ماهیت و جایگاه مرکز گواهی ریشه در تراکنش‌های الکترونیکی

مصطفی بختیاروند*

تاریخ دریـافت ۸۶/۲/۴	تاریخ پذیرش ۸۶/۷/۱۴

درحالی‌که در بسیاری از کشورهای جهان شرایط استفاده از امضای دیجیتال فراهم شده، بحث‌ها درباره ارگان اداره‌کننده یعنی مرکز گواهی ریشه (یکی از عناصر مهم زیرساخت کلید عمومی)، در کشور ما هنوز به پایان نرسیده است. چنین مرکزی در رأس مجموعه‌های سلسله‌مراتبی قرار گرفته و مراجع فرعی را تصدیق می‌کند. شناخت ماهیت و نقش این مرکز در ایجاد اعتماد نسبت به تراکنش‌های الکترونیکی، قضاوت آگاهانه درباره نهاد اداره‌کننده آن را ممکن می‌سازد.

کلیدواژه‌ها: امضای دیجیتال؛ مراجع گواهی؛ زیرساخت کلید عمومی؛ مرکز ریشه

---

* عضو هیئت علمی دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران.
E-mail:mbakhtiarvand@gmail.com

مقدمه

شاید باور اینکه در آینده‌ای نه‌چندان دور، شبکه‌های رایانه‌ای و در رأس آنها اینترنت به تمام بخش‌های جامعه رخنه کرده و بیشتر امور شهروندان به‌صورت الکترونیکی انجام پذیرد؛ در کشور ما و در این مقطع زمانی بسیار دشوار و بیشتر به رؤیا شبیه باشد.

اما روند مجازی شدن کارها و محو شدن کاغذ و دیدارهای فیزیکی در ایران نیز شروع شده و خواه‌ناخواه با سرعت شگفت‌انگیزی ادامه خواهد یافت. چرا که ایران نیز به‌عنوان جزئی از جامعه جهانی، برای تعامل با دیگر کشورها به استفاده از فناوری‌های نوین نیازمند است. همچنین مزایای این فناوری‌ها در سطح داخلی به‌قدری چشمگیر است که خودبه‌خود و به‌طور گسترده به زندگی مردم وارد شده و به‌طور گسترده مورد استفاده قرار می‌گیرد.

با فراگیر شدن اینترنت، تراکنش‌های بسیاری به‌وسیله این رسانه انجام خواهد شد که از معاملات مهم تجاری و پرداخت‌های الکترونیکی، ارسال مدارک لازم برای ثبت‌نام در دانشگاه‌ها، درخواست استخدام در یک شرکت، تعامل ارگان‌های دولتی، تا تبادل نامه‌های خصوصی در نوسان خواهند بود.

علاوه بر منافع تراکنش‌های الکترونیکی، مشکلات آنها را نیز نباید فراموش کرد. یکی از مهم‌ترین این مشکلات مسئله امنیت این نوع ارتباطات است. هنگامی اعضای جامعه به استفاده از شبکه‌های رایانه‌ای روی خواهند آورد که نسبت به ایمنی روابط خود با این شبکه‌ها اطمینان داشته باشند.

بنابراین نمی‌توان از سویی مردم را به انجام تراکنش‌های الکترونیکی تشویق کرد و ازسوی دیگر، بدون ایجاد زیرساخت‌های ضروری، آنها را در محیط ناامنی رها کرده و به دست حیله‌گران و کلاهبرداران سودجو سپرد.

کشورهایی که شبکه‌های الکترونیکی را به‌طور فزاینده به‌کار می‌گیرند؛ به امنیت آنها نیز توجه دارند؛ چرا که به‌خوبی به نقاط ضعف این شبکه‌ها آگاهند.

از جمله راهکارهای امنیتی درباره پیغام‌های الکترونیکی، استفاده از مکانیسم‌هایی معروف

به امضاهای الکترونیکی است. این امضاها انواع مختلفی دارند که هریک سطح معینی از ایمنی را فراهم می‌سازد. ازاین‌رو در قوانین راجع به فضای سایبر، آثار حقوقی متفاوتی برای امضاهای الکترونیکی در نظر گرفته شده است. هم‌اکنون ایمن‌ترین نوع امضای الکترونیکی، امضای دیجیتال است که در آن از فناوری رمزنگاری کلید عمومی استفاده می‌شود.

به‌کارگیری امضای دیجیتال، مستلزم بهره‌گیری از خدمات اشخاص ثالث موثقی است که به مراجع گواهی معروفند و به‌نوعی تعلق امضا را به شخص معینی تصدیق می‌کنند. نحوه تعامل این مراجع بسیار اهمیت دارد و الگوهای مختلفی برای آن شکل گرفته است. یکی از این الگوها، شیوه سلسله‌مراتبی است که در آن یک مرجع گواهی به نام مرجع (مرکز) ریشه در رأس مجموعه قرار گرفته و مراجع دیگر را تصدیق می‌کند.

مسئله مهم درباره زیرساخت سلسله‌مراتبی، تعیین نهادی است که وظیفه اداره مرکز ریشه را برعهده دارد. در سال‌های اخیر در کشور ما بحث‌های متعددی دراین‌باره انجام گرفته و اختلافات فراوانی به وجود آمده است.

این گزارش با هدف تبیین ماهیت مرکز گواهی ریشه و کارکرد آن و تلاش برای رفع مشکلات موجود دراین‌باره تهیه شده است.

۱ امضای الکترونیکی و آثار حقوقی آن

۱-۱ امضای الکترونیکی

همان‌گونه که در مقدمه بیان شد؛ فضای ارتباطات الکترونیکی، به دلیل مجازی بودن، به راهکارهایی برای تأمین امنیت نیازمند است. هنگام دریافت پیغام از اینترنت، گیرنده باید بتواند پدیدآورنده آن را شناخته و نسبت به اصالت محتوای پیغام اطمینان یابد. ازاین‌رو مکانیسم‌هایی شکل گرفته است که به‌طورکلی، امضای الکترونیکی[1] نامیده می‌شوند. در ذیل به برخی از تعاریف ارائه شده از امضای الکترونیکی اشاره می‌کنیم:

1.Electronic Signature

۱-۱-۱ قانون نمونه امضاهای الکترونیکی آنسیترال

کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد،[1] امضای الکترونیکی را به این صورت تعریف کرده است: «داده‌های الکترونیکی که به یک داده پیام منضم شده یا به‌صورت منطقی با آن مرتبطند و از آنها می‌توان جهت شناسایی امضاکننده داده پیام و دلالت بر تأیید اطلاعات موجود در داده پیام ازسوی وی استفاده نمود».

۱-۱-۲ تعریف دستورالعمل امضاهای الکترونیکی پارلمان اروپا

«داده‌های الکترونیکی که به دیگر داده‌های الکترونیکی منضم شده یا به‌صورت منطقی با آنها مرتبطند و به‌عنوان وسیله‌ای برای مستندسازی به‌کار می‌روند».

۱-۱-۳ قانون تجارت الکترونیکی جمهوری اسلامی ایران

در ایران امضای الکترونیکی این‌گونه تعریف می‌شود: «امضای الکترونیکی عبارت است از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده پیام، که برای شناسایی امضاکننده به‌کار می‌رود».

به‌این‌ترتیب امضای الکترونیکی عنوانی است کلی که می‌تواند مصادیق مختلفی داشته باشد. مواردی از امضای الکترونیکی عبارتند از: امضای دیجیتال، امضاهای مبتنی بر معرف‌های زیست‌شناختی[2] (مانند اسکن شبکیه چشم)،[3] تصویر رقمی شده امضای دستی[4] ــ که به پیغام الکترونیکی منضم شده ــ یا فقط اسم تایپ شده در انتهای نامه الکترونیکی.

در نتیجه باید توجه کرد که امضای دیجیتال، فقط یکی از انواع امضای الکترونیکی است و این دو اصطلاح گاه به اشتباه به‌جای یکدیگر به‌کار می‌روند که نباید آنها را باهم خلط کرد.

همچنین با دقت در این تعاریف درمی‌یابیم که قانون‌گذاران به دلیل توجه به تنوع

---

1. United Nations Commission on International Trade Law (UNCITRAL)
2. Biometrics
3. Retinal Scan
4. Digitized Handwritten Signature

روش‌های تولید امضای الکترونیکی و پیشرفت‌های سریع دراین‌باره آنها را به‌گونه‌ای تنظیم کرده‌اند که تمام انواع امضای الکترونیکی را دربرگیرد. بااین‌حال، در قوانین مختلف، معمولاً پس از ارائه تعریفی کلی از امضای الکترونیکی و شناختن اثر قانونی آن، نوع خاصی از این امضا، با عنوان امضای الکترونیکی پیشرفته،[1] ایمن[2] یا مطمئن (قانون تجارت الکترونیکی ایران) بیان شده و امتیازات ویژه‌ای برای آن در نظر گرفته می‌شود. علت پذیرش آثار قانونی خاص برای این نوع امضای الکترونیکی، آگاهی از این نکته است که همه امضاهای الکترونیکی ازنظر حقوقی، سطح یکسانی از امنیت را فراهم نمی‌کنند. برای مثال با آنکه تایپ کردن اسم نویسنده در پایان‌نامه الکترونیکی جزء تعریف عام امضای الکترونیکی به‌حساب می‌آید؛ اما هیچ‌گونه تضمینی نسبت به اصالت هویت اعلام شده ایجاد نمی‌کند.

در ماده (۲-۲) دستورالعمل امضاهای الکترونیکی اتحادیه اروپا

امضای الکترونیکی پیشرفته به‌صورت زیر تعریف شده است:

امضای الکترونیکی پیشرفته امضایی است که از شرایط ذیل برخوردار باشد:

۱. به‌صورت انحصاری با امضاکننده مرتبط باشد.

۲. شناسایی امضاکننده را ممکن سازد.

۳. با به‌کارگیری ابزاری ایجاد شده باشد که امضاکننده بتواند آنها را به‌طور انحصاری تحت کنترل خود درآورد.

۴. با داده‌های مربوط به خود به‌گونه‌ای در ارتباط بوده که هرگونه تغییر بعدی در آنها قابل کشف باشد.

ماده (۱-۵) این دستورالعمل مقرر می‌دارد که تحت شرایط معینی ازجمله پیشرفته بودن به مفهوم ماده (۲-۲)، امضای الکترونیکی به‌عنوان دلیل در دادگاه پذیرفته شده و از همان قدرت اثباتی امضای سنتی برخوردار خواهد بود.

---

1. Advanced Electronic Signature
2. Secure Electronic Signature

قانون تجارت الکترونیکی ایران در ماده (۱۰)، شرایط زیر را برای آنچه امضای الکترونیکی مطمئن نامیده می‌شود؛ ضروری دانسته است:

۱. نسبت به امضاکننده منحصربه‌فرد باشد.

۲. هویت امضاکننده داده پیام را معلوم نماید.

۳. به‌وسیله امضاکننده و یا تحت اراده انحصاری وی صادر شده باشد.

۴. به‌نحوی به یک داده پیام متصل شود که هر تغییری در آن داده پیام قابل کشف باشد.

ماده (۱۵) این قانون، برای امضای الکترونیکی مطمئن، اثری مانند اسناد رسمی قائل شده و نسبت به چنین امضایی، ادعای انکار یا تردید را نپذیرفته است و اثبات جعلی بودن آن را ضروری می‌داند.

باوجود اینکه در تعاریف ارائه شده از امضای الکترونیکی پیشرفته یا مطمئن، فقط مجموعه‌ای از خصایص (بدون توجه به فناوری به‌کار رفته) بیان شده است، هم‌اکنون فقط امضای دیجیتال این ویژگی‌ها را داراست. به این دلیل دست‌اندرکاران فناوری اطلاعات و ارتباطات در کشورهای مختلف به این نوع امضا توجه ویژه‌ای داشته و سعی کرده‌اند شرایط لازم را برای استفاده از آن فراهم سازند. به‌طوری‌که در برخی از کشورها قوانینی با عنوان قانون امضای دیجیتال به تصویب رسیده که از جمله می‌توان به قانون امضای دیجیتال ایالت یوتا در آمریکا اشاره کرد که اولین قانون دراین‌باره به‌شمار می‌رود.

باتوجه به اهمیت امضای دیجیتال و نقش حیاتی آن در برقراری امنیت در تراکنش‌های الکترونیکی، در ذیل مطالبی دراین‌باره ارائه می‌شود:

۲-۱ امضای دیجیتال[1]

ایجاد و بررسی اصالت امضای دیجیتال با استفاده از رمزنگاری[2] انجام می‌گیرد. رمزنگاری شاخه‌ای از ریاضیات کاربردی است که موضوع آن تبدیل پیغام‌ها به شکلی است که در حالت

1. Digital Signature
2. Cryptograohy

عادی قابل فهم و خواندن نباشد. در برابر این عملیات، عمل قابل فهم کردن پیغام رمزنگاری شده وجود دارد که آن نیز با استفاده از شاخه ریاضیات کاربردی امکان‌پذیر است. رمزنگاری مبتنی بر کلید عمومی، روشی است که در رابطه با امضای دیجیتال به‌کار می‌رود.

۱-۲-۱ رمزنگاری کلید عمومی[1]

برای رمزنگاری و رمزگشایی در این سیستم، از دو کلید[2] متفاوت استفاده می‌شود. به این دلیل به آن رمزنگاری نامتقارن[3] نیز می‌گویند. منظور از کلید، عددهای بسیار بزرگی است که در نتیجه اعمال مجموعه‌ای از فرمول‌های ریاضی بر اعداد اول تولید می‌شوند. باوجود این تفاوت این دو کلید ازنظر ریاضی با هم مرتبطند. متن رمزنگاری شده با یکی از این دو کلید، فقط با استفاده از کلید دیگر قابل رمزگشایی است. از این دو کلید، یکی برای ایجاد امضای دیجیتال به‌کار می‌رود و فقط امضاکننده یا نماینده وی از آن مطلع است که به آن کلید خصوصی[4] نیز می‌گویند؛ اما کلید دیگر که به‌منظور شناسایی و بررسی اصالت امضای دیجیتال مورد استفاده قرار می‌گیرد و افراد بیشتری از آن آگاهند؛ کلید عمومی نامیده می‌شود.

۱-۲-۲ ایجاد امضای دیجیتال

برای امضای دیجیتالی یک متن، امضاکننده آن قسمت از اطلاعات را که باید امضا شود، دقیقاً مشخص کرده و سپس با استفاده از نرم‌افزار مخصوصی، شکل فشرده‌ای از پیغام را تولید می‌کند. این شکل فشرده بیشتر با عنوان «چکیده پیغام»،[5] «اثر انگشت دیجیتال»، «ارزش خرد»[6] و یا «نتیجه خرد» پیغام نامیده می‌شود و همان‌گونه که از نام آن برمی‌آید معمولاً از پیغام بسیار کوچک‌تر است. عملیات انجام شده با این نرم‌افزار، به عملیات «خردسازی»[7] موسوم است که

---

1. Public Key Cryptography
2. Key
3. Assymetric cryptography
4. Private key
5. Message Digest
6. Hash Value
7. Hash Function

باعث می‌شود امضاکننده با داده کمتری مواجه باشد. نتیجه «خردسازی» نسبت به متن اصلی، منحصربه‌فرد بوده؛ به‌طوری‌که وقوع هرگونه تغییری در پیغام، در صورت به‌کارگیری همان نرم‌افزار، ناگزیر، نتیجه خرد متفاوتی در پی خواهد داشت. هرگاه یک عملیات خردسازی ایمن ــ که در اصطلاح عملیات «یکطرفه خردسازی»[1] نامیده می‌شود ــ به‌کار رود؛ تشخیص و کشف پیغام اولیه با علم به ارزش خرد آن غیرممکن خواهد بود. در نتیجه، عملیات خردسازی، نرم‌افزار ایجادکننده امضای دیجیتال را قادر می‌سازد که با کلید خصوصی، مقادیر کوچک‌تری از داده‌ها را رمزنگاری کند و همچنین دلیل محکمی مبنی‌بر ارتباط متقابل میان پیغام اصلی و چکیده آن فراهم آورده و بتواند، به نحو مطلوبی تضمین کند که از زمان امضا شدن به‌صورت دیجیتال، هیچ‌گونه تغییری در پیغام حاصل نشده است.

بنابراین آنچه امضا (رمزنگاری) می‌شود، درحقیقت شکل خرد شده پیغام است و امضاکننده، متن اصلی و امضای دیجیتال خود (نتیجه خرد رمزنگاری شده) را برای مخاطب ارسال می‌کند.

۳-۲-۱ بررسی اصالت امضای دیجیتال

بررسی اصالت امضا برعهده گیرنده پیغام است. وی پس از دریافت پیغام و شکل خرد آن، کلید عمومی امضاکننده را ــ که باید به طریقی به آن دسترسی داشته باشد ــ برای رمزگشایی شکل خرد پیغام به‌کار می‌برد. درصورت موفق بودن عملیات رمزگشایی، گیرنده در می‌یابد که این پیغام به‌وسیله کسی امضا شده که کلید خصوصی مرتبط با کلید عمومی در دسترس وی را در اختیار دارد.

گام بعدی بررسی تغییر یا عدم تغییر محتوای پیغام است. به‌این‌ترتیب گیرنده عملیات خردسازی را درباره پیغام اصلی، انجام می‌دهد (همانند عملیاتی که فرستنده انجام داده است)؛ اگر نتیجه به‌دست آمده با شکل خرد ارسالی فرستنده یکسان باشد؛ گیرنده از

1. One Way Hash Function

اصالت پیغام و عدم تغییر محتوای آن مطمئن می‌شود.

با توجه به مطالب ارائه شده درباره امضای دیجیتال، مشخص می‌شود که این امضا حتی از امضاهای دستی نیز قوی‌تر است؛ چرا که حفظ تمامیت و عدم تغییر پیغام را نیز در جریان مبادله تضمین می‌کند. ازاین‌رو قانون‌گذاران، از جمله قانون‌گذار جمهوری اسلامی ایران، قدرت اثباتی ویژه‌ای را برای آن در نظر گرفته‌اند.

اما همان‌گونه که گفته شد، گیرنده پیغام الکترونیکی امضا شده با استفاده از کلید خصوصی فرستنده، باید کلید عمومی فرستنده را نیز در اختیار داشته باشد. این امر با بهره‌گیری از خدمات اشخاصی به نام «مراجع گواهی» محقق می‌شود.

۲ مراجع گواهی[1]

جفت کلید عمومی و خصوصی، فقط دو عدد است. این اعداد هیچ ارتباط ذاتی با شخص معینی ندارند. بنابراین به‌منظور ارتباط کلیدها به یک شخص خاص (حقیقی یا حقوقی)، باید تدابیر ایمن و مناسبی اندیشیده شود.

اگر طرفین تراکنش الکترونیکی به یکدیگر اعتماد داشته و همچنین به ابزار مطمئنی دسترسی داشته باشند، می‌توانند کلیدهای عمومی را در اختیار یکدیگر قرار دهند. برای مثال یک‌طرف، کلید عمومی خود را به‌وسیله یکی از کارمندانش به طرف مقابل تسلیم کرده یا آنکه لوح فشرده[2] حاوی کلید عمومی را به‌صورت نامه‌ای با پست پیشتاز برای وی ارسال می‌کند.

اما انجام چنین کاری در تمام موارد به این سادگی نخواهد بود. اینترنت امکان برقراری ارتباط و انجام تراکنش را میان اشخاص (بدون توجه به مکان فیزیکی که در آن قرار دارند و نیز اینکه پیش از این با یکدیگر رابطه داشته‌اند یا خیر) فراهم ساخته است. سؤال این است که در چنین اوضاعی که هر طرف ممکن است با افراد متعددی ــ که هیچ‌گونه شناختی نسبت به آنها ندارد ــ ارتباط داشته باشد؛ چگونه می‌توان تعلق یک کلید

1. Certificate Authorities (CAs)
2. Compact Disk (CD)

عمومی را به شخص معینی اثبات کرد؟

ازاین‌رو ممکن است دارنده کلید عمومی با صدور اعلامیه‌ای (برای مثال با متن ذیل) این موضوع را مشخص کند:

«امضاهایی که به‌وسیله کلید عمومی زیر قابل شناسایی باشند به اینجانب تعلق دارند».

باوجود این، دیگران حق خواهند داشت که از پذیرش چنین اظهارات تأیید نشده‌ای امتناع کنند؛ به‌ویژه در فضای مجازی اینترنت و زمانی که طرفین پیش از این با یکدیگر رابطه‌ای نداشته‌اند که اثر قانونی چنین ادعاهایی را تثبیت کند. اشخاصی که در ارتباطات مبتنی بر اینترنت به چنین اعلامیه‌های تأیید نشده‌ای اطمینان می‌کنند با خطر اعتماد به یک جاعل و یا تحمل بار اثبات تعلق کلید عمومی به طرفی که منکر آن است مواجه خواهند بود.

راه‌حل دیگر برای ارتباط کلید عمومی با یک شخص معین، استفاده از خدمات اشخاص ثالث موثق، برای معرفی طرفین به یکدیگر است. این امر موجب حذف هزینه‌های ناشی از ملاقات حضوری، ارسال نامه، اعتماد به اعلان‌های تأیید نشده و ... می‌شود. این راهکار همان استفاده از مراجع گواهی است.

به‌منظور تصدیق تعلق جفت کلید به یک شخص معین، مرجع یک گواهی (سند الکترونیکی) صادر می‌کند. در این گواهی کلید عمومی به‌عنوان موضوع گواهی مشخص و تأیید شده است که شخص معرفی شده در گواهی، کلید خصوصی مربوط به این کلید عمومی را در اختیار دارد. این شخص در اصطلاح «مشترک» نامیده می‌شود. کارکرد اصلی و عمده گواهی، تصدیق تعلق جفت کلید به یک مشترک خاص است.

درصورت صدور گواهی، مشترک می‌تواند آن را به نامه‌های الکترونیکی خود منضم و برای مخاطبان ارسال کند.

مراجع گواهی در قالب سیستمی به نام «زیرساخت کلید عمومی»، فعالیت می‌کنند.

۱-۲ زیرساخت کلید عمومی[1]

زیرساخت کلید عمومی را می‌توان مجموعه‌ای از نرم‌افزارها، سخت‌افزارها، فناوری‌های رمزنگاری و خدماتی دانست که اشخاص را قادر می‌سازد امنیت ارتباطات خود را در شبکه‌های الکترونیکی تأمین کنند.

تأسیس زیرساخت کلید عمومی راهی است تا بتوان با آن نسبت به موارد ذیل اطمینان یافت:

۱. شخصی که به‌عنوان فرستنده پیغام معرفی شده؛ به‌واقع پدیدآورنده آن است.

۲. تکنیک‌های رمزنگاری به‌کار رفته، مطلوب و فاقد هرگونه مشکلی است.

۳. تمامیت داده‌ها در جریان مبادله پیغام حفظ شده است.

و ... .

برای دستیابی به این اهداف، زیرساخت کلید عمومی ممکن است خدمات زیر را ارائه دهد:

۱. اداره کلیدهای رمزنگاری ــ که به‌منظور ایجاد و شناسایی امضای دیجیتال به‌کار رفته‌اند،

۲. اداره کلیدهای رمزنگاری، به‌منظور برقراری ارتباطات محرمانه (در مواردی که این ارتباطات مجاز است)،

۳. تصدیق مطابقت کلید عمومی با یک کلید خصوصی معین،

۴. تولید کلیدهای عمومی و خصوصی برای اشخاص،

۵. انتشار یک دفترچه راهنمای ایمن حاوی کلیدهای عمومی یا گواهی‌ها،

۶. اداره ابزار و وسایل شخصی مانند کارت‌های هوشمند ــ که می‌توانند اشخاص را با استفاده از اطلاعات شخصی منحصربه‌فرد معرفی کرده یا کلیدهای خصوصی آنها را تولید یا ذخیره کنند،

۷. کنترل هویت اشخاص و ارائه خدمات به آنها،

۸. ارائه خدمات ثبت تاریخ[2] (به‌طور معمول مدت اعتبار گواهی).

---

1. Public Key Infrastructure (PKI)
2. Time Stamp

علاوه بر مراجع گواهی، معمولاً مراکز دیگری نیز در زیرساخت کلید عمومی شکل می‌گیرند که برخی از خدمات مربوط به گواهی را انجام می‌دهند از جمله این مراکز می‌توان به مراجع ثبت اشاره کرد. مراجع ثبت به ارائه دو کارکرد می‌پردازند:

۱. جمع‌آوری اطلاعات درباره اشخاص، تأیید هویت و صحت اطلاعات ارائه شده به‌وسیله آنها؛ یعنی اطمینان یافتن از اینکه متقاضی گواهی، همان کسی است که ادعا می‌کند و اطلاعاتی از جمله اشتغال به حرفه معین که خواستار درج آنها در گواهی است؛ با واقع منطبق باشد.

۲. تشخیص و تصدیق انطباق کلیدهای عمومی و خصوصی متقاضیان با یکدیگر.

به‌این‌ترتیب مرجع ثبت مجموعه‌ای از اطلاعات را درباره متقاضیان گواهی تهیه می‌کند و مراجع گواهی می‌توانند دراین‌باره به آنها مراجعه کنند.

۲-۲ ماهیت دولتی یا خصوصی مراجع گواهی

مراجع گواهی می‌توانند دولتی یا خصوصی باشند. در برخی کشورها ممکن است این دیدگاه حاکم باشد که بنا به دلایل امنیتی یا نظم عمومی فقط ارگان‌های دولتی می‌توانند به‌عنوان مراجع گواهی اجازه فعالیت داشته باشند. اما بسیاری از دولت‌ها براین عقیده‌اند که خدمات مربوط به گواهی باید در معرض رقابت شرکت‌ها و مؤسسات خصوصی نیز قرار گیرند.

۲-۳ مراجع گواهی و دفترخانه‌های اسناد رسمی

باوجود تشابه نسبی وظیفه اصلی مراجع گواهی با یکی از کارکردهای دفترخانه‌های اسناد رسمی (تصدیق امضای افراد)، نباید تصور کرد که مراجع گواهی همان وظایف دفاتر اسناد رسمی را برعهده دارند. درحقیقت آنچه به‌وسیله مرجع گواهی تأیید می‌شود عبارت است از قرارگیری داده‌های ضروری برای ایجاد و شناسایی امضای دیجیتال (جفت کلید عمومی و خصوصی) در اختیار شخص معرفی شده. بنابراین امضای دیجیتال اشخاص به‌طور

غیرمستقیم به‌وسیله مرجع گواهی تصدیق می‌شود. درحالی‌که سردفتر به‌طور مستقیم تعلق امضایی معین را به شخص خاصی گواهی می‌کند.

همچنین مرجع گواهی، صحت تراضی طرفین و قرارداد منعقده را تأیید نکرده و برخلاف سردفتر دراین‌باره هیچ‌گونه وظیفه‌ای برعهده ندارد.

۲-۴ آزادی یا محدودیت فعالیت مراجع گواهی

مسئله دیگر درباره مراجع گواهی عبارت است از اینکه آیا این اشخاص برای فعالیت و ارائه خدمات به اعضای جامعه، ملزم به کسب مجوز ازسوی مقامات عمومی هستند یا خیر؟

براساس قوانین برخی از کشورها، فعالیت مراجع گواهی باید با اجازه مقام صالح انجام گیرد. برای مثال قانون امضای دیجیتال ایالت یوتای آمریکا، اجازه وزارت بازرگانی را برای چنین فعالیتی ضروری می‌داند.

کشورهای آلمان و ایتالیا نیز به تقلید از سیستم پذیرفته شده در یوتا، ابتدا قوانینی درباره امضای دیجیتال تصویب و نظام حاکم بر زیرساخت کلید عمومی را به‌طور مفصل بیان کردند. به موجب این مقررات، مراجع گواهی هنگامی می‌توانستند در این کشورها به ارائه خدمات بپردازند که مجوز لازم را از مقام صالح دریافت کرده باشند.

تأسیس سیستم‌های ملی صدور مجوز با مخالفت کمیسیون اروپا مواجه شد؛ چرا که اگر کشورهای عضو اتحادیه اروپایی، ارائه خدمات مربوط به گواهی را به اجازه قبلی مقامات هر کشور منوط کرده و قواعد فنی خاص خود را درباره محصولات مرتبط با امضای الکترونیکی اتخاذ می‌کردند؛ فعالیت ارائه‌دهندگان این خدمات در سطح اروپا و نیز تأمین محصولات وابسته به امضای الکترونیکی در بازار داخلی این قاره غیرممکن یا دست‌کم بسیار دشوار می‌شد.

به‌این‌ترتیب کمیسیون اروپا با انتشار اعلامیه‌ای به کشورهای عضو، در سال ۱۹۹۷، اعلام داشت: «رویکردهای قانونی و فنی مختلف، مانعی جدی برای بازار داخلی محسوب

شده و توسعه فعالیت‌های نوین اقتصادی را ــ که با تجارت الکترونیکی مرتبط است ــ متوقف خواهد کرد. بنابراین ایجاد یک چارچوب سیاست‌گذاری در اتحادیه اروپایی به‌منظور تضمین امنیت و اعتماد در ارتباطات الکترونیکی و حفاظت از عملکرد بازار داخلی بسیار ضرورت دارد. اتحادیه اروپایی نمی‌تواند شاهد وضعیت قانونی ناهماهنگ درزمینه‌ای باشد که برای اقتصاد و جامعه اهمیت حیاتی دارد».

در نتیجه، ممنوعیت منوط کردن ارائه خدمات مربوط به گواهی به اجازه قبلی به یکی از ارکان اساسی به دستورالعمل اتحادیه اروپایی تبدیل شد: دسترسی به این بازار باید آزاد و بدون هرگونه مانعی باشد. این قاعده نه فقط درباره مراجع گواهی؛ بلکه نسبت به همه تأمین‌کنندگان خدمات مرتبط با گواهی از جمله مراجع ثبت و ... اعمال می‌شود.

در راستای تحقق این هدف، بند «۱» ماده (۳) دستورالعمل اتحادیه اروپا، کشورهای عضو را ملزم می‌کند تا تضمین کنند که ارائه خدمات مرتبط با گواهی به اجازه قبلی منوط نباشد.

باوجود این، اصل آزادی ارائه خدمات مرتبط با گواهی در این دستورالعمل به دو طریق تعدیل شده است:

الف) براساس بند «۲» ماده (۳) این دستورالعمل، کشورهای عضو می‌توانند با رعایت بند «۱»، برای ارتقای سطح خدمات ارائه شده، سیستم‌های داوطلبانه دریافت مجوز تأسیس کنند. شرایط دریافت مجوز در این سیستم‌ها باید شفاف، متناسب و عاری از هرگونه تبعیض باشد.

ب) بند «۳» ماده (۳) این دستورالعمل، کشورهای عضو را ملزم کرده تا سیستم‌هایی کارآمد برای نظارت بر فعالیت مراجع گواهی موجود در قلمرو خود ایجاد کنند. این سیستم‌ها گواهی‌های حائز شرایط[1] (ضمیمه‌های یک و دو دستورالعمل) صادر می‌کنند. البته سیستم‌های نظارتی بیشتر کشورهای اروپایی به حدی سخت‌گیرانه است که آنها را به نظام صدور مجوز فعالیت نزدیک می‌گرداند. شاید دلیل این امر، تلاش برای افزایش کیفیت خدمات مراجع گواهی این کشورها، برای حضور و رقابت مؤثرتر در سطح اروپا و جهان باشد.

---

1. Qualified Certificates

۲-۵ وظایف مراجع گواهی

با توجه به متون قانونی مختلف، اهم وظایف مراجع گواهی را می‌توان در موارد زیر خلاصه کرد:

۱. اطمینان یافتن از تعلق جفت کلید به متقاضی گواهی،

۲. تشخیص صحت اطلاعاتی مانند اشتغال به حرفه معین که متقاضی خواستار درج آنها در گواهی است،

۳. صدور گواهی،

۴. ابطال یا تعلیق گواهی؛ گواهی معمولاً برای مدت زمان محدودی اعتبار داشته و دارای تاریخ انقضاست که در خود گواهی درج می‌شود. بااین‌حال، پیش از این تاریخ نیز ممکن است به تقاضای خود دارنده (برای مثال به هنگام لو رفتن کلید خصوصی) و البته با رعایت حقوق اشخاص ثالث، یا رأساً و به تشخیص خود مرجع (مانند وقتی که مرجع اطلاع یابد که اطلاعات مندرج در گواهی از ابتدا با واقعیت منطبق نبوده یا دیگر واقعیت ندارد) گواهی باطل یا معلق شود. مرجع گواهی باید به‌طور منظم، فهرست گواهی‌های باطل شده را اعلام کند،

۵. در دسترس قرار دادن گواهی برای استفاده اشخاص،

۶. پایبندی به اظهارات درباره نحوه ارائه خدمات،

۷. به‌کارگیری سیستم‌ها، رویه‌ها و منابع انسانی مطمئن برای ارائه خدمات،

۸. رعایت حریم خصوصی اعضای جامعه.

۲-۶ مسئولیت مراجع گواهی

مسئولیت مراجع گواهی می‌تواند ناشی از عدم ایفای تعهدات قراردادی (مسئولیت قراردادی) یا ارتکاب تقصیر (تجاوز از رفتار شخص متعارف و معقول در همان اوضاع و احوال) یا رعایت نکردن تکالیف خاصی باشد که قانون برعهده مراجع گواهی قرار داده است.

ماده (۹) قانون آنسیترال درباره مسئولیت مدنی مراجع گواهی بیان می‌دارد که مرجع در برابر خسارات ناشی از قصور خود در انجام وظایف، مسئول است. براساس این ماده، اثبات تقصیر مرجع گواهی ضرورت دارد و این یعنی اعمال قواعد عمومی مسئولیت مدنی.

ازنظر ما پیروی از قواعد عمومی مسئولیت در اقامه دعوا علیه مراجع گواهی با موقعیت این مراجع و فلسفه وجودی آنها سازگاری ندارد. مراجع گواهی به‌منظور برقراری ثبات و امنیت در ارتباطات الکترونیکی ایجاد می‌شوند و نظام قانونی باید به گونه‌ای باشد که به‌کارگیری حداکثر دقت و رعایت احتیاط را به‌وسیله آنها موجب شود. همچنین مشخص نیست که باوجود سیستم‌های پیچیده رایانه‌ای چگونه می‌توان تقصیر مرجع گواهی را ثابت کرد؟

ازاین‌رو، ماده (۶) دستورالعمل اتحادیه اروپایی، مرجع گواهی را در برابر هرگونه خسارت وارد به اشخاصی که به گواهی اعتماد مشروع می‌کنند، مسئول می‌داند؛ مگر آنکه مرجع بی‌تقصیری خود را ثابت کند.

البته آنچه منطقی‌تر به نظر می‌رسد، برقراری نظام مسئولیت محض[1] برای مراجع گواهی است. به این معنا که مرجع گواهی زمانی از مسئولیت معاف شود که وجود قوه قاهره را اثبات کند. در این صورت مراجع گواهی از بیمه‌هایی که برای فعالیت‌های آنها ارائه می‌شود بیشتر استفاده خواهند کرد.

۲-۷ نحوه تعامل مراجع گواهی

گواهی دیجیتال صادر شده به‌وسیله مرجع نیز مانند دیگر اسناد الکترونیکی مبادله شده میان کاربران شبکه، باید درجه‌ای از امنیت را در خود داشته باشد، تا گیرنده از صدور گواهی به‌وسیله مرجع اعلام شده و همچنین مصون ماندن محتوای آن از تغییر و تحریف اطمینان یابد. این مهم با استفاده از امضای دیجیتال مرجع گواهی محقق می‌شود. بنابراین مرجع نیز باید امضای دیجیتال داشته باشد.

---

1. Strict Liability

مسئله قابل طرح در این بحث، به چگونگی اطمینان یافتن از تعلق کلید عمومی اعلام شده به مرجع، مربوط می‌شود. در این حالت مرجع نیز باید به گونه‌ای تعلق کلید عمومی مرتبط با کلید خصوصی را ــ که گواهی به‌وسیله آن امضا شده ــ به خود ثابت کند. مراجع گواهی، معمولاً به طریقی مطمئن و خارج از خط (برای مثال هنگام مراجعه متقاضی برای دریافت گواهی خود) کلید عمومی را به اطلاع کاربران می‌رسانند. گواهی که در آن خود مرجع، تعلق کلید عمومی را به خود تصدیق می‌کند، «گواهی خودامضا» و مرجع مورد نظر «مرجع گواهی ریشه»[1] نامیده می‌شود.

اما ممکن است کلید عمومی مرجع گواهی، خود موضوع گواهی صادر شده ازسوی مرجع دیگر باشد؛ یعنی مرجع دیگری تعلق این کلید را به مرجع تأیید کند. در این صورت مسئله نحوه تعامل مراجع گواهی طرح می‌شود. الگوهای مختلفی برای این تعامل شکل گرفته است که در ذیل به مهم‌ترین این الگوها اشاره می‌کنیم:

۱-۷-۲ شیوه سلسله‌مراتبی[2]

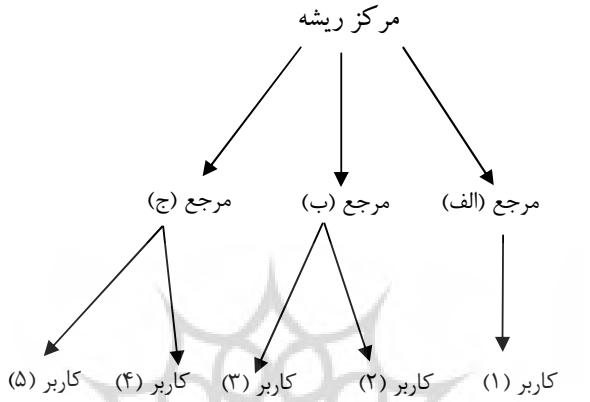
در این روش، مراجع گواهی با یک مرجع مشترک ــ که یک مرجع (مرکز) گواهی ریشه است ــ سازماندهی می‌شوند. مرجع گواهی ریشه برای مراجع فرعی، گواهی صادر کرده و تعلق یک کلید عمومی معین را به هریک از آنها تصدیق می‌کند. مراجع فرعی ممکن است برای مراجع پایین‌تر از خود در سلسله‌مراتب یا کاربران، گواهی صادر کنند. در شیوه سلسله‌مراتبی، کاربران باید از کلید عمومی مرجع ریشه مطلع باشند. در نتیجه مرجع ریشه باید به طریقی مطمئن، کلید عمومی خود را به آگاهی آنها برساند. گواهی که این مرجع دراین‌باره صادر می‌کند، خود امضاست.

در شیوه سلسله‌مراتبی، اصالت هر گواهی را می‌توان به‌وسیله بررسی مسیر تصدیق‌ها[3]

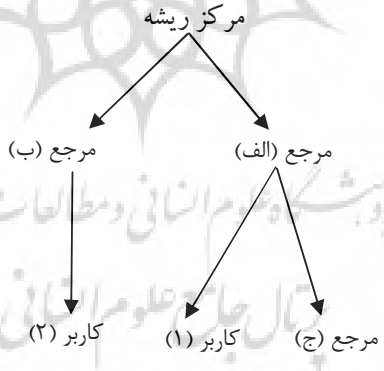
---

1. Root Certificate Authorities
2. Hierarchical
3. Certification Paths

ــ که به مرکز ریشه منتهی می‌شود ــ تشخیص داد. در حقیقت، مرکز ریشه به‌عنوان نقطه اعتماد مجموعه تلقی می‌شود. شکل‌های ۱ و ۲ بیانگر نحوه قرار گرفتن مراجع گواهی در روش سلسله‌مراتبی است:



شکل ۱ صدور گواهی برای مراجع فرعی فقط به‌وسیله مرجع ریشه



شکل ۲ صدور گواهی به‌وسیله مراجع فرعی برای مراجع پایین‌تر از خود یا کاربران

در این روش، مسیرهای تصدیق، کوتاه و فاقد پیچیدگی هستند، در نتیجه بررسی اصالت امضای دیجیتال ساده‌تر بوده و زمان چندانی برای آن صرف نمی‌شود.

روش سلسله‌مراتبی، تعداد مراجعی را که به‌طور مستقیم باید مورد اعتماد واقع شوند کاهش می‌دهد اما اصلی‌ترین نقطه ضعف این روش، به مرکز گواهی ریشه مربوط می‌شود. اگرچه ممکن است مراجع فرعی برای پیوستن به مجموعه و دریافت گواهی ازسوی مرکز ریشه مبالغی پرداخت کنند؛ اما فعالیت این مرکز عواید چندانی دربرنخواهد داشت. مسلم است در چنین وضعیتی، مدیریت مرکز گواهی ریشه، حتی اگر ارگان دولتی باشد، متحمل پذیرش مسئولیت زیادی نخواهد شد و احتمال دارد مسئولیت به‌عنوان موضوعی، میان طرف‌های اعتمادکننده و مراجع فرعی باقی بماند.

به‌علاوه، افشای کلید خصوصی مرکز ریشه، اعتماد موجود را در مجموعه خدشه‌دار خواهد ساخت. و قاعدتاً گواهی‌های صادر شده باید از درجه اعتبار ساقط شوند و کلید عمومی جدید مرجع به اطلاع کاربران برسد. این امر مستلزم صرف هزینه هنگفتی خواهد بود.

کشور آلمان مثال بارزی از کاربرد سیستم سلسله‌مراتبی است. در این کشور، تمام مراجع گواهی (صادرکننده گواهی‌های حائز شرایط) که به‌وسیله دولت آلمان تأیید شده‌اند، زیرمجموعه یک مرجع گواهی ریشه قرار می‌گیرند که به‌وسیله مرجع تنظیم‌کننده پست و مخابرات اداره می‌شود.

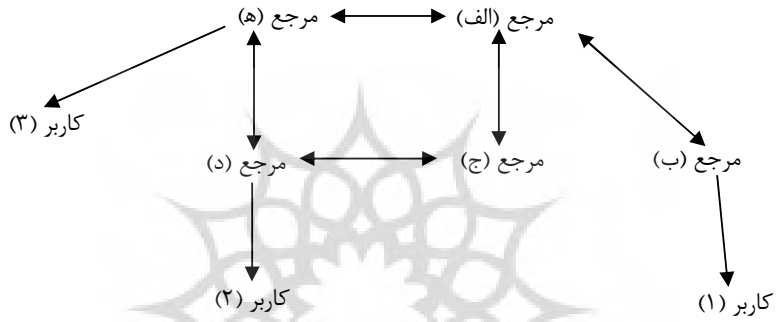
همچنین در کره جنوبی از شیوه سلسله‌مراتبی پیروی شده و ارگان امنیت اطلاعات کره، مرکز گواهی ریشه را ــ که به‌وسیله وزارت اطلاعات و ارتباطات آن کشور ایجاد شده ــ اداره می‌کند. گفتنی است که ارگان امنیت اطلاعات کره جنوبی یکی از سازمان‌های وابسته وزارت اطلاعات و ارتباطات این کشور است.

کشور مصر نیز به تأسیس مرکز ریشه مبادرت کرده است. مسئولیت اداره این مرکز در این کشور برعهده ارگان توسعه صنعت فناوری اطلاعات قرار دارد که به وزارت ارتباطات و فناوری اطلاعات وابسته است.

مرکز گواهی ریشه هند به‌وسیله وزارت ارتباطات و فناوری اطلاعات تأسیس شده و با نظارت آن وزارتخانه اداره می‌شود.

۲-۷-۲ شیوه تصدیق متقاطع[1]

در این روش، مراجع گواهی مستقل، یکدیگر را به‌صورت متقابل تصدیق می‌کنند (برای یکدیگر گواهی صادر می‌کنند) و به‌این‌ترتیب مجموعه‌هایی از روابط مبتنی بر اعتماد، میان مراجع گواهی ایجاد می‌شود. (شکل ۳)



شکل ۳ تصدیق متقاطع

هرطرف اعتمادکننده، با کلید عمومی مرجع نزدیک خود ــ که به‌طورکلی مرجع صادرکننده گواهی اوست ــ در ارتباط است. وی اصالت هر گواهی را با بررسی مسیر تصدیقی که به این مرجع گواهی منتهی می‌شود در نظر می‌گیرد. به فرض کاربر (۱) نامه‌ای الکترونیکی از کاربر (۲) دریافت می‌کند. کاربر (۱)، از کلید عمومی مرجع (ب) و کاربر (۲) از کلید عمومی مرجع (د) مطلع است. با توجه به شکل ۳، مسیرهای تصدیق مختلفی از کاربر (۲) شروع و به‌کاربر (۱) ختم می‌شود. ساده‌ترین راه برای کاربر (۱) آن است که ابتدا گواهی کاربر (۲) ــ که از سوی مرجع گواهی (د) ــ سپس گواهی خود مرجع (د) ــ

1. Cross Certification

که به‌وسیله مرجع (ج) ــ و در نهایت گواهی مرجع (ج) ــ که به‌وسیله مرجع (ب) ــ صادر شده را بررسی کند.

در روش تصدیق متقاطع یا شبکه‌ای،[1] گروه جدیدی از کاربران به آسانی می‌توانند به مجموعه بپیوندند: هریک از مراجع موجود در مجموعه، رابطه‌ای مبتنی بر اعتماد را از طریق تصدیق متقابل، با مرجع گواهی این کاربران برقرار می‌کند. به‌علاوه، افشای کلید خصوصی یک مرجع، به کل مجموعه آسیب وارد نمی‌سازد. جبران آثار لو رفتن کلید خصوصی یکی از مراجع، فقط مستلزم آن است که مراجعی که برای این مجمع گواهی صادر کرده‌اند؛ آن را ابطال کرده و کلید عمومی جدید و گواهی‌های امضا شده به‌وسیله کلید خصوصی مربوط به آن به طریقی ایمن، میان دارندگان گواهی‌های آن مرجع توزیع شود.

روش تصدیق شبکه‌ای به دلیل تصدیق‌های مختلف، ماهیت پیچیده‌ای دارد و برخلاف شیوه سلسله‌مراتبی، بررسی مسیرهای تصدیق به‌راحتی امکان‌پذیر نیست؛ زیرا کاربر با گزینه‌های متعددی مواجه است.

۳-۷-۲ استفاده از مرجع گواهی پل[2]

این مرجع برای ارتباط مجموعه‌های مختلف مراجع گواهی، (بدون توجه به شیوه سازماندهی آنها)، طراحی شده است. برخلاف روش تصدیق متقاطع، مرجع پل به‌طور مستقیم برای کاربران، گواهی صادر نمی‌کند. تمام کاربران مجموعه‌های مستقل مرجع پل را به‌عنوان یک واسطه تلقی می‌کنند. این مرجع روابط دوجانبه‌ای را با مجموعه‌های مختلف برقرار می‌کند (تصدیق متقاطع). چنین روابطی را می‌توان به‌منظور تشکیل یک پل اعتماد ــ که کاربران مجموعه‌های متفاوت را به هم متصل می‌کند ــ به‌کار گرفت.

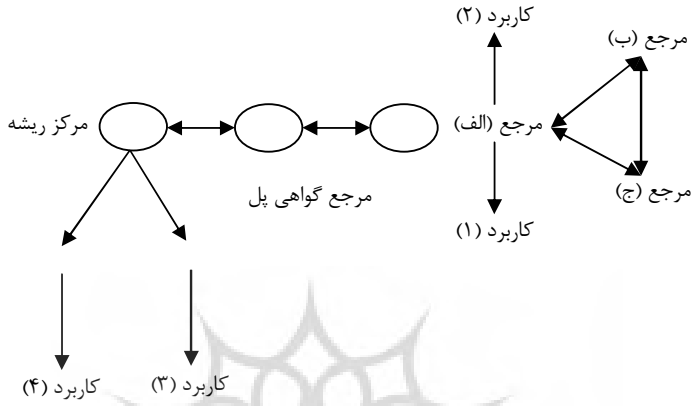
چنانچه مجموعه‌ای به‌صورت زیرساخت سلسله‌مراتبی باشد، مرجع گواهی پل با مرکز گواهی ریشه رابطه برقرار خواهد کرد؛ اما هرگاه مجموعه به‌صورت شیوه تصدیق متقاطع

---

1. Mesh Certification
2. Bridge Certificate Authorities

باشد، مرجع پل فقط با یکی از مراجع مجموعه رابطه خواهد داشت. به‌هرحال مرجعی که با مرجع پل رابطه تصدیق متقابل دارد؛ مرجع اصلی نامیده می‌شود.

شکل ۴ بیانگر موقعیت مرجع گواهی پل و ارتباط آن با مجموعه‌های مختلف است.



شکل ۴ مرجع گواهی پل زیرساخت سلسله‌مراتبی شیوه تصدیق متقاطع

استفاده از مرجع گواهی پل، تشخیص مسیر تصدیق را در مقایسه با روش تصدیق متقاطع، آسان‌تر می‌سازد. کاربران معمولاً مسیر خود را تا مرجع پل می‌شناسند و فقط باید مسیر تصدیق از این مرجع تا گواهی کاربر مقابل را تعیین کنند. به‌علاوه زیرساخت مبتنی بر مرجع پل، مسیرهای اعتماد کوتاه‌تری نسبت به روش تصدیق متقابل خواهد داشت. بااین‌حال، تشخیص مسیر تصدیق نسبت به روش سلسله‌مراتبی مشکل‌تر بوده و طول مسیر تصدیق معمولاً دو برابر می‌شود.

برای مثال دراین‌باره می‌توان از زیرساخت فدرال کلید عمومی[1] دولت آمریکا نام برد. زیرساخت مبتنی بر مرجع پل در کشورهایی مانند کانادا و ژاپن نیز ایجاد شده است.

1. Federal Public Key Infrastructure

۳ مراجع گواهی در ایران

باب دوم قانون تجارت الکترونیکی جمهوری اسلامی ایران با عنوان «دفاتر خدمات صدور گواهی الکترونیکی» شامل دو ماده ذیل است:

ماده (۳۱) در تعریف این عبارت بیان می‌دارد: «دفاتر خدمات صدور گواهی الکترونیکی واحدهایی هستند که برای ارائه خدمات صدور امضای الکترونیکی در کشور تأسیس می‌شوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به‌روز نگهداری گواهی‌های اصالت امضای الکترونیکی می‌باشد».

ماده (۳۲) وظیفه تهیه آیین‌نامه، ضوابط تأسیس و شرح وظایف این دفاتر را برعهده سازمان مدیریت و برنامه‌ریزی، وزارتخانه‌های بازرگانی، ارتباطات و فناوری اطلاعات، امور اقتصادی و دارایی و دادگستری نهاده است.

باوجود گذشت حدود سه سال‌ونیم از تصویب قانون تجارت الکترونیکی، هنوز این آیین‌نامه به تصویب نرسیده است و این در حالی است که خبر تأسیس مرکز گواهی ریشه و شروع فعالیت آن در پاییز سال ۱۳۸۵ منتشر شد. بنابراین به نظر می‌رسد که در کشور ما سیستم سلسله‌مراتبی پذیرفته شده است.

حال سؤال این است که با نبود سند لازم درباره مراجع گواهی، فعالیت مرکز ریشه چه مفهومی دارد؟

مسئله دیگر به نهاد اداره‌کننده مرکز گواهی ریشه مربوط می‌شود. موضوعی که تاکنون اختلافات و بحث‌های دامنه‌داری را موجب شده است.

به نظر می‌رسد برای تعیین ارگانی با صلاحیت مدیریت مرکز ریشه، فارغ از هرگونه پیش‌داوری، باید ماهیت این مرکز را در نظر داشت و نیز وظیفه و کارکرد ارگان‌هایی را مورد توجه قرار داد که برای پذیرش مسئولیت مرکز ریشه پیشنهاد شده‌اند.

توجه به مطالب مربوط به زیرساخت سلسله‌مراتبی، ماهیت مرکز ریشه را تبیین می‌کند. درحقیقت مرکز ریشه ابزاری است برای ایجاد اعتماد در کاربران نسبت به مراجع

فرعی و گواهی‌هایی که صادر می‌کنند. همچنین مسلم است که زیرساخت کلید عمومی برای موثق کردن تراکنش‌های الکترونیکی کاربران و با هدف اطمینان اشخاص نسبت به اصالت هویت یکدیگر و نیز محتوای پیغام‌های مبادله شده، تأسیس می‌شود.

تراکنش‌های انجام شده اینترنتی و دیگر شبکه‌های رایانه‌ای می‌تواند ماهیت‌های مختلفی داشته باشد. فردی که می‌خواهد نامه‌ای خصوصی را به دیگری برساند؛ به‌منظور صرفه‌جویی در وقت و هزینه، آن را با پست الکترونیکی برای وی ارسال می‌کند. گاهی دو تاجر برای انجام معامله تجاری مانند خرید مواد خام مورد نیاز برای تولید محصولی معین، از اینترنت استفاده می‌کنند. مصرف‌کننده‌ای که به مزایای خرید الکترونیکی واقف است با مراجعه به پایگاه (سایت) اینترنتی فروشنده، کالایی را از وی می‌خرد. این کالا ممکن است دارای ماهیت مجازی باشد (برای مثال یک کتاب الکترونیکی) که در این صورت فروشنده می‌تواند آن را به‌وسیله اینترنت تحویل دهد یا اینکه دارنده یک حساب اینترنتی به‌جای حضور در بانک، می‌تواند با استفاده از اینترنت، وجوه را از حساب خود به حساب دیگری به‌وسیله بانک انتقال می‌دهد. با گسترش دولت الکترونیکی، خدماتی که به‌طور سنتی و با حضور فیزیکی افراد در محل و استفاده از کاغذ انجام می‌شد، در قالب الکترونیکی به شهروندان ارائه خواهد شد، برای مثال در وب‌سایت شهرداری فرم‌های لازم قرار داده شده و متقاضیان با تکمیل آنها خواهان دریافت خدمت مربوط خواهند شد. تعامل ارگان‌های دولتی با یکدیگر نیز به‌طور الکترونیکی انجام شده و حتی انتخابات نیز به شکل الکترونیکی برگزار خواهد شد.

بنابراین تراکنش‌های الکترونیکی اعضای جامعه انواع مختلفی داشته و به شکل خاصی محدود نمی‌شود. در نتیجه، گواهی‌های صادر شده درباره کلید عمومی آنان نیز می‌تواند کاربرد عام داشته باشد؛ به این معنا که دارنده مجاز باشد امضای دیجیتال خود را در تراکنش‌های مختلف به‌کار برد. گاه نیز ممکن است مرجع گواهی اعلام کند که استفاده از گواهی فقط در تراکنش‌های خاصی مجاز است.

به نظر می‌رسد با این توضیحات، بسیاری از سوءتفاهم‌های پیش‌آمده درباره نهاد اداره‌کننده مرکز ریشه برطرف شود.

مرجع ریشه عبارت است از مرجعی که گواهی مربوط به کلید عمومی آن خود امضاست؛ یعنی تعلق کلید عمومی به مرجع ریشه به‌وسیله مرجع دیگری تصدیق نمی‌شود. در روش سلسله‌مراتبی، مرجعی که در رأس مجموعه قرار می‌گیرد؛ یک مرجع ریشه است.

حال سؤال این است که در جمهوری اسلامی ایران منظور از مرجع ریشه چیست؟

اگر براساس سیاست دولت، توسعه زیرساخت کلید عمومی به شیوه‌ای غیر از روش سلسله‌مراتبی باشد؛ مراجع گواهی متعددی ممکن است گواهی‌های خود را به‌صورت خودامضا ارائه کنند. در این صورت هریک از این مراجع، مرجع ریشه خواهند بود. در نتیجه مرجع یا مراجعی که مجوز فعالیت را در کشور از مقام صالح دریافت کنند می‌توانند در درجه اول، با توجه به قلمروی که در مجوز برای آنها تعیین شده و سپس با سیاست خود آنها، گواهی‌هایی برای استفاده در تراکنش‌های گوناگون یا تراکنش‌های معین صادر کنند.

با چنین فرضی، ممکن است دولت تشخیص دهد که اجازه صدور گواهی را در هر بخش به مرجعی معین واگذار کند برای مثال گواهی‌های مرتبط با بانکداری الکترونیکی را به بانک مرکزی، گواهی‌های تجار را به وزارت بازرگانی و همین‌طور گواهی‌های مورد استفاده برای تعامل مردم با نهادهای حکومتی و نیز تعامل این نهادها با یکدیگر، هر ارگان به‌طور جداگانه، صلاحیت تأسیس مرجع گواهی را داشته باشد و سایر گواهی‌ها به‌وسیله مراجع گواهی دیگری ــ که می‌توانند خصوصی باشند صادر شود.

اما هرگاه مسئولان فناوری اطلاعات و ارتباطات کشور خواستار تأسیس نظام سلسله‌مراتبی باشند؛ منظور از مرکز ریشه، مرجعی خواهد بود که در رأس مجموعه قرار دارد. در این حالت سخن گفتن از مرجع ریشه دیگری بیهوده است. چرا که کلید عمومی همه مراجع باید به‌وسیله این مرکز تصدیق شود و مراجع دیگر ریشه نبوده؛ زیرا گواهی آنها خودامضا نیست. آنچه باقی می‌ماند تعیین نهادی است که برای اداره مرکز ریشه انتخاب می‌شود.

با توجه به آنچه گفته شد درمی‌یابیم که نمی‌توان ارگانی مانند بانک مرکزی یا وزارت بازرگانی را به این دلیل که برخی از گواهی‌های صادره به‌وسیله مراجع فرعی در امور بانکی یا تجاری مورد استفاده قرار می‌گیرند؛ به‌عنوان متولی مرکز ریشه شناخت. به‌علاوه فلسفه وجودی مرکز ریشه برقراری اطمینان در کل زیرساخت است و در نظام سلسله‌مراتبی ماهیتی مستقل از مراجع فرعی و گواهی‌های صادر شده دارد.

اگر مأموریت مرکز ریشه به امور بانکی و پولی کشور محدود می‌شد؛ بی‌شک بانک مرکزی باید وارد عمل شده و به تأسیس آن مبادرت می‌کرد. همچنین درصورتی‌که کارکرد مرکز ریشه فقط تجاری باشد، اداره آن به‌وسیله وزارت بازرگانی منطقی جلوه می‌کرد؛ اما مرکز ریشه نقطه اعتمادی در زیرساخت است که برای موثق کردن ارتباطات و ایجاد اطمینان در کاربران نسبت به هویت طرف مقابل و نیز نسبت به محتوای پیغام‌های الکترونیکی تشکیل می‌شود.

منابع و مآخذ

American Bar Association, Digital Signature Guidelines.

Chen-chi lin, Chi-Sung laih, The GPKI Developing Status of Tiwan and Some major Asia Countries.

Directive 1999/93/ec of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.

Olnes John. PKI Interoperability by an Independent trusted Validation Authority.

Dumortier Jos. Legal Status of Qualified Electronic Signatures in Europe.

Kuhn Richard. Introduction to Public Key Infrastructure and the Federal PKI.

Three PKI Architectures-new Zealand E.government Programme.

Uncitral Model Law on Electronic Signatures With Guide to Enactment.

Utah digital signature act.

W E. Burr, Public Key Infrastructures (PKI) Technical Specifications.

T. Polk William & Nelson E. Hastings, Bridge Certification Authorities, connecting b2b Public Key Infrastructures.

http://www.rootca.or.kr.

هفته‌نامه عصر ارتباط، ۲۵ آذر ۱۳۸۵.