**معرفی پروتکل های احراز هویت**

**: (Security Assertion Markup Language) SAML**

اجازه دسترسی به برنامه های مختلف را فقط با یک بار احراز هویت میدهد و به عبارت دیگر با ارائه روشی فناوری SSO را پیاده سازی می کند که پروتکل استاندارد را بر اساس XML ارائه می دهد.

SSO یا Single Sign On چیست؟

یک سرویس متمرکز تائید هویت است که تنها با یک نام کاربری کاربر میتواند به چند برنامه دسترسی داشته باشد. به عنوان مثال اگر در google حساب Gmail خود را ثبت کنیم میتوانیم به چند برنامه مانند Youtube و یا غیره دسترسی داشته باشیم.

**OpenID :**

تکنولوژی احراز هویت کاربری در یک وبگاه از طریق وبگاه دیگر است .در واقع همان پیاده سازی فناوری SSO به شمار می رود. مانند SAML. به درگاهی که درخواست احراز هویت را می دهد OpenID Provider می گویند.

**: OAUTH**

پروتکلی برای دادن مجوز دسترسی از یک سرویس به سرویس دیگر بدون به اشتراک گذاشتن نام کاربری و رمز عبور است.یکی از رایج ترین روش های انتقال مجوز از یک سرویس یک پارچه احراز هویت (SSO) به سامانه های دیگر است.

**امنیت در معماری MicroService**

**الگوی Api Gateway :**

**الگوی BFF :**

مخفف عبارت Backend For Frontend است

**مباحث تکمیلی**

**Defense In Depth یا DID چیست؟**

دفاع در عمق یا DID به یک رویکرد امنیت اطلاعات اشاره دارد که در آن یک سری مکانیزم ها و کنترل های امنیتی به طور مدبرانه در سراسر یک شبکه کامپیوتری لایه بندی می شوند تا از محرمانه بودن، یکپارچگی و در دسترس بودن شبکه و داده های درون آن محافظت کنند. با این رویکرد در صورتی که یکی از مکانیزم ها شکست بخورد، در لایه ی بعدی مکانیزم بعدی جلوی خطر را خواهد گرفت. این رویکرد به طور قابل توجهی امنیت شبکه را در برابر بسیاری از حمله ها تقویت می کند.