جمهوری اسلامی ایران

وزارت بازرگانی

معاونت برنامه‌ریزی و امور اقتصادی

دستورالعمل اجرایی گواهی الکترونیکی مرکز دولتی صدور گواهی ریشه

نسخه قابل انتشار

۱۳۸٦/۷/۳۰

بسم الله الرحمن الرحیم

فهرست

مفاهیم ۱۲

۱) مقدمه ۱۶

۱-۱) خلاصه ۱۷

۱-۲) شناسه سند ۱۷

۱-۳) اجزاء و کاربردها ۱۸

۱-۳-۱) موجودیت‌های زیرساخت کلید عمومی ۱۸

۱-۳-۲) کاربردهای زیرساخت کلید عمومی ۲۲

۱-۴) جزئیات تماس ۲۴

۱-۴-۱) راهبری سیاست‌ها ۲۴

۱-۴-۲) اطلاعات تماس مرکز ریشه دولتی صدور گواهی ۲۵

۲) مقررات عمومی ۲۶

۲-۱) وظایف و مسئولیت‌ها ۲۶

۲-۱-۱) وظایف شورای سیاست‌گذاری گواهی الکترونیکی ۲۶

۲-۱-۲) وظایف کمیته نظارتی شورا..... ۲۸

۲-۱-۳) وظایف مرکز دولتی صدور گواهی ریشه..... ۲۸

۲-۱-۴) وظایف دفتر ثبت نام ریشه..... ۳۱

۲-۱-۵) وظایف مراکز صدور گواهی میانی..... ۳۲

۲-۱-۶) وظایف طرفهای اعتماد کننده..... ۳۶

۲-۱-۷) وظایف مخزن..... ۳۷

۲-۲) الزامات..... ۳۸

۲-۲-۱) الزامات مرکز دولتی صدور گواهی و ثبت نام ریشه..... ۳۸

۲-۳) تعهدات مالی..... ۴۱

۲-۳-۱) ادعای خسارت توسط طرفهای اعتماد کننده..... ۴۱

۲-۳-۲) قیمومیت..... ۴۱

۲-۴) تفسیر قانون و ضمانت اجرایی..... ۴۱

۲-۴-۱) قوانین حاکم..... ۴۱

۲-۴-۲) اعتبار، بروزرسانی، انتشار و عدم وابستگی بخشها..... ۴۲

۲-۴-۳) روال‌های حل اختلاف..... ۴۲

۲-۵) تعرفه‌ها ۴۳

۲-۵-۱) تعرفه صدور یا تجدید گواهی ۴۳

۲-۵-۲) تعرفه دسترسی به اطلاعات وضعیت گواهی ۴۳

۲-۵-۳) تعرفه سایر خدمات مانند تعرفه دسترسی به اطلاعات سند سیاست‌های گواهی الکترونیکی مرکز ریشه ۴۴

۲-۵-۴) تعرفه بازپرداخت در صورت انصراف از درخواست گواهی ۴۴

۲-۶) مخزن و انتشار ۴۴

۲-۶-۱) انتشار اطلاعات مرکز دولتی صدور گواهی ریشه ۴۴

۲-۶-۲) تناوب انتشار ۴۵

۲-۶-۳) کنترل دسترسی ۴۵

۲-۶-۴) مـــخـــــــــزن ۴۶

۲-۷) بازرسی ۴۷

۲-۷-۱) تناوب بازرسی ۴۷

۲-۷-۲) هویت و صلاحیت بازرس ۴۷

۲-۷-۳) روابط بازرس با مرکز مورد بازرسی ۴۷

۲-۷-۴) موضوعات مورد بازرسی ۴۸

۲-۷-۵) واکنش‌های اتخاذ شده در برخورد با نقایص ۴۸

۲-۷-۶) گزارش نتایج ۴۹

۲-۸) محرمانگی ۵۰

۲-۸-۱) انواع اطلاعاتی که باید محافظت شوند ۵۰

۲-۸-۲) اطلاعاتی که محرمانه محسوب نمی شوند ۵۱

۲-۸-۳) انتشار اطلاعات ابطال و تعلیق ۵۱

۲-۸-۴) ارائه اطلاعات به مراجع قضائی یا سازمان‌ها ۵۲

۲-۸-۵) ارائه اطلاعات طبق درخواست مراکز صدور گواهی میانی ۵۲

۲-۸-۶) سایر شرایط انتشار اطلاعات ۵۲

۲-۹) حق مالکیت معنوی ۵۳

۳) احراز هویت ۵۴

۳-۱-۱) انواع نام‌ها ۵۴

۳-۱-۲) نیاز به نام‌های با معنی ۵۴

۳-۱-۳) قواعد تفسیر قالب مختلف نام‌ها ۵۵

۳-۱-۴) یکتایی نام‌ها ۵۵

۳-۱-۵) روال حل اختلاف در مورد نام‌ها ۵۶

۳-۱-۶) احراز هویت و نقش علائم تجاری ۵۶

۳-۱-۷) روش اثبات مالکیت کلید خصوصی ۵۶

۳-۱-۸) احراز هویت سازمان‌ها ۵۷

۳-۱-۹) احراز هویت افراد حقیقی ۵۸

۳-۲) روال تجدید کلید ۵۸

۳-۲-۱) روال تجدید کلید گواهی ۵۸

۳-۲-۲) تجدید گواهی ۵۹

۳-۲-۳) بروزرسانی گواهی ۵۹

۳-۳) دریافت یک گواهی جدید پس از ابطال ۶۰

۳-۴) درخواست ابطال ۶۱

۴) خواسته‌های عملیاتی ۶۲

۴-۱) درخواست گواهی ۶۲

۴-۲) مرحله صدور گواهی ۶۵

۴-۳) پذیرش گواهی ۶۶

۴-۴) ابطال و تعلیق گواهی ۶۶

۴-۴-۱) شرایط ابطال ۶۶

۴-۴-۲) کسانی که می‌توانند درخواست ابطال کنند ۶۸

۴-۴-۳) روال درخواست ابطال گواهی ۶۹

۴-۴-۴) مهلت ابطال ۷۱

۴-۴-۵) شرایط تعلیق ۷۱

۴-۴-۶) کسانی که می‌توانند درخواست تعلیق کنند ۷۱

۴-۴-۷) روال درخواست تعلیق ۷۱

۴-۴-۸) محدودیت‌های مدت زمان تعلیق گواهی ۷۱

۴-۴-۹) تناوب صدور لیست گواهی‌های باطل شده ۷۲

۴-۴-۱۰) ملزومات بررسی لیست گواهی‌های باطل شده ۷۲

۴-۴-۱۱) قابل دسترسی بودن سرویس ابطال/اعلام برخط وضعیت گواهی ۷۲

۴-۴-۱۲) روش‌های دیگر آگاهی از ابطال ۷۳

۴-۴-۱۳) ملزومات راه‌های دیگر آگاهی از ابطال ۷۳

۴-۴-۱۴) مقررات خاص مرتبط با در خطر افشا قرار گرفتن کلید ۷۳

۴-۵) روال بازرسی امنیتی ۷۳

۴-۵-۱) انواع وقایع قابل ثبت ۷۴

۴-۵-۲) تناوب پردازش اطلاعات وقایع ثبت‌شده ۷۹

۴-۵-۳) دوره نگهداری از اطلاعات وقایع ثبت‌شده ۷۹

۴-۵-۴) حفاظت از اطلاعات بازرسی امنیتی ۸۰

۴-۵-۵) روال‌های تهیه نسخه پشتیبان از اطلاعات بازرسی امنیتی ۸۰

۴-۵-۶) سیستم جمع‌آوری اطلاعات بازرسی امنیتی ۸۱

۴-۵-۷) اطلاع به مسبب واقعه ۸۱

۴-۵-۸) ارزیابی آسیب‌پذیری ۸۲

۴-۶) بایگانی اطلاعات ۸۲

۴-۶-۱) اطلاعاتی که می‌بایست بایگانی شوند ۸۲

۴-۶-۲) دوره نگهداری اطلاعات بایگانی شده ۸۳

۴-۶-۳) حفاظت از بایگانی ۸۳

۴-۶-۴) روال‌های تهیه نسخه پشتیبان از بایگانی ۸۴

۴-۶-۵) نیازهای مهر زمانی اطلاعات بایگانی ۸۴

۴-۶-۶) سیستم جمع‌آوری بایگانی ۸۵

۴-۶-۷) روال‌های دریافت و بررسی اطلاعات بایگانی ۸۵

۴-۷) گردش کلید ۸۵

۴-۸) بازیابی به علت سوانح غیر مترقبه و در خطر افشا بودن ۸۶

۴-۸-۱) از بین رفتن تجهیزات، نرم افزارها و داده ها ۸۶

۴-۸-۲) ابطال گواهی مرکز دولتی صدور گواهی ریشه ۸۷

۴-۸-۳) در خطر افشا قرار گرفتن کلید مرکز دولتی صدور گواهی ریشه ۸۸

۴-۸-۴) بازیابی خرابی پس از وقوع حوادث طبیعی یا حوادث دیگر ۸۸

۴-۹) توقف سرویس‌دهی مرکز دولتی صدور گواهی ۸۹

۵) راهبری ۹۰

۵-۱) روال تغییر ۹۰

۵-۲) روال انتشار و اطلاع رسانی ۹۲

۵-۳) روال تائید اسناد دستورالعمل اجرائی و سیاست‌های گواهی الکترونیکی ۹۲

۶) مراجع ۹۳

۷) ضمیمه-الف ۹۴

۷-۱) گواهی خودامضای ریشه ۹۴

۷-۲) گواهی میانی ۹۵

۷-۳) لیست گواهی‌های باطل شده مرکز دولتی صدور گواهی ریشه ۹۷

۸) ضمیمه- ب ۹۹

۸-۱) واژه‌نامه ۹۹

مفاهیم

دستورالعمل اجرایی گواهی الکترونیکی: دستورالعمل اجرایی که مرکز صدور گواهی برای صدور گواهی از آن استفاده می‌کند و مجموعه دستورالعمل‌هایی است که منطبق با سند سیاست‌های گواهی جهت تشریح جزئیات عملکرد مدیریت گواهی‌های الکترونیکی در مرکز ریشه و مراکز میانی تدوین می گردد.

اطلاعات فعال‌ساز: اطلاعات خصوصی(غیر از کلیدها) که برای دسترسی به ماجول‌های رمزنگاری مورد نیاز هستند.

امضای الکترونیکی: مقداری که توسط الگوریتم رمزنگاری محاسبه شده و به یک شی اطلاعاتی افزوده می‌شود، به گونه‌ای که هر گیرنده اطلاعات بتواند منبع و تمامیت اطلاعات را تشخیص دهد.

گواهی میانی: گواهی مرکز صدور گواهی میانی که توسط مرکز صدور گواهی ریشه امضا می‌شود و به مرکز صدور گواهی میانی اجازه صدور گواهی برای صاحبان‌امضا را می‌دهد.

گواهی خودامضا: یک گواهی الکترونیکی که در آن، کلید عمومی گواهی و کلید خصوصی استفاده شده برای امضای گواهی، اجزا یک زوج کلید متعلق به امضا کننده هستند. این گواهی‌ها با مجوزها و نظارت تعریف شده در مصوبات شورا ایجاد می‌شوند.

زنجیره گواهی: زنجیره منظم گواهی الکترونیکی که به طرف اعتماد کننده توانایی ارزیابی صحت امضای آخرین گواهی این زنجیره را می‌دهد.

زیرساخت کلید عمومی: مجموعه‌ای از نرم افزارها ،سخت افزارها ،سیاست‌ها ، فرآیندها روال‌های مورد نیاز برای مدیریت گواهی‌ها و زوج کلیدها

سیاست‌های گواهی الکترونیکی: مجموعه سیاست‌های گواهی الکترونیکی مشتمل بر سیاست‌ها ، قوانین و مقررات و روش‌های فنی و حقوقی و ساختاری که مطابق با استانداردهای بین‌المللی تدوین شده و حداقل خواسته‌ها و الازمات پایده سازی مراکز صدور گواهی، دفاتر ثبت نام، صاحبان امضا و طرف‌های اعتماد کننده را مشخص می کند. تدوین این سیاست‌های گواهی برای مرکز ریشه الزامی است و می تواند برای مرکز میانی به طور جداگانه تنظیم گردد.

صاحب‌امضا: شخصی که برای وی گواهی الکترونیکی صادر شده است و می‌تواند از کلید خصوصی مرتبط با کلید عمومی درون گواهی استفاده کند.

طرف اعتماد کننده: شخصی که به اعتبار اطلاعات گواهی الکترونیکی اعتماد می‌کند.

کلید خصوصی: جزء مخفی زوج کلید رمزنگاری که برای رمزنگاری نامتقارن استفاده می‌شود.

کلید عمومی: جزء زوج کلید رمزنگاری که قابل افشا برای عموم می‌باشد و در الگوریتم رمزنگاری نامتقارن استفاده می‌شود.

گواهی الکترونیکی: داده الکترونیکی حاوی اطلاعاتی در مورد مرکز صادر کننده گواهی، مالک گواهی، تاریخ صدور و انقضا، کلید عمومی مالک و یک شماره سریال میباشد که توسط یک مرکز صدور گواهی تولید و امضا شده به گونه ای که هر شخصی میتواند به صحت ارتباط بین کلید عمومی و مالک گواهی اطمینان کند.

لیست گواهی‌های باطل شده: یک ساختار داده که گواهی‌های الکترونیکی را که دیگر توسط صادر کننده گواهی معتبر به حساب نمی‌آیند، لیست می‌کند. بعد از اینکه یک گواهی در لیست گواهی‌های باطل شده وارد می‌شود، از لیست‌گواهی‌های باطل شده بعدی پس از انقضا حذف می‌شود.

سخت‌افزار سخت‌افزاری رمزنگاری: مجموعه‌ای از سخت‌افزار، نرم‌افزار و ترکیب آنها که فرایند و منطق رمزنگاری را مانند الگوریتم رمزنگاری اجرا می‌کند و در محدوده رمزنگاری سخت‌افزارقرار دارد.

مخزن: یک پایگاه داده ذخیره و انتشار گواهی‌های الکترونیکی و اطلاعات مربوط به آنها جهت بهره برداری طرف‌های اعتماد کننده است .

دفتر ثبت نام: یک موجودیت اختیاری در زیر ساخت کلید عمومی می‌باشد که گواهی‌های الکترونیکی یا لیست گواهی‌های باطل شده را امضا نمی‌کند 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.

مرکز صدور گواهی: موجودیتی که گواهی الکترونیکی صادر می‌کند و پیوند بین داده‌های گواهی را ضمانت می‌کند.

مرکز صدور گواهی میانی: یک مرکز صدور گواهی که با کسب مجوز از یک مرکز ریشه و گرفتن گواهی خود را از آن مرکز صدور گواهی ریشه می‌تواند برای صاحبان امضا گواهی صادر کند.

مرکز صدور گواهی ریشه: یک مرکز صدور گواهی که مستقیماً مورد اطمینان موجودیت نهایی می‌باشد. به دست آوردن کلید عمومی مرکز صدور گواهی ریشه نیاز به مکانیسم‌های ضامن سلامت و دست نخوردگی دارد.

موجودیت نهایی: موجودیتی که از کلیدها و گواهی‌ها برای ایجاد یا تشخیص صحت امضا یا محرمانگی آن استفاده می‌کند.موجودیت‌های نهایی صاحبان امضا، سازمان‌ها یا طرفهای اعتماد کننده می‌باشند.

عنوان گواهی: نامی که به اطلاعات موجود در گواهی الکترونیکی، بخصوص به مقدار کلید گواهی الکترونیکی پیوند داده شده است.

۱) مقدمه

"دستورالعمل اجرایی گواهی الکترونیکی[۱]" مرکز دولتی صدور گواهی ریشه[۲] بر اساس "سیاست‌های گواهی الکترونیکی[۳]" ریشه در راستای ایجاد زیرساخت کلید عمومی[۴] در کشور، تولید شده است. این دستورالعمل بر پایه استاندارد X.509 تنظیم شده و با قانون تجارت الکترونیکی جمهوری اسلامی ایران و آیین نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی مصوب ۱۳۸۶/۶/۱۱ هیئت دولت همخوانی دارد.

این دستورالعمل چگونگی ایجاد و مدیریت مراکز صدور گواهی میانی را توسط مرکز دولتی صدور گواهی الکترونیکی ریشه مشخص می‌کند.

[1] Certificate Practice Statement
[2] Root Certificate Authority
[3] Certificate Policy
[4] Public Key Infrastructure

۱-۱) خلاصه

مرکز دولتی صدور گواهی الکترونیکی ریشه، بالاترین مرکز دولتی صدور گواهی[1] در ساختار سلسله مراتبی مراکز صدور گواهی الکترونیکی جمهوری اسلامی ایران می‌باشد. مرکز دولتی صدور گواهی الکترونیکی ریشه نقطه اطمینان زیر ساخت کلید عمومی می‌باشد.

شورای سیاست‌گذاری گواهی الکترونیکی، سازمان مدیریتی مرکز دولتی صدور گواهی الکترونیکی ریشه می‌باشد. کلیه تغییرات در دستورالعمل اجرایی گواهی الکترونیکی مرکز دولتی صدور گواهی الکترونیکی ریشه تنها پس از تصویب این شورا، قابل اجرا است. این دستورالعمل، فقط به موجودیت‌های وابسته به مرکز دولتی صدور گواهی الکترونیکی ریشه شامل دفتر ثبت نام ریشه[2] و مراکز صدور گواهی میانی[3] که گواهی خود را از این مرکز دریافت کرده‌اند، می‌پردازد.

۱-۲) شناسه سند

از این پس، سند فعلی بنام سند دستورالعمل اجرایی گواهی الکترونیکی ریشه شناخته می‌شود. این سند در اولین جلسه شورای سیاست گذاری گواهی الکترونیکی کشور مورخ ۱۳۸۶/۰۷/۳۰ به تصویب رسید. تاریخ انتشار

[1] Certificate Authority
[2] Root Registration Authority
[3] Intermediate certificate Authorities

سند ۱۳۸۶/۰۷/۳۰ می‌باشد. آخرین نسخه این سند در سایت مرکز دولتی صدور گواهی ریشه به آدرس http://www.rca.gov.ir قابل دسترسی است.

۱-۳) اجزاء و کاربردها

۱-۳-۱) موجودیت‌های زیرساخت کلید عمومی

۱-۳-۱-۱) شورای سیاست‌گذاری گواهی الکترونیکی

به منظور حفظ یکپارچگی و جلوگیری از تفکیک راهکارها و استانداردهای بکار گرفته شده در مراکز صدور گواهی ریشه و میانی و نیز سیاست‌گذاری در زمینه فعالیت‌های مرکز دولتی صدور گواهی ریشه و به روز رسانی این دستورالعمل و تأیید تطابق دستورالعمل اجرایی تمام مراکز صدور گواهی با سند سیاست‌های گواهی الکترونیکی مرکز ریشه و این دستورالعمل ، شورایی به نام شورای سیاست‌گذاری گواهی الکترونیکی کشور تشکیل شده است. از این پس، در این سند شورای سیاست‌گذاری گواهی الکترونیکی کشور ، به اختصار "شورا" نامیده می‌شود.

۱-۳-۱-۲) کمیته نظارتی شورا

به منظور انجام فعالیت‌های نظارتی، شورا کمیته‌ای با نام کمیته نظارتی را با عضویت ۵ نفر (ترجیحا از اعضای خود) به مدت یک سال انتخاب می کند.

۱-۳-۱-۳) مرکز دولتی صدور گواهی ریشه

مرکز دولتی صدور گواهی ریشه نقطه اطمینان زیر ساخت کلید عمومی می‌باشد.

این مرکز براساس مفاد بند الف از ماده ۴ آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و طی اولین جلسه شورای سیاست گذاری گواهی الکترونیکی کشور در مورخ ۱۳۸۶/۷/۳۰ مجوز ایجاد، امضاء و صدور گواهی‌های میانی را دریافت کرده است. یک مرکز صدور گواهی ریشه مسئول تمام ابعاد صدور و مدیریت گواهی‌های میانی، شامل نظارت بر فرآیند ثبت نام، فرآیند احراز هویت، فرآیند صدور گواهی‌های میانی، انتشار این گواهی‌ها، لغو آنها و تجدید کلید؛ و تضمین تطابق تمام ابعاد خدمات و عملیات این مرکز و زیرساخت مربوط به صدور گواهی تحت سیاست‌های گواهی الکترونیکی ریشه و مطابق با خواسته‌ها و ضمانت‌های آن سیاست‌ها، می‌باشد.

۱-۳-۱-٤) دفتر ثبت نام ریشه

دفتر ثبت نام ریشه موجودیتی است که برای جمع‌آوری و بررسی صحت اطلاعات مربوط به هویت مراکز صدور گواهی میانی که در گواهی الکترونیکی وارد خواهد شد، با مرکز دولتی صدور گواهی ریشه عقد قرارداد کرده است.

۱-۳-۱-۵) مرکز صدور گواهی میانی

به مراکز صدور گواهی که مجوز فعالیت و گواهی خود را از یک مرکز ریشه دریافت نموده‌اند، مرکز صدور گواهی میانی گفته می‌شود. مراکز صدور گواهی میانی صلاحیت صدور و ابطال گواهی الکترونیکی صاحبان امضا را دارا می‌باشند.

مراکز صدور گواهی میانی به منظور دریافت گواهی خود باید مطابق با شرایط سیاست‌های گواهی الکترونیکی ریشه عمل کنند. به علاوه این مراکز باید توانایی مدیریت موارد زیر را دارا باشند:

- زیر ساخت کلید عمومی؛
- تکنولوژی امضای الکترونیکی و صدور گواهی؛
- تعهدات و مسئولیت‌های مربوطه، بین مراکز صدور گواهی، دفاتر ثبت نام و طرفهای اعتماد کننده.

۱-۳-۱-۶) صاحبان امضاء[1]

صاحب امضاء موجودیتی است که نامش در "عنوان" گواهی ثبت می‌شود.

هر چند مراکز صدور گواهی از نظر فنی در زیرساخت کلید عمومی، یک صاحب امضاء می‌باشند اما عبارت صاحب امضاء در این سند به کسانی اشاره دارد که از یک مرکز صدور گواهی میانی، گواهی دریافت نموده‌اند.

۱-۳-۱-۷) طرفهای اعتماد کننده

طرف اعتماد کننده موجودیتی است که به درستی پیوند میان نام صاحب امضاء با کلید عمومی‌اش اعتماد می‌کند. طرف اعتماد کننده مسئول کنترل اعتبار گواهی الکترونیکی از طریق بررسی اطلاعات گواهی می باشد و از گواهی الکترونیکی برای موارد زیر می تواند استفاده کند:

- اطمینان از یکپارچگی و عدم تغییر پیام با امضای الکترونیکی
- تشخیص سازنده و ارسال کننده پیام
- برقرای ارتباط محرمانه با صاحب گواهی الکترونیکی

[1] Subscriber

۱-۳-۲) کاربردهای زیرساخت کلید عمومی

مرکز دولتی صدور گواهی الکترونیکی ریشه جمهوری اسلامی ایران، ۲ نوع گواهی صادر می‌کند:

الف) گواهی خود امضاء؛

ب) گواهی‌های میانی.

گواهی خود امضاء یک نقطه اطمینان برای مرکز دولتی صدورگواهی ریشه ایجاد می‌کند. گواهی میانی توسط مرکز دولتی صدور گواهی ریشه برای مراکز صدور گواهی مورد تأیید صادر می‌شود و داشتن یک گواهی میانی به معنای صلاحیت صدور گواهی برای صاحبان امضاء می‌باشد.

عنوان گواهی خودامضاء، نام مرکز دولتی صدورگواهی ریشه می‌باشد و مانند هر گواهی دیگری، گواهی خودامضاء شامل کلید عمومی صاحب آن که همان مرکز دولتی صدور گواهی الکترونیکی ریشه است، می‌باشد. هر کسی می‌تواند از گواهی خودامضاء برای بررسی صحت امضای گواهی میانی و لیست گواهی‌های باطل شده که توسط مرکز دولتی صدور گواهی ریشه صادر شده است، استفاده کند.

عنوان گواهی میانی نام مرکز صدور گواهی میانی درخواست‌کننده گواهی می‌باشد. تعداد مراکز صدور گواهی میانی ممکن است بیشتر از یکی باشد. در گواهی میانی کلید عمومی مرکز صدور گواهی میانی نیز وجود

دارد. هر کسی می‌تواند از گواهی میانی برای بررسی اعتبار گواهی صاحبان امضاء و لیست گواهی‌های باطل شده امضا شده توسط مرکز صدور گواهی الکترونیکی میانی، استفاده کند.

به منظور استفاده از گواهی‌ها، طرفهای اعتماد کننده می‌بایست گواهی خودامضاء مرکز دولتی صدور گواهی الکترونیکی ریشه یا کلید عمومی آن مرکز را از یک کانال امن دریافت کنند.

سپس طرفهای اعتماد کننده با استفاده از کلید عمومی مطمئن می‌توانند از صحت امضای گواهی‌های میانی و لیست گواهی‌های باطل شده ارائه شده توسط مرکز دولتی صدور گواهی الکترونیکی ریشه، اطمینان حاصل کنند.

طرفهای اعتماد کننده می‌بایست از محیط اطلاعاتی مطمئنی، مانند سیستم‌های عملیاتی ایمن و سیستم‌های کاربردی مورد اطمینان برای ذخیره اطلاعات مهم استفاده کنند. این امر باعث جلوگیری از تعویض گواهی خود امضاء مرکز دولتی صدور گواهی الکترونیکی ریشه با گواهی‌های دیگر و یا تعویض کلید عمومی مرکز دولتی صدور گواهی الکترونیکی ریشه با کلیدی دیگر می‌شود. طرفهای اعتماد کننده همچنین می‌بایست از صحت گواهی خود امضاء و کلید عمومی مرکز دولتی صدور گواهی الکترونیکی ریشه قبل از استفاده از آنها، اطمینان حاصل کنند.

در نتیجه، طرفهای اعتماد کننده می‌توانند از این اطلاعات به منظور اعتماد یا عدم اعتماد به گواهی‌هایی که توسط یک مرکز صدور گواهی میانی ارائه شده، استفاده کنند.

طرفهای اعتماد کننده باید پیش از استفاده از سرویس‌های مرکز صدور گواهی، از مطالب این دستورالعمل اجرایی، آگاهی کامل داشته باشند و همچنین به تعهدات مذکور در این دستورالعمل برای طرفهای اعتماد کننده، پایبند باشند و هرگونه تغییر در این سند را از طریق مخزن پیگیری نمایند.

۱-۳-۲-۱) ممنوعیت‌های استفاده از گواهی

- ارسال و دریافت اطلاعات نظامی طبقه‌بندی شده یا عملکرد تاسیسات هسته‌ای
- ارتکاب جرم

۱-٤) جزئیات تماس

۱-٤-۱) راهبری سیاست‌ها

مرکز دولتی صدور گواهی الکترونیکی ریشه مسئولیت تولید دستورالعمل اجرایی گواهی الکترونیکی ریشه را دارد. این دستورالعمل تنها پس از دریافت مجوز از شورا قابل اجرا است.

آدرس: خیابان کارگر شمالی، روبروی پارک لاله، ساختمان ۲۴۰، طبقه ۵، دفتر توسعه تجارت الکترونیکی

۱-٤-۲) اطلاعات تماس مرکز ریشه دولتی صدور گواهی

سئوالات مربوط به این دستورالعمل، توسط مرکز دولتی صدور گواهی ریشه پاسخ داده می‌شود:

آدرس الکترونیکی: oec@prd.moc.gov.ir

تارنما: http://www.prd.moc.gov.ir

شماره تلفن: :۰۲۱-۶۶۹۲۴۶۲۳

شماره فکس: ۰۲۱-۶۶۹۲۶۳۲۶

۲) مقررات عمومی[1]

۲-۱) وظایف و مسئولیت‌ها

۲-۱-۱) وظایف شورای سیاست‌گذاری گواهی الکترونیکی

وظایف و مسئولیت‌های شورای سیاست‌گذاری گواهی الکترونیکی شامل موارد زیر می‌باشد:

- بررسی سیاستهای کلان و برنامه های مربوط به حوزه زیرساخت کلید عمومی کشور و ارایه آن به شورای عالی فناوری اطلاعات کشور جهت تصویب
- صدور مجوز ایجاد مرکز ریشه
- تصویب و به روزرسانی سیاستها و دستورالعمل گواهی مراکز ریشه و میانی
- تصویب استانداردها، رویه‌ها و دستورالعملهای اجرایی گواهی الکترونیکی
- ایفای نقش به عنوان مرجع هماهنگ کننده در مورد فعالیت حوزه‌های گوناگون اجرایی برای ارایه خدمات رایانه‌ای صدور گواهی مبتنی بر زیرساخت کلید عمومی و نحوه تعامل مراکز صدور گواهی

[1] General Provisions

داخلی با مرکز صدور گواهی خارجی و هرگونه تفسیر یا کاربردپذیری مفاد سیاست‌های گواهی ریشه و میانی

- نظارت عالیه و بررسی گزارش عملکرد و تخلفات احتمالی مراکز ریشه و میانی و در صورت لزوم لغو مجوز آنها.
- تصویب و بروزرسانی دستورالعمل تایید مراکز صدور گواهی جهت ایجاد، امضا و صدور گواهی‌های الکترونیکی؛
- تصمیم‌سازی در زمینه ایجاد، حذف و اعمال تغییرات در حوزه‌های مختلف زیرساخت کلید عمومی فضای تبادل اطلاعات کشور و سایر فعالیت‌های لازم برای توسعه و بهبود زیر ساخت کلید عمومی در کشور؛
- نظارت بر عملکرد زیرحوزه‌ها جهت حفظ تعامل و سازگاری با یکدیگر در سطح ملی و با سایر حوزه‌ها در سطح بین‌المللی؛
- بررسی راه‌حل‌های ارائه شده توسط مراکز صدور گواهی یا مراجع اعلام وضعیت گواهی‌ها در برخورد با مشکلات امنیتی؛

۲-۱-۲) وظایف کمیته نظارتی شورا

وظایف این کمیته عبارت است از:

- صدور گواهی الکترونیکی (تولید کلید خود امضا) مرکز دولتی گواهی الکترونیکی ریشه
- صدور گواهی الکترونیکی مراکز میانی که شورای سیاست گذاری دستورالعمل اجرایی آنها را تصویب کرده است
- نظارت بر فعالیت و شیوه عملکرد مرکز دولتی گواهی الکترونیکی ریشه و مراکز میانی
- بررسی اختلافات حل نشده مرکز دولتی گواهی الکترونیکی ریشه با مراکز میانی
- جلسات کمیته با حضور ۳ نفر از اعضا رسمیت می یابد.
- در مراسم صدور گواهی الکترونیکی (تولید کلید خود امضا) مرکز دولتی گواهی الکترونیکی ریشه حضور تمامی اعضای کمیته الزامی است.
- کمیته در دوره‌های زمانی که شورا مشخص خواهد کرد، گزارش جمع‌بندی خود از نظارت بر مراکز ریشه و میانی را به شورا ارایه خواهد داد.

۲-۱-۳) وظایف مرکز دولتی صدور گواهی ریشه

مرکز دولتی صدور گواهی الکترونیکی ریشه در موارد زیر مسئول است:

- پیشنهاد سیاست ها و دستورالعمل گواهی مرکز دولتی ریشه و ارایه به شورا جهت تصویب
- اجرای سیاست‌ها و دستورالعمل‌های شورا
- بررسی و تصویب سیاست‌ها و دستورالعمل مراکز میانی
- بررسی و احراز شرایط لازم و صلاحیت متقاضیان ایجاد مراکز میانی و صدور مجوز برای آنها
- حصول اطمینان از ثبت اطلاعات معتبر و مناسب در گواهی‌های خود و نگهداری مدارک و شواهد دال بر صحت این اطلاعات
- حصول اطمینان از عملکرد صحیح مراکز میانی
- اطلاع‌رسانی به صاحبان امضا و طرفهای اعتمادکننده در مورد هرگونه تغییر در کارکرد مرکز میانی
- تضمین ارایه خدمات تأیید صحت گواهیها به صورت سریع و مطمئن
- تضمین محرمانه بودن داده‌های مربوط به امضا در فرآیند ایجاد این داده‌ها برای جلوگیری از شبیه‌سازی گواهیها
- ارائه دستورالعمل اجرایی گواهی الکترونیکی و تغییرات بعدی آن به شورا، برای ارزیابی مطابقت با سیاست‌های گواهی دیجتال ریشه؛
- اطمینان از تطابق عملکرد مرکز دولتی با سیاست‌های گواهی الکترونیکی ریشه و این دستورالعمل؛

- بیان روال‌های درخواست گواهی‌های میانی برای مراکز صدور گواهی بالقوه؛
- نظارت بر عملکرد دفتر ثبت نام طرف قرارداد خود نموده و در صورت احراز تخلف طبق ضوابط با آن برخورد کرده و در صورت لزوم با رعایت تمهیدات پیش‌بینی شده در دستورالعمل گواهی نسبت به لغو مجوز دفتر ثبت‌نامه متخلف اقدام خواهد نماید.
- اطمینان از دریافت درخواست گواهی صرفاً از دفتر ثبت نام ؛
- صدور و انتشار گواهی‌ها؛
- ابطال گواهی مراکز میانی که بر خلاف تعهداتشان عمل کرده‌اند (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 باید به روش مندرج در بند (خ) ماده (۵) آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و درج در روزنامه‌رسمی جمهوری اسلامی ایران فهرست گواهی‌های باطل شده را منتشر نماید)؛
- ابلاغ و اطلاع‌رسانی به مراکز صدور گواهی میانی در مورد هرگونه تغییر در کارکرد مرکز دولتی صدورگواهی ریشه که تغییر ایجاد شده در منافع صاحبان امضاء و طرفهای اعتماد کننده، در راستای امنیت یا همکاری متقابل، تاثیرگذار باشد. به عنوان مثال: تمدید طول عمر یک گواهی ریشه خود امضاء؛

- فراهم آوردن سرویس‌های یک مخزن برخط[1] مطابق با تعهدات بخش ۲-۱-۷) و آگاه‌سازی عرضه‌کننده سرویس مخزن از این تعهدات؛
- ارسال گواهی‌ها و لیست گواهی‌های باطل شده به مخزن؛
- تولید کلیدهای خصوصی مرکز دولتی صدور گواهی الکترونیکی ریشه به طور ایمن؛
- اطمینان از نگهداری ایمن کلیدهای خصوصی مرکز دولتی صدور گواهی الکترونیکی ریشه.

۲-۱-٤) وظایف دفتر ثبت نام ریشه

دفتر ثبت نام ریشه در موارد زیر مسئولیت دارد:

- اطمینان از اینکه عملیات آن مطابق با این دستورالعمل انجام می‌گیرد؛
- احراز هویت مراکز صدور گواهی میانی بالقوه هنگام درخواست گواهی میانی و درخواست ابطال گواهی؛
- تحویل گواهی صادر شده به مرکز صدور گواهی میانی درخواست‌کننده.

[1] Online Repository

۲-۱-۵) وظایف مراکز صدور گواهی میانی

مراکز صدور گواهی میانی که خود مشترکین مرکز دولتی صدور گواهی الکترونیکی ریشه هستند در موارد زیر مسئولیت دارند:

- بررسی صلاحیت و صدور مجوز برای دفاتر ثبت‌نام ذی‌ربط
- تضمین ارایه خدمات صدور و لغو گواهیها به صورت مطمئن.
- تضمین ارایه خدمات تأیید صحت گواهیها به صورت سریع و مطمئن.
- تضمین محرمانه بودن داده‌های مربوط به امضا در فرآیند ایجاد این داده‌ها برای جلوگیری از شبیه‌سازی گواهیها.
- حصول اطمینان نسبت به موارد زیر:

۱- در لحظه صدور گواهی الکترونیکی، اطلاعات مندرج در گواهیها صحیح باشند.

۲- در هنگام صدور گواهی الکترونیکی، امضا کننده مشخص شده در گواهی، داده‌های ایجاد و وارسی امضای الکترونیکی را دریافت نموده و داده ایجاد امضای الکترونیکی تحت کنترل انحصاری وی باشد.

۳- کلیه اطلاعات مرتبط با گواهی الکترونیکی را تا مدت زمان تعیین شده در دستورالعمل گواهی به صورت الکترونیکی حفظ نماید.

۴- تاریخ و ساعت صدور و لغو یک گواهی به دقت تعیین شده و قابل تشخیص باشد.

۵- عدم کپی یا ذخیره داده ایجاد امضای الکترونیکی متقاضیان را تضمین نماید.

۶- گواهی قابل دسترسی برای عموم نباشد، جز در مواردی که صاحبان گواهیها رضایت خود را اعلام کرده‌اند یا نوع گواهی انتشار عمومی را ایجاب نماید.

۷- در صورت امکان مرکز میانی و با دریافت درخواست دفترثبت نام، یک مهر زمانی به داده‌های الکترونیکی ضمیمه شود.

تبصره ۱- هر مرکز میانی موظف است فهرستی از گواهیهایی را که توسط آن مرکز صادر می‌شود با ذکر تاریخ صدور، نام صاحب گواهی و نوع گواهی تهیه و منتشر نماید. اطلاعات مزبور باید در جایگاه اینترنتی مربوط درج گردد.

تبصره ۲- مرکز میانی بر عملکرد دفاتر ثبت نام طرف قرارداد خود نظارت داشته و در صورت احراز تخلف طبق ضوابط با آن برخورد کرده و در صورت لزوم با رعایت تمهیدات پیش‌بینی شده در دستورالعمل گواهی نسبت به لغو مجوز دفتر ثبت نام متخلف اقدام خواهد نمود.

- تدوین دستورالعمل اجرایی گواهی الکترونیکی خود مطابق با سیاست‌های گواهی الکترونیکی ریشه؛
- مطابقت فعالیت‌ها با مقررات دستورالعمل اجرایی گواهی الکترونیکی خود و قرارداد بین مرکز صدور گواهی میانی با مرکز دولتی صدور گواهی الکترونیکی ریشه و آگاهی از این مطلب که مرکز صدور گواهی میانی مسئول هر گونه خسارت وارده ناشی از تخطی از موارد فوق می‌باشد؛
- فراهم آوردن اطلاعات معتبر برای مرکز دولتی صدور گواهی الکترونیکی ریشه در مورد درخواست گواهی‌های میانی (مطابق با بخش ۴-۱) این دستورالعمل)؛
- پذیرش یا رد گواهی میانی خود، پس از دریافت ابلاغیه صدور گواهی (مطابق با بخش ۴-۳) این دستورالعمل)؛
- آگاهی کامل از این امر که پذیرش گواهی میانی صادر شده توسط مرکز دولتی صدور گواهی الکترونیکی ریشه بدین معناست که مرکز صدور گواهی میانی صحت اطلاعات آن گواهی را تائید می‌کند؛
- تولید ایمن کلیدهای خصوصی خود (مطابق با سیاست‌های گواهی الکترونیکی ریشه و دستورالعمل اجرایی مربوطه)؛
- اطمینان از نگهداری ایمن و استفاده صحیح از کلیدهای خصوصی خود؛

- آگاهی کامل از نتایج قانونی تولید امضای الکترونیکی با استفاده از کلید خصوصی متناظر با کلید عمومی موجود در گواهی خود؛
- آگاهی کامل از این امر که تولید امضای الکترونیکی با استفاده از کلید خصوصی فقط در زمانی که گواهی صادر شده از سوی مرکز ریشه اعتبار دارد و مرکز صدور گواهی میانی، پذیرش گواهی را تأیید کرده باشد و گواهی باطل نشده باشد، امکان پذیر است؛
- اطلاع رسانی سریع به مرکز دولتی صدور گواهی الکترونیکی ریشه در موقع بروز هرگونه حادثه مانند گم شدن یا در خطر افشا قرار گرفتن کلید و درخواست ابطال گواهی (مطابق با قسمت ۴-۴) این دستورالعمل)؛
- آگاهی از این امر که مسئولیت کامل مرکز صدور گواهی میانی تا قبل از انتشار اطلاعات مربوط به ابطال گواهی‌اش ، توسط مرکز دولتی صدور گواهی الکترونیکی ریشه، کماکان پابرجاست.
- اجرای تعهدات یا مسئولیت‌ها در قبال طرفهای اعتماد کننده و آگاهی کامل از این مسئله که مرکز صدور گواهی میانی نمی‌تواند از غیر قابل دسترس بودن خدمات گواهی و مخزن مرکز دولتی صدور گواهی الکترونیکی ریشه برای نقض تعهدات خود در مورد طرفهای اعتماد کننده استفاده کند.

۲-۱-٦) وظایف طرفهای اعتماد کننده

طرفهای اعتماد کننده در موارد ذیل مسئولیت دارند:

- مطابقت با این دستورالعمل در هنگام استفاده از گواهی‌های صادر شده توسط مرکز دولتی صدور گواهی الکترونیکی ریشه و یا در هنگام درخواست اطلاعات منتشر شده در مخزن مرکز دولتی صدور گواهی الکترونیکی ریشه؛
- دریافت گواهی خود امضای مرکز دولتی صدور گواهی الکترونیکی ریشه، از طریق کانال توزیع مطمئن؛
- تشخیص قابلیت بکارگیری گواهی‌های صادر شده توسط مرکز دولتی صدور گواهی الکترونیکی ریشه از طریق بررسی کاربرد کلید آنها که توسط مرکز دولتی صدور گواهی الکترونیکی ریشه تأیید شده است؛
- تشخیص اعتبار گواهی‌های صادر شده توسط مرکز دولتی صدور گواهی الکترونیکی ریشه از طریق بررسی لیست گواهی‌های باطل شده منتشر شده در مخزن؛
- بررسی صحت امضای الکترونیکی گواهی‌ها و لیست گواهی‌های باطل شده منتشر شده توسط مرکز دولتی صدور گواهی الکترونیکی ریشه؛

- اطمینان از ایمن بودن محیط رایانه‌ای طرفهای اعتماد کننده و اطمینان از قابل اعتماد بودن سیستم‌های کاربردی و آگاهی کامل از این مسئله که در غیر این صورت هر گونه خسارت خرابی متوجه طرفهای اعتماد کننده می‌باشد؛
- اجرای تعهدات یا مسئولیت‌ها در قبال سایر طرفهای اعتماد کننده و آگاهی کامل از این مسئله که غیر قابل دسترس بودن خدمات صدور گواهی و یا مخزن مرکز دولتی صدور گواهی الکترونیکی ریشه نمی‌تواند باعث نقض تعهدات طرفهای اعتماد کننده شود.

۲-۱-۷) وظایف مخزن

مخزن مرکز دولتی صدور گواهی الکترونیکی ریشه در موارد زیر مسئولیت دارد:

- انتشار منظم گواهی‌های صادر شده، لیست گواهی‌های باطل شده و سایر اطلاعات مربوطه مطابق با بخش ۲-۶) این دستورالعمل اجرایی؛
- انتشار آخرین اطلاعات سیاست‌های گواهی الکترونیکی ریشه و این دستورالعمل ؛
- فراهم نمودن مکانیزم‌های کنترل دستیابی به راهبری مخزن به منظور محافظت از اطلاعات مخزن مطابق با بخش ۲-۶-۳) این دستورالعمل؛
- اطمینان از در دسترس بودن مخزن.

۲-۲) الزامات

۲-۲-۱) الزامات مرکز دولتی صدور گواهی و ثبت نام ریشه

مرکز دولتی صدور گواهی الکترونیکی ریشه، تضمین می‌کند که فعالیت‌هایش مطابق با سیاست‌های گواهی الکترونیکی ریشه انجام می‌شود و همچنین متعهد می‌شود که روال‌های لازم جهت پیاده‌سازی فرآیند صدور و ابطال گواهی‌ها، سرویس های مخزن و ارائه لیست گواهی‌های باطل شده را مطابق با این دستورالعمل انجام دهد.

دفتر ثبت نام ریشه، تضمین می‌کند که فعالیت‌هایش مطابق با سیاست‌های گواهی الکترونیکی ریشه انجام می‌شود و همچنین متعهد می‌شود که روال‌های لازم جهت احراز هویت درخواست صدور و ابطال گواهی‌ها، اطلاع‌رسانی به مراکز صدور گواهی میانی را مطابق با این دستورالعمل انجام دهد.

۲-۲-۱-۱) خسارت های تحت پوشش و رفع مسئولیت از مرکز دولتی صدور گواهی

صاحبان امضا و طرفهای اعتماد کننده نباید برای استفاده از گواهی‌ها یا تصمیم مراکز صدور گواهی برای ابطال گواهی‌ها هیچ‌گونه ادعایی علیه مرکز ریشه داشته باشند. تحت هیچ شرایطی مرکز دولتی صدور گواهی الکترونیکی ریشه مسئول هرگونه خسارت مستقیم، غیرمستقیم، تصادفی، استنتاجی، خاص یا کیفری در مورد گواهی‌هایی که توسط مراکز میانی که گواهی آنها توسط مرکز صدور گواهی ریشه تحت سیاست‌های گواهی الکترونیکی ریشه و این دستورالعمل صادر شده‌اند، نمی‌باشد.

مراکز صدور گواهی میانی نباید هیچ‌گونه ادعای خسارت از مرکز دولتی صدور گواهی الکترونیکی ریشه و شورا برای مواردی مانند ابطال گواهی مرکز صدور گواهی میانی داشته باشند.

صاحبان امضا و طرفهای اعتماد کننده نباید هیچ‌گونه ادعای خسارت به دلیل اطلاعات اشتباه وضعیت گواهی فراهم شده توسط سرور و سرویس‌های مراکز صدور گواهی میانی از مرکز دولتی صدور گواهی ریشه داشته باشند.

۲-۲-۱-۲) محدوده خسارات

میزان خسارت ناشی از خطا در عملیات مرکز دولتی صدور گواهی ریشه یا دفتر ثبت نام بر اساس فصل دوم از مبحث سوم قانون تجارت الکترونیکی تعیین می‌شود. مرکز دولتی صدور گواهی ریشه از هرگونه تعهدی نسبت به پرداخت خسارت ناشی از استفاده گواهی که مطابق با سیاست‌های گواهی الکترونیکی ریشه و این دستورالعمل صادر شده، رفع مسئولیت می‌کند.

۲-۲-۱-۳) موارد دیگر

مرکز دولتی صدور گواهی الکترونیکی ریشه، هیچ گونه مسئولیتی در قبال خسارت‌های مستقیم و یا غیرمستقیم، اتفاقی، خاص یا کیفری که در اثر شرایط اضطراری ایجاد شده را متوجه خود نمی‌داند. چنانچه مرکز دولتی صدور گواهی الکترونیکی ریشه برای نگهداری، گسترش و انتقال سیستم‌های سرویس‌دهی خود، مجبور به

متوقف نمودن ارائه خدمات صدور گواهی و یا مخزن شود، این امر را در مخزن اعلام می‌کند و به آگاهی کلیه مراکز صدور گواهی میانی می‌رساند و هیچ گونه مسئولیتی در قبال خسارت‌های مستقیم و یا غیرمستقیم، اتفاقی، خاص یا کیفری ناشی از این امر را نمی‌پذیرد.

در صورتی که مرکز صدور گواهی میانی و یا موجودیت‌های گرداننده مرکز صدور گواهی میانی برای ابطال گواهی به دلیل خطر افشا (طبق بخش ۴-۴) این دستورالعمل) اقدام کنند، مرکز دولتی صدور گواهی الکترونیکی ریشه فعالیت‌های مربوط به ابطال گواهی را که شامل تأیید اعتبار درخواست، ابطال گواهی و صدور لیست گواهی‌های باطل شده می‌باشد، در کمتر از ۱۲ ساعت کاری بعد از دریافت درخواست ابطال گواهی و تعیین اعتبار درخواست انجام می‌دهد.

باید به این امر توجه شود که تا زمان انتشار اطلاعات مربوط به گواهی باطل شده در مخزن، مرکز صدور گواهی الکترونیکی میانی مسئولیت هرگونه استفاده از گواهی و یا کلید خصوصی مربوطه را طبق آنچه در این دستورالعمل بیان شده برعهده دارد و همچنین مرکز صدور گواهی میانی تا زمان انتشار اطلاعات مربوط به گواهی باطل شده مسئولیت انجام عملیات مناسب را برای حفظ طرفهای اعتماد کننده از خسارت دارد.

۲-۳) تعهدات مالی

۲-۳-۱) ادعای خسارت توسط طرفهای اعتماد کننده

شورا ، مرکز دولتی صدور گواهی الکترونیکی ریشه، و دفتر ثبت نام ریشه فعالیت‌های خود را مطابق با این دستورالعمل و سیاست‌های گواهی الکترونیکی ریشه برای اطمینان خود انجام می‌دهند و هیچگونه مسئولیت مالی برای سوء استفاده از گواهی توسط طرفهای اعتماد کننده را متوجه خود نمی‌دانند.

۲-۳-۲) قیمومیت

صدور گواهی، توسط مرکز دولتی صدور گواهی ریشه، شورا و دفتر ثبت نام ریشه مطابق با این دستورالعمل، رابطه کارگزاری، قیمومیت یا نمایندگی بین مرکز دولتی صدور گواهی ریشه، شورا و دفتر ثبت نام ریشه با مراکز صدور گواهی میانی، صاحبان امضا و طرفهای اعتماد کننده برقرار نمی‌کند.

۲-٤) تفسیر قانون و ضمانت اجرایی

۲-٤-۱) قوانین حاکم

قوانین جمهوری اسلامی ایران، قانون تجارت الکترونیکی (مصوب ۱۳۸۲/۱۰/۲۴) و آیین‌نامه اجرایی ماده (۳۲) قانون تجارت الکترونیکی (مصوب در جلسه مورخ ۸۶/۶/۱۱ هیئت وزیران) حاکم بر کلیه فعالیت‌ها و

قراردادهای بین مرکز دولتی صدور گواهی الکترونیکی ریشه و مراکز دیگر که در این دستورالعمل بیان شده است، می‌باشند.

۲-٤-۲) اعتبار، بروزرسانی، انتشار و عدم وابستگی بخشها

در صورتی که یکی از موارد ذکر شده در این دستورالعمل نادرست و یا نامعتبر باشد. اعتبار سایر قسمتها، همچنان پابرجاست تا زمانی که کل سند بروزرسانی شود. فرآیند بروزرسانی این دستورالعمل در بخش ۵-۱) توضیح داده شده است. زمان انتشار نسخه ویرایش شده سند، کلیه بخش‌های این سند با قسمت بروزرسانی شده ادغام می‌شوند و نسخه جدید را تشکیل می‌دهند.

۲-٤-۳) روال‌های حل اختلاف

هرگونه اختلاف بین مرکز دولتی صدور گواهی ریشه و مراکز صدور گواهی میانی می‌بایست در اولین فرصت از طریق مذاکره بین آنها حل شود.

اختلافی که از این طریق حل نشود می‌بایست از طریق شورا، پیگیری شود.

نهایتا چنانچه شورا نیز از حل اختلاف عاجز باشد، اختلاف از طریق مراجع قضائی قابل پیگیری خواهد بود.

۲-۵) تعرفه‌ها

در حال حاضر، کلیه هزینه‌های مرکز دولتی صدور گواهی الکترونیکی ریشه جمهوری اسلامی ایران از طریق خود این سازمان تامین می‌شود. بهرحال مرکز دولتی صدور گواهی الکترونیکی ریشه جمهوری اسلامی ایران برای تامین هزینه فعالیت‌های خود حق دریافت هزینه را از مراکز صدور گواهی میانی، برای خود محفوظ می‌دارد. این درآمدها تنها برای تأمین هزینه‌های فعالیت مرکز دولتی صدور گواهی استفاده خواهد شد.

در صورتی که سیاست دریافت هزینه مرکز دولتی صدور گواهی الکترونیکی ریشه جمهوری اسلامی ایران در آینده تغییر کند این تغییر در دستورالعمل اجرایی گواهی الکترونیکی ریشه، برطبق قوانین اجرایی بروزرسانی می‌شود و مکانیزم جدید دریافت هزینه و یا روال جدید بازپرداخت منتشر می‌شود.

۲-۵-۱) تعرفه صدور یا تجدید گواهی

به طور رایگان انجام می‌شود.

۲-۵-۲) تعرفه دسترسی به اطلاعات وضعیت گواهی

به طور رایگان انجام می‌شود.

۲-۵-۳) تعرفه سایر خدمات مانند تعرفه دسترسی به اطلاعات سند سیاست‌های گواهی الکترونیکی مرکز ریشه

به طور رایگان انجام می‌شود.

۲-۵-٤) تعرفه بازپرداخت در صورت انصراف از درخواست گواهی

در حال حاضر هزینه‌ای دریافت نمی‌شود، اما در صورت دریافت هزینه، امکان بازپرداخت آن وجود ندارد.

۲-٦) مخزن و انتشار

۲-٦-۱) انتشار اطلاعات مرکز دولتی صدور گواهی ریشه

مرکز دولتی صدور گواهی الکترونیکی ریشه اطلاعات زیر را منتشر می‌کند :

- کلیه گواهی‌های میانی صادر شده توسط مرکز دولتی صدور گواهی ریشه؛
- آخرین نسخه منتشر شده لیست گواهی‌های باطل شده؛
- گواهی خود امضاء.(حداقل تا زمانی که مدارک امضاء شده توسط کلید خصوصی گواهی خود امضاء منقضی نشده‌اند، باید در دسترس باشد)؛
- سیاست‌های گواهی الکترونیکی ریشه؛
- خلاصه‌ای از آخرین نسخه این دستورالعمل اجرایی شامل بخش های ۱، ۲، ۳، ۴ و ۸؛

- لیست گواهی‌های تعاملی که بر مبنای توافق دو جانبه با سایر مراکز ریشه (در سطح ملی و بین‌المللی) صادر شده توسط مرکز صدور گواهی ریشه.

۲-٦-۲) تناوب انتشار

مرکز دولتی صدور گواهی الکترونیکی ریشه، لیست گواهی‌های باطل شده را، حتی اگر هیچ تغییری یا بروزرسانی در آن انجام نشده باشد، به صورت ادواری حداکثر هر شش ماه یکبار منتشر کرده، در مخزن نگهداری می‌نماید. در صورت ابطال گواهی مراکز صدور گواهی میانی، مرکز صدور گواهی ریشه بلافاصله یک لیست گواهی باطل شده صادر کرده و در مخزن منتشر مینماید.

۲-٦-۳) کنترل دسترسی

برای حفظ امنیت، سایت مرکز دولتی صدور گواهی الکترونیکی ریشه همیشه به صورت برون خط عمل می‌کند. بنابراین به دلیل عدم وجود هرگونه اتصال شبکه مستقیم و یا غیر مستقیم بین سایت مرکز دولتی صدور گواهی الکترونیکی ریشه و مخزن، لیست گواهی‌های باطل شده و گواهی‌های صادر شده توسط مرکز دولتی صدور گواهی الکترونیکی ریشه نمی‌توانند مستقیماً از طریق شبکه‌های رایانه‌ای به مخزن فرستاده شوند.

بنابراین جهت انتشار لیست گواهی‌های باطل شده و گواهی‌ها در مخزن، افراد خاصی که توسط مرکز دولتی صدور گواهی الکترونیکی ریشه برای انتقال این اطلاعات در نظر گرفته شده‌اند، آنها را از طریق وسایل ذخیره اطلاعات مانند CD-ROM و DVD-ROM انتقال می‌دهند.

اطلاعات انتشار یافته در مخزن مرکز دولتی صدور گواهی الکترونیکی ریشه برای فعالیت کلیه مراکز صدور گواهی میانی و طرفهای اعتماد کننده بر طبق آنچه در بخش ۲-۶-۱) این دستورالعمل بیان شده، ضروری می‌باشد. بنابراین دسترسی عمومی به اطلاعات این مخزن وجود دارد. تنها افراد خاص که توسط مرکز دولتی صدور گواهی الکترونیکی ریشه تأیید صلاحیت شده‌اند اجازه بروز رسانی اطلاعات موجود در مخزن را دارند. کنترل‌های دسترسی از طریق کارکردهای راهبری، تخصیص نقش‌ها و وظایف تعریف شده آنها، تنظیم می‌شوند. مرکز دولتی صدور گواهی الکترونیکی ریشه تمام تلاش خود را در جهت در دسترس بودن مخزن بکار خواهد گرفت.

۲-٦-٤) مـــــخـــــــــــزن

مخزن توسط خود مرکز دولتی صدور گواهی الکترونیکی ریشه راه‌اندازی می‌شود. در صورتی که فعالیت مخزن به هر دلیلی، اعم از اشکال در سیستم یا دلایل دیگر مختل شود، مرکز دولتی صدور گواهی الکترونیکی ریشه می‌بایست در مدت ۲ روز کاری، مشکل را برطرف کرده و فعالیت مخزن را ادامه دهد.

آدرس اینترنتی مخزن عبارتست از http://www.rca.gov.ir/repository

۲-۷) بازرسی

۲-۷-۱) تناوب بازرسی

بازرسی کارکرد مرکز دولتی صدور گواهی ریشه حداقل سالی یکبار از طرف شورا انجام می‌شود و با این عمل، تطابق فعالیت‌های این مرکز با سیاست‌های گواهی الکترونیکی ریشه و این دستورالعمل تأیید می‌گردد.

۲-۷-۲) هویت و صلاحیت بازرس

بازرس باید با سیاست‌های گواهی الکترونیکی و دستورالعمل اجرایی گواهی الکترونیکی مرکز دولتی صدور گواهی ریشه کاملا آشنا باشد. بازرس باید در زمینه‌های امنیت اطلاعات و رمزنگاری زیرساخت کلید عمومی دارای صلاحیتهای علمی و فنی لازم بر طبق دستورالعمل شورا باشد.

۲-۷-۳) روابط بازرس با مرکز مورد بازرسی

بازرس از طریق عقد قرارداد، توسط شورا تعیین می‌شود و با مرکز دولتی صدور گواهی ریشه، از نظر سازمانی، جدا می‌باشد.

۲-۷-٤) موضوعات مورد بازرسی

موارد زیر تحت بازرسی قرار می‌گیرند:

- اطمینان از این که مرکز دولتی صدور گواهی ریشه مطابق با مفاد این دستورالعمل عمل می‌کند؛
- این دستورالعمل به صورت تفصیلی کارکرد فنی، پرسنلی و روال‌های مرکز دولتی صدور گواهی ریشه را که کاملاً با سیاست‌های گواهی الکترونیکی ریشه تطابق دارد، مطرح می‌کند؛
- اطمینان از اعمال درست کنترل‌های امنیتی.

۲-۷-۵) واکنش‌های اتخاذ شده در برخورد با نقایص

چنانچه هرگونه ناهمخوانی بین فعالیت‌های مرکز دولتی صدور گواهی و ثبت نام ریشه با سیاست‌های گواهی الکترونیکی ریشه، این دستورالعمل یا قراردادهای گواهی‌های میانی مشاهده شود، فعالیت های زیر انجام می‌شود:

- بازرس باید ناهمخوانی را کاملاً ثبت نماید؛
- بازرس باید به طرف‌های مشخص شده در بخش۲-۷-۶)، ناهمخوانی را ابلاغ کند؛
- مرکز دولتی صدور گواهی ریشه، راه حلی همراه با زمان پیش بینی شده برای اجرای آن به شورا پیشنهاد می‌کند؛

- شورا راه حل مناسب که می‌تواند شامل جلوگیری از فعالیت مرکز دولتی صدور گواهی ریشه یا در صورت لزوم ابطال گواهی این مرکز باشد را، تعیین کند.

پس از تصحیح ناهمخوانی شورا می‌تواند مجوز از سرگیری فعالیت مرکز دولتی صدور گواهی را صادر کند. چنانچه گواهی مرکز بدلیل عدم تطابق کارکرد با سیاست‌های گواهی الکترونیکی ریشه و این دستورالعمل باطل شده باشد، مرکز دولتی صدور گواهی ریشه می‌بایست مطابق با بخش ۴-۸-۲) عمل کند.

۲-۷-٦) گزارش نتایج

بازرس باید نتیجه بازرسی را به شورا گزارش کند. نتایج به مرکز دولتی صدورگواهی ریشه نیز گزارش می‌شود.

۲-۸) محرمانگی[1]

۲-۸-۱) انواع اطلاعاتی که باید محافظت شوند

اطلاعات هر درخواست گواهی که توسط مرکز دولتی صدور گواهی الکترونیکی ریشه نگهداری می‌شود و در گواهی‌های صادر شده وجود ندارد، بصورت محرمانه نگهداری می‌شود و کلیه کارمندان فعلی و سابق می‌بایست در حفظ محرمانگی این اطلاعات کوشا باشند.

در مورد مرکز دولتی صدور گواهی الکترونیکی ریشه، می‌توان به موارد زیر اشاره کرد:

- کلیه کلیدهای خصوصی و کلمات رمز عبور که در مرکز دولتی صدور گواهی الکترونیکی ریشه به کار گرفته می‌شوند، محرمانه‌اند؛
- اطلاعات درخواست گواهی که توسط مرکز دولتی صدور گواهی الکترونیکی ریشه نگهداری می‌شود، نباید بدون رضایت مراکز صدور گواهی میانی یا درخواست مراجع قضائی و حقوقی منتشر شوند؛
- کلیه اطلاعات مربوط به پیگیری ثبت وقایع که توسط مرکز دولتی صدور گواهی الکترونیکی ریشه ایجاد و یا نگهداری می‌شوند، محرمانه‌اند؛

[1] confidentiality

- کلیه اسناد طبقه‌بندی شده و کتابچه‌های راهنمای مرکز دولتی صدور گواهی الکترونیکی ریشه محرمانه‌اند.

۲-۸-۲) اطلاعاتی که محرمانه محسوب نمی شوند

- گواهی‌ها و لیست گواهی‌های باطل شده و اطلاعات دیگری (مانند سیاست‌های گواهی الکترونیکی) که در مخزن انتشار می‌یابند محرمانه نیستند؛
- کلیه اطلاعات شناسایی و اطلاعات دیگری که در گواهی ذکر شده‌اند محرمانه نیستند، مگر آنکه اساسنامه و یا توافقنامه خاصی چنین حکم کند.

۲-۸-۳) انتشار اطلاعات ابطال و تعلیق

مرکز دولتی صدور گواهی الکترونیکی ریشه، هیچ گونه اطلاعاتی در مورد گواهی‌های معلق منتشر نمی‌کند. زیرا اساساً مرکز دولتی صدور گواهی الکترونیکی ریشه سرویس تعلیق گواهی ندارد.

اطلاعات مربوط به گواهی‌های باطل شده مطابق با بخش ۲-۸-۲) این دستورالعمل، محرمانه تلقی نمی‌شوند و در مخزن منتشر شده و در دسترس عموم قرار می‌گیرند.

۲-۸-٤) ارائه اطلاعات به مراجع قضائی یا سازمان‌ها

در صورتی که مراجع قضایی، اطلاعات محرمانه‌ای را که در بخش ۲-۸-۱) این دستورالعمل به آن‌ها اشاره شد، برای جستجو و بازرسی شواهد درخواست کنند، مرکز دولتی صدور گواهی ریشه، این اطلاعات را تنها در صورت ارائه حکم مرجع قضایی در اختیار آن‌ها قرار می‌دهد. در این صورت این مرکز حق خود را برای دریافت هزینه فراهم آوردن اطلاعات، محفوظ می‌داند.

۲-۸-٥) ارائه اطلاعات طبق درخواست مراکز صدور گواهی میانی

مراکز صدور گواهی میانی می‌توانند درخواست دسترسی به هرگونه اطلاعات شخصی خود را که موجود در پرونده‌های دفتر ثبت نام ریشه می‌باشد، داشته باشند. در این صورت، مرکز دولتی صدور گواهی ریشه حق خود را برای دریافت هزینه فراهم آوردن این اطلاعات، محفوظ می‌داند.

اطلاعات خصوصی مراکز صدور گواهی میانی نباید بدون اجازه رسمی آنها در اختیار اشخاص دیگر قرار گیرد مگر با حکم مراجع قضایی.

۲-۸-٦) سایر شرایط انتشار اطلاعات

اطلاعات محرمانه مرکز دولتی صدور گواهی الکترونیکی ریشه تنها در صورت ارائه حکم مراجع قضایی و قانونی افشا می‌شود.

۲-۹) حق مالکیت معنوی

مرکز دولتی صدور گواهی الکترونیکی ریشه، کلیه حقوق مالکیت معنوی کلیدهای خصوصی و رمزهای مشترک خود را متعلق به خود می‌داند. مراکز صدور گواهی میانی، کلیه حقوق مالکیت معنوی کلیدهای خصوصی خود را متعلق به خود می‌دانند.

در هر صورت مرکز دولتی صدور گواهی الکترونیکی ریشه، کلیه حقوق مالکیت معنوی گواهی‌هائی که صادر کرده است- هر چند کلید عمومی مراکز صدور گواهی میانی در آن‌ها باشد- را متعلق به خود می‌داند. مرکز صدور گواهی الکترونیکی ریشه کلیه حقوق مالکیت معنوی عنوان گواهی خود امضاء یا گواهی‌هایی را که توسط این مرکز صادر شده متعلق به خود می‌داند.

مرکز دولتی صدور گواهی الکترونیکی ریشه، تمامی تلاش خود را بکار می‌گیرد تا نام‌های واگذار شده به مراکز صدور گواهی میانی درست باشند. در هر صورت، مرکز دولتی صدور گواهی الکترونیکی ریشه در قبال حل اختلاف مالکیت نام‌های مراکز صدور گواهی میانی مسئول نیست. در صورتی که در مورد ثبت نام مراکز صدور گواهی اختلافی پیش آید، مرکز صدور گواهی میانی می‌بایست این اختلاف را از طریق قانونی پیگیری نماید و مرکز دولتی صدور گواهی الکترونیکی ریشه را برای حفظ حقوق خود از نتایج آن آگاه کند.

۳) احراز هویت

ثبت نام اولیه منظور از ثبت نام اولیه دریافت و بررسی درخواست گواهی برای اولین بار از طرف مراکز صدور گواهی الکترونیکی میانی می‌باشد.

۳-۱-۱) انواع نام‌ها

نام‌های گواهی‌های صادر شده توسط مرکز دولتی صدور گواهی الکترونیکی ریشه که شامل گواهی خود امضای مرکز دولتی صدور گواهی الکترونیکی ریشه و گواهی‌های میانی مراکز صدور گواهی میانی می‌شود، با نام‌های ترکیبی X.500 مطابقت دارد.

۳-۱-۲) نیاز به نام‌های با معنی

نام‌هایی که مراکز برای گواهی‌های میانی درخواست می‌کنند، می‌بایست با دامنه نام‌های تایید شده توسط شورا مطابقت داشته باشد. همچنین نام‌ها می‌بایست هویت مرکز صدور گواهی را نشان دهند.

نام‌های ترکیبی مراکز صدور گواهی میانی که گواهی خود را از مرکز دولتی صدور گواهی ریشه دریافت کرده‌اند از قالب زیر استفاده می‌کند:

cn={نام گواهی مرکز صدور گواهی میانی}, ou= {نام مرکز صدور گواهی}, o={توسط شورا تعیین شود}, c=IR

۳-۱-۳) قواعد تفسیر قالب مختلف نام‌ها

مرکز دولتی صدور گواهی ریشه تنها از استاندارد X.500 برای تفسیر نام‌های ترکیبی استفاده می‌کند.

۳-۱-٤) یکتایی نام‌ها

دفتر ثبت نام ریشه یگانگی نام‌های سازمان‌های درخواست‌کننده برای گواهی‌های میانی را بررسی می‌کند. نام ترکیبی مراکز صدور گواهی میانی باید دارای نام سازمان برای اطمینان از یکتایی نام باشند.

عنوان گواهی می‌بایست در مورد شرکت‌ها، با نامی که سازمان ثبت اسناد و املاک کشور تأیید کرده یکسان باشد. در مورد سازمان‌ها و بخش‌های دولتی این نام می‌بایست با نامی که معاونت برنامه‌ریزی و نظارت راهبردی ریاست جمهوری تأیید کرده، یکسان باشد.

چنانچه نامی که انتخاب شده تکراری باشد، مرکز درخواست‌کننده می‌بایست نام درخواستی خود را تغییر دهد.

گواهی خود امضاء مرکز دولتی صدور گواهی الکترونیکی ریشه از ترکیب نامگذاری زیر استفاده می‌کند:

cn={توسط شورا تعیین شود}، O = {توسط شورا مشخص شود},C = IR

علاوه بر این در گواهی خود امضای مرکز دولتی صدور گواهی الکترونیکی ریشه، عنوان گواهی با نام صادر کننده همخوانی دارد.

۳-۱-۵) روال حل اختلاف در مورد نام‌ها

دفتر ثبت نام ریشه می‌بایست در صورت مواجهه با هر گونه اختلاف در مورد نام‌گذاری گواهی‌های میانی، آنرا بررسی و تصحیح نماید. در صورت نیاز، دفتر ثبت نام ریشه می‌بایست موضوع را با مرکز دولتی صدور گواهی ریشه و شورا هماهنگ نماید.

۳-۱-٦) احراز هویت و نقش علائم تجاری

مرکز دولتی صدور گواهی ریشه در صورت اطلاع، هرگز برای نامی که یک دادگاه قانونی آنرا سوء استفاده از علامت تجاری سازمان دیگر تشخیص داده است، گواهی صادر نخواهد کرد.

۳-۱-۷) روش اثبات مالکیت کلید خصوصی

مرکز دولتی صدور گواهی الکترونیکی ریشه صحت پیوند بین کلید خصوصی مرکز صدور گواهی مورد بحث را با کلید عمومی گواهی مربوطه، بررسی می‌کند.

مرکز دولتی صدور گواهی الکترونیکی ریشه برای تشخیص صحت امضاء در فایل درخواست گواهی، از کلید عمومی PKCS#10 همان فایل استفاده می‌کند و با اینکار، مالکیت کلید خصوصی را برای مرکز صدور گواهی تضمین می‌کند.

۳-۱-۸) احراز هویت سازمان‌ها

فرم درخواست گواهی میانی که توسط مراکز صدور گواهی ارائه می‌شود می‌بایست شامل نام سازمان، مکان و هر اطلاعات دیگری که برای شناسایی آن سازمان کافی است، باشد. دفتر ثبت نام ریشه وجود سازمان درخواست کننده همچنین اسناد رسمی، هویت نماینده و صلاحیت نماینده برای نمایندگی سازمان را بررسی می‌کند. نماینده سازمان باید برای درخواست گواهی شخصاً اقدام کند.

به علاوه مرکز دولتی صدور گواهی ریشه اطلاعات زیر را برای هر درخواست گواهی مراکز صدور گواهی میانی ثبت می‌کند:

- هویت نماینده سازمان؛
- یک متن امضا شده توسط نماینده سازمان که هویت سازمان را تایید می‌کند؛
- روش استفاده شده برای احراز هویت سازمان شامل شماره ثبت سازمان؛
- تاریخ احراز هویت.

در این فرایند همچنین باید هویت نماینده مطابق با بخش ۳-۱-۹) تایید شود.

۳-۱-۹) احراز هویت افراد حقیقی

سازمانها می‌بایست نماینده‌ای را به همراه اسناد رسمی جهت درخواست گواهی‌های میانی به دفتر ثبت نام ریشه معرفی نمایند. فرآیند احراز هویت مطابق آنچه در ذیل بیان شده است می‌باشد:

- نماینده می‌بایست در هنگام درخواست، شناسنامه و کارت ملی یا گذرنامه و کارت ملی خود را جهت احراز هویت ارائه نماید. شماره ملی، نام و آدرس ثابت محل اقامت نماینده با اطلاعات موجود در درخواست گواهیِ سازمان درخواست کننده، مطابقت داده می‌شود؛
- بررسی مدارک مربوط به اختیارات نماینده؛
- نماینده می‌بایست متنی حاوی هویت خود را به صورت دستی در مقابل مسئول دفتر ثبت نام ریشه امضا نماید.

۳-۲) روال تجدید کلید

۳-۲-۱) روال تجدید کلید گواهی

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

طول کلید خصوصی مرکز دولتی صدور گواهی الکترونیکی ریشه ۲۰۴۸ بیت است و برای مدت ۱۰ سال اعتبار دارد. مرکز دولتی صدور گواهی الکترونیکی ریشه، به دلایل زیر ممکن است زوج کلید خود را تجدید کند و گواهی خود امضاء جدیدی ارائه نماید:

- زوج کلید فعلی منقضی شده باشد؛
- امنیت زوج کلید فعلی در خطر باشد برای مثال کلید خصوصی در خطر افشا قرار بگیرد.

مراکز صدور گواهی میانی که قصد تجدید کلید دارند، می‌بایست درخواست گواهی جدید خود را به دفتر ثبت نام ریشه تحویل دهند و دفتر ثبت نام ریشه، احراز هویت مرکز درخواست کننده گواهی‌های میانی را مطابق با قسمت ۰ این دستورالعمل انجام می‌دهد.

۳-۲-۲) تجدید گواهی

مرکز دولتی صدور گواهی الکترونیکی ریشه تجدید گواهی خودامضاء خود و گواهی میانی مراکز صدور گواهی میانی را ممنوع اعلام می‌دارد.

۳-۲-۳) بروزرسانی گواهی

مرکز دولتی صدور گواهی الکترونیکی ریشه بروزرسانی گواهی خودامضاء خود و گواهی میانی مراکز صدور گواهی میانی را ممنوع اعلام می‌دارد.

۳-۳) دریافت یک گواهی جدید پس از ابطال

درصورتیکه که گواهی خودامضای مرکز دولتی صدور گواهی ریشه باطل شود، کلیه مراحل صدور گواهی مرکز ریشه باید تکرار شود.

در صورت ابطال گواهی مراکز صدور گواهی میانی، فعالیت‌های مربوط به احراز هویت درخواست گواهی جدید مطابق قوانینی که در بخش ۰ ذکر شد، انجام می‌شود.

درصورتیکه ابطال گواهی به دلیل لغو نمایندگی مرکز صدور گواهی باشد، مرکز دولتی صدور گواهی ریشه از مرکز صدور گواهی موردنظر می‌خواهد تا کلیه ماجول‌های رمزنگاری گواهی‌های خود را صفر کند.

درصورتیکه ابطال گواهی به دلیل در خطر افشا قرار گرفتن باشد ولی سخت‌افزار رمزنگاری در خطر افشا قرار نگرفته باشد، مرکز دولتی صدور گواهی ریشه از مرکز صدور گواهی موردنظر می‌خواهد تا کلیه ماجول‌های رمزنگاری گواهی‌های خود را صفر کند و یک کلید جدید تولیدکند، از مرکز دولتی صدور گواهی ریشه بخواهد که برای کلید جدید گواهی صادر کند و کلیه گواهی‌های صاحبان امضا را با استفاده از کلید جدید دوباره صادر کند.

درصورتیکه اطلاعات فعال‌ساز توکن سخت‌افزار رمزنگاری در خطر افشا قرار گرفته باشد، مرکز صدور گواهی مورد نظر باید اطلاعات فعال‌ساز جدید نیز فراهم کند.

درصورتیکه شورا تصمیم بگیرد که گواهی مرکز دولتی صدور گواهی ریشه را باطل کند، به اطلاع مرکز دولتی صدور گواهی ریشه می‌رساند تا یک لیست گواهی باطل شده حاوی گواهی خود و تمام گواهی‌هایی که صادر کرده است، تولید کند. سپس مرکز دولتی صدور گواهی ریشه سخت‌افزار رمزنگاری گواهی‌های خود را صفر می‌کند. درصورت ادامه فعالیت‌های مرکز دولتی صدور گواهی ریشه، مرکز دولتی صدور گواهی ریشه تمام گواهی‌های مراکز صدور گواهی میانی را با استفاده از گواهی خودامضای جدید خود، امضا می‌کند.

درصورتیکه اطلاعات فعال‌ساز سخت‌افزار رمزنگاری مرکز دولتی صدور گواهی ریشه در خطر افشا قرار گرفته باشد، مرکز دولتی صدور گواهی ریشه اطلاعات فعال‌ساز جدید نیز فراهم می‌کند.

۳-٤) درخواست ابطال

احراز هویت درخواست ابطال گواهی‌های مراکز صدور گواهی میانی مطابق موارد ذکر شده در بخش ۳-۱-۸) و ۳-۱-۹) توسط دفتر ثبت نام ریشه انجام می‌شود.

٤) خواسته‌های عملیاتی

٤-١) درخواست گواهی

فرآیند اولیه:

درخواست اولیه:

درخواست گواهی‌های میانی می‌بایست به همراه دستورالعمل اجرایی گواهی الکترونیکی و فایلی شامل یک درخواست PKCS#10 به صورت رسمی به دفتر ثبت نام ریشه ارسال شود. چنانچه مرکز صدور گواهی درخواست‌کننده از سیاست‌های صدور گواهی غیر از سیاست‌های گواهی الکترونیکی ریشه استفاده کند، آنگاه سیاست‌های صدور گواهی آن مرکز نیز می‌بایست به همراه درخواست گواهی ارسال شود. دفتر ثبت نام ریشه بر مبنای ماده ۷ آیین‌نامه مصوب و سیاست‌های ابلاغی شورا نسبت به پذیرش یا رد درخواست اقدام و نتیجه را به دبیرخانه شورا جهت طرح در شورا اعلام می‌کند.

شناسایی و احراز هویت:

در صورت پذیرش ، شناسایی و احراز هویت درخواست کنندگان مطابق با روال‌های تعریف‌شده در بخش ۳-۱-۸) و ۳-۱-۹) توسط دفتر ثبت نام ریشه انجام می‌شود.

بررسی مدارک:

دفتر ثبت نام ریشه کلیه مدارک مربوط به درخواست‌های گواهی را بررسی می‌کند و چنانچه مطالب دیگری نیاز باشد، آنها را درخواست می‌کند یا مرحله بعد را شروع می‌کند.

ارسال مدارک به شورا:

دفتر ثبت نام فایل درخواست گواهی را به همراه مدارک برای شورا ارسال می‌کند.

بررسی صحت:

شورا وظیفه حصول اطمینان از بررسی تناسب دستورالعمل اجرایی یک مرکز صدور گواهی میانی را با سیاست‌های گواهی الکترونیکی ریشه برعهده دارد. هیچ گونه ناهمخوانی تکنولوژیکی بین عامل درخواست کننده و مرکز دولتی صدور گواهی الکترونیکی ریشه نمی‌بایست وجود داشته باشد. چنانچه سیاست‌های گواهی الکترونیکی ریشه استفاده نشود، نگاشت سیاست باید بررسی شود. نباید هیچ تضادی بین دستورالعمل اجرایی گواهی الکترونیکی عامل درخواست‌کننده با سیاست‌های گواهی الکترونیکی به‌کار گرفته شده توسط آنها وجود داشته باشد. نهایتا در صورت تایید دستورالعمل اجرایی (و در صورت وجود سند سیاست‌ها) توسط شورا مرحله بعدی انجام می‌گیرد.

چنانچه درخواست گواهی توسط شورا پذیرفته نشود، عامل درخواست کننده از طریق نامه رسمی که شامل دلایل عدم پذیرش درخواست می‌باشد، مطلع خواهد شد.

هماهنگی:

جلسه‌ای جهت هماهنگی بین مرکز ریشه و عامل درخواست کننده گواهی برگزار می‌شود، در این جلسه به موارد زیر پرداخته می‌شود:

- پیش‌از برگزاری جلسه می‌بایست هویت نماینده درخواست‌کننده، بر اساس روال مذکور در بخش ۳-۱-۹) تشخیص داده شده و تأیید شود؛
- شرایط ادامه کار با عامل درخواست‌کننده مورد توافق قرار گیرد؛
- چنانچه درخواست گواهی میانی پذیرفته شود این کار با امضای قرارداد گواهی میانی تکمیل می‌شود؛ و موافقت با تاسیس مرکز میانی رسما به اطلاع عامل درخواست کننده می‌رسد.

مرحله تاسیس مرکز میانی

مرکز میانی الزامات تاسیس را براساس ماده ۷ آیین‌نامه ابلاغی به شرح زیر آماده می‌کند:

- معرفی پنج نفر دارای مدرک تحصیلی مرتبط مورد تأیید وزارتخانه‌های علوم، تحقیقات و فناوری و بهداشت، درمان و آموزش پزشکی با شرایط زیر:

۱- سه نفر کارشناس دارای مدرک تحصیلی دانشگاهی و ترجیحاً دارای تجربه فعالیت مرتبط

۲- دو نفر با مدرک کاردانی در رشته‌های مرتبط با فناوری اطلاعات و ارتباطات یا حداقل سه سال تجربه در حوزه‌های مرتبط با فناوری اطلاعات و ارتباطات همراه با مجوز طی دوره آموزشی از مراکز فنی و حرفه‌ای

- تأمین مکان فیزیکی مناسب همراه با تجهیزات سخت‌افزاری و نرم‌افزاری لازم اعلام شده از سوی مرکز دولتی ریشه به نحوی که امنیت فنی و رمزنگاری را تضمین نماید و مورد تأیید بازرسان مرکز ریشه قرار گرفته باشد
- ارایه تضمین معتبر متناسب با مبلغ تعیین شده توسط مرکز دولتی ریشه

٤-۲) مرحله صدور گواهی

کمیته نظارت شورا با حضور در مرکز دولتی صدور گواهی الکترونیکی ریشه فرایند صدور گواهی را انجام می‌دهد و بعد از صدور گواهی، عامل درخواست کننده از طریق نامه رسمی که شامل گواهی صادر شده نیز می‌باشد، از این موضوع آگاه می‌شود.

٤-٣) پذیرش گواهی

بعد از دریافت نامه رسمی پذیرش درخواست، عامل درخواست کننده (از این پس مرکز صدور گواهی میانی نامیده می‌شود) می‌بایست صحت اطلاعات مذکور در گواهی(ها) را تأیید نماید. چنانچه این اطلاعات درست باشد مرکز صدور گواهی میانی می‌بایست سند پذیرش را امضاء و جهت تکمیل فرآیند پذیرش گواهی باز پس فرستد. بعد از دریافت سند پذیرش گواهی، مرکز دولتی صدور گواهی الکترونیکی ریشه گواهی(های) صادر شده را در مخزن منتشر خواهد کرد. چنانچه مرکز صدور گواهی میانی در بازپس فرستادن اسناد امضاء شده کوتاهی کند، این امر به منزله انصراف او از پذیرش گواهی تلقی می‌شود. در این صورت مرکز دولتی صدور گواهی الکترونیکی ریشه بدون ابلاغ مجدد این گواهی را باطل می‌کند.

٤-٤) ابطال و تعلیق گواهی

٤-٤-١) شرایط ابطال

گواهی خودامضا مرکز دولتی صدور گواهی ریشه در صورت در خطر افشا قرار گرفتن یا تشخیص شورا باطل می‌شود.

در صورت وقوع هر یک از موارد زیر مرکز صدور گواهی میانی می‌بایست ابطال گواهی(های) خود را درخواست کند:

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

به علاوه مرکز دولتی صدور گواهی الکترونیکی ریشه، گواهی‌های مراکز صدور گواهی میانی را بدون تأیید آنها در صورت بروز هر یک از شرایط زیر باطل خواهد کرد:

- نادرستی مطالب هر یک از بخش‌های گواهی؛
- استفاده غیرمجاز یا درخطر افشا بودن کلید خصوصی مرکز صدور گواهی میانی؛
- در صورت استفاده غیرمجاز، جعل و در خطر افشا قرار گرفتن کلید خصوصی مرکز دولتی صدور گواهی الکترونیکی ریشه، کلیه گواهی‌های میانی امضاء شده توسط مرکز دولتی صدور گواهی الکترونیکی ریشه می‌بایست باطل شوند؛
- گواهی(های) مراکز صدور گواهی میانی مطابق با مفاد دستورالعمل اجرایی گواهی الکترونیکی ریشه صادر نشده باشند؛

- مراکز صدور گواهی میانی مطابق با مفاد دستورالعمل اجرایی گواهی الکترونیکی ریشه یا قرارداد گواهی‌های میانی یا قوانین کشور عمل نکند؛
- درخواست ابطال گواهی توسط یک سازمان ناظر بر مرکز صدور گواهی میانی یا از طریق مراجع قانونی صورت گیرد؛
- مرکز دولتی صدور گواهی الکترونیکی ریشه به فعالیت خود پایان دهد.

٤-٤-٢) کسانی که می‌توانند درخواست ابطال کنند

- عواملی که از مرکز دولتی صدور گواهی الکترونیکی ریشه گواهی گرفته‌اند می‌توانند برای گواهی میانی خود درخواست ابطال نمایند؛
- سازمان‌های ناظر بر عوامل فوق (مذکور در بند ۱)؛
- هر سازمان یا شخصی که دارای مدارک دال بر درخطر افشا قرارگرفتن کلید مراکز صدور گواهی میانی یا مرکز دولتی صدور گواهی ریشه می‌باشد، باید سریعاً این مدارک را دراختیار مرکز دولتی صدور گواهی ریشه یا کمیته نظارت شورا بگذارد.

٤-٤-٣) روال درخواست ابطال گواهی

کمیته نظارت شورا در صورت احراز خطر افشای کلید گواهی ریشه موضوع را به شورا اطلاع می‌دهد و شورا برای بررسی آن جلسه فوق‌العاده برگزار می‌کند. در صورت تایید خطر، شورا به طور رسمی به مرکز دولتی صدور گواهی ریشه نیاز به ابطال گواهی خود را اطلاع می‌دهد.

مرکز دولتی صدور گواهی ریشه این درخواست را احراز هویت می‌نماید. این امر در مورد گواهی‌های میانی می‌تواند با اقدام مستقیم مرکز ریشه یا اعلام کمیته نظارت شورا یا شورا انجام شود. سپس، مرکز ریشه گواهی مراکز صدور گواهی میانی را با قرار دادن شماره سریال آن در لیست گواهی‌های باطل شده و گواهی خود را از طریق قراردادن شماره سریال گواهی خودامضای خود و گواهی‌های مراکز صدور گواهی میانی که صادر کرده است در لیست گواهی‌های باطل شده، انجام می‌دهد.

درخواست‌های ابطال توسط سازمان‌ها و اشخاص دیگر مطابق با روال‌های زیر انجام می‌شود:

فرآیند اولیه:

درخواست اولیه:

در خواست می‌بایست از طریق نامه رسمی که شامل فرم تکمیل شده ابطال گواهی است، صورت گیرد.

احراز هویت:

انجام شود.۳-۱-۹) و ۳-۱-۸)احراز هویت عامل درخواست‌کننده می‌بایست مطابق با قسمت

بررسی درخواست :

درخواست تحویل داده شده بررسی خواهد شد تا مشخص شود آیا ابطال گواهی امکانپذیر است یا خیر.

تصمیم گیری:

در این مرحله مشخص خواهد شد که آیا مدارک دیگری جهت ورود به مرحله بعد از دارنده گواهی درخواست شود، یا رد درخواست ابطال طی یک نامه رسمی به مرکز درخواست‌کننده اعلام شود.

در صورت رد درخواست، دلایل رد در نامه قید خواهند شد.

ابطال گواهی:

چنانچه درخواست ابطال گواهی معتبر باشد، مرکز دولتی صدور گواهی الکترونیکی ریشه می‌بایست گواهی را باطل کرده و آن را در لیست گواهی‌های باطل شده وارد نموده و لیست گواهی‌های باطل شده را به مخزن ارسال نماید. خود مرکز صدور گواهی میانی و سازمان ناظر بر آن از طریق نامه رسمی از ابطال گواهی آگاه خواهند شد. اطلاعات وضعیت گواهی به مخزن ارسال شده و می‌بایست تا زمان انقضای گواهی‌ها در مخزن منتشر شوند.

٤-٤-٤) مهلت ابطال

این دستورالعمل هیچ مهلتی برای ابطال قائل نمی‌شود. مرکز دولتی صدور گواهی ریشه، گواهی‌ها را به سرعت پس از دریافت درخواست صحیح ابطال، باطل می‌کند.

٤-٤-٥) شرایط تعلیق

سرویس تعلیق گواهی توسط مرکز دولتی صدور گواهی الکترونیکی ریشه، ارائه نمی‌شود.

٤-٤-٦) کسانی که می‌توانند درخواست تعلیق کنند

کاربردی ندارد.

٤-٤-٧) روال درخواست تعلیق

کاربردی ندارد.

٤-٤-٨) محدودیت‌های مدت زمان تعلیق گواهی

کاربردی ندارد.

٤-٤-٩) تناوب صدور لیست گواهی‌های باطل شده

مرکز دولتی صدور گواهی ریشه لیست گواهی‌های باطل شده را هر شش ماه یکبار منتشر می‌کند و فیلد "nextupdate" لیست را تاریخ "thisupdate" به اضافه ۱۸۰ روز تعیین می‌کند. لیست گواهی‌های باطل شده حتی اگر هیچ تغییری یا بروزرسانی در آن انجام نشده باشد برای اطمینان کاربران از دسترسی به اطلاعات ابطالی کنونی باید منتشر شود. درصورت نیاز به ابطال گواهی مراکز صدور گواهی میانی به دلیل خطر افشا، مرکز دولتی صدور گواهی ریشه لیست گواهی‌های باطل شده را بلافاصله، در کمتر از ۱۲ ساعت کاری پس از دریافت خبر نیاز به ابطال گواهی باید منتشر کند.

٤-٤-١٠) ملزومات بررسی لیست گواهی‌های باطل شده

قبل از بازبینی لیست گواهی‌های باطل شده در مخزن، طرف اعتماد کننده می‌بایست امضای بکار رفته در لیست را به منظور تائید اعتبار لیست گواهی‌های باطل شده بررسی کند.

٤-٤-١١) قابل دسترسی بودن سرویس ابطال/اعلام برخط وضعیت گواهی

مرکز دولتی صدور گواهی ریشه دارای سرویس اعلام برخط وضعیت نمی‌باشد. اطلاعات مربوط به وضعیت گواهی‌ها در مخزن به صورت برون از خط بروزرسانی می‌شود.

٤-٤-١٢) روش‌های دیگر آگاهی از ابطال

راه دیگری برای بررسی ابطال گواهی‌ها وجود ندارد.

٤-٤-١٣) ملزومات راه‌های دیگر آگاهی از ابطال

کاربردی ندارد.

٤-٤-١٤) مقررات خاص مرتبط با در خطر افشا قرار گرفتن کلید

چنانچه کلید خصوصی مرکز صدور گواهی میانی در خطر افشا باشد، مرکز دولتی صدور گواهی الکترونیکی ریشه در لیست گواهی باطل شده منتشر شده دلیل ابطال این گواهی را "در خطر افشا بودن کلید" ذکر خواهد کرد.

٤-٥) روال بازرسی امنیتی

ثبت وقایع می‌بایست برای کلیه فعالیت‌هایی که مربوط به امنیت مرکز دولتی صدور گواهی ریشه هستند، انجام شود. فایل‌های ثبت وقایع می‌بایست به صورت خودکار توسط سیستم تولید شوند یا به صورت دستی در فرم کاغذی و یا سایر مکانیسم‌های فیزیکی ساخته شوند.کلیه فایل‌های ثبت وقایع اعم از الکترونیکی و غیر

الکترونیکی در هنگام بررسی وقایع باید در دسترس باشند. مدت زمانی که باید فایل‌های ثبت وقایع مربوط به هر رخداد قابل ثبت تعریف شده در این بخش، نگهداری شوند با توجه به قسمت ۴-۶-۲) تعیین می‌شود.

٤-٥-١) انواع وقایع قابل ثبت

وقایع زیر در مرکز دولتی صدور گواهی الکترونیکی ریشه باید توسط سیستم یا بصورت دستی در فرم‌های آماده، ثبت شوند:

وقایع سیستم:

- هر تغییری در پارامترهای ثبت وقایع مانند تغییر دوره تناوب یا نوع رخدادهای ثبت شده؛
- تغییر حداکثر دفعات ورود مشخصات برای احراز هویت؛
- تعریف، حذف یا اضافه‌کردن کاربران و نقش‌ها؛
- تغییر حقوق دسترسی یک نقش یا یک شناسه کاربری؛
- خاموش و روشن شدن سیستم؛
- هر تلاشی برای تغییر و یا از بین بردن وقایع ثبت‌شده؛
- تلاش های موفق و ناموفق برای دستیابی به یک نقش؛

- چنانچه راهبر سیستم، شناسه کاربری را که به دلیل تلاش ناموفق ورود به سیستم قفل شده است، از حالت قفل بیرون بیاورد؛
- کلیه تلاش‌های ورود به برنامه‌های کاربردی مرکز دولتی صدور گواهی ریشه ؛
- دسترسی به پایگاه داده‌های داخلی مرکز دولتی صدور گواهی ریشه؛
- تنظیم مجدد ساعت سیستم عامل.

وقایع انسانی و محیطی:

- ورود و خروج متصدیان و یا افراد دارای مجوز ورود؛
- ورود و خروج تجهیزات از مرکز دولتی؛
- نصب سیستم عامل؛
- نصب نرم‌افزار صدور گواهی ؛
- نصب HSM ؛
- انتصاب کارکنان مرکز دولتی صدور گواهی ریشه؛
- آموزش کارکنان مرکز دولتی صدور گواهی ریشه؛
- دریافت سخت افزار و نرم افزار؛

- تغییرات در پیکربندی سرویس دهنده مرکز دولتی صدور گواهی ریشه:
  - سخت افزار؛
  - نرم افزار؛
  - سیستم عامل؛
  - فایل‌های ترمیمی[1].
- دسترسی کارکنان به مکان استقرار مرکز دولتی صدور گواهی الکترونیکی ریشه ؛
- دسترسی به تجهیزات مرکز دولتی صدور گواهی ریشه.

عملیات مدیریت گواهی:

- صدور گواهی توسط مرکز دولتی صدور گواهی ریشه در هر زمان؛
- هرگونه استفاده از کلید خصوصی مانند امضای گواهی‌ها؛
- تمام درخواست‌های گواهی و پردازش آنها؛
- تمام درخواست‌های ابطال گواهی و پردازش آنها؛
- تغییر وضعیت یک گواهی؛

[1] Patch

- تهیه نسخه پشتیبان از پایگاه داده‌های داخلی مرکز دولتی صدور گواهی ریشه؛
- تهیه نسخه پشتیبان از فایل‌های ثبت وقایع؛
- بازیابی پایگاه داده‌های داخلی مرکز دولتی صدور گواهی الکترونیکی ریشه؛
- تخریب وسایلذخیره‌سازی؛
- دستکاری فایل‌ها (مانند ایجاد، تغییر نام، انتقال)؛
- ارسال هر داده به مخزن؛
- قراردادن یک گواهی در توکن؛
- تجدید گواهی مرکز دولتی صدور گواهی الکترونیکی ریشه؛

تغییر در سیاست‌ها:

- هر تغییری در پروفایل لیست گواهی‌های باطل شده؛
- هر تغییری در پروفایل یک گواهی؛
- هر تغییری در سند سیاست‌ها و یا دستورالعمل اجرایی گواهی الکترونیکی مرکز دولتی صدور گواهی الکترونیکی ریشه؛
- تغییر در مستندات آموزشی مرکز دولتی؛

- هر تغییر مرتبط با امنیت در پیکربندی مرکز دولتی صدور گواهی الکترونیکی ریشه ؛
- تغییر نحوه احراز هویت توسط راهبر سیستم (برای مثال، استفاده از روش‌های بیومتریک)..

حوادث:

- کلیه هشدارها در مورد در خطر افشا بودن کلید خصوصی؛
- موارد مشکوک یا شناخته شده نقض امنیت فیزیکی؛
- خرابی تجهیزات؛
- زمان و مدت قطع جریان برق؛
- خرابی در سیستم UPS .

خطاها:

- خطاهای نرم‌افزاری و شرایط رخداد آنها؛
- نقض مواد آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی؛
- نقض مواد سیاست‌های گواهی الکترونیکی ریشه؛
- نقض مواد دستورالعمل اجرایی گواهی الکترونیکی ریشه.

برای هر یک از وقایع قابل ثبت فرم ثبت واقعه مطابق با حداقل‌های تعیین شده در سند سیاست‌های گواهی مرکز ریشه باید تکمیل گردد.

٤-٥-٢) تناوب پردازش اطلاعات وقایع ثبت‌شده

مرکز دولتی صدور گواهی الکترونیکی ریشه می‌بایست هر شش ماه یکبار کلیه رخدادهای مهم را بررسی مجدد و پیگیری کند. این فعالیت شامل اعمالی از قبیل بررسی اطلاعات ثبت شده وقایع سیستمی و اسناد کاغذی ثبت وقایع جهت اطمینان از عدم دستکاری آنها و بازرسی همه ورودی‌های آن و جستجوی هرگونه اخطار و یا ناهماهنگی می‌باشد.

کلیه فعالیت‌هایی که براساس این نتایج انجام می‌شود می‌بایست مستندسازی شده و با رعایت طبقه‌بندی برای شورا ارسال شوند.

٤-٥-٣) دوره نگهداری از اطلاعات وقایع ثبت‌شده

اطلاعات وقایع ثبت‌شده باید در سایت مرکز دولتی صدور گواهی ریشه برای ۱ سال نگه‌داری شوند، این اطلاعات همچنین باید مطابق با بخش‌های ۴-۵-۴)، ۴-۵-۵)، ۴-۵-۶) و ۴-۶) نگه‌داری شوند. حذف فایل‌های ثبت وقایع که تاریخ نگهداری آنان منقضی شده است از سیستم مرکز دولتی صدور گواهی ریشه، تنها و تنها توسط نمایندهٔ تعیین شده توسط شورا انجام می‌گیرد.

٤-٥-٤) حفاظت از اطلاعات بازرسی امنیتی

- کلیه اطلاعات وقایع ثبت شده فعلی و بایگانی شده باید توسط امضای الکترونیکی و تکنولوژی رمزگذاری محافظت شوند و در CD-ROM، DVD-ROM و یا یک وسیله ذخیره‌سازی غیرقابل تغییر نگهداری شوند؛
- کلیدهای خصوصی که برای امضای فایل‌های ثبت وقایع به کارگرفته شده‌اند نباید برای هیچ منظور دیگری به کار روند؛
- گزارشهای ثبت وقایع که به صورت دستی ایجاد شده‌اند می‌بایست به مکان امنی انتقال یابند.

٤-٥-٥) روال‌های تهیه نسخه پشتیبان از اطلاعات بازرسی امنیتی

- از کلیه وقایع ثبت شده الکترونیکی و خلاصه وقایع ثبت‌شده می‌بایست پس از انجام هرگونه عملیاتی در مرکز نسخه پشتیبان تهیه شود. یک نسخه از فایل‌های ثبت وقایع می‌بایست هر شش ماه یکبار به سایت پشتیبان ریشه ارسال شود؛
- مرکز دولتی صدور گواهی ریشه باید به صورت شش ماه یکبار از فایل‌های وقایع ثبت‌شده نسخه پشتیبان تهیه کند و سیستم بازرسی باید به صورت خودکار اطلاعات وقایع ثبت‌شده را به صورت روزانه، هفتگی و ماهانه بایگانی کند.

- مرکز دولتی صدور گواهی الکترونیکی ریشه می‌بایست فایل‌های ثبت وقایع را در مکان ایمن ذخیره کند.

٤-٥-٦) سیستم جمع‌آوری اطلاعات بازرسی امنیتی

فرآیند ثبت وقایع می‌بایست با راه اندازی سیستم مرکز دولتی صدور گواهی الکترونیکی ریشه فعال شود و تنها در زمان متوقف شدن عملیات مرکز دولتی صدور گواهی الکترونیکی ریشه متوقف شود. چنانچه مشخص شود که در سیستم ثبت وقایع اشکالی وجود دارد و تمامیت سیستم و محرمانگی اطلاعات درخطر است، آنگاه مرکز دولتی صدور گواهی الکترونیکی ریشه می‌بایست فعالیت های صدور گواهی خود را به غیر از فرآیند ابطال گواهی به طور موقت تا زمانی که مشکل برطرف شود، متوقف کند.

٤-٥-٧) اطلاع به مسبب واقعه

هنگامیکه یک واقعه ثبت شد، ضرورتی ندارد که سیستم ثبت وقایع، مسبب واقعه ثبت شده را از این موضوع آگاه کند.

٤-٥-٨) ارزیابی آسیب‌پذیری

تمام عوامل صدور گواهی الکترونیکی اعم از مرکز ریشه دولتی، مراکز میانی و دفاتر ثبت نام آنها موظف به حفظ یکپارچگی مدیریت گواهی الکترونیکی می‌باشند. به همین منظور ارزیابی های زیر باید صورت پذیرد:

- ارزیابی آسیب‌پذیری سیستم‌های عملیاتی؛
- ارزیابی آسیب‌پذیری تاسیسات فیزیکی؛
- ارزیابی آسیب‌پذیری سیستم‌های مرکز صدور گواهی.

٤-٦) بایگانی اطلاعات

٤-٦-١) اطلاعاتی که می‌بایست بایگانی شوند

مطابق با سیاست‌های گواهی الکترونیکی ریشه اطلاعات زیر می‌بایست در مورد عملیات مرکز دولتی صدور گواهی و ثبت نام ریشه بایگانی شوند:

- تغییرات یا به روز رسانی پیکربندی تجهیزات؛
- درخواست گواهی یا درخواست ابطال؛
- درخواست و پاسخ وضعیت گواهی؛

- مستند سازی احراز هویت صاحب امضاء؛
- مستند سازی رسید و پذیرش گواهی؛
- مستند سازی رسید توکن؛
- کلیهٔ گواهی‌ها یا لیست گواهی‌های باطل شده (یا اطلاعات ابطالی دیگر) هنگام صدور یا انتشار؛
- اطلاعات بازرسی امنیتی؛
- اطلاعات دیگر یا برنامه های مورد نیاز برای تشخیص محتویات بایگانی؛
- کلیه مکاتبات با شورا ، کمیته نظارتی شورا و مراکز دیگر و بازرسان ثبت وقایع.

٤-٦-٢) دوره نگهداری اطلاعات بایگانی شده

زمان نگهداری اطلاعات ثبت‌شده در بایگانی مرکز دولتی صدور گواهی الکترونیکی ریشه ۲۵ سال است.

نرم افزارهای لازم برای بازخوانی و پردازش اطلاعات بایگانی شده نیز می‌بایست تا ۲۵ سال نگهداری شود.

٤-٦-٣) حفاظت از بایگانی

- هیچ فردی حق تغییر، از بین بردن و یا نوشتن بر روی اطلاعات بایگانی شده را ندارد؛
- مرکز دولتی صدور گواهی الکترونیکی ریشه می‌تواند اطلاعات بایگانی شده را به وسایل ذخیره‌سازی دیگر، در صورتی که سطح امنیت آن از وسیله اولیه کمتر نباشد، انتقال دهد؛

- وسیله ذخیره‌سازی اطلاعات بایگانی‌شده می‌بایست در یک محل ذخیره‌سازی مطمئن و ایمن نگهداری شود.

٤-٦-٤) روال‌های تهیه نسخه پشتیبان از بایگانی

مرکز دولتی صدور گواهی الکترونیکی ریشه از بایگانی‌های اطلاعات گواهی‌های صادر شده الکترونیکی به صورت شش ماه یکبار نسخه پشتیبان تهیه می‌کند و بایگانی کامل را نیز هر شش ماه یکبار انجام می‌دهد.

کلیه نسخه‌های پشتیبان تهیه شده از بایگانی در مرکز پشتیبان ریشه دولتی خارج از سایت اصلی نگهداری می‌شود.

٤-٦-٥) نیازهای مهر زمانی اطلاعات بایگانی

داده‌های بایگانی شده الکترونیکی (مانند گواهی‌ها، لیست گواهی‌های باطل شده، وقایع ثبت شده و غیره) می‌بایست دارای امضای الکترونیکی و مهر زمانی باشند به‌گونه‌ای که بتوان درستی مهر زمانی را بررسی کرد. مهرهای زمانی که بر روی این اطلاعات قرار دارند مهرهای زمانی الکترونیکی که از یک منبع دیگر دریافت می‌شوند نیستند بلکه از ساعت سیستم عامل رایانه استخراج می‌شوند. ساعت کلیه رایانه‌های مرکز دولتی صدور گواهی الکترونیکی ریشه به منظور حفظ دقت و قابلیت اعتماد می‌بایست مرتباً به صورت دوره‌ای تنظیم شوند. کلیه اطلاعات فعالیت‌های ثبت شده در فرم کاغذی نیز باید دارای تاریخ و در صورت لزوم دارای مهر زمانی

باشد. زمان و تاریخ درج شده در فرم فعالیت‌های ثبت شده کاغذی غیرقابل تغییراست مگر با اجازه و تائید بازرسان.

٤-٦-٦) سیستم جمع‌آوری بایگانی

مرکز دولتی صدور گواهی الکترونیکی ریشه چنین سیستمی ندارد.

٤-٦-٧) روال‌های دریافت و بررسی اطلاعات بایگانی

دسترسی به اطلاعات بایگانی تنها در صورت وجود درخواست کتبی شورا، اکثریت کمیته نظارت، بازرس شورا یا یک مرجع قضایی امکان‌پذیر می‌باشد. بازرسان مسئول بررسی اطلاعات بایگانی می‌باشند. در صورت بایگانی به صورت کاغذی، تاریخ و امضای بایگانی‌ها باید کنترل شود همانطور که امضای الکترونیکی بایگانی‌های الکترونیکی کنترل می‌شود.

٤-٧) گردش کلید

کلید خصوصی مرکز دولتی صدور گواهی الکترونیکی ریشه نباید زودتر از ۶ ماه مانده به تاریخ انقضای گواهی خودامضای مرکز، تجدید شود، همزمان یک گواهی جدید خودامضای مرکز دولتی صدور گواهی الکترونیکی

ریشه توسط این مرکز صادر خواهد شد. همچنین این گواهی می‌بایست به کلیه طرفهای اعتماد کننده تحویل داده شود.

سازمان‌هایی که دارای گواهی میانی هستند نباید کلید امضاء خود را زودتر از ۲ ماه قبل از به پایان رسیدن زمان اعتبار گواهی‌هایشان تعویض کنند و (مطابق با قسمت ۴-۱)) می‌بایست بعد از تولید کلید جدید، گواهی جدیدی را از مرکز دولتی صدور گواهی الکترونیکی ریشه درخواست کنند.

٤-٨) بازیابی به علت سوانح غیر مترقبه و در خطر افشا بودن

٤-٨-١) از بین رفتن تجهیزات، نرم افزارها و داده ها

مرکز دولتی صدور گواهی الکترونیکی ریشه باید روال‌هایی جهت بازیابی تجهیزات، نرم افزارها و داده ها که به علت سوانح غیرمترقبه و یا در خطر افشا بودن از بین رفته‌اند تعریف نماید. تمرین بازیابی خرابی به صورت سالیانه انجام می‌شود. چنانچه تجهیزات مرکز دولتی صدور گواهی الکترونیکی ریشه صدمه دیده باشند یا از کار افتاده باشند ولی کلیدهای امضاء آسیبی ندیده باشند، عملکردهای مرکز دولتی صدور گواهی الکترونیکی ریشه می‌بایست هر چه زودتر از سرگرفته شود، بطوریکه به عملکردهای مخزن اولویت بیشتری داده شود.

٤-٨-٢) ابطال گواهی مرکز دولتی صدور گواهی ریشه

در صورت نیاز به ابطال کلید عمومی مرکز دولتی صدور گواهی ریشه، این مرکز باید مطابق با دستورالعمل اجرایی گواهی الکترونیکی خود عمل کند و به مراجع زیر خبر ابطال کلید عمومی را ابلاغ کند:

- شورا و کمیته نظارتی آن؛
- مراکز صدور گواهی میانی؛
- دفاتر ثبت نام؛
- صاحبان امضا؛
- مراکز صدور گواهی ریشه خارجی و داخلی که به مرکز دولتی صدور گواهی ریشه (از طریق توافق دو جانبه[1]) اعتماد کرده‌اند.

همچنین مرکز دولتی صدور گواهی ریشه باید اقدامات زیر را انجام دهد:

- شماره سریال گواهی را در مخزن منتشر کند؛
- کلیه گواهی‌های مراکز صدور گواهی میانی امضا شده توسط گواهی ابطالی را باطل کند.

[1] Cross Certificate

روال بازیابی کلیدها در صورت از بین رفتن کلید گواهی امضاء در سند بازیابی خرابی مرکز دولتی صدور گواهی ریشه تشریح شده است. تمرین بازیابی خرابی به صورت سالیانه انجام می‌شود.

٤-٨-٣) در خطر افشا قرار گرفتن کلید مرکز دولتی صدور گواهی ریشه

در صورت در خطر افشا قرار گرفتن کلید مرکز دولتی صدور گواهی ریشه، گواهی خود امضایی که کلید آن در خطر افشا قرار گرفته، باید از برنامه‌های کاربردی طرفهای اعتماد کننده برداشته شود و به جای آن گواهی جدید از طریق یک ساز و کار امن توزیع شود.

روال بازیابی کلیدها در شرایط فوق، در سند بازیابی خرابی مرکز دولتی صدور گواهی ریشه تشریح شده است. تمرین بازیابی خرابی به صورت سالیانه انجام می‌شود.

٤-٨-٤) بازیابی خرابی پس از وقوع حوادث طبیعی یا حوادث دیگر

مرکز دولتی صدور گواهی ریشه باید تمرین بازیابی خرابی برای ایمن‌سازی تجهیزات را به صورت سالانه انجام دهد.

٤-۹) توقف سرویس‌دهی مرکز دولتی صدور گواهی

در صورتیکه فعالیت‌های مرکز دولتی صدور گواهی الکترونیکی ریشه به پایان برسد، این مرکز جهت خاتمه فعالیت خود روال‌های تعریف شده توسط شورا را اجرا خواهد کرد. برای به حداقل رساندن تاثیرات خاتمه فعالیت بر مراکز صدور گواهی میانی و صاحبان امضاء، مرکز دولتی صدور گواهی الکترونیکی ریشه باید:

- مراکز صدور گواهی میانی را از این امر آگاه کند و این مطلب را حداقل ۳ ماه قبل از خاتمه فعالیت مرکز دولتی صدور گواهی ریشه در مخزن اعلام کند؛
- کلیه گواهی‌های باطل نشده یا گواهی‌های منقضی نشده را در زمان خاتمه فعالیت خود باطل نماید و کلیه اطلاعات ثبت شده را به مرکز مورد تایید شورا، با حفظ امانت تسلیم کند.

۵) راهبری

۵-۱) روال تغییر

نیاز به تغییرات در این دستورالعمل به منظور اطمینان به آن باید به صورت دوره‌ای و سالیانه بررسی شود. تغییرات می‌توانند به صورت ضمیمه به دستورالعمل اجرایی گواهی الکترونیکی یا اساساً دوباره‌نویسی آن، انجام شوند. چنانچه سیاست‌های گواهی الکترونیکی ریشه یا شناسه آن تغییر کند، آنگاه این دستورالعمل می‌بایست مطابق با تغییرات سیاست‌های گواهی الکترونیکی ریشه یا شناسه آن تغییر کند.

مطالبی که بدون اطلاع رسانی می‌توانند تغییر کنند:

تنها تغییرات ویرایشی و اصلاحات سبک نگارشی می‌توانند بدون اطلاع رسانی در این دستورالعمل اعمال شوند.

مطالبی که برای تغییر احتیاج به اطلاع رسانی دارند:

الف - تغییراتی که می‌تواند بر نحوه عملکرد مراکز صدور گواهی میانی و طرفهای اعتماد کننده که از این دستورالعمل استفاده می‌کنند، تاثیر چشمگیر داشته باشد، می‌بایست ۳۰ روز قبل از اعمال تغییرات در دستورالعمل اجرائی در مخزن منتشر شود؛

ب- در غیر این صورت، سایر تغییرات از ۱۵ روز قبل می‌بایست منتشر شوند.

مکانیسم اطلاع رسانی:

کلیه تغییرات در این دستورالعمل می‌بایست در مخزن منتشر شوند. چنانچه تغییرات از دسته تغییرات ذکر شده در بالا (مطالبی که برای تغییر احتیاج به اطلاع رسانی دارند) باشد، می‌بایست ابلاغ رسمی به مراکز صدور گواهی که گواهی میانیشان مستقیماً توسط مرکز دولتی صدور گواهی الکترونیکی ریشه صادر شده، صورت گیرد.

دوره نظرخواهی

(۱) چنانچه تغییرات از موارد مذکور در بند الف مطالبی که برای تغییر احتیاج به اطلاع رسانی دارند باشد، دوره نظرخواهی از زمان اعلام تغییرات روی سایت مخزن به مدت ۱۵ روز خواهد بود.

(۲) چنانچه تغییرات از موارد مذکور در بند ب مطالبی که برای تغییر احتیاج به اطلاع‌رسانی دارند باشد، دوره نظرخواهی از زمان اعلام تغییرات روی سایت مخزن به مدت ۷ روز خواهد بود.

سازوکار مدیریت نظرات:

هر نظر و پیشنهادی در مورد تغییرات می‌بایست توسط فرمی که در مخزن صدور گواهی ریشه قرار دارد قبل از اتمام آخرین مهلت نظرخواهی دریافت شود. تمام نظرهای دریافت‌شده برای تصمیم‌گیری در مورد تغییرات و نحوه اعمال آنها، بازبینی و بررسی می‌شوند.

۵-۲) روال انتشار و اطلاع رسانی

بخش قابل انتشار دستورالعمل اجرایی گواهی الکترونیکی جدید (تغییر یافته) می‌بایست ظرف مدت ۱۵ روز در مخزن منتشر شود و از زمان انتشار قابل اجرا است.

۵-۳) روال تائید اسناد دستورالعمل اجرائی و سیاست‌های گواهی الکترونیکی

بعد از این که این دستورالعمل توسط شورا تایید شد، باید بخش‌های قابل انتشار آن توسط مرکز دولتی صدور گواهی الکترونیکی ریشه منتشر شود. چنانچه تغییراتی در سیاست‌های گواهی الکترونیکی ریشه اعمال شده و منتشرشود، این دستورالعمل می‌بایست مطابق با آن تغییر کند و به شورا تسلیم شود.

٦) مراجع

راهنمای تهیه دستورالعمل اجرایی گواهی الکترونیکی؛

RFC 2527؛

RFC 3280؛

Government Root Certification Authority Certification Practice Statement؛

Summary of the Certification Practice Statement for the External Certificate Authority Root CA .

۷) ضمیمه-الف

۷-۱) گواهی خودامضای ریشه

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
Version	ویرایش	V3
Serial Number	شماره سریال	باید منحصر بفرد باشد
Issuer Signature Algorithm	الگوریتم امضای صادر کننده	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	نام ترکیبی صادر کننده	cn={توسط شورا تعیین شود}، O = { توسط شورا }, C = IR{مشخص شود}
Validity Period	دوره اعتبار	Generalized سال از تاریخ صدور که در قالب X Time.نمایش داده می‌شود
Subject Distinguished Name	نام ترکیبی دارنده گواهی	cn={توسط شورا تعیین شود}، O = { توسط شورا }, C = IR{مشخص شود}
Subject Public Key Information	اطلاعات کلید عمومی دارنده گواهی	کلید RSA با پیمانه X، بیتی rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	شناسه یکتای صادر کننده	وجود ندارد
Subject Unique Identifier	شناسه یکتای دارنده گواهی	وجود ندارد
Issuer's Signature	امضای صادر کننده	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	ملحقات	
Authority key identifier	شناسه کلید مرکز	Octet String(مقدار ۲۰ بایتی تابع درهم‌سازی SHA-1 بر روی اطلاعات باینری کلید عمومی مرکز صدور گواهی ریشه که بصورت DER کدگذاری شده باشد)

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
subject key identifier	شناسه کلید دارنده گواهی	Octet String(مقدار ۲۰ بایتی تابع درهم‌سازی SHA-1 بر روی اطلاعات باینری کلید عمومی مرکز صدور گواهی ریشه که بصورت DER کدگذاری شده باشد)
key usage	کاربرد کلید	c=yes; digitalSignature, keyCertSign, cRLSign
Extended key usage	کاربردهای توسعه یافته کلید	وجود ندارد
Private key usage period	دوره کاربرد کلید خصوصی	وجود ندارد
Certificate policies	سیاست‌های گواهی الکترونیکی	c=no; {شناسه سیاست‌ها}
Policy Mapping	نگاشت سیاست	وجود ندارد
subject Alternative Name	نام بدیل دارنده گواهی	وجود ندارد
Issuer Alternate Name	نام بدیل صادر کننده	وجود ندارد
Subject Directory Attributes	مشخصات دایرکتوری دارنده گواهی	وجود ندارد
Basic Constraints	قیود اساسی	c=yes; cA=True; هیچ قید در مورد طول مسیر وجود ندارد
Name Constraints	قیود نام	وجود ندارد
Policy Constraint	قیود سیاست‌ها	وجود ندارد
CRL Distribution Point	نقطه انتشار لیست گواهی‌های باطل شده	وجود ندارد

۷-۲) گواهی میانی

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
Version	ویرایش	V3
Serial Number	شماره سریال	باید منحصر بفرد باشد

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
Issuer Signature Algorithm	الگوریتم امضای صادر کننده	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	نام ترکیبی صادر کننده	cn={توسط شورا تعیین شود}، O = { توسط شورا}, C = IR{مشخص شود}
Validity Period	دوره اعتبار	Generalized سال از تاریخ صدور که در قالب X نمایش داده می‌شود.Time
Subject Distinguished Name	نام ترکیبی دارنده گواهی	cn={نام گواهی مرکز صدور گواهی}, ou= { نام مرکز}, c=IR{توسط شورا تعیین شود}, o={صدور گواهی}
Subject Public Key Information	اطلاعات کلید عمومی دارنده گواهی	کلیدRSA با پیمانه X،بیتی rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	شناسه یکتای صادر کننده	وجود ندارد
Subject Unique Identifier	شناسه یکتای دارنده گواهی	وجود ندارد
Issuer's Signature	امضای صادر کننده	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	ملحقات	
Authority key identifier	شناسه کلید مرکز	Octet String(مقدار ۲۰ بایتی تابع درهم‌سازی SHA-1 بر روی اطلاعات باینری کلید عمومی مرکز صدور گواهی ریشه که بصورت DER کدگذاری شده باشد)
subject key identifier	شناسه کلید دارنده گواهی	Octet String(مقدار ۲۰ بایتی تابع درهم‌سازی SHA-1 بر روی اطلاعات باینری کلید عمومی مرکز صدور گواهی میانی که بصورت DER کدگذاری شده باشد)
key usage	کاربرد کلید	c=yes; digitalSignature, keyCertSign, cRLSign
Extended key usage	کاربردهای توسعه یافته کلید	وجود ندارد
Private key usage period	دوره کاربرد کلید خصوصی	وجود ندارد
Certificate policies	سیاست‌های گواهی الکترونیکی	c=no; {شناسه سیاست‌ها}

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
Policy Mapping	نگاشت سیاست	وجود ندارد
subject Alternative Name	نام بدیل دارنده گواهی	وجود ندارد
Issuer Alternate Name	نام بدیل صادر کننده	وجود ندارد
Subject Directory Attributes	مشخصات دایرکتوری دارنده گواهی	وجود ندارد
Basic Constraints	قیود اساسی	c=yes; cA=True; path length constraint = 0
Name Constraints	قیود نام	c=no; permitted subtrees: ou={ نام مرکز صدور توسط شورا تعیین شود}, ou=ECA, o={گواهی میانی}, c=IR
Policy Constraint	قیود سیاست‌ها	وجود ندارد
Authority Information Access	دسترسی به اطلاعات مرکز	c=no; optional; pointer to OCSP Responder
CRL Distribution Point	نقطه انتشار لیست گواهی‌های باطل شده	این فیلد حتماً باید وجود داشته باشد ;c = no

۷-۳) لیست گواهی‌های باطل شده مرکز دولتی صدور گواهی ریشه

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
Version	ویرایش	V3
Issuer Signature Algorithm	الگوریتم امضای صادر کننده	sha-1WithRSAEncryption
Issuer Distinguished Name	نام ترکیبی صادر کننده	cn={توسط شورا تعیین شود}, ou=CA, o={ توسط شورا تعیین شود}, c=IR
thisUpdate	بروزرسانی جاری	UTCT
nextUpdate	بروزرسانی بعدی	UTCT; thisUpdate + 6 months
Revoked certificates list	لیست گواهی‌های باطل شده	زوج مرتب‌هایی (صفر یا بیشتر) متشکل از شماره

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
		)UTCTسریال گواهی و تاریخ ابطال (مطابق با
CRL extensions	ملحقات لیست گواهی‌های باطل شده	
CRL Number	شماره لیست گواهی‌های باطل شده	یک عدد صحیح
Authority Key Identifier	شناسه کلید مرکز	مقدار ۲۰ بایتی تابع)c=no; Octet String بر روی اطلاعات باینری کلید SHA-1درهم‌سازی عمومی مرکز دولتی صدور گواهی ریشه که بصورت DER کدگذاری شده باشد)
CRL entry extensions	ملحقات ورودی لیست گواهی‌های باطل شده	
Invalidity Date	تاریخ پایان اعتبار	اختیاری است
Reason Code	کد دلیل	این فیلد حتماً باید وجود داشته باشد

۸) ضمیمه- ب

۸-۱) واژه‌نامه

مخفف	لغت	معنی
FIPS	Federal information processing standard	راهنمایی‌های تخصصی که موسسه ملی استانداردها و تکنولوژی آمریکا برای تهیه تجهیزات سیستم و سرویس پردازشگر اطلاعاتی تهیه کرده‌است.
KEA	Key Exchange Algorithm	یک الگوریتم قرارداد کلید که از کلید نامتقارن ۱۰۲۴ بیت استفاده می‌کند و توسط NSA توسعه یافته و به صورت سری طبقه‌بندی شده بود.
NSA	National Security Agency	سازمان حفاظت اطلاعات وزارت دفاع ایالت متحده آمریکا که مسئولیت‌های دولتی اساسی در رابطه با امنیت اطلاعات طبقه‌بندی شده و امنیت اطلاعات حساس طبقه‌بندی نشده سیستم‌های امنیتی ملی دارد.
PKCS	PKCS	مجموعه‌ای از مشخصات منتشرشده توسط آزمایشگاه‌های RSA برای ساختار داده‌ها و کاربرد الگوریتم رمزنگاری نامتقارن.
PKCS #10	PKCS #10	یک استاندارد از سری PKCS می‌باشد که ترکیب درخواست گواهی الکترونیکی را تعریف می‌کند. درخواست PKCS#10 دارای نام ترکیبی و کلید عمومی می‌باشد و می‌تواند شامل مشخصه‌های دیگر نیز باشد و توسط موجودیت درخواست‌کننده امضا می‌شود.
RSA	Rivest-Shamir-Adleman	الگوریتم رمزنگاری نامتقارن که در سال ۱۹۷۷ توسط ران ریوست، ادی شمیر و لئونارد آدلمن اختراع شده است.
SSL	Secure Sockets Layer	یک پروتکل اینترنتی که از رمزنگاری پیوسته بر اساس اتصال، برای فراهم کردن سرویس محرمانگی و تمامیت اطلاعات برای ترافیک بین مشتری و سرور استفاده می‌کند و به صورت اختیاری احراز هویت موجودیت‌ها را بین مشتری و سرور انجام می‌دهد.

Triple DES	Triple DES	یک رمزگذاری بلوکی براساس DES که هر بلوک ۶۴ بیتی از متن عادی را با به کار بردن الگوریتم رمزنگاری داده ۳ بار متوالی با استفاده از ۲ یا ۳ کلید متفاوت با طول کلید ۱۱۲ یا ۱۶۸ بیت، تغییر شکل می‌دهد.
X.500	X.500	استاندارد سرویس دایرکتوری اتحادیه ارتباطات بین‌المللی (ITU) و سازمان بین‌المللی استاندارد (ISO) می‌باشد.
X.509	X.509	نظریه ITU-T که یک چهارچوب برای فراهم و پشتیبانی کردن سرویس‌های احراز هویت منبع داده‌ها و احراز هویت موجودیت مستقل تعریف می‌کند.(مانند قالب‌های گواهی الکترونیکی X.509)

لغت	معادل	معنی
آسیب‌پذیری	Vulnerability	نقص یا ضعف در طراحی، پیاده‌سازی، عملیات و مدیریت سیستم که می‌تواند باعث تخطی از سیاست امنیت سیستم شود.
دستورالعمل اجرایی گواهی الکترونیکی	Certificate practice statement	دستورالعمل اجرایی که مرکز دولتی صدور گواهی برای صدور گواهی از آن استفاده می‌کند.
ابطال گواهی	Certificate Revocation	اعلام اینکه گواهی الکترونیکی معتبری که توسط یک مرکز صدور گواهی صادر شده است دیگر معتبر نمی‌باشد، معمولاً دارای تاریخ ابطال نیز می‌باشد.
اختیارات	Authorization	حقی که برای یک موجودیت سیستمی برای دسترسی به منابع قائل می‌شوند.
اطلاعات فعال ساز	Activation data	اطلاعات خصوصی(غیر از کلیدها) که برای دسترسی به ماجول‌های رمزنگاری مورد نیاز هستند.
اطمینان	Assurance	مشخصه‌ای از سیستم اطلاعاتی، که اطمینان می‌دهد سیستم مطابق با سیاست‌های امنیتی کار می‌کند.
اعتبار	Authenticity	اصل، قابل اطمینان و قابل تشخیص بودن.

لغت	معادل	معنی
اعتبار گواهی	Validity of Certificate	یک واحد داده در گواهی الکترونیکی که دوره زمانی اعتبار پیوند بین اطلاعات گواهی را مشخص می‌کند (مگر در زمانی که گواهی در لیست گواهی‌های باطل شده قرار بگیرد).
اعداد تصادفی	Random numbers	رشته اعداد غیر قابل حدسی که مقدار هر عدد، اتفاقی به دست آمده و وابسته به مقدار اعداد قبلی و بعدی نمی‌باشد.
امضا الکترونیکی	Digital Signature	مقداری که توسط الگوریتم رمزنگاری محاسبه شده و به یک شی اطلاعاتی افزوده 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. موقعیت یک سیستم در نتیجه اجرای اقدامات حفاظت از سیستم.
انقضا گواهی	Certificate Expiration	عدم اعتبار گواهی به دلیل پایان طول عمر تخصیص یافته به گواهی.
انکار ناپذیری	Non-repudiation	حفاظت در مقابل انکار دروغی دخالت در ارتباط.
بازرسی	Compliance Audit	بررسی و بازبینی مستقل اسناد و فعالیت‌های سیستم برای تشخیص کفایت کنترل‌های سیستم، اطمینان از مطابقت با دستورالعمل اجرایی و روال‌های آن، شناسایی نقص در سرویس صدور گواهی و پیشنهاد تغییرات به منظور اقدام متقابل.
بازیابی کلید	Key Recovery	فرایند به دست آوردن مقدار یک کلید رمزنگاری که قبلاً برای انجام عملیات رمزنگاری استفاده می‌شده است.
بایگانی	Archive	مجموعه‌ای از اطلاعات که برای مدت زمان طولانی برای مقاصدی مانند پشتیبانی سرویس ثبت وقایع، سرویس تمامیت سیستم ذخیره می‌شوند.
بررسی صحت هویت	Identity Verification	ارائه اطلاعات برای اثبات واقعیت هویت ادعا شده.
بروزرسانی گواهی	Certificate Update	فرایندی که توسط آن اطلاعات (به غیر از کلید گواهی) گواهی الکترونیکی موجود، بخصوص اختیارات داده شده به مالک، با صدور گواهی جدید تغییر می‌کند.

لغت	معادل	معنی
پایگاه داده‌ها	Database	مجموعه‌ای از اطلاعات مرتبط منطقی.
پروتکل	Protocol	مجموعی‌ای از قوانین برای اجرا و کنترل نوعی ارتباط بین سیستم‌ها.
پروتکل اعلام برخط وضعیت گواهی‌ها	Online certificate status protocol	یک پروتکل اینترنتی برای به دست‌آوردن وضعیت اعتبار و اطلاعات مرتبط با گواهی الکترونیکی توسط مشتری از سرور.
پیکربندی	Configuration	تنظیمات نرم‌افزاری و سخت‌افزاری سیستم‌های رایانه‌ای.
پیمانه	Modulus	مقدار ثابت تعریف شده در حساب پیمانه‌ای و معمولاً بخشی از کلید عمومی رمزنگاری نامتقارن بر اساس حساب پیمانه‌ای می‌باشد.
پیوند	Bind	با اجرای مکانیسم‌هایی، ارتباط جدانشدنی برقرار کردن، برای مثال استفاده از امضای الکترونیکی برای برقراری پیوند بین صاحب‌امضا و کلید عمومی گواهی.
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.
تجارت الکترونیکی	Electronic commerce	انجام ارتباطات و تراکنش‌های کاری از طریق شبکه و با استفاده از رایانه‌ها، به ویژه خریدن و فروختن کالاها و خدمات و انتقال وجوه از طریق ارتباط الکترونیکی.
تجدید کلید گواهی	Certificate Rekey	فرایند تجدید کلید عمومی گواهی الکترونیکی موجود با صدور گواهی جدید دارای کلید متفاوت جدید.
تجدید گواهی	Certificate Renewal	فرایند تمدید اعتبار اطلاعات گواهی الکترونیکی با صدور گواهی جدید.
تحلیل مخاطره	Risk Assessment	فرایندی که به صورت سیستماتیک منابع سیستمی مهم و تهدیدهای به این منابع را تشخیص داده و میزان خسارت را بر اساس تناوب و هزینه، وقوع برآورد کرده و اقدامات متقابلی را برای به حداقل رسانیدن امکان وقوع پیشنهاد می‌کند.
ترمیم خرابی	Disaster Recovery	فرایندی که کلیه اطلاعات از دست رفته را در زمان وقوع آتش، تخریب، حوادث طبیعی، یا خرابی سیستم بازیابی می‌کند.
تعلیق گواهی	Certificate Suspension	عدم اعتبار موقت گواهی الکترونیکی.

لغت	معادل	معنی
تعیین هویت-شناسایی	Identification	شناسایی و تشخیص موجودیت سیستمی از موجودیت‌های دیگر توسط سیستم از طریق ارائه شناسه.
توصیف‌کننده سیاست	Policy qualifier	اطلاعات وابسته به سیاست‌های گواهی الکترونیکی و موجود در فیلد الحاقی "توصیف‌کننده سیاست" که در گواهی الکترونیکی X.509, v3 قرار می‌گیرد.
توکن	Token	یک وسیله الکترونیکی برای کنترل دسترسی می‌باشد و می‌توان از آن برای به دست آوردن حق دسترسی استفاده کرد. بین طرف‌های درگیر مطابق با پروتکل هماهنگی استفاده مشترک استفاده می‌شود. معمولاً موجودیت فعلی دارای توکن، دسترسی انحصاری به منبع دارد.
تولید کلید	Key Generation	فرایند ایجاد رشته‌ای از علائم که یک کلید رمزنگاری را ایجاد می‌کنند.
تولیدکننده شماره‌های تصادفی	Random Number Generator	فرایند تولید سری اعداد غیرقابل حدس، که به صورت یکنواخت پخش‌شده اند.
تهیه نسخه پشتیبان	Backup	روال کپی کردن اطلاعات به منظور اطمینان از بازیابی آنها در زمان تخریب یا از دست دادن این اطلاعات.
ثبت وقایع	Audit Log	ثبت اطلاعات مورد نیاز به منظور ایجاد مسئولیت در قبال حوادث سیستم و عملیات موجودیت‌های سیستمی که باعث وقوع این حوادث می‌شوند.
ثبت نام	Registration	یک اقدام یا فرایند اجرایی برای ثبت اولیه نام و مشخصه‌های دیگر یک موجودیت در مرکز صدور گواهی (پیش از صدور گواهی الکترونیکی).
حساب پیمانه‌ای	Modular Arithmetic	شاخه‌ای از علم حساب برای اعداد صحیح است که در آن به هنگام شمارش، اعداد بعد از رسیدن به یک مقدار مشخص (پیمانه) به مقدار آغازین برمی‌گردند.
حسگر	Sensor	بخشی از یک دستگاه اندازه‌گیری که به تغییرات محیطی عکس‌العمل نشان می‌دهد.
حق مالکیت معنوی	Intellectual Property Right	حق کنترل و ایجاد مزایا از آنچه اختراع، اکتشاف یا ایجاد شده است.
خطر افشا قرار گرفتن	To be Compromised	یک حادثه امنیتی که تحت آن اطلاعات در معرض دسترسی غیرمجاز بالقوه قرار می‌گیرند.

لغت	معادل	معنی
درخواست گواهی	Certificate request	یک قالب تراکنشی مستقل از الگوریتم، تعریف شده توسط PKCS#10 ، حاوی نام ترکیبی و تعدادی مشخصه اختیاری می‌باشد که توسط موجودیت درخواست‌کننده گواهی امضا شده است، به مرکز صدور گواهی فرستاده شده و مرکز آنرا به گواهی الکترونیکی X.509 تبدیل می‌کند.
دسترسی‌پذیری	Availability	تحویل دادن اطلاعات به شخص درست، در زمان مناسب.
دسترسی	Access	توانای ارتباط با سیستم به منظور استفاده از منابع سیستم در جهت کنترل اطلاعات یا به دست آوردن اطلاعات موجود در سیستم.
دستیابی قانونی به کلید	Key Escrow	تکنیک بازیابی کلید به منظور ذخیره اطلاعات کلید رمزنگاری با مسئولیت شخص سومی (مسئول دستیابی قانونی) به منظور بازیابی کلید و استفاده از آن در شرایط خاص.
دیواره آتش	Firewall	یک اتصال بین شبکه‌ای که ترافیک اطلاعاتی بین شبکه‌های متصل را محدود میکند و منابع سیستمی شبکه را در مقابل مخاطرات شبکه‌های دیگر محافظت می‌کند.
وسیله ذخیره‌سازی	Media	آنچه اطلاعات در آن نوشته و ذخیره می‌شود.
رک	Rack	کابینتی که سرور یا ایستگاه کاری ذخیره‌سازی در آن قرار می‌گیرد.
رمز مشترک	Shared Secret	کلید مخفی یا اطلاعات دیگری که توسط دو طرفی که می‌خواهند رابطه ایمن ایجاد کنند، نگه‌داری می‌شود. این اطلاعات ممکن است برای اجرای احراز هویت، تجدید کلید، رمزنگاری و آشکارسازی استفاده شود.
رمزگذاری	Encryption	تغییر اطلاعات (پیام عادی) به قالبی که اطلاعات اولیه را پنهان می‌کند و از استفاده یا آشکار کردن این اطلاعات جلوگیری می‌کند.
رمزنگاری	Cryptography	علم ریاضی تغییر داده‌ها به منظور نامفهوم کردن معنای آنها، جلوگیری از تغییرات و استفاده غیرمجاز می‌باشد. در صورتیکه تغییر قابل برگشت باشد، این علم به بازیابی اطلاعات رمزنگاری شده نیز می‌پردازد.
زنجیره گواهی	Certification Path	زنجیره منظم گواهی الکترونیکی که به طرف اعتماد کننده توانایی ارزیابی صحت امضای آخرین گواهی این زنجیره را می‌دهد.

لغت	معادل	معنی
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 گرفتن کلید خصوصی از اطلاعات کلید عمومی وجود نداشته باشد.
زیر ساخت کلید عمومی	Public Key Infrastructure	مجموعه‌ای از سیاست‌ها، فرایندها، نرم‌افزارها و ایستگاه‌های کاری مورد نیاز برای اداره گواهی‌ها و زوج‌کلیدها می‌باشد (مانند صدور، نگه‌داری و ابطال گواهی‌الکترونیکی).
سخت‌افزار	Hardware	اجزا فیزیکی سیستم رایانه‌ای.
سرور-خدمتگزار	Server	یک موجودیت سیستمی که در جواب درخواست‌های موجودیت‌های سیستمی دیگر به نام مشتری، سرویس فراهم می‌کند.
سطح استحکام الگوریتم	Strength of algorithm	استحکام یک الگوریتم از میزان انتروپی که در متن رمز شده ایجاد می‌کند، مشخص می‌شود. لذا استحکام یک الگوریتم رابطه مستقیم با دو عامل روش ریاضی مورد استفاده و طول کلید الگوریتم دارد.
سطح اطمینان	Assurance Level	یک سطح بخصوص در مقیاس مرتبه‌ای که نشان‌دهنده اطمینان به مطابقت هدف مورد بررسی با نیازها می‌باشد.
سیاست‌های امنیتی	Security policy	مستندی حاوه مجموعه‌ای از دستورات، اقدامات و روال‌های مشخص‌کننده کنترل‌های امنیتی مدیریت، توزیع و حفاظت از دارایی‌ها می‌باشد.
سیاست‌های گواهی الکترونیکی	Certificate Policy	مجموعه‌ای از قوانین که الزمات و سیاست‌های زیر ساخت کلید عمومی را مشخص می‌کند.
سیستم	system	در دستورالعمل اجرایی گواهی الکترونیکی به معنای سیستم اطلاعاتی مکانیزه می‌باشد.
سیستم عامل	Operating System	برنامه رایانه که عملیات اساسی سیستم را انجام می‌دهد(اجرایی برنامه‌ها، تهیه لیست از فایل‌های موجود) مانند MS windows .
شبکه	Network	مجموعه‌ای از رایانه‌های میزبان که با شبکه‌های دیگر یا شبکه اینترنت اطلاعات مبادله می‌کنند.

لغت	معادل	معنی
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، منحصربفرد می‌باشد.
شماره شناسایی شخصی	User PIN	یک شماره شناسایی شخصی که دسترسی به وظایف و اطلاعات ذخیره‌شده در سخت‌افزار مربوطه را کنترل‌می‌کند.
شناسه	Object Identifier	نامی منحصربفرد و رسمی، تشکیل شده از مجموعه‌ای از اعداد (تخصیص یافته توسط استاندارد ASN.1) که برای اشاره به اشیا با ویژگی‌های مشخص استفاده می‌شود.
شناسه سیاست گواهی	Policy Object Identifier (POID)	نامی منحصربفرد و رسمی، تشکیل شده از مجموعه‌ای از اعداد (تخصیص یافته توسط استاندارد ASN.1) که برای اشاره به سیاست‌نامه گواهی الکترونیکی استفاده می‌شود.
صاحب امضا	Subscriber	شخصی که برای وی گواهی الکترونیکی صادر شده است و می‌تواند از کلید خصوصی مرتبط با کلید عمومی درون گواهی استفاده کند.
صفر کردن	Zeroize	پاک کردن اطلاعات ذخیره‌شده به گونه‌ای که غیرقابل استفاده و بازیابی شوند، بخصوص کلید ذخیره‌شده در سخت‌افزار رمزنگاری یا ابزار دیگر.
طرف اعتماد کننده	Relying Party	شخصی که به اعتبار اطلاعات گواهی الکترونیکی اعتماد می‌کند.
طول کلید	Key Length	تعداد علائم (معمولاً در قالب بیت) مورد نیاز برای ارائه مقدار یک کلید رمزنگاری.
علامت تجاری	Trade Mark	علامت انتخاب شده توسط تولید کننده برای متمایز کردن محصولات خود از محصولات تولید شده توسط اشخاص دیگر.
عنوان گواهی	Subject Name	نامی که به اطلاعات موجود در گواهی الکترونیکی، بخصوص به مقدار کلید گواهی الکترونیکی پیوند داده شده است.
فایل ترمیمی	Patch	بروزرسانی نرم‌افزار به منظور رفع مشکلات در نسخه‌های قبلی آن.
فیلد	Field	بخشی از گواهی که محتوی آن نوع خاصی از داده‌ها (از پیش تعریف شده توسط استاندارد X.509) می‌باشد.
کارت هوشمند	smart card	یک وسیله در سایز کارت اعتباری محتوی یک یا چند مدار مجتمع که وظایف پردازشگر مرکزی رایانه، حافظه و میانگر ورودی/خروجی را به عهده دارد.

لغت	معادل	معنی
کانال	Channel	مسیر انتقال اطلاعات در یک سیستم.
کلمات رمز-اسم رمز	Password	اطلاعات احراز هویت محرمانه که معمولا از رشته‌ای از حروف تشکیل می‌شود.
کلید امضا	Signature key	کلیدی که برای امضا کردن استفاده می‌شود.
کلید خصوصی	Private Key	جزء مخفی زوج کلید رمزنگاری که برای رمزنگاری نامتقارن استفاده می‌شود.
کلید رمزنگاری	Encryption Key	یک کلید رمزنگاری که برای رمز کردن داده‌های برنامه‌های کاربردی استفاده می‌شود.
کلید عمومی	Public key	جزء زوج کلید رمزنگاری که قابل افشا برای عموم می‌باشد و در الگورتم رمزنگاری نامتقارن استفاده می‌شود.
شورای سیاست‌گذاری گواهی الکترونیکی	National PKI Commission	به منظور حفظ یکپارچگی و جلوگیری از تفکیک راهکارها و استانداردهای بکار گرفته شده در مراکز صدور گواهی ریشه و میانی و نیز سیاست‌گذاری در زمینه فعالیت‌های مرکز دولتی صدور گواهی ریشه و تصویب سیاست‌های گواهی الکترونیکی ریشه و تایید تطابق دستورالعمل اجرایی تمام مراکز صدور گواهی با این سیاست‌ها، شورای به نام شورای سیاست‌گذاری گواهی الکترونیکی تشکیل می‌شود.
کنترل دسترسی	Access Control	حفاظت از منابع سیستمی در مقابل دسترسی غیر مجاز.
گواهی امضا	signature certificate	یک گواهی الکترونیکی، محتوی یک کلید عمومی که برای شناسایی امضای الکترونیکی بیشتر از رمزنگاری داده‌ها و عملیات رمزنگاری دیگر استفاده می‌شود.
گواهی میانی	Subject Certificate	گواهی مرکز صدور گواهی میانی که توسط مرکز دولتی صدور گواهی ریشه امضا می‌شود و به مرکز صدور گواهی میانی اجازه صدور گواهی برای صاحبان امضا را می‌دهد.
گواهی خودامضا	Self-signed Certificate	یک گواهی الکترونیکی که در آن، کلید عمومی گواهی و کلید خصوصی استفاده شده برای امضای گواهی، اجزا یک زوج کلید متعلق به امضا کننده هستند.
گواهی الکترونیکی	Digital Certificate	یک گواهی در قالب شی داده‌ای الکترونیکی که به آن یک امضای الکترونیکی بر اساس آن شی داده‌ای اضافه می‌شود

لغت	معادل	معنی
گواهی مورد اطمینان	Trusted certificate	یک گواهی که طرفهای اعتماد کننده به اعتبار آن، بدون نیاز به ارزیابی صحت گواهی مذکور، اطمینان می‌کنند. بخصوص گواهی الکترونیکی که برای فراهم کردن اولین کلید عمومی گواهی در زنجیره گواهی استفاده می‌شود.
الگوریتم	Algorithm	مجموعه محدود دستورالعمل‌های گام‌بگام برای حل کردن مسائل و روال‌های محاسباتی، بخصوص روال‌هایی که توسط رایانه اجرا می‌شوند.
الگوریتم متقارن	Symmetric Algorithm	یک الگوریتم رمزنگاری که در آن کلید رمزنگاری می‌تواند از کلید آشکارسازی محاسبه شود و بالعکس. در بیشتر الگوریتم‌های متقارن کلید رمزنگاری و آشکارسازی یکی هستند.
لیست گواهی‌های باطل شده	Certificate Revocation List	یک ساختار داده که گواهی‌های الکترونیکی را که دیگر توسط صادر کننده گواهی معتبر به حساب نمی‌آیند را لیست می‌کند.بعد از اینکه یک گواهی در لیست گواهی‌های باطل شده وارد می‌شود، از لیست‌گواهی‌های باطل شده بعدی پس از انقضا حذف می‌شود.
سخت‌افزار سخت‌افزاری رمزنگاری	Hardware Encryption Module/HSM	مجموعه‌ای از سخت‌افزار، نرم‌افزار و ترکیب آنها که فرایند و منطق رمزنگاری را مانند الگورتم رمزنگاری اجرا می‌کند و در محدوده رمزنگاری سخت‌افزار قرار دارد.
محرمانگی	Confidentiality	عدم افشا یا در دسترس قراردادن اطلاعات برای اشخاص، موجودیت‌ها و یا روال‌ها.
مخاطره	Risk	امکان خسارت. احتمال اینکه یک تهدید خاص باعث ایجاد آسیب‌پذیری خاص و نتایج مخرب خاص شود.
مخزن	Repository	یک سیستم ذخیره و پخش گواهی‌های الکترونیکی و اطلاعات مربوط به آنها (مانند لیست گواهی‌های باطل شده) برای طرفهای اعتماد کننده.
مدیریت کلید	Key Management	فرایند کنترل کلیدهای رمزنگاری و موارد مرتبط با آنها (مانند مقدار اولیه) طی طول عمر آنها در یک سیستم رمزنگاری که شامل مرتب‌سازی، تولید، پخش، ذخیره، بارگیری، دستیابی قانونی، بایگانی، بازرسی و تخریب آنها می‌شود.

لغت	معادل	معنی
مدیریت مخاطرات	Risk Management	فرایند شناسایی، کنترل، حذف یا به حداقل رسانیدن حوادث نامعلوم که ممکن است بر منابع سیستم تاثیرگذار باشند.
مرجع اعلام برخط وضعیت	OCSP Responder	سروری که وضعیت گواهی را مطابق با پروتکل اعلام وضعیت گواهی به صورت برخط ارائه می‌کند.
دفتر ثبت نام	Registration Authority	یک موجودیت اختیاری در زیر ساخت کلید عمومی می‌باشد که گواهی‌های الکترونیکی یا لیست گواهی‌های باطل شده را امضا نمی‌کند 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.
مرکز صدور گواهی	Certificate Authority	موجودیتی که گواهی الکترونیکی صادر می‌کند و پیوند بین داده‌های گواهی را ضمانت می‌کند.
مرکز صدور گواهی میانی	Subject CA	یک مرکز صدور گواهی که گواهی خود را از مرکز دولتی صدور گواهی ریشه دریافت می‌کند و می‌تواند برای صاحبان امضا گواهی صادر کند.
مرکز دولتی صدور گواهی الکترونیکی ریشه	Root CA	یک مرکز صدور گواهی که مستقیماً مورد اطمینان موجودیت نهایی می‌باشد. به دست آوردن کلید عمومی مرکز دولتی صدور گواهی ریشه نیاز به مکانیسم‌های ضامن سلامت و دست نخوردگی دارد.
مسیریاب	Router	یک رایانه شبکه‌ای که بسته‌های پروتکل اینترنت را که مقصدشان خود رایانه نیست، به خارج هدایت می‌کند.
مشتری	Client	یک موجودیت سیستمی که از موجودیت سیستمی دیگری که سرور نامیده می‌شود درخواست سرویس کرده و از این سرویس استفاده می‌کند.
مقداردهی اولیه	Initialization	یک پارامتر ورودی که الگوریتم رمزنگاری را مقداردهی اولیه می‌کند.
مکانیسم 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.

لغت	معادل	معنی
ملحقات گواهی	Certificate Extensions	اطلاعاتی که برای اضافه کردن اختیاری به گواهی X.509, v3 تعریف شده‌اند.
موجودیت نهایی	End entity	موجودیتی که از کلیدها و گواهی‌ها برای ایجاد یا تشخیص صحت امضا یا محرمانگی آن استفاده می‌کند.موجودیت‌ها نهایی صاحبان امضا، سازمان‌ها یا طرفهای اعتماد کننده می‌باشند.
مهر زمانی	Time Stamp	امضای الکترونیکی که دارای تاریخ و ساعت می‌باشد و گواهی می‌کند که محتویات آن در زمان مشخصی امضا شده‌اند.
میان‌شبکه	Internetwork	سیستمی از شبکه‌های به هم پیوسته. شبکه‌ای از شبکه‌ها.
نام ترکیبی	Distinguished Name	یک شناسه منحصربفرد که شی موجود در درخت اطلاعاتی دایرکتوری(DIT) قالب X.500 را ارائه می‌کند.
نقطه اطمینان	Trust Anchor	گواهی مرکز دولتی صدور گواهی ریشه که از کانالی مطمئن دریافت شده است.
نگاشت سیاست	Policy Mapping	زمانیکه یک مرکز صدور گواهی موجود در یک دامنه به مرکز صدور گواهی دیگری در دامنه دیگر گواهی دهد، سیاست‌های گواهی الکترونیکی موجود در دامنه دیگر ممکن است که توسط مرکز صدور گواهی دامنه اول معادل با سیاست‌های گواهی موجود در دامنه اول تشخیص داده شود.
ورود به سیستم	Login	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 می‌کند، انجام می‌شود.
ورودی	Entry	اطلاعات وارد شده در مستندات، نرم‌افزارهای کاربردی، پایگاه داده‌ها.
ویروس	Virus	یک قسمت مخفی و خود تکرار نرم‌افزاری رایانه‌ای دارای منطق 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 باید برای فعال شدن ویروس اجرا شود.
هویت	Identity	مجموعه‌ای از مشخصات محسوس و نامحسوس شخصی که اشخاص را از یکدیگر متمایز می‌کند.

لغت	معادل	معنی
تمامیت	Integrity	عدم تخریب یا تغییر غیر مجاز اطلاعات.