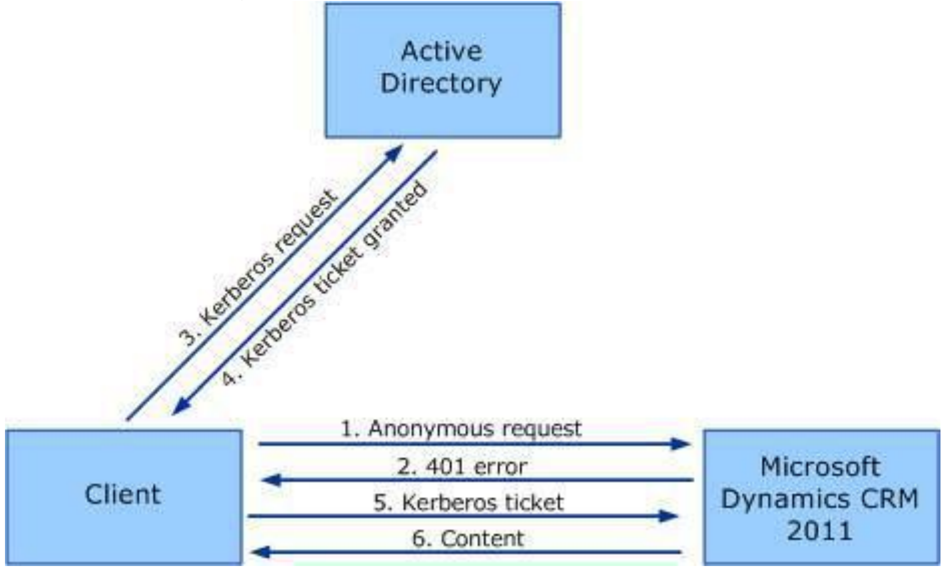
CRM 2011 – Authentication Model

Authentication models supported by Microsoft Dynamics CRM 2011. Understanding the security model is very critical to architecting solutions for Dynamics CRM. The security model determination could be influenced by various factors like Online vs On-premise, upgrade from 4.0 scenario, partial trusts between domains etc.

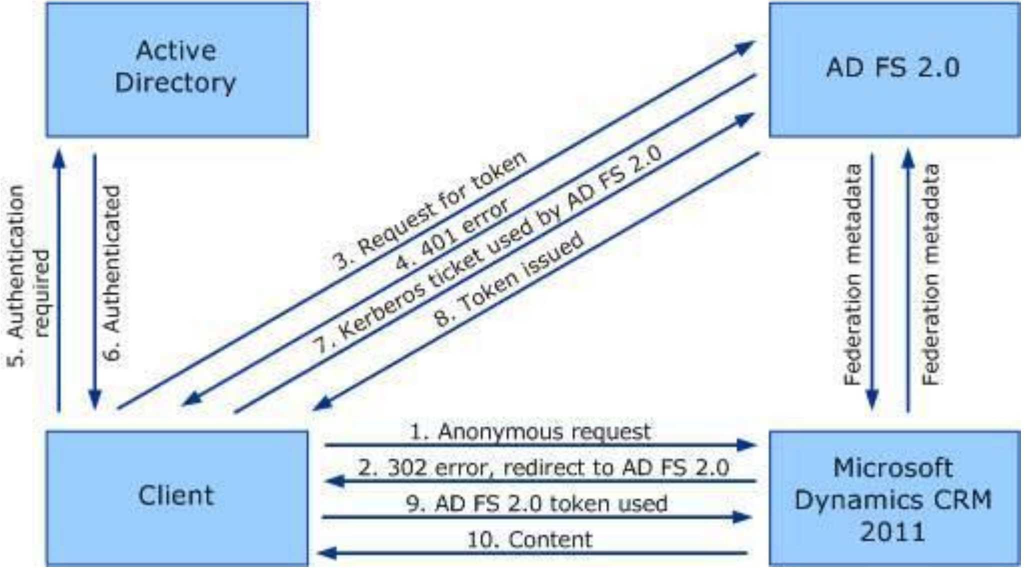
Microsoft Dynamics CRM supports the following authentication scenarios.

1. Active Directory



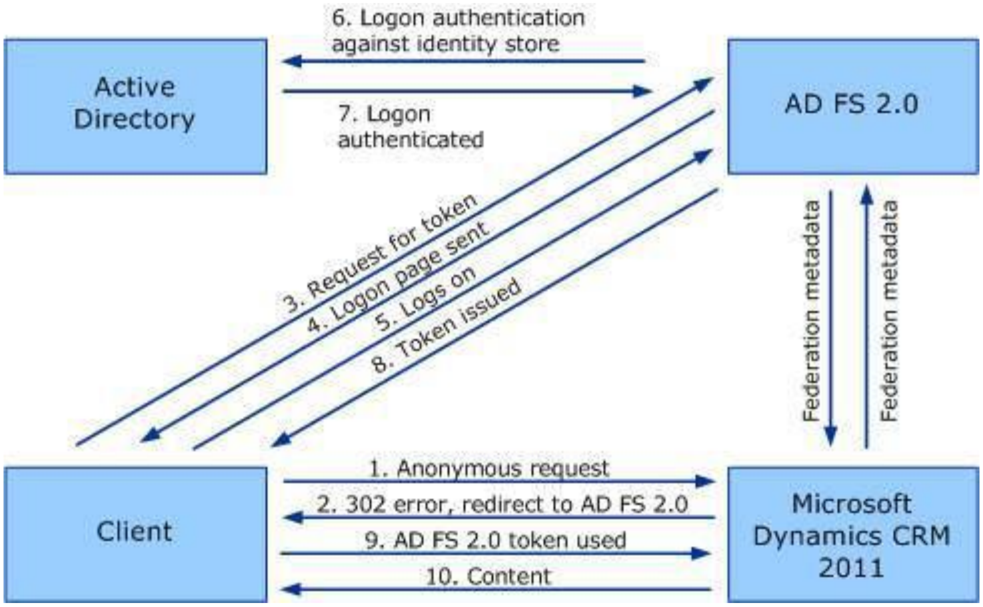
So, active directory authentication is pretty straightforward. As in the picture above, the client uses the Kerberos ticket granted by AD to authenticate with CRM.

2. Active Directory through Federation/Claims based internal

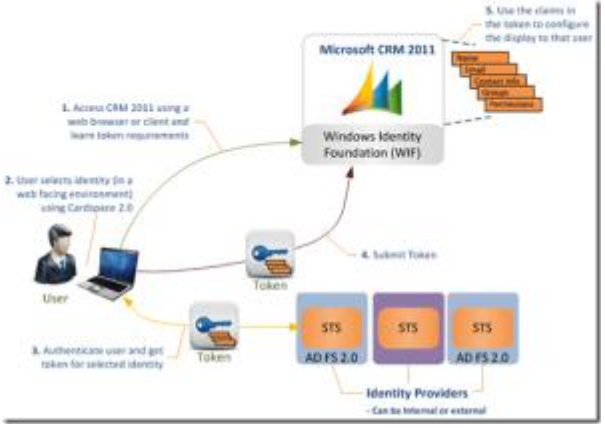


So for multiple domain non-trusted environments, ADFS 2.0 could come to rescue as a trusted claims provider to facilitate internal authentication. After authenticated with the client's domain, the Kerberos ticket is used to obtain claims token from federation service which is used by the client to authenticate with CRM.

3. Claims based external scenarios



Unlike the internal claims based scenario, the user authentication here does not include Kerberos ticket. On successful authentication, ADFS issues the token which is used by the client to authenticate with CRM.


5. Use the claims in the token to configure the display to that user
Microsoft CRM 2011
Name
Email
Contact info
Group
Permissions
1. Access CRM 2011 using a web browser or client and learn token requirements
Windows Identity Foundation (WIF)
2. User selects identity (in a web facing environment) using Cardspace 2.0
User
Token
4. Submit Token
3. Authenticate user and get token for selected identity
Token
STS
AD FS 2.0
STS
STS
AD FS 2.0
Identity Providers
- Can be Internal or external

Deployment Types Support

Deployment	Authentication model
Microsoft Dynamics CRM Online	Claims-based or Active Directory (through federation)
Microsoft Dynamics CRM 2011 on-premises	Claims-based or Active Directory
Microsoft Dynamics CRM 2011 (IFD)	Claims-based or Active Directory

OrganizationServiceProxy

Thankfully, for all our API calls, the authentication complexity is taken care of by the organization service proxy. As you will find in SDK samples, code below can be used to get an instance of the organization proxy.

```
using (OrganizationServiceProxy _serviceProxy = new OrganizationServiceProxy(organizationUri, homeRealmUri, userCredentials, deviceCredentials))
```

OR

```
OrganizationServiceProxy _serviceProxy = ServerConnection.GetOrganizationProxy(serverConfig)
```

Impersonation:

An Active Directory account always impersonates a CRM User to perform CRM operations. Even if the impersonated CRM User is directly associated with the Active Directory account. An Execution Account must provide a Caller for CRM operations, either directly or indirectly. Therefore, impersonation is unavoidable. It holds true that CRM impersonation implicitly inherits ASP.Net impersonation, which does not explicitly declare a Caller unless specifically configured. Ergo, impersonation can occur implicitly, or explicitly.

Explicit Impersonation:

Explicit Impersonation can be done using CallerID property of organizationserviceproxy.

```
OrganizationServiceContext orgContext = new OrganizationServiceContext(_serviceProxy);
_userId = (from user in orgContext.CreateQuery<SystemUser>()where user.FullName == “John Doe”
select user.SystemUserId.Value).FirstOrDefault();
// Explicit Impersonation
_serviceProxy.CallerId = _userId;
```

The user (impersonator) must have the ActOnBehalfOf privilege or be a member of the PrivUserGroup group inActive Directory.

Supported Authentication Scenarios

Microsoft Dynamics CRM supports the following authentication scenarios for each deployment type.

How Claims-based Authentication Works

A request to authenticate a user is sent from Microsoft Dynamics CRM 2011 or Microsoft Dynamics CRM Online or a custom application to the STS server. The STS server determines whether the user should be authenticated, and if so, issues a signed and encrypted SAML token that contains user authentication information. The token has a finite life span and may have to be periodically refreshed depending on how long your application is using the token. This is discussed in more detail later in this topic.

How Active Directory Authentication Works

A request to authenticate a user is sent from Microsoft Dynamics CRM or a custom application to Active Directory. The WCF stack manages the authentication process for Microsoft Dynamics CRM SDK API calls from an application, whereas Internet Information Services (IIS) manages authentication for a web application.

Unsupported Authentication Scenarios

Use of client certificates is not supported by the Microsoft Dynamics CRM SDK. If you configure the Microsoft Dynamics CRM website to require IIS client certificates, you will get authentication failures for any applications that were built using the SDK.

[Applies to: Microsoft Dynamics CRM 2011 and Microsoft Dynamics CRM Online]

Claims-based authentication provides an industry standard security protocol to authenticate a user on a host computer. Claims-based authentication is a set of WS-* standards describing the use of a Security Assertion Markup Language (SAML) token in either passive mode (when WS-Federation is used with the Microsoft Dynamics CRM 2011 and Microsoft Dynamics CRM Online web application) or active mode (where WS-Trust in used with Windows Communication Foundation (WCF) clients). This authentication works together with WCF to provide secure user authentication and a communication channel with a Microsoft Dynamics CRM server. All Microsoft Dynamics CRM editions support claims-based authentication.

Claims-based authentication requires the availability of a security token service (STS) running on a server. An STS server can be based on Active Directory Federation Services (AD FS) V2, or any platform that provides the official STS protocol. For more information, see the following topics in the Microsoft Dynamics CRM 2011 Implementation Guide:

To access a claims configured Microsoft Dynamics CRM 2011 or Microsoft Dynamics CRM Online server by using the Microsoft Dynamics CRM SDK methods, you must first install Windows Identity Foundation (WIF) on your development computer. The Windows Identity Foundation download installs the Microsoft.IdentityModel.dll assembly, which is referenced by the Microsoft Dynamics CRM SDK assemblies at run time. This requirement applies only to code built using Microsoft .NET Framework 4. Microsoft .NET Framework 4.5 includes the required identity namespace.