دانشگاه علمی‌کاربردی

عنوان

امضای دیجیتالی

استاد محترم

آقای مهندس احمد پهلوان

نگارش

فرناز رضوانی

تابستان 84

فهرست مطالب

مقدمه

فصل دوم - تفسیري باري مدل قانوني

فصل سوم- نیازمندیهای قانونی

فصل چهارم - گسترش ایمني SOAP

مقدمه

بخش اول-مدل قانون UNCITRAL درامضاهای الکترونیکی (2001)

مقاله اول- حدود وحوزه استعمال:

این قانون در جایی بکار می‌رود که امضاهای الکترونیکی در محتویات فعالیتهای بازرگانی استفاده می‌شوند که در اصل هیچ دستوری از قانون اداره شده برای محافظت ومصرف کنندگان را در بر نمی‌گیرد وشامل آنها نمی‌شود.

مقاله دوم- تعریفات:

برای اهداف این قانون:

a) امضای الکترونیکی در اصل اطلاعاتی را معنی می‌دهند که بطور منطقی به شکل الکترونیکی، با یک پیام اطلاعاتی ضمیمه و یا همراه می‌شود که ممکن است برای شناسایی کردن امضا کننده در رابطه با پیام اطلاعاتی و نشان دادن موافقت امضا کننده در مورد اطلاعت گنجانده شده در پیام اطلاعاتی استفاده شد.

B) گواهینامه و سند رسمی‌در واقع یک پیام اطلاعاتی یاتایید وتصدیق رکورد دیگری را معنی می‌دهد که ارتباط میان یک امضا کننده واطلاعات ایجاد شده از یک امضا را در بر دارد.

C) پیام اطلاعاتی در حقیقت اطلاعات ایجاد شده فرستاده شده، دریافت شده یا خیره شده توسط ابزار الکترونیکی و اپتیکال و یا ابزاری شبیه به آنها را معنی می‌دهد که نه تنها به مبادله اطلاعات الکترونیکی (EDI)، پست الکترونیکی، تلگرام، تلکس و تله کپی محدود نمی‌شود بلکه یا بر روی واسطه خود عمل می‌کند یا بر روی واسطه شخصی که آن را ارائه می‌دهد عمل می‌کند.

d) امضاء کننده با الواقع شخصی را معنی می‌دهد که اطلاعات ایجاد شده توسط امضاء را منعقدمی‌کند که این مطلب یا بر روی واسطه خودش عمل می‌کند ویا بر روی واسطه شخصی که آن را ارائه می‌دهد عمل می‌کند.

e) فراهم کننده خدمات گواهینامه یا سند رسمی‌در اصل شخصی را معنی می‌دهد که اسناد رسمی‌وگواهینامه ها را صادر می‌کند وممکن است خدمات دیگری که وابسته به امضاهای الکترونیکی هستند را فراهم کند.

f) شخص مورد اعتماد ومطمئن در اصل شخصی را معنی می‌دهد که می‌تواند در زمینه و بنیاد یک گواهینامه یا سند رسمی‌و یا یک امضای الکترونیکی عملیاتی را انجام دهد.

کمیسیون، متن زیر را برای کشورهای مشترک المنافع انگلستان که ممکن است گسترش وتوسعه قابلیت استعمال این قانون را طلب کنند، ارائه و پیشنهادی می‌دهد: این قانون در جایی بکار می‌رود که در اصل امضاهای الکترونیکی مورد استفاده می‌گیرند، به استثنای موقعیتها و شرایطی که در پایین اعلام شده است. واژه بازرگانی یا تجاری باید به یک تفسیری گسترده اتلاق شود که موضوعات و مباحث برخاسته از همه رابطه ها و ارتباطات یک ماهیت و طبیعت بازرگانی و تجاری را بپوشاند، خواه اینکه قرار دادی و پیمانی باشد یا نباشد که البته شامل ارتباطات یک ماهیت تجاری می‌شود اما محدود به معاملات و داد و ستدهای زیر نمی‌شود که عبارتند از: هر معامله تجاری که برای ذخیره کردن یا معامله کالا و خدمات بکار می‌رود، توافق توزیع، نمایندگی و یا معرفی کالای تجاری، بصورت فاکتور در آوردن و فاکتور، اجاره دادن، ساختار و بنای کارها، تجزیه و تحلیل ومشورت کردن، طرح کردن و ساختن و اداره کردن، جواز دادن، سرمایه گذاری کردن، از لحاظ مالی اداره کردن و یا همکاری کردن در شغل و حرفه، حمل کالاها و مسافران توسط راههای هوایی، دریایی، راه آهن و جاده است.

مقاله سوم- رفتار وعکسل العمل مساوی تکنولوژیهای امضاء:

هیچ چیزی در این قانون به استثنای مقاله پنجم نباید اثر قانونونی هر روش بوجود آورنده امضای الکترونیکی را که نیازمندیهایی که به مقاله ششم، پاراگراف اول نسبت داده می‌شود را مستثنی، محدود و یا محروم ومعزول کند در غیر اینصورت نیازمندیهای قانون کاربردی و قابل استعمال را ظاهر می‌کند.

مقاله چهارم- تفسیر وترجمه:

(1) در تفسیر ترجمه این قانون، در نظر داشتن بنیاد تفسیری و نیاز به پیشرفت در متحده الشکلی و یکسانی استعمالش و اعتبار کالا از مسائل عمده و قابل توجه در این قانون است.

(2) درخواستها و سوالات مرتبط با مطالب و مباحث اداره شده توسط این قانون که بطور تشریحی در آن مستقر نمی‌شوند. در شکلی یکنواخت و یکسان با اصول کلی ای که این قانون بر روی آنها پایه ریزی می‌شود. مقرر و نشانده می‌شوند.

مقاله پنجم- اصلاح و دگرگونی توسط توافق:

مواد و بندهای این قانون ممکن است فسخ و یا کاسته شوند و یا اینکه اثر آنها توسط توافق می‌توانند متفاوت شوند، مگر اینکه موافقت قانونی و معتبر نباشد و یا اینکه تحت قانون قابل استعمالی موثر واقع نشود.

مقاله ششم- موافقت و انجام کار توسط یک نیازمندی برای یک امضا:

(1) در جایی قانون نیاز به امضای یک شخص دارد که نیازمندی در ارتباط با یک پیام اطلاعاتی ظاهر می‌شود. اگر یک امضای الکترونیکی به همان اندازه و درجه اطمینان استفاه شود آنگاه این امضاء

برای هدفی که در آن پیام اطلاعاتی بوجود آورده می‌شود و یا ارتباط داده می‌شود. اختصاص داده خواهد شد.

(2)پاراگراف اول به این منظور بکار می‌رود که ببینیم آیا نیازمندی که در آن هست در شکل یک ضمانت نسبت داده می‌شود و یا اینکه آیا این قانون به سادگی، نتایجی را برای فقدان یک امضاء فراهم می‌کند یا نه!

(3)یک امضای الکترونیکی مورد توجه و رسیدگی قرار می‌گیرد برای مطمئن شدن از هدف بر طرف کردن نیازهایی که در پاراگراف اول نسبت داده می‌شود، اگر

a) اطلاعات ایجاد شده توسط امضاء که در محتویات متن است فقط به شخص امضاء کننده ونه هیچ شخص دیگری نسبت داده می‌شود.

b) اطلاعات و دانستی های بوجود آمده توسط امضاء که در زمان امضاء کردن پدیدار شده اند تحت کنترل امضاء کننده ونه هیچ شخص دیگری است.

c) هر اصلاح، تغییر و تبدیلی که بعد از زمان امضاء کردن در یک امضای الکترونیکی بوجود می‌آید. قابل آشکار سازی است.

d) جایی که یک هدف از نیازمندی قانونی برای یک امضاء در اصل فراهم کردن تعهد واطمینان جهت درستی وصحت اطلاعاتی است که بعد از زمان امضاء کردن بوجود می‌آید.با هر اصلاح، تغییر و تبدیلی که بعد از زمان امضاء کردن قابل آشکار سازی است. مرتبط می‌شود.

4) پاراگراف سوم توانایی هر شخص را محدود نمی‌کند به:

a) دایر ومستقر کردن در هر روش دیگری که برای هدف بر طرف سازی نیازمندیهایی که به پاراگراف اول نسبت داده می‌شود و قابلیت اطمینان یک امضای الکترونیکی را فراهم می‌کند

b) ذکر واظهار کردن گواهی غیر قابل اعتماد و اطمینان یک امضای الکترونیکی

5) بندها و مواد این مقاله برای مطالب داخل کروشه [...] پایین بکار نمی‌رود.

مقاله هفتم- رضایتمندی و برطرف سازی مقاله ششم:

(1) (هر شخص، سازمان و یا اختیارات واعتبارات، خواه خصوصی باشند یا عمومی، بصورت قانونی در آوردن کشور مشترک المنافع انگلستان بعنوان یک کشور ذی صلاحیت تفکیکی ومشخص می‌شود) می‌تواند تعیین کند که امضاهای الکترونیکی، بندها و مواد مقاله ششم این قانون را قانع و رفع حالت می‌کند.

(2) هر تعیینی که تحت پاراگراف اول ساخته می‌شود باید محتوی استاندارد های بین المللی شناخته شده باشند.

(3) هیچ چیزی در این مقاله بر روی عملکرد دستورات قانون بین المللی خصوصی اثر نمی‌گذارد.

مقاله هشتم- هدایت وراهنمایی امضاء کننده:

(1) جایی که اطلاعات ایجاد شده توسط امضاء می‌توانند برای بوجود آوردن یک امضایی که اثر قانونی دارد، بکار روند هر امضاء کننده باید:

A)توجه مستدلی را برای اجتناب و پرهیز از کاربرد غیر مجاز در مورد اطلاعات ایجاد شده توسط امضایش را تمرین کند.

B)بدون تاخیر و وقفه غیر ضروری و زائد. ابزار و وسایلی را مورد استفاده قرار دهد که توسط فراهم کننده خدمات گواهینامه و اسناد رسمی‌مطابق با مقاله نهم این قانون ساخته

می‌شود و یا به عبارتی دیگر تلاشهای مستدلی را بکار می‌برد که برای اطلاع دادن به هر شخصی که می‌تواند بطور مستدل توسط امضاء کننده برای اطمینان حاصل کردن از خدمات و یا فراهم کردن خدمات در تقویت و پشتیبانی از امضای الکترونیکی استفاده کند اگر: (i) امضاء کننده بداند که اطلاعات بوجود آمده توسط امضاء بطور قرار داد غیر رسمی‌و قولنامه تسویه و مصالحه شده است و یا (ii) شرایط محیطی، رویدادها وچگونگی انجام این رویدادهای شناخته شده یک شروعی را برای یک ریسک اساسی و مهم به امضاء کننده ارائه دهد که در اینصورت اطلاعات ایجاد شده توسط امضاء بطور قرار دادی غیر رسمی، تسویه و مصالحه شده است.

(c)در جای که یک سند رسمی‌و گواهینامه برای تقویت و پشتیبانی از امضای الکترونیکی استفاده می‌شود، توجه مستدلی را برای اطمینان یافتن از صحت، درستی و تکمیل همه موضوعات ارائه های ساخته شده توسط امضاء کننده تمرین می‌کند که مربوط به سراسر گواهینامه یا سند رسمی‌هستند و یا اینکه در چرخه موجودیش احاطه شده در این سند رسمی‌می‌باشند.

(2) یک امضاء کننده باید در برداشته باشد نتایج قانونی عدم موفقیتش را که توسط آن نیازمندیهای پاراگراف اول بر طرف می‌شود. در بر داشته باشد

مقاله نهم- هدایت و راهنمایی فراهم کننده خدمات سند رسمی‌یا گواهینامه

(1) جایی که یک فراهم کننده خدمات گواهینامه یا سند رسمی، خدماتی را برای حمایت و پشتیبانی از یک امضای الکترونیکی فراهم می‌کند که می‌تواند برای اثر قانونی بعنوان یک امضاء استفاده شود که البته فراهم کننده خدمات گواهینامه باید:

a) مطابق با نمایشها و ارائه هایی که توسط آن و با توجه به تجربه ها، کارها و سیاستهایش ساخته می‌شود، عمل می‌کند.

b) توجه مستدلی را برای اطمینان یافتن از صحت، درستی و تکمیل همه موضوعات نمایشها وارائه های ساخته شده توسط امضاء کننده بوجود آمده است راتمرین کند که مربوط به همه جوانب گواهینامه و سند رسمی‌هستند و یا اینکه در چرخه موجودیش احاطه شده در این سند رسمی‌می‌باشند.

c) ابزار قابل دسترس و مستدلی را فراهم کند که توانایی تهیه یک شخص مورد اعتماد را برای تحقیق و ثابت کردن گواهینامه یا سند رسمی‌داشته باشد:

(i)شناسایی کردن فراهم کننده خدمات گواهینامه یا سند رسمی

(ii) امضاء کننده که در گواهینامه یا سند رسمی‌شناخته می‌شود، کنترلی بر روی اطلاعات ایجاد شده توسط امضاء در زمانی که سند رسمی‌گواهینامه فرستانده می‌شود دارد

(iii) اطلاعات ایجاد شده توسط امضاء در زمان صدور گواهینامه و یا قبل از آن معتبر و قانونی می‌باشند. (d) ابزار قابل دسترس و مستدلی را فراهم کند که توانایی تهیه شخص مورد اعتماد را برای تحقیق و اثبات کردن گواهینامه یا سند رسمی‌داشته باشد یا در غیر اینصورت

(i) روش بکار برده شده ای را برای شناسایی امضاء کننده استفاده کند.

ii)هر محدودیتی در هدف یا ارزیابی برای اطلاعات ایجاد شده توسط امضاء و یا گواهینامه ممکن است استفاده شود.

iii) اطلاعات ایجاد شده توسط امضاء معتبر و قانونی هستند و بصورت قرار داد غیر رسمی‌و قولنامه، تسویه نمی‌شوند.

(iv) هر محدودیت در هدف یا توسعه و گسترش مسئولیت و آمادگی مقرر شـده، توسـط فـراهم کننده خدمات گواهینامه یا سند رسمی‌تصریح می‌شود.

(v) دانستن این مطلب که آیا ابزار موجود به امضاء کننده توجه و تذکری مطابق با مقاله هشتم، پاراگراف اول (b) در این قانون می‌دهد یا نه (vi) فهمیدن این مطلب که آیا خدمات زمانبدی شده و فسخ شده ارائه می‌شود یا نه e جایی که خدمات تحت پاراگرافهای فرعی (d) (v) ارائه می‌شوند. یک ابزاری را برای امضاء کننده فراهم می‌کند که تذکری را مطابق یا مقاله هشتم، پاراگراف اول (b) در این قانون می‌دهد. جایی که خدمات تحت پاراگرافهای (d) (vi) ارائه می‌شود، قابلیت دسترسی به یک خدمات بهنگام و فسخ شده ای را اطمینان می‌دهد. (f) سیستمهای مورد اعتماد، روندهای عمل و منابع بشری را در انجام خدماتش مورد استفاده قرار دهد.

(2) یک فراهم کننده خدمات گواهینامه یا سند رسمی‌باید نتایج قانونی عدم مـوفقیتش را بـرای نیازمندیهای پاراگراف اول روفع آنها در برداشته باشد.

مقاله دهم- درستی وقابلیت اعتماد:

برای اهداف مقاله نهم، پاراگراف اول (f) در این قانون تعیین و با توسعه هر سیستم، روندهای عمل ومنابع بشری مورد استفاده قرار داده شده توسط یک فراهم کننده خدمات گواهینامه یا سند رسمی، مورد اعتماد هستند که البته شامل فاکتورهای زیر می‌شود:

a) منابع بشری و مالی که شامل وجود مساعده ها، سرمایه ها وچیزهای با ارزش ومفید می‌شود.

b) کیفیت سیستمهای نرم افزاری وسخت افزاری

c) روندهای عملی که برای پیشرفت تدریجی دادن هر گواهینامه یا سند رسمی‌و استعمالاتی برای گواهینامه ها و نگهداری رکوردها استفاده می‌شود.

d) قابلیت دسترسی به اطلاعت برای امضاء کنندگان شناخته شده در گواهینامه و اشخاص مورد اعتماد نهانی.

e) قابلیت تنظیم و توسعه تحقیق و بازرسی توسط یک شخص ونیروی مستقل.

f) وجود یک اظهار نامه و یا بیانیه توسط یکی از کشورهای مشترک المنافع انگلستان، یک اعتبار نامه یا فراهم کننده خدمات گواهینامه با در نظر داشتن برآوردی که سابقا ذکر شده بود.

g) هر فاکتور مناسب دیگر:

مقاله یازدهم- هدایت و راهنمایی شخص مورد اعتماد:

یک شخص مورد اعتماد در اصل نتایج قانونی عدم موفقیتش را در بر دارد:

a) داشتن گامهای مستدل برای رسیدگی کردن به قابلیت اطمینان یک امضای الکترونیکی

b) جایی که یک امضای الکترونیکی توسط یک گواهینامه دادن حمایت و پشتیبانی می‌شود، گرفتن و در نظر داشتن گامهای مستدل:

i) رسیدگی کردن به قابلیت اعتماد واعتبار، وقفه یا فسخ گواهینامه دادن،

ii) مشاهده کردن همه محدودیتها با توجه به گواهینامه دادن.

مقاله دوازدهم- شناسایی گواهینامه ها و امضاهای الکترونیکی بیگانه:

(1) در تعیین و توسعه یک گواهینامه یا یک امضای الکترونیکی بطور قانونی موثر واقع می‌شود. وهیچ توجهی نباید داده به :

a) موقعیت جغرافیایی که گواهینامه یا سند رسمی‌فرستاده می‌شود و یا امضای الکترونیکی بوجود آورده و یا استفاده می‌شود.

b) موقعیت جغرافیایی که مکان شغلی فرستنده یا امضاء کننده است.

(2) یک گواهینامه ای که به خارج فرستاده شده، اگر بطور اساسی و عمده یک سطح برابـری از قابلیت اطمینان و اعتماد را ارائه دهد آنگاه باید بعنوان یک گواهینامه صادر شده، اثر قانونی یکسانی را در بر داشته باشد.

(3) یک امضای الکترونیکی بوجود آمده و یا استفاده شده در خارج، اگر بطور اساسی و عمده یک سطح برابری از قابلیت اطمینان و اعتماد را ارائه دهد آنگاه باید بعنوان یک امضای الکترونیکی بوجود آمده یا استفاده شده، اثر قانونی یکسانی را داشته باشد.

(4) در تعیین اینکه آیا یک گواهینامه یا یک امضای الکترونیکی بطور اساسی وعمده یک سـطح برابری از قابلیت اطمینان واعتماد را برای اهداف پاراگراف دوم یا سـوم ارائـه مـی‌دهـد یـا نـه، بایـد استاندارد های بین المللی شناخته شده و یا فاکتورهای مناسب دیگری را در بر داشته باشد.

(5) با وجود اینکه توافق در میان بخشهای پاراگرافهای 2،3و 4 همانطور کـه در میـان خودشـان است بکار می‌رود و برای استفاده انواع معینی از امضاهای الکترونیکی و گواهینامه ها در نظر گرفتـه شده است اما این توافق باید برای اهداف شناسایی میان مرزی مناسب وکافی شناخته شود، مگر اینکه این توافق معتبر وقانونی نباشد و یا تحت قانون قابل استفاده موثر نباشد.

بخش دوم- راهنمایی برای صورت قانونی به مدل قانونی دادن UNCITRAL درامضاهای الکترونیکی (2001)

اهداف این سازمان:

در آماده سازی وتعدیل کردن مدل قانون UNCITRAL در امضاهای الکترونیکی (همچنین در این انتشار بعنوان مدلی از قانون یا مدل جدیدی از قانون نسبت داده می‌شود)، کمیسیون ملتهای متحده در قانون تجارت بین المللی (UNCITRAL) بر این امر متفکر واندیشناک شدند که این مدل قانون یک ابزار موثرتری برای صورت امروزی دادن به قانونگذاریشان است اگر زمینه واطلاعات توصیفی که برای شعب زیادی از دولتها و قانونگذاران فراهم می‌شود، آنها را در استفاده از این مدل قانون کمک ویاری کند. همچنین کمیسیون از این احتمال آگاه و مطلع بود که این مدل قانون در یک تعداد از کشورهای مشترک المنافع با آشنایی محدود شده به نوع تکنیکهای ارتباطی که در این مدل قانون مورد مطالعه قرار می‌گیرد، استفاده خواهد شد. این راهنمایی، بیشتر از سوی کارآزمودگان این مدل قانون صادر می‌شود که همچنین برای مصرف کنندگان دیگر این متن مفید واقع می‌شود که مصرف کنندگان دیگر آن عبارت از قاضی ها، قانونگذاران، شاغلین اهل این حرفه خاص واعضای انجمن علمی‌می‌باشند. اینگونه اطلاعات می‌توانند کشورهای مشترک المنافع را در مورد مطالعه قرار دادن بندها و موادی که باید در پذیرفتن نمونه های مخصوص ملی که ناگزیر از اینگونه تغییرات و تحقیقات هستند، کمک می‌کند. در آماده سازی این مدل از قانون، این مطلب وا نمود می‌شود که این مدل قانون توسط یک چنین راهنمایی ضمیمه وهمراه خواهد شد. برای مثال، این مطلب تصمیم گیری می‌شود که تعدادی از نتایج که در این مدل قانون جای داده و مستقر نمی‌شود، به آدرس راهنمایی شده توسط کشورهای مشترک المنافع که این مدل از قانون را وضع می‌کنند فرستاده می‌شوند. اطلاعات ارائه شده در این راهنمایی برای توضیح دادن این مطلب مورد نظارت قرار می‌گیرد

که چرا بندها و مواد در این مدل قانون بعنوان ساختارهای اساسی مورد نیاز یک وسیله قانونی طراحی شده برای بدست آوردن مشاهدات این مدل قانون گنجانده شده است.

(2) راهنمایی حاضر برای وضع قانون توسط پیرو محرمانه ای برای درخواست UNCITRAL مهیا شده است که در نزدیکی جلسه سی و چهارم در سال 2001 ساخته شد. این مطلب بر روی سنجش، مشاوره، نظرات و تصمیم های کمیسیون در آن جلسه پایه ریزی می‌شود. در صورتی که این مدل از قانون تعدیل می‌شود،به همان اندازه که در ملاحظات گروه کار تجارت الکترونیکی صورت می‌گیرد که کار آماده سازی را هدایت می‌کند.

فصل دوم

تفسیری برای این مدل از قانون I- هدف و اساس این مدل قانونی

A- هدف:

استفاده افزایش یافته تکنیکهای معتبر سازی الکترونیکی بعنوان جانشینهایی برای امضاهای دست نوشته شده و دیگر روندهای معتبر سازی سنتی و رسمی، پیشنهاد شده است، که نیاز به یک شبکه قانونی ویژه را برای عدم قطعیت اثر قانونی که می‌تواند از استفاده اینگونه تکنیکهای مدرن و امروزی نتیجه شود را کاهش می‌دهد. (که می‌تواند بطور کلی بعنوان امضاهای الکترونیکی نسبت داده شوند).

خطری که دسترسیهای قانونی گرفته شده در کشورهای مختلف را با توجه به امضاهای الکترونیکی تغییر ومختلف می‌کند، برای مواد و بندهای قانونی و یکنواخت همشکل، دایر کردن قوانین بنیادی را که ذاتا یک پدیده و واقعه بین المللی است را مکشوف می‌سازد که در اینصورت هماهنگی قانونی به همان اندازه قابلیت عملکرد متقابل تکنیکی می‌باشد.

با ساختن اصول اساسی توسعه نیافته در مقاله هفتم مدل قانون UNCITRAL بر روی تجارت الکترونیکی و با توجه به تکمیل عملکرد امضاء در یک محیط الکترونیکی، این مدل جدید قانون برای کمک کردن به کشورهای مشترک المنافع در تاسیس کردن یک شبکه قانونی مدرن، هماهنگ شده و مطلوب جهت آدرس دادن موثرتر برای امضاهای الکترونیکی طراحی می‌شود. در یک الحاقیه حائز اهمیت برای مدل قانون UNCITRAL در تجارت الکترونیکی، مدل جدید قانون، استاندارد های کاربردی را بر خلاف قابلیت اطمینان تکنیکی امضاهای الکترونیکی که می‌توانند اندازه گیری شوند، ارائه می‌شوند. علاوه بر این، این مدل قانون یک پیوستگی میان قابلیت اعتماد تکنیکی و اثر قانونی که ممکن است از یک امضای الکترونیکی داده شده انتظار رود، فراهم می‌کند. این مدل قانون بطور عمده به UNCITRAL در تجارت الکترونیکی توسط وفق دادن یک دسترسی تحت اثر قانونی یک تکنیک امضای الکترونیکی داده شده که ممکن است قبلا مقرر شده باشد، اضافه می‌شود. (یا ناحیه

تشخیص داده شده برای اینکه واقعا مورد استفاده قرار گیرد). بدین ترتیب، اینگونه مدل قانونی که برای فراهم کردن موجبات پیشرفته در نتیجه امضاهای الکترونیکی و اطمینان حاصل کردن از این که تکنیکهای امضای الکترونیکی معین می‌توانند قانونا بر طبق معاملات و داد وستدهای حائز اهمیت موثق و مورد اعتماد شوند، مورد نظارت و اداره قرار می‌گیرند، علاوه بر این، با مستقر کردن قابلیت انعطاف پذیری اختصاصی برای یک مجموعه از قوانین بنیادی هدایت کردن بخشهای مختلفی که می‌توانند در استفاده امضاهای الکترونیکی گنجانده شوند، این مدل قانونی می‌تواند در شکل دادن هماهنگ تر تجارت و تمرینات بازرگانی و تجاری کمک کند.(یعنی امضا کنندگان، اشخاص مورد اعتماد و فراهم کنندگان خدمات در گواهینامه بخش سوم).

مشاهدات این مدل از قانون که شامل توانایی برای تهیه کردن یا به آسانی انجام دادن استفاده امضاهای الکترونیکی و فراهم کردن رفتاری مساوی برای مصرف کنندگان شواهد پایه ریزی شده بر روی کاغذ ومصرف کنندگانی که اطلاعات آنها پایه ریزی شده بر روی کامپیوتر است برای فراهم کردن وسایل پیشرفت اقتصادی و فعالیت مفید در تجارت بین المللی لازم و ضروری است با بهم پیوستن و شبیه سازی روندهایی در این مدل از قانون که مشمول مرور زمان می‌شوند(و همچنین بندها و موادی از این مدل قانونی UNCITRAL در تجارت الکترونیکی) در قانونگذاری ملی اش برای این موقعیتها یعنی جایی که بخشها برای استفاده از ابزار الکترونیکی ارتباطی بکار می‌رود، یک وضع قانون بطور اختصاصی محیط نیمه طبیعی را بوجود خواهد آورد.دسترسی نیمه طبیعی که در مدل قانون UNCITRAL واقع در تجارت الکترونیکی استفاده می‌شود می‌تواند جهت فراهم کردن اصولی برای تامین زیانها توسط بیمه در همه موقعیتهای واقعی یعنی جایی که اطلاعات بوجود آورده، ذخیره و با یکدگیر مرتبط می‌شوند، تحت نظارت قرار خواهند گرفت و صرفنظر از اینگونه اطلاعات

می‌توانند ضمیمه و الصاق شوند. (نگاه کنید به راهنمـایی وضـع قـانون UNCITRAL در تجـارت الکترونیکی واقع در پاراگراف 24). کلماتی که رد (یک محیط نیمه طبیعی) بکار رفته است همانطور که در مدل قانون UNCITRAL در تجارت قانونی والکترونیکی موجود است. اصول غیر امتیازی را در میان اطلاعات حمایت شده توسط عاملی مانند کاغذ واطلاعات مرتبط شده و ذخیره شده بصورت الکترونیکی منعکس می‌کند. قانون جدید از این مدل بطور مساوی اصولی را منعکس می‌کند که هیچ امتیاز نشان تمیزی را نباید میان تکنیکهای مختلف ساخته شود که ممکن است برای مرتبط کردن یا ذخیره اطلاعات بطور الکترونیکی استفاده شود، یک اصل کلی است که اغلب بعنـوان حـد متوسـط تکنولوژی داده می‌شود (CN,9/484/ و پاراگراف 23)

B – زمینه

این مدل از قانون یک گام جدیدی را در یک مجموعه از ابزار وسایل بین المللی منصوب می‌کند که توسط UNCITRAL تعدیل و وفق داده می‌شـود کـه بطـور ویـژه بـر روی نیازهـای تجـارت الکترونیکی متمرکز می‌شوند یا در ذهن نیازهای ابزار مدرن و امروزی ارتباطات را مهیا و آماده سازی می‌کند. در اولین طبقه بندی، ابزار و وسایل مخصوصی آماده کار می‌شود که شامل راهنمایی قانونی در انتقال الکترونیکی سرمایه (1987)، مدل قانون UNCITRAL در انتقال اعتبـار بصـورت بـین المللی و مدل قانون UNCITRAL در تجارت الکترونیکی (1996,1998) می‌شود. دومین طبقـه بندی شامل همه کنفرانسها و قرار دادهای نیمه رسمی‌بین المللی و ابزار قانونگذاری دیگر که توسـط UNCITRAL از سال 1978 تعدیل شده اند و همه پیشرفتهایی که از نظر ظـاهر سـازی کـاهش یافته اندو احاطه ارتباطات تحقق بخشیده شده را معنی می‌دهند، می‌شود.

بهترین ابزار شناخته شده UNCITRAL در زمینه تجارت الکترونیکی همان مدل قانون UNCITRAL در تجارت الکترونیکی است که آماده سازی آن در سال 1990 از مصرف توسعه یافته ابزار مدرن ارتباطی از قبیل پست الکترونیکی وتبادل الکترونیکی اطلاعات برای هدایت معاملات تجاری بین المللی استنتاج می‌شود. از این مطالب فهمیده می‌شود که تکنولوژی های جدید که به سرعت توسعه یافته اند بیشتر بعنوان حمایتهای تکنیکی از قبیل بزرگراههای اطلاعاتی و اینترنت که بطور گسترده تری در دسترس هستند، گسترش خواهند یافت. به هر حال، بطور قانونی ارتباط اطلاعات حائز اهمیت در شکل پیامهای بی کاغذ توسط موانع قانونی برای مصرف اینگونه پیامها ویا توسط عدم قطعیت در اثر یا قابلیت اعتبارشان بی نتیجه می‌شوند و به تاخیر خواهند افتاد. با یک نظریه در سهولت مصرف افزایش یافته ابزار مدرن وامروزی ارتباطات، UNCITRAL یک مدل قانونی UNCITRAL را در تجارت الکترونیکی مهیا و آماده کرده است هدف مدل قانون UNCITRAL در تجارت الکترونیکی، ارائه کردن قانونگذاران ملی در یک مجموعه از قوانین قابل قبول بین المللی است که چگونگی یک تعداد از اینگونه موانع قانونی را که ممکن است بر طرف شوند و چگونگی مطمئن تر ساختن محیط قانونی را که ممکن است. برای آنچه که بعنوان تجارت الکترونکیی شناخته شده بوجود آید را نشان می‌دهد. (8) رای و تصمیم توسط UNCITRAL برای مدل قانونگذاری فرمول بندی شده در تجارت الکترونیکی بر پاسخگویی در این امر پایه ریزی شده که، در یک تعداد از کشورها، با وجود ارتباطات قانونگذاری اداراه شده و ذخیره اطلاعات باز هم این امر ناکافی و قدیمی‌به نظر می‌رسد زیرا توجه دائم به استفاده تجارت الکترونیکی ندارد. در موارد و حالتهای معین، با وجود قانگذاری باز هم محدودیتهای در مصرف ابزار و وسایل مدرن و امروزی در ارتباطات نسبت داده شده و دلالت می‌کند برای مثال می‌توان اسناد و مدارک اصلی را که نوشته

وامضاء شده را نـام بـرد. بـا توجـه بـه تصـوراتی در مـورد اینگونـه اسـناد و مـدارک، مـدل قـانون UNCITRAL در تجارت الکترونیکی یک دسترسی را تعدیل می‌کند که بر روی تعادل عملکردی پایه ریزی شده است. دسترسی معادل و مشابه عملکردی بر روی یک تجزیـه و تحلیـل از اهـداف و عملکردهای نیازمندیهای سنتی و رسمی‌پایه ریزی می‌شود که با یک نقطه نظر برای تعیین چگونگی این اهداف یا علملکردها می‌تواند تکنیکهای تجارت الکترونیکی را تکمیل و صورت عمل دهـد. (نگـاه کندی به راهنمایی در وضع قانون مدلUNCITRAL در تجارت الکترونیکی، پاراگراف 18-15)

در زمانی که مدل قانون UNCITRAL در تجارت الکترونیکی مورد آماده سازی قرار می‌گیـرد، یک تعداد کمی‌از کشورها بندها و مواد ویژه ای را برای سرو کار داشتن با جنبه های معینی از تجارت الکترونیکی تعدیل کرده اند. بهر حال، در آنجا هیچ قانونگذاری وجود ندارد که با تجارت الکترونیکی، بعنوان یک اصل وعمومیت سرو کار داشته باشد. این مطلب می‌تواند در عدم قطعیت قانونی وقابلیت اعتبار اطلاعات ارائه شده در یک شکل دیگری از یک سند کاغذی سنتی نتیجه شود. علاوه بر این، هنگامی‌که قوانین منطقی و دقیق در همه کشورها، مورد نیاز واقع می‌شود آنگاه اسـتفاده از EDI و پست الکترونیکی منتشر خواهد شد. این نیاز همچنین در بسیاری از کشورها بـا توجـه بـه اینگونـه تکنیکهای ارتبـاطی ماننـد تلـه کپـی و تلکـس، احسـاس مـی‌شـود. تحـت مقالـه 2 (b) از قـانون UNCITRAL در تجارت الکترونیکی، EDI بعنوان انتقال الکترونیکـی اطلاعـات از کـامپیوتر بـه کامپیوتر با استفاده از یک استاندارد توافق شده برای ساختار اطلاعات تعریف می‌شود.

مدل قانون UNCITRALدر تجارت الکترونیکی همچنین به رفع خسارت ضررها و زیانهایی که از قانونگذاری نامناسب و ناکافی منشعب می‌شود کمک می‌کند این قانونگذاری نامناسب در سطح ملی، موانعی را برای تجارت بین المللی بوجود می‌آورد که یک مقدار حائز اهمیت و قابل توجهی را برای استفاده از تکنیکهای ارتباطات مدرن و امروزی مرتبط می‌کند. برای یک توسعه بزرگ، عدم توافق در میان آنها و عدم قطعیت در مورد آنها دستورات و طرز اداره قانون ملی، مصرف این گونه تکنیکهای ارتباطی را نظارت و اداره می‌کند که می‌توانند برای محدود کردن توسعه شغل که ممکن است بازارهای بین المللی را در دسترس قرار دهد را نتیجه دهند. (11) علاوه بر این، در یک سطح بین المللی، مدل قانونی UNCITRAL در تجارت الکترونیکی می‌تواند در موارد معین یک وسیله برای تفسیر کردن وجود قرار دادهای غیر رسمی‌بین المللی و دیگر ابزار بین المللی که موانع قانونی را برای استفاده تجارت الکترونیکی بوجود می‌آورند. مفید و سودمند واقع شود برای مثال شواهد و مدارک معینی وتعهدات قرار دادی و پیمانی را که به شکل نوشته شده ساخته می‌شوند را مشمول مرور زمان می‌کنیم. در میان بخشهای کشورهای مشترک المنافع اینگونه ابزار و وسایل بین المللی توافقی را برای مدل قانون UNCITRAL در تجارت الکترونیکی بعنوان یک قانون تفسیر می‌تواند ابزاری را جهت شناختن استفاده تجارت الکترونیکی و مرتفع ساختن نیاز به مذاکره در مورد پروتکل که ابزار بین المللی را در بر دارد فراهم کند.

C- تاریخچه:

بعد از تعدیل و درست کردن مدل قانون UNCITRAL در تجارت الکترونیکی، کمیسون در جلسه بیست و نهمین در سال 1996 تصمیم گرفت که به صدور امضاهای دیجیتالی واختیارات گواهینامه در نمایندگی مکافیت دهد. گروه کادر تجارت الکترونیکی برای امتحانی جهت قابلیت

تناسب و مطلوبیت و همچنین اجرای آماده سازی قوانین یکنواخت در این مباحث مورد سئوال واقع شدند.این مطلب شامل توافقی می‌شود که در مورد قوانین متحد الشکل برای آماده سازی بکار می‌رود وباید با اینگونه نتایجی که بعنوان بنیاد قانونی از روند های عمل گواهینامه حمایت می‌کند، سرو کار داشته باشد که البته شامل موارد زیر می‌شود: ظاهر کردن اعتبار سازی دیجیتالی و تکنولوژی گواهینامه دادن، قابلیت کاررد روند عمل در گواهینامه دادن، اثبات و اختصاص تعیین مکان ریسک و جلب اعتماد مصرف کنندگان و فراهم کنندگان که در محتویات مصرف تکنیکهای گواهینامه دادن گنجانده می‌شوند، صدور اختصاصی گواهینامه بواسطه استفاده از دفاتر ثبت اسناد، اتصال وتلفیق توسط مرجع ها. (13) در جلسه سی ام در سال 1997، کمیسیون کار جلسه سی و یکم را به گروه کار گزارش داده است. (A/CN.9/437) که بر روی بیناد یک یادداشت نوشته شده بر روی کاغذ بطور محرمانه هدایت می‌شود.(A/CN.9/WG.IV/WP.71) گروه کار به کمیسیون نشان داد که این مطلب نتایجی را بعنوان یک امر مهم و مورد نیاز برای کار بدست آورده است که هماهنگی و سازگاری را در قانونگذاری این عرصه در بر دارد. گروه کار به نتایج مقدماتی رسیده است که این مطالب عملی و قابل اجرا برای مبادرت کردن به آماده سازی قوانین متحد الشکل این طرح در صدور امضاهای دیجیتالی و اختیاراتی برای گواهینامه بود و همچنین ممکن و میسر در موضوعات و مباحث مرتبط می‌شد. گروه کار یاد آوری کرد که در کنار امضاهای دیجیتالی و اختیاراتی برای گواهینامه، کار در عرصه تجارت الکترونیکی نیز می‌تواند نیاز به آدرس دادن داشته باشد که عبارتند از: صدور تناوبهای الکترونیکی و تکنیکی برای به رمز نوشتن توسط کلید عمومی، نتایج کلی عملکردهای انجام شده توسط فراهم کنندگان خدمات بخش سوم، بستن قرار داد و معاهده بصورت الکترونیکی (A/CN.9/437,paras 156, 757) کمیسیون، نتایجی را که توسط گروه کار بدست آمده را

تصدیق و امضاء می‌کند و آن را برای آماده سازی قوانین متحده الشکل درنتایج قانونی امضاهای دیجیتالی واختیاراتی در گواهینامه واگذار و محول می‌کند.

با توجه به هدف دقیق وساختار متحد الشکل قوانین، کمیسیون بطور عمده با این مطلب توافق می‌کند که هیچ تصمیمی‌نباید در نخستین مرحله روند عمل ساخته شود، این مطلب احساس می‌شد که، هنگامیکه کار گروه بطور اختصاصی توجه اش را بر روی نتایج امضاهای دیجیتالی بطور آشکار متمرکز می‌شود آنگاه نقش برتر و برجسته توسط با رمز نوشتن کلید عمومی‌بازی می‌شود. بدین ترتیب، قوانین یکنواخت و متحد الشکل نباید استفاده از تکنیکهای معتبر سازی را منع کند. علاوه بر این، در سرو کار داشتن با رمز نویسی توسط کلید عمومی، قوانین متحدالشکل ممکن است نیاز به تطبیق دادن سطوح مختلف ایمن سازی و شناسایی کردن اثرات قانونی مختلف و سطوح قابلیت اعتماد که مرتبط با انواع مختلف خدمات هستند، داشته باشد که در محتویات امضاهای دیجیتالی گنجانده می‌شوند. با توجه به اختیاراتی که در گواهینامه وجود دارد، هنگامیکه مقادیر ارزیابی استانداردهای مشتق شده از بازار توسط کمیسیون شناسایی می‌شود آنگاه این مطلب بطور گسترده احساس می‌شود که کار گروه ممکن است با برقراری یک کمیته مقدار استاندارد ها روبررو شود که توسط اختیارات گواهینامه با آنها تماس حاصل می‌شود.

کار گروه با آماده سازی قوانین متحد الشکل در سی و دومین جلسه که بر روی بنیاد یک یادداشت آماده شده توسط secrateriat است، شروع می‌شود (A/CN.9/WG.17/WP.73).

در جلسه سی و یکم در سال 1998 کمیسیون کار گروه را در جلسه سی و دوم گزارش داد. (A/CN.9/446) این مطلب قابل ذکر است که کار گروه در جلسه سی و یکم و سی دوم مشکلات ارائه شده را در بدست آوردن یک نتیجه معمولی و رایج از قانون جدید آزمایش کرده است که

برخواسته از استفاده افزایش یافته امضاهای دیجیتالی و دیگرامضاهای الکترونیکی است . یک توافـق عمومی‌با وجود این که چگونگی این تنایج را توضیح می‌دهد باز هم ممکن است بطور بین المللی در یک شبکه قانونی قابل قبول، مرتب وتصحیح شود که این امر بطور عمده توسط کمسـیون احسـاس می‌شود.

گروه کار در اصل اصلاح و تجدیدی نظر بر روی قوانین متحدالشکل را در جلسه سی و سـوم در سال 1998 انجام می‌دهد و در جلسه سی و چهارم در سال 1999 بر روی بنیاد یادداشـتهای آمـاده توسـط secretariat کـار مـی‌کنـد. گزارشـتات جلسـات در اسـناد و مـدارک A/CN.9/457,A/CN.9/454 گنجانده می‌شوند.

در جلسه سی و سوم، کمیسیون به گروه کار در مورد دو جلسه قبل گزارش می‌دهـد. (A/CN 9/454,A/CN.9/457) کمیسیون تقدیرش را برای تلاشهایی که توسط گروه کار صورت گرفته در آماده سازیش برای قوانین متحد الشکل ویکنواخت توضیح داد. هنگامی‌که کمیسیون بطور کلی، مورد توافق واقع شد، پیشروی حائز اهمیتی در این جلسات در ارتباط نتایج قانونی امضـاهای الکترونیکـی ساخته می‌شود. همچنین این مطلب احساس می‌شود که گروه کار در ساختار یک توافق عمومی‌بعنوان یک سیاست قانوگذارنده با مشکلاتی مواجه شده اند که در این سیاست، قوانین متحد الشکل باید پایه ریزی بشوند.

نقطه نظری که در آن بطور متداول دسترسی بدست آمده توسط گروه کار توضیح داده می‌شود، بطور کافی گروه کار نیاز شغلی را برای قابلیت انعطاف پذیری در استفاده امضاهای الکترونیکی ودیگر تکنیکهای معتبر سازی منعکس نمی‌کند. بطور معمول و متداول، قوانین متحد الشکل تاکید مفرط را بر روی تکنیکهای امضای دیجیتالی و درون حوزه فعالیت امضاهای دیجتالی وهمچنین بـر روی یـک

استعمال مخصوص که قسمت سوم گواهینامه را در بر دارد، جایگذای می‌شود. این مطلب ارائه و پیشنهاد می‌شود که کار بر روی امضاهای الکترونیکی توسط گروه کار یا باید به نتایج قانونی گواهینامه محدود شود و یا اینکه به تعویق انداخته شود تا تمرینات و تجارب بازار بهتر مستقر شوند. یک نقطه نظری که برای اهداف تجارت بین المللی توضیح داده می‌شود این است که بیشتر نتایج قانونی که برخواسته از استفاده امضاهای الکترونیکی است تا کنون در تجارت الکترونیکی واقع در مدل قانونی UNCTTRAL تجزیه وتحلیل شده است.

بطور گسترده مستولی شدن بر این نقطه نظر و بکار واداشتن آن چنین بود که گروه کار باید وظیفه اش را در بنیاد دستور و وکالت نامه اصلی اش دنبال کند. با توجه به نیاز برای قوانین متحد الشکل درامضاهای الکترونیکی این مطلب توضیح داده شده بود که در بسیاری از کشورها راهنمایی گرفتن از مدل قانون UNCTTRAL توسط اختیارات دولتی و قانون گذاری مورد توقع و انتظار واقع می‌شود که در روند عمل آماده سازی قانوگذاری در صدور و امضاهای الکترونیکی بودند و شامل تاسیس و برقراری شالوده ها و سازمانهای کلید عمومی(PKI) یا دیگر پروژه های وابسته به این مبحث می‌شود (نگاه کنید به A/CN.9/457 paxi 19) همانطور که برای تصمیمی‌که توسط گروه کار جهت متمرکز کردن بر روی نتایج PKI واصطلاحات علمی‌یا فنی PKI عمل شد، این مطلب قابل ذکر است که بازی متقابل ارتباطات میان انواع مجرای بخشهای مرتبط با یک مدل PKI امکان پذیر است اما مدلهای دیگر قابل حصول وتصور نبودند برای مثال جایی را می‌توان نام برد که هیچ فراهم کننده خدمات برای گواهینامه های مستقل وجود ندارد یکی از مزیتهای عمده برای متمرکز شدن بر روی نتایج PKI در اصل به آسانی انجام دادن ساختار سازی قوانین متحد الشکل توسط رجوع به سه

عملکرد یا نقش با توجه به کلیدهای جفتی است که عبارتند از: امضاء کننـده کلیـد و عملکـرد آن، عملکرد گواهینامه و عملکرد اطمینان سازی است.

بعد از مباحثه، کمیسیون مجددا تصمیمات اولیه اش را تصدیق کرد تا امکان پذیری آماده سـازی اینگونه قوانین متحد الشکل و اطمینان، توضیح داده شده در مورد آن توسط گروه کار در جلسات در شرف وقوع انجام شد.

گروه کار در جلسه سی و پنجمش در سپتامبر سال 1999 به کارش ادامه داد و در جلسه سی و ششـــم در فبریـــه 2000 بـــر روی بنیـــاد نکتـــه هـــای آمـــاده شـــده کـــارکرد. (A/CN.9/WG.IV/WP.82,A/CN.9/WG.IV/WP.84)

در جلسه سی و سومش در سال 200 کمیسیون تقدیرش را برای تلاشهای توسعه داده شده توسط گروه کار توصیف کرد و پیشروی بدست آمده در آماده سازی قوانین متحد الشکل را تشریح کرد. به گروه کار اصرار ورزیده می‌شد که کارش را با توجه به قوانین متحد الشکل در جلسـه سـی و هفـتم تکمیل کند. در آماده سازی مدل قانون UNCITRAL، گروه کار توجه کرد به این مطلب که فراهم کردن یک سری اطلاعات الحاقی تکمیل کننده که مرتبط با مدل قانون UNCITRAL است امری مفیـد و سـودمند مـی‌باشـد. بـا پیـروی از دسترسـی گرفتـه شـده از آمـاده سـازی مـدل قـانون UNCITRAL در تجارت الکترونیکی، حمایت و تقویت کلی برای یک طرح پیشنهاد بوجود آمد که متضمن این مطلب بود که مدل جدید قانون UNCITRAL باید توسط یک راهنمایی جهت کمک کردن به کشورهای مشترک المنافع در وضع کردن قانون و بکار بردن مدل قانون انجام شود. در ایـن رابطه کمیسیون از گروه کار درخواست کرد که راهنمایی طرح را برای وضع قانون مرور کند.

گروه کار آماده سازی قوانین متحد الشکل و یکنواخت را در جلسه سی و هفـتمش در سـپتامبر 2000 تکمیـل کـرد کـه گـزارش و شـرح حـال آن جلسـه در مـدرک و سـند معرفـی بـا عنـوان A/CN.9/483 گنجانده می‌شود. در محتویات جلسات سی و هفتم و هشتم، گروه کار همچنین در مورد راهنمایی وضع قانون در بنیاد یک طرح مهیا شده بحث کـرد (AKN.9/WG.IV/WP.88) گزارش وشرح حـال جلسـه سـی و هشـتم کـه توسـط گـروه کـار انجـام شـد در مـدرک و سـند A/CN9.484 گنجانده می‌شود. گروه کار متذکر و یاد آور شد که قوانین متحد الشکل ویکنواخت به همراه راهنمای طرح جهت وضع قانون باید به کمیسیون جهت تجدید نظر و تعدیل در جلسه سی و چهارم در سال 2001 ارائه داده شود.

در آماده سازی برای جلسه سی و چهارم کمیسیون، متن مدل قانون برگزیده شده که توسط گروه کار تصویب شد برای همه دولتها جهت علاقمند کردن سازمانهای بین المللی بـرای تفسـیر ونظریـه دادن، دایر و منتشر شد. در آن جلسه کمیسیون گزارش کار جلسات سی و هفتم و سی و هشتم را به گروه کار ارائه داد . در شروع این مباحثه، کمیسیون نظریه ها و طرحهایی را که از دولتها و سازمانهای بین المللی بدست آمده بود را مـورد توجـه و مطالعـه قـرار داد. (ضـمیمه 3-1 و A/CN-9/492) ملاحضات تکمیل شده اش در طرحهای پیشنهادی که توسط نمایندگی های موجود در بنیاد نظریات ارائه شده توسط دولتها و ارگانهای بین المللی برخواسته شده بود کمیسیون با یک مرور و تجدید نظر قاعده دارد د رمقالات طرح و یک تجدید نظر در راهنمایی وضع قانون یک پیشرفت تدریجی کرد. بعد از ملاحظه و رسیدگی به متن مدل قانون برگزیده شده که توسط گروه بر گزیننده و راهنمایی کننده وضع قانون اصلاح و تجدید نظر شده بود، کمیسیون در جلسه هفتصـد و بیسـت و هفـتم در پـنجم جولای 2001 تصمیم و رای زیر را تعدیل و درست کرد: کمیسیون ملتهای متحده در قانون تجـارت

بین المللی: یاد آوری می‌کند که دستور و تعهدش تحت تجزیه و تحلیل و راه حل اشتراکی کلی (xx1)2205 درهفدهم دسامبر سال 1966 صورت گرفته است که در جهت هماهنگی پیشرفته بیشتر ومتحد الشکل کردن قانون تجارت بین المللی با توجه به علایق همه افراد در ذهن آنها است مخصوصا آنهایی که در کشورهای توسعه یافته هستند برای توسعه مفرط تجارت بین المللی بکار می‌رود. همچنین یاد آور می‌شود که توصیه در ارزیابی قانونی رکوردهای کامپیوتری توسط کمیسیون تعدیل و درست می‌شود و در جلسه هجدهم ارائه می‌شود و مدل قانون UNCITRAL در تجارت الکترونیکی که توسط همین کمیسیون تعدیل شده در جلسه بیست ونهم سال 1996 مطرح شد و توسط یک مقاله الحاقی 5 مجددا بوسیله کمیسیون در جلسه سی و یکم سال 1998حرج و تعدیل شد. این کمیسیون متقاعد کرد که مدل قانون UNCTTRAL در تجارت الکترونیکی یک کمک قابل توجهی به کشورهای مشترک المنافع در تهیه کردن و سهولت اجرای استفاده از تجارت الکترونیکی بواسطه افزایش اداره قانوگذاریشان برای استفاده از تناوبهای و تغییرات برای اشکال پایه ریزی شده بر روی کاغذ ارتباطات و ذخیره اطلاعات بواسطه فرمول بندی اینگونه قانوگذاریها است.این کمیسیون سودمندی فراوانی را در مورد تکنولوژیهای جدید استفاده شده برای هویت شخصی در تجارت الکترونیکی و معمولا در امضاهای الکترونیکی را پیشنهاد می‌دهد. این کمیسیون خواستار ساختار اصول اساسی توسعه نیافته را در مقاله هفتم مدل قانون UNCITRAL در تجارت الکترونیکی با توجه به تکمیل عملکرد امضاء در یک محیط الکترونیکی برایشان رفع نیاز می‌کرد. کمیسیون همچنین متقاعد کرد که قطبیت قانونی در تجارت الکترونیکی توسط هماهنگی قوانین قطعی و معین در شناسایی قانونی امضاهای الکترونیکی بطور تکنولوژی بنادی تعریف می‌شود. کمیسیون تصور کرد که مدل قانون UNCITRAL در امضاهای الکترونیکی بطور قابل توجه و حائز

اهمیت به کشورهای مشترک المنافع در افزایش دادن اداره قانوگذاریشان برای استفاده از تکنیکهای قانونی سازی مدرن و در فرمول بندی کردن اینگونه قانوگذاری کمک خواهد کـرد. کمیسـیون ثابـت کرده که این قانون یک نظریه ای است که برقراری و تاسیس مدل قانونگذاری را در راحت اجرا کردن استفاده از امضاهای الکترونیکی با یک روش قابل قبول برای کشورهای مشترک المنافع بـا قانونهـای مختلف و سیسمتهای اجتماعی واقتصادی متفاوت نشان می‌دهد و می‌تواند وسیله توسـعه هماهنـگ سازی را در ارتباطات اقتصادی بین المللی فراهم کند. توافقهای امضاهای الکترونیکی در مدل قـانون UNCITRAL همانطور که در ضمیمه و پیوست II نشان داده شده برای گزارش کمیسیون ملتهای متحده در قانون تجارت بین المللی در اجلاس سی و چهارم همراه بـا راهنمـایی بـرای وضـع قـانون UNCITRAL ظـاهر مـی‌شـود. درخواسـتهای کـاملا محرمانـه بـرای انتقـال مـتن مـدل قـانون UNCITRAL در امضاهای الکترونیکی همراه با راهنمایی جهت وضع قـانون UNCITRAL بـه دولتها و دیگر سازمانهای بین المللی ارائه می‌شود. همچنین توصیهای مناسب و مطلوبی را کشورهای مشترک المنافع در ارتباط با امضاهای الکترونیکی تعدیل شده در سال 1996 برای سهولت کار ارائه می‌دهد.

II. مدل قانون UNCITRAL بعنوان یک ابزار برای هماهنگ سازی قانونها:

همانطور که در مدل قانون UNCTTRAL در تجارت الکترونیکی گفته شد، قانون جدید به شکل یک متن قانونگذاری شده ای است که به کشورهای مشترک المنافع برای همکاری در قانون ملی شان توصیه می‌شود. مدل قانون با متقابل عمل کردن عملکرد طبیعی قوانین بین المللی خصوصی اداره نمی‌شود. بر خلاف یک قرار داد غیر رسمی‌بین المللی، مدل قانونگذاری به این امر نیاز ندارد که کشورهای مشترک المنافع آن را برای اعلام کردن به ملتهای متحده و یا دیگر کشورهایی که ممکن است این قانونگذاری را داشته باشند، وضع قانون شود.

در ترکیب واتصال متن این قانونگذاری در سیستم قانونی یک کشور مشترک االمنافع می‌تواند تعدادی از بندها و ماده های این قانون را اصلاح کند ویا اینکه تعدادی از آنها را کنار بگذارد. در مورد یک قرار داد غیر رسمی، قابلیت امکان پذیری تغییرات برای متن یکنواخت و متحد الشکل توسط قسمتهایی از کشورهای مشترک المنافع ساخته می‌شود که محدودتر می‌باشد.

قرار دادهای رسمی‌قانون تجارت معمولا یا بطور کلی استثناها را نهی می‌کنند و یا فقط تعداد کمی‌از آنها را مجاز می‌کنند. قابلیت انعطاف پذیری ذاتی در قانگذاری واقع در مواردی که احتمالا کشورهای مشترک المنافع، خواهان تغییر و اصلاحاتی در آن هستند قبل از وضع آن بعنوان یک قانون ملی آماده و مهیا خواهد شد. بهر حال، این مطلب نشان می‌دهد که درجه و قطعیت هماهنگ سازی بدست آمده بواسطه این مدل قانونگذاری شباهتش به یک قرار داد غیر رسمی‌کمتر می‌باشد. در هر صورت، این مضرات مدل قانونگذاری می‌تواند توسط این واقعیت که تعداد کشورهای مشترک المنافع هوا کننده این مدل قانوتگذاری در اصل بیشتر از تعداد کشورهای مشترک المنافع خوا خواه یک قرار

داد غیر رسمی‌است، متعادل و متوازن شود. که در دستور بدست آمده از یک درجه رضـایتمندی از هماهنگ سازی این مطلب به کشورهای مشترک المنافع توصیه می‌شود.

این مطلب توسط تعدادی از کشورها مورد مطالعه وبررسی قرار گرفته است که نتایج قـانونی مـرتبط بـا اسـتفاده از امضـاهای الکترونیکـی تـا کنـون توسـط مـدل قـانون UNCTTRAL در تجارت الکترونیکی تجزیه وتحلیل شده است و برای تعدیل و وفق دادن بیشتر قوانین در امضاهای الکترونیکی طرح ریزی نمی‌کند بلکه تجارب بازار را در عرصه های جدید بهتر برقرار می‌کند. بهر حال، کشورهای مشترک المنافع در وضع قانون جدید در کنار مدل قانون UNCTTRAL در تجارب الکترونیکی می‌تواند مزیتهای الحاقی واضافی را انتظار داشته باشد. در این کشورها در اصل اختیارات قانوگذاری و دولتی در روند عمل آماده سـازی قـانون برای نتایج صدور امضاهای الکترونیکی می‌باشد که شامل برقراری PKI و قطعیت در بندها وماده های قانون ارائه شده برای راهنمایی ابزار بین المللی است که توسط نتایج PKI و اصطلاحات فنی موجود در آن آماده سازی و مهیا می‌شود. برای همه کشورها، این مدل از قانون یک سری دستورات بینادی را پیشنهاد و ارائه می‌دهد که می‌توانند بیش از مدل PKI استفاده و به کار برده شوند زیرا آنها با نقش متقابل و عملکرد مجزایی مواجه می‌شوند که در همه انواع امضاهای الکترونیکی گنجانده می‌شـوند و یک عملکرد سومی‌که دراین انواع معین از امضاهای الکترونیکی وجود خواهد داشت.

III نشانه گذاریهای کلی وعمده در امضاهای الکترونیکی- A: عملکردهای این نوع امضاها:

مقاله هفتم از مدل قانون UNCTTRAL پایه ریزی شده بر روی شناسایی عملکردهای یک امضاء در یک محیط کاغذی است. در آماده سازی مدل قانون UNCTTRAL در تجارت الکترونیکی، گروه کار بر روی عملکردهای زیر که توسط امضاهای دست نوشته انجام شدند، بحث کرد: شناسایی یک شخص، فراهم کردن قطعیت برای اختیارات شخصی که شخص در عمل امضاء کردن دارد، محلق شدن شخص به محتویات یک سند و مدرک علاوه بر این، مطلب شایان ذکر است که یک امضاء می‌تواند عملکردهای گوناگونی را که وابسته به ماهیت سندی است که امضاء می‌شود، انجام دهد. مثلا یک امضا می‌تواند نظارت بر یک قسمت از محتویات قرار داد راتصدیق کند.

B: امضاهای دیجیتالی و دیگر امضاهای الکترونیکی:

در بحث مطلوبیت و قابلیت اجرای آماده سازی مدل جدید قانون UNCTTRAL و در تعریف هدف قوانین متحد الشکل و یکنواخت در امضاهای الکترونیکی، UNCTTRAL در اصل تکنیکهای مختلفی از امضای الکترونیکی را مورد آزمایش قرار داده است که یا در حال حاضر مورد استفاده قرار می‌گیرد و یا تحت توسعه می‌باشد. هدف معمول این تکنیکها فراهم کردن معادلات عملکردی از قبیل امضاهای دست نوشته شده و انواع دیگر مکانیسم های معتبر سازی استفاده شده در یک محیط کاغذی است (یعنی مهر وممها و بر چسب ها) تکنیکهای مشابه می‌توانند عملکردهای الحاقی را در محدوده فعالیت تجارت الکترونیکی که مشتق شده از عملکردهای یک امضاء است، انجام دهد. اما این عمل با هیچ معادله دقیق و کاملی در یک محیط پایه ریزی شده بر روی کاغذ مرتبط نمی‌باشد و آنها بهم وابسته نیستند.

امضاهای الکترونیکی در تکنیکهای دیگری از رمز نویسی با کلید عمومی:

در کنار امضاهای دیجیتالی که بر روی رمز نویسی با کلیدعمومی‌پایه ریـزی شـده اسـت، ابـزار و وسایل مختلف دیگری وجود دارد که در نظریه حاشیه ای موجود در مکانیسم های امضا الکترونیکی تحت پوشش قرار می‌گیرد که می‌توانند بطور متداول و مرسوم استفاده شوند یا برای استفاده بیشتر مورد مطالعه و بررسی قرار گیرد. برای مثال تکنیکهای قطعی و معین در اعتبار سازی بواسطه یک ابزار وسیله بیومتریک که بر روی امضاهای دست نوشته شده پایه ریزی شدند مورد اطمینان قرار می‌گیرد در چنین ابزاری، یک امضاء کننده بطور دستی وبا استفاده از یک قلم مخصوص امضاء خواهد کرد که یا برروی صفحه کامپیوتر و با بر روی پد دیجتالی می‌باشد. امضای دست نوشته شده سـپس توسـط کامپیوتر تجزیه و تحلیل خواهند شد وبعنوان یک سری مقادیری که اعداد آن به رمـز نوشـته شـده ذخیره می‌شوند که می‌تواند به یک پیام اطلاعاتی ضمیمه شود.

امضاهای دیجیتالی در رمز نویسی با کلید عمومی:

در نقطه نظر افزایش استفاده از تکنیکهای امضای دیجیتالی در تعدادی از کشورها مقدمات گفتـه شده در پایین ممکن است در رمز نویسی با کلید عمومی‌برای امضاهای دیجیتالی کمک کند.

نظریه های تکنیکی واصطلاحات فنی- (i) رمز نویسی:

امضاهای دیجیتالی با استفاده از رمز نویسی به وجود آورده می‌شوند و مورد تحقیق و بررسی قرار می‌گیرند. شاخه از ریاضیات کاربردی که خودش را با پیام انتقال داده شده مرتبط می‌کند علی الظاهر از شکل پیچیده و نامفهوم به شکل اصلی اش بر می‌گردد. امضاهای دیجیتالی آنچه را که بعنوان رمز نویسی با کلید عمومی‌شناخته شده بود را استفاده می‌کند که اغلب بر روی اسـتفاده از عملکردهـای الگوریتمی‌برای بوجود آوردن دو تفاوت که بطور ریاضی گونه با کلید ها مرتبطند، پایه ریزی می‌شود.

یکی از اینگونه کلید ها برای بوجود آوردن یک امضای دیجیتالی یا اطلاعات انتقال یافته که علی الظاهر بشکل پیچیده و نامفهوم است استفاده می‌شود و دیگری برای تحقیق و بررسی در مورد یک امضای دیجیتالی یا برگرداندن پیام به شکل اصلی اش مورد استفاده قرار می‌گیرد. تجهیزات کامپیوتر نرم افزارها دو نوع از این کلیدها را که اغلب بطور اشتراکی به سیسمتهای رمز نویسی و یا بطور اختصاصی تر به سیسمتهای رمزی نویسی نامتقارن نسبت داده می‌شوند، مورد استفاده قرار می‌دهند این کلیدها در جایی قرار دارند که برای استفاده از الگوریتمهای نامتقارن مورد اطمینان می‌باشند. هنگامی‌که استفاده از رمز نویسی یکی از ساختارهای عمده امضاهای دیجیتالی است واقعیت علامت رمزی که یک امضای دیجیتالی برای معتبر ساختن یک پیام حاوی اطلاعات دیجیتالی مورد استفاده قرار می‌دهد نباید با یک استفاده کلی تر رمز نویسی برای اهداف اطمینان سازی مختل و درهم بر هم شود. قابلیت اطمینان سازی در تقلب یک روشی است که برای رمز نویسی یک ارتباط الکترونیکی فقط توسط شخص گیرنده پیام قابل خواندن می‌باشد و به جز این شخص هیچ فرد دیگری این توانایی را نخواهد داشت.

کلیدهای عمومی‌وکلیدهای خصوصی:

کلید های تکمیلی استفاده شده برای امضاهای دیجیتالی در اصل کلید خصوصی وکلید عمومی‌نامیده می‌شوند که در کلید خصوصی می‌توان گفت که فقط توسط شخص امضاء کننده و برای بوجود آوردن امضای دیجیتالی مورد استفاده قرار رمی‌گیرد و در کلید عمومی‌می‌توان گفت که به طور معمول و گسترده تر توسط یک شخص مورد اعتماد برای تحقیق ورسیدگی به امضاهای دیجیتالی مورد استفاده قرار می‌گیرد. از استفاده کننده از یک کلید خصوصی انتظار می‌رود که کلید خصوصی را بطور سری و محرمانه نگهداری کند. این مطلب باید تذکر داده شود که مصرف کننده منحصر به فرد

نیازی به شناختن ودانستن کلیدخصوصی ندارد. اگر تعداد زیادی از افراد به تحقیق و بررسی امضاهای دیجیتالی امضاء کننده نیاز داشته باشند آنگاه کلید عمومی‌باید قابل دسترس باشد یا اینکه بـه همـه آنها توزیع شود بطور مثال با منتشر کردن آن در یک مخزن ویا هـر شـکل دیگـری از دسـتور نامـه عمومی، یعنی جایی که دسترسی به آن با سهولت و سرعت انجام شود. گر چه کلیدهای جفتی بطور ریاضی گونه بهم مرتبط هستند اما اگر یک رمزنویسی نامتقارن و نامتناسب طراحی و بطور مطمـئن وایمن استفاده شود آنگاه مشتق شدن کلید خصوصی از دانش واطلاعاتی که در کلید عمومی‌وجـود دارد یک امر غیر ممکن خواهد شد.

عملکرد اختلاط و بازسازی:

علاوه بر تولید یک کلیدجفتی، روند بنیادی واصلی دیگری وجود دارد که به طـور کلـی بعنـوان عملکرد باز سازی عنوان می‌شود و در بوجود آوردن و تحقیق و بررسی کردن در مـورد یـک امضـای دیجیتالی مورد استفاده قرار می‌گیرد یک عملکرد بازسازی در اصل یک روند ریاضی گونه است که بر روی الگوریتمی‌پایه ریزی می‌شود که یک ارائه و نمایش دیجیتالی را بوجود می‌آورد، یا شکل متراکم شده و بهم فشرده شده پیام را اغلب به عنوان یک خلاصه پیام ارائه می‌دهد. هنگـامی‌کـه عملکـرد بازسازی یکسان مورد استفاه قرار می‌گیرد هر تغییر برای پیام یک بازسازی مختلفی را بطور غیر قابل تغییر نتیجه خواهد داد.

امضای دیجیتالی:

برای امضاء کردن یک مدرک یاهر بخش اطلاعات دیگر، امضاء کننده اول بطور مختصر و مفید، حد و مرزهای آنچه را که باید امضاء شود را معین می‌کند. سپس یک عملکرد بازسازی در نرم افزار امضاء کننده می‌تواند یک نتیجه بازسازی یکنواختی را برای اطلاعاتی که باید امضاء شوند، محاسبه کند که

این عمل بدین ترتیب است که نرم افزار امضاء کننده، نتایج بازسازی را به یک امضای دیجیتالی با استفاده از کلید خصوصی امضاء کننده انتقال می‌دهد. نرم افزار امضای دیجیتالی یک مقدار منحصر به فردی برای اطلاعات امضاء شده و اطلاعات استفاده شده با کلید خصوصی است که در اینصورت به پیام ذخیره شده یا انتقال یافته دسترسی پیدا می‌کند.

تصدیق و تصویب امضاهای دیجیتالی:

تصدیق و تصویب امضاهای الکترونیکی یک روند کنترل امضای الکترونیکی توسط رجوع به پیام اصلی و یک کلید عمومی‌داده شده است. و در نتیجه تعیین کردن این مطلب که آیا امضای دیجیتالی برای پیامهایی که با استفاده از کلید خصوصی به کلید عمومی‌ارجاع داده شده می‌شوند، بوجود می‌آید یا نه! تصدیق وتصویب امضاهای دیجیتالی توسط محاسبه یک بازسازی جدید پیامهای اصلی بوسیله عملکرد بازسازی یکسان انجام می‌شود. سپس با استفاد از کلید عمومی‌و بازسازی جدید، تصویب کننده کنترل می‌کند که آیا امضای الکترونیکی با استفاده از مرتبط شدن با کلید خصوصی بوجود می‌آید یا نه و آیا اخیرا بازسازی محاسبه شده با بازسازی اصلی که در طول روند امضاء کردن دیجیتالی انتقال داده می‌شود، هماهنگ و سازگار است یا نه! نرم افزار تصویب کننده، امضاهای الکترونیکی را تصدیق خواهد کرد اگر: a کلید خصوصی امضاء کننده برای امضاء کردن بطور دیجیتالی استفاده شود که در اینصورت کلید عمومی‌امضاء کننده فقط یک امضای دیجیتالی بوجود آمده توسط این کلید خصوصی را تصدیق و تصویب می‌کند. b پیامهای غیر متناوب و تغییر نیافته ای که برای اینکه توسط تصویب کننده محاسبه شود در طول روند تصویب از امضاهای دیجیتالی نتیجه شود.

شالوده و زیر سازی کلید عمومی‌ذخیره کنندگان خدمات گواهینامه:

برای تصدیق و تصویب کردن یک امضای دیجیتالی، تصویب کننده باید بـه کلیـد عمـومی‌امضـاء کننده دسترسی داشته باشد و اطمینان حاصل کند که این مرتبط با کلید خصوصی امضـاء کننـده می‌شود. بهر حال، یک جفت کلید عمومی‌و کلید خصوصی، هیچ پیوستگی رمزی و اساسی برای هـر شخصی ندارد، بلکه این به آسانی یک جفت عدد می‌باشد. یک مکانیسـم الحـاقی بـرای پیوسـتن و مشارکت کردن یک شخص مخصوص یا ماهیـت ویـژه بـرای ایـن کلیـدهای جفتـی ضـروری و لازم می‌باشد. اگر رمز نویسی با کلید برای بکار بردن اهداف اداره شده اش مورد استفاده قرار گیرد، آنگاه این مطلب نیاز به فراهم کردن یک روش برای ساخت کلید های قابل دسترس در گوناگونی گسترده ای از اشخاص دارد که تعداد زیادی از آنها برای امضاء کننده شناخته شده نیستند و هیچ ارتباطی بین بخشها گسترش نیافته است برای این اثر، بخشهای احاطه شده باید یک درجه ای از اطمینـان را در کلیدهای خصوصی و عمومی‌داشته باشند. سطح درخواسـت شـده از اطمینـان ممکـن اسـت میـان اشخاصی وجود داشته باشند که نسبت به یکدیگر اعتماد دارند، کسانی که با یکـدیگر در یـک دوره زمانی سرو کار دارند، کسانی که با یکدیگر بر روی سیستم ها ارتباط برقرار می‌کنند، کسانی که درون یک گروه و با هم عملیاتی را انجام می‌دهند و یا کسانی که توانایی اداره کردن معاملاتشـان را بطـور قرار دادی و پیمانی دارند بهر حال، سطح یکسانی اطمینان نمی‌تواند ظاهر شود هنگامی‌که اشـخاص بطور نامکرر با یکدیگر سرو کار دارند، بر روی یک سیستم ارتباط برقرار نکنند. برای عملکردهایشـان در یک گروه نباشند یا اینکه توافقهای مشترکی در تجارت نداشته باشند و یـا قانونونهـای دیگـری را برای اداره کردن روابطشان در بر نداشته باشند علاوه بر این، چون رمز نویسی با کلیـد عمـومی‌یـک تکنولوژی ریاضی گونه سطح بالا است پس در نتیجه همه مصرف کنندگان باید در مهـارت دانـش و

امنیت اشخاص که صادر کننده این کلیدهای خصوصی وعمومی‌هستند دارای یک اطمینان خـاطری باشند.

خلاصه ای از روند امضاهای دیجیتالی:

استفاده از امضاهای دیجیتالی معمولا شامل روندهای عمل ذکر شده در پایین مـی‌شـوند کـه یـا توسط خود امضاء کننده انجام می‌شود یا توسط گیرنده پیام امضاء شده بطور دیجیتالی انجام می‌شود.

A مصرف کننده یک کلید جفتی رمز نویسی منحصر به فردی را بوجود می‌آورد ویـا اینکـه ایـن کلیدها به او داده می‌شود. B شخص امضاء کننده یک پیامی‌را بر روی کامپیوتر مهیا و آماده می‌کند (برای مثال، بشکل یک پیام در پست الکترونیکی). C امضاء کننده یک خلاصه ای از پیام را با استفاده از یک الگوریتم بازسازی ایمن آماده سازی می‌کند. ایجاد امضای دیجیتالی از یک نتیجه بازسازی که از پیام امضاء شده مشتق می‌شود استفاده می‌کند. D شخص امضاء کننده با اسـتفاده از یـک کلیـد خصوصی، خلاصه پیام را کشف رمز می‌کند. کلیدخصوصی برای متن خلاصه شده پیام با استفاده از یک الگوریتم ریاضی گونه بکار برده می‌شود. امضاهای دیجیتالی شامل خلاصه پیامهـای کشـف رمـز شده می‌شوند. E شخص امضاء کننده بطور برجسته، امضای دیجیتالی اش را به پیام نزدیک می‌کند و یا به آن ضمیمه می‌کند. F شخص امضاء کننده در اصل امضای دیجیتالی و پیام را بطور الکترونیکی به شخص مورد اعتماد می‌فرستد. G شخص مورد اعتماد، کلید عمومی‌شخص امضـاء کننـده بـرای تصدیق و تصویب کردن امضاهای دیجیتالی شخص امضاء کننده بکار می‌بـرد. تصـدیق و تصـویب بـا استفاده از کلید عمومی‌شخص امضاء کننده یک سطح ضمانت تکنیکی را فراهم می‌کند که پیام را از امضاء کننده می‌آورد.

H شخص مورد اعتماد یک خلاصه ای از پیام را با استفاده از الگـوریتم بازسـازی مشـابه بوجـود می‌آورد. I شخص مورد اعتماد دو نوع خلاصه پیام را باهم مقایسه می‌کند. اگر آنهـا یکسـان باشـند، آنگاه شخص مورد اعتماد می‌داند که پیام بعد از اینکه امضاء می‌شود هیچ تغییری پیدا نکرده اسـت حتی اگر ذره ای در پیام بعد از اینکه آن بصورت دیجیتالی امضاء شده است، تغییر ایجاد شده، پیام خلاصه شده توسط شخص مورد اعتماد امضاء کننده متفاوت می‌شود.

سطح تفاوت قابلیت اعتماد با مشاوره قانونی:

بواسطه یک رجوع به نظریه مرکزی یک سطح برابر قابلیت اطمینان و اعتماد، اطلاعات و دانشهای پاراگراف دوم می‌تواند اختلاف و تفاوت قابل توجه و حائز اهمیتی را میان نیازمندیهای مشاوره قانونی منحصر به فرد ویژه ای را ارائه دهد. نیازمندی برابری، همانطور که در پاراگراف دوم استفاده شد، این معنی را نمی‌دهد که سطح قابلیت اطمینان یک گواهینامه در کشور بیگانه باید دقیقا قابل بکابری بـا گواهینامه ای باشد که در داخل کشور صادر می‌شود. (پاراگراف 32 A/CN.9/482)

شناسایی تعدادی از اثرات قانونی برای موافقت کردن قوانین کشورهای بیگانه :

پاراگرافهای 2 و 3 بطور گسترده با آزمایش قابلیت اعتماد میان مرزی استفاده شده سرو کار دارند هنگامیکه دسترسی یافتن به قابلیت اطمینان یک گواهینامه در کشور بیگانه یا امضـای الکترونیکـی اتفاق بیفتد. بهر حال، در آماده سازی Model law، این مطلب در ذهن بوجود می‌آید که وضع قانون در کشورهای مشترک المنافع برای بر طرف کردن نیاز جهت یک آزمایش قابلیت اطمینان با توجه به امضاها یا معتبر سازی های گواهینامه ها درخواست می‌شود که این عمل هنگامی‌اتفاق می‌افتـد کـه وضع قانون در کشورهای مشترک المنافع قانون مشاوره حقوقی را از امضاء یا گواهینامه فراهم شده از یک استاندارد کافی قابلیت اطمینان مرتفع سازد. همچنـین تکنیکهـای قـانونی بواسـطه شناسـایی

پیشرفته قابلیت اطمینان گواهینامه ها و امضاها و کامل کردن آنها با قانون یک کشور بیگانه می‌تواند توسط یک وضع قانون در کشورهای مشترک المنافع ساخته شود و شامل هیچ پیشنهاد مخصوصی هم نباشد.

شناسایی توافقهایی میان اشخاص علاقمند به استانداردهای بین المللی:

نظریه استاندارد بین المللی شناخته شده باید بطور گسترده برای پوشاندن استانداردهای تجاری وتکنیکی بین المللی تفسیر شود (یعنی استانداردهای مشتق شده از بازار). استانداردهای بین المللی شناخته شده می‌توانند مانند تجارب تجاری، قانونی و تکنیکی پذیرفته شده نشان دهند که آیا توسط یک سکتور خصوصی یا عمومی‌برای کاربردهای بین المللی پذیرفته شده اند یا نه! اینگونه استانداردها می‌توانند بشکل نیازمندیها، توصیه ها، خطوط راهنما، کدهای هدایت کننده و یا حالتهای دیگری از بهترین تجارب ظاهر شوند. پاراگراف پنجم برای شناسایی توافقهایی میان اشخاص علاقمند شده با توجه به مصرف انواع معین امضاهای الکترونیکی و گواهینامه ها بعنوان زمینه های کافی برای شناسایی میان مرزی فراهم می‌کند. این مطلب همانطور که در مقاله پنجم گنجانده می‌شود باید تذکر داده شود که پاراگراف پنجم بر جابه جا کردن وتعویض هیچ قانون تعهدی نظارت نمی‌کند خصوصا قانون تعهدی که برای امضاهای دست نوشته ای بکار می‌رود که در کشورهای مشترک المنافع وضع شده است.

پاراگراف پنجم برای اثر گذاشتن بر روی تصریح های قراردادی جهت شناسایی مصرف امضاهای الکترونیکی یا گواهینامه بدون هیچ مشکلی می‌تواند از لحاظ شناسایی قانونی جستجو شود. اما این مطلب شایان ذکر در اینجا است که پاراگراف پنجم هیچ اثری بر روی موقعیت و شرایط قانونی شخص ثالث نخواهد گذاشت علاوه بر این مطلب باید گفت که، فراهم کنندگان خدمات گواهینامه نیز

گواهینامه هایی را با سطوح مختلفی از قابلیت اطمینان، مطابق با اهدافی که برای گواهینامه ها جهت استفاده توسط مشتریان تحت نظارت واقع می‌شوند صادر می‌کنند. وابسته بودن بر روی سطح قابـل توجهی از قابلیت اطمینان گواهینامه ها وامضاهای الکترونیکی می‌تواند اثرات قانونی مختلفی را بوجود آورد برای مثال در کشورهای معین، حتی گواهینامه هایی که گهگاه به سطح پایین و یا ارزیابی پایین نسبت داده می‌شوند می‌توانند نمونه های معینی از اثرات قانونی به شمار آیند.

فصل سوم

نیازمندیهای قانونی مراجعه با تکنولوژی جدید امضا کردن

خلاصه مطلب

شناسایی امضای الکترونیکی و پیام های الکترونیکی، مشکلات بسیاری را در ارتباط بااستعمال آنها در سیستم های قانونی مختلف بوجودمی‌آورد(بعنوان مثال، ماشینهای گوینده اتوماتیک و ...) امضای الکترونیکی قبلا در محاکم و دادگاهها غیر مجاز و نپذیرفتنی به شمار می‌رفت حتی اگر مجاز و پذیرفتنی محسوب شود، باز هم اشخاصی که از این مسائله استفاده می‌کنند باید قبلا از سوی یک قاضی مدارکی داشته باشد که وترجمه شده باشد واگر از این تکنیک کسی استفاده کند که آگاه و بااطلاع نباشد در نتیجه مظنون ومشکوک به شمار خواهد رفت. در واقع امضا الکترونیکی حتی اگر از سوی یک قانونگذار بی اساس دانسته شود و به رسمیت شناخته نشود باز هم یک ضمانت کیفی و اطمینان به اجرای امر بی نظیری را توسط امضای دست نویس ارائه می‌دهد. با وجود این اگر ستون قانونی بعنوان یک اصلیت مناسب واقع نشود، یک نهفتگی ساده در این متنها بعنوان یک جواب کافی و مناسب برای مشکلاتی که با آنها مواجه می‌شویم، محسوب نمی‌شود. بنابر این تغییر و تبدیل هایی در قانون باید صورت گیرد. همه قانون دانها وحقوقدانها به این نیازمندی و ضرورت اگاهی و واقف می‌باشد. موسسات حقوقی بین المللی اکنون هم از نظر عمومی‌و هم خصوصی در حال کشمکش هستند تا وسایل پیشرفت شناسایی اصول قانونی استانداردرا در عرصه های مشخص و ویژه ای فراهم کنند (حقوق گمرکی، بانکها، ...)نیازمندیهای قانونی که مرتبط با تعریف امضا رسمی‌و متداول هستند. چه چیز می‌باشند. چگونه می‌توان به این نیازمندیهای قانونی با تعریف یک امضای الکترونیکی صورت عمل داد؟ از نقطه نظر قانون، کدام جریمه ها و می‌توانند توسط مقایسه میان این دو نوع امضا گذاشته شوند؟ اثر تکنیکی اصول قانونی طرح شده توسط موسسات حقوقی بین المللی برای ETD (انتقال الکترونیکی اطلاعات چیست؟ اینها سئوالاتی هستند که در محتویات این متن با آنها سروکار داریم).

مقدمه

این مطلب که همیشه قانون تعدادی تاخیر و وقفه باتوجه به واقعیت و اصل یک موضوع دارد یک بیانیه و اظهار نامه معمولی است. درخصوص امضای الکترونیکی، آشکار کردن درستی این بیانیه و اثبات وظیفه ما است. هنگامیکه یک قانون گذار (وکیل با قاضی) این تکنیکها را دریافته است، او می‌تواند قوانین مناسب برا گسترش دهد. بدین ترتیب یک قانون و قاعده نه تنها به توسعه های تکنیکی آسیب نمی‌رساند بلکه یک سری تعهداتی را جهت استفاده مطمئن و ایمن، برای مفاهیم تکنیکی مطابق با گسترش سطح دانش تکنیکی فراهم می‌کند. این متن حاضر شده در اینجا که توسط یک دانشمند متبحر در کامپیوتر و وکلای مرکز تحقیقات کامپیوتر و قانون Namur بوجود آمده است. در نخستین گام ما یک مقایسه ای بین امضای رسمی‌و متداول وامضای الکترونیکی انجام می‌دهیم در دومین گام ما یک تجزیه و تحلیل کوتاهی را در مورد قوانین اخیر UNCID ارائه می‌دهیم که می‌تواند بعنوان یک استاندارد بین المللی برای داد و ستدها و مصالحه نامه های EDI مورد مطالعه قرار گیرد وآخرین گام، با توجه خاصی به در روش تکنیکهای امضا خواهیم پرداخت که می‌تواند بعنوان ارزیاب این قوانین UNCID مورد استفاده قرار گیرد.

مقایسه میان امضای رسمی‌و متداول وامضای الکترونیکی

امضای رسمی‌و متداول

عملکردها: گرچه هیچ تعریف جهانی برای قانون امضا وجودندارد. اما با وجود این حقوقدانها دریافتند که این مساله یک هدف دو منظور را آشکار می‌کند که اولا در رابطه با شناسایی امضا کننده

و ثانیا در رابطه باتوضیح یک اراده و اختیار برای قبول کـردن موضـوع تعلیمـات و دسـتورات اجـرا می‌شود.

شناسایی صاحب امضا: امضایی از شخص که علامت تجاری بی نظیر وشخصی است هنگامی‌که به یک دستور و مدرک ضمیمه می‌شود می‌تواند مولف عمل را به همان اندازه حضور فیزکی اش تعیین کند.

توصیف خواسته و اراده: باامضا کردن یک مدرک و یاسند، صاحب امضا خواسته اش را برای عملی شدن قسمتی از یک انتگرال توضیح می‌دهد که نتایج قانونی آن را بطور قانونی در برمیگیرد.

شکل و ترکیب: امضا باید پایانی مشابه با رژیمهای قانونی و دسـتورات قـانونی داشـته باشـد. امـا ضرورتهای فیزیکی واقعی برای ان صورت عمل دادن به شکل پایانی اش است که مـی‌توانـد از یـک سیستم قانونی به سیستم دیگر تغییر یابد.

امضای الکترونیکی:

عملکردها: امضای الکترونیکی یک علامت و نشان غیر قابل تولیدمجدد است (مانند مجموعه ای از خصوصیات) که به یک مدرک یا سند پیوست و ضمیمه می‌شود. این مطلب بعنوان یک خروجـی از الگوریتم پیچیده وترکیبی به شمار می‌رود که اطلاعات خروجی را می‌تواند در سه گروه وظیفه مختلف متغیرها، طبقه بندی کند. 1- اطلاعات منحصر به فرد سری برای فرستنده 2- اطلاعات شناخته شده توسط فرستنده و آدرس 3- اطلاعاتی که مرتبط با محتویات خود مدرک یا سند است. در این شرایط امضای الکترونیکی دو چیز را تعریف می‌کند: یکی شناسایی فرستنده سند است و دیگری رسـمیت دادن به محتویات سند می‌باشد.

شکل وترکیب: امضای الکترونیکی یک مجموعه ای از خصوصیات و ویژگی های کوتاهی است که در پایان یک سندگذاشته می‌شود. با توجه به نیازمندیهای سیستم های قانون مدنی، این مطلب واضح و آشکار است که در خواستهای تنظیمی‌درخصوص شکل امضا درتماس با همه تکنیکهای امضا قرار ندارند.اولا: در موارد معین، امضای الکترونیکی در گام اول فقط توسط ماشین قابل خواندن است و این کار بطور مستقیم توسط گیرنده انجام نمی‌شود. ثانیا: درموارد دیگر این امضاهای الکترونیکی هرگز قابل خواندن نمی‌باشند.در بسیاری از قوانین مدنی کشورها، نیازمندی دیگری بعنوان یک بحث، بر خلاف شناسایی یک ارزیابی مالی قانونی در مورد امضای الکترونیکی می‌تواند مورد مطالعه قرار گیرد. بر طبق پاره ای از دادگاهها (بعنوان مثال دادگاه عالی بلژیک) تکنیکهای امضاء باید هویت فرستنده را توضیح دهد. این نیازمندی توسط تکنیکهای مسلم و معین قانونی و معتبر مانند خصوصیات و ویژگیهای فیزیکی لمس می‌شود. (عنبیه، خون، چهره،... که مزیت شناسایی شخص را توسط دستگاه دسترسی ظاهر می‌کند). قوانین معینی مانند قانون Luxem bourg در سال 1986 بطور سریع ویژه تغییر و تبدیل یافته اند تا اینکه پذیرش روندهای جدید قانونی مانند امضای الکترونیکی امری میسر شود. قانون Luxembourg امضاء را بعنوان همه معانی که برای شناختن فرستنده یک پیام حاوی کد رمزی بکار می‌رود، تعریف می‌کند مشکل شکل و ترکیب تنظیمی‌امضاء بطور قطعی می‌تواند مشکل عمده ای برای گرفتن پذیرش آن از دادگاه ها بعنوان امضا باشد

مقایسه امضای رسمی‌و متداول با امضای الکترونیکی

معرفی یک تکنیک شناسایی برای امضای الکترونیکی، جهان حرفه و شغل را مجبور خواهد کرد که با آن موافقت وهمراهی کند. بنابراین تغییرات عمده قبلی مجبور می‌شوند تا اطمینانی را حاصل کنند

که آیا امضای متداول و رسمیو امضای الکترونیکی به عملکرد های مشابه صورت عمل دهند یا نـه! یک تجزیه وتحلیل مقایسه میان عملکردهای مختلف ما را کنترل این مطالب کمک خواهد کرد.

توضیح وتفسیری در مورد طرح کلی:

شناسایی بخشها: برای شناسایی فرستنده باید گفت که امضای دستی یک شکل معتبر متداول از یک بند است. بنابراین شناختن شخصی که می‌خواهد با محتویات سند موافقت و سازگاری کند امری میسر و ممکن می‌شود.بهره حال، امنیت یک امضاء مطلق و کامل نمی‌باشد. مثلا یک امضای دسـتی ممکن است که بواسطه تعدادی ویژگی مرتبا دستخوش تغییرات متناوب باشد و یا اینکه ممکن است که این امضاء مورد تقلید و کپی قرار گیرد.

به همان مراتب فاکتور امنیت برای امضای الکترونیکی که ناموفق تر است بکار می‌رود و این امر به دو دلیل است: از یک سو این که امضای اتوماتیک وار بطور سیستمی‌کنترل و چک می‌شوند و از سوی دیگر اینکه این امضاء مرتبط محتویات موجود در سند می‌باشد. برای شناسایی گیرنده باید بگـوییم، علاوه برآنچه که تا کنون گفته شد، امضای الکترونیکی می‌تواند در روشی انجام شود که نه تنها مرتبط با اطلاعات در فرستنده ومحتویات است بلکه مقداری از این اطلاعات در گیرنده نیز وجود دارد. در این مورد، امضاء نیز شخصی که آن را می‌فرستد را شناسایی خواهد کرد. چیزی که در اینجا به طور واضح غیر ممکن می‌باشد این است که بدست آوردن امضای متداول و رسمی‌مطلبی غیر عملی است.

اراده و درخواستی برای موافقیت وهمراهی با محتویات سند:

یک تکنیک شناسایی باید موافقت امضاء کننده را برای محتویات سند نشان دهد. امـا ایـن فقـط زمانی می‌تواند محفوظ و اطمینان داده شود که یک شرایط ویژه ای اتفاق بیفتد. مثلا اینکه امضاء باید یک عملکرد جداگانه ای از نوشتن خود متن باشد. امضای الکترونیکی باید بواسطه یک رویه مختلف

بنیاد نهاده شود که معمولا شود، که معمولا اینکار توسط شخصی که امضا متعلق به اوست (یا نماینده قانونی آن شخص) انجام می‌شود. بنابر این، امضای الکترونیکی دقیقا مانند امضای رسمی‌و متداول به حضور فیزیکی بشر نیاز دارد، ولی در عوض شخص در اینجا یک امضای واقعی دارد، امضای الکترونیک فقط می‌تواند توسط شخص بنیاد نهاده شود. این مطلب در این واقعیت وجود دارد که امضای الکترونیکی بطور فیزیکی، جدا از مجموعه نوشتجاتی از متن است که در پایان صفحه نشان داده خواهد شد.

محتویات سند:

امضاء نشان می‌دهد که بطور واقع یک شخص با محتویات سند موافقت کرده است این مطلب فقط می‌تواند زمانی اتفاق بیفتد که سند توسط یک اشتباه یا توسط یک تقلب بعد از امضای شخص دستخوش تغییر نشده باشد. امضای الکترونیکی، علاوه بر عملکردهای رسمی‌و متداول امضای دستی، اطمینان دادن به این عملکرد معتبر و قانونی را نیز تعریف خواهد کرد. این مطلب بدین دلیل ممکن می‌شود که تعریف امضای الکترونیکی مطابق با محتویات سند امضاء شده می‌باشد. بنابراین، امضایی که دارای رمز عددی است بهترین ضمانت عملی برای تغییر و تبدیلهای موجود در متن است.

موقعیتهای مناسب قوانین و اصول جدید:

حتی اگر امضای الکترونیکی به عملکردهای مختلف امضای دستی صورت عمل بدهد و برای ما قابلیت اطمینان و درجه امنیت بیشتری را نسبت به امضای متداول و رسمی‌فراهم کند باز هم شناسایی آن به یک تعدیل و توافق توسط سیستم قانونی مطابق با مشکل نیازمندیها شکل وترکیب نیاز دارد. در حال حاضر، پیش بینی کردن اینکه آیا یک دادگاه ارزیابی آزمایشی و مشروط را در رویداد یک مجادله برای جدیدترین تکنیکهای اعتباری و قانونی می‌دهد یا نه امری بسیار مشکل

می‌باشد. بهر حال، با توجه به پیشگویی در مورد ارزیابی قانونی جدیدترین مفـاهیم اعتبـار سـازی و قانونی، شناختن درجه قابلیت اطمینان امری بسیار سودمند است. دو نظر در رای متضاد می‌تواند در آن حدود نقل و ایراد شود: اولین آنها ایتالیایی است و دومنین نظر متعلق به آلمانیها می‌باشد.

در ایتالیا، با توجه به قرار داد تلکس، دادگاه مجزایی از Ascoli piceno برگزار می‌شود که نشان دادن یک تلکس فرستاده شده توسط تله تایپ را بر عهده دارد که در واقع توسط خود فرستنده بـه یک آدرس فرستاده می‌شود. اما این مطلب یک احتمال است که ممکنه توسط مفاهیم مختلف تغییر یافته و منقطع شود. در آلمان، بعبارتی دیگر، یک کارشناس می‌گوید: قبل از یک دادگاه که شناسایی فرستادن آدرس با تله تایپ بر عهده دارد، آزمایش در مورد حقیقی بودن شخصی که پیام را می‌فرستد لازم وضروری نمی‌باشد.

قوانین و قواعد UNCID: قوانین UNCLD باید در شبکه تجارت بین المللی دریافت شود، یعنی جایی که امنیت و اطمینان یک نقش مهمی‌را بازی می‌کند. آنها توسط یک کمیته مشترک و پیوسته متعلق به دفتر کار بین المللی تجاری (یک سازمان غیر دولتی) طرح می‌شوند که متشکل از اعضـای کمیسیون ملی در قانون تجارت بین المللی (UNCITRAL) است و قوانین UNCID بـا مشـکل پذیرش قانونی سرو کار ندارند. آنها قوانین را در یک پذیرفتگی اثر نمی‌دهند. اگر یک سند نوشته شده توسط قانون مورد نیاز واقع شود آنگاه قوانین UNCID از نظر قدرتی ضعیف می‌شـوند. در عـوض، قوانینی که برای فراهم کردن یک مدل از قرار داد برای مصرف کننده EDI است یک بنیاد و شالوده ای را می‌تواند بنیاد فهمد ؟ که توافق ارتباط نام دارد. شکل و جزیئیات این توافقها مطابق با اندازه و نوع مصرف کننده تغییر خواهد کرد بطور مثال قوانین UNCID برای ODETTE (سازمان تبادل اطلاعات بواسطه انتقال از فاصله دور در اروپا و (بواسطه انتقال از فاصله دور در اروپا) و DISH (تبادل

اطلاعات برای انتقال دادن، گروه صادر کنندگان، متصدی حمل و نقل بار وانتقال خطوطی که در یک پروژه راهنمایی EDI مشارکت دارند) بکار می‌روند. بهر حال، قوانین NUCID بیشتر از یک نقطه شروع می‌شوند: آنها همچنین یک سطح پذیرفته شده از رفتار حرفه ای را با عنوان یک کد و رمز هدایت مفید و کامل تعریف می‌کند. با تعریف تعدادی از نیازمندیهای تکنیکی برای EDI، قوانین UNCID امنیت این شکل از ارتباطات و در نتیجه قابلیت پذیرش یک سند الکترویکی را در پیش چشم های قاضی افزایش خواهد داد.

اصول و پایه های قوانین UNCID:

مطابق با معرفی یاداداشت نوشته شده توسط ICC، کمیته مشترک، کارش را بر روی پنج اصل پایه ریزی می‌کند. قوانین باید: 1- در آسان کردن مصرف EDI بواسطه یک کد موافق رهبری میان بخشهای بکار گرفته شده در اینگونه مبادلات الکترونیکی فرض می‌شوند.

2- فقط برای تبادل اطلاعات بکار می‌روند نه برای مفهوم پیامهای اطلاعات تجارتی منتقل شد.

3- مصرف ISO واستانداردهای دیگر را بطور بین المللی برای اجتناب از اختلال بهم مربوط سازند.

4- با پرسشهایی در مورد امنیت تحقیق و رسیدگی و تصدیق و استقرار، معتبر سازی ارتباط بخشها و ذخیره سازی بخشها سرو کار دارد.

5- یک نقطه کانونی و مرکزی را برای تفسیر و بیان یک نتیجه بین المللی هماهنگ شده واستفاده از یک کد و رمز بنیادی قرار می‌دهند.

تجزیه و تحلیل قوانین:

بیشتر مقاله ها با مسئله معتبر سازی و قانونی سازی سرو کار دارند. معتبر کردن محتوی اطلاعاتی درست وکامل است و در رابطه با درستی و صحت شخص نماینده، معتبر سازی پیام را صادر می‌کند. ما بر روی این مشکل بر می‌گردیم در بخش بعدی واقع در این گزارش که مرتبط با شناخت یک انتقال است. در قوانین UNCID، شناخت دارای تعهد نمی‌باشد، فرستنده مجبور است آن را بواسطه یک شرط و حکم در توافق ارتباط درخواست کند. با پیروی کردن از آن ، مقاله بعدی مقرر می‌کند که فرستنده یک انتقال می‌تواند گیرنده ای را برای تایید کردن محتویات یک یا چند پیام در انتقال درخواست می‌شود، اگر آن به درستی در مفهوم و ماهیت صحیح ظاهر شود. بیشتر عناصر مرتبط با مشکلات مسئولیت می‌باشد اما دو تا از این عناصر با شواهد و قرائن مرتبطند که آن دو عبارتند از:

1- آیا قوانینی در اندازه گیری های امنیت و آسایش موجودی در این مساله وجود دارد؟

2- آیا قوانین خاصی در مورد امضا کردن وجود دارد؟

امضای الکترونیکی و قوانین UNCID:

بطور مختصر و مفید باید بگوییم که در رابطه با دو سوالی که در بخش قبل شده ما بعد از این چگونگی تجزیه وتحلیل امضای الکترونیکی و تکنیکهای وابسته به آن را انجام خواهیم داد که نه فقط مورد توجه قوانین UNCID قرار می‌گیرد بلکه چگونگی اینکه آنها می‌توانند به این قوانین صورت عمل دهند را نیز معین می‌کند. ما در اینجا یک سری از عملکردهایی که در زیر آمده است را مورد تجزیه وتحلیل قرار می‌دهیم.

1- امضای الکترونیکی و شناسایی صاحب این امضاء (عملکرد طبقه بندی شده امضاء کردن).

2- امضای الکترونیکی و تحقیق و آزمایش عدم قابلیت خرید و فروش یک سند (عملکرد الحاقی داده شده به امضاء توسط یک مفاهیم تکنیکی جدید).

3- امنیت و جلوگیری از تقلب در انتقال.

امضا بعنوان شناسایی هویت امضاء کننده: یکی از عملکردهای امضای الکترونیکی این است که شناسایی هویت امضاء کننده را امکان پذیر می‌کند.

اجازه بدهید در مورد چگونگی این امر که قوانین UNCID با این موضوع به طور جدی برخورد و در مورد آن صحبت می‌کنند، بحث نماییم. قوانین زیر در مورد این موضوع بحث می‌نماید.

- یک پیغام اطلاعات تجاری ممکن است مربوط به یک یا چندین معامله باشد و باید حاوی یک شناساینده مناسب برای هر معامله باشد و وسیله ای برای اثبات این امر که پیغام کامل است و مطابق TDI-AP مورد نظر صحیح می‌باشد.

- برگ انتقال باید فرستنده و گیرنده را مشخص نماید: این برگ باید شامل وسایل اثبات چه از طریق روش استفاده شده در خود برگ انتقال یا بوسیله دیگر روش های فراهم شده توسط TDI-AP مورد نظر،تکمیل رسمیو صحت انتقال باشد.

قوانین UNCID:

شناسایی شرکت کنندگان در انتقال (فرستنده و گیرنده را) پیشنهاد می‌دهد و همچنین شناسایی پیام ها ومعاملات را ارائه می‌دهد. امضای الکترونیکی و دیگر روش های کلاسیک از پیام های بی شمار و متوالی، چنین شناسایی را مجاز می‌سازد.

امضا بعنوان یک سند غیر قابل تغییر (تشخیص)

دیگر عملکرد امضای الکترونیکی این است که کنترل غیر قابل تغییر بودن محتوای پیام را کنترل می‌نماید. در حقیقت، باید گفت که امضای الکترونیکی تنها تغییر ساختگی یا نادرست را شناسایی می‌نماید، اما از هر گونه خطا و اشتباه جلوگیری می‌نماید. قوانین زیر در این موضوع بحث می‌نماید

a-5) دو طرفی که در یک TDI-AP ربط دارند باید مطمئن باشند انتقال های آنها در نوع کامل و صحیح می‌باشد.

و مطابق TDI- AP مربوطه مطمئن می‌باشد، و باید مراقب باشند که، از قابلیت آنها برای دریافت این برگه های انتقال مطمئن باشید.

b-5) واسطه ها در برگه های انتقال باید تذکر داده شود تا مطمئن شوند که تغییر غیر مجاز در انتقال ها و جود ندارد که لازم باشد دوباره منتقل شود و محتوای اطلاعات چنین انتقالاتی برای هیچ فرد غیر مجاز قانونی فاش نگشته است.

a,6) یک پیام اطلاعات تجاری ممکن است مربوط به یک یا چند معامله تجاری باشد و باید حاوی یک شناساینده مناسب برای هر معامله باشد و وسیله ای برای اثبات این امر که پیغام کامل است ومطابق TDI_AP صحیح می‌باشد.

b,6) برگ انتقال باید فرستنده و گیرنده را مشخص نماید، این برگ باید شامل وسایل اثبات چه از طریق روش استفاده شده در خود برگ انتقال و یا بوسیله دیگر روش های فراهم شده توسط TDI-AP مورد نظر، تکمیل رسمیو صحت انتقال باشد.

7c,) اگر معیار انتقال در ترتیب (درجه)، به نظر خوب نیاید، و شکل صحیح و کاملی نداشته باشد، گیرنده باید، هر چه سریعتر فرستنده را مطلع نماید.

d,7) اگر گیرنده برگ انتقال متوجه شود که این برگ برای وی در نظر گرفته نشده است، باید هر چه زودتر رفتاری منطقی اتخاذ کرده و فرستنده را مطلع کند و اطلاعات ثبت شده در چنین برگ انتقالی را از سیستم خود حذف نماید، و این جدا از اطلاعاتی معامله ای است که ثبت شده است.

a,10) هر طرف معامله باید مطمئن شود که ثبت اطلاعات معامله کامل برای تمامی‌برگه های انتقال، زمانی که آنها این برگه ها را فرستاده یا دریافت می‌کنند بدون هیچ تغییری حفظ شده است.

هر طرف معامله باید برای ایجاد چنین آرایشی (نظامی) به گونه ای که برای اطلاعات اشاره شده در پاراگراف (b) این مقاله اشاره شده است لازم و ضروری است که احساس مسئولیت نماید که بعنوان یک ثبت صحیح از انتقالات هنگامی‌که توسط طرفین فرستانده و گرفته می‌شود مطابق با پاراگراف a این مقاله آماده شده است.

e10) هر طرف معامله باید به این نکته توجه کند که شخص مسئول سیستم پردازش اطلاعات طرف معامله مورد نظر، یا چینن شخص ثالثی که معمولا توسط دو طرف معامله یا وسیله قانون توافق می‌شود، درجایی که لازم است، گواهی می‌دهد که ثبت اطلاعات معامله وهر نسخه برداری برداشته شده از این اطلاعات صحیح است.

پرسش 8- باید در مورد امضاء قوانینی وجود داشته باشد.

موارد a,5) و (a,6) و (b,7) بیان می‌دارد که معاملات انجام شده و پیام های تبادل شده باید کامل و مطمئن باشد. تکمیل و صحت باید توسط تفاهم نام استفاده شده در برگه انتقال به اثبات برسد. ما در اینجا مثالی نوعی برای به کارگیری روش های اثبات و به طور خاص تر امضای الکترونیکی داریم. موارد (7,c) و (7,d) موارد خاصی از سه مورد قبلی هستند هنگامی‌که یک برگ انتقال (یا یک پیام) به شکل ناقص و نادرست دریافت می‌شود و یا به شخص مورد نظر نمی‌رسد.

گیرنده باید فرستنده را هر چه زودتر مطلع سازد و باید پیام رسیده شده را از بین برد. این مشخصه ها تکمیل، تصحیح وایمنی آن باید بوسیله روش های تشخیص، به اثبات برسد.

مورد b,5) اشاره می‌کند که هیچ تغییری نباید در محتوای در زیر توسط رابط ها در انتقال انجام پذیرد.

چگونه می‌توانیم مطمئن باشیم که هیچ تغییری صورت نگرفته است مطمئنا به وسیله تشخیص هویت و روش های امضا در مورد مشکل حفاظت از نشانه های معاملات در ثبت اطلاعات معامله (فایل ثبت) مواد (10,a) . (10,d), (10,e) وضع می‌کند که حفاظت باید به روشی صحیح و بدون هر نوع تغییری در محتوای برگه انتقال یا پیام ها (نگهداشته شده بعنوان نشانه) صورت گیرد و بعلاوه از این موارد حمایت و نگهداری شود.یکبار دیگر، ما در حوزه کاربرد، ثبت و تکنیک های امضا هستیم.

Encryption (رمز دار کردن)

اکنون ما تجزیه وتحلیل خواهیم کرد که چگونه قوانین UNCID مشکل رمزدار کردن مدارک را در نظر گرفته اند.

(5a) طرفین شرکت کننده در TDI-AP باید مطمئن باشند کـه انتقـال آنهـا و در نـوع کامـل وصحیح می‌باشد و مطابق TDI-AP مربوطه مطمئن می‌باشد و باید مراقب باشند که از قابلیت (کامل و صحیح می‌باشد و مطابق TDI-AP مربوطه مطمئن می‌باشد و باید مراقب باشند که از قابلیت) آنها برای دریافت این برگه های انتقال مطمئن باشند.

(b,5) واسطه ها در برگه های انتقال باید تذکر داده شود تا مطمئن نشوند که تغییری غیر مجاز در انتقالات وجود ندارد که لازم باشد دوباره منتقل می‌شود و محتوای اطلاعات چنین انتقالاتی برای هیچ فرد غیر مجاز (غیر قانونی) فاش نگشته است.

(a,6) یک پیام اطلاعات تجاری ممکن است مربوط به یک یا چند معامله تجاری باشد و باید حاوی یک شناساینده مناسب برای هر معامله باشد و وسیله ای برای اثبات این امر که پیغام کامل است و مطابق TDI-AP صحیح می‌باشد.

(B,6) برگ انتقال باید فرستنده و گیرنده را مشخص نماید. این برگ باید شامل وسایل اثبات چه از طریق روشی درخود برگ انتقال استفاده شود. و یا بوسیله دیگر روش های فراهم شده توسط TDI-AP مورد نظر، تاییدی بر رسمی‌بودن و صحت انتقال باشد.

(e,7) اگر معیار انتقال در ترتیب (درجه) به نظر خوب نیاید، و شکل صحیح و کاملی نداشته باشد گیرنده باید هر چه سریعتر فرستنده را مطلع نماید.

(d,7) اگر گیرنده یک برگ انتقالی، متوجه شود که این برگ برای وی در نظر گرفته نشده است، باید هر چه زودتر رفتاری منطقی اتخاذ کرده و فرستنده را مطلع نماید و اطلاعات ثبت شده در چنین برگ انتقالی را از سیستم خود حذف نماید و این جدا از اطلاعات معامله ای است که ثبت شده است.

(a,9) دو طرف معامله ممکن است توافق کنند تا حفاظت خاصی را اتخاذ نمایند این حفاظت ممکن است بوسیله رمز دار کردن یا توسط روش های دیگر باشد که برخی یا تمامی‌اطلاعات بین آنها مبادله گردد.

(b,9) گیرنده یک برگ انتقال که اینگونه مورد حفاظت قرار گرفته است باید مطمئن باشد که حداقل سطح مشابهی از حفاظت برای هر برگ انتقال در آینده به کار خواهد رفت.

(a,10) هر طرف معامله، باید مطمئن شود که ثبت اطلاعات معامله کامل برای تمامی‌برگه های انتقال زمانی که آنها این برگه ها را فرستاده یا دریافت می‌کنند بدون هیچ تغییری حفظ شده است.

(d,10) هر طرف معامله باید برای ایجاد چنین نظامی‌به گونه ای که برای اطلاعات اشاره شد در

پاراگراف (b) این مقاله اشاره شده است که لازم و ضروری است احساس مسئولیت نماید که بعنوان یک ثبت صحیح از انتقالات هنگامی‌که توسط طرفین فرستاده و گرفته می‌شود و مطابق با پاراگراف a این مقاله آماده شده است

(e,10) هر طرف معامله باید به این نکته توجه کند که شخص مسئول سیستم پردازش اطلاعات طرف معامله مورد نظر، یا چنین شخصی ثالثی که معمولا توسط دو طرف معامله یا بوسیله قانون در جایی که لازم است توافق می‌شود، گواهی می‌دهد که ثبت اطلاعات معامله و هر نسخه برداری برداشته شده از این اطلاعات صحیح است.

پرسش 5: آیا باید قوانینی در مورد امنیت و دیگر قوانینی در مورد اطلاعات مبادله شده وجود داشته باشد؟

پرسش 7: آیا باید قوانینی در مورد رمز گذاری یا دیگر معیارهای امنیتی وجود داشته باشد؟ ابتدا ما، باید اشاره کنیم که قوانین UNCID مشخصا برای توضیح مشکل رمز گذاری که توسط مواد (a,9), (b,9) و پرسش ها توضیح داده شده اتخاذ شده اند. مواد (5,a) , (b,5) به مشکل ایمنی و افشاء نشدن یک برگ معامله و یا پیام برای شخص غیر مجاز مربوط می‌گردد. تنها روش حفاظت در مقابل افشا شدن این است همچنین از محرمانه بودن محتوی مدرک اطمینان یافته و بنابراین از روش ها و تکنیک های رمز گذاری استفاده کنیم.

مواد (a,6) , (6,b) , (7,c) , (7,d) در مورد تکمیل و تصحیح برگ های انتقال و پیام هاست. چگونه ممکن است که هر اشتباه و یا خطایی در طی انتقال آشکار شود؟ جدا از تکنیک های اثبات، رمز گذاری امکان شناسایی و آشکار سازی را ممکن می‌سازد. بعلاوه، اگر تغییری در پیام رمز گذاری شده قبلی انجام شود، گیرنده پیام از مشکل آگاه خواهد شد زیرا برای وی این امکان وجود ندارد که

آن را به طور صحیح رمز گذاری نماید. این امر توسط یک روش رمز گذاری ویژه تضمین می‌گردد که اگر یک اشتباه در طی انتقال یک پیام رمز دار شده رخ دهد، رمز گذاری پیام اشتباه شده و در نتیجه دیگر پیام ها به شدت و به طور کامل با موارد اصلی متفاوت خواهد بود. و در نتیجه یک پیام غیر قابل درک خواهد بود. مشکلی اصلی و مهم وجود دارد که استفاده از تکنیک رمز گذاری را توسط قوانین UNCID (d,7), (c,7) محدود می‌سازد. در حقیقت، اگر شخصی پیامی‌با اشتباه ویا آدرس غلط دریافت نماید وی قادر نخواهد بود پیام را رمز گشایی نماید و آدرس صحیح فرستنده را پیدا کند. و بنابراین، برای وی غیر ممکن است تا فرستنده را در مورد این اشتباه آنگونه که از وی در دو مواد خواسته شد مطلع نماید. و در نهایت، فایل های ثبت، توصیف شده در مواد (10,a)(10,d) (10,e) باید از استراق سمع (فاش شدن) توسط تکنیک های رمز گذاری حفاظت شود.

نتیجه گیری: ما با اشاره به دو دیدگاه، قاضی امریکایی به این نتجه می‌رسیم که:

1- همانگونه که توسط دادگاه عالی Nebraska، نبراسکا، در سال 1965 نشان داده شده اکنون زمان آن است که حقیقت، تجارت و تجربه تخصصی را به صحنه دادگاه بیاوریم اکنون زمان آن است که امضای الکترونیکی را همانند امضای سنتی توسط دادگاه ها، معتبر در نظر بگیریم.

2- با توجه به دیدگاه دیگر قاضی امریکایی در سال 1976 بعنوان یکی از اشخاصی که مانند بسیاری دیگر، رسیدهای کامپیوتری شده زیادی در طی برنامه های حساب و کتاب خود برای پرداخت از زمان های قدیم دریافت می‌نمایم، من آمادگی ندارم تا بپذیرم که محصول کامپیوتر برابر با حکم و فرمان مقدسی است (به عبارت دیگر، اعتبار

امضای الکترونیکی بر پایه سطح ایمنی است که روش های انتخاب شده قادر به اثبات آن می‌باشند.

3- در این مورد، دادگاه به این نکته توجه می‌نماید که نه تنها معیارهای تکنیکی و فنی که معیارهای تشکیلاتی اتخاذ شده با مسئولیت سیستم کامپیوتری، مطابق اهمیت و مشخصه معاملات توسط این سیستم نتیجه گیری می‌گردند.

4- در نهایت، به منظور جلوگیری از عدم اطمینان در مورد قبول قانونی وسایل مدرن ثبت و تایید، و به شدت پیشنهاد می‌گردد که هر طرف معامله، که قصد استفاده از این مورد را دارند پیشاپیش در مورد ثبت اعتبار تکنولوژی که آنها برای معاملات نتیجه گیری شده مورد استفاده قرار خواهند داد، توافق نمایند. از این نقطه نظر، کد UNCID می‌تواند بعنوان مدلی مناسب مورد توجه قرار گیرد.

فصل چهارم

گسترش ایمنی SOAP

امضای دیجیتالی

خلاصه: این مدرک (سند) به قوانین پردازش و نحوه ورودی هد SOAP برای انتقال اطلاعات امضای دیجیتالی در داخل یک نامه SOAP 1.1 اختصاص دارد.

وضعیت:

این سند یک پیشنهاد به کنسرسیوم شکبه گسترده جهانی است. برای لیست کاملی از تمامی‌پیشنهادات شناخته شده لطفا به پیشنهادات شناخته شده،W3C، مراجعه کنید. این سند یاداشتی است که تنها برای بحث توسط W3C، در دسترس قرار گرفته است. این سند یادداشتی است که تنها برای بحث توسط W3c در دسترس قرار گرفته است. انتشار این یادداشت توسط w3c هیچ تاییدی را توسط تیم W3c یا W3C یا هر عضوی از w3C نشان نمی‌دهد. W3C هیچ کنترل ویرایشی برآماده سازی این یادداشت ندارد. این سند کاری در حال پیشرفت است و می‌تواند به روز شود، جایگزین گردد و یا هر زمان با دیگر سند ها به طور کامل عرضه شود.

لیستی از سندهای تکنیکی اخیر W3C را می‌توانید در صفحه گزارشات تکنیکی بیابید.

جدول محتویات 1) انگیزه: الف) پیمان ملی ب) نحوه ورودی و ثبت: الف) محل اسم ب) مدخل ثبت امضا ج) نشانه SOAP- SEC د) مثال 3) قوانین پردازش الف) سنل و دخل ثبت امضا ب) تایید مدخل ثبت امضا 4) مسئله ایمنی 5) منابع

1) انگیزه: انگیزه برای این یادداشت، ارائه روشی استاندارد برای استفاده از نحوه امضای دیجیتالی XML (امضا – XML برای امضای پیام های SOAP 1.1 می‌باشد. ما برای این منظور یک مدخل ثبت SOAP را تعیین می‌نماییم. ما هچنین، تعریفی از یک محل اسم گسترده برای افزودن مشخصه های امنیتی به ثبت (سر دسته) SOAP ارائه می‌دهیم. منظور ما از گسترش این

است که عوامل جدید می‌تواند به برنامه اضافه کاری افزوده شود اما عوامل در برنامه کار تغییر تخواهد کرد. قصد ما این است که دیگر مشخصه های ایمنی را مانند امور محرمانه پیام های SOAP 1.1 به این محل اسم با استاندارد های مناسب افزوده شود، مثلا رمز گذاری XML موجود، در دسترس می‌باشد. آنچه ما به طور ویژه به یادداشت دیگری یا گروه کاری دیگر موکول خواهیم کرد تعریف پروتکل (پیمانی) تایید برای، SOAP منظور ما از پیمان، انتظاری برای پردازش توسط گیرنده یک پیام امضا شده، رمز گذاری شده است.

الف پیمان ملی: کلمات کلیدی، (باید) ، (نباید)، (ملزم بودن)، (خواستن) (نخواستن)، (پیشنهاد دادن)، (ممکن بودن) و امکان داشتن در این سند، همانگونه که در RFC 2119 (KEYWORDS) کلمات کلیدی توضیح داده است، تفسیر شده است. محل اسم URI ها در شکل کلی (برخی URI برخي كاربردهاي مربوط یا موضوعات- مربوط) ارائه می‌دهد که در RFC 2396 (URI) مشخص شده است. پیشوند های محل اسم، "SOAP- ENV" و "DS" استفاده شده در این مدرک در محل های اسامی‌به ترتیب آمده است.

2- نحو ورودی سر دسته دهد، : الف و2 محل اسم: محل اسم XML ×, URL (XML-NS) که باید با انجام این مشخصات مورد استفاده قرار گیرد. پیشوندهای "SOAP- SEC"، استفاده شده در این مشخصات با این URI همراه هستند.

ب-2 ورودی هد (سر دسته) امضاء: ورودی هد (امضای SOAP- SEC) ، توسط برنامه زیر توضیح داده می‌شود. (برنامه،XML)، (برنامه 2، XML) عامل < امضای: SOAP-SEC > حاوی یک امضای دیجیتالی واحد است که از مشخصات امضای XML پیروی می‌نماید. (امضا XML)

ج-2 ویژگی SOAP_SEC:id عامل < مرجع : DS > لازم است تا به قسمت امضا شده نامه SOAP اشاره کند. این امر می‌تواند از طریق استفاده از شناساننده XML بدست آید.تقاضا نامه ها مسئول تشخیص این امر هستند که کدام ویژگی ها از نوع idd هستند. برای کمک به تقاضا نامه ها برای تشخیص ویژگی های نوع ID این ویژگی با نام ویژگی جهانیid: SOAP-SEC توضیح داده می‌شود. این ویژگی ممکن است برای اشاره به قسمت امضاء شده نامه SOAP مورد استفاده قرار گیرد.

د-2 مثال: اینجا مثالی از پیام SOAP با ورودی سر دسته امضا، وجود دارد که بدنه SOAP امضا شده و در تنیجه امضا ≤ امضا :ds> به امضا< SOAP-SEC> اضافه شده است به یاد داشته باشید که ویژگی URI در عامل < مرجع :ds> به عامل SOAP:Body SOAP- ENV> اطلاق می‌گردد.

قوانینی پردازش:

ورودی هد امضاء برای انجام یک شکایت رسمی‌امضاء با مشخصات امضای XML (امضا- XML) با یک نامه SOAP به منظور امضا کردن یک یا چند عامل در نامه SOAP مورد استفاده قرار می‌گیرد. ورودی هد امضای چند گانه، ممکن است، به یک نامه SOAP تنهامجرد) با دیگر عوامل امضا شده روی هم قرار گرفته یا منفضل اضافه شود. یک نسخه بعدی از این مشخصات ممکن است، بیشتر به نحوه امضا منجر شود تا دیگر امضا -XML از طریق، گسترش (ابر نامه- XML) در مدل پر محتوا < امضای: SOAP- SEC> مجاز نشناخته شود.

مطابق ساختن تقاضانامه های SOAP به این مشخصه ها باید به این شرایط زیر تخصیص یابد.

1)تقاضا باید قادر به پردازش امضای XML همانگونه که در مشخصات امضای XML آمده است باشد.(امضا- XML).

2)اگر یک تقاضای SOAP تطبیق داده شده به یک ورودی هد (سر دسته) < امضای: SOAP- SEC> در سر دسته SOAP اضافه گردد، ورودی سر دسته باید یک عامل < امضای :ds> داشته باشد که مطابق، مشخصات امضای- XML [امضا – XML] باشد. تمامی‌عوامل < مرجع :ds> مشتمل در این امضا باید به یک منبع در نامه SOAP ضمیمه اطلاق شود و یا به منبعی در بسته پیام SOAP ضمیمه اطلاق می‌شود (الحاق- SOAP) در صورتی که نامه در بسته پیام SOAP 1.1 اولیه باشد. (الحاق- SOAP).

3)هنگامی‌که کاربرد (تقاضای) SOAP تطبیق شده یک پیام SOAP را دریافت می‌کند، که حاوی یک یا چند ورودی سر دسته (هد) < امضا:SOAP-SEC> است که برای هر یک از این تقاضا باید گام های زیر را انجام داد: 1) تصمیم بگیرید که می‌خواهید ورودی سر دسته (هد) را پردازش کنید یا نه (چه به صورت اجباری یا داوطلبانه)

2) اگر این پردازش صورت گرفت، تقاضا نامه باید سعی کند که امضا را با استفاه از مدل پردازش امضای XML (امضای –XML) اثبات کنید.

به یاد داشته باشید که کانالیزه کردن (مشروع کردن) XML (XML-CL4N) از < امضای :ds> و دیگر منابع امضا شده باید هر یک از طریق متن خود صورت پذیرد. این بدین معنی است که در میان دیگر موارد که شکل مشروع دارند،[XML-CL4N] از < امضای :ds> همیشه اظهاریه محل اسم را برای SOAP- SEC,SOAP-ENV به اسم می‌برند. بقیه این بخش کاربردهایی را توصیف می‌کنند که برای ورودی هد (رهبر) امضا اجرا شده است.

الف-3: نسل ورودی هد سر دسته (رهبر) امضا: یک روش برای ایجاد یک ورودی سر دسته < امضا:SOAP- SEN> به قرار زیر است:

1) مقصد نام SOAP را با پیکره و سر دسته های لازم و ضروری مشخص کنید.

یک الگو از عامل < امضای: ds> ایجاد کنید. الگوهتور می‌شود که حاوی محتویات خالی (تهی)

2) برای عوامل < ارزش امضا: ds >یا ارزش خلاصه :ds> باشد اما محتویات با ارزش مناسب برای عوامل ماند < روش امضای: :ds> و < مرجع: ds> برای محاسبه آنها مورد نیاز است.

3) یک ورودی در (سر دسته) جدید < امضاء : SOAP-SEC> ایجاد نمایید والگو را به این ورودی بیفزایید.

4) یک ورودی سر دسته (هد) < امضای: SOAP=SEC> برای سر دسته AOAP بیفزایید.

5) یک مشخصه، بازیگر SOAP را بیفزایید ومشخصات را در ورودی در صورت لزوم اضافه کنید.

6) عوامل، < ارزش امضا: ds> و < ارزش خلاصه > را مطابق نسل اصلی مشخصات امضای XML (امضای -XML) محاسبه کنید.

فیلتر کردن راه x می‌تواند برای اختصاصی کردن موارد (مباحث) مورد استفاده قرار گیرد تابه گونه ای که در مشخصات امضای- XML توصیف گردید، امضا گردد (امضا XML) اگر چه، از زمانی که مدل مبادله پیام SOAP باعث کاربردهای میانی می‌گردد و نامه را تغییر می‌دهد (برای مثال باعث حذف وافزودن ورودی هد (سر دسته) می‌گردد) فیلتر کردن راه x همیشه به موارد مشابه پس از رساندن پیام ختم نخواهد شد. استفاده از فیلتر کردن راه x باید مورد توجه و دقت قرار گیرد به طوری که فقدان تایید مستمر بستگی به چنین تغییری ندارد. تغییر شکل که در مشخصات امضای XML-

(امضای XML) توضیح داده شده است، ممکن است هنگامی‌که کل نامه امضا می‌شود شامل دیگر ورودی (سر دسته) مفید باشد

ب-3: اثبات ورودی سند (هد) امضا: اثبات یک ورودی هد < امضای: SOAP-SEC> دچار ایراد می‌شود اگر:

1) نحوه محتویات ورودی سر دسته با این مشخصه ها مطابقت نمی‌کند

2) و یا اعتبار امضا مشتمل در ورودی سر دسته مطابق تایید اصلی از مشخصات امضای XML دچار مشکل می‌شود

3) یا دریافت برنامه کاربردی (تقاضا نامه) امضا را به برخی دلایل رد خواهد کرد، برای مثال، امضا توسط یک کلید غیر قابل اعتماد ایجاد شده باشد)

اگر اعتبار ورودی سر دسته امضا از بین برود، تقاضا نامه ها ممکن است نقص فرستنده را گزارش دهد. این امر خارج از حوزه این مشخصات برای چگونگی کنار آمدن با این مورد است

4- تمرکز امنیت :

این مشخصات استفاده از امضای XML را در سر دسته های SOAP11 توضیح می‌دهد. به عنوان یکی از بلوک های ساخت پیام های SOAP امنیت دهنده، مقصود بر آن است که در ارتباط با دیگر روش های امنیتی مورد استفاده قرار گیرد. نیاز است امضای دیجیتالی در متن دیگر مکانیزم های امنیتی مورد درک قرار گیرد. امضاهای دیجیتالی مطابق IETF RFC 2828(DIGSIG) هستند. مقداری (ارزشی)، که با الگوریتم رمز گشایی مورد استفاده قرار می‌گیرد و به گونه ای به موضوع اطلاعات مربوط است که هر گیرنده اطلاعاتی می‌تواند از امضا برای تغییر مبناء و منشاء اطلاعات استفاده کند. اطلاعات یا تغییر شکل رمز گشایی شده، یک بخش اطلاعاتی به گیرنده بخش

اطلاعات اجازه می‌دهد که منبع و منشاء بخش اطلاعات را ثابت کند و از تقلب جلوگیری می‌نماید. برای مثال، امضای دیجیتالی به تنهایی صحیح بودن پیام را ثابت نمی‌کند. شخص می‌تواند یک پیام امضا شده را ثبت نماید و با آن مقابله کند. برای جلوگیری از این نوع حملات، امضای دیجیتالی باید با یک وسیله مناسب تر ترکیب شود تا از واحد بودن پیام اطمینان حاصل شود، مثلا ثبت زمان، یک راه برا افزودن این اطلاعات جایگزین کردن یک عامل اضافی است که فرزند < امضا > حساب می‌شود. هنگامی‌که امضای دیجیتالی مورد استفاده قرار می‌گیرد، تا هویت طرف فرستنده تغییر داده شود، فرستنده باید وضعیت کلید خصوصی را ثابت کند و بهبود بخشد. یک روش برای کسب این امر استفاه از نوع پاسخ پروتکل است. استفاده کنندگان باید همچنین، از تمامی‌عوامل امنیتی که برای استفاده از امضای دیجیتالی به طور کلی و به خصوصی در امضای XML رخ می‌دهد آگاه باشند. برای ایجاد اطمینان بر پایه امضای دیجیتالی، نکات دیگر از تکنولوژی وجود دارد که باید ارتباط با امضا توضیح داده شود. باید مدل حقیقی سند شناسایی وجود داشته باشد.

باید راهی (روشی) وجود داشته باشد تا کلید وسند اطمینان نگهداری و ایجاد شود. و باید روشی وجود داشته باشد تا اثبات کند که سند شناسایی باطل نشده است.

راه حل امضای مربوط به انگشت یا سر پنجه:

نیاز در مشاغل و تاسیسات صنعتی تجارتی:

با وجود اینکه سودها و استفاده های سر شاری توسط استفاده از شبکه E-mail, web ودسترسی الکترونیکی به اسناد و مدارک حساس و بحرانی ساخته می‌شود اما باز هم این سودها بطور مکرر توسط وقفه هایی در فراهم آوردن امضاهای با دست نوشته شده برای معاملات و داد و ستدهای مهم انجام شده وتحت تاثیر واقع می‌شوند. امضاهای الکترونیکی مربوط به سر پنجه یا انگشتان بطور صحیح

وایمن، هدایت کردن معاملات و داد و ستدهای بزرگ را با استفاده از E-mail, web امری ممکن می‌سازند. بهر حال تا کنون، استفاده از آنها بطور انگشت نما به سازمانهای بزرگی که پیچیدگی و سختی استفاده از عناصر تشکیل دهنده شالوده کلید عمومی‌را در جای مناسب قرار داده اند، محدود شده است.

تفاوت روشهای ایمن وقابل اعتماد

این روشها یک دسترسی ابداع شده جدیدی را برای امضاهای مربوط به سر پنجه یا انگشتان که حذف می‌کنند نیاز به صورت عمل دادن به پیچیدگی راه حل PKI را گسترش داده اند. در این روشها تولیدات بعنوان یک راه حلی هستند که به سادگی و راحتی گسترش یافته وصف آرایی می‌شوند که معاملات و دادو ستدها را بصورت امضاهای انگشتی و کاملا تحقیق شده فراهم می‌کنند بدون اینکه مصرف کننده در آن داشته باشد یا اینکه تغییراتی در روند مشاغل پدید آید. بر خلاف راه حل هایی دیگری که فقط امضاهای مربوط به انگشتان را برای هر دوره و جلسه فراهم می‌کنند، روشهای ایمن وقابل اعتماد امضاء می‌کنند هر معامله و داد و ستد را با فراهم کردن بالاترین سطح اطمنیان وایمنی ممکن که وجود دارد. علاوه بر فراهم کردن یک امضای مربوط به سر پنجه و راه حل آن با استفاده از گواهی نامه ها و اعتبارنامه های X.509 مصرف کننده وایمن ترین امضای صنعتی باید بگوییم که امضای ما و راه حل آن نیز جلوگیری از تقلب، قانون داشتن، معتبر سازی و اختیاراتی وقابلیتهای تحقیق و رسیدگی را در همه معاملات و داد و ستدها فراهم می‌کند. علاوه بر فراهم کردن این مزیتها، روشهای ایمن و قابل اطمینان نیاز به پس ورد وکلمه رمز را هنگام محافظت شما از مشکلاتی که بطور ذاتی در نقیصه های خدمات windows TM, IIS وجود دارند را از بین می‌برند. راه حل روشهای ایمن و قابل اطمینان برای آدرس دادن به نتایج توسعه و هزینه راه حلهای ایمن و پیشرفته توسعه

داده شده است که در تواناییش برای کاهش هزینه های توسعه بطور قابل توجه و حائز اهمیت و افزایش سهولت استفاده منحصر به فرد می‌باشد.

ساختار ها ومزیت ها

راه حل مشتری راه مدخل روشهای ایمن و قابل اطمینان پهناورترین مجموعه از قابلیتهای امضاء وابسته به پنجه و سر انگشتان را در صنعت ارائه می‌دهد که این مطلب می‌تواند بعنوان یک مسئله با اهمیت روز گسترش باید و یا اینکه می‌تواند به سهولت اداره کردن هر نیازمندی ایمن سازی کمک کند. این راه حل می‌تواند یک مجموعه گسترده ای از ایمن سازی را فراهم کند که شامل موارد زیر می‌شود.

1- جلوگیری از تقلب د رمعاملاتی که از امضای وابسته به پنجه استفاده می‌کند.

2- جلوگیری از تقلب در داد و ستدهایی که ازامضای دیجیتالی استفاده می‌کنند و بر روی علائم رمزی و مشخصه پایه ریزی شده اند.

3- جلوگیری از تقلب در دادو ستدهای بیومتریک (زیست سنجی) که از امضای دیجیتالی استفاده می‌کنند و بر روی علائم رمزی و مشخصه پایه ریزی شده اند.

خواه شما در حال نگاه کردن به صورت عمل دادن و یک قابلیت امضای دیجیتالی بنیادی باشید یا فراهم کردن یک علامت رمزی اغوا کننده و راه حل بیومتریک، در هر دو صورت راه حلهای قابل اطمینان و ایمن شما را در سرعت و سهولت کار کمک می‌کند. یکی از مهمترین جنبه های راه حل ما این است که این روشهای ایمن نیازی به هیچگونه تغییر رفتاری در بخش مصرف کنندگان ندارند یعنی هنگامی‌که این راه حل نصب می‌شود این مطلب کاملا واضح و شفاف است که نیاز به هیچگونه

مداخله مصرف کننده ندارد. راه حل روشهای ایمنی برای امضاهای دیجیتالی موارد زیر را فراهم می‌کند.

1-ایمن سازی کلی وجامع در سطح معاملات و داد و ستدها، نه فقط در سطح جلسه و دوره ها که شامل موارد زیر می‌شوند.

الف: جلوگیری از تقلب شدید

ب: معتبر سازی وقانونی کردن مصرف کننده

ج: اختیاراتی برای مصرف کننده.

د: امضاهای دیجیتالی

ه: قابلیتهای بررسی و تحقیق در مورد معاملات و داد و ستدها

2- روند موثرتری برای اسناد و مدارک که شامل مورد زیر می‌شود:

الف: امضاهای دیجیتالی روشهای ایمن و با اطمینان می‌توانند کارها و اوراق نوشتنی، وقفه ها و حرکات را در روند عمل هزینه های اقباض وادا کاهش می‌دهد.

3- کاهش دادن قابلیت تقلب و جعل اسناد

4- قابلیتهای امضاهای دیجیتالی قابل تحقیق و بررسی که نتیجه اثبات شده قابل اجرایی را برای دسترسی و انتقال فراهم می‌کنند.

5-دسترسی و تقربی که پایه ریزی شده بر اساس گواهینامه X-509 است.

6-سهولت استفاده: عملکردهای ایمن سازی که روشن و شفاف هستند برای استفاده مصرف کننده، نیاز به هیچنوع تغییرات رفتاری در روند کار ندارد.

7-مدیریت اتوماتیک وار ایمن سازی، موجب سهولت اجرای کار می‌شود.

8-هزینه کلی پایین تر نسبت داده شده، معتبر سازی قوی برای مصرف کننده و ایمن سازی بالغ بر 90٪ پیشنهادات رقابتی ارائه می‌دهد. راه حل امضای دیجیتالی روشهای ایمن و با اطمینان به راحتی در کمتر از 30 روز در بیشتر سازمانها گسترش می‌یابد.

مثالهایی از عناصر تشکیل دهنده و اجرای کار

سازمانها نیز مانند شرکتهای بیمه متعهد می‌شوند که در قبال فعالیتهای قابل توجه و حائز اهمیت از مقدار کاغذ کم کنند و به جای آن از نماینده سازمان و تنیظم کننده شبکه ها در کشور استفاده کنند. متاسفانه، بیشتر این عملکردها ناموفق بوده اند که دلیل آن ناشی از نیاز داشتن امضاهای تازه در بسیاری از معاملات است. بهر حال، با صورت عمل ددن به راه حل امضای دیجیتالی روشهای ایمن و با اطمینان، گسترش دادن امضاهای دیجتیالی با نمایندگان و تنظیم کنندگان از نظر اقتصادی امری ممکن است. با جایگزین کردن امضاهای دیجتالی به جای امضای تر و مرطوب بطور قابل توجهی مقدار کاغذ در معاملات کاسته شده و بطور نمایشی می‌تواند ایمن سازی بهبود بخشیده شود.

رقابت و مبارزه طلبی:

اگر شما در حال نگاه کردن به صورت عمل دادن به امضاهای دیجیتالی در سازمانتان هستند. ما دو خدمات را به شما ارائه می‌دهیم که به شما تولید و ایجاد بعدی را که یک حق انتخاب و تمایل با دوامی‌است را اثبات خواهد کرد روشهای ایمن سازی و با اطمینان به سایت شما خواهد آمد و به شما کمک می‌کند تا یک برنامه ارزیابی را گسترش دهید و یا اینکه بتوانیم یک دسترسی آزادانه را در ایمن سازی فراهم کنیم و سپس به شما نشان خواهد داد که چگونه راه حلهای ما می‌تواند نیازهای امضای دیجتالی را برای شما مرتفع سازد.

امضای دیجیتالی: امضای دیجتالی (یا کلید عمومی‌امضای مربوط به سر پنجه یا انگشتان) یک نوع ارزش معتبر سازی و رسمیت دادن به اطلاعات دیجتالی مشابه با امضاهای فیزیکی معمولی بر روی کاغذ است با این تفاوت که در آن به استفاده از تکنیکهایی از زمینه علم و رمز نویسی کلید عمومی‌صورت عمل داده می‌شود. بطور کلی یک روش امضای دیجیتالی دو الگوریتم مکمل را تعریف می‌کند که یکی برای علامت گذارن وامضا کردن است و دیگری برای تحقیق و بررسی بکار می‌رود که در این حالت خروجی روند امضاء کردن فیزیک امضای دیجتالی نامیده می‌شود. امضای دیجیتالی نیز بعنوان یک واژه گسترده تری از احاطه و محاصره تکنیکهای کلید عمومی‌و جامع امضای دیجتالی و کدهای معتبر سازی پیام استفاده شده است. امضاهای دیجتالی در برخی جنبه ها متفاوت از نقاط مقابلشان در امضاهای فیزیکی هستند. واژه امضای الکترونیکی ، گر چه گهگاهی برای موارد یکسان بکار می‌رود اما یک مفهوم جداگانه ای در قانون معمولی دارد یعنی آن بر می‌گردد به چندین نوع نه فقط لزوما به آنهایی که با رمز نوشته شده اند یا آنهایی که دارای مکانیسم هایی برای شناسایی عامل ایجاد کننده یک پیام الکترونیکی هستند. امضاهای الکترونیکی شامل قابلیت آدرسهای تلکس می‌شوند به همان اندازه که انتقال FAX امضاهای با دست نوشته شده بر روی یک کاغذ سند شامل این قابلیت هستند.

کاربردها

سه دلیل معمول برای بکار بردن یک امضای دیجیتالی برای ارتباطات وجود دارد که عبارتند از:

صحت و اعتبار:

سیستمهای رمز نویسی برای هر کسی فرستادن یک پیام را با استفاده از کلید عمومی‌تعریف می‌کند. یک امضاء پذیرنده و دریافت کننده پیام را مطمئن می‌کند که فرستنده حقیقتا کسی است

که ادعا می‌کند. البته، گیرنده نمی‌تواند 100٪ مطمئن باشد که فرستنده حقیقتا کسی است که ادعا به بودن آن را می‌کند: گیرنده فقط زمانی می‌تواند مطمئن باشد که سیستم رمز نویسی آسیب دیده و منقطع شده باشد. اهمیت اعتبار و صحت بطور ویژه در یک زمینه مالی واضح و آشکار است. برای مثال : فرض کنید که یک بانک آموزشهایی را از دفاتر شعبه به دفتر مرکزی بشکل (a,b) بفرستد که در آن a شماره حساب و b مقدار اعتبار حساب است. یک مشتری غیر مستقیم و گمراه ممکن است 100 t را به ودیعه بگذارد و در نتیجه انتقال و پس از آن بطور مکرر انتقال مجدد (a,b) را مشاهده کند که این مطلب بعنوان یک مبادرت به حرکت متناوب شناخته می‌شود.

درستی و صحت

هر دوی این بخشها همیشه اطمینان به این مطلب را ارائه خواهند داد که یک پیام در طول انتقال اصلاح و متناوبا تغییر پیدا نکرده است. جلوگیری از تقلب این امر را برای بخش سوم که خواندن یک پیام است مشکل می‌کند اما این بخش سوم با وجود این می‌تواند قادر به تغییر دادن و اصلاح کردن آن در یک روش مفید باشد. یک مثال مشهور برای به تصویر کشاندن این مطلب اینست که این امر مبادرت به شباهت سازی ساختمانی و اساسی بین دوجیز می‌باشد: توجه کنید که بانک مشابهی مانند بانکی که قبلا اشاره شد آموزشهایی را از دفاتر شعبه اش به دفتر مرکزی به شکل (a.b) می‌فرستد یعنی a شماره حساب و b مقدار اعتبار حساب است.یک مشتری غیر مستقیم و گمراه ممکن است که 100 t را ودیعه بگذارد و در نتیجه انتقال و پس از آن انتقال (a,b) و یک نمونه میلیونر شدن است در یک زمینه رمز نویسی، کلمه انکار کردن و قبول نداشتن به عمل رد کردن مشارکت توسط یک پیام بر می‌گردد. گیرنده یک پیام ممکن است که پافشاری کند تا فرستنده به امضا در دستور ممانعت

کردن از انکاری بعدی نزدیک شود در نتیجه ممکن است که گیرنده پیامی‌رابه یک قسمت سوم برای اثبات کردن بنیادش نشان دهد.

اجر و صورت عمل دادن

طرحهای امضای دیجتالی به رمز نویسی کلید عمومی‌و جامع استفاده می‌کنند. در این رمز نویسی هر مصرف کننده یک جفت کلید دارد که یکی عمومی‌و دیگری خصوصی است کلید عمومی‌که آزادانه توزیع می‌شود اما کلید خصوصی بطور سری و مطمئن نگه داشته می‌شود. نیاز دیگری که وجود دارد اینست که باید برای مشتق شدن و استنتاج شدن کلید خصوصی

از کلید عمومی‌غیر عملی شود. یک طرح کلی و جامع امضای دیجتالی شامل الگوریتمهای زیر می‌شود:

1- الگوریتم تولید یک کلید

2- الگوریتم امضاء وعلامتگذاری

3- الگوریتم تحقیق و آزمایش است.

برای مثال، مورد مطالعه و توجه قرار دهید. موقعیتی را که در آن Bob یک پیام به Alice می‌فرستد و می‌خواهد که اهل کجا بودن او را مورد آزمایش و اثبات قرار دهد. Bob پیامش را به Alice می‌فرستد و به یک امضای دیجتالی دست می‌یابد. امضای دیجیتالی با استفاده از کلید خصوصی مربوط به Bob بوجود می‌آید و یک شکل ساده مقدار معانی رمزی اعداد را می‌دهد (بطور طبیعی بعنوان یک رشته از اعداد جفتی ارائه می‌شود) یک گیرنده، یعنی Alice می‌تواند کنترل کند که آیا واقعا پیام از سوی Bob توسط حرکت طولی الگوریتم تحقیق و آزمایش بر روی پیام، رویهم رفته با امضاء وکلید عمومیBob آمده یا نه! اگر آنها سازگار و تلفیق شوند، آنگاه Alice می‌تواند

مطمئن شود که بطور واقع پیام از سوی Bob بوده است. زیرا الگوریتم علامتگذاری و امضاء تا جایی طراحی می‌شود که برای ساختن یک امضاء جهت سازگار و موافق کردن پیام داده شده بسیار مشکل است. بطور معمول تر، برای دلایل موثر ، نخست Bob قبل از علامتگذاری و امضاء یک عملکرد اختلاط رمز نویسی را برای پیام بکار می‌برد. این مطلب امضاء و علامتگذاری را کوتاهتر می‌سازد و بدین ترتیب زمان را ذخیره می‌کند زیرا بطور کلی آمیزش و اختلاط سریعتر از امضاء وعلامتگذاری در اجرا می‌باشد. بهر حال، اگر الگوریتم خلاصه پیام نا ایمن باشد آنگاه آن برای امضاهای دیجیتالی جعلی بکار می‌رود.

تعدادی از الگوریتم های امضا دیجیتالی:

1- اختلاط و ریزه ریزه کردن کامل حوزه، RSA-PSS و ... که بر روی RSA پایه ریزی شده

2- DSA

3- ECDSA

4- طرح امضای ELGAMAL

حالت رایج استفاده – قانونی کاربردی:

همه طرحهای امضای دیجیتالی، چندین نیازمندی مقدمی‌دارند که بدون هیچ علامت یا امضایی می‌توانند چیزی را که اصلا بصورت تئوری رمز نویسی یا استقرار قانونی نیست را معنی دهند.

1- نخست، الگوریتم های کیفی تعدادی از الگوریتم های کلیدعمومی‌با نام ایمن بودن شناخته می‌شوند یعنی با جملات کاربردی بر خلاف آنها شناخته شده اند.

2- دوم: اجراهای کیفی یک اجرای الگوریتم مناسب و خوب همراه با اشتباهات کار نخواهد کرد.

3- سوم، یک کلید خصوصی باید بطور واقع سری باقی بماند.

مقدمه:

در دستور بکار اندازی مزیتهای پست الکترونیکی، سیستمهای ارتباطی مورد نیاز واقع می‌شوند که معتبر سازی و قانونی سازی پیامهای مبادله شده را تعریف کنند. هر دوی این هدفها می‌توانند توسط استفاده از امضای دیجیتالی بدست آورده شوند یعنی یک مقدار وابسته پیام که می‌تواند فقط توسط فرستنده پیام که بر روی مقداری اطلاعات خصوصی پایه ریزی شده، محاسبه شود.طرحهای امضاو علامتگذاری می‌توانند به دو طبقه تقسیم شوند: درست و فیصله داده شده. علامتگذاریها و امضاهای درست می‌توانند توسط فرستنده و گیرنده بوجود آیند و کنترل شوند یک حقوقدان و قاضی می‌تواند در مستقر کردن مباحثات ممکن خوانده شود. در یک طرح امضای فیصل داده شده بعبارتی دیگر، همه ارتباطات یک داور و فتوی دهنده را به اصطلاح در بر می‌گیرند یعنی کسی که به پیامهای علامتگذاری و امضاء شده رسمیت می‌دهد و آنها را قانونی می‌کند. امنیت وابسته به درستی و قابلیت اعتماد داروهایی است که دسترسی به محتویات پیامها دارند. این متن چهار طرح جدید دیجیتالی را معرفی می‌کند که این وابستگی را کاهش می‌دهد. طرحها شامل یک یا چند داوری می‌شود که پیامها را قانونی کرده وامضاها را رسمیت می‌بخشد. در دستور پنهان کردن محتویات پیامها اطلاعاتی که از طریق این داورها و حکم دهنگان فرستاده می‌شوند تحت یک کلید شناخته شده با رمز نوشته می‌شوند که تنها این کلید برای فرستنده s و گیرنده (R) می‌باشد. با وجود این، داور حکم دهنده (A) اطلاعات کافی را برای ممانعت کردن فرستنده وگیرنده از دادن یک تفسیر نادرست به یک پیام علامتگذاری وامضاء شده دریافت می‌کند.

کلید سری $k_k^s = x$ کلید عمومی $k_x^p = x$ کلید تقسیم شده توسط K_{xy}=y,x

عملکرد انحصاری بیت= θ عملکرد رمز توسط کلید $D_k=k$ عملکرد با رمز نوشتن توسط کلید $E_k=k$

سیستم رمز نویسی با کلید سری فیصل دهنده:

در ساختاریو $<V,M_t \ldots M_t,.W>$ می‌توان گفت که v یک بردار تصادفی از بیتm است و $W=V_0\ M_1\ldots..M_t$ با استفاده از طرح باز خورد جلوگیری از تقلب بصورت رمزی همانطور که در پایین آمده نوشته می‌شود.

برداری تصادفی v برای تغییر قیافه و حالت دادن پیامهای تکرار شده ودنباله های بیت هایی که اغلب در شروع پیامها اتفاق می‌افتد، استفاده می‌شود برای سهولت ارائه و معرفی ما از علائم رمزی استفاه خواهیم کرد.

$$C=E_{KSR}(<V,Soybean\text{-}id,Rsuser\text{-}id,Rsuser\text{-}id,seq.nr,\ data,\ w>$$

یعنی .$C=<c_o,\ldots,c_{t+1}>$:

$C_o=E_{KSR}\ (V)$

$C_1=\ E_{KSR}\ (M_1\ \theta\ C_1)$

$C_2=\ E_{KSR}\ (M_2\ \theta\ C_1)$

$C_t=\ E_{KSR}\ \ (M_t\ \theta\ c_{t-1})$

$C_{t+1}=\ E_{KSR}\ \ (W\ \theta\ C_t)$

با استفاده از علائم رمزی مشابه C' همانطور که در پایین آمده است تعریف می‌شود:

$$C'=E_{KSR}(<V',soybean\text{-}id,Rsuser\text{-}id,seq.nr,\ c,w'>$$

در اینجا v' یک بردار تصادفی بیت m و w' مقدار بلوکهای قبلی هستند.

فرستنده های c' به A آن را کشف رمز می‌کنند. و برای نتیجه گیری کردن معتبر سازی پیام و تستهای قانونی سازی آن بکار می‌رود. اکنون A به W' تنزل پیدا می‌کند و به C'_{t+1} که یک پرچم پیام صحیح یا پیام اشتباه است اضافه می‌شود.

$$C''=E_{KRA}(<V'',V',soybean\text{-}id,Rsuser\text{-}id,seq.nr,c,c'_{t+6},\ flag\ ,w''>).$$

سیستم رمز نویسی با کلید عمری فیصل دهنده:

این طرح و بر روی سیستم رمز نویسی کلید عمومیRivest- shamir-Adleman پایه ریزی می‌شود. a و b در اینجا اعداد مجاز بزرگی هستند که در سیستم استفاده می‌شوند پیام $M=<M_1,.....M_t>$ می‌تواند بصورت زیر کشف رمز شود:

$C_o=E_k(V),C_1=E_k(M_1+C_o)\ldots.,C_t=E_k(M_t+C_t\text{-}1)$ جایی که v یک عدد تصادفی کمتر از ab است آنگاه می‌توان گفت:

$$C_{t+1}=E_k(w+C_t)0$$

$W=V+M_1+\ldots+M_t$ با استفاده از علائم رمزی معرفی شده در بخش 2 ما می‌توانیم چنین بنویسیم: $C=E_k(<V,M_1,\ldots,M_t,W>)$ و با استفاده از این روند بازخورد جلوگیری از تقلب c''',C'',C می‌توانند بشکل زیر تشکیل شوند:

$$C' = Ep_{KR}(DK_s^s(<V,s-id,R-id,seq-nr,data,w>)$$
$$C'' = Ep_{KA}(DK_s^s(<V',-id,R-id,seq-nr,C',W'>)$$
$$C'' = Ep_{KR}(DK_s^s(<V'',s-id,R-id,seq-nr,time,date,c',\ flag,w''>)$$

سیستم کلید عمومی‌فیصل داده شده (n,i):

این طرح که نیاز خواهد داشت به یک روند مدیریت کلید ساده تر ا زآنچه که تا کنون توضیح داده شده است، یک ترکیبی از طرحهای علامتگذاری وامضای بخش 3 و 4 است.

نتیجه گیری:

چهار طرح علامتگذاری و امضای دیجیتالی که در این متن ارائه شدند، بر روی صحت و درستی فیصل دهندگان طرحهای قبلی محور قرارر نگرفته اند. یک هزینه شاخص و برجسته در مقابل امنیت، به فاکتورهایی تقسیم خواهد شد که انتخاب یکی از این چهار سیستم را برای استعمالات ویژه نتیجه می‌دهد. برای یک لیست مرجعها و یک رفتار مفاهیم ارائه شده در اینجا که با جزئیات بیشتری شرح داده شده اند، خواننده باید به [1] برگردانده شود.

مرجع ها:

1. S.ALK, H.Meijer طرحهای علامتگذاری وامضای دیجیتالی برای شبکه های ارتباطی کامپیوتر- پیشرفت تدریجی داشتن در مورد قابل تبادل نظر ارتباطات اطلاعاتی IEEE- شهر مکزیکو- اکتبر 1981 -41 تا 37.pp.

ضمائم

بانکداری الکترونیکی- مقدمه

امکان انجام عملیات بانکی به صورت الکترونیک و از راه دور همیشه به عنوان مهم ترین پیش فرض ونیاز تجارت الکترونیک و به عنوان عامل اصلی باز دارنده گسترش آن در کشور مطرح بوده است.

بانکداری الکترونیکی در طی سالیان متمادی مسیر گشترش خود را در کشورهای پیشرفته طی نموده و با ایجاد مسیرهای جدید ارتباط مشتری با بانک، کاهش چشگمیر حضور مشتریان در شعب، به خصوص در شهرهای بزرگ را در بر داشته است. در طی چند سال اخیر با گسترش فن آوری اطلاعات و ارتباطات و مطرح شده هر چه بیشتر تجارت الکترونیک به عنوان روشی برای انجام عملیات داد وستد، چه در سطح مشتریان خرد و کلان (B2B'B2C)، کشورهای پیشرفته دارای امکانات بانکداری الکترونیک، خود را در موقعیت ممتاز به دلیل دارا بودن بستری مهم برای انجام تراکنش های مالی دیده و با استفاده از این امکانات به عنوان پیش نیاز اصلی تجارت الکترونیک و تمرکز بر گسترش کاربردهای آن، به پیشرفت های چشمگیری در داد و ستد های الکترونیکی دست یافته اند.

با درک این نیاز طی سالهای اخیر بانک کشاورزی فعالیت ههای زیر بنایی مهمی‌را انجام داده است که زمینه لازم را برای حرکت به سوی بانکداری الکترونیکی به نحوی که بتواند پاسخگوی تقاضاهای تجارت الکترونیک و داد و ستدهای داخلی باشد، ایجاد خواهد نمود.

این گزارش با ارائه مراحل چند گانه حرکت چندین ساله بانک کشاورزی در خود کار سازی عملیات بانکی خود، سرعت بخشیدن در ارائه خدمات به مشتری وایجاد کانال های جدید خدمات، پیشرفت های حاصله در این زمینه را شرح داده و مواردی را که توسعه آنها ساختار مورد نیاز تجارت الکترونیک را ایجاد خواهد نمود. و از طرف بانک در دست اقدام می‌باشد، ارائه می‌نماید.

الزامات بانکداری الکترونیکی در توسعه ی تجارت الکترونیکی

جمعه 3 مهر 1383
دکتر فرهاد دژپسند

اشاره: معاون وزیر بازرگانی هم در همایش پول الکترونیکی به ایراد سخنرانی پرداخت و دیدگاه های خود را مطرح نمود. با هم متن سخنرانی وی را می‌خوانیم.

بحث الکترونیکی کردن امور به خصوص تجارت، یکی از مقولات بسیار مهم اساسی است که باید از زوایای گوناگون مورد توجه و تامل قرار گیرد. وقتی که موقعیت خودمان را در اقتصاد بین الملل مرور می‌کنیم و عدم تحقیق اهداف را تحلیل می‌کنیم، یکی از گلوگاه‌های اساسی، توانایی اندک در استفاده از فرصت‌هایی است که می‌تواند در کشور تحولات مثبت ایجاد کند. وقتی که در عرصه ی جهانی دو انقلا بزرگ، یعنی انقلاب فناوری اطلاعات و ارتباطات و انقلاب جهانی شدن را مرور می‌کنیم، به این می‌اندیشیم که برای بیشینه کردن یا حتی برای دستیابی به حد قابل قبول در زمینه ی حضور در اقتصاد بین الملل، باید از همه ی فرصت‌ها استفاده بکنیم. به عبارتی همت خودمات را معطوف کنیم که باید با بهره گیری از این فرصت‌ها؛ تبعات منف را به حداقل ممکن کاهش دهیم ونیز از تبدیل فرصت‌ها به تهدیدها نیز جلوگیری کنیم و بتوانیم جایگاه شایسته ی خودمان را پیدا کنیم. وقتی شاخص‌ها را مقایسه می‌کنیم، می‌بینیم که در برخی از شاخص‌ها سهم کوچکی داریم. مثلا سهم ما در جمعیت جهان حدود 1 درصد است. یامثلا از نظر مساحت 1 درصد است. به همین تناسب هم از نظر حضورمان در اقتصاد جهانی دوست داریم حداقل این سهم را داشته باشیم. نکته ی دوم که نگرانی ما را بیشتر می‌کند، این است که سهم ما در یک روند نزولی طی دو دهه کاهش پیدا کرده است. این نکته دوم که نگرانی جدی تری ایجاد می‌کند. اکنون زمان آن است، که از خود بپرسیم چرا؟ ما در

پیدایی علل وقوع این موقعیت ممکن است دلایل زیادی را بر شماریم و فهرست کنیم. اما از آنجا که قرار است راجع به حضورمان در بازار بین المللی بحث بکنیم، نیازمند این هستیم که عوامل موثر در ایجاد این تعامل را نگاه بکنیم. ما با مجموعه ای مواجه هستیم که دارای سلایق مختلف و با سرعت بسیار بالا در حال تحول است با مجموعه ای مواجه هستیم که دارای سلایق مختلف و با سرعت بالا در حال تحول است. ما با مجموعه ای که از فناوری بهره مند هستند که با روند نمایی در حال رشد است. با جوامعی روبه رو هستیم که به واسطه ی تحولات و نو آوری‌های خودشان، به شدت دارند هزینه‌های تولید کالا و خدمات را کاهش می‌دهند و هم به خاطر بهره مندی از بازار مصرف و منابع کشورهایی مانند ما، چه منابع طبیعی و فیزیکی وچه منابع انسانی، دارند استفاده می‌کنند و از این منابع مزیت نسبی خودشان را تبدیل به مزیت رقابتی می‌کنند. با گذشت زمان نیز فاصله را کاهش و حضور خودشان را افزایش می‌دهند. در مواجه با این شرایط اگر ما هوشیاری لازم را به خرج ندهیم، همان طور دو دهه ی قبل، سهم ما از 49 صدم درصد به کمتر از 43 صدم درصد کاهش یافته، باز هم این روند ادامه خواهد یافت بدین روی باید به شدت به دنبال استفاده ی حداکثری از فرصت‌های خلق شده در عرصه ی دانش و فناوری دنیای پیرامون باشیم. ما اگر بخواهیم در عرصه ی اقتصادی وتجارت از مزیت رقابتی بهره مند شویم و در اقتصاد بین المللی حضور یابیم و سهممان را افزایش بدهیم، باید هزینه ی تمام شده ی تولید کالا و خدمات را کاهش بدهیم. باید ضریب انتشار اطلاعات مربوط به کالا و خدمات ومزایایی تولیداتمان اعم از کالا و خدمات را کاهش بدهیم. باید ضریب انتشار اطلاعات مربوط به کالا و خدمت و مزایای تولیداتمان اعم از کالا و خدمات را افزایش بدهیم. باید فرصت‌هایی که امکان عرضه یی تولیداتمان در دنیای بیرون را افزایش می‌دهد، مورد استفاده قرار دهیم. برای این که به بهترین وجه در بازار بین الملل خودمان را نشان بدهیم، باید از چند مقوله ای

که امرزو در عرصه ی اقتصاد تجاری بین الملل به شدت مورد استفاده است و با روند نمایی در حال افزایش است، استفاده بکنیم. باید روی پدیده ی تجارت الکترونیکی تمرکز کنیم منظـور از تجـارت الکترونیکی کلیه ی امور مروبط به تجارت، اعم از جستجو، مذاکره، انعقاد قرار داد و پرداخت در محیط الکترونیکی اعم از شبکه‌های اینترنتی و رایانه ای است. در این تعریف، از یک زاویه تجارت الکترونیکی یک مکعبی است که از تجارت سنتی تا تجارت خالص الکترونیکی در دو ضلع این مکعب باید حرکت بکنند. از کالاها و خدمات فیزیکی گرفته تا دیتجیتال. این یک زاویه ی تفکیک و تعمق اسـت. یـک زاویه دیگر درون بنگاه‌ها است که بایـد کشـب و کـار را نیـز الکترونیکـی کنـیم. اینجـا داد و سـتد الکترونیکی فراتر می‌رویم. چرا که تجارت الکترونیکی می‌تواند در سطح بین بنگاه‌هـای اقتصـادی بـا مشتری، بین بنگاه‌های اقتصادی باهم، بین بنگاه‌های اقتصادی با دولت و بین دولت‌ها با یکدیگر باشد. یک سری الزامات مترتب بر تجارت الکترونیکی را سازمان بدهیم.

وقتی که که امروز بدبینانه ترین برآورد به ما می‌گوید که تجارت الکترونیکی به طور متوسط در دوره ی زمانی سال‌های 2002 تا 2006 سالانه 54 درصد رشد دارد، وقتی که آمارها برای برخـی از کشورها بالای 100 درصد رشد قایل می‌شوند، وقتی که می‌بینیم خیلی از خرید و فروش‌ها در محیط الکترونیکی دارد صورت می‌گیرد و اگر ما نتوانیم خودمان را در این عرصه وارد کنیم و از این محیط استفاده الکترونیکی را سازمان بدهیم. لوازم تجارت الکترونیکی در چند بخش تفکیک می‌شود. بخشی بر می‌گردد به زیر ساخت‌ها اعم از فنی، نیروی انسانی، حقوق و قضـایی. بخشـی بـر مـی‌گـردد بـه لجستیک که در این بحث گمرک، حمل ونقل و بانکداری را می‌بینـیم. امـا در ایـن میـان بانکـداری الکترونیکی دارای نقش خاصی است. چرا که اساس خلق پول برای تجارت بوده است. کافی است ما

مروری سریع داشته باشیم هنوز تفکیک حریم‌ها صورت نگرفته و مالکیت‌ها تفکیک نشده کـه داد و ستد موضوعیت پیدا کند، از آن پس می‌بینیم تامین نیازها با مبادلات صورت می‌گیرد.

در مراحل آغازین داد و ستد و معامله به صورت پایاپای صورت می‌گیرد، امـا مشـکلات فراوانـی مبادلات پایاپای بشر را به سمت یک معیار واحد ارزش هدایت می‌کند. به این ترتیب بشر پول کالایی می‌رسد. اما در گام بعدی بشر متوجه می‌شود که این کالا به عنوان وسیله مبادله عیوب زیادی دارد با سرعت پول کالایی تبدیل به پول فلزی می‌شود. البته همه ی این کارها برای تسهیل تجـارت اسـت. حالا در ایران کاغذی می‌شود تا به امروز که تبدیل به پول الکترونیکی می‌گردد.

حالا در ایران اگر مـا خواسـتار توسـعه ی تجـارت الکترونیکـی هسـتیمف بایـد روی بانکـداری الکترونیکی بیشتر بیشتر تمرکز کنیم و مورد توجه قرار بدهیم. به دو دلیل روی بانکداری الکترونیکی تاکید داریم. یکی این که می‌خواهیم در این محیط در امور بانک‌ها گام‌های سـریع تـر و بلنـد تـری برداریم. دوم این که این نظام بانکی ما متاسفانه گاه گاهی به خاطی غیر رقابتی بودن کلی سیسـتم، نیازمند دستورات مرجع بالاتر است. البته خوشبختانه در شورای عالی بانک‌ها و مجمع عمومی‌بانکها و حتی در دولت هم به شدت روی این مقوله تاکید می‌شود اما در ایران ما بیشتر نیاز داریم که بتوانیم این کار را انجام بدهیم. پس ما باید این امر را به سرعت بیشتر انجام بدهیم تا کار با بـه یـک جـای مناسب برسانیم.چون پول الکترونیکی یک حلقه ای است در یک زنجیره ی بزرگ که اگر به این مهم دست پیدا کنیم، به تدریج به بقیه ی حلقه‌های مرتبط با آن نیز دست پیدا می‌کنیم. اما اگر چنـین نباشد، نمی‌توانیم از این الزامات استفاده بکنیم.

در سال 2004 برآورد می‌شود که هر کاربر اینترنت به طور متوسط 585 دلار پرداخت خود را به صورت بر خط انجام بدهد. پیش بینی می‌شود این رقم در سال 2008 به 780 دلار، یعنی 1/5 برابر

برسد. وقتی که ما پول را وسیله ی مبادله، وسیله ی ارزش گذاری و وسیله ی ذخیره می‌دانیم، این تعریف برای انواع پول‌ها صادق است. از جمله کارت اعتباری، کارت بدهی، کیف پـول الکترونیکـی و سایر کارت‌ها انتشار پول الکترونیکی یکی از مقولات جدی است. وقتی پول غیر الکترونیکـی مطـرح می‌شود، ناشر این پول را یک مرجع است. به همین دلیل در تیوری‌های عرضه و تقاضای پول، بحث عرضه را که مطرح می‌کنند یک خط عمومی‌برایش متصور می‌شوند، چون معتقدنـد بانـک مرکـزی سایت گزار اصلی میزان عرضه ی پول است، اما وقتی که همین را در محیط پول الکترونیکی بررسی می‌کنند به واسطه ی این که ناشر پول الکترونیکی دیگر فقط مراجع دلتی نیستند، یک تاثیر اساسی در مباحث مروبط به عرضه ی پول برای آن قایل می‌شوند انتشار پول الکترونیکی را نهادهای جدیـد انجام می‌دهند. علاوه بر بانک‌ها، موسساتی مثل ویـزاو مسـتر کـارت شـرکت‌های ارتباطـات راه دور، شرکت‌های فناوری اطلاعات مثل کیف دیجتیال یا هو و مایکروسافت این وظیفه و کارکرد را به عهده می‌گیرند. بنابراین یک سری مشکلاتی به وجود می‌آید که در تجارت مورد توجه قرا ر می‌گیرد مثل این که آیا این نوع پول‌های منتشر شده در عملیاتی مثل اخذ و وصول مالیات، همان اعتبار را دارد. آیا امنیت واطمینان لازم را در مقوله ی مبادلات همان طور که ما برای پول منتشر شـده توسـط بانـک مرکزی داشتیم، اینجا نیز داریم و اگر نه تجارت در مقیاس بزرگ را چگونه باید انجام دهـیم؟ کـاملا درست است. آن اطمینان وامنیت را ندارد. اما چون فواید بی شمار دیگری دارد، سـعی مـی‌کنیم بـا تعبیه ی سیستم‌های امنیتی حاشیه ای نگرانی‌ها را به حداقل کاهش دهیم تا بتـوانیم از فوایـد آن بیشترین استفاده را بکنیم پرسش دیگر این است که با این کار آیا نقش بانک مرکزی کاهش پیـدا می‌کند؟ پاسخ منفی است از یک سو اساسا در کشورهایی مثل ما که موسسات خصوصی انتشار پول الکترونیکی از قوام لازم برخوردار نیستند، اتفاقا بانک مرکزی با ورود سریع تر به این عرصه و با تجهیز

خودش به واسطه ی اطمینانی که برخوردار نیستند، اتفاقا بانک مرکزی با ورود سریع تر به این عرصه و با تجهیز خودش به واسطه ی اطمینانی که ایجاد می‌کند و به واسطه ی امنیتی که پول منتشر شده توسط بانک مرکزی دارد، آن اقتدار می‌کند، دیگر در این عرصه کارکرد خودش را از دست می‌دهد. لذا همچنان بانک مرکزی به عنوان تولیت شواری عالی باید کارکرد خودش را داشته باشد که بتواند این کار را بکند. چون هنوز بحث نرخ بهره در این سیستم با حدود و دامنه ای که توسط بانـک مرکـزی تعیین می‌شود کارش را انجام بدهد. پرسش دیگر اینجاست که بانک مرکزی در ارتباط با تاثیری که تغییر شکل پول به حالت الکترونیکی روی تقاضای پول دارد، چه باید بکند؟ بانک مرکزی به واسطه ی ویژگی‌هایی که پول متعارف دارد، امنیت، مقبولیت و مسایل قـانونی اش، بایـد تـلاش بکنـد بخـش خصوصی متولی نشر این پول باشد. بانک مرکزی نمی‌تواند این نقش خودش را ایفا کند و حضورش را عرصه ی بازار پول حفظ کند. البته بحث‌هایی مثل کاهش حق ضرب، کاهش هزینه‌های مترتب بر این کار، کاهش ذخایر قانونی مواردی است که در ترازنامه بانک مرکزی تاثیراتش را می‌گذارد. یک نگرانی که وجود دارد و برخی از مقالات انتقادی که در زمینه ی مخاطرات پول الکترونیکی ارایه می‌شود نیز روی آن تاکید دارند، روند الکترونیکی کردن بانک و تولید و تهیه ی پول الکترونیکی است. اساسا این نگرانی‌هایی که ممکن است نظام پولی ما را به هم بریزد، اساسا نگرانی بی اساسی است به اعتقاد من یکی از بحث‌های جدی ما در بانکداری الکترونیکی باید داشته باشیم، بحث اتاق پایاپای چک است که ما این را به شدت باید دنبال کنیم و این کار را انجام بدهیم. مرکز تسویه ی چک در بانـک مرکـزی امروز در 150 شعبه کشور وجود دارد. اما یک نگرانی جدی و محوری این است که هیچ کدام مکانیزه و بر خط نیستند. در گزارشی که اخیرا در یکی از مجامع رسمی‌ارایه شد، گفته بودند که حداقل یک ماه طول می‌کشد تا چک‌ها مبادله بشود. ولی بررسی‌های ما 15 روز را نشان می‌دهـد. 15 روز بـرای

این امر خیلی زیاد است. بنابراین باید بحث اتاق پایاپای چک را با توجه به نیازمندی‌های پول الکترونیکی سازمان بدهد. اساسا پرداخت مبتنی بر کارت را از زوایای گوناگونی ما باید در سیستم راه بیاندازیم بعضی از مقولات هستند که همیشه نمی‌توانیم منتظر انجام آنها باشیم و انجام هر یک را لازمه ی دیگری بدانیم. پیشنهاد بنده به شورای عالی بانک‌ها این بود که ما از دولت تقاضا می‌کنیم تمام پرداخت حقوق کارمندان ابتدا در مقیاس ستادی، بعد در مقیاس استانی، از طریق حساب‌های منوط به کارت صورت بگیرد. این امر به طور خودکار استفاده از این کارت را جا می‌اندازد و تعمیم می‌دهد. ما نگران مقاومت فرهنگی در مقابل استفاده از این کار نخواهیم بود. البته پدیده ای نیست که امروز اراده بکنیم فردا تحقق پیدا کند اما اتفاقا این امر کمک می‌کند همچنین فرهنگ استفاده از این نوع کارت‌ها تعمیم پیدا کند. از سوی دیگر بانک‌های ما انگیزه ی بیشتری پیدا می‌کنند برای مجهز شدن به این سیستم این که ما امروز فقط 5 تا بانکمان به مرکز شتاب وصل هستند، یکی از نگرانی‌های جدی است و جالب این است که همه ی این 5 بانک هم بانک‌های دولتی نیستند. به عبارت دیگر این سوال وجود دارد که چرا بانک‌های دولتی ما در دستیابی به این مهم تعلل می‌کنند. علی رغم این که در تمامی‌جلسات وقتی در مجامع و شورای بانک‌ها راجع به بودجه بحث می‌شود، اولین سوالی این است که بودجه ی لازم برای بانکداری الکترونیکی تصویب شده است یا نه؟ اما امروز متاسفانه مرکز شتاب از حضور حدود 7 بانک دولتی بی بهره است البته خوشبختانه دو بانک بزرگ دولت وصل هستند، ولی هنوز این سوال وجود دارد که چرا؟ بنابراین یکی از مقولات بسیار مهم این است که بحث پروسه ی اتصال به شکبه ی شتاب را جدی تر انجام بدهیم. این بحث‌ها عمدتا به بحث تجارت داخلی مربوط می‌شود. در تجارت خارجی اتفاقا برای افزایش سهممان در بازار جهان باید سیستم تسویه ی بین المللی، شبکه ی سوییچ عملیات بانکی و بین بانکی و داخلی و خارجی و شبکه

ی Swift را به طور جدی مورد توجه قرار بدهیم. چرا که اگر نخواهیم این کار را بکنیم، به شدت مشکل خواهیم داشت. اگر نتوانیم بین شعبه ی مرکزی و بانک‌های تجاری و بانک‌های خارجی ارتباط بر خط برقرار بکنیم، اساس پدیده ی استفاده از بانکداری الکترونیکی در مقوله ی تجارت خارجی ما را با مشکل مواجه می‌کند.

امروزه می‌گویند 2/5 میلیون کارت وجود دارد، اما همه این 2/5 میلیون کارت بدهی است. ما اصلا کارت اعتباری نداریم واین بحث خیلی مهمی‌است. خوشبختانه ما در ایران تجربه کارتهای غیر بانکی را هم داریم. به عبارتی وقتی که ما می‌گوییم بانکداری الکترونیکی، پول الکترونیکی یکی از ملزومات اجتناب ناپذیر آن است. اگر ما آن را نداشته باشیم، تجارت الکترونیکی ما روی زمین است. در مدل بخشی تجارت الکترونیکی اساسا حضور موسسات خصوصی انتشار پول الکترونیکی، خیلی مشکلات را حل کرده است. یعنی شعبه‌های بسیار زیادی بدون اینکه بانک باشند، این کار را کرده اند. خوشختانه در ماده 12 برنامه چهارم، الزامات الکترونیکی کردن و الکترونیکی شدن تمام بانک‌ها در سال اول مورد توجه قرار گرفته و در آن تاکید بشده هم برای مشتریان در سطح ملی و هم در سطح بین المللی باید اعمال گردد. بانک مرکزی برای این که این مهم را انجام دهد، با چالش‌هایی مواجه است. اولین چالشی که بانک مرکزی با آن مواجه است یکپارچگی بین زیر ساخت سازمان بانک‌های مرکزی و سایر بانک‌ها با کاربران فناوری اطلاعات است. در این زمینه مشکلاتی وجود دارد. اعم از زیر ساخت‌ها روشها و اصول مدیریتی الان 4 سال است نظام بانکی ما می‌گوید من برای بانکداری ال 15000 پورت نیاز دارم. مهمترین نویدی که داده شد ما تا پایان شهریور 3500 پورت تجهیز می‌کنیم. دومین چالشی که ما در این عرصه داریم این است که بخش خصوصی در ایران هنوز خودش را به طور جدی با این پدیده تطبیق نداده است. حتی ثمین کارت هم حضور بخش خصوصی را نشان

نمی‌دهد. در حالی که ما می‌بینیم در سایر کشورها روی بخش خصوصی تاکید دارند. البته شاید بخشی هم به خاطر این است که شاید در کشورهای پیشرو مثل امریکا موتور و آغازگر تجارت الکترونیکی بخش خصوصی بوده اما این مقوله و این موانع را ما داریم. مثلا هماهنگی را وقتی ما مطرح می‌کنیم در آمریکا 12 بانک خزانه داری فدرال این کشور یک مرکزی را تشکیل داده اند که بانک مرکزی الان به این مهم اقدام کرده و یک شورایی با حضور یکی از اعضای هیات مدیره همه بانک‌ها در حال تشکیل است که این کار را هدایت بکند. هر عضوی از هیات مدیره هر بانکی که در این زمینه متخصص است درواقع جمع کرده و یک نهادی را تشکیل داده که این کار را بتواند انجام بدهد. این مهم است که باید ما سریع تر این کار را انجام بدهیم.

به دو نکته در زمینه بانک‌ها در محیط بانکداری الکترونیکی اشاره می‌کنیم. نکته اول این که ما نباید همیشه منتظر باشیم که برای ما دستور العمل لازم را صادر بکنند و بعد گام برداریم. ما وقتی که ارزیابی می‌کنیم می‌بینیم که متاسفانه همین امسال اخرین ارزیابی که به خاطر بررسی گزارش ملی تجارت الکترونیکی مناسب با مولفه‌های آنکتاد بررسی کردیم از میان بانک‌های ما 4 تا بانک خوشبختانه جلو هستند اما این 4 بانک هم فاصله زیادی دارند و متاسفانه در همین بانک‌ها هنوز مشکل استفاده از دستگاه‌های خود پرداز و POSها را داریم. باید همت جدی به این امر اختصاص پیدا کند. یعنی به عبارتی همیشه نمی‌شود تقصیر را به گردن مخابرات انداخت. به عبارتی بانک‌ها باید این کار را بکنند. بحث نیروی انسانی نیز مقوله ای بسیار مهم و کلیدی است. خوشبختانه بانکی که در سال 82 با ارزش بسیار بالاتری مواجه بوده بانکی بوده که دو سال قبل تمام ورودی‌های نیروی انسانی را محدود کرده بود به نیروی انسانی واجد شرایط خاصی از نظر علمی‌و آکادمیک. سطح علم و مدرک همکاران عزیز، ارجمند و زحمتکش ما در نظام بانکی است. خود یکی از معضلات است. مقوله بسیار

مهم تر و سومین بحثی که ما داریم مشکل قوانین است. خوشبختانه با ابلاغ قانونی تجارت الکترونیکی خیلی از مشکلات حل شد یعنی امضای الکترونیکی تایید شد داده پیام به عنوان سند تلقی شد اما هنوز چک الکترونیکی سفته الکترونیکی و اساسا اسناد تجارت الکترونیکی مشخص نیست که از نظر قانون مجوز دارند یا نه؟ بنابر این مجموعه ای نیاز داریم که بتوانیم بانکداری و پول الکترونیکی را متناسب با سرعت تجارت الکترونیکی داشته باشیم. هفت سال است که قانون تجارت در کشور وجود دارد و به جز یکی دو بار که اصلاح مختصر داشته اصلاح نشده است. خوشبختانه ما در اصلاح و بازنگری این قانون به طور جدی توجه خود را معطوف کردیم به تطبیق این قانون با محیط الکترونیکی به ویژه اسناد تجاری را به طور جدی مورد توجه قرار دادیم که امیدواریم بتوانیم بخشی از نیازها را تامین بکنیم.

کارت‌های هوشمند و پول خرد الکترونیکی، اولویت نخست نیازها

گفت و گونی تکفا با دکتر ولی فاطمی

اشاره: گفت و گو با دکتر فاطمی، پس از آن انجام می‌شد که ما یک میزگرد با مدیران بانک‌های بزرگ برگزار کرده بودیم و پس از نکات و مشکلاتی که از قبل با آنها آشنا شده بودیم، گفت وگوی تخصصی تری را با دکتر فاطمی‌انجام دهیم. وی که دوره‌های کارشناسی و کارشناسی ارشد خود را در دانشگاه صنعتی شریف و دوره ی دکتری را در دانشگاه صنعتی امیر کبیر در رشته ی مهندسی کامپیوتر گذرانده است، سوابق و تجارت کاری بسیار مفید و ارزنده ای در زمینه ی سیستم‌های اتوماسیون بانکی، با شرکت لاله کامپیوتر و یکی از صندوق‌های قرض الحسنه در زمینه ی طراحی سیستم و بالاخره با شرکت کیش ویر در راستای طراحی و پیاده سازی سیستم‌های اتوماسیون بانکی همکاری داشته است. بانک ملت، بانک سامان، بانک اقتصاد نوین، موسسه ی اعتباری توسعه و صندوق انصار جز و مراکزی هستند که دکتر فاطمی‌در زمینه ی طراحی سیستم بانکداری الکترونیکی با آنها کار می‌کند. وی همچنین با کمیته ی پرداخت خود بانک مرکزی نیز همکاری می‌کند. اطلاعات و تجربیات وسیع و عملی دکتر فاطمی‌می‌تواند برای ما و شما جالب و خواندنی باشد:

فکر می‌کنید از چه زمانی در ایران خرید اینترنتی قابل اجرا باشد؟

ما در زمینه ی پرداخت الکترونیکی یا اینترنتی از چند سال پیش کارمان را با بانک سامان شروع کرده ایم، یکی از مهمترین دستاوردهایی که در حال حاضر وجود دارد، مربوط به بحث بانک اینترنتی است، به طوری که شما بتوانید عملیات بانکی به راحتی و بدون نیاز به حضور در شعبه انجام بدهید. یعنی علاوه بر اطلاع رسانی، دریافت صورت حساب و موجودی، بتوانید تبادل الکترونیکی پول را نیز اجرا کنید، به عنوان مثال درخواست وام یا چک را بتوانید در اینترنت انجام دهید یا عملیات کارت را

آنجا ثبت کنید. به طور کلی یک دروازه ای برای ورود به دنیای تجارت الکترونیکی (E-Commerce) فراهم شده است. در کنار این خدمات، ما بحث پرداخت اینترنتی را با پیاده سازی دو استاندارد مختلف برای پرداختهای خرد و کلان به انجام رسانده ایم. در مورد پرداختهای خرد قاعدتا سهولت و سادگی استفاده خیلی مهم است. و امنیت در اولویت دوم اهمیت می‌باشد. البته بیمه در کنار این قضیه لازم است، اما بیمه ی مربوط به ان هم خیلی سنگین نیست. بحث دیگر در مورد پرداختهای کلان است که بیشتر در مورد معاملات بین سازمان‌های تجاری با یکدیگر (B2B) و یا بین سازمان‌های تجاری با دولت (B2G) و یا بین دولتها با یکدیگر (G2GH) برای تبادل مبالغ زیاد می‌شود، یعنی مبالغ بالای چند صد هزار تومان یا چند میلیون تومان در این سطوح، دیگر اشخاص، کمتر درگیر هستند و بیشتر شرکتها لازم دارند که ارتباطات مالی خودشان را انجام دهند. در این پروتکل امنیت اولویت اول است و عدم انکار طرفین در انجام معامله اصل اساسی است. یعنی در دنیای مجازی یا اینترنت، ثبت سوابق و کار باید به گونه ای انجام شود که هیچ کس نتواند درستی آن را انکار کند. پروتکل مشهوری که در این زمینه در تمام دنیا وجود دارد، (ست) (Set) است که ما شکل ساده شده ای از این پروتکل را اجرا کرده ایم. این دو نرم افزار در حال حاضر در بانک سامان عملیاتی شده است. تا کنون در سطح کشور نزدیک به 60 مورد عقد قرار داد انجام شده و به زودی ارایه ی خدمات خرید یا فروش مجازی شروع می‌شود. این خدمات در حال حاضر با کارت بانک سامان در حال اجرا و قابل توسعه به عملیات کارتهای عضو شتاب نیز می‌باشد. البته ما این خدمات را با کارتهای عضو شتاب شروع و به صورت آزمایشی هم چند هفته راه اندازی کردیم، اما متاسفانه به خاطر نگرانی از عدم امنیت کافی در زیر ساخت کارتهاهای بانک‌های بزرگ و واکنش منفی چند بانک دولتی به توصیه ی بانک مرکزی به طور محدود تا زمانی که در یک کمیته ی خاص در بانک مرکزی

ضرورت‌های بستر امنیتی برای بانک‌ها تدوین و ارایه شود، متوقف شده است. در زمانی که بانک‌ها در یک زمان بندی منطقی این امنیت را اجرا بکنند، این خدمات را به صورت یک کار فراگیر می‌توانیم انجام دهیم. من می‌توانم قول بدهم که ظرف 3-2 ماه آینده شرکت‌های بسیار زیادی خواهیم داشت که این سرویس را به مردم ارایه خواهند کرد.

یعنی واقعا می‌توان امیدوار بود که ظرف 3-2 ماه آینده بانکداری اینترنتی در ایران راه اندازی شده باشد؟

پرداخت اینترنتی حتما راه خواهد افتاد. خدمات بانک اینترنتی را بعضی بانک‌ها در حال حاضر همه دارند. من بیشتر منظورم موضوع پرداخت اینترنتی بود. همین الان شما می‌توانید با استفاده از اینترنت، یک خرید کارت تلفن یا کارت اینترنت را داشته باشید. اول مهر، زمان افتتاح سایت رجا به عنوان یک سایت مورد نیاز قشر گسترده ای از مردم، یک حرکت مناسبی خواهد بود. کافی است بانک مرکزی هم آن محدودیت را از روی بانک‌ها بر دارد که ما می‌توانیم به سرعت این خدمات را به صورت گسترده به مردم ارایه بدهیم. شرکت‌ها با جدیت تمام علاقمند هستند که این خدمات را ارایه کنند. یعنی بر عکس بیشتر بانک‌ها که آمادگی پذیرش این ریسک را ندارند. شرکت‌هایی هم داریم که ریسک کامل عملیات را می‌پذیرند. هر چند که فروشنده بابت فروش اینترنتی یک درصدی از پرداخت را هزینه می‌کند، فروشنده‌های بسیاری به این قضیه علاقمند هستند و استقبال بیش از حد است. سیستم‌های بانکی دولتی به خاطر ماهیت دولتی بودن خود، عموما نگران مشکلات عملیات باشند، تا اینکه به صورت کلی بحث در آمد و خدمات را ببینند. به این دلیل که هنوز در سیستم‌های دولتی ما مدیریت ریسک (Resk Managemevnt) و کارایی جایگاهی ندارد. نمی‌توانیم بگوید که این مدیری باید در مقابل کاری که انجام داده، این قدر ریسک پذیری داشته باشد. به خاطر چند هزار

تومان یک مدیر دولتی که چندین میلیون تومان گردش مـالی (Turn Orer) داشـته بـاز خواسـت می‌شود و این یکی از بزرگ ترین معضل‌ها در سیستم‌های دولتی ایران است. اگر مـا بتـوانیم بحـث مدیریت ریسک را جا بیاندازیم و از آن طرف بیمه‌ها هم برخورد فعال تری داشته باشند، طبیعتا نـه ضرر مالی متوجه بنگاه‌های مالی می‌شود و نه مدیری متهم می‌شـود. اسـتفاده کننـده از خـدمات و فروشنده، هر یک هزینه ی محدودی را می‌پردازند و در مقابل از یک سرویس خیلی خوب و راحـت بهره می‌گیرند.

با توجه به اینکه سیستم خرده فروشی در ایران هنوز حالت سنتی دارد و فروشگاه‌های زنجیره ای بزرگ و گسترده به اندازه ی کافی موجود نیست، فکر می‌کنیـد فروشـگاه‌های کوچک می‌توانند سرویس اینترنتی را ارایه بدهند؟

واقعیت این است که اگر ما بخواهیم سراغ خیلی خرده فروشی خیابانی برویم، شـاید مشـکلاتی داشته باشد، ولی یک چیز خوبی که در این مدت من خود در تبلیغات دیده ام، خیلی از مغازه‌هـای معمولی، کالاهای خود را در رادیو یا تلویزیون یا روزنامه آگهی می‌کنند. این نشان می‌دهـد کـه ایـن خرده فروش آنچنان که ما فکر می‌کنیم در حد یک بقالی نیست. وقتی مثلا یـک مـانتو فروشـی در خیابان ولیعصر تهران آگهی تلویزیونی پخش می‌کند و چندین میلیون برای آگهی اش هزینه میکند این نشان می‌دهد که فرهنگ فروش، حتی در فروشگاه‌های کوچک نیز مطـرح شـده اسـت. فـروش اینترنتی هم یکی از راه‌های خیلی خوب برای عرضه یا ارایه ی محصول است. یک بستر سـازی کـه اتفاقا چند شرکت بزرگ و خصوصی دارند آن را انجام می‌دهند، ایجاد فروشگاه‌های مجازی بـزرگ و فروش و عرضه یا اجاره ی فضای لازم است. در این فروشگاه دیگر بحث زمین نیست که شما یک ملک را اجاره کنید، مثلا یک یا چند کیلو بایت را رزرو می‌کنید و از این را محصولتان را عرضه می‌کنیـد.

یعنی من فکر می‌کنم در مدت کوتاهی این فرهنگ برای اغلب فروشگاه‌های معتبر جا می‌افتد. جاهایی که محصولات خاصی را عرضه می‌کند، قطعا برایشان صرف می‌کند که سالیانه مبلغ صد هزار تومان هزینه کنند و کل اجناسشان را در اینترنت عرضه نمایند. ما در ایران بین 3 تا 4 میلیون کارت در دست مردم داریم. 500 هزار تا از این 4-3 میلیون خیلی راحت می‌توان گفت که به اینترنتی دسترسی دارند.

شما می‌دانید که نزدیک 50 درصد نقل و انتقال پول در شهرهای بزرگ، به ویژه تهران انجام می‌شود. ما حداقل اگر این قسمت را پوشش بدهیم، به اندازه ی کافی تبادل پول را کم می‌کنیم یکی از بزرگترین مشکلات بانک مرکزی بحث گردش پول و از رده خارج کردن پول‌های فرسوده است. خوشبختانه بانک مرکزی نزدیک به 2 یا 3 ماه است که بعد از یک دوره رکود چند ساله، در این قضیه خیلی خوب فعال شده الان کمیته‌هایی هم برای این کار تشکیل شده اند. یکی از این کمیته‌ها، کمیته ی پرداخت پول الکترونیکی یا پرداخت خرد است که بعد از ابلاغیه ای که آقای رییس جمهور مبنی بر تعیین 3 ماه برای برنامه ریزی پول الکترونیک و تبادل الکترونیکی پول، این کمیته ظرف برای عملیاتی سازی آن انجام وظیفه می‌کند.

به ویژه در زمینه ی کارت‌های هوشمند نیز در ایران یک مقدار مشکل داریم. کارت‌های مغناطیسی از نظر بحث امنیت جواب گو نیستند. کارت‌های هوشمند هم به خاطر انحصاری فناوری شان در دست شرکت‌هایی که ما مشکل تحریم را با آنها داریم، امکان استفاده از امکانات موجود دنیا را در این زمینه به ما نمی‌دهد. در مورد ویزا و مستر کارت، امکان صدور برای بانک‌های ایران وجود ندارد و متاسفانه سایر کارهایی که در بانک‌های ما تا به حال انجام شده، بیشتر کارهایی بوده که یک دیدگاه‌های سلیقه ای و بومی‌شده در آن به کار گرفته شده است. الان مشکلی که داریم 3 یا 4 نوع

کارت داریم و این کارت‌ها هیچ کدام نمی‌توانند در بانک‌های دیگر پذیرفته شوند. مثل مشکلی که ما در زمینه ی چک‌ها داشتیم که با ابتکار ارایه ی ایران چک این مساله حل شد. البته مرکز شتاب در حال حاضر توسط بانک مرکزی برای پرداخت کارتی بین بانکی راه انـدازی شـده، ولـی فعـلا فقـط کارت‌های مغناطیسی را قبول می‌کند. بانک مرکزی برای تدوین استاندارد صدور کارت هوشمند فعال شده است. این وحدت رویه باعث می‌شود که همه ی بانک‌ها در آینده از یک الگوی خاص اسـتفاده کنند و بتوانند کارت‌های همدیگر را پرداخت کنند و امیدواریم هم در قضیه ی پرداخت و هم قضیه ی خدمات فروشگاهی (POS)،ATM و این طور مسایل هم به این وحدت رویه برسیم. مشکلی که الان در ایران داریم این است که نمی‌توانید بستر ویزا و مستر کارت را داشته باشیم. بانک مرکزی باید وحدت رویه را برای همه ی سطوح ایجاد بکند.

بحث دیگر، توسعه ی بستر پذیرش کار در فروشگاه‌ها می‌باشد. در حال حاضر حتی 10 هزار پایانه ی فروشگاهی هم نداریم طبق برآوردی که انجام شده، در ایران حدود 300 هزار تا از این پایانه‌ها لازم می‌باشد تا وقتی که به آن نقطه نرسیم، همیشه مجبوریم یک مقدار پول در جیبمان بگذاریم بانـک مرکزی باید انگیزه و زمینه ی این سرمایه گذاری را فراهم آورد. بانک‌هـای دولتـی در حـال حاضـر توانایی و انگیزه ی کافی برای این کار را ندارند و طبق دستور ریاست جمهوری قرار است شرکت‌های خصوصی در این قضیه فعال شوند که حرکت بسیار بسیار زیبا و مثبتی اسـت.چاره ی دیگـری هـم نداریم. اگر بخواهیم منتظر باشیم که سیستم دولتی فعال شود یا بحث‌های تحریم حل بشود، زمـان می‌برد. بحث سوم هم بحث شبکه‌ها یا سوییچ‌هایی است که باید برای مبـادلات ایجـاد شـود. بانـک مرکزی فعلا مرکز شتاب را راه اندازی کرده و باید با اصلاح و تکمیل آن به بهتر شدن خدمات کمک کند.

در مورد پرداخت‌های خرد فرمودید که این مساله حل شده و ظرف چند ماه آتی به جاهای خوبی می‌رسیم. در مورد پرداخت‌های کلان چه برنامه‌هایی در دست اجرا است؟

در مورد پرداخت کلان، به صورت آزمایشی با چند شرکت این کار اجرا شده است. مشکل ترین قسمت، نیاز به گواهی نامه ی دیجیتالی است و این که وزارت بازرگانی برای صدور گواهی نامه‌های دیجیتالی برای افرادی که می‌خواهند از این پروتکل استفاده کنند آمادگی داشته باشد. تا وقتی که وزارت بازرگانی که از طرف دولت برای انجام این کار مامور شده و قرار دادی را که برای این کار دارد، نتواند اجرا کند، هر کاری که انجام بشود، یک کار محدود است. شاید یک بانک به تنهای بخواهد گواهی نامه صادر کند، ولی جزو ضوابط گواهی نامه‌های دیجیتالی این است که باید این گواهی نامه از یک مرکز معتبر بین المللی گرفته شده باشد و هیچ کدام از این مراکز بین المللی به راحتی آن را به ما نمی‌دهند. من هفته ی پیش شنیدم که یک گواهی نامه از کشور سوئد گرفته شد، اگر قضیه ی بستر گواهی نامه ی دیجیتالی حل بشود، فقط مشکل قوانین و مقررات قضایی را داریم که امیدوارم طبق لوایحی که مجلس برای تجارت الکترونیکی تصویب کرده و در رفت و برگشت با شورای نگهبان است، آن مسایل هم حل بشود. باید کار را شروع کنیم و برویم جلو و کم کم مشکلات را حل کنیم. اگر مشکلات زمان بر بین دولت و مجلس و شورای نگهبان نباشد، قطعا دولت می‌تواند در یک پروسه ی اصلاحی آزمایشی ظرف مدت 6 ماه با 5 –4 لایحه ی مکمل به یک نقطه ی مناسبی برسد. اگر این دو نکته را ما حل کنیم، دیگر برای پرداخت کلان هیچ مشکلی نداریم. در پرداخت کلان مبالغ بالا است و بیمه به این راحتی جلو نمی‌آید. من فکر می‌کنم از نظر فنی، آمادگی کامل وجود دارد. ما نمونه ی شرکت‌ها و بانک‌هایی را داریم که آمادگی کامل دارند. البته این کار به صورت محدود همین الان هم راه افتاده، اما با توافق طرفین. الان خود فروشنده امضا می‌کند و وکالت می‌دهد که من همه

ی مشکلات احتمالی را قبول می‌کنم. خوب در بحث تجارت عمومی‌نمی‌توان با همه قـرار داد امضـا کرد، بلکه باید به یک نحوی دلایل محکمه پسند برای هر کاری وجود داشته باشد. اگر این دو مشکل را از نظر فنی حل بکنیم، می‌توانیم در مورد پرداخت کلان اینترنتی فراگیر هم امیدوار باشیم.

در پرداخت‌های اینترنتی یکی از مشکلات، امضای الکترونیکی است. یکی از مـدیران بانک‌ها در میزگردی که داشتیم اذعان داشت که هنوز امضای الکترونیکی از نظر دایـره ی حقوقی بانک‌ها قابل اعتماد نیست. این مشکل به ویژه در مورد پرداخت‌های کلان چگونـه حل شده است؟

در پروتکل پرداخت کلان نیاز به اداره یا گواهی نامه‌های دیجیتالی است. امضـای دیجیتـالی بـه کمک گواهی نامه ی دیجیتالی انجام می‌شود. یعنی وقتی شخصی گواهی نامه را دریافـت کـرد، بـه کمک آن هر گواهی نامه دیجیتالی انجام می‌شود. یعنی وقتی شخصی گواهینامه را دریافت کرد، بـه کمک آن هر سند اینترنتی یا الکترونیکی را می‌تواند امضای دیجیتالی کند. ولی بدون این قضیه، ما تنها راهی که داریم، همان طور که اشاره کـردم، توافـق در قـرار داد اسـت. نمونـه اش هـم همـین کارت‌های خود پرداز است که بانک از دارنده ی کارت، تعهد می‌گیرد که هر گونه عملیات که از طریق دستگاه خود پرداز با کارت وی انجام بشود، با مسوولیت خود دارنده است. ما مجبور هستیم با قرار داد و وکالت نامه کار کنیم و در واقع ادارات حقوقی بانک‌ها با این فرم‌ها و تعهدهایی که از افراد می‌گیرند، مسولیت را از خود سلب می‌کنند. ادارات حقوقی بانک‌ها طبق قوانین قضـایی تـا زمـانی کـه قـانون پذیزش امضای الکترونیکی در مجلس تصویب و به سیستم قضایی و ادارات حقوق بانک‌ها و کلا اعلام نشود، نمی‌توانند کار دیگری بکنند.

می‌دانید که گواهی نامه ی دیجیتالی را قرار است دفاتر اسناد رسمی‌به مردم بدهند. همان طور که برای در خواست شناسنامه به اداره ی ثبت مراجعه می‌کنیم برای گواهی نامه‌ی دیجیتالی هم مراجعه می‌کنیم. یعنی یک پروسه ای است که در نهایت سیستم قضایی انجام می‌دهد. در سیستم پرداخت کلان هم فروشنده و هم خریدار باید گواهی نامه داشته باشد تا بتوانند باهم تبادل مالی انجام بدهند.

این گواهی نامه‌ها با شماره ی ملی افراد ارتباط دارد؟

قطعا باید به نحوی اطلاعات انحصاری هم جز و مشخصات گواهی نام ثبت شود که از تکراری بودن جلوگیری شود. البته یکی از مهم ترین روال‌های احراز هویت کامل برای جلوی از تکرار می‌باشد. البته داشتن دو گواهی نامه مشکلی ایجاد نمی‌کند، اشکال عمده گرفتن گواهی نامه با عناوین جعلی می‌باشد. همین دلیل هم بدون احراز هویت این است که کسی به اسم شخص دیگری بتواند گواهی نامه بگیرد. به همین دلیل احراز هویت یکی از بخش‌های ضروری است و به همین دلیل هم بدون احراز هویت حضوری به هیچ عنوان گواهی نامه به کسی داده نمی‌شود.

گواهی نامه اصلی یا مادر باید در یکی از شرکت‌های بین المللی ثبت می‌شود؟

در خصوص این بحث فرض کنید در ویندوز (Windows) بخواهید یک امضای دیجیتالی یا یک کار اینترنتی انجام شود، یک تعدادی گواهی نامه ی مادر در داخل خود نرم افزار وجود دارد اگر گواهی نامه ی شما از طریق گواهی نامه‌های مادر قابل شناسایی باشد، به سادگی عملیات امضای دیجیتالی انجام می‌گیرد. در غیر اینصورت باید یک گواهی نامه ی جدید روی آنها درج (Insert) شود. از این نظر یک الزام صد در صد نیست، ولی یک الزام عملیاتی است که اگر نباشد، درد سر ساز است.

این مساله مشکلات امنیتی ایجاد نمی‌کند؟ یعنی آن شرکت بین المللی به تمام مبادلات ما دسترسی پیدا نمی‌کند؟

ببینید، این دیگر بر می‌گردد به فناوری که وجود دارد الان گواهی نامه‌ها را مثلا از نظر الگوریتم رمز نگاری از RSA 1024 بیت استفاده می‌کنند. تا الان در دنیا توانایی شکستن تا 512 بین طول کلید، آن هم با حجم عملیات و هزینه‌های سنگین فراهم شده است.

من از دید شرکت صادر کننده ی گواهی نامه بحث می‌کنم، نه یک هکر.

پروتکل طوری است که کلید اصلی امنیتی را خود شما دارید. در واقع در این پروتکل، یک کلید مخفی دارد و یک کلید عمومی‌وجود دارد. کلید عمومی‌در اختیار همه، ازجمله صادر کننده ی گواهی نامه قرار می‌گیرد، اما کلید مخفی در اختیار خود شخص است بنابراین امنیت در دست خود شما است. نکته ی مهم پروتکل این است که فقط با کلید خصوصی رمز باز می‌شود و هیچ کس دیگری نمی‌تواند آن را باز کند. بحث امنیتش اینجاست که به چه احتمالی می‌توان از کلید عمومی‌به کلید خصوصی رسید دقیقا این نکته امنیتی اینجاست. این احتمال برای بیت‌های پایین الان کم کم دارد راحت می‌شود. اما برای بیت‌های 1024 هنوز امکان پذیر نمی‌باشد . البته باید در طول زمان با پیشرفت فناوری از طول کلید طولانی تر نیز استفاده گردد.

سناریوی خرید را اگر ممکن است برای ما تشریح کنید که به چه ترتیب شروع می‌شود و ادامه پیدا می‌کند؟ این مساله در پروتکل پرداخت خرد و کلان چه تفاوتی دارد؟

در پرداخت فرد خریدار پس از اینکه با فروشنده بر سر خرید توافق کرد، به بانک اعلام می‌کند که می‌خواهم این مبلغ را در وجه آن فروشنده پرداخت کنم. ما در این پروتکل رابطه ی بین فروشنده و خریدار را برای دستور خرید حذف کرده ایم. رابطه بین خریدار و بانک وجود دارد. یعنی خریدار به بانک می‌گوید که این مبلغ در وجه فروشنده پرداخت بشود. با این دستور آن مبلغ در وجه فروشنده پرداخت می‌شود و یک رسید دریافت می‌کند. خریدار رسید را به فروشنده تحویل می‌دهد. فروشنده

رسید را با بانک چک می‌کند. اگر بانک تایید کرد که این مبلغ به حساب وی واریز شـده، جـنس را تحویل خریدار می‌دهد یا خدمات را ارایه می‌کند. مثلا رمز و مشخصات یک کارت تلفن را به خریدار می‌دهد یا مثلا بلیط برایش صادر می‌شود شما چک را در ذهنتان بیاورید. خریدار چکی را به فروشنده می‌دهد خریدار به بانک دستور می‌دهد. که این مبلغ را به حساب فروشنده واریز کن). بانک هم پول را واریز می‌کند و رسید به او می‌دهد خریدار خودش رسید را تحویل فروشنده می‌دهد فروشنده رسید را با بانک چک می‌کند. کل عملیات به صورت الکترونیکی انجام می‌شود. در قضیه ی پرداخت کلان، یک مقدار قضیه سناریو سخت تر است، چرا که امنیت باید بیشتر باشد. در پرداخت خـرد سـناریو بـا 3 مرحله ی ساده، تکمیل می‌شود، اما در پرداخت کلان، شاید 9 مورد رفت و آمد وجود دارد. خریدار در واقع از فروشنده تقاضای خرید می‌کند. فروشنده به خریدار فاکتور امضا شده می‌دهد. به عبـارت بهتر یک فاکتور امضا می‌کند. خریدار هم فاکتور را امضا می‌کند و به فروشنده بر می‌گرداند. اصل عدم انکار در این پروتکل مهم است. باید مراحل دقیق و کامل باشد که هیچ کـس نتوانـد رد کنـد. بعـد فروشنده فاکتور را برای بانک می‌فرستد. بانک مبلغ را پرداخت و تایید آن را به فروشنده ارسال و در نهایت فروشنده تاییدیه ی دریافت پول را به خریدار اعلام می‌کند.

اگر بعد از طی این مراحل، در نهایت کالا به دست خریدار نرسید، چه می‌تواند بکند؟

در اینجا به بحث تقدم و تاخر زمانی اشاره نگردید. بـرای بعضـی از کالاهـا، بانـک بـه فروشـنده می‌گوید تا فاکتور امضا شده ی کاغذی یا مثلا تا رسید امضای شده ی مشتری تحویل بانـک نشـود، پول پرداخت نمی‌گردد. یعنی باید شرکت رسید کالا را تحویل دهد. اگر نیاز به ارسال کالا باشد، عموما پرداخت در وجه فروشگاه پس از تایید دریافت کالا توسط خریدار صورت می‌گیرد. بیمـه هـم اینجـا دخالت می‌کند. شرکتی که حمل و نقل کالا را بر عهده دارد، باید تضمین کافی یا بیمه نامه ی لازم را

داشته باشد. بنابراین فرض بر این است که جنس حتما می‌رسد و اگر نرسد، بیمه خسارت خریدار را جبران می‌کند.

خریدار با فروشنده ارتباط بر قرار می‌کند و زیر رسید فروشنده را امضا می‌کند. قاعدتا فروشنده با این اسم رمز یا امضا آشنا می‌شود. چه تضمینی هست که خود فروشنده از این امضا سود استفاده نکند؟

به نکته ی خوبی را اشاره کردید امضا یک عدد یا رمز نیست. عدد امضا یک تابع ریاضی است که بر اساس مبلغ فاکتور، شماره ی فاکتور و اطلاعات فروشنده و خریدار متغیر است یعنی یک مجموعه ی اطلاعات باهم ترکیب و امضای الکترونیکی گرفته می‌شود. این اطلاعات ثابتی نیست که با یک بار، استفاده افشا گردد. در ضمن فقط رایانه می‌تواند تایید کند.

اشاره داشتید به کلیدهای عمومیو خصوصی لطفا در این مورد توضیح بیشتری ارایه فرمایید.

گواهی نامه‌های دیجیتالی بر زیر ساخت کلید عمومی (Public Key Infrastructure-PKI)ارایه شده‌اند. در این الگوریتم که اصطلاحا به الگوریتم رمزنگاری نامتقارن هم معروف است، دو کلید وجود دارد. یک کلید مخفی خصوصی (Private) و یک کلید عمومی(Public) اطلاعاتی که به کمک کلید خصوصی رمز بشود، فقط به کمک کلید عمومیقابل باز شدن است و بر عکس، اطلاعاتی که با کلید عمومیرمز بشود، فقط با کلید خصوصی قابل باز شدن است. بنابراین اگر من به عنوان یک فرستنده ی A بخواهم اطلاعاتی برای گیرنده ی B بفرستم، با کلید عمومیB رمز می‌کنم کلید عمومیآن کلیدی است که در اختیار همه است، مثل نشانی پست الکترونیکی این اطلاعات رمز شده را فقط و فقط شخص B می‌تواند با کلید خصوصی خود باز کند.

با سرعت بسیار پایین اینترنت در ایران، به نظر شما برای عمومی‌شدن پرداخت اینترنتی مشکلی ایجاد نمی‌شود؟ پرسش دیگر این که حتی طراحی و پشتیبانی سایت‌ها نیز در ایران خیلی ضعیف است به عنوان مثال وقتی 50 نفر هم زمان بخواهند وارد سایت بسیاری از موسسات بزرگ دولتی شوند، مشکل پیدا می‌کند. به نظر شما چه راه حلی وجود دارد؟

تا جایی که من اطلاع دارم متاسفانه هنوز بسترهای خیلی پرسرعت خدمات اینترنت نداریم. اتفاقا مشکل خوبی را شما اشاره کردید. شما می‌دانید که اغلب میزبان‌های اینترنتی ما در کشورها خارجی مثل کانادا هستند، اگر میزبان اینترنت در کشور خودمان باشد، سرعت خدمات رسانی در ایران خیلی بیشتر می‌شود. این مساله یک ضرورت بسیار جدی است. من فکر می‌کنم وقتی نیازش کم کم ایجاد بشود، برنامه ریزی برای آن هم تسریع می‌شود. اخیرا شرکتهای خصوصی هم در این زمینه فعال شده اند قوانین و مقررات هم تا اندازه ای برای این کار تصویب شده است. با کارهای اخیر شرکت مخابرات، مثل راه اندازی نقطه‌هایی دسترسی انتهایی شبکه ی دیتایی کشور (PAP) در این زمینه به نحوی دارد تسریع می‌شود. متاسفانه مشکل دیگر، سکون سال 96 در دنیا در زمینه ی کوچک سازی (Down Sizing) است که به ایران هم منتقل شد، بدون اینکه تب دومش، یعنی استفاده از رایانه‌های بزرگ، به عنوان پردازش گر اصلی به ایران برسد. البته شاید دلیل عمده اش هم تحریم‌هایی است که برای ایران در نظر گرفته شده است. صرفا از نظر فناوری، تحت تاثیر این تحریم‌هایی است که برای ایران در نظر گرفته شده است. صرفا از نظر فناوری، تحت تاثیر این تحریم‌ها بسترهای اساسی فناوری ما تضعیف و از نیازها عقب افتاده ایم. درست است که از نظر بعد سیاسی می‌گوییم تحریم را تحمل می‌کنیم، اما خوب در بعد فناوری برای ما مشکل ایجاد می‌کند رایانه‌های بزرگمان (Main Frame) هم اصلا در اندازه ای نیستند که کارهای سنگین و جدید را انجام دهند و البته که

فناوری‌های دست دوم است. اخیرا بعضی از بانک‌ها سرورهای جدیدی خریده اند، ولی خوب هیچ کدام به صورت جدی مورد استفاده قرار نگرفته اند واقعیت این است که ما فناوری سرورهای بزرگ می‌خواهیم و آن هم هزینه‌ها و مجوزهای لازم را می‌خواهد. همین که مدیریت کشور به این باور برسد که باید این کار را انجام بدهد، من فکر می‌کنم در نظامات بین المللی می‌توان بستر لازم را فراهم کرد و با توجه به این که در حال حاضر بیشتر میزبان‌های اینترنتی یا روی رایانه ی شخصی (PC) است یا روی رایانه‌های بزرگی که راندمان زیادی ندارند، قطعا با عمومی‌و فراگیر شدن سرویس‌ها دچار مشکل خواهیم شد.

مشکل دیگری که وجود دارد بحث بستر مخابراتی است. به عنوان مثال وقتی که بخواهیم بانکداری الکترونیکی در ایران داشته باشیم، اولین الزامی‌که برای ما ایجاد می‌کند، این است که به طور هم زمان تمام شعب اتصال بر خط داشته باشند.

برای ارایه‌ی سرویس‌های خدمات نوین تمام سیستم‌های بانک‌ها به صورت متمرکز خواهند بود. خدمات اینترنتی با تجربه ی موجود در بانک خصوصی با 20 شعبه، وقتی محور شعبه قرار گیرد، شدیدا دچار مشکل می‌شود. بنابراین در صورت تمرکز همین که مرکز بانک ارتباط مطمئن اینترنتی داشته باشد کافی خواهد بود و اتصال بر خط شعب برای بانک اینترنتی ضرورتی ندارد.

بحث این است که ما قبل از بانکداری اینترنتی، باید بانکداری بر خط (Online Banking) را داشته باشیم تا بتوانیم خدمات بانکداری اینترنتی ارایه کنیم. شعبه‌های بانک‌های ما، بیشتر جزیره‌های مستقل از هم هستند که لازم است اطلاعات به صورت متمرکز فقط در مرکز بانک به صورت بر خط در اختیار شعبه‌ها قرار گیرد.

ولی مدیران بانک‌ها از ضعف بستر مخابراتی به عنوان یک مشکل اساسی یاد می‌کنند.

بانک‌های ملی، صادرات و کشاورزی تمام شعبشان از سیستم ماهواره استفاده می‌کنند. بستر مخابرات هم هیچ نقشی ندارد. به نظر من این توجیه مدیران ما است. سیستم سیبا، سیستم سپهر، سیستم مهر و به طور کلی تمام سیستم‌های جاری از ماهواره استفاده می‌کنند و طبق ادعای شرکت خدمات، 99/7 درصد ضریب دسترس ماهواره یشان است. یعنی 3 دهم درصد در سال قطعی داشته اند. ما عموما یاد گرفته ایم که بگوییم دیگری مشکل دارد. درست است که مخابرات خوب نداریم، اما این که هر مشکلی را به مخابرات ارتباط بدهیم، این را من قبول ندارم. من از مخالف‌های جدی این بحث هستم. مخابرات ما خوب نیست، ولی هر مشکلی هم که داریم، مربوط به مخابرات نیست.

بحث فرهنگ سازی پرداخت الکترونیکی در ایران هنوز جا نیفتاده است. به نظر شما وظیفه ی چه کسی است که روی این مقولات فرهنگ سازی کند؟ دولت، بانک‌ها یا بخش خصوصی؟

خوشبختانه پس از این کنفرانس پول الکترونیکی که به همت شورای عالی اطلاع رسانی برگزار شد، یک محمل خیلی خوبی را برای توسعه در تمام زمینه‌ها ایجاد کرد بعد از آن کنفرانس جلسه ای که با حضور رییس جمهور، مدیر عاملان بانک‌ها و وزارت فناوری اطلاعات و دارایی و همه ی اجزای درگیر برگزار شد، بر طبق آن، کمیته ی پیگیری شکل گرفت که جلسات آن تشکیل می‌شود. همه ی این اجزا دارند شناسایی می‌شوند و برای تک تک آنها برنامه ریزی می‌شود. در بحث فرهنگ سازی، روابط عمومی‌تمام بانک‌ها فعال شده اند. حتی بودجه اش را هم شورای عالی اطلاع رسانی قبول کرده که یک سری فرهنگ سازی عمومی‌توسط بانک‌ها صورت گیرد. برای بحث بیمه پیشنهاد شده است که دولت تضمین بیمه را بر عهده بگیرد. حتی بودجه اش را هم شورای عالی اطلاع رسانی قبول کرد که یک سری فرهنگ سازی عمومی‌توسط بانک‌ها صورت گیرد. برای بحث بیمه پیشنهاد شده است

که دولت تضمین بیمه را به عهده بگیرد. برای تجهیزات خود پرداز بانک‌ها تشویق شده اند تا سال آینده 21 هزار دستگاه خود پرداز نصب نمایند. تعداد کارت‌ها قرار است تا سال آینده طبق برنامه ریزی 2 برابر بشود این کمیته، وظیفه ی برنامه ریزی و پیگری اقدامات اجزای درگیر در اجرای این عملیات را بر عهده دارد. من فکر می‌کنم اولین نتایج این حرکت، ظرف دو سه ماه آینده خودش را نشان بدهد و تا آخر امسال و اوایل سال آینده بتوانیم وضعیت خوبی داشته باشیم.

چنانچه نکته دیگری هست بفرمایید

ما چون نمی‌توانیم در ایران شرکت‌های معتبر صدور و استاندارد سازی کارت داشته باشیم، باید یک کسی متولی باشد. دو تا سناریو داریم، یکی این که یک شرکت خصوصی مثل ویزا که متعلق به بانک‌ها باشد این کار را بکند. سناریوی دیگر این که بانک مرکزی این کار را انجام بدهد که خوشبختانه بانک مرکزی این مسوولیت را پذیرفته و امیدوار هستم که این حرکت را بتواند در زمان خیلی خوبی اجرا کند. از جمله وظایف بانک مرکزی این است که وحدت رویه را برای بانک‌ها ایجاد نماید. الان در ایران حرکت‌های گوشه و کناری انجام شده که جواب گو نیستند و نمی‌توانند موفق باشند یکی بحث کارت سوخته است، یکی بحث کارت مترو است، پارکومتر، کارت اتوبوس. ببینید برای همه ی اینها تبلیغ شده، اما هیچ کدام از این پروژه‌ها موفق نیستند، مگر اینکه بانک مرکزی یک باید کارت هوشمند استانداردی برای پرداخت پول خرد با یک شناسه ی کاربردی (Applivation ID) ثابت که همه ی بانک‌ها بتوانند این کارت را برای مشتریانشان صادر کند این کارت به عنوان کیف پول الکترونیکی و به جای حمل پول خرد مورد استفاده قرار می‌گیرد. به طوری که در مترو، در پارکومتر، در پمپ بنزین و ... بتوان از آن برای پرداخت استفاده نمود. بانک مرکزی خوشبختانه این نقش را شروع کرده و اگر بتواند ظرف چند ماه آینده این استاندارد را اعلام کند و اجازه ی صدور این

کارت را به بانک‌ها بدهد، فکر می‌کنم یک حرکت سریع وخوبی انجام خواهد شد. به جای ایـن کـه کارت مترو یک کارت اتوبوس، یک کار ت تلفن و ....، به مردم بدهیم، باید یک کارت به عنوان کارت هوشمند پرداخت پول خرد به مردم داده شود با داشتن این کارت، مشکل پرداخت همه ی سازمان‌ها می‌تواند به راحتی حل شود. پیشنهاد این است که این کارت رمز نداشته باشد. می‌شود تعریف کرد که قابل شارژ باشد یا نباشد، چون رمز ندارد و اگر کسی کیف شما را بزند، نمی‌توانید شکایت کنید کـه شماره ی سریال این پول ما ل من بوده کارت گم شده و هر کس می‌تواند از آن استفاده کنـد ایـن کارت که سقفش مثلا 10 یا 20 هزار تومان است، به جای پول خرد در دست مردم هست. دیگر لازم نیست که هر بانک یک R&D داشته باشد. ما خیلی امیدواریم که بانک مرکزی این حرکـت را بـه سرعت به یک نقطه ای برساند که به یک محصول تبدیل شود. به جای این که راه رفته ی همـه ی کشورها را طی کنیم، می‌توانیم با یک حرکت شش ماهه یا یک ساله، ببینیم که یک کارت پرداخت داریم و می‌توانیم با امنیت و خیال راحت خدماتمان را دریافت نماییم. ما امیدواریم که به زودی یک کارت اعتباری (Credit Card)، کارت پول و کارت پول خرد استاندارد ملی داشته باشیم. الان رایان کارت، ثمین کارت، کارت هوشمند بانک ملت، بانک کشاورزی و ... هر کدام یک الگوی خاصی دارند. امیدواریم که اراده ی عمومی‌و اراده ی ملی برای این عملیات تقویت شود و بتواند به نقطه ی مثبتی برسد. ما خیلی امیدواریم زودتر مردم ما از این خدمت استفاده کنند.

سیاستنامه تجارت الکترونیکی، بانک مرکزی جمهوری اسلامی‌ایران را موظف کرده بود که تا پایان سال گذشته بانکداری الکترونیکی را به صورت کامل راه اندازی کند ولی تا کنون بانکداری الکترونیکی راه اندازی نشده است، همین امر موجب نارضایتی وزارت بازرگانی از بانک مرکزی شده و بارها مسئولان این وزارتخانه یکی از دلایل محقق نشدن چرخه کامل تجارت الکترونیکی را تاخیر در اجرای پروژه‌های بانکداری الکترونیکی عنوان کرده اند با وجود الزام بانک مرکزی بر راه اندازی بانکداری الکترونیکی تا پایان سال 83، چرا پدر خوانده، بانک‌ها به وعده خود عمل نکرده است؟

اول اینکه ما در جایی وعده نداده ایم: اگر شما درجایی وعده ای از طرف بانک مرکزی سراغ دارید به من هم بگویید تا در جریان قرار بگیرم. دوم اینکه بعضی از مسائل دستوری نیست، زمان می‌خواهد. زیر ساخت می‌خواهد نیازمند امکانات، وقت، آموزش، تربیت نیروی انسانی، تغییر فرهنگ و ... است. اینها نیز مسائلی نیست که با یک دستور و یا یک جلسه ویا تصمیم 4 نفر محقق شود. مثل این است که شما در جایی بگویید تصمیم دارید ظرف 3 ماه تبدیل به بزرگ ترین کشور صنعتی دنیا شوید. این حرف خیلی قشنگ است ولی اجرایی شدن آن ساده نیست. اولین پارامتری که در بانکداری الکترونیکی دخیل است و شالوده بانکدار الکترونیکی به شمار می‌آید. سیستم ارتباطی است، یعنی شعب بانک‌ها باید بتوانند با یکدیگر متصل شوند و سیستم یکپارچه ای را تشکیل دهند. به عبارت دیگر اقصی نقاط کشور باید با یکدیگر مرتبط شوند، دیگر فقط مسئله بانک هم نیست. اگر شما بخواهید شعب مجازی راه اندازی کنید هر کسی باید بتواند از طریق یک سیستم ارتباطی مطمئن و پرسرعت از منزل و یا محل کار به مرکز یک بانک وصل باشد تا بتواند کارهای بانکی اش را انجام دهد.

هنوز هم که اینجا نشسته ایم، نمی‌توانیم بگوییم دیگر هیچ مشکل ارتباطی نداریم. هر چند در نمیه دوم سال 83 و نیمه اولی سال 84 زحمات زیادی توسط وزارت ICT کشیده شد تا این پورت‌ها وخطوطی که بانک‌ها می‌خواهند حتی الامکان در اختیارشان قرار دهند ولی هم اکنون نیز اگر با بانک‌ها صحبت کنید، متوجه می‌شوید که نواقصی وجود دارد هنوز پوشش لازم داده نشده است. دوم اینکه بانکداری الکترونیکی یک سیستم و یک مجموعه است واین نیست که برویم یک کامپیوتر بخریم و به برق وصلش کنیم، آنگاه بگوییم حالا بانکداری الکترونیکی داریم مجموعه ای مانند مسائل فرهنگی، ارتباطی، تکنولوژیکی، ساختاری، سیستم‌ها و ... در این امر دخیل هستند، یعنی از یک طرف کل مشتری‌های بانک‌ها باید با این سیستم‌های جدید آشنای داشته باشند و از طرف دیگر بانک‌ها باید ساختارها و روش‌ها و .... را تغییر اساسی دهند تا با بانکداری الکترونیکی منطبق شوند و از طرف دیگر قوانین و مقررات کشور نیز با بانکداری الکترونیکی هماهنگ شود، سیستم قضایی کشور آشنایی کافی با این نوع بانکداری را پیدا کند و قوانین و مقررات لازم را در اختیار داشته باشد تا بتوانند با جرایم الکترونیکی مسائل الکترونیکی برخورد کند و در نهایت شبکه ارتباطی باید شبکه ارتباطی پر سرعت و قدرتمند و مطمئنی باشد و از امنیت لازم نیز برخوردار باشد.

چرا زمانی که سیاستنامه تجارت الکترونیکی تدوین می‌شد، بانک مرکزی به عنوان مجری بانکداری الکترونیکی باید پیش بینی‌های لازم را انجام می‌داد...

در تدوین سیاستنامه تجارت الکترونیکی هیچ نقش و دخالتی نداشتیم، عده ای نشسته بودند در مورد تجارت الکترونیکی مسائلی را مطرح کرده بودند، آن هم روی کاغذ مسائل روی کاغذ خیلی راحت است ولی اینکه آن مسائل به مرحله اجرا در آید، کار چندان ساده ای نیست.

همان بخشی هم که در ارتباط با بانکداری نیست هنوز به مرحله اجرا در نیامده است.

سیاستنامه تجارت الکترونیکی به عنوان مکمل برنامه سوم توسعه تدوین شد تا برنامه‌هایی که برنامه سوم توسعه به آنها توجه نشده بود، مورد توجه بیشتر قرار گیرد.

نمی‌خواهم آن را نفی کنم، می‌خواهم بگویم تدوین سیاستنامه قدم مثبتی بوده که برداشته شده است ولی حتی پیشرفته ترین کشورهای دنیا اعلام نکرده اند که بانکداری الکترونیکی ما تکمیل شده است. همیشه فناوری در حال پیشرفت و تغییر است هر روز پدیده جدیدی می‌آید و تمامی‌فناوری باید در جهت تکاملی خود پیش برود. بانکداری الکترونیکی طی 2 یا 3 سال گذشته چنان رشدی کرده که طی 50 سال گذشته نداشته است، یعنی اگر تمام فعالیت‌هایی که از 50 سال پیش تا 4 سال قبل و بعد کارنامه 4 سال گذشته را در نظر بگیریم، متوجه می‌شویم که این کارنامه به مراتب درخشان تر و پر بار تر از کارنامه 50 سال قبل ما در زمینه مکانیزه کردن خدمات بانکی و بانکداری الکترونیکی است.

ولی به هیچ وجه نباید دلمان را خوش کنیم که کارمان تمام شده است. کاری که انجام داده ایم در قدم اول ایجاد یک سوئیچ ملی بود، بانک‌هایی که حتی شعبشان با یکدیگر در ارتباط نبودند را به صورت شبکه یکپارچه در آوریم. این بزرگ ترین گامی‌بود که تا پایان سال 83 برداشته و در سال 84 تقویت شد. سپس این سیستم گسترش پیدا کرد وعلاوه بر پیام‌های پایانه‌های فروش و حتی پایانه‌های اینترنتی را می‌گیرد. بنابراین امروز هر بانکی هر تعداد دستگاه خود پرداز خود را و یا تعداد پایانه‌های فروش را افزایش دهد و یا نسبت به توسعه وگسترش شعب مجازی خودش اقدام کند، سیستم سوئیچ ملی ما و یا شتاب این امکان را دارد که بتواند تمام این پیام‌ها را بپذیرد و سیستم تسویه را بین بانک‌ها انجام دهد یعنی هم اکنون این مرکزیت در بانک مرکزی ایجاد شده است.

قبل از اینکه در دیگر فعالیتهای صورت گرفته از سوی بانک مرکزی بپردازد، می‌خواهم به سیستم تسویه حساب بین بانکی شتاب اشاره کنم: هر چند از طریق ATM تمامی‌بانک‌ها، با هر کارتی می‌توان پول برداشت کرد ولی امکان واریز وجه هنوز فراهم نشده است

مناقصه راه اندازی تسویه حساب بین بانکی برگزار شده و از بین چند شرکت، 2 شرکت برای عقد قرار داد انتخاب شده اند وهم اکنون شرکت ملی انفورماتیک در حال بررسی وضعیت این 2 شرکت است.

طبق قرار داد، شرکت منتخب با همکاری شرکت ملی انفورماتیک موظف است ظرف مدت 6 ماه سیستم RTGS را در کشور راه اندازی کند.

در این صورت می‌توان امیدوار بود که تا پایان سال، سیستم تسویه حساب بین بانکی به صورت کامل اجرایی شود؟

اگر مشکلی پیش نیاید، همینطور است.

چه زمانی نتیجه قطعی مناقصه اعلام خواهد شد؟

به زودی.

یکی دیگر از فعالیت‌های صورت گرفته از سوی بانک مرکزی، تلاش برای اتصال به شبکه بانکی جهانی است...

بله، همانطور است، یکی از قدم‌های مثبت بانک مرکزی طی چند سال گذشته که چندی پیش نتیجه داد، اتصال به شبکه بانکی بحرین مرکز مالی و بانکی کشورهای جنوبی حاشیه خلیج فارس به

شمار می‌آید از طریق بحرین در نظر داریم ظرف چند ماه آینده به سایر کشورهای حاشیه خلیج فارس نیز متصل شویم. از طرف دیگر مذاکره با شرکت China union pay برای اتصال به شبکه بانکی کشورهای آسیای شرقی در دستور کاری بانک کشورهای آسیای شرقی در دستور کاری بانک مرکزی قرار گرفته است شرکت china union pay هم اکنون با نصب 580 هزار خود پرداز در کشورهای آسیای دور مانند چین، کره، ماکائو، هنگ کنگ، تایلند، مالزی و در این اواخر اندونزی سوئیچ بانکی تمامی‌این کشورها را به یکدیگر متصل کرده است در صورت اتمام مذاکرات با این شرکت و رسیدن به توافق، سوئیچ شتاب به شرق دور نیز وصل خواهد شد.

چه زمانی اتصال شبکه بانکی ایران به چین قطعی خواهد شد؟

از نظر فنی می‌توان گفت که ظرف 3 ماه، شبکه بانکی ایران به شرق دور وصل خواهد شد ولی ابتدا باید مذاکرات به اتمام برسد و به یک توافق نهایی برسیم. امیدوارم که مذاکرات هر چه زودتر به نتیجه برسد.

اما اتصال به شبکه بحرین نزدک به دو سال طول کشید

اتصال سویئچ بانکی شتاب به بحرین اولین تجربه بود، حالا می‌توانیم با این تجزیه موفق با هر کشور دیگری وارد مذاکره شویم.

اتصال به شکبه بانکی بین المللی در مرحله اول اتصال به شبکه بانکی کشورهای حاشیه خلیج فارس به منظور ایجاد شرایط مناسب برای مسافران ایرانی به این کشورها و یا بالعکس در دستور کاری ایران قرار گرفت. فکر نمی‌کنید اگر کشور دیگری مانند عربستان سعودی و یا امارت که روابط گسترده تری با ایران دارند در دستور کاری بانک مرکزی قرار می‌گرفت، اهداف دولت ایران سریع تر محقق می‌شد؟

هنگامی‌که پیوستن به سوئیچ بانکی کشورهای حاشیه خلیج فارس در دستور کاری قرار گرفت، مذاکره را به طور همزمان با چند کشور آغاز کردیم ولی مذاکره با بحرین زودتر به نتیجه رسید.

آیا سایر کشورهای جنوبی خلیج فارس با اتصال سوئیچ ایران با سوئیچ بانکی کشورشان موافق هستند؟

تمامی‌این کشورها موافقت خود را اعلام کرده اند.

چرا اتصال به شبکه بانک‌های اروپایی در دستور کاری بانک مرکزی قرا ر نمی‌گیرد؟

با چند کشور اروپایی وارد مذاکره شده ایم که امیداواریم مذاکرات هر چه زودتر جواب دهد. باید توجه داشت که شرایط ایران به دلیل تحریم‌ها با شرایط سایر کشورها متفاوت است، اگر ما نیز مثل باقی کشورها بودیم با اتصال به یک سویئچ به سویئچ بین المللی وصل می‌شدیم.

شما در بخشی از صبحت تان به مشکلات ارتباطی بانک‌ها با یکدیگر اشاره کردید ولی اگر سراغ مخابرات برویم، می‌گوید پورت‌های ما آماده است، بانک‌ها، مشکلات فنی دارند و از این پورت‌ها استفاده نمی‌کنند، به نظر شما مشکل کجاست؟

مسئله ای که شما می‌گویید چرا ظرف 2 ماه این کار انجام نشد، پیچیدگی‌های خاص خودش را دارد و درست همین جا خودش را نشان می‌دهد. در یک جایی که بانک‌ها نیاز به خط دارند، مخابرات خط ندارد و در جایی که مخابرات خط دارد بانک‌ها نیاز به خط ندارند.

جلسات خیلی زیادی تشکیل شده و توانسته اند تا این مرحله کار پیش بیایند. کار پیچیده است در نظر داشته که هر کاری که بخواهیم انجام دهیم باید تجهیزاتش را از خارج وارد کنیم: این در حالی است که کشورهای سازنده تجهیزات نیز از زمان شروع اجرای پروژه بانکداری الکترونیکی تا زمانی که توانستند بگویند ما باکنداری الکترونیکی داریم، حدود 5 سال طول کشیده است. مشاور خارجی نیز

اعلام کرده است زمان لازم برای پیاده سازی سیستم‌های مورد نیاز بانکداری الکترونیکی، حدود 5 سال است البته اگر همه چیز خوب پیش برود و مشکلی پیش نیاید.

زمان پایه چه سالی است؟

ما از سال 80 راه اندازی سیستم‌های فرعی را آغاز کردیم ولی نصب وراه اندازی سیستم‌های اصلی را می‌خواهیم از نیمه دوم سال 84 آغاز کنیم.

در شرایطی فعلی، شما وضعیت بانکداری الکترونیکی را چگونه می‌بینید؟

مشکلات ساختاری داریم که باید حل شود: یکی از این مشکلات این است که تعداد دستگاه‌های خود پرداز به تعداد جمعیت خیلی کم است در کشور ما به ازای هر یک میلیون نفر، 49 دستگاه خود پرداز وجود دارد: در حالی که در کشورهای پیشرفته دنیا علی رغم اینکه از پول کمتر استفاده می‌کنند به ازای هر یک میلیون نفر، هزار دستگاه خود پرداز وجود دارد. حال این وضع به مراتب در مورد دستگاه‌های پایانه‌های فروش بدتر است. نسبت ما به دنیا، نسبت خیلی ضعیفی است، بنابراین باید به سرعت دستگاه‌های خود پرداز و پایانه‌های فروش را افزایش دهیم. یکی دیگر از مشکلات ساختاری ما کوچک بودن اسکناس‌هایمان است به طور مثال بزرگ ترین ارزش پولمان 2 هزار تومان است خوب اگر تعدادی مردم از دستگاه‌های خود پرداز پول بگیرند، پول خود پرداز تمام می‌شود و مرتب باید پول جدید در این دستگاه قرار داد، حال اگر رقم اسکناس‌های ما مثل بقیه جاهای دنیا درشت تر شود، این مشکل رفع می‌شود و یک فرد با یک بار مراجعه به بانک می‌تواند نیاز چند روزشان را بر طرف کند. از طرف دیگر مردم ما هنوز عادت دارند که از پول نقد استفاده کنند، فروشگاه‌ها نیز پول نقد بگیرند و برایشان خیلی سخت است که به جای پول نقد از کارت پلاستیکی استفاده کنند، بالاخره فرهنگ سازی لازم است.

به پول پلاستیکی اشاره کردید یاد دستور العمل پول الکترونیکی افتادم طبق آن دستور العمل قرار بر این شده بود که اواخر خرداد 84 پول الکترونیکی در کشور اجرایی شود

هم اکنون پول الکترونیکی حالت اجرایی به خود گرفته است.

در شرایط فعلی پس از جلسات مرتب فقط یک دستور العمل کاربرد پـول الکترونیکـی صادر شده است؟

نه این طور نیست شما اگر به تعداد تراکنش‌های توجه کنید، متوجه این امر خواهید شد تعداد تراکنش‌های انجام شده از طریق شبکه شتاب در سال 81 و 360 هزار تراکنش بوده است در حـالی که این رقم در پایان سال 83 به 385 میلیون رسید و پیش بینی می‌شود تا پایان سال 84 به بالاتر از 500 میلیون تراکنش برسد و میزان رشد غیر قابل تصور است.

هم اکنون شرایطی فراهم شده است که مردم کارت‌های نقدی، کارت‌هـای اعتبـاری و کارت‌های پیش پرداخت را می‌شناسند ولی هنوز واژه پول الکترونیکی نه تنها برای مردم نا آشنا است بلکه کارشناسان بانکی نیز به یک تعریف واحد برای آن نرسیده انـد. عـده ای کارت‌های بانکی را پول الکترونیکی به شمار می‌آورند وعده ای دیگر خصوصیات پول را برای پول الکترونیکی قائل هستند. تعریف بانک مرکزی برای پول الکترونیکی چیست و بالاخره پول الکترونیکی در کدام قالب جا می‌گیرد؟

اصولا وقتی جابه جای پول به صورت فیزیکی صورت می‌گیرد به آن می‌گویند پول کاغذی، ولی وقتی جابه جایی به صورت الکترونیکی صورت می‌گیرد به آن پول الکترونیکی می‌گوییم: یعنی اینکه اگر شما بتوانید پولی را از حسابی در یک بانک به حساب دیگر در بانک دیگر منتقل کنید بدون اینکه

به صورت فیزیکی کار صورت گیرد و یا کارمندی در آن دخالت داشته باشد، پول الکترونیکی می‌گوییم بعضی وقت‌ها ممکن است پول کاغذی و الکترونیکی باهم مخلوط شوند و شما یک کاری را که انجام می‌دهید از هر دوی آنها استفاده کنید مانند دریافت و پرداخت پول از دستگاه‌های خود پرداز.

در حال حاضر بیشتر روش سنتی در کشور مورد استفاده قرار می‌گیرد؟

اگر کل نقل و انتقال‌های پولی را در نظر بگیریم، در بعد داخلی روش سنتی و در بعد بین المللی روش الکترونیکی به کار می‌رود یعنی نقل وانتقال پولی ما به خارج از کشور به طور عمده الکترونیکی است و از طریق سوئیفت انجام می‌شود و در داخل کشور به صورت فیزیکی و دستی است و باید به مرور این بخش را به سوی الکترونیکی سوق دهیم.

فرق بانکداری سنتی و الکترونیکی چیست؟

در بانکداری سنتی مشتری با دو محدودیت عمده مواجه است: یکی محدودیت زمانی و دیگری محدودیت مکانی ولی بانکداری الکترونیکی این 2 محدودیت را از جلوی پای مشتری بر می‌دارد یعنی شما در هر ساعتی از شبانه روز و در هر روز هفته می‌توانید کار بانکی خود را در محیط کار یا منزل یا حتی به وسیله تلفن همراه انجام دهید.

با طرح این سوال می‌خواستم به اینجا برسم که آیا بانک‌ها ساز و کار فعالیت 24 ساعته را دارند.

یکی از مشکلات همین جا است. اگر قرار شد شما 24 ساعته به مشتری‌ها سرویس بدهید باید شیفتی در بانک داشته باشید که پشتیبان سیستم باشد: در حقیقت باید سیستم پشتیبانی و مانیتورینگ 24 ساعته داشته باشیم وعملیات بانکداری الکترونیکی در هر بانک به طور 24 ساعته و موثر پشتیبانی شود و قتی دیدند که یک دستگاه کار نمی‌کند، بلافاصله مشکل دستگاه را حل و باید

کاری انجام دهند که مردم شبانه روز از این سیستم استفاده کنند. هنوز این قضیه در بعضی از بانک‌ها جا نیفتاده است کارمندان بعد از وقت اداری هنگامیکه بانک را تعطیل می‌کنند، دیگر می‌روند به امید خدا، حالا اگر دستگاه ATM پولش تمام شد، دیگر تمام شده است یا اگر سیستم‌های الکترونیکی با مشکلی روبه رو شد از پشتیبانی 24 ساعته و موثر برخوردار نیستند.

یکی از مشکلاتی که بانکداری الکترونیکی با آن مواجه است، هماهنگ نبودن PSPها با بانک‌ها است. هم اکنون موافقت اصولی 10، PSP صادر شده است ولی بسیاری از آنـان از دستور العمل‌های صادر شده از سوی بانک مرکزی گلایه دارند و آنها را غیر شفاف می‌دانند و عده ای بازار را غیر شفاف می‌دانند، به نظر مشکل PSPها کجاست؟

فکر می‌کنم همان مشکل دومی‌است، دستور العمل‌های بانک مرکزی کاملا شفاف است و تا کنون هیچ کدام از شرکت‌های ارائه دهنده خدمات نیامده اند بگویند من اینجا ابهام دارم، اگر بگویند سریع ابهام را رفع می‌کنیم ولی مشکل اینجاست که خود بانک‌ها با PSP رقابت می‌کنند. در حقیقت هـر بانکی خود شرکتی درست کرده با عنوان PSP و چون از ابتدا به دلایل امنیتی اعلام کردیم که PSP باید به بانک‌ها متصل و بانک‌ها به شتاب وصل شوند، وقتی PSP می‌خواهد بـه بانـک وصـل شـود، بانک‌ها تحویلشان نمی‌گیرند چون بانک‌ها خود شرکتی راه اندازی کرده اند که از طریق آن خـدمات خود را انجام می‌دهند و از طرف دیگر هم بانک‌هـا یـا انگیزه‌هـای لازم را ندارنـد و یـا از تـوان لازم برخوردار نیستند تا به آن سرعتی که ما درنظر داریم شبکه پایانه‌های فروش را گسترش دهنـد، بـه ناچار باید از PSPها استفاده کنیم. از همین رو احتمال دارد و در آینده نزدیک تصمیم بگیـریم بـه PSPها مجوز دهیم تا بتوانند مستقیما به بانک مرکزی و شتاب وصل شوند.

در این صورت می‌توان به گسترش پایانه‌های فروش امیدوار بود.

بحثی که شما در ابتدای صحبت در مورد تجارت الکترونیکی مطرح کردید. به همین جا بر می‌گردد. باید بتوانیم تمامی‌واحدهای صنفی را به POS مجهز کنیم. امیدوارم که دستگاه‌های مسئول مانند وزرات بازرگانی هر چه زودتر واحدهای صنفی را مکلف به نصب POS کند .

وزارت بازرگانی این کار را کرده و قرار شده است تمامی‌واحدهای صنفی ظرف 5 سال به پایانه‌های مکانیزه فروش مجهز شوند...

چه طور برای نصب PCS یک زمان 5 ساله تعیین می‌کنند ولی برای بانک مرکزی زمان سه ماهه در نظر می‌گیرند؟ نصب POS که خیلی راحت تر است تا تغییرات فراگیر یک سیستم بانکی با تمام ابعاد حقوقی، ساختاری، انسانی، آموزشی، فناوری و فرهنگی آن.