Identity & Access Control in .NET (Core)

Dominick Baier
http://leastprivilege.com
@leastprivilege

Brock Allen
http://brockallen.com
@brocklallen

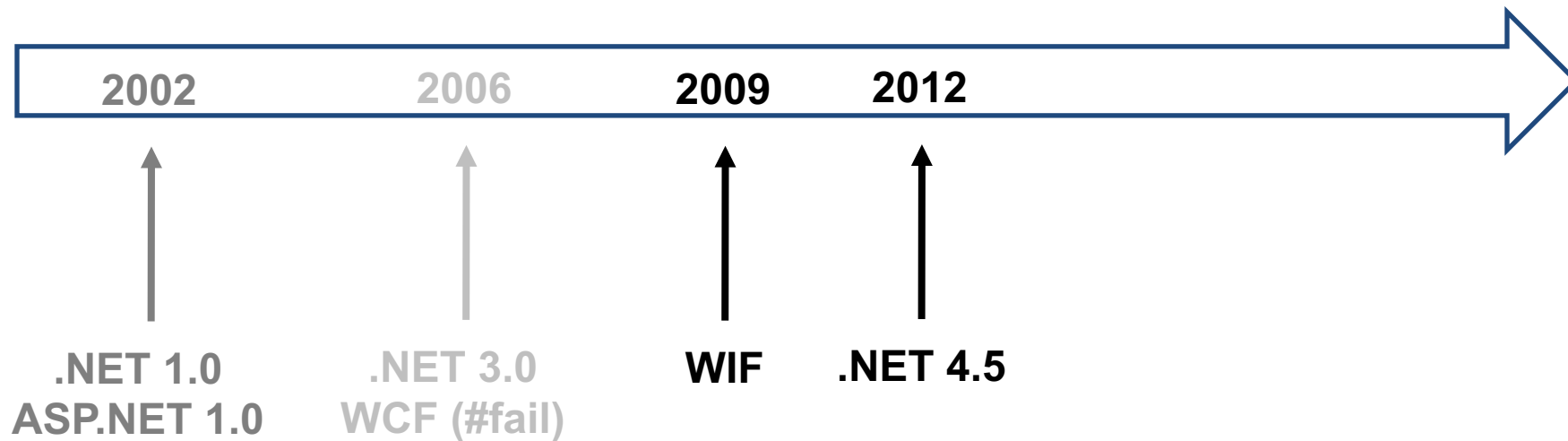# Modern Application Architecture
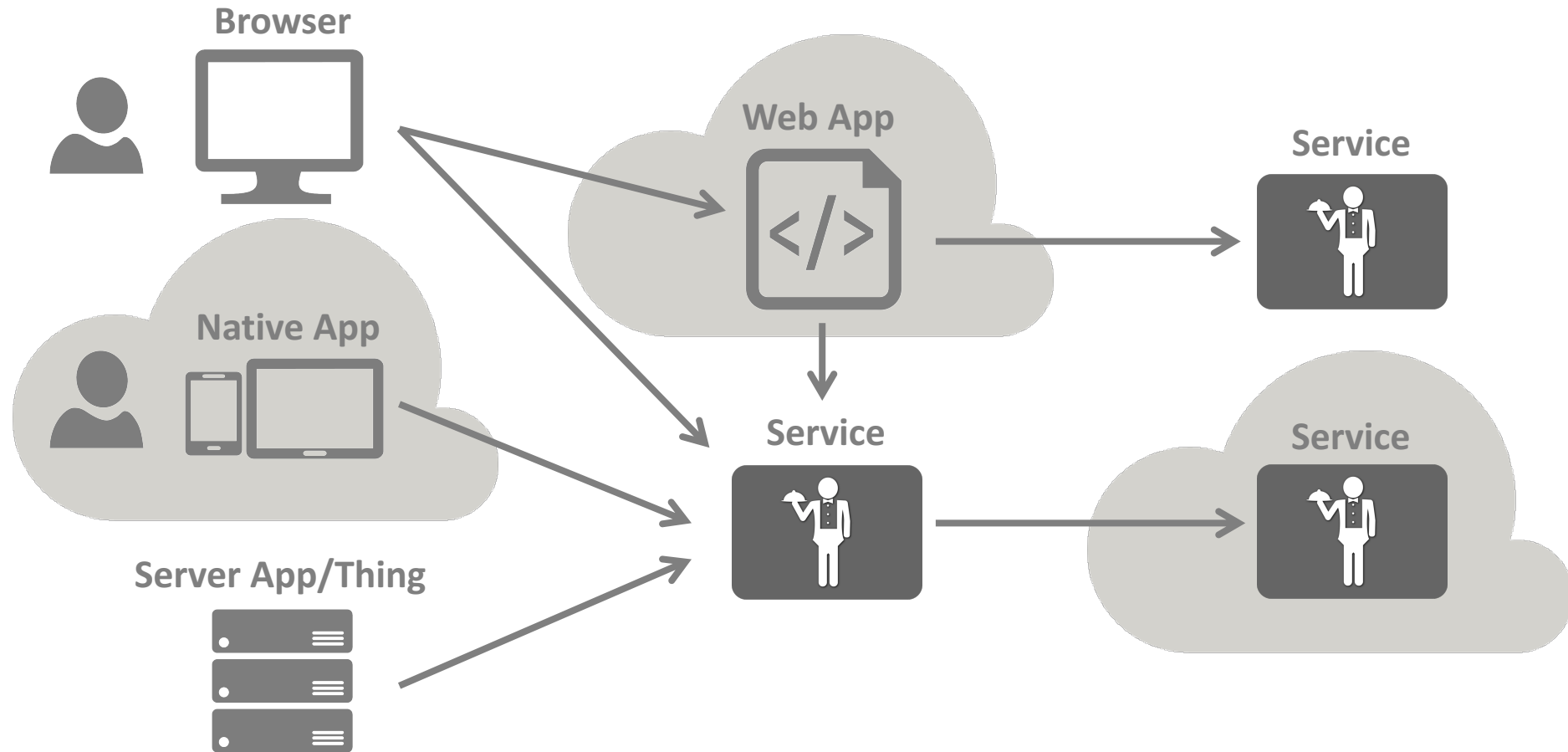
Initial Design

```
public interface IIdentity
{
  bool IsAuthenticated { get; }
  string AuthenticationType { get; }
  string Name { get; }
}
```

```
public interface IPrincipal
{
  IIdentity Identity { get; }
  bool IsInRole(string roleName);
}
```

Updates to .NET Identity over Time

WIF & .NET 4.5

- **Claims-based identity**
- **Support for security tokens**
- **External authentication**

Claims

- **More flexible way to model identity data**
  - keys and values
  - concept of an issuer

- **Claim examples**
  - Bob is an administrator
  - Jim's email address is jim@foo.com
  - Alice's user id is #123
  - Alice works in the sales department

Claim

- **Statement about an entity made by someone else**

```
public class Claim
{
    public virtual string Type { get; }
    public virtual string Value { get; }
    public virtual string Issuer { get; }

    // rest omitted
}
```

ClaimsPrincipal & ClaimsIdentity

```csharp
interface IIdentity
{
  bool IsAuthenticated       { get; }
  string AuthenticationType { get; }
  string Name                { get; }
}
```
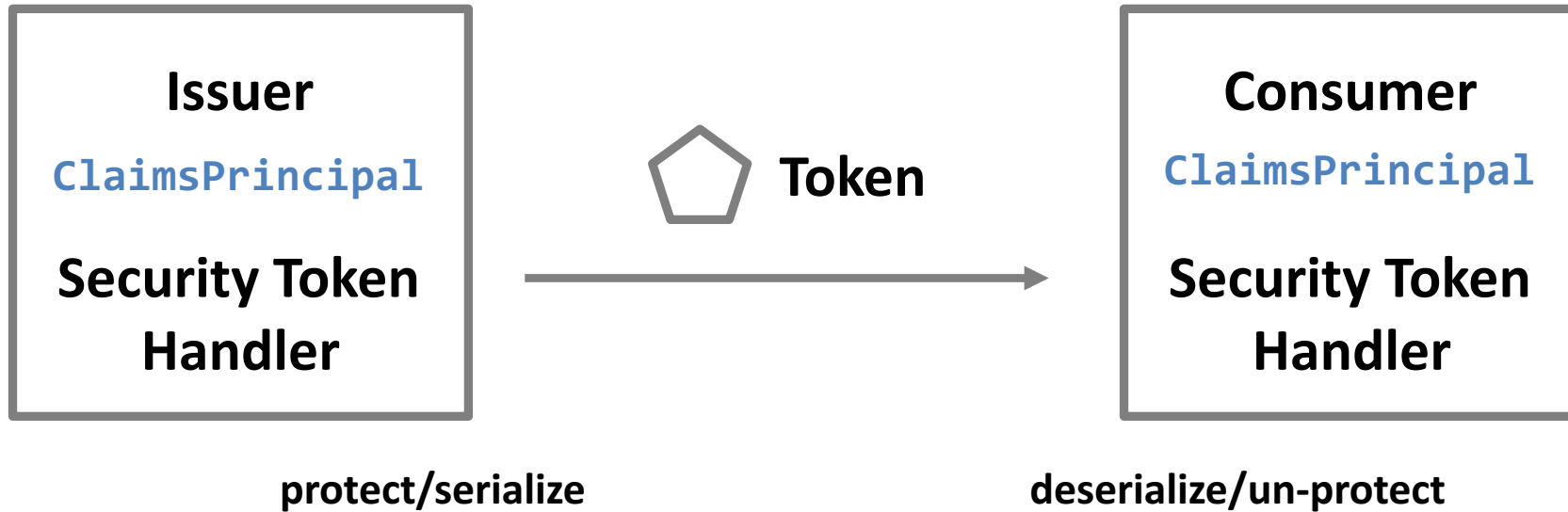
```csharp
interface IPrincipal
{
  IIdentity Identity { get; }
  bool IsInRole(string roleName);
}
```

```csharp
public class ClaimsIdentity : IIdentity
{
  IEnumerable<Claim> Claims { get; }
}
```
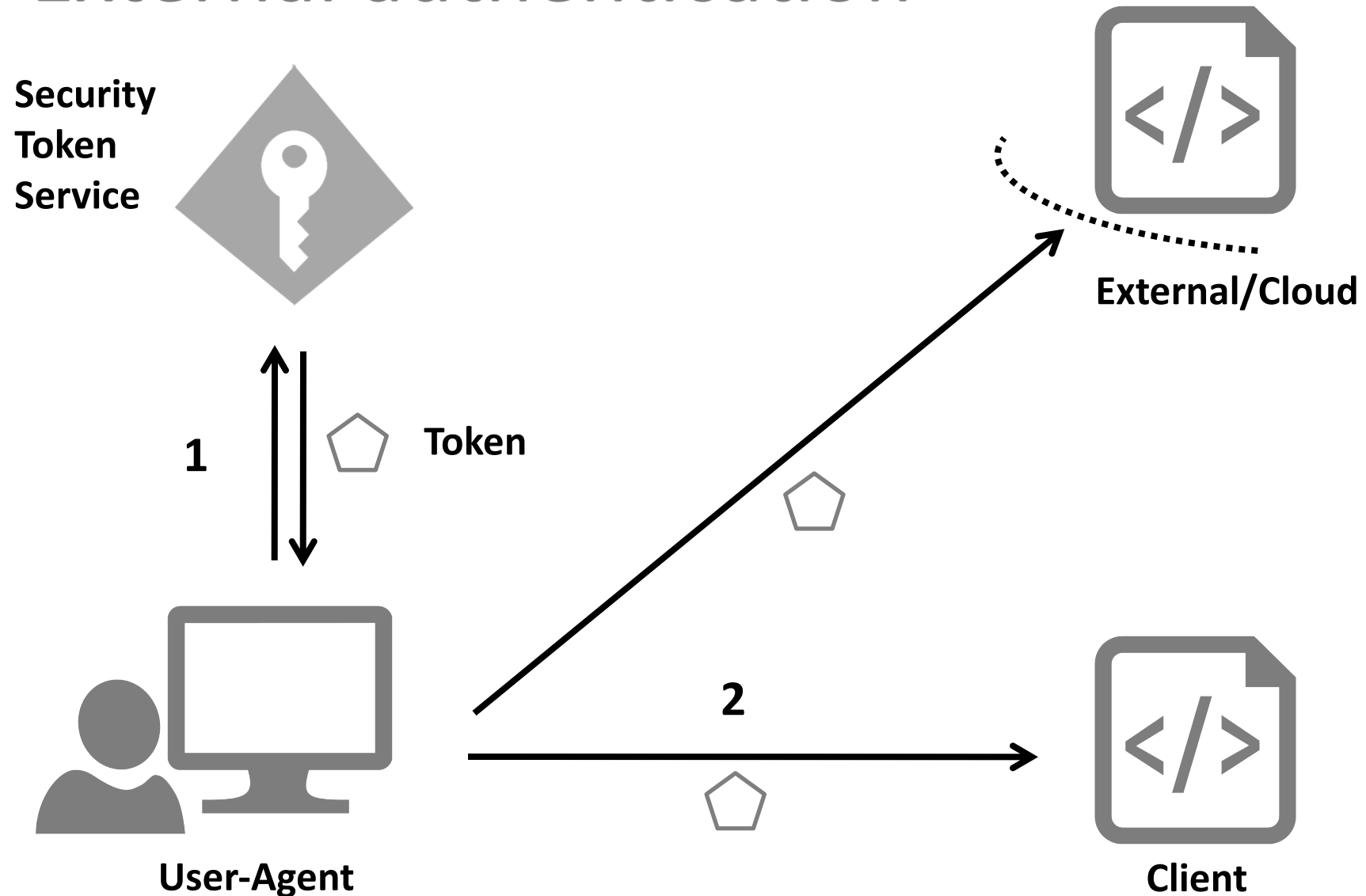
```csharp
public class ClaimsPrincipal : IPrincipal
{
  ReadOnlyCollection<ClaimsIdentity> Identities { get; }
}
```

Security Tokens

External authentication

Security
Token
Service

External/Cloud

1

Token

2

User-Agent

Client

Next...