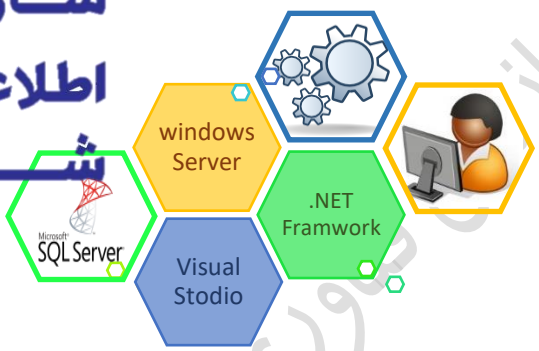
سازمان فناوری اطلاعات و ارتباطات شهرداری قم

Q.M.i.C.T.O



دستورالعمل

احراز هویت و دسترسی

کاربران برنامه های نرم افزاری

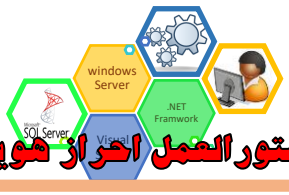
شهرداری قم

Qom Municipality

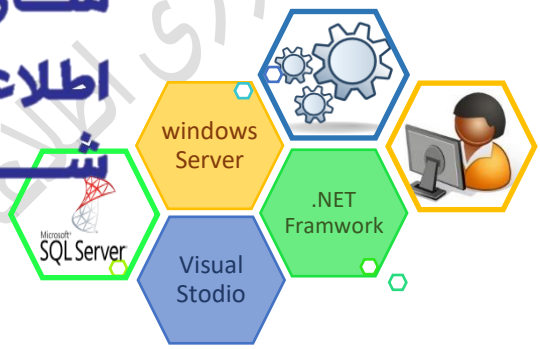
User Authentication & Authorization Plan

شناسنامه

کد شناسه :	APD.IT.STD.004
تاریخ انتشار :	۱۳۹۷/۰۴/۱۲
شماره ویرایش :	F02
تهیه :	کورش محمدحسینی
تایید :	حیدر مرتضوی
تایید نهایی :	کورش محمدحسینی
تصویب :	همایون یزدانپناه



سازمان فناوری اطلاعات و ارتباطات شهرداری قم
Q.M.i.C.T.O



فصل اول

اهداف و تعاریف

۱. هدف

این سند به منظور تعیین معماری، روش ها و الزامات احراز هویت کاربران برنامه های نرم افزاری در شهرداری قم تدوین شده است. و براساس آن هر برنامه نرم افزاری (اپلیکیشن، سرویس، سیستم، سامانه، پرتال، وب سایت، و امثالهم) مرتبط با شهرداری قم و اجزاء تابعه آن می باید در حوزه احراز هویت کاربران، واجد این الزامات باشند.

۲. دامنه کاربرد

الزامات ارائه‌شده در این سند، معیارهای قابل پذیرش در حوزه احراز هویت کاربران برنامه های نرم افزاری در تمامی پروژه‌هایی است که بصورت کامل یا جزئی، دارای بخش های نرم‌افزاری می باشند، و از این منظر، دامنه آن شامل هیچگونه محدودیتی از نظر حجم پروژه، نوع نرم افزارها، نوع کاربرد، تعداد کاربران، متدولوژی، چهارچوبه (Framework)، سکو (Platform)، بانک اطلاعاتی و غیره، نمی باشد

در طول سند، هر زمان نیاز بوده است، استثنائات، و یا خصوصیات ویژه ای را، براساس شرایط خاص برنامه های نرم افزاری و یا ویژگی های آنها، به دقت در نظر گرفته شده است که منحصر به همان موارد بوده و قابل تفسیر و شمول به کلیت سند نبوده و جامعیت دامنه کاربرد آن را محدود نمی سازد

۳. تعاریف

در نگارش این سند، از اصطلاحات زیر استفاده شده است :

۳,۱. *پروژه :* منظور از پروژه در این سند، هر پروژه فناوری اطلاعات و ارتباطات است که منجر به تولید یا استفاده از یک برنامه نرم افزاری در شهرداری قم و یا یکی از اجزاء تابعه آن بشود

۳,۲. *برنامه نرم افزاری* : در این مستند هر جا از این واژه استفاده می شود منظور هر سیستم نرم افزاری، اپلیکیشن، سرویس، سیستم، سامانه، پرتال، وب سایت، و امثالهم است که قرار است در حوزه کارفرما یا دستگاه نظارت و یا تحت نظر کارفرما و یا دستگاه نظارت راه اندازی گردد

۳,۳. *احراز هویت* ***Authentication*** : مجموعه عملیاتی است که طی آن بررسی و راستی آزمایی مربوط به نام کاربری و گذواژه وارد شده توسط کاربران، انجام می شود. این عملیات معمولا در ابتدای ورود کاربر به برنامه انجام شده و نتیجه آن صدور مجوز ورود یا عدم ورود کاربر درخواست کننده به برنامه نرم افزاری می باشد. در حال حاظر سرویس **Active Directory** در شهرداری قم این فرآیند را به عهده دارد

۳,۴. *سرویس احراز هویت متمرکز* ***CAS*** *(Central Authentication Service)* : یک سرویس نرم افزاری با یکی از استانداردهای رایج است که توسط دستگاه نظارت آماده سازی شده و قابلیت تعریف کاربران و مدیریت آنها را دارا میباشد. این سرویس می تواند **Active Directory** یا هر سرویس دیگری باشد که دستگاه نظارت اعلام نماید

۳,۵. *تعیین سطوح دسترسی* ***Authorization*** : مجموعه عملیاتی است که طی آن مشخص می شود که چه کاربرانی به چه بخش هایی از برنامه نرم افزاری، چه نوع دسترسی باید داشته باشند و همچنین شامل اعمال این دسترسی ها برای کاربران مورد نظر می باشد

۳,۶. *مستندات* : کلیه مدارک و اسناد کاغذی یا الکترونیکی است، که در جریان اجرای پروژه ایجاد می گردد. مانند: مکاتبات انجام شده بین طرفین و دستگاه نظارت، ابلاغیه ها، اخطاریه ها، صورتحسابها، صورتجلسات، مستندات فنی، مستندات آموزشی و ...

۳,۷. *کارفرما* : منظور از کارفرما در این مستند شهرداری قم یا یکی از اجزاء آن می باشد

۳,۸. *مجری* : شخص حقوقی یا حقیقی که برنامه نرم افزاری یا خدمات نرم افزاری را به کارفرما ارایه می نماید

۳,۹. *دستگاه نظارت* : منظور از دستگاه نظارت در این مستند، سازمان فناوری اطلاعات و ارتباطات شهرداری قم می‌باشد که وظیفه نظارت بر عملکرد مجری را برعهده دارد و کلیه مراسلات و مکاتبات و ابلاغیه ها توسط وی انجام شده و کلیه پرداخت ها می باید با تایید وی صورت پذیرد

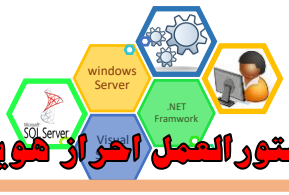
۳,۱۰. *کاربر* : هر فرد حقیقی است (اعم از کارکنان و مستخدمین کارفرما و یا دستگاه نظارت، شهروندان، مشتریان و ذی نفعان برنامه های نرم افزاری) که بهره بردار و یا استفاده کننده از یک برنامه نرم افزاری می باشد

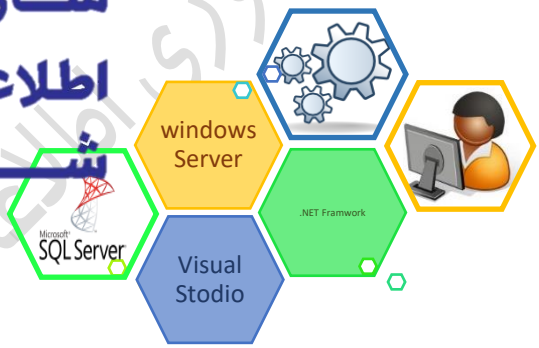
۴. منابع و مراجع

۴,۱. Microsoft MSDN

۴,۲. منابع و مستندات اصول مهندسی سیستم های نرم افزاری

۴,۳. روش های مرسوم و روال های تجربی سیستم های نرم افزاری معتبر





فصل دوم

معماری

در این فصل ابتدا فارغ از اینکه چه برنامه نرم افزاری مخاطب این سند می باشد، به تشریح معماری قابل قبول (معماری مطلوب) ساختار سطوح دسترسی در یک برنامه نرم افزاری می پردازیم، سپس در فصل سوم به این موضوع خواهیم پرداخت که برنامه های نرم افزاری قابل پذیرش، در رابطه با این معماری مطلوب، چه قابلیت هایی را باید داشته باشند

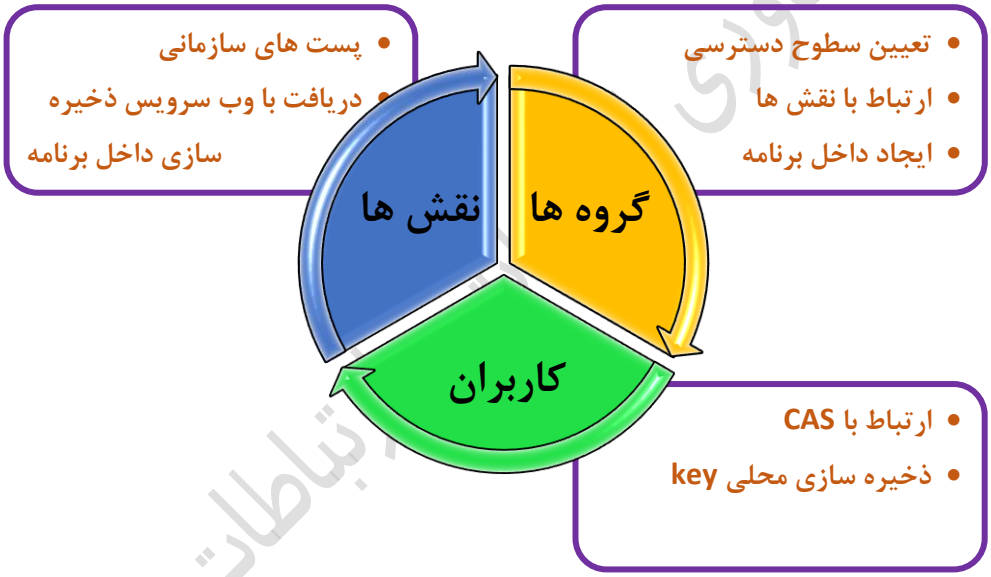
۱. معماری مطلوب

سطوح دسترسی در معماری مطلوب، می بایست دارای سه سطح به شرح ذیل باشد :

۱,۱. سطح نقش ها ← پست ها یا جایگاه های سازمانی

۱,۲. سطح کاربران ← ارتباط با افراد

۱,۳. سطح گروه ها ← تعریف دسترسی ها



۲. معماری مطلوب Authentication

احراز هویت کاربران (**Authentication**) در معماری مطلوب، شامل آیتم های اساسی زیر است :

۲,۱. برنامه های نرم افزاری برای برای شناسایی و احراز هویت کاربران، از سرویس **CAS** به صورت **OnLine** استفاده می کنند

۲,۲. در این روش، هر برنامه نرم افزاری در ابتدای ورود کاربران (**Log-in**) نام کاربری و گذرواژه وارد شده توسط کاربر را با استفاده از وب سرویس به سمت سرویس دهنده ی **CAS** ارسال میکند و در صورت دریافت تاییدیه اصالت اطلاعات وارد شده، به کاربر اجازه ورود به برنامه را می دهد

۲,۳. در این معماری، برنامه های نرم افزاری اطلاعات کاربری کاربران (شامل : نام کاربری، گذرواژه و ...) را در دیتابیس های خود ذخیره سازی نمی کنند، و فقط یک کلید ارتباطی از مجوز (**Account**) هر کاربر را ذخیره سازی کرده و سایر اطلاعات به صورت کاملا **OnLine** بررسی و اصالت سنجی می شوند

۳. معماری مطلوب Authorization

تعیین سطوح دسترسی کاربران (**Authorization**) در معماری مطلوب، شامل آیتم های اساسی زیر است :

۳,۱. هر برنامه نرم افزاری دارای ساختار داخلی خود برای تنظیم سطوح دسترسی می باشد

۳,۲. در این روش، پس از احراز هویت کاربر و ورود وی به برنامه نرم افزاری، براساس تنظیماتی که برای وی انجام شده است به بخش های مشخص شده ای از برنامه دسترسی مشخص شده ای اعطا می شود

۳,۳. در این روش، برای تعیین جزئیات سطوح دسترسی از گروه ها استفاده می شود، به این معنی که ابتدا گروه های دسترسی در برنامه تعریف و برای هر کدام از آنها سطح دسترسی خاص آن گروه تعیین می گردد

۳,۳,۱. در شرایط خیلی ویژه در مورد برنامه های نرم افزاری بسیار کوچک و با درجه اهمیت بسیار پایین، با تعداد کاربر زیر ده نفر و در صورت موافقت دستگاه نظارت، تعریف اجزاء سطوح دسترسی می تواند مستقیما برای کاربران انجام شود و چنین برنامه های نرم افزاری می توانند فاقد مفهوم گروه در معماری سطوح دسترسی باشند

۳,۴. سپس مشخص می شود که هر یک از پست های سازمانی (نقش ها) به کدام گروه دسترسی تعلق دارند. به این صورت جزئیات سطوح دسترسی هر پست سازمانی تعیین میشود

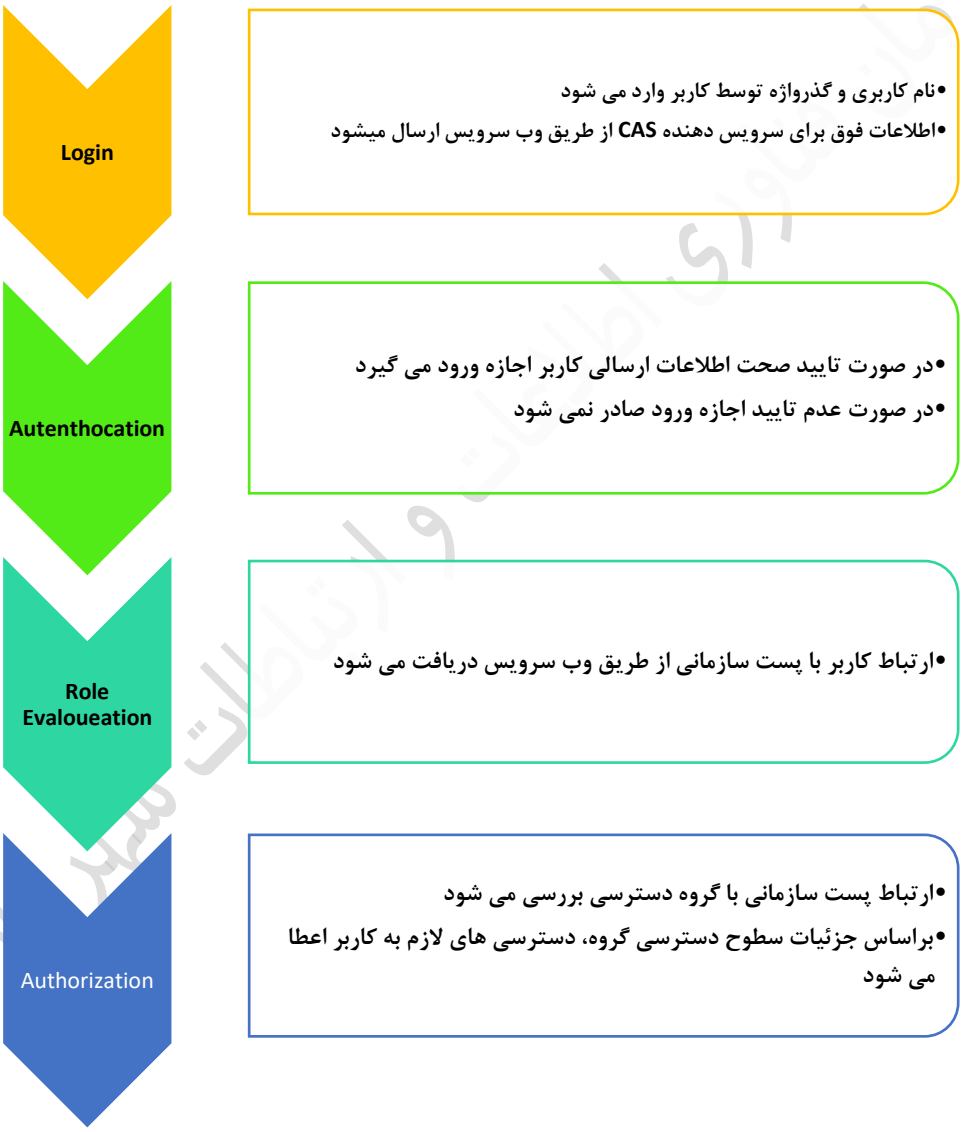
۳,۵. سپس مشخص می شود که هر پست سازمانی (نقش) متعلق به کدام کاربر است، به این ترتیب جزئیات سطوح دسترسی هر کاربر مشخص می شود

۳,۶. فرآیندهای فوق ممکن است به صورت دستی و یا در صورت تامین زیرساخت های لازم (وب سرویس ها) به صورت خودکار به شرح ذیل انجام شوند :

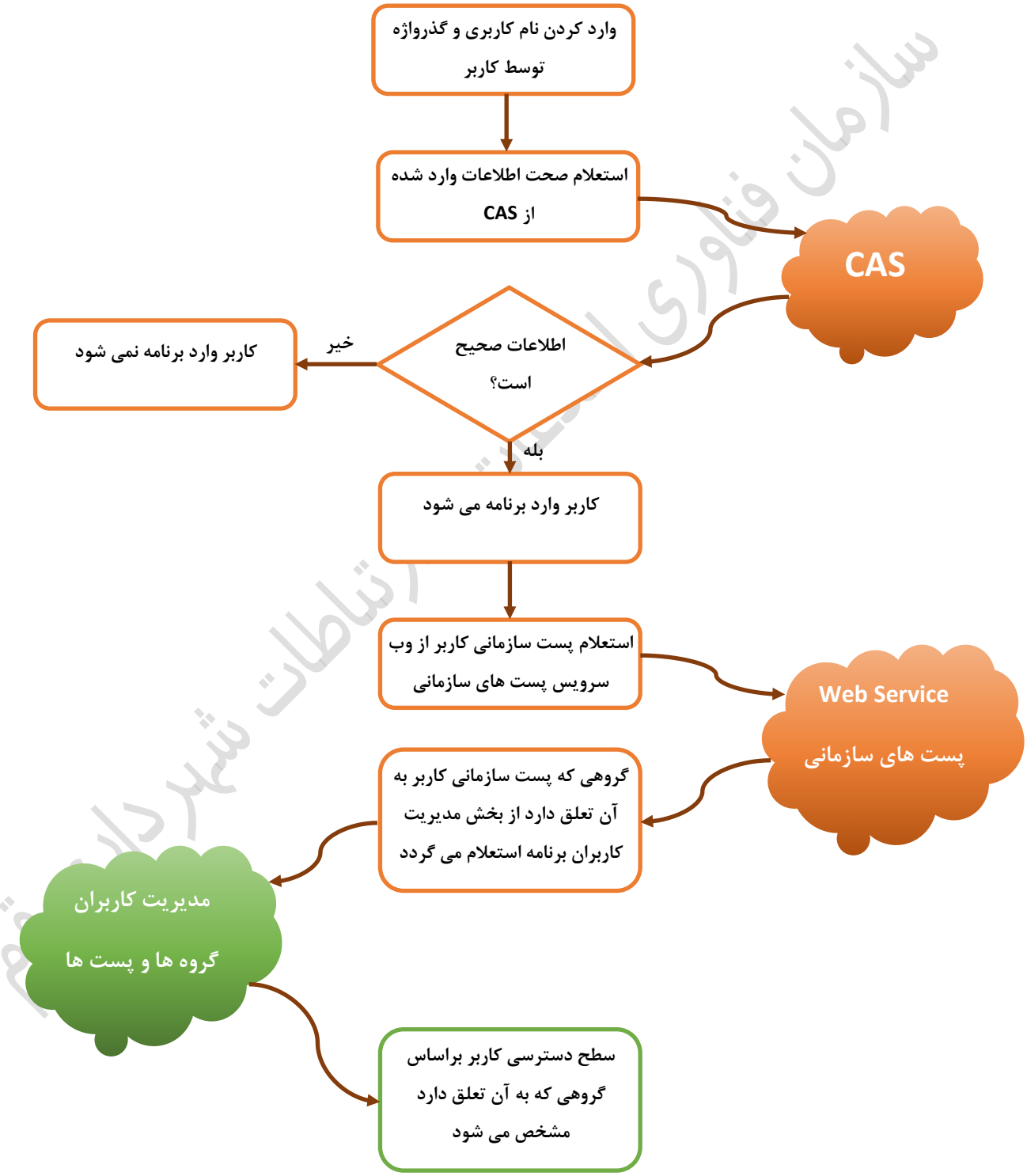
۳,۶,۱. برای ایجاد و بروزرسانی ساختار پست های سازمانی به جای روش دستی در برنامه نرم افزاری، می توان از وب سرویس چارت و تشکیلات سازمانی که توسط برنامه نرم افزاری منابع انسانی (یا مشابه آن) ارایه می شود استفاده نمود

۳,۶,۲. برای مشخص کردن ارتباط هر پست سازمانی با کاربر مربوط به آن به جاری روش دستی می توان از وب سرویس ابلاغ ها که توسط برنامه نرم افزاری کارگزینی (یا مشابه آن) ارایه می شود استفاده نمود

۳,۷. دیاگرام ارتباطی دسترسی ها در سه سطح مربوطه را در نمودار زیر قابل مشاهده است :



مراحل احراز هویت و تعیین سطوح دسترسی یک کاربر



فصل سوم

الزامات

۱. قابلیت تعریف نقش ها (الزامات Authorization)

۱,۱. قابلیت تعریف نقش ها براساس ساختار درختی (ایجاد چارت سازمانی) وجود داشته باشد. در این مستند نقش ها معادل پست های سازمانی که در ساختار سازمانی وجود دارند در نظر گرفته می شوند. این ساختار سازمانی توسط، دستگاه نظارت به مجری اعلام خواهد شد

۱,۲. در صورت اعلام دستگاه نظارت و ارایه وب سرویس چارت (ساختار) سازمانی، می بایست ساختار سازمانی و پست های مورد نظر از طریق وب سرویس مذکور دریافت و در دیتابیس برنامه نرم افزاری، ذخیره شود

۱,۳. می باید همواره، آخرین وضعیت ساختار سازمان از طریق وب سرویس مذکور و در زمانبندی های قابل تنظیم در قسمت تنظیمات، بروزرسانی شود (Automatic Scheduled Syncing)

۱,۴. پس از هر بار Sync شدن فوق، ارتباط کاربران تعریف شده در برنامه نرم افزاری، با پست های سازمانی مجددا بررسی و تغییرات جدید اعمال شود و با توجه به آن به صورت اتوماتیک سطح دسترسی کاربران تغییر پیدا کند، بطور مثال: زمانی که کاربری در کارگزینی مشغول بکار است و جایگاه کارشناس کارگزینی در ساختار سازمانی برای وی در نظر گرفته شده است، براساس نقشی که برای وی در برنامه نرم افزاری، در نظر گرفته شده و همچنین تنظیمات برنامه، به گروه کاربران کارگزینی متصل است، و هنگامی که وب سرویس ساختار سازمانی اعلام می کند که جایگاه وی تغییر و به عنوان کارشناس در حوزه مالی مشغول بکار شده است، می باید به صورت خودکار دسترسی وی به گروه کاربران مالی تغییر نماید. در صورتیکه برنامه نرم افزاری، بر اساس کارتابل عمل می کند می باید به صورت خودکار دسترسی کارتابل قبلی از وی گرفته شده و دسترسی کارتابل جدید به وی داده شود

۱,۵. قابلیت اتصال کاربران به نقش ها وجود داشته باشد. هر کاربر را باید بتوان به چندین نقش به صورت همزمان مرتبط کرد. اما هر نقش در یک زمان فقط به یک کاربر باید متصل شود

۱,۶. ترجیحا، قابلیت ارتباط یک نقش به چند کاربر دیگر غیر از کاربر اصلی، نیز تحت عنوان نقش تفویض شده وجود داشته باشد. در این حالت تمام فعالیت های کاربری که دارای تفویض است، با نشانه گذاری مناسب مشخص شود. همچنین امکانات لازم برای تفویض دسترسی وجود داشته باشد

۱,۷. در حالت غیرمتصل به وب سرویس ساختار سازمانی، امکان حذف هر نقش می بایست وجود داشته باشد لیکن بررسی شود که کاربری به آن نقش متصل می باشد یا نه و در صورت اتصال با نمایش پیام مناسب از حذف جلوگیری شود. همچنین در صورتیکه نقش مورد نظر دارای سابقه اثری در برنامه نرم افزاری، می باشد و یا اگر برنامه نرم افزاری، به صورت کارتابلی کار می کند و در آن کارتابل مواردی وجود دارد و یا سابقه گردش مستندات از آن کارتابل وجود دارد، امکان حذف نباید وجود داشته باشد و فقط باید بتوان آن نقش را غیر فعال کرد

۱,۸. در حالت متصل به وب سرویس ساختار سازمانی، حذف و یا غیرفعال سازی نقش ها از طریق سرویس دهنده وب سرویس انجام می گردد. در همین راستا برنامه نرم افزاری، باید واجد وب سرویس هایی برای پاسخگویی به درخواست سرویس دهنده در خصوص وجود اثر و یا سابقه فعالیت نقش مورد نظر باشد

۲. قابلیت تعریف گروه ها (الزامات Authorization)

۲,۱. قابلیت تعریف گروه ها (ترجیحا به صورت ساختار درختی) در برنامه نرم افزاری، باید وجود داشته باشد

۲,۲. قابلیت تعیین سطوح دسترسی، در حد مورد نیاز (فرم ها، گزارشات، روال ها، فیلدها و در صورت نیاز رکوردها) برای هر گروه وجود داشته باشد

۲,۳. انواع دسترسی های مورد نیاز، شامل چهار سطح (CRUD) به شرح ذیل هستند :

۲,۳,۱.ایجاد Create

۲,۳,۲.مشاهده Read

۲,۳,۳. ویرایش Update

۲,۳,۴.حذف Delete

۲,۴. منظور از سطوح دسترسی به فرم ها اینست که چه گروهی از کاربران، به چه فرم هایی، دسترسی ایجاد، و یا مشاهده و یا ویرایش و یا حذف را داشته باشند (بطور مثال : فرم صدور سند)

۲,۵. منظور از سطوح دسترسی به گزارشات اینست که چه گروهی از کاربران، به چه گزارشاتی، دسترسی ایجاد، و یا مشاهده و یا ویرایش و یا حذف را داشته باشند (بطور مثال : گزارش بیلان مالی)

۲,۶. منظور از سطوح دسترسی به فیلدها اینست که چه گروهی از کاربران، به چه فیلدهای اطلاعاتی، دسترسی ایجاد، و یا مشاهده و یا ویرایش و یا حذف را داشته باشند (بطور مثال : دسترسی مشاهده یا تغییر فیلد ضریب حق مسئولیت). این قابلیت ترجیحا باید، برای تمامی فیلدهای برنامه نرم افزاری وجود داشته باشد. (با موافقت دستگاه نظارت شمول این قابلیت می تواند به فیلدهای کلیدی تقلیل پیدا کند. در چنین شرایطی لیست فیلدهای کلیدی می بایست به تایید دستگاه نظارت برسد)

۲,۷. منظور از سطوح دسترسی به روال ها اینست که چه گروهی از کاربران، دسترسی انجام چه روال هایی در سیستم را داشته باشند (بطور مثال : دسترسی به فرآیند صدور چک) این قابلیت برای تمامی روال ها و فرآیندهای برنامه نرم افزاری، می بایست وجود داشته باشد

۲,۸. منظور از سطوح دسترسی به رکوردها اینست که چه گروهی از کاربران، دسترسی به چه بخشی از اطلاعات را داشته باشند و چه بخش هایی را نداشته باشند. این قابلیت ترجیح موکد است و در شرایطی براساس اعلام نیاز حوزه بهره بردار ممکن است به الزام تبدیل شود (بطور مثال : کاربران مالی شهرداری منطقه یک فقط به اسناد مربوط به منطقه خود دسترسی داشته باشند)

۲,۹. قابلیت حذف گروه ها در سامانه می بایست وجود داشته باشد، لیکن در هنگام حذف، بررسی شود که نقشی به آن متصل نشده باشد و دارای زیرگروه هم نباشد. در غیر اینصورت ضمن نمایش پیام مناسب از حذف آن جلوگیری شود

۲,۱۰. در صورت اعلام دستگاه نظارت و ارایه سرویس متمرکز Authorization (بطور مثال : NetSqlAzMan) می بایست بر اساس متدهای ارایه شده مربوطه، در این خصوص اقدام گردد. بطور معمول این روال ها شامل ایجاد ارتباط فیمابین برنامه نرم افزار و سرویس مذکور، تعریف سطوح دسترسی در آن سرویس، و فراخوانی مجدد سطوح دسترسی مربوطه در اجزاء مختلف برنامه نرم افزاری، از سرویس Authorization است

در چنین حالتی اطلاعات مربوط به این موضوع نمی باید در دیتابیس برنامه نرم افزاری ذخیره شوند، تمامی اطلاعات مربوط به این موضوع می باید در دیتابیس سرویس متمرکز **Authorization** ذخیره شوند

توجه : این قابلیت جزء الزامات فعلی دستگاه نظارت نمی باشد و در صورت تصویب سازمانی برای اجرا، به طرق مقتضی برنامه ریزی های عملیاتی و فنی لازم برای آن دیده خواهد شد

۳. قابلیت وجود کاربر Super Admin (الزامات Authorization)

۳,۱. ترجیحا می باید، در برنامه نرم افزاری، به صورت پیش فرض یک کاربر با عنوان فوق و کلید واژه پیش فرض وجود داشته باشد

۳,۲. کلید واژه کاربر فوق در دیتابیس نباید قابل مشاهده باشد

۳,۳. قابلیت تغییر کلید واژه فوق از داخل برنامه و فقط برای کاربر فوق وجود داشته باشد

۳,۴. کاربر فوق نباید به هیچ یک از منوهای سیستم و دیتاها و گزارشات و فرم ها دسترسی داشته باشد و فقط باید قادر باشد از طریق پنل خاصی، کاربران **Admin** را ایجاد، حذف، فعال و غیرفعال نماید

۳,۵. این کاربر همچنین باید قادر به انجام تنظیمات پایه برنامه نرم افزاری، منجمله تنظیم ارتباط با **CAS**، تنظیم ارتباطات با دیتابیس و سایر سرورها و امثالهم باشد. این کاربر می باید حداقل سطح دسترسی پیش فرض را به شکلی دارا باشد که در مواقع بروز مشکلات ارتباطی یا نصب اولیه برنامه و یا سایر شرایط مورد نیاز بتواند برای رفع مشکلات از آن استفاده شود

۳,۶. ترجیحا می باید، در صورت اعلام دستگاه نظارت، برای **Login** کاربران **Super Admin** به برنامه نرم افزاری، علاوه بر کلید واژه، از سطح دوم احراز هویت نیز به صورت توامان استفاده گردد

۳,۷. ترجیحا می باید، کاربر **Super Admin** باید بتواند تعیین کند که برای **Login** کاربران **Admin** به نرم افزار مورد نظر، علاوه بر کلید واژه، از سطح دوم احراز هویت نیز به صورت توامان استفاده گردد یا خیر

۴. قابلیت وجود کاربران Admin (الزامات Authorization)

۴,۱. کاربر **Admin** کاربری است که به ابزار مدیریت کاربران دسترسی داشته و قادر است سایر کاربران را در سیستم ایجاد، ویرایش، حذف، فعال و غیرفعال نماید

۴,۲. کاربران **Admin**، به ابزار مدیریت گروه ها شامل : ایجاد، ویرایش و حذف، دسترسی دارند

۴,۳. کاربران **Admin**، به ابزار مدیریت نقش ها، شامل : ایجاد ، حذف ، ویرایش، فعال و غیرفعال کردن نقش ها (در حالت غیرمتصل به وب سرویس چارت سازمانی)، دسترسی دارند

۴,۴. کاربران **Admin**، همچنین دسترسی برقراری و تغییر ارتباطات بین نقش و گروه ها (در حالت کلی) و ارتباطات بین نقش ها و کاربران (در حالت غیرمتصل به وب سرویس ساختار سازمانی) را دارا می باشند

۴,۵. کاربر **Admin** نباید امکان ایجاد کاربران **Admin** دیگر را داشته باشد و اینکار فقط از طریق کاربر **Super Admin** باید قابل انجام باشد

۵. قابلیت تعریف کاربران (الزامات Authentication)

۵,۱. برنامه نرم افزاری، باید دارای پنل ساده و Visual با کاربری آسان باشد که بتوان در آن کاربران را : ایجاد، فعال، غیرفعال، در شرایط خاص ویرایش و در شرایط خاص حذف کرد

۵,۲. برای تعریف کاربران، می بایست از وب سرویس CAS، که دستگاه نظارت ارایه می نماید، به صورت ارتباط وب سرویسی OnLine استفاده شود. به این صورت که با وارد کردن نام کاربری CAS فرد مورد نظر یا بوسیله جستجو در لیستی از نام کاربری که از وب سرویس CAS دریافت می شوند کاربر جدید را بتوان ایجاد کرد

۵,۳. اطلاعات User و Pass کاربران نمی باید تحت هیچ شرایطی، توسط برنامه نرم افزاری، ذخیره شود و فقط میباید کلید شناسایی کاربر از سرویس CAS دریافت و در دیتابیس ذخیره شود

۵,۴. امکان ایجاد کاربران درون برنامه ای و بدون استفاده از سرویس CAS بطور کلی و موکدا باید غیرفعال شود

۵,۵. صحت نام کاربری و گذرواژه وارد شده و وضعیت فعال یا غیرفعال بودن کاربر در هر بار Login از سرویس CAS به صورت Online دریافت شود

۵,۶. قابلیت فعال یا غیرفعال سازی کاربران مستقل از سرویس CAS باید در برنامه نرم افزاری وجود داشته باشد

۵,۷. اولویت بررسی فعال بودن کاربر، ابتدا سرویس CAS و سپس برنامه نرم افزاری است

۵,۸. ترجیحا می باید، وضعیت فعال بودن کاربری که Login نموده است، در بازه های زمانی قابل تنظیم در قسمت تنظیمات، میبایست بررسی شده و در صورت غیرفعال شدن کاربر، دسترسی به برنامه نرم افزاری، با اعلام پیام مناسب قطع، و کاربر، از برنامه بیرون برده شود

۵,۹. امکان حذف یک کاربر در برنامه نرم افزاری، وجود داشته باشد، لیکن قبل از حذف، می باید بررسی شود که اثری از فعالیت کاربر، ثبت شده است یا خیر. در صورت وجود هر گونه سابقه فعالیت کاربر، نباید امکان حذف کاربر وجود داشته باشد و باید با نمایش پیام مناسب، از حذف کاربر جلوگیری شود. در چنین شرایطی فقط امکان غیرفعال سازی کاربر می بایست وجود داشته باشد

۵,۱۰. ترجیحا می باید، در صورت تنظیم دوره های زمانی برای تعویض گذرواژه در CAS، وقتی که کاربر در برنامه نرم افزاری، قصد لاگین دارد، با ارتباط وب سرویسی با CAS، موضوع را دریافت کرده و با پیام مناسب، منقضی شدن اعتبار گذرواژه وی را اعلام و از کاربر خواسته شود جهت تغییر گذرواژه به پنل مربوطه مراجعه نماید. همچنین ترجیحا لینک ارتباطی با پنل مربوطه نیز در همان پیام نمایش و با یک کلیک کاربر به پنل مربوطه منتقل شود

۵,۱۱. در صورتیکه نام کاربری در CAS یا برنامه نرم افزاری، غیرفعال شده است در هنگام تلاش کاربر برای ورود، این موضوع با نمایش پیام مناسب به وی اطلاع رسانی شود

۵,۱۲. زمانی که با یک نام کاربری به برنامه نرم افزاری، ورود شده است، ورود مجدد با همان نام کاربری مقدور نباشد

۵,۱۳. ارسال و دریافت اطلاعات نام کاربری و گذرواژه به سمت CAS، وب سرویس ها، بانک اطلاعاتی و غیره فقط به صورت رمزنگاری شده می بایست انجام شود

۵,۱۴. بهتر است در صورت تلاش برای ورود با گذرواژه اشتباه برای اولین بار، قابلیت **Captcha** فعال شده و از کاربر درخواست شود که برای ورود علاوه بر گذرواژه، **Captcha** را نیز وارد نماید. در چنین حالتی با **Refresh** کردن صفحه و یا بستن و باز کردن برنامه نیز کماکان می بایست **Captcha** درخواست گردد

۵,۱۵. در صورت تلاش برای ورود با گذرواژه اشتباه به تعداد دفعات مشخص، می بایست ضمن غیرفعال سازی اکانت مربوطه، موضوع را طی پیام سیستمی (درون برنامه ای و یا فراخوانی یک وب سرویس اطلاع رسانی بین سیستمی و یا ارسال پیامک) به افراد مشخص شده اطلاع رسانی نماید. این افراد و روش اطلاع رسانی و تعداد دفعات اشتباه می باید، در پنل مدیریت باید قابل انتخاب و یا تعریف باشند

۵,۱۶. در نسخه هایی از برنامه که برای محیط وب و یا ویندوز دسکتاپ تهیه می شوند نمی باید امکانی برای ذخیره سازی محلی گذرواژه تعبیه شود (بطور مثال : استفاده از کوکی) اما این امکان در نسخه های موبایل اپلیکیشن بلامانع است

۶. ثبت وقایع کاربری Log Management

۶,۱. تمامی اقدامات یک کاربر در سامانه (حتی **Super Admin**) می بایست به صورت کامل ثبت شوند

۶,۲. اطلاعات موجود در بخش ثبت وقایع تحت هیچ شرایطی نباید امکان حذف را داشته باشند (بجز از طریق دسترسی مستقیم به بانک اطلاعاتی)

۶,۳. امکان مشاهده آسان و جستجوی تمامی اقدامات انجام شده توسط هر کاربر در محیط **Visual**، وجود داشته باشد

۶,۴. امکان مشاهده آسان تمامی اقدامات انجام شده روی هر رکورد اطلاعاتی با ابزار جستجوی آسان در محیط **Visual**، وجود داشته باشد

۶,۵. گزارشات فوق با فیلتر گذاری دوره زمانی و نوع اقدام (**CRUD**) قابل مشاهده باشد

۶,۶. در خصوص ویرایش فیلدها، مقدار قبل از هر ویرایش نیز قابل مشاهده باشد

۶,۷. تمامی محیط های جستجو و گزارش گیری لاگ ها، باید در پنل های گرافیکی ساده و آسان و **Visual** طراحی شده باشند

۶,۸. علاوه بر سایر موارد، بصورت ویژه موارد زیر در ثبت در **Log** مورد توجه قرار گیرند :

۶,۹. زمان و آدرس **IP** ورود و خروج کاربر

۶,۱۰. زمان و آدرس **IP** و نام کاربری در صورت ورود گذرواژه اشتباه به همراه گذرواژه اشتباهی که وارد شده است

۶,۱۱. زمان و آدرس **IP** و نام کاربری در صورت غیرفعال شدن اکانت کاربر توسط نرم افزار مورد نظر

۶,۱۲. زمان و آدرس **IP** و نام کاربری در صورتی که **Captcha** اشتباه وارد شده باشد

۶,۱۳. زمان و آدرس **IP** و نام کاربری در صورت ورود ناموفق به سایر دلایل به همراه دلیل عدم موفقیت (مانند عدم پاسخگویی وب سرویس **Active Directory** و ...)

۶,۱۴. زمان و آدرس **IP** و نام کاربری تراکنش های مربوط به داده ها (**CRUD**) شامل : ایجاد، خواندن، ویرایش، حذف

۶,۱۵. زمان و آدرس **IP** و نام کاربری اقدامات مربوط به فرآیندها، مانند : صدور حکم، صدور سند، صدور چک، ابطال قبض انبار و ....

۶,۱۶.زمان و آدرس IP و نام کاربری اقدامات مربوط به فرآیندهای مدیریت برنامه نرم افزاری، مانند : تغییر سطح دسترسی کاربران، گروها و نقش ها ، افزودن ، حذف کردن ، غیرفعال کردن یک کاربر و ....

۷. قابلیت احراز هویت دو مرحله ای

۷,۱. منظور از احراز هویت دو مرحله ای اینست که همه یا تعداد مشخص شده ای از کاربران برای ورود به برنامه نرم افزاری، ملزم باشند علاوه بر وارد کردن نام کاربری و گذواژه، توسط روش های دیگری اصالت هویت خود را به برنامه نرم افزاری ارایه نمایند

۷,۲. برنامه نرم افزاری ترجیحا می باید چنین قابلیتی را به همراه امکان فعال یا غیرفعال سازی این قابلیت را فراهم آورد. به این معنا که برای همه یا تعداد مشخصی از کاربران بتوان تعیین کرد که پس از وارد کردن گذرواژه، از کاربر خواسته شود که مرحله دیگری از تایید هویت خود را انجام دهد

توجه : این قابلیت جزء الزامات فعلی دستگاه نظارت نمی باشد و در صورت تصویب سازمانی برای اجرا، به طرق مقتضی برنامه ریزی های عملیاتی و فنی لازم برای آن دیده خواهد شد

۷,۳. در پنل مدیریت کاربران باید بتوان مشخص کرد که کدام کاربر یا همه کاربران می بایست احراز هویت دو مرحله ای داشته باشند

۷,۴. برای هر کاربر بتوان مشخص کرد در صورتیکه لازم است به صورت دو مرحله ای ورود نماید ولی فقط مرحله اول آن را انجام دهد، به چه گروهی مرتبط شود (بطور مثال : اگر کاربر مشخصی به صورت دو مرحله ای احراز هویت نمایید دارای سطح دسترسی **Admin** در برنامه نرم افزاری بوده و اگر فقط مرحله اول احراز هویت را انجام دهد دارای سطح دسترسی کاربران عمومی سازمان پسماند باشد)

۷,۵. نمونه هایی از مرحله دوم تایید هویت به شرح ذیل هستند :

۷,۵,۱.ارسال پیامک حاوی پین کد به گوشی تلفن همراه کاربر، که کاربر می باید آنرا در کادر مربوطه وارد نماید

۷,۵,۲.درخواست پاسخ برای سوال شخصی تصادفی که کاربر در هنگام تکمیل پروفایل خود به آنها پاسخ داده است

۷,۵,۳. متصل کردن یک توکن سخت افزاری به کامپیوتری که برنامه نرم افزاری در حال اجرا روی آن است

۷,۵,۴. استفاده از یک دستگاه سخت افزاری ایجاد کننده پین کدهای یکبار مصرف و ورود آن در کادر مربوطه

۷,۵,۵. تایید هویت با استفاده از روش های بایومتریک مثلا : بررسی اثر انگشت کاربر با استفاده از یک سنسور یا با استفاده از ابزارهای درونی گوشی های تلفن همراه (بطور مثال : گوشی های تلفن همراه سامسونگ چنین امکانی را در اختیار برنامه های کاربردی قرار میدهند که از احراز هویت بایومتریک گوشی برای ورود استفاده نمایند)

۸. گزارشات سطوح دسترسی :

در برنامه نرم افزاری می باید گزارشات لازم و کافی در خصوص سطوح دسترسی و کاربران وجود داشته باشد، نمونه هایی از گزارشات مورد نیاز به شرح زیر هستند :

۸,۱. گزارش کاربران متصل شده به یک نقش (مستقیم و با تفویض)

۸,۲. گزارش نقش های متصل شده به یک کاربر

۸,۳. گزارش نقش های متصل شده به یک گروه

۸,۴. گزارش مجموع دسترسی های یک گروه یا یک نقش یا یک کاربر به تفکیک نوع آن

۸,۵. گزارش کاربران فعال و غیرفعال شده در برنامه نرم افزاری، به همراه اطلاعاتی مانند : تاریخ غیرفعال شدن، سیستم غیرفعال کننده (یا دستی)، کاربر غیرفعال کننده و ...