط به وجود یا عدم وجود، مقداردهی و پردازش الحاقیه‌های گواهی در سند جامع پروفایل‌های زیرساخت کلید عمومی کشور بیان شده است.

---

[1] Profile

[2] Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002

[3] Certificate Extensions

۷-۱-۳ شناسه الگوریتم‌ها

گواهی‌های صادر شده توسط مرکز دولتی ریشه به وسیله یکی از الگوریتم‌های زیر امضا می‌گردد:

- **sha256withRSAEncryption** OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- **sha-1WithRSAEncryption** OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 5}

گواهی‌های صادر شده توسط مراکز میانی به وسیله یکی از الگوریتم‌های زیر امضا می‌گردد:

- **sha256withRSAEncryption** OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- **sha-1WithRSAEncryption** OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- **SHA384WithRSAEncryption** OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
- **ecdsa-with-Sha224** OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 1}
- **ecdsa-with-Sha256** OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}
- **ecdsa-with-Sha384** OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}
- **ecdsa-with-Sha512** OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 4}
- **id-Ed25519** OBJECT IDENTIFIER ::= {
  iso(1) identified-organization(3) thawte(101) id-EdDSA25519(112)}

زیرساخت کلید عمومی کشور متشکل از دو ساختار سلسله مراتبی G2 و G3 می‌باشد. ساختار G2 سازگار با تابع درهم‌ساز[1] SHA1 است و می‌تواند در سخت‌افزارها و نرم‌افزارهایی که از این تابع درهم‌ساز پشتیبانی می‌نمایند مورد استفاده قرار گیرد. ساختار G3 نیز سازگار با تابع درهم‌ساز SHA256 بوده و جهت ارائه سطح امنیت بالاتر پیش‌بینی شده است.

از تاریخ ۱۳۹۸/۰۲/۱۷ صدور و تمدید گواهی مراکز میانی توسط مرکز دولتی ریشه در ساختار سلسله مراتبی G2 در زیرساخت کلید عمومی کشور متوقف شده است. کلیه مراکز میانی می‌بایست نسبت به دریافت گواهی-های خود در ساختار سلسله مراتبی G3 و صدور گواهی موجودیت نهایی در این ساختار اقدام نمایند.

۷-۱-۴ قالب نام‌ها

نحوه مقداردهی نام ترکیبی مربوط به مالک و صادرکننده گواهی می‌بایست مطابق با بخش ۳-۱ باشد.

---

[1] Hash Function

۷-۱-۵ محدودیت‌های نام‌گذاری

فیلد الحاقی name constraints می‌بایست مطابق آنچه در سند جامع پروفایل‌های زیرساخت کلید عمومی کشور شرح داده شده است، در گواهی قید شود.

۷-۱-۶ شناسه سیاست‌های گواهی

مرکز صدور گواهی می‌بایست از صحت مقدار شناسه یا شناسه‌های سیاست گواهی که در گواهی قرار می‌گیرد، مطمئن شود. شناسه مختص هر سطح گواهی در بخش ۱-۲ مشخص شده است.

۷-۱-۷ کاربرد الحاقیه Policy Constraints

الحاقیه Policy Constraints می‌بایست مطابق آنچه در سند جامع پروفایل‌های زیرساخت کلید عمومی کشور شرح داده شده است، در گواهی قرار بگیرد.

۷-۱-۸ ساختار و معنای الحاقیه "Policy Qualifier"

گواهی‌های نسخه سوم X.509 حاوی یک توصیف‌کننده سیاست در فیلد الحاقی Certificate Policies می‌باشند که به عنوان مثال به نشانی دسترسی به دستورالعمل اجرایی اشاره می‌نماید.

۷-۱-۹ پردازش معنایی برای الحاقیه حیاتی Certificate Policies

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

۷-۲ پروفایل لیست گواهی‌های باطل شده

پروفایل لیست گواهی‌های باطل شده می‌بایست مطابق با استاندارد RFC5280 باشند. لیست گواهی‌های باطل شده می‌بایست حداقل شامل فیلدهای اصلی و مقادیر تعیین شده برای آن‌ها که در جدول زیر به آن‌ها اشاره شده است، باشد:

جدول ۴۴ الزامات خصوصیات لیست ابطال

فیلد	الزامات خصوصیات لیست ابطال
version	در بخش ۷-۲-۱ توضیح داده شده است.
Signature Algorithm	شناسه الگوریتم بکار رفته جهت امضای CRL (بخش ۷-۱-۳).
Issuer	نام ترکیبی موجودیتی که CRL را امضا و تولید می‌نماید.
Effective Date	تاریخ صدور CRL.

فیلد	الزامات خصوصیات لیست ابطال
Next Update	تاریخی که CRL بعدی صادر خواهد شد. ملزومات تناوب صدور لیست گواهی‌های باطل شده در بخش ۴-۹-۷ بیان شده است.
Revoked Certificates	لیست گواهی‌های باطل شده شامل شماره سریال گواهی‌های باطل شده و تاریخ ابطال

۷-۲-۱ شماره نسخه

مرکز صدور گواهی می‌بایست از نسخه دوم X.509 لیست گواهی‌های باطل‌شده منطبق با RFC5280 پشتیبانی نماید.

۷-۲-۲ الحاقیه‌های CRL و CRL Entry

الزامات مربوط به وجود یا عدم وجود، مقداردهی و پردازش الحاقیه‌های CRL و CRL Entry در سند جامع پروفایل‌های زیرساخت کلید عمومی کشور بیان شده است.

۷-۳ پروفایل OCSP

۷-۳-۱ شماره نسخه

مرکز صدور گواهی می‌بایست از نسخه اول OCSP تعریف شده در RFC2560 و به‌روزرسانی‌های بعدی آن پشتیبانی نماید.

۷-۳-۲ الحاقیه‌های OCSP

الحاقیه‌های OCSP می‌بایست منطبق با سند جامع پروفایل‌های زیرساخت کلید عمومی کشور به کار رود. سرویس‌دهنده پاسخگوی OCSP می‌بایست جهت جلوگیری از حملات تکرار[1] و اطمینان سرویس‌گیرنده OCSP از تازگی[2] پاسخ OCSP، از الحاقیه Nonce توصیف شده در RFC2560 و به‌روزرسانی‌های بعدی آن استفاده نماید. این الحاقیه با مقدار الحاقیه Nonce موجود در درخواست OCSP که از سوی سرویس‌گیرنده OCSP ارسال می‌شود، مقداردهی می‌گردد.

---

[1] Reply Attacks

[2] freshness

۸ بازرسی تطابق و سایر ارزیابی‌ها

بازرسی تطابق با هدف حصول اطمینان از عملکرد مراکز صدور گواهی و به منظور بررسی تطابق عملیات مراکز صدور گواهی با الزامات و فرایندهای بیان شده در سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و دستورالعمل اجرایی مراکز میانی به عمل می‌آید. در زیرساخت کلید عمومی کشور، بازرسی تطابق به دو صورت تعریف شده است:

- **بازرسی شورا:** بر اساس ماده ۳ آیین‌نامه ۳۲ قانون تجارت الکترونیکی ایران یکی از وظایف و مسئولیت‌های شورا، نظارت عالیه و بررسی گزارش عملکرد و تخلفات احتمالی مراکز ریشه و میانی می‌باشد. بر این اساس به منظور اعمال نظارت بر عملکرد مرکز دولتی ریشه و مراکز میانی، می‌بایست بازرسی دوره‌ای از این مراکز زیر نظر شورا و توسط بازرس یا بازرسین مورد تأیید شورا صورت گیرد.
- **بازرسی مرکز دولتی ریشه:** بر اساس ماده ۵ آیین‌نامه ۳۲ قانون تجارت الکترونیکی ایران یکی از وظایف و مسئولیت‌های اصلی مرکز دولتی ریشه، حصول اطمینان از عملکرد صحیح مراکز میانی می‌باشد. مرکز دولتی ریشه به منظور حصول اطمینان از عملکرد صحیح مراکز میانی، از این مراکز به عمل خواهد آورد.

۸-۱ تناوب و شرایط ارزیابی

بازرسی تطابق برای کلیه مراکز صدور گواهی می‌بایست مطابق با جدول زیر انجام گیرد.

جدول ۴۵ تناوب و شرایط ارزیابی

سطح اطمینان	تناوب و شرایط ارزیابی
سطح ۱	به تشخیص مرکز دولتی ریشه انجام می‌گیرد.
سطح ۲	به تشخیص مرکز دولتی ریشه و حداقل یک‌بار در سال انجام می‌گیرد.
سطح ۳	
سطح ۴	به تشخیص مرکز دولتی ریشه و حداقل دوبار در سال انجام می‌گیرد.

ضمن اینکه زمان و تناوب بازرسی وابسته به میزان کارکرد مرکز صدور گواهی، متغیر است.

۸-۲ هویت و صلاحیت ارزیاب

بازرسی مرکز دولتی ریشه از مراکز میانی توسط یک یا چند تن از کارشناسان واجد شرایط و مجاز مرکز دولتی ریشه در حوزه‌های تعیین شده در بخش ۸-۴ انجام می‌گیرد و بازرسی شورا توسط یک یا چند شخص حقیقی یا حقوقی مورد تأیید شورا انجام می‌پذیرد.

بازرس می‌بایست با زیرساخت کلید عمومی و استانداردهای آن، سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشورو دستورالعمل اجرایی گواهی الکترونیکی مراکز میانی و مصوبات شورا کاملاً آشنا باشد.

۸-۳ ارتباط ارزیاب با مرکز مورد ارزیابی

بازرسی از کلیه مراکز صدور گواهی می‌بایست منحصراً توسط اشخاص تعیین شده در بخش ۸-۲ انجام گیرد.

۸-۴ موضوعات مورد ارزیابی

محدوده ارزیابی در فرایند بازرسی تطابق مرکز صدور گواهی می‌بایست **حداقل** شامل موضوعات زیر باشد:

- دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی، دستورالعمل‌های فنی، فرایندی و پرسنلی مرکز صدور گواهی و طرح فنی تجهیزات و ساختمان مرکز؛
- بررسی تطابق مرکز میانی، شامل ساختمان، تجهیزات و همچنین کلیه سخت‌افزارها، نرم‌افزارها، نیروی انسانی و فرایندهای بکار گرفته در مرکز، با دستورالعمل‌ها و مستندات قید شده در بند اول؛
- بررسی تطابق تجهیزات، نرم‌افزارها و عملکرد دفاتر ثبت نام با دستورالعمل اجرایی مرکز میانی.

۸-۵ اقدامات اتخاذ شده در برخورد با نقایص

در صورت احراز مغایرت در فرایند بازرسی با سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی مورد بازرسی و یا در صورت آشکار شدن هر گونه نقص و یا مشکل امنیتی در طی فرایند بازرسی می‌بایست اقدامات زیر انجام شود:

- بازرس می‌بایست نقص و یا ناهمخوانی را ثبت نماید؛
- بازرس می‌بایست به طرف‌های تعیین شده در بخش ۸-۶ ناهمخوانی و یا نقص را اعلام نماید؛
- مرکز صدور گواهی می‌بایست در مدت زمان تعیین شده توسط مرجع بازرسی کننده، نسبت به رفع نواقص و ناهمخوانی‌ها اقدام نماید؛
- در صورت عدم اصلاح نقص یا ناهمخوانی توسط مرکز صدور گواهی در زمان پیش بینی شده، گزارش مغایرت می‌بایست به اطلاع شورا برسد؛

- شورا می‌تواند راه‌کار مناسبی که شامل تمدید مدت زمان اصلاح نواقص، تعلیق گواهی مرکز صدور گواهی و جلوگیری از فعالیت مرکز صدور گواهی و یا در صورت لزوم ابطال گواهی مرکز صدور گواهی باشد را تعیین نماید.

۸-۶ گزارش نتایج

نتایج بازرسی مرکز دولتی ریشه از مراکز میانی می‌بایست به شورا ارائه گردد؛ ضمن اینکه این نتایج می‌بایست به عنوان اطلاعات محرمانه در نظر گرفته شده و نباید افشا شوند مگر در صورت لزوم با موافقت یا پیرو مجوز مراجع قضایی ذیصلاح.

۹ سایر موارد حقوقی و مربوط به کسب و کار

۹-۱ تعرفه‌ها

مراکز صدور گواهی می‌بایست صرفاً نسبت به دریافت تعرفه از خدماتی اقدام نمایند که از سوی هیئت دولت و یا سایر مراجع ذیصلاح ابلاغ شده است.

۹-۱-۱ تعرفه‌های صدور یا تمدید گواهی

حق ثبت دفاتر ثبت نام مراکز صدور گواهی برای تمامی عملیات مرتبط با گواهی الکترونیکی می‌بایست از تعرفه‌های ابلاغیه هیئت دولت و یا سایر مراجع ذی‌صلاح، تبعیت نماید.

۹-۱-۲ تعرفه‌های دسترسی به گواهی

در حال حاضر نظر به عدم ابلاغ تعرفه از سوی هیئت دولت و یا سایر مراجع ذی‌صلاح، برای دسترسی به گواهی‌ها تعرفه‌ای دریافت نمی‌شود. در صورت تعریف و ابلاغ تعرفه از سوی هیئت دولت و یا سایر مراجع ذی‌صلاح ، ملاک عمل قرار خواهد گرفت.

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

در حال حاضر نظر به عدم ابلاغ تعرفه از سوی هیئت دولت و یا سایر مراجع ذی‌صلاح، برای کلیه خدمات مربوط به ابطال و اعلام وضعیت گواهی تعرفه‌ای دریافت نمی‌گردد. در صورت تعریف و ابلاغ تعرفه از سوی هیئت دولت و یا سایر مراجع ذی‌صلاح ، ملاک عمل قرار خواهد گرفت.

۹-۱-۴ تعرفه سایر خدمات

در حال حاضر نظر به عدم ابلاغ تعرفه از سوی هیئت دولت و یا سایر مراجع ذی‌صلاح، برای سایر خدمات تعرفه‌ای دریافت نمی‌شود. در صورت تعریف و ابلاغ تعرفه از سوی هیئت دولت و یا سایر مراجع ذی‌صلاح ، ملاک عمل قرار خواهد گرفت.

۹-۱-۵ سیاست استرداد

برای کلیه گواهی‌های صادر شده مرکز دولتی ریشه، مراکز میانی و دفاتر ثبت نام، در صورت انصراف از درخواست گواهی قبل از صدور گواهی امکان استرداد وجود دارد و در صورت انصراف بعد از صدور گواهی

امکان استرداد وجود نخواهد داشت. شرایط استرداد می‌بایست در دستورالعمل اجرایی مراکز میانی درج شود. همچنین شرایط آن می‌تواند در توافق‌نامه متقاضی صدور گواهی الکترونیکی به اطلاع وی برسد.

۹-۲ مسئولیت مالی

۹-۲-۱ پوشش بیمه‌ای

پوشش بیمه‌ای در حال حاضر توسط مرکز دولتی ریشه پشتیبانی نمی‌شود، با این وجود مراکز میانی می‌توانند با پیش بینی شرایط بیمه در دستورالعمل خود، با انعقاد قرارداد با شرکت‌های بیمه رسمی کشور، متقاضیان صدور گواهی الکترونیکی را از تسهیلات بیمه بهره‌مند نمایند.

۹-۲-۲ سایر دارایی‌ها

لازم است که مراکز میانی غیر دولتی دارای منابع مالی کافی برای ادامه عملکرد و انجام وظایف و پذیرش مسئولیت‌های خود باشند. مجموعه دارایی‌های مراکز غیردولتی می‌بایست به حدی باشد که خطرات مسئولیت نسبت به مالکان گواهی و طرف‌های اعتماد کننده را تا میزان قابل توجهی پوشش دهد.

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

در حال حاضر پوشش بیمه‌ای همه جانبه ای پیش بینی نشده است، با این وجود برخی از مراکز میانی اشتباهاتی که در فرایند صدور توسط آن مرکز یا سایر اشتباهاتی که در نتیجه قصور و اهمال این مراکز در رعایت ضوابط مربوطه و یا بر اثر نقض وظایف قراردادی بوده را بیمه می‌نمایند، مشروط بر اینکه که متقاضی صدور گواهی الکترونیکی به وظایف قانونی و قراردادی خود عمل نموده باشد. لازم است که اطلاعات مربوط به این ضمانت‌ها در دستورالعمل اجرایی مراکز میانی درج شود.

۹-۳ محرمانگی اطلاعات کسب و کار

۹-۳-۱ محدوده اطلاعات محرمانه

مراکز صدور گواهی می‌بایست اطلاعاتی نظیر اطلاعات ارایه شده زیر را به صورت محرمانه محافظت نماید:

- اطلاعات هر درخواست گواهی که توسط مراکز صدور گواهی نگهداری می‌شود و در گواهی‌های صادر شده وجود ندارد، می‌بایست به صورت محرمانه نگهداری شود.
- کلیه کلیدهای خصوصی و داده‌های فعال‌ساز که در مراکز صدور گواهی و دفاتر ثبت نام بکار گرفته می‌شود؛

- سوابق کاربرد معاملاتی و سوابق کاربرد گواهی الکترونیکی؛
- اطلاعات درخواست گواهی مراکز میانی و دفاتر ثبت نام که ممکن است شامل اطلاعاتی نظیر طرح تجاری، اطلاعات فروش، اسرار تجاری باشد؛
- کلیه اطلاعات مربوط به پیگیری ثبت وقایع که توسط مرکز صدور گواهی ایجاد و نگهداری می‌شوند؛
- تمهیدات امنیتی که برای طرح فنی تجهیزات، ساختمان، نرم‌افزارها و اجرای خدمات گواهی و خدمات تخصیص یافته است.

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

- کلیه اطلاعات موجود در مخزن مراکز صدور گواهی، محرمانه محسوب نمی‌گردد؛
- کلیه اطلاعات شناسایی و اطلاعات دیگری که در گواهی‌ها درج می‌شوند، محرمانه محسوب نمی‌شوند، مگر آنکه در توافق‌نامه‌های منعقده خلاف آن تصریح شده باشد.

۹-۳-۳ مسئولیت محافظت از اطلاعات محرمانه

مراکز صدور گواهی و دفاتر ثبت نام مسئولیت محافظت از کلیه اطلاعات محرمانه در برابر افشا و دسترسی غیر مجاز برای اشخاص غیر مجاز را دارد.

۹-۴ محافظت از اطلاعات خصوصی

هرگونه اطلاعات مربوط به درخواست‌کننده یا مالک گواهی که توسط مراکز صدور گواهی نگهداری می‌شود و در گواهی‌های صادر شده وجود ندارد به عنوان اطلاعات خصوصی یا شخصی تلقی می‌شود. به طور کلی هر قسم اطلاعاتی که بالقوه قابل استفاده به ضرر شخص موضوع اطلاعات یا حداقل به سود اشخاص دیگر باشند را شامل می‌شود. همچنین باید دانست که منظور از اطلاعات خصوصی در این بحث لزوماً اطلاعات سری و دارای ماهیت محرمانه نیست.

۹-۴-۱ طرح حریم خصوصی

طرح حریم خصوصی مالکان گواهی الکترونیکی بر اساس 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.

مراکز میانی می‌توانند در چارچوب قوانین جمهوری اسلامی ایران، طرح حریم خصوصی مورد نظر را در سند دستورالعمل‌های اجرایی خود اعلام نمایند.

۹-۴-۲ اطلاعاتی که خصوصی محسوب می‌شوند

هر گونه اطلاعات درباره درخواست کننده گواهی که جهت صدور گواهی الکترونیکی در اختیار مراکز صدور گواهی قرار می‌گیرد، و عموماً قابل دسترسی نمی‌باشد، خصوصی محسوب می‌شود.

۹-۴-۳ اطلاعاتی که خصوصی محسوب نمی‌شوند

اطلاعات موجود در گواهی منتشر شده که به سهولت قابل رؤیت می‌باشد و یا اطلاعات CRL صادر شده، خصوصی محسوب نمی‌گردد.

۹-۴-۴ مسئولیت محافظت از اطلاعات خصوصی

مراکز صدور گواهی و دفاتر ثبت نام موظفند از کلیه اطلاعات شخصی و خصوصی مالکان گواهی محافظت نمایند.

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

مراکز صدور گواهی مجاز به انتقال اطلاعات خصوصی مالکان گواهی به غیر نمی‌باشند. در صورتی که مالک گواهی قصد داشته باشد که اطلاعات خصوصی او در اختیار ثالث قرار بگیرد، می‌بایست به موجب نامه رسمی و کتبی رضایت خود را به مرکز صدور گواهی اعلام نماید.

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

در شرایطی که به موجب قوانین موضوعه کشور در راستای حفظ امنیت و نظم عمومی و حمایت از حقوق شهروندان، و کشف جرم و تعقیب مجرم، مراکز صدور گواهی موظف به ارائه اطلاعات خصوصی مالکان گواهی به مراجع قضایی و یا ضابطین قضایی می‌باشند، همکاری مذکور صرفاً با دریافت حکم قضایی رسمی، تنظیم شده توسط مرجع ذیصلاح خطاب به مرکز صدور گواهی مربوطه انجام خواهد پذیرفت.

۹-۴-۷ سایر شرایط افشای اطلاعات

قابل اعمال نیست.

۹-۵ حق مالکیت معنوی

- **حق مالکیت معنوی گواهی و اطلاعات ابطال گواهی؛** مالکیت معنوی کلیه گواهی‌های صادره و اطلاعات ابطال گواهی‌ها، متعلق به مراکز صدور گواهی می‌باشد. مالکان گواهی و طرف‌های

اعتماد کننده اجازه استفاده از گواهی‌های صادره را در کاربردهای مجاز و مصارف قانونی مطابق با دستورالعمل تدوین شده مراکز صدور گواهی و توافق‌نامه‌های منعقده، دارا می‌باشند.

- **حق مالکیت معنوی اسناد؛** حق مالکیت معنوی کلیه اسناد تنظیم شده در مراکز صدور گواهی، از جمله دستورالعمل اجرایی صدور گواهی در انحصار مطلق مراکز صدور گواهی تنظیم کننده اسناد می‌باشد.
- **حق مالکیت معنوی نام‌ها؛** هر گواهی الکترونیکی که توسط مراکز صدور گواهی الکترونیکی بر اساس ضوابط صادر می‌شود، در بر گیرنده 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 گواهی، متعلق به مالک این گواهی می‌باشد.
- **سایر موارد؛** حق مالکیت معنوی کلیه اطلاعات منتشر شده در مخزن متعلق به مراکز صدور گواهی می‌باشد.

۹-۶ مسئولیت‌ها و التزامات

۹-۶-۱ مسئولیت‌ها و التزامات مراکز صدور گواهی

۹-۶-۱-۱ التزامات مرکز دولتی ریشه

مرکز دولتی ریشه در موارد زیر مسئولیت دارد:

- پیشنهاد سیاست‌ها و دستورالعمل اجرایی گواهی الکترونیکی مرکز دولتی ریشه و اسناد مرتبط و ارائه به شورا جهت تصویب؛
- اجرای سیاست‌ها و دستورالعمل‌های شورا؛
- به‌روزرسانی این سند به ضمیمه سایر اسناد لازم و ارائه به شورا جهت تصویب؛
- تضمین انطباق عملکرد مرکز دولتی ریشه با این سند؛
- بررسی و تایید دستورالعمل اجرایی گواهی الکترونیکی مراکز میانی؛
- بررسی و احراز شرایط لازم و صلاحیت متقاضیان ایجاد مراکز میانی و صدور مجوز برای آن‌ها؛
- اخذ التزام مناسب از متقاضیان تأسیس مراکز میانی حین تأسیس این مراکز؛

- حصول اطمینان از ثبت اطلاعات معتبر و مناسب در گواهی‌های صادر شده و نگهداری مدارک و شواهد دال بر صحت این اطلاعات؛
- انجام بازرسی‌های دوره‌ای و مقطعی جهت حصول اطمینان از عملکرد صحیح مراکز میانی؛
- اطلاع رسانی عمومی به مالکان گواهی و طرف‌های اعتماد کننده در مورد تغییرات اساسی در عملکرد مراکز صدور گواهی الکترونیکی؛
- ابطال گواهی مراکز میانی که بر خلاف تعهداتشان عمل نموده‌اند؛
- انتشار ابطال مجوز مراکز میانی در سایت و اطلاع رسانی عمومی از طریق درج در روزنامه رسمی؛
- رسیدگی به شکایات واصله مالکان گواهی الکترونیکی و سایر موجودیت‌ها از مراکز میانی؛
- تضمین امنیت داده‌های مربوط به امضا در فرایند ایجاد این داده‌ها برای جلوگیری از شبیه سازی گواهی‌های مراکز میانی
- تضمین ارائه خدمات اعلام وضعیت گواهی مراکز میانی به صورت مطمئن

۹-۶-۱-۲ مسئولیت‌ها و التزامات مراکز صدور گواهی الکترونیکی میانی

مراکز میانی می‌بایست موارد زیر را تضمین نمایند:

- تدوین سند دستورالعمل اجرایی و اخذ تأییدیه از مرکز دولتی ریشه
- 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 مراکز میانی؛
- انطباق و به‌روزرسانی سند دستورالعمل اجرایی گواهی الکترونیکی مراکز میانی با این سند و اخذ تأییدیه از مرکز دولتی ریشه؛
- بررسی صلاحیت و صدور مجوز برای دفاتر ثبت نام متعلق به خود؛
- تضمین ارایه 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 مرکز میانی و دفاتر ثبت نام متعلق به خود؛
- در صورت انجام عملیات تولید زوج کلید به نمایندگی از متقاضی، این عملیات به روش امن و منطبق با بخش ۶-۱-۱-۳ انجام شود؛

- حصول اطمینان از اینکه تولید زوج کلید تحت کنترل انحصاری مالک گواهی باشد؛
- تضمین عدم نسخه برداری از زوج کلید تولید شده توسط مرکز میانی و دفاتر ثبت نام وابسته؛
- مطابقت فعالیت‌های مرکز میانی با این سند، استانداردهای ارائه شده توسط مرکز دولتی ریشه، دستورالعمل اجرایی گواهی الکترونیکی و قرارداد بین مرکز میانی با مرکز دولتی ریشه؛
- تضمین اعمال استانداردهای زیرساخت کلید عمومی کشور؛
- اعلام پذیرش یا رد گواهی میانی خود، 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؛
- اطلاع رسانی سریع به مرکز دولتی ریشه در موقع بروز هرگونه حادثه مانند گم شدن یا در خطر افشا قرار گرفتن کلید و در خواست ابطال گواهی؛
- التزام به قوانین حاکم موضوعه؛
- رعایت موارد امنیتی فیزیکی و الکترونیکی؛
- آگاهی از این مطلب که مرکز میانی مسئول هر گونه خسارت وارده ناشی از تخطی از موارد فوق می‌باشد.

۹-۶-۲ مسئولیت‌ها و التزامات دفاتر ثبت نام

دفاتر ثبت نام مراکز میانی می‌بایست موارد زیر را تضمین نمایند:

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

۹-۶-۳ مسئولیت‌ها و التزامات مالکان گواهی

یک مالک گواهی که برای او توسط یکی از مراکز صدور گواهی، گواهی صادر شده است می‌بایست موارد زیر را تضمین نماید:

- اعتبارسنجی گواهی در زمان استفاده از گواهی مطابق با بخش ۴-۵-۲ از این سند؛
- تولید زوج کلید به روش امن و منطبق با بخش ۶-۱-۱-۳؛
- نگهداری کلید خصوصی به گونه‌ای که اشخاص غیر مجاز هیچ‌گونه دسترسی به آن نداشته باشند؛
- ارائه اطلاعات صحیح مرتبط با تقاضا و اعلام تغییر این اطلاعات در دوره اعتبار گواهی؛
- از گواهی منحصراً می‌بایست در کاربردهای مجاز و قانونی مطابق با کاربردهای مندرج در گواهی استفاده نماید؛
- ارائه درخواست ابطال گواهی مطابق با بخش ۴-۹-۱-۲؛
- اطمینان از اینکه نرم‌افزار بکار گرفته شده، در آزمایشگاه زیرساخت کلید عمومی کشور ارزیابی شده و مورد تأیید مرکز دولتی ریشه باشد؛
- اطمینان از ایمن بودن محیط رایانه‌ای مورد استفاده؛
- پایبندی به قراردادهای فی‌ما بین متقاضی و مرکز صدور گواهی؛
- بکارگیری گواهی در سطح اطمینان متناسب با سطوح اطمینان تعریف شده در بخش ۱-۱؛

۹-۶-۴ مسئولیت‌ها و التزامات طرف‌های اعتماد کننده

طرف اعتماد کننده می‌بایست شرایط زیر را قبل از اعتماد به گواهی در نظر داشته باشد:

- استفاده از مخزن معتبر اعلام شده توسط مرکز صدور گواهی؛
- اعتبارسنجی گواهی در زمان استفاده از گواهی مطابق با بخش ۴-۵-۲ از این سند؛
- دریافت گواهی خودامضای مرکز دولتی ریشه و همچنین گواهی مرکز میانی صادر کننده گواهی از طریق کانال توزیع مطمئن؛
- اطمینان از اینکه گواهی منحصراً در کاربردهای مجاز و قانونی مطابق با کاربردهای مندرج در گواهی بکار گرفته شده است؛
- اطمینان از اینکه نرم‌افزار بکار گرفته شده، در آزمایشگاه زیرساخت کلید عمومی کشور ارزیابی شده و مورد تأیید مرکز دولتی ریشه باشد؛
- اطمینان از اینکه گواهی در سطح اطمینان متناسب با سطوح اطمینان تعریف شده در بخش ۱-۱ بکار گرفته شده باشد؛

- اطمینان از ایمن بودن محیط رایانه‌ای طرف‌های اعتماد کننده؛
- 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

۹-۶-۵-۱ *التزامات شورای سیاست گذاری گواهی الکترونیکی کشور*

مطابق با ماده ۳ آیین نامه اجرایی ماده ۳۲ قانون تجارت الکترونیک، وظایف شورای سیاست گذاری گواهی الکترونیکی کشور عبارتند از:

- بررسی سیاست‌های کلان و برنامه‌های مربوط به حوزه زیر ساخت کلید عمومی کشور؛
- صدور مجوز ایجاد مراکز صدور گواهی الکترونیکی؛
- تصویب سیاست‌ها و دستورالعمل‌های اجرایی گواهی الکترونیکی مراکز صدور گواهی الکترونیکی؛
- تصویب استانداردها، فرایندها و دستورالعمل‌های اجرایی مراکز صدور گواهی الکترونیکی؛
- نظارت عالیه و بررسی گزارش عملکرد و تخلفات احتمالی مرکز ریشه و مراکز میانی در صورت لزوم لغو مجوز آن‌ها؛
- اتخاذ تصمیم در خصوص ایجاد، حذف و اعمال تغییرات در حوزه‌های مختلف زیر ساخت کلید عمومی کشور و سایر فعالیت‌های لازم برای توسعه و بهبود زیر ساخت کلید عمومی کشور؛
- انجام بازرسی از مراکز صدور گواهی الکترونیکی بنا به تشخیص شورا؛
- رسیدگی به اختلافات ایجاد شده بین مراکز صدور گواهی الکترونیکی؛
- رسیدگی به تخلفات گزارش شده مراکز میانی از سوی مرکز دولتی ریشه؛
- نظارت بر عملکرد زیر حوزه‌ها جهت حفظ تعامل و سازگاری با یکدیگر بر سطح ملی و با سایر حوزه‌ها در سطح بین‌المللی.

۹-۶-۵-۲ *التزامات کمیته نظارتی شورا*

مسئولیت‌های این کمیته عبارت است از:

- صدور گواهی الکترونیکی و تولید کلید خودامضا برای مرکز دولتی گواهی الکترونیکی ریشه؛
- صدور گواهی الکترونیکی مراکز میانی که مرکز دولتی ریشه دستورالعمل اجرایی آن را تصویب کرده است؛
- نظارت بر فعالیت و شیوه عملکرد مرکز دولتی ریشه و مراکز میانی؛

- کمیته در دوره‌های زمانی که شورا مشخص خواهد کرد، گزارش جمع بندی خود از نظارت بر مراکز ریشه و میانی را به شورا ارائه خواهد داد.

تبصره- مرجع حل اختلافات ابتدایی مرکز دولتی ریشه و مراکز میانی کمیته نظارتی می‌باشد.

تبصره- جلسات کمیته با حضور ۳ نفر از اعضاء رسمیت می‌یابد. در مراسم صدور گواهی الکترونیکی (تولید کلید خودامضا) مرکز دولتی گواهی الکترونیکی ریشه حضور تمامی اعضای کمیته الزامی است.

۹-۷ عدم پذیرش مسئولیت‌ها و التزامات

به جز مسئولیت‌ها و التزاماتی که در این سند به آن اشاره شد مرکز دولتی ریشه تحت هیچ شرایطی مسئول خسارات مستقیم، غیر مستقیم، تصادفی، استنتاجی، خاص یا کیفری در مورد گواهی‌هایی که توسط مراکز میانی صادر شده است، نمی‌باشد.

مراکز میانی نمی‌توانند از مرکز دولتی ریشه و شورا برای مواردی مانند ابطال یا تعلیق گواهی مرکز میانی ادعای خسارت نمایند. مالکان گواهی و طرف‌های اعتماد کننده نیز نمی‌توانند با استناد به اطلاعات اشتباه وضعیت گواهی فراهم شده توسط مراکز میانی از مرکز دولتی ریشه ادعای خسارت نمایند.

۹-۸ محدودیت مسئولیت‌ها

مراکز صدور گواهی هیچ‌گونه مسئولیتی در مورد خسارت‌های ناشی از پذیرش گواهی‌های صادر شده از سوی طرف‌های اعتماد کننده و یا عدم پذیرش یک گواهی معتبر و یا پذیرش یک گواهی باطل شده یا معلق توسط طرف‌های اعتماد کننده، نمی‌پذیرند.

۹-۹ خسارت‌ها

مراکز صدور گواهی الکترونیکی میانی در صورت اعمال درست سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و ارائه خدمات در راستای قوانین تجارت الکترونیکی و این دستورالعمل اجرایی، هرگونه پرداختی جهت جبران خسارت ناشی از پذیرش و یا عدم پذیرش گواهی‌های صادر شده را نمی‌پذیرد. به علاوه، مرکز دولتی ریشه از هر گونه قصور در انجام تعهدات و عدم توجه منطقی طرف‌های اعتماد کننده و مالکان گواهی رفع مسئولیت می‌نماید.

۹-۱۰ دوره و خاتمه

۹-۱۰-۱ دوره

مادامی که نسخه جدید این سند تصویب و منتشر نشده است، این سند معتبر می‌باشد.

۹-۱۰-۲ خاتمه

به مجرد تصویب و انتشار نسخه جدید، اعتبار این سند، خاتمه می‌یابد.

۹-۱۰-۳ اثرات خاتمه و ابقا

تعریف نشده است.

۹-۱۱ اعلان‌های خاص و ارتباط بین موجودیت‌ها

مراکز صدور گواهی و دفاتر ثبت نام می‌بایست با یکدیگر در ارتباط باشند. این ارتباط ممکن است از طریق ایمیل، فکس، صفحات وب یا هر طریق دیگری که در این سند یا دستورالعمل اجرایی پیش بینی می‌گردد، انجام شود. اطلاع رسانی یا اعلان خاص در این قسمت از آنچه در زمینهٔ انتشار اطلاعات (طبع و نشر) از طریق مخزن در بخش ۲-۲ گفته شد متفاوت می‌باشد.

مراکز صدور گواهی و دفاتر ثبت نام می‌بایست در زمینهٔ اقداماتی که بر روابط آن‌ها با یکدیگر تأثیرگذار است، اطلاع رسانی داشته باشند. به عبارت دیگر اگر دفتر ثبت نام بخواهد به قرارداد خود با مرکز میانی خاتمه دهد موظف است مرکز میانی مزبور را از این اقدام مطلع نماید. همچنین در مواردی که عملیات مرکز صدور گواهی به علت سازماندهی مجدد تشکیلات خاتمه می‌یابد یا قرارداد مرکز میانی با مرکز دولتی ریشه منقضی شده و فعالیت مرکز میانی خاتمه می‌یابد. قبل از خاتمه فعالیت مراکز صدور گواهی می‌بایست اطلاعات این مراکز بایگانی شود.

۹-۱۲ تغییرات

۹-۱۲-۱ فرایند تغییر

هر گونه تغییر در این سند می‌بایست پس از تصویب شورا به صورت عمومی در وب سایت مرکز منتشر شود.

۹-۱۲-۲ دوره و مکانیزم اطلاع‌رسانی

کلیه تغییرات پس از تصویب در این سند می‌بایست حداکثر تا ۵ روز کاری در وب سایت مرکز دولتی ریشه منتشر شود.

۹-۱۲-۳ شرایطی که OID می‌بایست تغییر نماید

کاربردی ندارد.

۹-۱۳ فرایندهای حل اختلاف

در مواقع بروز اختلاف بین مرکز دولتی ریشه و مراکز میانی، ابتدا کمیته نظارتی شورا به اختلاف آن‌ها رسیدگی می‌نماید و در صورت عدم حل اختلاف موضوع در شورا پیگیری می‌شود. هرگونه اختلاف بین مراکز میانی و مالکان گواهی می‌بایست از طریق هیئت حل اختلاف در مراکز میانی برطرف شود و چنانچه اختلافات حادث شده از این طریق حل نشود و به تشخیص مرکز دولتی ریشه قابلیت حل و فصل در این مرکز را هم نداشته باشد، با طرح دعوا در مراجع قضایی ذیصلاح دعوا فیصله می‌یابد.

۹-۱۴ قوانین حاکم

کلیه قوانین موضوعه جمهوری اسلامی ایران از آن جمله قانون تجارت الکترونیکی (مصوب ۱۳۸۲/۱۰/۲۴)، آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی (مصوب در جلسه مورخ ۱۳۸۶/۶/۱۱ 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.

۹-۱۶-۱ توافق‌نامه کلی

تعریف نشده است.

۹-۱۶-۲ تخصیص

تعریف نشده است.

۹-۱۶-۳ عدم وابستگی

مرکز دولتی ریشه دارای شخصیت حقوقی مستقل می‌باشد که در چارچوب قوانین به استقلال عمل می‌نماید.

۹-۱۶-۴ اجرای تعرفه‌های وکالت و فسخ مالکیت

تعریف نشده است.

۹-۱۶-۵ فورس‌ماژور

موارد فورس‌ماژور همان است که در قوانین عام جمهوری اسلامی ایران تدوین شده است. مراکز میانی در صورت تمایل و تا حدی که در قوانین تدوین شده مجاز است، می‌توانند گستره شمول موارد فورس‌ماژور را بسط دهند.

۹-۱۷ سایر قیود

تعریف نشده است.