امضاهای دیجیتالی، گواهی امضاهای الکترونیکی و تجارت الکترونیک

نوشته: ۱) برایان گلادمن: مشاور امنیت اطلاعات (انگلیس)
۲) کارل الیسون: متخصص شرکت اینتل (آمریکا)
۳) نیکلاس بوهم: مشاور حقوقی (انگلیس)

مترجمان: ۱) **سلیمان فدوی**[۱]
۲) **محمد رضا ملکی**[۲]

۱ـ مقدمه

در رمزنگاری، آن‌گونه که از ۳۵۰۰ سال پیش تا اواسط دهه ۱۹۷۰ مرسوم بوده است، از رمزی استفاده می‌شد که هم رمزگذار و هم رمزگشا از آن آگاه بودند. هرکس که این رمز را در اختیار داشت، می‌توانست یکی از دو کار را انجام دهد (اصطلاحاً به رمز یاد شده **کلید** گفته می‌شد). در رمزنگاری با کلید عمومی، دو **کلید** متفاوت وجود دارد که یکی از آنها برای رمزگذاری بر روی داده‌ها و دیگری برای گشودن همان رمز مورد استفاده قرار می‌گیرد. در حالی که یکی از این کلیدها محرمانه و خصوصی نگه‌داشته می‌شود، دیگری برای اطلاع عموم انتشار خواهد یافت. سیستم مذکور چنان طراحی شده است که اطلاع از کلید عمومی، به تنهایی موجب تعیین ارزش کلید اختصاصی نخواهد شد.

---

۱. سردفتر دفترخانه ۴۴۳ تهران و عضو هیئت علمی دانشکده حقوق.

۲ . دانشجوی کارشناسی ارشد (حقوق تجارت بین الملل) دانشکده حقوق دانشگاه شهید بهشتی

به طور طبیعی چنین فرض می‌شود که کنترل کلید اختصاصی تنها در اختیار یک نفر است که در اینجا اختصاراً به او **دارنده کلید** می‌گوئیم. رمزنگاری با کلید عمومی می‌تواند هم به منظور ویژگی محرمانه بودن و هم برای ساخت امضاهای الکترونیکی به کار رود.

محرمانه بودن وقتی تجلی می‌یابد که کلید رمزگشا، خصوصی و محرمانه نگاه داشته شود و کلید رمزگذاری به طور عام برای مردم افشا گردد. به نحوی که هرکس بتواند کلید عمومی را در اختیار داشته و هر پیامی را رمزگذاری نماید، لیکن فقط دارنده کلید اختصاصی است که قادر به گشودن آن خواهد بود.

با داشتن یک امضای دیجیتالی که به طور صحیح تأیید گردیده باشد، متوجه می‌شویم که پیام امضاء شده پس از امضاء تغییر نیافته و تثبیت امضاء با یک کلید اختصاصی معین صورت گرفته است.

۲ـ امضاهای دیجیتالی

برای ساخت امضاء الکترونیکی، به یک جفت کلید نیاز خواهیم داشت. یک کلید رمز به صورت دیجیتال که برای امضاء انواع داده‌ها استفاده می‌شود و یک کلید عمومی تأیید امضاء دیجیتال که دیگران آن را به کار می‌برند تا یقین حاصل نمایند که امضاء دریافتی با کلید امضاء مربوطه ساخته شده است.

هر چند اصطلاح «امضاء» هم برای امضاهای دست نویس و هم برای امضاهای دیجیتال به کار می‌رود، لیکن در عمل، این دو امضاء ویژگی‌های کاملاً متفاوتی با یکدیگر دارند. هرگاه سندی که به نحو دیجیتال امضاء شده باشد، به هر شکلی مخدوش گردد، امضاء ذیل آن تأیید نخواهد شد. با این وجود، کلید اختصاصی سازنده امضاء ممکن است مورد استفاده هر کسی قرار گیرد که به آن دست یابد. این واقعیت باعث می‌شود تا امضاء دیجیتالی شبیه به مهر گردد.

از سوی دیگر، امضاء دست نویس با صاحب خود ارتباطی زیست شناختی دارد اما استفاده از آن بر روی یک سند مانع تغییر پنهانی سند توسط امضاء کننده نمی‌شود. امضاء مکتوب مدرکی است دال بر تأیید سند توسط صاحب امضاء آن، حال آنکه امضاء دیجیتالی دلیلی بر عملکرد یک کلید اختصاصی بر روی سند می‌باشد.

امضاء دیجیتالی است که به ما می‌گوید یک سند دیجیتالی از زمان امضاء به بعد تغییر کرده یا نکرده است. با این وجود در صورت فقدان اطلاعات بیشتر، امضاء دیجیتالی مؤید مشارکت شخص خاصی در فرآیند امضاء کردن نیست. اگر کلید رمز گواهی امضاء به تنهایی در اختیار یک نفر باشد می‌توان این‌گونه فرض کرد که امضاء، نماینده رضایت همان فرد است و اسناد امضاء شده توسط کلید رمز حقیقتاً توسط فرد مورد نظر امضاء شده است. این ساز و کار بسیار شبیه نحوه عملکرد ماشین نویسی چک است. تا زمانی که به خوبی از ماشین حفاظت شود و تنها امضاء کنندگان مجاز به آن دسترسی پیدا کنند، امضاء ماشینی می‌تواند مبین امضاء انسانی باشد که جایگزین آن شده است. با این وجود احراز این نکته که کلید امضاء در زمان یک امضاء خاص، تحت کنترل فرد معینی قرار داشته و اینکه آن شخص واقعاً می‌دانسته که با این کلید چه چیزی را امضاء می‌کند فرآیند دشواری است.

۱ ـ۲) شناسایی دارنده کلید:

اگر فردی که او را می‌شناسیم و به وی اعتماد داریم کلید تأیید امضاء خود را در اختیارمان بگذارد می‌توانیم کلید مذکور را با هویت او مرتبط سازیم. البته اگر اطمینان داشته باشیم که تنها همان فرد به کلید دسترسی دارد. تحت چنین شرایطی می‌توانیم نام یا هر مشخصه دیگر را که از نظر ما مبین هویت طرف مقابل است، با کلید تأییدی که در اختیارمان گذاشته می‌شود، مرتبط سازیم. البته بعداً خواهیم دید که می‌توان از این طریق اطلاعات زیادی را با کلید رمز گواهی امضاء مرتبط ساخت.

اگر ناشناسی بخواهد کلید تأیید امضایی را که مبین امضایش است، در اختیارمان قرار دهد، اطلاعات ما بسیار کمتر خواهد بود. ما می‌توانیم متنی را به وی بدهیم تا امضاء کند و چنانچه امضایش معتبر باشد، در این صورت می‌توانیم نتیجه بگیریم که وی به کلید رمز امضاء دسترسی دارد اما نمی دانیم که آیا دیگران نیز همین کلید رمز را دارند یا خیر ؟ بنابراین از استفاده انحصاری آنها از این کلید، اطمینان نخواهیم داشت، به علاوه چون وی را کاملاً نمی شناسیم، فرد ناشناس می‌تواند ادعا کند که همان شخص معین است مگر اینکه بدشانس بوده و خود را جای شخصی معرفی نماید که ما وی را کاملاً می‌شناسیم. در

مجموع دشوار است که بتوان از هویت مالک کلید تأیید امضاء اطمینان حاصل نمود مگر اینکه کلید را از کسی دریافت کنیم که وی را می‌شناسیم و به وی اعتماد داریم.

۳ـ گواهی امضاهای دیجیتالی

همان گونه که گفتیم، اگر دوستی کلید تأیید امضاء خود را به ما بدهد می‌توانیم کلید تأیید را با نام وی مرتبط نموده و به یاد آوریم که کلید امضاء خاصی در اختیار آن دوست است. از این طریق هر سندی که دوستمان با چنین امضایی ارسال دارد می‌توان کنترل شده محسوب و صحت انتساب آن را به وی تاکید کرد. ممکن است ما کلید تأیید امضای دوستمان را به سایرین نیز بدهیم تا آنها هم بتوانند صحت امضاء ذیل سند ارسالی را تأیید نمایند. برای حفاظت از رابطه منطقی میان کلید تأیید امضاء و نام دارنده آن می‌توان ترکیب **کلید ـ نام** را برای ثبت منشأ امضاء در جایی ذخیره نمود و یک امضاء دیجیتالی از طرف خود به آن ضمیمه نمائیم.

گواهی امضاء الکترونیکی در حقیقت ترکیب امضاء شده کلید تأیید امضاء و نام یا هر مشخصه دیگر دارنده کلید رمز (که مبین هویت وی است) را در بر دارد. از طریق گواهی امضاء الکترونیکی، حتی اگر شخصی کلید تأیید امضاء را مستقیماً از ارسال کننده سند حاوی امضاء دریافت نکرده باشد، می‌تواند با استفاده از گواهی امضاء الکترونیکی از صحت انتساب امضاء به صاحب آن مطمئن گردد. هنگامی که مبادرت به صدور گواهی امضاء الکترونیکی می‌نمائیم، در واقع چنین اظهار می‌داریم که از نظر ما، نام درج شده در گواهی امضاء متعلق به کلید رمز امضاء مربوطه شخص تنظیم کننده سندی است که امضاء دیجیتالی اولیه به وی منتسب گردیده است و بدین صورت گواهی امضاء مبین گواهی هویت گردد. شخصی که از گواهی امضاء برای تشخیص هویت ارسال کننده سند استفاده می‌کند ممکن است بخواهد اطمینان حاصل کند که تنها ارسال کننده به کلید اختصاصی رمزگذاری امضاء دسترسی دارد، چون کنترلی بر این مسئله نداریم، لذا نمی توانیم استفاده انحصاری فرستنده سند از کلید اختصاصی را تضمین کنیم و به همین دلیل، گواهی امضاء الکترونیکی متضمن چنین ادعایی نیست. در اینجا باید میان اعتماد به امضاء و اعتماد به صاحب امضاء قائل به تفکیک شد.

امضای دیجیتالی، در شرایط مطلوب، این اطمینان را به وجود می‌آورد که شخص یا موسسه معینی، داده ای را امضاء نموده است، اما صرف امضاء بیانگر نکته ای در باب قابلیت اعتماد به امضاء کننده نمی‌باشد، این امر درباره امضاهای عادی نیز مصداق دارد. البته در امضاهای سنتی، امضاء بیش از آنکه با سند مرتبط باشد با صاحب خود ارتباط دارد، حال آنکه امضاء دیجیتالی ویژگی‌های متضادی دارد و بیشتر با سند مرتبط است. دلیل این امر نیز آسانی نشر کلید تأیید امضاء دیجیتالی و ادعای تعلق آن به دیگری و گریز از مسئولیت در قبال آن است.

گواهی امضاء سبب می‌شود تا مشکل ناشناس بودن فرستنده سند حاوی امضاء دیجیتالی تا حدی برطرف شود. در تشریح این مطلب می‌توان عنوان داشت چون به کسانی که آنها را می‌شناسیم، اعتماد داریم و چون کلید تأیید امضایی را که در اختیارمان می‌گذارند، حمل بر صحت می‌کنیم، بنابراین کسان دیگری که به پشت گرمی گواهی امضایی که ما صادر می‌نماییم (به لحاظ اعتمادشان به ما) به کسانی که ما آنها را تأیید می‌کنیم نیز اعتماد می‌کنند، بدین ترتیب شبکه ای از اعتماد متقابل شکل می‌گیرد. اما این موضوع، همه مشکلات را حل نمی‌کند چرا که ممکن است به سبب عدم شناخت فردی، گواهی امضاء او را نیز قابل اعتماد نشماریم.

ما می‌توانیم مصر باشیم که گواهی امضاها نیز باید امضاء شوند اما ناگزیر، این روند باید در جایی متوقف شود و در انتهای این سلسله، یک کلید تأیید امضای امضاء نشده قرار بگیرد. معمولاً کلید آخر، **کلید ریشه** خوانده می‌شود و باید به دنبال راهی بود تا بتوان قابلیت اعتماد به آن را تضمین کرد (این مساله متعاقباً مورد بحث قرار خواهد گرفت) در نهایت، گواهی امضاء دیجیتالی مجموعه‌ای از داده‌ها است که با یک کلید امضاء دیجیتالی تأیید شده است.

دارنده کلید امضاء، تأیید کننده صحت و اعتبار محتوای گواهی امضاء می‌باشد و هرجا که کلید ریشه تأیید امضاء موجود باشد، صحت ویژگی‌های مذکور به گونه‌ای مشخص تر برای کلید رمز امضاء که با این کلید تأیید امضاء مرتبط است، تضمین می‌گردد.

آسیب پذیری امضاهای دیجیتالی و نحوه استفاده از آنها، در پاره‌ای از موارد، عملا به

معنای ناکار آمدی گواهی‌های یاد شده خواهد بود که باید در طراحی سیستم‌های استفاده کننده از آنها لحاظ گردد. یکی از کاربردهای گواهی امضاء که پیشتر به آن اشاره شد، گواهی ارتباط یک نام با یک کلید معین است. در اینجا گواهی شامل کلید تأیید مرتبط با اطلاعاتی خواهد بود که به دارنده کلید اجازه می‌دهد تا مورد شناسائی قرار گیرد. شخص امضاء کننده چنین متنی، ممکن است تضمین کند که فرد شناسائی شده به کلید رمز امضاء مرتبط با کلید تأیید عمومی موجود در گواهی‌ها دسترسی داشته باشد. امضاء کننده هم‌چنین ممکن است ادعا کند که نامبرده همان شخص شناسائی شده‌ای است که کلید اختصاصی را در اختیار دارد. جزئیات مطالب ادعایی وی ضمن یک گواهی به اطلاعاتی وابسته خواهد شد که خارج از خود گواهی قرار دارد و نوعاً به آن **اظهارنامه نحوه عملکرد گواهی** گفته می‌شود.

برای کنترل اعتبار امضاء دیجیتالی لازم است یک کلید تأیید قابل اعتماد در اختیار داشته باشیم. چنین کلیدی ممکن است فعلا موجود باشد که در این صورت تأیید امضاء فوراً صورت می‌پذیرد. با این وجود اگر کلید تأیید امضاء در قالب یک گواهی ارائه شود، اعتبار امضاء روی متن مورد گواهی باید کنترل شود. در چنین مرحله‌ای احتمال دارد که این روند بارها تکرار شود چون تأیید امضاء روی متن مورد گواهی، خود به گواهی دیگری نیاز دارد.

در نهایت ما باید به کلیدی دسترسی پیدا کنیم که بدانیم می‌توان به آن اعتماد کرد و یا نیازی به امضاء مجدد نباشد. در صورت اخیر یک راه کنترل اعتبار امضاء، درج کردن آن در کتابی است که به طور گسترده در دسترس عموم باشد. اخیرا برای تحقق این منظور، مجموعه ای تحت عنوان **ثبت جهانی کلیدهای قابل اعتماد** منتشر شده است.

۴ـ انواع گواهی امضاهای الکترونیکی

۱ـ۴ـ گواهی امضاء هویتی

گواهی امضاء هویتی نوعی از گواهی امضاء الکترونیکی است که از ترکیب کلید تأیید امضاء و اطلاعات کافی جهت شناسایی دارنده کلیدی که انتظار می‌رود استفاده کننده انحصاری آن باشد، ساخته می‌شود. این نوع گواهی امضاء از آنچه که در بدو امر به نظر

می‌رسد، ابهام آمیز تر بوده و بعداً به تفصیل در مورد آن بحث و گفتگو خواهد شد.

۲ـ۴ـ گواهی امضاء عضویت

در چنین گواهی امضایی، بدون اینکه هویت دقیق فرستنده سندی تصدیق گردد، عضویت وی در گروه یا سازمانی خاص تأیید می‌شود. بسیار پیش می‌آید که امضاء خاصی برای تجویز یک معامله ضروری است، اما هویت امضاء کننده اهمیت چندانی ندارد. این گواهی نشان می‌دهد که دارنده کلید رمز امضاء مثلاً پزشک یا وکیل است. دارو سازان برای فروختن دارو به مراجعین، نیاز به گواهی پزشک دارند اما نیاز ندارند بدانند کدام یک از اطباء مجازند تا ذیل نسخه را امضاء نمایند.

در این مثال امضاء کننده هر که باشد، حق تجویز فروش و تحویل دارو را دارا است و هویت وی تأثیر چندانی در موضوع ندارد. گواهی عضویت هم‌چنین می‌تواند گواهی مجوز تلقی شود، ممکن است چنین تصور شود که کلید رمز پزشک بدون درج هویت وی ممکن است اختیار وی در صدور نسخه‌های پزشکی را زیر سؤال برد. با این وجود چنین گواهی امضایی حاوی هویت دارنده کلید نیست، صادر کننده گواهی از هویت وی با خبر است و در صورت نیاز امکان شناسایی وی وجود دارد.

۳ـ۴ـ گواهی امضاء مجوز

در این نوع گواهی امضاء، مقام صادر کننده با امضاء خود عملی را مجاز می‌دارد. مثلاً بانکی با صدور گواهی امضاء، برداشت وجه از حساب شماره معینی را اجازه می‌دهد. از همین راه است که برخی از موسسات، دسترسی به صفحات اینترنتی مربوط به خود را کنترل می‌کنند. یعنی تنها به کسانی گواهی مجوز می‌دهند که مبلغ مورد درخواست آنها را پرداخت کرده باشند. در این روش مشتری با وارد کردن نام کاربر، رمز عبور یا رمز ورودی که از طرف موسسه یا شرکت در اختیارش قرار گرفته، به صفحه مورد نظر دسترسی می‌یابد.

در اینجا، هویت دارنده گواهی امضاء، نه تنها اهمیت چندانی ندارد، حتی ممکن است درج آن نامطلوب هم باشد. مثلاً در انتقال الکترونیکی پول نقد، چنانچه بخواهیم الگوی پول سنتی را که معرف میزان معینی از ارزش اقتصادی بدون توجه به منشأ آن است مبنای کار خود قرار دهیم، نباید هویت دارنده گواهی را مد نظر قرار دهیم. در عملیات بانکی

ممکن است گواهی هویت برای افتتاح حساب مورد استفاده قرار گیرد اما گواهی امضاء حاوی اطلاعات و داده‌هایی مشعر بر هویت دارنده گواهی نخواهد بود. برای احراز هویت وی، بانک می‌تواند با مراجعه به بانک‌های اطلاعاتی خود، نام دارنده شماره حساب معین و کلید مربوط به وی را معین نماید.

قراردادن نام یا سایر مشخصات دارنده در گواهی امضاء، عملاً نامطلوب است، زیرا این حالت باعث می‌شود تا با پاره ای از خطرات اضافی مواجه گردند. مثلاً از آنجا که گواهی‌های امضاء در سیستم بانکی جا به جا می‌شوند، لذا همراه داشتن هویت دارنده گواهی، سبب می‌شود تا سایر بانک‌ها از فهرست مشتریان بانک صادر کننده گواهی مجوز آگاهی یابند. مضافاً، قوانین مربوط به حفاظت از حریم خصوصی اشخاص ممکن است چنین روش‌هایی را منع کنند. زیرا بانک صادر کننده گواهی، در عمل بدین وسیله اطلاعات شخصی دارنده را در اختیار اشخاص ثالث می‌گذارد.

هر چند ممکن است استدلال شود که راه‌هایی برای کنترل چنین خطراتی وجود دارد با این حال بهترین شیوه، عدم درج اطلاعات شخصی در گواهی‌های مجوز است. این نکته بیانگر یک اصل بنیادین در گواهی امضاء است، بدین شرح که اطلاعات موجود در گواهی‌ها منحصراً به اندازه رفع ضرورت و نه بیشتر از آن درج می‌گردد. این بدان معنا است که گواهی‌های خاص که برای مصارف معین طراحی شده اند بیشتر از گواهی‌های عمومی که سهل الوصول و چند منظوره هستند، کارایی دارند.

۵ ـ طرف‌های گواهی امضاء

عموماً سه طرف در فرآیند استفاده از گواهی امضاء دخیل و ذی‌نفع هستند اول: **طرف درخواست کننده:** که به گواهی امضاء نیاز دارد و آن را برای بهره‌مندی دیگران عرضه می‌دارد. درخواست کننده معمولاً تمام یا بخشی از اطلاعات موجود در گواهی امضاء را ارائه می‌کند. **دوم: طرف صادر کننده:** که گواهی امضاء را پس از وارد کردن اطلاعات یا کنترل صحت آنها امضاء دیجیتالی می‌کند. **سوم: طرف یا طرف‌های تأیید کننده:** که گواهی امضاء را معتبر شناخته و به آن اعتماد می‌کنند. مثلاً شخص درخواست کننده، مدارک کتبی مبین هویت خویش را به یک بنگاه دولتی می‌دهد. بنگاه که در اینجا صادر کننده است، گواهی

هویتی صادر می‌نماید که هرگاه درخواست کننده بخواهد حساب بانکی باز کند، مورد اعتماد بانک یا مرجع تأیید کننده قرار می‌گیرد. گاه به جای طرف تأیید کننده از اصطلاح طرف اعتماد کننده، استفاده می‌شود که می‌تواند گمراه کننده باشد، زیرا شخص بدواً مندرجات گواهی را تأیید و سپس به آن اعتماد می‌کند.

مثلاً در یک معامله که از طریق کارت‌های اعتباری صورت می‌گیرد، ممکن است گروه زیادی بر محتوای کارت اعتماد کنند، اما مراجع اندکی اعتبار آن را کنترل می‌کنند. پس طرف تأیید کننده شخصی است که ابتدا صحت و اعتبار گواهی را تأیید و متعاقباً بدان اعتماد می‌کند نه شخصی که بدون احراز چنان اعتباری صرفاً بر مبنای آن عمل می‌کند. البته طرف‌های گواهی امضاء بسته به نوع معامله، ممکن است متفاوت باشند اما الگوی عمومی همان است که شرح دادیم.

۶ ـ گواهی امضاهای الکترونیکی (بسته و باز)

در بسیاری از موارد، طرف‌های مرتبط با گواهی امضاء الکترونیکی آن را در چارچوبی وسیع‌تر از روابط قراردادی خود مورد استفاده قرار می‌دهند. به عنوان مثال هر گاه یک مشتری مبادرت به افتتاح حساب بانکی نماید، میان وی و بانک، در خصوص نحوه فعال کردن حساب، قراردادی منعقد می‌شود. در چنین شرایطی وقتی گواهی امضاء دیجیتالی مورد استفاده می‌گیرد، قرارداد موجود میان طرفین می‌تواند شرایط استفاده از گواهی امضاء نظیر مسائل مربوط به مسئولیت در قبال وقایع نامطلوب را پیش بینی و مقرر بدارد. مثال فوق نمونه ای از گواهی امضاء بسته می‌باشد که در آن همه طرف‌های دخیل تحت التزام یک رابطه قراردادی موسع فعالیت می‌کنند.

در مقابل، گواهی امضاء باز نوعی از گواهی امضاء است که یکی از طرف‌های ذی مدخل (معمولاً طرف تأیید کننده) در هیچ‌یک از توافقات راجع به استفاده از گواهی امضاء شرکت ندارد. مثلاً میان پزشک و نهاد حرفه ای که برای وی گواهی عضویت صادر می‌کند، معمولاً رابطه قراردادی وجود دارد، اما بیمار که در صورت جعلی بودن گواهی، در معرض خطر قرار می‌گیرد هیچ رابطه قراردادی برای استفاده از گواهی ندارد. این مثال نوعی از گواهی امضاء است که طرف متکی بر گواهی مجوز ممکن است در معرض خطر باشد اما

هیچ مبنای توافق شده ای برای مطالبه خسارت نداشته باشد.

تأیید کننده گواهی امضاء باز، دشواری‌های متفاوتی پیش روی خود دارد. **اولاً:** نمی‌تواند فوراً اطمینان یابد که گواهی امضاء قابل اعتماد است و یا اینکه گواهی مجوز اصولاً به طور دقیق برای چه منظوری صادر شده است. تأیید کننده ممکن است هویت نهاد صادر کننده گواهی مجوز را بشناسد اما ممکن است از میزان دقت اعمال شده در صدور گواهی مجوز و کاربرد دقیق آن بی اطلاع باشد. **ثانیاً:** چون وی طرف هیچ یک از قراردادهای ناظر بر استفاده از گواهی مجوز نیست، لذا نمی‌تواند از میزان مسئولیت دارنده گواهی مجوز مطلع شود، هر چند ممکن است پاره ای از این مسائل در متن گواهی ذکر شده باشد، به هر حال اطلاع کامل از آنها مستلزم کاوشی توان فرسا است.

هم‌چنین ضرورت دارد که بدانیم آیا مفاد قانونی که در حوزه قضائی محل صدور گواهی مجوز قابلیت اجرائی دارند، در حوزه صلاحیتی محل استفاده گواهی مذکور نیز قابل اعمال هستند تعارض قوانین و رویه‌ها در این زمینه موجب تحدید هر چه بیشتر استفاده از گواهی امضاهای باز خواهد شد. مقامات صادر کننده گواهی مجوز تلاش دارند تا چارچوب‌های متحد الشکلی را تدوین نمایند اما تازگی و ناشناختگی این مفهوم نوظهور نیازمند گذشت زمان قابل توجهی است. مضافاً این برداشت هر روز تقویت می‌گردد که گواهی امضاهای باز برای تجارت الکترونیک ضروری نبوده و گواهی امضاهای بسته به خوبی خلأ آنها را پر خواهند کرد.

۷ ـ اعتماد و اطمینان به امضاها و گواهی امضاهای الکترونیکی

۱ ـ ۷ـ اعتماد و اطمینان به گواهی امضاء

ضروری است میان اعتبار یک امضاء و اعتبار داده‌های سندی که امضاء شده قائل به افتراق شویم. حقیقت این است که امضای درج شده بر روی سند، می‌بایست تا حدودی تضمین کننده صحت هویت محتویات سند باشد اما این بدان معنا نیست که مفاد سند به گونه غیر قابل انکاری صحیح هستند، لذا همیشه امکان جعل داده‌های موجود در سند وجود دارد. به علاوه ممکن است ساز و کارهای اجرائی صدور گواهی امضاء مختل شده باشد.

در اکثر گواهی‌های هویت، کلید تأیید امضاء با نام شخص یا شیء پیوند می‌خورد. این کار با ایجاد یک نام و یا رشته ای از حروف و اعداد انجام می‌شود و متضمن نواقص بسیاری است که اگر نام انتخاب شده منحصر به فرد نباشد، تضمینی وجود ندارد که اگر گواهی معتبر باشد، لزوماً کلید امضاء مربوط نیز معتبر خواهد بود، زیرا ممکن است این کلید امضاء متعلق به نام مشابه دیگری باشد. در عمل صادر کننده و تأیید کننده گواهی امضاء از مجموعه اسامی شناخته شده ای استفاده می‌کنند اما تضمینی وجود ندارد که این اسامی مربوط به همان اشخاص مورد نظر باشند. به عنوان مثال جان اسمیتی که صادرکننده گواهی امضاء می‌شناسد ممکن است با جان اسمیتی که تأیید کننده می‌شناسد متفاوت باشد. حتی بدتر از آن، ممکن است اطلاعات اضافی نظیر نام و تاریخ تولدی که صادر کننده برای ساختن یک اسم منحصر به فرد از آن بهره می‌برد، در اختیار تأیید کننده نباشد، در نتیجه وقتی تأیید کننده، برای تأیید امضاء جان اسمیت درخواست گواهی می‌کند، تعدادی از گواهی امضاهای قابل اعتماد را دریافت خواهد کرد که به هیچ‌کدام نمی‌تواند اعتماد کند، زیرا نمی‌داند کدام یک را مورد استفاده قرار دهد.

اگر از گواهی امضایی که بیش از همه احتمال صحتش را می‌دهد، استفاده کند، در فرایند مستحکم رمز نگاری، نوعی گمانه زنی انسانی ذی مدخل می‌گردد. گواهی امضاهایی که امضاء را به داده‌های زیست شناختی مرتبط می‌نمایند، بسیاری از این مشکلات را حل خواهند نمود اما توسعه نیافتگی زیر ساخت‌های ایجاد چنین امضاهایی دورنمای استفاده وسیع از آنها را در مقطع کنونی غیرملموس می‌سازد.

به همین جهت احراز هویت دشوارتر از آن است که در اولین نگاه به نظر می‌آید اما تحلیل دقیق تر نشان می‌دهد که اصولاً احراز هویت در بسیاری از مواقعی که ما انتظار داریم مورد نیاز نیست، هر چند بخشی از کارکرد احراز هویت بر عهده گواهی امضاء است لیکن چنین پدیده ای هرگز نمی‌تواند به تنهایی از پس این کار برآید.

به علاوه اگر با کلید مجهول المالکی روبه رو شویم باید به سایر زیر ساخت‌های گواهی امضاء دسترسی یابیم تا بتوانیم مالکش را پیدا کنیم اما هم اینکه چنین عملی را انجام دادیم نه تنها باید به آنچه که نزدیک و در دسترس ما است، اعتماد کنیم بلکه باید به

طراحی، عملکرد و نحوه فعالیت چنین زیر ساختی نیز اعتماد داشته باشیم. حرکت از سمت اعتماد به مالک به سوی اعتماد به یک زیر ساخت بزرگ، گام بسیار بلندی است که آسیب‌های امنیتی جدیدی را مطرح می‌سازد. بنابراین جای تعجب نیست که متخصصین به طور جزئی برنامه‌هایی را بررسی نمایند که بتوان آنها را چنان مهندسی نمود که نیاز به چنین زیر ساخت‌های حجیمی از بین برود.

در حال حاضر باوری در حال قوت گرفتن است مبنی بر اینکه بسیاری از برنامه‌های مربوط به امضاهای دیجیتالی می‌توانند با موفقیت به گونه‌ای طراحی شوند که به زیر ساخت‌های موجود نیازی نباشد.

۲ ـ۷ ـ اعتماد و اطمینان در کلید رمزهای گواهی امضاء

جذابیت مراجع گواهی کننده و اشخاص ثالث ذی‌نفوذ در صدور گواهی امضاهای الکترونیکی، باعث گردیده تا از یاد ببریم که امضاهای دیجیتالی دربرگیرنده چیزی بیش از گواهی امضاء هستند. گواهی امضاها فقط اعتماد و اطمینان در خصوص اجزای عمومی جفت کلید رمز را فراهم می‌آورند و اطمینانی در مورد سایر حلقه‌های این رشته، یعنی کلید رمز امضاء، ایجاد نمی کنند. با وجود مراجع گواهی کننده معتبر، ممکن است امضاء هیچ ارزشی نداشته باشد چراکه تضمینی درباره محیط مجازی که امضاء در آن ساخته، ذخیره و استفاده شده است، وجود ندارد.

برای اعتماد به امضاء دیجیتالی نه تنها باید مالکیت استفاده کننده بر کلید تأیید امضاء احراز شود بلکه باید بر استفاده انحصاری وی از کلید رمز امضاء نیز آگاه باشیم. باید یادآور شد که در اینجا نگرانی‌هایی وجود دارد. به عنوان مثال، ممکن است مالک کلید رمز امضاء با بی‌دقتی آن را برای دیگران افشاء کند یا رایانه وی از امنیت لازم برخوردار نباشد یا کسی کلید رمز را سرقت کند و نیز ممکن است پس از اینکه کاربر کلید رمز را فعال کرد، کسی بتواند به رایانه وی دسترسی فیزیکی پیدا کند و از کلید استفاده نماید یا اینکه خود کاربر چیزی را امضاء کند اما بعد پشیمان شود و با انتشار کلید رمز امضاء خود عملاً آن را از حیز انتفاع ساقط نماید.

تفکیک این مورد از سرقت کلید رمزهای امضاء بدون تقصیر مال باخته ناممکن است

و نباید کاربر را به خاطر آنچه توان جلوگیری از آن را ندارد، تنبیه نمود. امضاهای دیجیتالی ممکن است بدون دسترسی به کلید رمزهای امضاء هم قابل جعل باشند. ترکیب همین الزامات چالش‌های عظیمی را فرا روی وی قرار می‌دهد که بسیاری باور دارند تفوق بر آنها ورای سطح فناوری‌های موجود است. ساز و کارهای نرم افزار محوری برای ذخیره کلیدهای رمز، ناتوان از تأمین سطح امنیتی مورد نیاز هستند و این بدان معنا است که حفاظت‌های سخت افزاری نیز برای کسب اطمینان از اصالت امضاهای الکترونیکی ضروری است.

کارت‌های هوشمند گرچه یکی از گزینه‌های موجود هستند اما از استحکام لازم برای کلید گذاری برخوردار نبوده و در برابر حملاتی که ممکن است منجر به افشای کلید رمز شود نیز مصونیت ندارند. اگر کلید رمز در جای دیگری تولید و بعداً به کارت هوشمند منتقل گردد، این حقیقت که داده‌ها در دو جا وجود دارند، امکان کپی برداری و جعل را افزایش می‌دهد، در یک موقعیت ایده‌آل ممکن است کلید رمز را در خود کارت قرار داد و داده‌هایی که قرار است امضاء شوند بعداً به همان کارت وارد شده و امضاء شوند، بدین ترتیب کلید رمز هرگز از کارت جدا نخواهد شد و این داده‌ها هستند که برای امضاء به کارت اضافه می‌شوند.

از این طریق حتی دارنده کارت نیز از کلید رمز آگاه نمی گردد. متاسفانه این بدان معناست که پردازشگر موجود در کارت باید به قدری قوی باشد که بتواند حجم گسترده‌ای از اطلاعات ورودی را بدون تاخیر قابل ملاحظه، ذخیره سازی، پردازش و امضاء نماید که این امکان فعلا وجود ندارد. مشکل دیگر کارت‌های هوشمند و سایر جایگزین‌های پیشنهادی این است که توجهی که نسبت به مسائل مربوط به مسئولیت و قانونگذاری راجع به مراجع گواهی کننده مبذول گردیده، درباره سایر گزینه‌ها اعمال نشده است.

این امر موجب شگفتی است، چرا که خطرات نهفته در ساز و کارهای جایگزین، بیشتر شده و غلبه بر آنها دشوارتر است. ممانعت کاربران از رجوع از امضاء خود، واقعیت و نیاز غیر قابل انکاری است که به سختی بتوان تا مدتی پاسخی برای آن یافت. در نتیجه برنامه‌های عملی سازنده امضاهای دیجیتالی باید با وجود امکان رجوع از امضاء فعال گردند. فقدان

ویژگی‌هایی نظیر قابل رجوع بودن، به معنی ناکارآمدی امضاهای دیجیتالی نیست. کارت‌های اعتباری هم به کاربران اجازه می‌دهند تا موارد خاصی را در صورت حساب ماهیانه نپذیرند اما این به معنای عدم کارآیی کارت‌های اعتباری نیست. به علاوه کلید اتومبیل و منزل هم بدون اینکه حامل مفهوم عدم قابلیت رجوع باشند، به عنوان ابزارهای کنترل و دسترسی کاربرد بسیار زیادی دارند.

۳ـ۷ـ اعتماد و اطمینان نسبت به امضاء

در امضاء سنتی، شخص سند را می‌بیند و با خودکار آن را امضاء می‌کند اما این فرایند در امضاء دیجیتالی پیچیده تر است. معمولاً کارتی هوشمند به ورودی سخت افزاری که متصل به کامپیوتر است، داخل شده و کلید رمز داخل آن به سندی که روی نمایشگر است منتقل گردیده و آن را امضاء می‌کند. اما دارنده کلید می‌بایست از کجا بداند که امضاء او ذیل همان سندی است که روی نمایشگر درج شده نه بر روی سندی دیگر ؟ یا دارنده کلید رمز از کجا می‌تواند مطمئن باشد که کلید رمز به گونه‌ای در جایی ذخیره نشده که امکان جعل آن را برای سایر کاربران همان رایانه فراهم آورد و اگر در نقطه پایانی، یک قرارداد فروش می‌بایست گواهی گردد، مشتری یا تاجر چگونه می‌بایست بداند که پایانه کامپیوتر به نحوی طراحی نشده که یکی از آنها یا هر دوی آنها را فریب دهد ؟

فرایند امضاء دیجیتالی در مقایسه با امضاهای سنتی دست نویس، تبیین دو شعار حصول اطمینان از صحت گواهی امضاء و دقت آن را نیز دشوار می‌سازد. اگر این موضوع در دادگاه طرح شود اثبات اعتبار فرایند امضای دیجیتالی کار آسانی نخواهد بود. چک کردن امضاء مندرج بر یک سند، بخش مهمی از فرایند تأیید امضاء است و این بدان معناست که پایانه‌های تأیید امضاء، نیاز به دسترسی به تعدادی از کلید تأیید امضاء دارند.

همان گونه که پیشتر نیز گفتیم همواره در انتهای مجموعه گواهی‌ها، کلیدی وجود دارد که نمی‌تواند امضاء شود و قابلیت اعتماد به آن کلید می‌بایست از راه دیگری احراز گردد. بنابراین تمامی ایستگاه‌های تأیید امضاء، عموماً شامل یک کلید مورد اعتماد هستند که برای کامل کردن آخرین حلقه ارتباط در سلسله گواهی‌ها مورد استفاده قرار می‌گیرد.

مثلاً ممکن است یک پایانه فروش، کلید تأیید امضائی را برای کارت اعتباری (همانند

مستر کارت) و تمامی کارت‌های اعتباری که این شرکت شناسایی نموده در نظر بگیرد. می‌توان این کلیدها را مستقیماً از خود شرکت تهیه نمود و در نتیجه به اصالت آنها اطمینان داشت اما از کجا باید مطمئن بود که ارزش رایانه ای کلید پس از ساخت پایانه تغییر نکرده باشد ؟

سازنده پایانه می‌تواند این کلیدها را امضاء و در پایانه، کلید تأیید امضائی نصب نماید که برای تأیید امضاء به کار رود. اما اکنون نیازمند اطلاع از عدم تغییر کلید تأیید امضاء هستیم. این بدین معناست که می‌بایست حداقل یک کلید تأیید در اختیار باشد که مطمئن باشیم از زمان ساخت تغییر نکرده و مبنای اعتماد در پایانه قرار گرفته است. از آنجا که باید قویا از این امر مطمئن بود، لذا لازم است کلید به گونه‌ای وارد پایانه گردد که تغییر آن به راحتی صورت نگیرد. حتی اگر به نحوه نگهداری کلید تأیید توسط پایانه مطمئن باشیم، موارد بسیار زیادی هم وجود دارد که باید در خصوص آنها اطمینان حاصل نمود. چنانکه نشان دادیم، باید مطمئن شد، آنچه که بر روی صفحه نمایشگر درج گردیده واقعاً همان سندی است که امضاء شده و کلید رمزهای امضاء به هیچ وجه تحریف نشده اند. پس امنیت پایانه علاوه بر گواهی امضاها به عوامل دیگری نیز بستگی دارد به ویژه باید مطمئن باشیم که نرم افزار و سخت افزار مربوطه دقیقاً و منحصراً همان چیزی را انجام می‌دهند که ما از آنها انتظار داریم.

هم‌چنین باید بدانیم که سخت افزار رایانه، به ویژه در زمان امضاء به وسیله شخص مذکور، به طور صحیح فعال شده و نرم افزار آن مجموعه مورد تأیید بوده که جزء جزء آن به نحو قابل اعتمادی طراحی و پس از ساخت تغییر داده نشده است. در مقایسه با گواهی امضاهای سنتی، گواهی امضاهای دیجیتالی فرایند ابهام آمیز و پیچیده تری دارند که اعتماد به آنها را دست کم در سطح مصرف کنندگان شخصی مشکل می‌کند مگر اینکه نهاد ویژه‌ای، خطرات ناشی از چنین امضاهایی را تحت پوشش بیمه ای خود قرار دهد.

۸ ـ امضاهای دیجیتالی و گواهی امضاها در تجارت الکترونیکی

توسعه تجارت الکترونیک به مولفه‌های زیادی نیازمند است که یکی از آنها امنیت زیر ساخت‌ها است. تأمین ایمنی زیر ساخت‌ها گرچه شرط لازم است، ولی به هیچ وجه شرط

کافی نیست. با این وجود، در اینجا تنها همین جنبه مورد مطالعه قرار گرفته است و تذکر این نکته ضروری است که ایمنی تنها یکی از عوامل لازم جهت توسعه تجارت الکترونیک می‌باشد.

۱ ـ ۸ ـ نگرانی‌ها و انتظارات مصرف کنندگان

نگرش مصرف کنندگان نسبت به ایمنی در تجارت الکترونیک در سطح کلان، به وسیله پوشش رسانه ای مربوط به این موضوع شکل می‌گیرد. انجام معاملات الکترونیکی محتاج به شبکه‌های بزرگی نظیر اینترنت است. در این قسمت ترس و نگرانی مصرف کنندگان از معاملات الکترونیکی چشمگیر است. حقیقت یاد شده، مصرف کنندگان را با این تصور مواجه می‌سازد که در صورت استفاده از زیر ساخت‌های موجود برای معاملات الکترونیکی با خطرات گسترده ای رو به رو خواهند شد اما واقعیت چیز دیگری است. از مجموع میلیاردها معامله اینترنتی که هر روز صورت می‌گیرد، تنها بخش کوچکی با مشکلات امنیتی مواجه می‌شوند. هم اکنون در عمل مهم‌ترین خطر معاملات الکترونیکی، ریسک ناشی از اعتمادی است که می‌توان به طرف دیگر معامله داشت. در مقایسه باید گفت خطرات ناشی از مداخله زیر ساخت‌های واسط ناچیز است و می‌توان با استفاده از پروتکل‌های رمز نگاری نوین که بر مبنای **نهایت به نهایت** عمل می‌کنند از میان برداشته شود. تجار در استفاده از کارتهای اعتباری، نگرانی زیادی نسبت به امضاء طرف دیگر ندارند چرا که در انجام یک معامله، بیشتر به کارت اعتماد می‌کنند تا به هویت دارنده آن. هرچند مشتری در مقابل ضرر مالی تضمین مناسبی اخذ می‌کند اما به هر حال ترجیح می‌دهد با شرکتی که آن را می‌شناسد، معامله نماید تا اینکه شرکتی دروغین خود را به جای شرکت شناخته شده، معرفی نماید.

یکی از ویژگی‌های مهم امضاهای دیجیتالی این است که روابط مبتنی بر اعتماد را حفظ می‌کند اما قادر نیست در جایی که اعتمادی وجود ندارد اعتماد را خلق کند. مثلاً اگر به سازمان نظام پزشکی انگلستان اعتماد داشته باشیم و آن مرجع نیز مطمئن باشد که فلان فرد پزشک است، بنابراین می‌توان آسوده خاطر بود که آن فرد پزشک است. البته اعتماد بر مبنای امضاء دیجیتالی نظام پزشکی چیز تازه ای نیست بلکه ابقای رابطه مبتنی

بر حسن ظن موجود در یک چارچوب گسترده تر است.

واقعیت این است که در عمل، اعتمادها اغلب در سطح محلی شکل می‌گیرند. دلیل این امر نیز واضح است چراکه یکی از خصلت‌های روابط انسانی اعتماد است و اعتماد به اشخاص ناشناس معقول نمی‌باشد. بنابراین در حالیکه مراجع تولید استاندارد و دولت‌ها تمرکز خود را بر روی گواهی‌های هرمی، به صورت از بالا به پایین، معطوف می‌دارند، کاربران خصوصی بیشتر از آنکه به رمز نگاری‌های با کلید عمومی تمایل نشان دهند، تمایل دارند تا امضاء همکاران و دوستانشان را در فایل‌های خود ذخیره نمایند. به همین دلیل است که در تجارت نیز گواهی امضاهای بسته مورد اعتماد قرار می‌گیرند.

هر چند ممکن است امضاهای دیجیتالی، عرضه کننده الگوهای جدیدی از اعتماد باشند، لیکن تجربه و سایر فناوری‌ها نشان می‌دهد که کاربری سریع امضاهای الکترونیکی در افزایش روابط مبتنی بر اعتماد موجود و تلاش در جهت افزایش تأثیر و کارآمدی آنها موثر بوده است.

۲ـ ۸ ـ طرف‌های معتمد

برای درک بهتر عناصر ذی‌مدخل در یک معامله متضمن امضاء دیجیتالی، جا دارد تا روند انجام آن را شرح دهیم. اگر یک مشتری کارت اعتباری از صادر کننده کارت درخواست نماید تا پیش از تصمیم راجع به اعطا یا عدم اعطای کارت نکاتی را کنترل کند. به این ترتیب، هرگاه کارت صادر شود از مشتری انتظار می‌رود تا آن را امضاء کند اما شرکت در پی تأیید مستقل انتساب حقیقی امضاء به مشتری نیست.

این امر در مورد امضاهای سنتی صورت نمی‌پذیرد و دلیل روشنی در دست نیست تا در مورد امضاهای دیجیتالی نیز اعمال شود. مهم این است که رابطه مشتری و شرکت، تابع یک رابطه دو سویه و تحت حاکمیت قراردادی قرار گیرد تا این رابطه، شرایط استفاده از کارت و امضاهای دیجیتالی مربوطه را تشریح کند، به همین ترتیب، شرکت صادر کننده کارت‌های اعتباری، قراردادی دو جانبه با تجار منعقد خواهند نمود که مبین شرایط پرداخت مبالغ خرج شده با این کارت‌ها است. در این قرارداد می‌توان نحوه استفاده از امضاء دیجیتالی را نیز معین نمود. بنابراین مشاهده می‌نمائیم که بجای یک رابطه باز سه طرفه،

اعتماد به امضاء دیجیتالی بر مبنای روابط بسته و دو جانبه شکل می‌گیرد. از آنجا که در این نوع معاملات، تمامی روابط می‌تواند تحت اراده شرکت صادر کننده کارت اعتباری یا بانک‌های ذی مدخل قرار گیرد، لذا نیازی به زیر ساخت‌هایی نظیر مراجع گواهی کننده احساس نمی‌شود.در اینجا نقش عمده شرکت تولیدکننده کارت اعتباری، دادن تضمین برای تعهدات مالی هر یک از تجار و مصرف کننده در مقابل یکدیگر است.

یکی از راه‌های اعطای چنین تضمینی، استفاده از یک گواهی امضاء الکترونیکی برای امضاهای هر دو طرف می‌باشد. وقتی دو طرف به امضاء الکترونیکی یکدیگر اعتماد کنند، می‌توانند اطمینان داشته باشند که منافع مالی شان با گواهی امضاء صادره از طرف شرکت صادر کننده کارت اعتباری تضمین خواهد شد. این شیوه ای است که به وسیله آن گواهی امضاء برای دادن تضمین مورد استفاده قرار می‌گیرد.

۳ ـ ۸ ـ تضمینات مالی

اگر قرار به توسعه تجارت الکترونیکی باشد، شرکت‌های صادر کننده کارت‌های اعتباری باید گواهی امضاهایی صادر نمایند که شکل نوینی از تضمینات را در اختیار هر دو طرف (تاجر و مشتری) بگذارد تا خرید کردن، با استفاده از همان مزایا و تضمینات قبلی امکان پذیر گردد. هر چند ظاهر این نوع ارتباط، رابطه سه جانبه به نظر می‌رسد، لیکن در حقیقت این نوع ارتباط، از دو رابطه دو جانبه مجزا و بسته تشکیل شده است. به علاوه در این نوع ارتباط، شخص ثالث، امضاء دیجیتالی را در مفهوم هویتی آن گواهی نمی‌کند بلکه در عوض از آنها برای قادر ساختن دارندگان کلید مبنی بر اعطای تضمینات گواهی کننده امضاء بهره می‌برد.

باید توجه داشت که امضاهای دیجیتالی که در اینجا به کار می‌رود فرع بر رابطه مبتنی بر اعتماد میان طرفین است. امضاهای دیجیتالی آشکارا برای تحقق این روابط ضروری نیستند چرا که دقیقا مشتمل بر همان ساختارهایی هستند که در معاملات با کارتهای اعتباری مورد استفاده قرار می‌گیرند بنابراین استفاده از امضاهای دیجیتالی بیشتر متوجه فعال سازی و گسترش روابط مبتنی بر اعتماد طرفینی است تا معرفی چیزی که کاملاً نو و تازه باشد.

۴ـ ۸ ـ تعهدات حرفه ای و خدماتی

تعدادی از نهادهای حرفه ای هم اینک سعی دارند تا برای اعضاء خود گواهی امضاء الکترونیکی عضویت صادر نمایند. به عنوان مثال به برخی از این نهادهای مهم که تمایل به چنین امری دارند، نظیر کانون‌های حرفه ای پزشکی، حقوقی، حسابداری و حرف مهندسی رسمی می‌توان اشاره نمود. در این موارد، گواهی امضاء به دارنده آن حق می‌دهد تا به عنوان عضو جامعه حرفه ای مربوطه فعالیت نماید. این نوع گواهی امضاء حتی می‌تواند برای حمایت از انواع تعهداتی که سازمان‌های بازرگانی عرضه می‌دارند، مورد استفاده قرار گیرد.

جوامع تجاری اغلب عضو سازمان‌هایی هستند که فعالیت آنها به منظور جلب اطمینان عمومی قاعده مند می‌باشد نظیر اتحادیه آژانس‌های مسافرتی بریتانیا. چنین مؤسساتی از گواهی امضاء الکترونیکی به منظور تسهیل مبادلات تجاری خود سود می‌برند. سازمان‌هایی که استفاده از گواهی‌های عضویت را مد نظر قرار می‌دهند، می‌توانند شخصاً واحد مرجع گواهی امضاء را فعال کنند یا به طور جایگزین از خدمات تأمین کنندگان گواهی امضاء استفاده نمایند. باید توجه داشت که گواهی‌ها برای اعطای نوعی مجوز به دارندگان آن اعطا می‌شوند. نظیر مجوز فعالیت حرفه‌ای به عنوان پزشک یا وکیل. در چنین مواردی مرجع گواهی کننده، نهاد حرفه‌ای است که فعالیت یا شغل مورد بحث را قاعده مند می‌سازد.

بنابراین باز هم از امضاهای دیجیتالی برای نمایندگی دسته ای از ارتباطات مبتنی بر اعتماد موجود در شکل الکترونیکی استفاده می‌شود.

۵ ـ ۸ ـ گواهی‌های هویت

دولت‌ها همواره با بهره گیری از اسنادی نظیر شناسنامه، گذرنامه و گواهینامه رانندگی سعی در شناسایی شهروندان خود دارند، لذا چنانچه دولت‌ها انتظار داشته باشند که این نقش سنتی را با صدور گواهی‌های هویت الکترونیکی به دنیای جدید نیز گسترش دهند، انتظار یاد شده واقع بینانه خواهد بود. مثلاً گواهی‌هایی که ممکن است در قالب کارت‌های هوشمند صادر گردند، قادرند جایگزین گذرنامه شده و جابجایی مسافر و کنترل مرزها را آسان نمایند. به شیوه نا صحیح، اغلب این‌گونه فرض می‌شود که به منظور استقرار تجارت الکترونیکی، وجود گواهی هویت نیازی مبرم محسوب می‌شود. با این وجود، بخش اعظم

تجارت الکترونیکی مربوط به نقل و انتقال الکترونیکی پول است که به شکل مستقیم هیچ‌گونه وابستگی به اطلاعات هویتی ندارد. آنچه که باید گواهی شود، مجوز نقل و انتقال وجوه در میان حساب‌ها است. هر چند موسسات مالی، اطلاعات هویتی صاحبان حساب مفروض را در اختیار دارند، لیکن فرایند عملی مداخله در یک معامله الکترونیکی مستلزم دسترسی به چنین اطلاعات نمی‌باشند.

باید توجه داشت که این بدان معنا نیست که اطلاعات هویتی در تجارت الکترونیکی اهمیتی ندارد. مثلاً مصرف کنندگان مایلند پیش از انجام و پیگیری معاملات از نام شرکت‌های طرف معامله و هویت آنها آگاه باشند. به علاوه عامل تعیین هویت در اینجا زمانی ارزش دارد که همراه خود دسته بزرگتری از مشخصه‌ها را به همراه آورد، نظیر شهرت تجاری و اعتباری که به شدت مورد علاقه و توجه مصرف کنندگان است.

۶ ـ ۸ ـ ویژگی‌های گواهی امضاهای دیجیتالی

مثال‌های فوق در خصوص استفاده از امضاهای دیجیتالی ویژگی‌های مشترکی به شرح زیر دارند.

اولاً: در هر یک از این برنامه‌ها، امضاء دیجیتالی برای حمایت از روابط اعتماد آمیز قبلی به کار می‌رود. این روابط قبلاً وجود داشته و تازه نیستند. ارزش امضاء دیجیتالی گسترش این روابط به فضای مجازی یا بهسازی روش‌های استفاده و اجرای آنها است.

ثانیاً: گواهی حاوی کلید تأیید امضاء، به دارنده کلید اجازه می‌دهد تا تعهد معینی را پذیرفته یا خدمت خاصی را دریافت نماید. از نظر مالی، اجازه تجارت تحت شرایط مقرر توسط شرکت صادر کننده گواهی و از نظر حرفه ای، اجازه ارائه خدمتی که توسط سازمان گواهی کننده نظام مند شده است و از نظر هویتی، اجازه دریافت مزایایی که دولت به شهروندان خود اعطا می‌کند، را به دارنده آن می‌دهد.

ثالثاً: از همه مهم تر و در همه موارد، بنگاه گواهی کننده چیزی را تأمین می‌کند که طرف‌های اعتماد کننده آن را ارزشمند می‌شمارند. از نقطه نظر مالی، نقش صادر کننده گواهی، مشابه نقش شرکت‌های صادر کننده کارت‌های اعتباری در دادن تضمین به هر طرف که در صورت قصور طرف دیگر تعهدات وی ایفا خواهد شد، می‌باشد.

در مثال حرفه ای و خدماتی سازمان صادر کننده گواهی، حیثیت حرفه ای خود را پشتیبان نام عضو نهاد حرفه ای مربوط قرار می‌دهد و ممکن است حسن انجام کار عضو خود را با تعهد به جبران خسارت در صورت وقوع زیان بیمه نماید. در مثال هویتی، گواهی می‌تواند توسط یک بنگاه دولتی صادر و توسط بنگاه دولتی دیگر مورد استفاده قرار گیرد. اگر دولت دیگری بخواهد در زمان کنترل مرزی به گذرنامه ای اعتماد کند، می‌تواند مطمئن شود که دارنده گذرنامه، شهروند کشور معینی است که با کشور متبوع کنترل کننده وی، معاهده استرداد مجرمین را امضاء نموده یا ننموده است و از این طریق، کشور پذیرنده می‌تواند مطمئن شود که حتی پس از عبور فرد خاطی از مرز نیز قادر است وی را به خاطر اعمال غیر قانونی که انجام داده، تعقیب نموده و مسئول شناسد.

در عمل ماموران کنترل مرزی نمی‌توانند به این روش اطمینان کامل داشته باشند، زیرا ممکن است گذرنامه دیجیتالی جعلی باشد. به علاوه ممکن است شهروند مزبور در کشور متبوعش اقامت نداشته باشد و در هر حال بسیار بعید است که کشور صادر کننده گذرنامه دیجیتالی، در صورتی که گذرنامه اشتباها صادر شده باشد، حق رجوعی را برای طرف مقابل قائل گردد. با این وجود، رویه معمول نشان می‌دهد که اکثر گذرنامه‌ها معتبر و بیشتر دولت‌ها در راستای معاضدت قضایی با یکدیگر همکاری می‌کنند و این بدان معنا است که آنان می‌توانند با وجود فقدان تضمینات مطلق و خدشه ناپذیر به صحت چنین اسنادی اعتماد نمایند.

هم‌چنین در جایی که درخواست کننده و اعتماد کننده یکسان اند، گذرنامه دیجیتالی می‌تواند مثالی از گواهی امضاء الکترونیکی تلقی گردد چرا که شخص ثالث می‌تواند برای مراجعت به کشور خود به منظور پذیرفته شدن به عنوان یک شهروند، به اتکای همین گذرنامه عمل کند. در مثال‌های یاد شده، اعتماد کنندگان از صادر کنندگان گواهی مزایای نسبتا متفاوتی دریافت می‌دارند. در مثال نخست، آنان تضمینی قوی به دست می‌آورند که معاملات متضمن امضاهای الکترونیکی از هر گونه خطر مصون بمانند.

در مثال دوم آنان مطمئن اند با کسی معامله می‌کنند که مورد پشتیبانی یک سازمان تجاری یا حرفه ای قرار دارد و احتمالاً در قبال خسارات وارده غرامت وی را پرداخت خواهند

نمود. در مثال سوم یعنی گذرنامه دیجیتالی، هر چند این احتمال وجود ندارد که در صورت اشتباه در صدور گذرنامه، خسارت دولت دیگر جبران شود، لیکن گذرنامه یاد شده به احتمال قوی معتبر است و دولت زیان دیده به طور متعارف می‌تواند انتظار داشته باشد که با درخواست استرداد مجرمین وی، موافقت خواهد شد. بنابراین در این مورد ارزش گواهی امضاء به عدم پرداخت غرامت در مقابل موارد نادر، ناکارآمدی آن نیست بلکه اعتبار آن به انتظاراتی باز می‌گردد که صحت بخش عمده ای از این گواهی‌ها را ایجاد می‌کند. بنابراین هر چند گواهی‌های معدودی ممکن است صحیح نباشند، اما چیزی از ارزش کلی آنها نمی‌کاهد، مشروط بر اینکه درصد بالایی از آنها درست عمل شده باشند. پس ارزش گواهی‌ها به صحت مطلقشان نیست، بلکه به احتمال بالای صحت آنها است.

۹ ـ مراجع ثالث گواهی کننده امضاء دیجیتالی:

اگر تصور نمائیم که مراجع ثالث گواهی کننده بخواهند از نظر تجاری موفقیتی به دست آورند الزاماً در اختصاص نام‌ها به دارندگان کلید، تا آن حد که در اینجا مورد بحث است، می‌بایست خدمت یا ارزش افزوده ای را ایجاد یا ارائه نمایند، تصور یاد شده، تصوری اشتباه است. با این وجود مسلم نیست که چنین خدمتی عملاً مورد نیاز تجار باشد چرا که تجارت بدون آن هم برای مدت مدیدی به خوبی امکان پذیر است.

موسسات مالی حامی تجارت مدرن، هم اکنون نیز طرق قابل قبولی برای شناسایی مشتریان خود دارند و بعید است انجام این کار را به یک شخص خارجی سپرده و برای ارائه آن خدمات وجهی پرداخت نمایند. شرکت‌های عرضه کننده گواهی امضاهای مستقل، بدون آنکه خدمت جدیدی ارائه دهند، خود یک طرف معتمد اضافی در شبکه روابط مبتنی بر اعتمادها را به وجود می‌آورند. در عمل دشوار است این خدمت را که تجارت وابسته به آن است، امر مهمی بدانیم.

نگرانی دیگر این است که توجه به این گواهی ها از دیدگاه فنی و حقوقی تردیدهایی را در خصوص استفاده از امضاهای دیجیتالی ایجاد کند. به همین سبب برای سازمانها مشکل است تا در زمینه‌هایی که احتمال تأثیر گذاری برنامه‌های سود زا بیشتر از امضاهای دیجیتالی باشد، سرمایه گذاری نمایند. در نتیجه، تمرکز بر گواهی امضاهای دیجیتالی

هویتی بیش از آنکه باعث توسعه بخش تجارت الکترونیکی گردد، مانع آن خواهد بود.

۱۰ ـ استانداردهای فنی برای امضاهای دیجیتالی و گواهی امضاهای الکترونیکی

چنانچه ساز و کارهای متعدد و متفاوتی برای ساخت امضاهای دیجیتالی به کار رود، پراکندگی چشمگیر و مشکلات ناشی از فعل و انفعالات متقابل این ساز و کارها بروز خواهند نمود. با این وجود، تلاش در جهت استاندارد سازی و توافق بر روی الگوریتم‌ها یا ساز و کارهای ویژه، متضمن این خطر خواهد بود که ممکن است سرمایه گذاری وسیع بر یک راه حل خاص انجام شود که بعداً ضعف‌های جدی آن آشکار گردد.

به همین سبب یادآوری این نکته مهم است که هر گونه قانونگذاری درباره امضاهای دیجیتالی نمی‌بایست به فناوری خاصی که برای ساخت امضاء دیجیتالی لازم است، وابسته گردد. اگر چنین تفکیکی حفظ شود، هر گاه غیر موثر بودن فناوری بعداً معلوم شود، ممکن است بدون خدشه به مفاد قانون مربوطه با خلق فناوری دیگر، نقض یاد شده ترمیم گردد. این امر در مورد برنامه‌هایی که باید نوشته شوند نیز صادق است و بدین ترتیب وابستگی به ساز و کارهای خاص از میان می‌رود.

اهمیت پرهیز از چنین وابستگی فنی توسط یک واقعه جدید به خوبی نشان داده شده است. الگوریتم MD5که به طور گسترده در ایجاد امضاهای دیجیتالی مورد استفاده قرار گرفته بود، دارای نقایصی تشخیص داده شد که گاه امکان جعل امضاء را فراهم می‌نمود. در نتیجه، از این به بعد الگوریتم یاد شده توصیه نمی‌شود. اما اگر الگوریتم فوق الذکر به عنوان یک استاندارد الزامی تعیین شده بود، بنیان کلی گواهی امضاهای دیجیتالی فرو می‌ریخت. بنابراین مهم است که برنامه‌های متضمن امضاهای دیجیتالی، به کاربران خود اختیار انتخاب و انجام کارهای متعددی را برای ساخت امضاء دیجیتالی بدهند. اگر تنها یکی از این ساز و کارها وجود داشته و بعدها معیوب از کار در آید، برنامه یاد شده کلا ناکارآمد خواهد شد.

با این وجود، اگر تعداد کافی از گزینه‌ها در دسترس باشد، می‌توان یکی از آنها را برای استفاده فوری به کار بست. اجتناب از الزام به استفاده از ساز و کارهای خاص امضاء

دیجیتالی در نگاه اول ممکن است به بخش بندی و تقسیم بازار بیانجامد، با این وجود در عمل طراحی الگوریتم‌ها با کیفیتی که آزادانه در دسترس عموم قرار گیرند بسیار دشوار است. جمله فوق بدین معنا است که تعداد نسبتا کمی از الگوریتم‌ها رواج خواهند یافت.

دلیل دیگری که برای اجتناب از الگوریتم‌های تحمیلی وجود دارد این است که برنامه‌های مختلف، اغلب نیازمند ساز و کارهای متفاوتی هستند. برای مثال، اعمال فرایند ساخت یک امضاء دیجیتالی در یک نرم افزار یا کارت هوشمند، متضمن ملاحظات متفاوتی است که همین موضوع می‌تواند به استفاده از الگوریتم‌های متفاوت بیانجامد.

بنابراین در سطح الگوریتمی، باید از وسوسه ایجاد یک استاندارد مبتنی بر یک یا چند الگوریتم معدود پرهیز نمود. تجربه نشان داده است که خطرات ناشی از پراکندگی سرمایه‌گذاری، احتمال وقوع چندانی ندارد و مزایای این تنوع بخشی آن‌قدر زیاد است که گوناگونی راه حل‌ها را به صورت یک الزام مطرح می‌سازد. هرچند باید از استاندارد سازی الگوریتم‌ها دوری جست، لیکن الزاماتی وجود دارد که در هر الگوریتمی که برای ساخت امضاء دیجیتالی به کار گرفته می‌شود باید از آنها تبعیت کند. برای امضاهای دیجیتالی باز، بسیار مهم است که همه طرف‌های استفاده کننده از امضای باز، الگوریتم مورد استفاده آن را بدانند و این بدان معنا است که الگوریتم مذکور باید به شکلی آزادانه و قابل دسترس انتشار یابد. هر چند عدم وجود مبلغی تحت عنوان حق اختراع یا حق امتیاز در استفاده از امضاء دیجیتالی یک الزام مطلق نیست اما مطلوبیت بالایی دارد. مهمتر اینکه به منظور جلب اطمینان کلی جامعه به این ساز و کارها، نشر آنها ضروری است.

نیاز به استفاده از الگوریتم‌های سازنده امضاء دیجیتالی که منتشر شده و در سطح گسترده مورد استفاده قرار گیرند، جهت تضمین نکته سنجی‌های قابل ملاحظه در طراحی آنها اهمیت می‌یابد. طراحی الگوریتم‌های رمز نگار بسیار مشکل است و حتی ممکن است متخصصین نیز در طراحی آنها مرتکب اشتباهات نا ملموسی گردند که کشف آنها بسیار دشوار است. الزام عملی دیگر استفاده از الگوریتم‌های طراحی شده برای ساخت امضاء دیجیتالی برای همین منظور است نه برای تضمین محرمانه بودن اطلاعات، دلیل آن نیز می‌تواند سیاسی و فنی باشد. از نظر فنی کاربرد مختلف امضاء دیجیتالی و از دیدگاه

سیاسی، سری بودن اطلاعات نیازمند ویژگی‌های الگوریتمی متفاوتی هستند.

بسیاری از دولت‌ها محدودیت‌هایی را برای محرمانه بودن مبادله اطلاعات اعمال می‌کنند و همین امر استفاده از هر گونه فناوری ساخت امضاهای دیجیتالی را که بتواند مستقیماً از محرمانه بودن مبادلات حمایت کند، محدود می‌سازد.

۱۱ـ نتیجه

امضاهای دیجیتالی کاربردهای بالقوه ای در تجارت الکترونیک دارند اما تلاش برای به کارگیری آنها به نحوی که منعکس کننده امضاهای مکتوب باشند احتمال تأثیر ضعیفی دارد، چرا که قیاس مزبور گمراه کننده است. وجود اشخاص ثالث معتمد به عنوان مراجع گواهی کننده امضاهای دیجیتالی، اغلب به وسیله قیاس با نقش موسسات مالی در تجارت سنتی توجیه می‌شود. با این وجود، چنین قیاسی ظاهرا بر مبنای یک سوء برداشت از آنچه که موسسات مالی فراهم می‌آورند استوار است، زیرا عناصر مداخله کننده در روابط مبتنی بر اعتماد، ظاهرا سه جانبه هستند.

هرگاه این روابط با جزئیات بیشتری تحلیل شوند، آشکار می‌گردد که اغلب چیزی جز رشته ای از روابط بسته و دو جانبه نیستند که با یکدیگر ترکیب می‌شوند تا ظاهر یک رابطه سه جانبه را به خود بگیرند. به همین خاطر بعید به نظر می‌رسد گواهی امضاهای باز در تجارت الکترونیک نقش مهمی ایفا نمایند.

هم‌چنین آشکار می‌گردد که گواهی امضاهای دیجیتالی بیشتر به عنوان ساز و کارهایی برای انضمام یک اجازه به امضاهای دیجیتالی به کار می‌روند تا برای پیوند نام‌ها و هویت‌ها به امضاهای دیجیتالی (چنانچه قیاس با امضاهای مکتوب این توقع را در ما ایجاد می‌کند). همین ویژگی‌های ترکیبی استفاده از امضاهای دیجیتالی، نه به عنوان محمل‌هایی برای هویت بلکه به عنوان ساز و کارهایی تلقی می‌گردند که می‌تواند روابط مبتنی بر اعتماد بسته را که تجارت بر آن استوار است، نمایندگی کند. گواهی امضاهای دیجیتالی هویتی و مراجع گواهی کننده مربوطه در توسعه تجارت الکترونیک در مقطع کنونی نقش کمرنگی دارد. به عبارت ساده، این نوع گواهی هویتی برای چنین مقاصدی ضروری نیستند و به نظر می‌رسد بیشتر از اینکه بازار الکترونیک را توسعه بخشند، ظهور

آن را به تاخیر می‌اندازند.

گواهی امضاها و مراجع گواهی کننده که ساز و کارهایی برای اداره اجزاء کلید عمومی جفت کلیدها هستند مورد توجه و مباحثه فراوان بوده اند. بر عکس، اداره اجزاء کلید امضاء خصوصی جفت کلیدها توجهی را که شایسته آن بوده است، دریافت نداشته اند. این امر تعجب آور است، زیرا بسیاری اعتقاد دارند که مسائل فنی و حقوقی مرتبط با این اجزاء مهم ترند، به ویژه برای امضاهای مکتوب، چرا که این طرف اعتماد کننده است که بار اثبات اصالت آنها را بدوش می‌کشد. با این وجود طرح‌های دولت انگلستان برای امضاهای دیجیتالی دارای مجوز، قراردادن مسئولیت نقض بر عهده دارنده کلید را پیشنهاد می‌کنند. چنین گامی خطرات مهمی را متوجه مصرف کنندگان می‌سازد، زیرا فناوری موجود برای اداره کلید خصوصی در حال حاضر قادر به تأمین امنیت مورد نیاز برای حمایت از چنین تحولی نیست.