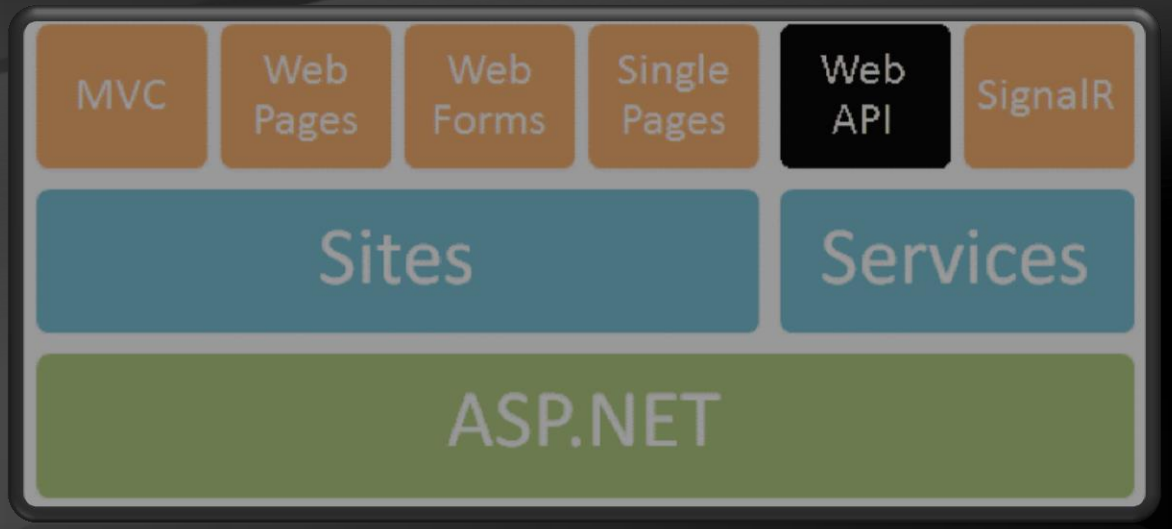
Telerik Academy



ASP.NET Identity

ASP.NET Web Forms

Telerik Software Academy

http://academy.telerik.com

ASP.NET

.Net Ninja

Telerik Academy

Table of Contents

- Basics of Authentication and Authorization
- Old ASP.NET Membership
  - Windows Authentication
  - Forms Authentication
- Old Users and Roles
- Old Membership Provider
- Getting Current User Information at the server

Telerik Academy

Table of Contents

- Introduction to ASP.NET Identity
- Basic ASP.NET Identity Template
- Database Identity Tables
- Basic functionality
- Extending the built-in user profile
- User roles
- OAuth 2.0 authentication
- Cookie information

Telerik Academy

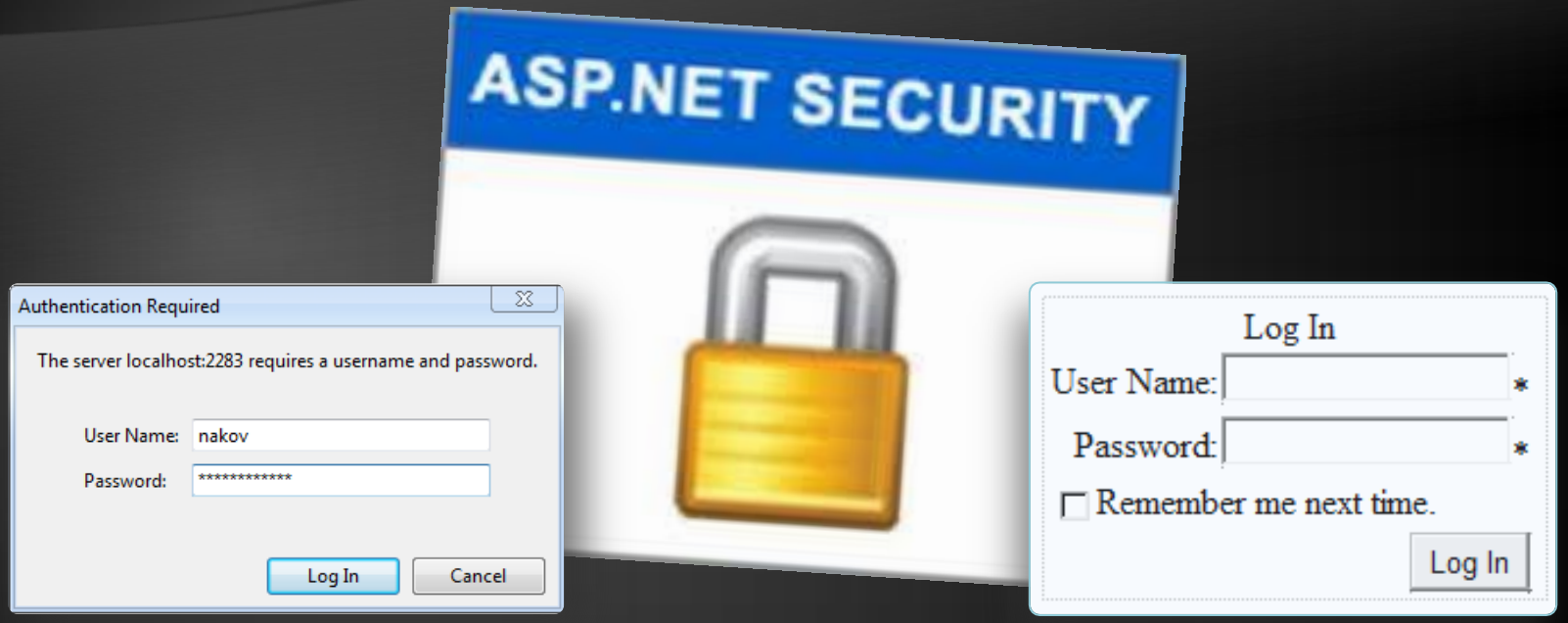
Authentication and Authorization

Main difference

Basics

- Authentication
  - The process of verifying the identity of a user or computer
  - Questions: Who are you? How you prove it?
  - Credentials can be password, smart card, etc.
- Authorization
  - The process of determining what a user is permitted to do on a computer or network
  - Question: What are you allowed to do?

Telerik Academy



Old Windows and Forms Authentication in ASP.NET

Telerik Academy

Old Authentication in ASP.NET

- Windows Authentication
  - Uses the security features integrated into the Windows operating systems
  - Uses Active Directory / Windows accounts
- Forms Authentication
  - Uses a traditional login / logout pages
  - Code associated with a Web form handles users authentication by username / password
  - Users are usually stored in a database

Telerik Academy

Windows Authentication

- In Windows Authentication mode the Web application uses the same security scheme that applies to your Windows network
- Network resources and Web applications use the same:
  - User names
  - Passwords
  - Permissions
- It is the default authentication when a new Web site is created

Telerik Academy

Windows Authentication (2)

- The user is authenticated against his username and password in Windows
  - Known as NTLM authentication protocol
- When a user is authorized:
  - ASP.NET issues an authentication ticket (which is a HTTP header)
  - Application executes using the permissions associated with the Windows account
  - The user's session ends when the browser is closed or when the session times out

Windows Authentication (3)

- Users who are logged on to the network
  - Are automatically authenticated
  - Can access the Web application
- To set the authentication to Windows add to the `Web.config`:

```
<authentication mode="Windows" />
```

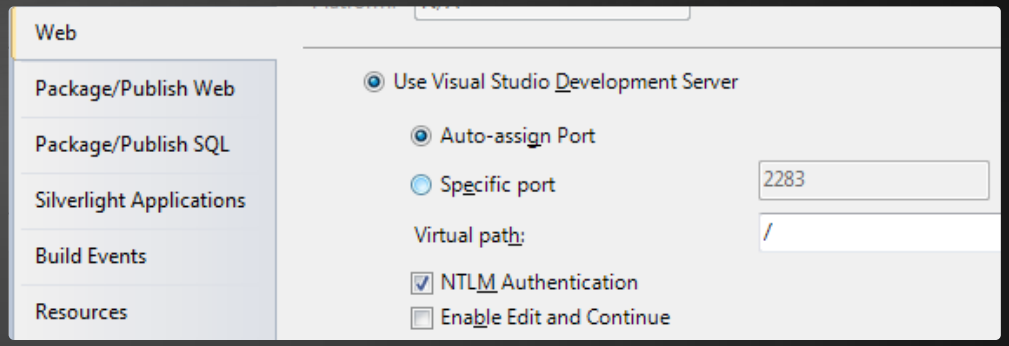
- To deny anonymous users add:

```
<authorization>
  <deny users="?"/>
</authorization>
```

Telerik Academy

Windows Authentication (4)

- The Web server should have NTLM enabled:



- HTTP requests:

```
GET /Default.aspx HTTP/1.1
…
```

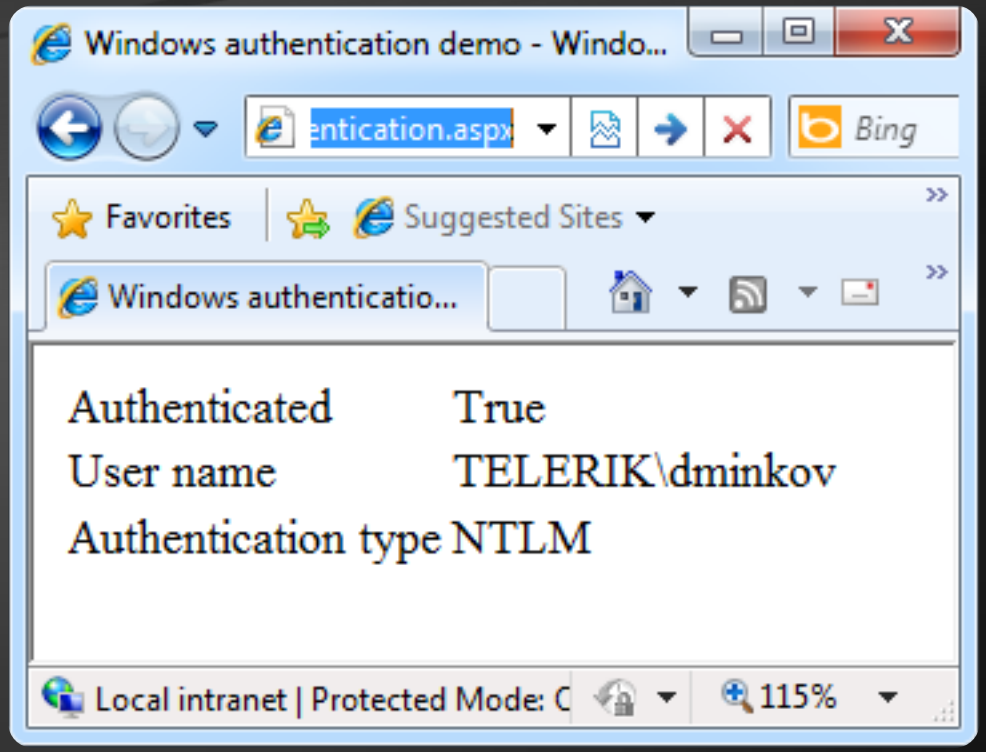
```
GET /Default.aspx HTTP/1.1
Authorization: NTLM tESsB/
yNY3lb6a0L6vVQEZNqwQn0sqZ…
```

- HTTP responses:

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: NTLM
```

```
HTTP/1.1 200 OK
…
<html> … </html>
```

Telerik Academy



Windows Authentication

Live Demo

Telerik Academy

Forms Authentication

- Forms Authentication uses a Web form to collect login credentials (username / password)
- Users are authenticated by the C# code behind the Web form
- User accounts can be stored in:
  - `Web.config` file
  - Separate user database
- Users are local for the Web application
  - Not part of Windows or Active Directory

Forms Authentication (2)

- Enabling forms authentication:
  - Set authentication mode in the `Web.config` to `"Forms"`

```
<authentication mode="Forms" />
```

  - Create a login ASPX page
  - Create a file or database to store the user credentials (username, password, etc.)
  - Write code to authenticate the users against the users file or database

Telerik Academy

Configuring Authorization in Web.config

- To deny someone's access add <deny users="…"> in the <authorization> tag
- To allow someone's access add <allow users="…"> in the authorization tag
- <deny users="?" /> denies anonymous access

```
<system.web>
  <authorization>
    <deny users="?"/>
  </authorization>
</system.web>
```

- <deny users="*" /> denies access to all users

Telerik Academy

Configuring Authorization in Web.config (2)

- Specifying authorization rules in Web.config:

```
<location path="RegisterUser.aspx">
  <system.web>
    <authorization>
      <allow roles="admin" />
      <allow users="Pesho,Gosho" />
      <deny users="*" />
    </authorization>
  </system.web>
</location>
```

- The deny/allow stops the authorization process at the first match
  - Example: if a user is authorized as Pesho, the tag <deny users="*" /> is not processed

Telerik Academy

Implementing Login / Logout

- Logging-in using credentials from `Web.config`:

```
if (FormsAuthentication.Authenticate(username, passwd))
{
  FormsAuthentication.RedirectFromLoginPage(
    username, false);
}
else
{
  lblError.Text = "Invalid login!";
}
```

This method creates a cookie (or hidden field) holding the authentication ticket.

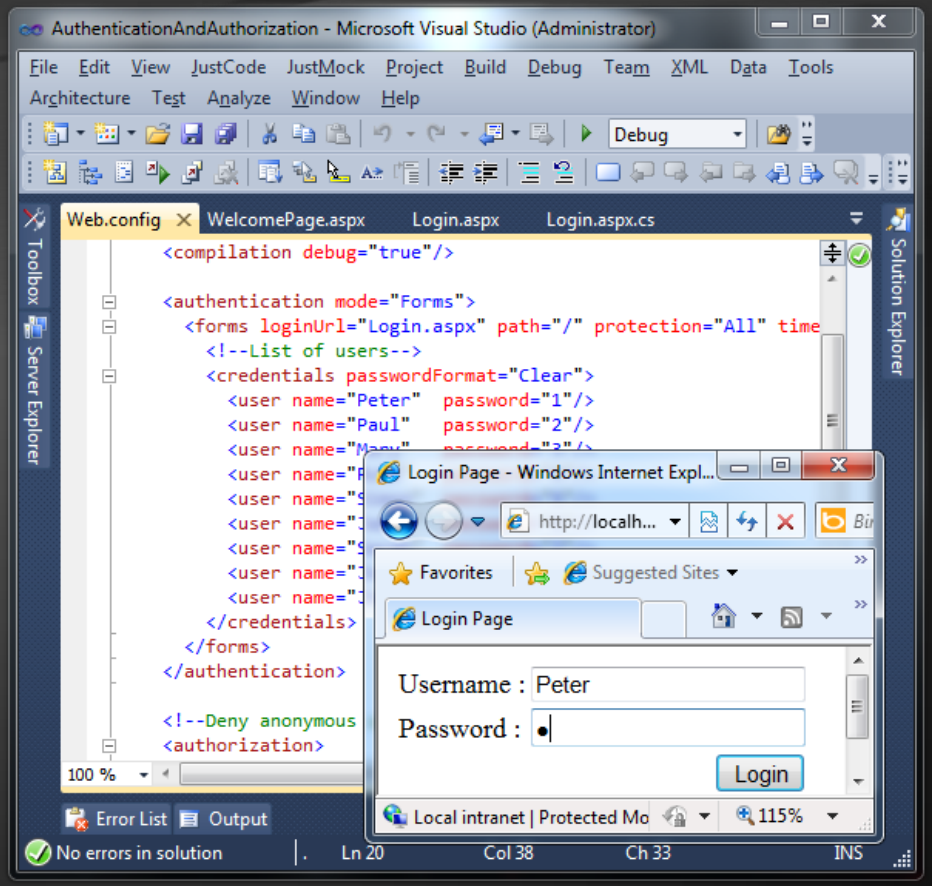
- Logging-out the currently logged user:

```
FormsAuthentication.SignOut();
```

- Displaying the currently logged user:

```
lblInfo.Text = "User: " + Page.User.Identity.Name;
```

Telerik Academy



Forms Authentication

Live Demo

Telerik Academy

Old Users and Roles

Membership Provider and Roles Provider

Telerik Academy

Users, Roles and Authentication

- User is a client with a Web browser running a session with the Web application
- Users can authenticate (login) in the Web application
  - Once a user is logged-in, a set of roles and permissions are assigned to him
  - Authorization in ASP.NET is based on users and roles
  - Authorization rules specify what permissions each user / role has

Telerik Academy

ASP.NET Membership Providers

- Membership providers in ASP.NET
  - Simplify common authentication and user management tasks
    - `CreateUser()`
    - `DeleteUser()`
    - `GeneratePassword()`
    - `ValidateUser()`
    - …
  - Can store user credentials in database / file / etc.

Telerik Academy

Roles in ASP.NET

- Roles in ASP.NET allow assigning permissions to a group of users
  - E.g. "Admins" role could have more privileges than "Guests" role
- A user account can be assigned to multiple roles in the same time
  - E.g. user "Peter" can be member of "Admins" and "TrustedUsers" roles
- Permissions can be granted to multiple users sharing the same role

Telerik Academy

ASP.NET Role Providers

- Role providers in ASP.NET
  - Simplify common authorization tasks and role management tasks
    - `CreateRole()`
    - `IsUserInRole()`
    - `GetAllRoles()`
    - `GetRolesForUser()`
    - …
  - Can store user credentials in database / file / etc.

Telerik Academy

Registering a Membership Provider

- Adding membership provider to the `Web.config`

```
<membership defaultProvider="MyMembershipProvider">
  <providers>
    <add connectionStringName="UsersConnectionString"
      minRequiredPasswordLength="6"
      requiresQuestionAndAnswer="true"
      enablePasswordRetrieval="false"
      requiresUniqueEmail="false"
      applicationName="/MyApp"
      minRequiredNonalphanumericCharacters="1"
      name="MyMembershipProvider"
      type="System.Web.Security.SqlMembershipProvider"/>
  </providers>
</membership>
```

Telerik Academy

Registering a Role Provider

- To register role provider in ASP.NET 4.0 add the following to the `Web.config`:

```
<roleManager enabled="true" defaultProvider="MyRoleProvider">
  <providers>
    <add connectionStringName="UsersConnectionString"
      name="MyRoleProvider"
      type="System.Web.Security.SqlRoleProvider" />
  </providers>
</roleManager>

<connectionStrings>
  <add name="UsersConnectionString"
    connectionString="Data Source=.\SQLEXPRESS;Initial
      Catalog=Users;Integrated Security=True"
    providerName="System.Data.SqlClient" />
</connectionStrings>
```

Telerik Academy

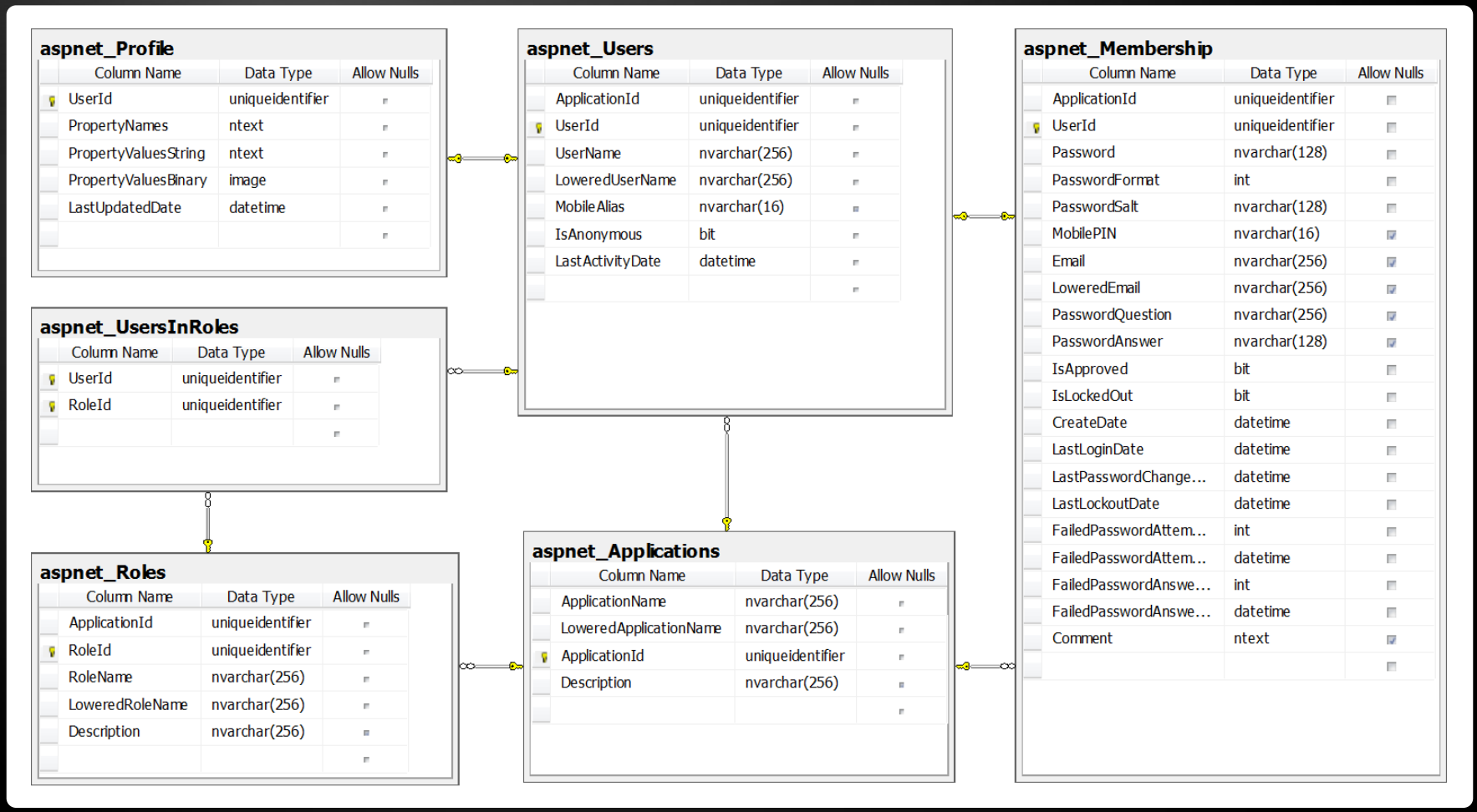
The SQL Registration Tool: aspnet_regsql

- The built-in classes `System.Web.Security.SqlMembershipProvider` and `System.Web.Security.SqlRoleProvider` use a set of standard tables in the SQL Server
  - Can be created by the ASP.NET SQL Server Registration tool (`aspnet_regsql.exe`)
  - The `aspnet_regsql.exe` utility is installed as part of with ASP.NET 4.0:

```
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\
aspnet_regsql.exe
```

Telerik Academy

The Standard ASP.NET Applications Database Schema



Telerik Academy

ASP.NET Membership API

- Implementing login:

```
if (Membership.ValidateUser(username, password))
{
  FormsAuthentication.RedirectFromLoginPage(
    username, false);
}
```

- Implementing logout:

```
FormsAuthentication.SignOut();
```

- Creating new user:

```
Membership.CreateUser(username, password);
```

Telerik Academy

ASP.NET Membership API (2)

- Getting the currently logged user:

```
MembershipUser currentUser = Membership.GetUser();
```

- Creating new role:

```
Roles.CreateRole("Admins");
```

- Adding user to existing role:

```
Roles.AddUserToRole("admin", "Admins");
```

- Deleting user / role:

```
Membership.DeleteUser("admin", true);
Roles.DeleteRole("Admins");
```

Telerik Academy

Membership Provider

Live Demo

Telerik Academy

Getting User Information

From the Back-end C#

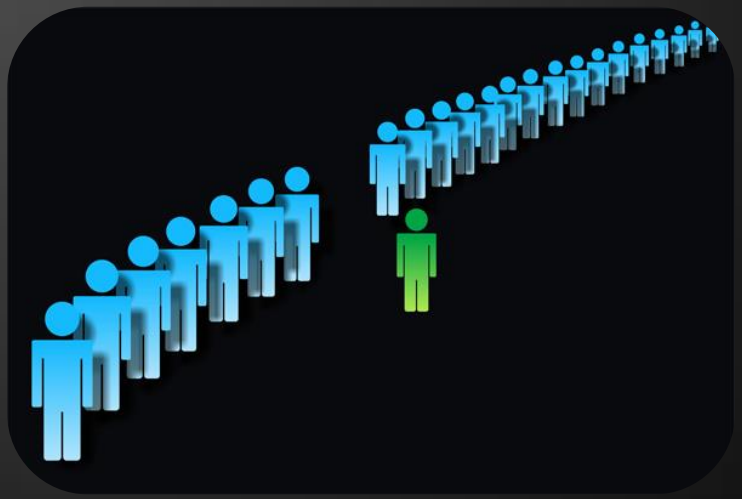
Getting User Information

- You can get basic user information by using the User class in the back-end
- By User class:
  - IsInRole(string) method
  - Identity property
    - string Name property
    - bool IsAuthenticated property
    - string AuthenticationType property

Telerik Academy

Introduction to Identity

Who are you?



ASP.NET Identity

- The new membership system for building ASP.NET applications
- Makes it easy to integrate user specific profile data with the application data
- Allows you to control the persistence model of your application
  - Local database
  - External service store

Telerik Academy

Basic Template With Identity

- Creates basic web application
- Contains useful libraries
- Contains User access options
- Ready to use:
  - Models for extending profiles
  - Register, Login, Manage pages
  - Local cookie-based authentication
  - Remote OAuth services – Facebook, Google, Twitter, etc.

Telerik Academy

Basic Template

Live Demo with Web Forms and MVC

Telerik Academy

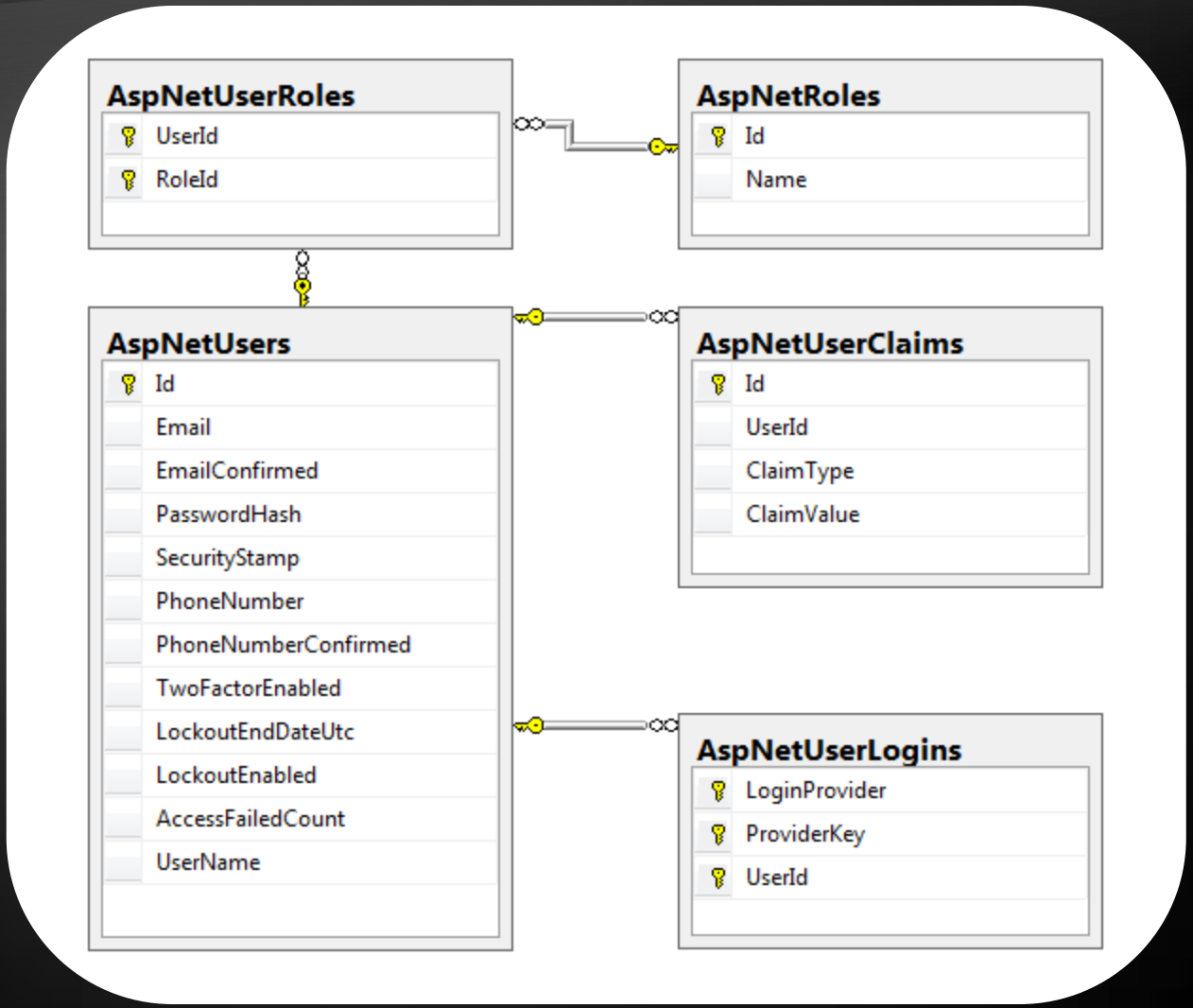
Identity Database

Where are you?

Local Database Tables

- Tables
  - AspNetRoles – role types
  - AspNetUserClaims – external services claims
  - AspNetUserLogins – user logins and types
  - AspNetUserRoles – user roles
  - AspNetUsers – user profile information

Local Database Tables



Telerik Academy

Local Database

Live Demo with Web Forms and MVC 5

Telerik Academy

Basic Functionality

This is how we do it!

Register

- Front-end
  - Provide fields for Username, Password, etc.
  - Provide submit button
  - Provide validation messages
- Back-end
  - Get UserManager
  - Create User instance
  - Create local user through IdentityManager
  - If success – sign in and redirect the page

Login

- Front-end
  - Provide fields for Username, Password
  - Provide submit button
  - Provide validation messages
- Back-end
  - Get UserManager
  - Use PasswordSignIn
  - Log in the user
  - If success – redirect the page to return URL

Telerik Academy

Register and Login

Live Demo with Web Forms and MVC 5

Telerik Academy

Extending User Profile

Additional properties

Extending User Profile

- Steps
  - Add properties to Models/IdentityModel/ApplicationUser
  - ApplicationDbContext should inherit IdentityDbContext and have constructor
  - Enable migrations for the project/data layer
  - In Global.asax add database initializer
  - All UserManager instances should take ApplicationDbContext as parameter
  - Use ApplicationUser everywhere

Telerik Academy

Extended User Profile

Live Demo with Web Forms

Telerik Academy

User Roles

Who is authorized

User Roles

- Role-based authorization
- Control over the application modules
- Categorizing users and memberships
- Defined in Web.config

```
<location path="About">
    <system.web>
      <authorization>
        <allow roles="Admin"/>
        <deny users="*"/>
      </authorization>
    </system.web>
</location>
```

Telerik Academy

User Roles

Live Demo with Web Forms

Telerik Academy

Remote Authentication

Easier than your ex!

Telerik Academy

Claims-base authentication (1)

- Claims
  - Piece of information identifying user
  - Sent as key-value pairs
  - Contains authentication token and/or signature
- Claims-based authentication
  - Users authenticate on remote system
  - Information is passed to the application
  - User is authenticated and recognized

Telerik Academy

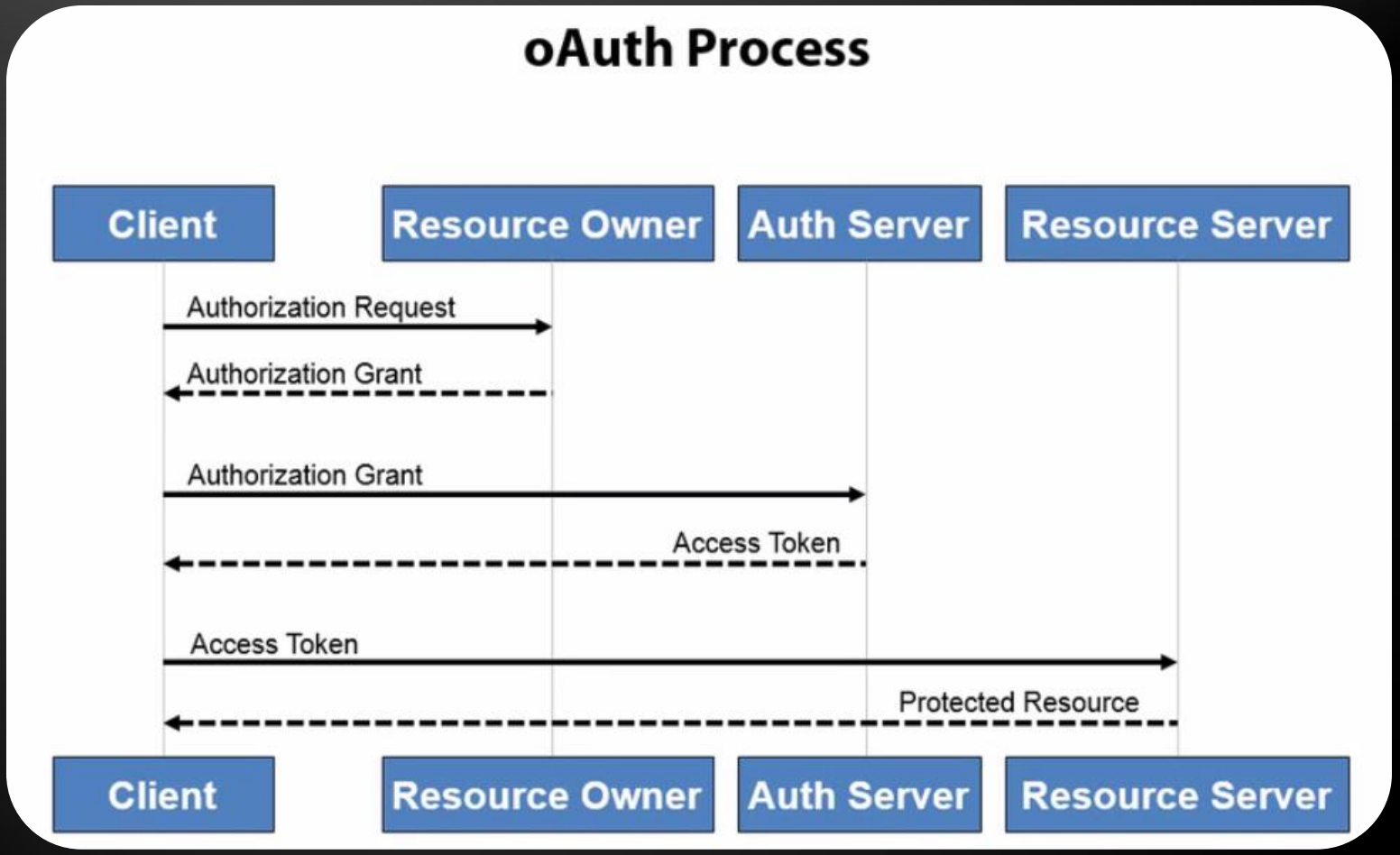
Claims-base authentication (2)

- Authentication flow
  - User makes request to application
  - System redirects to external page
  - After authentication the external system returns back to the application with user information
  - Application makes request to external system to validate user
  - User gets access to the application

OAuth2

- OAuth
  - Allow secure authentication
  - Simple and standard protocol
  - Can be used by web, desktop or mobile apps
- Steps
  - Users tries to authenticate at application
  - Application relies on remote service
  - Application receives access token
  - User gets access

OAuth2 Process



Telerik Academy

Facebook Authentication

Live Demo with Web Forms

Telerik Academy

Cookie Information

Where to find user information

Cookie

- Identity cookie: .AspNet.Application
- Contains information about the application
- Contains information about the logged user
- Heavily encrypted
- If wrong hands find it – serious damage!
- For security – use https/SSL protocol

Telerik Academy

Cookie Information

Live Demo with Web Forms

Telerik Academy

ASP.NET Identity

http://academy.telerik.com

Homework

1. Create a Chat canal web application.
   - Users must have First name, Last name and e-mail fields. Display name should be First name + Last Name
   - There is only one canal where every registered user can only post (create) a message
   - There must be Moderator role, which can post and edit all the posted content
   - There must be Administrator role, which can post, edit and delete all the posted content

Free Trainings @ Telerik Academy

- C# Programming @ Telerik Academy
  - csharpfundamentals.telerik.com

- Telerik Software Academy
  - academy.telerik.com

- Telerik Academy @ Facebook
  - facebook.com/TelerikAcademy

- Telerik Software Academy Forums
  - forums.academy.telerik.com