جمهوری اسلامی ایران
مرکز دولتی صدور گواهی الکترونیکی ریشه

پیاده سازی سطوح اطمینان
در زیرساخت کلید عمومی کشور

طبقه‌بندی: عادی

شماره بازنگری :۱.۲

تاریخ بازنگری : ۱۳۸۸/۱۰/۱

فهرست مطالب

عنوان **صفحه**

۱- مقدمه ۲

۲- تعاریف ۲

۳- سطوح اطمینان در سیستم های دولتی ۲

۳-۱- نظام شناسایی ۳

۳-۲- احراز هویت ۴

۴- انواع گواهی ۴

۵- مشخصات سطوح مختلف اطمینان ۴

۵-۱- افشاء کلید خصوصی ۴

۵-۲- تفکیک نقش ها ۵

۵-۳- دوره اعتبار گواهی ۵

۵-۴- تهیه نسخه پشتیبان ۵

۵-۵- فاصله درخواست و صدور گواهی ۶

۵-۶- بازرسی بیرونی ۶

۵-۷- نام گذاری ۶

۵-۸- تصرف کلید خصوصی ۷

۵-۹- ثبت وقایع ۷

۵-۱۰- طول کلید ۷

۵-۱۱- محافظت از کلید خصوصی ۷

۵-۱۲- افشاء کلید خصوصی ۸

۶- شناسه سطوح اطمینان ۹

۶-۱- امضاء دیجیتال ۹

۶-۲- محرمانگی ۹

۶-۳- احراز هویت ۹

۷- سطوح اطمینان مراکز ۹

۷-۱- سطوح اطمینان مراکز مختلف ۱۰

۸- نیازمندی های ماژول های رمزنگاری ۱۱

۱- مقدمه

به طور کلی در مورد ارائه خدمات درون دولت دو نوع از ذینفعان شرکت دارند: گروهی که شناسایی افراد را بر عهده دارند (Identity Provider) و آنهایی که خدمات را ارائه می‌کنند (Service Provider). یک موجودیت ساده می‌تواند در یک یا هر دو گروه مشارکت داشته باشد. ارائه کنندگان خدمات لازم است به اطلاعاتی که توسط تامین کننده شناسایی افراد برایشان ارسال شده است اعتماد نمایند. ارائه‌کننده خدمات در مورد اینکه خدمات را به کدام موجودیت ارائه کند حق تصمیم‌گیری داشته و این تصمیم بر اساس اطلاعاتی است که توسط تامین‌کنندگان شناسایی افراد ارائه می‌شود. برخی از اطلاعات ارسال شده می‌تواند در مورد سطوح اطمینانی باشد که برای مدیریت شناسایی و روش مورد استفاده برای احراز هویت استفاده خواهد شد. مدیریت شناسایی و تکنولوژی احراز هویت در یک دستگاه دارای یک رویه مشخص است ولی در میان تمامی دستگاه‌ها در دولت ممکن است طیف وسیعی از روش‌ها را دربرگیرد. عدم وجود اطلاعات مربوط به سطوح اطمینان می‌تواند مانعی بر سر راه اعتماد باشد به همین جهت تعریف سطوح اطمینان از اهمیت زیادی برخوردار خواهد بود.

۲- تعاریف

- **شناسایی (Identification):**

فرآیند تعیین هویت موجودیت قبل از صدور گواهی الکترونیکی

- **سطح اطمینان (Assurance Level):**

درجه یقین صاحب منبع به شناسایی موجودیت

- **احراز هویت (Authentication):**

محرز شدن هویت موجودیت در زمان تقاضای دسترسی به خدمات ویا منابع شبکه، بعد از صدور گواهی الکترونیکی

۳- سطوح اطمینان در سیستم های دولتی

سطوح اطمینان سیستم‌های دولتی بر اساس میزان ریسک آنها تعیین و اندازه‌گیری می‌شود بدین ترتیب که ریسک‌های سیستم‌های دولتی اندازه‌گیری شده و به چهار دسته کلی تقسیم می‌شوند و مطابق این دسته‌بندی نظام شناسایی و احراز هویت مطابق با سطوح اطمینان شکل می‌گیرد.

جدول ۱ سطوح اطمینان در سیستم های دولتی

سطح اطمینان	تعریف
سطح ۰	
سطح ۱	هیچگونه تهدیدی وجود ندارد.
سطح ۲	با تعداد محدودی تهدید بر روی شبکه روبرو است.
سطح ۳	با تهدیدات زیادی بر روی شبکه و تعداد محدودی تهدید توسط کاربران خرابکار داخلی مواجه است.

سطح ۴	با تهدیدات زیادی هم بر روی شبکه و هم از طریق کاربران داخلی مواجه است.

۳-۱- نظام شناسایی

جدول ۲ نظام شناسایی

سطح اطمینان	نحوه شناسایی
سطح ۱	بدون نیاز به تشریفات ثبت نام و بر پایه دانش و اعتماد موجود
سطح ۲	۲ سری مدرک شناسایی معتبر که یکی از آنها عکس‌دار باشد باضافه مدارک لازم دیگر که با توجه به نوع فعالیت در حوزه‌های متفاوت تعریف خواهد بود.
سطح ۳	به صورت رو در رو و ارائه ۲ سری مدارک شناسایی و کسب امتیاز بالای ۱۰۰ و مخصوص کارکنان و سازمان‌های دولت و افراد حقیقی و حقوقی طرف قرارداد با دولت
سطح ۴	به صورت رو در رو و ارائه ۲ سری مدارک شناسایی و کسب امتیاز بالای ۱۵۰ و مخصوص کارکنان دولت و افراد حقیقی و حقوقی طرف قرارداد با دولت

مدارک		امتیاز	مثال
سابقه کار مورد قبول دستگاه		۱ تا ۳ سال ۱۰ امتیاز ۳ تا ۵ سال ۲۰ امتیاز ۵ تا ۱۰ سال ۴۰ امتیاز بالای ۱۰ سال ۶۰ امتیاز	مثال: (حداقل امتیاز) ۱۰۰ امتیاز= دومدرک(۸۰) + نوع قرارداد(۱۰) + ۳ سال سابقه(۱۰) ۱۵۰ امتیاز= دو مدرک (۸۰) + شغل مدیر (۵۰) + رسمی(۱۰) + سابقه (۱۰) ۱۵۰ امتیاز = دو مدرک (۸۰) + شغل مدیر (۵۰) + سابقه ۳ تا ۵(۲۰) ۱۵۰ امتیاز = دو مدرک (۸۰) + نوع قرارداد(۱۰) + بالای ۱۰ سال (۶۰)
عنوان شغلی		مدیرکل به بالا ۵۰ امتیاز	
نوع قرارداد		رسمی و پیمانی ۱۰ امتیاز	
حداکثر دو مدرک	شناسنامه	۴۰ امتیاز	
	کارت ملی	۴۰ امتیاز	
	گذرنامه	۲۰ امتیاز	
	گواهینامه	۲۰ امتیاز	

۳-۲- احراز هویت

جدول ۳ احراز هویت انواع گواهی‌ها

سطح اطمینان	تعریف
سطح ۱	استفاده از گواهی X.509 توسط توکن و یا به صورت نرم‌افزاری و همراه با پین‌کد و یا کلمه عبور
سطح ۲	استفاده از گواهی X.509 توسط توکن و یا به صورت نرم‌افزاری و همراه با پین‌کد و یا کلمه عبور
سطح ۳	استفاده از انواع سخت‌افزارهای مبتنی بر گواهی x.509 مانند توکن‌های رمزنگاری
سطح ۴	استفاده از انواع سخت‌افزارهای مبتنی بر گواهی x.509 مانند توکن‌های رمزنگاری

۴- انواع گواهی

جدول ۴ انواع گواهی با توجه به سطوح اطمینان

نام گواهی	سطح اطمینان	تعریف
برنز	سطح ۱ (Rudimentary)	این سطح از گواهی قابلیت استفاده در تمامی دستگاه‌های دولتی و خصوصی را دارا می‌باشد.
نقره	سطح ۲ (Basic)	این سطح از گواهی قابلیت استفاده در تمامی دستگاه‌های دولتی و خصوصی را دارا می‌باشد.
طلا	سطح ۳ (Medium)	این سطح از گواهی قابلیت استفاده در تمامی دستگاه‌های دولتی را دارا می‌باشد.
پلاتین	سطح ۴ (High)	این سطح از گواهی قابلیت استفاده در تمامی دستگاه‌های دولتی را دارا می‌باشد.

۵- مشخصات سطوح مختلف اطمینان

۵-۱- افشاء و مفقود شدن کلید خصوصی

جدول۵ افشاء و مفقود شدن کلید خصوصی

سطح اطمینان	گمشدن و یا افشاء کلید خصوصی
سطح ۱	ابطال گواهی، انتشار CRL حداقل هر ۳۰ روز و ۱ روز در صورت افشاء کلید خصوصی
سطح ۲	ابطال گواهی، انتشار CRL حداقل هر ۲۴ ساعت و ۶ ساعت در صورت افشاء کلید خصوصی

سطح ۳	ابطال گواهی، انتشار CRL حداقل هر ۱۲ ساعت و ۲ ساعت در صورت افشاء کلید خصوصی
سطح ۴	ابطال گواهی، انتشار CRL حداقل هر ۴ ساعت و ۱/۲ ساعت در صورت افشاء کلید خصوصی

۵-۲- تفکیک نقش ها

جدول۶ تفکیک نقش ها

سطح اطمینان	تفکیک نقش‌ها
سطح ۱	کلیه وظایف صدور گواهی می‌تواند توسط ۱ نفر انجام شود
سطح ۲	وظایف صدور گواهی حداقل باید توسط ۲ نفر انجام شود
سطح ۳	وظایف صدور گواهی حداقل باید توسط ۳ نفر انجام شود
سطح ۴	وظایف صدور گواهی حداقل باید توسط ۳ نفر انجام شود

۵-۳- دوره اعتبار گواهی

جدول۷ دوره اعتبار گواهی

سطح اطمینان	دوره اعتبار گواهی
سطح ۱	حداکثر ۶ سال
سطح ۲	حداکثر ۴ سال
سطح ۳	حداکثر ۲ سال
سطح ۴	حداکثر ۱ سال

۵-۴- تهیه نسخه پشتیبان از کلیدها

جدول ۸ تهیه نسخه پشتیبان از کلیدها

سطح اطمینان	نسخه پشتبان از کلیدهای محرمانگی مراکز CA وکاربران
سطح ۱	الزامی به Backupگیری کلیدهای محرمانگی نمی‌باشد
سطح ۲	کلیدهای محرمانگی باید Backupگیری شوند
سطح ۳	کلیدهای محرمانگی باید Backupگیری شوند
سطح ۴	کلیدهای محرمانگی باید Backupگیری شوند

۵-۵- فاصله درخواست و صدور گواهی

جدول ۹ فاصله درخواست و صدور گواهی

سطح اطمینان	فاصله بین درخواست و صدور گواهی
سطح ۱	هیچ قیدی وجود ندارد
سطح ۲	گواهی‌های کاربران نهایی در عرض پنج روز از زمان درخواست دفتر ثبت نام صادر می‌شوند
سطح ۳	گواهی‌های کاربران نهایی در عرض دو روز از زمان درخواست دفتر ثبت نام صادر می‌شوند
سطح ۴	گواهی‌های کاربران نهایی به محض درخواست دفتر ثبت نام صادر می‌شوند

۵-۶- بازرسی بیرونی

جدول ۱۰ بازرسی بیرونی

سطح اطمینان	بازرسی بیرونی
سطح ۱	بازرسی بیرونی به منظور بررسی تمکین از سیاست‌های امنیتی، هر ۳ سال یکبار انجام می‌شود
سطح ۲	بازرسی بیرونی به منظور بررسی تمکین از سیاست‌های امنیتی، هر ۲ سال یکبار انجام می‌شود
سطح ۳	بازرسی بیرونی به منظور بررسی تمکین از سیاست‌های امنیتی، هر ساله انجام می‌شود
سطح ۴	بازرسی بیرونی به منظور بررسی تمکین از سیاست‌های امنیتی، هر ساله انجام می‌شود

۵-۷- نام گذاری

جدول ۱۱ نام گذاری

سطح اطمینان	نیازمندی‌های نام‌گذاری
سطح ۱	گواهی‌های نهایی نیاز به Distinguished name ندارند
سطح ۲	گواهی‌های نهایی نیاز به Distinguished name دارند
سطح ۳	گواهی‌های نهایی نیاز به Distinguished name دارند
سطح ۴	گواهی‌های نهایی نیاز به Distinguished name دارند

۵-۸- تصرف کلید خصوصی

جدول ۱۲ تصرف کلید خصوصی

سطح اطمینان	مقررات اثبات تصرف
سطح ۱	کاربران نهایی نباید تصرف کلید خصوصی را برای دریافت گواهی به اثبات برسانند
سطح ۲	کاربران نهایی باید تصرف کلید خصوصی را برای دریافت گواهی به اثبات برسانند
سطح ۳	کاربران نهایی باید تصرف کلید خصوصی را برای دریافت گواهی به اثبات برسانند
سطح ۴	کاربران نهایی باید تصرف کلید خصوصی را برای دریافت گواهی به اثبات برسانند

۵-۹- ثبت وقایع

جدول ۱۳ ثبت وقایع

سطح اطمینان	نیازمندی‌های نگهداری ثبت وقایع
سطح ۱	نیازی به مشخص نمودن مدت زمان نگهداری وقایع نیست
سطح ۲	وقایع ثبت شده مرکز باید برای ۷ سال نگهداری شود
سطح ۳	وقایع ثبت شده مرکز باید برای ۱۰ سال نگهداری شود
سطح ۴	وقایع ثبت شده مرکز باید برای ۲۰ سال نگهداری شود

۵-۱۰- طول کلید

جدول ۱۴ طول کلید

سطح اطمینان	معیار طول کلید نامتقارن
سطح ۱	کلیدها باید معادل امنیتی ۱۰۲۴ معیار RSA باشند
سطح ۲	کلیدها باید معادل امنیتی ۱۰۲۴ معیار RSA باشند
سطح ۳	کلیدها باید معادل امنیتی ۲۰۴۸ معیار RSA باشند
سطح ۴	کلیدها باید معادل امنیتی ۲۰۴۸ معیار RSA باشند

۵-۱۱- محافظت از کلید خصوصی

جدول ۱۵ اطلاع رسانی در مورد محافظت از کلید خصوصی

سطح اطمینان	اطلاع رسانی در مورد محافظت از کلید خصوصی

سطح ۱	نیازمندی خاصی وجود ندارد
سطح ۲	اطلاع دادن به صاحب امضاء در مورد رعایت ملاحظات مربوط به حفظ کلیدخصوصی
سطح ۳	امضاء مستندی که نیازمندی‌های مربوط به ملاحظات حفظ کلید خصوصی توسط صاحب امضاء را قبل از صدور گواهی مشخص نموده باشد
سطح ۴	امضاء مستندی که نیازمندی‌های مربوط به ملاحظات حفظ کلید خصوصی توسط صاحب امضاء را قبل از صدور گواهی مشخص نموده باشد

جدول ۱۶ نیازمندی های مربوط به محافظت از کلید خصوصی

سطح اطمینان	حداقل نیازمندی‌های مربوط به محافظت از کلید خصوصی
سطح ۱	کلید امضاء CA و کلیدهای خصوصی کاربران نهایی ممکن است در سخت‌افزار یا نرم‌افزار ذخیره شوند
سطح ۲	کلید امضاء CA باید در سخت‌افزار و کلیدهای خصوصی کاربران نهایی ممکن است در سخت‌افزار یا نرم‌افزار ذخیره شوند
سطح ۳	کلید امضاء CA و کلیدهای خصوصی کاربران نهایی باید در سخت‌افزار ذخیره شوند
سطح ۴	کلید امضاء CA و کلیدهای خصوصی کاربران نهایی باید در سخت‌افزار ذخیره شوند

۵-۱۲- افشاء کلید خصوصی

جدول ۱۷ وسعت خسارات در صورت افشاء کلید خصوصی

سطح اطمینان	وسعت خسارات در صورت افشاء کلید خصوصی
سطح ۱	هیچ ضرر و زیانی در صورت افشاء کلید خصوصی کاربران نهایی پدید نمی‌آید
سطح ۲	زیان‌هایی در صورت افشاء کلیدهای خصوصی محرمانگی بوجود می‌آید
سطح ۳	زیان‌های جدی در صورت افشاء کلیدهای خصوصی محرمانگی بوجود می‌آید
سطح ۴	زیان‌های شدیدی در صورت افشاء کلیدهای خصوصی محرمانگی بوجود می‌آید

۶- شناسه سطوح اطمینان

۶-۱- امضاء دیجیتال

جدول ۱۸ شناسه سیاست های سطوح مختلف امضاء دیجیتال

سطح اطمینان	OID
سطح ۱	2.16.364.101.1.1.1.1.1
سطح ۲	2.16.364.101.1.1.1.2.1
سطح ۳	2.16.364.101.1.1.1.3.1
سطح ۴	2.16.364.101.1.1.1.4.1

۶-۲- محرمانگی

جدول ۱۹ شناسه سیاست های سطوح مختلف محرمانگی

سطح اطمینان	OID
سطح ۱	2.16.364.101.1.1.2.1.1
سطح ۲	2.16.364.101.1.1.2.2.1
سطح ۳	2.16.364.101.1.1.2.3.1
سطح ۴	2.16.364.101.1.1.2.4.1

۶-۳- احراز هویت

جدول ۲۰ شناسه سیاست های سطوح مختلف احراز هویت

سطح اطمینان	OID
سطح ۱	2.16.364.101.1.1.3.1.1
سطح ۲	2.16.364.101.1.1.3.2.1
سطح ۳	2.16.364.101.1.1.3.3.1
سطح ۴	2.16.364.101.1.1.3.4.1

۷- سطوح اطمینان مراکز

مراکز مختلف با توجه به نوع گواهی قابل ارائه، تقسیم‌بندی می‌شوند و یک مرکز صدور گواهی می‌تواند سیاست‌های گواهی را برای بیشتر از یک سطح اطمینان پیاده سازی نماید. هیچ موافقت نامه جهانی در مورد استانداردی برای توصیف سطوح اطمینان وجود ندارد. استاندارد دولت کانادا، دولت آمریکا، دولت استرالیا دارای چهار سطوح اطمینان Rudimentary, Basic, Medium و High بوده که گاهی با عناوین Level 1, 2, 3, 4 نام‌برده می‌شوند.

جدول۲۱ سطوح مراکز و سطوح گواهی های قابل ارائه آنها

CA Class	سطح گواهی قابل ارائه
Class 1	Level 1
Class 2	Level 1, 2
Class 3	Level 1, 2, 3
Class 4	Level 1, 2, 3, 4

۷-۱- سطوح اطمینان مراکز مختلف

جدول ۲۲ سطوح مختلف مراکز صدور گواهی الکترونیکی

CA Class	سطح گواهی قابل ارائه
مرکز دولتی ریشه	Class 4
مرکز میانی دولتی عام	Class 4
مرکز میانی دولتی	Class 3
مرکز بیرونی	Class 3

۸- نیازمندی های ماژول های رمزنگاری

جدول ۲۳ نیازمندی های ماژول های رمزنگاری

مراکز ثبت نام	کاربران	مراکز صدور گواهی	Latest version of FIPS 140 series	**سطح اطمینان**
Level 1 (Hardware or Software)	N/A	(Software)	N/A	سطح ۱
Level 1 (Hardware or Software)	Level 1 (Hardware or Software)	Level 2 (Hardware)	Required	سطح ۲
Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Required	سطح ۳
Level 3 (Hardware)	Level 3 (Hardware)	Level 3 (Hardware)	Required	سطح ۴

مراجع و ماخذ:

1. Implementing Levels of Assurance in a Trust Federation using PKI and Shibboleth, Australian Access federation
2. Verisign Key Hierarchy
3. PKI CP Requirements for Certificate Levels of Assurance, USA
4. X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), USA
5. http://www.tbs-sct.gc.ca/pki-icp/guidedocs/oids/oids08-eng.asp, Canada