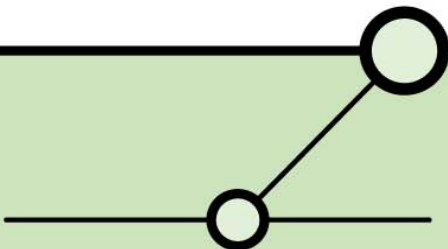


Rollen-basierte Anwendungs-Sicherheit mit Microsoft Authorization Manager

Dominick Baier (dbaier@ernw.de)
www.ernw.de



- Security Consultant und ISO17799 Lead Auditor
- Software Architekt für verteilte Anwendungen unter Windows
 - IIS6
 - .NET Framework
 - XML Web Services
 - SQL Server 2000
- Durchführen von Pen Tests und Audits für Software und Netzwerke

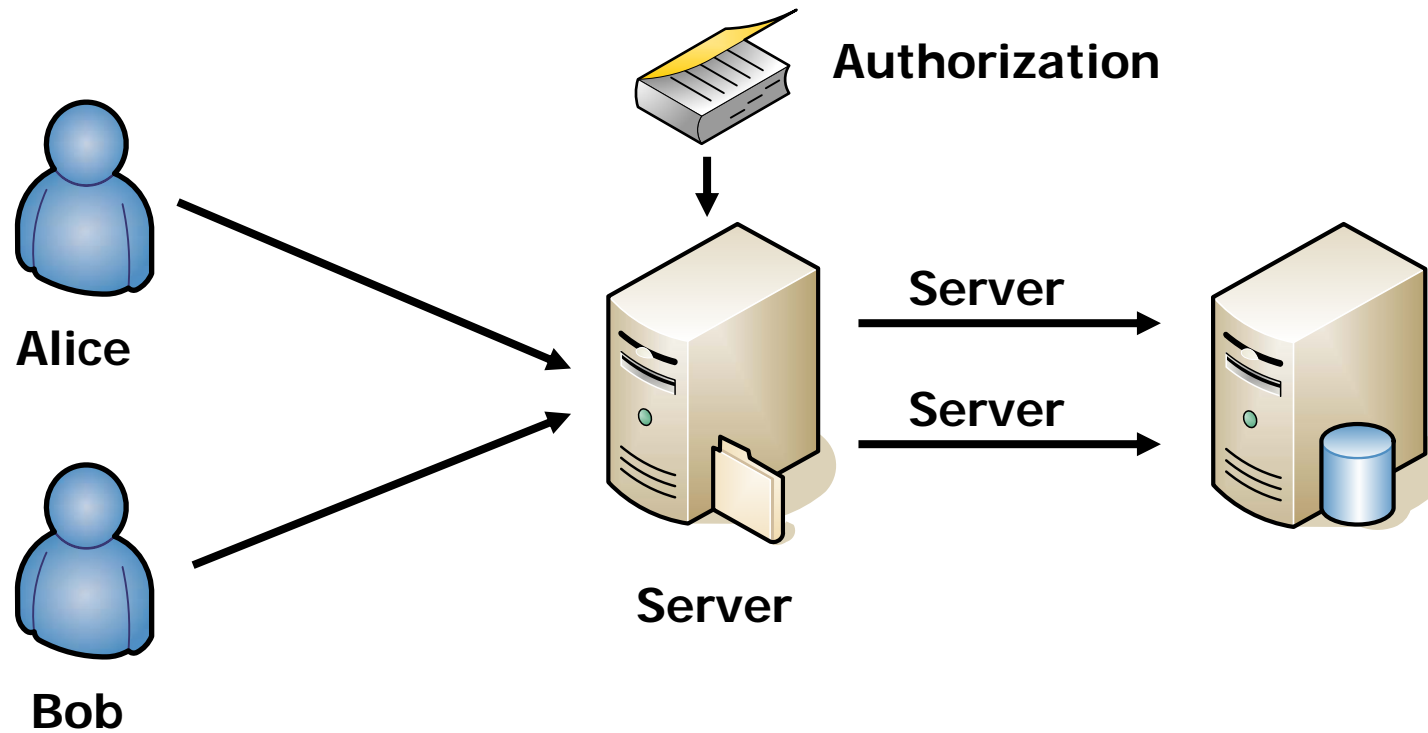
- Neue Betriebssystem Komponente
 - Windows Server 2003
 - Windows 2000 SP4
 - Windows XP SP1

- Soll das Problem der "Anwendungs-verwalteten Autorisierung" lösen

Was ist das ??

- Windows bietet seit der ersten NT Version ACLs auf Betriebssystem-Ressourcen

- Doch wie kann man ACLs auf Geschäfts-Prozesse legen?
 - Neuer Kunde anlegen
 - EMail an Kunde verschicken
 - Spesenabrechnung genehmigen



Die Lösung ?

The screenshot displays three software interfaces. On the left is the 'Exchange System Manager' showing a tree view of connectors. In the top-left is 'SQL Server Enterprise Manager' showing a list of logins for a local instance. On the right is the 'Oracle Enterprise Manager-Konsole, Standalone' showing a hierarchical tree of database objects and a table listing system tables.

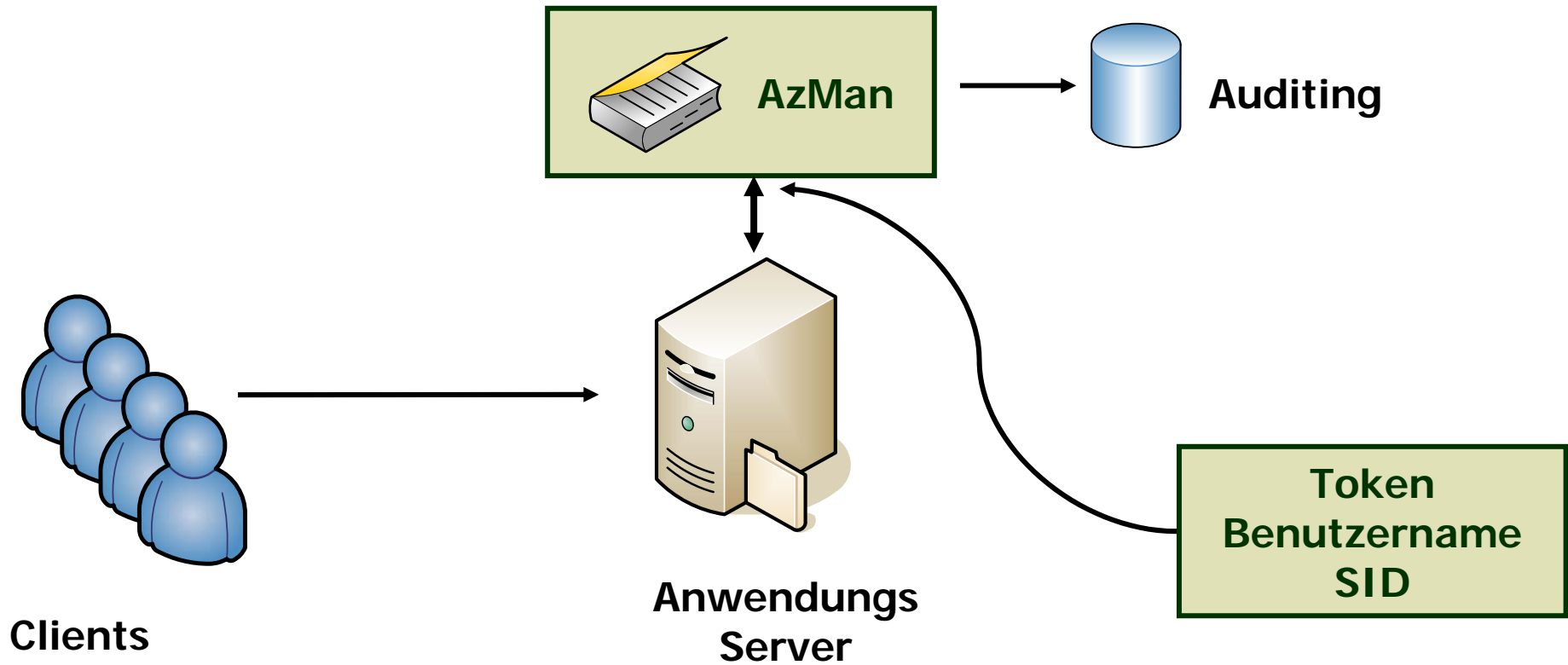
Name	Type	Server Access	Default Date
BUILTIN\Administrators	Windows G...	Permit	master
HOME\dominick	Windows User	Permit	Northwind
nt authority\network service	Windows G...	Permit	master
sa	Standard	Permit	master

Table	Tablespace	Partitioniert	Zeilen	Zuletzt analysiert
ACCESS\$	SYSTEM	No		
AQ\$_MESSAGE_TYPES	SYSTEM	No		
AQ\$_PENDING_MESSAGES	SYSTEM	No		
AQ\$_PROPAGATION_STATUS	SYSTEM	No		
AQ\$_QUEUE_STATISTICS	SYSTEM	No		
AQ\$_QUEUE_TABLE_AFFINITIES	SYSTEM	No		
AQ\$_SCHEDULES	SYSTEM	No		
ARGUMENT\$	SYSTEM	No		
ASSOCIATION\$	SYSTEM	No		
ATEMPTAB\$		No		
ATTRCOL\$	SYSTEM	No		
ATTRIBUTE\$	SYSTEM	No		
AUD\$	SYSTEM	No		
AUDIT\$	SYSTEM	No		
AUDIT_ACTIONS	SYSTEM	No		
BOOTSTRAP\$	SYSTEM	No		
CCOL\$	SYSTEM	No		
CDEF\$	SYSTEM	No		
CLUS\$	SYSTEM	No		
COL\$	SYSTEM	No		
COLLECTION\$	SYSTEM	No		
COLTYPE\$	SYSTEM	No		
COM\$	SYSTEM	No		
CON\$	SYSTEM	No		
CONTEXT\$	SYSTEM	No		
DBMS_ALERT_INFO	SYSTEM	No		
DBMS_LOCK_ALLOCATED	SYSTEM	No		
_default_auditing_options_	SYSTEM	No		
DEFROLES	SYSTEM	No		
DEPENDENCY\$	SYSTEM	No		
DIM\$	SYSTEM	No		
DIMATTR\$	SYSTEM	No		
DIMJOINKEY\$	SYSTEM	No		
DIMLEVEL\$	SYSTEM	No		
DIMLEVELKEY\$	SYSTEM	No		
DIR\$	SYSTEM	No		
DUAL	SYSTEM	No		
DUC\$	SYSTEM	No		
...

- Jede Anwendung muss die Autorisierung selbst durchführen
- Die Autorisierungs-Informationen werden an den unterschiedlichsten Stellen abgelegt
 - Datenbank
 - Text-Datei
 - Active Directory
 - NTFS ACLs

- AzMan bietet eine einfache und einheitliche Schnittstelle für
 - Die Autorisierung selbst
 - Die Speicherung der Konfiguration
 - Das Auditing

Authorization Manager



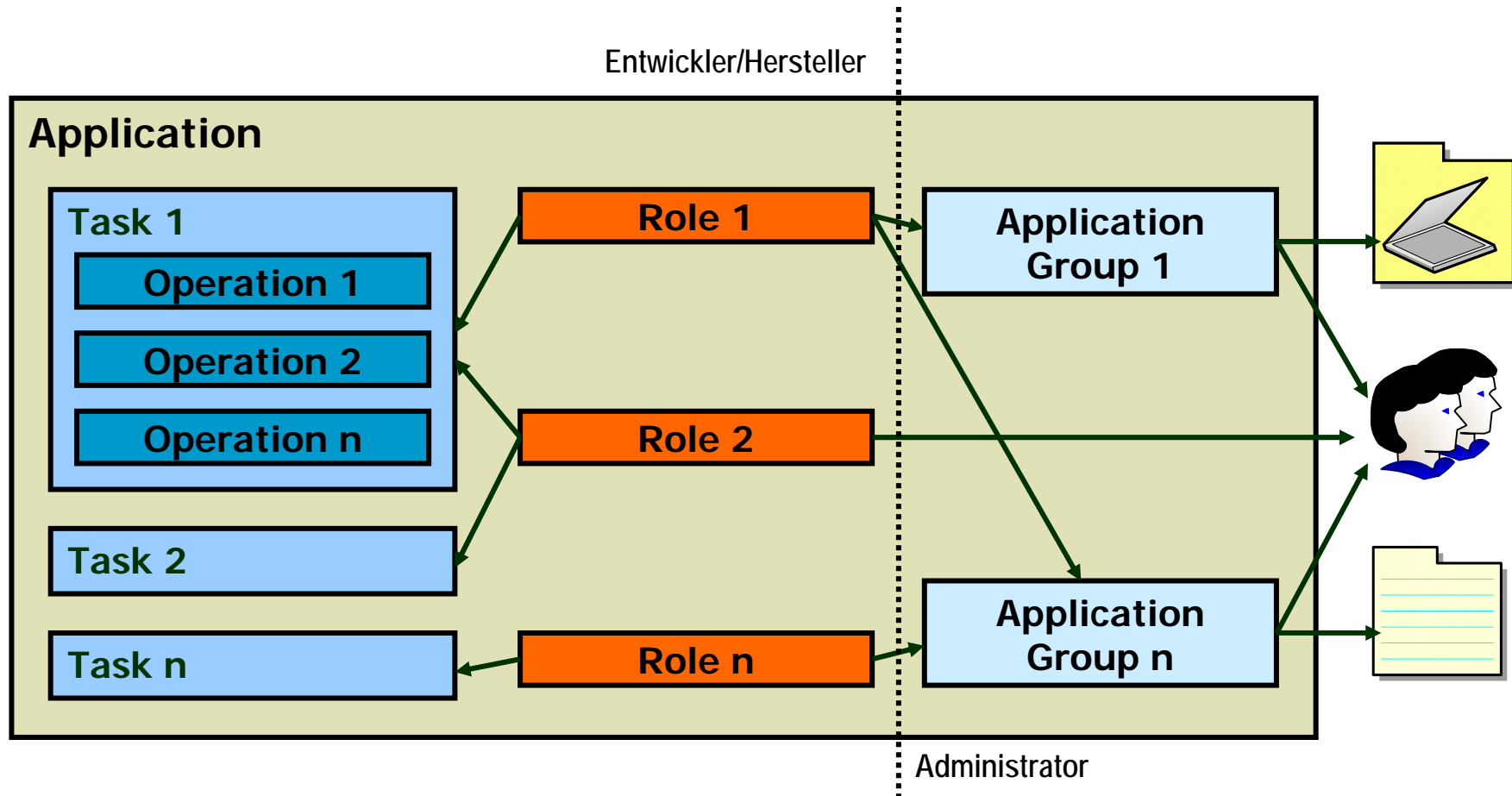
- Zwei Parteien beteiligt
 - Anwendung, die Rechte zu vergeben hat
 - Administrator, der diese Rechte vergibt

- AzMan MMC SnapIn verfügt deshalb über zwei Modi
 - Developer
 - Administrator

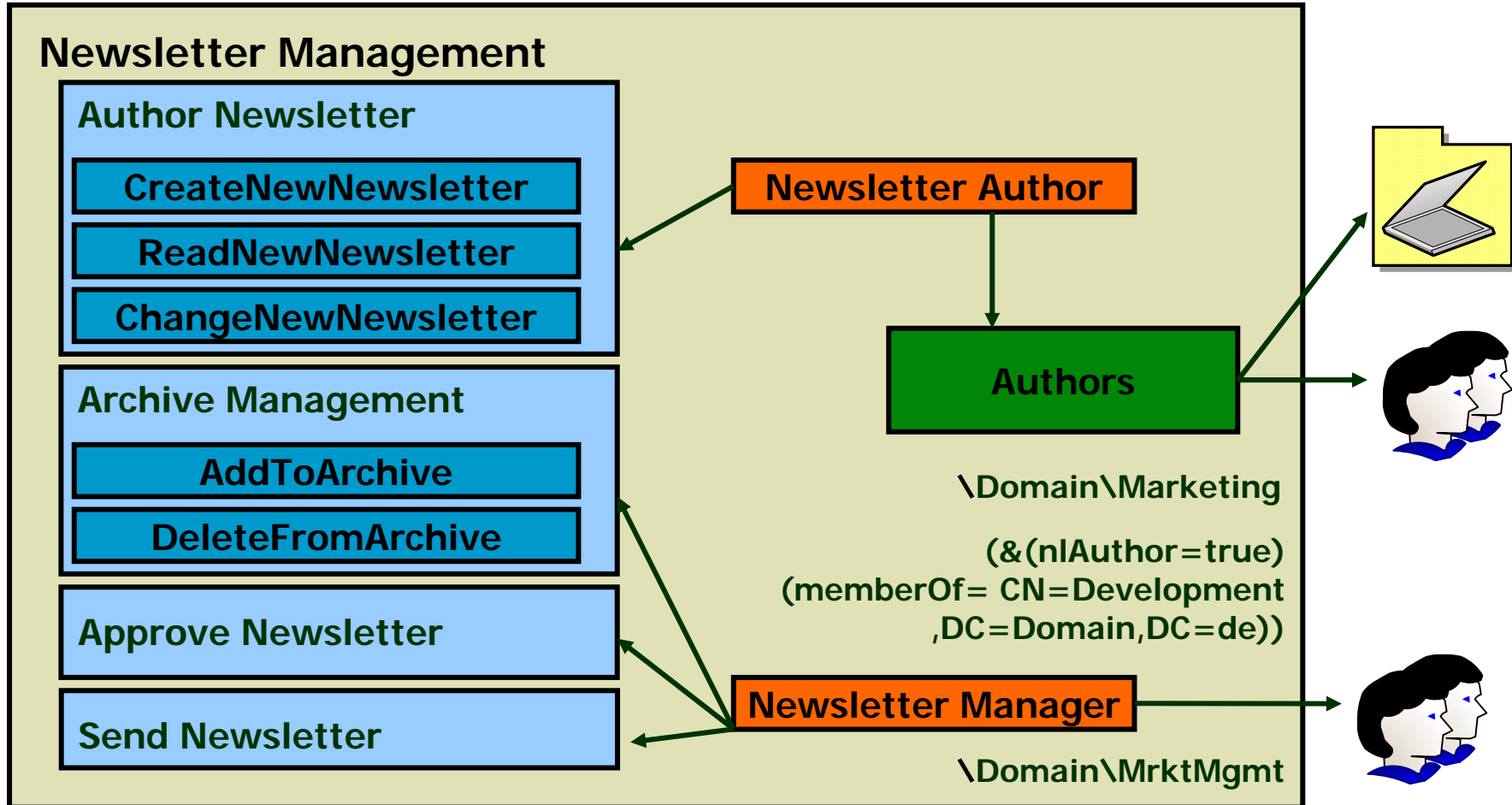
- Programmier-Schnittstelle für alle gängigen Sprachen
 - C++, C#, Windows Scripting Host

- Die AzMan Einstellungen werden in einem sog. Store abgelegt
 - XML Datei
 - ◆ leicht zu handeln
 - ◆ leicht zu konvertieren

 - Active Directory (W2K3 Functionality Level)
 - ◆ Delegation of Administration
 - ◆ Concurrent Editing
 - ◆ Replikation
 - ◆ Auditing



Authorization Manager



- Der API teilt sich in zwei Bereiche
 - Verwaltung des Authorization Stores
 - ◆ z.B. Installations-Skripte
 - Zugriffs-Überprüfungen
 - ◆ "Darf der Benutzer diese Aktion durchführen"
 - ◆ Einhaltung der im AzMan definierten Policy

Beispiel Installations-Skript (VBScript)

```
'Anwendung anlegen
Set Appl = pAzManStore.CreateApplication("NewsletterManagement")

'Operationen anlegen
Set Op1 = Appl.CreateOperation("ApproveNewsletter")
Op1.OperationID = CLng(1)

'Taks anlegen
Set Task1 = Appl.CreateTask("Approve Newsletter")
Task1.AddOperation CStr("ApproveNewsletter")

'Rollen Anlegen
Set RoleA = Appl.CreateRole("Newsletter Manager")
RoleA.AddTask("Newsletter Manager")
```

Laden einer Policy (C#)

```
AzAuthorizationStore store = new AzAuthorizationStoreClass();

// Öffnen eines XML Stores
store.Initialize(0, @"msxml://d:\etc\azNewsletter.xml", null);

// Öffnen eines Active Directory Stores
store.Initialize(0, @"msldap://CN=MyAuthorizationStore,
  CN=Program Data,DC=STREETMARKET,DC=net", null);

// Laden der AzMan Anwendung
IAzApplication app = store.OpenApplication(
  "Newsletter Management", null);
```

```
// Initialisieren des Az Stores für den aktuellen Benutzer
IAzClientContext ctx =
    app.InitializeClientContextFromName(name, null);

// Ermitteln der Rollen des Benutzers
string[] roles = GetRoles(ctx);

// Durchführen einer Autorisierung
bool allowed = AccessCheck(ctx, AzOperations.ApproveNewsletter,
    "Newsletter April 2004");
```

- Die Anwendung kann auch optional weitere Informationen an den Authorization Manager übergeben
- In der AzMan Policy lassen sich Skripte hinterlegen, die aufgrund dieser Informationen Entscheidungen treffen
- Somit lassen sich z.B. folgende Szenarien lösen
 - Ein Kunde darf nur während der normalen Geschäftszeiten angelegt werden
 - Der Newsletter Manager darf nur Newsletter genehmigen, die er nicht selbst geschrieben hat

- Die Anwendung übergibt an AzMan die Information, ob der zu genehmigende Newsletter selbst geschrieben wurde
- Die Policy entscheidet ob dies zulässig ist

```
AzBizRuleContext.BusinessRuleResult = false  
self = AzBizRuleContext.GetParameters("self")
```

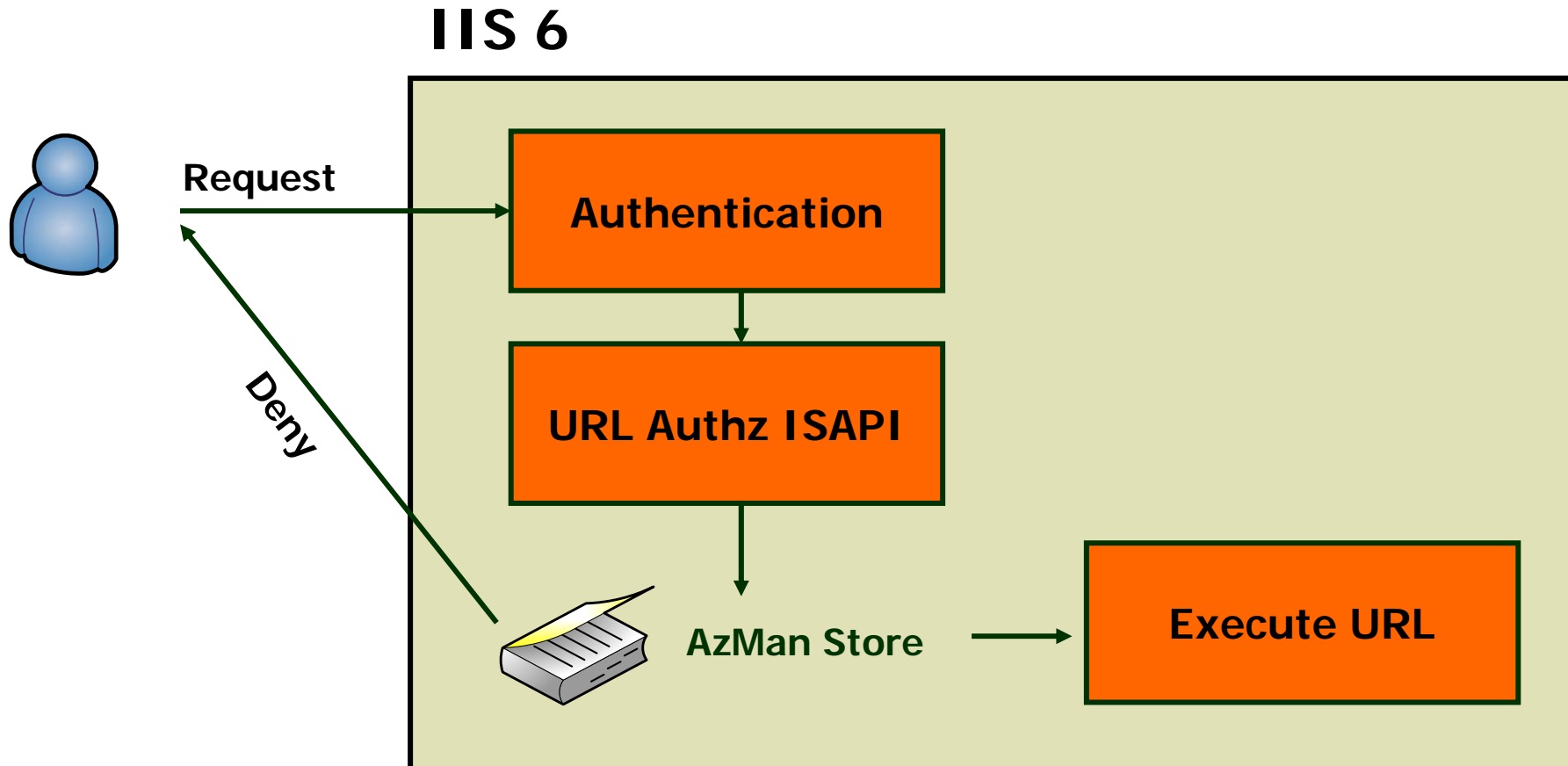
```
if self = false then  
    AzBizRule.BusinessRuleResult = true
```

■ ISAPI Extension

- Mappt virtuelle Verzeichnisse/Dateien auf Tasks
- Der Administrator kann in AzMan Konsole konfigurieren, welche Benutzer oder Gruppen auf welche Web Anwendungen Zugriff haben

- In Verbindung mit AD Replikation ideal um Policies für Web Cluster synchron zu halten

IIS 6 URL Authorization



- <http://msdn.microsoft.com/msdnmag/issues/03/11/AuthorizationManager/default.aspx>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/security/athmanwp.asp>
- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/authm_topnode.asp

- <http://www.ernw.de/publikationen/azMan.zip>

Fragen ?