

پروتکل UMA احراز اصالت تحت وب

UMA Web Service Authentication Protocol

ارائه دهنده: پویا ستاری
استاد محمد مهدی شیرمحمدی

پاییز ۱۴۰۰

پروتکل UMA

پروتکل ۲.۰ User Managed Access یا UMA یک پروتکل استاندارد کنترل دسترسی است که بر مبنای ۲.۰ OAuth ساخته شده است و اشتراک شخص به شخص را امکان پذیر می سازد.

UMA این توانایی را به مالکین منابع می دهد تا کنترل اینکه چه کسی می تواند از طریق یک سرور کنترل دسترسی مرکزی به منابع محافظت شده آن ها (دارایی های دیجیتال) بدون توجه به محل استقرار منابع دسترسی پیدا کند را به دست بگیرند.

به عنوان مثال ، یک فرد مسن داده های مربوط به سلامتی (مانند نسخه های پزشکی و گزارش آزمایش خون) را با پزشکان ، شرکت بیمه خود و اعضای خانواده به اشتراک می گذارد.

پروتکل UMA

اشتراک گذاری منابع می تواند به صورت انتخابی انجام شود که به افراد کمک می کند کنترل اشتراک منابع خود را به روشی مطمئن و ایمن بدست گیرند. ویژگی این پروتکل این است که دارندگان منابع نیازی به حضور آنلاین در زمان دسترسی ندارند زیرا اشتراک بین طرفین توسط سیاست های از پیش تعیین شده انجام می شود.

استفاده از استانداردهای UMA ۲.۰ شما را قادر می سازد به موارد زیر دست پیدا کنید:

- زمینه : (Context) لحظه مناسب تصمیم گیری برای به اشتراک گذاشتن است.
- کنترل : (Control) قدرت اشتراک گذاری صرفا آنچه که مالک منبع می خواهد.
- انتخاب : (Choice) توانایی تصمیم گیری مستقل.
- احترام : (Respect) توجه به تمایلات شخصی.

ویژگی های UMA ۲.۰

۱. ارائه گرنٹ UMA ۲.۰ برای اخذ مجوز دسترسی OAuth ۲.۰

مشخص می کند که چگونه مشتری باید از تیکت مجوز برای

درخواست توکن دسترسی OAuth ۲.۰ استفاده کند تا بدون

توجه به زمانی که مالک منبع مجوز دسترسی را اعطا کرده است ،

به یک منبع محافظت شده دسترسی پیدا کند.

۲. کنترل دسترسی هم پیمان برای UMA ۲.۰ این امکان را می

دهد که سرور کنترل دسترسی (Authorization Server)

و سرور منابع (Resource Server) تا حد زیادی مستقل از

هم و هم پیمان باشند. استفاده از این ویژگی در کنار گرنٹ

UMA اختیاری است.

ساختار ۲.۰ UMA

پروتکل UMA از ۵ نقش تشکیل شده است:

۱. مالک منابع: موجودیتی که اجازه دسترسی به یک منبع محافظت شده را می دهد.
۲. درخواست دهنده: شخصی است که به وسیله یک کلاینت به دنبال دسترسی به یک منبع محافظت شده است.
۳. کلاینت: برنامه ای است که از طرف درخواست کننده با اجازه مالک منبع، درخواست منابع محافظت شده را می دهد.
۴. سرور منابع: سروری که میزبان منابع محافظت شده است و توانایی واکنش به درخواست های منابع محافظت شده را دارد.
۵. سرور کنترل دسترسی: سروری که از منابع میزبانی شده توسط سرور منابع به نمایندگی از مالک منبع محافظت می کند.

پروفايل UMA

پروفايل UMA از دو جزء اصلي تشكيل شده:

۱. Protection API

۲. UMA Grant

