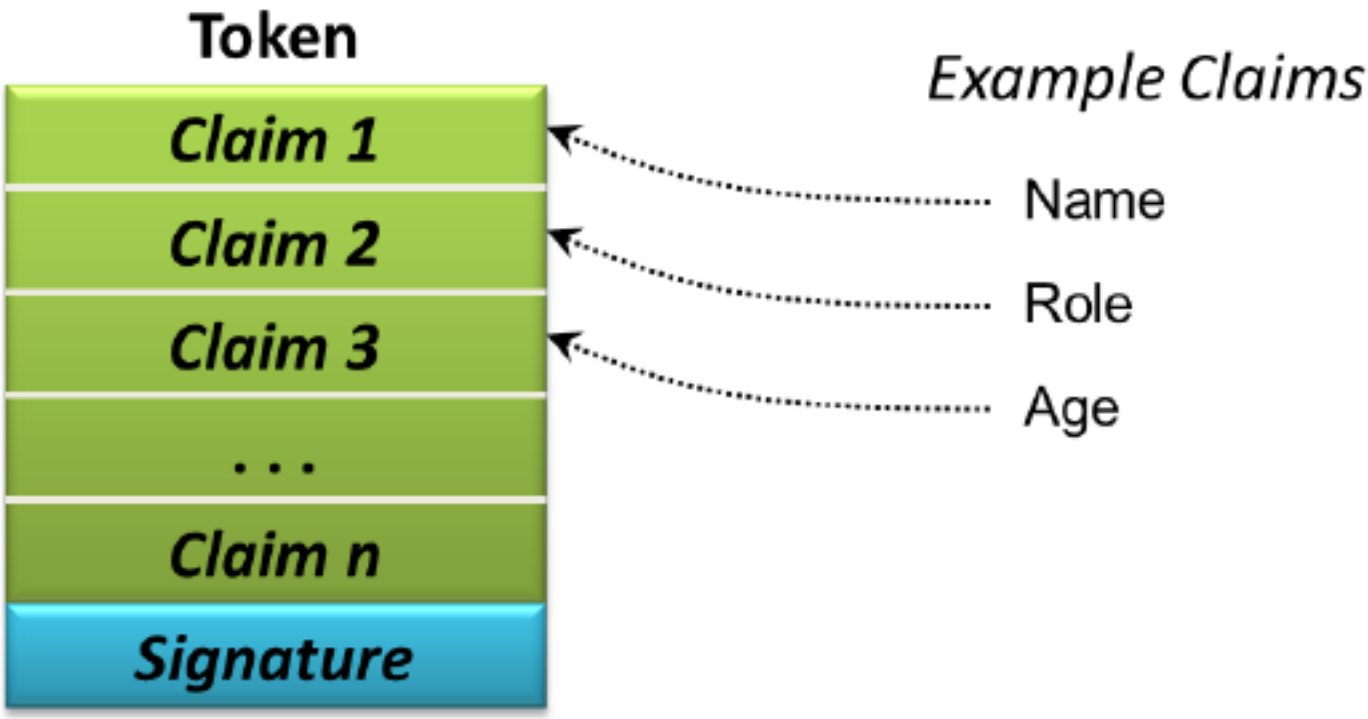
عنوان: **مروری بر Claim**
نویسنده: محمد باقر سیف اللهی
تاریخ: ۱۳۹۱/۰۶/۱۱ ۰:۴۹
آدرس: www.dotnettips.info
گروه‌ها: SharePoint, Authentication

تعریف :

در این پست قصد دارم در مورد claim که از آن به عنوان یک Abstraction برای شناسایی نام برده شده ، صحبت کنم و گریزی با ارتباط آن با شیرپوینت بزنم . مایکروسافت در جایی Claim را این گونه تعریف کرده بود : یک عبارت که یک شیئ ، آن را در باره خودش یا شیئ دیگری می‌سازد . Claim یک Abstraction برای شناسایی فراهم می‌کند . برای مثال میتوان گفت که یک عبارت که شامل نام ، شناسه ، کلید ، گروه بندی ، ظرفیت و ... باشد ، فراهم می‌کند .

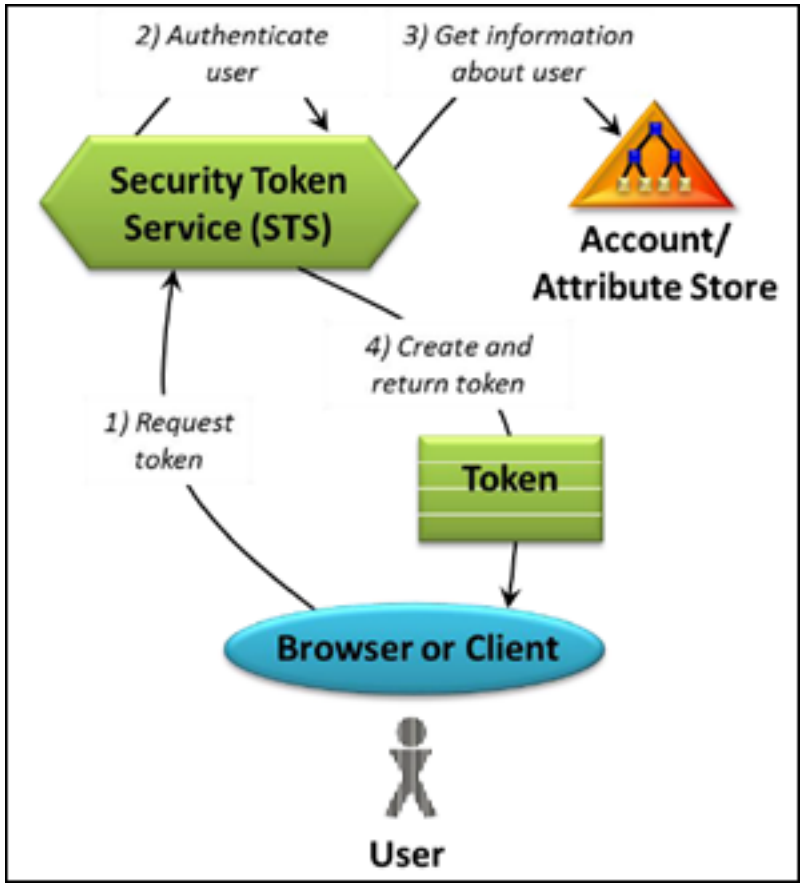
لازم است به تعریف Token هم اشاره ای شود . هنگامی که یک شناسه دیجیتالی در شبکه در حال گذر است ، فقط حاوی مجموعه ای از بایت‌ها است .(ارجاع به مجموعه ای از بایت‌ها که حاوی اطلاعات شناسایی به عنوان یک Token امنیتی با فقط یک Token باشد، امری عادی است) . در محیطی که بر مبنای Claim بنا شده است ، یک Token حاوی یک یا چند Claim است که هر یک می‌تواند برخی تکه‌های اطلاعاتی را برای شناسایی (بیشتر در مورد کاربران و افراد استفاده می‌شود) ، در خود جای دهد



Claimها تقریبا هر چیزی را در مورد یک کاربر می‌تواند ارائه دهد. . برای مثال در Token تصویر بالا ، 3 claim اول به اطلاعات نام و نقش و سن کاربر اشاره دارند .

فراهم کننده - توزیع کننده :

Claimها توسط یک فراهم کننده (Provider) توزیع می‌شوند (Issuer) و سپس به آنها یک یا چند مقدار ، اختصاص می‌یابد و در Security Token هایی که توسط یک توزیع کننده ، توزیع می‌شوند ، بسته بندی می‌شود و معمولا به عنوان Security Token Service یا STS شناخته می‌شوند . برای مشاهده تعریف اصطلاحات مرتبط به Claim به اینجا مراجعه کنید



STS ، می‌تواند توسط چند Identity Provider - IdP به مالکیت در بیاید . یک فراهم کننده شناسه در STS یا IP-STS ، یک سرویس است که درخواست‌ها را برای اطمینان از شناسایی Claimها مدیریت می‌کند . یک IP-STS از یک پایگاه داده که Identity Store نامیده می‌شود برای نگهداری و مدیریت شناسه‌ها و خصیصه‌های مرتبط با آنها استفاده می‌کند .Identity Store می‌تواند یک دیتا بیس معمولی مانند SQL Server باشد یا یک محیط پیچیده‌تر مانند Active Directory . (از قبیل Active Directory Lightweight Directory Service یا Domain Services) .

قلمرو - Realm

بیانگر مجموعه ای از برنامه‌ها ، URLها ، دامنه‌ها یا سایت هایی می‌باشد که برای Token ، معتبر باشد .معمولا یک Realm با استفاده از دامنه (microsoft.com) یا مسیری داخل دامنه (microsoft.com/practices/guides) تعریف می‌شود .بعضی وقت‌ها یک realm ، به عنوان Security Domain بیان می‌شود چرا که تمام برنامه‌های داخل یک مرز امنیتی ویژه ای را احاطه کرده است .

Identity Federation

Identity Federation در حقیقت دریافت کننده Token هایی است که در خارج از Realm شما ایجاد شده اند و در صورتی Token را می‌پذیرد که شما Issuer یا توزیع کننده را مورد اطمینان معرفی کرده باشد . این امر به کاربران اجازه می‌دهد تا بدون نیاز به ورود به realm تعریف شده خودشان ، از realm دیگری وارد برنامه شوند . کاربران با یک بار ورود به محیط برنامه ، به چندین realm دسترسی پیدا خواهند کرد .

Relying party application

هر برنامه سمت client که از Claim پشتیبانی کند

مزایای Claim

جدا سازی برنامه از جزییات شناسایی

انعطاف پذیری در احراز هویت

Single sign-on

عدم نیاز به VPN

متحد کردن مجموعه با دیگر شرکت ها

متحد کردن مجموعه با سرویس‌های غیر از AD

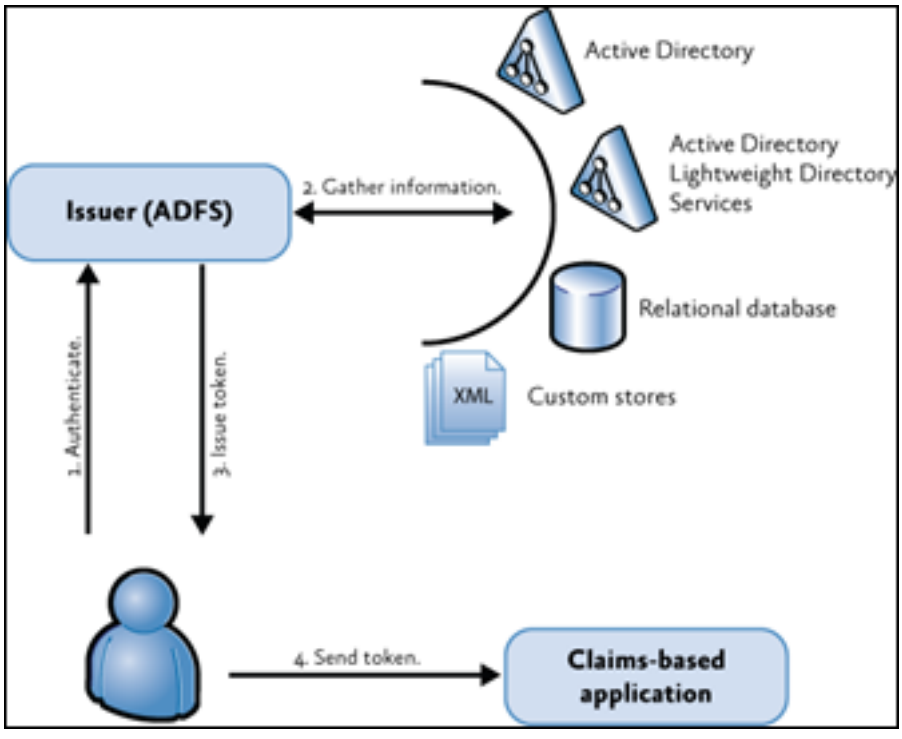
عناصر Claim

Claim شامل عناصر زیر می‌باشد :
Token

Claim

Provider/Issuer
Sharepoint STS
ADFS
ACS
OID
و غیره,

توزیع کننده‌ی ADFS



پرنکل‌ها و Tokenهای Claim

شاید این بخش ، یکی از سردرگم کننده‌ترین مفاهیم باشد . هنگامی که صحبت از Claim می‌شود ، عده ای دچار این عدم توجه صحیح می‌شوند که هر دو نوع مختلفی از Tokenها که با Claimها استفاده می‌شوند ، توسط تمام برنامه‌ها پشتیبانی نمی‌شوند . نکته قابل توجه نوع پروتکلی است که می‌خواهید از آن استفاده کنید و باید کامل از آن مطلع باشید .

Security Token هایی که در اینترنت رفت و آمد می‌کنند ، معمولا یکی از دو نوع زیر هستند :

- توکن‌های Security Assertion Markup Language یا SAML که ساختار XMLی دارند و encode شده اند و داخل ساختارهای دیگر از قبیل پیغام‌های HTTP و SOAP جای می‌گیرند

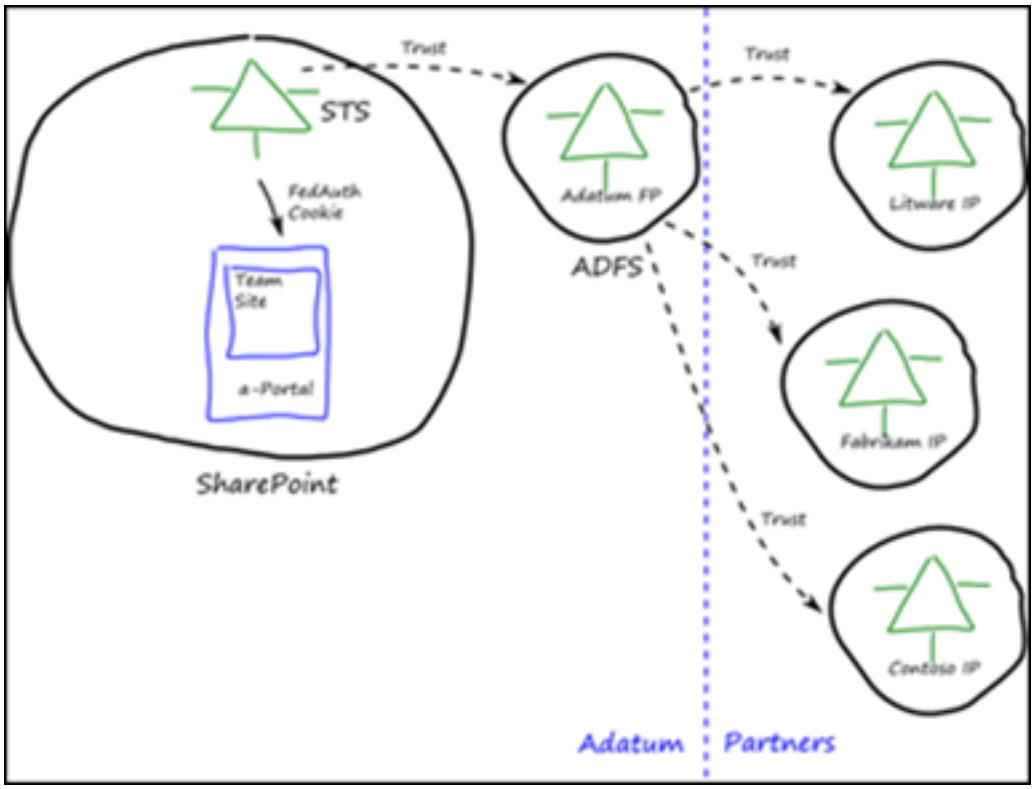
- Simple Web Token یا SWT که درون هدرهای درخواست یا پاسخ HTTP جای میگیرند .(WS-Federation)

نوع متفاوتی از Token که وابسته به مکانیسم احراز هویت است، ایجاد شده است . برای مثال اگر از Claim با Windows Sign-in استفاده می‌کنید ، شیرپوینت 2010 ، شیئ UserIdentity را به شیئ ClaimIdentity نبدیل می‌کند و claim را تقویت کرده و Token حاصله را مدیریت می‌کند . (این نوع Toaken جزء SAML نمی‌شود)

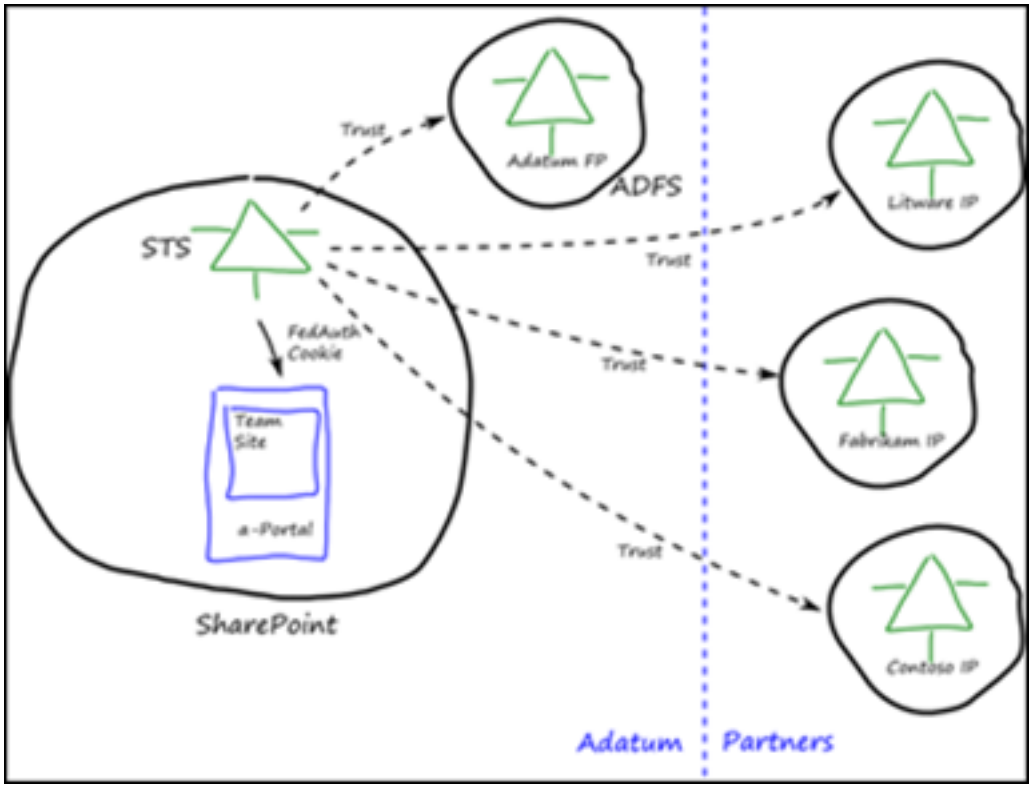
تنها راه به گرفتن توکن‌های SAML ، استفاده از یک Provider برای SAML است . مانند Windows Live ID یا ADFS . [+]

معماری برنامه‌های مبتنی بر Claim

نام مدل : Direct Hub Model



نام مدل : Direct Trust Model



مزایا :

- مدیریت راحت‌تر برای multiple trust relationships در ADFS نسبت به Sharepoint
- مدیریت ساده‌تر در single trust relationship در شیرپوینت و عدم نیاز به فراهم کننده‌های سفارشی سازی شده برای Claim
- قابلیت استفاده از ویژگی‌های ADFS برای پیگیری توزیع Token ها
- ADFS از هز دوی SAML و WS-Federation پشتیبانی می‌کند
- توزیع کننده ADFS اجازه می‌دهد تا خصیصه‌های LDAP را از AD استخراج کنید
- ADFS به شما اجازه استفاده از قواعد دستوری SQL را برای استخراج داده‌ها از دیگر پایگاه‌های داده می‌دهد
- کارایی و اجرای مناسب

معایب :

- کند بودن
- عدم پشتیبانی از SAML-P
- نیازمند تعریف کاربرها در AD یا نواحی مورد اطمینان

موفق باشید

نظرات خوانندگان

نویسنده: آزاده
تاریخ: ۱۳۹۲/۰۹/۱۰ ۱۵:۵۹

سلام . خسته نباشید.
سوالی داشتم ، اگر به عنوان مثال من دو کلاس شرکت و کارمند رو داشته باشم که رابطه یک به چند دارند. و هر کاربری که login کرد لازم باشه که فقط اطلاعات شرکت خودش رو ببینه ولی تنها role admin لازمه که اطلاعات همه شرکت رو پس از login ببیند. در اینصورت به نظر شما نیازی هست که از Claim base استفاده کنم با توجه به معایبی که گفته شده یا خیر؟
ممنونم

نویسنده: محمد باقر سیف اللهی
تاریخ: ۱۳۹۲/۰۹/۱۱ ۱۱:۳۶

سلام...
این مفهوم در لایه‌های زیر ساختی یک Application استفاده می‌شود (وابسته به Platform یا حتی پایین‌تر در infrastructure و در لایه‌های پیاده سازی برنامه با این مفهوم کاربرد ندارد). ضمنا بحث claim وابسته به مفهوم Authentication می‌باشد ولی مسئله شما با مفهوم Authorization سروکار دارد.

این موارد برای مقیاس‌های بالا (مانند یک سازمان با کاربران زیاد و پیچیدگی‌های معماری بالا) نمود بیشتری پیدا می‌کند . بیان معایب دلیلی بر کاربردی نبودن آن نیست و با امکان سنجی می‌توان کاربردی و مفید بودن آن را سنجید.
موفق باشید

نویسنده: غلامرضا
تاریخ: ۱۳۹۳/۰۶/۰۶ ۱۵:۵۶

سلام . ببخشید به چه صورت میتونم تو asp.net webforms از claim base authorizatoin استفاده کنم . اگه منبع هم معرفی کنید ممنون میشم.

نویسنده: محمد باقر سیف اللهی
تاریخ: ۱۳۹۳/۰۶/۰۶ ۱۷:۴۶

سلام
این پیوندها را بررسی کنید codeproject
codeproject
msdn - Sample Code
msdn
موفق باشید