باسمه تعالى



دانشگاه صنعتی شریف

نحوه عملكرد سامانهى تداركات الكترونيك دولت (ستاد)

تمرین یک، درس رمزنگاری پیشرفته، دکتر سلماسی زاده

پوریا شفیقی ملکشاه ۹۹۲۰۶۱۶۳

زمستان ۹۹

💠 معرفی:

سامانه ی تدارکات الکترونیک دولت (به اختصار: ستاد)، سامانه ای دولتی –حاکمیتی است که وظیفه تجمیع و بهرهورسازی بخشی از معاملات تجاری دولت را برعهده دارد. این سامانه بر محور دسترسی آزاد به اطلاعات و حق برابر برای شهروندان ایجاد شده و سازمان ها و نهادهای مربوطه را قادر می کند معاملات خود را در بستری امن و شفاف انجام دهند.

اهداف اصلی ایجاد این سامانه و خواص آن را را می توان در کلیات زیر برشمرد.

- ۱. شفاف شدن معاملات: بواسطه التزام نهادها در استفاده از این سامانه، امکان فساد اعم از واگذاری خارج از ضوابط، زد و بند، دلالی و ... حداقل شده و علاوه بر نهادهای نظارتی مثل سازمان بازرسی و تعزیرات ، امکان رصد عمومی نیز فراهم است.
- 7. ایمنی معامله: بواسطه رعایت پرتکل ایمن در کل فرایند معامله، امکان استفاده از خلاهای قانونی، کلاهبرداری و ... کاهش دارد.
 - ۳. جلوگیری از قاچاق: بواسطه استفاده از "ایران کد" سلامت کالا تضمین شده و امکان ورود کالای قاچاق به مصارف دولت کاهش میابد.
 - ۴. کاهش هزینه های دولت: با عمومی شدن فرایندها و رقابت بین اشخاص برای انتخاب به عنوان طرف معامله، منافع دولت بیشینه می گردد.
- ۵. دسترسی برابر: با این سامانه امکان و فرصت برای همه شهروندان برابر می شود و رانت اطلاعاتی از بین می رود.



سایت شامل سه بخش اصلی است. خرید جزیی و متوسط، مناقصه و مزایده. هر کدام از این موارد به زیر بخش هایی تقسیم می شوند.



شکل ۱: بخش های اصلی

• خرید جزیی و متوسط: این بخش مربوط به کالاهایی است که سازمان مربوطه قصد واگذاری آن را داشته و همچنین کالا یا خدمتی که متقاضی بکارگیری است. در این بخش با عنوان تامین کننده یا خریدار می توان اقدام کرد. به طور معمول تقاضاها روزهای معینی در سامانه باقی مانده و در نهایت از بین متقاضیان، طرف قرارداد انتخاب می شود.



شکل ۲: بخش خرید جزیی و متوسط

مناقصه: این بخش از سامانه ستاد خریدهای عمده دستگاه های اجرایی را با استفاده از برگزاری انواع مناقصه ها طبق قانون برگزاری مناقصات امکان پذیر میکند. مدیران و مسئولان روی برگزاری این مناقصه ها در سایت ستاد نظارت دارند که تاخیری در روند اجرای آن ها ایجاد نشود. همچنین نهادهای نظارتی بر مناقصه ها و معاملات نظارت دقیق دارند که از تخلفات آگاه شوند.

مراحل برگزاری مناقصه ها در سایت ستاد ایران به شکل زیر انجام میگیرد.

 ۱. انواع مناقصه های عمومی و محدود کالا/ خدمات با فهرست بها و بدون فهرست بها ثبت و منتشر میشوند

۲. فراخوان های ارزیابی کیفی نیز ثبت و منتشر میشوند

۳. اسناد مشاهده و دانلود میشوند

۴. ارسال پیشنهادها به وسیله پاکت های الف، ب و ج

۵. ارسال پاسخ استعلام

۶. اصلاح مناقصه های منتشر شده

۷. بازپس گیری پیشنهادها و ارسال مجدد

٨. بازگشایی پاکت ها با امضای الکترونیکی تمامی اعضای کمیسیون مناقصه

۹. بررسی پاکت ها توسط کمیته فنی در مراحل مختلف

۱۰. تهیه لیست کوتاه

۱۱. اعلام به برنده

۱۲. پذیرش برنده

۱۳. انعقاد قرارداد با امضای الکترونیکی مسئولین دستگاه و تامین کننده

۱۴. ارسال و دریافت کالا/ صورت وضعیت خدمات

1۵. انجام انواع پرداخت در قالب پیش پرداخت، علی الحساب و قطعی (به صورت الکترونیکی/غیر الکترونیکی) با امضای الکترونیکی صاحبان امضاء از طریق سامانه مناقصه

در این بخش نیز امکان اقدام به عنوان مناقصه گذار و مناقصه گر وجود دارد.



شکل ۳: دو حالت شرکت در مناقصه

مزایده: فرایند مزایده به این شکل است که ابتدا فروشنده حداقل قیمت اموال خود را برای فروش مشخص میکند، بعد از آن خریداران قیمت های پیشنهادی خود را برای خرید آن اموال میدهند. قیمتی که پیشنهاد میشود باید برابر یا بیشتر از قیمت مشخص شده توسط فروشنده باشد. در نهایت کالا با بالاترین قیمتی که پیشنهاد شده است خریداری خواهد شد.

اینجا یک دسته بندی روی مزایده اموال تملیکی و مزایده دستگاه اجرایی وجود دارد و پس از انتخاب، انتخاب نقش های مزایده گر و مزایده گزار در دسترس است.

قابل توجه مناقصه گران محترم، پیشنهادهای شما (پاکت های الف، ب و ج) با استفاده از استاندارد FIPS 140-2 در زمـان ارسال پیشنهاد توسط مناقصه گر با الگوهای ترکیبی و چند لایه ای، رمزنگاری می شوند.

شكل ٤: تضمين امنيت ياكت هاى مناقصه



در بحث تامین امنیت معامله عوامل متعددی اثر گذارند. در اینجا به بررسی دو مورد اکتفا می شود.

- رمزگذاری پاکتها: برای تضمین سلامت مناقصه لازم است که که محتوای پاکتها قبل از موعد بازگشایی افشا نشود که بحث رمزنگاری این بخش بر عهده استاندارد Federal Information Processing Standards) FIPS 140-2 می باشد.
- امضا دیجیتال: احراز اصالت افراد طرف قرارداد بوسیله امضا دیجیتال مبتنی بر رمزنگاری کلید عمومی انجام می شود. در این فرایند فرد متقاضی بوسیلهی کلید خصوصی خود، متعهد می گردد.

لازم به ذکر است در این روش از توکنها استفاده می شود.



شکل ۵: توکن به عنوان کلید خصوصی