شناسه دیجیتال (DOI): 10.22106/JLJ.2018.31406

زیرساخت فنی ـ حقوقی تصدیق هویت در بانکداری نوین با نگاهی به جرم دسترسی غیرمجاز

حسین میرمحمدصادقی*
افشین آذری‌متین**

چکیده

امضای کاغذی رکن اساسی احراز هویت در بانکداری سنتی است، این شکل سنتی از امضا در بانکداری نوین (بانکداری الکترونیکی و مجازی) تغییر ماهیت داده و تبدیل به امضای الکترونیکی ساده و مطمئن شده است. کلیه خدماتی که در بانکداری نوین ارائه می‌شود، مستلزم صدور امضای الکترونیکی از طرف کاربران است، بستر و ساختار امضاهای جدید به گونه‌ای است که نوع جرایم را از امضای سنتی متمایز کرده است. این مقاله قصد دارد از طریق مطالعات میدانی و کتابخانه‌ای، ساختار فنی امضای الکترونیکی در سیستم بانکی را با تعاریف ارائه‌شده در قانون تجارت الکترونیک تطبیق دهد تا در گذر این توصیف، جرم جعل غیررایانه‌ای و دسترسی غیرمجاز در بانکداری سنتی و نوین مقایسه شود. بدیهی است بررسی به‌عمل‌آمده می‌تواند مقدمه‌ای باشد تا بسترهای فنی غیرموجه بانکداری الکترونیکی شناسایی شده و از این رهگذر تدابیر پیشگیرانه وضعی و فنی مناسب در بانکداری نوین پیش‌بینی گردد.

کلیدواژه‌ها: امضای الکترونیکی، گواهی الکترونیکی، گذرواژه، توکن، دسترسی غیرمجاز.

* عضو هیأت علمی دانشکده حقوق دانشگاه شهید بهشتی (نویسنده مسئول) Drsadeghi128@ yahoo.com
** دانش‌آموخته دکتری حقوق کیفری و جرم‌شناسی دانشگاه شهید بهشتی Azarimatin@gmail.com
تاریخ دریافت: ۹۴/۰۸/۱۲ تاریخ پذیرش: ۹۵/۰۲/۱۰

مقدمه

قانون تجارت الکترونیک در سال ۱۳۸۲ تصویب شد. بند ۴ ماده ۱۰ قانون برنامه چهارم توسعه مصوب ۱۳۸۳ دولت را مکلف کرد که از سال اول برنامه نسبت به برقراری نظام بانکداری الکترونیک در کلیه بانک‌های کشور اقدام نماید، زیرا استقرار تجارت الکترونیک جز در بستر انجام تراکنش‌های پولی و مالی الکترونیک میسر نیست. به این ترتیب عملیات بانکداری الکترونیکی در بستر شبکه مخابرات، اینترنت یا ماهواره با استفاده از سخت‌افزارها و نرم‌افزارهای پیشرفته شکل گرفت. بانکداری الکترونیک به مشتریان بانک‌ها این امکان را داد که تمامی عملیات بانکی خود را شامل دریافت و واریز پول، انتقال وجه، پرداخت قبوض، دریافت مانده حساب، مشاهده صورتحساب، خرید شارژ سیم کارت، پرداخت اقساط، وصول چک و دریافت وجه اوراق بهادار را به دو صورت حضوری و غیرحضوری از یک محیط الکترونیکی دریافت نمایند.[1] بند الف ماده ۴۹ قانون برنامه پنجم توسعه مصوب ۱۳۸۹ نیز بانک‌ها را مکلف کرده است تا اقدام به تبدیل کلیه حساب‌ها به صورت متمرکز نمایند. بنابراین در شیوه بانکداری جدید، مشتریان بانک‌ها می‌توانند علاوه بر اینکه از خدمات بانکداری سنتی استفاده می‌کنند، از خدمات بانکداری الکترونیکی نیز بهره‌مند شوند. در این حالت همه شعب بانک‌ها بصورت آنلاین و یکپارچه با یکدیگر در ارتباط هستند و دیگر نیازی نیست که مشتری فقط به شعبه بانک افتتاح‌کننده حساب مراجعه کند. تمامی شعب بانک، کلیه خدمات را به متقاضیان ارائه کرده و امضایی که از طرف مشتریان بانک‌ها معرفی و در رایانه اسکن شده است، قابل رویت برای همه شعب بانک است. چک‌ها در همه شعب بانک‌ها قابل وصول است. در کنار ابزارهای فیزیکی مثل دسته چک یا دفترچه حساب، کارت‌های اعتباری بانکی نیز وجود دارد و خدمات بانکی ۲۴ساعته ارائه و محدود به ساعت مشخصی نیست و جای تحویل‌داران بانک‌ها را تجهیزات و دستگاه‌های الکترونیکی اشغال کرده است. به جای اینکه احراز هویت چهره به چهره انجام شود، کارت‌های اعتباری نشان‌دهنده هویت فرد است و احراز هویت توسط تجهیزات هوشمند انجام می‌شود. در چنین فضایی نیز مفهوم امضا متفاوت است و ماده ۶۶ قانون ثبت که امضای ثبت سند را دلیل رضایت محسوب داشته، دیگر به صورت علامت و نشانه روی کاغذ تحقق نیافته، بلکه اعداد و حروفی است که توسط کاربر در صفحه کلید دستگاه درج و برای تطابق با قسمت اطلاعات مرکزی بانک ارسال می‌شود. در صورتی که رمز تطابق داشته باشد، اجازه انتقال وجه، برداشت از حساب و ... داده می‌شود. در این حالت امضا متشکل از یک سری اطلاعات

۱. بندهای (هـ) و (ی) ماده یک آیین‌نامه نظام بانکداری الکترنیکی منتشره در روزنامه رسمی شماره ۱۸۳۶۹ مورخ ۸۷/۱/۱۵.

کامپیوتری است که در قالب عدد و حروف است و با کاربر توافق شده که اسـتفاده از ایـن اعـداد و حروف به منزله امضا و قبول و تأیید شرایط است. این امضا، امضای الکترونیکی است.

توصیف مزبور که تعریف امضای الکترونیکی در بانک به عنوان زیرساخت اصلی در بانکداری نوین است،[1] با امضای دستی در بانکداری سنتی تفاوت اساسی دارد. هر چنـد در رابطه با امضای الکترونیکی مقالات متعددی نوشته شده، اما ساختار این نوع امضا در بانک تعریف نشده اسـت و بـه جـرم مقـارن آن در بانکـداری سـنتی پرداختـه نشـده و سؤالات ذیل بدون پاسخ باقی مانده است.

- امضای الکترونیکی چگونـه در بانـک از همـان اهـداف و کارکردهـای امضـای سنتی (دستی) برخوردار است؟
- امضای الکترونیکی در بانکداری نوین بر اساس چه ساختاری طراحی شده است؟
- چه جرمی در بانکداری الکترونیکی مقارن جعل در بانکداری سنتی است؟

تعریف امضای الکترونیکی در قانون تجارت الکترونیک دارای توصیف کلی اسـت و باید با ابزارها و زیرساخت‌های بانکداری الکترونیک تطبیق داده شـود. بـه همـین دلیـل لازم است براساس زیرساخت‌های فنی و حقوقی بانکداری الکترونیک، ساختار امضای الکترونیکـی در بانک توصیف شود. تمرکز مطالب مقاله نیز بر همین اساس طراحی شـده اسـت. بـدین منظور به روش توصیفی ـ تبیینی، ابعاد حقـوقی امضـای دسـتی و ابعـاد فنـی ـ حقـوقی امضای الکترونیک و انواع آن بررسی شده است. مطالعات این تحقیق کتابخانه‌ای و میدانی است و قسمت میدانی از طریق واحدهای انفورماتیک بانک‌ها انجام شده است. سپس جرم دسترسی غیرمجاز نسـبت بـه دو نـوع امضـای الکترونیـک سـاده و مطمـئن (دیجیتـال) به‌صورت گذرا بررسی شده است، این مطالعه می‌تواند زمینه شناسایی زیرساخت‌های فنـی غیرموجـه در بانکـداری الکترونیکـی و تـدوین قـانون جزایـی متناسـب بـا بانکـداری الکترونیکی را فراهم کند. بدیهی است شناسایی زیرساخت‌های فنی غیرموجه برای ارائه تدابیر پیشگیرانه وضعی مناسب نیاز به تحقیق دیگری دارد. چـون امضـای الکترونیکـی ساده در بانکداری الکترونیکی و امضای الکترونیکی مطمئن در بانکداری مجازی کـاربرد دارد، دو قسمت بعدی مقاله بر همین اساس تقسیم‌بندی شده است.

۱. بانکداری سنتی و جعل

بند (الف) ماده ۳۱ قانون پولی و بانکی کشور مصوب ۱۳۵۱ تشکیل بانک را به صـورت شرکت سهامی عام مجاز دانسته است و ایجاد شعب بانک‌هـا بـا اخـذ شناسـه اختصاصـی از

۱. اصطلاح بانکداری نوین دو عنوان بانکداری الکترونیکی و بانکداری مجازی را در بر می‌گیـرد (مبینـی دهکـردی، علـی؛ رسولی‌نژاد، احسان، شکل‌دهی به فضای نوین: رویکرد دانش بنیان، چاپ اول، نشر نور علم، ۱۳۹۰، ص. ۱۹۶).

بانک مرکزی امکان‌پذیر است.[1] در نظام بانکداری سنتی شعب بانک به عنوان مرکز اصلی فعالیت‌های بانکی محسوب شده و حضور مشتریان بانک در شعب بانک‌ها به منظور افتتاح حساب و دریافت خدمات بانکی و اعتباری الزامی است. مشتریان بانک شامل اشخاص حقیقی و حقوقی ایرانی یا خارجی، قبل از دریافت هر گونه خدمات باید بر اساس شناسه اختصاصی[2] احراز هویت شوند. مدارک شناسایی اشخاص حقیقی شامل کارت ملی، شناسنامه، گواهینامه و گذرنامه و برای اشخاص حقوقی گواهینامه ثبت شرکت است. این سطح از شناسایی مشتریان، شناسایی اولیه است که در این شناسایی مشخصات اظهارشده مشتری با مدارک شناسایی او تطبیق داده خواهد شد. مشتریان گذری بانک که رابطه آنها فاقد استمرار است پس از شناسایی اولیه قادر خواهند بود از خدمات غیرپایه بانک نظیر حواله وجوه، دریافت و پرداخت وجه، خرید و فروش ارز و موارد مشابه استفاده کنند. خدمات پایه مثل افتتاح انواع حساب بانکی، اعطای تسهیلات، صدور ضمانت‌نامه، اعتبارات اسنادی به مشتریان دائمی یا دارای رابطه مستمر با بانک قابل ارائه است که شناسایی کامل شده باشند؛ یعنی نوع، ماهیت و میزان فعالیت آنها مشخص شده باشد.[3]

امضای اسناد بانک از ضروریات[4] ارائه خدمات پایه و غیرپایه در سیستم بانکی است. پس، امضا در بانک دارای دو نقش اساسی است. اول اینکه هویت طرف قرارداد برای بانک محرز شده[5] و دوم به منزله پذیرش تعهدات سند از طرف خدمات‌گیرندگان

۱. بند (و) ماده ۲۰ قانون پولی و بانکی کشور ۱۳۵۱، ایجاد شعبه یا باجه ـ بخشی از شعبه است که در غیر محل شعبه دایر می‌شود و قسمتی از عملیات شعبه که تعهدی برای شعبه ایجاد نمی‌کند را انجام می‌دهد ـ را صرفاً با اخذ شناسه اختصاصی از بانک مرکزی امکان‌پذیر دانسته است. آیین‌نامه ایجاد یا تعطیل شعبه یا باجه مؤسسات اعتباری در داخل کشور مصوب شورای پول و اعتبار ۹۱/۵/۱۰ و دستورالعمل اجرایی موضوع ماده ۱۴ آیین‌نامه ایجاد یا تعطیل شعبه یا باجه مؤسسات اعتباری در داخل کشور مصوب شورای پول و اعتبار ۱۳۹۲/۷/۷ به تفصیل ضوابط مربوطه را تعیین کرده است. ماده ۸۱ آیین‌نامه نحوه تأسیس و اداره مؤسسات اعتباری غیردولتی ۱۳۹۳ نیز ایجاد شعبه یا باجه را در چارچوب ضوابط شورای پول و اعتبار امکان‌پذیر دانسته است.

۲. علی‌رغم اینکه طبق ماده ۹۹۲ قانون مدنی و ماده ۳۶ قانون ثبت احوال ۱۳۵۵ شناسنامه ملاک تعیین هویت اشخاص است ولی بر اساس مقررات ذیل احراز هویت مراجعان بانک‌ها مطابق شناسه اختصاصی صورت می‌پذیرد: الف ـ آیین‌نامه مستندسازی جریان وجوه در کشور ۱۳۸۷؛ ب ـ قانون و آیین‌نامه اجرایی مبارزه با پولشویی مصوب ۱۳۸۶ و ۱۳۸۸؛ ج ـ قانون و آیین‌نامه اجرایی الزام اختصاص شماره ملی و کدپستی برای کلیه اتباع ایرانی مصوب ۱۳۷۶ و ۱۳۸۷؛ د ـ آیین‌نامه تعیین شماره اختصاصی برای اشخاص خارجی مرتبط با کشور ۱۳۸۷؛ ه ـ آیین‌نامه اختصاص شناسه ملی به کلیه اشخاص حقوقی ایرانی ۱۳۸۷.

۳. نحوه شناسایی مشتریان بانک بر اساس دو دستور العمل جداگانه مربوط به پولشویی که توسط شورای عالی مبارزه با پولشویی در سال ۱۳۹۰ تصویب شده است، صورت می‌پذیرد: الف ـ دستورالعمل چگونگی شناسایی مشتریان ایرانی مؤسسات اعتباری؛ ب ـ دستورالعمل چگونگی شناسایی مشتریان خارجی مؤسسات اعتباری.

۴. خلیل میثاقی ممقانی، ابراهیم، «نقش امضا و اثر انگشت از نظر قانونی»، ماهنامه کانون سر دفتران، دوره اول، شماره ۱۸۶، تیر ۱۳۵۴، ص. ۳۵.

۵. ماده ۸۶ قانون ثبت ۱۳۱۰ سردفتر را مکلف به تحصیل اطمینان از هویت متعاملین نموده است. در صورتی که سردفتر راجع به هویت متعاملین تردید داشته باشد، مطابق ماده ۵۰ قانون ثبت با دو شاهد تصدیق

بانک است. به عبارت دیگر امضای دستی یا سنتی که شخص سند را دیده و با خودکار آن را امضا کرده، نشانه‌ای است که شخص آن را تنفیذ کرده و دلالت بر قصد و اراده صاحب امضا دارد، طبق ماده ۱۹۱ قانون مدنی به عنوان آخرین اراده شخص به طور مکتوب محسوب شده و به همین دلیل هر قرارداد کتبی برای آن که واجد آثار حقوقی گردد نیازمند امضا یا تأسیسات مشابهی مانند اثر انگشت، مهر و نظایر اینهاست. مواد ۱۳۰۱ قانون مدنی و ۶۵ قانون ثبت امضا را بدین معنی دانسته که شخص جامعیت سند را تایید کرده و بیان داشته که به محتویات آن متعهد و پایبند است. سندی که دارای امضا باشد طبق ماده ۱۹۴ قانون آیین دادرسی مدنی ۱۳۷۹ و ماده ۱۲۵۸ قانون مدنی یکی از دلایل اثبات دعوا است. ماده ۱۲۸۷ قانون مدنی اسناد رسمی را تعریف کرده، بنابراین اسناد تنظیمی در بانک طبق ماده ۱۲۸۹ قانون مدنی عادی هستند. یعنی بر اساس ماده ۷۰ قانون ثبت علاوه بر ادعای جعل، انکار و تردید نیز نسبت به آنها مسموع است.

بدین ترتیب دو نوع جرمی که با امضا در بانک ارتباط دارد، یکی مربوط به ساختن یا تغییر دادن اسناد سجلی است،[1] که در خدمات پایه و غیرپایه مشابه است چون در هر دو حالت منوط به احراز هویت است[2] و افراد می‌توانند از این طریق هویت مجعول اتخاذ و با هویت غیرواقعی چک وصول کرده یا از طریق افتتاح حساب بانکی وام دریافت کرده یا ضامن شوند.[3] افتتاح چنین حسابی جزو اهداف پول‌شویان و تحصیل‌کنندگان مال نامشروع است و آنان را قادر خواهد ساخت وجوهی را که از سایر جرایم تحصیل کرده‌اند، بدون شناسایی انتقال داده، مصرف کرده یا برداشت نمایند. پس حسابی که بدین طریق افتتاح شده، اگر جزء حساب‌های جاری باشد، امکان کلاهبرداری با استفاده از دسته چکی که از بانک تحویل گردیده وجود دارد.[4] دومی ساختن یا تغییر دادن اسناد بانکی است. توضیح داده شده که سند بانکی سند عادی است. اسناد بانکی عادی بر دو نوع هستند. امکان دارد توسط بانک امضا و صادر شده

← هویت خواهد کرد. اضافه می‌شود که طبق بند ۳ ماده ۴۹ قانون ثبت و ماده ۲۰ قانون دفاتر اسناد رسمی و کانون سر دفتران و دفتریاران ۱۳۵۴ امضای مسلم‌الصدور همان تصدیق امضای ذیل اسناد عادی توسط دفاتر اسناد رسمی است. بدین ترتیب ثبت امضا پس از احراز هویت امضاکننده و ثبت نمونه امضای وی در دفتر گواهی امضا انجام خواهد شد.

۱. مواد ۱۰ و ۱۳ قانون تخلفات، جرایم و مجازات‌های مربوط به اسناد سجلی و شناسنامه مصوب مجمع تشخیص مصلحت نظام ۱۳۷۰ مواردی از جعل اسناد سجلی را پیش‌بینی کرده است.

۲. میرمحمد صادقی، حسین، جرایم علیه اموال و مالکیت، چاپ سی و پنجم، نشر میزان، ۱۳۹۲، ص. ۳۱۶.

۳. تسهیلاتی که در بانک‌ها بدین ترتیب پرداخت شده معمولاً جزو مطالبات سوخت‌شده است. بند ژ ماده ۱ آیین‌نامه وصول مطالبات سررسید گذشته، معوق و مشکوک‌الوصول مؤسسات اعتباری (ریالی و ارزی) ۱۳۸۸ در تعریف مطالبات سوخت‌شده بیان داشته، آن بخش از مطالبات مؤسسات اعتباری است که صرف نظر از تاریخ سررسید به دلایل متقن از قبیل فوت یا ورشکستگی بدهکار و یا علل دیگر قابل وصول نیست.

۴. فخاری، امیرحسین، اندیشه‌های حقوقی (۳): حقوق تجارت، چاپ اول، انتشارات مجد، ۱۳۸۷، ص. ۱۴۱.

باشند؛ مانند ضمانت‌نامه‌های صادره، چک‌های تضمین‌شده[1] و بین‌بانکی،[2] فیش‌های واریز وجه به حساب و یا دفترچه و گواهی سپرده بانکی و یا مثل دسته چک در حساب جاری که نوشتن مندرجات و امضای چک بر عهده صاحب حساب است. در این حالت اگر چک امضا نداشته باشد، چون قابلیت ایراد ضرر به غیر نداشته و صرفاً شبیه‌سازی خط دیگری است، سندیت نداشته و جعل نیست. ولی لزومی ندارد شباهتی بین امضای تقلبی و اصلی وجود داشته باشد. همین که احتمال به اشتباه انداختن تحویل‌دار بانک وجود داشته باشد، وی فریب خورده و پول را پرداخت کند، جعل تحقق یافته است. از آنجا که جعل مقدمه‌ای برای استفاده بعدی از سند مجعول یا کلاهبرداری است، پس جرم مستقلی محسوب است و ارتکاب جرایم بعدی مشمول تعدد مادی خواهد بود.[3]

۲. زیرساخت‌های بانکداری الکترونیکی

عملیات بانکی در بانکداری الکترونیکی به صورت لحظه‌ای در تمام شعب بانک در سراسر کشور انجام می‌شود. حساب‌های بانکی دارای کارت‌های پرداخت[4] مرتبط با آن بوده و اطلاعات شناسایی یا حساب بانکی افراد در کارت‌های با جنس پلاستیکی روی نوار مغناطیسی (کارت‌های مغناطیسی) یا تراشه الکترونیکی (کارت‌های هوشمند) ذخیره شده است. ارتباطات الکترونیکی با حساب از طریق کانال‌های خودپرداز، پایانه فروش[5] به صورت حضوری (تماسی) و درج رمز اول کارت یا از طریق بانکداری همراه و تلفن بانک[6] یا درگاه‌های اینترنتی بانک به صورت غیرحضوری (غیر تماسی) انجام می‌شود. ارائه خدمات پایه به صورت الکترونیکی و انجام هر گونه تراکنش الکترونیکی که با حضور شخص از طریق شعب بانک ارائه می‌شود. بدون شناسایی کامل مشتری

۱. هیأت عمومی دیوان عالی کشور در رأی شماره ۷۴ مورخ ۱۳۴۶/۱۰/۲۷ جعل این‌گونه چک‌ها را در حکم جعل اسکناس محسوب کرده است.

۲. میرمحمد صادقی، حسین، منبع پیشین، ص. ۳۱۹.

۳. میرمحمد صادقی، حسین، جرایم علیه امنیت و آسایش عمومی، چاپ بیست و دوم، نشر میزان، ۱۳۹۲، ص. ۳۲۹.

۴. انواع کارت پرداخت که به عنوان ابزار برداشت پول یا خرید کالا است عبارتند از : الف ـ کارت‌های بدهی (debit card) از طریق حساب‌های متمرکز مشتریان بانک امکان برداشت تا سقف موجودی را امکان‌پذیر ساخته است. ب ـ کارت هدیه با سقف مبلغ مشخص که پرداخت و خرید از طریق سامانه متمرکز کارت انجام می‌شود. ج ـ کارت کیف پول الکترونیک یا کارت‌های هوشمند، در این‌گونه کارت‌ها، ارزش پول مستقلاً بر روی فیزیک کارت و در تراشه ذخیره شده است. د ـ کارت اعتباری (credit card) در این نوع کارت، بدون آنکه شخص حساب بانکی داشته باشد، از طریق سقف اعتباری که به وی تخصیص یافته است، می‌تواند نسبت به خرید کالا و خدمات اقدام نماید.

۵. دستگاهی است که با پذیرش کارت بانکی امکانی را فراهم کرده وجه به صورت الکترونیکی از حساب دارنده کارت به حساب فروشنده منتقل شود.

۶. در بانکداری همراه و تلفن بانک، ارائه خدمات بانکی به صورت غیرحضوری از طریق سامانه‌های تلفن همراه یا ثابت انجام می‌شود.

نباید انجام شود[1] و افتتاح انواع حساب برای اولین مراجعه ارباب رجوع، صدور انواع کارت‌های پرداخت و نصب هر گونه ابزار پذیرش مثل پایانه‌های فروش یا درگاه‌های اینترنتی مجازی[2] پیش از شناسایی کامل مشتری ممنوع است.[3] تطبیق هویت ارباب‌رجوع و ثبت تراکنش[4] در مراجعات حضوری از طریق ابزارهای شناسایی فیزیکی (نظیر کارت) و یک ابزار پذیرش فیزیکی (نظیر پایانه فروش) انجام شده و یا در روش غیرحضوری از طریق یک ابزار شناسایی مجازی (نظیر شناسه و رمز اینترنتی) و یک درگاه پذیرش مجازی (نظیر تارنمای اینترنتی) تحقق می‌یابد. پس اگر برای امضا دو کارکرد قائل شویم، یکی تأیید هویت و دیگری پذیرش تعهدات است. عرف رایج در نظام بانکداری سنتی هم این کارکردهای امضا را تایید کرده و در عمل اگر شخصی قصد وصول وجه چکی را داشته باشد، دو امضا از دریافت‌کننده وجه اخذ خواهد شد، یکی برای شناسایی و دیگری به معنی تأیید دریافت وجه است. اگر هم کسی چکی امضا کند، چون در زمان افتتاح حساب احراز هویت شده است، یک امضا کفایت می‌کند.

در بانکداری الکترونیک هم همین ترتیب رعایت می‌شود. در روش حضوری (تماسی) قرار دادن کارت پرداخت در درگاه‌های حضوری برای شناسایی دریافت‌کننده خدمات الکترونیکی است و درج رمز اول در دستگاه خود پرداز یا پایانه فروش به‌منزله تأیید تراکنش و قبول شرایط درخواست است.[5] بنابراین تراکنش‌های الکترونیکی بدین طریق دو نوع ماهیت دارند: یکی ماهیت فیزیکی و دیگری ماهیت مجازی. ماهیت

۱. ماده ۱۳ دستورالعمل چگونگی شناسایی مشتریان ایرانی مؤسسات اعتباری ۱۳۸۹ شورای عالی مبارزه با پولشویی.

۲. مواد ۲، ۳ و ۴ دستورالعمل رعایت مقررات مبارزه با پولشویی در حوزه نظام‌های پرداخت و بانکداری الکترونیکی ۱۳۸۹ شورای عالی مبارزه با پولشویی.

۳. ماده ۸۷ قانون نظام صنفی کشور ۱۳۹۲ و تبصره آن فعالیت افراد صنفی در فضای مجازی را مستلزم اخذ پروانه از اتحادیه، مطابق آیین‌نامه تصویبی دانسته است. بند ۱ـ۱ از ماده یک آیین‌نامه سامان‌دهی فعالیت و نظارت بر فروشگاه‌های مجازی ۱۳۸۸ وزارت بازرگانی، فروشگاه مجازی را یک واحد اقتصادی بر شمرده که از طریق شبکه‌های رایانه‌ای از جمله اینترنت و توسط اشخاص حقیقی و حقوقی اداره و دارای مجوز از مرکز امور اصناف و بازرگانان وزارت بازرگانی است، طبق دستورالعمل اعطای نماد اعتماد الکترونیکی و نظارت بر فعالیت کسب وکارهای اینترنتی ۱۳۹۲ مصوب کمیته نظارت بر کسب و کارهای اینترنتی مرکز توسعه تجارت الکترونیک وزارت صنعت و معدن و تجارت، کسانی که قصد کسب و کارهای اینترنتی (مجازی) داشته باشند، پس از احراز هویت و صلاحیت می‌توانند ا قدام به دریافت نماد اعتماد نمایند. بنابراین کسب و کارهای مجازی در صورتی قادرند که از درگاه‌های اینترنتی سیستم بانکی برای خرید مشتریان خود استفاده نمایند که اقدام به دریافت نماد اعتماد نموده باشند.

۴. تراکنش یک پیام الکترونیکی است که مشتری بانک از طریق یکی از درگاه‌ها نظیر خودپرداز یا پایانه فروش تقاضا کرده است و بدین ترتیب برداشت یا انتقال وجه به شبکه الکترونیکی بانکی ارسال می‌شود. همچنین به عملیاتی که بر اساس درخواست کاربر منجر به تغییر در حساب یا بانک اطلاعات شود، تراکنش گفته‌اند.

۵. طبق ماده ۵ دستورالعمل رعایت مقررات مبارزه با پولشویی در حوزه نظام‌های پرداخت بانکداری الکترونیکی، تطبیق هویت ارباب رجوع با اقلام اطلاعاتی شناسایی مشتری در مراجعات غیرحضوری از طریق ابزارهای شناسایی است.

فیزیکی همان جسم کارت است و ماهیت مجازی در حقیقت رمزی است که تنها خود فرد از آن آگاه است. پس اگر جسم کارت به هر شکلی جعل شود، رمز کارت یا ماهیت مجازی، جعل تراکنش‌های الکترونیکی را دشوار خواهد کرد.

در روش غیرحضوری دو امکان وجود دارد. اگر ارائه خدمات کارت‌محور باشد، نظیر حالتی که شخص قصد پرداخت قبوض خدماتی مثل آب، برق، گاز و ... را دارد یا پس از خرید از فروشگاه مجازی و ارتباط با درگاه[1] پذیرش مجازی بانک، بعد از ثبت اطلاعات کارت شامل شماره، کد اعتبارسنجی[2] و تاریخ انقضا در درگاه، تا زمانی که رمز دوم یا رمز اینترنتی ثبت نشود پرداخت یا انتقال وجه محقق نخواهد شد. بنابراین این نوع درگاه برای پرداخت‌های بانکی استفاده‌شده و دارای شماره رمز جداگانه از درگاه‌های حضوری (رمز اول) است. در حالت دوم[3] که مبتنی بر شماره حساب بانکی است،[4] اینکه کاربر (مشتری بانک) به شبکه یا پایگاه داده بانک دسترسی داشته و از خدمات بانکی استفاده کند، مستلزم ثبت نام کاربری و گذر واژه یا رمز عبور در سامانه بانک است. این اطلاعات قبلاً از طرف بانک به وی اختصاص داده شده است. بر این اساس شیوه گواهی و امضای الکترونیکی که در نظام بانکداری الکترونیک استفاده می‌شود، روش گذرواژه، عبارت عبور یا شماره شناسایی شخصی است[5] و طبق ماده (۷) قانون تجارت الکترونیک ۱۳۸۲ از جایگاه قانونی امضای دستی برخوردار است. امضایی که بدین ترتیب به مشتریان بانکی اختصاص یافته، به دلیل اینکه طبق تبصره ۲ ماده ۴ آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیک ۱۳۸۶ از طرف مرکز ریشه مستقل

۱. درگاه‌ها جایگاه‌هایی می‌باشند که خدمات بانکداری الکترونیکی را ارائه می‌نمایند. خودپرداز، کارت‌خوان فروشگاهی، اینترنت بانک و موبایل بانک و تلفن بانک جزء درگاه‌ها می‌باشند.

۲. کد اعتبارسنجی (cvv2) عددی است که طول آن بین سه تا چهار رقم است، در سامانه کارت بانک تعریف شده و معمولاً پشت کارت درج می‌شود.

۳. شبا عبارت است از شماره حساب بانکی ایران که به منظور تسهیل مبادلات بین‌بانکی تعریف شده است. شبا مستقل از نظام شماره‌گذاری داخلی هر یک از بانک‌ها است. اما در محاسبه شبا از نظام شماره‌گذاری حساب داخلی بانک‌ها استفاده شده است. بنابراین در حال حاضر تنها معیار برای انتقال وجوه مشتریان بانک‌ها از طریق سامانه‌های تبادلات بانکی بانک مرکزی بین بانک‌ها، شماره حساب بانکی ایران و شماره حساب شخص است.

۴. احمدی، سیدمحمود؛ خندان سویری، مهدی، نظام‌های پرداخت و بانکداری الکترونیک در ایران، پژوهشکده پولی و بانکی بانک مرکزی، ۱۳۹۴، ص. ۲۳۲.

۵. رمز اول بصورت محرمانه و در پاکت مهر و موم شده به دارندگان کارت بانکی تحویل خواهد شد. این رمز ثابت است ولی به صورت دوره‌ای توسط دارنده کارت قابل تغییر است. اما رمز دوم یا رمز اینترنتی می‌تواند ثابت باشد یا متغیر. در حالتی که رمز متغیر است، روشی که بانک‌ها به کار گرفته‌اند به این ترتیب است که پس از وارد کردن نام کاربری شخص، از طریق پیامک برای هر بار ورود رمز جدید از طرف بانک اختصاص خواهد یافت یا از طرف بانک، دستگاه‌های رمزساز به صاحب حساب تحویل شده تا پس از درج نام کاربری یک رمز جدید که دارای مدت زمان اعتباری مشخص است، اختصاص یابد.

حوزه نظام بانکی ایجاد نگردیده، طبق ماده ۱۱ آیین‌نامه اجرایی قانون مزبور[۱] صرفاً در حوزه داخلی بانک‌ها اعتبار داشته و طبق ماده ۶ قانون تجارت الکترونیکی ۱۳۸۲ امضای ساده (غیرمطمئن)[۲] است.[۳]

بر این اساس اگر تراکنش را مترادف داده‌پیام در بند (الف) ماده ۲ قانون تجارت الکترونیکی قلمداد کنیم، یعنی تولید و ارسال اطلاعات کاربران بانکی مثل انتقال وجه یا دریافت صورتحساب از طریق درگاه‌های اختصاص داده شده حضوری یا غیرحضوری است و شماره عبارت عبوری که در صفحه کلید دستگاه ثبت شده، علامت[۴] منضم به داده‌پیام است، هویت امضاکننده را تأیید کرده و همان امضای الکترونیکی نامیده‌شده در بند (ی) ماده ۲ قانون تجارت الکترونیکی است.[۵] این امضا در مقایسه با امضای الکترونیکی مطمئن یا دیجیتال امنیت پایین‌تری دارد. البته برای اینکه امنیت انتقال اطلاعات ارتقا یابد و از سرقت و استراق سمع اطلاعاتی نظیر گذرواژه جلوگیری شود، در حال حاضر توسط بانک‌ها از راه‌حل‌های مرکب استفاده شده است. ترکیبی از گذرواژه و پرتکل‌های امنیتی از این قبیل است که امکان برقراری ارتباط بین سرویس‌دهنده و کاربر را به صورت رمزشده فراهم کرده و برای دیگران غیر قابل خواندن است.[۶]

بنابراین امضای ساده بر اساس اینکه از چه نوع درگاهی استفاده شود، حالت‌های مختلف دارد. اگر از دستگاه‌های خودپرداز یا پایانه‌های فروشگاهی استفاده گردد، کارت پرداخت بانکی به علاوه رمز اول کارت که چهاررقمی است و در زمان تحویل کارت به دارنده آن اختصاص داده شده و قابل تغییر توسط دارنده از طریق دستگاه خودپرداز است، یک نوع امضای ساده است. حالت دیگری که این امضا دارد و به

۱. با توجه به اینکه بانک‌ها اقدام به صدور گواهی الکترونیکی به معنی خاص آن نمی‌نمایند، بنابراین مشمول ممنوعیت مندرج در ماده ۶ دستور العمل اجرایی سامان‌دهی مراکز صدور گواهی الکترونیکی میانی ۱۳۸۸ شورای سیاست‌گذاری گواهی الکترونیکی نیستند.

۲. از جمله امضاهای دیگری که با فناوری ساده تولید می‌گردد، امضای دستی اسکن‌شده، امضا با قلم نوری و کلیک کردن بر روی گزینه تأیید است. امضاهای با فناوری زیست‌سنجی یا بیومتریک نیز وجود دارد که مبنای تشخیص هویتی که استفاده کرده‌اند بر اساس خصیصه‌های منحصر به فرد فیزیکی و رفتاری کاربر است؛ مانند اثر انگشت، تصویر شبکیه چشم، شکل هندسی دست و انگشت یا شناسایی از طریق صدا.

۳. شمس، عبدالله، آیین دادرسی مدنی، جلد ۳، چاپ بیست و سوم، انتشارات دراک، ۱۳۹۲، ص. ۱۴۸.

۴. بند الف ماده ۳۰ قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری، علامت را تعریف نموده است. بدین معنا که هر نشان قابل رویتی است که بتواند کالاها یا خدمات اشخاص حقیقی یا حقوقی را از هم متمایز سازد. این تعریف با این عبارت که امضای الکترونیکی را علامت دانسته از جهاتی شباهت دارد، زیرا علامت را معرف شخص دانسته است.

۵. طبق ماده ۱۳۰۴ قانون مدنی، لازم نیست در اسناد کاغذی امضا همراه با متن در یک برگه باشد. بلکه امضا می‌تواند در برگ جداگانه درج شده باشد، بدین ترتیب امضای الکترونیکی که علامت منضم‌شده یا متصل-شده به داده پیام تعریف شده است، دارای اعتبار است.

۶. زرکلام، ستار، اعتمادسازی در تجارت الکترونیکی، چاپ اول، شهر دانش، ۱۳۹۰، ص. ۱۴۷.

عنوان رمز دوم یا اینترنتی شناخته شده، قابل استفاده در زمانی است که کاربر قصد بهره‌برداری از درگاه‌های اینترنتی بانک یا فروشگاه‌های مجازی را دارد و با وارد کردن مشخصات کارت پرداخت بانکی (شامل شماره کارت، کد اعتبارسنجی و تاریخ انقضاء) و رمز دوم خواهد توانست اقدام به پرداخت قبوض خدماتی یا کالای خریداری‌شده کند.

در استفاده از خدمات بانکداری اینترنتی که مبتنی بر شماره حساب است، نام کاربری و گذرواژه اختصاصی شخصی همان امضای ساده است، در این حالت گذرواژه یا ثابت (ایستا) است، یعنی در هر بار ورود یک رمز استفاده خواهد شد که امکان تغییر نیز برای کاربر وجود دارد، یا بصورت پویا (متغیر) است، یعنی در هر بار ورود یک رمز جداگانه به کاربر از طرف بانک اختصاص داده خواهد شد. اختصاص رمز متغیر در سیستم بانکی دو صورت دارد، در حالت اول، پس از اینکه کد کاربری در سامانه بانک ثبت شد به شماره تلفن همراهی که از قبل به بانک اعلام شده است، شماره رمز پیامک خواهد شد یا بانک دستگاه‌های رمزساز (توکن) در اختیار مشتریانش قرار داده تا هر زمان شخص قصد استفاده از خدمات بانکداری الکترونیکی را داشته باشد از طریق این دستگاه هر بار یک شماره رمز تولید و اختصاص داده شود. در نتیجه می‌توان گفت سامانه‌های بانکی به شیوه نصب گذرواژه دارای تدابیر امنیتی است و نوع جرایمی که علیه امضای الکترونیکی ساده وجود دارد، بسته به نوع درگاه بانکی و نوع رمز مورد استفاده به شرح ذیل متفاوت است:

الف ـ چنانچه دسترسی به سامانه بانکی از طریق درگاه‌های غیرحضوری مثل اینترنت یا تلفن بانک باشد، امکان دارد، همراه با سایر بزه‌ها باشد. پس، برای اینکه دسترسی به سامانه بانک‌ها به طور غیرمجاز امکان‌پذیر گردد یا باید با بهره‌گیری از دانش فنی، نقض تدابیر حفاظتی صورت پذیرد. به عنوان نمونه اگر کسی با انتشار نرم‌افزار مخرب (ویروس‌ها و کرم‌های رایانه‌ای رخنه‌گر) و تخریب گذرواژه اقدام به دسترسی غیرمجاز نماید، مرتکب سه بزه مندرج در قانون مجازات اسلامی شامل انتشار نرم‌افزار زیان‌بخش (بند الف ماده ۷۵۳) تخریب داده (ماده ۷۲۶) و دسترسی غیرمجاز (ماده ۷۲۹) شده است و اگر کسی از طریق شیوه‌های مهندسی اجتماعی[1] به گذر واژه دسترسی یابد، یا به وسیله

۱. فیشینگ (Phishing) نوعی از حملات مهندسی اجتماعی بر پایه فریب افراد به منظور سرقت از حساب مالی کاربران است که برای دسترسی به رمزهای عبور شخصی کاربران استفاده شده است. کلاهبرداران از طریق حمله فیشینگ به دنبال به دست آوردن اطلاعاتی نظیر کلمه کاربری، رمز عبور، شماره ۱۶رقمی کارت بانکی و کد اعتبارسنجی از طریق درگاه‌های پرداخت آنلاین هستند. در این روش صفحه‌ای مشابه یکی از سایت‌ها همچون بانک ساخته شده و هنگامی که کاربر وارد سایت جعلی شده و اطلاعات خود را وارد کند، اطلاعات وی از طریق سایت جعلی برای نفوذگر ارسال و به سرقت می‌رود، بدین ترتیب نفوذگر توانسته وارد

شنیدن، یافتن یا ربودن و پیدا کردن اتفاقی گذرواژه[1] به سامانه بانکی رخنه نموده و دسترسی غیر مجاز حاصل شود هر چند تدابیر امنیتی حفاظت‌شده سامانه به روش فنی برداشته نشده است، به دلیل اینکه مبنای جرم‌انگاری دسترسی غیرمجاز، حمایت از محرمانگی داده یا سامانه است، به همین دلیل رخنه‌گری محسوب شده و جرم انجام‌شده دسترسی غیر مجاز است.[2] به همین ترتیب دسترسی غیر مجاز زمانی که گذرواژه از شخص دیگری گرفته شده است تحقق خواهد یافت، بند ب ماده ۷۵۳ قانون مجازات اسلامی ناظر به دسترسی غیر مجاز است و در این بند، فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم کند، جرم و قابل مجازات می‌داند.

ب ـ استفاده از درگاه‌های حضوری مثل دستگاه خودپرداز یا پایانه‌های فروش، مستلزم قرار دادن کارت در دستگاه و ثبت رمز اول است. دسترسی غیرمجاز به سامانه مستلزم ساختن کارت بانکی است که روش‌های مختلفی مثل اسکیمینگ[3] دارد یا احتمال دارد کارت بانکی ربوده یا پیدا شده باشد و سپس دستیابی به شماره گذرواژه است، می‌تواند مشابه قبل به روش‌های فنی[4] یا

← حساب کاربری دیگران شود. نوعی دیگر از مهندسی اجتماعی که به نفوذ کلامی یا رفتاری متکی است، با اشخاص تماس تلفنی گرفته شده، می‌گویند قرعه‌کشی شده و وجهی برنده شده‌اند و برای واریز وجه باید کارت بانکی داشته باشند. با این ترفند اشخاص به سمت دستگاه خودپرداز هدایت شده و برای اینکه متوجه نوع عملیات بانکی نشوند، توصیه می‌گردد تا از منوی انگلیسی استفاده کنند. سپس کاربر بدون اینکه متوجه شود چه عملیات بانکی انجام می‌دهد، اقدام به ثبت گذرواژه و انتقال وجه به حساب مورد نظر فرد تماس‌گیرنده می‌کند. به دلیل اینکه اقدامات مرتکب متکی به دانش فنی نیست، نفوذ به سیستم‌های رایانه‌ای نبوده و مبتنی بر فریب کاربر است و تحت عنوان کلاهبرداری سنتی قابل تعقیب و مجازات است.

۱. در مواردی که رمزنگاری به صورت پویا است، دسترسی فیزیکی به سیم‌کارت تلفن همراه و دستگاه رمزساز ضروری است.

۲. عالی‌پور، حسن، حقوق کیفری فناوری اطلاعات، چاپ اول، انتشارات خرسندی، ۱۳۹۰، ص. ۱۷۳.

۳. اسکیمینگ (Skimming) به کپی‌کردن غیرقانونی داده‌های نوار مغناطیسی کارت بانکی روی کارت دیگر گویند، اسکیمرها دستگاه‌های الکترونیکی کوچکی هستند که به وسیله سارقین (اسکیمرها) در محل ورودی دستگاه خودپرداز نصب می‌شود و از این طریق اقدام به کپی‌کردن داده‌های نوار مغناطیسی کارت کاربران در کارت دیگر می‌نمایند و یا با قراردادن صفحه کلید بدلی که دقیقاً شبیه صفحه کلید اصلی دستگاه خودپرداز است، به گونه‌ای روی آن قرار می‌گیرد که کاربر متوجه این موضوع نیست که یک صفحه کلید اضافه روی شماره‌های اصلی قرار گرفته است و بدین ترتیب تمامی اطلاعات مورد نیاز برای دسترسی به حساب افراد را بدست می‌آورند.

۴. در فارمینگ (Pharming) کاربر یک ایمیل ظاهراً صحیح را باز می‌کند و بدین ترتیب یک کلیدخوان را روی سیستم خود نصب کرده است. کلیدخوان برنامه‌ای است که کلیدهایی را که توسط کاربر زده می‌شود ثبت می‌کند و نام کاربری و رمز عبور ثبت‌شده برای نفوذگر ارسال می‌شود.

غیرفنی به دست آید، اگر به طور همزمان کارت جعلی در دستگاه قرار داده شده و استفاده شود و گذرواژه در صفحه کلید دستگاه ثبت شود، امکان دسترسی غیرمجاز و عملیات بانکی فراهم خواهد شد. در این حالت سه جرم قانون مجازات اسلامی به وقوع پیوسته است: جعل کارت (بند ب ماده ۷۳۴)، استفاده از کارت جعلی (ماده ۷۲۵) و دسترسی غیرمجاز (ماده ۷۲۹).

۳. زیرساخت‌های بانکداری مجازی

امضای دیجیتال پیشرفته‌ترین، مطمئن‌ترین و پرکاربردترین روش جهت احراز اصالت و اطمینان از دست‌نخوردگی اطلاعات الکترونیکی است. به علاوه غیرقابل انکار نیز هست.[۱] اصلی‌ترین رکن امضای دیجیتال گواهی الکترونیکی است. گواهی الکترونیکی نوعی گواهی دارای ماهیت الکترونیکی است که حاوی اطلاعات هویتی مالک گواهی و تأییدیه مراکز میانی صدور گواهی است. مرکز صدور گواهی الکترونیکی ریشه مجوز ایجاد، امضا و صدور گواهی‌های مراکز میانی را در زیرساختی تحت عنوان زیرساخت کلید عمومی کشور[۲] زیر نظر شورای سیاست‌گذاری گواهی الکترونیکی برعهده دارد.[۳]

از لحاظ حقوقی، تعاملات الکترونیکی امن در ایران تحت نظارت قانون تجارت الکترونیکی ۱۳۸۲ و آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی ۱۳۸۶ است. بدین ترتیب کسانی که متقاضی دریافت امضای الکترونیکی باشند، باید به دفاتر ثبت نام گواهی الکترونیکی مراجعه کنند. این دفاتر متقاضیان را احراز هویت کرده،

۱. ماده ۱۰ قانون تجارت الکترونیکی در تعریف امضای الکترونیکی مطمئن (دیجیتال) توضیح داده است که امضایی است که نسبت به امضاکننده منحصر به فرد بوده و تحت اراده انحصاری وی صادر شده باشد و به همین دلیل در ماده ۱۴ این قانون داده‌پیام‌های مطمئن را از حیث محتویات و امضا در حکم امضای معتبر و قابل استناد در مراجع قضایی دانسته است.

۲. سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور مصوب شورای سیاست‌گذاری گواهی الکترونیکی کشور ۹۱/۴/۷ در بر دارنده مجموعه‌ای از ضوابط و الزامات عملیاتی و امنیتی حاکم بر زیرساخت کلید کشور است. زیرساخت کلید عمومی یا PKI (public key Infrastructure) به مجموعه‌ای از خدمات، محصولات، سیاست‌ها، فرایندها و سیستم‌های نرم‌افزاری و سخت‌افزاری گفته شده که جهت مدیریت و به‌کارگیری گواهی الکترونیکی و به منظور ارائه سرویس‌های امنیتی مختلف مبتنی بر رمزنگاری کلید عمومی استفاده شده است.

۳. از لحاظ فنی، امضای الکترونیکی از طریق رمزنگاری نامتقارن تولید می‌گردد. در زیرساخت کلید عمومی صاحب امضا دارای یک زوج کلید (شامل کلیدهای عمومی و خصوصی) و گواهی الکترونیکی مرتبط با آن است. یک کلید برای رمزنگاری و دیگری برای رمزگشایی است. دو کلید از نظر ریاضی با هم ارتباط دارند؛ به گونه‌ای که داده رمزنگاری‌شده با هر یک، قابل رمزگشایی با دیگری است. بندهای ج، ح، و خ ماده یک آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی ۱۳۸۶، از زوج کلید با عناوین داده‌های ایجاد و وارسی امضای الکترونیکی یاد کرده است.

درخواست‌ها را برای صدور گواهی الکترونیکی به مراکز میانی[1] ارسال و سپس مراکز میانی که از مراکز دولتی صدور گواهی الکترونیکی ریشه[2] مجوز گرفته‌اند، گواهی الکترونیکی[3] صادر و سایر خدمات ارائه می‌کنند. مرکز دولتی صدور گواهی الکترونیکی ریشه هم پس از کسب مجوز از شورای سیاست‌گذاری گواهی الکترونیکی شروع به فعالیت خواهد کرد.[4] بدین ترتیب می‌توان گفت که امضای الکترونیکی در کشور از مدل سلسله مراتبی تبعیت می‌کند. تبصره ۲ ماده ۴ آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی اشاره دارد که سیستم بانکی می‌تواند در صورتی که مجوز شورای سیاست‌گذاری گواهی الکترونیکی کشور را اخذ نماید، اقدام به ایجاد مرکز ریشه مستقل نماید و تبصره ۲ ماده ۱۲ این آیین‌نامه تصریح کرده است که شعب بانک‌ها می‌توانند به عنوان دفاتر ثبت‌نام مراکز میانی تحت نظارت مرکز ریشه نظام بانکی فعالیت کنند. با توجه به اینکه در تبصره و بند (ب) ماده ۴۹ قانون برنامه پنج‌ساله توسعه جمهوری اسلامی ایران ۱۳۸۹، بانک مرکزی مکلف گردیده است که نسبت به ایجاد و بهره‌برداری مرکز صدور گواهی الکترونیک و استفاده از امضای الکترونیک برای شبکه بانکی اقدام نمایند، بانک مرکزی به منظور اینکه امنیت بانکداری الکترونیکی را ارتقا دهد و بستر صدور گواهی امضای دیجیتال و ایجاد هویت دیجیتالی امن را فراهم نماید اقدام به پیاده‌سازی سامانه نماد[5] (نظام مدیریت امنیت داده‌ها) نموده است.[6] در این راستا بانک مرکزی در اردیبهشت ماه ۱۳۹۲ اقدام به انتشار دو سند کرده، خط‌مشی مرکز گواهی که نیازمندی‌های عملیاتی، حقوقی و فنی مرکز گواهی را تشریح کرده و دستورالعمل اجرایی مرکز گواهی که به تشریح دستورالعمل‌ها و روش‌های اجرایی برای صدور و نگهداری و استفاده از گواهی‌های صادره توسط مرکز گواهی بانک مرکزی پرداخته است. بر اساس این اسناد، صدور گواهی به شکل ساختار سلسله مراتبی است و

۱. دستورالعمل اجرایی مراکز صدور گواهی الکترونیکی میانی مصوب شورای سیاست‌گذاری گواهی الکترونیکی کشور ۱۳۸۸/۲/۱۹.

۲. سیاست‌های گواهی مرکز ریشه مصوب شورای سیاستگذاری گواهی الکترونیکی کشور ۸۶/۷/۳۰.

۳. به منظور استفاده از گواهی که معرف مرکز گواهی، صاحب و دارنده گواهی، کلید عمومی، دوره اعتبار و شماره سریال گواهی است، ابزاری فیزیکی بنام توکن در اختیار صاحب یا دارنده گواهی قرار گرفته است. دو نوع از این ابزار در حال حاضر کاربرد دارد که یکی کارت هوشمند و دیگری توکن (USB) است.

۴. مرکز دولتی صدور گواهی الکترونیکی ریشه، مجوز تأسیس مراکز میانی دولتی بازار سرمایه، نفت، بازرگانی، و مرکز میانی پارس ساین را صادر کرده است.

۵. نماد سامانه‌ای به منظور تضمین امنیت، محرمانگی، صحت، دقت و انکارناپذیری در نظام بانکی است.

۶. سامانه نهاب (نظام هویت سنجی الکترونیکی بانکی) به عنوان پرتال نماد پیاده‌سازی شده است، شعب بانک‌هایی که به عنوان دفاتر پیشخوان خدمات گواهی الکترونیک بانکی (نماد) می‌باشند، از طریق این سامانه اقدام به تخصیص شماره شناسایی منحصر به افراد در شبکه بانکی می‌نمایند، این شماره شهاب (شناسه هویت الکترونیکی بانکی) است.

مرکز گواهی ریشه بانک مرکزی که در بالاترین سطح قرار دارد، مراکز گـواهی بـانکی و گواهی مشتریان بانکی[1] را در ذیل خود جای داده است. بدین ترتیـب دفـاتر پیشـخوان خدمات گواهی بانکی هویت اشخاص متقاضی را با ارائه اسـناد و مـدارک مثبتـه احـراز کرده و توکن فیزیکی که از طرف مرکز گواهی اختصاص داده شده است را به متقاضیان تحویل خواهند داد. پیش‌بینی شده است تا فعال‌سازی تـوکن بـرای شناسـایی صـاحب گواهی از طریق ابزار دسترسی گذرواژه بیومتریک (مثل اثر انگشت) باشد تا در حد لزوم داده‌های فعال‌سازی از استفاده غیرمجاز محافظت گردد. بنابراین، این سامانه دارای یـک زیرساخت یکپارچه است و این امکان را در اختیار مشتریان شبکه بانکی قرار داده است تا صرف‌نظر از اینکه کدام بانک به آنها خدمات ارائه مـی‌دهـد، بتواننـد بـا یـک گـواهی امضای دیجیتال از خدمت کلیه بانک‌ها استفاده نماینـد.[2] پـس صـدور گـواهی امضـای دیجیتال برای مشتریان شبکه بانکی و ایجاد پایگـاه جـامع اطلاعـات هـویتی مشـتریان حقیقی و حقوقی به عنوان زیربنای بانکداری اینترنتی و بانکداری مجازی اسـت.[3] بـدین ترتیب می‌توان گفت که امضای الکترونیکی مطمئن (دیجیتال) به عنوان بستر بانکداری مجازی، قابل استفاده از طریق سامانه نماد برای همه بانک‌هـا اسـت. ایـن امضـا همـان توکن یا دستگاه سخت‌افزار و رمزنگاری است که حاوی ابزاری از جنس داده الکترونیکی بوده و به عنوان گواهی الکترونیکی شناخته می‌شود.[4] این ابزار می‌تواند یک نرم‌افـزار یـا یک کارت هوشمند باشد که نسبت به توکن ضریب امنیتی پایین‌تـری دارد. بـه محـض

۱. صدور گواهی برای کارکنان بانک‌ها، کارکنان دفاتر پیشخوان خدمات گواهی، تجهیزات سخت‌افزاری عملیـات بین بانکی و درون بانکی با مرکز گواهی بانکی است و مرکز گواهی مشتریان بانکی اقـدام بـه صـدور گـواهی برای مشتریان حقیقی یا حقوقی بانک یا سامانه‌ها می‌نماید.

۲. با توجه به اینکه سامانه نماد راه‌اندازی نشده است، در حال حاضر شاهد به‌کارگیری گـواهی‌هـای الکترونیکـی داخلی در سیستم بانکی می‌باشیم که در بسیاری از موارد اسـتانداردهای منطبـق بـا سیاسـت‌هـای شـورای سیاست‌گذاری گواهی الکترونیکی کشور رعایت نشده و حتی الزامات امنیتی نظیر ساختار پروفایـل گـواهی، طول کلید، پارامترهای کلید و دوره اعتبار گواهی مد نظر قرار نگرفته است.

۳. شورای پول و اعتبار در تاریخ ۱۳۹۰/۲/۲۷ آیین‌نامه تأسیس و فعالیت بانک‌های مجازی را تصـویب نمـوده اسـت. بانک مجازی بانکی است که شعبه ندارد و دریافت سپرده، اعطای اعتبار، صدور حوالـه، ضـمانت‌نامـه و گشـایش اعتبارات اسنادی را از طریق درگاه‌های الکترونیکی مثل اینترنت، خودپرداز، پایانه فـروش، تلفـن همـراه و غیـره انجام می‌دهد. به دلیل اینکه مرکز گواهی مشتریان بانکی راه‌اندازی نشده، تاکنون هیچ بانـک مجـازی در کشـور مجوز فعالیت دریافت نکرده است. لازم به ذکر است، مطابق بند (د) ماده ۴۶ قانون برنامه پنج‌ساله پـنجم توسـعه ۱۳۸۹ و آیین‌نامه اجرایی آن ۱۳۹۱، وزارت کشور (سـازمان ثبـت احـوال) مکلـف اسـت در صـدور کـارت‌هـای هوشمند ملی، امضای الکترونیکی را پیش‌بینی نماید، شیوه تصدیق هویت و دسترسـی بـه اطلاعـات شـخص در کارت نیز منوط به انطباق اثر انگشت صاحب کارت و اثر انگشت ذخیره‌شده در تراشه است.

۴. بند (ج) ماده یک آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکـی مصـوب ۱۳۸۲ گـواهی الکترونیکـی را تعریف نموده است، داده الکترونیکی حاوی اطلاعاتی در مورد مرکز صـادرکننده گـواهی، مالـک گـواهی، تـاریخ صدور و انقضا، کلید عمومی مالک و یک شماره سریال است که توسط مرکز میانی تولید شده است، بـه گونـه‌ای که هر شخص می‌تواند به صحت ارتباط بین کلید عمومی و مالک آن اعتماد کند.

اینکه مشتری بانک کد کاربری و گذرواژه اختصاص داده شده را وارد نماید، این ابزار به صورت خودکار اقدام به تولید رمز نموده و داده‌پیام‌های ارسالی را رمزنگاری و برای مخاطب[1] که همان بانک است ارسال خواهد کرد. ماده ۱۵ قانون تجارت الکترونیکی ۱۳۸۲ نسبت به این امضا انکار و تردید را مسموع ندانسته و صرفاً ادعای جعل را پذیرفته است. بدین ترتیب می‌توان گفت که سامانه‌های بانکی به شیوه رمزنگاری دارای تدابیر حفاظتی است، رمزنگاری از طریق توکن (تراشه) یا کارتی که به سیستم رایانه‌ای کاربر وصل شده است انجام گرفته و صرفاً از طریق درگاه‌های مجازی یا اینترنتی امکان دسترسی به سرویس‌دهنده‌های مرکزی در مراکز نگهداری داده بانک‌ها فراهم است. پس دسترسی غیرمجاز به سامانه بانک یا مستلزم ساختن غیرمجاز توکن یا کارت است که دستیابی به الگوریتم‌های رمزنگاری ضروری است. در این صورت اگر از توکن استفاده شود و دسترسی غیرمجاز صورت پذیرد، مشمول سه عنوان کیفری قانون جرایم رایانه‌ای است. جعل (بند ب ماده ۷۳۴)، استفاده از تراشه (توکن) جعلی (ماده ۷۳۵) و دسترسی غیرمجاز (ماده ۷۲۹) عنوان این جرایم است.

روش دیگری که برای دستیابی غیرمجاز وجود دارد، استفاده از توکن (تراشه) بدون رضایت صاحب آن است که امکان دارد مفقود یا سرقت شده و یا بدون اجازه صاحب آن استفاده شده باشد. پس هر چند دسترسی غیرمجاز به روش فنی انجام نشده، چون هدف از جرم شناختن دسترسی غیرمجاز حمایت از سامانه‌های حفاظت شده است می‌توان گفت دسترسی غیرمجاز تحقق یافته است.[2]

دستگاهی که توکن نامیده شده و در قانون جرایم رایانه‌ای به عنوان تراشه شناخته شده است، از لحاظ فنی سخت‌افزار امنی است که از طریق واسطه‌های نرم‌افزاری، امکان نگهداری امن کلیدهای رمزنگاری و اجرای ایمن مکانیزم‌های رمزنگاری را با کارایی مطلوب فراهم آورده است. بدین ترتیب سامانه و داده‌ها دارای تدابیر حفاظتی است. پس اگر کسی تدابیر تأمینی سامانه را نقض کند، تدابیر تأمینی داده‌ها را نیز نقض کرده است. این حالت مشمول تعدد مادی است و بر اساس ماده ۱۳۴ قانون مجازات اسلامی ۱۳۹۲ تعیین کیفر می‌گردد. از طرف دیگر، چون عملیات

۱. طبق بند (ج) ماده ۲ قانون تجارت الکترونیکی ۱۳۸۲ مخاطب شخصی است که اصل‌ساز قصد دارد وی داده‌پیام را دریافت کند.

۲. با توجه به ماده ۵۶ قانون جرایم رایانه (۷۸۳ بخش تعزیرات قانون مجازات اسلامی) ماده ۶۸ قانون تجارت الکترونیکی نسخ ضمنی شده است. لازم به توضیح است که رفتارهای ورود و تغییر در قانون جرایم رایانه‌ای آمده است و رفتارهای محو و توقف هم بر ضد تمامیت داده و سامانه هستند و با جعل نزدیکی ندارند و از طرف دیگر مصادیقی که برای استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضا به طورخاص آورده شده است، در حالت اول، استفاده از کلید اختصاصی بدون مجوز صادرکننده به عنوان دسترسی غیرمجاز است و دو حالت بعدی همان تولید غیرقانونی توکن یا کارت هوشمند (جعل) است.

رمزنگاری در امضای دیجیتال ماهیت جداگانه از رمز دارد، اگر کسی قصد داشته باشد تا به محتوای کلید خصوصی دسترسی یافته و با کشف رمز اقدام به جاسوسی، کلاهبرداری یا سرقت نماید، چون مستلزم دسترسی به داده‌های در حال انتقال به سامانه‌های رایانه‌ای است، مرتکب جرم شنود غیرمجاز قانون جرایم رایانه‌ای (ماده ۷۳۰) گردیده است.

نتیجه‌گیری

از بعد فنی و اجرایی ابزارهای احراز هویت و دسترسی به خدمات بانکداری الکترونیک تعریف و احصاء شده، ولی تاکنون مستندسازی قانونی انجام نشده است. نوآوری تحقیق پیش رو از این جهت است که اقدام به برقراری ارتباط بین ابعاد فنی و حقوقی این ابزارها که امضای الکترونیکی نامیده می‌شود، نموده است و بر اساس تعاریفی که در بند (ی) ماده (۲) و ماده (۱۰) قانون تجارت الکترونیک از امضای الکترونیکی ذکر شده و تعاریف فنی که از ابزارهای امنیتی بانکداری الکترونیکی وجود دارد، مصادیق امضای الکترونیکی را در بانکداری نوین تعریف کرده است. بر این اساس عمده‌ترین تفاوتی که بین امضای الکترونیکی ساده و دیجیتال (پیشرفته) وجود دارد وجود کلید عمومی در فرایند امضا است. امضای الکترونیک ساده صرفاً روش ساده‌ای از وارد کردن متون و یا اشکال خاصی به درون دستگاه الکترونیکی است و ثبت تراکنش مستلزم استفاده از رمز اول یا رمز اینترنتی است. ولی امضای دیجیتال، نرم افزاری است که در دستگاه سخت‌افزار رمزنگاری (توکن) که توسط یک مرکز صدور گواهی الکترونیکی پشتیبانی شده است. این امضا از جنس داده‌های الکترونیکی است، بر اساس توابع ریاضی ساخته‌شده و با متن سند ترکیب و داده‌های خود را تبدیل به محتوای رمزی می‌کند، به طوری که جز توسط کلید مقارنی که جفت نرم‌افزار تولید امضا است، رمزگشایی نمی‌شود. بدین ترتیب هر گیرنده اطلاعاتی می‌تواند منبع و تمامیت اطلاعات را تشخیص دهد. این ساختار برای افزایش ضریب امنیتی تبادلات الکترونیکی بین‌بانکی است، امکان ایجاد پایگاه جامع اطلاعات هویتی مشتریان را فراهم کرده و به عنوان جزء اساسی سامانه نماد (نماد مدیریت امنیت داده‌ها) که توسط بانک مرکزی طراحی و پیاده‌سازی شده است، به حساب می‌آید. پس امضای الکترونیکی ساده در بانکداری اینترنتی همان نام کاربری و گذرواژه است. گذرواژه از کاراکترهای مختلف مثلاً ترکیب حروف و ارقام تشکیل شده، ثابت یا متغیر است یا در پرداخت‌های مبتنی بر کارت که از طریق درگاه‌های الکترونیکی انجام می‌شود، رمز دوم (اینترنتی) است و در خدماتی که از درگاه‌های حضوری مثل خودپرداز ارائه می‌شود همان کارت پرداخت بانکی مغناطیسی یا هوشمند است که به همراه ثبت گذرواژه (رمز اول) که در دستگاه درج می‌شود، امکان تراکنش بانکی را فراهم کرده است، مفهوم امضای الکترونیکی ساده را تشکیل می‌دهد. ساختار امضای الکترونیکی دیجیتال (مطمئن) یا پیشرفته نیز همان دستگاه سخت‌افزار رمزنگاری (توکن) یا کارت است، از مجموعه‌ای از سخت‌افزار و نرم‌افزار تشکیل شده که ترکیب آنها فرایند و منطق رمزنگاری را به طور خودکار اجرا می‌کنند. با توجه به تعریفی که در ماده ۱۰ قانون تجارت الکترونیکی از

امضای مطمئن ارائه شده است، ثبت نام کاربری و گذرواژه برای دسترسی به سامانه نماد یا ثبت گذرواژه برای راه‌اندازی توکن از اجزای امضای دیجیتال نیست. بنابراین می‌توان گفت که امضا الکترونیکی همان رمز است که در نوع ساده به صورت دستی به دستگاه وارد می‌شود ولی در نوع دیجیتال نرم‌افزار متصل به رایانه به طور خودکار رمز را وارد می‌نماید. بنابراین باید بین دو مفهوم رمز و رمزنگاری تفاوت قایل شد. در رمزنگاری از نوعی رمز یا کد استفاده می‌شود. یعنی به جای کلمات واقعی از کلمات کُدشده استفاده می‌شود. بنابراین اگر در حال انتقال شنود شود، معنی آن برای همه به جز دریافت‌کننده نامفهوم است، مگر اینکه شخصی که دسترسی غیرمجاز یافته است بتواند رمزگشایی کند.

ممکن است به تعریف امضای الکترونیکی ایرادی وارد باشد. ایرادی که از نظر فنی ـ حقوقی به این فرضیه وارد است، تعریف امضای الکترونیکی ساده در بانک است. شاید این سؤال مطرح شود که در تعریف قانونی امضای الکترونیکی ساده آمده است، امضای الکترونیکی علامت منضم‌شده به داده پیام است. چگونه ممکن است گذرواژه و کارت بانکی ترکیب و متصل به تراکنش بانکی شوند و مشابه امضای الکترونیکی مطمئن (دیجیتال) که از طریق رمزنگاری صادر می‌شود، گذرواژه و کارت بانکی جزء جدایی‌ناپذیر محتوای پیام اصلی شده و بدین ترتیب به نحو منطقی به داده‌پیام (تراکنش) متصل شود. برای پاسخ دادن به این ایراد باید گفت که بستر تراکنش‌های بانکی بین کاربر و سرویس‌دهنده‌های بانکی ترکیبی از گذرواژه و پروتکل‌های امن است. رمزنگاری محتوای پیام‌ها حاصل ترکیب رمز و تراکنش بانکی است. بدین ترتیب است که گذرواژه و کارت بانکی نیز به عنوان امضای الکترونیکی به حساب می‌آیند.

از طرف دیگر جرم مستقیم که نسبت به این نوع امضا واقع می‌شود، برخلاف امضای دستی که جعل است، دسترسی غیرمجاز بوده و جعل رایانه‌ای می‌تواند جرم ثانویه باشد. به همین دلیل بزه دسترسی غیرمجاز یک جرم مانع (بازدارنده) است و علی‌رغم اینکه به عنوان یک رفتار مقدماتی می‌تواند دروازه سایر جرایم رایانه‌ای باشد، ولی الزامی ندارد پس از دسترسی غیرمجاز جرایم دیگری مثل کلاهبرداری، سرقت، تخریب و غیره واقع شود، هر دو عمل از لحاظ کیفر در حکم یک عمل تلقی شود. بنابراین اگر دسترسی غیرمجاز با سایر جرایم رایانه‌ای همراه باشد، همچنان جرایم جداگانه بوده و از موارد تعدد واقعی جرایم است. اما موضوع دیگری که در رابطه با جرم دسترسی غیرمجاز قابل ذکر است این نکته می‌باشد که اگر موضوع جرم سامانه‌هایی باشد که حاوی داده‌های سری است و شخص تدابیر چنین سامانه‌هایی را نقض کند، اگر قصد دسترسی به این داده‌های سری را داشته باشد هر چند به داده‌های سری دسترسی نیابد، مشمول ماده ۷۳۲ قانون مجازات اسلامی می‌گردد.

منابع

- احمدی، سیدمحمود؛ خندان سویری، مهدی، نظام‌های پرداخت و بانکداری الکترونیک در ایران، پژوهشکده پولی و بانکی بانک مرکزی، ۱۳۹۴.
- خلیل میثاقی ممقانی، ابراهیم، «نقش امضا و اثر انگشت از نظر قانونی»، ماهنامه کانون سر دفتران، دوره اول، شماره ۱۸۶، تیر ۱۳۵۴.
- زرکلام، ستار، اعتمادسازی در تجارت الکترونیکی، چاپ اول، شهر دانش، ۱۳۹۰.
- شمس، عبدالله، آیین دادرسی مدنی، جلد ۳، چاپ بیست و سوم، انتشارات دراک، ۱۳۹۲.
- عالی‌پور، حسن، حقوق کیفری فناوری اطلاعات، چاپ اول، انتشارات خرسندی، ۱۳۹۰.
- فخاری، امیرحسین، اندیشه‌های حقوقی (۳): حقوق تجارت، چاپ اول، انتشارات مجد، ۱۳۸۷.
- قنبری، علیرضا، حقوق تجارت الکترونیک، چاپ اول، انتشارات جنگل، ۱۳۹۳.
- مبینی دهکردی، علی؛ رسولی‌نژاد، احسان، شکل‌دهی به فضای نوین: رویکرد دانش بنیان، چاپ اول، نشر نور علم، ۱۳۹۰.
- میرمحمد صادقی، حسین، جرایم علیه اموال و مالکیت، چاپ سی و پنجم، نشر میزان، ۱۳۹۲.
- ــــــــــــــــــ ، جرایم علیه امنیت و آسایش عمومی، چاپ بیست و دوم، نشر میزان، ۱۳۹۲.