



مناقصه گزاری الکترونیک

زهرا گمار

دانشجوی کارشناسی ارشد دانشکده صنایع دانشگاه صنعتی شریف
zgomarkp@yahoo.com

واژه‌های کلیدی

مناقصه الکترونیک
دستورالعمل مناقصه الکترونیک
سیاست‌های امنیتی
مکانیزم‌های امنیتی
قرارداد الکترونیکی
بایست‌های قانونی
تجارت الکترونیکی

چکیده

مناقصه یکی از مهمترین تعاملات صاحبان کسب و کار با یکدیگر و با دولت می باشد. در این راستا، مناقصه الکترونیک به عنوان یکی از مهمترین کاربردهای فناوری اطلاعات و ارتباطات از طریق اصلاح و بهبود فرآیندهای سنتی، از سویی می تواند بعلت طیف گسترده تامین کنندگان و تنوع ارائه خدمات و کالا باعث افزایش استقبال بازار و رقابت و لذا کاهش قیمت توام با کیفیت بهتر پیشنهادات شود. از طرفی اطلاع رسانی گسترده و متمرکز و ایجاد فرصتهای یکسان برای شرکت عموم مردم حتی در مقیاس جهانی،

شفافیت، رعایت تساوی، اعتماد و انکارناپذیری را برای طرفین مناقصه به ارمغان آورد.

مقدمه

برگزاری مناقصه بعنوان یکی از اصلی‌ترین تعاملات صاحبان کسب و کار با یکدیگر و نیز با دولت، امروزه به یکی از مهمترین فعالیتهای سازمانهای معتبر تبدیل شده است.

رشد روزافزون تعداد سازمانها و شرکتها و پراکندگی جغرافیایی آنها (جهانی شدن اقتصاد) از یک طرف و فزاینده تنوع ارائه خدمات و فعالیتهای آنها از سوی دیگر باعث شده تا اکثر سازمانهای بزرگ دولتی و غیردولتی، با برگزاری مناقصه جهت خرید کالا و خدمات، مفهوم تازه‌ای به برون سپاری بدهند.

برگزاری مناقصه عبارتست از فرآیند رقابتی تعیین برنده برای خرید کالا و خدمات از اشخاص حقوقی براساس محاسبه بهترین خدمات و پایین‌ترین قیمت پیشنهادی توسط شرکت کنندگان در مناقصه.

همچنین روند رو به رشد توسعه کاربردهای فناوری اطلاعات و ارتباطات و حرکت به سمت دنیای دیجیتالی از طریق اصلاح و بهبود فرآیندهای سنتی، سبب افزایش اثر بخشی سیستمها و ایجاد رضایت مندی صاحبان کسب و کار گشته و زندگی بشر را متحول نموده است. ابداع مدل مناقصه‌گذاری الکترونیکی نیز در همین راستا است.

مناقصه‌گذاری الکترونیکی، معمولاً با مدل‌های کسب و کار B2B و G2B مطرح می‌شود و راهکاری است الکترونیکی برای تسهیل انجام فرآیند برگزاری مناقصه که می‌تواند شامل کلیه مراحل از آگهی و ارایه مدارک مناقصات تا ارزیابی و عقد قرارداد بصورت الکترونیکی باشد. تعاریف دیگری نیز برای آن وجود دارد که در ادامه می‌آید:

- از نظر خریدار، مناقصه الکترونیکی، وسیله اطلاع‌رسانی، دعوت، ارزش‌گذاری و انتخاب تأمین‌کننده برای مناقصه جهت محصولات و یا سرویسها بصورت الکترونیکی است.
- از نظر شرکت کنندگان، مناقصه الکترونیکی، ارسال الکترونیکی مدارک قابل رقابت جهت تأمین محصولات یا سرویسها است.
- مناقصه‌گذاری الکترونیکی، شامل برگزاری مناقصه در محیطی با امنیت بالا، تحت فناوری اینترنت و خارج ساختن فرآیند از حالت سنتی و مستندات فیزیکی است.

در این راستا، قوانین هر کشور و سیاستهای امنیتی، اهمیت ویژه پیدا می‌کند. منافع ناشی از آن مواردی نظیر طیف وسیعتری از تأمین‌کنندگان است که انتظار می‌رود ما را به سوی قیمت پائین‌تر باکیفیت بهتر و سرعت بالاتر راهنمایی کند.

از نظر شرکت کنندگان، فرصتهای بیشتر جهت شرکت در مناقصات، حتی در سطح جهانی، هزینه کمتر ارسال مدارک و بعضاً حتی شرکت در بخشهای کوچکتر برای شرکت‌های کوچکتر و یا مناقصات با تشریح مساعی^۱ (اگر سایت مربوطه آن را پشتیبانی کند)، از عمده مزایای مناقصه الکترونیکی می‌باشند.

البته منبع اصلی درآمد ناشی از این سیستمها، کاهش هزینه بعثت اتوماتیک شدن فرآیند مناقصه و نیز پیشنهادات کارآمد تر و به صرفه‌تر می‌باشد.

در این رابطه فواید این سیستم بصورت خلاصه در ذیل می‌آید:

- کاهش زمان فرآیند مناقصه‌گذاری
- ایجاد اطلاعات مدیریت کیفیت
- افزایش استقبال بازار

۱) collaborative tendering

- کاهش هزینه انجام مناقصه برای طرفین ذینفع
 - کاهش نیاز به فعالیت نیروی انسانی
 - افزایش یکپارچگی و شفاف سازی
 - امکان استاندارد سازی فرآیند و مستندات مناقصه
 - افزایش فرصتهای یکسان برای عموم مردم
 - اطلاع رسانی گسترده و متمرکز به عموم بصورت الکترونیکی
 - فرصت برای پاسخ گویی شفاف تر و بهتر به ابهامات موجود در زمان مناقصه
 - کاهش هزینه های در حال جریان مناقصات^۲ نظیر کاهش حجم مصرف کاغذ، کاهش در حجم فاکس و تلفن بین خریدار و شرکت کنندگان در مناقصه و کاهش پرینت
 - کاهش خطاهای ناشی از عدم انتقال کامل دیتا و نیز تهیه و تحلیل مدارک مناقصه
 - افزایش فرصتها جهت مقایسه اطلاعات کیفی و کمی و لذا ارزیابی سریعتر و دقیقتر شرکت کنندگان
- در این رابطه یک شرکت بطور نمونه، که به نوبه خود مناقصات محدود و عام بسیاری را برای واگذاری طراحی، خرید و اجرای جزیره های مختلف فنی-صنعتی و نیز خرید انواع خدمات و کالاهای عمومی برگزار می کند، بعنوان مناقصه گزار و نیز مدیریت پشتیبانی پایگاه الکترونیکی این سیستم انتخاب گردیده است.

شرایط و زمینه های لازم جهت انجام مناقصه گزاری الکترونیکی

- امضای الکترونیکی اسناد و مدارک تهیه شده توسط شرکت کنندگان در مناقصه توسط PKI (زیر ساختار کلید عمومی^۳) که توسط شرکت بازرگانی ایجاد کننده آن پشتیبانی شود و این شرکت توسط مناقصه گذار مورد تایید باشد.
- امضای الکترونیکی مدارک تهیه شده توسط مناقصه گذار که توسط PKI ایجاد و مدیریت می گردد و در مناقصات وابسته به دولت توسط PKI دولتی، مجوز اجرایی گرفته باشد.
- اصول سنتی برگزاری مناقصه را باید با استفاده از یک صندوق مناقصه مجازی^۴ حفظ کرد. کار این صندوق آن است که اجازه دسترسی به پاکات شرکت کنندگان را تا زمان ارسال تمامی پیشنهادات و یا اتمام مهلت مشخص تعیین شده ندهد.
- یکپارچگی^۵ مدارک مناقصه ذخیره شده از طریق استفاده از زیر ساختار فنی مناسب حفظ گردد.
- حفظ امنیت و دستورالعملهای بهره برداری مربوطه

امنیت در مناقصات الکترونیکی

۲) cost of running tenders 3)public key infrastructure ۴)virtual tender box 5)integrity 6)transparent

برای موفقیت این سیستم فرآیند آن باید عادلانه و روشن باشد تا جلوی هرگونه تبانی گرفته شود و لذا باید شامل مکانیزمهای امنیتی مناسب جهت افزایش قابلیت اطمینان سیستم باشند. از طرفی سیستمهای دارای مکانیزمهای امنیتی ویژه لزوماً نمی‌توانند نیازمندیهای قانونی برای عقد یک قرارداد الکترونیکی پیچیده را تامین کنند. عواملی نظیر آسانی جستجو و ترکیب کردن مدارک الکترونیکی، حذف و کپی و... از جمله عوامل مهمی است که یکپارچگی، کپی‌رایت و محرمانگی را به خطر می‌اندازد. عدم تماس فیزیکی در راه‌های الکترونیکی و لذا عدم توانایی برای اهراز هویت همیشه به عنوان اصلی‌ترین دلیل باعث صرف نظر بعلت سلب اعتماد مردم از این راه‌ها شده است.

مهمترین مشکل در این سیستمها امکان تبانی است و بارزترین نوع آن، امکان درز اطلاعات به علت عدم آب‌بندی سیستم است.

مساله دیگری که در اینجا مطرح می‌گردد، نحوه عمل و برخورد یکسان است. یکسانی برخورد با تمام شرکت‌کنندگان، رقابت عادلانه را ایجاد می‌کند که به نوبه خود منجر به صرفه‌بهینه اقتصادی جهت مناقصه‌گذار می‌گردد. این امر مستلزم فرآیند شفاف است که به خوبی مانیتور و رکورد شود. هدف مانیتور کردن جمع‌آوری شواهد و نیز آشکار سازی هرگونه تبانی است. با کمک شواهد یک قربانی ناشی از تبانی، می‌تواند به دنبال حفاظت حقوق قانونی خود باشد. رخنه غیر قابل ردگیری^۷، محرمانگی سیستم را از بین می‌برد. در این حالت استفاده بدون حفاظت از این سیستم در واقع زمینه‌ای ایجاد می‌کند که تبانیها بدون آشکار سازی، انجام می‌گردند. پس برای برقراری امنیت اطلاعاتی باید مهارت و معلومات هم‌فنی و هم‌قانونی به کار گرفته شوند. از طرفی یک سیستم امن با مکانیزمهای به‌عنوان مثال SSL و یا امضای الکترونیکی لزوماً نیازمندیهای قانونی را برآورده نمی‌کند. به‌عنوان مثال امضای الکترونیکی قابلیت بررسی و تایید برای طولانی مدت را پس از لغو کلید ندارد. خلاصه باید مطمئن بود که مطالب و مسائل قانونی بخشی از سیاستهای امنیتی است و این که امنیت بخشی از طراحی این سیستم است. پس تعریف صحیح امنیت، قدم اول طراحی یک سیستم موفق است.

فرآیند مناقصه‌گذاری استاندارد

فرآیند مناقصه‌گذاری سنتی بر همگان روشن است. در این بخش می‌خواهیم با توجه به این روال سنتی و قوانین، امکانات و محدودیتهای موجود به ارائه مدلی جهت شرکتهای مختلف مناقصه‌گزار ایرانی بپردازیم. در این مدل، مناقصه‌گزار خود دارنده سیستم و بهره‌بردار آن است. این مدل برای شرکت‌کنندگان نیز جالب توجه است، زیرا تنها به اینترنت جهت برداشت مدارک و نیز ارسال پیشنهادات نیاز دارد.

در این مدل، مناقصات خاص و عام هر دو نوع در نظر گرفته شده است.

در این راستا چند سناریو به شرح ذیل در نظر گرفته می‌شود:

- تعریف مناقصه در سیستم

۷) undetectable breach

در این بخش، مناقصه گزار که خود پشتیبان و بهره بردار سیستم نیز هست، به وارد کردن اطلاعات مربوط به مناقصه نظیر نام، نوع (اعم از محدود یا عام)، مهلت دریافت مدارک، مهلت ارسال پیشنهادات و تاریخ گشایش پاکات می پردازد.

- انتشار آگهی:

معرفی مناقصه عام در روزنامه های کثیرالانتشار بصورت آگهی سه سطری که در آن مناقصه گزار تنها به ذکر نام دستگاه مناقصه گزار، مختصری از موضوع مورد مناقصه و تاریخ مهلت ارسال پیشنهادات می پردازد و در انتهای آگهی اعلام می دارد که برای اطلاعات بیشتر به سایت مراجعه نمایند. همچنین این آگهی در سایت شرکت مناقصه گزار نیز قرار می گیرد. اما باید توجه کرد که بعلمت محدودیتهای قانونی نمی توان فقط به آگهی در سایت اکتفا کرد و وجود آگهی در روزنامه، الزامی است.

- ارزیابی کیفی و تهیه لیست مناقصه

مناقصه گذار در مناقصات محدود، بر اساس لیست سازمان برنامه و بودجه و امتیاز شرکتها در آن (در مناقصات ساختمانی) و یا لیست شرکت کنندگانی که پس از ارزیابی فنی و نیز توانایی های مالی، آنها را ارجح می داند، لیست مدعوین را تهیه می کند و برای آنها دعوت نامه میفرستد. این دعوت نامه شامل نام، شرح مختصری از پروژه، سه تاریخ مذکور در بالا و مبلغ و شماره حساب مربوط به خرید اسناد است.

همچنین در این دعوت نامه از شرکت کنندگان خواسته شده که قبل از مراجعه حضوری جهت خرید اسناد اقدام، فیش پرداخت توسط نماینده آنها به مناقصه گزار تحویل و درازای آن کدورمز عبور که فقط منحصر به آن مناقصه است و نیز کلید عمومی جهت رمز گشایی مدارک مناقصه پس از دریافت را تحویل گیرند. این کدورمز تا تاریخ گشایش پاکات معتبر است. خاطر نشان می گردد که خرید اسناد از روی اینترنت بعلمت عدم ارائه آن از سوی بانکها و پشتیبانی های لازم و نیز تمهیدات قانونی امنیتی، عملاً در حال حاضر امکان پذیر نمی باشد.

لازم به ذکر است که این بند فقط شامل مناقصات محدود است. لیست شرکتهایی که اظهار تمایل کرده اند به همراه کدورمز آنها در سیستم وارد و برای آن مناقصه در پایگاه داده، حفظ میگردد.

- قراردادن اسناد در دسترس شرکت کنندگان

در هنگام برگزاری مناقصه علاوه بر اینکه اطلاعاتی نظیر موارد شرح داده شده در بالا، در سایت قرار می گیرد، برای هر مناقصه سند نیز تهیه می گردد که حاوی شرایط و مشخصات مربوط به کالا یا خدمات مورد نیاز مناقصه گزار می باشد. مناقصه گزار این اسناد را بصورت pdf و zip وارد سیستم می نماید.

بنا به نوع مناقصه، این اسناد توسط عموم و یا فقط توسط دعوت شدگانی که اعلام تمایل کرده و کدورمز خود را دریافت کرده اند، قابل مشاهده و دسترسی است. اسناد مناقصات محدود با کلید مندرج در آیتم فوق، توسط مناقصه گزار، رمز شده است. دریافت اسناد مناقصات عمومی از طریق پایگاه الکترونیکی جهت علاقمندان به منظور فرهنگ سازی و نیز مشکلات پرداخت الکترونیکی که در بالا عنوان شد، رایگان است و مناقصه گزار فقط در صورتی که بخواهد پیشنهاد تهیه و ارسال کند، باید اقدام به خرید اسناد نماید.

همچنین جمله "دریافت اسناد از طریق سایت اینترنتی در صورت عدم ارائه پیشنهاد، رایگان می باشد" را در انتهای آگهی روزنامه ای خود اضافه می نماید.

به محض دریافت اسناد مناقصه، حسب نوع آن، اطلاعات مربوط به خریدار اسناد ثبت و مناقصه گزار می تواند اطلاعات آنها را مشاهده نماید.

از دریافت کنندگان اسناد مناقصات عمومی، درخواست می شود که اصطلاحاً پیش ثبت نام شوند و این پیش ثبت نام به منظور گرفتن آدرس الکترونیکی جهت دادن اطلاع به آنها در صورت ارسال متمم به سایت است.

از ثبت نام کامل آنها در این مرحله، به علت جلوگیری از افزایش حجم بی رویه پایگاه داده بعلمت مراجعات کنجکاوانه و کند شدن بهبود سیستم بدلیل حجم زیاد اطلاعات درخواستی خودداری می گردد.

- ارسال متمم

در صورت نیاز به هرگونه اصلاحیه و یا مدرک تکمیلی، به کلیه شرکت کنندگان فوق الذکر که اقدام به برداشت اسناد کرده اند، نامه الکترونیکی ارسال و جهت دریافت متمم از آنها دعوت بعمل می آید. دریافت اسناد یا متمم آنها فقط تا تاریخ مندرج در مرحله تعریف مناقصه امکان پذیر است، پس از این تاریخ، اسناد مناقصه از وضعیت فعال به بایگانی تغییر یافته و آرشیو می گردند.

- دریافت پیشنهادات

در این مرحله، با توجه به مهلت دریافت پیشنهاد، شرکت کنندگان مجاز (در مناقصه محدود) با وارد کردن کد و رمز و یا شرکت کنندگان عمومی پس از ثبت اطلاعات خود، می توانند پیشنهاد خود را بصورت الکترونیکی ارسال نمایند. او میتواند با کلید خود، پیشنهاد را امضاء و مهر الکترونیکی کرده سپس ارسال نماید. این کلید حتی در دسترس مپنا نیز نمی باشد. مرکز ارائه دهنده این کلید ها، بایستی مورد تایید مناقصه گزار باشد تا از هرگونه حملات احتمالی جلوگیری گردد. اطلاعات این پیمانکاران نیز به تناسب ذخیره می گردد.

در مرحله دریافت پیشنهادات، از پیمانکار مناقصه عمومی ثبت نام بعمل آمده و اطلاعات وی در پایگاه داده حفظ می گردد که بعداً قابل بازبینی و جستجو می باشد.

- گشایش پاکات

طبق تاریخ مندرج در تعریف مناقصه، در حضور نماینده سیستم و نیز اعضاء کمیسیون گشایش پاکات که در این شرکت فرضی سه تن هستند و وارد کردن کدورمز هر کدام از آنها و بررسی تاریخ توسط سیستم و بازبینی و بررسی ضمانتهای شرکت کنندگان در هر دو نوع مناقصه و دریافت فیش پرداختی جهت شرکت در مناقصه و خرید اسناد در مناقصات عام (خرید اسناد برای کسانی که پیشنهاد می دهند، الزامی است)، پاکات فنی و پیشنهادات قیمت پیمانکاران باز می گردد. از آنجایی که کلیه پیشنهادات توسط خود شرکتها مهر و موم الکترونیکی شده که کلید آن فقط در دسترس خود پیمانکار است، پیشنهادات بایستی پس از دریافت پیشنهاد از سیستم، توسط پیشنهاددهنده رمز گشایی گردد. صورتجلسه در حضور شرکت کنندگان بصورت دستی تهیه می گردد.

- اعلام نتیجه مناقصه

پس از مشخص شدن شرکت برنده مناقصه، مناقصه گزار صورتجلسه های اولیه و فنی (در صورت وجود) و صورتجلسه تعیین برنده مناقصه و نیز هویت وی (که در روز بازگشایی پاکات مشخص و تهیه گردیده است) را به آدرس شرکتهای پیشنهاد دهنده ارسال می کند.

بدین ترتیب اطلاعات کاملی از برندگان مناقصات مختلف نیز بصورت مجتمع جمع آوری می گردد.

طبیعت قانونی مناقصه

محدوده های قانونی اصلی که روی فرآیند مناقصه الکترونیکی تاثیر گذارند، بایدهایی را برای هر بخش و نیز طراحی سیستم ایجاد می کنند. این بایدها هستند که مشخص می کنند چطور هر بخش در فرآیند باید عمل کند. قوانین مربوط به عقد قرارداد، آزادی عمل اطلاعات، کپی رایت، تجارت و قوانین تبادلات الکترونیکی و نیز استانداردهای برگرفته شده از آنها بنا به اقتضای هر کشور باید در طراحی فرآیند مورد توجه قرار گیرند.

بایدها برای مناقصه گزار و سیاستهای در نظر گرفته شده برای آن

تمهیدات لحاظ شده در سیستم :	بایدها برای مناقصه گذار :
<p>➤ تهیه مدارک گویا و ارسال از طریق اینترنت و دسترسی کلیه شرکت کنندگان بنا به اقتضای نوع مناقصه به مدارک خوانا و واضح</p> <p>➤ دسترسی تمامی افراد حقوقی به اینترنت و لذا توانایی شرکت در مناقصات بنا به اقتضای نوع مناقصه</p> <p>➤ دعوت از شرکتهایی که در ارزیابی فنی مالی، مناسب تشخیص داده شده اند</p> <p>➤ تعریف زمان کافی در سیستم و امکان افزایش آن در نسختهای بعدی</p> <p>➤ ارسال مدارک مناقصات خاص که خود "فقط قابل خواندن" هستند، با امضاء و مهر و موم الکترونیکی و دادن کد و رمز به شرکت کنندگان ثبت نام شده در مناقصات محدود. در مناقصات عام، چون هر فرد حقوقی مجاز به شرکت می باشد، مدارک بصورت "فقط قابل خواندن" در سایت ارائه می گردد.</p> <p>➤ نیاز به ورود مسئول سایت و نیز اعضای کمیسیون و وارد کردن کد و رمز توسط آنها و نیز بررسی خودکار زمان در سیستم برای برداشت پیشنهاد و ثبت هر گونه دسترسی غیر مجاز در پایگاه داده</p> <p>➤ فقط ثبت قیمت پیشنهادی شرکت کنندگان در سیستم به جهت ارسال صورتجلسه گشایش پاکات به آنها</p> <p>➤ با تعیین دقیق محدوده های کاری و خدماتی در مدارک مناقصه و امتیاز بندی آنها</p> <p>➤ تهیه صورتجلسه از گشایش پاکات و ارسال به شرکت کنندگان حاضر</p>	<ul style="list-style-type: none"> ▪ تعریف روشن از پروژه و نیز مدارک مناقصه ▪ قابل دسترس بودن اطلاعات، برای شرکت کلیه شرکت کنندگان بالقوه ▪ ایجاد شرایط مساوی برای دعوت کلیه شرکت کنندگان بالقوه در مناقصه خاص ▪ دادن زمان کافی ▪ حفظ امنیت و محرمانگی مدارک ارسال شده ▪ عدم گشایش پاکات قبل از تاریخ مقرر ▪ عدم انتشار هرگونه اطلاعاتی از شرکت کنندگان غیر از قیمت آنها ▪ ارزیابی با شرایط یکسان مندرج در مدارک مناقصه برای همه ▪ رکورد کلیه مذاکرات گشایش پاکات

بایدها برای شرکت کنندگان و سیاستهای در نظر گرفته شده برای آن در سیستم

تمهیدات لحاظ شده در سیستم :	باید ها برای شرکت کننده:
<p>➤ تهیه لیست شرکت کنندگان و دعوت از آنان در مناقصات خاص .</p> <p>➤ صحت این امر در پیشنهاد وی مشخص و لذا قابل ارزیابی است.</p> <p>➤ ارسال پیشنهاد با ثبت اطلاعات و مشخصات وی در مناقصات عام و یا با دادن کد و رمز جهت ورود در مناقصات محدود. علاوه بر این پیشنهاد آنان باید "فقط قابل خواندن باشد: آنان می توانند علاوه بر امضاء الکترونیکی ، از هر نوع مهر و موم الکترونیکی ، بشرط قابل تایید بودن مرکز ارائه دهنده آن از سوی مناقصه گزار استفاده کنند.</p> <p>➤ استفاده از مهر الکترونیکی زمان و مهر تهیه کننده</p>	<ul style="list-style-type: none"> ▪ ارسال مدارک براساس ظرفیت و توانایی خویش ▪ ارزیابی کامل مدارک مناقصه گزار ▪ گوشزد آرام اشکالات در مدارک مناقصه به مناقصه گزار ▪ عدم ورود به فعالیتهای تبانی گرایانه ▪ حفظ محرمانگی در کلیه مراحل ▪ شرکت کننده مجاز به استفاده ، نگهداری ، کپی و باز تولید اطلاعات یا در اختیار قراردادن آنها به نفر سوم نیست

بایدها برای سیستم و سیاستهای در نظر گرفته شده برای آن در سیستم

تمهیدات لحاظ شده در سیستم :	بایدها برای اجرای سیستم الکترونیکی:
<p>➤ استفاده از کد و رمز عبور در مناقصات عام. انجام ثبت نام در مناقصات عام</p> <p>➤ "فقط قابل خواندن بودن " مدارک ، استفاده از امضاء الکترونیک</p> <p>➤ "فقط قابل خواندن بودن " مدارک مناقصه ونیز پیشنهادات ، استفاده از امضاء الکترونیک</p> <p>➤ در مناقصات خاص، استفاده از کد و رمز عبور. در مناقصات عام ،انکار از سوی پیشنهاد دهنده سودی برای وی و ضرری برای مناقصه گزار و سیستم در بر</p>	<ul style="list-style-type: none"> ▪ اهراز هویت شرکت کنندگان. ▪ محرمانگی و شخصی بودن مدارک، جهت اطمینان از آنکه فقط ، بخشهای درگیر ، توانا برای دیدن هستند. ▪ یکپارچگی مدارک، باید مدارک بدون تغییر نگهداری شود. ▪ انکار ناپذیری

ندارد. ثبت نام شرکت کننده و زمان برای برداشت مدارک مناقصه و ارسال پیشنهاد در پایگاه داده	
➤ سیستم ۲۴/۷ پیش بینی می شود. تکرار برداشت مدارک مناقصه و نیز ارسال پیشنهاد، قبل از اتمام زمان آن، بنا به نوع مناقصه، توسط شرکت کنندگان بلا مانع است.	▪ قابلیت دسترسی، دقت و کامل بودن مدارک

تطبیق نیازهای کسب و کار با سیاست های امنیتی

فرایند مناقصه ها و محدودیت های قانونی که در بالا مورد بحث قرار گرفت، مجموعه مشخصی از دستورالعمل ها هستند که مشخص می کنند در مجموعه اعمالی که در یک فرایند مناقصه الکترونیک صورت می پذیرند، چه چیزی مجاز است و چه چیزی مجاز نیست. این اعمال مجموعه مدارکی در طی زمان ایجاد می کنند که شامل بخش عمده ای از مدارک قرارداد نیز هست.

مدارکی که از لحاظ قانونی قابل استناد هستند مهمترین چیزی است که از طرفین درگیر در فرایند یک قرارداد چند میلیون دلاری بصورت قانونی حمایت می کند. این بخش باید با دستورالعمل های امنیتی لازم الاجرا در یک سیستم مناقصه الکترونیکی تطبیق داشته باشد. به این ترتیب می توان از تولید مدارک قانونی قابل استناد اطمینان حاصل کرد.

سیستم مناقصه الکترونیک مجموعه ای از کار بران، رسانه، اطلاعات و مجموعه عملیاتی است که کاربران را قادر می سازد در فرایند آن مشارکت داشته باشند. عملیات مختلف وضعیت سیستم مناقصه الکترونیک را تغییر می دهند. سیاست های امنیتی یک سیستم مناقصه الکترونیک مجموعه عملیاتی را مشخص می کنند که یک سیستم مناقصه الکترونیک را از یک وضعیت امن به یک وضعیت امن دیگر می برند. تهدیدها و تخلف های ممکن مجموعه عملیات هایی هستند که سیستم مناقصه الکترونیک را از یک وضعیت امن به یک وضعیت ناامن می برند. مکانیزم امنیتی سیستم مناقصه الکترونیک مجموعه مکانیزم هایی است که یا از تغییر وضعیت امن به غیر امن جلوگیری می کند یا این تغییر را کشف و ثبت می کند.

عنصر اصلی درگیر در سیستم مناقصه الکترونیک کاربران هستند که شامل مناقصه گران و اشخاص ثالث مورد اعتماد هستند. رسانه الکترونیکی شامل رسانه ارتباطی و پایگاه های داده است.

عملیات اصلی در یک سیستم مناقصه الکترونیک مستند سازی، ارزیابی، نگهداری مستندات و ارتباطات است. داده دیجیتالی جدید در طی فرایند مناقصه الکترونیکی در نتیجه تعامل کاربر با رسانه الکترونیکی و داده های دیجیتال قدیمی تولید می شود. نگهداری اسناد شامل ارزیابی اسناد، کپی کردن، پرینت گرفتن، تغییر و توزیع اسناد می باشد. این اعمال می توانند تاریخچه های دسترسی به اسناد برای سیستم مناقصه الکترونیک ایجاد کنند. برای یک سیستم مناقصه الکترونیک تهدیدها از دو ناحیه نشات می گیرند: فرایند مرسوم قدیمی و معرفی تکنولوژی الکترونیکی جدید. تهدیدها و سیاست های امنیتی در هر مرحله مورد بحث قرار می گیرند.

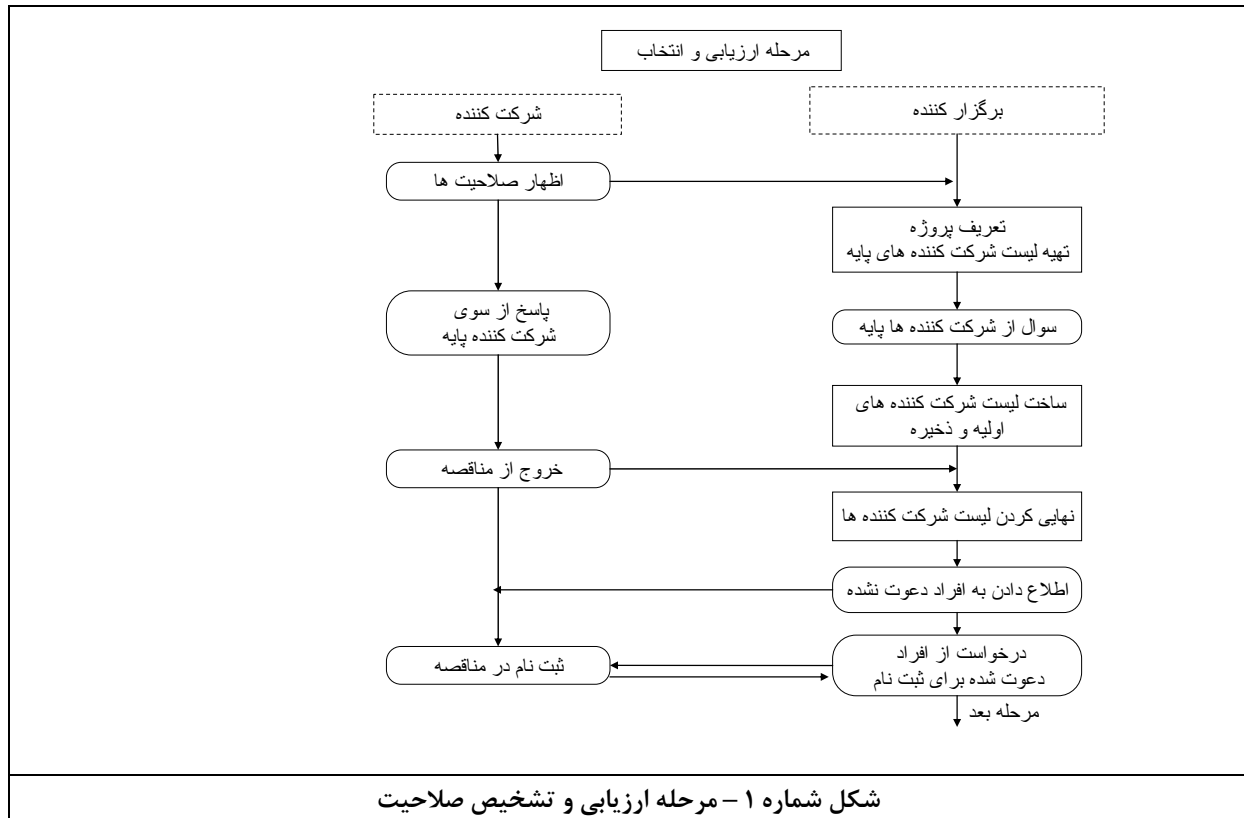
❖ مرحله ارزیابی و تولید لیست مناقصه کننده ها

هدف این مرحله تولید یک لیست نهایی از شرکت کننده ها در مناقصه از یک لیست مناسب از پیش تصویب شده است. شکل شماره ۱ فرایند و طرفین درگیر در این مرحله از مناقصه را نمایش می دهد. فلش های افقی نشان دهنده ارتباطات بین برگزار کننده و شرکت کننده در مناقصه می باشد. خطوط عمودی نشان دهنده قدم های فرایند کسب و کار می باشند. مستطیل ها

نشان دهنده فعالیت های داخلی می باشند. مستطیل های گوشه گرد فعالیت های ارتباطی را مشخص می کنند. برای استخراج لیست نهایی شرکت کننده ها سه چرخه انتخاب وجود دارد. برگزارکننده یک لیست پایه با توجه به مشخصات شرکت کننده در مناقصه (مشخصات فنی و مالی) تهیه می کند. بعد از سوال و جواب های اولیه یک لیست اولیه و یک لیست رزرو تهیه می کند. پس از دریافت تاییدهای نهایی از سوی شرکت کننده ها مبنی بر علاقه آنها برای شرکت در مناقصه لیست نهایی تهیه می شود. در مناقصه الکترونیک، باید از شرکت کننده های احتمالی درخواست کرد که بصورت رسمی در مناقصه ثبت نام کنند. این کار برای رسمی کردن کلیدها و فعالیت های ارتباطی جهت یک فرایند پیوسته انجام می شود.

مستندات اصلی که در این مرحله تولید می شوند شامل صلاحیت های شرکت کننده ها است که وارد سیستم شده است همراه با تعریف پروژه و لیست های شرکت کننده ها است که توسط برگزارکننده تهیه شده است. همچنین اطلاعاتی نیز از ثبت فعالیت ها بدست آمده است. از دیدگاه اجبارهای قانونی و فرایند کسب و کار، ما مجموعه از سیاست ها امنیتی را که برای این مرحله لازم است همراه با تهدیدهای مربوط به آن فراهم کرده ایم. چون سیاست های امنیتی محدودیت اعمالی است که طرفین در فرایند مناقصه می توانند انجام دهند، این سیاست ها در جدول ۱ به چهار دسته تقسیم شده اند.

سیاست های امنیتی مربوط به ارتباطات به شرح زیر هستند: تشخیص هویت طرفین ارتباط، ثبت تاریخ و زمان پیغام، اطمینان از عدم فاش نشدن ارتباط و عدم دستکاری پیغام. از تهدیدهای ممکن می توان جعل هویت، انکار پیغام، انکار زمان پیغام، استراق سمع و دست خوردگی پیغام را نام برد. برگزارکننده مناقصه باید از صحت توصیف پروژه مطمئن شود و از آنچه می تواند موجب گمراهی شود خودداری کند. در ارزیابی می بایست قواعد ارزیابی در مورد تمام شرکت کننده ها بطور منصفانه و بدون اعمال تبعیض به نفع شرکت کننده های مطلوب انجام شود. در نگهداری اسناد، برگزارکننده اسناد می بایست نسبت به صحت اسناد، حفظ محرمانگی و قابلیت استناد اسناد اطمینان حاصل کند. همه اطلاعات قبل از مناقصه باید برای تمامی شرکت کننده های احتمالی جدا از این که شرکت کننده مطلوب برگزارکننده باشند یا نه، فراهم باشد. وسایل ارتباطی غیر قابل اطمینان مستقیماً قابلیت استناد مدارک را زیر سوال می برند.



شکل شماره ۱ - مرحله ارزیابی و تشخیص صلاحیت

سیاست	تهدید
ارتباطات: تشخیص هویت طرفین ارتباط - ثبت مشخصات وی در سیستم ثبت تاریخ و زمان اطمینان به حفظ محرمانه ارتباط اطمینان از عدم خوردن پیغام اولیه - ارسال فکس	جعل هویت، انکار انکار زمان ارتباط استراق سمع دستکاری پیغام
اسناد: اطمینان از صحیح بودن توصیف	گمراه کننده بودن
ارزیابی: اطمینان از اعمال منصفانه و یکسان قواعد لیست های شرکت کننده ها تنها از شرکت کننده های صلاحیت دار تشکیل شده است	تبعیض به نفع شرکت کننده مطلوب تبعیض به نفع شرکت کننده مطلوب
نگهداری اسناد: اطمینان از این که توصیف پروژه یکسانی برای تمامی شرکت کننده ها ارسال شده است. اطمینان از صحت سند اطمینان از اعتبار و سندیت اطلاعات دیجیتال اطمینان از حفظ محرمانه اطلاعات دیجیتال	تبعیض به نفع شرکت کننده مطلوب نقض درستی اطلاعات جعل هویت، نقض حقوق دسترسی افشای اطلاعات محرمانه
جدول شماره ۱ - سیاست های امنیتی و تهدیدهای امنیتی در مرحله ارزیابی و تشخیص صلاحیت	

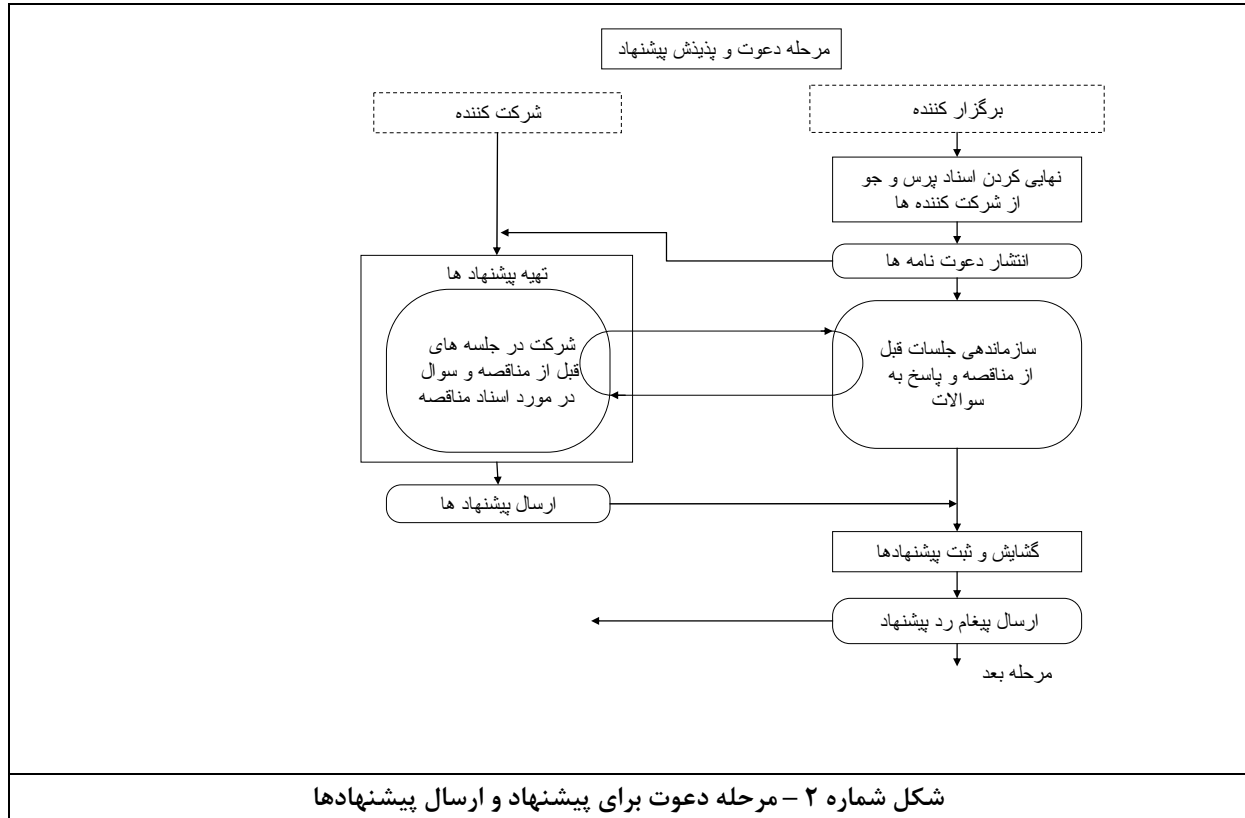
❖ مرحله دعوت برای پیشنهاد و ارسال پیشنهادها

این مرحله نقطه شروع فرایند قرارداد است و هر مرحله آن می‌بایست از لحاظ قانونی ثبت و مورد تایید قرار گیرد. در شکل شماره ۲ می‌بینید که برگزارکننده باید اسناد دعوت از شرکت کننده ها را کامل کرده و آنها را دعوت نموده و جلسات قبل از برگزاری مناقصه را تشکیل دهد و به هرگونه سوالی از سوی شرکت کننده ها پاسخ دهد. شرکت کننده ها باید اسناد خود برای شرکت در مناقصه را حاضر کرده و در محدوده زمانی مشخص شده ارسال کنند. بعد از ارسال پیشنهادها و مهلت ارسال، برگزارکننده پیشنهادها را با تاخیر را رد می‌کند، و پیشنهادهای وارده را ثبت و باز می‌کند.

اسناد اصلی که در این مرحله تولید می‌شوند شامل این اسناد هستند: اسناد مناقصه که توسط برگزارکننده تهیه شده‌اند، دعوت نامه های ارسالی برای شرکت کننده‌ها، اطلاعات جلسه‌ها، یادداشت‌ها و گزارشات کمیته ارزیابی، درخواست‌های پیشنهادها، پاسخ‌های شرکت کننده ها به نقاط مبهم پیشنهادها، اطلاع‌های رد پیشنهاد، تعاملات ثبت شده و اسناد پذیرفته شده شرکت کننده‌ها. برگزارکننده همچنین فعالیت‌هایی را برای پردازش این حجم فزاینده اسناد اضافه کرده است.

این مرحله‌ای است که برگزارکننده و شرکت کننده در فرایند عقد قرارداد وارد می‌شوند. بیشتر سیاست‌های امنیتی از مرحله اول به این مرحله منتقل می‌شوند تا از تشکیل مدارک قابل استناد از لحاظ قانونی اطمینان حاصل کنیم. برگزارکننده همچنین ناچار است از اتکاپذیری مکانیزم امضای دیجیتال، و اتکاپذیری مدارک قرارداد تولید شده از لحاظ قانونی در بلند

مدت اطمینان حاصل کند. همچنین برگزار کننده می‌بایست مطمئن شود که شرکت کننده قادر است اطلاعات را به نحو احسن مهوروموم و حفظ نماید. این سیاست های اضافه جهت مقابله با انکار امضا، لغو کلیدها و تبانی بین طرفین انجام می‌شود. سیستم غیر امن نه تنها قادر نیست مدارک قابل استناد جهت ارایه به دادگاه تولید و نگهداری کند، بلکه امکان تبانی را نیز در فرایند افزایش می‌دهد.



سیاست	تهدید
<p><i>ارتباطات:</i></p> <p>تشخیص هویت طرفین ارتباط - ثبت نام شرکت کننده عام ونیز کد و رمز عبور برای مناقصه خاص</p> <p>ثبت تاریخ و زمان در پایگاه داده</p> <p>اطمینان به حفظ محرمت ارتباط - رمز نگاری⁹</p> <p>اطمینان از حفظ صحت¹⁰ پیغام - "فقط قابل خواندن بودن پیغام"، رمز نگاری</p> <p>فرایند قابل اتکای امضای دیجیتال</p>	<p>جعل هویت، انکار</p> <p>انکار زمان ارتباط</p> <p>استراق سمع</p> <p>دستکاری پیغام</p> <p>انکار، مدرک غیر قابل استناد</p>
<p><i>اسناد:</i></p> <p>اطمینان از صحیح بودن اسناد و منصفانه بودن شرایط</p> <p>اطمینان از عدم دست خوردن و صحت سند - "فقط قابل خواندن بودن مدارک، رمز نگاری، مهر و موم الکترونیکی"</p>	<p>گمراه کننده بودن</p> <p>نقض درست.</p>
<p><i>نگهداری اسناد:</i></p> <p>اطمینان از این که اسناد مناقصه یکسانی برای تمامی شرکت کننده‌ها ارسال شده است. - فقط یک بار بارگذاری مدارک در سایت توسط مسئول سایت، سرویس ۲۴/۷، امکان تکرر در برداشت مدارک</p> <p>اطمینان از درستی و قابلیت اطمینان اسناد</p> <p>اطمینان از سندیت اطلاعات دیجیتال - "فقط قابل خواندن بودن مدارک، فرآیند قابل اتکای امضاء الکترونیک"</p> <p>اطمینان از حفظ محرمت اطلاعات دیجیتال - کد و رمز در مناقصات خاص، ثبت نام و کلیه مشخصات شرکت کننده در هر مرحله از ارتباط در پایگاه داده</p> <p>اطمینان از این که اسناد، مدارک قرارداد، اطلاعات تاریخچه فرایند بصورت بلند مدت قابل اثبات هستند - استفاده از کلید با ماندگاری طولانی¹¹</p> <p>اطمینان از این که کلیه اسناد شفاف سازی و اصلاحیه‌های اسناد مناقصه در دسترس تمامی شرکت کننده ها قرار دارد. - ارسال نامه الکترونیکی بصورت "فقط قابل خواندن" با امضاء الکترونیک به کلیه ثبت نام شدگان در مناقصه خاص (اعم از کسی که برای برداشت مدارک تاکنون اقدام کرده یا خیر) ونیز به آدرس ثبت شده کلیه برداشت کنندگان در مناقصات عام بصورت همزمان</p> <p>شرکت کننده اسناد پیشنهاد را بصورت مهر و موم شده ارسال کند.</p>	<p>تبعیض به نفع شرکت کننده مطلوب</p> <p>نقض درست اطلاعات</p> <p>جعل هویت، نقض حقوق دسترسی</p> <p>افشای اطلاعات محرمانه</p> <p>ابطال کلید ها</p> <p>تبعیض به نفع شرکت کننده مطلوب</p> <p>تبانی، افشای قیمت، نقض محرمت اطلاعات</p>

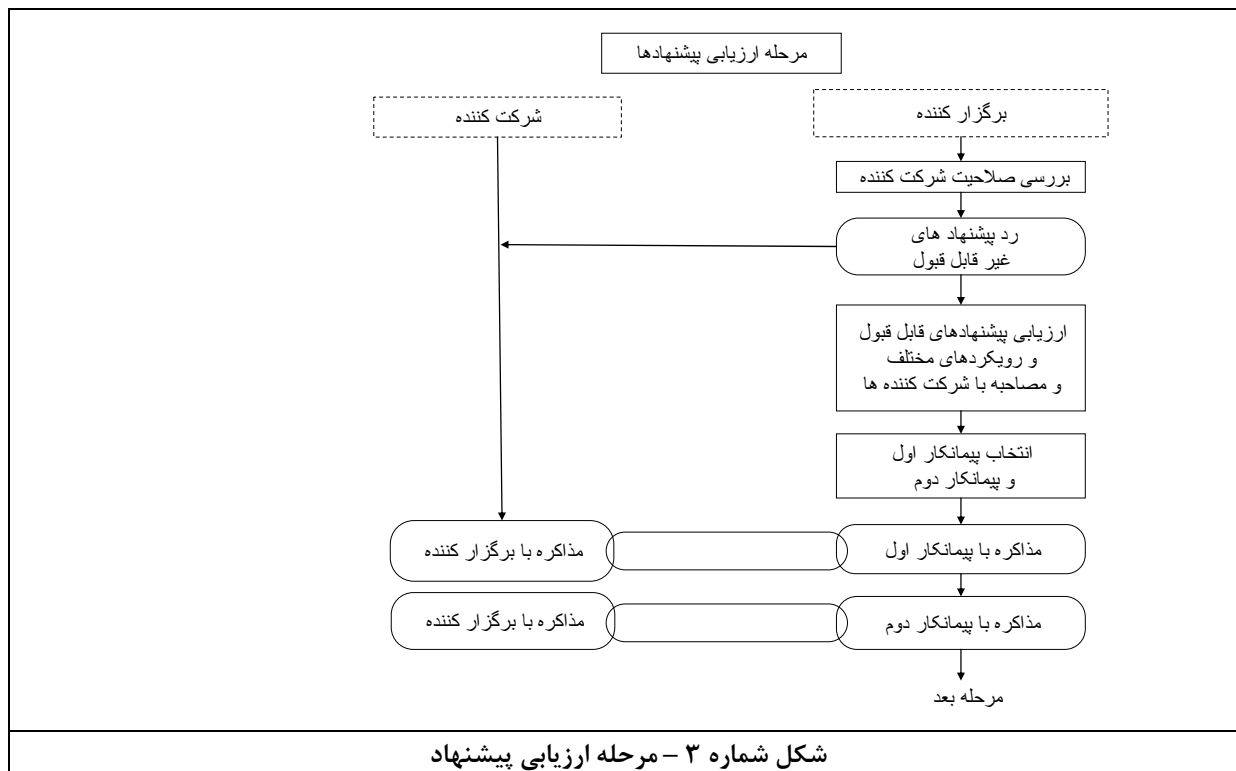
9)encryption

10)integrity

جدول شماره ۲ - سیاست های امنیتی و تهدیدات مرحله دعوت برای پیشنهادهای و ارسال پیشنهادهای

❖ مرحله ارزیابی پیشنهاد

در این مرحله برگزار کننده بر فرایند ارزیابی کنترل کامل دارد. در اغلب مواقع شفاف سازی شرایط قرارداد نیاز به مذاکرات پس از مناقصه دارد. به نوبه خود این کار می‌تواند باعث عقد قراردادهای سازش کارانه نیز شود. استراتژی امنیتی این مرحله افزایش قابلیت اتکا و شفافیت است همراه با قابلیت استناد قانونی. فعالیت های اصلی در این مرحله عبارتند از ارزیابی اسناد پیشنهاد ارسال شده، و انجام مذاکرات پس از مناقصه. شکل شماره ۳ نشان می‌دهد که برای ارزیابی، برگزارکننده باید صلاحیت شرکت کننده را چک کرده، پیشنهادهای ارسال شده و رویکردهای مختلف درون آنها را مورد ارزیابی قرار دهد. بعد از ارزیابی، برگزار کننده می‌تواند پیشنهاد پذیرفته شده اول، و پیشنهاد مطلوب بعدی را انتخاب کند. برای مذاکره، برگزار کننده ابتدا می‌بایست با شرکت کننده مطلوب اول مذاکره کند. در صورتی که شرکت کننده رد شود، برگزار کننده می‌تواند مذاکره را با شرکت کننده دوم شروع کند. برگزار کننده همچنین فعالیت‌های دیگری را نیز باید انجام دهد، مانند رد کردن پیشنهادهای غیر قابل قبول، ثبت تاریخچه فعالیت‌های انجام شده در فرایند پردازش دیجیتال اسناد. اسناد تولید شده در این مرحله شامل پیغام‌های اطلاع عدم پذیرش، نتایج ارزیابی، مذاکرات ضبط شده، و سایر اطلاعات ثبت شده است. همانند دو مرحله پیش، در این مرحله می‌بایست همان سیاست های امنیتی اتخاذ شود (جدول شماره ۳) تا در صورتی که کسی فرایند مناقصه را به مبارزه طلبید، برگزار کننده مناقصه قادر باشد مدارک قابل استناد برای اثبات قضایی ارائه کند. برای مذاکره در مورد قرارداد، بسته به آنچه که در اسناد مناقصه گفته شده است، این مرحله باید بتواند به طرفین کمک کند تا قدم‌های فرایند مذاکره مانند پیشنهاد، پیشنهاد متقابل و پذیرش را برای هر یک از مفاد مورد مذاکره تشخیص دهند. بدون پیمودن تمامی چرخه مذاکره در مورد قرارداد، برخی از مفاد معتبر نبوده و مسولیتی در قبال آنها متوجه طرفین نیست.



شکل شماره ۳ - مرحله ارزیابی پیشنهاد

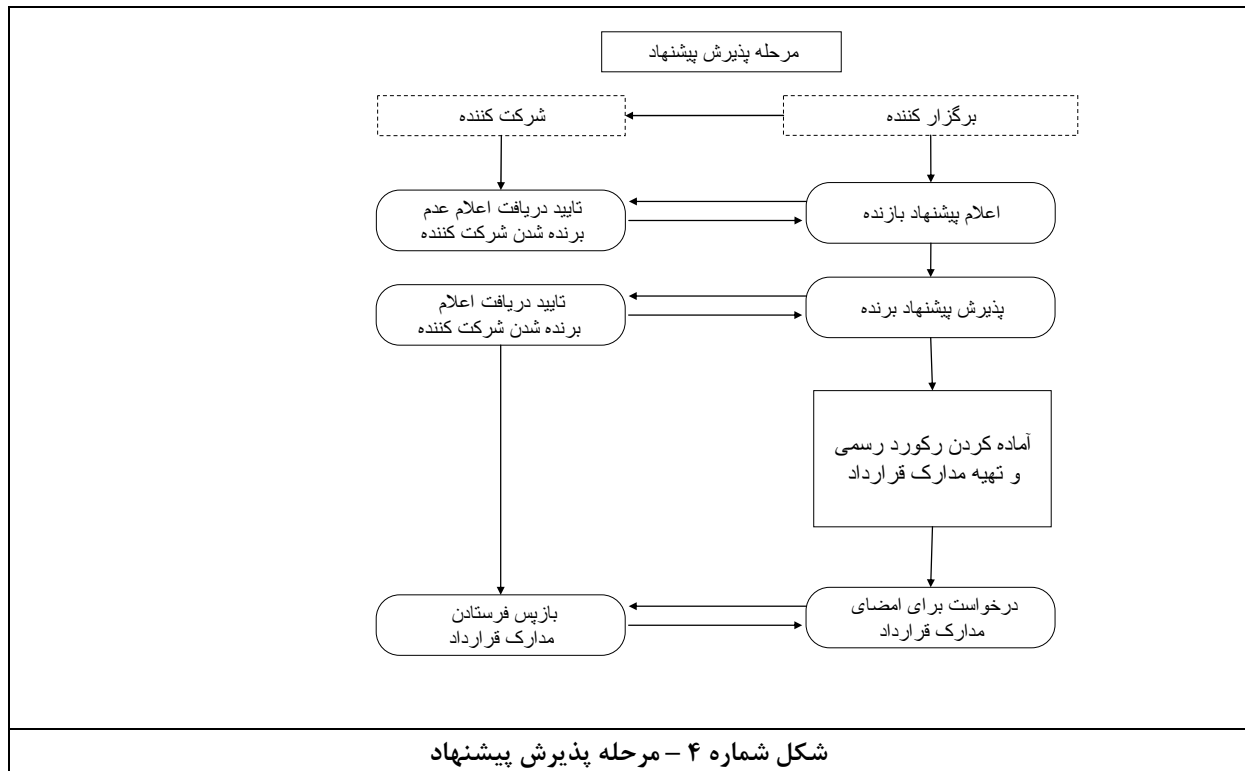
جدول شماره ۳ - سیاست امنیتی و تهدیدهای مرحله ارزیابی پیشنهادها

سیاست	تهدید
<p><i>ارتباطات:</i></p> <p>تشخیص هویت طرفین ارتباط ثبت تاریخ و زمان اطمینان به حفظ محرمت ارتباط اطمینان از حفظ صحت (integrity) پیغام محدود کردن مذاکره پس از مناقصه به تایید شرایط مفاد قرارداد پیمودن تمامی چرخه مذاکره در مورد مفاد قرارداد فرایند قابل اتکای امضای دیجیتال</p>	<p>جعل هویت، انکار انکار زمان ارتباط استراق سمع دستکاری پیغام تبانی، کاهش قیمت انکار مفاد قرارداد، عدم توافق در مورد مفاد انکار، مدرک غیر قابل استناد</p>
<p><i>اسناد:</i></p> <p>رسمی کردن هر بند مورد توافق و امضای آن فرایند قابل اتکای امضای دیجیتال</p>	<p>ستیزه و انکار انکار، مدرک غیر قابل استناد</p>
<p><i>ارزیابی:</i></p> <p>اعمال سیستم سنجش بصورت یکسان انتخاب پیشنهاد مطلوب اول و پیشنهاد مطلوب بعدی از میان پیشنهادهای مورد قبول</p>	<p>تبعیض به نفع شرکت کننده مطلوب تبعیض به نفع شرکت کننده مطلوب</p>
<p><i>نگهداری اسناد:</i></p> <p>برگزار کننده پیشنهادها را پس از اتمام مهلت یا پس از دریافت تمامی پیشنهادها باز کند. ثبت مشخصات فرد بازکننده همراه با زمان و شاهد آن تغییر قیمت مجاز نیست جلوگیری از افشای غیر مجاز اطلاعات (طراحی پیشنهادها) اطمینان از سندیت اطلاعات دیجیتال اطمینان از حفظ محرمت اطلاعات دیجیتال اطمینان از این که اسناد پیشنهادها صحیح و قابل اطمینان هستند اطمینان از این که اسناد، مدارک قرارداد، اطلاعات تاریخچه فرایند بصورت بلند مدت قابل اثبات هستند</p>	<p>نقض قوانین باز کردن نقض قوانین باز کردن نقض صحت (integrity) نقض محرمت، نقض قانون کپی رایت جعل هویت، نقض حقوق دسترسی افشای اطلاعات محرمانه نقض صحت (integrity) ابطال کلیدها</p>

❖ پذیرش پیشنهاد

این آخرین مرحله فرایند مناقصه است. فعالیت های این مرحله به این شکل اجرا می شوند که برگزار کننده بصورت رسمی برنده مناقصه را اعلام کرده و شرکت کننده هایی را که برنده نشده اند را نیز مطلع می کند. شرکت کننده رسیده دریافت اعلام برنده شدن خود را از برگزار کننده صادر می کند. برگزار کننده اطلاعات مربوط به انتخاب شرکت کننده برنده را بطور رسمی ثبت می کند و مدارک قرارداد رسمی را برای هر دوطرف به شکل فرم های استاندارد، جهت امضا آماده می کند. فرایند کسب و کار این مرحله در شکل ۴ نمایش داده شده است.

اسناد تولید شده در این مرحله عبارتند از اعلام رسمی برنده شدن شرکت کننده، اعلام و خلاصه توضیحات ارسالی به بازنده‌ها، رکورد رسمی فرایند مناقصه، مدارک امضا شده قرارداد و فعالیت های ضبط شده .
سیاست های امنیتی و تهدیدهای معمول برای این مرحله در جدول شماره ۴ آمده است. در جدول شماره ۴ ملاحظه می‌کنید که این مرحله ناگزیر است بیشتر سیاست‌های پایه گفته شده در مراحل قبل را اعمال کند. نیازمندی اصلی در این مرحله این است که مدارک قرارداد قابل اتکا در بلند مدت فراهم شود.



سیاست	تهدید
ارتباطات: تشخیص هویت طرفین ارتباط ثبت تاریخ و زمان اطمینان به حفظ محرمانه ارتباط اطمینان از حفظ صحت (integrity) پیغام فرایند قابل اتکای امضای دیجیتال	جعل هویت، انکار انکار زمان ارتباط استراق سمع دستکاری پیغام انکار، مدرک غیر قابل استناد
اسناد: تهیه مدارک رسمی قرارداد که توسط هر دو طرف امضا شده است تهیه گزارش رسمی فرایند مناقصه همراه با مدارک	انکار دعاوی در مورد روند، فرایند غیر شفاف
نگهداری/اسناد: اطمینان از صحت (integrity) مدارک قرارداد اطمینان از این که اسناد، مدارک قرارداد، گزارش فرایند مناقصه و مدارک بصورت بلند مدت قابل اثبات هستند	انکار، مدرک غیر قابل استناد

جدول شماره ۴ - سیاست امنیتی و تهدیدهای مرحله پذیرش پیشنهاد

مکانیزم‌های امنیتی ضروری برای مناقصه الکترونیک

تهدیدها نقض احتمالی مشخصه‌های امنیتی یا سیاست‌های امنیتی لازم در فرایند مناقصه الکترونیک هستند. مکانیزم‌های امنیتی ابزارهای تکنیکی برای اعمال سیاست‌های امنیتی هستند. بخش پیش نیازمندی‌های لازم جهت حفاظت در برابر تهدیدها مشخص شد. مکانیزم‌های امنیتی لازم در جدول شماره ۵ آمده است. این مکانیزم‌ها را می‌توان جهت حفاظت در برابر تهدیدهای امنیتی اصلی در سیستم مناقصه الکترونیک بکار برد.

تهدیدها	مکانیزم‌های امنیتی
پایه جعل عنوان استراق سمع انکار امضا انکار زمان امضا نقض صحت ^{۱۲} نقض حقوق دسترسی نقض محرمانگی اطلاعات ابطال کلید	احراز هویت حفظ محرمانگی مکانیزم امضای قابل اتکا برچسب زمان صحت کنترل دسترسی، نظارت مداوم امنیتی حفظ محرمانگی، کنترل دسترسی، نظارت مداوم امنیتی برچسب زمان
پیشرفته دعوی در مورد رویه دعوی در مورد مواد قرارداد فریب تبعیض به نفع پیمانکار مطلوب فرایند غیر شفاف نقض قوانین بازکردن پیشنهادها	مدارک زنجیره‌ای با برچسب زمانی مواد زنجیره‌ای با برچسب زمانی قابلیت اعتماد تشکل گروه مناقصه با الگوی اطلاعات امنیتی مشترک جهت افزایش اعتماد پذیری قابل اثبات عمومی ^{۱۳} الگوی قیمت دادن بصورت مهر و موم شده، حق دسترسی، نظارت مداوم امنیتی

جدول شماره ۵ - تهدیدهای معمول و مکانیزم‌های امنیتی لازم

از جدول‌های قبلی، می‌بینیم که تعدادی از نیازمندیهای امنیت و تهدیدات مرتبط با آنها، در بسیاری از مراحل مناقصه و دسته بندیهای عملیاتی لیست شده اند. این تهدیدات شامل تغییر هیئت، استراق سمع و نادیده گیری امضا می

12)integrity

13)public verifiability

باشند. که تهدیدات پایه ای را برای سیستم مناقصه ایجاد می کنند و نیاز دارند که سیستم سرویسهای امنیتی اصولی بیشتری را مثل اهرزهویت، محرمانگی، یکپارچگی و طرح امضای قابل اعتماد را ایجاد کند. برای مثال، یک استراق سمع کننده ارتباطات ناامن را می تواند مونیور کرده و اطلاعات ارزشمندی را جمع آوری کند. آنها همچنین ممکن است که از رموز عبور برای نقش یک مسئول با مجوز اجرایی را بازی کردن، استفاده کنند تا اینکه اطلاعات محرمانه را بدزدند یا یکپارچگی مدرک از بین ببرند. باقراردادن این مکانیزمهای امنیتی پایه، یک سیستم می تواند سرویسهای امنیتی پیشرفته تری را ایجاد کند همانند طرح اشتراک رمز^{۱۴} برای افزایش اعتبار مناقصه و نیز زنجیره زمانی مذاکرات و عناوین قراردادی^{۱۵} اینها برای یک سیستم مناقصه الکترونیکی قابل اعتماد ضروری هستند. برای مثال یک عنوان قراردادی نامعتبر در هر کدام از حالات ذیل ممکن است اتفاق بیفتد:

عدم تشخیص درست و کامل فرادامضا کننده، یکپارچگی اولیه نقض شده، یکپارچگی اولیه پس از ابطال کلیدها قابل بررسی نباشد و یا آنکه فرآیند قرارداد کامل نباشد.

سه دسته اول به وسیله مکانیزمهای امنیتی اولیه مثل اهرزهویت، طرح امضاء قابل اعتماد و طرح مهر با زمان^{۱۶} پیش گیری می گردند.

دو نوع بعدی، بهر حال نیازمند طرحهای پیچیده تری هستند مثل زنجیره زمانی مذاکرات قراردادی^{۱۷}

منابع و مراجع

۱. سیستم مناقصه گزاری الکترونیکی کشور، محمد تقی عیسیایی، سنا مژده، به رخ لوایی، علی شمس

14)secret sharing scheme

15) time chaining contract negotiations & terms

16) time stamp scheme

17) time stamped chain of contract negotiations