امضای دیجیتال
کارت شناسایی دیجیتال
در محیطهای اینترنت
با استفاده از شناسه نوین

شرکت برنامه نویسان
رایانه ای نوین افزار (برنا)

خلاصه:

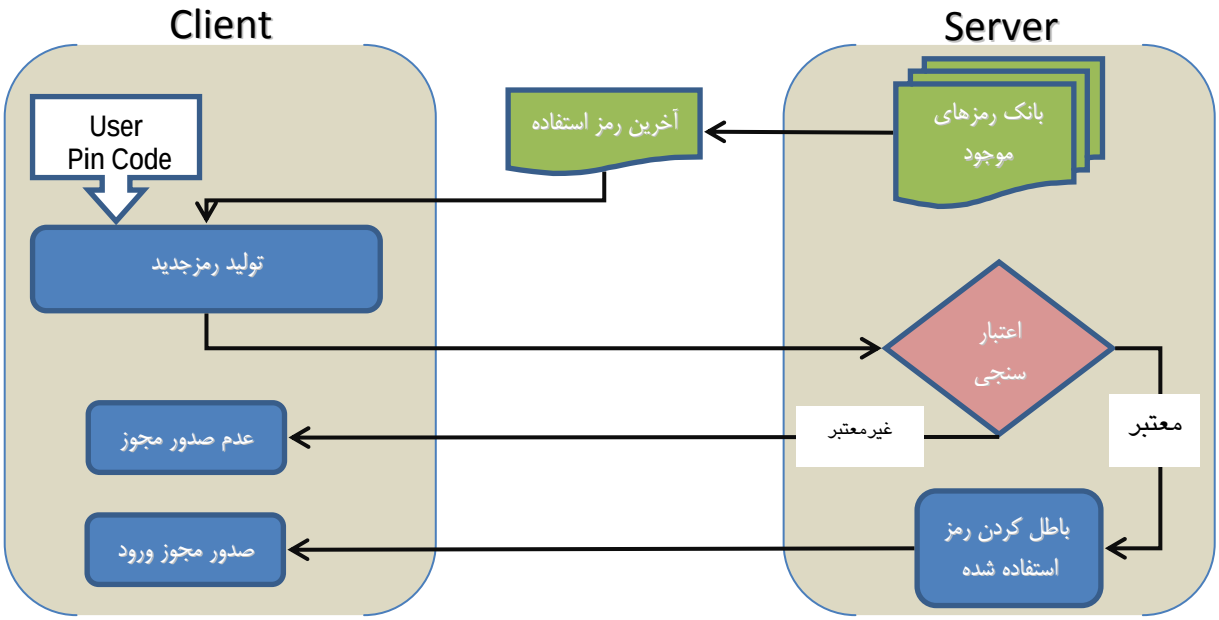
نبود روش مطمئنی برای احراز هویت کاربران اینترنت و نبود تضمینی برای جلوگیری از انکار احتمالی کاربران یا جلوگیری از دستکاری اطلاعات توسط افراد غیرمجاز و همچنین نبود روشی مطمئن برای ارسال نامه های محرمانه که مهمترین مشکلات در راه تحقق دولت الکترونیک میباشد , ما را بر آن داشت که راه حلی را به صورت سخت افزار با عنوان امضای دیجیتال و کارت شناسایی دیجیتال طراحی و پیاده سازی کنیم. این وسیله یک کامپیوتر کوچک (میکروکنترلر) است که از طریق درگاه USB با کامپیوتر شخصی کاربر در ارتباط است. شناسه (token) یک وسیله سخت افزاری است که از نظر ظاهری در ابعاد و اندازه های یک cool disk است و به پورت USB رایانه شخصی وصل می گردد. شناسه وسیله ای است برای شناسایی کاربران محیطهای مجازی مانند اینترنت که علاوه بر احراز هویت می تواند اطلاعاتی را که کاربر ایجاد یا تغییر می دهد امضای دیجیتال کند.

این وسیله کاربردهای مختلفی دارد که مهمترین آنها بحث کارت شناسایی و امضای دیجیتال و نامه محرمانه است که در ادامه مطلب بصورت جداگانه به توضیح در مورد یکایک آنها پرداخته ایم:

در سیستمهای مجازی نظیر اینترنت به دلیل عدم رویارویی مستقیم با خود کاربر و عدم رویت آن باید روالی برای احراز هویت فرد مورد نظر وجود داشته باشد. اولین کاربرد شناسه در شناسایی و احراز هویت کاربران است، یعنی از این وسیله می توان به عنوان کارت شناسایی (سطح دسترسی) کاربران در محیط های مجازی مانند پورتالهای سازمانی، سیستم های اتوماسیون اداری و هر محیط مجازی دیگر که بحث کاربر در آن وجود دارد استفاده کرد و این وسیله را جایگزین رایجترین و در عین حال پر خطر ترین روش شناسایی یعنی username و password کرد.

چنانکه می دانیم نام کاربری و رمز عبور یک واقعیت مجازی است و دزدیده شدن یا لو رفتن آن قابل احساس نمی باشد و اگر چنین اتفاقی رخ دهد، تا زمانیکه سوء استفاده یا خرابکاری به نام کاربر اتفاق نیافتد کاربر از لو رفتن سطح دسترسی خود بی اطلاع است. ولی این وسیله سخت افزاری یک واقعیت فیزیکی بوده و گم شدن یا دزدیده شدن آن کاملا محسوس و در همان دقایق اول نبود آن مشخص می شود. از طرفی دیگر مانندکارت خودپرداز بانک دارای PIN Code است و به تنهایی غیر قابل سوء استفاده می باشد. این کاربرد وسیله (احراز هویت افراد) را اصطلاحا ***کارت شناسایی دیجیتال*** می گویند.

برای استفاده از این وسیله از یکی از قابلیتهای این وسیله استفاده می شود که رمزنگاری متقارن AES با کلید ۱۲۸ بیتی منحصر بفرد است. روال احراز هویت بصورت زیر است:



مراحل کار بصورت زیر است:

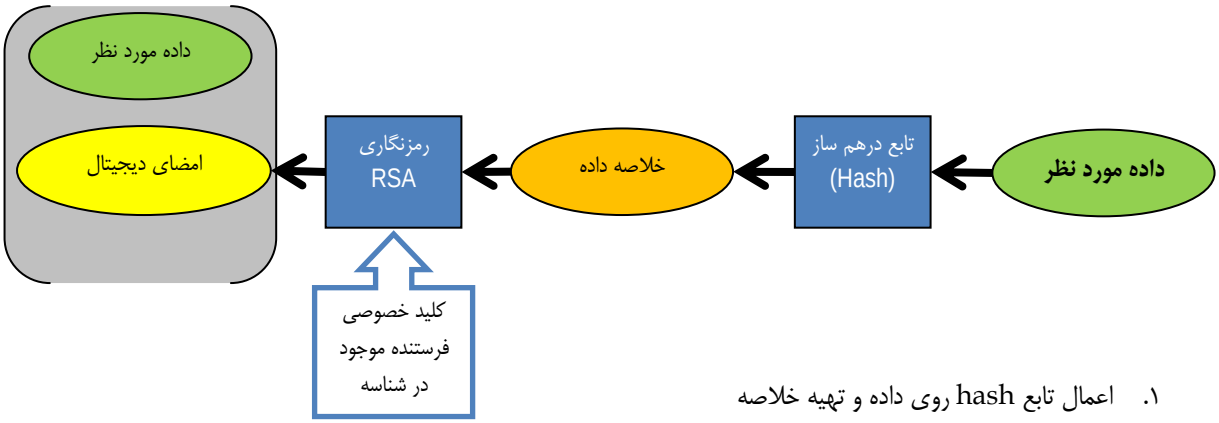
۱. کاربر شناسه را به رایانه شخصی وصل می کند
۲. شماره سریال وسیبله که منحصربفرد است، خوانده شده و به سرور ارسال می شود
۳. آخرین رمز استفاده شده برای آن شماره سریال به رایانه کاربر ارسال می شود
۴. کاربر PIN Code خود را وارد می کند
۵. در صورت صحیح بودن پین کد رمز جدید با الگوریتم AES داخل شناسه از روی رمز دیافت شده از سرور ساخته می شود
۶. رمز جدید به سرور ارسال و بر اساس بانک رمزها سرور درستی آن را بررسی می کند
۷. در صورت معتبر بودن، آخرین رمز استفاده شده بروزرسانی می شود و احراز هویت انجام می گردد.

یعنی شماره سریال شناسه همان فاکتوری است که ارتباط ۱-۱ با کاربر دارد و روال فوق صحت شناسه کاربر را تست می کند.

کاربران در محیطهای مجازی عملیاتی را انجام می دهد ولی به دلیل اینکه این عملیات امکان شبیه سازی یا دستکاری را دارد اعتماد متقابل کاربر و سیستم دچار خدشه می شود. یعنی هم کاربر مطمئن نیست که اطلاعات ممکن است در راه یا روی سرور دستکاری شود و هم سرور (صاحب سیستم) برای جلوگیری از انکار احتمالی کاربر , برای عمل انجام داده , تضمینی ندارد. کاربرد دیگری که این وسیله دارد و می تواند برای حل این مشکل استفاده شود، بحث امضای دیجیتال آن است. امضای دیجیتال گذاشتن یک رد پا یا اثر منحصر بفرد است که از سوی کاربر روی داده هایی که ایجاد می کنند یا تغییر می دهند یا تایید می کنند و خلاصه هر تراکنشی که در آن محیط مجازی انجام می دهند. این اثر منحصر بفرد بدون حضور وسیله غیر قابل شبیه سازی است حتی توسط مدیران/ صاحبان سیستم، برنامه نویسان سیستم و حتی توسط هکرها نیز قابل شبیه سازی نیست.

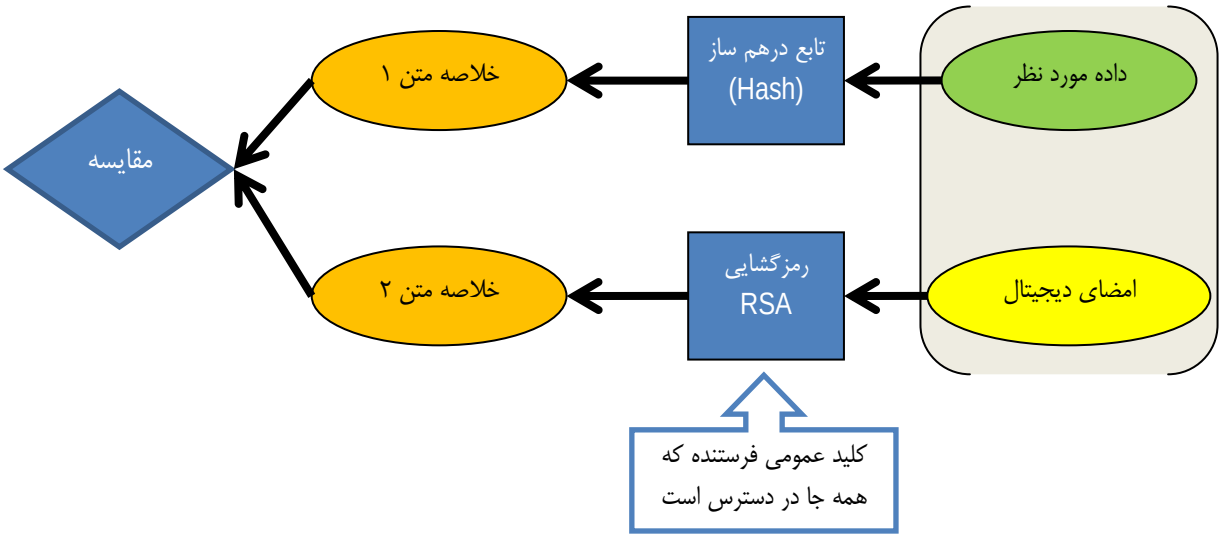
منشا این اثر الگوریتم رمزنگاری نامتقارن RSA و یک عدد ۱۰۲۴ بیتی است که در وسیله سخت افزاری ذخیره شده و به آن کلید خصوصی یا Private Key می گویند. تعداد حالات ممکن برای این مقدار، عددی با بیش از ۳۰۰ رقم است , پس بنابراین عملا غیر قابل حدس زدن است . این الگوریتم بر اساس دو کلید کار می کند که یک کلید را به عنوان کلید عمومی در اختیار همه کاربران قرار می دهند و دیگری کلید خصوصی است که فقط در شناسه کاربر ذخیره است. هر داده ای که با یکی از این کلید ها رمزنگاری شود با کلید دیگر رمزگشایی می شود.

رمزنگاری RSA روال بسیار سنگینی دارد و انجام آن طولانی است. بدین منظور برای امضای دیجیتال به جای اینکه کل متن، داده یا اطلاعات را رمز کنیم با یکی از توابع درهم ساز (Hash) به خلاصه متن می رسیم. این توابع اصطلاحا یکطرفه قوی هستند و بازیابی داده اصلی از روی خلاصه تقریبا غیر ممکن است. با تلفیق رمزنگاری RSA و یک الگوریتم درهمساز دلخواه مانند MD5 یا SHA-1 می توان اطلاعات را امضای دیجیتال کرد. برای استفاده از این وسیله برای امضای دیجیتال اطلاعات روال زیر انجام می گردد:



۱. اعمال تابع hash روی داده و تهیه خلاصه
۲. اتصال شناسه به یکی از پورتهای USB رایانه
۳. دریافت PIN Code از کاربر برای دسترسی به کلید خصوصی داخل شناسه
۴. رمزنگاری خلاصه با کلید خصوصی فرستنده که در شناسه است
۵. الحاق خلاصه رمزشده (امضا) به داده اصلی

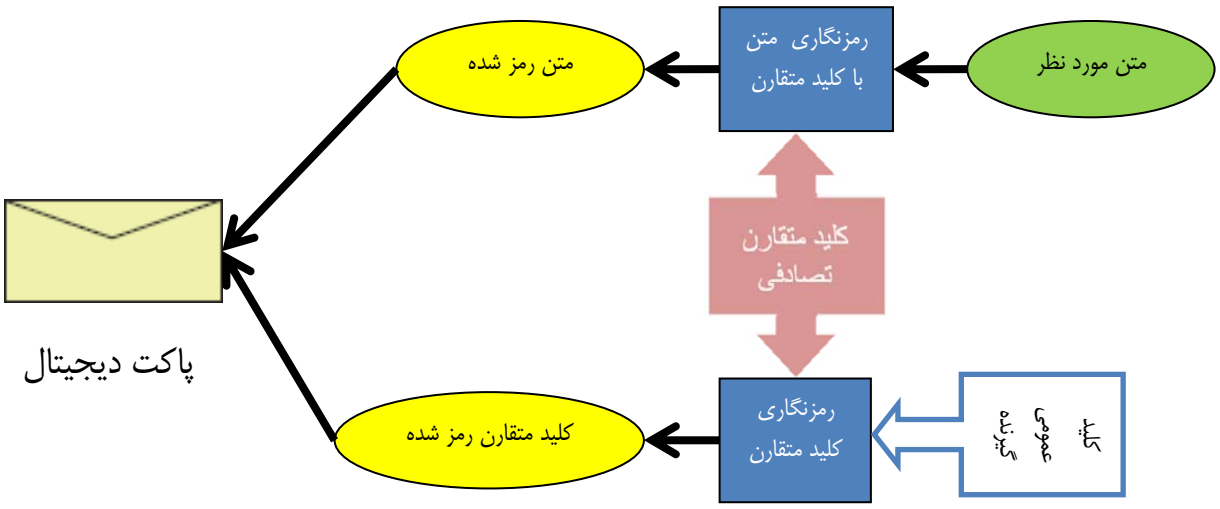
هنگامی که می خواهیم از صحت اطلاعات (دستنخوردگی) داده یا امضای دیجیتال مطلع شویم باید آنرا به روش زیر امتحان کرد:



۱. جداسازی داده و امضا از هم
۲. اعمال تابع hash روی داده و تهیه خلاصه ۱
۳. دریافت کلید عمومی کاربر فرستنده از مرجع کلید عمومی کاربران
۴. رمزگشایی امضا با استفاده از کلید عمومی فرستنده (خلاصه ۲)
۵. مقایسه خلاصه ۱ و خلاصه ۲ جهت تصدیق امضا

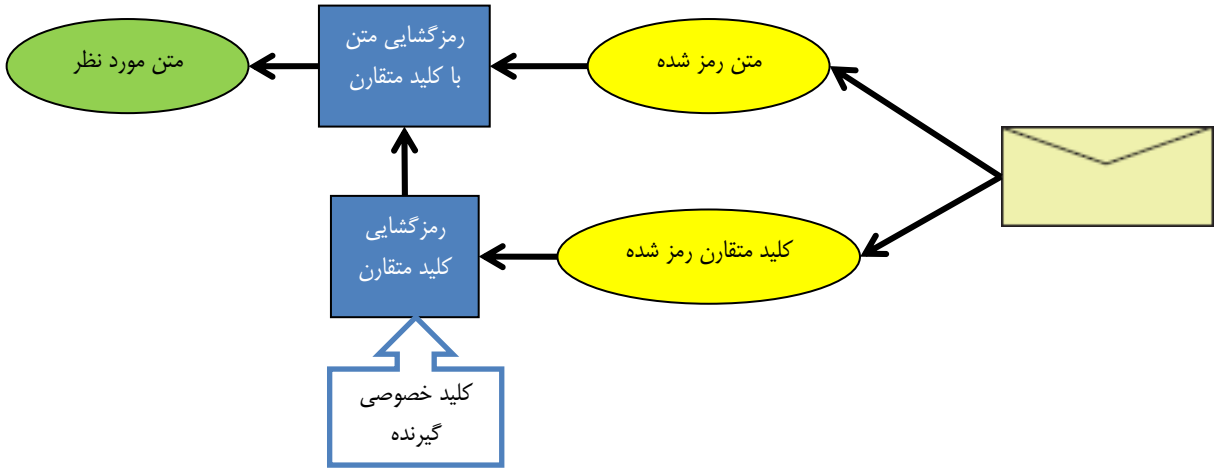
با عملیات فوق هم از بابت احراز هویت فرد ایجاد کننده اطلاعات مطمئن می شویم و هم از بابت دستخوردگی اطلاعات در راه یا روی سرور. در صورتی که جواب مقایسه منفی بود به قاطعیت نتیجه می گیریم که داده یا امضا دستکاری شده است و یا اطلاعات را کاربر دیگری ایجاد کرده است.

در برخی از سیستم ها وجود امکاناتی برای ارسال داده های کاملا محرمانه لازم است. در این سیستم ها الگوریتمها و روالهایی ایجاد شده است که بدلیل اطلاع برنامه نویسان یا مدیران آن سیستم از روال، امکان بازیابی اطلاعات محرمانه توسط افرادی غیر از کاربر مقصد امکانپذیر است. با استفاده از امکانات همین وسیله می توان در محیطهای مجازی نامه های واقعا محرمانه ارسال کرد به طوری که به هیچ وجه بدون وجود شناسه مقصد (کاربر گیرنده) اطلاعات غیرقابل فهم و غیر قابل بازیابی باشد. بدین منظور از الگوریتم RSA موجود در این وسیله و ترکیب آن با یک الگوریتم متقارن نظیر AES، Bluefish یا 3DES استفاده می شود. به این کاربرد اصطلاحاً پاکت دیجیتال گفته می شود که روال ایجاد نامه محرمانه آن بصورت زیر است:



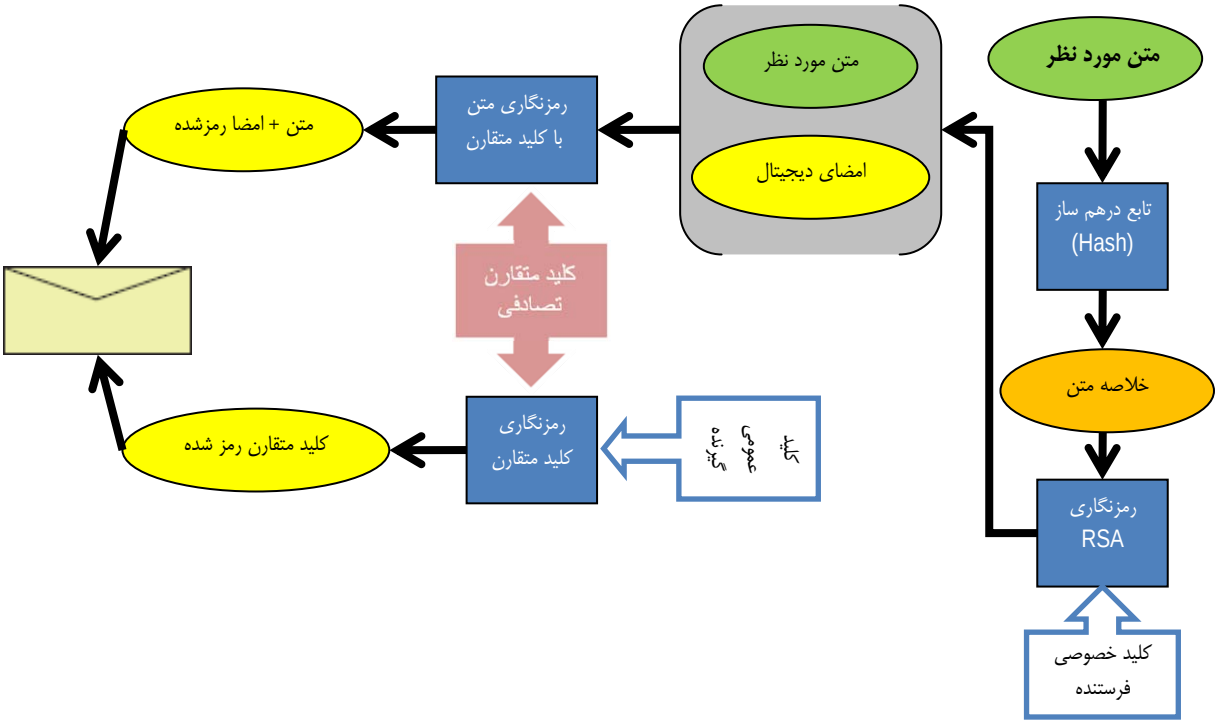
۱. یک کلید به صورت تصادفی سمت فرستنده ایجاد می شود
۲. اطلاعات با استفاده از کلید رمزنگاری متقارن تصادفی رمزنگاری می شود
۳. کلید عمومی کاربر گیرنده از مرجع کلیدهای عمومی کاربران دریافت می شود
۴. رمزنگاری کلید متقارن با کلید عمومی گیرنده (مقصد)
۵. ادغام داده رمزشده با کلید متقارن رمزشده (پاکت دیجیتال)

سمت گیرنده نحوه بازیابی متن نامه به صورت زیر اتفاق می افتد:



۱. جداسازی متن رمزشده و کلید متقارن رمزشده
۲. اتصال شناسه به یکی از پورتهای USB رایانه
۳. وارد کردن PIN Code توسط کاربر برای دسترسی به کلید خصوصی داخل شناسه
۴. بازیابی کلید متقارن با رمزگشایی کلید رمز شده با استفاده از کلید خصوصی داخل شناسه
۵. رمزگشایی متن با استفاده از کلید متقارن بازیابی شده

درنهایت می توان این دو روش فوق (پاکت دیجیتال و امضای دیجیتال) را با هم تلفیق کرد و پاکت دیجیتال امضادار را ایجاد کرد:



بدیهی است که روال فوق دو قسمت اصلی دارد:

۱. امضا کردن متن نامه
۲. تبدیل متن+امضای دیجیتال به پاکت دیجیتال

مزایا و ویژگیها:

- تکنولوژی کاملاً بومی (این طرح بصورت صد در صد از مرحله طراحی تا تولید در داخل کشور انجام شده است)
- عدم وابستگی به کشورهای دیگر در صورت تحریم
- یک واقعیت فیزیکی و اطلاع سریع گم شدن یا دزدیده شدن
- استفاده از درگاه USB و عدم نیاز به تجهیزات اضافی برای ارتباط با رایانه
- جلوگیری از انکار احتمالی کاربران در مقابل عمل انجام شده در محیطهای مجازی
- اعتبار بخشیدن به اطلاعات به دلیل جلوگیری از دستکاری های احتمالی
- امکان ارسال داده های کاملا محرمانه به سایر کاربران
- وسیله غیر قابل کپی برداری و غیر قابل شبیه سازی
- شکیل، کوچک و قابل حمل و هزینه بسیار پایین
- کاربری راحت هم برای برنامه نویسان و هم برای کاربران نهایی

کاربردها:

- کارت شناسایی دیجیتال
- امضای دیجیتال
- پاکت دیجیتال (نامه محرمانه)
- پاکت دیجیتال امضادار
- قفل سخت افزاری

افتخارات :

- گواهی ثبت اختراعات به شماره ۳۸۵۰۳۲۵۳ و ۸۶۰۱۰۸۰۴ در اداره ثبت اختراعات و مالکیت معنوی.

- عضو انجمن مخترعین ایران

- عضو بنیاد ملی نخبگان

- تاییدیه علمی از سازمان پژوهشهای علمی و صنعتی ایران

- گواهی و مجوز شرکت فناور از پارک علم و فناوری خراسان رضوی

- استاندارد CE (استاندارد اروپا) از شرکت MIC

- پروانه بهره برداری از سازمان صنایع و معادن

- دارای لوح تقدیر از وزارت علوم ,تحقیقات و فن آوری

- دارای لوح تقدیر از وزارت کار و امور اجتماعی

- برنده جایزه اول (کمان زرین) درسومین جشنواره شیخ بهایی اصفهان و لوح ویژه یونسکو

- برگزیده (لوح زرین) در چهارمین جشنواره شیخ بهایی اصفهان

- رتبه اول ششمین جشنواره فن آفرینی فردوسی مشهد

- برگزیده جشنواره نوآوری و شکوفایی استان خراسان

- برگزیده جشنواره نوآوری و شکوفایی کشوری به عنوان دستاورد ویژه

مشتریان :

اجراشده

- دانشگاه فردوسی مشهد , نیشابور , گلپایگان , زابل , اصفهان,زنجان , خرمشهر , ایلام , الزهرا ,تربیت معلم تهران وتبریز
- دانشگاه آزاد اسلامی واحد مشهد , یزد , نیشابور , بجنورد , شیروان , چناران , نجف آباد , قوچان , کاشمر, فردوس
- دانشگاه غیر انتفاعی آمل , خیام مشهد , خراسان
- دانشگاه پیام نور مشهد , قوچان , نیشابور , سرخس و فریمان
- دانشگاه علمی و صنعتی خراسان
- دانشگاه مدیریت صنعتی خراسان
- بانک مسکن
- شهرداری مشهد , تهران , قم و شیراز
- پایانه بار سیمان مشهد
- شرکت سما سامانه (فروشنده نرم افزار آموزش به بیش از ۱۴۰ دانشگاه)
- شرکت آریانیک
- شرکت فراگستر
- شرکت آی کن
- شرکت فورسان
- شرکت مدار
- شرکت سیستم های هوشمند نسل سوم

در حال تست :

- ستاد کل ناجا
- شرکت رایانه قدس رضوی و زیر مجموعه های آن
- وزارت علوم تحقیقات و فناوری
- دانشگاه قزوین , تبریز ,تهران , امیرکبیر , کاشان
- شهرداری اصفهان , تهران
- استانداری اصفهان

قیمت محصول :

قیمت هر توکن طبق جدول زیر میباشد .

از ۱ عدد تا ۱۰۰۰ عدد ۸۵،۰۰۰ ریال

از ۱۰۰۱ تا ۵۰۰۰ عدد ۸۵،۰۰۰ ریال با چاپ اختصاصی بر روی توکن ها

۸۰،۰۰۰ ریال بدون چاپ اختصاصی بر روی توکن ها

از ۵۰۰۱ به بالا ۸۵،۰۰۰ ریال با چاپ و قاب اختصاصی برای توکن ها

۸۰،۰۰۰ ریال با چاپ اختصاصی بدون قاب اختصاصی برای توکن ها

۷۵،۰۰۰ ریال بدون چاپ و قاب اختصاصی برای توکن ها

❖ لازم به ذکر است که کلیه نرم افزارها , ابزارهای جانبی و آموزشهای لازم تا پیاده سازی کامل بصورت رایگان می باشد و فقط هزینه توکن ها دریافت میگردد.

آدرس : مشهد , کیلومتر ۱۲ جاده قوچان , پارک علم و فناوری خراسان , واحد ۴۱۳ تلفن ۵۰۰۳۴۸۵-۰۵۱۱
مدیر عامل: مهندس صاحبکار ۰۹۱۵۳۱۳۶۹۴۲