以IdentityServer4为例

从认证服务器获取公匙

从http://localhost:5000/.well-known/openid-configuration/jwks获取公匙，返回数据如下：

{

"keys":[

{

"kty":"RSA", // 使用RSA算法

"use":"sig", // 类型为签名

"kid":"03ece87289fe54eee377a1380b0e49a2", // 与token有关

"e":"AQAB", // RSA算法中的e，base64url（注意与base64的区别）

"n":"3JjRAiTwPOCDrWFcsHDovYDuBaqWuSSLxSp27Bc6rDnsepkw-yISVRlM4C-MwgL4wiDZnnQBv9-zZi8on0\_L1L7UuuN5HFvvd01xApIWGdhJwQl2ijltwOKG8osxQQXtkDLOPOxhV-Fs5K9KQWW0AXdkPUXYulP3854MXmNWOqtC3fhMg78MUZAAKGrj67qk0tRdtxXIgF\_Mqn5cMsEq8X7xWcbcPwWuc\_NsfSxs43Y-p-7THMrv8vRzIQFUO27WGMZP9cTlXx0\_OuhRaNnZUJoamp89-j-XMBfYzsCFyD\_a3dBdUMvNtvgDq4IylA1oyT1F\_J8xi4SPHwtNvnWxLQ", // RSA算法中的n，base64url（注意与base64的区别）

"alg":"RS256" // 哈希算法名称，使用“SHA256”哈希算法。

}

]

}

从认证服务器获取共享Token

eyJhbGciOiJSUzI1NiIsImtpZCI6IjAzZWNlODcyODlmZTU0ZWVlMzc3YTEzODBiMGU0OWEyIiwidHlwIjoiSldUIn0.eyJuYmYiOjE1NDMxOTkxNTksImV4cCI6MTU0MzIwMjc1OSwiaXNzIjoiaHR0cDovL2xvY2FsaG9zdDo1MDAwIiwiYXVkIjpbImh0dHA6Ly9sb2NhbGhvc3Q6NTAwMC9yZXNvdXJjZXMiLCJhcGkxIl0sImNsaWVudF9pZCI6Im12YyIsInN1YiI6IjQxMjciLCJhdXRoX3RpbWUiOjE1NDMxOTkxNTIsImlkcCI6ImxvY2FsIiwibmFtZSI6IjE4ODg4ODg4ODg3Iiwic2NvcGUiOlsib3BlbmlkIiwicHJvZmlsZSIsImFwaTEiLCJvZmZsaW5lX2FjY2VzcyJdLCJhbXIiOlsicHdkIl19.vGn\_PiK\_aomcVfGBGX0QH6-1ySd5Viv4ZHDA1s2xZ5HstgS07WawQpxbSG83aLAig\_NpKiTR3aNZKTQ40s4PgUJLJ7x1WTaJUxJApWYi9oLsPxK6p7sxi3OPPHGWIKpka4ht\_p\_9SY13oToWvBECkhU6F2Oeo3iEKWmGy4n3aOLHuQe4rNEVrKnVD9DXLUbwK8dgBeRj7DsKyrVtjMzMHG9tpeepzt\_EktbRKG-rjezgGRb-421b8b3SNDBT9g\_sTjV6VvxHdXS3zHAIU1nbxD66cEFVfoo7F63643RTEtjNJRB1mlicbJdknzoF-d-QFIh\_xtTkTZjzoa7ZL7DrQQ

Token有三部分组成

第三部分 = 第一部分 + “.” + 第二部分

使用RSA验证共享token

static void Main(string[] args)

{

RSAParameters param = new RSAParameters()

{

Exponent = FromBase64Url("AQAB"),

Modulus = FromBase64Url("3JjRAiTwPOCDrWFcsHDovYDuBaqWuSSLxSp27Bc6rDnsepkw-yISVRlM4C-MwgL4wiDZnnQBv9-zZi8on0\_L1L7UuuN5HFvvd01xApIWGdhJwQl2ijltwOKG8osxQQXtkDLOPOxhV-Fs5K9KQWW0AXdkPUXYulP3854MXmNWOqtC3fhMg78MUZAAKGrj67qk0tRdtxXIgF\_Mqn5cMsEq8X7xWcbcPwWuc\_NsfSxs43Y-p-7THMrv8vRzIQFUO27WGMZP9cTlXx0\_OuhRaNnZUJoamp89-j-XMBfYzsCFyD\_a3dBdUMvNtvgDq4IylA1oyT1F\_J8xi4SPHwtNvnWxLQ"),

};

RSA rSA = RSA.Create(param);

var ispass = rSA.VerifyData(UTF8Encoding.UTF8.GetBytes("eyJhbGciOiJSUzI1NiIsImtpZCI6IjAzZWNlODcyODlmZTU0ZWVlMzc3YTEzODBiMGU0OWEyIiwidHlwIjoiSldUIn0.eyJuYmYiOjE1NDMxOTkxNTksImV4cCI6MTU0MzIwMjc1OSwiaXNzIjoiaHR0cDovL2xvY2FsaG9zdDo1MDAwIiwiYXVkIjpbImh0dHA6Ly9sb2NhbGhvc3Q6NTAwMC9yZXNvdXJjZXMiLCJhcGkxIl0sImNsaWVudF9pZCI6Im12YyIsInN1YiI6IjQxMjciLCJhdXRoX3RpbWUiOjE1NDMxOTkxNTIsImlkcCI6ImxvY2FsIiwibmFtZSI6IjE4ODg4ODg4ODg3Iiwic2NvcGUiOlsib3BlbmlkIiwicHJvZmlsZSIsImFwaTEiLCJvZmZsaW5lX2FjY2VzcyJdLCJhbXIiOlsicHdkIl19"),

FromBase64Url("vGn\_PiK\_aomcVfGBGX0QH6-1ySd5Viv4ZHDA1s2xZ5HstgS07WawQpxbSG83aLAig\_NpKiTR3aNZKTQ40s4PgUJLJ7x1WTaJUxJApWYi9oLsPxK6p7sxi3OPPHGWIKpka4ht\_p\_9SY13oToWvBECkhU6F2Oeo3iEKWmGy4n3aOLHuQe4rNEVrKnVD9DXLUbwK8dgBeRj7DsKyrVtjMzMHG9tpeepzt\_EktbRKG-rjezgGRb-421b8b3SNDBT9g\_sTjV6VvxHdXS3zHAIU1nbxD66cEFVfoo7F63643RTEtjNJRB1mlicbJdknzoF-d-QFIh\_xtTkTZjzoa7ZL7DrQQ"),

HashAlgorithmName.SHA256,

RSASignaturePadding.Pkcs1);

}

public static byte[] FromBase64Url(string base64Url)

{

string padded = base64Url.Length % 4 == 0

? base64Url : base64Url + "====".Substring(base64Url.Length % 4);

string base64 = padded.Replace("\_", "/")

.Replace("-", "+");

return Convert.FromBase64String(base64);

}

验证token是否过期

Token第二部分base64解码如下

{

"nbf":1543199159,

"exp":1543202759,

"iss":"http://localhost:5000",

"aud":["http://localhost:5000/resources","api1"],

"client\_id":"mvc",

"sub":"4127",

"auth\_time":1543199152,

"idp":"local",

"name":"18888888887",

"scope":["openid","profile","api1","offline\_access"],"

amr":["pwd"]

}

其中exp保存过期时间，为unix时间戳，示例为2018/11/26 11:25:59过期