

Digital Signature

امضای دیجیتال

New technology of Information Security

فناوری نوین امنیت اطلاعات

در فرایندهای کسب و کار

- 1 مقدمه
- 2 مشکلات و مسائل امنیتی در مبادلات الکترونیکی
- 3 الزامات و مفاهیم امنیتی در دنیای مجازی
- 4 راهکارها و ابزارهای امنیتی (امضای دیجیتال)
- 5 کاربردهای گواهی دیجیتال در تبادلات اینترنتی
- 6 کاربردهای امضای دیجیتالی در انواع کسب و کار

سوال؟

✓ آیا تا به حال به هویت فردی که برای شما ایمیل فرستاده شک کرده اید؟

✓ آیا مطمئن هستید اطلاعاتی که بصورت الکترونیکی مبادله می شود در بین راه دستکاری نشده است؟

✓ در هنگام خرید اینترنتی آیا اطلاعات حساب شما محرمانه می ماند؟

✓ در هنگام بازدید از یک سایت اینترنتی آیا به جعلی بودن آن شک کرده اید؟

مقدمه

- ✓ امروز مدیریت اسناد الکترونیکی ، ارسال و دریافت آن ها بخش بزرگی از فعالیت های اجرایی را شامل می شود.
- ✓ یکی از تکنولوژی هایی که موجب افزایش اعتماد به این فرایند گردیده ، امضای دیجیتال است.
- ✓ در اسناد مکتوب ، امضا ، نشان تایید تعهدات قبول شده در آن سند به شمار می آید.
- ✓ در اسناد الکترونیکی هم نیازمند امضای الکترونیکی هستیم.

مقدمه

✓ امروزه امنیت فضای الکترونیکی ، وجهه‌ای از امنیت ملی هر کشور را به تصویر می‌کشد.

✓ اعتبارات مالی بیشتر و بیشتر به صورت الکترونیکی جا بجا می‌شوند.

✓ سوء استفاده از ضعف های امنیتی و ناآگاهی کاربران بیش از هر زمان دیگری در دسترس ماجراجویان و جاسوسان دنیای مجازی قرار دارد.

✓ و هر یک از این عوامل خود به تنهایی دلیل محکمی برای جدی گرفتن موضوع امنیت اطلاعات در فضای سایبری است.

مشکلات و مسائل امنیتی در مبادلات الکترونیکی

✓ در یک ارتباط ایده‌آل:

✓ **مبدأ و مقصد** یکدیگر را می‌شناسند و با هم در ارتباطند

✓ هیچ **شخص ثالثی** در این میان به اطلاعات مبادله شده بین آن‌ها دسترسی ندارد

✓ اطلاعات ارسالی به طور **کامل و سالم** به مقصد می‌رسند

مشکلات و مسائل امنیتی در مبادلات الکترونیکی

در یک سیستم واقعی ممکن است:

- ✓ ارتباط بین مبدأ و مقصد مورد حمله قرار گیرد ،
- ✓ داده‌ها مخدوش یا مفقود شوند ،
- ✓ یا مورد استراق سمع واقع شوند.
- ✓ رابطه گرافیکی یک پایگاه اینترنتی معتبر جهت ربودن اطلاعات محرمانه دقیقاً کپی شده باشد (Phishing).
- ✓ همچنین احتمال دارد شخصی لحظه به لحظه هر آنچه را که شما با رایانه انجام می‌دهید مشاهده و ثبت نماید.

الزامات و مفاهیم امنیتی در دنیای مجازی



احراز و تصدیق هویت

کلمه عبور

- کد رمز یا **کلمات عبور** با اطلاعات ذخیره شده در سیستم مطابقت داده می شود و عملیات احراز هویت صورت می گیرد.

علائم زیست سنجی

- برای احراز هویت از سنجش و تحلیل **خصوصیات منحصر به فرد** شخصی استفاده می شود. **اثر انگشت** ، **شکل عنبیه** یا **شبکیه چشم** ، **فرم دست** و **چهره فرد**

سخت افزاری

- **کارت های هوشمند**: این کارت ها می توانند حاوی کلید خصوصی افراد ، گواهی نامه کلید عمومی و دیگر اطلاعات مفید باشند.
- **توکن های امنیتی**: سخت افزاری کوچک است که برای ورود کاربر یک سرویس رایانه ای به سامانه بکار می رود و جهت احراز هویت ، تعیین اعتبار ، نگهداری امن و جلوگیری از دسترسی غیر مجاز به داده های محرمانه کاربر

راهکارها و ابزارهای امنیتی در دنیای مجازی

مجموعه‌ای از **فنون ریاضی** برای حفاظت از اطلاعات و هنر نوشتن به صورت رمز است بطوریکه هیچ‌کس به غیر از دریافت کننده مورد نظر نتواند محتوای پیام یا مستندات را بخواند.

رمزنگاری

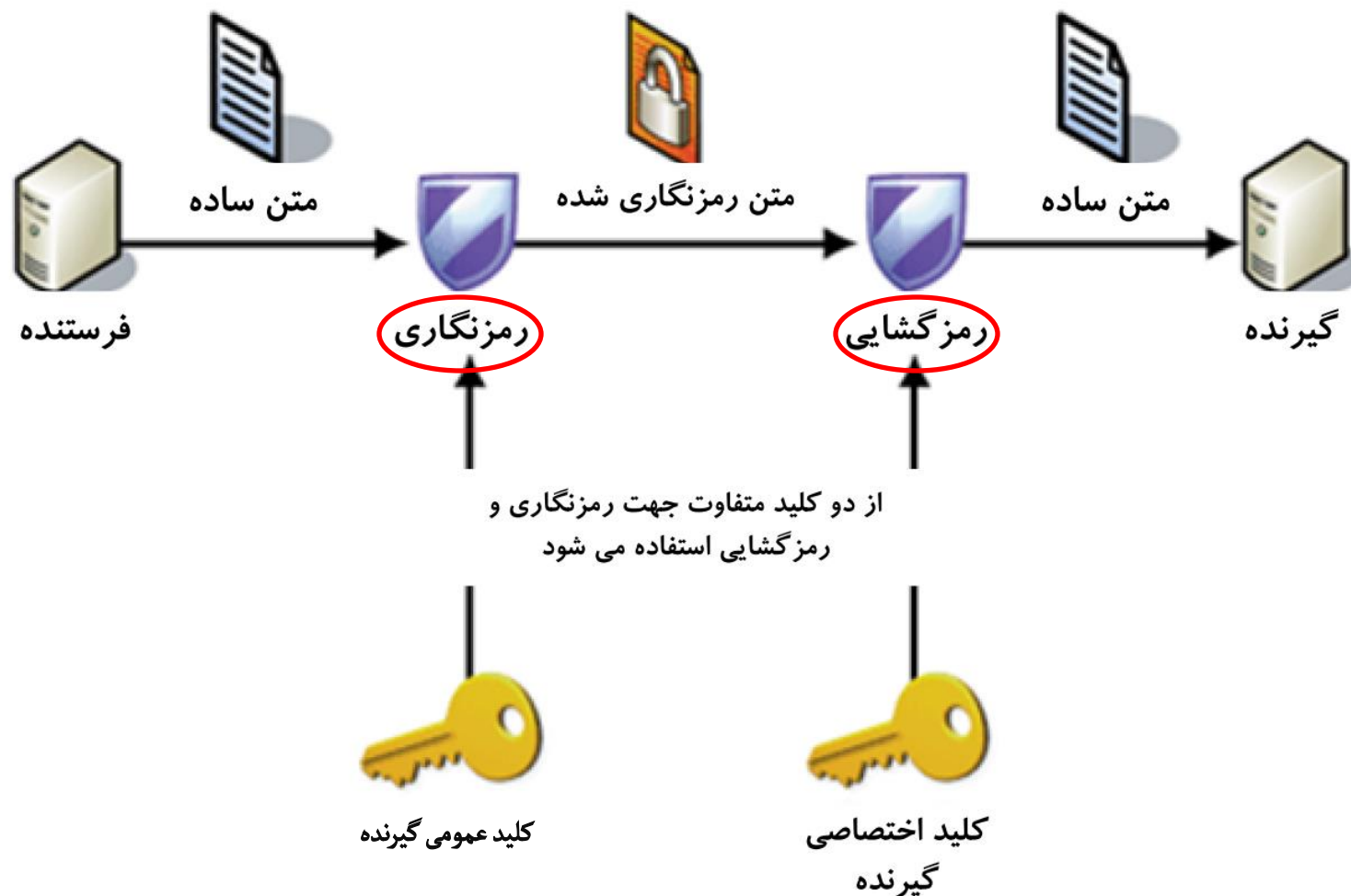
الگوریتم متقارن: در این روش از یک کلید مشترک برای رمزنگاری و رمزگشایی استفاده می‌شود.

الگوریتم نامتقارن: به جای یک کلید مشترک از یک جفت کلید به نام‌های کلید عمومی و خصوصی استفاده می‌شود.

الگوریتم هش (Hash): توابع ریاضیاتی هستند. هنگامی که داده‌ای به عنوان ورودی به این تابع داده می‌شود، چکیده‌ای از آن مجموعه داده تولید می‌شود که منحصر به فرد و قابل بازگشت است.

الگوریتم های
رمزنگاری

فرایند رمز نگاری و رمز گشایی



راهکارها و ابزارهای امنیتی در دنیای مجازی

امضای دیجیتال:

- ✓ نوعی رمزنگاری نامتقارن است (کلید عمومی و خصوصی)
- ✓ خصوصیات امضای دستی را در فضای الکترونیکی فراهم می سازد
- ✓ هر موجودیت منحصر به فرد در فضای مجازی دارای امضای دیجیتالی خاص خود است
- ✓ می توان مستندات ، پیغام ها و داده های الکترونیکی را توسط امضای دیجیتال تأیید کرد.
- ✓ می توان مطمئن بود تولید کننده امضا چه کسی است
- ✓ می توان مطمئن بود اطلاعات پس از امضا، تغییر نکرده است

راهکارها و ابزارهای امنیتی در دنیای مجازی

امضای دیجیتال:

- ✓ کلید خصوصی فرد به صورت امن در وسیله‌ای مانند **کارت هوشمند** یا **توکن** نگهداری می‌شود
- ✓ با توجه به **عدم امکان جعل امضای دیجیتال**، اسناد یا پیام‌های امضاء شده **غیر قابل انکار** است
- ✓ مراجع قضایی می‌توانند از این خصوصیت جهت **استناد قانونی** به سند الکترونیکی استفاده کنند

راهکارها و ابزارهای امنیتی در دنیای مجازی

گواهی دیجیتال:

✓ یک سند الکترونیکی امضاء شده و غیر قابل جعل است

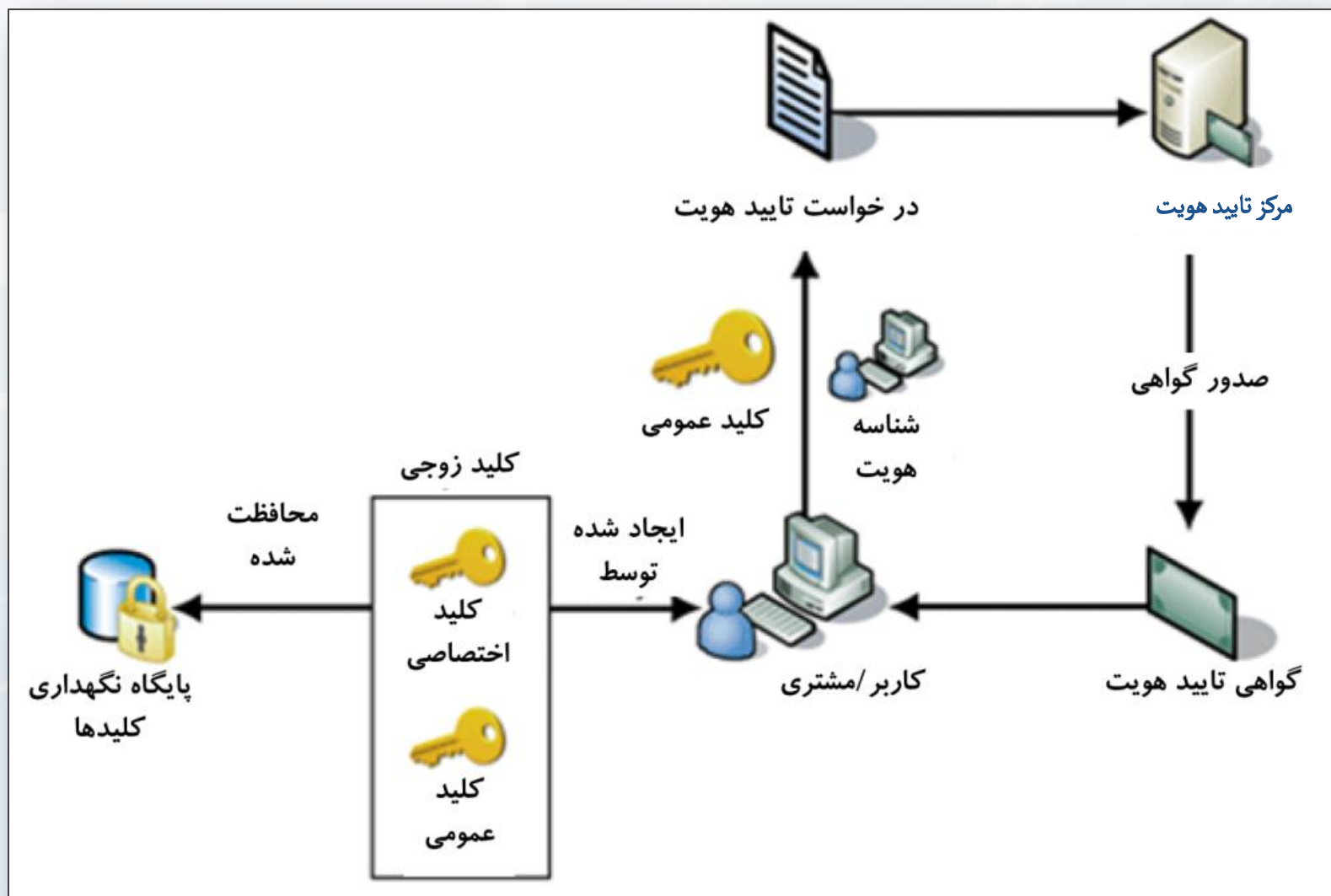
✓ معرف هویت فردی است که صاحب امضاء دیجیتالی است

✓ توسط مرکز صدور گواهی پس از اطمینان از صحت هویت فرد و تحت قوانین معینی برای یک شخص، سخت افزار یا نرم افزار صادر می شود

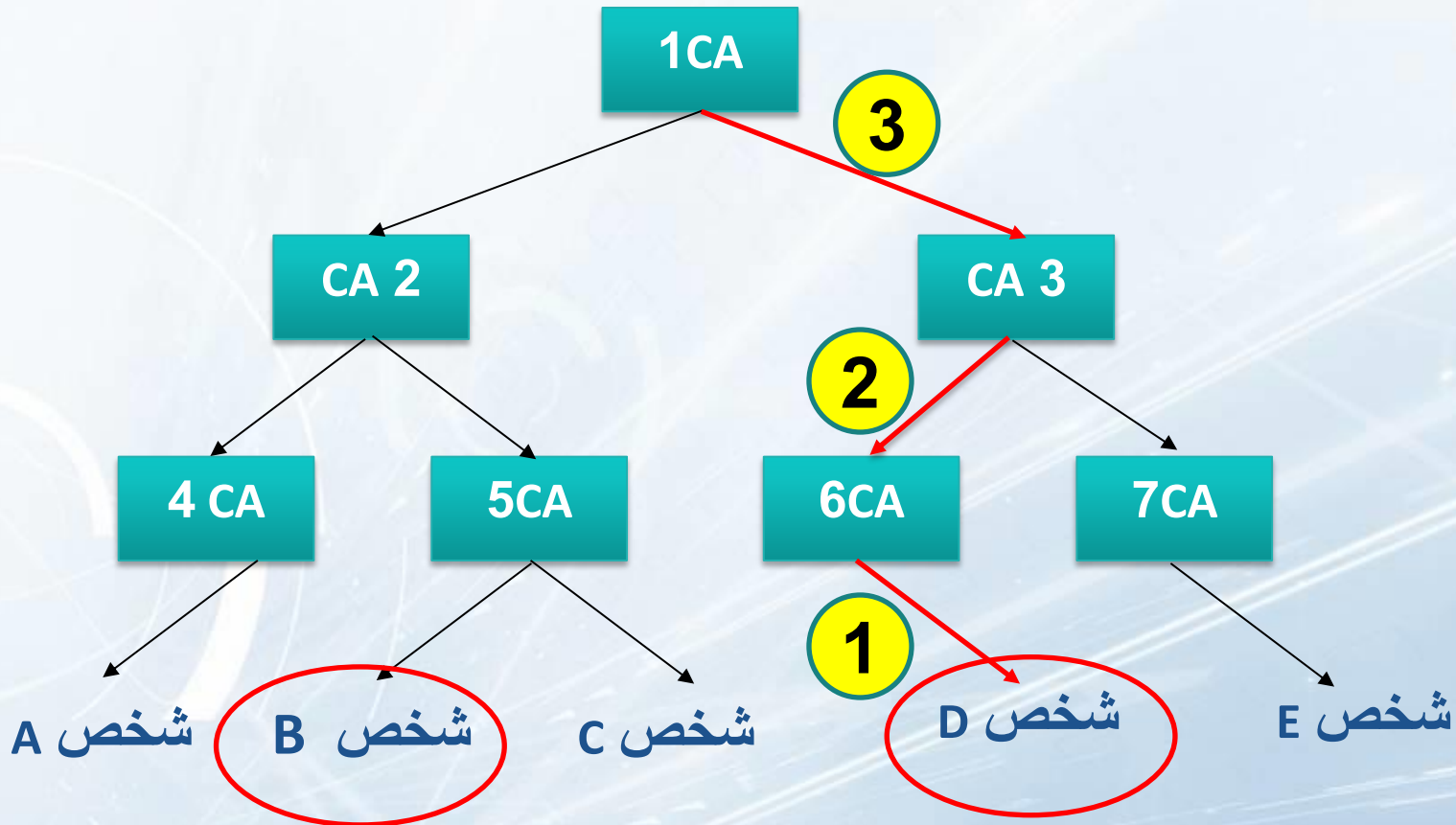
✓ متناظر با هر گواهی، یک کلید خصوصی وجود دارد.



طرف سوم مورد اعتماد جهت تعیین هویت کاربران



سلسله مراتب مراجع معتبر تایید هویت



کاربردهای گواهی دیجیتالی در تبادلات اینترنتی

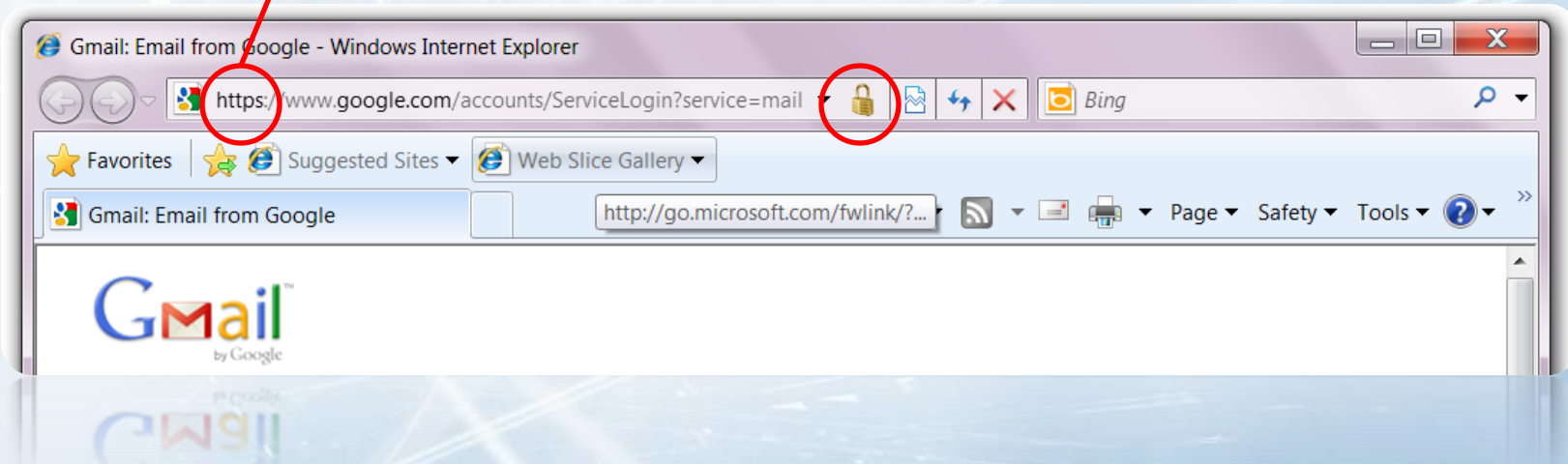
لایه اتصال امن (SSL):

پروتکلی (مجموعه‌ای از قوانین) جهت برقراری ارتباطات ایمن میان سرویس دهنده و سرویس گیرنده در اینترنت است

و از این پروتکل برای امن کردن پروتکل‌های غیر امن نظیر HTTP، LDAP، IMAP و ... استفاده

می‌شود.

HTTPS



کاربردهای گواهی دیجیتالی در تبادلات اینترنتی

استاندارد تبادل الکترونیکی امن (SET):

این استاندارد ابتدا مورد توجه شرکت‌هایی مانند Visa ، MasterCard ، Netscape و مایکروسافت قرار گرفت

به دنبال تامین امنیت و محرمانگی **تبادلات مالی اینترنتی** بکار می رود.

با استفاده از **رمزنگاری** و **گواهی‌نامه‌های دیجیتال** زنجیره‌ای از اعتماد بین فروشنندگان ، بانک‌ها و مشتریان ایجاد می‌کند.

استاندارد **secure MIME**:

بر اساس این استاندارد ، الزامات امنیتی **احراز هویت** ، **تمامیت پیام** ، **انکارناپذیری** (با استفاده از امضای دیجیتال) و **محرمانگی و امنیت** (با استفاده از رمزنگاری) برای **نامه‌ها و پیام‌های الکترونیکی** تامین می‌گردد .

کاربردهای امضای دیجیتالی در انواع کسب و کار

تبادلات
B2B

تایید هویت طرفین معامله-اطمینان از عدم تغییر و دستکاری ارتباطات مربوط به معامله -در سفارشات خرید ، قبض‌های رسید ، فرم‌های وب ، یا سیستم‌های خرید آنلاین به امضای دیجیتالی نیاز است.

تبادلات
B2C

امضای دیجیتال عمدتاً به منظور احراز هویت مشتری و اطمینان از عدم تغییر جزئیات معامله در حین ارتباط- در دیگر حوزه‌های کسب و کار با مشتری مانند خدمات مالی ، بانکداری الکترونیک ، تبادلات سهام و بیمه

تبادلات
G2G

در تعاملات بین نهادهای دولتی- احراز هویت و تمامیت پیام‌ها و اسناد مبادله شده بوده و اغلب انکارناپذیری

تبادلات
G2B

احراز هویت آن‌ها و اطمینان از عدم انکار و عدم تغییر ارتباطات فی‌مابین- پیشنهادات مناقصه‌ای را به صورت دیجیتالی امضاء شود -دولت‌ها می‌توانند سفارشات خرید خود را به صورت دیجیتالی تایید کنند

تبادلات
G2C

احراز هویت شهروندان-اطمینان از عدم تغییر پیام‌ها - رای گیری الکترونیکی —خدمات آنلاین مانند: مجوز فعالیت ، احداث یا بهره‌برداری-دریافت اظهار نامه مالیاتی

نتیجه گیری

- ❖ در حال حاضر امنیت در فضای مجازی یکی از مهم ترین مسایل حوزه ارتباطات است.
- ❖ امضای دیجیتالی یکی از راهکارهایی است که برای جلوگیری از بروز این مشکل معرفی گردید.
- ❖ امضای دیجیتال مزایای بیشتری نسبت به امضای دستی دارد: (محرمانگی-تمامیت- انکار ناپذیری- احراز و تصدیق هویت)
- ❖ با بکارگیری امضای دیجیتالی و ایجاد بسترهای امن ارتباطی می توان به توسعه بخش هایی چون دولت الکترونیک و تجارت الکترونیک امیدوار شد.

پایان

با تشکر از توجه شما