مرکز صدور گواهی الکترونیکی میانی پارس‌ساین

دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی پارس‌ساین

شماره سند.... SSW_PS_PKI_88217_11

تاریخ..... ۲۵ تیر ۱۳۹۳

نگارش..... ۱/۳

طبقه‌بندی..... عادی

آدرس: تهران، خیابان آزادی، خیابان حبیب‌الله، خیابان قاسمی غربی، شماره ۳۷، طبقه پنجم

تلفن: ۲۰-۶۱۹۷۵۵۰۰ (۰۲۱) **فاکس**: ۶۶۰۹۰۲۹۹ (۰۲۱) **سایت اینترنتی**: www.parssignca.ir

حق طبع و نشر

فهرست مطالب

فهرست جداول

۱ مقدمه

سیستم‌های رمزنگاری کلید عمومی، با هدف ایجاد امنیت در تبادل اطلاعات با فراهم نمودن خدمات امنیتی مختلف از قبیل تمامیت[1]، محرمانگی اطلاعات، و احراز هویت موجودیت‌ها طراحی شده‌اند. زیرساخت کلید عمومی (PKI)[2]، به مجموعه‌ای از خدمات، محصولات، سیاست‌ها، فرایندها، و سیستم‌های نرم‌افزاری و سخت‌افزاری گفته می‌شود که هدف آن، فراهم نمودن زیرساختی برای مدیریت گواهی‌های الکترونیکی و ارائه سرویس‌های امنیتی مبتنی بر رمزنگاری کلید عمومی می‌باشد.

مرکز صدور گواهی الکترونیکی میانی خصوصی پارس‌ساین، یک زیرساخت کلید عمومی جهت صدور و مدیریت گواهی‌های الکترونیکی طراحی و پیاده‌سازی نموده است. «دستورالعمل اجرایی گواهی الکترونیکی[3]» این مرکز بر اساس «سیاست‌های گواهی الکترونیکی[4] زیرساخت کلید عمومی کشور» (منتشرشده توسط مرکز دولتی صدور گواهی ریشه)، تنظیم شده است. این دستورالعمل اجرایی شیوه‌ها و چگونگی اعمال رویه‌های اتخاذشده توسط مرکز میانی خصوصی پارس‌ساین جهت فراهم نمودن خدمات گواهی الکترونیکی از قبیل صدور، تمدید، و ابطال گواهی‌ها و اعلام وضعیت (ابطال یا عدم ابطال) گواهی ها، را بیان می‌دارد؛ همچنین بر اساس استاندارد X.509 و مطابق با RFC 3647 تهیه و تنظیم شده است.

در این سند، منظور از «مرکز صدور گواهی الکترونیکی میانی خصوصی پارس‌ساین»، مجموعه «مرکز صدور گواهی الکترونیکی خصوصی پارس‌ساین» و «دفاتر ثبت‌نام وابسته به این مرکز» می‌باشد. همچنین، در برخی موارد جهت اختصارنویسی به جای «مرکز صدور گواهی الکترونیکی میانی خصوصی پارس‌ساین»، «مرکز دولتی صدور گواهی الکترونیکی ریشه»، و «شورای سیاست‌گذاری گواهی الکترونیکی کشور»، به ترتیب از «مرکز میانی خصوصی پارس‌ساین»، «مرکز ریشه»، و «شورا» استفاده شده است.

[1] Integrity
[2] Public Key Infrastructure
[3] Certificate Practice Statement (CPS)
[4] Certficate Policy (CP)

۱-۱ خلاصه

مرکز میانی خصوصی پارس‌ساین، یک مرکز صدور گواهی در ساختار سلسله مراتبی مراکز صدور گواهی جمهوری اسلامی ایران می‌باشد. این مرکز آمادگی ارائه خدمات گواهی برای کاربردهای تعریف‌شده در زیرساخت کلید عمومی کشور دارد.

این سند شامل مجموعه‌ای از قواعد و دستورالعمل‌های اجرایی است که مرکز میانی خصوصی پارس‌ساین به منظور صدور و مدیریت گواهی‌های الکترونیکی در نظر گرفته است.

بر اساس مصوبات شورای سیاست‌گذاری گواهی الکترونیکی کشور[۱]، مرکز صدور گواهی خصوصی پارس‌ساین یک مرکز صدور گواهی در کلاس ۲ می‌باشد که قابلیت صدور گواهی در سطوح اطمینان ۱ و ۲ تعریف‌شده در جدول ۱-۱ را دارد[۲].

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

[۱] برای آگاهی از وظایف و افراد تشکیل‌دهنده این شورا به سند «سیاست‌های گواهی زیرساخت کلید عمومی کشور» منتشرشده توسط مرکز ریشه مراجعه نمایید.

[۲] کلاس مرکز صدور گواهی الکترونیکی میانی خصوصی پارس‌ساین که در این سند قید شده، بر اساس مصوبه مورخ ۱۳۸۸/۳/۳۱ در نظر گرفته شده است.

جدول ۱-۱ سطوح اطمینان گواهی در مرکز میانی خصوصی پارس‌ساین

سطح اطمینان	سطح گواهی	کاربرد
سطح ۱	برنز	این سطح پایین‌ترین درجه اعتماد به هویت مالک گواهی را فراهم می‌نماید. یکی از کاربردهای اولیه این سطح، فراهم کردن سرویس امنیتی تمامیت یا اطمینان از دست‌نخوردگی برای اطلاعاتی که امضا شده است، می‌باشد. استفاده از سطح ۱ برای تراکنش‌هایی که نیاز به احراز هویت دارند مناسب نمی‌باشد ولی چنانچه در یک ارگان یا سازمان فرایند هویت‌شناسی درخواست‌کنندگان گواهی، به صورت مستقل از مرکز صدور گواهی یا دفاتر ثبت‌نام ذی‌ربط صورت پذیرد، استفاده از این گواهی جهت کاربرد احراز هویت صرفاً داخل محدوده همان ارگان یا سازمان، بلامانع می‌باشد. استفاده از این سطح برای تراکنش‌هایی که نیاز به محرمانگی دارند (پست الکترونیک امن) توصیه نمی‌شود، ولی چنانچه امکان استفاده از گواهی‌های سطوح بالاتر وجود نداشته باشد، استفاده از این سطح بلامانع است. این سطح از گواهی می‌تواند در محیط‌هایی که مخاطرات و خسارات ناشی از سوء استفاده، جعل و افشاء اطلاعات پایین است، مورد استفاده قرار گیرد.
سطح ۲	نقره	این سطح برای محیط‌هایی که در آن مخاطرات و خسارات ناشی از سوء استفاده، جعل و افشاء اطلاعات چندان زیاد نمی‌باشد (حد متوسط)، مورد استفاده قرار می‌گیرد. از گواهی‌های این سطح با در نظر گرفتن بند اول، می‌توان برای تراکنش‌هایی که نیاز به تمامیت، احراز هویت، انکارناپذیری، و محرمانگی دارند استفاده نمود.

۱-۲ نام و شناسه سند

این سند به نام سند «دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی پارس‌ساین» شناخته می‌شود. تاریخ انتشار سند، ۱۳۹۳/۰۴/۲۵ می‌باشد. آخرین نسخه این سند در سایت مرکز میانی پارس‌ساین به نشانی www.parssignca.ir قابل دسترسی است.

شناسه سیاست‌هایی که این سند بر اساس آن‌ها تنظیم شده، طبق آنچه مرکز ریشه به مرکز میانی خصوصی پارس‌ساین اعلام نموده است، برای هر سطح اطمینان در جدول ۱-۲ آمده است.

جدول ۱-۲ شناسه سیاست‌های سطوح اطمینان

سطح اطمینان	شناسه سیاست‌های سطوح اطمینان
سطح ۱	۲.۱۶.۳۶۴.۱۰۱.۱.۱.۱
سطح ۲	۲.۱۶.۳۶۴.۱۰۱.۱.۱.۲

۱-۳ اجزای زیرساخت کلید عمومی

۱-۳-۱ مراکز صدور گواهی الکترونیکی[1]

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

۱-۳-۱-۱ مرکز دولتی صدور گواهی الکترونیکی ریشه

مرکز دولتی صدور گواهی الکترونیکی ریشه، نقطه اعتماد[2] در زیرساخت کلید عمومی کشور می‌باشد. این مرکز بر اساس مفاد بند الف از ماده ۴ آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و طی اولین جلسه شورای سیاست‌گذاری گواهی الکترونیکی کشور مورخ ۱۳۸۶/۰۷/۳۰ مجوز ایجاد، امضا، صدور، و ابطال گواهی الکترونیکی مراکز صدور گواهی میانی را دریافت کرده است. مرکز دولتی صدور گواهی الکترونیکی ریشه مسئول تمام ابعاد مدیریت مراکز صدور گواهی میانی، شامل نظارت بر فرایندهای ثبت‌نام، احراز هویت، صدور گواهی مراکز میانی، انتشار و ابطال گواهی‌ها و تجدید کلید می‌باشد. همچنین، تضمین تطابق تمام ابعاد خدمات و عملیات این مراکز با سیاست‌های زیرساخت کلید عمومی کشور، بر عهده مرکز صدور گواهی ریشه است.

[1] Certificate Authority (CA)
[2] Trust Point

۱-۳-۱-۲ مرکز صدور گواهی الکترونیکی میانی

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

مراکز صدور گواهی الکترونیکی میانی به‌منظور دریافت گواهی خود باید مطابق با سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور عمل کنند. همچنین، این مراکز باید توانایی مدیریت موارد زیر را دارا باشند:

- زیرساخت کلید عمومی
- فناوری امضای دیجیتال و صدور گواهی
- تعهدات و مسئولیت‌های مربوطه بین مراکز صدور گواهی، دفاتر ثبت‌نام، مالکان گواهی، و طرف‌های اعتمادکننده.

مرکز میانی پارس‌ساین یک مرکز صدور گواهی الکترونیکی میانی خصوصی می‌باشد. این مرکز طی پانزدهمین جلسه شورای سیاست‌گذاری گواهی الکترونیکی کشور مورخ ۱۳۹۰/۰۳/۲۴ مجوز تأسیس و طی جلسه شورای مذکور مورخ ۱۳۹۱/۰۴/۲۸ گواهی الکترونیکی خود را دریافت نموده است. مرکز میانی خصوصی پارس‌ساین گواهی‌های الکترونیکی برای اشخاص حقیقی و حقوقی صادر می‌نماید. این گواهی‌ها نام و مشخصات یک فرد یا سازمان را به یک کلید عمومی پیوند می‌دهند. این کلید عمومی در کاربردهایی مانند تصدیق امضای فرد یا سازمان مورد استفاده قرار می‌گیرد.

۱-۳-۲ دفاتر ثبت‌نام

دفتر ثبت‌نام[1] موجودیتی است که وظیفه احراز هویت و بررسی صحت اطلاعات دریافت‌شده از سوی درخواست‌کنندگان گواهی الکترونیکی را بر عهده دارد. در واقع دفتر ثبت‌نام با بررسی هویت درخواست‌کننده، وظیفه تنظیم درخواست‌های صدور گواهی، ابطال گواهی، و تمدید گواهی را بر عهده دارد. دفتر ثبت‌نام باید مورد تأیید مرکز صدور گواهی میانی باشد و یک گواهی توسط این مرکز برای آن صادر شده باشد.

1 Registration Authority (RA)

کلیه درخواست‌های تنظیم‌شده توسط دفاتر ثبت‌نام وابسته به مرکز میانی خصوصی پارس‌ساین، با استفاده از کلید خصوصی متناظر با گواهی الکترونیکی آن دفتر که توسط مرکز صدور گواهی الکترونیکی پارس‌ساین صادر شده، امضا می‌شوند. سپس، امضای کلیه درخواست‌های ارسال‌شده از سوی دفتر ثبت‌نام، توسط مرکز صدور گواهی خصوصی پارس‌ساین تصدیق می‌شوند. بدین ترتیب هویت موجودیت ارسال کننده درخواست و صحت محتویات درخواست احراز می‌گردد.

۱-۳-۳ مالکان گواهی[1]

مالک گواهی به موجودیتی گفته می‌شود که از مرکز میانی خصوصی پارس‌ساین، گواهی دریافت می‌کند و نام او به عنوان نام مالک گواهی ثبت می‌شود. هویت مالک گواهی قبل از صدور گواهی، توسط دفتر ثبت‌نام بررسی و احراز می‌شود.

مالک گواهی ممکن است یک شخص، یک سازمان و یا اجزای زیرساختی مثل دیواره آتش، سرویس‌دهنده مورد اعتماد[2] و یا هر ابزار دیگری باشد که در یک سازمان جهت برقراری ارتباط امن مورد استفاده قرار می‌گیرد.

۱-۳-۴ طرف‌های اعتمادکننده[3]

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

۱-۳-۵ اجزای دیگر

تعریف نشده است.

1 Subscriber
2 Trusted Server
3 Relying Parties

۱-۴ کاربردهای گواهی[1]

۱-۴-۱ مصارف مناسب گواهی

مرکز صدور گواهی خصوصی پارس‌ساین برای کاربردهای مختلف، گواهی‌های متناسب با این کاربردها را صادر می‌نماید. انواع گواهی‌های قابل صدور توسط مرکز صدور گواهی خصوصی پارس‌ساین منطبق با مصوبات شورای سیاست‌گذاری گواهی الکترونیکی کشور است. به تناسب انواع گواهی‌های تعریف شده توسط مرکز ریشه، کاربردهای مختلفی برای این گواهی‌ها در نظر گرفته شده است. انواع گواهی‌های قابل صدور توسط مرکز میانی خصوصی پارس‌ساین در جدول ۱-۳ نمایش داده شده است.

جدول ۱-۳ انواع مقاصد مورد استفاده گواهی

کاربرد / نوع گواهی	توضیحات
گواهی امضا	این گواهی جهت امضای اسناد و تراکنش‌های الکترونیکی و همچنین احراز هویت کاربران مورد استفاده قرار می‌گیرد.
گواهی پست الکترونیکی امن	این گواهی از طریق پروتکل S/MIME، امکان تأمین امنیت پست الکترونیکی را فراهم می‌سازد.
گواهی احراز هویت	این گواهی جهت احراز هویت مالکان گواهی جهت ورود به سیستم‌ها مورد استفاده قرار می‌گیرد. مثالی از این گواهی، گواهی MS SmartCard Logon می‌باشد که می‌تواند برای ورود به سیستم از طریق احراز هویت دوعاملی مبتنی بر کلید عمومی، در سیستم‌های متعلق به مایکروسافت مورد استفاده قرار گیرد. از طریق این گواهی می‌توان با استفاده از یک کارت هوشمند یا توکن عملیات ورود به سیستم (Logon) را انجام داد.
گواهی سرور	این گواهی به منظور تصدیق اصالت یک سرویس‌دهنده (Server) به کار می‌رود. همچنین با استفاده از این گواهی، یک ارتباط امن و رمزگذاری‌شده بین سرویس‌دهنده و سرویس‌گیرنده (Client) ایجاد می‌شود. دو نمونه از کاربردهای رایج این گواهی عبارتند از گواهی SSL/TLS در کاربرد HTTPS و گواهی Domain Controller؛ گواهی HTTPS به منظور تصدیق اصالت یک وب‌سایت به کار می‌رود. همچنین، با استفاده از این گواهی یک ارتباط امن و رمزگذاری‌شده بین برنامه مرورگر و وب‌سایت

1 Certificate Usage

	ایجاد می‌شود. گواهی Domain Controller نیز جهت ورود به سیستم در یک Domain و در سمت سرور (Domain Controller) مورد استفاده قرار می‌گیرد. سرور از این گواهی برای معرفی خود به سایر کامپیوترها جهت فراهم نمودن قابلیت MS Smart Card Logon استفاده می‌کند.
گواهی مهر سازمانی	این گواهی به عنوان گواهی امضای یک شرکت یا سازمان تلقی شده و می‌تواند به عنوان مهرسازمانی آن شرکت یا سازمان در قالب امضای دیجیتال مورد استفاده قرار گیرد.
گواهی Code Signing	این گواهی جهت اطمینان از اصالت و حفظ جامعیت نرم‌افزارهای مختلف به ویژه نرم‌افزارهایی که از طریق اینترنت منتشر می‌شوند نظیر Java Applet و ActiveX به‌کار می‌رود. بنابراین زمانی که کاربران نرم‌افزار امضا شده با کلید خصوصی متناظر با گواهی را دانلود می‌نمایند، می‌توانند نسبت به صحت محتوای منبع[1] و نیز جامعیت آن از طریق این گواهی مطمئن باشند.
گواهی دفتر ثبت‌نام (RA)	گواهی متعلق به دفاتر ثبت‌نام وابسته به مرکز میانی خصوصی پارس‌ساین که جهت امضای درخواست‌ها در سمت دفتر ثبت‌نام مورد استفاده قرار می‌گیرد.
گواهی OCSP Signing	گواهی متعلق به سرور پاسخگوی OCSP که جهت امضای پاسخ‌های OCSP تنظیم شده توسط این سرور، مورد استفاده قرار می‌گیرد.
گواهی مراکز مهر زمانی[2]	اصولاً مهر زمانی جهت ثبت دقیق زمان، هنگام امضای اسناد مختلف از جمله قراردادها و یا توافق‌نامه‌ها و بایگانی آن‌ها مورد استفاده قرار می‌گیرد. با استفاده از مهر زمانی، می‌توان به‌طور شفاف اثبات نمود که داده‌های متناظر با یک مهر زمانی، از زمان مشخص‌شده در مهر زمانی، تغییر داده نشده است. گواهی مهر زمانی جهت انجام عملیات امضا در فرایند مهر زمانی توسط مرکز مهر زمانی مورد استفاده قرار می‌گیرد.

۱-۴-۲ مصارف غیرمجاز گواهی

مصارف غیرمجاز گواهی به شرح زیر می‌باشد:

1 Source
2 Time Stamping Authority (TSA)

- گواهی‌ها نباید در حوزه‌ای که متناقض با قانون و مخالف با نظم عمومی باشد، مورد استفاده قرار گیرند. برای نمونه، نباید از گواهی امضای کد برای امضای دیجیتال کدهای مخرب استفاده شود.
- طبق سیاست‌های کنونی زیرساخت کلید عمومی کشور، نباید از گواهی الکترونیکی در سرویس‌های محرمانگی و رمزنگاری استفاده شود. در غیر این صورت، مرکز میانی خصوصی پارس‌ساین هیچ‌گونه تعهدی نسبت به عواقب ناشی از استفاده از گواهی در سرویس محرمانگی ندارد.
- از گواهی‌های الکترونیکی فقط باید در کاربرد(های) در نظر گرفته شده برای همان نوع گواهی که در بخش ۱-۴-۱ قید شده است، استفاده گردد.
- گواهی‌های صادرشده برای اشخاص و سرویس‌گیرندگان، جهت استفاده در برنامه‌های کاربردی سرویس‌گیرنده بوده و نباید به عنوان گواهی سرویس‌دهنده و یا گواهی سازمانی مورد استفاده قرار گیرد.
- گواهی مرکز صدور گواهی خصوصی پارس‌ساین نباید برای کاربردی غیر از حوزه عملیاتی مرکز صدور گواهی الکترونیکی به‌کار رود.
- گواهی موجودیت‌های نهایی نباید به عنوان گواهی مرکز صدور گواهی الکترونیکی به‌کار رود.

۱-۵ راهبری سیاست‌ها[1]

۱-۵-۱ سازمان راهبری سند

مرکز میانی خصوصی پارس‌ساین مسئولیت تدوین، اصلاح و بازنگری، و انتشار این سند را بر عهده دارد. این دستورالعمل تنها پس از دریافت مجوز از مرکز ریشه قابل اجرا می‌باشد. تنها مرجع مجاز برای تفسیر این سند مرکز صدور گواهی الکترونیکی پارس‌ساین بوده و این مرکز پاسخگوی هرگونه سؤال و ابهام در ارتباط با این سند، منطبق با اطلاعات تماس قید شده در بخش ۱-۵-۲ خواهد بود.

۱-۵-۲ اطلاعات تماس

سؤالات مربوط به این دستورالعمل، توسط مرکز میانی خصوصی پارس‌ساین پاسخ داده می‌شود. اطلاعات

1 Policy Administration

تماس با این مرکز در جدول ۱-۴ آمده است.

جدول ۱-۴ اطلاعات تماس مرکز میانی خصوصی پارس‌ساین

نشانی پایگاه وب	www.parssignca.ir
نشانی پست الکترونیکی	parssign@amnafzar.ir
شماره تلفن	(۰۲۱) ۶۱۹۷۵۵۰۰-۲۰
شماره فکس	(۰۲۱) ۶۶۰۹۰۲۹۹
نشانی	تهران، خیابان آزادی، خیابان حبیب‌الله، خیابان قاسمی غربی، شماره ۳۷، طبقه پنجم

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

شورای سیاست‌گذاری گواهی الکترونیکی کشور مسئولیت تأیید مطابقت این دستورالعمل اجرایی با سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور را بر اساس گزارش ارائه‌شده توسط مرکز ریشه بر عهده دارد. این دستورالعمل اجرایی تنها در صورت تأیید توسط مرکز ریشه و شورا قابل اجرا می‌باشد.

۱-۵-۴ فرایند تأیید دستورالعمل اجرایی

مرکز میانی خصوصی پارس‌ساین پس از ارائه درخواست رسمی و مدارک لازم به مرکز دولتی صدور گواهی الکترونیکی ریشه، دستورالعمل اجرایی گواهی (سند پیش رو) خود را که بر اساس استاندارد RFC3647 و منطبق با سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور تدوین نموده، به همراه اسناد و مدارک مرتبط دیگر به مرکز ریشه ارائه می‌نماید. بررسی‌های لازم در رابطه با این سند توسط مرکز ریشه صورت می‌گیرد. پس از مشخص شدن اشکالات و اصلاح آن‌ها توسط مرکز میانی خصوصی پارس‌ساین، سند مجدداً برای مرکز ریشه ارسال می‌شود. در صورت مورد تأیید قرار گرفتن سند دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی توسط مرکز ریشه، این سند به شورای سیاست‌گذاری ارائه شده و با تأیید نهایی شورا، مورد تأیید قرار می‌گیرد.

۱-۶ تعاریف و اختصارات

در جدول ۱-۵، لیستی از اختصارات استفاده شده در این سند به همراه معانی آن‌ها آورده شده است.

جدول ۱-۵ اختصارات

اختصار	لغت	معنی
CA	Certificate Authority	موجودیتی که مجاز به صدور، ابطال، تمدید، و به طور کلی مدیریت گواهی‌های الکترونیکی می‌باشد.
CP	Certificate Policy	مجموعه‌ای از قوانین که الزامات و سیاست‌های زیرساخت کلید عمومی را مشخص می‌کند.
CPS	Certificate Practice Statement	دستورالعمل اجرایی برای صدور، ابطال، و مدیریت گواهی که توسط مرکز میانی منتشر می‌شود و درخواست‌کنندگان گواهی، مالکان گواهی، طرف‌های اعتمادکننده، و دفاتر ثبت‌نام وابسته به آن مرکز، ملزم به پیروی از آن هستند.
CRL	Certificate Revocation List	یک ساختار داده حاوی لیستی از گواهی‌های الکترونیکی است که پیش از سررسید تاریخ انقضای آن‌ها باطل‌شده و معتبر محسوب نمی‌شوند.
CSR	Certificate Signing Request	یک قالب تراکنشی تعریف شده توسط استاندارد PKCS#10، حاوی نام متمایز و تعدادی مشخصه اختیاری و کلید عمومی می‌باشد که توسط موجودیت درخواست‌کننده گواهی الکترونیکی به طور الکترونیکی امضا شده و به مرکز صدور گواهی فرستاده می‌شود. سپس مرکز صدور گواهی، گواهی X.509 متناظر با آن CSR را صادر می‌نماید.
DN	Distinguished Name	یک شناسه منحصر به فرد که با استفاده از آن می‌توان در یک درخت اطلاعاتی دایرکتوری (DIT) با قالب X.500، یک شی را شناسایی کرد.
FIPS	Federal Information Processing Standard	راهنمایی‌های تخصصی که موسسه ملی استانداردها و تکنولوژی آمریکا برای تهیه تجهیزات سیستم‌ها و سرویس‌های پردازش اطلاعات تدوین کرده است.
IETF	Internet Engineering Task Force	IETF جامعه بین‌المللی بزرگی از طراحان شبکه، اپراتورها، فروشندگان، و محققان مرتبط با سیر تکاملی معماری اینترنت و کارکرد روان و دقیق اینترنت است.

OCSP	Online Certificate Status Protocol	پروتکلی مبتنی بر درخواست و پاسخ است که جهت اعلام برخط وضعیت ابطال یا اعتبار گواهی X.509 به‌کار می‌رود.
OID	Object Identifier	شناسه‌ای منحصر به فرد و رسمی، تشکیل شده از مجموعه‌ای از اعداد (تعریف شده در استاندارد ASN.1) که برای اشاره به اشیا با ویژگی‌های مشخص استفاده می‌شود.
PKCS#10	Public Key Cryptography Standard	استاندارد رمزنگاری کلید عمومی شماره ۱۰ که یک ساختار برای درخواست گواهی الکترونیکی تعریف می‌کند. درخواست PKCS#10 دارای نام متمایز، کلید عمومی، و دیگر اطلاعات مورد نیاز برای درخواست گواهی می‌باشد. این درخواست توسط موجودیت درخواست‌کننده گواهی به طور الکترونیکی امضا می‌شود.
PKI	Public Key Infrastructure	به مجموعه‌ای از خدمات، محصولات، سیاست‌ها، فرایندها، و سیستم‌های نرم‌افزاری و سخت‌افزاری گفته می‌شود که جهت مدیریت و به‌کارگیری گواهی‌های الکترونیکی و به‌منظور ارائه سرویس‌های امنیتی مختلف مبتنی بر رمزنگاری کلید عمومی[1] مورد استفاده قرار می‌گیرد.
PKIX	Public Key Infrastructure (X.509)	گروه PKIX در سال ۱۹۹۵ با هدف توسعه استانداردهای اینترنت برای پشتیبانی از زیرساخت‌های کلید عمومی مبتنی بر گواهی الکترونیکی X.509، تأسیس شد.
RA	Registration Authority	یک موجودیت اختیاری در زیرساخت کلید عمومی می‌باشد که وظایفی از قبیل ثبت درخواست‌های مرتبط با گواهی الکترونیکی (از جمله صدور گواهی)، احراز هویت درخواست‌کنندگان و دریافت و بررسی صحت مدارک و اطلاعات مورد نیاز از آن‌ها را بر عهده دارد.
RFC	Request For Comment	توافق‌نامه منتشر شده توسط IETF در توصیف روش، رفتار، پژوهش، و یا نوآوری برای کار با اینترنت و سیستم‌های متصل به اینترنت می‌باشد.
RSA	RSA	الگوریتم رمزنگاری کلید عمومی که در سال ۱۹۷۸ توسط سه نفر با نام‌های ران ریوست، ادی شامیر، و لئونارد آدلمن اختراع شده است.
SSL	Secure Socket Layer	یک پروتکل اینترنتی که از رمزنگاری برای فراهم کردن سرویس محرمانگی و تمامیت اطلاعات برای ترافیک بین سرویس‌گیرنده و سرویس‌دهنده

[1] Public Key Cryptography

		استفاده می‌کند و به صورت اختیاری احراز هویت موجودیت‌ها را بین سرویس‌گیرنده و سرویس‌دهنده انجام می‌دهد.
URL	Uniform Resource Locator	رشته‌ای از کاراکترها است که مکان منبعی که در اینترنت قابل دسترس است را مشخص می‌کند.
X.500	X.500	مجموعه‌ای از استانداردهای ارائه شده توسط اتحادیه ارتباطات بین‌المللی (ITU-T) و سازمان استاندارد جهانی (ISO) است که جزئیات «سرویس دایرکتوری» را توصیف می‌کند.
X.501	X.501	استانداردی در مجموعه استانداردهای سری X.500 است. یک موجودیت شبکه مثل مسیریاب ممکن است به شناسه X.501 برای استفاده از سرویس دایرکتوری LDAP و یا تولید درخواست‌های گواهی PKCS نیاز داشته باشد.
X.509	X.509	استانداردی در مجموعه استانداردهای سری X.500 است که برای احراز هویت در مجموعه سیستم دایرکتوری تعریف شده است در حالی که اکنون خارج از سیستم دایرکتوری، موفق‌ترین استاندارد برای صدور گواهی‌های الکترونیکی به شمار می‌رود.

در جدول ۱-۶، لیستی از اصطلاحات استفاده شده در این سند و تعاریف آن‌ها آورده شده است.

جدول ۱-۶ اصطلاحات و تعاریف آن‌ها

لغت	معادل انگلیسی	تعریف
ابطال گواهی	Certificate Revocation	اعلام این‌که یک گواهی الکترونیکی معتبری که توسط یک مرکز صدور گواهی الکترونیکی صادر شده، با وجود این‌که دارای مهلت اعتبار می‌باشد، توسط مرکز صدور گواهی باطل شده و معتبر محسوب نمی‌شود.
احراز هویت	Authentication	فرایند شناسایی هویتی که توسط یک شخص یا برای یک موجودیت سیستمی ادعا شده است.
احراز هویت بایومتریک	Biometric Authentication	احراز هویت الکترونیکی اشخاص بر اساس مشخصات فیزیکی آن‌ها مثل اثر انگشت و غیره.
مجازشماری	Authorization	مکانیزمی که بر اساس آن مشخص می‌شود موجودیتی که هویت واقعی آن احراز شده، مجوز انجام چه کارها و عملیاتی را دارد.

اطلاعات فعال‌ساز	Activation data	اطلاعاتی خصوصی (غیر از کلیدها) که برای دسترسی به ماژول‌های رمزنگاری مورد نیاز هستند.
اطمینان	Assurance	مشخصه‌ای از سیستم اطلاعاتی که اطمینان می‌دهد سیستم مطابق با سیاست‌های امنیتی کار می‌کند.
اعتبار	Authenticity	اصل، قابل اطمینان، و قابل تشخیص بودن.
اعتبار گواهی	Validity of certificate	یک واحد داده در گواهی الکترونیکی که بازه زمانی اعتبار گواهی را مشخص می‌کند.
امحا	Zeroize	روشی برای پاک کردن الکترونیکی اطلاعات ذخیره‌شده با تغییر محتویات مخزن اطلاعات است به طوری که از بازیابی اطلاعات جلوگیری شود.
امضای دیجیتال	Digital signature	چکیده اطلاعات یک سند الکترونیکی، رشته‌ای است که به روش خاصی از متن آن سند استخراج می‌شود. حاصل رمزگذاری این رشته با کلید خصوصی صاحب سند، امضا نامیده می‌شود که به اصل سند ضمیمه و ارسال می‌شود به گونه‌ای که با استفاده از آن، گیرنده سند می‌تواند منبع و تمامیت محتویات سند را تشخیص دهد.
امنیت	Security	اقداماتی که برای حفاظت از محرمانگی، تمامیت، و دسترس‌پذیری یک سیستم انجام می‌شوند.
انقضای گواهی	Certificate Expiration	عدم اعتبار گواهی به دلیل پایان طول عمر تخصیص یافته به آن گواهی.
انکارناپذیری	Non-repudiation	مجموعه مکانیزم‌هایی که به پیام‌ها و تراکنش‌ها پشتوانه حقوقی می‌بخشد و با استفاده از آن، فرستنده نمی‌تواند به هر طریق ارسال پیام خود را انکار کند و گیرنده نیز نمی‌تواند منکر دریافت پیام شود.
بازرسی تطابق	Compliance Audit	بررسی و بازبینی مستقل اسناد و فعالیت‌های سیستم برای تشخیص کفایت کنترل‌های سیستم، اطمینان از مطابقت با دستورالعمل اجرایی و روال‌های آن، شناسایی نقص در سرویس صدور گواهی و پیشنهاد تغییرات به منظور اقدام متقابل.

بازیابی کلید	Key Recovery	فرایند به دست آوردن مقدار یک کلید رمزنگاری که قبلاً برای انجام عملیات رمزنگاری استفاده می‌شد.
بایگانی	Archive	مجموعه‌ای از اطلاعات که برای مدت زمان خاصی برای مقاصدی مانند پشتیبانی سرویس ثبت رویدادها و سرویس تمامیت سیستم ذخیره می‌شوند.
بررسی صحت هویت	Identity Verification	بررسی صحت اطلاعاتی که برای اثبات یک هویت ادعا شده ارائه شده است.
پاسخگوی OCSP	OCSP Responder	سرویس‌دهنده‌ای که وضعیت ابطال یا اعتبار گواهی X.509 را به صورت برخط اعلام می‌نماید. ماهیت پروتکل OCSP مبتنی بر درخواست و پاسخ است.
پروتکل اعلام بر خط وضعیت گواهی‌ها	Online Certificate Status Protocol	یک پروتکل اینترنتی که با استفاده از آن، سرویس‌گیرنده می‌تواند وضعیت اعتبار گواهی الکترونیکی و اطلاعات مرتبط را از سرویس دهنده دریافت کند.
پیکربندی	Configuration	تنظیمات نرم‌افزاری و سخت‌افزاری سیستم‌های رایانه‌ای.
تجدید کلید گواهی	Certificate Rekey	فرایند تجدید کلید عمومی گواهی الکترونیکی موجود با صدور یک گواهی جدید با اطلاعات همسان با گواهی قبلی اما با یک کلید عمومی و شماره سریال جدید، و احتمالاً یک بازه اعتبار جدید.
ترمیم خرابی	Disaster Recovery	فرایندی که کلیه اطلاعات از دست رفته و سرویس‌های مختل‌شده در زمان وقوع آتش، تخریب، حوادث طبیعی، یا خرابی سیستم را بازیابی می‌کند.
تعلیق گواهی	Certificate Suspension	عدم اعتبار موقت گواهی الکترونیکی.
تمامیت	Integrity	مجموعه مکانیزم‌هایی که از هرگونه تغییر، تکرار یا حذف غیرمجاز اطلاعات یک پیام جلوگیری می‌کنند و یا حداقل باعث کشف چنین اقداماتی می‌شوند.
تمدید گواهی	Certificate Renewal	فرایند تمدید اعتبار گواهی الکترونیکی با صدور یک گواهی جدید همسان به گواهی قبلی اما با بازه اعتبار و شماره سریال متفاوت.
توکن	Token	یک رسانه الکترونیکی قابل حمل جهت نگهداری ایمن زوج‌کلید رمزنگاری و مقادیر مربوط به شناسایی و انجام محاسبات مرتبط به

		آن‌ها (به عنوان مثال عملیات رمزنگاری مختلف) می‌باشد.
تولید کلید	Key Generation	فرایند تولید کلیدهای رمزنگاری
ثبت‌نام	Registeration	یک اقدام یا فرایند اجرایی برای ثبت اولیه نام و مشخصه‌های دیگر یک موجودیت در دفتر ثبت‌نام (پیش از صدور گواهی الکترونیکی).
الحاقیه‌های گواهی	Certificate Extensions	اطلاعاتی که برای افزودن مشخصات اضافی به گواهی X.509 V3 تعریف شده‌اند.
حق مالکیت معنوی	Intellectual Property Right	حق کنترل و ایجاد مزایا نسبت به آنچه اختراع، اکتشاف، یا ایجاد شده است.
در خطر افشا قرار گرفتن	To be Compromised	یک حادثه امنیتی که تحت آن اطلاعات محرمانه در معرض دسترسی غیرمجاز قرار می‌گیرند.
درخواست گواهی	Certificate Request	درخواست صدور گواهی که توسط متقاضی به دفتر ثبت‌نام ارائه می‌شود.
دسترسی	Access	فراهم بودن امکان ارتباط با سیستم به منظور استفاده از منابع سیستم جهت کنترل اطلاعات یا به دست آوردن اطلاعات موجود در سیستم.
دسترس‌پذیری	Availability	امکان دسترسی به اطلاعات توسط شخص مجاز و در زمان لازم.
دستورالعمل اجرایی گواهی الکترونیکی	Certificate Practice Statement	دستورالعمل اجرایی برای صدور، ابطال، و به طور کلی مدیریت گواهی الکترونیکی که توسط مرکز صدور گواهی منتشر می‌شود و درخواست‌کنندگان گواهی، مالکان گواهی، طرف‌های اعتمادکننده، و دفاتر ثبت‌نام آن مرکز ملزم به پیروی از آن هستند.
دستیابی قانونی به کلید	Key Escrow	تکنیک بازیابی کلید به منظور ذخیره اطلاعات کلید رمزنگاری با مسئولیت شخص سومی (مسئول دستیابی قانونی) به منظور بازیابی کلید و استفاده از آن در شرایط خاص.
دفتر ثبت‌نام	Registration Authority	یک موجودیت اختیاری در زیرساخت کلید عمومی می‌باشد که وظایفی از قبیل ثبت درخواست‌های مرتبط با گواهی الکترونیکی (مثل صدور گواهی)، احراز هویت درخواست‌کنندگان و دریافت و بررسی صحت مدارک و اطلاعات مورد نیاز از آن‌ها را بر عهده

		دارد.
دیواره آتش	Firewall	یک اتصال بین شبکه‌ای که ترافیک شبکه را کنترل می‌کند و منابع سیستمی شبکه را در مقابل تهدیدهای شبکه‌ای محافظت می‌کند.
زنجیره گواهی	Certification path	زنجیره منظمی از گواهی‌های الکترونیکی که به طرف اعتمادکننده توانایی ارزیابی صحت امضا و جعلی نبودن آخرین گواهی این زنجیره را می‌دهد.
زوج‌کلید	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 به‌دست آوردن کلید خصوصی از کلید عمومی وجود نداشته باشد.
زیرساخت کلید عمومی	Public Key Infastructure	به مجموعه‌ای از خدمات، محصولات، سیاست‌ها، فرآیندها و سیستم‌های نرم‌افزاری و سخت‌افزاری گفته می‌شود که جهت مدیریت و به‌کارگیری گواهی‌های الکترونیکی و به منظور ارائه سرویس‌های امنیتی مختلف مبتنی بر رمزنگاری کلید عمومی مورد استفاده قرار می‌گیرد.
سرویس‌دهنده	Server	یک موجودیت سیستمی که در جواب درخواست‌های موجودیت‌های سیستمی دیگر به نام سرویس‌گیرنده (کلاینت)، سرویس فراهم می‌کند.
سطح اطمینان گواهی	Certificate Assurance Level	میزان اطمینانی که می‌توان به پیوند بین اطلاعات مالک گواهی با کلید عمومی آن گواهی داشت، با استفاده از معیاری به نام سطح اطمینان گواهی مشخص می‌شود. این معیار، همچنین نشان‌دهنده میزان امنیت لحاظ‌شده در فرایند تولید گواهی و زوج‌کلید مرتبط با آن، و استفاده از کلید خصوصی متناظر با کلید عمومی مالک گواهی می‌باشد.
سیاست‌های گواهی	Certificate Policies	مجموعه‌ای از قوانین که الزامات و سیاست‌های زیر ساخت کلید عمومی را مشخص می‌کند.
سیستم‌عامل	Operating System	نرم‌افزاری که عملیات اساسی سیستم (مانند مدیریت منابع رایانه، اجرای برنامه‌های کاربردی، فراهم نمودن سیستم فایل) را انجام

		می‌دهد.
شماره سریال	Serial Number	یک مقدار عددی که توسط صادرکننده گواهی در گواهی درج می‌شود و بین تمام گواهی‌های تولیدشده توسط صادرکننده گواهی، منحصر به فرد می‌باشد.
شناسایی	Identification	شناسایی و تشخیص یک موجودیت از موجودیت‌های دیگر، از طریق بررسی مدارک شناسایی اشخاص و اطلاعات شناسایی دیگر از قبیل گذرواژه، اطلاعات بایومتریک و غیره.
شناسه شی	Object Identifier	نامی منحصر به فرد و رسمی، تشکیل شده از مجموعه‌ای از اعداد (تخصیص یافته توسط استاندارد ASN.1) که برای اشاره به اشیا با ویژگی‌های مشخص (مانند الگوریتم‌های رمزنگاری، سیاست‌های گواهی الکترونیکی و غیره) استفاده می‌شود.
شناسه سیاست گواهی الکترونیکی	Policy Object Identifier (POID)	شناسه‌ای منحصر به فرد و رسمی، تشکیل شده از مجموعه‌ای از اعداد (تخصیص یافته توسط استاندارد ASN.1) که برای اشاره به سیاست‌های گواهی الکترونیکی متعلق به یک مرکز صدور گواهی الکترونیکی به‌کار می‌رود.
طرف اعتمادکننده	Relying Party	فرد یا موجودیتی است که به پیوند اطلاعات مالک گواهی الکترونیکی با کلید عمومی آن گواهی اعتماد می‌کند. در اینجا منظور از گواهی، گواهی موجودیت دیگری است که طرف اعتمادکننده از آن برای عملیاتی مثل تصدیق و بررسی تمامیت یک پیام امضاشده الکترونیکی، شناسایی ایجادکننده پیام، یا برقراری ارتباطات محرمانه با آن موجودیت استفاده می‌کند.
طول کلید	Key Length	تعداد علائم مورد نیاز (معمولاً در قالب بیت) برای نمایش مقدار یک کلید رمزنگاری.
علامت تجاری	Trade Mark	علامت ثبت‌شده رسمی توسط یک تولیدکننده برای متمایز کردن محصولات خود از محصولات تولید شده توسط اشخاص یا تولیدکننده‌های دیگر.
فیلد	Field	بخشی از گواهی که محتوای 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، حافظه و واسط ورودی/ خروجی را به عهده دارد.
کانال	Channel	مسیر انتقال اطلاعات در یک سیستم.
گذرواژه	Password	اطلاعات احراز هویت محرمانه که معمولاً از رشته‌ای از کاراکترها تشکیل می‌شود.
گواهی امضا	Signature Certificate	یک گواهی الکترونیکی، حاوی یک کلید عمومی که از آن جهت امضای دیجیتال اسناد و داده‌ها و تصدیق امضای دیجیتال استفاده می‌شود.
گواهی الکترونیکی	Digital Certificate	یک ساختار داده الکترونیکی که بر اساس محتوای آن، یک امضای دیجیتال در آن قرار می‌گیرد و برای پیوند دادن نام و مشخصات یک موجودیت به کلید عمومی او مورد استفاده قرار می‌گیرد.
گواهی مورد اعتماد	Trusted Certificate	یک گواهی که طرف‌های اعتمادکننده به اعتبار آن بدون نیاز به ارزیابی صحت اطلاعات آن، اعتماد می‌کنند. به خصوص گواهی الکترونیکی که برای فراهم کردن اولین کلید عمومی گواهی در زنجیره گواهی استفاده می‌شود. برای مثال، در زیرساخت کلید عمومی کشور، گواهی مرکز دولتی صدور گواهی الکترونیکی ریشه، یک گواهی مورد اعتماد است.
گواهی میانی	Intermediate Certificate	گواهی مرکز صدور گواهی الکترونیکی میانی که توسط مرکز دولتی صدور گواهی الکترونیکی ریشه امضا می‌شود و به مرکز صدور گواهی میانی اجازه صدور گواهی برای مالکان گواهی را می‌دهد. برای مثال، گواهی مرکز صدور گواهی الکترونیکی پارس‌ساین، یک گواهی از این نوع است.
الگوریتم	Algorithm	مجموعه متناهی از دستورالعمل‌های گام به گام برای حل کردن مسأله‌ها و روال‌های محاسباتی، به خصوص روال‌هایی که توسط رایانه اجرا می‌شوند.
الگوریتم رمزنگاری	Asymmetric Encryption Algorithm	یک الگوریتم رمزنگاری که در آن از یک کلید برای رمزنگاری و از یک کلید دیگر (متفاوت با کلید رمزنگاری) برای رمزگشایی استفاده

نامتقارن		می‌شود.
لیست گواهی‌های باطل شده	Certificate Revocation List	یک ساختار داده حاوی لیستی از گواهی‌های الکترونیکی است که پیش از منقضی شدن آن‌ها، توسط صادرکننده گواهی باطل شده و معتبر محسوب نمی‌شوند.
ماژول امنیتی سخت‌افزاری	Hardware Security Module (HSM)	نوعی ماژول سخت‌افزاری امن که امکان نگهداری امن کلیدهای رمزنگاری و اجرای ایمن و سریع عملیات رمزنگاری با کارایی مطلوب را فراهم می‌آورد.
مالک گواهی	Subscriber	موجودیتی که برای وی گواهی الکترونیکی صادر شده است و می‌تواند از کلید خصوصی مرتبط با کلید عمومی درون گواهی استفاده کند.
مأمور امنیتی PKI	PKI Security Officer	فردی که مسئولیت بررسی و تفویض مجوز دسترسی به سیستم‌ها و اطلاعات امنیتی حساس و به طور کلی کنترل امنیت را بر عهده دارد.
محرمانگی	Confidentiality	غیرقابل مشاهده بودن اطلاعات برای اشخاص، موجودیت‌ها، یا فرایندهای غیرمجاز.
مخزن	Repository	محل ذخیره و انتشار گواهی‌های الکترونیکی و اطلاعات مربوط به آن‌ها مانند لیست گواهی‌های باطل شده، سند دستورالعمل اجرایی گواهی الکترونیکی، و غیره.
مدیریت کلید	Key Management	فرایند تولید، انتشار، تبادل، و ذخیره‌سازی امن کلیدها و کنترل دسترسی به آن‌ها در طول عمر کلید می‌باشد.
مرکز دولتی صدور گواهی الکترونیکی ریشه	IR Governmental Root CA	یک مرکز صدور گواهی الکترونیکی که مستقیماً مورد اطمینان موجودیت‌های نهایی است. مرکز دولتی صدور گواهی الکترونیکی ریشه، نقطه اطمینان در زیرساخت کلید عمومی کشور می‌باشد. این مرکز بر اساس مفاد بند الف از ماده ۴ آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و طی اولین جلسه شورای سیاست‌گذاری گواهی الکترونیکی کشور مورخ ۱۳۸۶/۰۷/۳۰ مجوز ایجاد، امضا، صدور و ابطال گواهی الکترونیکی مراکز صدور گواهی میانی را دریافت کرده است.

مرکز صدور گواهی	Certificate Authority	موجودیتی که وظیفه صدور و مدیریت گواهی‌های الکترونیکی را بر عهده دارد و پیوند بین اطلاعات گواهی و مالک گواهی را ضمانت می‌کند.
مرکز صدور گواهی میانی	Subordinate CA	یک مرکز صدور گواهی که گواهی خود را از مرکز دولتی صدور گواهی ریشه دریافت می‌کند و می‌تواند برای مالکان گواهی، گواهی صادر کند.
مسیریاب	Router	یک سیستم شبکه‌ای که بسته‌های پروتکل اینترنت را که مقصد آن‌ها خود سیستم نیست به بیرون از شبکه هدایت می‌کند.
سرویس‌گیرنده	Client	یک موجودیت سیستمی که از موجودیت سیستمی دیگری که سرویس‌دهنده نامیده می‌شود درخواست سرویس کرده و از این سرویس استفاده می‌کند.
مکانیسم m از n	m out of n mechanism	تقسیم یک وظیفه بین n موجودیت به گونه‌ای که هر تعداد کمتر از m نفر نتوانند کل وظیفه را انجام دهند و برای انجام وظیفه، حداقل حضور m نفر از آن n نفر لازم می‌باشد (m<n).
موجودیت نهایی	End entity	موجودیتی که از کلیدها و گواهی‌ها برای ایجاد یا تشخیص صحت امضا یا محرمانگی آن استفاده می‌کند. در واقع، موجودیت‌های نهایی می‌توانند مالکان گواهی، سازمان‌ها، یا طرف‌های اعتماد کننده باشند.
مهر زمانی	Time stamp	امضای دیجیتالی که دارای تاریخ و ساعت می‌باشد و اطمینان می‌دهد که محتویات داده‌های امضاشده، در زمان مشخصی امضا شده‌اند.
نام متمایز	Distinguished Name	یک شناسه منحصر به فرد که با استفاده از آن می‌توان در یک درخت اطلاعاتی دایرکتوری (DIT) با قالب X.500 ، یک شی را شناسایی کرد.
نام مالک گواهی	Subject Name	نامی که به دارنده گواهی اختصاص داده شده است که می‌تواند یک شخص باشد یا وسایل و تجهیزاتی که گواهی را مورد استفاده قرار می‌دهند. در رابطه با گواهی‌های سازمانی، نامی که توصیف کننده سازمان می‌باشد.

پشتیبان	Backup	یک کپی از فایل‌ها، اطلاعات و برنامه‌هایی که برای بازیابی اطلاعات استفاده می‌شوند.
ورود به سیستم	Login/Logon	دسترسی یک موجودیت سیستمی به منابع سیستم، که معمولاً از طریق فراهم کردن نام کاربری و گذرواژه برای سیستم کنترل دسترسی که کاربران را احراز هویت می‌کند، انجام می‌شود.
ورودی	Entry	اطلاعات واردشده در مستندات، نرم‌افزارهای کاربردی، و پایگاه داده‌ها.
هویت	Identity	مجموعه ای از مشخصات محسوس و نامحسوس یک موجودیت که آن را از دیگر موجودیت‌ها متمایز می‌کند.

۲ انتشار و وظایف مخزن

۲-۱ مخزن

مرکز میانی خصوصی پارس‌ساین، مسئول مخزن متعلق به مرکز صدور گواهی خود می‌باشد. گواهی‌های صادرشده توسط مرکز صدور گواهی خصوصی پارس‌ساین در مخزن نگهداری می‌شوند. مرکز صدور گواهی خصوصی پارس‌ساین همچنین لیست گواهی‌های باطل‌شده (CRL) را در مخزن قرار می‌دهد. به علاوه، آخرین نسخه از این دستورالعمل اجرایی پس از تأیید توسط مرکز دولتی صدور گواهی ریشه در مخزن قرار می‌گیرد. برای دسترسی به مخزن، به نشانی اینترنتی www.parssignca.ir مراجعه شود.

۲-۲ انتشار اطلاعات گواهی

مرکز میانی خصوصی پارس‌ساین حداقل اطلاعات زیر را از طریق مخزن منتشر می‌کند تا در دسترس مالکان گواهی و طرف‌های اعتمادکننده قرار گیرد:

- کلیه گواهی‌های صادرشده توسط مرکز صدور گواهی خصوصی پارس‌ساین؛
- آخرین نسخه منتشرشده CRL؛
- گواهی‌های مرکز صدور گواهی خصوصی پارس‌ساین که توسط مرکز دولتی صدور گواهی ریشه صادر شده است؛
- آخرین نسخه از سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور (CP)؛
- آخرین نسخه از این دستورالعمل اجرایی گواهی الکترونیکی (CPS)؛
- توافق‌نامه با مالک گواهی؛
- توافق‌نامه با طرف‌های اعتمادکننده.

۲-۳ زمان یا تناوب انتشار

زمان‌بندی و تناوب انتشار گواهی‌های مالکان گواهی، لیست گواهی‌های باطل‌شده، و نسخه‌های به‌روز شده سند جاری توسط مرکز میانی خصوصی پارس‌ساین به صورت زیر می‌باشد:

- گواهی‌های متقاضیان گواهی پس از صدور، در مخزن منتشر می‌شوند.
- مرکز صدور گواهی خصوصی پارس‌ساین، CRL را حتی اگر هیچ تغییر یا به‌روزرسانی در آن انجام نشده باشد، در تناوب‌های خاصی که در بخش ۴-۹-۷ ذکر شده، منتشر می‌نماید. در صورتی که دلیل ابطال یک گواهی افشای کلید خصوصی باشد، بلافاصله پس از ابطال گواهی، یک نسخه به‌روز شده CRL صادر می‌شود.
- هر نسخه به‌روز شده از این دستورالعمل، پس از تأیید توسط مرکز دولتی صدور گواهی ریشه منتشر می‌گردد.

۲-۴ کنترل دسترسی به مخازن

اطلاعات منتشرشده در بخش مخزن سایت مرکز میانی خصوصی پارس‌ساین برای عموم به صورت فقط خواندنی[1] قابل دسترسی است. مرکز میانی خصوصی پارس‌ساین تدابیر امنیتی خاصی را جهت جلوگیری از اضافه کردن، پاک کردن، و تغییر در محتویات مخزن توسط افراد غیرمجاز اندیشیده است.

اعمال هرگونه تغییر روی مخزن فقط توسط نقش‌های قابل اطمینان (بخش ۵-۲-۱) که توسط مرکز میانی خصوصی پارس‌ساین تأیید صلاحیت شده‌اند، صورت می‌گیرد. این افراد جهت دسترسی به مخزن توسط سیستم‌عامل و برنامه کاربردی مخزن احراز هویت می‌شوند. همچنین، جهت حفظ امنیت، ارتباط بین مرکز صدور گواهی و مخزن به صورت امن و با استفاده از پروتکل SSL می‌باشد.

1 Read Only

۳ شناسایی و احراز هویت

۳-۱ نام‌گذاری

هر موجودیت مالک گواهی، طبق PKIX Part1، یک نام کاملاً متمایز و یکتا به فرم استاندارد X.501 در فیلدهای «نام مالک گواهی[1]» و «نام صادرکننده گواهی[2]» دارد که به صورت نام ترکیبی[3] هستند. در این بخش به نحوه نام‌گذاری و شناسایی مالکان گواهی پرداخته شده است. الزامات نام‌گذاری برای تمامی انواع یا کاربردهای گواهی الکترونیکی به طور کامل در «سند جامع پروفایل‌های زیرساخت کلید عمومی کشور» تشریح شده است.

۳-۱-۱ انواع نام‌ها

الزامات نام‌گذاری که در گواهی‌های صادرشده توسط مرکز میانی خصوصی پارس‌ساین رعایت می‌شود در جدول ۳-۱ آمده است:

جدول ۳-۱ الزامات نام‌گذاری

سطح اطمینان	الزامات
سطوح ۱ و ۲	• هر موجودیت یک نام کاملاً متمایز و یکتا به فرم استاندارد X.501 در فیلدهای "Subject" و "Issuer" دارد. • می‌تواند با استفاده از فیلد الحاقی "subjectAltName"، نام اختیاری در قالب دیگری برای موجودیت تعیین شود. • نام ترکیبی (DN)، به فرم یک رشته قابل چاپ X.501 در گواهی ثبت شده و دارای مقدار است.

1 Subject Name
2 Issuer Name
3 Distinguished Name

۳-۱-۲ نیاز به نام‌های بامعنی

الزامات بامعنی بودن نام‌ها در گواهی‌هایی که توسط مرکز میانی خصوصی پارس‌ساین صادر می‌شوند، در جدول ۳-۲ آمده است:

جدول ۳-۲ نیاز به نام‌های بامعنی

سطح اطمینان	الزامات
سطح ۱	با توجه به اینکه هویت مالکان گواهی توسط مرکز صدور گواهی یا دفتر ثبت‌نام بررسی نمی‌گردد، لزوماً نیاز به استفاده از نام‌های بامعنی و قابل فهم نمی‌باشد، مگر آنکه فرایند شناسایی توسط یک ارگان یا سازمان به صورت مستقل از مرکز صدور گواهی انجام شود.
سطح ۲	از نام‌های بامعنی و قابل فهم استفاده می‌گردد. همچنین محتوای فیلد مالک گواهی (Subject) و صادرکننده (Issuer) با نام شناسایی موجودیت مرتبط می‌باشد. ضمن این‌که فیلدهای مذکور، منطبق با سند جامع پروفایل‌های زیرساخت کلید عمومی کشور مقداردهی می‌گردد.

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

در مرکز میانی خصوصی پارس‌ساین برای گواهی‌های سطح ۲، از نام‌های مستعار و غیر واقعی استفاده نمی‌شود. با توجه به اینکه هویت مالکان گواهی سطح ۱ توسط مرکز صدور گواهی یا دفتر ثبت‌نام بررسی نمی‌گردد، برای این سطح چنین محدودیتی وجود ندارد.

۳-۱-۴ قواعد تفسیر قالب‌های مختلف نام‌ها

تعریف نشده است.

۳-۱-۵ یکتایی نام‌ها

یکتایی نام در مرکز میانی خصوصی پارس‌ساین رعایت می‌شود. مرکز صدور گواهی پارس‌ساین از نام‌های ترکیبی X.501 مورد تایید شورای سیاست‌گذاری، استفاده می‌نماید. مرکز صدور گواهی پارس‌ساین از شماره سریال یا اطلاعات دیگری برای حفظ یکتایی نام ترکیبی استفاده می‌کند.

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

مرکز میانی خصوصی پارس‌ساین در صورت اطلاع، برای نامی که یک دادگاه قانونی آن را سوءاستفاده از علامت تجاری یک سازمان تشخیص داده است، گواهی صادر نمی‌کند.

متقاضیان گواهی نباید در درخواست‌های گواهی خود از نام‌هایی استفاده کنند که حقوق مالکیت معنوی دیگران را نقض کند. مرکز میانی خصوصی پارس‌ساین هیچ مسئولیتی جهت بررسی و تصدیق حق مالکیت معنوی نامی که در درخواست گواهی آمده است، ندارد. همچنین این مرکز مسئول داوری و حل و فصل اختلافات پیش‌آمده مربوط به مالکیت نام دامنه، نام تجاری، علامت تجاری یا نام سرویس نمی‌باشد.

۳-۲ هویت‌شناسی اولیه

۳-۲-۱ روش اثبات مالکیت کلید خصوصی

از آن جایی که عملیات تولید کلید به طور معمول توسط درخواست‌کننده گواهی صورت می‌گیرد، تناظر کلید خصوصی و کلید عمومی متقاضی گواهی باید برای مرکز میانی ثابت شود. روش اثبات مالکیت کلید خصوصی در مرکز میانی خصوصی پارس‌ساین در جدول ۳-۳ آمده است.

جدول ۳-۳ روش اثبات مالکیت کلید خصوصی

سطح اطمینان	الزامات
سطح ۱	اثبات مالکیت کلید خصوصی مورد نیاز نمی‌باشد.
سطح ۲	قبل از صدور گواهی، مالکیت کلید خصوصی کاربران نهایی باید برای مرکز میانی خصوصی پارس‌ساین ثابت شود. روش اثبات مالکیت کلید خصوصی در مرکز میانی خصوصی پارس‌ساین، استفاده از استاندارد PKCS#10 جهت ایجاد یک «درخواست امضای گواهی[1]» از سوی درخواست‌کننده گواهی می‌باشد. دفتر ثبت‌نام با بررسی صحت امضای روی درخواست گواهی که با استفاده از استاندارد PKCS#10 تنظیم شده است، به مالکیت کلید خصوصی درخواست‌کننده گواهی پی می‌برد. همچنین در صورتی که عملیات تولید کلید توسط دفتر ثبت‌نام صورت گیرد، تناظر بین کلید عمومی موجود در درخواست با کلید خصوصی تولید شده، برای مرکز صدور گواهی خصوصی پارس‌ساین احراز می‌گردد.

۳-۲-۲ شناسایی سازمان‌ها

درخواست گواهی از سوی یک سازمان، توسط یک فرد به نمایندگی از سازمان مربوطه و به صورت حضوری در یکی از دفاتر ثبت‌نام مرتبط با مرکز میانی خصوصی پارس‌ساین ارائه می‌شود. درخواست گواهی به نام یک سازمان باید شامل نام، نشانی اقامتگاه و اسناد حقوقی و رسمی سازمان برای اثبات وجود سازمان باشد. گواهی‌هایی که می‌تواند برای سازمان‌ها صادر شود عبارتند از گواهی‌های مهر سازمانی، گواهی Code Signing، گواهی SSL/TLS، Domain Controller و گواهی‌های وابسته به مراکز صدور گواهی.

فردی که به نمایندگی از سازمان به دفتر ثبت‌نام مراجعه کرده است، جهت انجام عملیات احراز هویت سازمان، مدارک زیر را باید به دفتر ثبت‌نام ارائه دهد:

- کپی آگهی تأسیس روزنامه رسمی و آخرین تغییرات روزنامه رسمی ممهور به مهر شرکت/مؤسسه؛

1 Certificate Signing Request (CSR)

- یک برگ درخواست گواهی الکترونیکی بر روی سربرگ سازمان که حاوی مشخصات فرد نماینده (حداقل شامل نام، نام خانوادگی، و شماره ملی) و مشخصات گواهی درخواستی (حداقل شامل نوع گواهی و نام متقاضی گواهی) نیز می‌باشد که:
  - برای سازمان توسط بالاترین مقام سازمان مرتبط با متقاضی گواهی، امضا و ممهور به مهر سازمان می‌گردد.
  - برای شرکت/مؤسسه توسط نماینده شرکت/مؤسسه که حق امضای اسناد تعهدآور را دارد، امضا و ممهور به مهر شرکت/مؤسسه می‌گردد.

دفتر ثبت‌نام جهت شناسایی هویت سازمان و هویت فرد نماینده سازمان، اقدامات زیر را باید انجام دهد:

- شناسایی و تأیید هویت نماینده سازمان به صورت حضوری و مطابق با بخش ۳-۲-۳ و ۳-۲-۵؛
- بررسی صحت و اصالت مدارک تحویل داده شده؛
- نگهداری و ثبت نسخه‌ای از نوع و جزئیات شناسایی مورد استفاده در تأیید هویت سازمان و تاریخ احراز هویت، حداقل در طول دوره عمر گواهی صادرشده.

۳-۲-۳ احراز هویت افراد

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

در صورت درخواست گواهی توسط خود شخص، بررسی‌های لازم جهت احراز هویت وی توسط متصدی دفتر ثبت نام انجام می‌گیرد. در جدول ۳-۴، نحوه شناسایی شخص برای گواهی‌های سطوح مختلف، آورده شده است.

جدول ۳-۴ نحوه شناسایی شخص با توجه به سطوح اطمینان گواهی درخواست شده

سطح اطمینان	نحوه شناسایی
سطح ۱	بدون نیاز به تشریفات و بر پایه اطلاعات خوداظهاری و اعتماد صورت می‌گیرد.
سطح ۲	• به صورت حضوری و ارائه دو نوع مدرک شناسایی معتبر ذکر شده در بندهای زیر: ○ اصل و کپی کارت ملی؛ ○ اصل و کپی شناسنامه؛ ○ اصل و کپی گذرنامه؛ ○ اصل و کپی گواهی‌نامه رانندگی. • چنانچه قبلاً برای یک متقاضی، گواهی سطح دوم و یا سوم صادر شده باشد و کلید خصوصی متناظر با گواهی در خطر افشا قرار نگرفته باشد، متقاضی گواهی می‌تواند از طریق امضای الکترونیکی یک داده (مثلاً یک فرم درخواست گواهی) با استفاده کلید خصوصی متناظر گواهی قبلی خود، درخواست گواهی نماید؛ در این حالت، مرکز میانی از طریق یک شناسه رهگیری که در زمان ثبت‌نام اولیه در اختیار متقاضی قرار داده، فرایند شناسایی موجودیت را انجام می‌دهد.

فرایند احراز هویت برای خود شخص در سطح ۲ به صورت زیر می‌باشد:

- شخص مورد نظر که به عنوان درخواست‌کننده گواهی به یکی از دفاتر ثبت‌نام مرکز میانی خصوصی پارس‌ساین مراجعه می‌نماید، باید هنگام ارائه درخواست گواهی، مدارک شناسایی لازم را به دفتر ثبت‌نام ارائه دهد؛
- فرم مربوط به درخواست گواهی که توسط خود شخص تکمیل و امضا شده است، باید به دفتر ثبت‌نام ارائه شود؛
- علاوه بر فرم، مدارک مرتبط با گواهی مورد نظر (مثلاً پرینت WHOIS در کاربرد HTTPS از گواهی سرور) باید به دفتر ثبت‌نام تحویل داده شود؛
- صحت مدارک ارائه‌شده از سوی درخواست‌کننده گواهی و تطابق آن با اطلاعات موجود در فرم درخواست گواهی توسط متصدی دفتر ثبت‌نام بررسی می‌شود.

مرکز میانی خصوصی پارس‌ساین، نسخه‌ای از روش و جزئیات شناسایی به‌کار رفته در احراز هویت فرد را حداقل در طول دوره عمر گواهی صادر شده برای وی، نگهداری می‌کند.

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

یک فرد می‌تواند درخواست گواهی خود را از طریق فرد دیگری با اعطای نمایندگی رسمی به وی، ارائه دهد. فرایند هویت‌شناسی برای نماینده متقاضی گواهی، مطابق با آنچه در زیر بیان شده است، می‌باشد:

- در سطح ۱، نیاز به احراز هویت نماینده متقاضی گواهی نمی‌باشد.
- فرایند احراز هویت برای نماینده متقاضی گواهی در سطح ۲ به صورت زیر می‌باشد:
  - مدارک لازم مطابق با بخش ۳-۲-۳-۱ علاوه بر متقاضی، از نماینده وی که به عنوان نماینده درخواست‌کننده گواهی به دفتر ثبت‌نام مراجعه می‌نماید، توسط متصدی دفتر ثبت‌نام دریافت می‌شود؛
  - مجوزی رسمی مبنی بر اعطای نمایندگی که درخواست‌کننده گواهی به نماینده خود داده است، توسط متصدی دفتر ثبت‌نام بررسی و از صحت آن اطمینان حاصل می‌شود؛
  - بخش مربوط به نماینده متقاضی گواهی در فرم درخواست گواهی توسط نماینده، تکمیل و امضا می‌شود؛
  - صحت مدارک ارائه‌شده از سوی درخواست‌کننده گواهی و تطابق آن با اطلاعات موجود در فرم درخواست گواهی توسط متصدی دفتر ثبت‌نام بررسی می‌شود.

مرکز میانی خصوصی پارس‌ساین، نسخه‌ای از روش و جزئیات شناسایی به کار رفته در تأیید هویت نماینده و درخواست‌کننده گواهی را حداقل در طول دوره عمر گواهی نگاه می‌دارد.

۳-۲-۳-۳ شخصی برای نقش سازمانی خود درخواست گواهی نماید

قبل از ثبت و ارسال درخواست به مرکز صدور گواهی خصوصی پارس‌ساین، دفتر ثبت‌نام مطابق با بخش ۳-۲-۳-۱، هویت فردی را که درخواست صدور گواهی برای نقش سازمانی خود دارد، شناسایی می‌کند. علاوه بر این، دفتر ثبت‌نام از این‌که فرد برای این نقش سازمانی مجاز می‌باشد، اطمینان حاصل می‌نماید (طبق بخش ۳-۲-۵).

برای احراز هویت شخصی که برای نقش سازمانی درخواست گواهی می‌کند، علاوه بر مدارک اشاره شده در بخش ۳-۲-۳-۱، معرفی‌نامه‌ای از سازمان جهت شناسایی سمت فرد در سازمان و واحد سازمانی مربوطه نیاز می‌باشد.

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

۳-۲-۴ اطلاعات تصدیق‌نشده مالکان گواهی

اطلاعاتی که درخواست‌کننده گواهی به دفتر ثبت‌نام ارائه می‌نماید و احتیاج به بررسی و تصدیق ندارد، در جدول ۳-۵ آمده است.

جدول ۳-۵ اطلاعاتی که مورد احراز هویت قرار نمی‌گیرند

سطح اطمینان	اطلاعاتی که مورد احراز هویت قرار نمی‌گیرند
سطح ۱	هیچ اطلاعاتی تصدیق نمی‌شود.
سطح ۲	اطلاعاتی که در گواهی قید می‌شود ولی در مراحل احراز هویت تصدیق نمی‌شود: • واحد سازمانی (OU)؛ • آدرس ایمیل؛ • نام استان (فیلد State)؛ • نام شهرستان (فیلد Locality).

۳-۲-۵ اعتبارسنجی مرجع ذی‌صلاح

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

- موجودیت سازمان را از طریق اسناد و مدارک رسمی و قانونی ارائه شده پیگیری کند؛
- برای سطح اطمینان ۲، حداقل با برقراری تماس با سازمان مربوطه، از صلاحیت شخص مراجعه‌کننده جهت ارائه درخواست گواهی، اطمینان حاصل نماید.

۳-۲-۶ شرایط تعامل با سایر نهادها

در حال حاضر تعریف نشده است.

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

منظور از تجدید کلید یک گواهی این است که یک گواهی همسان با گواهی قبلی صادر گردد، با این تفاوت که گواهی جدید دارای یک کلید عمومی جدید و متفاوت (متناظر با یک کلید خصوصی متفاوت)، یک شماره سریال جدید، و احتمالاً یک بازه اعتبار جدید می‌باشد. تجدید کلید، مستلزم ابطال گواهی قبلی و تولید زوج کلید و درخواست امضای گواهی جدید است. در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین به طور مستقیم پشتیبانی نمی‌شود، ولی با استفاده از رویه‌های ابطال گواهی و درخواست ایجاد گواهی جدید (که هر دو رویه در این سند تشریح شده است)، به طور غیرمستقیم از این سرویس پشتیبانی می‌شود.

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

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

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

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

۳-۴ شناسایی و احراز هویت برای درخواست ابطال

روال شناسایی و احراز هویت برای درخواست ابطال عبارت است از بررسی و تصدیق این‌که شخص یا سازمانی که درخواست ابطال گواهی مالک گواهی را داده است، مالک واقعی گواهی و یا یک نماینده مجاز از طرف مالک گواهی می‌باشد.

فرایند درخواست ابطال گواهی و شناسایی مالک گواهی یا درخواست‌کننده ابطال گواهی مطابق با بخش‌های ۳-۲-۲ و ۳-۲-۳ صورت می‌گیرد با این تفاوت که دفتر ثبت‌نام اطلاعات و مدارک ارائه‌شده توسط درخواست‌کننده ابطال گواهی را با اطلاعات و مدارک موجود در پایگاه‌داده و بایگانی خود که هنگام درخواست صدور گواهی برای شخص یا سازمان مربوطه ثبت گردیده، مقایسه می‌نماید. در صورت

1 Re-Key

تطابق، دفتر ثبت‌نام درخواست ابطال گواهی را تأیید و برای مرکز صدور گواهی جهت پردازش ارسال می‌نماید. درخواست ابطال گواهی توسط متصدی دفتر ثبت‌نام ثبت و نگهداری می‌شود.

۴ الزامات عملیاتی چرخه حیات گواهی

۴-۱ درخواست گواهی

درخواست‌کننده گواهی و دفاتر ثبت‌نام مرکز میانی خصوصی پارس‌ساین مراحل زیر را هنگام ارائه درخواست گواهی، باید انجام دهند:

- شناسایی درخواست‌کننده گواهی توسط دفتر ثبت‌نام مطابق با بخش ۳-۲؛
- ثبت اطلاعات درخواست‌کننده گواهی مطابق با این دستورالعمل اجرایی توسط دفتر ثبت‌نام؛
- تولید زوج‌کلید و ارائه کلید عمومی به همراه هر درخواست گواهی از سوی درخواست‌کننده طبق بخش ۶-۱-۱-۳. لازم به ذکر است که امکان تولید کلید بر روی توکن سخت‌افزاری درخواست‌کننده در دفتر ثبت‌نام وجود دارد؛
- حصول اطمینان از تناظر کلید عمومی ارائه شده، با کلید خصوصی نزد درخواست‌کننده گواهی مطابق با بخش ۳-۲-۱ توسط دفتر ثبت‌نام.

همه مراحل فوق باید قبل از صدور گواهی کامل شود.

۴-۱-۱ موجودیت‌های مجاز جهت ارائه درخواست گواهی

افرادی که می‌توانند یک درخواست گواهی ارائه نمایند عبارتند از:

- شخصی که می‌خواهد مالک گواهی شود؛
- نماینده مجاز برای یک سازمان یا موجودیت (جهت ارائه درخواست گواهی برای شخص دیگر، نقش سازمانی، دستگاه یا برنامه کاربردی و یا ارائه درخواست گواهی‌های سازمانی).

۴-۱-۲ فرایند ثبت‌نام و مسئولیت‌ها

هر شخص یا سازمانی که قصد درخواست صدور یک گواهی از مرکز میانی خصوصی پارس‌ساین را دارد، باید مراحل زیر را طی کند:

- پس از تولید زوج‌کلید، یک فایل درخواست امضای گواهی (CSR) مطابق با استاندارد PKCS#10 ایجاد کرده و فایل CSR را به دفتر ثبت‌نام تحویل دهد. درخواست‌کننده می‌تواند در صورت تمایل، فرایند ایجاد CSR و تولید کلید بر روی توکن سخت‌افزاری خود را به دفتر ثبت‌نام واگذار نماید؛
- مدارک و اطلاعات لازم جهت ارائه یک درخواست گواهی را مطابق با بخش ۳-۲ به دفتر ثبت‌نام ارائه نماید؛
- فرم درخواست گواهی را تکمیل نماید و توافق‌نامه شرایط حاکم بر استفاده از گواهی را بپذیرد.

۴-۲ بررسی درخواست گواهی

۴-۲-۱ اجرای فرایند شناسایی و احراز هویت

دفتر ثبت‌نام باید اطلاعات مورد نیاز ارائه شده توسط متقاضی گواهی جهت صدور یک گواهی توسط مرکز صدور گواهی خصوصی پارس‌ساین را مطابق با بخش ۳-۲، شناسایی و احراز هویت کند.

۴-۲-۲ تأیید یا رد درخواست‌های گواهی

دفتر ثبت‌نام یک درخواست گواهی را در صورتی که کلیه اطلاعات ارائه‌شده توسط متقاضی گواهی مطابق با بخش ۳-۲ با موفقیت شناسایی و احراز هویت گردد، تأیید می‌نماید. ضمناً دفتر ثبت‌نام یک درخواست گواهی را رد می‌کند اگر هر یک از موارد زیر اتفاق بیفتد:

- شناسایی و احراز هویت اطلاعات ارائه شده توسط درخواست‌کننده مطابق با بخش ۳-۲ با موفقیت و به طور کامل صورت نگیرد؛
- فایل درخواست امضای گواهی (CSR) تحویل داده شده توسط درخواست‌کننده در قالب استاندارد PKCS#10 نباشد، مطابق با سیاست‌های مرکز صدور گواهی الکترونیکی ریشه ایجاد نشده باشد، یا عملیات اثبات مالکیت کلید خصوصی با موفقیت صورت نگیرد؛

- درخواست‌کننده گواهی توافق‌نامه سطح ارائه خدمات را نپذیرد؛
- درخواست‌کننده گواهی به تذکرات و درخواست‌های دفتر ثبت‌نام در زمان تعیین‌شده پاسخ ندهد؛
- دفتر ثبت‌نام به این نتیجه برسد که صدور گواهی برای درخواست‌کننده گواهی منجر به سوءاستفاده، ارتکاب جرم، نقض قانون، یا بدنامی مرکز میانی خصوصی پارس‌ساین می‌گردد.

۴-۲-۳ مدت رسیدگی به درخواست گواهی

مرکز صدور گواهی خصوصی پارس‌ساین درخواست‌های گواهی را پس از تأیید درخواست مربوطه توسط دفتر ثبت نام و ارسال آن به مرکز صدور، پردازش کرده و گواهی مورد نظر را صادر می‌نماید. حداکثر مدت زمان فرایند رسیدگی به درخواست گواهی برای سطوح اطمینان مختلف، مطابق با جدول ۴-۱ می‌باشد:

جدول ۴-۱ مدت فرایند رسیدگی به درخواست گواهی

سطح اطمینان	حداکثر فاصله بین درخواست و صدور گواهی
سطح ۱	قید خاصی وجود ندارد.
سطح ۲	گواهی‌های کاربران نهایی حداکثر طی مدت ۵ روز کاری از زمان ارسال درخواست از سوی دفتر ثبت‌نام، صادر می‌شوند.

۴-۳ صدور گواهی

۴-۳-۱ اقدامات مرکز در طول صدور گواهی

مرکز صدور گواهی خصوصی پارس‌ساین پس از تصدیق امضای CSR دریافت شده از سوی دفتر ثبت‌نام، گواهی را بر اساس اطلاعات موجود در CSR تصدیق شده، صادر می‌نماید.

الزامات مدت‌زمان ارسال درخواست صدور گواهی به مرکز صدور گواهی خصوصی پارس‌ساین توسط دفتر ثبت‌نام در جدول ۴-۲ آمده است.

جدول ۴-۲ الزامات مدت زمان ارسال درخواست صدور توسط دفتر ثبت‌نام به مرکز صدور گواهی خصوصی پارس‌ساین

سطح اطمینان	الزامات زمانی
سطح ۱	پس از تکمیل مراحل درخواست صدور توسط متقاضی، دفتر ثبت‌نام در بازه زمانی

سطح اطمینان	الزامات زمانی
	حداکثر ۷ روز کاری، باید درخواست را برای مرکز صدور گواهی پارس‌ساین ارسال نماید.
سطح ۲	پس از تکمیل مراحل درخواست صدور توسط متقاضی، دفتر ثبت‌نام در بازه زمانی حداکثر ۵ روز کاری، باید درخواست را برای مرکز صدور گواهی پارس‌ساین ارسال نماید.

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

مرکز صدور پس از بررسی درخواست صدور گواهی، از طریق دفتر ثبت‌نام و به یکی از شیوه‌های زیر، صدور موفقیت‌آمیز یا عدم آن را (با ذکر دلایل) به متقاضی گواهی اطلاع می‌دهد.

شیوه‌های اطلاع‌رسانی عبارتند از:

- پست الکترونیکی؛
- تماس تلفنی؛
- فکس؛
- حضور متقاضی به دفتر ثبت‌نام.

۴-۴ پذیرش گواهی

۴-۴-۱ چگونگی پذیرش گواهی

تکمیل و امضای فرم درخواست صدور/تمدید گواهی که متقاضی گواهی به دفتر ثبت‌نام ارائه می‌دهد، به منزله پذیرش گواهی متناظر با آن درخواست از سوی مالک گواهی می‌باشد.

پس از صدور گواهی و انتشار آن در مخزن، دفتر ثبت‌نام باید به یکی از شیوه‌های اطلاع‌رسانی که در بخش ۴-۳-۲ به آن اشاره شد، به مالک گواهی اطلاع‌رسانی کند.

۴-۴-۲ انتشار گواهی توسط مرکز صدور گواهی

مرکز صدور گواهی خصوصی پارس‌ساین گواهی‌های صادرشده را از طریق مخزن منتشر می‌کند.

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

مرکز صدور گواهی خصوصی پارس‌ساین، در صورت عدم صدور موفقیت‌آمیز گواهی درخواست‌کننده، موضوع را به اطلاع دفتر ثبت‌نام می‌رساند.

۴-۵ کاربرد گواهی و زوج‌کلید

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

استفاده از کلید خصوصی متناظر با کلید عمومی موجود در گواهی تنها در صورتی مجاز می‌باشد که مالک گواهی توافق‌نامه سطح ارائه خدمات را پذیرفته و فرم درخواست گواهی را امضا نماید.

مالک گواهی باید گواهی را طبق قانون و مطابق با توافق‌نامه سطح ارائه خدمات، سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور (CP)، و این دستورالعمل اجرایی گواهی (CPS) مورد استفاده قرار دهد. استفاده از گواهی نباید متناقض با فیلد KeyUsage از الحاقیه‌های[1] گواهی باشد؛ به عبارت دیگر، تنها برای کاربردهایی استفاده شود که در این فیلد ذکر شده است.

مالک گواهی نباید از کلید خصوصی خود در کاربردهای غیرمجاز و به قصد ضرر رساندن به دیگران استفاده کند. همچنین نباید با منقضی شدن و یا باطل شدن گواهی از کلید خصوصی متناظر با آن گواهی استفاده نماید. در غیر این صورت، مرکز میانی خصوصی پارس‌ساین هیچ‌گونه مسئولیتی را در قبال پیامد-های ناشی از این کار بر عهده نمی‌گیرد.

۴-۵-۲ کاربرد گواهی و کلید عمومی برای طرف اعتمادکننده

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

[1] Extension

در یک زنجیره گواهی، هر گواهی توسط صادرکننده آن گواهی امضا شده است و این زنجیره، از گواهی کاربر یا موجودیت نهایی تا گواهی متعلق به مرکز صدور گواهی ریشه امتداد دارد. به عنوان مثال، یک زنجیره گواهی ممکن است شامل گواهی کاربر که توسط مرکز صدور گواهی خصوصی پارس‌ساین امضا شده، گواهی مرکز صدور گواهی خصوصی پارس‌ساین که توسط مرکز ریشه امضا شده، و گواهی متعلق به مرکز صدور گواهی ریشه (که توسط خودش امضاشده) باشد.

طرف‌های اعتماد کننده باید همواره به تناسب استفاده از گواهی با اهداف و کاربردهای تعیین شده و عدم استفاده از گواهی در کاربردهای منع‌شده توسط سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و دستورالعمل اجرایی مرکز میانی خصوصی پارس‌ساین توجه داشته باشند. علاوه بر این، قبل از اعتماد به یک گواهی، جهت اعتبارسنجی زنجیره گواهی باید حداقل موارد زیر را در نظر داشته باشند:

- وجود یا عدم وجود گواهی متعلق به صادرکننده گواهی مورد نظر در زنجیره گواهی؛
- تناسب استفاده از گواهی با اهداف و کاربردهای تعیین‌شده برای آن گواهی و عدم استفاده از گواهی در کاربردهای منع‌شده توسط سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و این دستورالعمل اجرایی (مرکز میانی خصوصی پارس‌ساین مسئولیتی در قبال عدم تناسب استفاده طرف اعتمادکننده از گواهی با کاربردهای تعیین‌شده ندارد)؛
- اعتبار امضای کلیه گواهی‌های موجود در زنجیره گواهی؛
- استفاده از گواهی در کاربردهای متناسب با کاربردهای تعیین‌شده در الحاقیه‌های گواهی (مثل الحاقیه KeyUsage). به عنوان مثال، اگر کاربرد امضای دیجیتال برای گواهی فعال نشده باشد، از این گواهی نباید برای امضا استفاده شود؛
- وضعیت (ابطال یا عدم ابطال) گواهی مالک گواهی و کلیه گواهی‌های متعلق به مراکز صدور گواهی موجود در زنجیره گواهی. اگر هر یک از گواهی‌های موجود در زنجیره گواهی باطل شده باشد، طرف اعتمادکننده منحصراً مسئول اعتماد به گواهی مالک گواهی و امضای تصدیق شده توسط این گواهی می‌باشد؛
- اعتبار کلیه لیست‌های گواهی‌های باطل شده مرتبط با زنجیره گواهی.

با فرض این که از گواهی در کاربرد مناسب استفاده می‌شود، طرف‌های اعتمادکننده باید از نرم‌افزار و یا سخت‌افزار مناسب جهت انجام عملیات تصدیق امضا، اعتبارسنجی زنجیره گواهی و یا دیگر عملیات رمزنگاری وابسته به کلید عمومی استفاده کنند. این عملیات یکی از شرایط اعتماد به گواهی است که شامل

شناسایی یک زنجیره گواهی و تصدیق امضای روی تمام گواهی‌های موجود در زنجیره گواهی نیز می‌باشد. منظور از نرم‌افزار مناسب، نرم‌افزاری است که طرف اعتمادکننده اطمینان دارد که آن نرم‌افزار، عملیات تصدیق امضا، بررسی اعتبار گواهی، بررسی زنجیره گواهی، و دیگر عملیات ذکرشده در بالا را به درستی انجام می‌دهد.

۴-۶ تمدید گواهی[1]

منظور از تمدید گواهی، تولید یک گواهی جدید همسان با گواهی قبلی است با این تفاوت که گواهی جدید دارای یک مدت اعتبار متفاوت و یک شماره سریال متفاوت می‌باشد.

۴-۶-۱ شرایط تمدید گواهی

تمدید یک گواهی تنها در شرایط زیر امکان‌پذیر است:

- درخواست تمدید گواهی قبل از مدت زمان مشخصی که به انقضای گواهی باقی‌مانده است، به دفتر ثبت‌نام ارائه شود. این مدت زمان در زیر آمده است:
- از آن‌جایی که طبق سند «سیاست‌های گواهی الکترونیکی در زیرساخت کلید عمومی کشور» در سطح ۱ امنیتی، برای مدت‌زمان لازم جهت رسیدگی به درخواست گواهی توسط مرکز صدور گواهی قید خاصی وجود ندارد، در این حالت، مالک گواهی موظف است حداقل دو هفته قبل از انقضای گواهی، درخواست تمدید گواهی را به دفتر ثبت‌نام ارائه نماید.
- برای سایر سطوح، مجموع حداکثر مدت‌زمان لازم برای ارسال درخواست تمدید توسط دفتر ثبت‌نام (طبق بخش «بررسی درخواست‌های تمدید گواهی») و حداکثر مدت‌زمان لازم برای رسیدگی به درخواست گواهی توسط مرکز صدور گواهی خصوصی پارس‌ساین (طبق سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور»).
- گواهی باطل نشده باشد؛
- مجموع دوره اعتبار گواهی‌های صادرشده (مجموع دوره اعتبار گواهی جدید و قدیم) از الزامات قید شده در بخش ۶-۳-۲ پیروی نماید؛

[1] Certificate Renewal

- پایان دوره اعتبار گواهی تمدید شده از پایان دوره اعتبار گواهی مرکز صدور گواهی الکترونیکی پارس‌ساین تجاوز نکند.

۴-۶-۲ متقاضیان تمدید گواهی

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

- مالک گواهی یا نماینده مجاز وی؛
- دفاتر ثبت‌نام.

۴-۶-۳ بررسی درخواست‌های تمدید گواهی

در فرایند تمدید گواهی، اپراتور دفتر ثبت‌نام اطمینان حاصل می‌کند که شخص یا سازمانی که درخواست‌کننده تمدید گواهی است، مالک واقعی گواهی یا نماینده مجاز وی می‌باشد. کلیه مدارک ارائه‌شده به دفتر ثبت‌نام در فرایند احراز هویت برای تمدید گواهی مشابه بخش ۳-۲ می‌باشد با این تفاوت که دفتر ثبت‌نام، اطلاعات و مدارک ارائه‌شده توسط درخواست‌کننده را با اطلاعات و مدارک موجود در بایگانی خود که هنگام درخواست صدور گواهی برای شخص یا سازمان مربوطه ثبت گردیده، مقایسه می‌نماید. در صورت تطابق این اطلاعات و مدارک، دفتر ثبت‌نام درخواست تمدید گواهی را تأیید نموده و جهت پردازش به مرکز صدور گواهی ارسال می‌نماید.

مدت‌زمان ارسال درخواست تمدید گواهی توسط دفتر ثبت‌نام به مرکز صدور گواهی در جدول ۴-۳ آمده است.

جدول ۴-۳ الزامات مدت زمان ارسال درخواست تمدید توسط دفتر ثبت‌نام به مرکز صدور گواهی

سطح اطمینان	الزامات زمانی
سطح ۱	پس از تکمیل مراحل درخواست تمدید توسط متقاضی، دفتر ثبت‌نام در بازه زمانی حداکثر ۷ روز کاری، باید درخواست را برای مرکز صدور گواهی پارس‌ساین ارسال نماید.
سطح ۲	پس از تکمیل مراحل درخواست تمدید توسط متقاضی، دفتر ثبت‌نام در بازه زمانی حداکثر ۵ روز کاری، باید درخواست را برای مرکز صدور گواهی پارس‌ساین ارسال نماید.

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

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

۴-۶-۵ چگونگی پذیرش گواهی تمدیدشده

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

۴-۶-۶ انتشار گواهی‌های تمدیدشده توسط مرکز

گواهی‌های جدید صادرشده که مدت اعتبار آن‌ها تمدید شده است و از سوی مالک گواهی پذیرفته شده‌اند، از طریق مخزن مرکز میانی خصوصی پارس‌ساین منتشر می‌شوند.

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

دفتر ثبت‌نام از صدور گواهی که درخواست تمدید آن را تأیید و ثبت نموده بود، مطلع می‌شود.

۴-۷ تجدید کلید گواهی[1]

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

1 Certificate Re-Key

۴-۷-۱ شرایط تجدید کلید گواهی

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

۴-۷-۲ متقاضیان گواهی با کلید عمومی جدید

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

۴-۷-۳ بررسی درخواست‌های تجدید کلید گواهی

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

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

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

۴-۷-۵ چگونگی پذیرش گواهی با کلید جدید

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

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

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

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

در حال حاضر سرویس تجدید کلید در مرکز میانی خصوصی پارس‌ساین ارائه نمی‌شود.

۴-۸ اصلاح گواهی[1]

در حال حاضر قابل اعمال نیست.

[1] Certficate Modification

۴-۸-۱ شرایط اصلاح گواهی

در حال حاضر قابل اعمال نیست.

۴-۸-۲ متقاضیان اصلاح گواهی

در حال حاضر قابل اعمال نیست.

۴-۸-۳ بررسی درخواست‌های اصلاح گواهی

در حال حاضر قابل اعمال نیست.

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

در حال حاضر قابل اعمال نیست.

۴-۸-۵ چگونگی پذیرش گواهی اصلاح شده

در حال حاضر قابل اعمال نیست.

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

در حال حاضر قابل اعمال نیست.

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

در حال حاضر قابل اعمال نیست.

۴-۹ ابطال و تعلیق گواهی

۴-۹-۱ شرایط ابطال

زمانی که پیوند بین مشخصات مالک گواهی و کلید عمومی گواهی دیگر اعتباری نداشته باشد، گواهی باطل می‌شود.

۴-۹-۱-۱ شرایط ابطال گواهی الکترونیکی مرکز صدور گواهی خصوصی پارس‌ساین

در صورت وقوع هر یک از موارد زیر مرکز صدور گواهی خصوصی پارس‌ساین ابطال گواهی خود را از مرکز ریشه درخواست می‌کند:

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

همچنین گواهی مرکز صدور گواهی خصوصی پارس‌ساین، توسط مرکز ریشه و منطبق با سیاست‌های این مرکز قابل ابطال است. حداقل در صورت وقوع هر یک از موارد زیر، مرکز ریشه اقدام به ابطال گواهی مرکز صدور گواهی خصوصی پارس‌ساین بدون تأیید او می‌نماید:

- در صورت ابطال گواهی مرکز ریشه؛
- در صورت بروز تخلف مرکز صدور گواهی خصوصی پارس‌ساین یا دفاتر ثبت‌نام وابسته به آن از مندرجات موجود در سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و تأیید این تخلف توسط شورا؛
- محرز شدن صدور گواهی مبتنی بر اظهارات خلاف واقع اعم از عمدی و غیرعمدی مرکز صدور گواهی میانی پارس‌ساین و تأیید آن توسط شورا؛
- درخواست ابطال از سوی مراجع قضائی ذیصلاح؛
- پایان فعالیت مرکز ریشه.

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

در صورت وقوع هر یک از موارد زیر مالک گواهی و یا نماینده مجاز وی باید ابطال گواهی خود را از مرکز صدور گواهی خصوصی پارس‌ساین درخواست کند:

- کلید خصوصی مالک گواهی احتمالاً یا مطمئناً در خطر افشا باشد؛
- اطلاعات موجود در گواهی (نظیر مشخصات مالک گواهی) به هر دلیلی تغییر کند. اطلاعاتی که طبق بخش ۳-۲-۴ در فرایند احراز هویت تصدیق نمی‌شوند، مشمول این مورد نمی‌شود؛
- دیگر نیازی به گواهی نباشد؛ این امر ممکن است به علت توقف فعالیت یک سازمان و یا توقف فعالیت یک شخص در یک سازمان و یا تغییر جایگاه (سمت) سازمانی مالک گواهی باشد.

علاوه بر این، در صورت بروز هر یک از شرایط زیر، مرکز صدور گواهی خصوصی پارس‌ساین، گواهی مالکان گواهی را بدون تأیید آن‌ها باطل می‌کند:

- در صورت استفاده غیرمجاز، جعل، و در خطر افشا قرار گرفتن کلید خصوصی مرکز صدور گواهی خصوصی پارس‌ساین و یا باطل شدن گواهی مرکز دولتی صدور گواهی الکترونیکی ریشه؛
- درخواست ابطال از سوی مراجع قضائی ذیصلاح؛
- تخطی مالک گواهی از تعهداتش؛
- پایان فعالیت مرکز صدور گواهی الکترونیکی پارس‌ساین؛
- پایان فعالیت مرکز دولتی صدور گواهی الکترونیکی ریشه؛
- فوت مالک گواهی.

لازم به ذکر است طبق توافق‌نامه‌ای که بین مرکز میانی خصوصی پارس‌ساین و مالکان گواهی صورت می‌گیرد، مالکان گواهی ملزم هستند که در صورت به خطر افتادن یا احتمال به خطر افتادن کلید خصوصی خود، در اسرع وقت این موضوع را به مرکز اطلاع داده و جهت ابطال گواهی اقدام کنند.

۴-۹-۲ متقاضیان درخواست ابطال

۴-۹-۲-۱ موجودیت‌های نهایی

لیست موجودیت‌های مجاز به ارائه درخواست گواهی در جدول ۴-۴ آمده است.

جدول ۴-۴ موجودیت‌های مجاز به ارائه درخواست ابطال گواهی

سطح اطمینان	موجودیت‌های مجاز به ارائه درخواست ابطال گواهی الکترونیکی
سطح ۱	قید خاصی وجود ندارد.
سطح ۲	• مالک گواهی؛ • نماینده مجاز از سوی مالک گواهی (بخش ۳-۲-۳)؛ • نماینده مجاز از یک سازمان جهت ارائه درخواست ابطال گواهی‌های سازمانی و یا گواهی یکی از کارکنان سازمان (بخش ۳-۲-۳)؛ • نماینده مجاز برای ابطال گواهی دفاتر ثبت‌نام؛ • مراجع قضایی ذیصلاح.

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

موجودیت‌های مجاز جهت ارائه درخواست ابطال گواهی مرکز صدور گواهی خصوصی پارس‌ساین عبارتند از:

- نماینده مجاز مرکز صدور گواهی خصوصی پارس‌ساین برای ابطال گواهی این مرکز؛
- مراجع قضایی ذیصلاح؛
- شورا؛
- مرکز دولتی صدور گواهی الکترونیکی ریشه.

۴-۹-۳ فرایند رسیدگی به درخواست ابطال

هر درخواست ابطال گواهی که به مرکز میانی خصوصی پارس‌ساین ارائه می‌شود، باید تنها یک گواهی را مشخص کرده، دلیل ابطال گواهی را شرح داده و مطابق با بخش ۳-۴ احراز هویت شود. چنانچه دلیل درخواست ابطال گواهی در معرض خطر افشا قرار گرفتن کلید یا شک به کلاه‌برداری باشد، باید در درخواست ابطال مالک گواهی ذکر شود.

اگر درخواست ابطال معتبر باشد، مرکز صدور گواهی آن را از طریق قرار دادن شماره سریال و دیگر اطلاعات مربوط به ابطال (مثل دلیل ابطال گواهی و زمان ابطال گواهی)، باطل می‌کند. فرایند رسیدگی به درخواست ابطال در جدول ۴-۵ شرح داده شده است.

جدول ۴-۵ فرایند رسیدگی به درخواست ابطال

سطح اطمینان	فرایند رسیدگی به درخواست ابطال
سطح ۱	هیچ قیدی وجود ندارد.
سطح ۲	مرکز میانی خصوصی پارس‌ساین باید موارد زیر را انجام دهد: ۱. شناسایی و احراز هویت درخواست‌کننده ابطال گواهی (مطابق با بخش ۳-۴)؛ ۲. ثبت و نگهداری تمام اطلاعات مربوط به درخواست؛ ۳. به‌روز نمودن لیست گواهی‌های باطله.

۴-۹-۴ مهلت اعلام درخواست ابطال

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

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

مرکز صدور گواهی خصوصی پارس‌ساین با دریافت هر درخواست ابطال از سوی دفتر ثبت‌نام، بعد از تصدیق آن گواهی قیدشده در درخواست را مطابق با الزامات زمانی جدول ۴-۶ باطل نموده و به تفکیک سطح امنیتی گواهی مورد نظر، لیست ابطال گواهی‌ها را منطبق با جدول ۴-۹ از طریق مخزن منتشر می‌نماید.

جدول ۴-۶ مدت رسیدگی به درخواست ابطال توسط مرکز صدور گواهی

سطح اطمینان	الزامات زمانی
سطح ۱	الزام خاصی در نظر گرفته نشده است.
سطح ۲	• چنانچه درخواست ابطال در ساعات کاری توسط مرکز صدور گواهی دریافت گردد، در کمتر از ۲ ساعت پس از دریافت آن، پردازش می‌شود. • چنانچه درخواست ابطال خارج از ساعات کاری دریافت گردد، حداکثر تا پایان دومین ساعت کاری روز بعد، پردازش می‌شود. • چنانچه درخواست ابطال خارج از ساعات کاری دریافت گردد و روز بعدی نیز یک روز کاری نباشد، پردازش درخواست حداکثر ۲۴ ساعت طول خواهد کشید.

لازم به ذکر است که الزامات مدت زمان ارائه درخواست تأییدشده ابطال از سمت دفتر ثبت‌نام به مرکز صدور گواهی طبق جدول ۴-۷ می‌باشد.

جدول ۴-۷ الزامات مدت زمان ارسال درخواست ابطال توسط دفتر ثبت‌نام به مرکز صدور گواهی

سطح اطمینان	الزامات زمانی
سطح ۱	پس از تکمیل مراحل درخواست ابطال توسط متقاضی، دفتر ثبت‌نام در بازه زمانی حداکثر ۵ روز کاری، باید درخواست را برای مرکز صدور گواهی پارس‌ساین ارسال نماید.
سطح ۲	پس از تکمیل مراحل درخواست ابطال توسط متقاضی: • چنانچه درخواست ابطال در ساعات کاری توسط مرکز صدور گواهی دریافت گردد، در کمتر از ۲ ساعت پس از دریافت آن، ارسال می‌شود. • چنانچه درخواست ابطال خارج از ساعات کاری دریافت گردد، حداکثر تا پایان دومین ساعت کاری روز بعد، ارسال می‌شود. • چنانچه دلیل ابطال، افشای کلید خصوصی باشد، درخواست بلافاصله ارسال می‌شود.

۴-۹-۶ الزامات بررسی ابطال توسط طرف‌های اعتمادکننده

طرف اعتمادکننده قبل از استفاده از گواهی باید وضعیت (ابطال یا عدم ابطال) آن را بررسی نماید. چنانچه در شرایط خاص، دسترسی به اطلاعات وضعیت گواهی امکان‌پذیر نباشد، مسئولیت اعتماد به گواهی بر عهده طرف اعتمادکننده می‌باشد. الزامات بررسی وضعیت گواهی در جدول ۴-۸ آورده شده است:

جدول ۴-۸ الزامات بررسی وضعیت ابطال گواهی توسط طرف‌های اعتمادکننده

سطح اطمینان	الزام کنترل وضعیت ابطال گواهی
سطوح ۱ و ۲	طرف اعتمادکننده باید: • در فرایند اعتبارسنجی زنجیره گواهی وضعیت ابطال یا عدم ابطال کلیه گواهی‌های موجود در زنجیره را در آخرین لیست گواهی‌های باطل‌شده که توسط مرکز صدور گواهی آن منتشرشده، بررسی نماید؛ • صحت و تمامیت لیست گواهی‌های باطل شده را بررسی نماید.

آخرین CRL منتشرشده جهت بررسی وضعیت گواهی‌ها، در آدرس‌های زیر قابل دریافت می‌باشد.

برای گواهی‌های سطح یک:

- http://www.parssignca.ir/class1/PS_CAL1.crl
- https://www.parssignca.ir/class1/PS_CAL1.crl

- ldap://parssignca.ir/cn=ParsSign Private Intermediate Bronze CA – G2+serialNumber=61053494000000000004,dc=level1,dc=Intermediate CA,dc=G2,c=ir?certificateRevocationList;binary

برای گواهی‌های سطح دو:

- http://www.parssignca.ir/class2/PS_CAL2.crl
- https://www.parssignca.ir/class2/PS_CAL2.crl

۴-۹-۷ تناوب صدور لیست گواهی‌های باطل‌شده

مرکز صدور گواهی خصوصی پارس‌ساین لیست گواهی‌های باطل‌شده را حتی اگر هیچ تغییر یا به‌روزرسانی در آن انجام نشده باشد، برای اطمینان کاربران از دسترسی به اطلاعات ابطال به‌روز، به صورت دوره‌ای منتشر می‌کند و لیست گواهی‌های باطل‌شده قبلی را از مخزن برمی‌دارد. الزامات مربوط به تناوب انتشار صدور لیست گواهی‌های باطل‌شده توسط مرکز میانی خصوصی پارس‌ساین در جدول ۴-۹ قید شده است.

جدول ۴-۹ تناوب صدور CRL

سطح اطمینان	تناوب صدور لیست گواهی‌های باطل‌شده
سطح ۱	• نسخه به‌روز شده CRL هر ۳۰ روز، حداقل یک‌بار صادر می‌شود. • در صورتی که دلیل ابطال یک گواهی، افشای کلید خصوصی متناظر آن باشد، حداکثر ۱ روز پس از دریافت و پردازش درخواست ابطال گواهی توسط مرکز صدور گواهی خصوصی پارس‌ساین، یک نسخه به‌روزشده CRL صادر می‌گردد.
سطح ۲	• نسخه به‌روز شده CRL هر ۲۴ ساعت حداقل یک‌بار، صادر می‌شود. • در صورتی که دلیل ابطال یک گواهی افشای کلید خصوصی متناظر آن باشد، بلافاصله پس از ابطال گواهی، یک نسخه به‌روز شده CRL صادر می‌شود.

۴-۹-۸ حداکثر تأخیر انتشار لیست گواهی‌های باطل‌شده

در مرکز صدور گواهی خصوصی پارس‌ساین، لیست گواهی‌های باطل‌شده به صورت خودکار و بلافاصله پس از ابطال گواهی، در مخزن منتشر می‌شود. حداکثر تأخیر مجاز بین ابطال یک گواهی و انتشار لیست گواهی‌های باطل‌شده حداکثر ۲ ساعت می‌باشد.

۴-۹-۹ دسترسی برخط به کنترل وضعیت ابطال

در حال حاضر این سرویس پشتیبانی نمی‌شود.

۴-۹-۱۰ الزامات کنترل برخط وضعیت ابطال

در حال حاضر این سرویس پشتیبانی نمی‌شود.

۴-۹-۱۱ سایر روش‌های ممکن اعلان ابطال

در حال حاضر روش دیگری پشتیبانی نمی‌شود.

۴-۹-۱۲ الزامات خاص در صورت افشای کلید

در صورت افشای کلید خصوصی، مرکز صدور گواهی باید بعد از ابطال گواهی، لیست گواهی‌های باطل‌شده به‌روز شده را مطابق با بخش ۴-۹-۷ منتشر نماید.

۴-۹-۱۳ شرایط تعلیق

بر اساس سیاست‌های مرکز ریشه، در حال حاضر امکان تعلیق گواهی‌های الکترونیکی در زیرساخت کلید عمومی کشور وجود ندارد.

۴-۹-۱۴ متقاضیان درخواست تعلیق گواهی

تعریف نشده است.

۴-۹-۱۵ فرایند رسیدگی به درخواست تعلیق

تعریف نشده است.

۴-۹-۱۶ محدودیت‌های دوره تعلیق

تعریف نشده است.

۴-۱۰خدمات وضعیت گواهی

مرکز صدور گواهی خصوصی پارس‌ساین وضعیت گواهی‌ها را از طریق لیست گواهی‌های باطل‌شده، اعلام و منتشر می‌کند.

۴-۱۰-۱ ویژگی‌های عملیاتی

آخرین نسخه به‌روز شده لیست گواهی‌های باطل‌شده از طریق مخزن مرکز میانی خصوصی پارس‌ساین قابل دریافت است.

ویژگی‌های عملیاتی لیست گواهی‌های باطل‌شده در بخش ۷-۲ قید شده است.

۴-۱۰-۲ دسترس‌پذیری خدمت

همواره وضعیت هر گواهی در طول عمر آن گواهی، از طریق مخزن مرکز صدور گواهی خصوصی پارس‌ساین انتشار یافته و در دسترس عموم قرار می‌گیرد.

۴-۱۰-۳ ویژگی‌های اختیاری

تعریف نشده است.

۴-۱۱پایان اشتراک

مرکز میانی خصوصی پارس‌ساین، پیرو سیاست‌های گواهی زیرساخت کلید عمومی کشور، در صورت وقوع یکی از شرایط ذیل می‌تواند به ارائه خدمات گواهی الکترونیکی به مالک گواهی پایان دهد:

- با منقضی شدن گواهی در صورتی‌که مالک گواهی مجدداً درخواست صدور گواهی ننماید؛
- با ابطال گواهی در صورتی‌که مالک گواهی درخواست صدور گواهی جدید ننماید.

۴-۱۲امانت‌گذاری و بازیابی کلید[1]

در حال حاضر قابل اعمال نیست.

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

تعریف نشده است.

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

قابل اعمال نیست.

1 Key escrow and recovery

۵ کنترل‌های امکانات، تجهیزات، مدیریتی و عملیاتی

۵-۱ کنترل‌های فیزیکی

مرکز صدور گواهی الکترونیکی پارس‌ساین دارای تجهیزاتی است که فقط مختص به فعالیت‌های این مرکز می‌باشد و از آن‌ها در فعالیت‌های غیرمرتبط با مرکز استفاده نمی‌شود.

برای حفاظت از نرم‌افزارها و سخت‌افزارها، کنترل‌های امنیت فیزیکی مورد نیاز منظور شده است.

۵-۱-۱ ساختمان و محل سایت

مرکز صدور گواهی خصوصی پارس‌ساین در محیط حفاظت شده‌ای فعالیت می‌کند که در آن از استفاده غیرمجاز، دسترسی و افشای اطلاعات حساس و سری چه به صورت آشکار و چه به صورت پنهان جلوگیری می‌شود.

ساختمان این مرکز بر اساس ملزومات امنیتی خاص به گونه‌ای طراحی و ساخته شده است که دسترسی به تجهیزات مرکز، مستلزم عبور از لایه‌های امنیت فیزیکی مختلف با سطوح امنیتی مختلف است.

۵-۱-۲ دسترسی فیزیکی

مرکز صدور گواهی خصوصی پارس‌ساین با لایه‌های امنیت فیزیکی مختلفی محافظت می‌شود که در آن دسترسی به لایه پایین‌تر مستلزم عبور از لایه بالایی می‌باشد. دسترسی به هر لایه برای کارکنان مجاز نیازمند استفاده از تجهیزات بایومتریک می‌باشد. افراد و کارکنان غیرمجاز اجازه ورود به اماکن حساس و محافظت‌شده را ندارند.

تجهیزات دفاتر ثبت‌نام (مانند سیستم ثبت درخواست) از دسترسی غیرمجاز محافظت می‌شوند. دفاتر ثبت‌نام کنترل‌های دسترسی فیزیکی متناسب با سطح تهدیدات امنیتی را اجرا می‌کنند. مکانیزم‌های امنیتی اتخاذشده، متناسب با سطح تهدید در محیط تجهیزات دفتر ثبت‌نام است.

کلیه دستگاه‌های رمزنگاری مرکز میانی خصوصی پارس‌ساین که قابل حمل هستند، در زمان بلااستفاده بودن، در محفظه‌ای امن نگهداری می‌شوند. اطلاعات فعال‌ساز به خاطر سپرده می‌شوند یا در سطحی معادل با امنیت دستگاه رمزنگاری، ذخیره و ثبت می‌شوند. این اطلاعات درون دستگاه رمزنگاری ذخیره نمی‌شوند.

هر متصدی پیش از خروج از سایت، یک بازرسی امنیتی شامل موارد زیر به همراه تاریخ، زمان و امضای شخص بازرس، به صورت مکتوب تهیه کرده و بایگانی می‌نماید:

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

سایت تجهیزات مرکز میانی خصوصی پارس‌ساین با سیستم‌های تشخیص نفوذ محافظت می‌شود. علاوه بر این، حداقل هر ۲۴ ساعت بررسی می‌شود تا اطمینان حاصل گردد که هیچ تلاشی مبنی بر مقابله با مکانیزم‌های امنیتی صورت نگرفته است.

۵-۱-۳ تهویه هوا و منبع تغذیه برق

تأسیسات مرکز میانی خصوصی پارس‌ساین شرایط زیر را پشتیبانی می‌کند:

- تغذیه دستگاه‌های الکترونیکی به صورت بلا انقطاع با استفاده از UPS و مولد دیزلی؛
- استفاده از سیستم‌های تهویه مطبوع جهت کنترل دما و رطوبت.

۵-۱-۴ جلوگیری از آب‌گرفتگی

مرکز میانی خصوصی پارس‌ساین جهت جلوگیری از نفوذ آب به تجهیزات خود اقدامات پیشگیرانه لازم را به عمل آورده است. برای مثال، تجهیزات، روی میزها و یا در مکانی مرتفع‌تر از کف اتاق قرار داده می‌شوند. همچنین در نواحی مشکوک به نشت آب، حسگرهای رطوبتی نصب می‌شود. اشخاصی که در مرکز

میانی خصوصی پارس‌ساین مسئولیت وسایل کنترل آتش را بر عهده دارند، بر عملکرد درست این وسایل نظارت داشته و از نفوذ آب به نواحی خارج از محدوده آتش پیشگیری می‌کنند.

۵-۱-۵ پیشگیری و محافظت در مقابل آتش

مرکز میانی خصوصی پارس‌ساین جهت پیشگیری از آتش‌سوزی و مقابله با آن، اقدامات و ملاحظات لازم را به عمل آورده است که در طرح ترمیم خرابی و طرح تداوم خدمات این مرکز به آن پرداخته شده است.

۵-۱-۶ حفاظت از رسانه‌های ذخیره‌سازی

کلیه وسایل ذخیره‌سازی طوری نگهداری می‌شوند که در معرض آب، آتش، الکترومغناطیس و دیگر عوامل محیطی قرار نگیرند. وسایل حاوی اطلاعات بازرسی امنیتی، بایگانی‌ها یا نسخه‌های پشتیبانی اطلاعات در مکانی جدا از تجهیزات مرکز میانی خصوصی پارس‌ساین نگهداری می‌شوند.

۵-۱-۷ انهدام ضایعات

کلیه وسایل حاوی اطلاعات حساس مرکز میانی خصوصی پارس‌ساین، در صورت عدم استفاده، به صورتی که اطلاعات موجود در آن‌ها غیر قابل بازیابی باشد، منهدم می‌شوند. ضمن این‌که سخت‌افزارهای رمزنگاری بی‌مصرف یا غیر قابل استفاده در مرکز، شامل توکن‌ها و HSM قبل از امحای سخت‌افزاری، جهت اطمینان و در صورت امکان، امحای نرم‌افزاری (همراه با بازنویسی[1] فضای حافظه) می‌گردند. کارکنان مرکز میانی خصوصی پارس‌ساین قبل از تخریب این وسایل دلیل آن را ذکر می‌کنند.

۵-۱-۸ نسخه پشتیبان خارج از سایت

مرکز میانی خصوصی پارس‌ساین از اطلاعات حساس خود طبق برنامه منظمی یک نسخه پشتیبان تهیه کرده و در مکانی خارج از سایت با کنترل‌های فیزیکی و فرایندی که در سطح امنیتی سیستم عملیاتی مرکز میانی خصوصی پارس‌ساین است، نگهداری می‌کند.

1 Overwrite

۵-۲ کنترل‌های فرایندی

۵-۲-۱ نقش‌های مورد اطمینان

نقش‌های مورد اطمینان در مرکز میانی خصوصی پارس‌ساین شامل کلیه کارکنانی در مرکز می‌باشد که به فرایندهای احراز هویت و عملیات اجرایی اصلی مرکز دسترسی و یا کنترل دارند و در رده‌های مختلف فعالیت می‌نمایند. شرایط و الزاماتی که در بخش ۵-۳ ذکر شده است، برای افرادی که به عنوان نقش مورد اطمینان انتخاب می‌شوند، بررسی می‌شود.

در مرکز میانی خصوصی پارس‌ساین برخی نقش‌های مورد اطمینان و شرح وظایف هر یک به صورت زیر است:

مدیر مرکز میانی خصوصی پارس‌ساین:

مرکز میانی خصوصی پارس‌ساین به عنوان بخشی از واحد زیرساخت کلید عمومی در شرکت امن‌افزار گستر شریف فعالیت‌های خود را انجام می‌دهد. مدیر مرکز میانی خصوصی پارس‌ساین زیر نظر مدیر واحد زیرساخت کلید عمومی، در ارتباط مستقیم با مدیر دفاتر ثبت‌نام، مدیر مرکز صدور گواهی، و مدیر نگهداری و پشتیبانی است تا بر کلیه عملیاتی که در این مرکز انجام می‌شود، کنترل و نظارت داشته باشد. وی کلیه هماهنگی‌های مورد نیاز، جهت پیشبرد اهداف مرکز را انجام می‌دهد و در صورت نیاز، راهنمایی‌ها و مشاوره‌های لازم را از مدیر واحد زیرساخت کلید عمومی درخواست می‌کند.

مدیر مرکز میانی خصوصی پارس‌ساین از دانش، اطلاعات و تجربیات لازم و کافی مدیریتی و توانایی و تجربه کافی در زمینه دانش زیرساخت کلید عمومی[1] برخوردار می‌باشد. همچنین با کلیه فعالیت‌هایی که جهت صدور گواهی در بخش‌های مختلف مرکز انجام می‌پذیرد، روند اجرای امور و کلیه کارکنان مرکز میانی خصوصی پارس‌ساین به تفکیک وظایف آشنا می‌باشد.

مدیر مرکز میانی خصوصی پارس‌ساین در قبال کارکنان، پیمانکاران و کاربران شخص ثالث مسئولیت‌های زیر را دارد:

- نظارت بر عملیات تولید کلید مرکز میانی در مراسم تولید کلید؛
- مدیریت و نظارت بر فعالیت‌ها و وظایف کارشناس امنیت اطلاعات؛
- مدیریت و نظارت بر فعالیت‌ها و وظایف مدیر دفاتر ثبت‌نام؛

[1] PKI

- مدیریت و نظارت بر فعالیت‌ها و وظایف مدیر مرکز صدور گواهی؛
- مدیریت و نظارت بر فعالیت‌ها و وظایف مدیر نگهداری و پشتیبانی؛
- اطمینان از مسئولیت‌پذیری این افراد در قبال امنیت اطلاعات قبل از اعطای مجوز دسترسی به اطلاعات مهم و محرمانه مرکز میانی خصوصی پارس‌ساین؛
- کنترل نیازهای آموزشی کارکنان مرکز و پیگیری جهت رفع آن‌ها؛
- ارائه راهنمایی‌های لازم مبتنی بر انتظارات مرکز میانی خصوصی پارس‌ساین از کارکنان؛
- تشویق کارکنان به برآوردن سیاست‌های مرکز میانی خصوصی پارس‌ساین؛
- اطمینان از آگاهی افراد در مورد مسئولیت‌های محول شده به آن‌ها؛
- تطبیق سیاست‌های استخدام با سیاست‌های مرکز میانی خصوصی پارس‌ساین.

مدیر دفاتر ثبت‌نام:

بررسی هویت درخواست‌کنندگان و تنظیم درخواست صدور، ابطال و تمدید گواهی در دفاتر ثبت‌نام (شامل دفتر ثبت‌نام پارس‌ساین و دیگر دفاتر ثبت‌نام مرکز میانی خصوصی پارس‌ساین) صورت می‌گیرد.
مدیر دفاتر ثبت‌نام از دانش و اطلاعات کافی مدیریتی برخوردار بوده و با کلیه فعالیت‌هایی که در یک دفتر ثبت‌نام صورت می‌گیرد و روند اجرای امور، آشنا می‌باشد.
مدیر دفاتر ثبت‌نام زیر نظر مدیر مرکز میانی خصوصی پارس‌ساین، فعالیت‌های این مراکز را کنترل و نظارت می‌نماید. عمده وظایفی که وی در مرکز میانی خصوصی پارس‌ساین بر عهده دارد، عبارتند از:

- بررسی درخواست‌های تشکیل دفتر ثبت‌نام؛
- بررسی تطابق عملیات صورت‌گرفته در دفاتر ثبت‌نام با دستورالعمل اجرایی مرکز میانی خصوصی پارس‌ساین؛
- ارائه راهنمایی‌های لازم به کارکنان دفاتر ثبت‌نام؛
- تشویق آن‌ها به برآوردن سیاست‌های مرکز میانی خصوصی پارس‌ساین؛
- اطمینان از آگاهی این افراد در مورد مسئولیت‌های محول شده به آن‌ها؛
- اطمینان از مسئولیت‌پذیری کارکنان دفاتر ثبت‌نام.

مدیر دفتر ثبت‌نام پارس‌ساین:

دفتر ثبت‌نام پارس‌ساین یکی از دفاتر ثبت‌نام فعال در مرکز میانی خصوصی پارس‌ساین است. مدیر دفتر ثبت‌نام پارس‌ساین با کلیه فعالیت‌هایی که در دفتر ثبت‌نام پارس‌ساین صورت می‌گیرد و روند اجرای امور،

آشنا می‌باشد و به گونه‌ای آن‌ها را مدیریت و کنترل می‌نماید که در روند انجام فعالیت‌ها و عملکردها خللی ایجاد نشود.

عمده وظایفی که مدیر دفتر ثبت‌نام پارس‌ساین در مرکز میانی خصوصی پارس‌ساین بر عهده دارد عبارتند از:

- بررسی تطابق عملیات صورت‌گرفته در دفتر ثبت‌نام پارس‌ساین با دستورالعمل اجرایی و سیاست‌های امنیتی مرکز میانی خصوصی پارس‌ساین؛
- نظارت بر فعالیت‌های کارکنان و ارائه راهنمایی‌های لازم به آن‌ها؛
- انتقال مشکلات و مسائل موجود در دفتر ثبت‌نام پارس‌ساین به مدیر دفاتر ثبت‌نام و درخواست راهنمایی و مشاوره از وی.

مدیر مرکز صدور گواهی:

در مرکز صدور گواهی کلیه عملیات مربوط به مدیریت گواهی الکترونیکی شامل صدور، ابطال، انتشار، و تمدید، انتشار CRL و غیره صورت می‌گیرد.

مدیر مرکز صدور گواهی با کلیه فرایندهایی که در مرکز صدور گواهی جهت مدیریت گواهی‌ها انجام می‌گیرد و روند اجرای فعالیت‌ها، آشنا می‌باشد. وی آشنایی کافی در زمینه دانش زیرساخت کلید عمومی دارد.

مدیر مرکز صدور گواهی زیر نظر مدیر مرکز میانی خصوصی پارس‌ساین فعالیت‌های خود را انجام می‌دهد و در ارتباط مستقیم با اپراتور مرکز صدور گواهی است. این شخص وظیفه دارد تا کلیه عملیاتی را که در مرکز صدور گواهی انجام می‌گیرد، کنترل و نظارت نماید.

مدیر مرکز صدور گواهی مسئولیت‌های زیر را بر عهده دارد:

- بررسی تطابق عملیات صورت‌گرفته در مرکز صدور گواهی با دستورالعمل اجرایی مرکز میانی خصوصی پارس‌ساین؛
- اطمینان از آگاهی اپراتور صدور گواهی در مورد مسئولیت‌های محول شده به وی؛
- اطمینان از مسئولیت‌پذیری اپراتور صدور گواهی؛
- ارائه راهنمایی‌های لازم به اپراتور صدور گواهی.

کارشناس امنیت اطلاعات:

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

عمده وظایف کارشناس امنیت اطلاعات به شرح زیر می‌باشد:

- نظارت بر اجرای درست استانداردهای امنیتی IT در کلیه فعالیت‌های انجام شده در مرکز میانی خصوصی پارس‌ساین؛
- پیاده‌سازی و نگهداری سیستم مدیریت امنیت اطلاعات؛
- ارتقا و نظارت بر امنیت شبکه و اطلاعات مرکز؛
- تحلیل ریسک‌های امنیتی متوجه مرکز؛
- تعریف پروژه‌ها و ارائه سیاست‌هایی در راستای بهبود امنیت مرکز؛
- ارزیابی امنیتی مرکز به صورت دوره‌ای؛
- برقراری امنیت در منابع انسانی (منابع انسانی شامل کلیه افرادی است که در مرکز میانی خصوصی پارس‌ساین فعالیت می‌کنند)؛
- فعالیت‌های راهبری مانند مدیریت ماژول‌های امنیتی و عملیات کنترلی و نظارتی؛
- عملیات بازرسی داخلی از مرکز صدور گواهی خصوصی پارس‌ساین و دفتر ثبت‌نام پارس‌ساین و مستندسازی آن‌ها؛
- بایگانی مطمئن مستنداتی که هنگام بازرسی از مرکز تهیه می‌شود؛
- کنترل امنیتی فرایند تولید کلید در مراسم تولید کلید.

اپراتور احراز هویت:

احراز هویت، فرایند شناسایی هویتی است که توسط یک شخص یا برای یک موجودیت سیستمی ادعا شده است.

اپراتور احراز هویت فردی است که در دفتر ثبت‌نام فعالیت می‌کند و مسئولیت احراز هویت افراد متقاضی درخواست‌های مرتبط با گواهی (مثل صدور، ابطال، و غیره) را بر عهده دارد. این فرد باید بر روند اجرای عملیات احراز هویت متقاضی تسلط کافی داشته و از مطالب مندرج در توافق‌نامه سطح ارائه خدمات، تعداد و نوع مدارک مورد نیاز برای هر موجودیت و برای هر نوع گواهی، کاملاً آگاهی داشته باشد.

در دفتر ثبت‌نام پارس‌ساین، اپراتور احراز هویت وظایف زیر را بر عهده دارد:

- دریافت و کنترل مدارک شناسایی متقاضی و نماینده او (در صورت ارائه درخواست توسط نماینده متقاضی) جهت احراز هویت موجودیت با توجه به نوع گواهی مورد درخواست و این‌که گواهی برای چه موجودیتی درخواست شده است؛
- بررسی انطباق توکن ارائه شده توسط متقاضی صدور گواهی با لیست توکن‌های معتبر و قابل اطمینانی که توسط مرکز ریشه منتشر شده است؛
- دریافت اصل قبض واریزی مطابق با مبالغ تعیین‌شده برای هر نوع درخواست، طبق تعرفه‌های مالی مشخص‌شده از سوی مرکز ریشه؛
- بایگانی مدارک شناسایی متقاضی و نمایندگان او (در صورت ارائه درخواست توسط نماینده)، اصل قبض واریزی، و دیگر مستندات.

اپراتور ثبت درخواست:

اپراتور ثبت درخواست فردی است که در دفتر ثبت‌نام فعالیت می‌کند و مسئولیت ثبت کامپیوتری درخواست‌های صدور، تمدید، و ابطال گواهی را بر عهده دارد.

اپراتور ثبت درخواست باید آشنایی کامل با سرویس‌های ارائه شده در نرم‌افزار RA را داشته باشد و از نحوه کار با این نرم‌افزار کاملاً مطلع باشد.

اپراتور ثبت درخواست در دفتر ثبت‌نام وظایف زیر را دارد:

- انجام عملیات کامپیوتری ثبت درخواست صدور، تمدید، و ابطال گواهی و امضای آن درخواست؛
- کنترل تناظر بین کلید خصوصی و کلید عمومی متقاضی با بررسی صحت امضای روی درخواست گواهی که با استفاده از استاندارد PKCS#10 تنظیم شده است (در صورتی که تولید کلید از سوی متقاضی انجام شده باشد)؛
- تولید کلید بر روی توکن سخت‌افزاری متقاضی و نیز ایجاد CSR (در صورتی که تولید کلید به نمایندگی از متقاضی توسط دفتر ثبت‌نام انجام شده باشد).

اپراتور مدیریت گواهی:

اپراتور مدیریت گواهی شخصی است که زیر نظر مدیر مرکز صدور گواهی فعالیت می‌کند و مسئولیت مدیریت درخواست‌های مرتبط با گواهی را بر عهده دارد.

اپراتور مدیریت گواهی بر سرویس‌های ارائه شده در نرم‌افزار CA تسلط کامل داشته و با همه امکانات و قابلیت‌های این نرم‌افزار آشنا می‌باشد.

وظایف عمده اپراتور مدیریت گواهی الکترونیکی عبارتند از:

- رسیدگی و تأیید درخواست‌های امضا شده توسط دفتر ثبت‌نام (صدور، ابطال، و تمدید گواهی)؛
- پشتیبان‌گیری دوره‌ای از سرویس‌دهنده CA و پایگاه داده آن.

کارشناس نگهداری و پشتیبانی مرکز داده:

کارشناس نگهداری مرکز داده، دارای دانش کاملی درباره نحوه پشتیبانی، نگهداری، و عملکرد مرکز داده می‌باشد.

وظایف عمده کارشناس نگهداری مرکز داده عبارتند از:

- نظارت بر عملیات مرکز داده؛
- مدیریت دسترسی فیزیکی به تجهیزات مرکز داده؛
- نظارت و کنترل سیستم‌های تهویه و خنک‌کننده؛
- نظارت و کنترل سیستم‌های اطفاءحریق؛
- نظارت و کنترل سیستم دوربین‌های مداربسته؛
- نظارت و کنترل سیستم برق مرکز داده از جمله UPS و ژنراتور؛
- همکاری با کارشناسان دیگر در صورت لزوم به منظور رفع مشکلات یا بهبود سرویس‌دهی مرکز داده؛
- مطلع کردن مدیر نگهداری و پشتیبانی از هر گونه تغییری که در مرکز داده صورت می‌گیرد؛
- پاسخگویی و راهنمایی کاربران در حوزه وظایف؛
- مستندسازی فعالیت‌ها و سرویس‌های ارائه شده و تهیه و تدوین گزارش و آمارهای درخواستی در حوزه وظایف.

کارشناس نگهداری و پشتیبانی شبکه:

کارشناس نگهداری و پشتیبانی شبکه، دارای دانش و اطلاعات کاملی از کاربرد و نحوه عملکرد تجهیزات شبکه می‌باشد.

وظایف عمده کارشناس نگهداری شبکه عبارتند از:

- نگهداری از کلیه تجهیزات شبکه بر اساس استانداردهای فناوری اطلاعات و ارتباطات؛
- مطلع کردن مدیر نگهداری و پشتیبانی از هر گونه تغییری که در شبکه صورت می‌گیرد؛
- نظارت و بازرسی کلیه عملیات و رویدادهای شبکه در تناوب‌های مشخص؛

- نظارت و بازرسی کلیه عملیات و رویدادهای امنیتی سیستم‌های دیواره‌های آتش و سیستم‌های تشخیص و جلوگیری از نفوذ در تناوب‌های مشخص؛
- شناسایی و رفع مشکلات شبکه‌ای هر یک از سیستم‌های شبکه موجود در مرکز مثل دیواره‌های آتش، سوئیچ‌ها، و غیره؛
- نصب و پیکربندی سیستم‌عامل و نرم‌افزارهای امنیتی مثل آنتی‌ویروس و دیواره‌های آتش بر روی سیستم‌ها؛
- پاسخگویی و راهنمایی کاربران در حوزه وظایف؛
- مستندسازی فعالیت‌ها و سرویس‌های ارائه شده و تهیه و تدوین گزارش و آمارهای درخواستی در حوزه وظایف.

کارشناس نگهداری و پشتیبانی نرم‌افزار:

نگهداری و پشتیبانی نرم‌افزار شامل کلیه عملیاتی است که جهت توسعه و بهبود عملکرد نرم‌افزارهای موجود در مرکز و رفع مشکلات آن‌ها انجام می‌گیرد.

کارشناس نگهداری و پشتیبانی نرم‌افزار دارای آشنایی فنی کافی با نرم‌افزارها و سخت‌افزارهای مرکز می‌باشد.

وظایف عمده کارشناس نگهداری و پشتیبانی نرم‌افزار عبارتند از:

- نصب نرم‌افزارهای RA و CA؛
- نصب و پیکربندی کلیه نرم‌افزارهای مرتبط با صدور گواهی مانند نرم‌افزارهای مخزن و پایگاه داده؛
- شناسایی و رفع مشکلات پیش‌آمده در نرم‌افزارها؛
- ارائه راهکارهای مناسب و پیاده‌سازی آن‌ها جهت بهبود و توسعه نرم‌افزارها؛
- نظارت و پیگیری نگهداری نرم‌افزارها (مثلاً نظارت بر روند تهیه فایل پشتیبان از پیکربندی نرم‌افزارها به صورت دوره‌ای و بایگانی آن‌ها)؛
- پاسخگویی و راهنمایی کاربران در حوزه وظایف؛
- مستندسازی فعالیت‌ها و سرویس‌های ارائه شده و تهیه و تدوین گزارش و آمارهای درخواستی در حوزه وظایف.

کارشناس نگهداری و پشتیبانی سخت‌افزار:

نگهداری و پشتیبانی سخت‌افزار شامل کلیه عملیاتی است که جهت رفع مشکلات و بهبود عملکرد سخت‌افزارهای موجود در مرکز صورت می‌گیرد.

وظایف عمده کارشناس نگهداری و پشتیبانی سخت‌افزار عبارت است از:

- نصب و پیکربندی ملزومات سخت‌افزاری؛
- ارائه مشاوره فنی، کنترل و نظارت در امر تهیه تجهیزات سخت‌افزاری مورد نیاز مرکز؛
- بررسی فنی قطعات و سخت‌افزارهای خریداری شده؛
- تشخیص مشکلات سخت‌افزاری سیستم‌ها و رفع مشکلات به‌وجود آمده؛
- نظارت بر فرایند ارسال تجهیزاتی که نیاز به تعمیر دارند و کنترل کیفیت تعمیر تجهیزات؛
- پاسخگویی و راهنمایی کاربران در حوزه وظایف؛
- مستندسازی فعالیت‌ها و سرویس‌های ارائه شده و تهیه و تدوین گزارش و آمارهای درخواستی در حوزه وظایف.

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

برای افزایش امنیت، فعالیت‌های حساس مرکز میانی خصوصی پارس‌ساین با حضور بیش از یک نقش مورد اطمینان انجام می‌گیرد. این امر از فعالیت‌های مخرب که احتیاج به تبانی دارند، جلوگیری می‌کند.

تعداد افراد مورد نیاز برای هر نقش در سطوح اطمینان مختلف در جدول ۵-۱ آمده است:

جدول ۵-۱ تعداد افراد مورد نیاز برای هر نقش

سطح اطمینان	افراد مورد نیاز برای هر نقش
سطح ۱	توسط ۱ نفر انجام می‌گیرد.
سطح ۲	برای نقش‌هایی که انجام وظایف آن‌ها مستلزم دسترسی به اطلاعات حساس مرکز میانی خصوصی پارس‌ساین مانند کلید خصوصی می‌باشد، حداقل ۲ نفر مورد نیاز است. برای انجام وظایف سایر نقش‌ها، ۱ نفر کافی است.

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

کلیه کارکنان مرکز میانی خصوصی پارس‌ساین که به عنوان نقش مورد اطمینان (مندرج در بخش ۵-۲-۱) در مرکز فعالیت می‌کنند، قبل از شروع به فعالیت، شناسایی و احراز هویت می‌شوند. تمهیداتی که برای شناسایی و احراز هویت هر نقش برای هر سطح اطمینان اتخاذ شده است، عبارتند از:

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

۵-۲-۴ نقش‌های مستلزم تفکیک وظایف

در مرکز میانی خصوصی پارس‌ساین نقش‌هایی که ارتباط مستقیم با مشتری دارند (مانند نقش‌های مرتبط با احراز هویت درخواست‌کنندگان) و نقش‌های مرتبط با عملیات صدور گواهی و همچنین نقش‌های راهبر سیستم دارای وظایف تعریف‌شده و مجزایی می‌باشند. این نقش‌ها به همراه وظایف تعریف‌شده برای آن‌ها در بخش ۵-۲-۱ آمده است.

۵-۳ کنترل کارکنان

مرکز میانی خصوصی پارس‌ساین کارکنان خود را با آموزش کافی برای وظایف‌شان آماده می‌کند. کارهایی که به کارکنان واگذار می‌شود، متناسب با وظایف تعریف‌شده و حدود اختیارات آن‌ها است. علاوه بر این، کارکنان قبل از شروع فعالیت خود موارد زیر را انجام می‌دهند:

۱. تعهد کتبی به منظور رعایت مقررات و عدم افشای اطلاعات حساس و مرتبط با امنیت مرکز یا اطلاعات کاربر امضا می‌کنند؛

۲. با امضای قرارداد، به شرایط و ضوابط موقعیتی که در آن قرار می‌گیرند، پایبند می‌شوند؛

۳. آموزش‌های لازم متناظر با وظایفی که بر عهده دارند را دریافت و آمادگی لازم را کسب می‌کنند.

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

مرکز میانی خصوصی پارس‌ساین در جذب نیروی انسانی به عنوان نقش‌های مورد اطمینان، سوابق، مهارت فنی و قابلیت امانت‌داری آن‌ها را در نظر می‌گیرد. علاوه بر این، تمام کارکنان مرکز دارای تابعیت ایرانی بوده و دارای گواهی عدم سوء پیشینه از نیروی انتظامی جمهوری اسلامی ایران می‌باشند.

افرادی که برای کار با تجهیزات مرکز میانی خصوصی پارس‌ساین انتخاب می‌شوند، دارای مشخصات زیر می‌باشند:

- با موفقیت یک دوره مناسب آموزش را به پایان رسانده‌اند؛
- توانایی خود را برای انجام وظایفی که به ایشان محول شده به اثبات رسانده‌اند؛
- مورد اطمینان هستند؛
- هیچ شغل یا وظیفه دیگری که روی انجام وظایف محوله به آن‌ها تأثیرگذار باشد، ندارند؛
- در گذشته به دلیل کوتاهی و یا عدم اجرای وظایف از هیچ مرکز صدور گواهی دیگری برکنار نشده‌اند؛
- دارای سوء پیشینه نبوده و یا گواهی عدم سوء پیشینه‌شان با اطلاع قبلی باطل نشده است؛
- دارای محکومیت کیفری نیستند.

۵-۳-۲ رویه بررسی سابقه افراد

فرایند بررسی‌های مربوط به سوابق و پیشینه افراد متقاضی جهت تصدی نقش‌های مورد اطمینان در مرکز میانی خصوصی پارس‌ساین به طور خلاصه در زیر آورده شده است:

- بررسی سوابق کاری و مشاغل قبلی متقاضی؛
- بررسی توصیه‌نامه‌های حرفه‌ای؛
- بررسی مدارک مرتبط با سوابق قبلی متقاضی؛
- بررسی آخرین مدرک تحصیلی متقاضی و تطابق آن با نقش در نظر گرفته شده؛
- بررسی عدم سوء پیشینه و نیز سوابق کیفری متقاضی؛
- بررسی سوابق بیمه متقاضی (در موارد خاص)؛
- به عمل آوردن مصاحبه فنی و تخصصی با متقاضی جهت اطمینان از صلاحیت وی جهت تصدی نقش در نظر گرفته‌شده.

۵-۳-۳ الزامات آموزشی

مرکز میانی خصوصی پارس‌ساین آموزش‌های مورد نیاز برای کارکنان خود را متناسب با وظایف و فعالیت های آن‌ها فراهم می‌کند که به صورت دوره‌ای و در صورت نیاز این برنامه‌های آموزشی مرور و اضافه می‌گردد.

برنامه‌های آموزشی شامل موارد زیر می‌باشند:

- آشنایی با اصول امنیتی و ساختار مرکز میانی خصوصی پارس‌ساین؛
- چگونگی کار با نرم‌افزارها و سخت‌افزارهای در حال استفاده؛
- چگونگی گزارش‌دهی و رسیدگی به حوادث؛
- آشنایی با فرایندهای ترمیم خرابی و تداوم کسب و کار؛
- آشنایی با اقدامات امنیتی لازم برای اعمال شرایط سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور؛
- آموزش‌های خاص در صورت لزوم.

۵-۳-۴ الزامات آموزش مکرر و متناوب

مرکز میانی خصوصی پارس‌ساین حداقل یک بار در سال برنامه‌های آموزشی جدیدی را فراهم می‌کند و دانش کارکنان خود را به‌روزرسانی می‌کند تا مطمئن شود که این افراد سطح مهارت مورد نیاز را برای انجام مسئولیت‌های خود در مرکز میانی خصوصی پارس‌ساین، احراز کرده‌اند. همچنین هرگونه تغییر در عملکرد مرکز میانی خصوصی پارس‌ساین در قالب یک برنامه آموزشی به کارکنان ارائه می‌شود. اجرای این برنامه‌های آموزشی مستند می‌شود.

۵-۳-۵ دوره زمانی و ترتیب چرخش کار

در حال حاضر اعمال نشده است.

۵-۳-۶ جریمه‌های اقدامات خارج از محدوده اختیارات

در صورت انجام عملی غیرمجاز یا مشکوک به غیرمجاز توسط کارکنان، مدیر مرکز میانی خصوصی پارس‌ساین جریمه متناسب با اقدام غیرمجاز انجام شده را در نظر گرفته و در صورت صلاحدید، به ادامه همکاری شخص خاطی با مرکز پایان می‌دهد.

۵-۳-۷ الزامات پیمانکاران مستقل

مرکز میانی خصوصی پارس‌ساین طی قراردادها و تفاهم‌نامه‌هایی شرایط و ضوابط همکاری را مشخص می‌کند تا کلیه مراکز طرف قرارداد و اشخاص ثالث طبق سیاست‌های مرکز میانی خصوصی پارس‌ساین و دستورالعمل اجرایی گواهی الکترونیکی عمل کنند.

۵-۳-۸ مستندات فراهم‌شده برای کارکنان

مرکز میانی خصوصی پارس‌ساین مستندات مورد نیاز را به تناسب شرح وظایف کارکنان، در اختیار آن‌ها قرار می‌دهد تا کارکنان مسئولیت‌های خود را به خوبی انجام دهند.

۵-۴ فرایندهای ثبت رویدادهای بازرسی

در این بخش، فرایندهای مرتبط با رویدادها در مرکز میانی خصوصی پارس‌ساین توصیف شده است.

۵-۴-۱ انواع رویدادهای قابل ثبت

مرکز میانی خصوصی پارس‌ساین ظرفیت ثبت همه رویدادهای مربوط به امنیت سیستم مرکز صدور گواهی (شامل دیواره‌های آتش، دایرکتوری‌ها، و سرورهای میزبان نرم‌افزار CA و RA) را در فایل‌های ثبت رویدادهای بازرسی امنیتی دارد. همچنین، قابلیت ثبت رویدادهای امنیتی در سیستم‌عامل‌های تجهیزات مرکز، هنگام شروع به کار سیستم به طور خودکار فعال می‌باشند.

رویدادهای زیر در مرکز میانی خصوصی پارس‌ساین توسط سیستم یا نرم‌افزار CA یا RA ثبت می‌گردد:

- ورود و خروج به برنامه‌های کاربردی مرکز صدور گواهی یا دفتر ثبت‌نام؛
- هر تلاش ناموفق برای ورود به برنامه‌های کاربردی مرکز صدور گواهی یا دفتر ثبت‌نام؛

- تلاش برای تعیین و حذف گذرواژه، یا تغییر مجوزهای ورود به برنامه‌های کاربردی مرکز صدور گواهی یا دفتر ثبت‌نام؛
- تغییر، حذف، یا اضافه کردن کاربران و نقش‌ها در برنامه‌های کاربردی مرکز صدور گواهی یا دفتر ثبت‌نام؛
- هر تغییر در پیکربندی مرکز صدور گواهی یا دفتر ثبت‌نام که پس از هر تغییر، یک نسخه از فایل پیکربندی همراه با امضا و زمان انجام آن، در پایگاه داده ذخیره می‌شود؛
- پس از هر تغییر در پروفایل گواهی، یک نسخه از فایل حاوی پیکربندی پروفایل به همراه امضا و زمان انجام آن، در پایگاه داده ذخیره می‌شود؛
- پشتیبان‌گیری و بازیابی پایگاه داده؛
- تولید کلیدهای مرکز صدور گواهی؛
- صدور، ابطال، و تمدید گواهی‌ها؛
- امضای لیست گواهی‌های باطل‌شده؛
- تولید درخواست‌های تنظیم و تأییدشده در دفاتر ثبت‌نام؛
- ارسال هر داده‌ای به مخزن؛
- انجام عملیات نوشتن ناموفق در مخزن گواهی‌ها و لیست گواهی‌های باطل‌شده؛
- خطاهای رخ داده در سیستم.

کلیه رویدادهای ثبت‌شده (به صورت دستی یا الکترونیکی) دارای تاریخ و زمان رویداد می‌باشند. رویدادهای مربوط به RA یا CA به‌صورت مجزا ثبت می‌شوند و می‌توانند هنگام افزوده شدن به پایگاه داده، در پایگاه‌های داده مجزا و یا پایگاه داده مشترک، ثبت شوند.

مرکز صدور گواهی، اطلاعاتی که به صورت دستی یا الکترونیکی توسط سیستم مرکز صدور گواهی ثبت نشده‌اند را جمع‌آوری می‌نماید. این اطلاعات عبارتند از:

- رویدادهای مربوط به دسترسی‌های فیزیکی؛
- تغییرات مربوط به پیکربندی سیستم؛
- تغییرات مربوط به کارکنان مرکز صدور گواهی؛
- گزارشات مربوط به اختلافات و تفاهم‌ها؛
- گزارشات مربوط به از بین رفتن اطلاعات حساس؛

- نسخه‌های قبلی و جاری دستورالعمل اجرایی گواهی الکترونیکی؛
- گزارشات مربوط به ارزیابی آسیب‌پذیری؛
- گزارشات مربوط به ارزیابی تهدیدات و مخاطره‌ها؛
- خرابی تجهیزات؛
- زمان و مدت قطع جریان برق؛
- گزارشات مربوط به قبول بازدید و بازرسی؛
- نسخه‌های قبلی و جاری توافق‌نامه کاربر و دیگر اطلاعاتی که مالک گواهی با آن‌ها موافقت کرده است؛
- انتصاب کارکنان مرکز؛
- آموزش کارکنان مرکز.

۵-۴-۲ تناوب پردازش اطلاعات رویدادهای ثبت‌شده

مرکز میانی خصوصی پارس‌ساین به صورت دوره‌ای کلیه رویدادهای مهم را بررسی مجدد و پیگیری می‌کند. این فعالیت شامل اعمالی از قبیل بررسی اطلاعات ثبت‌شده رویدادهای سیستمی و اسناد کاغذی ثبت رویدادها جهت اطمینان از عدم دستکاری آن‌ها و بازرسی همه ورودی‌های آن می‌باشد. هر جا که یک اخطار و ناهماهنگی مشاهده شود، تحقیقات کامل‌تر و بیشتری انجام می‌شود و همه رویدادهای الکترونیکی و دستی، شامل رویدادهای سمت دفتر ثبت‌نام، بررسی می‌شوند. کارشناس امنیت اطلاعات در مرکز میانی خصوصی پارس‌ساین مسئول انجام این بازرسی می‌باشد. کلیه فعالیت‌هایی که در این بازنگری‌ها صورت می‌گیرد، مستند می‌شوند.

در جدول ۵-۲ تناوب این دوره بر اساس سطح اطمینان، مورد بررسی قرار گرفته است:

جدول ۵-۲ تناوب پردازش اطلاعات رویدادهای ثبت‌شده

سطح اطمینان	تناوب پردازش اطلاعات رویدادهای ثبت‌شده
سطح ۱	پردازش و بازنگری رویدادها حداقل هر شش ماه یک‌بار صورت می‌گیرد.
سطح ۲	پردازش و بازنگری رویدادها حداقل هر دو ماه یک‌بار صورت می‌گیرد.

۵-۴-۳ دوره نگهداری از اطلاعات رویدادهای ثبت‌شده

رویدادهای ثبت‌شده مرکز، حداقل ۲ ماه در سایت نگهداری می‌شود و پس از آن به روشی که در بخش ۵-۵-۲ آورده شده است، حفظ و نگهداری می‌گردد.

۵-۴-۴ محافظت از اطلاعات رویدادهای ثبت‌شده

رویدادهای ثبت‌شده توسط یک سرویس‌دهنده رویدادنگار[1] محافظت و نگهداری می‌گردد و افراد مجاز تنها پس از احراز هویت می‌توانند به سرویس‌دهنده دسترسی داشته باشند. بدین ترتیب، امکان مشاهده، تغییر، حذف، یا تخریب این اطلاعات برای افراد غیرمجاز وجود ندارد. همچنین فردی که موظف به بایگانی اطلاعات رویدادهای ثبت‌شده است، قادر به تغییر اطلاعات نیست. یک نسخه پشتیبان از اطلاعات رویدادهای ثبت‌شده در مکانی خارج از سایت اصلی نگهداری می‌شود.

۵-۴-۵ فرایندهای پشتیبان‌گیری از رویدادهای بازرسی

تهیه نسخه پشتیبان از رویدادهای ثبت شده، روزانه به صورت افزایشی و ماهانه به طور کامل صورت می‌گیرد.

۵-۴-۶ سامانه جمع‌آوری اطلاعات بازرسی

اطلاعات بازرسی (رویدادهای سیستمی) در نرم‌افزار، شبکه، و سیستم‌عامل تولید و ثبت می‌شود. اطلاعات بازرسی دستی توسط کارکنان مرکز میانی خصوصی پارس‌ساین در فرم‌های مربوطه ثبت می‌گردد.

فرایند ثبت رویدادها با راه‌اندازی سیستم مرکز میانی خصوصی پارس‌ساین فعال می‌شود و تنها هنگام توقف عملیات مرکز، متوقف خواهد شد. چنانچه مشخص شود که در سیستم ثبت رویدادها اشکالی وجود دارد به‌طوری که تمامیت سیستم و محرمانگی اطلاعات را به مخاطره می‌اندازد، مرکز صدور گواهی خصوصی پارس‌ساین فعالیت‌های صدور گواهی خود را به غیر از فرایند ابطال گواهی، به طور موقت تا زمانی که مشکل برطرف شود، متوقف می‌کند.

1 Log server

۵-۴-۷ تذکر به مسبب رویداد

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

۵-۴-۸ ارزیابی آسیب‌پذیری

رویدادها در فرایند بازرسی، به منظور ارزیابی آسیب‌پذیری سیستم ثبت می‌گردند. در مرکز میانی خصوصی پارس‌ساین، اطلاعات ثبت وقایع امنیتی برای وقایعی مانند فعالیت‌های ناموفق تکراری برای دسترسی به سیستم، اقدام برای به‌دست آوردن اطلاعات محرمانه، تلاش برای دسترسی به فایل‌های سیستمی و پاسخ‌های تأیید نشده، بررسی و بازبینی می‌شوند. همچنین، پیوستگی اطلاعات ثبت وقایع امنیتی بررسی و خلاصه نتایج حاصل مستند می‌شود.

۵-۵ بایگانی اطلاعات

۵-۵-۱ انواع اطلاعات قابل بایگانی

مرکز میانی خصوصی پارس‌ساین اطلاعات زیر را بایگانی می‌نماید:

- دستورالعمل‌های اجرایی گواهی؛
- هر توافق‌نامه پیمانی که مرکز میانی خصوصی پارس‌ساین به آن مقید است؛
- پیکربندی تجهیزات سیستم؛
- درخواست‌ها (صدور، ابطال، و تمدید گواهی)؛
- مستندات احراز هویت درخواست‌کننده و مالک گواهی مطابق با بخش ۳-۲-۳؛
- مستندات دریافت رسید از متقاضی و پذیرش گواهی مطابق با بخش ۴-۴؛
- کلیه گواهی‌ها و لیست گواهی‌های باطل‌شده (یا اطلاعات ابطال دیگر)؛
- کلیه رویدادهای ثبت‌شده (مطابق با بخش ۵-۴)؛
- فایل‌های درخواست امضای گواهی (CSR)؛
- تاریخ و دلیل ابطال گواهی‌های باطل‌شده؛
- کلیه گزارشات مربوط به بازرسی داخلی؛

- نسخه پشتیبان پایگاه داده سیستم صدور و مدیریت گواهی الکترونیکی؛
- توافق‌نامه‌های بین مالک گواهی یا درخواست‌کننده و مرکز میانی خصوصی پارس‌ساین؛
- توافق‌نامه یا قراردادهای منعقد شده بین مرکز میانی خصوصی پارس‌ساین و دفاتر ثبت‌نام؛
- کلیه مکاتبات با شورا، مراکز دیگر و بازرسان ثبت وقایع.

۵-۵-۲ دوره نگهداری اطلاعات بایگانی‌شده

اطلاعات ثبت‌شده در بایگانی مرکز میانی خصوصی پارس‌ساین برای هر سطح اطمینان مطابق با جدول ۵-۳ نگهداری می‌گردد.

جدول ۵-۳ دوره نگهداری اطلاعات ثبت‌شده در بایگانی

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

۵-۵-۳ محافظت از بایگانی

از بایگانی اطلاعات طوری محافظت می‌شود که فقط افراد مجاز پس از احراز هویت توسط سیستم، می‌توانند به آن دسترسی داشته باشند. بایگانی اطلاعات در یک سیستم امن ذخیره‌سازی می‌شود تا از معرض دید افراد غیرمجاز، تغییر، حذف یا عملیات پنهانی دیگر محفوظ بماند. کارکنان مجاز با وسایل دسترسی امن خود به سخت‌افزار نگهدارنده اطلاعات بایگانی و نرم‌افزارهایی که این اطلاعات را پردازش می‌کنند، دسترسی دارند.

۵-۵-۴ فرایندهای پشتیبان‌گیری از بایگانی

در مرکز میانی خصوصی پارس‌ساین، از اطلاعات الکترونیکی به صورت دوره‌ای نسخه پشتیبان تهیه می‌شود. فرایند تهیه نسخه پشتیبان در جدول ۵-۴ آمده است.

جدول ۵-۴ فرایند پشتیبان‌گیری از اطلاعات بایگانی

سطح اطمینان	فرایند پشتیبان‌گیری از اطلاعات بایگانی
سطح ۱	الزامی در نظر گرفته نشده است.
سطح ۲	از بایگانی اطلاعات الکترونیکی به صورت افزایشی و به طور کامل و ماهیانه نسخه

سطح اطمینان	فرایند پشتیبان‌گیری از اطلاعات بایگانی
	پشتیبان تهیه می‌شود.

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

گواهی‌ها، لیست گواهی‌های باطل‌شده و کلیه اطلاعات مربوط به ابطال گواهی که در پایگاه داده مرکز میانی خصوصی پارس‌ساین بایگانی شده است، شامل زمان و تاریخ ثبت اطلاعات نیز می‌باشد. کلیه اطلاعات بایگانی‌شده در فرم‌های کاغذی نیز باید دارای تاریخ باشند.

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

اطلاعات الکترونیکی بایگانی در مرکز میانی خصوصی پارس‌ساین به صورت امن و مطمئن در رسانه‌های ذخیره‌سازی نگهداری می‌شود. مستندات کاغذی در محفظه‌های امن نگهداری می‌شوند.

۵-۵-۷ فرایندهای به‌دست آوردن و بررسی اطلاعات بایگانی

مرکز میانی خصوصی پارس‌ساین تمامیت اطلاعات بایگانی‌شده را به‌صورت دوره‌ای مورد ارزیابی قرار می‌دهد. در جدول ۵-۵ جزئیات این فرایند آمده است.

جدول ۵-۵ فرایندهای به‌دست آوردن و بررسی اطلاعات بایگانی

سطح اطمینان	فرایندهای به‌دست آوردن و بررسی اطلاعات بایگانی
سطح ۱	فرایند خاصی در نظر گرفته نشده است.
سطح ۲	• تنها افراد مورد اطمینان مجاز می‌توانند به اطلاعات بایگانی‌شده دسترسی پیدا کنند. • تمامیت اطلاعات بایگانی‌شده، هر ۶ ماه یک بار مورد بررسی قرار می‌گیرد. همچنین تمامیت کپی‌های کاغذی خارج از سایت نیز هر ۱ سال یک بار بررسی می‌شود. برای اطمینان از تمامیت داده‌های الکترونیکی، این داده‌ها امضای دیجیتال می‌شوند.

۵-۶ تغییر کلید

مرکز میانی خصوصی پارس‌ساین در مواردی که احساس کند کلید خصوصی مرکز صدور گواهی افشا

1 Time Stamp

شده و یا در خطر افشا قرار دارد و یا در صورت بروز مشکلات دیگر که مرکز تشخیص دهد کلید خصوصی باید تجدید شود، اقدام به تجدید کلید خصوصی می‌کند. بدین منظور، مرکز میانی خصوصی پارس‌ساین درخواست تجدید کلید خود را به مرکز ریشه ارائه می‌دهد. در صورت تأیید درخواست ارائه شده از سوی مرکز ریشه، مرکز میانی خصوصی پارس‌ساین اقدام به تولید زوج‌کلید و فایل CSR جدید می‌نماید. فایل CSR در اختیار مرکز ریشه قرار می‌گیرد تا گواهی جدید صادر شود. مرکز صدور گواهی خصوصی پارس‌ساین، گواهی جدید را از طریق مخزن منتشر می‌کند و از آن پس گواهی‌های صادرشده و لیست گواهی‌های باطل‌شده را با کلید خصوصی جدید امضا می‌کند.

در مرکز میانی خصوصی پارس‌ساین فرایند تجدید کلید برای مالکان گواهی در حال حاضر پشتیبانی نمی‌شود.

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

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

اگر مشخص شود که تلاشی برای هک کردن مرکز میانی خصوصی پارس‌ساین صورت گرفته و یا اطلاعات به شکل پنهانی دیگری در معرض افشا شدن قرار دارند، به‌منظور تعیین نوع و میزان آسیب وارد شده، این تلاش‌ها بررسی می‌شوند. اگر احتمال رود که کلید خصوصی افشا شده است، فرایندهایی که در بخش ۵-۷-۳ آمده است، انجام می‌شود. در غیر این صورت، آسیب پنهانی واردشده ارزیابی می‌شود تا اقدامات مقتضی صورت گیرد.

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

مرکز میانی خصوصی پارس‌ساین جهت بازیابی عملیات مرکز هنگام بروز خرابی که منجر به از بین رفتن تجهیزات، نرم‌افزار و اطلاعات می‌شود، تمهیدات لازم را در نظر گرفته است.

استراتژی بازیابی خرابی مرکز میانی خصوصی پارس‌ساین بر سه اصل زیر بنا نهاده شده است:

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

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

۱. پاسخ سریع با هدف ارزیابی سطح خرابی، تعیین برنامه و افراد مربوطه؛
۲. فراهم نمودن حداقل سطح سرویس؛
۳. بازیابی سرویس‌های کلیدی؛
۴. بازیابی فرایند کسب و کار به حالت عادی.

برای انجام عملیات فوق، تیم پاسخ‌گویی به حادثه در مرکز میانی خصوصی پارس‌ساین با ارزیابی سطح خرابی، تیم بازیابی خرابی را تشکیل می‌دهد. وظایف عمده تیم بازیابی خرابی عبارتند از:

- دریافت مجوز جهت دسترسی به تجهیزات آسیب‌دیده و یا محل وقوع حادثه؛
- تأمین تجهیزات اداری و فضای کار مورد نیاز؛
- تأمین و نصب اجزای سخت‌افزاری مورد نیاز؛
- تأمین و آماده‌سازی رسانه پشتیبان؛
- بازگردانی سیستم‌عامل و برنامه‌های مورد استفاده؛
- بازگردانی داده‌ها؛
- آزمایش عملیاتی سیستم به همراه ملاحظات امنیتی؛
- اتصال سیستم به شبکه و یا سیستم‌های خارجی مرتبط؛
- گزارش عملیات انجام شده و وضعیت موجود به تیم پاسخ‌گویی به حادثه.

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

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

- صدور و انتشار گواهی‌ها و لیست ابطال را متوقف می‌کند؛
- درخواست ابطال گواهی خود را به مرکز دولتی صدور گواهی الکترونیکی ریشه ارائه می‌نماید؛
- یک زوج‌کلید جدید تولید کرده و درخواست صدور گواهی جدید را به مرکز دولتی صدور گواهی الکترونیکی ریشه ارائه می‌نماید؛
- با ابطال گواهی افشاشده و صدور گواهی جدید، کلیه گواهی‌های معتبری که قبلاً توسط کلید افشاشده، امضا شده بود را باطل می‌نماید؛

- CRL جدید را از طریق مخزن منتشر می‌کند.

اگر کلید خصوصی مالک گواهی افشا شود و یا در خطر افشا قرار بگیرد، مالک گواهی می‌بایست فوراً جهت ارائه درخواست ابطال گواهی به یکی از دفاتر ثبت‌نام مرکز میانی خصوصی پارس‌ساین مراجعه نماید. با ابطال گواهی، تمام طرف‌های اعتمادکننده از طریق لیست گواهی‌های باطل شده که توسط مرکز منتشر می‌شود، از ابطال گواهی مذکور اطلاع می‌یابند.

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

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

مرکز میانی خصوصی پارس‌ساین تمهیدات لازم را برای تداوم ارائه خدمات خود و بازیابی خرابی در صورت وقوع خرابی در نظر گرفته است. این تمهیدات به صورت کامل مستند شده و در اختیار کارکنان مرکز قرار داده شده است تا در شرایط اضطراری روش مناسب و مطمئنی برای از سرگیری فعالیت‌های مرکز پیش رو داشته باشند.

طرح تداوم ارائه خدمات شامل موارد زیر می‌باشند:

- تخصیص نقش‌های مورد نیاز برای انجام مسئولیت‌های مختلف به کارکنان مرکز و تشکیل تیم‌های مورد نیاز؛
- تعیین و مستندسازی کلیه عملیات و فرایندهایی که قبل از پیاده‌سازی طرح باید دنبال شود؛
- چگونگی پاسخ به حادثه در شرایط اضطراری به طوری که کمترین آسیب به فرایند کسب و کار مرکز وارد شود؛
- چگونگی بازگردانی فرایندهای کسب و کار به حالت عادی؛
- چگونگی بازیابی خرابی‌های ممکن؛
- پیاده‌سازی آزمون جهت حصول اطمینان از عملیاتی بودن طرح؛
- اطلاع‌رسانی و ارائه آموزش‌های لازم جهت پیشگیری از تکرار خرابی‌ها.

۵-۸ توقف فعالیت مرکز صدور گواهی یا دفتر ثبت‌نام

در صورتی که لازم شود مرکز میانی خصوصی پارس‌ساین فعالیت خود را متوقف کند، این مرکز قبل از توقف عملیات، این موضوع را به مرکز ریشه، مالکان گواهی، و دیگر موجودیت‌های متأثر اطلاع‌رسانی می‌کند.

به محض توقف فعالیت مرکز میانی خصوصی پارس‌ساین، کلیدهای خصوصی که وجود داشته‌اند یا ممکن است برای عملیات رمزنگاری مرکز میانی استفاده شوند، با دلیل ابطال متوقف شدن سرویس[1]، باطل می‌شوند. علاوه بر این، مرکز میانی خصوصی پارس‌ساین مطابق با بخش ۶-۲-۱۰ کلیدهای خصوصی را از بین می‌برد. همچنین، لیست گواهی‌های باطل شده تولید و منتشر می‌شوند.

مراحل قابل اجرا برای توقف عملیات مرکز صدور گواهی خصوصی پارس‌ساین به شرح زیر است:

- اطلاع‌رسانی به مرکز دولتی صدور گواهی الکترونیکی ریشه و طرح مسأله در شورا حداقل ۴ ماه قبل از پایان فعالیت مرکز میانی خصوصی پارس‌ساین؛
- اطلاع‌رسانی به موجودیت‌های متأثر از خاتمه فعالیت مرکز، مثل مالکان گواهی، طرف‌های اعتمادکننده، دفاتر ثبت‌نام و مشتریان؛
- ابطال گواهی مرکز صدور گواهی خصوصی پارس‌ساین توسط مرکز ریشه؛
- حفاظت از بایگانی‌های مرکز میانی خصوصی پارس‌ساین برای مدت زمان تعیین‌شده در این سند و ارائه آن‌ها به یک مرجع معتبر که توسط شورا تعیین می‌شود.

هنگام توقف عملیات مرکز میانی خصوصی پارس‌ساین، این مرکز اطلاعات خود را توسط متولی مجاز و طبق الزامات بایگانی تعیین‌شده در بخش ۵-۵ نگهداری می‌نماید. این اطلاعات شامل موارد زیر می‌باشد:

- گواهی مرکز صدور گواهی خصوصی پارس‌ساین؛
- گواهی‌های صادره؛
- لیست گواهی‌های باطل‌شده؛
- اطلاعات بازرسی امنیتی که در بخش ۵-۴ آمده است؛ و
- دیگر اطلاعات بایگانی‌شده همان‌طور که در بخش ۵-۵ آمده است.

1 Cessation of service

هنگام توقف عملیات، مرکز میانی خصوصی پارس‌ساین برای نگهداری هـر داده (مثـل گـذرواژه) اطمینـان حاصل می‌کند که آن داده قابل استفاده است (برای مثـال، داده‌هـای رمـز شـده در آینـده قابـل رمزگشـایی می‌باشند). لازم به ذکر است که اطلاعات به صورت امن به مکان‌هایی که در آن‌جا نگهداری خواهنـد شـد، منتقل می‌شوند (مطابق با بخش ۵-۱-۸).

۶ کنترل‌های امنیتی فنی

این بخش به تشریح اقدامات امنیتی قابل انجام توسط مرکز میانی خصوصی پارس‌ساین برای حفاظت از کلیدهای رمزنگاری و داده‌های فعال‌سازی (مانند گذرواژه) می‌پردازد.

۶-۱ تولید و نصب زوج‌کلید

۶-۱-۱ تولید زوج‌کلید

۶-۱-۱-۱ تولید زوج‌کلید مرکز صدور گواهی خصوصی پارس‌ساین

انجام عملیات تولید کلید برای مرکز صدور گواهی خصوصی پارس‌ساین در مراسم تولید کلید و مطابق با سیاست‌های امنیتی مرکز ریشه صورت می‌گیرد. مرکز صدور گواهی خصوصی پارس‌ساین از زوج‌کلید الگوریتم RSA جهت صدور گواهی، پشتیبانی می‌نماید.

سیاست‌های امنیتی در نظر گرفته شده توسط مرکز میانی خصوصی پارس‌ساین، برای تولید زوج‌کلید مرکز صدور گواهی، در جدول ۶-۱ قید شده است:

جدول ۶-۱ تولید زوج‌کلید مرکز صدور گواهی

سطح اطمینان	تولید زوج‌کلید مرکز صدور گواهی
سطح ۱	با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور و توسط نقش مورد اعتماد و مجاز صورت می‌پذیرد.
سطح ۲	• توسط یک متصدی با نقش مورد اعتماد و مجاز برای تولید کلید صورت می‌پذیرد. • داخل ماژول امنیتی سخت‌افزاری امنیتی انجام می‌پذیرد که حداقل الزامات بخش ۶-۲-۱ را در بر می‌گیرد. • با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت

سطح اطمینان	تولید زوج‌کلید مرکز صدور گواهی
	می‌پذیرد. • در سطح سوم انجام عملیات تولید کلید از طریق کنترل چندنفره مطابق با بخش ۶-۲-۲ صورت می‌گیرد.

۶-۱-۱-۲ تولید زوج‌کلید دفاتر ثبت‌نام

سیاست‌های امنیتی در نظر گرفته شده توسط مرکز میانی خصوصی پارس‌ساین، برای تولید زوج‌کلید دفتر ثبت‌نام، در جدول ۶-۲ قید شده است:

جدول ۶-۲ تولید زوج‌کلید دفتر ثبت‌نام

سطح اطمینان	تولید زوج‌کلید دفتر ثبت‌نام
سطح ۱	با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت می‌پذیرد.
سطح ۲	• داخل ماژول امنیتی سخت‌افزاری انجام می‌پذیرد که حداقل الزامات بخش ۶-۲-۱ را در بر می‌گیرد. • با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت می‌پذیرد.

۶-۱-۱-۳ تولید زوج‌کلید مالک گواهی

متقاضی درخواست گواهی به دو روش می‌تواند به تولید زوج‌کلید اقدام کند:

- شخص متقاضی گواهی، خود به تولید زوج‌کلید اقدام کند و فایل CSR را مطابق با استاندارد PKCS#10 به دفتر ثبت‌نام تحویل دهد؛
- تولید زوج‌کلید بر روی توکن سخت‌افزاری[۱] متقاضی و نیز تولید CSR، در دفتر ثبت‌نام صورت گیرد.

تولید زوج‌کلید در دفتر ثبت‌نام، فقط با استفاده از توکن‌های قابل اطمینان و معتبری که مورد تأیید مرکز ریشه می‌باشد، انجام می‌شود. از این‌رو، دفتر ثبت‌نام انطباق توکن ارائه شده توسط متقاضی صدور گواهی را با توکن‌های مورد تأیید مرکز ریشه، بررسی می‌کند.

۱ طبق سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور»، تولید کلید به‌صورت نرم‌افزاری صرفاً باید توسط مالک گواهی صورت گیرد.

چگونگی انجام عملیات تولید زوج‌کلید برای مالکان گواهی درجدول ۶-۳ آمده است.

جدول ۶-۳ تولید زوج‌کلید مالکان گواهی

سطح اطمینان	تولید زوج‌کلید مالکان گواهی
سطح ۱	تولید زوج‌کلید مالکان گواهی با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت می‌پذیرد.
سطح ۲	• تولید زوج‌کلید برای مالک گواهی در یک توکن نرم‌افزاری و ترجیحاً سخت‌افزاری که در آن حداقل الزامات بخش ۶-۲-۱ رعایت شده است، صورت می‌پذیرد (تولید کلید به صورت نرم‌افزاری صرفاً توسط مالک گواهی صورت می‌گیرد و کلید عمومی متناظر در قالب استاندارد PKCS#10 به دفتر ثبت‌نام تحویل داده می‌شود). • تولید زوج کلید برای مالکان گواهی با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت می‌پذیرد.

۶-۱-۲ تحویل کلید خصوصی به موجودیت نهایی

عملیات تولید کلید خصوصی مالک گواهی معمولاً توسط درخواست‌کننده گواهی انجام می‌شود و نیازی به تحویل کلید به وی نمی‌باشد. با این حال، در صورتی که کلید خصوصی مالک گواهی توسط دفتر ثبت‌نام تولید شود، لازم است کلید خصوصی به صورت امن به وی تحویل داده شود. چگونگی انجام این کار در مرکز میانی خصوصی پارس‌ساین، در جدول ۶-۴ آورده شده است.

جدول ۶-۴ تحویل کلید خصوصی به مالک گواهی

سطح اطمینان	تحویل کلید خصوصی به مالک گواهی
سطح ۱	الزامی در نظر گرفته نشده است.
سطح ۲	چنانچه عملیات تولید کلید توسط دفتر ثبت‌نام به نمایندگی از مالک گواهی صورت گیرد، این عملیات با استفاده از توکن سخت‌افزاری که مورد تأیید مرکز ریشه می‌باشد، انجام می‌گیرد و کلید خصوصی از طریق این سخت‌افزار در اختیار مالک گواهی قرار داده می‌شود. تولید کلید به صورت نرم‌افزاری صرفاً توسط مالک گواهی صورت می‌گیرد.

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

کلید عمومی مالک گواهی در قالب یک فایل درخواست امضای گواهی (CSR) مطابق با استاندارد PKCS#10 پس از تنظیم درخواست نهایی و امضای درخواست توسط دفتر ثبت‌نام، در اختیار مرکز صدور گواهی خصوصی پارس‌ساین قرار می‌گیرد.

۶-۱-۴ تحویل کلید عمومی مرکز صدور گواهی خصوصی پارس‌ساین به طرف‌های اعتمادکننده

مرکز صدور گواهی خصوصی پارس‌ساین گواهی خود (که حاوی کلید عمومی مرکز است) را از طریق مخزن مرکز میانی خصوصی پارس‌ساین در اختیار طرف‌های اعتمادکننده قرار می‌دهد. دسترسی و اعمال تغییر در مخزن فقط توسط نقش‌های مجاز مرکز میانی خصوصی پارس‌ساین امکان‌پذیر است، لذا تمامیت و صحت کلید عمومی تأمین می‌شود.

۶-۱-۵ طول کلید

مرکز میانی خصوصی پارس‌ساین از الگوریتم RSA برای تولید زوج‌کلید استفاده می‌کند. حداقل طول کلید در نظر گرفته‌شده برای موجودیت‌ها در جدول ۶-۵ آمده است:

جدول ۶-۵ طول کلید موجودیت‌ها

سطح اطمینان	طول کلید
سطوح ۱ و ۲	حداقل طول کلید برای مرکز صدور گواهی خصوصی پارس‌ساین، ۲۰۴۸ بیت RSA و حداقل طول کلید برای دفتر ثبت‌نام و مالکان گواهی، ۱۰۲۴ بیت RSA می‌باشد.

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

در حال حاضر تعریف نشده است.

۶-۱-۷ موارد کاربرد کلید (طبق فیلد کاربرد کلید[1] در X.509 v3)

موارد کاربرد کلید در جدول ۶-۶ آمده است.

[1] Key Usage

جدول ۶-۶ موارد کاربرد کلید

سطح اطمینان	موارد کاربرد کلید
سطح ۱	الزامی در نظر گرفته نشده است.
سطح ۲	مالک گواهی باید از کلید خصوصی متناظر با گواهی الکترونیکی خود، صرفاً در کاربردهای در نظر گرفته شده در فیلد KeyUsage و ExtendedKeyUsage گواهی استفاده نماید. کاربردهای در نظر گرفته شده برای گواهی الکترونیکی در بخش ۱-۴-۱ توصیف شده است. ضمن این‌که فیلد کاربرد کلید گواهی مطابق با «سند جامع پروفایل‌های زیرساخت کلید عمومی کشور» به‌کار می‌رود.

۶-۲ محافظت از کلیدهای خصوصی و کنترل‌های مهندسی ماژول امنیتی

۶-۲-۱ کنترل‌ها و استانداردهای ماژول‌های امنیتی

کلید خصوصی مرکز صدور گواهی خصوصی پارس‌ساین در یک ماژول امنیتی سخت‌افزاری (HSM) ذخیره می‌گردد که در آن ملزومات امنیتی مطابق با آخرین نسخه استاندارد FIPS 140-2 در سطح سوم رعایت شده است.

همچنین انجام عملیات تولید کلید برای مرکز صدور گواهی خصوصی پارس‌ساین و امضای کلیه گواهی‌های صادرشده توسط این مرکز از طریق این HSM به‌صورت داخلی و توسط تراشه[1] صورت می‌گیرد.

الزامات مربوط به کنترل‌ها و استانداردهای ماژول‌های امنیتی در زیرساخت کلید عمومی کشور، در جدول ۶-۷ خلاصه شده است:

جدول ۶-۷ الزامات ماژول‌های امنیتی

سطح اطمینان	آخرین نسخه FIPS 140	مراکز صدور گواهی	دفتر ثبت‌نام	مالکان گواهی
سطح ۱	مورد نیاز نیست.	حداقل الزامات سطح	حداقل الزامات سطح	مورد نیاز نیست.

[1] On-board

سطح اطمینان	آخرین نسخه FIPS 140	مراکز صدور گواهی	دفتر ثبت‌نام	مالکان گواهی
		دوم FIPS 140 اعمال شده باشد.	اول FIPS 140 اعمال شده باشد.	
سطح ۲	مورد نیاز است.	حداقل الزامات سطح سوم FIPS 140 اعمال شده باشد.	حداقل الزامات سطح دوم FIPS 140 اعمال شده باشد.	حداقل الزامات سطح اول و ترجیحاً سطح دوم FIPS 140 اعمال شده باشد.

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

طبق سیاست‌های گواهی الکترونیکی زیر ساخت کلید عمومی کشور، کنترل چند نفره در عملیات تولید و استفاده از کلید خصوصی در مرکز میانی خصوصی پارس‌ساین، در سطوح ۱ و ۲ مورد نیاز نیست.

۶-۲-۳ دستیابی قانونی به کلید خصوصی

قابل اعمال نیست.

۶-۲-۴ پشتیبان‌گیری از کلید خصوصی

مرکز صدور گواهی خصوصی پارس‌ساین، زوج کلید خود را بر روی ماژول امنیتی سخت‌افزاری (HSM) ذخیره می‌کند. برای جلوگیری از خسارت‌های ناشی از خرابی HSM و عدم دسترسی به کلید خصوصی، از زوج‌کلید مرکز صدور گواهی پارس‌ساین، پشتیبان تهیه می‌گردد تا در مواقع خرابی، بتوان کلیدها را بازگردانی نمود (لازم به ذکر است طبق سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور، این مرکز پشتیبان‌گیری از زوج‌کلید سطح یک را به طور اختیاری انجام می‌دهد). پشتیبان‌گیری از کلیدها شامل کپی کردن کلیدها به صورت امن به رسانه پشتیبان‌گیری و طبق بخش‌های ۶-۲-۶ و ۶-۲-۷ می‌باشد.

زوج‌کلیدها روی پارتیشن‌های HSM ذخیره می‌شوند. بنابراین، می‌بایست از پارتیشن‌های HSM پشتیبان تهیه نمود. پشتیبان‌گیری از محتویات پارتیشن‌های HSM یکی از عملیاتی است که در طول مراسم تولید کلید انجام می‌شود. برای انجام عملیات پشتیبان‌گیری، از توکن پشتیبان استفاده می‌گردد. با اتصال توکن

پشتیبان به HSM و وارد کردن دستور مربوط به پشتیبان‌گیری از پارتیشن مورد نظر، محتویات پارتیشن بدون افشای کلیدها روی توکن پشتیبان، پشتیبان‌گیری می‌شوند. سپس این توکن به مکان امنی انتقال یافته و به صورت کاملاً محافظت‌شده در آن‌جا نگهداری می‌گردد.

۶-۲-۵ بایگانی کلید خصوصی

قابل اعمال نیست.

۶-۲-۶ انتقال کلید خصوصی به/از یک ماژول امنیتی

مرکز میانی خصوصی پارس‌ساین جهت حفظ امنیت کلیدهای خصوصی تدابیر امنیتی لازم را اندیشیده است. این تدابیر امنیتی برای سطوح امنیتی مختلف در مرکز میانی خصوصی پارس‌ساین، در جدول ۶-۸ آورده شده است.

جدول ۶-۸ انتقال کلید خصوصی به یا از یک ماژول امنیتی

سطح اطمینان	انتقال کلید خصوصی به/از یک ماژول امنیتی
سطح ۱	رویه خاصی در نظر گرفته نشده است.
سطح ۲	مرکز میانی خصوصی پارس‌ساین عملیات تولید کلید برای گواهی مرکز صدور گواهی خود را توسط HSM انجام می‌دهد. همچنین جهت بازیابی کلید در صورت خرابی HSM، یک نسخه پشتیبان از کلید خصوصی به صورت رمزشده به توکن پشتیبان انتقال داده می‌شود و این توکن به صورت کاملاً محافظت‌شده نگهداری می‌شود.

۶-۲-۷ ذخیره‌سازی کلیدهای خصوصی در ماژول امنیتی

کلیدهای خصوصی مرکز میانی خصوصی پارس‌ساین در یک ماژول امنیتی که الزامات قید شده در بخش ۶-۲-۱ در آن رعایت شده است، ذخیره می‌شوند.

۶-۲-۸ روش فعال‌سازی کلید خصوصی

برای پیشگیری از دسترسی غیرمجاز به ماژول‌های امنیتی، استفاده از کلید خصوصی ذخیره شده در یک ماژول، نباید بدون در اختیار داشتن داده‌های فعال‌ساز امکان‌پذیر باشد.

در مرکز میانی خصوصی پارس‌ساین، داده‌های فعال‌ساز در حالت‌های مختلف به صورت زیر استفاده می‌گردد:

جدول ۶-۹ فعال‌سازی کلید خصوصی

سطح اطمینان	فعال‌سازی کلید خصوصی
سطح ۱	از طریق گذرواژه صورت می‌گیرد.
سطح ۲	اگر کلید خصوصی داخل توکن ذخیره شده باشد، جهت فعال‌سازی و استفاده از کلید خصوصی، از گذرواژه توکن استفاده می‌گردد. همان‌طور که در بخش ۶-۱-۱-۳ بیان شد، چنانچه کلید خصوصی توسط متصدی دفتر ثبت‌نام برای مالک گواهی تولید شود، این عملیات بر روی توکن سخت‌افزاری انجام می‌شود. بعد از تحویل سخت‌افزار حاوی کلید خصوصی مالک گواهی، به وی اعلام می‌شود که در اسرع وقت گذرواژه سخت‌افزار رمزنگاری خود را تغییر دهد؛ اگر کلید خصوصی داخل HSM ذخیره شده باشد، جهت فعال‌سازی کلید خصوصی از ترکیب گذرواژه و توکن استفاده می‌گردد.

علاوه بر این، هنگام ورود اطلاعات فعال‌ساز در موارد مندرج در جدول ۶-۹، از افشای اطلاعات جلوگیری می‌شود. برای مثال، هنگام ورود اطلاعات، اطلاعات روی صفحه نمایش نشان داده نمی‌شوند.

۶-۲-۹ روش غیرفعال نمودن کلید خصوصی

جهت غیرفعال‌سازی کلیدهای خصوصی متناظر با گواهی‌های سطح ۲ که در توکن و یا HSM ذخیره شده‌اند، عملیات خروج از سیستم[1] صورت می‌گیرد. خروج از سیستم ممکن است با بسته‌شدن نشست تشکیل‌شده بین توکن یا HSM با نرم‌افزار و یا جدا کردن توکن از سیستم و قطع برق HSM صورت گیرد. همچنین، وقتی کلیدهای خصوصی غیرفعال می‌شوند، قبل از این‌که حافظه تقسیم‌بندی شود از حافظه پاک می‌شوند. چنانچه کلیدها روی فضایی از دیسک ذخیره شده باشند، قبل از این‌که فضا برای سیستم عامل آزاد شود، بازنویسی می‌شوند.

1 Logout

۶-۲-۱۰ روش انهدام کلید خصوصی

مرکز میانی خصوصی پارس‌ساین جهت پیشگیری از سوءاستفاده از کلید خصوصی، کلیدهای خصوصی خود را زمانی که دیگر به آن‌ها نیازی نیست، از بین می‌برد. این کار از طریق اجرای دستور امحا[1] که با بازنویسی فضای حافظه همراه می‌باشد، انجام می‌شود.

۶-۲-۱۱ رده‌بندی ماژول‌های امنیتی

به بخش ۶-۲-۱ مراجعه شود.

۶-۳ سایر ابعاد مدیریت زوج‌کلید

۶-۳-۱ بایگانی کلید عمومی

مرکز میانی خصوصی پارس‌ساین، کلیدهای عمومی متناظر با گواهی‌های خود و همچنین کلیدهای عمومی متناظر با گواهی‌های صادرشده را مطابق با بخش ۵-۵-۲ بایگانی می‌کند.

۶-۳-۲ دوره‌های عملیاتی گواهی و دوره‌های استفاده از زوج‌کلید

دوره عملیاتی یک گواهی تا پایان بازه اعتبار آن و قبل از ابطال گواهی است و دوره عملیاتی زوج‌کلید مشابه دوره عملیاتی گواهی می‌باشد. الزامات مربوط به طول کلید و دوره اعتبار گواهی‌هایی که مرکز میانی خصوصی پارس‌ساین برای موجودیت‌های نهایی صادر می‌نماید، طبق جدول ۶-۱۰ می‌باشد:

جدول ۶-۱۰ طول کلید و حداکثر دوره اعتبار گواهی برای موجودیت‌های نهایی

سطح اطمینان	طول کلید (برحسب بیت)	حداکثر دوره اعتبار گواهی
سطح ۱	۱۰۲۴	۳ سال
	۲۰۴۸	۸ سال
سطح ۲	۱۰۲۴	۲ سال
	۲۰۴۸	۸ سال

1 Zeroization

۶-۴ اطلاعات فعال‌ساز

۶-۴-۱ تولید و به‌کارگیری اطلاعات فعال‌ساز

اطلاعات فعال‌ساز، جهت فعال‌سازی کلید خصوصی مطابق با بخش ۶-۲-۸ به‌کار می‌رود. جهت استفاده از اطلاعات فعال‌ساز کلیدهای خصوصی در مرکز میانی خصوصی پارس‌ساین از گذرواژه‌های مناسب استفاده می‌شود. گذرواژه‌های انتخاب‌شده شرایط زیر را پوشش می‌دهد:

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

۶-۴-۲ محافظت از اطلاعات فعال‌ساز

جدول ۶-۱۱ محافظت از اطلاعات فعال‌ساز

سطح اطمینان	محافظت از اطلاعات فعال‌ساز
سطح ۱	رویه خاصی در نظر گرفته نشده است.
سطح ۲	برای امنیت بیشتر، اطلاعات فعال‌ساز کلید خصوصی مرکز صدور گواهی که تنها در اختیار نقش‌های مرتبط با مدیریت ماژول امنیتی قرار دارد، به صورت نوشته نگهداری نشده و به حافظه سپرده می‌شود؛ در صورت نوشتن، این اطلاعات در سطحی معادل با امنیت دستگاه رمزنگاری نگهداری می‌شوند. همچنین، اطلاعات فعال‌ساز کلیدهای خصوصی مالکان گواهی منحصراً نزد خود آن‌ها محفوظ می‌ماند.

۶-۴-۳ سایر ابعاد اطلاعات فعال‌ساز

تعریف نشده است.

۶-۵ کنترل‌های امنیتی رایانه

۶-۵-۱ الزامات فنی ویژه امنیت رایانه

تدابیر امنیتی زیر در سیستم‌عامل‌ها اتخاذ شده است:

۱. امکان ورود به سیستم تنها پس از احراز هویت متمرکز؛
۲. ایجاد دسترسی کنترل‌شده به اطلاعات و برنامه‌ها بر اساس هویت تعریف شده در سیستم؛
۳. تنظیم و راه‌اندازی سیستم ثبت وقایع و بازبینی آن‌ها؛
۴. تجهیز سیستم‌های حساس به سیستم‌های آنتی‌ویروس با قابلیت‌های زیر:
   - امکان به‌روزرسانی با آخرین لیست ویروس‌های شناسایی‌شده؛
   - امکان جستجو در تمام فایل‌های سیستمی و غیر سیستمی به صورت خودکار؛
   - ثبت وقایع مرتبط به بررسی سیستم و وجود ویروس‌های احتمالی و نتیجه عملکرد برنامه روی آن‌ها.

علاوه بر این، تدابیر امنیتی زیر در نرم‌افزارهای ثبت‌نام و صدور گواهی اتخاذ شده است:

۱. شناسایی و احراز هویت دو عاملی کاربران به صورت متمرکز؛
۲. کنترل دسترسی به خدمات مرکز با استفاده از تعریف نقش‌های مجزا؛
۳. اعمال محدودیت در دسترسی به سرویس‌ها با استفاده از مجوزهای تعریف‌شده برای هر نقش؛
۴. استفاده از رمزنگاری در ارتباط نشست‌ها و امنیت پایگاه داده؛
۵. ثبت سوابق عملیات و داده‌های ممیزی.

۶-۵-۲ رده‌بندی امنیت رایانه

جدول ۶-۱۲ رده‌بندی امنیت رایانه

سطح اطمینان	رده‌بندی امنیت رایانه
سطح ۱	برخی عناصر مرکز میانی خصوصی پارس‌ساین، در این مرکز مورد آزمون قرار گرفته است.
سطح ۲	عناصر اصلی مرکز میانی خصوصی پارس‌ساین مثل نرم‌افزارهای مرکز صدور گواهی و دفتر ثبت‌نام به تأیید آزمایشگاه مرکز تحقیقات صنایع انفورماتیک رسیده است. عناصری مانند HSM و توکن‌های سخت‌افزاری نیز توسط مرکز دولتی صدور گواهی الکترونیکی ریشه ارزیابی و

سطح اطمینان	رده‌بندی امنیت رایانه
	تأیید شده‌اند.

۶-۶ کنترل‌های فنی چرخه حیات

۶-۶-۱ کنترل‌های توسعه سامانه

نرم‌افزار مرکز صدور گواهی و دفتر ثبت‌نام پارس‌ساین تحت یک روش ساخت‌یافته، طراحی و توسعه یافته است. فرایند طراحی و توسعه این نرم‌افزارها توسط آزمایشگاه مورد اعتماد مرکز ریشه مورد آزمایش قرار می‌گیرد.

سخت‌افزارهای خریداری شده در مرکز میانی خصوصی پارس‌ساین، با روش‌های امن و به صورت مهر و موم‌شده حمل و تحویل مرکز می‌شوند. این سخت‌افزارها توسط پرسنل آموزش‌دیده نصب می‌گردند.

۶-۶-۲ کنترل‌های مدیریت امنیت

سخت‌افزارها و نرم‌افزارهای مرکز میانی خصوصی پارس‌ساین به طور اختصاصی برای انجام وظایف مربوط به مرکز میانی خصوصی پارس‌ساین مورد استفاده قرار می‌گیرند. سیستم مرکز میانی خصوصی پارس‌ساین حاوی هیچ برنامه کاربردی، وسایل سخت‌افزاری، اتصالات شبکه، و مؤلفه‌های نرم‌افزاری که مربوط به عملیات این مرکز نیستند، نمی‌باشد.

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

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

- نرم‌افزارهایی هستند که توسط توسعه‌دهنده نرم‌افزار ارائه شده است؛
- قبل از نصب تغییر داده نشده است؛

- نسخه مورد نظر برای استفاده است.

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

مرکز میانی خصوصی پارس‌ساین تمامیت پایگاه‌داده مرکز را به صورت دوره‌ای بررسی می‌کند که جزئیات آن در جدول ۶-۱۳ آورده شده است:

جدول ۶-۱۳ بررسی دوره‌ای تمامیت پایگاه داده مرکز میانی خصوصی پارس‌ساین

سطح اطمینان	بررسی دوره‌ای تمامیت پایگاه‌داده
سطح ۱	الزام خاصی وجود ندارد، با این حال برای افزایش امنیت، در بازه‌های زمانی خاصی تمامیت پایگاه‌داده مرکز بررسی می‌شود.
سطح ۲	به محض نصب، و حداقل یک‌بار در ماه، تمامیت پایگاه‌داده مرکز بررسی می‌شود.

۶-۶-۳ کنترل‌های امنیتی چرخه حیات

پیاده‌سازی نشده است.

۶-۷ کنترل‌های امنیتی شبکه

در مرکز صدور گواهی خصوصی پارس‌ساین، جهت اطمینان از امنیت سرویس‌دهنده‌ها و جلوگیری از تهدیدات شبکه، از دیواره آتش و UTM به عنوان یک لایه امنیتی استفاده شده و همچنین جهت محافظت از مخزن در مقابل تهدیدات شبکه از UTM به عنوان یک لایه امنیتی بین مخزن و کاربران استفاده شده است.

برخی از سرویس‌های امنیتی پشتیبانی شده توسط UTM مورد استفاده در مرکز صدور گواهی خصوصی پارس‌ساین عبارتند از:

- بازرسی حالتمند (Stateful Inspection)

- ترجمه آدرس شبکه[1] (NAT)
- سیستم تشخیص و جلوگیری از حملات[2] (IDPS)
- کلیه پیکربندی‌های امنیتی لازم در دیواره‌های آتش و سایر تجهیزات شبکه طوری تنظیم شده است که تنها سرویس‌های مشخصی برای سیستم‌ها و کاربران خاصی قابل دسترسی است.

۶-۸ مهر زمانی

در حال حاضر، پشتیبانی نمی‌شود.

1 Network Address Translation
2 Intrusion Detection and Prevention System

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

۷-۱ پروفایل گواهی

پروفایل گواهی‌های صادر شده توسط مرکز صدور گواهی خصوصی پارس‌ساین منطبق با RFC 5280[2] و «سند جامع پروفایل‌های زیرساخت کلید عمومی کشور» در نظر گرفته شده است. فیلدهای یک گواهی X.509 حداقل شامل فیلدهای قیدشده در جدول ۷-۱ می‌باشد. هر فیلد با توجه به قیودی که برای مقادیر آن‌ها تعیین شده است، مقداردهی می‌شود. تشریح کامل پروفایل‌های گواهی الکترونیکی در «سند جامع پروفایل‌های زیرساخت کلید عمومی کشور» آورده شده است.

جدول ۷-۱ فیلدهای گواهی X.509

فیلد	مقدار
Version	شماره نسخه گواهی.
Serial Number	شماره سریال گواهی که برای هر گواهی صادر شده توسط مرکز صدور گواهی خصوصی پارس‌ساین مقداری منحصر به فرد می‌باشد.
Signature Algorithm	شناسه الگوریتم به کار رفته جهت امضای گواهی (بخش ۷-۱-۳).
Issuer	در بخش ۷-۱-۴ توضیح داده شده است.
Valid From	تاریخ شروع اعتبار گواهی.
Valid to	تاریخ پایان اعتبار گواهی.
Subject	در بخش ۷-۱-۴ توضیح داده شده است.
Subject Public Key	کلید عمومی مالک گواهی که مطابق با RFC 5280 کدگذاری می‌گردد.

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

SignatureValue	امضای گواهی که مطابق با RFC 5280 تولید و کدگذاری می‌گردد.

۷-۱-۱ شماره نسخه

گواهی‌های صادر شده توسط مرکز صدور گواهی خصوصی پارس‌ساین منطبق با نسخه سوم استاندارد X.509 می‌باشد.

۷-۱-۲ الحاقیه‌های گواهی[1]

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

۷-۱-۳ شناسه الگوریتم‌ها

گواهی‌های صادر شده توسط مرکز صدور گواهی خصوصی پارس‌ساین به وسیله یکی از الگوریتم‌های زیر امضا می‌گردد:

- **sha256withRSAEncryption** OBJECT IDENTIFIER::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- **sha1withRSAEncryption** OBJECT IDENTIFIER::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

زیرساخت کلید عمومی کشور متشکل از دو ساختار سلسله‌مراتبی G2 و G3 می‌باشد. ساختار G2 سازگار با تابع درهم‌ساز[2] SHA1 است و می‌تواند در سخت‌افزارها و نرم‌افزارهایی که از این تابع درهم‌ساز پشتیبانی می‌نمایند مورد استفاده قرار گیرد. ساختار G3 نیز سازگار با تابع درهم‌ساز SHA256 بوده و جهت ارائه سطح امنیت بالاتر پیش‌بینی شده است.

۷-۱-۴ قالب نام‌ها

مرکز صدور گواهی خصوصی پارس‌ساین نام ترکیبی مالکان گواهی را مطابق با بخش ۳-۱ مقداردهی می‌نماید. نام ترکیبی در گواهی مرکز صدور گواهی خصوصی پارس‌ساین توسط مرکز ریشه تعیین شده است.

1 Certificate Extensions
2 Hash Function

۷-۱-۵ محدودیت‌های نام‌گذاری

مطابق با «سند جامع پروفایل‌های زیرساخت کلید عمومی کشور»، استفاده از فیلد الحاقی Name Constraints در گواهی ممنوع می‌باشد.

۷-۱-۶ شناسه سیاست‌های گواهی

هر سطح گواهی دارای شناسه‌ای است که در بخش ۱-۲ مقدار آن مشخص شده است. مرکز صدور گواهی این مقدار را مطابق با بخش ۱-۲ در الحاقیه Certificate Policies گواهی قرار می‌دهد.

۷-۱-۷ کاربرد الحاقیه Policy Constraints

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

۷-۱-۸ ساختار و معنای الحاقیه Policy Qualifier

گواهی‌های نسخه سوم X.509 حاوی یک توصیف‌کننده سیاست در فیلد الحاقی Certificate Policies می‌باشند. در این توصیف‌کننده نشانی دسترسی به سند پیش رو آورده می‌شود. همچنین یک توصیف‌کننده اختیاری دیگر با شناسه User Notice در همین فیلد الحاقی قرار می‌گیرد که متن آن در زیر آورده شده است:

Any use of this certificate constitutes acceptance of the ParsSign Certificate Practice Statement (CPS) which limits liability and is available at the above URL.

عبارت بالا به این معنی است که استفاده از گواهی توسط طرف‌های اعتمادکننده به منزله پذیرش «دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی پارس‌ساین» می‌باشد. URL ذکرشده به آدرس URL مربوط به سند «دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی پارس‌ساین» اشاره دارد که در گواهی (در فیلد Certificate Policies) قید شده است.

۷-۱-۹ پردازش معنایی برای الحاقیه Certificate Policies

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

۷-۲ پروفایل لیست گواهی‌های باطل‌شده

پروفایل لیست گواهی‌های باطل‌شده در مرکز میانی خصوصی پارس‌ساین مطابق با استاندارد RFC 5280 می‌باشد. لیست گواهی‌های باطل‌شده حداقل شامل فیلدهای اصلی و مقادیر تعیین شده برای آن‌ها می‌باشد که در جدول ۷-۲ به آن‌ها اشاره شده است:

جدول ۷-۲ فیلدهای اصلی CRL

فیلد	مقدار
Version	به بخش ۷-۲-۱ مراجعه شود.
Signature Algorithm	به بخش ۷-۱-۳ مراجعه شود.
Issuer	نام ترکیبی موجودیتی که CRL را تولید و امضا می‌نماید.
Effective Date	تاریخ صدور CRL.
Next Update	تاریخی که CRL بعدی صادر خواهد شد.
Revokation List	لیست گواهی‌های باطل شده شامل شماره سریال گواهی‌های باطل‌شده و تاریخ ابطال آن‌ها.

۷-۲-۱ شماره نسخه

مرکز میانی خصوصی پارس‌ساین از نسخه دوم X.509 لیست گواهی‌های باطل‌شده منطبق با RFC 5280 پشتیبانی می‌کند.

۷-۲-۲ الحاقیه‌های CRL و CRL Entry

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

۷-۳ پروفایل OCSP

در حال حاضر سرویس OCSP پشتیبانی نمی‌شود.

۷-۳-۱ شماره نسخه

پشتیبانی نمی‌شود.

۷-۳-۲ الحاقیه‌های OCSP

پشتیبانی نمی‌شود.

۸ بازرسی تطابق و سایر ارزیابی‌ها

بازرسی تطابق با هدف حصول اطمینان از عملکرد صحیح مرکز میانی خصوصی پارس‌ساین و به‌منظور بررسی تطابق عملیات این مرکز با الزامات و فرایندهای بیان‌شده در سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و دستورالعمل اجرایی مرکز میانی خصوصی پارس‌ساین به عمل می‌آید. بازرسی تطابق در مرکز میانی خصوصی پارس‌ساین به دو صورت زیر انجام می‌شود:

- بازرسی شورا: بر اساس ماده ۳ آیین‌نامه ۳۲ قانون تجارت الکترونیکی ایران، به‌منظور اعمال نظارت عالیه بر عملکرد مرکز میانی خصوصی پارس‌ساین، بازرسی دوره‌ای از این مرکز زیر نظر شورا و توسط بازرس یا بازرسان مورد تأیید شورا صورت می‌گیرد.
- بازرسی مرکز ریشه: بر اساس ماده ۵ آیین‌نامه ۳۲ قانون تجارت الکترونیکی ایران، مرکز ریشه به‌منظور حصول اطمینان از عملکرد صحیح مرکز میانی خصوصی پارس‌ساین، بازرسی دوره‌ای از این مرکز به عمل می‌آورد.

۸-۱ تناوب و شرایط ارزیابی

بازرسی تطابق در مرکز میانی خصوصی پارس‌ساین از سوی مرکز ریشه، مطابق با جدول ۸-۱ انجام می‌گیرد.

جدول ۸-۱ تناوب و شرایط ارزیابی

سطح اطمینان	تناوب و شرایط ارزیابی
سطح ۱	الزامی در نظر گرفته نشده است.
سطح ۲	بازرسی تطابق حداقل یک‌بار در سال انجام می‌گیرد.

۸-۲ هویت و صلاحیت ارزیاب

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

بازرس باید با زیرساخت کلید عمومی و استانداردهای آن، سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور، دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی پارس‌ساین، و مصوبات شورا کاملاً آشنا باشد.

۸-۳ ارتباط ارزیاب با مرکز مورد ارزیابی

بازرسی مرکز ریشه از مرکز میانی خصوصی پارس‌ساین توسط اشخاصی که دارای شرایط ذکر شده در بخش ۸-۲ می‌باشند، انجام می‌گیرد.

۸-۴ موضوعات مورد ارزیابی

موضوعات مورد ارزیابی در فرایند بازرسی تطابق مرکز میانی خصوصی پارس‌ساین حداقل شامل موارد زیر می‌باشد:

- دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی پارس‌ساین، دستورالعمل‌های فنی، فرایندی و پرسنلی مرکز میانی خصوصی پارس‌ساین و طرح فنی تجهیزات و ساختمان مرکز؛
- بررسی تطابق مرکز میانی خصوصی پارس‌ساین (شامل ساختمان، تجهیزات، کلیه سخت‌افزارها، نرم‌افزارها، نیروی انسانی و فرایندهای به‌کار گرفته در مرکز) با دستورالعمل‌ها و مستندات قید شده در بند اول؛
- بررسی تطابق تجهیزات، نرم‌افزارها و عملکرد دفاتر ثبت‌نام با دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی پارس‌ساین.

۸-۵ اقدامات اتخاذشده در برخورد با نقایص

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

- نقص و یا ناهمخوانی ثبت می‌شود؛
- به طرف‌های تعیین‌شده در بخش ۸-۶ ناهمخوانی و یا نقص ثبت‌شده، اعلام می‌شود؛
- مرکز میانی خصوصی پارس‌ساین در مدت زمان تعیین‌شده توسط مرجع بازرسی‌کننده، نسبت به رفع نواقص و ناهمخوانی‌ها اقدام می‌نماید؛
- در صورت عدم اصلاح نقص یا ناهمخوانی توسط مرکز میانی خصوصی پارس‌ساین در زمان پیش‌بینی شده، گزارش مغایرت به اطلاع شورا می‌رسد؛
- شورا می‌تواند راهکار مناسبی که شامل تمدید مدت زمان اصلاح نواقص، جلوگیری از فعالیت مرکز میانی خصوصی پارس‌ساین و یا در صورت لزوم ابطال گواهی مرکز صدور گواهی باشد را تعیین نماید.

۸-۶ گزارش نتایج

نتایج بازرسی مرکز ریشه از مرکز میانی خصوصی پارس‌ساین به شورا ارائه می‌گردد. این نتایج به عنوان اطلاعات محرمانه تلقی شده و فقط در صورت لزوم و با موافقت مراجع قضایی ذیصلاح یا پیرو دستور آن‌ها افشا می‌شوند.

۹ سایر موارد حقوقی و مربوط به کسب و کار

۹-۱ تعرفه‌ها

۹-۱-۱ تعرفه‌های صدور یا تمدید گواهی

مرکز صدور گواهی الکترونیکی میانی پارس‌ساین، جهت صدور و یا تمدید گواهی، از تعرفه‌های ابلاغیه هیئت دولت تبعیت می‌نماید.

۹-۱-۲ تعرفه‌های دسترسی به گواهی

در حال حاضر، تا زمانی که از سوی مرکز دولتی صدور گواهی الکترونیکی ریشه اعلام نشود، هزینه‌ای جهت دسترسی به گواهی دریافت نمی‌گردد.

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

در حال حاضر، تا زمانی که از سوی مرکز ریشه اعلام نشود، هزینه‌ای برای خدمات مربوط به ابطال و اعلام وضعیت گواهی دریافت نمی‌گردد.

۹-۱-۴ تعرفه سایر خدمات

مرکز میانی خصوصی پارس‌ساین برای خدمات دسترسی به سند «دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی پارس‌ساین» و مخزن گواهی الکترونیکی تعرفه‌ای دریافت نمی‌کند.

۹-۱-۵ سیاست استرداد

طبق بخش ۴-۴-۱، امضای فرم درخواست صدور و یا تمدید گواهی توسط متقاضی، به منزله پذیرش گواهی از سوی مالک گواهی است. بنابراین، پس از امضای فرم مذکور، امکان استرداد وجود نخواهد داشت. به عبارت دیگر، تنها قبل از امضای فرم درخواست، امکان استرداد وجود دارد.

۹-۲ مسئولیت مالی

۹-۲-۱ پوشش بیمه‌ای

در حال حاضر پشتیبانی نمی‌شود.

۹-۲-۲ سایر دارایی‌ها

مرکز میانی خصوصی پارس‌ساین دارای منابع مالی کافی برای ادامه عملکرد و انجام وظایف و پذیرش مسئولیت‌های خود می‌باشد.

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

در صورتی که گواهی صادرشده با ارائه دلایل منطقی که نشان‌دهنده قصور مرکز میانی خصوصی پارس‌ساین باشد، مورد قبول متقاضی گواهی قرار نگیرد (به عنوان مثال، عدم تطابق اطلاعات داخل گواهی با اطلاعات ارائه شده توسط متقاضی)، مرکز صدور گواهی خصوصی پارس‌ساین مجدداً برای وی گواهی صادر می‌نماید.

۹-۳ محرمانگی اطلاعات کسب و کار

۹-۳-۱ محدوده اطلاعات محرمانه

مرکز میانی خصوصی پارس‌ساین اطلاعاتی نظیر اطلاعات زیر را به صورت محرمانه نگهداری و محافظت می‌نماید:

- آن بخش از اطلاعات مربوط به درخواست گواهی که توسط مرکز میانی خصوصی پارس‌ساین نگهداری می‌شود و در گواهی‌های صادر شده وجود ندارد؛
- کلیه کلیدهای خصوصی و داده‌های فعال‌ساز که در مرکز صدور گواهی خصوصی پارس‌ساین و دفاتر ثبت‌نام مربوطه به کار گرفته می‌شود؛
- سوابق کاربرد معاملاتی و سوابق کاربرد گواهی الکترونیکی؛
- اطلاعات درخواست گواهی که ممکن است شامل اطلاعاتی نظیر طرح تجاری، اطلاعات فروش، یا اسرار تجاری باشد؛
- کلیه اطلاعات مربوط به پیگیری ثبت وقایع که توسط مرکز میانی خصوصی پارس‌ساین ایجاد و نگهداری می‌شوند؛
- تمهیدات امنیتی که برای طرح فنی تجهیزات، ساختمان، نرم‌افزارها و اجرای خدمات گواهی تخصیص یافته است.

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

اطلاعات زیر محرمانه محسوب نمی‌شوند و به تمهیدات خاصی از سوی مرکز میانی خصوصی پارس‌ساین جهت محافظت آن‌ها نیاز نمی‌باشد:

- کلیه اطلاعات موجود در مخزن مرکز صدور گواهی خصوصی پارس‌ساین؛
- کلیه اطلاعات شناسایی و اطلاعات دیگری که در گواهی‌ها درج می‌شوند، مگر آنکه در توافق‌نامه‌های منعقده خلاف آن تصریح شده باشد.

۹-۳-۳ مسئولیت محافظت از اطلاعات محرمانه

مرکز صدور گواهی خصوصی پارس‌ساین و دفاتر ثبت‌نام مربوطه مسئول حفظ کلیه اطلاعات محرمانه در برابر افشا و دسترسی غیرمجاز هستند.

۹-۴ محافظت از اطلاعات خصوصی

بخشی از اطلاعات درخواست گواهی که توسط مرکز میانی خصوصی پارس‌ساین نگهداری می‌شود و در گواهی‌های صادر شده وجود ندارد، به عنوان اطلاعات خصوصی درخواست‌کننده یا مالک گواهی تلقی می‌شود. مرکز میانی خصوصی پارس‌ساین مسئول محافظت از این اطلاعات خصوصی می‌باشد.

۹-۴-۱ طرح حریم خصوصی

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

۹-۴-۲ اطلاعاتی که خصوصی محسوب می‌شوند

کلیه اطلاعات مربوط به درخواست‌کنندگان گواهی که جهت صدور گواهی به دفتر ثبت‌نام وابسته به مرکز صدور گواهی خصوصی پارس‌ساین داده شده‌اند، و به صورت عمومی از طریق گواهی یا مخزن قابل دسترسی نمی‌باشد، خصوصی محسوب می‌شود.

۹-۴-۳ اطلاعاتی که خصوصی محسوب نمی‌شوند

کلیه اطلاعات موجود در گواهی‌های منتشر شده (که به سهولت قابل رؤیت می‌باشد) و اطلاعات درج‌شده در CRL، خصوصی محسوب نمی‌شوند.

۹-۴-۴ مسئولیت محافظت از اطلاعات خصوصی

مرکز صدور گواهی پارس‌ساین و دفاتر ثبت‌نام وابسته، مسئول محافظت از کلیه اطلاعات خصوصی درخواست‌کنندگان و مالکان گواهی در مقابل هرگونه دسترسی و افشا توسط افراد غیرمجاز می‌باشند.

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

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

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

در شرایطی که به موجب قوانین موضوعه کشور در راستای حفظ امنیت و نظم عمومی و حمایت از حقوق شهروندان و کشف جرم و تعقیب مجرم، مرکز میانی خصوصی پارس‌ساین موظف به ارائه اطلاعات خصوصی درخواست‌کنندگان و مالکان گواهی باشد، همکاری مذکور تنها با دریافت حکم قضایی رسمی، تنظیم شده توسط مرجع ذیصلاح انجام می‌پذیرد.

۹-۴-۷ سایر شرایط افشای اطلاعات

قابل اعمال نیست.

۹-۵ حق مالکیت معنوی

- **حق مالکیت معنوی گواهی و اطلاعات ابطال گواهی:** مالکیت معنوی کلیه گواهی‌های صادرشده و اطلاعات ابطال آن‌ها به مرکز میانی خصوصی پارس‌ساین تعلق دارد. مالکان گواهی و طرف‌های اعتمادکننده می‌توانند از گواهی‌ها تنها در کاربردهای مجاز و مصارف قانونی مطابق با دستورالعمل تدوین شده مرکز صدور گواهی و توافق‌نامه‌های منعقده استفاده کنند.
- **حق مالکیت معنوی اسناد:** حق مالکیت معنوی کلیه اسناد تنظیم‌شده در مرکز میانی خصوصی پارس‌ساین از جمله سند «دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی پارس‌ساین» در انحصار مرکز میانی خصوصی پارس‌ساین می‌باشد.
- **حق مالکیت معنوی نام‌ها:** هر گواهی صادرشده بر اساس ضوابط توسط مرکز صدور گواهی خصوصی پارس‌ساین، در برگیرنده مالکیت معنوی آن نام برای مالک گواهی می‌باشد. این نام

در انحصار مالک گواهی می‌باشد و هیچ شخص دیگری حق ثبت مجدد آن برای خود را ندارد.

- **حق مالکیت معنوی کلیدها:** حق مالکیت معنوی زوج‌کلید متناظر با گواهی، متعلق به مالک آن گواهی می‌باشد.
- **سایر موارد:** حق مالکیت معنوی کلیه اطلاعات منتشر شده در مخزن مرکز میانی خصوصی پارس‌ساین، متعلق به این مرکز می‌باشد.

۹-۶ مسئولیت‌ها و التزامات

۹-۶-۱ مسئولیت‌ها و التزامات مراکز صدور گواهی

۹-۶-۱-۱ التزامات مرکز دولتی صدور گواهی الکترونیکی ریشه

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

۹-۶-۱-۲ مسئولیت‌ها و التزامات مرکز صدور گواهی الکترونیکی میانی خصوصی پارس‌ساین

مرکز میانی خصوصی پارس‌ساین موارد زیر را تضمین می‌نماید:

- تدوین سند دستورالعمل اجرایی گواهی الکترونیکی و به‌روزرسانی آن مطابق با سند سیاست‌های گواهی زیرساخت کلید عمومی کشور و انتشار آن پس از اخذ تأییدیه از مرکز صدور گواهی الکترونیکی ریشه؛
- ایجاد و امضای گواهی برای متقاضیان گواهی پس از احراز هویت آن‌ها توسط دفتر ثبت‌نام و اثبات مالکیت کلید خصوصی آن‌ها؛
- ارائه خدمات اعلام وضعیت (ابطال یا عدم ابطال) گواهی‌ها مطابق با این دستورالعمل اجرایی؛
- قابل دسترس بودن مخزن در هر زمان مطابق با این دستورالعمل اجرایی؛
- بررسی صلاحیت و صدور مجوز برای دفاتر ثبت‌نام متعلق به خود؛

- ارائه خدمات مدیریت گواهی الکترونیکی شامل صدور، ابطال، و انتشار گواهی؛
- انجام بازرسی‌های دوره‌ای از مرکز صدور گواهی و دفاتر ثبت‌نام وابسته؛
- تولید کلید به نمایندگی از متقاضی به روش امن و منطبق با بخش ۶-۱-۱-۳؛
- عدم نسخه‌برداری از زوج‌کلید تولیدشده برای مالک گواهی، توسط مرکز صدور گواهی و دفاتر ثبت‌نام وابسته؛
- مطابقت فعالیت‌های مرکز صدور گواهی با این سند، سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور، استانداردهای ارائه شده توسط مرکز ریشه، و قرارداد بین مرکز میانی خصوصی پارس‌ساین و مرکز ریشه؛
- تضمین اِعمال استانداردهای زیرساخت کلید عمومی کشور؛
- اعلام پذیرش یا رد گواهی میانی خود پس از دریافت ابلاغیه صدور گواهی (پذیرش گواهی میانی صادر شده توسط مرکز دولتی صدور گواهی ریشه بدین معنا است که مرکز میانی خصوصی پارس‌ساین صحت اطلاعات آن گواهی را تأیید می‌کند)؛
- صدور گواهی الکترونیکی با استفاده از کلید خصوصی فقط هنگامی‌که گواهی مرکز صادرشده از سوی مرکز ریشه اعتبار داشته باشد؛
- اطلاع‌رسانی سریع به مرکز ریشه هنگام بروز هرگونه حادثه مانند در خطر افشا قرار گرفتن کلید یا عدم دسترسی به آن و درخواست ابطال گواهی در این موارد؛
- التزام به قوانین حاکم موضوعه؛
- رعایت موارد امنیتی فیزیکی و الکترونیکی؛
- آگاهی از این مطلب که مرکز میانی مسئول هرگونه خسارت وارده ناشی از تخطی موارد فوق می‌باشد.

۹-۶-۲ مسئولیت‌ها و التزامات دفاتر ثبت‌نام

دفاتر ثبت‌نام وابسته به مرکز صدور گواهی خصوصی پارس‌ساین موارد زیر را تضمین می‌نمایند:

- انجام عملیات مطابق با دستورالعمل اجرایی مرکز میانی خصوصی پارس‌ساین، استانداردهای ارائه شده توسط مرکز ریشه و نیز قراردادهای بین دفاتر ثبت‌نام و مرکز میانی خصوصی پارس‌ساین؛

- دریافت درخواست صدور، تمدید و ابطال گواهی و تحویل به مرکز صدور گواهی الکترونیکی پارس‌ساین؛
- انجام عملیات احراز هویت متقاضی و بررسی صحت اطلاعات تحویل شده به دفتر ثبت‌نام؛
- التزام به قوانین حاکم موضوعه؛
- رعایت موارد امنیتی فیزیکی و الکترونیکی.

۹-۶-۳ مسئولیت‌ها و التزامات مالکان گواهی

یک مالک گواهی که برای او توسط مرکز صدور گواهی خصوصی پارس‌ساین گواهی صادر شده است باید موارد زیر را تضمین نماید:

- اعتبارسنجی گواهی هنگام استفاده از گواهی مطابق با بخش ۴-۵-۲ این سند؛
- تولید زوج‌کلید به روش امن و مطابق با بخش ۶-۱-۱-۳؛
- نگهداری کلید خصوصی به گونه‌ای که اشخاص غیرمجاز هیچ‌گونه دسترسی به آن نداشته باشند؛
- ارائه اطلاعات صحیح مرتبط با تقاضا و اعلام تغییر این اطلاعات در دوره اعتبار گواهی به مرکز میانی خصوصی پارس‌ساین؛
- استفاده از گواهی فقط در کاربردهای مجاز و قانونی مطابق با کاربردهای مندرج در گواهی؛
- ارائه درخواست ابطال گواهی مطابق با بخش ۴-۹-۱-۲؛
- حصول اطمینان از این‌که نرم‌افزار استفاده شده، مورد تأیید مرکز ریشه می‌باشد و در آزمایشگاه زیرساخت کلید عمومی مرکز ریشه ارزیابی شده است. منظور از نرم‌افزار، نرم‌افزارهایی است که برای تولید زوج کلید و استفاده از گواهی (مثلاً نرم‌افزار امضاکننده با استفاده از کلید خصوصی) استفاده می‌شوند؛
- اطمینان از ایمن بودن محیط رایانه‌ای مورد استفاده به ویژه هنگام تولید زوج‌کلید؛
- پذیرش کلیه مسئولیت‌ها و عواقب ناشی از استفاده از گواهی برای انجام عملیات محرمانگی، توسط مالک گواهی؛
- پایبندی به قراردادهای منعقد شده بین متقاضی و مرکز میانی خصوصی پارس‌ساین؛
- به‌کارگیری گواهی در سطح اطمینان متناسب با سطوح اطمینان تعریف‌شده در بخش ۱-۱.

۹-۶-۴ مسئولیت‌ها و التزامات طرف‌های اعتمادکننده

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

- استفاده از مخزن معتبر اعلام‌شده توسط مرکز صدور گواهی خصوصی پارس‌ساین؛
- اعتبارسنجی گواهی هنگام استفاده از گواهی مطابق با بخش ۴-۵-۲ این سند؛
- دریافت گواهی خودامضای مرکز دولتی صدور گواهی الکترونیکی ریشه و گواهی مرکز صدور گواهی الکترونیکی پارس‌ساین از طریق کانال توزیع مطمئن؛
- اطمینان از این‌که گواهی فقط در کاربردهای مجاز و قانونی مطابق با کاربردهای مندرج در گواهی به‌کار گرفته شده است؛
- حصول اطمینان از این‌که نرم‌افزار به‌کار گرفته شده مورد تأیید مرکز ریشه می‌باشد و در آزمایشگاه زیرساخت کلید عمومی کشور ارزیابی شده است. منظور از نرم‌افزار، نرم‌افزاری است که عملیاتی از قبیل بررسی صحت و اعتبار گواهی، تصدیق امضا، احراز هویت، و تمامیت داده‌های امضاشده را انجام می‌دهد؛
- حصول اطمینان از این‌که گواهی در سطح اطمینان متناسب با سطوح اطمینان تعریف شده در بخش ۱-۱ به‌کار گرفته شده باشد؛
- اطمینان از ایمن بودن محیط رایانه‌ای خود؛
- نگهداری اطلاعات امضاشده و نیز اطلاعات مربوط به امضا، گواهی و فرایندهای مرتبط با عملیات رمزنگاری تا زمان مقتضی.

۹-۶-۵ مسئولیت‌ها و التزامات سایر موجودیت‌ها

تعریف نشده است.

۹-۷ عدم پذیرش مسئولیت‌ها و التزامات

به جز مسئولیت‌ها و التزامات اشاره‌شده در این سند، مرکز میانی خصوصی پارس‌ساین هیچ‌گونه مسئولیتی در قبال خسارات مستقیم، غیرمستقیم، تصادفی، استنتاجی، خاص یا کیفری در مورد گواهی‌هایی که توسط این مرکز صادرشده، نمی‌پذیرد.

همچنین مرکز در قبال موارد زیر هیچ‌گونه مسئولیتی را نمی‌پذیرد:

- استفاده از گواهی توسط طرف‌های اعتمادکننده و مالک گواهی برای کاربردهای محرمانگی؛
- اختلاف میان مالکان گواهی و درخواست‌کنندگان گواهی در مورد نام‌ها؛
- مشکلات پیش‌آمده برای کلید خصوصی مالکان گواهی پس از تحویل توکن یا کارت هوشمند حاوی کلید؛
- مشکلات پیش‌آمده به دلیل استفاده از گواهی توسط مالک گواهی در کاربردهای غیرمجاز؛
- انتشار اطلاعات در مورد سرویس‌هایی که پشتیبانی نمی‌شود؛ شامل سرویس‌های تعلیق، تجدید، و به‌روزرسانی گواهی.

۹-۸ محدودیت مسئولیت‌ها

در قبال خسارت‌های ناشی از پذیرش گواهی‌های صادرشده، عدم پذیرش یک گواهی معتبر، و پذیرش یک گواهی باطل‌شده از سوی طرف‌های اعتمادکننده، هیچ‌گونه مسئولیتی متوجه مرکز میانی خصوصی پارس‌ساین نخواهد بود.

۹-۹ خسارت‌ها

مرکز میانی خصوصی پارس‌ساین در صورت اعمال درست سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور و ارائه خدمات در راستای قوانین تجارت الکترونیکی و این دستورالعمل اجرایی، هیچ‌گونه پرداختی را جهت جبران خسارات ناشی از پذیرش و یا عدم پذیرش گواهی‌های صادر شده نمی‌پذیرد.

چنانچه مرکز به هر دلیل مجبور به متوقف نمودن ارائه خدمات صدور گواهی و یا مخزن شود، این امر را از طریق مخزن به آگاهی مالکان گواهی، دفاتر ثبت‌نام، و طرف‌های اعتمادکننده می‌رساند و در قبال خسارات مستقیم، غیرمستقیم، تصادفی، استنتاجی، خاص یا کیفری در مورد گواهی‌های صادرشده توسط این مرکز، هیچ‌گونه مسئولیتی را نمی‌پذیرد.

مرکز صدور گواهی خصوصی پارس‌ساین و دفاتر ثبت‌نام وابسته به آن در مورد خساراتی که در شرایط زیر ایجاد شده باشند، هیچ‌گونه تعهدی ندارند:

- ارائه اطلاعات اشتباه هنگام درخواست گواهی توسط درخواست‌کننده یا مالک گواهی؛

- استفاده از گواهی‌های باطل‌شده یا گواهی‌های منقضی‌شده توسط طرف‌های اعتمادکننده و مالکان گواهی؛
- استفاده از گواهی توسط طرف‌های اعتمادکننده و مالکان گواهی در کاربردهای ممنوع و غیرمجاز؛
- قصور و کوتاهی در انجام تعهدات و عدم توجه منطقی توسط طرف‌های اعتمادکننده و مالکان گواهی.

۹-۱۰دوره و خاتمه

۹-۱۰-۱ دوره

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

۹-۱۰-۲ خاتمه

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

۹-۱۰-۳ اثرات خاتمه و ابقا

تعریف نشده است.

۹-۱۱اعلان‌های خاص و ارتباطات بین موجودیت‌ها

مرکز صدور گواهی خصوصی پارس‌ساین و دفاتر ثبت‌نام وابسته، با یکدیگر در ارتباط هستند. این ارتباط از طریق ایمیل، فکس، وب‌سایت و هر روش ممکن دیگری برقرار می‌شود. اطلاع‌رسانی یا اعلان خاص در این قسمت از آن‌چه در زمینه انتشار اطلاعات از طریق مخزن در بخش ۲-۲ گفته شد، متفاوت است.
مرکز صدور گواهی خصوصی پارس‌ساین و دفاتر ثبت‌نام وابسته در زمینه اقداماتی که بر روابط آن‌ها با یکدیگر تأثیرگذار است، اطلاع‌رسانی انجام می‌دهند. اگر یک دفتر ثبت‌نام بخواهد به قرارداد خود با مرکز میانی خصوصی پارس‌ساین خاتمه دهد، موظف است قبل از خاتمه مرکز را از این موضوع مطلع نماید. همچنین در مواردی که عملیات مرکز صدور گواهی به علت سازماندهی مجدد تشکیلات خاتمه می‌یابد یا

قرارداد مرکز صدور گواهی با مرکز ریشه منقضی شده و فعالیت مرکز خاتمه می‌یابد، این امر به اطلاع دفاتر ثبت‌نام می‌رسد.

۹-۱۲تغییرات

۹-۱۲-۱ فرایند تغییر

مرکز میانی خصوصی پارس‌ساین هرگونه تغییر در دستورالعمل اجرایی گواهی الکترونیکی را به تأیید مرکز ریشه رسانده و پس از آن، از طریق وب‌سایت در اختیار عموم قرار می‌دهد.

۹-۱۲-۲ دوره و مکانیزم اطلاع‌رسانی

در صورتی که تغییرات در این سند اندک و دارای اثرگذاری ناچیز باشد (مثلاً اصلاح اشکالات نگارشی و املایی، و غیره)، این تغییرات بدون اطلاع‌رسانی اِعمال می‌شود. در مواردی که تغییرات عمده و قابل توجهی در این سند اعمال شود، پس از تصویب توسط مرکز ریشه حداکثر تا ۵ روز کاری در وب‌سایت مرکز میانی خصوصی پارس‌ساین قرار می‌گیرد.

۹-۱۲-۳ شرایطی که OID می‌بایست تغییر نماید

کاربرد ندارد.

۹-۱۳فرایندهای حل اختلاف

هرگونه اختلاف میان مرکز ریشه و مرکز میانی خصوصی پارس‌ساین، ابتدا از طریق کمیته نظارتی شورا[1] مورد رسیدگی قرار می‌گیرد؛ در صورت عدم حل اختلاف، مسأله به شورا ارجاع می‌شود.
هرگونه اختلاف میان مرکز میانی خصوصی پارس‌ساین و مالکان گواهی از طریق هیئت حل اختلاف در مرکز میانی برطرف می‌شود. در صورتی که اختلافات حادث‌شده از این طریق حل نشود و به تشخیص

[1] برای آگاهی از وظایف و افراد تشکیل‌دهنده این کمیته به بخش ۱-۳-۵ از سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور»، مراجعه کنید.

مرکز ریشه قابلیت حل و فصل در این مرکز را هم نداشته باشد، مسأله بـا طـرح دعـوا در مراجـع قضـایی ذیصلاح فیصله می‌یابد.

۹-۱۴قوانین حاکم

کلیه قوانین موضوعه جمهوری اسلامی ایران از جمله قانون تجارت الکترونیکـی (مصـوب ۱۳۸۲/۱۰/۲۴)، آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی (مصوب در جلسه مورخ ۱۳۸۶/۶/۱۱ هیئت وزیـران) و همچنین مصوبات شورای سیاست‌گذاری گواهی الکترونیکی کشور، حاکم بر کلیه فعالیت‌ها و قراردادهـای بین مرکز میانی خصوصی پارس‌ساین با مالکان گواهی و طرف‌های اعتمادکننده می‌باشد.

۹-۱۵تطابق با قوانین اجرایی

این دستورالعمل اجرایی با قوانین اجرایی بخش ۹-۱۴ تطابق دارد.

۹-۱۶ملاحظات متفرقه

تعریف نشده است.

۹-۱۶-۱ توافق‌نامه کلی

تعریف نشده است.

۹-۱۶-۲ تخصیص

تعریف نشده است.

۹-۱۶-۳ عدم وابستگی

در صورتی که مراجع ذیصلاح یکی از مفاد این سند را نادرست، نامعتبر یا غیر قابـل اعمـال بداننـد، سـایر مفاد آن تا زمان اصلاح سند، معتبر و لازم‌الاجرا خواهد بود.

۹-۱۶-۴ اجرای تعرفه‌های وکالت و فسخ مالکیت

تعریف نشده است.

۹-۱۶-۵ فورس‌ماژور

موارد فورس‌ماژور همان است که در قوانین عام جمهوری اسلامی ایران تدوین شده است. مرکز میانی خصوصی پارس‌ساین می‌تواند تا حدی که در قوانین تدوین شده مجاز است، گستره شمول موارد فورس‌ماژور را بسط دهد.

۹-۱۷سایر قیود

تعریف نشده است.