جمهوری اسلامی ایران
وزارت بازرگانی

مرکز صدور گواهی الکترونیکی میانی بازرگانی

Ministry of Commerce
Intermediate Certification Authority
MOC-ICA

دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی بازرگانی

Certificate Practice Statement
(CPS)

طبقه بندی : عادی

ویرایش : ۱/۰

تاریخ انتشار : ۱۳۸۶/۰۷/۳۰

فهرست مطالب

مفاهیم

دستورالعمل اجرایی گواهی الکترونیکی[1]*: دستورالعمل اجرایی که مرکز صدور گواهی الکترونیکی برای صدور گواهی از آن استفاده می‌کند و مجموعه دستورالعملهایی است که منطبق با سند سیاست گواهی جهت تشریح جزئیات عملکرد مدیریت گواهی‌های الکترونیکی در ریشه و مراکز میانی تدوین می‌گردد.*

اطلاعات فعال‌ساز[2]*: اطلاعات شخصی(غیر از کلیدها) که برای دسترسی به دستگاه‌های رمزنگاری مورد نیاز هستند.*

امضای الکترونیکی[3]*: 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[4]*: 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[5]*: زنجیره منظم گواهی الکترونیکی که به طرف اعتماد کننده توانایی ارزیابی صحت امضای آخرین گواهی این زنجیره را می‌دهد.*

---

[1] *Activation Data*
[2] *Activation Data*
[3] *Digital Signature*
[4] *Self- Signed Certificate*
[5] *Certificate Chain*

زیرساخت کلید عمومی[1]*: مجموعه‌ای از سیاست‌ها، فرآیندها، نرم‌افزارها و ایستگاه‌های کاری مورد نیاز برای اداره گواهی‌ها و زوج کلیدها می‌باشد*

سیاست های گواهی الکترونیکی[2]: 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 الزامات پیاده‌سازی مراکز صدور گواهی، دفاتر ثبت نام، صاحبان امضاء و صرف‌های اعتماد کننده را مشخص می‌کند. تدوین این سیاست‌های گواهی برای مرکز ریشه الزامی است و می‌تواند برای مرکز میانی بطور جداگانه تنظیم گردد.

صاحب‌امضا[3]: 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[4]: شخصی که به اعتبار اطلاعات گواهی الکترونیکی اعتماد می‌کند.

کلید خصوصی[5]: جزء مخفی زوج کلید رمزنگاری که برای رمزنگاری نامتقارن استفاده می‌شود.

سیاست های گواهی الکترونیکی[6]*: 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 الزامات*

---

[1] *Public Key Infrastructure*

[2] *Certificate policy*

[3] *Subscriber*

[4] *Relaying Party*

[5] *Private Key*

[6] *Certificate policy*

پیاده‌سازی مراکز صدور گواهی، دفاتر ثبت نام، صاحبان امضاء و صرف‌های اعتماد کننده را مشخص می‌کند. تدوین این سیاست‌های گواهی برای مرکز ریشه الزامی است و می‌تواند برای مرکز میانی بطور جداگانه تنظیم گردد.

صاحب‌امضا [1]*: 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 [2]*: شخصی که به اعتبار اطلاعات گواهی الکترونیکی اعتماد می‌کند.*

کلید خصوصی [3] *: جزء مخفی زوج کلید رمزنگاری که برای رمزنگاری نامتقارن استفاده می‌شود.*

کلید عمومی [4]*: جزء زوج کلید رمزنگاری که قابل افشا برای عموم می‌باشد و در الگوریتم رمزنگاری نامتقارن استفاده می‌شود.*

گواهی الکترونیکی [5]*: داده الکترونیکی حاوی اطلاعاتی در مورد مرکز صادر کننده گواهی، مالک گواهی، تاریخ انقضا گواهی، کلید عمومی مالک و یک شماره سریال میباشد که توسط یک مرکز صدور گواهی امضا شده به گونه ای که هر شخصی میتواند به صحت ارتباط بین کلید عمومی و مالک گواهی اطمینان کند.*

لیست گواهی‌های باطل شده [1]*: 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.*

---

[1] *Subscriber*
[2] *Relaying Party*
[3] *Private Key*
[4] *Public Key*
[5] *Digital certificate*

دستگاه سخت‌افزاری رمزنگاری [۲]؛ *مجموعه‌ای از سخت‌افزار، نرم‌افزار و ترکیب آنها که فرآیند و منطق رمزنگاری را مانند الگوریتم رمزنگاری اجرا می‌کند.*

مخزن [۳]؛ *پایگاه داده ذخیره و انتشار گواهی‌های الکترونیکی و اطلاعات مربوط به آنها جهت بهره‌برداری طرفهای اعتماد کننده است.*

دفتر ثبت‌نام [۴]؛ *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 [۵]؛ *موجودیتی که گواهی الکترونیکی صادر می‌کند و پیوند بین داده‌های گواهی را ضمانت می‌کند.*

مرکز صدور گواهی میانی [۶]؛ *یک مرکز صدور گواهی که با کسب مجوز از یک مرکز ریشه و گرفتن گواهی خود از مرکز صدور گواهی ریشه می‌تواند برای صاحبان امضا گواهی صادر کند.*

مرکز صدور گواهی ریشه [۷]؛ *یک مرکز صدور گواهی الکترونیکی که مستقیماً مورد اطمینان موجودیت نهایی می‌باشد. به دست آوردن کلید عمومی مرکز صدور گواهی ریشه نیاز به مکانیزم‌های ضامن سلامت و دست نخوردگی دارد.*

---

[1] *CRL (Certificate Revokation List)*

[2] *Hardware security module*

[3] *Repository*

[4] *Registration Autority*

[5] *Certification Autority*

[6] *Certification Authority*

[7] *Root Certification Authority*

موجودیت نهایی[1]: 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 می‌باشند.

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

خدمات گواهی الکترونیکی[2]: به خدماتی نظیر ارائه گواهی الکترونیکی، خدمات مهر زمانی[3]، خدمات ارائه وضعیت بر خط گواهی[4] اطلاق می‌گردد.

کاربردهای گواهی الکترونیکی[5]: به هر نوع توسعه کاربرد خدمات گواهی الکترونیکی نظیر توسعه گواهی الکترونیکی در سامانه‌های کاربردی مانند سیستم الکترونیکی ثبت سفارش واردات، پست الکترونیکی امن[6]، گواهی Secure Socket Layer و کاربردهایی از این دست اشاره می‌نماید.

شیوه نامه کاربردی ؛ مجموعه دستورالعملهایی است که ضوابط، شیوه و جزئیات کاربرد خدمات و گواهی‌های صادره از سوی مرکز صدور گواهی الکترونیکی میانی بازرگانی را بیان نموده و منطبق با این دستورالعمل و رعایت قوانین حاکم مندرج در بند ۲-۴-۱ این دستورالعمل توسط مرکز صدور گواهی الکترونیکی میانی بازرگانی تهیه و پس از تایید کمیسیون گواهی الکترونیکی بازرگانی برای اخذ تایید نهایی و مجوز کاربرد در اختیار مرکز دولتی صدور گواهی الکترونیکی ریشه قرار می‌گیرد. برای هر کاربرد یک شیوه نامه کاربردی تهیه می‌گردد.

---

[1] End Entity
[2] Service
[3] Time Stamping
[4] Online Certificate Status Protocol
[5] Application
[6] Secure e-mail

۱) مقدمه

دستورالعمل اجرایی گواهی الکترونیکی میانی بازرگانی بر اساس "سیاست های گـواهی الکترونیکـی ریـشه " در راسـتای فراهم کردن سرویس‌های گواهی الکترونیکی در حوزه بازرگانی تولید شده است. این دستورالعمل بر پایه استاندارد X.509 و مطابق با RFC2527 تنظیم شده است و با قانون تجارت الکترونیکی ایران همخوانی دارد.

این دستورالعمل روال صدور و مدیریت گواهی الکترونیکی میانی بازرگانی را توسط مرکـز صـدور گـواهی الکترونیکـی میانی بازرگانی مشخص می‌کند. گواهی های صادر شده توسط این مرکز صدور گواهی به منظور فراهم آوردن سرویـسهای احراز هویت، انکارناپذیری، محرمانگی و تمامیت اطلاعات بـرای ارسـال اطلاعـات بـین مـشتری و سـرورهای الکترونیکـی استفاده می‌شود.

۱-۱) خلاصه

دستورالعمل اجرایی گواهی الکترونیکی، به موجودیت‌های وابسته به مرکز صـدور گـواهی الکترونیکـی میـانی بازرگـانی مانند صاحبان امضا (کاربران)، طرف های اعتماد کننده(سازمانهای بازرگانی و . . .) و دفاتر ثبت‌نام می‌پـردازد. ایـن سـند شرح کلیه فعالیت‌های مرکز صدور گواهی الکترونیکی، از زمان شروع به کار برای صدور گواهی تا زمان ابطال یـا تعـویض گواهی می‌باشد.

کمیسیون گواهی الکترونیکی میانی بازرگانی، سازمان مدیریتی مرکز صدور گواهی الکترونیکی می‌باشد. کلیـه تغییـرات در این دستورالعمل ، تنها پس از تایید کمیسیون مذکور قابل اجرا است.

۱-۲) شناسه سند

از این پس، این سند بنام سند دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی میانی بازرگانی شناخته می‌شود. تاریخ انتشار سند ۱۳۸۶/۰۷/۳۰ می‌باشد. آخرین نسخه این سند در سایت مرکز صدور گواهی الکترونیکی میانی بازرگانی به آدرس Http://www.mocca.ir قابل دسترسی است.

برای کسب اطلاعات بیشتر به سیاست های گواهی الکترونیکی ریشه به آدرس Http://www.rca.gov.ir رجوع شود.

۱-۳) اجزاء و کاربردها

۱-۳-۱) موجودیت های مرکز صدور گواهی الکترونیکی میانی بازرگانی

۱-۳-۱-۱) کمیسیون گواهی الکترونیکی میانی بازرگانی

کمیسیون گواهی الکترونیکی میانی بازرگانی که از این پس در این سند "کمیسیون" نامیده می‌شود، برای موارد ذیل تأسیس شده است:

- بازبینی دستورالعمل‌های اجرایی مرکز صدور گواهی الکترونیکی مربوط به خدمات گواهی تحت نظارت آن و بررسی تطابق آنها با سیاست های مرکز صدور گواهی الکترونیکی ریشه
- بازبینی نتایج بازرسی مرکز صدور گواهی الکترونیکی میانی تحت نظارت آن، جهت تطابق با مفاد سیاست‌های مرکز صدور گواهی الکترونیکی ریشه و دستورالعمل‌های تأیید شده و توصیه اقدامات اصلاحی یا پیشگیرانه مناسب، مانند لغو یا تغییر گواهی‌ها.

۱-۳-۱-۲) مرکز صدور گواهی الکترونیکی بازرگانی

مرکز صدور گواهی الکترونیکی میانی موجودیتی است که توسط مرکز صدور گواهی الکترونیکی ریشه مورد تائید قرار گرفته و مجوز ایجاد، امضاء و صدور خدمات گواهی الکترونیکی را دریافت کرده است.

دستورالعمل اجرایی مرکز گواهی الکترونیکی میانی بازرگانی از قواعد کلی سند سیاست‌های گواهی ریشه تبعیت می‌کند و خود دارای سند سیاست‌های گواهی نمی‌باشد.

۱-۳-۱-۳) دفتر ثبت نام

مرکز ثبت‌نام[1] گواهی الکترونیکی موجودیتی است که برای جمع‌آوری و بررسی صحت اطلاعات مربوط به هویت صاحبان امضاء که در گواهی الکترونیکی وارد خواهد شد، با مرکز صدورگواهی الکترونیکی میانی بازرگانی توافق نموده و براساس ضوابط ایجاد شده است. دفتر ثبت نام می‌بایست کارکردهای خود را با این دستورالعمل، تطابق دهد.

۱-۳-۱-٤) صاحبان امضاء[2]

صاحب امضاء موجودیتی است که نامش در "عنوان" گواهی الکترونیکی ثبت می‌شود و مدعی استفاده از کلید و گواهی‌اش بر طبق سیاست های گواهی الکترونیکی است.

۱-۳-۱-۵) طرف‌های اعتماد کننده[3]

طرف اعتماد کننده موجودیتی است که به درستی پیوند میان نام صاحب امضاء با کلید عمومی‌اش اتکاء (اعتماد) می‌کند و بر اساس این اعتماد برای بررسی یکپارچگی یک پیام امضا شده الکترونیکی، تشخیص سازنده پیام یا برقراری

---

[1] *Subscriber*

[2] *Subscriber*

[3] *Relying Parties*

ارتباط محرمانه، از گواهی شخص دیگری، استفاده می‌کند. طرف اعتماد کننده ممکن است از اطلاعات گـواهی الکترونیکـی (مانند شناسه سیاست گواهی)[1] برای تعیین تناسب گواهی با یک کاربرد خاص استفاده کند. طرف اعتماد کننده این کـار را با مسئولیت خود انجام می‌دهد. طرفهای اعتماد کننده حسب خدمات و کاربردهای گواهی الکترونیکی خواهندبود.

۱-۳-۲) کاربرد های گواهی الکترونیکی میانی بازرگانی

کلیه گواهی های الکترونیکی صادر شده توسط مرکز صدور گواهی الکترونیکی میانی تحت این آیین نامـه اجرایـی مـی باشند. این گواهی‌های در سامانه‌های کاربردی مورد استفاده قرار می‌گیرد. گواهی‌های صادر شـده تحـت ایـن آیـین نامـه مطابق با استاندارد X.509 V3 می باشند.

مرکز صدور گواهی الکترونیکی میانی بازرگانی برای خدمات و کاربردهای گواهی الکترونیکـی، گـواهی ۱۰۲۴ بیتـی بـا مدت اعتبار یک ساله صادر میکند.

۱-۳-۲-۱) ممنوعیت‌های استفاده از گواهی

ارسال و دریافت اطلاعات نظامی طبقه‌بندی شده یا عملکرد تاسیسات هسته‌ای

ارتکاب جرم

[1] *Policy Object Identifier (POID)*

۱-٤) جزئیات تماس

۱-٤-۱) راهبری سیاست‌ها

مرکز صدور گواهی الکترونیکی میانی بازرگانی، مسئولیت تولید شیوه نامه کاربردی اجرایی خدمات و کاربردهای گواهی‌الکترونیکی را دارد. این دستورالعمل تنها پس از دریافت مجوز از کمیسیون گواهی الکترونیکی وزارت بازرگانی و شورای سیاستگذاری گواهی الکترونیکی کشور قابل اجرا است.

آدرس پست الکترونیکی : info@mocca.ir

تارنما: Http://www.mooca.ir

شماره تلفن: ۸۸۹۶۳۲۷۷-۲۱-۰۰۹۸

شماره نمابر:۸۸۹۶۹۷۳۶-۲۱-۰۰۹۸

آدرس: تهران، بلوار کشاورز، خیابان شهید نادری، پلاک ۱۱

۱-٤-۲) اطلاعات تماس مرکز صدور گواهی الکترونیکی میانی بازرگانی

اطلاعات تماس شخص پاسخگو در مورد این دستورالعمل در زیر ارائه شده است:

آدرس پست الکترونیکی : info@mocca.ir

شماره تلفن: ۸۸۹۶۳۲۷۷-۲۱-۰۰۹۸

شماره نمابر: ۸۸۹۶۹۷۳۶-۲۱-۰۰۹۸

آدرس: تهران، بلوار کشاورز، خیابان شهید نادری، پلاک ۱۱

۱-٤-۳) مسؤل تطبیق دستورالعمل اجرایی با سیاست های مرکز صدور گواهی الکترونیکی ریشه

مرکز دولتی صدورگواهی الکترونیکی ریشه تطابق این دستورالعمل با سیاست ها (CP) و دستورالعمل اجرایی (CPS) مرکز دولتی صدور گواهی الکترونیکی ریشه ، را اعلام خواهد کرد.

۲) مقررات عمومی[1]

۲-۱) وظایف و مسئولیت‌ها

۲-۱-۱) وظایف کمیسیون گواهی الکترونیکی میانی بازرگانی

وظایف و مسئولیت‌های کمیسیون گواهی الکترونیکی میانی بازرگانی شامل موارد زیر می‌باشد:

- پیشنهاد و بروزرسانی رویه‌ها و دستورالعمل‌های اجرایی و شیوه‌نامه‌های کاربردی گواهی‌های الکترونیکی، خدمات و کاربردهای آن.؛
- بازرسی ادواری مرکز صدور گواهی الکترونیکی میانی بازرگانی به منظور تایید مطابقت با سیاست‌های مرکز صدور گواهی الکترونیکی ریشه و این آیین نامه؛
- بررسی راه‌حل‌های ارائه شده توسط مرکز صدور گواهی الکترونیکی میانی بازرگانی در برخورد با مشکلات و مسایل امنیتی.

۲-۱-۲) وظایف مرکز صدور گواهی الکترونیکی میانی بازرگانی

مرکز صدور گواهی الکترونیکی میانی بازرگانی در موارد زیر مسئولیت دارند:

- تدوین دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی خود مطابق با سیاست‌های مرکز صدور گواهی الکترونیکی ریشه ؛

General Provisions[1]

- مطابقت فعالیت‌ها با مقررات دستورالعمل اجرایی مرکز صدور گواهی الکترونیکی خود و قرارداد بین مرکز صدور گواهی میانی با مرکز 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 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 صدور گواهی الکترونیکی ریشه بدین معناست که مرکز صدور گواهی صحت اطلاعات آن گواهی را تائید می‌کند؛
- تولید ایمن کلیدهای خصوصی خود (مطابق با سیاست‌نامه مرکز صدور 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 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 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 مرکز صدور گواهی میانی تا قبل از انتشار اطلاعات مربوط به ابطال گواهی خود، توسط مرکز صدور گواهی الکترونیکی ریشه ، مسئولیت همه چیز را بر عهده دارد؛
- 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 صدور گواهی الکترونیکی ریشه برای نقض تعهدات خود در مورد طرفهای اعتماد کننده استفاده کند.
- تدوین شیوه‌نامه کاربردهای گواهی‌الکترونیکی میانی بازرگانی طبق چارچوبی که مرکز دولتی صدور گواهی ریشه اعلام خواهد کرد برای هر یک از کاربردهای گواهی الکترونیکی و ارائه آنها جهت تایید به کمیسیون گواهی میانی بازرگانی. هر شیوه نامه کاربردی تایید شده توسط کمیسیون باید جهت اخذ مجوز حداکثر ظرف مدت ۵ روز کاری به طور رسمی در اختیار مرکز دولتی صدور گواهی الکترونیکی ریشه قرار گیرد.

۲-۱-۳) وظایف دفاتر ثبت‌نام گواهی الکترونیکی

دفاتر ثبت‌نام در موارد زیر مسئولیت دارند:

- انجام عملیات مطابق با این دستورالعمل.
- احراز هویت و تصدیق مدارک ارایه شده متقاضی دریافت خدمات گواهی.
- ارسال درخواست متقاضی همراه با مدارک مربوطه به مرکز میانی بازرگانی.
- دریافت گواهی صادر شده از مرکز میانی بازرگانی و تحویل به متقاضی.

۲-۱-٤) وظایف صاحبان امضا

صاحبان امضا در موارد زیر مسئولیت دارند:

- مطابقت با قرارداد بین صاحبان امضا و مرکز صدور گواهی الکترونیکی و این آیین نامه؛
- ارائه اطلاعات دقیق و درست هنگام درخواست گواهی؛
- استفاده از گواهی های خود تنها برای مقاصد قانونی و مجاز مطابق با این آیین نامه و قانون حاکم؛
- تولید زوج کلید و محافظت از کلید خصوصی مطابق با دستورالعمل های ارائه شده؛
- اطلاع رسانی به دفاتر ثبت نام گواهی الکترونیکی در صورت تغییر اطلاعات موجود در گواهی؛
- اطلاع رسانی به دفاتر ثبت نام گواهی الکترونیکی در صورت در خطر افشا قرار گرفتن کلید خصوصی؛
- اطمینان از قراردادن پیغام زیردر تارنمای مرکز صدور گواهی الکترونیکی میانی بازرگانی که توسط طرف های اعتماد کننده مشاهده شود.

"اتکا به گواهی الکترونیکی صادر شده توسط مرکز صدور گواهی الکترونیکی تحت قوانین و مقررات دستورالعمل اجرایی گواهی الکترونیکی میانی بازرگانی (Http://www.mocca.ir)و قرارداد طرف های اعتماد کننده انجام می‌شود. اتکا به گواهی الکترونیکی صادر شده توسط مرکز صدور گواهی الکترونیکی میانی بازرگانی به معنای پذیرش شرایط دستورالعمل و قرارداد مذکور میباشد."

۲-۱-۵) 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 صدور گواهی الکترونیکی و یا در هنگام درخواست اطلاعات منتشر شده در مخزن این مرکز؛

- دریافت گواهی مرکز صدور گواهی الکترونیکی ، از طریق کانال توزیع مطمئن (مطابق با بخش ۶-۱-۳) این دستورالعمل) ؛
- تشخیص قابلیت بکارگیری گواهی‌های صادر شده توسط مرکز صدور گواهی الکترونیکی از طریق بررسی کاربرد کلید این گواهی‌ها که توسط مرکز صدور گواهی الکترونیکی تایید شده است؛
- تشخیص اعتبار گواهی‌های صادر شده توسط مرکز صدور گواهی الکترونیکی 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 صدور گواهی الکترونیکی ؛
- 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؛
- آگاهی کامل از این مسئله که غیرقابل دسترس بودن خدمات صدور گواهی و یا مخزن مرکز صدور گواهی نمی‌تواند باعث نقض تعهدات طرف‌های اعتماد کننده شود؛
- آگاهی کامل از این که استفاده از گواهی‌های صادر شده توسط مرکز صدور گواهی الکترونیکی بدین معناست که طرف‌های اعتماد کننده به کلیه تعهدات و مسئولیت های خود، مذکور در این دستورالعمل و قرارداد طرف های اعتماد کننده ، عمل می‌کنند.

۲-۱-۶) وظایف مخزن

مخزن مرکز صدور گواهی الکترونیکی میانی بازرگانی در موارد زیر مسئولیت دارد:

- انتشار منظم گواهی‌های صادر شده، لیست گواهی‌های باطل شده و سایر اطلاعات مربوطه مطابق بـا بخـش ۲-۶) این دستورالعمل اجرایی؛
- انتشار آخرین اطلاعات سیاست های مرکز صدور 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) التزامات

۲-۲-۱) التزامات مرکز صدور گواهی الکترونیکی میانی و دفاتر ثبت‌نام گواهی الکترونیکی

مرکز صدور گواهی الکترونیکی میانی دارای التزامات زیر می باشد:

- مرکز صدور گواهی الکترونیکی میانی باید خدمات یک مخزن برخط را مطـابق بـا شـرایط مـذکور در ایـن دستورالعمل و سیاست های گواهی الکترونیکی ریشه فراهم کند؛
- مرکز صدور گواهی الکترونیکی میانی باید مدیریت گواهی ها (صدور و ابطال گواهی) را مطابق با روال هـای مذکور در این دستورالعمل و سیاست های مرکز صدور گواهی الکترونیکی ریشه انجام دهد؛

دفاتر ثبت‌نام گواهی الکترونیکی نیز دارای التزامات زیر میباشند:

- دفاتر ثبت‌نام گواهی الکترونیکی باید فرآیند پذیرش درخواست صـدور و ابطـال گواهیهـای الکترونیکـی را مطابق با سیاست های مرکز صدور گواهی الکترونیکی ریشه و این دستورالعمل انجام دهند؛
- این دفاتر باید روال‌های لازم جهت احراز هویت درخواست صدور و ابطـال گـواهی‌هـا و اطـلاع‌رسـانی بـه درخواست کنندگان را مطابق با این دستورالعمل انجام دهند.

درخواست کنندگان، صاحبان امضا و طرف های اعتماد کننده از این مسئله آگاهی دارند کـه کاربردهـای مربـوط بـه گواهی‌های صادر شده توسط مرکز صدور گواهی الکترونیکی میانی وابسته به انتقال اطلاعات در زیرساخت اطلاعاتی ماننـد اینترنت، تلفن، شبکه‌های رایانه‌ای، سرورها، فایروالها، پروکسی ها، روترها، سویچ ها میباشد و ایـن تجهیـزات تحـت کنتـرل مرکز صدور گواهی الکترونیکی میانی و دفاتر ثبت نام گواهی الکترونیکی نمی باشند. مرکز صدور گواهی الکترونیکی میانی و دفاتر ثبت نام گواهی الکترونیکی مسئول هرگونه اشکال، تاخیر، خرابی در گواهی الکترونیکی یا لیست گواهی‌های باطل شـده در شرایطی که یکی از این تجهیزات ارتباطی باعث بروز مشکل شده باشند، نمی‌باشند.

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

صاحبان امضا و طرف‌های اعتماد کننده نباید برای استفاده از گواهی‌ها یا تصمیم مرکز صدور گواهی الکترونیکی بـرای ابطال گواهی‌ها هیچ‌گونه ادعایی علیه این مرکز داشته باشند. تحت هیچ شرایطی مرکز صـدور گـواهی الکترونیکـی مـسئول هرگونه خسارت مستقیم، غیرمستقیم، تصادفی، استنتاجی، خاص یا کیفری در مورد گواهی‌هایی که توسط این مرکـز تحـت سیاست های مرکز صدور گواهی الکترونیکی ریشه و این دستورالعمل صادر شده‌اند، نمی‌باشد.

به غیر از ضمانت های بخش ۲-۲-۱) مرکز صدور گواهی الکترونیکی از پیامدهای عدم صحت اطلاعات کسب شده از یک صاحب امضا در شرایطی که طبق روال‌های این آیین نامه (مطابق با سیاست هـای مرکـز صـدور گـواهی الکترونیکـی ریشه) عمل کرده باشد، رفع مسئولیت می‌کند.

به علاوه، مرکز صدور گواهی الکترونیکی از هر گونه کوتاهی در انجام تعهدات و عدم توجه منطقی طرف‌هـای اعتمـاد کننده و صاحبان امضا رفع مسئولیت می‌کند.

مسئولیت و نحوه پرداخت خسارت بابت ضرر و زیان ناشی از ابطال مرکز صدور گواهی میانی بازرگـانی بـه صـاحبان امضای الکترونیکی صادر شده از این مرکز و یا به دفاتر ثبت نام، در قرارداد منعقد شده بین طرفین مشخص می‌شود.

۲-۲-۱-۲) محدوده خسارات

میزان خسارت ناشی از خطا در عملیات مرکز صدور گواهی الکترونیکی یا دفاتر ثبت نام گواهی الکترونیکی ، حسب مورد بر اساس فصل دوم از مبحث سوم قانون تجارت الکترونیکی تعیین می‌شود. مرکز صدور گواهی الکترونیکی از هرگونه تعهدی نسبت به پرداخت خسارت ناشی از استفاده گواهی که مطابق با سیاست های گواهی الکترونیکی ریشه و این آیین نامه صادر شده نباشد رفع مسئولیت می‌کند.

۲-۲-۱-۳) موارد دیگر

مرکز صدور گواهی الکترونیکی ، هیچ گونه مسئولیتی در قبال خسارت‌های مستقیم و یا غیرمستقیم، اتفاقی، خاص یا کیفری که در اثر شرایط اضطراری نظیر جنگ و زلزله ایجاد شده را متوجه خود نمی‌داند. چنانچه مرکز صدور گواهی الکترونیکی 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 از این طریق به آگاهی صاحبان امضا و طرف های اعتماد کننده می‌رساند و هیچ گونه مسئولیتی در قبال خسارت‌های مستقیم و یا غیرمستقیم، اتفاقی، خاص یا کیفری ناشی از این امر را نمی‌پذیرد.

مرکز صدور گواهی الکترونیکی و دفاتر ثبت‌نام آن در مورد خسارت‌هایی که در شرایط زیر ایجاد شده باشند، هیچ گونه تعهدی ندارند:

- ارائه اطلاعات اشتباه هنگام درخواست گواهی توسط صاحبان امضا،
- استفاده از گواهی های باطل شده یا گواهی های منقضی شده؛
- استفاده از گواهی الکترونیکی صادر شده برای یک خدمت یا کاربرد در سایر زمینه‌ها و موارد غیر مجاز.

۲-۳) تعهدات مالی

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

مرکز صدور گواهی الکترونیکی و دفاتر ثبت‌نام آن فعالیت‌های خود را مطابق با این دستورالعمل و سیاست های گواهی الکترونیکی ریشه انجام می‌دهند و هیچگونه مسئولیت مالی در قبال طرف های اعتماد کننده در شرایط زیر ندارند:

- عدم موفقیت طرف‌های اعتماد کننده در انجام وظایفش ؛
- اتکا طرف‌های اعتماد کننده به گواهی‌هایی که باطل یا منقضی شده اند؛

۲-۳-۲) قیمومیت

صدور گواهی توسط مرکز صدور گواهی الکترونیکی و ثبت نام در دفاتر ثبت‌نام آن مطابق با این دستورالعمل، رابطه کارگزاری، قیمومیت یا نمایندگی بین مرکز صدور گواهی الکترونیکی، کمیسیون گواهی الکترونیکی میانی بازرگانی و دفاتر ثبت نام گواهی الکترونیکی با صاحبان امضا و طرف‌های اعتماد کننده برقرار نمی‌کند.

۲-٤) تفسیر قانون و ضمانت اجرایی

۲-٤-۱) قوانین حاکم

قوانین جمهوری اسلامی ایران شامل قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۲۴ و آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی مصوب ۸۶/۶/۱۱ حاکم بر کلیه فعالیت‌ها و قراردادهای بین مرکز صدور گواهی الکترونیکی میانی بازرگانی با صاحبان امضا و طرف های اعتماد کننده میباشد.

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

آیین نامه اجرایی مرکز صدور گواهی الکترونیکی ، قراردادهای صاحبان امضا و قراردادهای طرف اعتماد کننده شامل شرایط اعتبار، بروزرسانی، انتشار و عدم وابستگی به بخش‌ها می‌باشد. شرط عدم وابستگی به بخش‌ها بیانگر این است که عدم اعتبار یک بخش باعث عدم اعتبار بخش های دیگر نمیشود. شرط اعتبار تصریح می‌کند که مقررات قرارداد حتی پس از خاتمه یا انقضا قرارداد همچنان اجرا می‌شوند. شرط بروزرسانی تصریح می‌کند که کلیه توافق‌های در مورد موضوع قرارداد در قرارداد ثبت می‌شود. شرط انتشار در یک قرارداد شیوه فراهم کردن اطلاعات را توسط طرف‌ها برای یکدیگر بیان می‌کند.

۲-٤-۳) روال‌های حل اختلاف

اختلاف بین مرکز صدور گواهی الکترونیکی و صاحبان امضا باید مطابق با مقررات موجود در قرارداد قابل اجرای بین دو طرف حل شود.

قراردادهای صاحب امضا میانی وزارت بازرگانی و قراردادهای طرف اعتماد کننده باید حاوی شرط حل اختلاف باشد. این شرط تصریح می‌کند که روال‌های حل اختلاف نیاز به دوره مذاکرات ابتدایی برای ۶۰ روز دارند، سپس توسط مراجع قضایی جمهوری اسلامی ایران پیگیری می‌شوند.

۲-۵) تعرفه‌ها

در صورتی که سیاست دریافت هزینه مرکز صدور گواهی الکترونیکی در آینده تغییر کند، این تغییر در این دستورالعمل، برطبق قوانین اجرایی بروزرسانی شده و سازوکار جدید دریافت هزینه و یا روال جدید بازپرداخت منتشر می‌گردد.

۲-۵-۱) تعرفه صدور یا تجدید گواهی

تعرفه صدور یا تجدید گواهی با توجه به نوع کاربرد تعیین خواهد گردید.

توجه: تامین سخت‌افزار نگهداری گواهی بر عهده صاحب امضاء می‌باشد.

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 سیاست‌های گواهی الکترونیکی

به طور رایگان انجام می‌شود.

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

امکان هیچ نوع بازپرداختی وجود ندارد.

۲-٦) مخزن و انتشار

۲-٦-۱) انتشار اطلاعات مرکز صدور گواهی الکترونیکی

مرکز صدور گواهی الکترونیکی میانی بازرگانی اطلاعات زیر را منتشر می‌کند :

- این دستورالعمل؛
- قراردادهای صاحب امضا؛
- قراردادهای طرف اعتماد کننده؛
- گواهی مرکز صدور گواهی الکترونیکی و گواهی های صاحبان امضا؛

- لیست گواهی های باطل شده.

۲-۶-۲) تناوب انتشار

این آیین نامه مطابق با بخش ۸-۲) بروز رسانی شده و منتشر می‌شود.

۲-۶-۳) کنترل دسترسی

اطلاعات منتشر شده در مخزن مرکز صدور گواهی الکترونیکی اطلاعات قابل دسترسی برای عموم می‌باشند. دسترسی به این اطلاعات فقط برای مشاهده برای عموم آزاد است.

۲-۶-٤) مخزن

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

۲-۷) بازرسی

۲-۷-۱) تناوب بازرسی

کمیسیون گواهی الکترونیکی میانی بازرگانی، بازرسی مرکز را بصورت سالیانه انجام می‌دهد و با این عمل، تطابق فعالیت‌های این مرکز را با سیاست های گواهی الکترونیکی ریشه و این دستورالعمل تأیید می‌نماید.

۲-۷-۲) هویت و صلاحیت بازرس

بازرس باید دارای شرایط زیر باشد:

- امنیت اطلاعات و رمزنگاری زیرساخت کلید عمومی دارای مدرک معتبر باشد؛
- در مورد نحوه عملکرد و فعالیت‌های مرکز صدور گواهی الکترونیکی، اطلاعات لازم را داشته باشد؛
- با سیاست نامه گواهی الکترونیکی ریشه و این دستورالعمل اجرایی آن آشنایی کامل داشته باشد؛
- از مرکز صدور گواهی الکترونیکی میانی بازرگانی کاملاً مستقل باشد.

۲-۷-۳) ارتباط بازرسان با مرکز بازرسی شونده

لازم است بازرس و مرکز صدور گواهی الکترونیکی به منظور ارزیابی دقیق، مستقل و بدون غرض کاملاً به صورت سازمانی از یکدیگر جدا باشند اجرای بازرسی مورد نظر از طریق عقد قرارداد میان بازرس و کمیسیون مربوطه صورت می‌پذیرد.

۲-۷-٤) موضوعات مورد بازرسی

موارد زیر تحت بازرسی قرار می‌گیرند:

- اطمینان از این که مرکز صدور گواهی الکترونیکی مطابق با مفاد این دستورالعمل عمل می‌کند؛
- تطبیق این دستورالعمل با سیاست های گواهی الکترونیکی ریشه از طریق بررسی جزئیات کامل کارکرد فنی، روالی و پرسنلی مرکز صدور گواهی الکترونیکی؛
- اطمینان از اعمال درست کنترل‌های مورد نیاز امنیتی.

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

چنانچه هرگونه عدم انطباق بین فعالیت‌های مرکز صدور گواهی الکترونیکی با سیاست های گواهی الکترونیکی ریشه، این دستورالعمل یا قراردادهای گواهی‌های صاحبان امضا یا طرف‌های اعتماد کننده مشاهده شود، فعالیت های زیر انجام میشود:

- بازرس باید عدم انطباق را ثبت نماید؛
- بازرس می‌بایست به طرف های مذکور در بخش ۲-۷-۶) اطلاع رسانی کند؛
- مرکز صدور گواهی الکترونیکی ، راه حل مناسب و زمان مورد نیاز پیش بینی شده را برای رفع نقص به کمیسیون صدور گواهی میانی وزارت بازرگانی پیشنهاد نماید؛
- کمیسیون صدور گواهی میانی وزارت بازرگانی راه حل مناسبی را که می‌تواند شامل جلوگیری از فعالیت مرکز صدور گواهی الکترونیکی یا در صورت لزوم ابطال گواهی این مرکز باشد را، تعیین کند.

پس از تصحیح عدم انطباق،کمیسیون صدور گواهی میانی وزارت بازرگانی می‌تواند مجوز از سرگیری فعالیت مرکز صدور گواهی الکترونیکی را صادر نماید. چنانچه گواهی مرکز بدلیل عدم تطابق کارکرد با سیاست های گواهی الکترونیکی ریشه و این دستورالعمل باطل شده باشد، مرکز صدور گواهی الکترونیکی می‌بایست مطابق با بخش ۴-۸-۲) عمل کند.

۲-۷-۶) گزارش نتایج

بازرس باید گزارش نتیجه بازرسی را به کمیسیون صدور گواهی میانی وزارت بازرگانی ارایه نماید. یک نسخه ازاین نتایج نیز به مرکز صدورگواهی الکترونیکی میانی بازرگانی ارائه می‌شود تا در مواقع رجوع یا درخواست بازرس مرکز دولتی صدور گواهی الکترونیکی ریشه و کمیته نظارتی شورای سیاست‌گذاری گواهی الکترونیکی کشور یا درخواست کتبی مراجع قضایی در اختیار آنها قرار گیرد.

۲-۸) محرمانگی

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

اطلاعات هر درخواست گواهی که توسط مرکز صدور گواهی الکترونیکی نگهداری می‌شود و یا در فهرست 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 صدور گواهی الکترونیکی ، می‌توان به موارد زیر اشاره کرد:

- کلیه کلیدهای خصوصی و کلمات رمز که در داخل مرکز صدور گواهی الکترونیکی به کار گرفته می‌شوند، محرمانه هستند؛
- اطلاعات درخواست گواهی که توسط مرکز صدور گواهی الکترونیکی نگهداری می‌شود، نباید بدون رضایت صاحبان امضا یا درخواست مراجع ذیصلاح قانونی منتشر شوند؛
- کلیه اطلاعات مربوط به پیگیری ثبت وقایع که توسط مرکز صدور گواهی الکترونیکی ایجاد و یا نگهداری می‌شوند، محرمانه هستند؛
- کلیه گزارش‌های ثبت وقایع که هنگام بازرسی داخلی یا خارجی ایجاد شده‌اند محرمانه بوده و نباید در دسترس باشند (مگر در صورت درخواست مراجع ذیصلاح قانونی)،
- کلیه اسناد طبقه‌بندی شده و کتابچه‌های راهنمای مرکز صدور گواهی الکترونیکی محرمانه هستند.

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

- کلیه اطلاعاتی 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 صدور گواهی الکترونیکی ، هیچ گونه اطلاعاتی در مورد گواهی‌های معلق را منتشر نمی‌کند و اساساً این مرکز 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 سازمان ها

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 صدور گواهی الکترونیکی ، این اطلاعات را تنها در صورت ارائه حکم دادگاه در اختیار آن‌ها قرار می‌دهد. در این صورت این مرکز حق خود را برای دریافت هزینه فراهم آوردن اطلاعات، محفوظ می‌داند.

۲-۸-۵) ارائه اطلاعات طبق درخواست مالک

صاحبان امضا می‌توانند درخواست دسترسی به هرگونه اطلاعات شخصی خود را که موجود در پرونده‌های دفاتر ثبت‌نام گواهی مربوطه می‌باشد را داشته باشند. در این صورت، مرکز صدور گواهی الکترونیکی حق خود را برای دریافت هزینه فراهم آوردن این اطلاعات، محفوظ می‌داند.

اطلاعات خصوصی صاحبان امضا 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 صدور گواهی الکترونیکی تنها در صورت ارائه حکم مراجع قضایی افشا می‌شود.

۲-۹) حق مالکیت معنوی

مرکز صدور گواهی الکترونیکی ، کلیه حقوق مالکیت معنوی گواهی‌های الکترونیکی صادره را غیر از اطلاعاتی که توسط درخواست کننده فراهم شده و در گواهی مربوطه قرار دارد، متعلق به خود می داند. حق مالکیت معنوی اطلاعات فراهم شده توسط درخواست کننده گواهی متعلق به خود درخواست کننده میباشد.

کلیه درخواست کنندگان و صاحبان امضا به مرکز صدور گواهی الکترونیکی و دفاتر ثبت نام گواهی الکترونیکی اجازه غیر انحصاری استفاده، کپی، تغییر، انتشار برای عموم، پخش این اطلاعات را مطابق با قراردادهای صاحبان امضا، طرف های اعتماد کننده و این آیین نامه می دهند.

مرکز صدور گواهی الکترونیکی نیز به صاحبان امضا و طرف های اعتماد کننده اجازه غیر انحصاری کپی و پخش گواهی صادر شده توسط این مرکز را برای استفاده مطابق با قراردادهای صاحبان امضا و طرف های اعتماد کننده و این آیین نامه میدهد.

کلیه حقوق مالکیت معنوی این دستورالعمل متعلق به مرکز صدور گواهی الکترونیکی میانی بازرگانی می‌باشد.

۳) احراز هویت

۳-۱) ثبت‌نام اولیه

درخواست کننده گواهی الکترونیکی باید مراحل زیر را اجرا کند:

- سخت‌افزار نگهداری گواهی را مطابق با مشخصات فنی اعلام شده از جانب مرکز صدور گواهی میانی بازرگانی تهیه و زوج کلید ایمن و سالم بر روی آن تولید کند ؛
- مدارک مورد نیاز اعلام شده توسط دفاتر ثبت نام گواهی الکترونیکی را تهیه نماید؛

پس از اجرای مراحل فوق، درخواست کننده باید به یکی از دفاتر ثبت نام گواهی الکترونیکی مراجعت نموده و درخواست گواهی و مدارک مذکور را به مسئول مربوطه تحویل دهد. در دفاتر ثبت نام گواهی الکترونیکی درخواست کننده باید فرم درخواست گواهی الکترونیکی را کاملاً با اطلاعات حقیقی و صحیح تکمیل نموده و تایید نماید. پس از انجام مراحل فوق دفاتر ثبت نام گواهی الکترونیکی فرآیند احراز هویت درخواست کننده را آغاز می کند. در صورتیکه مرحله احراز هویت با موفقیت انجام شود، دفاتر ثبت‌نام گواهی الکترونیکی، صدور گواهی مورد نظر را از مرکز صدور گواهی الکترونیکی درخواست میکنند. پس از صدور گواهی، دفاتر ثبت نام گواهی الکترونیکی باید صدور گواهی را از طریق تلفن یا آدرس پست الکترونیکی به آگاهی درخواست کننده برسانند و آدرس سایتی را که درخواست کننده میتواند گواهی را از آن دریافت کند در اختیار وی قرار دهند.

در صورت عدم موفقیت مرحله احراز هویت، دفاتر ثبت نام گواهی الکترونیکی باید از طریق تلفن و یا آدرس پست الکترونیکی درخواست کننده را از این امر آگاه نمایند.

۳-۱-۱) انواع نام‌ها

نام‌های گواهی‌های الکترونیکی صادر شده توسط مرکز صدور گواهی الکترونیکی با نام‌های ترکیبی استاندارد X500 مطابقت دارد. در مورد گواهی خود مرکز صدور گواهی الکترونیکی نیز از همان نوع نام‌های ترکیبی استفاده می‌شود.

گواهی های صادر شده توسط مرکز صدور گواهی الکترونیکی باید شامل اطلاعات زیر باشند:

- "نام کشور" (C) که یک کد دو حرفی مطابق با ISO 3166 میباشد،
- "نام سازمان" (O) که درشرایطی که درخواست کننده یک فرد حقوقی باشد، نام سازمان درخواست کننده میباشد. در شرایطی که درخواست کننده یک فرد حقیقی باشد، نام سازمان میتواند نام درخواست کننده باشد؛
- "نام زیر سازمان" (OU) که یک فیلد اختیاری است. این فیلد میتواند برای تشخیص بین بخش های مختلف یک سازمان استفاده شود؛
- "نام مشترک" (CN) که نام و نام‌خانوادگی درخواست کننده گواهی بوده و مطابق با شناسنامه درخواست کننده گواهی می‌باشد.

۳-۱-۲) نیاز به نام‌های با معنی

زمانیکه از نام‌های ترکیبی استفاده می‌کنیم، نام مشترک باید صاحب امضاء را به گونه‌ای که به راحتی توسط شخص قابل فهم باشد معرفی کند. برای اشخاص معمولاً از نام مندرج در شناسنامه استفاده می‌شود. برای مؤلفه‌های سخت‌افزاری و نرم‌افزاری، می‌توان از نام مدل و شماره سریال و برای آدرس‌های اینترنتی از نام دامنه، استفاده کرد.

۳-۱-۳) قواعد تفسیر قالب مختلف نام‌ها

عنوان گواهی های الکترونیکی صادر شده توسط مرکز صدور گواهی الکترونیکی مطابق با بخش ۳-۱-۱) و ۳-۱-۲) تفسیر می شود.

۳-۱-٤) یکتایی نام‌ها

عنوان کلیه گواهی ها باید واضحاً مالک گواهی را معرفی کند. هر گواهی الکترونیکی باید دارای یک شماره سریال یکتا نیز باشد.

۳-۱-۵) روال حل اختلاف در مورد نام‌ها

عنوان گواهی‌های صادر شده توسط مرکز صدور گواهی الکترونیکی تنها براساس ترتیب مراجعه درخواست کنندگان به آنها تخصیص می یابد. قبول یک عنوان گواهی خاص توسط مرکز صدور گواهی الکترونیکی یا دفاتر ثبت نام گواهی الکترونیکی به معنای تخطی از قوانین کپی رایت و حق مالکیت معنوی نمیباشد.

مرکز صدور گواهی الکترونیکی مسئول حل اختلاف در مورد نام ها بین صاحبان امضا و درخواست کنندگان نمیباشد.

مرکز صدور گواهی الکترونیکی می‌بایست در صورت مواجهه با هر گونه اختلاف در مورد نام، آنرا بررسی و تصحیح نماید. در صورت نیاز، مرکز صدور گواهی الکترونیکی میانی بازرگانی می‌بایست موضوع را با کمیته نظارتی شورای سیاست گذاری گواهی الکترونیکی کشور هماهنگ نماید.

۳-۱-٦) احراز هویت و نقش علائم تجاری

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

۳-۱-۸) احراز هویت سازمان‌ها

نماینده موجودیت های سازمانی درخواست کننده باید همراه با درخواست گواهی و مدارک مورد نیاز وابـسته بـه هـر کاربرد به دفاتر ثبت نام گواهی الکترونیکی مراجعه نمایند(نماینده سازمان باید مطابق با اساسنامه سازمان مجاز بـه امـضا اسناد تعهدآور باشد)

مدارک مورد نیاز حداقل بایستی شامل مدارک زیر باشد:

- آگهی تاسیس شرکت؛
- اساسنامه شرکت؛
- کپی آگهی آخرین تغییرات روزنامه رسمی؛
- یک برگ درخواست گواهی الکترونیکی بر روی سر برگ شرکت با امضاء مـدیر عامـل و ممهـور بـه مهـر شرکت؛

در مورد سازمان های دولتی ارسال دو مورد آخر کافی میباشد.

دفاتر ثبت نام گواهی الکترونیکی برای احراز هویت نمایندگان شرکت ها مدارک زیر را بررسی می کند:

- شناسنامه و یا گذرنامه (بصورت خوانا)؛
- کارت ملی ؛

۳-۱-۹) تأیید هویت افراد حقیقی

در صورتیکه درخواست کننده یک فرد حقیقی باشد، باید شخصاً با در دست داشتن درخواست گواهی و مدارک زیر به دفاتر ثبت نام گواهی الکترونیکی مراجعه نماید:

- شناسنامه و یا گذرنامه (بصورت خوانا)؛
- کارت پایان خدمت و یا معافی (برای افراد ذکور)
- کارت ملی؛

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.

صاحبان امضایی که درخواست گواهی جدید می کنند، باید مراحل ثبت‌نام اولیه مذکور در ۳-۱) را کاملاً دوباره اجرا کنند.

دفاتر ثبت نام گواهی الکترونیکی باید صاحب امضا را از انقضا گواهی خود آگاه کند. صاحب امضا نیاز باید پس از انقضا گواهی، از آن استفاده نکند و گواهی منقضی شده را از کلیه دستگاه‌ها و نرم افزارهایی که از آن استفاده میکنند، حذف کند.

۳-۲-۲) تجدید گواهی

مرکز صدور گواهی الکترونیکی تجدید گواهی صاحبان امضا را ممنوع اعلام می‌دارد.

۳-۲-۳) بروزرسانی گواهی

مرکز صدور گواهی الکترونیکی بروزرسانی گواهی صاحبان امضا را ممنوع اعلام می‌دارد.

۳-۳) دریافت یک گواهی جدید پس از ابطال

بعد از ابطال گواهی صاحبان امضا، فعالیت های مربوط به شناسایی و احراز هویت درخواست گواهی جدید مطابق قوانینی که در بخش ۳-۱) ذکر شد، انجام می‌شود.

۳-٤) درخواست ابطال

صاحب امضا می تواند درخواست ابطال گواهی الکترونیکی خود را به دفاتر ثبت نام گواهی الکترونیکی ارایه بنماید. دفاتر ثبت نام گواهی الکترونیکی ابتدا روال های احراز هویت مذکور در بخش ۳-۱-۹) و ۳-۱-۸) را اجرا می نماید. در صورت اطمینان از اینکه درخواست کننده مالک گواهی الکترونیکی می باشد، دفاتر ثبت نام گواهی الکترونیکی درخواست ابطال گواهی مربوطه را به مرکز صدور گواهی الکترونیکی می فرستند. مرکز صدور گواهی الکترونیکی نیز پس از دریافت این درخواست با قرار دادن شماره سریال گواهی در لیست گواهی های باطل شده و انتشار این لیست، گواهی مربوطه را باطل می کند. پس از ابطال گواهی در خواست شده، دفاتر ثبت نام گواهی الکترونیکی باید مالک گواهی را از ابطال گواهی اش آگاه کنند.

٤) خواسته‌های عملیاتی

٤-۱) درخواست گواهی

به منظور درخواست گواهی الکترونیکی ، باید اقدامات مذکور در بخش ۳-۱) انجام شود.

فرم درخواست گواهی که درخواست کننده آنرا تکمیل و تایید می‌نماید، حاوی قرارداد صاحبان امضا می باشد. همچنین در این فرم درخواست کننده تبعیت خود را از این آیین نامه اعلام میکند.

دفاتر ثبت نام گواهی الکترونیکی احراز هویت درخواست کننده را مطابق با روالهای مذکور در بخش ۳-۱-۸) و ۳-۱-۹) انجام میدهد.

دفتر ثبت نام 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 یا درخواست گواهی را به طور کلی رد می‌کند.

٤-۲) صدور گواهی

دفاتر ثبت نام گواهی الکترونیکی ، پس از احراز هویت درخواست گواهی، این درخواست را برای مرکز صدور گواهی الکترونیکی ارسال می‌نماید. این مرکز نیز پس از دریافت درخواست گواهی، یک گواهی الکترونیکی مطابق با بخش ۷) تولید کرده و امضا می نماید.

٤-۳) پذیرش گواهی

پس از صدور گواهی و انتشار آن در مخزن، دفتر ثبت نام گواهی الکترونیکی مربوطه باید از طریق تلفن یا آدرس پست الکترونیکی به صاحب امضا اطلاع رسانی کند. همچنین باید آدرس دسترسی به گواهی مورد نظر را در اختیار وی قرار دهد.

٤-٤) ابطال و تعلیق گواهی

٤-٤-١) شرایط ابطال

مرکز صدور گواهی الکترونیکی ، در صورت وقوع هریک از شرایط زیر، گواهی صاحبان امضا را باطل میکند:

- در خطر افشا قرار گرفتن کلید خصوصی مرکز صدور گواهی ریشه یا کلید خصوصی مرکز صدور گواهی الکترونیکی میانی؛
- نقض قوانین این آیین نامه یا قرارداد صاحبان امضا توسط صاحب امضا؛
- هر گونه تغییر در اطلاعات گواهی صاحب امضا؛
- تشخیص اینکه گواهی بر اساس قونین این آیین نامه یا قرارداد صاحبان امضا صادر نشده است؛
- هر دلیلی که تمامیت، امنیت و اعتماد به گواهی صاحبان امضا یا گواهی مرکز صدور گواهی الکترونیکی را زیر سئوال ببرد؛
- درخواست ابطال گواهی توسط یک سازمان ناظر بر صاحب امضاء یا مراجع قضایی؛
- مرکز صدور گواهی الکترونیکی ریشه یا مرکز صدور گواهی الکترونیکی میانی به فعالیت خود پایان دهد.

صاحب امضاء در صورت وقوع هر یک از موارد زیر، می‌بایست ابطال گواهی(های) خود را درخواست کند:

- در خطر افشا قرار گرفتن کلید خصوصی صاحب امضاء ؛
- تغییر اطلاعات موجود در گواهی؛

در صورت ابطال گواهی صاحب امضا، دفاتر ثبت نام گواهی الکترونیکی باید از طریق آدرس پست الکترونیکی یا تلفن صاحب امضا را از این امر آگاه کند.

٤-٤-٢) کسانی که می توانند درخواست ابطال نمایند

- مراجع قانونی ذیصلاح میتوانند درخواست ابطال گواهی صاحبان امضا را بکنند؛
- صاحبان امضا می‌توانند شخصاً درخواست ابطال گواهی خود را بکنند.

٤-٤-٣) روال ابطال گواهی

صاحب امضا باید شخصاً برای ابطال گواهی خود به یکی از دفاتر ثبت نام گواهی الکترونیکی مراجعه نماید. دفاتر ثبت نام گواهی الکترونیکی ، احراز هویت عامل درخواست‌کننده ابطال گواهی را مطابق با بخش ۴-۱-۸ و ۳-۱-۹) انجام میدهد. سپس از مرکز صدور گواهی الکترونیکی درخواست ابطال گواهی را میکند. مرکز صدور گواهی الکترونیکی باید در عرض ۲۴ ساعت پس از دریافت درخواست ابطال با قراردادن شماره سریال گواهی در لیست گواهی های باطل شده، گواهی مورد نظر را باطل کند. در صورت ابطال گواهی صاحب امضا، دفاتر ثبت نام گواهی الکترونیکی باید از طریق آدرس پست الکترونیکی یا تلفن صاحب امضا را از این امر آگاه کند.

٤-٤-٤) مهلت ابطال

این دستورالعمل هیچ مهلتی برای ابطال قائل نشده و مرکز صدور گواهی الکترونیکی ، گواهی‌ها را به سرعت پس از دریافت درخواست صحیح ابطال، باطل می‌کنند.

همچنین صاحبان امضا باید به محض تشخیص در خطر افشا قرار گرفتن کلید خصوصی خود، از دفاتر ثبت نام گواهی الکترونیکی در خواست ابطال گواهی را بنمایند.

٤-٤-٥) شرایط تعلیق

سرویس تعلیق گواهی توسط مرکز صدور گواهی الکترونیکی ، 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 صدور گواهی الکترونیکی هر ۲۴ ساعت یکبار لیست گواهی‌های باطل شده را از طریق سایت خود منتشر خواهد کرد. در شرایط خاص، مرکز صدور گواهی الکترونیکی لیست گواهی های باطل شده را بیش از یکبار در هر ۲۴ ساعت منتشر خواهد کرد.

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

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

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

مرکز صدور گواهی الکترونیکی سرویس اعلام برخط وضعیت گواهی ارائه نمی کند.

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 صاحبان امضا در خطر افشا قرار گرفتن کلید خصوصی خود را تشخیص دهند، باید سریعاً از دفاتر ثبت نام گواهی الکترونیکی درخواست ابطال گواهی خود را بکنند. صاحب امضا نباید دیگر از این گواهی استفاده کند و باید آن را از تمام دستگاه‌ها و نرم افزارهایی که گواهی بر روی آنها نصب شده، حذف کند.

صاحب امضا مسئول بررسی دلیل در خطر افشا قرار گرفتن کلید خود می باشد و باید این مسئله را به اطلاع طرف های اعتماد کننده برساند.

٤-٥) روال بازرسی امنیتی

ثبت وقایع می‌بایست برای کلیه فعالیت‌هایی که مربوط به امنیت مرکز صدور گواهی الکترونیکی هستند، انجام شود. فایل‌های ثبت وقایع می‌بایست به صورت خودکار توسط سیستم تولید شوند یا به صورت دستی در فرم کاغذی و یا سایر مکانیزم‌های فیزیکی ساخته شود. کلیه فایل‌های ثبت وقایع اعم از الکترونیکی و غیر الکترونیکی در هنگام بررسی وقایع باید در دسترس باشند. فایل های ثبت واقعه به صورت ادواری بایگانی شده و از آنها نسخه پشتیبان تهیه میشود.

٤-٥-١) انواع وقایع قابل ثبت

ثبت وقایع امنیتی:

- هر تغییری در پارامترهای ثبت وقایع مانند تغییر دوره تناوب یا نوع رخدادهای ثبت شده و
- هر تلاشی برای تغییر و یا از بین بردن وقایع ثبت‌شده.

احراز هویت :

- تلاش های موفق و ناموفق برای دستیابی به یک نقش؛
- تغییر حداکثر دفعات ورود مشخصات برای احراز هویت؛
- حداکثر دفعات اقدام ناموفق برای ورود به سیستم؛
- چنانچه راهبر سیستم، حساب کاربری را که به دلیل تلاش ناموفق ورود به سیستم قفل شده است، از حالت قفل بیرون بیاورد.
- چنانچه راهبر سیستم نوع تشخیص هویت را تغییر دهد برای مثال به جای کلمه عبور از روش‌های بیومتریک استفاده کند.

انتشار اطلاعات:

- هر گونه درخواست دسترسی به اطلاعات امنیتی یا محرمانه؛

تولید کلید:

- هر زمان که مرکز صدور گواهی الکترونیکی کلیدی را تولید کند.

بارگذاری و ذخیره کلید خصوصی:

- هر زمانی که بارگذاری و ذخیره کلیدهای خصوصی انجام شود؛
- دسترسی به کلید خصوصی گواهی مرکز صدور گواهی الکترونیکی به منظور بازیابی کلید.

ورود، حذف، ذخیره کلیدهای عمومی مورد اطمینان:

- کلیه تغییرات بر روی کلیدهای عمومی مورد اطمینان که شامل اضافه و حذف آنها می‌شود.

استخراج کلیدخصوصی:

- استخراج کلید خصوصی (کلیدهایی که تنها برای یک نشست یا یک پیغام استفاده می‌شوند، مستثنی هستند).

ثبت‌نام گواهی:

- تمام درخواست‌های گواهی.

ابطال گواهی:

- تمام درخواست‌های ابطال گواهی.

تأیید تغییر وضعیت یک گواهی:

- تأیید یا رد تغییر وضعیت یک گواهی.

پیکربندی مرکز صدور گواهی الکترونیکی:

- هر تغییر مرتبط با امنیت در پیکربندی مرکز صدور گواهی الکترونیکی.

مدیریت شناسه های کاربران:

- نقش‌ها و کاربرانی اضافه یا حذف شوند و
- حقوق دسترسی یک نقش یا یک شناسه کاربری تغییر کند.

مدیریت پروفایل گواهی:

- هر تغییری در پروفایل یک گواهی.

مدیریت پروفایل لیست گواهی‌های باطل شده:

- هر تغییری در پروفایل لیست گواهی‌های باطل شده.

موارد دیگر:

- نصب سیستم عامل؛
- نصب برنامه های کاربردی زیر ساخت کلید عمومی؛
- نصب HSM ؛
- حذف HSM ؛
- تخریب HSM ؛
- راه اندازی سیستم؛
- کلیه تلاش‌های ورود به برنامه‌های کاربردی زیر ساخت کلید عمومی؛
- دریافت سخت افزار و نرم افزار؛
- تلاش برای تعیین اسم رمز؛
- تلاش برای تغییر اسم رمز؛
- تهیه نسخه پشتیبان از پایگاه داده داخلی مرکز صدور گواهی الکترونیکی ؛
- بازیابی پایگاه داده داخلی مرکز صدور گواهی الکترونیکی ؛
- دستکاری فایل‌ها (مانند ایجاد، تغییر نام، انتقال)؛
- ارسال هر مطلبی به مخزن؛
- دسترسی به پایگاه داده داخلی مرکز صدور گواهی؛
- کلیه درخواست‌ها در مورد در خطر افشا قرار گرفتن کلید؛
- قراردادن یک گواهی در سخت‌افزار نگهداری گواهی (توکن)

- انتقال سخت‌افزار نگهداری گواهی ؛ (توکن)
- صفر کردن سخت‌افزار نگهداری گواهی (توکن)
- تخصیص مجدد کلید مرکز صدور گواهی الکترونیکی.

تغییرات در پیکربندی سرویس دهنده مرکز صدور گواهی الکترونیکی:

- سخت افزار؛
- نرم افزار؛
- سیستم عامل؛
- فایل‌های ترمیمی (patch)
- اطلاعات امنیتی.

دسترسی فیزیکی/ امنیت سایت:

- دسترسی متصدیان به مکانی که مرکز صدور گواهی الکترونیکی در آنجا قرار دارد؛
- دسترسی به سرویس دهنده مرکز صدور گواهی و
- موارد مشکوک یا شناخته شده نقض امنیت فیزیکی.

ناهنجاری‌ها:

- شرایط خطای نرم‌افزاری (با توضیح حادثه)؛
- حملات شبکه‌ای (مشکوک یا قطعی) (با توضیح حادثه، نام مسئول گزارش دهنده حادثه و راه حل اجرا شده)؛
- خرابی تجهیزات (با توضیح حادثه، نام مسئول گزارش دهنده حادثه و راه حل اجرا شده)؛

- قطع جریان برق (با توضیح حادثه، نام مسئول گزارش دهنده حادثه و راه حل اجرا شده)؛
- خرابی در سامانه برق اضطراری (با توضیح حادثه، نام مسئول گزارش دهنده حادثه و راه حل اجرا شده)؛
- خرابی واضح و جدی در سرویس‌های شبکه و یا دسترسی به شبکه (با توضیح حادثه، نام مسئول گزارش دهنده حادثه و راه حل اجرا شده)؛
- نقص قوانین سیاست های گواهی الکترونیکی ریشه یا این دستورالعمل (با توضیح حادثه، نام مسئول گزارش دهنده حادثه و راه حل اجرا شده)؛
- تنظیم مجدد ساعت سیستم عامل.

٤-٥-٢) تناوب پردازش اطلاعات وقایع ثبت‌شده

مرکز صدور گواهی الکترونیکی می‌بایست به طور ماهیانه وقایع ثبت شده را بازرسی نماید. این فعالیت شامل اعمالی از قبیل بررسی فایل‌های ثبت وقایع جهت اطمینان از عدم بروز اشکال در آنها و جستجوی هرگونه اخطار یا ناهماهنگی می‌باشد. کلیه فعالیت‌هایی که براساس این نتایج انجام می‌شود، می‌بایست مستندسازی شده و برای کمیسیون صدور گواهی میانی بازرگانی ارسال شود.

همچنین در صورت بروز هرگونه رخداد یا اختلال در سیستم‌های مرکز صدور گواهی الکترونیکی ، کمیسیون وقایع ثبت‌شده مرکز را به منظور شناسایی فعالیت‌های غیرمجاز بررسی می‌کند.

٤-٥-٣) دوره نگهداری از اطلاعات وقایع ثبت شده

مرکز صدور گواهی الکترونیکی ، گزارش های ماهیانه از بازرسی اطلاعات ثبت شده را به مدت حداقل هفت سال نگه می‌دارد. اطلاعات وقایع ثبت شده نیز تا پس از انجام دو دوره بازرسی امنیتی توسط کمیسیون گواهی الکترونیکی میانی بازرگانی نگهداشته می شود.

٤-٥-٤) حفاظت از اطلاعات بازرسی امنیتی

- کلیه اطلاعات وقایع ثبت شده فعلی و بایگانی شده باید توسط امضای الکترونیکی و فن‌آوری رمزگذاری محافظت شوند و در لوح فشرده یا یک سخت‌افزار 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

می‌بایست از کلیه وقایع ثبت شده الکترونیکی و خلاصه وقایع ثبت‌شده به صورت ماهیانه نسخه پشتیبان تهیه شود. یک نسخه از فایل‌های ثبت وقایع می‌بایست بر اساس این دستورالعمل به خارج از سایت ارسال شود.

٤-٥-٦) سیستم جمع آوری اطلاعات بازرسی امنیتی

فرآیندهای ثبت وقایع می‌بایست با راه اندازی مرکز صدور گواهی الکترونیکی فعال شود و تنها در زمان متوقف شدن عملیات این مرکز متوقف شود. چنانچه مشخص شود که در سیستم ثبت وقایع اشکالی وجود دارد و یکپارچگی سیستم و محرمانگی اطلاعات درخطر است، آنگاه مرکز صدور گواهی الکترونیکی 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

پس از ثبت یک واقعه اطلاع به موجب واقعه توسط سیستم ثبت وقایع الزامی نمی‌باشد.

٤-٥-٨) ارزیابی آسیب‌پذیری

به بخش ۴-۵-۲) مراجعه شود.

٤-٦) بایگانی اطلاعات

٤-٦-١) اطلاعاتی که میبایست بایگانی شوند

مرکز صدور گواهی الکترونیکی تمام مدارک مرتبط با صدور گواهیها را (در قالب الکترونیکی یا کاغذی) بایگانی می کند. دفاتر ثبت نام گواهی الکترونیکی نیز کلیه مدارک احراز هویت درخواست کنندگان را بایگانی می کند. اطلاعات زیر توسط مرکز صدور گواهی الکترونیکی در ارتباط با صدور گواهی بایگانی میشود:

- فایل درخواست امضای گواهی (CSR)؛
- کلیه مدارک مرتبط با احراز هویت سازمان ها مذکور در بخش ۳-۱-۸)؛
- مدارک مرتبط با احراز هویت موجودیت های حقیقی مذکور در بخش ۳-۱-۹)؛
- قبول قرارداد صاحبان امضا و آیین نامه اجرایی گواهی الکترونیکی ؛
- کپی گواهی الکترونیکی صادر شده.

مرکز صدور گواهی الکترونیکی اطلاعات مربوط با درخواست ابطال گواهی ها را نیز بایگانی می کند. این اطلاعات شامل کلیه مدارک مرتبط با احراز هویت درخواست کننده ابطال مذکور در بخش ۳-۱-۸) و ۳-۱-۹) و دلیل درخواست ابطال می باشد. این اطلاعات و لیست گواهی های باطل شده مربوطه بایگانی می شوند.

مرکز صدور گواهی الکترونیکی ، علاوه بر اطلاعات مربوط به صدور و ابطال گواهی، اطلاعات زیر را نیز بایگانی می کند:

- نسخه های سیاست نامه گواهی الکترونیکی ریشه و این دستورالعمل ؛

- قرارداد های صاحبان امضا و طرف های اعتماد کننده؛
- اطلاعات مربوطه به راه اندازی تجهیزات سیستم مرکز صدور گواهی و استفاده از کلید خصوصی مرکز؛
- اطلاعات بازرسی امنیتی مطابق با بخش ۴-۵)؛
- کلیه داده‌ها و برنامه‌های کاربردی دیگر به منظور بررسی محتوای بایگانی ها.

٤-٦-٢) دوره نگهداری اطلاعات بایگانی شده

مرکز صدور گواهی الکترونیکی اطلاعات بایگانی را به مدت حداقل ۷ سال در مرکز نگه می دارد.

٤-٦-٣) محافظت از بایگانی

مرکز صدور گواهی الکترونیکی اطلاعات بایگانی را در یک محل ذخیره‌سازی مطمئن و ایمن نگهداری می کند، به گونه ای که از تغییر، تخریب و دسترسی غیر مجاز به این اطلاعات جلوگیری شود.

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

مرکز صدور گواهی الکترونیکی از بایگانی اطلاعات گواهی‌های صادر شده الکترونیکی به صورت ماهیانه نسخه پشتیبان تهیه می‌کند (بایگانی هر ماه به صورت کامل انجام میگیرد).

کلیه نسخه‌های پشتیبان تهیه شده از بایگانی باید در مرکز پشتیبان میانی بازرگانی نگهداری شود مرکز میانی مکلف است رسماً محل و مشخصات مرکز پشتیبان را به مرکز دولتی ریشه اعلام کند.

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 نمود. مهرهای زمانی که بر

روی این اطلاعات قرار دارند مهرهای زمانی الکترونیکی نیستند که از یک مؤلف ثالث دریافت می‌شوند بلکه آنها از ساعت سیستم عامل رایانه استخراج می‌شوند. ساعت کلیه رایانه‌های مرکز صدور گواهی الکترونیکی به منظور حفظ دقت و قابلیت اعتماد مرتباً به صورت دوره‌ای تنظیم می شود. 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 مگر با اجازه و تائید بازرسان غیرقابل تغییراست.

٤-٦-٦) سیستم جمع آوری بایگانی

مرکز صدور گواهی الکترونیکی چنین سیستمی ندارد.

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

کسب اطلاعات مربوط به بایگانی از طریق درخواست کتبی که به تأیید کمیسیون صدور گواهی الکترونیکی میانی بازرگانی رسیده باشد، انجام می‌شود. بازرسان مسئولیت بررسی اطلاعات مربوط به بایگانی را دارند. در صورتی که اطلاعات در فرم کاغذی باشند، اصالت تاریخ و امضای آن ها باید بررسی شود. همین طور درستی امضای الکترونیکی اطلاعات بایگانی شده نیز باید بررسی گردد.

٤-٧) گردش کلید

به منظور جلوگیری از در خطر افشا قرار گرفتن کلید خصوصی صاحبان امضا، گواهی آنها دارای مدت اعتبار محدودی می‌باشد. پس از انقضا گواهی، یک زوج کلید جدید باید تولید شده و همراه با درخواست گواهی صاحب امضا به دفاتر ثبت نام گواهی الکترونیکی ارائه شود. روال تجدید کلید گواهی صاحبان امضا در بخش ۳-۲) آمده است.

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 صدور گواهی الکترونیکی 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 هرساله انجام می‌شود.

سایت پشتیبان مرکز صدور گواهی الکترونیکی در شرایطی که مرکز صدور گواهی الکترونیکی مجبور به توقف عملیات مدیریت گواهی شود، قابل دسترس خواهد بود.

٤-٨-٢) ابطال گواهی مرکز صدور گواهی الکترونیکی

در صورت نیاز به ابطال کلید عمومی مرکز صدور گواهی الکترونیکی ، این مرکز باید مطابق با دستورالعمل اجرایی گواهی الکترونیکی خود عمل نماید و به مراجع زیر خبر ابطال کلید عمومی را اطلاع بدهد:

- کمیسیون گواهی الکترونیکی میانی بازرگانی
- مرکز دولتی صدور گواهی الکترونیکی ریشه ؛
- دفاتر ثبت‌نام مربوطه؛
- صاحبان امضا؛
- مراکز صدور گواهی خارجی و داخلی که به مرکز صدور گواهی الکترونیکی (از طریق توافق دوجانبه[1]) اعتماد کرده‌اند.

---

[1] *Cross Certificate*

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

٤-۸-۳) در خطر افشا قرار گرفتن کلید مرکز صدور گواهی الکترونیکی

در صورت در خطر افشا قرار گرفتن کلید مرکز صدور گواهی الکترونیکی ، این مرکز باید از مرکز صدور گواهی ریشه درخواست ابطال گواهی خود را بکند و مطابق با بخش ۴-۸-۲) به مراجع دیگر اطلاع رسانی کند.

٤-۸-٤) بازیابی خرابی پس از وقوع حوادث طبیعی یا حوادث دیگر

مرکز صدور گواهی الکترونیکی تمرین بازیابی خرابی برای ایمن‌سازی تجهیزات را به صورت سالانه انجام می دهد.

٤-۹) توقف سرویس دهی مرکز صدور گواهی *الکترونیکی*

در صورت توقف سرویس‌دهی مرکز صدور گواهی الکترونیکی ، کلیه گواهی های صادر شده توسط این مرکز باطل می‌شوند.

برای به حداقل رساندن تاثیرات خاتمه فعالیت، مرکز صدور گواهی الکترونیکی باید:

- صاحبان امضا را از این امر آگاه کند و این مطلب را حداقل یک ماه قبل از خاتمه فعالیت مرکز، در مخزن اعلام کند.
- کلیه گواهی‌های باطل شده و اطلاعات ثبت شده را مطابق با خواسته کمیسیون گواهی الکترونیکی میانی بازرگانی با حفظ امانت تسلیم کند.

۵) کنترل‌های امنیت فیزیکی، رویه‌ای، فردی

۵-۱) کنترل‌های فیزیکی

۵-۱-۱) ساختمان و مکان سایت

ساختمان مرکز صدور گواهی الکترونیکی واقع در بلوار کشاورز، خیابان نادری، جنب کوچه حجت دوست، پلاک ۱۱ و تجهیزات مورد استفاده در آن با استانداردهای موجود برای مراکز حساس مطابقت دارد. این در حالی است که سایر امکانات امنیتی فیزیکی مانند نگهبان، سیستم‌های نظارت با تلویزیون و حسگرهای مداربسته رطوبت، تشخیص حرکت و تشخیص دود به منظور حفظ امنیت در مرکز صدور گواهی الکترونیکی استفاده می‌شوند.

۵-۱-۲) دسترسی فیزیکی

دسترسی به ساختمان مرکز صدور گواهی الکترونیکی توسط ۶ لایه امنیتی کنترل می‌شود. اولین لایه مربوط به مراقبت ۲۴ ساعته از ورودی‌ها و ساختمان توسط نگهبان خارجی می‌باشد. دومین لایه مربوط به کنترل ورود و خروج افراد به طبقه ۴- می‌باشد. در این قسمت افراد از گیت می‌گذرند و ورود و خروج تجهیزات کنترل می‌شود. در لایه سوم و چهارم ورود و خروج با استفاده از کارت‌های هوشمند کنترل می‌شود. پنجمین لایه دسترسی افراد را به مرکز صدور گواهی الکترونیکی با استفاده از تجهیزات بایومتریک(fingerprint recognition) کنترل می‌نماید. همچنین در این لایه نگهبانی نیز ورود و خروج افراد را کنترل می‌نماید. اتاق سرور مرکز صدور گواهی الکترونیکی لایه ششم امنیتی را تشکیل می دهد، ورود و خروج افراد به لایه ششم با استفاده از تجهیزات بایومتریک کنترل می شود.

سیستم کنترل دسترسی مرکز صدور گواهی الکترونیکی توانایی محافظت از کلیه امکانات این مرکز را در برابر دسترسی غیرمجاز، دارد.

در صورتیکه هیچ یک از متصدیان مرکز داخل اتاق سرور نباشند ، مسئول امنیت فیزیکی سیستم تشخیص نفوذ را فعال کرده و توسط این سیستم از اتاق سرور مرکز صدور گواهی الکترونیکی محافظت می‌شود. علاوه بر این می‌بایست هر ۲۴ ساعت یکبار مسئول امنیت فیزیکی برای اطمینان از اینکه هیچ تلاشی در جهت از کار انداختن مکانیزم‌های امنیت فیزیکی انجام نشده است، بررسی انجام دهد.

همچنین رک‌ها در این مرکز از دسترسی غیر مجاز به کلیه تجهیزات سخت افزاری نرم‌افزاری و دستگاه‌های امنیتی سخت‌افزاری[1] جلوگیری می‌کنند.

کلیه تجهیزات ذخیره اطلاعات که از خارج وارد مرکز صدور گواهی الکترونیکی می‌شوند می‌بایست قبل از ورود در مورد ویروس‌های رایانه‌ای و یا هر نرم‌افزار دیگری که می‌تواند باعث اختلال و یا آسیب در عملکرد سیستم‌های این سازمان شود کنترل شوند.

تحت شرایط خاص ممکن است لازم باشد، افرادی به جز نقش‌های مورد اطمینان (بخش ۵-۲-۱) در قسمتی که تجهیزات مرکز صدور گواهی الکترونیکی وجود دارد، حضور داشته باشند. در چنین شرایطی حضور و دسترسی آن‌ها به سیستم‌ها فقط درصورتی امکان‌پذیر است که مسئول راهبری فنی یا مدیر مرکز در آن مکان حضور داشته باشند. همچنین کلیه فعالیت‌های این افراد در زمان حضور در مرکز ثبت شود. شرح این روال در سند سیاست‌نامه امنیت مرکز صدور گواهی الکترونیکی ذکر شده است. مسئول راهبری فنی یا مسئول امنیت فیزیکی می‌بایست بعد از خروج افراد خارجی فعالیت‌های زیر را انجام دهند:

- نحوه عملکرد تجهیزات و سیستم را کنترل نماید؛
- کلیه رکها را قفل کند؛

---

[1] *HSM*

- درستی فعالیت سیستم‌های محافظ را کنترل کند.

۵-۱-۳) سامانه تهویه و نیروی برق

علاوه برسیستم برق‌رسانی عمومی، مرکز صدور گواهی الکترونیکی می‌بایست از تجهیزاتی به منظور تامین برق این مرکز در صورت قطع برق و همچنین از سیستم UPS استفاده کند. تغییر سیستم برق عمومی با پشتیبانی به صورت خودکار انجام می‌شود و باید توانایی تامین برق کافی برای حداقل ۱ ساعت به منظور تهیه نسخه پشتیبان از اطلاعات کاری را داشته باشد.

تاسیسات مرکز صدور گواهی الکترونیکی باید سیستم کنترل درجه حرارت و رطوبت به منظور تامین محیط کارآمد برای عملیات را دارا باشد.

۵-۱-٤) جلوگیری از آب گرفتگی

تجهیزات مرکز صدور گواهی الکترونیکی در ساختمانی قرار گرفته‌اند که هیچ نوع سابقه سیل‌زدگی ندارد. این ساختمان دارای حس‌گرهای رطوبتی برای تشخیص نشت آب می‌باشند.

۵-۱-۵) پیش‌گیری و محافظت در مقابل آتش

مرکز صدور گواهی الکترونیکی دارای تجهیزات جلوگیری از آتش و حفاظت در مقابل آتش می‌باشد.

مرکز صدور گواهی الکترونیکی از سیستم اطفای حریق FM200 که با افشاندن گاز عمل اطفای حریق را انجام می‌دهد، استفاده می‌کند.این گاز دارای مشخصات زیر می‌باشد:

- با تراکم زیاد به حالت مایع درآمده، سپس به صورت مایع ذخیره می‌شود؛
- به صورت گاز بی‌رنگ، نارسانا خارج می‌شود؛

- از خود چیزی باقی نمی‌گذارد و میزان سمیت آن مانعی برای استفاده در مکان مسکونی نمی‌باشد؛
- اکسیژن را ازبین نمی‌برد، به همین دلیل برای مکان مسکونی مناسب می‌باشد؛
- سرعت تأثیر بر آتش بالایی نسبت به سیستم‌های اطفای حریق دیگر دارد.

۵-۱-٦) نگهداری سخت‌افزار ذخیره سازی

اطلاعات مربوط به ثبت وقایع باید برای حداقل ۲ دوره بازرسی در محل سایت مرکز صدور گواهی الکترونیکی قرار بگیرند.

۵-۱-۷) انهدام سخت‌افزار ذخیره سازی بلا استفاده

هنگامی که اطلاعات حساس و محرمانه و اسناد مرکز صدور گواهی الکترونیکی مذکور در بخش ۲-۸-۱)، غیرقابل استفاده می‌شوند، کلیه اطلاعات کاغذی می‌بایست توسط ماشین کاغذ خردکن از بین رفته و سخت‌افزارهای ذخیره‌سازی اطلاعات مانند و هارد دیسک‌ها می‌بایست به طور کلی فرمت شده و به طور فیزیکی نابود شوند.

۵-۱-۸) نسخه پشتیبان خارج از سایت

پشتیبانی در مرکز صدور گواهی الکترونیکی توسط توکن پشتیبان موجود در دستگاه HSM انجام می‌شود و توسط مسئول راهبری فنی به یک گاوصندوق امن منتقل می‌شود.

این توکن پشتیبان که به سایت پشتیبان منتقل شده، بهنگام بروز مشکل و از بین رفتن اطلاعات مرکز صدور گواهی الکترونیکی برای بازیابی خرابی مورد استفاده قرار می‌گیرد.

علاوه بر توکن حاوی کلید خصوصی مرکز صدور گواهی الکترونیکی ، برای هرگونه اطلاعات تغییر یافته یا تولید شده، سخت‌افزار ذخیره‌سازی حاوی این اطلاعات به سایت پشتیبان منتقل می‌شود.

۵-۲) کنترل‌های رویه‌ای

در ادامه به منظور حفظ امنیت مرکز صدور گواهی الکترونیکی ، این مرکز از کنترل‌های رویه‌ای برای تعریف نقش‌ها، تعداد افراد مورد نیاز برای هر نقش و احراز هویت هر نقش استفاده می‌کند.

۵-۲-۱) نقش‌های مورد اطمینان

نقش‌های اصلی مورد اطمینان برای اداره و راهبری مرکز صدور گواهی الکترونیکی میانی بازرگانی بشرح زیر است:

۱- مدیریت،

۲- پشتیبانی و راهبری فنی،

۳- مدیریت گواهی؛

۴- مدیریت سایت پشتیبان؛

۵- بازرسی و کنترل کیفیت،

۶- امنیت فیزیکی؛

۷- امور اداری و مالی،

۸- روابط عمومی و ارتباطات،

۹- امور دفاتر ثبت نام

جزئیات شرح وظایف هریک از مشاغل در سند منابع انسانی مرکز ذکر شده است.

سایت پشتیبان دارای نقش‌های مشابه سایت اصلی است. تعدد نقش با چارچوبی که سند منابع انسانی تعیین می‌کند، هم در سایت اصلی و هم در سایت پشتیبان مجاز است.

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

تعداد نفرات و تخصیص نیروی انسانی برای هر یک از نقش‌ها متناسب با حجم فعالیت‌ها و سیاست‌های اداره مرکز است که در سند منابع انسانی به تفصیل بیان شده است.

۵-۲-۳) احراز هویت هر نقش

مرکز صدور گواهی الکترونیکی از راهکارهایی مانند استفاده از کارت هوشمند، حساب‌های کاربری و سیستم‌های بایومتریک برای احراز هویت نقش‌های مورد اطمینان استفاده می‌کند.

۵-۳) کنترل کارکنان

۵-۳-۱) سابقه، قابلیت‌ها، تجربه و عدم سوء پیشینه

الف) موارد بررسی صلاحیت نیازهای امنیتی متصدیان نقش‌های مرکز صدور گواهی الکترونیکی شامل موارد زیر می‌باشد:

اطلاعات شخصی؛

تجارب؛

سوابق تحصیلی و حرفه‌ای؛

معرف ها؛

- مورد اطمینان بودن.

- جزئیات هر یک از موارد فوق در سند سیاست‌های امنیتی[1] مرکز آمده است.

ب) مدیریت نقش‌های امنیتی:

- کلیه متصدیان مرکز صدور گواهی الکترونیکی می‌بایست قبل از شروع به کار احراز هویت شوند. کلیه متصدیان می‌بایست از آموزش کافی برخوردار شوند و با امضای سندی مسئولیت اجرای وظایف خود را به عهده بگیرند. تمامی متصدیان باید هر ساله مورد سنجش قرار گیرند و چنانچه شخصی در این مرحله فاقد شرایط باشد، می‌بایست جایگزین شود.

پ) تغییر در متصدیان نقش‌های مرکز صدور گواهی الکترونیکی:

- در صورت استخدام و یا تغییر قرارداد کارمندان به خصوص در صورت استعفا یا پایان قرارداد، آنها نباید اطلاعات محرمانه مرکز صدور گواهی الکترونیکی را در اختیار دیگران قرار دهند.

ت) وظیفه افراد در حفظ محرمانگی اطلاعات :

- کلیه متصدیان مرکز صدور گواهی الکترونیکی می‌بایست قراردادی را برای حفظ محرمانگی اطلاعات مرکز صدور گواهی الکترونیکی که افشاء از طریق کپی برداری و انتشار اطلاعات یا روشهای دیگر را ممنوع می کند، امضاء کنند.

۵-۳-۲) رویه بررسی سابقه افراد

مرکز صدور گواهی الکترونیکی باید شرایط مذکور در بخش ۵-۳-۱) و مستندات مورد نیاز را برای بررسی سابقه افراد مطابق با سیاست های گواهی الکترونیکی ریشه کنترل نماید.

---

[1] *Security Policy*

۵-۳-۳) نیازهای آموزشی

نیازهای آموزشی هر یک از مشاغل به طور خلاصه در جدول زیر آمده است:

نقش	نیازهای آموزشی
مدیریت مرکز	• کنترل‌های امنیتی؛ • روال بازیابی خرابی؛
پشتیبانی و راهبری فنی	• نحوه دسترسی به تجهیزات مرکز صدور گواهی الکترونیکی ؛ • نصب، پیکربندی و نگهداری مرکز صدور گواهی الکترونیکی ؛ • روال ایجاد و نگهداری گواهی و لیست گواهی های باطل شده؛ • ایجاد روال پیکربندی پارامترهای ثبت وقایع؛ • روال تولید و تهیه نسخه پشتیبان از کلیدها؛ • روال بازیابی خرابی؛ • تهیه نسخه پشتیبان از وقایع؛
مدیریت گواهی	• نحوه دسترسی به تجهیزات مرکز صدور گواهی الکترونیکی ؛ • روال صدور گواهی‌ها؛ • روال ابطال گواهی‌ها؛ • روال بازیابی خرابی؛
امنیت فیزیکی	• روال پیکربندی کنترل‌های فیزیکی؛

نقش	نیازهای آموزشی
	• روال بازیابی خرابی.
امور دفاتر و مرکز ثبت‌نام	• آموزش‌های عمومی امنیت و گواهی الکترونیکی
اداری و مالی	• آموزش‌های عمومی امنیت و گواهی الکترونیکی
بازرسی و کنترل امنیت	• آموزش‌های عمومی امنیت و گواهی الکترونیکی، ISO27001, ISO9001

۵-۳-٤) تناوب برنامه‌های آموزشی و نیازهای آن

کلیه متصدیان باید از کلیه تغییرات مرکز صدور گواهی الکترونیکی در مورد بروزرسانی سخت‌افزار و نرم‌افزار، عملیات روزانه، سیاست های گواهی الکترونیکی، دستورالعمل اجرائی گواهی الکترونیکی آگاه باشند. برای اطمینان از اینکه کلیه متصدیان تغییرات را بطور کامل دریافته‌اند، هر تغییر مهمی در این رابطه نیازمند آموزش متصدیان و مستندسازی تغییرات می‌باشد.

۵-۳-۵) تناوب و توالی گردش شغلی

گردش شغلی در مرکز صدور گواهی الکترونیکی اجراء نمی‌شود. در صورت جابجایی متصدیان در بین نقش‌های مختلف تنها برآورده شدن نیازهای بخش ۵-۳-۱) و ۵-۳-۲)کافی می‌باشد.

۵-۳-٦) جریمه خروج از محدوده اختیارات

مرکز صدور گواهی الکترونیکی می‌بایست اقدامات کنترلی و انضباطی را برای کلیه کارکنانی که فعالیتهای غیر مجاز در مورد مرکز صدور گواهی الکترونیکی یا مخزن آن انجام می‌دهند، اعمال نماید. شرح این اقدامات کنترلی و انضباطی در سیاست‌نامه امنیتی مرکز صدور گواهی الکترونیکی ، ارائه شده است.

۵-۳-۷) تدوین رویه های مورد نیاز برای همکاری با پیمانکاران

فرآیند عقد قرارداد با کارمندان قراردادی و پیمانکاران در سند سیاست‌نامه امنیتی مرکز صدور گواهی الکترونیکی آمده است.

۵-۳-۸) مستندات فراهم شده برای کارکنان

مرکز صدور گواهی الکترونیکی می‌بایست کلیه مستندات شامل دستورالعمل اجرائی گواهی الکترونیکی و هر گونه اساسنامه یا قرارداد مرتبط را در اختیار کارکنان دفاتر ثبت نام گواهی الکترونیکی قرار دهد.

٦) کنترل های امنیتی فنی

٦-١) تولید و نصب زوج کلید

٦-١-١) تولید زوج کلید

مرکز صدور گواهی الکترونیکی زوج کلید را با استفاده از الگوریتم RSA تولید و آن را رمزنگاری کرده و در پایگاه داده مرکز نگهداری می کند.

٦-١-٢) تحویل کلید عمومی به مرکز صدور گواهی الکترونیکی

مطابق با روال درخواست گواهی، صاحبان امضا کلید عمومی خود را در یک فایل درخواست امضا گواهی یا CSR به مرکز صدور گواهی الکترونیکی تحویل می دهند.

٦-١-٣) تحویل کلید عمومی مرکز صدور گواهی الکترونیکی به طرف‌های اعتماد کننده

طرف‌ها ی اعتماد کننده میتوانند گواهی مرکز صدور گواهی الکترونیکی را از مخزن این مرکز دریافت کنند.

٦-۱-٤) طول کلید

صاحبان امضا باید درخواست های امضای گواهی خود را با طول کلید ۱۰۲۴ بیت به دفتر ثبت نام گواهی الکترونیکی تحویل دهند.

٦-۱-٥) تولید پارامترهای تولید کلید عمومی

پارامتر کلید عمومی الگوریتم RSA تهی می‌باشد.

٦-۱-٦) کنترل کیفیت پارامتر

به بخش ۶-۱-۵) رجوع شود.

٦-۱-۷) تولید کلید نرم افزاری/ سخت افزاری

تعیین روال تولید زوج کلید مورد نیاز برای گواهی الکترونیکی تنها بر عهده صاحبان امضا می باشد. مرکز صدور گواهی الکترونیکی و دفاتر ثبت نام گواهی الکترونیکی هیچ گونه مسئولیت در قبال تولید زوج کلید صاحبان امضا ندارند.

٦-۱-۸) موارد کاربرد کلید (طبق فیلد کاربرد کلید X.509 v3)

گواهی های صادر شده توسط مرکز صدور گواهی الکترونیکی دارای فیلد کاربرد کلید می باشد. صاحبان امضا و طرف های اعتماد کننده باید تنها از گواهی های صادر شده توسط مرکز صدور گواهی الکترونیکی مطابق با این دستورالعمل و قوانین حاکم استفاده کنند.

٦-۲) محافظت از کلیدهای خصوصی

٦-۲-۱) استانداردهای دستگاههای رمزنگاری

مرکز صدور گواهی الکترونیکی از دستگاههای سخت افزاری ایمن مطابق با استاندارد FIPS 140-1 استفاده می‌کند.

صاحبان امضا مسئول محافظت از کلید خصوصی مرتبط با کلید عمومی موجود در گواهی الکترونیکی خود می باشند.

٦-۲-۲) کنترل چند نفره دسترسی به کلید خصوصی (m از n)

در مرکز میانی پشتیبانی نمی‌شود.

٦-۲-۳) دستیابی قانونی به کلید خصوصی

دستیابی قانونی به کلید خصوصی مرکز صدور گواهی الکترونیکی امکان‌پذیر نیست.

٦-۲-٤) تهیه نسخه پشتیبان از کلید خصوصی

مرکز صدور گواهی الکترونیکی به منظور تهیه نسخه پشتیبان از کلید خصوصی، از پایگاه داده و کلید خصوصی خود نسخه پشتیبان تهیه میکند.

٦-۲-٥) بایگانی کلید خصوصی

کلید خصوصی مرکز صدور گواهی الکترونیکی که برای امضای الکترونیکی استفاده می شود، نمی‌تواند ذخیره شود.

٦-۲-٦) وارد کردن کلید خصوصی به دستگاههای رمزنگاری

روال وارد کردن کلید خصوصی با توجه به قابلیت‌های سخت‌افزارهای رمزنگاری مشخص می‌گردد.

٦-۲-۷) روش فعال سازی کلید خصوصی

روال فعال‌سازی کلید خصوصی با توجه به قابلیت‌های سخت‌افزارهای رمزنگاری مشخص می‌گردد.

٦-۲-۸) روش غیرفعال سازی کلید خصوصی

نقش‌های اجرایی مرکز صدور گواهی الکترونیکی می‌توانند به صورت دستی یا از طریق خارج کردن دستگاه رمزنگاری از HSM، قطع برق HSM یا خاموش کردن سیستم رایانه‌ای مرکز صدور گواهی الکترونیکی را غیرفعال کنند و برای فعال‌سازی دوباره این کلید باید روال مذکور در بخش ۶-۲-۷) را اجرا کنند.

٦-۲-۹) روش نابود کردن کلید خصوصی

به منظور جلوگیری از سوء استفاده از کلید خصوصی قدیمی مرکز صدور گواهی الکترونیکی ، که بر درست بودن گواهی‌های صادر شده تاثیر می‌گذارد، کلید خصوصی مرکز صدور گواهی الکترونیکی در زمان پایان چرخه حیات، نابود می‌شود. بنابراین بعد از اتمام فرآیند تولید کلید و صدور گواهی جدید، مرکز صدور گواهی الکترونیکی از فرآیند صفر کردن[1] در حافظه برای نابودی کلید خصوصی قدیمی خود که در دستگاه رمزنگاری سخت‌افزار ذخیره شده، استفاده می‌کند.

٦-۳) وجوه دیگر مدیریت زوج کلید

مرکز صدور گواهی الکترونیکی هیچ مسئولیتی در قبال کلید خصوصی صاحبان امضا ندارد.

---

[1] *Zeroize*

٦-٣-١) بایگانی کلید عمومی

مرکز صدور گواهی الکترونیکی بایگانی گواهی‌ها را انجام می دهد و همچنین با توجه به قوانین بخش ۴-۶) کنترلهای امنیتی بر سیستم بایگانی را انجام می‌دهد. نظر به اینکه بایگانی گواهی‌ها می‌تواند جایگزین بایگانی کلید عمومی شود، هیچ روال دیگری برای بایگانی کلید عمومی وجود ندارد.

٦-٣-٢) دوره تناوب کاربرد و کلیدهای خصوصی و عمومی

٦-٣-٢-١) دوره تناوب کاربرد کلیدهای خصوصی و عمومی برای مرکز صدور گواهی الکترونیکی

طول کلید RSA برای کلید عمومی و خصوصی مرکز صدور گواهی الکترونیکی ۱۰۲۴ بیت می‌باشد. زمان استفاده از گواهی کلید عمومی و کلید خصوصی حداکثر ۵ سال است.

٦-٣-٢-٢) دوره تناوب کاربرد کلید عمومی و خصوصی برای صاحبان امضا

مرکز صدور گواهی الکترونیکی گواهی های یک ساله صادر می کند.

٦-٤) اطلاعات فعال ساز

٦-٤-١) تولید و بکارگیری اطلاعات فعال‌ساز

مرکز صدور گواهی الکترونیکی Master key را در دستگاههای سخت افزاری رمزنگاری تولید و محافظت می نماید.

٦-٤-٢) محافظت از اطلاعات فعال‌ساز

اطلاعات فعال‌ساز مرکز صدور گواهی الکترونیکی از طریق اسم رمز و مطابق با مشخصات و قابلیت‌های سخت‌افزار رمزنگاری محافظت می‌شود.

٦-٤-٣) وجوه دیگر اطلاعات فعال‌ساز

هیچ قانونی برای وجوه دیگر اطلاعات فعال‌ساز وجود ندارد.

٦-٥) کنترل های امنیتی رایانه

٦-٥-١) نیازهای خاص امنیتی فنی رایانه

سیستم های رایانه‌ای که سرورهای مرکز صدور گواهی الکترونیکی بر روی آنها قرار دارد، مطابق بـا بخـش ٥-١) بـه صورت فیزیکی محافظت می شوند. سیستم عامل این سیستم ها، کنترل‌های امنیتی زیر را فراهم می نمایند:

- ورود به سیستم از طریق احراز هویت ؛
- فراهم آوردن قابلیت ثبت وقایع امنیتی؛
- محدود کردن دسترسی توسط سرویس‌های صدور گواهی و نقش‌های امنیتی؛
- اطمینان از امنیت پایگاه داده با استفاده از فن‌آوری رمزنگاری.

٦-٥-٢) درجه بندی امنیت رایانه

مرکز صدور گواهی الکترونیکی از سیستم‌های رایانهی با کنترل‌های امنیتی تعریف شـده در اسـتاندارد ISO 27001 استفاده می‌کند.

٦-٦) کنترل‌های فنی طول عمر

٦-٦-١) کنترل های توسعه سیستم

کاربردی ندارد.

٦-٦-٢) کنترلهای مدیریت امنیت

درستی تنظیمات و کنترل های امنیتی مذکور در این دستورالعمل سالیانه بررسی می شود.

٦-٧) کنترل های امنیت شبکه

شبکه مرکز صدور گواهی الکترونیکی می‌تواند از حمله‌های نفوذی از طریق بروزرسانی فایل‌های ترمیمی سیستم، جستجوی آسیب پذیری سیستم، تشخیص نفوذ به سیستم، سیستم دیواره آتش و مسیریاب فیلتر کننده جلوگیری کند.

٦-٨) کنترل های مهندسی دستگاه رمزنگاری

مطابق با قوانین بخش ۶-۱) و ۶-۲) می باشد.

۷) مشخصات گواهی و لیست گواهی‌های باطل شده

پروفایل گواهی‌های صادر شده توسط مرکز صدور گواهی الکترونیکی با پروتکل Secure Socket Layer هم خوانی دارد.

۷-۱) فرم مشخصات گواهی

۷-۱-۱) شماره نسخه

مرکز صدور گواهی الکترونیکی تنها در قالب X.509 نسخه ۳ گواهی صادر می‌کند.

۷-۱-۲) ملحقات گواهی

قوانین اضافه کردن، تخصیص مقدار و پردازش ملحقات گواهی در فرم گواهی توضیح داده شده‌اند.

۷-۱-۳) شناسه الگوریتم‌ها

در گواهی‌های صادر شده در مرکز صدور گواهی الکترونیکی از این الگوریتم‌هایی با این شناسه‌ها استفاده می‌شود:

شناسه	نام الگوریتم	کاربرد
1.2.840.113549.1.1.5	Sha1RSA	الگوریتم امضای مرکز صدور گواهی الکترونیکی

۷-۱-٤) قالب نام‌ها

محتوی فیلد "subject" و "issuer" گواهی‌ها باید مطابق با نام‌های ترکیبی X.500 باشند و نوع مشخصه‌ها باید مطابق با RFC2459 باشد.

۷-۱-۵) محدودیت در نام‌گذاری

هیچ محدودیتی برای نام‌گذاری گواهی‌ها غیر از موارد مذکور در سیاست های گواهی الکترونیکی ریشه و این دستورالعمل وجود ندارد.

۷-۱-٦) شناسه سیاست های گواهی الکترونیکی

کاربردی ندارد.

۷-۱-۷) کاربرد فیلد الحاقی "policyconstraints"

هیچ شرایطی وجود ندارد.

۷-۱-۸) نحو و معنای فیلد الحاقی " policyqualifiers"

گواهی‌های صادر شده تحت این سیاست های دارای فیلد الحاقی "policyqualifiers" نمی باشند.

۷-۱-۹) پردازش معنایی برای ملحقات الحاقی " certificatepolicy"

در سیاست های گواهی الکترونیکی ریشه فیلد الحاقی "سیاست های گواهی الکترونیکی" یک فیلد حیاتی نمی‌باشد.

۷-۲) مشخصات لیست گواهی‌های باطل شده

۷-۲-۱) شماره نسخه

لیست گواهی‌های باطل شده صادره تحت این آیین نامه باید از شماره نسخه تعریف شده در استانداردX.509 نسخه ۲، استفاده کنند [ISO 9594-8].

۷-۲-۲) لیست گواهی‌های باطل شده و فیلد الحاقی " CRLentry"

فرم تفصیلی لیست گواهی‌های باطل شده که استفاده از تمام ملحقات را تحت پوشش قرار می‌دهد، در ضمیمه الف این دستورالعمل آمده است.

۸) راهبری دستورالعمل گواهی الکترونیکی

۸-۱) 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 اساسا دوباره‌نویسی آن انجام شوند. چنانچه سیاست های گواهی الکترونیکی ریشه یا شناسه آن تغییر کند، آنگاه این دستورالعمل می‌بایست مطابق با تغییرات سیاست های 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 اطلاع‌رسانی دارند:

تغییراتی که می‌تواند بر نحوه عملکرد صاحبان امضا و طرف‌های اعتماد کننده که از این دستورالعمل استفاده می‌کنند، تاثیر چشمگیر داشته باشد، می‌بایست ۳۰ روز قبل از اعمال تغییرات به دستورالعمل اجرائی در مخزن منتشر شود.

مکانیزم 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، پیش از اعمال، می‌بایست ابلاغ رسمی این تغییرات مستقیماً توسط مرکز میانی به صاحبان امضا و طرف‌های اعتماد کننده و دفاتر ثبت نام طرف قرارداد، صورت گیرد.

۸-۲) روال انتشار و اطلاع رسانی

پیش از اعمال تغییر در این آیین نامه، اطلاعیه در مورد این تغییرات در مخزن مرکز صدور گواهی الکترونیکی منتشر خواهد شد.

۸-۳) روال تائید دستورالعمل اجرائی گواهی الکترونیکی

این دستورالعمل و تغییرات اعمال شده بر روی آن پس از تایید کمیسیون گواهی الکترونیکی بازرگانی برای اخذ تایید مطابقت با اسناد سیاست‌های گواهی الکترونیکی و دستورالعمل اجرایی مرکز ریشه در اختیار مرکز دولتی صدور گواهی مرکز ریشه قرار می‌گیرد. به محض دریافت تایید، دستورالعمل و تغییرات آن قابل اجرا و انتشار خواهد بود.

۹) مراجع

- راهنمای تهیه دستورالعمل اجرایی گواهی الکترونیکی؛
- سیاست های گواهی الکترونیکی ریشه ؛
- RFC 2527؛
- RFC 3280 ؛

۱۰) ضمیمه-الف

۱۰-۱) گواهی الکترونیکی صاحبان امضا

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
Version	*ویرایش*	V3
Serial Number	*شماره سریال*	باید منحصر بفرد باشد
Signature Algorithm	*الگوریتم امضای صادر کننده*	sha1RSA
Issuer	*نام ترکیبی صادر کننده*	Cn= Name & Family Name
Valid from	*تاریخ شروع اعتبار*	
Valid to	*تاریخ انقضا*	
Subject	*نام ترکیبی دارنده گواهی*	{Cn={FQDN}و ou={نام بخش‌های سازمانی,{ }=oنام سازمان{وc=IR
Public Key	*اطلاعات کلید عمومی دارنده گواهی*	کلید RSA با پیمانه X بیتی
Issuer Unique Identifier	*شناسه یکتای صادر کننده*	وجود ندارد
Subject Unique Identifier	*شناسه یکتای دارنده گواهی*	وجود ندارد
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 الکترونیکی 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 صاحب امضا که بصورت DER

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
		کدگذاری شده باشد)
key usage	*کاربرد کلید*	Digital signature, Non-Repudiation, Key Encipherment, Data Encipherment
Enhanced key usage	*کاربردهای توسعه یافته کلید*	Server Authentication (1.3.6.1.5.5.7.3.1)
Private key usage period	*دوره کاربرد کلید خصوصی*	وجود ندارد
Certificate policies	*سیاست های گواهی الکترونیکی*	وجود ندارد
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*	وجود ندارد
Name Constraints	*قیود نام*	وجود ندارد
Policy Constraint	*قیود سیاست های*	وجود ندارد
Authority Information Access	*دسترسی به اطلاعات مرکز*	وجود ندارد
CRL Distribution Point	*نقطه انتشار لیست گواهی‌های باطل شده*	URL=http://www.rca.gov.ir/LDAP

۱۰-۲) لیست گواهی های باطل شده

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
Version	*ویرایش*	V1
Signature Algorithm	*الگوریتم امضای صادر کننده*	sha1RSA
Issuer	*نام ترکیبی صادر کننده*	CN = Name & Family Name
thisUpdate	*بروزرسانی جاری*	UTCT

نام اصلی فیلد	نام فارسی فیلد	مقدار فیلد
nextUpdate	*بروزرسانی بعدی*	UTCT; thisUpdate + 24 h
Revoked certificates list	*لیست گواهی‌های باطل شده*	زوج مرتب‌هایی (صفر یا بیشتر) متشکل از شماره سریال گواهی و تاریخ ابطال (مطابق با UTCT)
CRL extensions	*ملحقات لیست گواهی‌های باطل شده*	
CRL Number	*شماره لیست گواهی‌های باطل شده*	یک عدد صحیح
Authority Key Identifier	*شناسه کلید مرکز*	c=no; Octet String(مقدار ۲۰ بایتی تابع درهم‌سازی SHA-1 بر روی اطلاعات باینری کلید عمومی مرکز صدور گواهی الکترونیکی که بصورت DER کدگذاری شده باشد)
CRL entry extensions	*ملحقات ورودی لیست گواهی‌های باطل شده*	
Invalidity Date	*تاریخ پایان اعتبار*	وجود ندارد.
Reason Code	*کد دلیل*	این فیلد حتماً باید وجود داشته باشد

۱۱) ضمیمه-ب

۱۱-۱) واژه‌نامه

مخفف	لغت	معنی
FIPS	Federal information processing standard	راهنمایی‌های تخصصی که موسسه ملی استانداردها و فن‌آوری ایالت متحده آمریکا برای تهیه تجهیزات سیستم و سرویس پردازشگر اطلاعاتی دولت آمریکا تهیه کرده‌است.
RSA	Rivest-Shamir-Adleman	الگوریتم رمزنگاری نامتقارن که در سال ۱۹۷۷ توسط ران ریوست، ادی شمیر و لئونارد آدلمن اختراع شده است.
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 گـواهی الکترونیکی	Certificate practice statement	دستورالعمل اجرایی که مرکز صدور گواهی الکترونیکی برای صدور گواهی از آن استفاده می‌کند.
ابطال گواهی الکترونیکی	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 دستگاه‌های رمزنگاری مورد نیاز هستند.
اطمینان	Assurance	مشخصه‌ای از سیستم اطلاعاتی، که اطمینان می‌دهد سیستم مطابق با سیاست‌نامه امنیتی کار می‌کند.
اعتبار	Authenticity	اصل، قابل اطمینان و قابل تشخیص بودن.
اعتبار گواهی	Validity of Certificate	یک واحد داده در گواهی الکترونیکی که دوره زمانی اعتبار پیوند بین اطلاعات گواهی 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.

لغت	معادل	معنی
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 الکترونیکی	Certificate Expiration	عدم اعتبار گواهی الکترونیکی 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 ارائه خدمات صدور گواهی الکترونیکی و پیشنهاد تغییرات به منظور اقدام متقابل.
بازیابی کلید	Key Recovery	فرآیند 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.

لغت	معادل	معنی
بروزرسانی گواهی	Certificate Update	فرآیندی که توسط آن اطلاعات (به غیر از کلید گواهی) گواهی الکترونیکی موجود، بخصوص اختیارات داده شده به مالک، با صدور گواهی جدید تغییر می‌کند.
پایگاه‌های داده	Database	مجموعه‌ای از اطلاعات مرتبط منطقی.
پروتکل	Protocol	مجموعی‌ای از قوانین برای اجرا و کنترل نوعی ارتباط بین سیستم‌ها.
پروتکل اعلام برخط وضعیت گواهی‌های الکترونیکی	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 که بر اساس حساب پیمانه‌ای می‌باشد.
پیوند	Bind	با اجرای مکانیزم‌هایی، ارتباط جدانشدنی برقرار کردن، برای مثال استفاده از امضای الکترونیکی برای برقراری پیوند بین صاحب‌امضا و کلید عمومی گواهی الکترونیکی.
احراز هویت	Authentication	فرآیند 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.

لغت	معادل	معنی
تجدید کلید گواهی الکترونیکی	Certificate Rekey	فرآیند تجدید کلید عمومی گواهی الکترونیکی موجود با صدور گواهی الکترونیکی جدید دارای کلید متفاوت جدید.
تجدید گواهی الکترونیکی	Certificate Renewal	فرآیند تمدید اعتبار اطلاعات گواهی الکترونیکی با صدور گواهی الکترونیکی جدید.
تحلیل مخاطره	Risk Assessment	فرآیندی 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	فرآیندی 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.
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 سیاست های 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.

لغت	معادل	معنی
تولید کلید	Key Generation	فرآیند ایجاد رشته‌ای از علائم که یک کلید رمزنگاری را ایجاد می‌کنند.
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.
ثبت‌نام	Registration	یک اقدام یا فرآیند اجرایی برای ثبت اولیه نام و مشخصه‌های دیگر یک موجودیت در مرکز صدور گواهی الکترونیکی (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 الکترونیکی	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.
سخت‌افزار ذخیره‌سازی	Media	آنچه اطلاعات در آن نوشته و ذخیره می‌شود.
رک	Rack	کابینتی که سرور یا ایستگاه کاری ذخیره‌سازی در آن قرار می‌گیرد.

لغت	معادل	معنی
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 الکترونیکی	Certification Path	زنجیره منظم گواهی الکترونیکی که به طرف اعتماد کننده توانایی ارزیابی صحت امضای آخرین گواهی این زنجیره را می‌دهد.
زوج کلید	Key Pair	مجموعه‌ای از کلیدهای مرتبط ریاضیاتی(کلید خصوصی و کلید عمومی) که برای رمزنگاری نامتقارن استفاده می‌شوند و به گونه‌ای تولید می‌شوند که امکان گرفتن کلید خصوصی از اطلاعات کلید عمومی وجود نداشته باشد.
زیر ساخت کلید عمومی	Public Key Infrastructure	مجموعه‌ای از سیاست‌ها، فرآیندها، نرم‌افزارها و ایستگاه‌های کاری مورد نیاز برای اداره گواهی‌ها و زوج‌کلیدها می‌باشد (مانند صدور، نگهداری و ابطال گواهی‌الکترونیکی).

لغت	معادل	معنی
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.
سیاست‌نامه امنیتی	Security policy	مستندی حاوی مجموعه‌ای از دستورات، اقدامات و روال‌های مشخص‌کننده کنترل‌های امنیتی مدیریت، توزیع و حفاظت از دارایی‌ها می‌باشد.
سیاست های گواهی الکترونیکی	Certificate Policy	مجموعه‌ای از قوانین که التزامات 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 ANSI.1) که برای اشاره به اشیا با ویژگی‌های مشخص استفاده می‌شود.
شیوه نامه کاربردی:	Application procedure	مجموعه دستورالعملهایی است که ضوابط، شیوه و جزئیات کاربرد خدمات و گواهی‌های الکترونیکی را بیان میکند
شناسه سیاست گواهی	Policy Object Identifier (POID)	نامی منحصربفرد و رسمی، تشکیل شده از مجموعه‌ای از اعداد (تخصیص یافته توسط استاندارد ANSI.1) که برای اشاره به سیاست های 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 دستگاه رمزنگاری یا ابزار دیگر.

لغت	معادل	معنی
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 الکترونیکی	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 اندازه کارت اعتباری محتوی یک یا چند مدار مجتمع که وظایف پردازشگر مرکزی رایانه، حافظه و میانگر ورودی/خروجی را به عهده دارد.
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.

لغت	معادل	معنی
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 کشور	Certification Policy management Consul	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 صدور گواهی ریشه و تصویب سیاست های گواهی الکترونیکی ریشه و تایید تطابق دستورالعمل اجرایی تمام مراکز صدور گواهی با این سیاست ها، شورایی به نام شورای سیاست‌گذاری گواهی الکترونیکی کشور 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 الکترونیکی مرکز صدور گواهی الکترونیکی میانی که توسط مرکز صدور گواهی الکترونیکی ریشه امضا می‌شود و به مرکز صدور گواهی الکترونیکی 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

لغت	معادل	معنی
		زوج کلید متعلق به امضا کننده هستند.
گواهی الکترونیکی	Digital Certificate	یک گواهی در قالب شی داده‌ای الکترونیکیی که به آن یک امضای الکترونیکی بر اساس آن شی داده‌ای اضافه می‌شود.
گواهی مورد اطمینان	Trusted certificate	یک گواهی الکترونیکی که طرف‌های اعتماد کننده به اعتبار آن، بدون نیاز به ارزیابی صحت گواهی الکترونیکی 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.
دستگاه سخت‌افزاری رمزنگاری	Hardware Encryption Module/HSM	مجموعه‌ای از سخت‌افزار، نرم‌افزار و ترکیب آنها که فرآیند و منطق رمزنگاری را مانند الگورتم رمزنگاری اجرا می‌کند و در محدوده رمزنگاری دستگاه قرار دارد.

لغت	معادل	معنی
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	فرآیند 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.
مدیریت مخاطرات	Risk Management	فرآیند 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 الکترونیکی را مطابق با پروتکل اعلام وضعیت گواهی به صورت برخط ارائه می‌کند.

لغت	معادل	معنی
مرکز ثبت‌نام	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 الکترونیکی	Certificate Authority	موجودیتی که گواهی الکترونیکی صادر می‌کند و پیوند بین داده‌های گواهی را ضمانت می‌کند.
مرکز صدور گواهی الکترونیکی میانی	Intermadiate/Subject CA	یک مرکز صدور گواهی الکترونیکی که گواهی خود را از مرکز صدور گواهی الکترونیکی ریشه دریافت می‌کند و می‌تواند برای صاحبان امضا گواهی صادر کند.
مرکز صدور گواهی الکترونیکی ریشه	Root CA	یک مرکز صدور گواهی الکترونیکی که مستقیماً مورد اطمینان موجودیت نهایی می‌باشد. به دست آوردن کلید عمومی مرکز صدور گواهی الکترونیکی ریشه نیاز به مکانیزم‌های 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.

لغت	معادل	معنی
مکانیزم M از N	M out of N mechanism	تقسیم یک وظیفه بین n موجودیت به گونه‌ای که هر تعداد کمتر از m نفر نتوانند کل وظیفه را انجام دهند و برای انجام وظیفه حداقل حضور m نفر از آن n نفر لازم می‌باشد.
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 گواهی‌های الکترونیکی 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 صدور گواهی الکترونیکی ریشه که از کانالی مطمئن دریافت شده است.

لغت	معادل	معنی
نگاشت سیاست	Policy Mapping	زمانیکه یک مرکز صدور گواهی الکترونیکی موجود در یک دامنه به مرکز صدور گواهی دیگری در دامنه دیگر گواهی دهد، سیاست های گواهی الکترونیکی موجود در دامنه دیگر ممکن است که توسط مرکز صدور گواهی الکترونیکی دامنه اول معادل با سیاست های 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، پایگاه‌های داده.
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.
تمامیت	Integrity	عدم تخریب یا تغییر غیر مجاز اطلاعات.