ارائهٔ خدمات به مردم بااستفاده از فناوری اطلاعات

هدف اصلی تحقق دولت الکترونیک ارائهٔ خدمات مؤثر و کارامد به شهروندان با استفاده از فناوری اطلاعات و ارتباطات است؛ به گونه‌ای که دولت، بیشتر و بهتر پاسخگوی نیازهای شهروندان باشد. از مزایای استفاده از فناوری اطلاعات در تعامل مردم و دولت می‌توان موارد در پی آمده را نام برد :

۱. قابلیت ارائه خدمات در تمام اوقات شبانه‌روز؛

۲. عدم نیاز به مراجعهٔ حضوری برای دریافت خدمات؛

۳. ارائه خدمات سریع و مطمئن.

برای موفقیت دولت الکترونیک به چند تحول اساسی در طرز تفکر سیستم دولتی نیاز است که مهمترین آنها به شرح در پی آمده است :

۱. جایگزینی دولت شهروند ـ محور و باز به جای دولت دیوان ـ محور

به طور سنتی دولت به جای مردم تصمیم می‌گیرد، اما در دولت نوین با ارائهٔ اطلاعات و مهارتها، شهروندان قادر خواهند بود که خودشان دست به انتخاب بزنند.

علاوه بر این به جای آنکه لازم باشد مردم برای امور مختلف به دولت مراجعه کنند، با ارائهٔ خدمات همزمان (online)، این دولت است که به مردم مراجعه می‌کند.

۲. پاسخگویی و شفافیت بیشتر به جای تصمیم‌گیری‌های غیرشفاف

قوانین، سیاستها و اجرای آنها مورد نظارت دقیقتری قرار می‌گیرد و اصلاحات آنها سریعتر اعمال می‌شود.

۳. سیاستگذاری بر اساس واقعیتها و تحلیل داده‌ها

سیاستگذاری‌ها بر پایهٔ آمار و اطلاعات از شهروندان و صاحبان مشاغل انجام می‌شود.

۴. نقش دولت از حالت دستوری به شکل پیشنهادی با تمرکز بر شکل‌دهی محیط تغییر می‌کند؛ به گونه‌ای که افراد قادر باشند بهترین تصمیم را خودشان اتخاذ کنند.

به طور کلی تعامل بین دولت و مردم بیشتر توسط خود مردم به پیش برده می‌شود. دولت به تنهایی خدمات را ارائه نمی‌کند، بلکه از همکاری شهروندان و صاحبان مشاغل برخوردار خواهد بود. مدیریت دولتی از حالت بالا به پایین متحول خواهد شد و بیشتر افراد دانشور[1] تصمیمهای مستقل مبتنی بر اطلاعات خواهند گرفت، بهبود کارایی، باعث کوچکتر شدن دولت شده و این به نوبه خود باعث آزاد شدن نیروی انسانی و اشتغال در بخش فناوری اطلاعات می‌شود. به این ترتیب پاسخگویی، شفافیت و بهره‌وری دولت به نحو چشمگیری افزایش خواهد یافت.

تغییرات ایجاد شده شامل حال دو گروه می‌شود:

۱. شهروندان و صاحبان مشاغل؛

۲. دولت و کارکنان آن.

۱. تغییرات مربوط به شهروندان و صاحبان مشاغل

تمام شهروندان دسترسی بهتری به خدمات خواهند داشت و طیف خدمات ارائه شده متناسب با نیازها گسترش خواهد یافت.

1. Knowledge-workers

آ) دسترسی بهتر به خدمات

خدمات در جایی ارائه خواهد شد که مردم هستند و نه در جایی که دولت است. به عنوان مثال برای تجدید گذرنامه به جای رفتن به اداره‌های دولتی و ایستادن در صفهای طولانی می‌توان در خانه از طریق رایانه شخصی (PC) یا کیوسک دولت الکترونیک در یک مجتمع اداری این کار را انجام داد. علاوه بر خدمات ارائه شده از طریق رایانهٔ شخصی و اینترنت، خدمات به تدریج از طریق تلفن نیز در دسترس خواهد بود.

ب) کیفیت بهتر خدمات

به دوباره‌کاری و پرکردن فرمهای مختلف نیازی نخواهد بود و خدمات، قابل اعتمادتر می‌شوند. به عنوان مثال چنانچه نشانی کسی تغییر کند با یک بار ارائهٔ آن می‌توان مطمئن بود که تمام اداره‌های دولتی از آن اطلاع دارند.

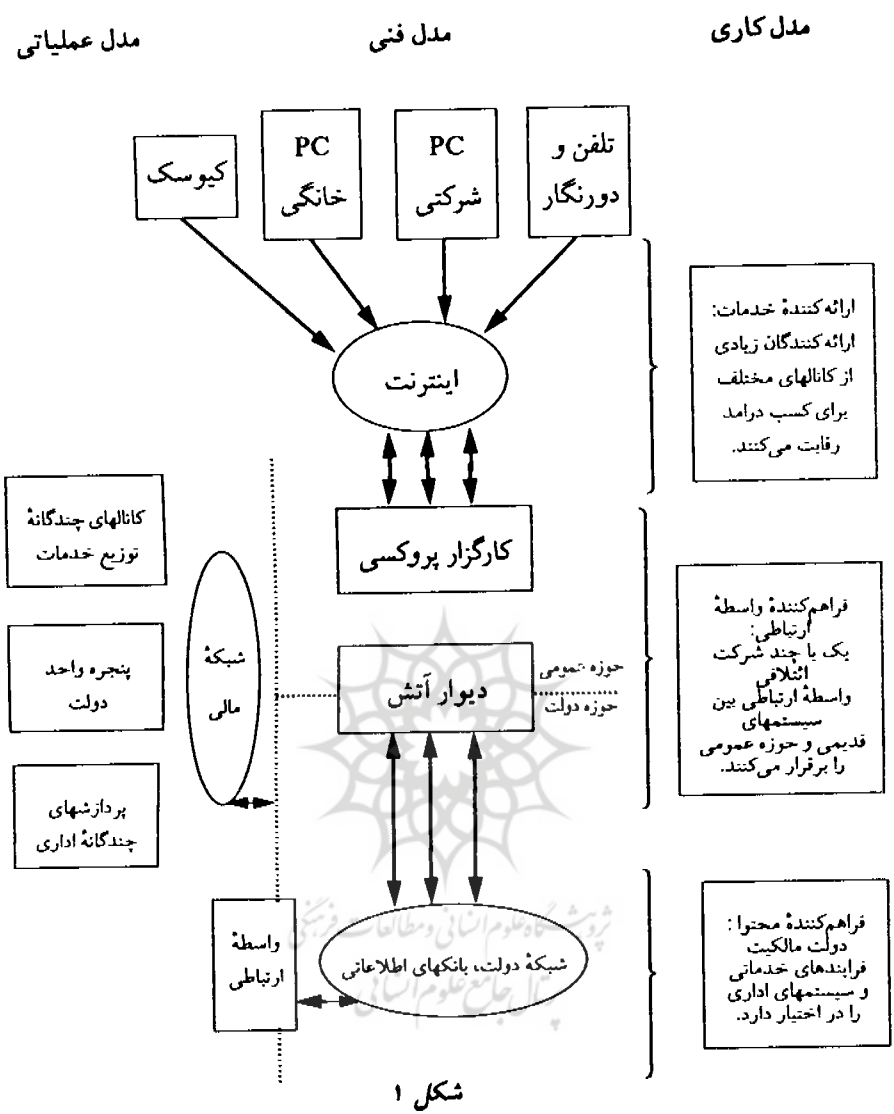
نکته‌های مربوط به محرمانه بودن و امنیت نیز مورد توجه قرار دارند. دولت، مالکیت تمام داده‌ها را برای خود محفوظ می‌دارد و دسترسی به آنها را به دقت کنترل کرده و هرگونه نقض قوانین را طبق قانون مجازات می‌کند.

ج) ارائهٔ خدمات نوین

علاوه بر بهبود خدماتی که قبلاً نیز ارائه می‌شد، فرصتهایی برای ارائهٔ خدمات نوین نیز به وجود می‌آید. دامنهٔ خدمات نوین فقط با هزینهٔ آنها محدود می‌شود.

د) روش نوین ارائهٔ خدمات

برای دستیابی به روشهای بهتر ارائهٔ خدمات باید این روشها مورد باز مهندسی قرار گیرد. مدل جدید ارائهٔ خدمات دولتی در شکل ۱ نشان داده شده است.



شکل ۱

در مدل سنتی، دولت هر دو نقش فراهم کننده و ارائه کننده را به عهده دارد. در مدل جدید سه نقش مجزا برای ارائهٔ خدمات در نظر گرفته شده است :

۱) فراهم‌کننده خدمات[1] ۲) فراهم‌کننده واسطهٔ ارتباطی[2] ۳) ارائه‌کننده خدمات.[3]

در این مدل دولت نقش فراهم کننده خدمات را به عهده دارد که مسئول ایجاد خدمات برای شهروندان و اطمینان از کیفیت آنهاست.

نقش فراهم‌کننده واسطهٔ ارتباطی، برقراری پیوند بین سیستمها و فرایندهای دولت و یک شبکهٔ عمومی است. این شبکه، تنها پنجره‌ای است که از طریق آن شهروندان و صاحبان مشاغل با تمام خدمات دولتی داخل و خارج کشور ارتباط می‌یابند. مردم قادر خواهند بود از طریق کیوسک‌های عمومی، رایانهٔ شخصی (PC)، تلفن یا تلویزیون با دولت ارتباط برقرار کنند.

دولت، اهداف و قوانین پایه را تدوین خواهد کرد و چگونگی ارائهٔ خدمات به عهده خود ارائه کنندگان خواهد بود. مدل جدید ارائهٔ خدمات به دولت اجازه می‌دهد که سیستمها و فرایندهای موجود را با سیستمهای جدید یکپارچه کند. اگر دولت بتواند مستقل از ارائه‌دهندگان خدمات کار کند، می‌توان بدون انتظار برای جایگزینی سیستمهای قدیمی، خدمات را فراهم کرد. علاوه بر این با ایجاد رقابت بین ارائه‌کنندگان خدمات برای ارائهٔ خدمات بهتر با قیمت ارزانتر، کارایی نیز افزایش می‌یابد.

۲. تغییرات ایجاد شده در دولت

دولت الکترونیک در مورد افزایش بهره‌وری عملیات داخلی دولت نیز مسؤول است. عملکرد دولت با استفاده از فرایندها و سیستمهای بهتر، بهبود خواهد یافت. این کاربردها با تغییرات ایجاد شده در راهبرد، مهارتها، سیستمها و ساختار و فرهنگ دولت پشتیبانی می‌شوند.

الف) تغییر در راهبردها

راهبردها به گونه‌ای تغییر می‌کنند و توسعه می‌یابند که نیازهای شهروندان و مشاغل

---

1. Service supplier
2. Gateway provider
3. Service provider

را به عنوان مراجعان اداره‌های دولتی برآورده کنند. در واقع سازمانهای دولتی باید در مورد چگونگی دسترسی مراجعان به خدمات، به طور جدیتر بیاندیشند و با ارائه کنندگان خدمات، همکاری کنند.

ب) افزایش مهارتها

کارمندان دولت باید به افرادی دانشور تبدیل شوند و مهارت آنها افزایش یابد. تمام کارکنان باید برنامهٔ مقدماتی آموزش فناوری اطلاعات (IT) را طی کنند و سپس درباره فناوری مربوط به شغلشان آموزش ببینند. تمام وزارتخانه‌ها و سایر بخشها باید درباره برنامه و راهبردهایشان، آموزشهایی ارائه دهند.

ج) سیستمها و فرایندها

سیستمها و فرایندها وارد عصری می‌شوند که بین تمام اداره‌ها و وزارتخانه‌ها در کل کشور و جهان ارتباط برقرار است. یک بانک اطلاعاتی مشترک واحد، عامل اساسی موفقیت دولت الکترونیک است. اطلاعات دولتی در اختیار کسانی که حق استفاده از آن را داشته باشند قرار می‌گیرد. بعضی اطلاعات باید توسط سیستمهای با امنیت زیاد و فناوری رمزنگاری، محافظت شوند. اطلاعات شخصی شهروندان کاملاً محرمانه است.

ایجاد ارتباط بین سیستمهای قدیمی و جدید نیز یکی از چالشهای تحقق دولت الکترونیک است.

د) ساختار

به تدریج که بهره‌وری کارکنان دولت بالا می‌رود و با سیستمها و فرایندهای بهتری پشتیبانی می‌شوند، ساختار دولت نیز تغییر خواهد کرد. یک دولت کوچک با لایه‌های کمتر، از عهده چالشهای آینده بهتر بر می‌آید و پاسخگوتر خواهد بود. پیش‌بینی می‌شود که ساختارهای تیمی و گروهی، جایگزین سلسله مراتب سنتی در اداره‌ها شود.

هـ) فرهنگ

پایهٔ تغییرات ایجاد شده در دولت، تغییر فرهنگ دولت است. دولت به سوی «شهروند ـ محوری» حرکت خواهد کرد و فرایندهای رسمی، اهمیت کمتری پیدا

می‌کنند و در مقابل، ارائهٔ خدمات به شهروندان، از اهمیت بیشتری برخوردار خواهد شد. اساسیترین تغییری که روی خواهد داد این است که کارمندان خود را به قوانین و فرایندهای متداول محدود نکنند، بلکه خود را با هدف ارائهٔ خدمات بهتر به مردم مجهز کنند. به طور کلی فرهنگ محصول‌گرایی و عملکردگرایی، حاکم خواهد شد.

برای ارائهٔ خدمات به صورت همزمان (online) لازم است یک جایگاه اینترنتی ایجاد شود که شهروندان و صاحبان مشاغل بتوانند کلیهٔ امور مرتبط با دولت را از طریق آن انجام دهند. این جایگاه اینترنتی «پورتال» نام دارد. هر چند که پورتال ظاهراً شبیه یک وب سایت است، اما بسیار پیچیده‌تر از یک وب سایت معمولی است و دارای ارتباطهای لازم با اداره‌های مختلف دولتی است. شهروندان برای انجام امور خود فقط با پورتال سر و کار خواهند داشت و با عملیات پشت صحنه کاری ندارند.

یکی از نکات مهم در ارائهٔ خدمات به شهروندان، احراز هویت متقاضیان دریافت خدمات است. در روش سنتی، اشخاص با مراجعهٔ حضوری و ارائهٔ مدارک شناسایی، هویت خود را ثابت می‌کنند. برای انجام امور به صورت الکترونیک لازم است احراز هویت نیز به صورت الکترونیک انجام گیرد. امضای دیجیتال، یکی از مهمترین راههای احراز هویت الکترونیک است.

در ادامهٔ مقاله، نظر به اهمیت پورتال و امضای دیجیتال، این گونه مباحث به طور مفصلتر توضیح داده خواهد شد.

۱. پورتال

از هدفهای اصلی دولت الکترونیک، سهولت ارتباط شهروندان با دولت و استفاده از فناوری اطلاعات برای انجام امور است. برای تحقق این هدف، پورتال به عنوان واسطهٔ بین شهروندان و دولت، نقش اساسی ایفا می‌کند.

در شیوه سنتی حکومت، شهروندان برای ارائهٔ درخواستهای خود و اخذ نتایج حاصله باید شخصاً و به صورت حضوری در ساعتهای مشخص به مراکز اداری مراجعه

کنند.

دولت الکترونیک، چشم‌انداز جدیدی برای کارمندان، صاحبان مشاغل و شهروندان ترسیم می‌کند. اتوماسیون اداره‌ها با رایانه‌ای کردن خدمات تا حد زیادی تحقق یافته است. استفاده از رایانه و یا ایجاد وب سایت، صرفاً به منظور اطلاع‌رسانی و بدون امکان انجام امور اداری، هدفهای دولت الکترونیک را تحقق نمی‌بخشد.

نخستین گامی که دولتها برای همزمان شدن (online) برمی‌دارند، راه‌اندازی صفحات وب ایستا بدون قابلیت تعامل است که می‌توان آنها را «بروشور» نامید. این سایتها را می‌توان با افزودن ویژگیهای تعاملی و پیوند به دیگر وب سایت‌ها بهبود بخشید، ولی در نهایت به صورت مخازن مجزای اطلاعات در می‌آیند.

در یک پورتال، کلیهٔ خدمات به صورت یکپارچه و مستقل از اینکه با کدام سازمان و اداره دولتی در ارتباط است ارائه می‌شود؛ به نحوی که شهروندان و صاحبان مشاغل فقط با مراجعه به آن می‌توانند کلیه اموری را که به دولت ارتباط پیدا می‌کند، انجام دهند.

اگر چه هر پورتال یک وب سایت است، ولی هر وب سایت یک پورتال نیست. گاهی چنین تصور می‌شود که پورتال چیزی بیش از یک وب سایت نیست، در حالی که وب سایت فقط لایهٔ بیرونی است که مردم از طریق آن ارتباط برقرار می‌کنند. عملیات یکپارچه و منسجمی که در پشت صحنه انجام می‌گیرد، عاملی است که امکان استفاده از پورتال را می‌دهد.

در واقع پورتال به عنوان واسطه‌ای بین کاربران و سازمانها و اداره‌های دولتی عمل می‌کند. یک فرایند اداری ممکن است به سازمانهای مختلفی ارتباط پیدا کند. در این صورت پورتال به صورت اتوماتیک و با استفاده از بانکهای اطلاعاتی اداره‌ها، عملیات را انجام می‌دهد و نتیجهٔ نهایی را بدون آنکه نیازی به مداخلهٔ کاربر در این فرایند باشد، در اختیار کاربر قرار می‌دهد. اصلیترین نقش پورتال به عنوان یک سایت قابل دسترس بودن است. تمام سازمانهای دولتی و خدمات مورد نیاز شهروندان، باید به صورت دسته‌بندی شده در این سایت ارائه شوند.

بعضی ویژگیهای اساسی یک پورتال عبارتند از :

۱. ارائهٔ خدمات احراز هویت مطمئن برای جلوگیری از تقلب؛

۲. امکان دسترسی به خدمات دولتی از مکانهای مختلف با استفاده از رایانهٔ شخصی (PC)، کیوسکها و...؛

۳. ارائهٔ خدمات یکپارچه و منسجم برای رفاه شهروندان و صاحبان مشاغل.

بخشهای اساسی یک پورتال عبارتند از :

۱. خدمات پورتال؛

۲. بخش بنیادی پورتال؛[1]

۳. ابزارهای یکپارچه‌سازی.[2]

۱. خدمات پورتال

یک لایهٔ نمایش اختصاصی و مشترک برای ارائهٔ تمام سیستمهای قدیمی به کار می‌رود. پنجره‌های هوشمند با امکانات مرور و وارد کردن داده‌ها، چارچوبی برای نمایش داده‌های قدیمی به وجود می‌آورند. کاربران با اشاره ماوس و کلیک کردن روی واسطه‌ها با تمام امکانات شبکه ارتباط برقرار می‌کنند. ابزارهای جستجو، دسته‌بندی و فهرست‌بندی اتوماتیک، داده‌ها را به صورت یکپارچه جمع‌آوری، سازماندهی و توزیع می‌کنند.

۲. بخش بنیادی پورتال

یک سیستم پیشرفته، دسترسی دائم و مطمئن به پورتال را تضمین می‌کند. این زیرساخت، پایه‌ای اساسی برای قابلیت اعتماد، مقیاس‌پذیری و خطاپذیری[3] سیستم می‌باشد.

۳. ابزارهای یکپارچه‌سازی

انتخاب فناوری مورد استفاده در پورتال باید از انتخاب بانکهای اطلاعاتی در

1. Portal Foundation
2. Integration tools
3. Fault-tolerance

بخشهای مختلف، مستقل باشد. زیرساخت ایجاد شده باید امکان حرکت از برنامه‌های قدیمی به سمت وب و تبادل اطلاعات بین برنامه‌های مختلف را بدهد.

یکپارچه‌سازی انتهایی، سیستمهای مختلف را به گونه‌ای ترکیب می‌کند که کارمندان و عموم مردم بدون نیاز به دانستن سازماندهی دولت، می‌توانند امور خود را انجام دهند.

استفاده‌کنندگان از خدمات پورتال را می‌توان به سه گروه تقسیم کرد :

۱. شهروندان؛

۲. صاحبان مشاغل؛

۳. دولت.

از جمله خدمات ارائه شده توسط پورتال عبارتند از :

ـ اسناد شخصی (گذرنامه، گواهینامهٔ رانندگی)؛

ـ گواهیها (گواهی تولد، گواهی ازدواج)؛

ـ مالیات؛

ـ تأمین اجتماعی؛

ـ ارتباط با پلیس؛

ـ تغییر نشانی؛

ـ ثبت وسیلهٔ نقلیه؛

ـ درخواست پروانهٔ ساختمان؛

ـ خدمات بهداشتی.

سازمانهای دولتی اغلب در وب سایت‌های خود اطلاعات بخشی خود را قرار داده‌اند، بدون آنکه به منظور دسترسی کاربران به اطلاعات، تمهیدی برای یکپارچه‌سازی انتهایی اندیشیده باشند. به همین دلیل بدون دانستن ساختار سازمان مورد نظر، اغلب دسترسی به اطلاعات مشکل است.

ویژگیهای پورتال

۱. ارائهٔ خدمات دولتی به صورت یکپارچه؛

۲. مدیریت محتوا[1] : صفحات وب ایستا و پویا و پیوندهای بین آنها؛

۳. مدیریت اسناد[2] : صفحات وب که اطلاعات موجود روی آنها به قوانین بستگی دارد و با تغییر قوانین نیز تغییر می‌کند؛

۴. سهولت استفاده از پورتال؛

۵. همکاری گروههای مختلف با یکدیگر از طریق ویدئو کنفرانس، پست الکترونیک و... که برخورد بین گروهها را کم می‌کند؛

۶. جامع بودن[3] : جمع‌آوری اطلاعات از منابع مختلف در یکجا و دسترسی به سیستمهای گوناگون از طریق پورتال؛

۷. جریان اسناد و امور اداری (Business Transport) : یک سند از بخشهای مختلف عبور می‌کند و در هر بخش، پردازش لازم روی آن صورت می‌گیرد. از این نظر پورتالها برای مدیریت اسناد، مفیدند؛

۸. ورود یک مرحله‌ای به سیستم[4] : با یک بار ورود به پورتال و احراز هویت برای ورود به سیستمهای دیگر، به احراز هویت نیازی نیست؛

۹. گزارش دقیق از رویدادهای سیستم به طوری که دقیقاً مشخص باشد که چه رویدادی در چه زمانی اتفاق افتاده است؛

۱۰. سیستم اعلان[5] : وقتی منتظر رویداد خاصی هستیم، سیستم به محض وقوع آن، ما را خبر می‌کند مثلاً از طریق پست الکترونیک یا پیام‌گیر یا تلفن و...؛

۱۱. دسته‌بندی اطلاعات و خدمات بویژه در مورد داده‌های ساختار نیافته و اطلاعاتی که در سندی خاص نیست و بین اسناد مختلف پخش شده است؛

---

1. Content Management
2. Document Management
3. Aggregation
4. Single sign on
5. Alert/Notification

۱۲. محتوا و خدمات پورتال باید مطابق نیاز کاربران تنظیم شود و نه ساختار سازمانی دولت؛

۱۳. سعی در جهت افزایش استفاده از پورتال و نظارت بر میزان استفاده از آن؛

۱۴. انتخاب نوع معینی از پورتال برای جلوگیری از دوباره کاری.

مراحل ایجاد پورتال

۱. پورتال اطلاع رسانی : ایجاد یک وب‌سایت اولیه به طوری که پایه‌ای برای طرحهای آینده باشد. می‌توان فرمهای دولتی را در این سایت قرار داد.

۲. ارائهٔ خدماتی که نیاز به امنیت بالایی ندارند و طراحی متمرکز برای ایجاد ارتباط مطابق هدفهای دولت از طریق پورتال.

۳. ارائهٔ کلیه خدمات به صورت همزمان (Online) به شهروندان، صاحبان مشاغل و کارمندان. الزامات امنیتی از طریق طرحهای پیشرو، مورد بررسی قرار می‌گیرند.

انواع پورتال

۱. پورتال عمومی[1]

الف) پورتال دولتی : تمام تعاملات بین اشخاص و صاحبان مشاغل با دولت و درون دولت از طریق آن انجام می‌گیرد.

ب) صنعتی : مانند پورتالهای مدیریت ساختمان، و پورتال آسانسور

ج) همگانی[2] : مانند سایتهای MSN و Yahoo

۲. پورتالهای حرفه‌ای[3]

الف) پورتال تجاری[4] : حقوق و دستمزد و پخش کالا

ب) پورتال افقی : اتصال افقی پورتالها

1. Public portal
2. General
3. Enterprise portal
4. Business area portal

۳. پورتالهای شخصی (مانند تلفن همراه)

در این حالت سیستم می‌فهمد که از چه وسیله‌ای استفاده می‌شود و بر اساس آن اطلاعات را در قالب مناسب ارسال می‌کند.

مزایای پورتال

۱. کاهش هزینهٔ کل مالکیت (TCO)[1] : هستهٔ سیستم دست نخورده باقی می‌ماند، ولی بخشهای مختلف را می‌توان برای استفاده از فناوریهای جدید تغییر داد؛

۲. استفاده بهینه از زیر ساخت‌های فناوری اطلاعات (IT) : فناوری اطلاعات از دههٔ ۶۰ میلادی وارد شده است، ولی استفاده بهینه از آن از سالهای ۹۶-۹۵ آغاز شده است؛

۳. قابلیت استفاده همزمان از فناوریهای مختلف : نیاز به حذف سیستمهای قدیمی نیست، بلکه فقط واسطه[2] تغییر می‌کند؛

۴. مقیاس‌پذیری : امکان افزایش یا کاهش حجم دسترسی؛

۵. قدرت ارائهٔ راه‌حل‌های مناسب در مدت کم.

۲. امضای دیجیتال

استفاده گسترده از تعاملات الکترونیک، مستلزم احراز هویت[3] استفاده‌کنندگان از سیستمهای مبتنی بر فناوری اطلاعات بویژه سیستمهای مرتبط با دولت الکترونیک (تعامل شهروندان با دولت) است.

یکی از راههای احراز هویت الکترونیک، امضای دیجیتال است. روشهای الکترونیک دیگر از جمله زیست‌سنجی[4] یا کارتهای هوشمند[5] برای احراز هویت وجود دارند. ولی این روشها به سخت‌افزار ویژه خود نیاز دارند و نمی‌توان آنها را به طور

---

1. Total cost of ownership
2. Interface
3. Authentication
4. Biometrics
5. Smart Cards

عمومی به کار برد. مزیت امضای دیجیتال آن است که روشی کاملاً نرم‌افزاری است و نیاز به سخت‌افزار ویژه ندارد. امضای دیجیتال در واقع روشی برای اثبات هویت ارائه می‌کند.

امضای دستی نیز روشی برای احراز هویت است. به این معنی که هم هویت فرد امضاکننده مشخص می‌شود و هم فرد امضاکننده اذعان می‌کند که امضا متعلق به اوست. برای جلوگیری از امور تقلبی نظیر جعل یا انکار امضا همان طور که مرسوم است با مراجعه به دفاتر اسناد رسمی «گواهی امضا» اخذ می‌شود. در این روش دفاتر اسناد رسمی به عنوان مرجعی امین با ملاحظهٔ مدارک هویت شخص امضاکننده گواهی می‌کنند که امضا متعلق به چه کسی است و در چه تاریخی انجام گرفته است. به این ترتیب امکان جعل و انکار امضا از بین می‌رود. مشابهٔ این فرایند با ایجاد زیر ساخت کلید عمومی (PKI) برای امضای دیجیتال اجرا می‌شود. در این زیرساخت، سازمانهای متصدی صدور گواهینامه ایجاد می‌شوند که وظیفهٔ آنها این است که با احراز هویت اشخاص حقیقی یا حقوقی، امضای دیجیتال متعلق به آنها را مورد تأیید قرار می‌دهند.

مثال دیگری که در مورد شناسایی[1] و احراز هویت[2] وجود دارد، استفاده از شناسه[3] و گذرواژه[4] برای اتصال به شبکه است. از طریق شناسه، کاربر شناسایی شده و با استفاده از گذرواژه (با فرض اینکه فقط در اختیار شخص مجاز قرار دارد) از یکی بودن هویت کاربر با هویت مشخص شده توسط شناسه اطمینان حاصل می‌شود.

امضای دیجیتال مبتنی بر یک فرایند ریاضی به نام رمزنگاری است و در این گزارش درباره رمزنگاری و کاربردهای آن از جمله امضای دیجیتال، توضیحاتی ارائه شده است.

رمزگذاری[5] عبارت است از تبدیل داده‌ها به نحوی که خواندن آنها بدون کلید غیرممکن باشد. رمزگذاری و رمزگشایی[6] عموماً به اطلاعات محرمانه‌ای که کلید نامیده

---

1. Identification
2. Authentication
3. Username
4. Password
5. Encryption
6. Decryption

می‌شود، نیاز دارند. بعضی کاربردهای ساده رمزنگاری عبارتند از : ارتباطات مطمئن، شناسایی و احراز درستی چیزی. کاربردهای پیچیده‌تر آن شامل سیستمهای تجارت الکترونیک، گواهی کردن، ارسال نامهٔ الکترونیک محرمانه و دسترسی راه دور به رایانه می‌شوند.

دو نوع سیستم رمزنگاری وجود دارد :

۱. کلید ـ سری[1] یا متقارن؛

۲. کلید ـ عمومی[2] یا نامتقارن.

در رمزنگاری به روش کلید ـ سری، از کلید یکسانی برای رمزگذاری و رمزگشایی استفاده می‌شود.

در رمزنگاری به روش کلید ـ عمومی، هر کاربر یک کلید عمومی و یک کلید اختصاصی دارد. کلید عمومی در دسترس همگان قرار می‌گیرد، در حالی که کلید اختصاصی، محرمانه است.

انواع مختلف رمزنگاری (متقارن و نامتقارن) معرفی شده و کاربردهای آن مورد بررسی قرار می‌گیرند.

بدون یک روش سازگار و فراگیر برای احراز هویت، امکان تحقق دیگر طرحهای دولت الکترونیک وجود ندارد.

رمزنگاری متقارن و نامتقارن

چالش عمده در رمزنگاری متقارن آن است که فقط فرستنده و گیرنده باید از کلید محرمانه آگاه باشند و هیچکس دیگر نباید آن را بداند.

تولید، ارسال و نگهداری کلیدها را مدیریت کلید می‌نامند. از آنجا که تمام کلیدها در رمزنگاری کلید ـ سری باید محرمانه باشند، فراهم کردن یک مدیریت مطمئن برای

---

1. Secret-key
2. Public-key

کلیدها بویژه در سیستمهای باز با تعداد زیادی کاربر، مشکل است.

برای حل مشکل مدیریت کلید در سال ۱۹۷۶ مفهوم رمزنگاری کلید ـ عمومی (نامتقارن) معرفی شد. این روش دارای دو کاربرد عمده است :

۱. رمزنگاری؛

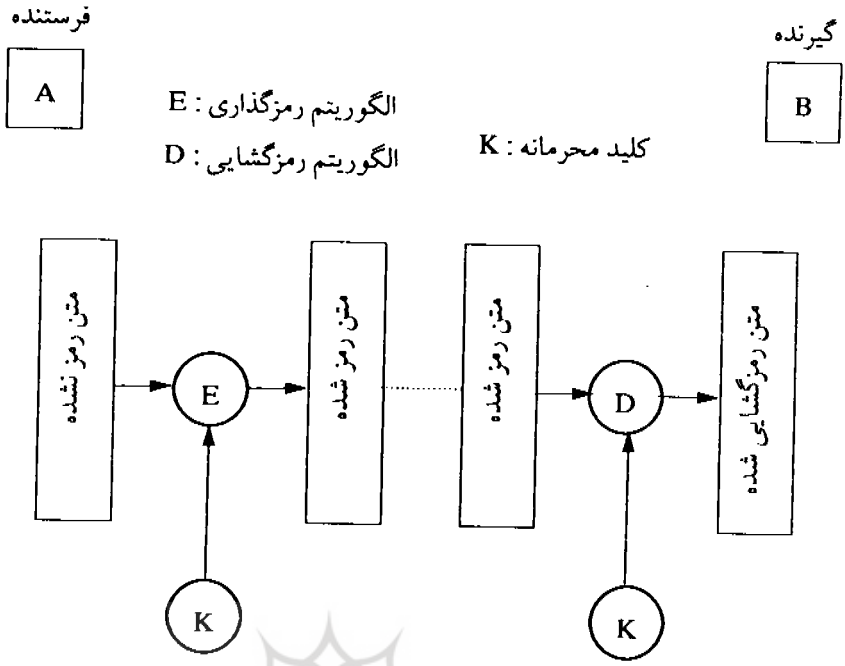
۲. امضای دیجیتال.

در این سیستم، هر شخص یک جفت کلید دریافت می‌کند که یکی کلید عمومی نام دارد و دیگری کلید اختصاصی. کلید عمومی برای اطلاع عموم منتشر می‌شود، ولی کلید اختصاصی محرمانه نگه داشته می‌شود. به این ترتیب دیگر نیاز نیست که فرستنده و گیرنده از یک کلید محرمانه مشترک استفاده کنند، بلکه تمام ارتباطات از طریق کلید عمومی انجام می‌شود و به ارسال کلید اختصاصی نیاز نیست. در این سیستم، احتیاج به برقراری یک کانال ارتباطی مطمئن نیست، بلکه تنها لازم است که کلیدها به روشی مطمئن به کاربرها اختصاص یابند.

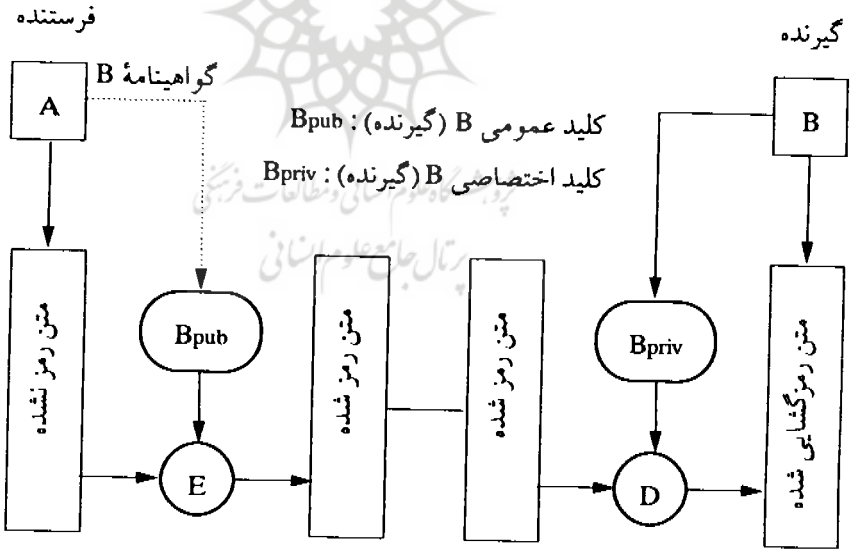
در سیستم رمزنگاری نامتقارن، کلید اختصاصی دارای یک رابطهٔ ریاضی با کلید عمومی است. بنابراین با به دست آوردن کلید اختصاصی از روی کلید عمومی، می‌توان این سیستم را مورد حمله قرار داد. روش متداول برای مقابله با این مشکل آن است که مسألهٔ به دست آوردن کلید اختصاصی از روی کلید عمومی را تا حد امکان مشکل کنیم.

مثالی ساده از رمزنگاری

فرض کنید A می‌خواهد یک نامهٔ محرمانه برای B بفرستد. برای این کار ابتدا A کلید عمومی B را در فهرست موجود پیدا می‌کند و با استفاده از آن، نامه را رمزنگاری می‌کند. B پس از دریافت نامه از کلید اختصاصی‌اش برای رمزگشایی و خواندن نامه استفاده می‌کند. به این ترتیب به جز B هیچکس نمی‌تواند این نامه را رمزگشایی کند؛ زیرا فقط B کلید اختصاصی B را می‌داند (شکلهای ۲ و ۳).



شکل ۲. رمزنگاری متقارن یا کلید ـ سری



شکل ۳. رمزنگاری نامتقارن یا کلید ـ عمومی

امضای دیجیتال و احراز هویت

در بعضی موارد لازم است منشاء یک سند، هویت فرستنده، تاریخ و زمانی که یک متن ارسال و یا امضا شده، هویت یک کاربر رایانه و... تأیید شود.

«امضای دیجیتال» یک ابزار رمزنگاری است که از طریق آن انجام موارد یاد شده امکان‌پذیر می‌شود. امضای دیجیتال یک متن، اطلاعاتی است که بر مبنای خود متن و کلید اختصاصی امضاکننده به دست می‌آید. این اطلاعات با استفاده از تابع در هم سازی و رمزنگاری توسط کلید اختصاصی، ایجاد می‌شود.

امضای دیجیتال و امضای دست‌نویس، هر دو متکی بر این واقعیت هستند که پیدا کردن دو نفر با یک امضا، تقریباً غیرممکن است.

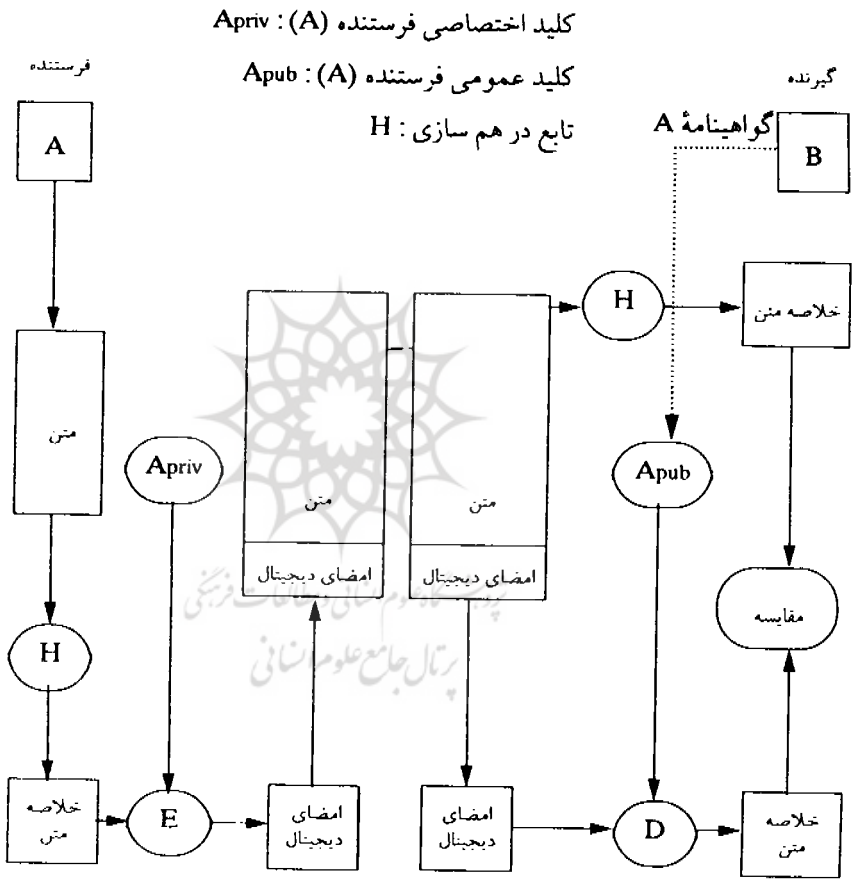
فرض کنید A می‌خواهد یک متن امضا شده برای B بفرستد. ابتدا A باید تابع در هم سازی را به متن اصلی اعمال کند تا خروجی حاصل که «خلاصه متن» نامیده می‌شود، به دست آید. برای ایجاد یک امضای دیجیتال به جای متن اصلی، «خلاصه متن» رمزنگاری می‌شود.

A خلاصه متن رمزنگاری شده و متن اصلی را (که می‌تواند رمزنگاری شده یا نشده باشد) برای B ارسال می‌کند. برای اینکه B بتواند صحت امضا را تأیید کند، باید همان تابع در هم سازی را به متن اصلی اعمال کند و خلاصه متن رمزگذاری شده را با استفاده از کلید عمومی A رمزگشایی کرده و این دو را با هم مقایسه کند. اگر حاصل این دو عملیات یکسان نباشد چند حالت وجود دارد : یا شخصی سعی می‌کند هویت A را جعل کند یا متن اصلی پس از امضای A تغییر کرده است و یا هنگام ارسال، خطایی رخ داده است (شکل ۴).

مثالی ساده از امضای دیجیتال

فرض کنید A می‌خواهد نامه‌ای برای B بفرستد. برای امضای نامه، A محاسبه‌ای انجام می‌دهد که ورودیهای آن کلید اختصاصی A و متن نامه می‌باشند. خروجی این

محاسبه، امضای دیجیتال نامیده می‌شود و به نامه پیوست می‌شود. برای اطمینان از صحت امضا، B محاسبه‌ای انجام می‌دهد که ورودیهای آن شامل متن نامه، امضای پیوست و کلید عمومی A هستند. اگر خروجی حاصل طبق یک رابطهٔ ریاضی از قبل تعریف شده درست باشد، امضا معتبر است، در غیر این صورت یا امضا جعلی است یا متن نامه تغییر یافته است.



شکل ۴. امضای دیجیتال

تابع درهم‌سازی[1]

تابع در هم سازی H، تبدیلی است که ورودی m را می‌گیرد و دنبالهٔ h با طول ثابت را بر می‌گرداند : $h = H(m)$

ویژگیهای اصلی یک تابع در هم سازی مناسب برای رمزنگاری به شرح در پی آمده است :

۱. ورودی دنباله‌ای با طول دلخواه است؛

۲. طول دنبالهٔ خروجی ثابت است؛

۳. محاسبهٔ H(X) برای هر X داده شده نسبتاً آسان است؛

۴. H(X) یکطرفه[2] است؛

۵. H(X) یک به یک[3] است.

تابع در هم سازی H را یکطرفه می‌گویند اگر معکوس کردن آن مشکل باشد؛ بدین معنی که با داشتن مقدار h پیدا کردن ورودی X به نحوی که H(X)=h، از نظر محاسباتی غیرممکن باشد.

اگر با داشتن X، پیداکردن ورودی Y به نحوی که H(X)=H(Y) از نظر محاسباتی غیرممکن باشد، در آن صورت تابع H را یک به یک ضعیف می‌نامند.

تابع H یک به یک قوی نامیده می‌شود؛ چنانچه پیدا کردن دو ورودی X و Y به نحوی که H(X)=H(Y) از نظر محاسباتی غیرممکن باشد.

خروجی تابع در هم سازی دقیقاً نماینده متنی است که از روی آن محاسبه شده و این مقدار «خلاصه متن»[4] نامیده می‌شود.

می‌توان «خلاصه متن» را به عنوان «اثر انگشت دیجیتال» متن اصلی در نظر گرفت. مهمترین کاربردهای تابع در هم سازی عبارت است از وارسی درستی متن و امضای دیجیتال.

---

1. Hash function
2. One-way
3. Collision free
4. Message digest

از آنجا که توابع در هم سازی اغلب از الگوریتم‌های رمزنگاری یا امضای دیجیتال سریعتر هستند، به جای اعمال فرایند رمزنگاری به خود متن، آن را به خروجی تابع در هم سازی که از متن اصلی کوچکتر است، اعمال می‌کنند. علاوه بر آن می‌توان خلاصه متن را در دسترس عموم قرار داد، بدون آنکه محتوای متن اصلی آشکار شود.

دکتر ساسان بصیری
مهندس پیام صالح
مدیریت توسعه‌فن‌آوری‌اطلاعات
مرکزتوسعه فن آوری ونوسازی اداری