Identification, Authentication, and Authorization

Use Case for Small / Medium Businesses

Andrew Bruce, CISSP, PMP, FITSP-D
CTO, RiVidium Corporation (http://www.rividium.com/)
andy.bruce@rividium.com
31 October 2010

Topic Summary:

- Definitions: Identification, Authentication, and Authorization (IAA).
- Analysis of a typical Small / Medium Business (SMB) network segment.
- Active Directory and Kerberos for IAA.
- Public Key Infrastructure (PKI) and.

Table of Contents

Illustration Index

About the Author

Andrew Bruce is Chief Technical Officer for RiVidium Incorporated, a Service Disabled Veteran Owned Small Business in the suburban Washington, DC area. RiVidium provides professional services to the Federal Government and the Department of Defense, specializing in customizing and developing architecture and governance models that leverage our proprietary technologies. Mr. Bruce's job responsibilities include: working directly with customers and partners for new business development, supporting proposal efforts, overseeing RiVidium's network infrastructure, working with project managers to ensure project completion, managing software development efforts throughout the entire system life-cycle, and leading new technology research and proofs-of-concept. After a career spanning decades in shrink-wrap, commercial, and corporate software development, Mr. Bruce is focusing on Information Assurance to achieve his goal of building and managing large data centers providing cloud computing utility services for commercial and Government customers.

1.0 Introduction

The typical Small / Medium size Business (SMB) must provide both intranet (internal) and extranet (external) access for its employees and customers based on roles, permissions, and clearance. This white paper looks at a notional SMB network and discusses how the SMB can implement Identification, Authentication, and Authorization (IAA) using simple techniques that leverage common network environments.

The notional internal corporate network consists of a small number of physical servers complemented by a much larger number of virtual servers. All of the internal servers and team member desktops run some variant of the Windows operating system and leverage a local Active Directory domain for IAA functions. The notional network does have non-Windows servers for specific customer projects, but these servers generally provide their own IAA solutions per customer requirements. This paper concentrates specifically on IAA within a typical corporate Active Directory environment.

Key points to consider as any part of an IAA solution include:

Manageable. SMBs are not known for having deep pockets to invest in a team of dedicated system administrators. Any IAA solution must be easily implemented and convenient to maintain.

Scalable. The goal of a typical SMB is not to become enamored of the “Small”; that is, the business needs to be prepared to expand. That next task order award may require significant growth in the corporate infrastructe and the IAA solution needs to be archictected with that target in mind.

Standards-based. Related to overall manageability, any IAA solution needs to be firmly rooted in proven concepts and technologies. For example, a hardened and patched Active Directory environment provides an excellent framework for a reliable and affordable corporate network solution.

Extensible. This whitepaper considers how a typical Active Directory implementation can be extended to support public key infrastructure (PKI) needs, with a use case of mapping SharePoint users to certificate-based logins. This ties in well to the larger requirement that any IAA solution must be capable of integrating with evolving technology standards.

This whitepaper closes with some specific recommendations and thoughts.

2.0 The Notional Network Segment

This paper concentrates on the following high-level notional network segment:

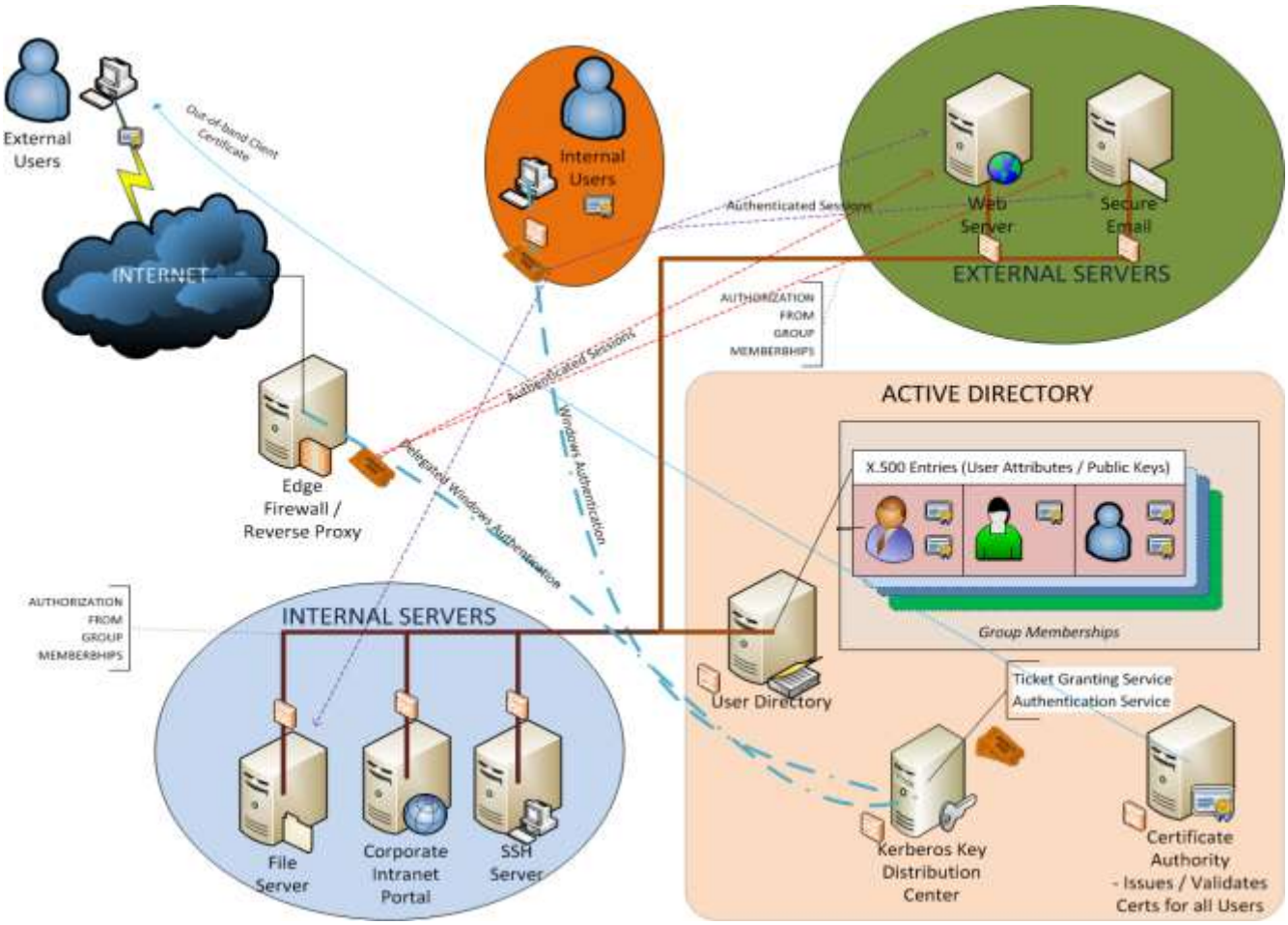


Figure 1: High-level network diagram

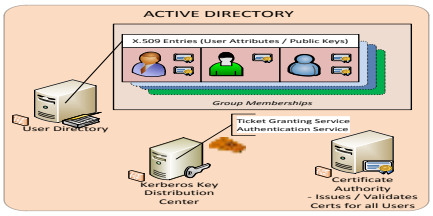
The major components include:

1. *Active Directory* – The primary IAA infrastructure.
2. *Internal Servers* – Servers providing functions such as file sharing.
3. *External Servers* – Servers providing functions such as email.
4. *Users* – These include both internal and external users.
5. *Gateway* – Provides proxy IAA functions for external users.

Future papers could cover VPN, SSH, and thin desktop / virtual desktop connectivity.

3.0 Active Directory and IAA

Active Directory (AD) provides all of the notional network's foundational IAA capabilities through three components: *User Directory*, *Kerberos sub-system*, and *PKI* (labeled "Certificate Authority" in the drawing).



3.1 User Directories and Identification

Active Directory provides scaled-down X.500 support[i] whereby each X.500 object has a set of attributes and group memberships (like the "User" object shown below). This supports the organization's security policy by means of group memberships (RBAC model); specific authorization ACLs almost exclusively target group memberships rather than individual users.

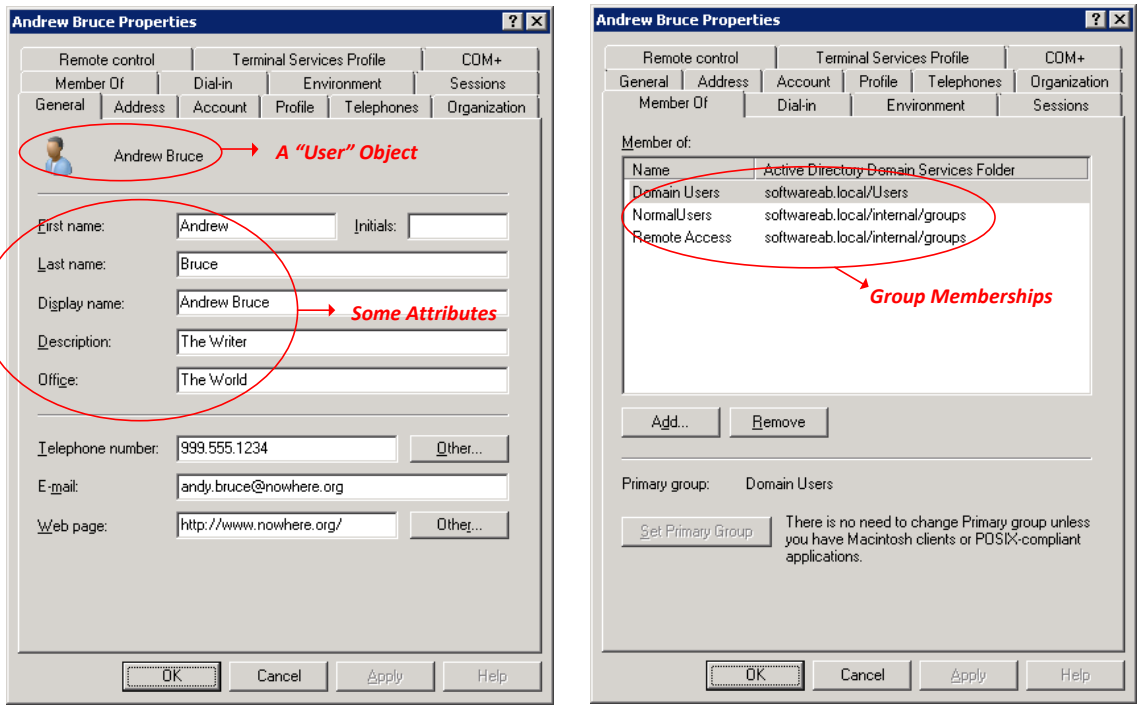


Figure 2: AD "User" object example

X.500 supports *identity* by assigning each object a unique identifier (the "distinguished name" or DN), such as:

```
CN=Andrew Bruce,OU=users,DC=softwareab,DC=local
```

The notional AD allows both UPNs and NetBIOS short names to be used; for example, "andy.bruce" maps to the DN above. An identity can also be claimed using a certificate (see the Recommendations).

3.2 Kerberos, Authentication, and Cryptography[ii]

The notional organizational network uses AD's Kerberos modules to verify a subject's claimed identity. (Note: Microsoft Kerberos itself provides no authorization, although version 5 can pass authorization information generated by other services.) Kerberos performs authentication using a two-phase approach: issuing first a "ticket-granting-ticket" (TGT), which itself is then used to request a "service ticket" (ST) to gain access to a desired resource. The Key Distribution Center (KDC) maintains a master list of all cryptovariables for all resources (the KDC must be highly protected).

3.2.1 The Ticket Granting Ticket (TGT)

The first phase of Kerberos authentication is analogous to purchasing a ticket to enter a fair's midway:

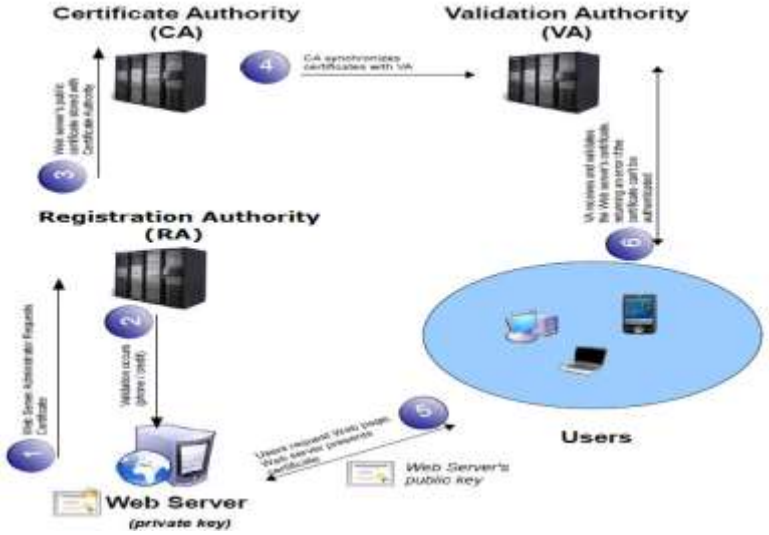
1. **User self-identifies.** An identifier tied to the X.500 directory must be provided to a process ("supplicant") like a workstation or gateway proxy. The supplicant uses symmetric encryption and a supported cryptographic function to exchange data with the Authentication Service (AS). AD supports the following functions: RC4-HMAC (128bit), DES-CBC-CRC (56bit), and DES-CBC-MD5 (56bit). Per current best practices, the notional network standardizes on the strongest encryption (RC4-HMAC) throughout the network.
2. **Kerberos verifies the identity.** In the simplest case, the user's login machine sends the user's password in MD5-encrypted ("hashed") form to the AS, and the AS validates this password hash against the keystore entry within the KDC.
3. **Kerberos issues the TGT.** Upon successful validation, the Ticket Granting Service (TGS) creates a TGT valid for a given time period (default is ten hours). The TGT proves that the user has been authenticated. The notional network's edge gateway receives a "proxy TGT" on behalf of each external user, allowing the gateway to "impersonate" that external user for proxy access to the internal servers.

3.2.2 The Service Ticket (ST)

Phase Two of the Kerberos model allows access to a "service" (such as to a Web server) by issuing a Service Ticket (analogous to purchasing a ride ticket once inside the midway):

1. **Supplicant requests the ST using the TGT**. For internal users, this occurs via their workstation. For external users, this occurs via the edge gateway.
2. **TGS verifies the TGT and issues the ST**. The TGT must be valid and non-expired. AD's Kerberos differs from MIT's in that the Authorization-Data ticket field contains internal unique identifiers for the X.500 entry and for group memberships. The end-service can use these identifiers to authorize the user.

3.3 PKI, IAA, and Cryptography



The notional network uses AD's built-in PKI to enable secure access to the corporate Web servers (both internal and external). The side diagram shows a simple PKI that highlights the standard interactions between the Web server, the PKI, and an end user. (In the notional organization, the RA, VA, and CA functions are all combined.)

Public key encryption works by having two keys with a mathematical relationship such that the "public" key can be computed from the "private" key, but it is computationally infeasible to go the other direction. The private key must be kept secure, while the public key can be shared. For each Web session between browser and server, the browser generates a temporary session key and encrypts it using the server's public key. The server then uses its private key to decrypt this received session key (valid only for the current Web session) and uses it for all subsequent data transmission to that client. This uses slow public-key cryptography[1] for the initial key exchange over the insecure transmission medium (Internet) and fast symmetric cryptography once the session is established.

The notional AD infrastructure standardizes on the RSA encryption function, which is based on the difficulty of factoring very large prime numbers. The algorithm's strength lies in its ability to generate two large prime numbers such that their product is of a given bit-length: 2048 bits is the currently accepted recommended length.

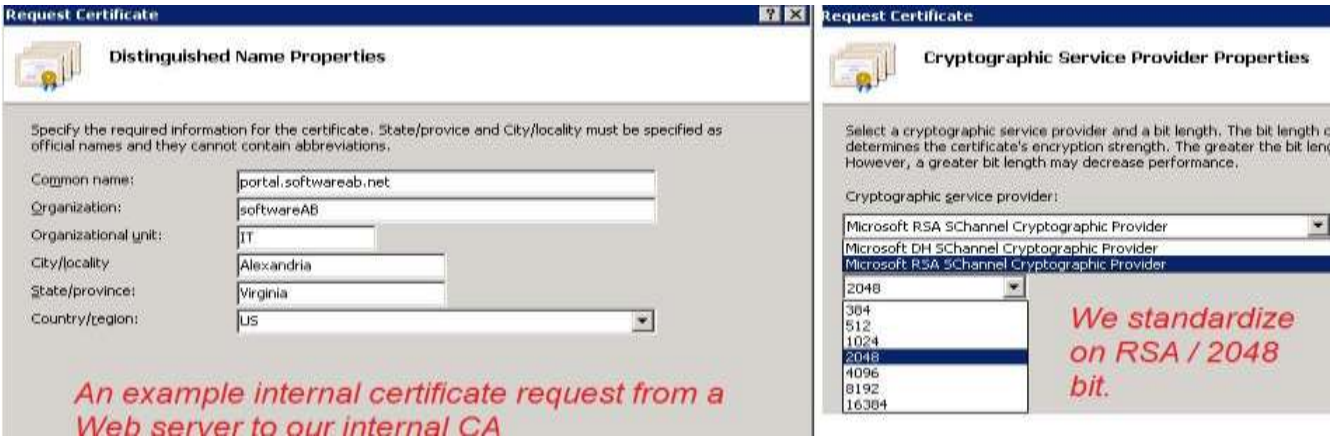


Figure 3: Web server certificate request

[1] Public-key cryptography can be up to *10,000 times slower* than secret key cryptography.

3.3.1 External Web Sites

As a case study consider how a company can use a commercial certificate (GoDaddy) for a corporate blog site.

First: Setup a Forward Lookup Zone on the local Domain Name Server (DNS) to allow internal users to use the external Web site name while keeping all network communications local:

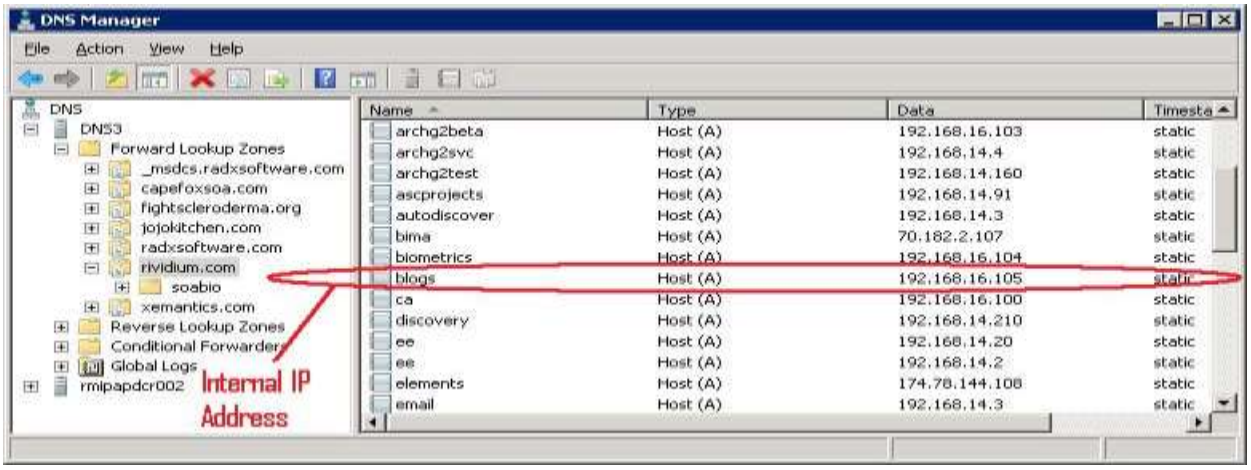


Figure 4: Internal DNS entry for blogs site

Second: Assign the GoDaddy certificate to the "blogs" Web server:

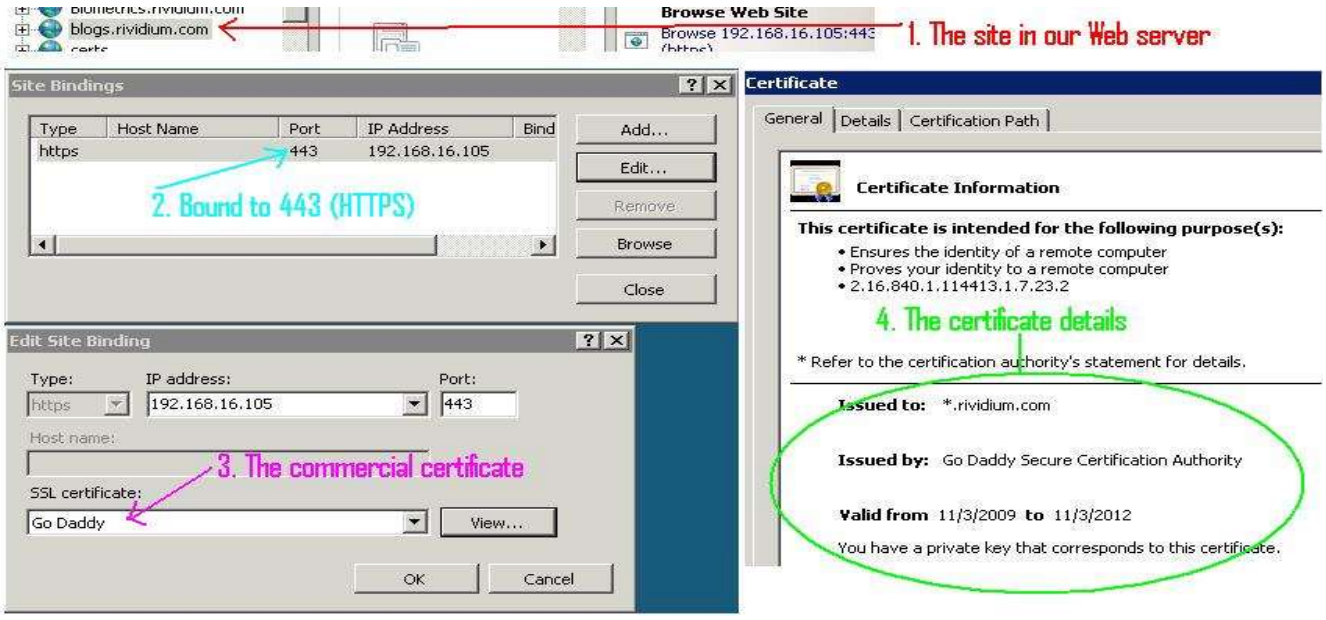
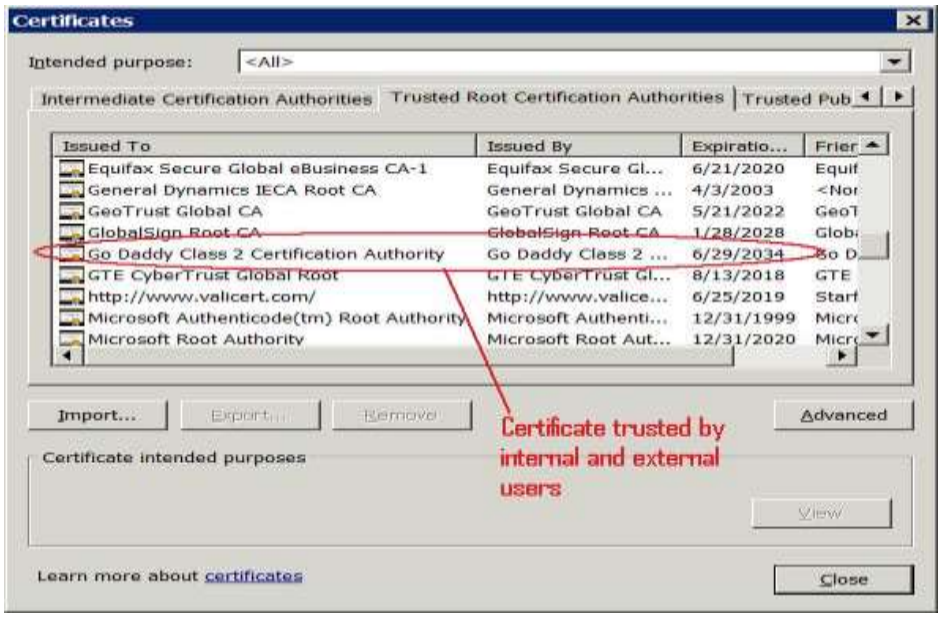


Figure 5: Commercial certificate for blogs site

Third: For all connections to the "blogs" site, the Web server presents the GoDaddy certificate to the client. GoDaddy has already negotiated with the major Web browser vendors to ensure that they trust all of GoDaddy's issued certificates (shown here for IE8).

The result: The corporate Web server can use the same certificate for access from both internal and external users.



3.3.2 Internal Web Sites

Using an existing internal Certificate Authority (CA) such as comes with Active Directory, one can generate a valid certificate for each intranet Web servers (shown below for an internal development server):

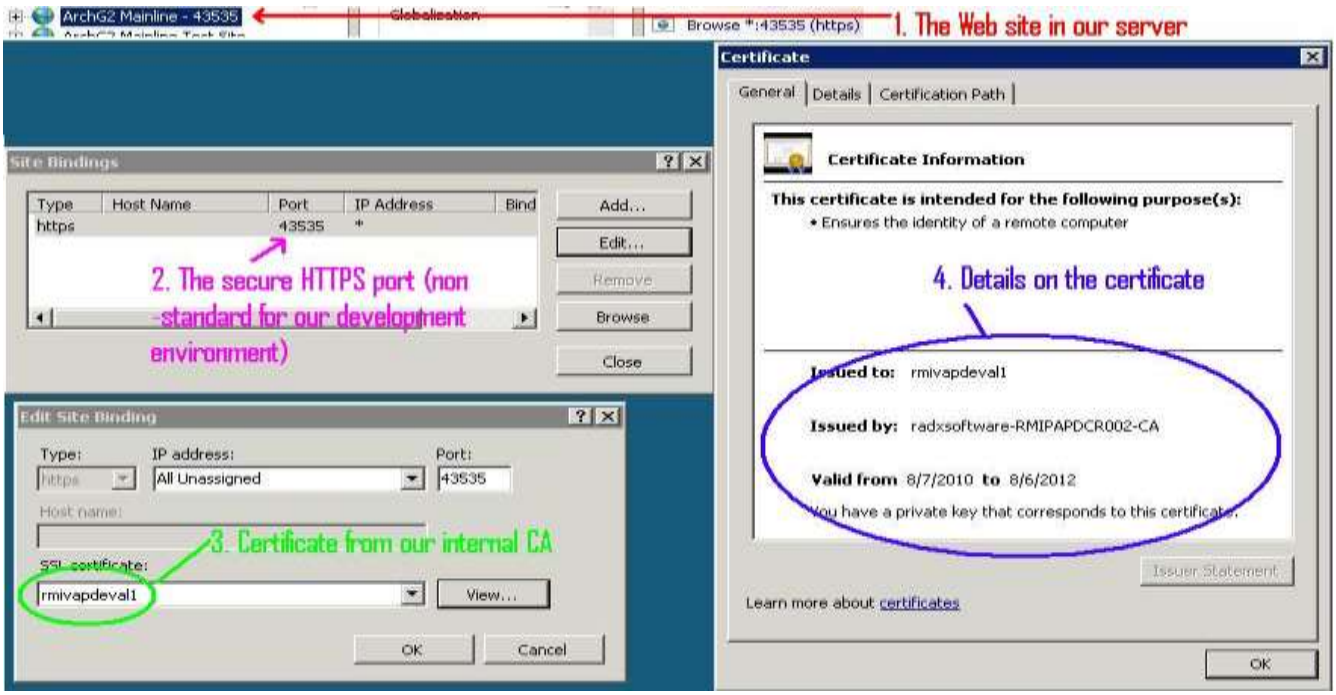


Figure 6: Intranet Web server certificate

Because AD automatically installs the CA's root certificate on all machines in the Active Directory domain, team members can connect to this site using Internet Explorer.

Interestingly enough, other browsers (like Firefox) do not use the Windows Trusted Root's keystore like Internet Explorer does. Connections to this same site from these browsers result in a certificate challenge until the user manually adds the internal CA's root certificate.

This non-IE certificate trust can be addressed both by training as well as by automated configuration rollouts via Group Policy Objects within AD.

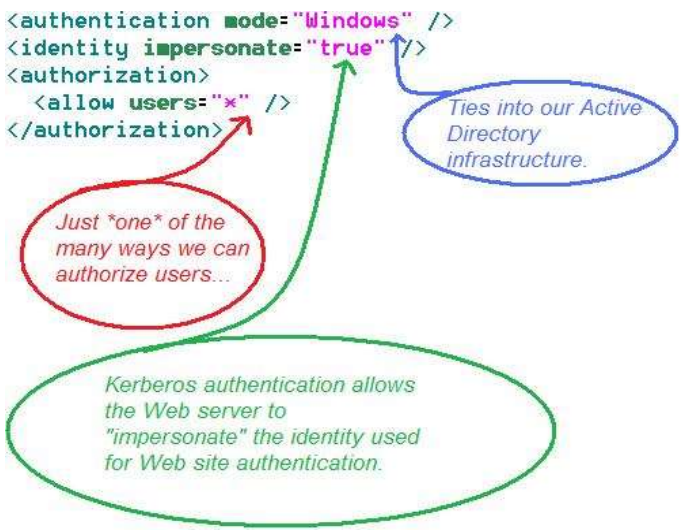
4.0 Authorization

While Kerberos generates a Service Ticket (ST) granting basic access to a "service," that service (such as the notional corporate intranet portal) must still authorize each user.

1. For all users, one way to approach Authorization is to standardize on on Windows Authentication. Internal users receive the (in)famous "logon box," while external users receive a challenge screen issued by thecorporate gateway.

Figure 7: Challenging internal / external users

2. Kerberos authenticates the user and issues an ST granting access to the Web server. Because the corporate portal uses SharePoint, it leverages Active Directory identity and group memberships via configuration entries in the *web.config* file.



3. The corporate portal can now authorize the user using a combination of methods:
   a. *Operating System* – The portal application can block or allow access to individual files (such as images or documents) by using Windows file system permissions.
   b. *Web Server* – Windows Internet Information Server (IIS) provides built-in capabilities to block or deny access to logical Web resources (such as a Web page) based on the user's identity.
   c. *Native* – SharePoint has its own permissions model based on "SharePoint users" and "SharePoint groups;" one ties these users and groups to corresponding entries in the Active Directory, which allows the organization to manage portal permissions from a single console.

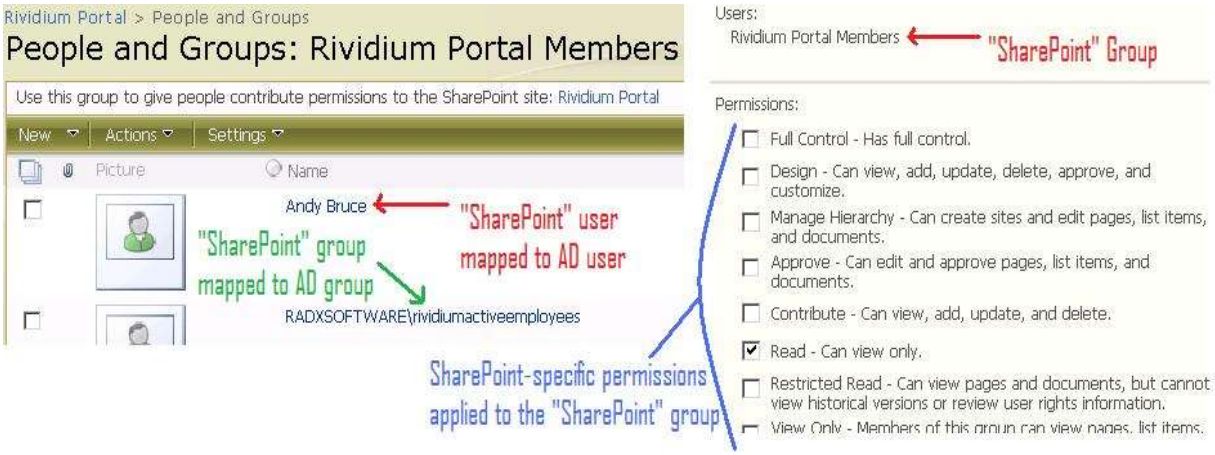


Figure 8: Authorization for an intranet portal

A Final Thought: **Authorization is complex to perform and difficult to troubleshoot**. This simple case study has touched on three completely independent authorization layers, any one of which could enforce a denial of access. Consider that these authorization layers are extensible: one could use custom software modules, or Security Access Markup Language (SAML), or even a semantic approach such as inferring "access rights from domain proximity" as proposed by Ángel García-Crespo et. al.[iii] When users call the Help Desk with an "Access Denied" problem, it can be difficult to determine just which authorization layer is at fault. A future paper could address this area more fully.

5.0 Recommendations

These recommendations are based on an interview with the Chief Operating Officer of a small company:

5.1 External Users and Certificates

An organization's Help Desk receives support calls when an external user forgets an assigned user name and / or password. These costs can be reduced by issuing "soft certs" to external users:

Step	Cost	Notes
Web servers allow certificates	None	Requires configuration change only
Issue "soft" user certificate	One week to define process	Create local AD account, associate soft certificate with that account
Integrate with Help Desk	Three days for training	Walk through processes and requirements: 1) receive strong pass phrase from remote user; 2) send "soft" certificate out-of-band via encrypted email; 3) walk external user through installation

An external user having this "soft" certificate installed on a workstation no longer requires a user ID to access the network; instead, one simply remembers the self-assigned pass phrase. This may outweigh the disadvantages of extra training and time for the help desk and the manual installation process on the external user's workstation. Christopher McLaughlin points out that "it can be a costly in terms of money and manpower to ensure that the risks soft certificates present to the business are managed effectively,"[iv] but for a typical small organization, the benefits outweigh the risks.

5.2 Employee Termination

Consider the problem in accounting for terminated employees; project managers can easily work in largely autonomous environments and can "forget" to tell IT about a termination. Reduce these problems by creating an automated "employee termination" process using an intranet corporate portal such as SharePoint.

Step	Cost	Notes
Define standard termination flow	One week	Research the existing processes
Create termination workflow	One week	Automate using standard SharePoint features to ensure notification on a termination event
Integrate with PMs / HR	Two day of training	Automatic notification helps ensure that the Active Directory environment is clean

While numerous other recommendations can be made, these two are low-cost and high-reward for a project-oriented SMB; such as a small Department of Defense contractor.

6.0 Acronyms

ACL – Access Control List; structure associated with a given resource (“object”) that enumerates permissions (read, write, etc.) assigned to users and groups.
AD – Active Directory; Microsoft’s network management infrastructure which provides user support, centralized server management, and organization-wide security policy support.
AS – Authentication Service (Kerberos)
CA – Certificate Authority (PKI)
DES-CBC-CRC / DES-CBC-MD5 – Data Encryption Standard Cipher Block Chaining Cyclic Redundancy Check / Message Digest 5; block-oriented encryption algorithms providing message integrity
DNS – Domain Naming Service
IE – Internet Explorer
KDC – Key Distribution Center (Kerberos)
MIT – Massachusetts Institute of Technology
PKI – Public Key Infrastructure
RA – Registration Authority (PKI)
RBAC – Role-based Access Control; users are assigned privileges based on their roles within the organization.
RC4-HMAC – Stream-oriented encryption algorithm providing message integrity (used by Kerberos starting with Windows 2000)
RSA – Rivest-Shamir-Adleman public-key encryption algorithm
SSH – Secure Shell; allows remote management of internal corporate resources
ST – Service Ticket (Kerberos)
TGT – Ticket-granting Ticket (Kerberos)
VA – Validation Authority (PKI)
VPN – Virtual Private Network; allows remote access to internal corporate resources
UPN – User Principal Name; Internet-style login name for a user (such as “andy.bruce@rividium.com”)

Reference List and End-notes

End-notes immediately follow this section.

Á. García-Crespo, et al., "SecurOntology: A semantic web access control framework," *Computer Standards & Interfaces (2009)*, doi:10.1016/j.csi.2009.10.003.

Bosworth, Seymour, M.E. Kabay, Eric Whyne, eds., "Chapter 37: PKI and Certificate Authorities." *Computer Security Handbook: Volume 1, 4th ed.* Hoboken, NJ: John Wiley & Sons, Inc., 2009.

McLaughlin, Christopher. 2008, "Proposed Model for Outsourcing PKI." *Master's Thesis*. University of London (Royal Holloway).

Microsoft Corporation. *Active Directory LDAP Compliance*. Redmond, WA: Microsoft Press, 2003.

Microsoft Corporation. "How the Kerberos Version 5 Authentication Protocol Works." *Microsoft TechNet*. http://technet.microsoft.com/en-us/library/cc772815(WS.10).aspx (accessed: October 7, 2010).

[i] Active Directory emulates the Lightweight Directory Access Protocol (LDAP), which is an "implementable" version of the X.500 model.

[ii] Microsoft's Kerberos implementation is based on RFC 1510.

[iii] Á. García-Crespo, et al., "SecurOntology: A semantic web access control framework," *Computer Standards & Interfaces (2009)*, doi:10.1016/j.csi.2009.10.003, pg. 3.

[iv] Christopher McLaughlin, 2008, "Proposed Model for Outsourcing PKI," *Master's Thesis*, University of London (Royal Holloway), pg. 66.