مطالعه حقوقی زیرساخت کلید عمومی

دکتر پرویز ساورائی*
دکتر باقر طاهریان‌فر**

چکیده

دفاتر خدمات صدور گواهی الکترونیکی موضوع ماده ۳۱ قانون تجارت الکترونیکی به‌عنوان واحدهایی که امر ارایه خدمات صدور امضای الکترونیکی را برعهده می‌گیرند، براساس تجویز آیین‌نامه اجرایی ماده ۳۲ قانون مذکور در حال تأسیس و شکل‌گیری است. دفاتر مذکور بر مبنای زیرساخت کلید عمومی که در واقع مهندسی امنیت مبادله اطلاعات در محیط غیرایمن اینترنت است، اقدام به‌صدور گواهی الکترونیکی می‌کنند. عملکرد زیرساخت کلید عمومی مبتنی بر روابط اجزای مختلف آن شکل می‌گیرد.

در این مقاله به‌بررسی چهارچوب زیرساخت کلید عمومی به‌عنوان ابزار احراز هویت و تصدیق تمامیت و صحت پیغام در محیط الکترونیکی و بخصوص اینترنت پرداخته می‌شود، همچنین ماهیت، اجزا و عملکرد تکنیکی زیرساخت کلید عمومی مورد بررسی قرار می‌گیرد، بدین‌نحو که ابتدا مفهوم زیرساخت کلید عمومی سپس اجزا و در ادامه عملکرد تکنیکی زیرساخت کلید عمومی مورد توجه قرار می‌گیرد. نتایج کلی تحقیق بیانگر آنست که با تکیه بر عملکرد تکنیکی زیرساخت کلید عمومی، امضای الکترونیکی قابل اطمینان شکل می‌گیرد که افزایش سطح اعتماد و اطمینان کاربران در محیط غیرایمن الکترونیکی و تضمین امنیت ارتباطاتی آنان بر روی شبکه‌های اینترنتی و حفظ محرمانگی پیغام را به‌دنبال خواهد داشت.

کلید واژه‌ها

زیرساخت کلید عمومی، مرجع گواهی، مرجع ثبت، مرجع بایگانی، امضای الکترونیکی و طرف اعتمادکننده.

---

* دانشیار دانشکده حقوق دانشگاه شهیدبهشتی تهران.
** دانش‌آموخته مقطع دکتری رشته حقوق خصوصی دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران.

مقدمه

پیشرفت فناوری اطلاعات موجب تغییر مبادلات تجاری از نوع سنتی به‌الکترونیکی شده است. تحول شگرف مزبور در سایه نظام‌مند کردن این قبیل مبادلات تجاری ضمن افزایش اعتماد و اطمینان کاربران در محیط غیرایمن الکترونیکی، امنیت ارتباطاتی آنان بر روی شبکه‌های اینترنتی را تضمین کرده است. در این راستا پس از پذیرش قانون نمونه آنسیترال در مورد تجارت الکترونیکی، قانون نمونه آنسیترال در مورد امضاهای الکترونیکی نیز در سال ۲۰۰۱ از سوی کمیسیون تجارت بین‌الملل سازمان ملل‌متحد با تأکید بر مسائل مربوط به‌امضای الکترونیکی و مراجع گواهی به‌تصویب رسید. بدین‌ترتیب عملکرد اصلی مراجع گواهی که مبتنی بر تضمین صحت فرآیند تصدیق امضای دیجیتال بر پایه زیرساخت کلید عمومی به‌عنوان ابزار احراز هویت و تصدیق تمامیت و صحت پیغام در محیط الکترونیکی و به‌طور ویژه اینترنت است، توجیه‌پذیر گردید. در این مقاله با بررسی حقوقی زیرساخت کلید عمومی، مفهوم و ماهیت زیرساخت کلید عمومی را مورد مطالعه قرار می‌دهیم سپس اجزای آن را خواهیم شناخت و در ادامه عملکرد تکنیکی زیرساخت کلید عمومی را مورد توجه قرار خواهیم داد.

۱ـ مفهوم زیرساخت کلید عمومی

زیرساخت کلید عمومی[1] را می‌توان مجموعه‌ای از نرم‌افزارها، سخت‌افزارها، فناوری‌های رمزنگاری و خدماتی دانست که اشخاص را قادر می‌سازد امنیت ارتباطاتی خود بر روی شبکه‌های الکترونیکی (اینترنتی) را تضمین نمایند.(۱) در واقع زیرساخت کلید عمومی مهندسی امنیت مبادله اطلاعات در محیط غیرایمن الکترونیکی است که برای بالا بردن سطح بالایی از اعتماد و اطمینان برای کاربران ضرورت دارد.

به‌طور کلی برای زیرساخت کلید عمومی می‌توان کارکردهای زیر را تصور نمود:

۱ـ شبکه‌ای است که ضمن تأیید هویت فرستنده،[2] تمامیت[3] و محرمانگی[4] پیغام را تضمین می‌نماید و احتمال هرگونه انکار بعدی[5] را منتفی می‌سازد.

۲ـ تکنیک‌های رمزنگاری به‌کار رفته در آن ایمن است.

۳ـ افراد را قادر می‌سازد تا در یک سازمان یا خارج از آن به‌اطلاعات دست یافته اعتماد کنند.

۴ـ الزام‌آور ساختن سیاست‌های زیرساخت را با استفاده از اطلاعات گواهینامه‌ها سرلوحه کار دارد.(۲)

۵ـ اطلاعات مورد اعتماد در خصوص اشخاص را در گواهینامه‌های دیجیتال نگهداری می‌کند و اطلاعات گواهینامه‌ها را با اطلاعات جدید تطبیق می‌دهد و یا آنها را مردود می‌نماید.

۶ـ امکان انتقال ایمن گواهینامه را بین اعضای زیرساخت فراهم می‌کند.

1. Publice key infrastructure (PKI)
2. Authentication
3. Integrity
4. Confidentiality
5. Non - repudiation

همچنین می‌توان موارد زیر را نیز به‌خدمات قابل ارایه توسط زیرساخت کلید عمومی افزود:

الف) ارایه خدمات ثبت تاریخ؛[1]

ب) اداره کلیدهای رمزنگاری که به‌صورت محرمانه به‌کار می‌روند؛[۳]

ج) تأیید مطابقت کلید عمومی با یک کلید خصوصی معین؛

د) ارایه یک فهرست ایمن حاوی کلیدهای عمومی یا گواهی؛

هـ) اداره کلیدهای رمزنگاری برای شناسایی امضای دیجیتال؛

و) ایجاد کلیدهای عمومی و خصوصی برای اشخاص.

چنانکه می‌بینیم زیرساخت کلید عمومی از یک طرف با استفاده از کلید عمومی و خصوصی به‌اثبات هویت فرستنده و تأیید محتوای پیغام می‌پردازد و از سوی دیگر به‌معنای تکنولوژی و تکنیک‌هایی است که در کنار هم ایمنی زیرساخت را فراهم می‌آورند. با این وجود تعاریف مذکور با ارایه وظایف زیرساخت کلید عمومی سعی در شناسایی مفهوم آن دارند، بنابراین می‌توان گفت زیرساخت کلید عمومی مجموعه‌ای از کارکردهای تکنولوژیک، خدمات تکنیکی و رویه‌های تجاری است که سبب ترتب اثرات حقوقی اسناد کاغذی بر ارتباطات شبکه‌های الکترونیکی می‌کردد.[۴]

در آیین‌نامه اجرایی ماده (۳۲) قانون تجارت الکترونیکی ایران مصوب ۱۳۸۲، زیرساخت کلید عمومی در بند (ش) ماده (۱) در مفهوم بین‌المللی آن چنین تعریف شده است: «مجموعه‌ای از نرم‌افزارها، سخت‌افزارها، سیاست‌ها، فرآیندها و روال‌های مورد نیاز برای مدیریت گواهی‌ها و زوج کلیدها».

سیاست‌های گواهی مجموعه سیاست‌های گواهی الکترونیکی می‌باشد که مشتمل بر سیاست‌ها، قوانین، مقررات و روش‌های فنی، حقوقی و ساختاری که مطابق با استانداردهای بین‌المللی تدوین شده است می‌باشد و حداقل خواسته‌ها و الزامات پیاده‌سازی مراکز صدور گواهی، دفاتر ثبت‌نام، صاحبان امضا و طرف‌های اعتمادکننده را مشخص می‌کند. تدوین این سیاست‌های گواهی برای مرکز ریشه الزامی است و می‌تواند برای مرکز میانی به‌طور جداگانه تنظیم کردد. (بند ژ ماده ۱ آیین‌نامه)

زوج کلید یا داده‌های ایجاد و وارسی امضای الکترونیکی[2] به‌کلید خصوصی و کلید عمومی مرتبط با آن در یک رمزنگاری نامتقارن اطلاق می‌کردد. (بند خ ماده ۱)

بر اساس بندهای (چ) و (ح) ماده (۱) داده‌های ایجاد و وارسی امضای الکترونیکی چنین تعریف شده است:

داده ایجاد امضای الکترونیکی، داده‌ای انحصاری نظیر رمز یا کلید خصوصی که امضاکننده برای ایجاد امضای الکترونیکی از آن استفاده می‌کند، می‌باشد و داده وارسی امضای الکترونیکی عبارت است از داده‌ای نظیر رمز یا کلید عمومی که برای بررسی و صحت امضای الکترونیکی مورد استفاده قرار می‌گیرد.

مرکز ریشه و مرکز میانی بر اساس بندهای (پ) و (ت) ماده (۱) به‌ترتیب عبارتند از: مرکز صدور گواهی الکترونیکی ریشه، موضوع بند (الف) ماده (۴) آیین‌نامه و مرکز صدور گواهی الکترونیکی میانی، موضوع بند (ب) ماده۴.

1. Time - stamping
2. Signature –verification data

ماده (۴).

با روشن شدن مفاهیم به‌کار رفته در تعریف زیرساخت کلید عمومی، یادآور می‌شویم که چون حوزه زیرساخت کلید عمومی نیازمند سیاست‌گذاری ویژه‌ای دانسته شده، بدین‌منظور شورایی تحت عنوان شورای سیاست‌گذاری گواهی الکترونیکی در نظر گرفته شده است. شورای مذکور که اعضایش بر طبق ماده ۲ آیین‌نامه انتخاب می‌شوند وظایف متعددی بر عهده دارد.[1]

شایان ذکر است که اعتبار و پذیرش گواهی الکترونیکی صادره از مرجع صدور گواهی خارجی بر اساس ماده ۱۸ آیین‌نامه، مشروط به‌توافق دوجانبه بین مرکز ریشه کشور و مرجع صدور گواهی خارجی با رعایت اصل شرط متقابل و تصویب شورا خواهد بود.

۲ـ اجزای زیرساخت کلید عمومی

عناصر تشکیل‌دهنده زیرساخت کلید عمومی عبارتند از: مرجع گواهی[2]، مرجع ثبت[3] و مرجع بایگانی[4] که در برقراری ارتباط امضاکننده،[5] تأمین‌کننده خدمات گواهی[6] و طرف اعتمادکننده[7] مورد استفاده قرار می‌گیرند.

۲ ـ ۱ ـ مرجع گواهی

گواهی در شبکه‌های الکترونیکی نقش اساسی در شناسایی هویت اشخاص دارد. فعالیت مهم مراجع گواهی مبتنی بر تضمین صحت فرآیند امضای دیجیتال است. این مراجع از مجموعه نرم‌افزار، سخت‌افزار و اشخاص تشکیل می‌شوند. مراجع گواهی شباهت زیادی با دفاتر اسناد رسمی دارند و همانند آنها برای برقراری ثبات و امنیت در اعمال حقوقی به‌وجود آمده‌اند، زیرا همان‌طوری که دفتر اسناد رسمی هویت طرفین را شناسایی و وقوع معامله، زمان و مکان آن را با تصدیق وجود قصد و رضای طرفین تأیید می‌نماید، مراجع مزبور نیز هویت درخواست‌کنندگان

---

۱. وظایف شورای سیاست‌گذاری طبق ماده ۳ آیین‌نامه اجرایی به‌شرح زیر است:
«الف) بررسی سیاست‌های کلان و برنامه‌های مربوط به‌حوزه زیرساخت کلید عمومی کشور و ارایه آن به‌شورای عالی فناوری اطلاعات کشور جهت تصویب؛
ب) صدور مجوز ایجاد مرکز ریشه؛
پ) تصویب و به‌روزرسانی سیاست‌ها و دستورالعمل گواهی مراکز ریشه و میانی؛
ت) تصویب استانداردها، رویه‌ها و دستورالعمل‌های اجرایی گواهی الکترونیکی،
ث) ایفای نقش به‌عنوان مرجع هماهنگ‌کننده در مورد فعالیت حوزه‌های گوناگون اجرایی؛
برای ارایه خدمات رایانه‌ای صدور گواهی مبنی بر زیرساخت کلید عمومی و نحوه تعامل مراکز صدور گواهی داخلی با مرکز صدور گواهی خارجی و هرگونه تفسیر یا کاربرد پذیری مفاد سیاست‌های گواهی ریشه و میانی؛
ج) نظارت عالیه و بررسی گزارش عملکرد و تخلفات احتمالی مراکز ریشه و میانی در صورت لزوم لغو مجوز آنها.»

2. Certification authority
3. Registration authority
4. Archives authority
5. Signature
6. Supplier of certification authority
7. Relying-party

صدور گواهی را شناسایی و امنیت معاملات را در محیط‌های الکترونیکی تضمین می‌نماید.گواهینامه صادره توسط مرجع گواهی ممکن است به‌صورت در دسترس مستقیم (بر خط)[1] و یا به‌صورت غیرقابل دسترسی مستقیم (خط بسته)[2] نگهداری شود.

به‌طور کلی می‌توان وظایف مراجع گواهی را در موارد زیر خلاصه نمود:

۱ـ تشخیص صحت اطلاعاتی که متقاضی خواستار درج آنها در گواهی می‌باشد، منجمله نام دارنده گواهی و کلید عمومی. بنابراین می‌بایستی تحقیق شود که داده‌های مربوط به‌شناسایی امضا با داده‌هایی که همان شخص جهت امضا به‌کار برده از نظر ریاضی ارتباط منطقی داشته باشند. بر اساس بند ۱ از ماده ۱۴ قانون ۹ ژوئیه ۲۰۰۱ بلژیک مرجع گواهی در قبال عدم صحت احتمالی اطلاعات مندرج در گواهی مسئولیتش مفروض است، مگر اینکه عدم تقصیرش را ثابت نماید.(۵)

۲ـ اطمینان از اینکه متقاضی گواهی، داده‌های مربوط به‌ایجاد امضا[3] و داده‌های مربوط به‌شناسایی امضای الکترونیکی را دارد. داده‌های مربوط به‌ایجاد امضا و داده‌های مربوط به‌شناسایی آن به‌ترتیب همانند کلید خصوصی و کلید عمومی هستند که هر یک کارکرد خاص خود را دارند.

۲ـ عمل مطابق با اظهارات اعلامی در خصوص سیاست‌ها و روش‌ها همچنین انجام مراقبت معقول و متعارف جهت کسب اطمینان از صحت و کامل بودن تمامی اظهارات مهمی که به‌وسیله مرجع گواهی اعلام شده و با گواهی مرتبط بوده و یا در آن درج شده باشد.[4]

۴ـ مرجع گواهی موظف است از سیستم‌ها، رویه‌ها و منابع انسانی مطمئن جهت ارایه خدمت استفاده نماید.[5]

۵ـ مرجع گواهی بایستی گواهی را در دسترس قرار دهد. بر اساس ماده ۱۰ قانون ۹ ژوئیه ۲۰۰۱ بلژیک، مرجع گواهی مکلف است:

یک دفتر راهنمای الکترونیکی حاوی گواهی‌های صادره و تاریخ انقضای آنهاست. بر طبق بند (ب) ضمیمه ۲ قانون فوق‌الذکر عملکرد دفتر راهنمای مذکور باید سریع و مطمئن باشد. به‌عبارت دیگر کاربران بتوانند با اطمینان کافی فوراً گواهی موردنظر را تحصیل نمایند. به‌موجب بند (ج) قانون مذکور نیز مرجع گواهی باید دقت کند که تاریخ و ساعت صدور و انقضای گواهی قابل تشخیص باشد، در صورت ارایه مطلوب خدمات، مرجع گواهی مسئول زیان‌های وارده و همچنین استفاده و بهره‌برداری از گواهی در خارج از زمان اعتبار آن، نخواهد بود.(۶)

۶ ـ صدور گواهی: در صورت تشخیص صحت اطلاعات، مرجع گواهی مکلف است گواهی مورد درخواست متقاضی را صادر نماید. مرجع مزبور با کلید خصوصی خود، گواهی صادره به‌استناد تعلق کلید عمومی به‌شخص متقاضی را، امضا می‌نماید. برای شناسایی این امضا می‌توان از کلید عمومی آن مرجع استفاده کرد، این کلید عمومی در گواهی توسط مرجع دیگری در تأیید تعلق آن به‌مرجع نخست صادر شده درج شده است. اعتبار گواهی

1. On-line
2. Off-line
3. Signature –creation data

۴. بندهای (الف) و (ب) ماده ۹ قانون نمونه آنیسترال در زمینه امضاهای الکترونیکی.
۵. بندهای (و) ماده ۹ قانون نمونه آنیسترال در زمینه امضاهای الکترونیکی.

دوم را نیز می‌توان از طریق کلید عمومی مرجع دوم که در گواهی مرجع سومی آمده استخراج کرد تا اینکه شخص نسبت به‌اصالت و اعتبار امضای مزبور اطمینان حاصل کند.[۷]

۷ـ ابطال گواهی: مدت زمان گواهی‌های صادره محدود است، دارنده می‌تواند هر زمان که بخواهد درخواست ابطال آن را تسلیم نماید. البته در صورتی‌که مشخص گردد گواهی بر اساس اطلاعات غیرصحیح یا غیرواقع صادر شده، مرجع صدور گواهی موظف است رأساً گواهی صادره را ابطال نماید،[۸] یا اینکه آن را به‌حالت تعلیق در آورد. در هر صورت مرجع مزبور مکلف است ضمن انتشار مطلب، اشخاصی را که با گواهی باطل یا تعلیق شده امضای دیجیتالشان قابل شناسایی است، مطلع نماید.[۹] بدیهی است ابطال از زمان ثبت در برابر اشخاص ثالث قابل استناد خواهد بود (ماده ۱۲ قانون بلژیک)

به‌هر ترتیب مرجع گواهی چه دولتی و چه خصوصی جهت مرتبط ساختن یک جفت کلید با یک امضاکننده، اقدام به‌صدور گواهینامه‌ای[۱] می‌کند که به‌عنوان یک سند الکترونیکی، یک کلید عمومی را به‌نام ثبت‌نام‌کننده با عنوان موضوع[۲] گواهی منتشر کند. در گواهینامه مذکور تعلق کلید خصوصی متناظر به‌امضاکننده معین گاهاً مورد تأیید قرار می‌گیرد، بنابراین مرتبط ساختن یک امضاکننده خاص به‌یک کلید عمومی عملکرد اصلی یک گواهینامه تلقی می‌شود.[۱۰] گواهینامه در بند ۹ ماده ۲ دستورالعمل اتحادیه اروپا بدین‌صورت تعریف شده است: «گواهی الکترونیکی[۳] که کلید عمومی را به‌شخص مرتبط ساخته و هویت وی را تأیید و تصدیق می‌کند».[۱۱]

در کشور ما بر اساس آیین‌نامه اجرایی ماده (۳۲) قانون تجارت الکترونیکی هم به‌ارگان‌های دولتی و هم به‌بخش خصوصی مجوز دخالت در صدور گواهی الکترونیکی داده شده است. چنانکه در ماده ۴ آیین‌نامه مذکور آمده است: «سطوح دفاتر خدمات صدور گواهی الکترونیکی موضوع ماده (۳۱) قانون به‌عنوان ارایه‌دهندگان خدمات گواهی الکترونیکی به‌شرح زیر تعیین می‌شوند:

الف) مرکز دولتی صدور گواهی الکترونیکی ریشه که با کسب مجوز از شورا فعالیت می‌نماید؛

ب) مرکز صدور گواهی الکترونیکی میانی که با کسب مجوز از ریشه مبادرت به‌صدور گواهی الکترونیکی نموده و سایر خدمات مربوط به امضای الکترونیکی را انجام می‌دهد؛

پ) دفتر ثبت‌نام گواهی الکترونیکی ...»

در تبصره ۱ ماده مذکور، مرکز دولتی صدور گواهی الکترونیکی را وابسته به‌مرکز توسعه تجارت الکترونیکی موضوع ماده (۸۰) قانون تجارت الکترونیکی دانسته و در تبصره ۲ نیز برای سیستم بانکی کشور این تسهیلات را قایل شده که با اخذ مجوز از شورای سیاست‌گذاری گواهی الکترونیکی در حوزه نظام بانکی مرکز ریشه مستقل ایجاد نماید. البته در این صورت مرکز یاد شده وابسته به‌مرکز توسعه تجارت الکترونیکی موضوع این ماده نخواهد بود.

برای ایجاد مراکز میانی حسب مورد توسط دستگاه‌های دولتی یا بخش غیردولتی ضوابط و شرایطی در نظر

1. Certificate
2. Subject
۳. گواهی الکترونیکی در بند (چ) ماده (۱) آیین‌نامه اجرایی ماده (۳۲) قانون تجارت چنین تعریف شده است: «داده الکترونیکی حاوی اطلاعاتی که در مورد مرکز صادرکننده گواهی، مالک گواهی، تاریخ صدور و انقضا، کلید عمومی مالک و یک شماره سریال که توسط مرکز میانی تولید شده، به‌گونه‌ای که هر شخص می‌تواند به‌صحت ارتباط بین کلید عمومی و مالک آن اعتماد کند».

گرفته شده که در صورت تحقق آنها مجوز تأسیس صادر خواهد شد.[1]

در صورتی که شرایط مذکور تحقق یابد مراکز ریشه مکلفند ظرف دو ماه نسبت به‌بررسی تقاضا، اقدام و نتیجه را به‌متقاضیان اعلام نمایند. (تبصره ۱ ماده ۷ آیین‌نامه مذکور)

ظرف مدت شش ماه از تاریخ صدور مجوز، اشخاصی که مجوز راه‌اندازی مرکز میانی را اخذ نموده‌اند، مکلفند نسبت به‌تأسیس مرکز اقدام نمایند والاّ مجوز آنها لغو شده تلقی خواهد شد (تبصره ۴ مادهٔ ۷ آیین‌نامه). بر اساس تبصره ۳ ماده ۷ آیین‌نامه مراکز میانی دولتی از ابتدای سال ۱۳۸۸ مجاز به‌ارایه خدمات گواهی الکترونیکی به‌بخش‌های غیردولتی خارج از حوزه فعالیت خود نخواهند بود. مضافاً اینکه بر اساس تبصره ۲ همان ماده مراکز میانی ایجاد شده توسط سازمان‌های دولتی بایستی به‌صورت غیرانتفاعی فعالیت نمایند.

برای مرکز میانی و مراکز ریشه در آیین‌نامه فوق‌الذکر وظایف مختلفی لحاظ شده است. وظایف مرکز ریشه در ماده ۵ آیین‌نامه تعیین شده است.[2]

مراکز میانی نیز ضمن رعایت مفاد دستورالعملهای گواهی[3] در زمان فعالیت وظایفی را بر اساس ماده ۸ آیین‌نامه

---

۱. این شرایط بر اساس ماده ۷ آیین‌نامه عبارتند از:

«الف) ارایه اساسنامه یا مجوز ثبت از مراجع ذیربط؛

ب) ارایه تقاضا از طرف متقاضی؛

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

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

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

ت) تأمین مکان فیزیکی مناسب همراه با تجهیزات سخت‌افزاری و نرم‌افزاری لازم اعلام شده از سوی مرکز ریشه به‌نحوی که امنیت فنی و رمزنگاری را تضمین نماید و مورد تأیید بازرسان مرکز ریشه قرار گرفته باشد؛

ث) ارایه تضمین معتبر مناسب با مبلغ تعیین شده توسط مرکز ریشه؛

ج) تدوین سیاست‌ها و دستورالعمل گواهی مرکز».

۲. «الف) پیشنهاد سیاست‌ها و دستورالعمل‌های گواهی مرکز ریشه و ارایه به‌شورا جهت تصویب

ب) اجرای سیاست‌های و دستورالعمل‌های شورا؛

ج) بررسی و تصویب سیاست‌ها و دستورالعمل‌های مراکز میانی؛

ت) بررسی و احراز شرایط لازم و صلاحیت متقاضیان ایجاد مراکز میانی و صدور مجوز برای آنها؛

ث) حصول اطمینان از ثبت اطلاعات معتبر و مناسب در گواهی‌ها و نگهداری مدارک و شواهد دال بر صحت این اطلاعات؛

ج) حصول اطمینان از عملکرد صحیح مراکز میانی؛

چ) ابطال گواهی مراکز میانی که برخلاف تعهداتشان عمل کرده‌اند؛

ح) اطلاع‌رسانی به‌صاحبان امضا و طرف‌های اعتمادکننده در مورد هرگونه تغییر در کارکرد مرکز میانی؛

خ) ایجاد و به‌روز رسانی یک مخزن بر خط و اطلاع‌رسانی خدمات آن».

۳. دستورالعمل گواهی عبارتست از مجموعه‌ای دستورالعمل که منطبق با سیاست‌های گواهی جهت تشریح جزییات عملکرد مدیریت گواهی‌های الکترونیکی در مرکز ریشه و مراکز میانی تدوین می‌گردد (بند (س) ماده (۱) آیین‌نامه اجرایی ماده ۳۲).

بر عهده خواهند داشت.[1]

علاوه بر وظایف مذکور، وظیفه حفظ محرمانگی داده‌های ایجاد امضای الکترونیکی نیز بر اساس ماده ۱۷ آیین‌نامه بر عهده مراکز میانی می‌باشد.

همان‌طور که گفتیم یکی از وظایف مراجع گواهی، ابطال گواهی در صورت وجود زمینه ابطال است. بنابراین در مواردی ضروریست ضمن حفظ سوابق موجود، گواهی الکترونیکی توسط صادرکننده آن ابطال گردد. بر اساس ماده ۱۹ آیین‌نامه اجرایی ماده (۳۲) قانون تجارت الکترونیکی ایران در شرایط زیر گواهی الکترونیکی صادر شده توسط مرکز میانی ابطال می‌شود:

«الف) درخواست ابطال توسط صاحب گواهی الکترونیکی و یا وکیل قانونی وی؛

ب) تخطی صاحب گواهی الکترونیکی از تعهداتش؛

پ) احراز صدور گواهی مبتنی بر اظهارات دروغ و اشتباه متقاضی؛

ت) مشاهده تخلف صاحب گواهی و یا دفاتر ثبت‌نام و مرکز میانی از مندرجات این آیین‌نامه که در این صورت مرکز ریشه دستور ابطال گواهی را صادر نماید؛

ث) احراز صدور گواهی الکترونیکی که شامل اطلاعات شخص ثالث بوده و گواهی بدون رضایت وی صادر شده باشد؛

ج) افشای کلید خصوصی نزد سایر افراد غیرمجاز».

چنانکه ملاحظه می‌شود علاوه بر اشکال عبارتی در مفاد بند (ت) ماده مذکور ابهام وجود دارد. مشخص نیست در صورت تخلف صاحب گواهی، دفاتر ثبت‌نام و مرکز میانی از مندرجات آیین‌نامه اجرایی و مشاهده آن تخلف از سوی مرکز ریشه، وی بایستی دستور ابطال گواهی را صادر نماید که اگر این چنین نیز باشد، مجری دستور باز

---

۱. ماده ۸ آیین‌نامه اجرایی مقرر می‌دارد:

«الف) بررسی صلاحیت و صدور مجوز برای دفاتر ثبت‌نام ذیربط؛ ب) تضمین ارایه خدمات صدور و لغو گواهی‌ها به‌صورت مطمئن؛ پ) تضمین ارایه خدمات تأیید صحت گواهی‌ها به‌صورت سریع و مطمئن؛ ت) تضمین محرمانه بودن داده‌های مربوط به‌امضا در فرآیند ایجاد این داده‌ها برای جلوگیری از شبیه‌سازی گواهی‌ها؛ ث) حصول اطمینان نسبت به‌موارد زیر:

۱ـ در لحظه صدور گواهی الکترونیکی، اطلاعات مندرج در گواهی‌ها صحیح باشند؛

۲ـ در هنگام صدور گواهی الکترونیکی، امضاکننده مشخص شده در گواهی، داده‌های ایجاد و وارسی امضای الکترونیکی را دریافت نموده و داده ایجاد امضای الکترونیکی تحت کنترل انحصاری وی باشد؛

۳ـ کلیه اطلاعات مرتبط با گواهی الکترونیکی را تا مدت زمان تعیین شده در دستورالعمل گواهی به‌صورت الکترونیکی حفظ نماید؛

۴ـ تاریخ و ساعت صدور و لغو یک گواهی به‌دقت تعیین شده و قابل تشخیص باشد؛

۵ـ عدم کپی یا ذخیره داده یا ایجاد امضای الکترونیکی متقاضیان را تضمین نماید؛

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

۷ـ در صورت امکان مرکز میانی و با دریافت درخواست دفتر ثبت‌نام، یک مهر زمانی به‌داده‌های الکترونیکی ضمیمه شود.

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

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

مشخص نشده یا اینکه مرکز میانی موظف است با مشاهده وقوع هرگونه تخلفی، گزارش مربوطه را به‌مرکز ریشه منعکس نماید و مرکز مزبور اقدام به‌صدور دستور ابطال گواهی نماید.

در حالت نخست مفاد بند (ت) با سایر موارد مذکور در ماده ۱۹ آیین‌نامه اجرایی که به‌ابطال گواهی توسط مرجع میانی می‌پردازد، ارتباطی نخواهد داشت و در حالت دوم به‌نظر می‌رسد مرکز میانی را مسئول گزارش تخلفات خود کرده‌ایم که چنین امری نیز عملاً هیچ‌گاه محقق نخواهد شد، کمااینکه با امر نظارت سلسله مراتبی نیز در تضاد است. با ملاحظه سایر مواد آیین‌نامه اجرایی معلوم می‌شود که مجوز استفاده از گواهی برای صاحب گواهی توسط مرکز میانی صادر شده و فعالیت دفاتر ثبت‌نام نیز بر اساس گواهی صادره توسط مرجع مذکور امکان‌پذیر است. مرکز ریشه نیز مجوز فعالیت مرکز را صادر و ابطال می‌کند، بنابراین به‌نظر می‌رسد هر چند تخلف از مفاد تعهدات سبب ابطال مجوز توسط مرجع صادرکننده گواهی است، لکن تخلف از مفاد آیین‌نامه که شامل تخلف از تعهدات نگردد با تصمیم مرکز ریشه ابطال گواهی را در پی خواهد داشت. بنابراین رسیدگی به‌تخلفات غیرقراردادی در هر صورت به‌عهده مرکز ریشه گذاشته شده است.

۲ ـ ۲ ـ مرجع ثبت

مرجع ثبت، اطلاعات درخواست‌کننده گواهی در زمان ثبت‌نام را بررسی و تصدیق می‌کند. نظر به‌اینکه ثبت‌نام‌کنندگان به‌عنوان موضوعات گواهی متعدد هستند، ایجاب می‌کند که تعداد مراجع ثبت نیز زیاد باشند تا با مراجعه به‌آنها ثبت‌نام در کمترین زمان ممکن و با صرف کمترین هزینه امکان‌پذیر گردد.

به‌طور خلاصه می‌توان کارکردهای زیر را برای مراجع ثبت در نظر گرفت:

۱ـ گردآوری اطلاعات در مورد افراد و تأیید هویت آنان و بررسی صحت اطلاعات ارایه شده به‌منظور کسب اطمینان از اینکه درخواست‌کننده همان شخصی است که ادعا می‌کند و همچنین اطلاعات مورد تقاضای وی جهت درج در گواهی صحیح ارایه گردیده است.

۲ـ تشخیص مرتبط بودن داده‌های مربوط به‌ایجاد امضا و داده‌های مربوط به‌شناسایی آن در صورت عدم وجود مرجع ثبت، وظایف مرجع مزبور توسط خود مرجع گواهی انجام خواهد شد. به‌هر حال در صورت تردید در اطلاعات مندرج در گواهی‌نامه صادره، مرجع ثبت ضمن بررسی اطلاعات مزبور، گواهینامه را تصدیق کرده یا مردود اعلام می‌نماید. در صورت اخیر مرجع ثبت، با اعلام رجوع از اعتبار گواهینامه به‌مرجع گواهی، گزارشی از تمامی گواهی‌نامه‌های رجوع شده به‌زیرساخت کلید عمومی ارسال می‌کند.

اگر مرجع ثبت طی یک گواهی صادره توسط مرجع گواهی شناسایی و تصدیق شود، مرجع ثبت پس از تنظیم گواهینامه برای شخص متقاضی آن را به‌صورت یک پیام دیجیتالی امضا شده برای مرجع گواهی ارسال می‌نماید.[۱۲]

با وجود اینکه مرجع ثبت گواهینامه را امضا نمی‌نماید، مزیت به‌کارگیری آن در فراهم آوردن سیستم امنیتی مطمئن‌تر و محافظت از اطلاعات محرمانه روشن می‌شود.[۱۳]

مراجع ثبت با توجه به‌اهمیت گواهینامه مورد درخواست، مدارک و اسناد متنوع و مختلفی را می‌تواند مطالبه کند. در حالی که جهت صدور گواهی برای مبادلات؛ با مبالغ کم به‌اظهارات متقاضی، کارت اعتباری و آدرس وی می‌تواند اکتفا نماید، برای گواهی‌های مهم‌تر، ادله قوی‌تر را می‌طلبد چنانکه در مورد اشخاص حقیقی، انجام مصاحبه، ارایه گواهی‌نامه رانندگی و سایر مدارک شناسایی ضرورت خواهد داشت و در مورد اشخاص حقوقی، کسب اطلاعات از مرجع ثبت شرکت‌ها، می‌تواند میزان اعتبار شرکت مزبور را روشن نماید. مضافاً اینکه بسته به‌موقعیتی که قرار است امضا در آن مورد استفاده قرار گیرد ادله‌ای مربوط به‌اقامتگاه فرد یا فعالیت‌های وی، مطالبه خواهد شد.(۱۴)

مراجع ثبت در آیین‌نامه اجرایی ماده ۳۲ قانون تحت شرایط و ضوابط خاصی تشکیل و اداره می‌شوند و وظایف ویژه‌ای را نیز به‌عهده دارند که ذیلاً به‌بررسی آن می‌پردازیم.

بر اساس ماده ۱۲ آیین‌نامه مذکور اشخاص حقیقی و صاحبان امضای اشخاص حقوقی دولتی یا غیردولتی که متقاضی دریافت مجوز راه‌اندازی دفاتر ثبت‌نام در کشور باشند باید شرایط عمومی و اختصاصی خاصی را احراز کنند.[۱] و وظایفی را با توجه به‌ماده ۱۳ بر عهده گیرند.[۲]

مضافاً دفاتر ثبت‌نام موظفند هنگام ثبت‌نام متقاضی گواهی الکترونیکی بر اساس ماده ۱۵ آیین‌نامه مذکور، امضای شخص را برای صحت اطلاعات ارایه شده (املایی و محتوایی) اخذ نموده و وی را از نحوه و شرایط دقیق استفاده از گواهی‌ها، از جمله محدودیت‌های حاکم بر استفاده، خدمات و شیوه‌های طرح و پیگیری دعوی مطابق سیاست‌ها و دستورالعمل گواهی میانی آگاه سازند.

در قبال خدماتی که دفاتر ثبت‌نام ارایه می‌کنند، بر اساس نوع گواهی و خدمات ارایه شده به‌متقاضیان با توجه به‌تعرفه‌ای که به‌پیشنهاد شورا به‌تصویب هیأت وزیران می‌رسد، حق‌الثبت مشخص و معینی را اخذ می‌نمایند (ماده

۱. این شرایط عبارتند از:
«الف) تابعیت جمهوری اسلامی ایران؛
ب) تدین و عاملیت به‌احکام اسلام یا پیروی از ادیان به‌رسمیت شناخته شده در قانون اساسی؛ پ) نداشتن پیشینه کیفری؛ ت) عدم تجاهر به‌فسق و داشتن صلاحیت اخلاقی و حسن سابقه؛ ث) عدم اعتیاد به‌موادمخدر؛ ج) انجام خدمت وظیفه عمومی یا معافیت دائم؛ چ) دارا بودن حداقل مدرک کاردانی مورد تأیید وزارتخانه‌های علوم، تحقیقات و فناوری و بهداشت درمان و آموزش پزشکی؛ ح) ارایه ضمانت معتبر؛ خ) داشتن سابقه کار حداقل سه سال متوالی یا پنج سال متناوب مورد تأیید مرکز میانی در بخش‌های مرتبط با فناوری اطلاعات.
تبصره ۱ـ نوع و میزان ضمانت معتبر بر اساس دستورالعمل دفاتر صدور گواهی الکترونیکی میانی پیش‌بینی می‌شود.
تبصره ۲ـ شعب بانک‌ها به‌عنوان دفاتر ثبت‌نام مراکز میانی تحت نظارت مرکز ریشه نظام بانکی از شمول این ماده و ماده ۱۴ مستثنی هستند.
تبصره ۳ـ اشخاصی که مبادرت به‌اخذ مجوز راه‌اندازی دفتر ثبت‌نام با ملاحظه شرایط این ماده می‌نمایند مکلفند ظرف چهار ماه از تاریخ صدور مجوز نسبت به‌تأسیس دفتر اقدام نمایند. در غیر این صورت مجوز مذکور لغو شده تلقی می‌گردد.
تبصره ۴ـ متقاضی تأسیس دفتر ثبت‌نام موظف به‌تأمین مکان فیزیکی منسب مطابق دستورالعمل گواهی میانی طرف قرارداد و تهیه و نصب تابلو با درج شماره مجوز دریافتی از مرکز یا مراکز میانی طرف قرارداد می‌باشد.»
۲. ماده (۱۲) وظایف دفاتر ثبت‌نام به‌شرح زیر می‌باشد:
الف) انجام عملیات مطابق با دستورالعمل گواهی مرکز میانی مربوط؛
ب) احراز هویت و تصدیق مدارک ارایه شده متقاضی دریافت خدمات گواهی؛
پ) ارسال درخواست متقاضی همراه با مدارک مربوطه به‌مرکز میانی مربوط؛
ت) دریافت گواهی صادر شده از مرکز میانی مربوطه و تحویل به‌متقاضی.

۱۶ آیین‌نامه مذکور)

در صورتی که ثبت گواهی بدون کسب مجوز از یک مرجع گواهی در مرجع ثبت انجام شود، مشمول مواد آیین‌نامه اجرایی ماده ۳۲ قانون نخواهد بود و در این خصوص ماده ۱۱ آیین‌نامه موصوف مقرر داشته است:

«کلیه مؤسسات اعم از دولتی یا غیردولتی می‌توانند در حوزه فعالیت داخلی خود بدون اخذ مجوز از مرکز ریشه مبادرت به‌ثبت و صدور گواهی نمایند. گواهی‌هایی که بدین‌صورت صادر می‌شود خارج از شمول مقررات این آیین‌نامه بوده و امضاهایی که به‌وسیله این گواهی‌ها تأیید می‌شوند، خارج از موضوع ماده ۱۰ قانون تجارت الکترونیکی ایران محسوب نخواهند شد».

چنانکه ملاحظه می‌شود در این ماده فقط به‌ثبت و صدور گواهی بدون اخذ مجوز از مرکز ریشه توسط مؤسسات دولتی یا غیردولتی اشاره شده و از مرکز میانی صحبتی به‌میان نیامده است. در حالی که مؤسسات غیردولتی جهت فعالیت به‌عنوان مرجع صدور گواهی فقط می‌توانند در قالب مراجع میانی تأسیس شوند و از طرف دیگر مرکز ریشه بر اساس بند (پ) ماده ۴ آیین‌نامه، دفتر ثبت‌نام گواهی الکترونیکی پس از اخذ مجوز فعالیت از حداقل یک مرکز میانی نسبت به‌ثبت و انتقال درخواست متقاضیان در خصوص صدور و لغو گواهی‌ها و سایر امور مربوط به‌آنها مطابق با ضوابط و دستورالعمل صادره از سوی مراکز میانی که تعهد همکاری با آنها را امضا نموده، اقدام می‌نماید. بنابراین مجوز مراجع ثبت نیز توسط مرکز ریشه صادر نمی‌شود.

با این توضیحات برای اصلاح عبارت ماده ۱۱ آیین‌نامه پیشنهاد می‌شود یا «مؤسسات غیردولتی» از متن حذف گردد یا اینکه به‌جای «مرکز ریشه» عبارت «مراکز صدور گواهی مربوطه» اضافه گردد که هم شامل مرکز ریشه و هم مراکز میانی شود.

۲ ـ ۳ ـ مرجع بایگانی[۱]

به‌دلیل انجام تغییرات اداری یا پرسنلی یا جلوگیری از احتمال دسترسی دیگران به‌کلیدهایی که جهت امضا کردن یا رمزنگاری به‌کار برده شده، بعضاً ضرورت می‌یابد که کلیدهای مذکور ابطال و مواردی دیگر جایگزین آنها شوند به‌منظور تشخیص اصالت پیام‌هایی که قبلاً و در گذشته با نام دارنده گواهی امضا شده است اسناد و مدارک مربوطه بایستی در جایی بایگانی و نگهداری شوند تا با رجوع به‌آنها بتوان نشان داد که آیا در زمان مورد ادعا از کلیدهای رمزنگاری و امضا استفاده شده یا خیر. در این‌گونه موارد معمولاً دارنده گواهی به‌مرجع گواهی مراجعه می‌کند حال اگر مرجع مربوط نتواند اطلاعات درخواستی را ارایه نماید، مشکلات عدیده‌ای بروز خواهد کرد.[۱۵]

برای حل این مشکل مرجعی به‌نام مرجع بایگانی ایجاد می‌شود که وظیفه‌اش ذخیره بلندمدت اطلاعات به‌نمایندگی از مراجع گواهی می‌باشد. مرجع بایگانی، اعتبار اطلاعات در زمان دریافت و عدم تغییر آنها را در زمان نگهداری تأیید می‌نماید. اطلاعات ارسالی توسط مرجع گواهی برای مرجع بایگانی بایستی به‌نحوی باشد که امکان تشخیص صدور حقیقی گواهی از ناحیه مرجع مزبور را فراهم آورد، ضمن اینکه بایستی مدت اعتبار آنها را نیز مشخص

۱. در آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی بند (ر) اصطلاح مخزن آورده شده که فقط برای استفاده طرف اعتمادکننده ایجاد شده و عبارت است از یک پایگاه داده ذخیره و انتشار گواهی‌های الکترونیکی و اطلاعات مربوط به‌آنها.

نماید. مرجع بایگانی در صورت بروز اختلاف بعدی میان اشخاص می‌تواند با مراجعه به‌اطلاعاتی که با توسل به‌مکانیسم‌های فنی و رویه‌های مناسب محافظت و نگهداری شده‌اند، تشخیص دهد که آیا کلید عمومی مرتبط با کلید خصوصی در امضای سند دخیل بوده‌اند یا خیر. بدین‌ترتیب تشخیص اصالت و اعتبار امضای اسناد در زمان‌های بعد فراهم می‌آید.(۱۶)

۲ ـ ۴ ـ کاربران زیرساخت کلید عمومی

با تدقیق در مباحث گذشته روشن می‌شود که کاربران زیرساخت کلید عمومی دو گروهند:

الف) ثبت‌نام‌کننده گواهی؛

ب) طرف اعتمادکننده.

ذیلاً در مورد هر یک از این کاربران توضیحاتی ارایه می‌نماییم:

۲ ـ ۴ ـ ۱ ـ ثبت‌نام‌کننده گواهی

ثبت‌نام‌کننده گواهی شخصی است که ضمن مراجعه به‌یک مرجع ثبت و اثبات هویت، درخواست صدور یک گواهی را به‌نام خود می‌نماید. ثبت‌نام‌کننده همان دارنده گواهی محسوب می‌شود که می‌تواند هر شخص حقیقی یا حقوقی باشد که گواهی برایش صادر می‌شود. بنابراین دارنده گواهی شخصی است که در گواهی معرفی شده و کلیه اطلاعات مربوط به‌هویت و شناسایی امضا و اطلاعات تکمیلی دیگری که بنا به‌تقاضای شخصی در گواهی درج شده و به‌وی تعلق دارد. ثبت‌نام‌کننده می‌تواند چند گواهی مختلف و در نتیجه چند امضای الکترونیکی با مشخصات مختلف داشته باشد و در جریان فعالیت‌های خود از آنها استفاده نماید، امری که در خصوص تعدد امضای دستی نیز امکان‌پذیر است.

ثبت‌نام‌کننده پس از صدور گواهی، موضوع گواهی محسوب می‌گردد.(۱۷) موضوع گواهی در مرحله بعد چنانکه در بند (د) ماده ۲ قانون نمونه آنیسترال در زمینه امضای الکترونیکی آمده است، به‌عنوان امضاکننده[1] عمل می‌کند. بر اساس این قانون «امضاکننده کسی است که داده‌های مربوط به‌ایجاد امضاء را در اختیار دارد و اصالتاً یا به‌نمایندگی از دیگری اقدام می‌کند».(۱۸) با مقایسه بین تعریف امضاکننده در بند (ل) ماده ۲ قانون تجارت الکترونیکی ایران با قانون نمونه آنیسترال به‌عنوان الگوی قانون تجارت الکترونیکی ایران، مشخص می‌شود که واژه قائم‌مقام در قانون تجارت الکترونیکی ایران در معنای اصطلاحی خود استفاده نشده بلکه منظور از قائم‌مقام، نماینده یا وکیلی است که برای دیگری امضا می‌کند، منجمله برای اشخاص حقوقی.

در مورد وظایف ثبت‌نام‌کننده (دارنده گواهی) و در مرحله بعد امضاکننده در ماده ۸ قانون نمونه آنیسترال آمده است:

«۱ـ هنگامی که داده ایجاد امضا برای ایجاد امضایی که دارای اثر حقوقی است به‌کار رود هر امضاکننده بایستی:

الف) مراقبت معمول و متعارفی را جهت جلوگیری از استفاده غیرمجاز از داده مربوط به‌تولید امضا به‌عمل آورد.

1. Signatory

ب) بدون تأخیر غیرموجه با استفاده از وسایلی که مرجع گواهی در اختیار گذاشته است بر طبق ماده ۹ این قانون، یا با به‌کار بردن طرق متعارف هر شخصی را که امضاکننده به‌طور معقول و متعارف احتمال می‌دهد به‌امضای الکترونیکی اعتماد کرده یا بر مبنای آن خدماتی ارایه می‌دهد مطلع سازد اگر:

I) امضاکننده بداند که داده‌های مربوط به‌ایجاد امضا به‌خطر افتاده (افشاشده) است؛ یا

II) اوضاع و احوالی که امضاکننده بر آن آگاه است این خطر اساسی را داشته باشد که داده مربوط به‌تولید امضا افشا شده باشد.

ج) هنگامی که برای تصدیق امضای الکترونیکی از گواهی استفاده می‌شود، امضاکننده بایستی جهت تضمین صحت و تکمیل بودن اظهارات پراهمیت مندرج در گواهی یا در ارتباط با آن که در زمان اعتبار گواهی از ناحیه وی ارایه می‌گردد دقت معقول و متعارفی داشته باشد.

۲ـ امضاکننده باید نتایج قانونی قصور در انجام تکالیف مذکور در پاراگراف نخست را بر عهده بگیرد.»

بند (الف) ماده فوق به‌مسئله حفظ محرمانگی داده‌ها می‌پردازد و در بند (ب) تقاضای ابطال گواهی تحت شرایط پیش‌بینی شده‌ای مدنظر است. بر طبق بند سوم ماده ۱۹ قانون بلژیک، امضاکننده نمی‌تواند پس از ابطال گواهی یا انقضای مدت آن، داده‌های مربوط به‌ایجاد امضا را برای امضا کردن استفاده نموده یا آنها را نزد مرجع گواهی دیگری تأیید نماید.[۱۹]

با دقت در قانون نمونه مشخص می‌گردد که بندهای (الف) و (ب) در خصوص همه امضاهای الکترونیکی قابل اعمال است، لکن بند (ج) فقط در مورد امضاهای الکترونیکی که به‌وسیله گواهی تصدیق می‌شوند، اعمال می‌گردد. مضافاً اینکه تعهد به‌اعمال دقت معقول و متعارف که در بند (الف) آمده است و به‌جلوگیری از بهره‌گیری غیرمجاز از داده تولید امضا مربوط می‌شود، یک تعهد مبنایی است که در بسیاری از قراردادها منجمله قراردادهای مربوط به‌استفاده از کارت‌های اعتباری نیز آورده می‌شود. با توجه به‌عبارت بند (ب) می‌توان گفت تکلیف آگاه‌سازی شامل مرجع گواهی و هر شخص ذینفع دیگر نیز می‌شود. مضافاً اینکه در این بند معیار قابل انعطافی تحت عنوان تلاش متعارف برای آگاه‌سازی هر شخصی که انتظار می‌رود در مواردی که امضای الکترونیکی در معرض خطر است و در عین حال به‌آن اعتماد کرده را ارایه نموده است. انجام این امر با توجه به‌امکانات عملی که از سوی مراجع در اختیار ثبت‌نام‌کننده گواهی قرار داده می‌شود تا در زمان به‌خطر افتادن امضای الکترونیکی مورد بهره‌برداری قرار گیرد، امکان‌پذیر می‌گردد.

همچنین در بند مزبور صرف تردید در خصوص محرمانگی داده‌های مربوط به‌ایجاد با مطابقت آنها با واقع، کافی دانسته شده است و حصول اطمینان ضرورتی ندارد. در بند (ج) که گواهی برای تأیید داده ایجاد امضا به‌کار می‌رود و بایستی اطلاعات ارایه شده از سوی متقاضی در خصوص اثبات هویت و سایر مشخصات ضروری وی، دقیق و کامل بوده تا از به‌خطر افتادن امنیت ارتباطات مبنی بر گواهی صادر شده جلوگیری به‌عمل آید. چرخه حیات گواهی نیز از زمان درخواست صدور گواهی تا انقضای مدت گواهی یا رجوع از آن را شامل می‌شود.

تکالیف امضاکننده به‌نحو دیگری نیز احصا شده است که به‌شرح زیر می‌باشد:

الف) نبایستی از گواهی برای هدفی غیر از آن چیزی که در سیاست‌های مرجع گواهی آمده است، استفاده نماید؛

ب) بایستی کلید خصوصی را همواره ایمن نگه دارد و در صورت تردید در تطابق کلیدها یا افشای کلید خصوصی بلافاصله تقاضای رجوع از گواهی را ارایه نماید.

ج) بایستی عنداللزوم، مرجع گواهی یا مرجع ثبت را برای تغییر اطلاعات یا لغو ثبت‌نام در جریان قرار دهد.[۲۰]

چنانکه دیدیم پاراگراف دوم از ماده ۸ قانون نمونه آنسیترال، نتایج قانونی قصور در تحقق مقررات را متوجه امضاکننده کرده و ارزیابی میزان مسئولیت وی را به‌قانون داخلی کشورها سپرده است. در حالی که بهتر بود تقصیر ثبت‌نام‌کننده (امضاکننده) در راستای ایمن نمودن PKI و روابط کاربران و استفاده‌کنندگان از خدمات الکترونیکی و الزام به‌اتخاذ تمامی تدابیر لازمه، مفروض در نظر گرفته می‌شد و وی مسئول جبران کلیه خسارات وارده به‌اشخاص استفاده‌کننده محسوب می‌گردید.

۲ ـ ۴ ـ ۲ طرف اعتمادکننده[1]

براساس بند (f) ماده ۲ قانون نمونه آنسیترال در زمینه امضاهای الکترونیکی طرف اعتمادکننده «شخصی است که ممکن است بر مبنای گواهی یا امضای الکترونیکی اقدام نماید». طرف اعتمادکننده از اطلاعات موجود در گواهی یک ثبت‌نام‌کننده استفاده نموده و با توجه به‌هویت ثبت‌نام‌کننده و کلید عمومی وی، کلید عمومی فهرست شده را با اطلاعات شخص مقایسه و بدین‌ترتیب از هویت فرستنده پیغام، صحت و تمامیت و محرمانه بودن آن اطمینان حاصل می‌کند.[۲۱] طرف اعتمادکننده در بند (د) ماده (۱) آیین‌نامه اجرایی ماده (۳) قانون تجارت الکترونیکی چنین تعریف شده است: «شخصی که به‌اعتبار اطلاعات گواهی الکترونیکی اعتماد می‌کند».

براساس ماده ۱۱ قانون نمونه آنسیترال در زمینه امضاهای الکترونیکی طرف اعتمادکننده مکلف است:

«الف) اقدامات معقول و متعارفی را جهت تشخیص قابل اعتماد بودن امضای الکترونیکی انجام دهد، یا

ب) در جایی که یک گواهی در تأیید امضای الکترونیکی صادر شده، اقدامات معقول و متعارفی جهت رعایت امور ذیل صورت دهد:

۱ـ بررسی اعتبار، تعلیق یا لغو گواهی

۲ـ بررسی محدودیت‌های برقرار شده برای گواهی

عواقب قانونی قصور در انجام تکالیف مذکور بر عهده طرف اعتمادکننده می‌باشد.»

طرف اعتماد کننده می‌تواند هر شخصی باشد اعم از اینکه با امضاکننده رابطه قراردادی داشته باشد یا با اشخاص دیگری به‌غیر از او. در حقیقت امضاکننده یا شخصی که خدمات گواهی را ارایه می‌کند نیز امکان دارد طرف اعتمادکننده باشند.

امضاکننده با توجه به‌کلید خصوصی و عمومی ایجاد شده و ارایه‌دهنده خدمات گواهی در حالتی که از مراجع دیگر گواهی دریافت نموده، امکان دارد که طرف اعتمادکننده محسوب گردند. ولی در هیچ صورتی تکلیف طرف

1. Relying Party

اعتمادکننده مبنی بر بررسی اعتبار گواهی، به‌عهده امضاکننده (ثبت‌نام‌کننده) نخواهد بود.[۲۲] طرف اعتمادکننده بایستی با توجه به‌اوضاع و احوال متعارف و معقول به‌یک امضا یا گواهی استناد نماید. اگر وی فقط یک مصرف‌کننده باشد قواعد حمایت از مصرف‌کنندگان شامل وی خواهد شد، قواعدی که در شکل‌گیری استانداردهای رفتار متعارف که در گسترش PKI لازم است، دخالت دارد.[۲۳]

۳ـ عملکرد تکنیکی زیرساخت کلید عمومی

عملکرد تکنیکی زیر ساخت کلید عمومی، شامل بررسی نحوه شکل‌گیری امضای الکترونیکی قابل اطمینان و محرمانگی پیغام می‌شود. در این مبحث ابتدا چگونگی تولید امضای دیجیتال و سپس محرمانه ساختن پیغام را خواهیم دید.

۳ ـ ۱ امضای دیجیتال

امضای دیجیتال یک نوع امضای الکترونیکی است که از رمزنگاری کلید عمومی استفاده می‌کند.[۲۴] امضای دیجیتال که مفهومی اخص از امضای الکترونیکی دارد، اغلب همراه با طرح‌ها و شماهای امضا[۱] به‌کار می‌رود.[۲۵] امضا بدون رمزنگاری فاقد اعتبار است.

در امضای دیجیتال با استفاده از رمزنگاری کلید عمومی از دو کلید عمومی و خصوصی برای ایجاد و تأیید امضا بهره‌برداری می‌شود. کلید خصوصی که فقط امضاکننده از آن مطلع است و از آن برای ایجاد امضای دیجیتال استفاده می‌کند و کلید عمومی که افراد بیشتری به‌آن دسترسی دارند و جهت تشخیص اصالت امضای دیجیتال مورد استفاده قرار می‌گیرد.[۲۶] علاوه بر تولید جفت کلید، فرآیند دیگری نیز که خردسازی یا چکیده کردن پیغام[۲] نامیده می‌شود در جریان ایجاد و تصدیق امضای دیجیتال به‌کار می‌رود.

خردسازی یک فرآیند ریاضی است که براساس یک الگوریتم، نمایشی دیجیتالی از پیغام ایجاد کرده یا شکلی فشرده از پیغام تولید می‌نماید که از آن به‌عنوان چکیده[۳] و یا اثر انگشت[۴] دیجیتال پیغام یاد می‌کنند، و به‌صورت یک ارزش خرد[۵] و نتیجه خرد[۶] در اندازه‌ای استاندارد ایجاد می‌شود. به‌رغم اینکه چکیده پیغام به‌طور معمول بسیار از خود پیام کوچک‌تر است، لکن نسبت به‌آن منحصر به‌فرد می‌باشد و هرگونه تغییری در پیغام نتیجه خرد متفاوتی در پی خواهد داشت. تشخیص و کشف پیغام نخستین از طریق دسترسی به‌چکیده و ارزش خرد آن با به‌کارگیری عملیات یکطرفه خردسازی[۷] غیرممکن خواهد بود.

عملیات خردسازی نرم‌افزار را قادر می‌سازد تا بر روی مقادیر کوچک‌تر و قابل پیش‌بینی‌تری از داده‌ها عمل

1. Signature Schemes
2. Hash Function
3. Message Digest
4. Finger Print (Digital f.)
5. Hash Result
6. Hash Value
7. one way Hash Function

کند، در عین حال ارتباط محکمی با محتوای پیغام اصلی نیز محفوظ باقی می‌ماند. از این طریق به‌نحو مطلوبی این تضمین فراهم می‌شود که از زمانی که پیغام، امضای دیجیتالی شده هیچ تغییر و اصلاحی در آن صورت نگرفته است.[۲۷]

از آنچه تاکنون گفته شده می‌توان نتیجه گرفت که استفاده از امضای دیجیتال شامل دو فرآیند زیر است:

۱ـ ایجاد امضای دیجیتال

برای امضای پیغام، امضاکننده آن قسمت از اطلاعات را که باید امضا شود دقیقاً مشخص می‌کند، سپس نرم‌افزار وی ضمن انجام عملیات خردسازی، یک چکیده پیغام منحصر به‌فرد تولید می‌کند. آنگاه نرم‌افزار امضاکننده، چکیده پیغام را با استفاده از کلید خصوصی به‌یک امضای دیجیتال تبدیل می‌کند. امضای مزبور هم نسبت به‌پیغام امضا شده و هم نسبت به‌کلید خصوصی استفاده شده برای ایجاد امضا منحصر به‌فرد است. معمولاً امضای دیجیتال ضمن الحاق به‌پیغام حسب مورد ذخیره شده یا همراه با آن منتقل می‌شود، مشروط بر آنکه امضای دیجیتال با پیغام مربوطه ارتباط قابل اعتمادی داشته باشد، ممکن است به‌عنوان یک داده جداگانه ذخیره یا ارسال شود.[۲۸]

۲ـ بررسی اصالت امضای دیجیتال و تمامیت پیغام

فرآیند چک کردن امضا از طریق مراجعه به‌پیغام اصلی و یک کلید عمومی مشخص است که از طریق آن معلوم می‌گردد امضای دیجیتال برای همان پیغام مشخص و با استفاده از کلید خصوصی مرتبط با کلید عمومی ایجاد شده یا خیر. به‌عبارت دیگر، بررسی امضای دیجیتال با مراجعه به‌پیغام اصلی و کلید عمومی امضاکننده که در اختیار دریافت‌کننده پیغام قرار گرفته است، انجام می‌شود و به‌وسیله آن تعیین می‌شود که آیا امضای دیجیتال با استفاده از کلید خصوصی که با کلید عمومی مرتبط و مکمل آنست برای همان پیغام ایجاد شده است یا خیر.

برای بررسی این موضوع پیغام ارسالی از امضای دیجیتال جدا می‌گردد، سپس امضای دیجیتال با بهره‌گیری از کلید عمومی ارسال‌کننده رمزگشایی شده و با استفاده از همان الگوریتمی که فرستنده استفاده کرده عمل چکیده کردن در مورد پیغام صورت می‌گیرد. این چکیده جدید با چکیده قبلی مقایسه می‌شود و اگر تغییری در پیغام انجام نشده باشد هر دو چکیده کاملاً با هم منطبق خواهند بود.[۲۹]

بنابراین کلید عمومی امضاکننده زمانی امضای دیجیتال را رمزگشایی خواهد کرد که کلید خصوصی امضاکننده برای امضای آن استفاده شده باشد، همچنین هر دو چکیده پیغام (چکیده پیام ایجاد شده به‌وسیله امضای دیجیتال رمزگشایی شده و چکیده حاصل از پیام محاسبه شده با اعمال الگوریتم خرد کردن) بایستی یکسان باشند تا هم هویت فرستنده شناسایی و اثبات شود و هم تمامیت پیام تصدیق گردد.[۳۰]

۳ ـ ۲ ـ محرمانگی پیغام

چنانکه در امضای دیجیتال دیدیم، پیغام اصلی به‌انضمام امضای دیجیتال ارسال می‌گردد. برای اینکه پیغام فقط توسط دریافت‌کننده قابل خواندن باشد ضروریست توسط نرم‌افزار ویژه‌ای رمزنگاری شده تا متصف به‌وصف

محرمانگی گردد.

برای رمزنگاری و مآلاً حصول محرمانگی، از یک الگوریتم تک‌کلیدی استفاده شده تا پیغام ساده با استفاده از الگوریتم متقارن و یک کلید رمزنگاری شده و آن را به‌شکل ناخوانا تبدیل و سپس ارسال نماید. گیرنده از یک کلید دیگر استفاده می‌کند تا متن رمزنگاری شده را به‌متن ساده تبدیل نماید. در زیرساخت کلید عمومی جهت رمزنگاری و محرمانه کردن، به‌لحاظ مشکلات موجود در سیستم رمزنگاری متقارن (ایراد انتقال کلید) و رمزنگاری نامتقارن (ایراد کندی سرعت محاسباتی)، ترکیبی از هر دو نوع رمزنگاری استفاده می‌شود. بدین‌منظور ارسال‌کننده با استفاده از یک کلید متقارن، پیغام را رمزنگاری نموده البته کلید مزبور با استفاده از کلید عمومی دریافت‌کننده رمزنگاری شده، سپس پیغام رمزنگاری شده و کلید متقارن برای دریافت‌کننده فرستاده می‌شود. وی با استفاده از کلید خصوصی خود کلید متقارن را رمزگشایی نموده و در انتها با استفاده از کلید متقارن که ارسال‌کننده به‌وسیله آن پیغام را رمزنگاری کرده، پیغام را رمزگشایی می‌نماید.[۳۱]

برای این که پیغام به‌شکل محرمانه امضا شود باید ابتدا با استفاده از یک کلید متقارن رمزنگاری شود که خود این کلید متقارن نیز با بهره‌گیری از کلید عمومی دریافت‌کننده رمزنگاری می‌گردد. سپس کلید متقارن رمزنگاری شده با پیغام رمزنگاری شده و امضای دیجیتال به‌وسیله کلید متقارن تلفیق می‌شود و برای دریافت‌کننده ارسال می‌گردد. وی امضای دیجیتال، کلید متقارن رمزنگاری شده به‌وسیله کلید عمومی خود و پیغام رمزنگاری شده به‌وسیله کلید متقارن را جدا نموده و کلید متقارن را با استفاده از کلید خصوصی خود رمزگشایی کرده آنگاه پیغام را با استفاده از کلید متقارن مذکور رمزگشایی می‌نماید. در پایان با استفاده از عمل خردسازی، چکیده پیغام تولید شده با چکیده پیغام ناشی از امضای دیجیتالی که با اعمال کلید عمومی ارسال کننده بر آن به‌دست آمده، مقایسه می‌گردد تا تمامیت پیغام و هویت فرستنده نیز اثبات گردد.[۳۲]

نتیجه‌گیری

با تصویب آیین‌نامه اجرایی ماده (۳۲) قانون تجارت‌الکترونیکی، خلأ قانونی موجود برطرف شده و بسیاری از ابهامات در حیطه صلاحیت‌ها و وظایف مراجع ارایه خدمات صدور گواهی الکترونیکی پاسخ داده شده و در نتیجه زیرساخت کلید عمومی به‌عنوان مجموعه‌ای از نرم‌افزارها، سخت‌افزارها، سیاست‌ها، فرآیندها و روال‌های مورد نیاز برای مدیریت گواهی‌ها و زوج کلیدها پایه‌گذاری و شورایی به‌نام شورای سیاست‌گذاری گواهی الکترونیکی مسئولیت حفظ یکپارچگی و سیاست‌گذاری در حوزه زیرساخت کلید عمومی کشور را عهده‌دار گردید. با تشکیل مرکز دولتی صدور گواهی الکترونیکی ریشه، مراکز صدور گواهی الکترونیکی میانی که با کسب مجوز از یک مرکز ریشه، می‌توانند به‌صدور گواهی الکترونیکی مبادرت نموده و سایر خدمات مربوط به‌امضای الکترونیکی را انجام دهند، فعالیت خود را آغاز می‌نمایند. ثبت و انتقال درخواست متقاضیان درخصوص صدور و لغو گواهی‌ها و سایر امور مربوط به‌آنها مطابق با ضوابط و دستورالعمل صادره از سوی مراجع میانی که تعهد همکاری با آنها را امضا نموده است، در دفتر ثبت‌نام گواهی الکترونیکی صورت می‌پذیرد دفاتر ثبت‌نام می‌توانند بنا به‌مورد توسط اشخاص حقیقی

یا حقوقی اعم از دولتی یا غیردولتی ایجاد شوند. با وجود اینکه کلیه مؤسسات اعم از دولتی یا غیردولتی می‌توانند در حوزه فعالیت داخلی خود بدون اخذ مجوز از مرکز ریشه مبادرت به‌ثبت و صدور گواهی نمایند، لکن باید توجه داشت که گواهی‌هایی که به‌این صورت صادر می‌شود خارج از شمول مقررات آیین‌نامه اجرایی بوده و امضاهایی که به‌وسیله این گواهی‌ها تأیید می‌شوند، خارج از موضوع ماده (۱۰) قانون تجارت الکترونیکی و صرفاً قابل استفاده در همان مؤسسات خواهد بود. پذیرش گواهی الکترونیکی صادره از مراجع صدور گواهی خارجی با رعایت اصل شرط عمل متقابل و تصویب شورا، مشروط به‌توافق دوجانبه بین مرکز ریشه کشور و مرجع صدورگواهی کشور خارجی امکان‌پذیر می‌باشد.

پی‌نوشت‌ها:

1- Kuhn, Dr. Richard & et al. introduction to public key infrastructure and the federal PKI, p.3 ,**www.pki.com [2004/04/04]**.

2- Pluswick. Leo, PKI Technical Concepts and Backgrounds, p.7 **www.icsalbas.com/html/communities/pki/pki-fag.pdf [2005/09/23].**

3- Uncitral Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, 1996, p. 4, **www.uncitral.org/english/texts/electcom/ml-ecomm.htm [2007/01/08].**

4- Luker, Mark, what is a public-key Infrastructure or PKI? p.2 **www.educause.edu.ir/library/pdf/DEC0103.pdf [2006/11/29].**

5- Gobert, Didier&Montero, Etienne, cadre juridique pour les signatures electroniques et les services de certification: analyse de loi du 9 juillet 2001, **p. 19, www.droitfundp.ac.be [2006/01/08].**

6- **Ibid**, p. 22.

7- Untitled author, Digital signature guidelines, tutorial, p. 2, **www.abanet.org/scitech/ec/isc/dsg-tutorial.html [2005/05/07].**

8- Gobert. Didier&Montero. Etienne, loverture de la preuve litterale aux ecrit sous forme electronique, pp 23-45, **www.droitfundp.ac.be [2005/02/10].**

9- **Ibid**, p. 3.

10- Uncitral Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, 1996, p. 5, **www.uncitral.org/english/texts/electcom/ml-ecomm.htm [2007/01/08].**

11- Electronic Signature Directive. European Union. December 1999, p. 2, http://eur-lex.europa.eu/**LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML [2007/02/09].**

12- Untitled author, Local registration authority, p.7, **www.fundserv.com [2006/12/11].**

13- Untiled author, Understanding public key infrastructure, p. 4, **www.directoreservice. [2006/11/18].**

14- Brazel, Lorna , 2003, **Electronic signatures legislation and practice,** sweet&Maxwell, pp.32-39.

15- Chissick, Michael and Kelman, Alistair, 2000, **Electronic commerce law and material, sweet&Maxwell, p.183.**

16- **Ibid**, p. 5.

17- Electronic Signature Directive, European Union, December 1999, p. 3, **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML[2007/02/09].**

18- Uncitral Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, 1996, p. 6, **www.uncitral.org/english/texts/electcom/ml-ecomm.htm [2007/01/08].**

19- Gobert, Didier&Montero, Etienne, loverture de la preuve litterale aux ecrit sous forme electronique, pp. 41-44, **www.droitfundp.ac.be [2005/02/10].**

20- Untitled author, Proposal for Liability of Certification Authority, Authentication and Notary Working Group, Electronic Commerce Promotion Council of Japan (ECOM), May 2000, p. 10, **www.ecom.jp/ecom-e/report/fall/proposalfor.pdf [2006/10/06].**

21- Pluswick, Leo, PKI Technical Concepts and Backgrounds, p. 8 **www.icsalbas.com/html/communities/pki/pki-fag.pdf [2005/09/23].**

22- Uncitral Model Law on Electronic Commerce with Guide to Enactment 1996. United Nations, 1996, p. 10, **www.uncitral.org/english/texts/electcnm/ml-ecomm.htm [2007/01/08].**

23- **Ibid**, p. 11.

24- Bloemers, Ralph O. Electronic and Digital Signatures, p.22 **www.stoel.com/resources/articles/ebusiness/ebi,2003.shtm [2006/02/08].**

25- Buldas, Ahto & Saarepera, Märt. Electronic Signatures System with Small Number of Private Keys, p. 8, **www.middleware.internet2.edu/pki03/presentations/08.pdf [2003/01/18].**

26- Uncitral Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, 1996, p. 12, **www.uncitral.org/english/texts/electcom/ml-ecomm.htm [2007/01/08].**

27- **Ibid**, p. 13.

28- Untitled author. Introduction to PKI-Public Key Infrastructure, European Master in Multimedia Projects, p. 3. **www.k-binder.be/papers/PKI-V11.pdf [2004/02/13].**

29- Buldas, Ahto & Saarepera, Märt, Electronic Signatures System with Small Number of Private Keys. p. 9, **www.middleware.internet2.edu/pki03/presentations/08.pdf [2003/01/18].**

30- Uncitral Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, 1996, p. 15, **www.uncitral.org/eoglish/texts/electcom/ml-ecomm.htm [2007/01/08].**

31- Untitled author. Introduction to Public Key Infrastructure, p. 4. **www.articsoft.com/wp-pki-intro.htm [2006/01/24].**

32- Untitled author, Introduction to PKI-Public Key Infrastructure. European Master in Multimedia Projects, p. 6, **www.k-binder.be/papers/PKI-V11.pdf [2004/02/13].**