«بسمه تعالی»

مدیریت هویت و دسترسی سازمانی

راهنمای دسترسی به توزیع مستقر در اینترنت سامانه مهاد

شناسه سند: eIAM_Mehad_Tech_100_1.0

عادی

اسفند ۱۴۰۱

تاریخچه

نسخه	تاریخ تهیه	تهیه کننده	تایید کننده	توضیحات
۱.۰	اسفند ۱۴۰۱	تیم پروژه	مدیر پروژه	نسخه اول به جهت ارائه به کارفرما تهیه گردید

فهرست مطالب

۱ مقدمه

با توجه به درخواست کارفرما مبنی بر راه‌اندازی بستری در اینترنت به جهت استفاده توسعه دهندگان سامانه‌های سازمان در نقش RP و انجام یکپارچه‌سازی آزمایشی با سرویس SSO راه‌اندازی شده در این پروژه با نام «مهاد»، چنین بستری استقرار یافت و دسترسی لازم از طریق اینترنت به آن داده شد. به منظور استفاده توسعه دهندگان سامانه های موردنظر از این سامانه، ضروری است که برخی پیکربندی‌ها نظیر آدرس سرویس انجام گردد. توصیف این پیکربندی‌ها موضوع این سند است و به توضیح پارامترها و مقادیر مورد نیاز برای اتصال و دریافت سرویس از سامانه مدیریت هویت و دسترسی مهاد می‌پردازد.

شایان ذکر است محیط مذکور صرفا به هدف یکپارچه‌سازی تستی و آزمون آن، آماده گردیده و فاقد هرگونه اطلاعات مهم می‌باشد. از آنجا که در مقطع کنونی فرض بر محدود بودن تعداد سامانه‌های RP است، مشخصات یک سامانه و یک کاربر فرضی نیز در این تنظیمات لحاظ گردیده است. در آینده نزدیک و با افزایش تعداد سامانه‌های موردنظر، زیرساختی برای تعریف و اختصاص سامانه‌های متعدد و مجزا درنظر گرفته خواهد شد که تداخلی در فرآیند آزمون و یکپارچه‌سازی توسعه‌دهندگان سامانه‌های مختلف پیش نیاید.

۲ اطلاعات پیکربندی

توسعه دهندگان سامانه‌های کاربردی و ارائه دهندگان سرویس با بکارگیری و استفاده از مولفه‌های آماده تامین کننده پروتکل OIDC می‌توانند با سامانه مدیریت هویت و دسترسی مهاد ارتباط برقرار نمایند. به منظور فراهم کردن ارتباط صحیح با سامانه مهاد بایستی مقادیر تعیین شده در جدول ذیل برای پارامترهای معین شده تنظیم گردد. در این جدول، فرض شده است که یک سامانه RP با عنوان Test_RP و یک کاربر با عنوان Bob از این سرویس استفاده خواهد نمود.

کلید	مقدار
SSOBaseAddr	https://matiran.iam.ir:8443
Issuer	{baseAddress}/realms/Test_Realm
AuthorizationEPUrl	{baseAddress}/realms/Test_Realm/protocol/openid-connect/auth
TokenEpUrl	{baseAddress}/realms/Test_Realm/protocol/openid-connect/token
ClientID	به ازائه هر سامانه جداگانه باید صادر گردد از راهبر مهاد بخواهید برای سامانه شما تعریف نماید
ClientSecret	به ازائه هر سامانه جداگانه باید صادر گردد از راهبر مهاد بخواهید برای سامانه شما تعریف نماید
username	bob
password	123

جهت دسترسی به سامانه مهاد در بستر اینترنت باید به نکات توجه نمایید:

- آدرس matiran.iam.ir باید در Host File کلاینت با آدرس ۱۹۲.۱۶۸.۱۱.۱۱۸ نگاشت گردد. مسیر Host File بیان شده در ادامه آورده شده است:
- در سیستم عامل ویندوز: C:\Windows\System32\drivers\etc\hosts
- در سیستم عامل لینوکس : /etc/hosts

۱- از آنجا که این ارتباط مجهز به پروتکل TLS است، ضروری است تنظیمات لازم برای این پروتکل اعمال گردد. به پیوست سند، فایل گواهینامه مرکز ریشه و زنجیره اعتماد آن نیز به همین منظور ارائه گردیده است. که باید در سیستم نصب گردد فایل های matiran.iam.ir.cer و Server_CA.cer

۲- به منظور کنترل دسترسی به این سرویس، پیش‌نیاز رویت آن، برقراری ارتباط VPN میباشد. ازینرو، پیش از انجام هر کاری ضروری است نرم افزار Keyhan-Client از وب سایت شرکت پیام پرداز به آدرس payampardaz.com دانلود و نصب شود و سپس توکن مجازی ارائه شده در پیوست سند حاضر به نرم افزار Keyhan-Client افزوده شود . پس از اتصال به اینترنت، از کلمه عبور در این نرم افزار جهت اتصال VPN استفاده شود.
(توکن مجازی و کلمه عبور به ازائه هر سامانه ایجاد و دراختیار راهبر سامانه قرار خواهد گرفت)

۳- آدرس سرور توکن جهت تنظیم در نرم Keyhan-Client : ۵.۱۶۰.۷.۱۰۱

۴- آدرس دسترسی به صفحه لاگین کاربر سامانه مهاد
https://matiran.iam.ir:8443/realms/Test_Realm/account/

۵–بعد از استقرار سامانه در حال توسعه در اینترنت باید پارامتر **callback url** را جهت تنظیم در سامانه مهاد به راهبر مهاد اعلام نمایید.