باسمه‌تعالی

"مشخصات و نیازمندی‌های فنی سامانه‌های نرم‌افزاری جهت سازگاری با سامانه احراز هویت متمرکز دانشگاه"

آذرماه ۱۳۹۵

مقدمه

سامانه‌های فاوا در سال‌های گذشته گسترش بسیاری یافته‌اند. استفاده از این سامانه‌ها نیاز روزافزونی به سادگی استفاده و امنیت به وجود آورده است. پیاده‌سازی راه‌حل مدیریت هویت و دسترسی کمک شایانی به افزایش امنیت و راحتی کاربران می‌نماید. زمانی که سامانه‌های هسته پیاده‌سازی شوند، اتصال سامانه‌های مختلف به این زیرساخت گام بسیار پراهمیتی خواهد بود و در این گام، سامانه‌های مختلف برای مدیریت هویت و کنترل دسترسی خود به این راه‌حل متصل می‌شوند. بدین منظور سامانه‌ها باید ملاحظات و مسائل فنی موردنیاز را رعایت کرده و از ویژگی‌های مربوطه پشتیبانی نمایند. مستند کنونی شامل مسائلی است که رعایت آن‌ها جهت سازگاری با زیرساخت مدیریت هویت و دسترسی دانشگاه ضروری است.

معرفی راهکار IAM

راهکار مدیریت هویت و دسترسی، مجموعه‌ای از ابزارهای زیرساختی، نرم‌افزاری و پروسه‌های اجرایی و آموزشی است که با استفاده از آن‌ها سازمان‌های بزرگ و کوچک نحوه دسترسی به منابع را در حوزه فن‌آوری اطلاعات، مدیریت می کنند. به زبان دیگر به مجموعه دیسیپلین‌ها و ابزارهایی که "به فرد یا سامانه صحیح اجازه دسترسی به منبع‌های صحیح در زمان صحیح و به دلایل صحیح" را می‌دهد، مدیریت هویت و دسترسی می‌گویند. امروز این راهکار با توجه به محیط‌های فناوری ناهمگون و همچنین به‌منظور پاسخ به نیازهای قانونی سخت‌گیرانه اهمیت بالایی یافته است.

بخش مدیریت هویت از "مدیریت هویت و کنترل دسترسی" چرخه ایجاد، تغییر و حذف هویت و بخش مدیریت دسترسی از این راهکار وظیفه کنترل و مدیریت دسترسی به سامانه‌های مختلف را به عهده خواهد داشت.

مخاطبان مستند

مخاطبان این مستند، طراحان، تهیه‌کنندگان، گسترش‌دهندگان و تجمیع کنندگان سامانه‌های دانشگاه هستند که در زیرساخت فن‌آوری اطلاعات نصب خواهند شد و در آن‌ها به هر شکل پروسه‌های احراز هویت و کنترل دسترسی انجام می‌شود.

خط‌مشی

خط‌مشی به دو بخش اصلی تقسیم می‌شود که در ادامه توضیح داده خواهد شد:

۱. مدیریت هویت و احراز هویت

۲. کنترل دسترسی

۱. مدیریت هویت و احراز هویت

به منظور اتصال سامانه‌ها به زیرساخت مدیریت هویت و احراز هویت یکپارچه دانشگاه، رعایت نکات زیر در طراحی و اجرا ضروری است:

۱. نرم‌افزار باید از سامانه احراز هویت مرکزی[۱] یا پروتکل LDAP جهت احراز هویت پشتیبانی نماید.

۱,۱. در راستای مجتمع سازی با سامانه احراز هویت مرکزی لحاظ نمودن نکات زیر ضروری است:

۱,۱,۱.سامانه از باید از پروتکل‌های زیر پشتیبانی نماید:

1- CAS v1, v2 and v3 Protocol
2- SAML v1 and v2 Protocol
3- SSL

۱,۱,۲.استفاده از آدرس در تنظیمات CAS به‌جای IP، به‌عنوان‌مثال:

- https://cas.sso.example-company.com

۱,۱,۳.استفاده از آدرس login/ برای ورود و logout/ برای خروج روی سرور CAS، با در نظر گرفتن اینکه این آدرس‌ها بتوانند تنظیم شوند و قابل تغییر باشند و پیشنهاد می‌شود نکات لازم در این رابطه در نظر گرفته شوند.

- https://cas.sso.example-company.com/login
- https://cas.sso.example-company.com/logout

۱,۱,۴.بازخوانی اطلاعات هویت مانند نام و نام‌خانوادگی از طریق پروتکل CAS یا از طریق اتصال LDAP بر اساس principal مشترک

۱,۲. در راستای مجتمع سازی با LDAP لحاظ نمودن نکات زیر ضروری است:

۱,۲,۱.پشتیبانی از روش‌های زیر

1- Bind
2- Search and Compare

---

[۱] JASIG CAS

۱,۲,۲.سامانه باید از پروتکل‌های زیر پشتیبانی نماید:

1- LDAP v1 & v2
2- SSL

۱,۲,۳.استفاده از آدرس در تنظیمات LDAP به‌جای IP، به‌عنوان‌مثال:

- https://core01.sso.example-company.com

۱,۲,۴.بازخوانی اطلاعات هویت مانند نام و نام‌خانوادگی از طریق پروتکل LDAP بر اساس principal مشترک

۲. نرم‌افزار باید بتواند ویژگی‌ها و آدرس‌های خاص مربوط به هویت خود را تغییر دهد:
۲,۱. تغییر آدرس ورود و خروج
۲,۲. تغییر صفحه تغییر رمز عبور یا حذف و غیرفعال کردن آن
۳. پشتیبانی از دریافت و انتخاب اطلاعات و Attribute ها به زبان‌های مختلف در پروتکل LDAP
۴. پشتیبانی از سرویس یا API مناسب جهت Provisioning & De-Provisioning یا امکان مستندسازی و در اختیار قرار دادن بخش‌هایی از Data Model و API جهت انجام این مسئله توسط سامانه احراز هویت متمرکز دانشگاه

۲. کنترل دسترسی

به منظور اتصال سامانه‌های نرم‌افزاری به سامانه کنترل دسترسی یکپارچه دانشگاه رعایت نکات زیر در طراحی و اجرا ضروری است:

۱. کنترل دسترسی با استفاده از مشخصه‌های کاربر و به روش Role Based صورت می‌پذیرد. مشخصه مهم مورداستفاده Role یا Group است.
۲. در سامانه‌های پیشرفته‌تر کنترل دسترسی با استفاده از Attribute و به‌صورت ABAC صورت می‌پذیرد. زمان و مکان نیز ازجمله Attribute های مورد هدف هستند.
۳. جهت استخراج Granted Authority ها استفاده از پروتکل SAML الزامی است. این پروتکل در ترکیب با CAS در هنگام بررسی، اعتبار بلیت مشخصه‌های کاربر را در اختیار نرم‌افزار قرار می‌دهد.
۴. استخراج اطلاعات مربوط به کاربران با استفاده از LDAP امکان‌پذیر است. پشتیبانی از این پروتکل الزامی است.

۵. جهت کنترل دسترسی پشتیبانی از پروتکل XACML الزامی است. این پروتکل در گسترش‌های بعدی سیستم به‌منظور کنترل دسترسی متمرکز استفاده خواهد گردید.

۶. اطلاعات مربوط به نقش کاربران، گروه‌های آن‌ها و دیگر مشخصه‌های کاربری آن‌ها در سامانه IAM نگهداری می‌شوند. این اطلاعات به‌صورت مداوم در معرض تغییر می‌باشند، نگهداری این اطلاعات به هر شکل در نرم‌افزارها غیرقابل‌قبول است. نگهداری این اطلاعات به‌صورت موقت (به‌عنوان‌مثال در طول مدت session) قابل‌قبول است.

۷. سامانه نرم‌افزاری می‌بایست به‌منظور تعریف نقش‌ها و مشخصه‌های خود در سامانه مرکزی از API مبتنی بر وب‌سرویس پشتیبانی نماید.