

Universal Certificate Authentication to Key Applications at Argonne National Laboratory

Doug Engert
Rich Raffenetti
David Salbego
John Volmer

Argonne National Laboratory
9700 South Cass Avenue, Argonne IL 60439

February 26, 2007

Argonne National Laboratory has implemented a laboratory-wide portal that provides centralized access to key administrative applications and employs certificates for authentication. This portal relies on an infrastructure comprising Microsoft Active Directory, Microsoft Certificate Services, Sun Microsystems Java Enterprise Suite, and open-source software. The capabilities of the Microsoft, Sun, and open-source products have enabled Argonne to readily deploy certificates for partial, as well as for end-to-end, authentication from all Argonne client operating systems. The Argonne experience demonstrates that certificate authentication to corporate applications is readily doable today. Further, the adoption of these technologies positions Argonne to exploit widespread certificate deployments, as intended by Homeland Security Presidential Directive-12.

Introduction

Challenge

In enabling certificate access to applications, organizations must address two issues:

- Providing users with certificates, and
- Enabling applications to accept certificates.

Users cannot be easily provided with certificates because certificates (and their corresponding private keys) are difficult — if not impossible — for users to simply manage. The certificate and private key comprise a few thousand bytes of binary data. Further, the private key must be safeguarded because control of the key is the basis for assuring identity.

Certificate authentication also cannot be easily incorporated into applications because enabling certificate authentication requires considerable technical knowledge of Public Key Infrastructure (PKI) concepts and public/private key algorithms.

Solution

Argonne National Laboratory has overcome both of these issues and enabled certificate authentication to corporate applications for most users by using commercially available and open-source technology. Argonne addressed the issue of providing users with certificates by adding Microsoft Certificate Services and the University of Michigan's KX.509 package to its authentication infrastructure. Microsoft Certificate Services enable organizations to issue either short-term or long-term certificates to hundreds of users. Simultaneously, Argonne adopted Sun Microsystems Java Enterprise Suite to incorporate certificate authentication into web-based applications. The Sun Microsystems suite includes simple mechanisms for adding certificate processing to applications.

The combination of these two commercial technologies and open-source software provided immediate and unexpected benefits. Not only do users have certificate-based application access, but in many cases, the approach that we used enables single sign-on. Further, with the addition

of smart cards, we were able to provide end-to-end authentication based on certificates.

An organization that is readily able to accept certificates for authentication is ideally positioned for the implementation of Homeland Security Presidential Directive-12 (HSPD-12). The intent of HSPD-12 is for smart cards containing certificates to be issued to all federal employees and contractors beginning in October 2006. An organization able to capitalize on the widespread availability of certificates can greatly simplify the user's password management burden.

This paper presents a detailed discussion of how Argonne National Laboratory addressed the two challenges associated with certificate access: providing user certificates and enabling applications.

Background

The Argonne National Laboratory authentication infrastructure has developed over the years from standalone Kerberos servers to a Distributed Computing Environment (DCE) and, recently, to Microsoft Active Directory. Active Directory has become Argonne's institutional authentication mechanism.

Upon date of hire, employees are provided with an identity in Active Directory, which is a combination data store and service provider. Domain controllers are computers that manage the data store and offer, for example, the following services to clients:

- Kerberos ticket services, and
- Lightweight Directory Access Protocol (LDAP) access to Active Directory's contents.

A *domain* is the collection of computers and users managed by an active directory instance.

Active Directory is a powerful tool in the management of a Microsoft Windows domain. It permits distribution of information and policies to all members of the domain, both client

computers and users. One use of Active Directory is to define trusted root certificate authorities. Certificate authorities defined in Active Directory are automatically trusted by all clients and domain controllers.

Approximately 60% of Argonne's desktop workstations have Microsoft Windows 2000/XP operating systems, and nearly all of these workstations are members of the ANL.GOV domain managed by Active Directory. The other 40% of Argonne's workstations are Macintosh (20%) and Unix (20%). Argonne's Mac and Unix workstations are not managed by Active Directory. Argonne's ANL.GOV domain processes 1,500 unique logins per day.

Because all employees are provided with an identity in the ANL.GOV domain (Active Directory), they all have Kerberos principals. All employees, regardless of their desktop platform, are able to acquire Kerberos authentication credentials from the authentication infrastructure.

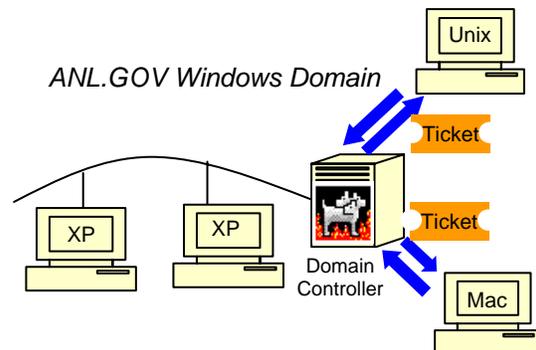


Fig 1: All Platforms Can Authenticate to Active Directory

As shown in Figure 1, Argonne's Unix and Mac computers can take advantage of the Kerberos services provided by Active Directory if they are configured to do so. Unix workstations implementing `pam_krb5` and Mac workstations configured to use Active Directory obtain Kerberos tickets automatically during login processing. If the computer is not configured to perform Kerberos logins, the Kerberos `kinit` command ("acquire a Kerberos ticket") can be run on the computer to acquire Kerberos credentials after logon.

Many of Argonne's administrative systems rely on the ANL.GOV domain to authenticate users, particularly systems that are used directly by all employees. These systems include high-profile applications such as Human Resources' Performance Appraisal and Open Enrollment systems.

Certificate Authentication Architecture

Certificate Issuance

In the spring of 2002, Argonne began experimenting with the University of Michigan's KX.509 suite to enable testing of certificates with real-world applications, particularly for the Globus project. Globus relies on certificates to perform user authentication, and KX.509 permits organizations with a Kerberos infrastructure to easily issue short-term user certificates. KX.509 constructs short-term certificates from existing Kerberos credentials.

Subsequently in 2004, Argonne began investigating two-factor authentication for its Microsoft Windows-based administrative users. Microsoft Windows naturally supports smart cards; the most straightforward path for enabling a smart card pilot was to install Microsoft Certificate Services.

Microsoft Certificate Services are primarily a certificate authority coupled with a web application. Smart cards require the deployment of Microsoft Enterprise Certificate Services¹.

Microsoft's Active Directory provides the framework for Enterprise Certificate Services. For example Certificate Services uses Active Directory to identify users for smart card issuance and to publish Certificate Revocation Lists (CRL). Additionally, Active Directory policies can draw on Enterprise Certificate Services. One of these policies (which will be discussed later) is the ability to automatically issue certificates to users — in effect, to auto-enroll users.

As an example, within 24 hours of our installation of Enterprise Certificate Services, all

of Argonne's 38 domain controllers detected its presence and requested domain controller certificates from Certificate Services. In response, Certificate Services automatically issued domain controller certificates to each of the domain controllers, as shown in Figure 2.

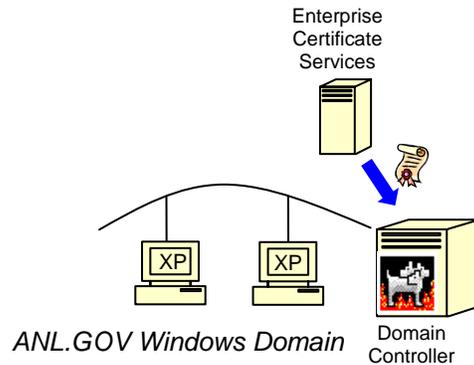


Fig. 2: Issuance of a Certificate to a Domain Controller

A web application associated with Enterprise Certificate Services provides the means to manually submit requests and obtain certificates. The web site acts as an enrollment station for agents to provide smart cards on behalf of clients.

Auto-Enroll Certificates

Microsoft Enterprise Certificate Services provide a capability known as Auto-Enroll Certificates. Auto-enrollment allows organizations to avoid the high effort costs associated with traditional certificate issuance by using domain policy to automatically issue certificates. No new services need to be installed to enable auto-enrollment.

Users who log in to Windows XP work stations and who are members of the domain are selected by group policy to trigger the auto-enrollment process. A certificate request is issued, and Certificate Services immediately responds with a certificate for the user. The certificate and private key are stored in the user's profile, and the certificate is propagated to the user's certificate store. Figure 3 depicts this process.

At Argonne, approximately 2,000 users are presently selected to receive auto-enroll login certificates. Each week, 600 Auto-Enroll

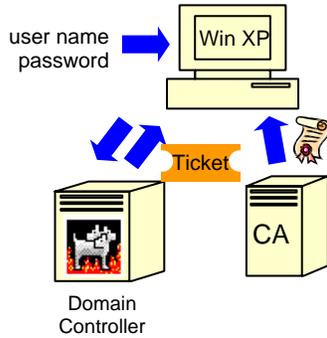


Fig. 3: Issuance of an Auto-Enroll Certificate to a User

Certificates are issued to users. These certificates have a lifetime of 30 days.

KX.509 Certificates

The University of Michigan's Kerberized Certificate Authority (KCA) and kx509 (an element of the KX.509 suite) programs are used to provide short-term certificates to users of workstations that are not members of the ANL.GOV domain managed by Active Directory. These tools provide the same service as the Auto-Enroll Certificate, i.e., short-term login certificates derived from login credentials. The KX.509 tools are available on workstations that do not run Windows, such as Unix and Macintosh, and to non-domain Microsoft Windows clients as well.

Two KCA servers issue certificates to users. KCA certificates are derived from the Kerberos tickets of the users who make kx509 requests. The certificate subject name is derived from the Kerberos principal name, and the certificate lifetime is the remaining lifetime of the Kerberos ticket used in the request. The subject name is always the same for a given user. Figure 4 shows the KX.509 certificate issuance process.

When kx509 is run on a Windows machine, the certificate and private key are stored in the user's certificate store, and are thus accessible — like any other certificate. When kx509 is run on a non-Windows machine, the certificate and private key are stored in the Kerberos ticket cache. Both are made available to applications via the KX.509 kpkcs11 executable.

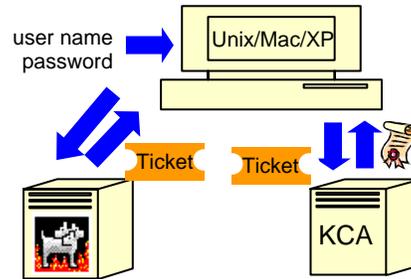


Fig. 4: Issuance of a KX.509 Certificate to a User

Because the certificate lifetime is usually less than a day, CRLs are not issued or checked. A user can also discard the certificate and the private key by using the kx509 program or by destroying the Kerberos ticket cache.

KX.509 certificates are rarely requested. The two KCA servers issue fewer than two certificates per day.

Smart Card Issuance

Smart card issuance requires the following two additional components beyond the installation of Microsoft Enterprise Certificate Services:

- The physical equipment of smart cards and readers, and
- Smart card middleware — specifically a Cryptographic Service Provider (CSP) that provides an interface between Microsoft Windows and the smart card.

Argonne chose Gemalto GemSAFE smart cards and Gemalto GemLIB v4.2 middleware for its smart card pilot². The middleware includes both a CSP for accessing the card, as well as a tool for managing the card.

Microsoft Enterprise Certificate Services provide a web interface for smart card issuance. The default interface assumes that smart cards will be issued in person by an authorized official, such as an enrollment agent. At Argonne, the Laboratory's Account Services personnel issue smart cards. Account Services personnel select the user who is being issued a smart card from Active Directory.

Portal Architecture

Microsoft Enterprise Certificate Services interact with the smart card to generate a public/private key pair, construct a certificate request, issue a certificate, and place the certificate on the smart card. Smart card issuance requires 5 minutes, and the certificate is valid for 2 years.

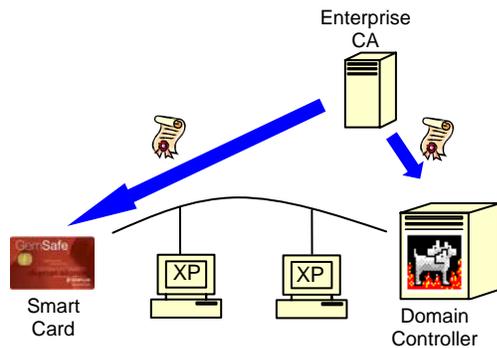


Fig. 5: Issuance of a Smart Card Certificate to a User

As shown in Figure 2 earlier, Microsoft Enterprise Certificate Services automatically issued certificates to domain controllers. With the issuance of a certificate to the user, as shown in Figure 5, a third-party trust model is created within the Windows domain.

Once issued, the smart card instantly enables login to Microsoft Windows workstations equipped with smart card readers and the smart card middleware. No additional configuration action is required by computer administrators. At login or when the smart card is inserted in the reader, the certificate is propagated to the user's certificate store.

Today, Microsoft smart card login certificates contain the *User Principal Name (UPN)* in the *Subject Alternate Name* field of the certificate. The UPN form is *username@domain*, which is the Active Directory identity of the user. This UPN is used by the domain controllers to select the user account for login when presented with a smart card. Thus, the mechanism for issuing the smart card requires smart card users to be members of Argonne's Microsoft Windows domain (ANL.GOV). Approximately 60 users at Argonne have smart cards.

In 2004, Argonne National Laboratory undertook a strategic business initiative to implement a web portal for its business systems. The developers envisioned a single framework that would serve as the official repository for all administrative applications and information — enabling Argonne to manage identities, roles, and responsibilities and providing employees with customized access to information. Employees would benefit from a single sign-on interface that would speed entry to the administrative applications.

Initially, the portal was designed to host in-house developed applications for Human Resources and Payroll transactions. The goal was to automate these tasks in order to significantly increase employee productivity.

Overview

The Argonne Administrative Systems Portal architecture is based on the 2005Q4 release of the Sun Java Enterprise System (JES). The JES suite consists of a number of related products, including a directory (LDAP) server, a web server, a Java application server, a portal server, and an access manager. These products represent the core of the product suite, and they are all in use at Argonne in a redundant, load-split architecture.

The Sun JES was chosen by Argonne for two primary reasons: past positive experience and attractive cost. Several of Sun's software products have been in use at the laboratory for many years, including the web server and directory server. Argonne had an established group of administrators who were familiar with Sun products and whose positive experiences with these products allowed us to experiment with additional Sun software. Sun software is also relatively inexpensive compared with other commercial software; the Sun JES software itself is free, although support is not. A comparison of the cost of the Sun software with that of competing commercial single sign-on and identity management products and our past positive experiences with Sun products made the

selection of Sun JES straightforward. The Sun JES suite is licensed across the Argonne campus.

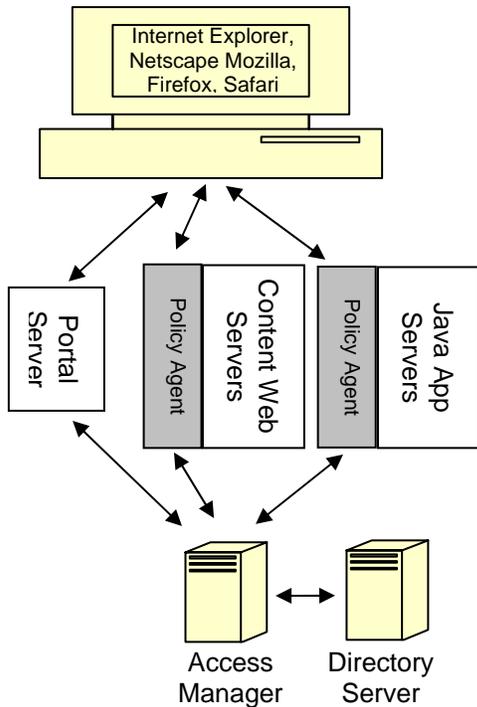


Fig. 6: Authentication Communication of the Sun Access Manager

Access Manager

The Access Manager is the central authentication and authorization mechanism used by other web services and resources. All requests for authentication, authorization, and session state flow through this service. As shown in Figure 6, the Access Manager is the key component — bringing together disparate web services and resources.

Authentication

A number of different authentication protocols (including LDAP, Unix, SecureID, RADIUS, and X.509) are accepted by the Access Manager. At Argonne, the LDAP and X.509 modules are used in production. The LDAP module is configured to work with Argonne’s Active Directory infrastructure for user name and password authentication. The X.509 module is configured to accept several types of X.509 user certificates for authentication.

These authentication modules may be *chained* together. Chaining allows multiple authentication modules to be used in succession. Rules define the requirements for each module. For example, users may be required to authenticate against module “A,” with authentication against module “B” being optional. Another scenario may require authentication against both module “A” and module “B.”

In Argonne’s scenario, two modules are chained together for public use: a certificate module and a user name and password module. The certificate module is invoked first. If a user has established a Transport Layer Security (TLS) connection to the Access Manager by using a client certificate, the certificate module attempts to use that certificate to authenticate the user. If no client certificate is available, a username and password prompt appears.

When an X.509 certificate is presented by an end user, it must be signed by a trusted certificate authority³, and there must be a map between a distinguished name component and the user profile stored in the LDAP server of the portal. The map defines which components of the presented certificate are to be used to locate the correct user profile in the LDAP server. The user profile specifies the Active Directory identity (i.e., Kerberos principal) of the user.

Authorization

The Access Manager employs an LDAP service to store configuration data, user session information, user portal profiles, and additionally authorization data such as group and role information. Applications use these authorization data to determine user privileges.

Argonne has developed an in-house centralized “role” (or group) management system called Information Services Authentication and Access Control (ISAAC). Users of ISAAC may create new roles, modify the membership of roles, and produce reports based on given criteria. Roles are defined and managed within ISAAC and distributed to multiple systems, including Oracle, Active Directory, and LDAP (for Access Manager).

Portal User Interface

The Argonne Administrative Systems Portal represents the gateway to other web applications and resources throughout the organization. This web site provides access to related applications. In Argonne's case, the portal is used to co-locate the entry points for many administrative systems required by individual employees. Users access the portal applications via their web browsers. One feature of portals is that users can customize their portal experience; their preferences are saved as part of their user profiles.

The Administrative Systems Portal relies on the Access Manager to provide authentication and authorization services. The portal also heavily relies on the directory service to store user profiles and related information. The Portal is the largest user of roles stored in Access Manager.

By utilizing roles, portal developers create a dynamic, customized end-user experience. An example role is "supervisor." After logging in to the portal through the Access Manager, an employee with a "supervisor" role will have additional application links visible to them. Applications such as "Performance Appraisal" will behave differently when used by a supervisor, as opposed to an employee.

Content Web and Java Application Servers

A number of web and application servers are used at Argonne, and many of them provide laboratory applications. The most well known is the Human Resources Performance Appraisal application. Frequently, these applications require authentication before they can be used. All portal-based applications use Access Manager Policy Agents to conduct authentication on their behalf. Different Policy Agents are available for a wide variety of web and application servers. For cases in which authentication is required, Argonne's web servers use TLS. The server certificates that enable TLS are signed by widely trusted external commercial certificate authorities. This approach allows all browsers, specifically the non-Active

Directory browsers, to automatically trust Argonne's administrative web servers.

The key to a seamless portal experience is single sign-on (SSO). Although not required, single sign-on allows users to jump from resource to resource and application to application within the portal without having to log in to each component individually. If a user had to provide credentials to each application he accessed, even if those credentials were identical, the experience would be severely diminished.

Policy Agents

The Access Manager provides for SSO capabilities within the portal through the Policy Agents, i.e., the security layer between the user and the resource. When a protected resource is accessed, the Policy Agent determines whether a user is authenticated, whether a resource is protected, and whether an authenticated user has access to a protected resource (authorization). These aspects are configured through the use of a local configuration file and a central policy repository located on the Access Manager.

Traditionally, simple web applications request a user name and password by using Hypertext Transfer Protocol (HTTP) *basic* authentication. For this type of authentication request, the web server instructs the client browser to bring up a pop-up window that asks for a user name and password. The provided user name and password are returned to the web server, which validates the response against a local data store (can be a simple text file or perhaps an LDAP server). If the proper information was provided by the client, the environmental variable *REMOTE_USER* is set by the web server. The web application can then use the *REMOTE_USER* variable in any way it wishes. The authentication layer is therefore separated from the application layer.

The Policy Agent works in a similar fashion. Accesses to protected URLs are intercepted by the Policy Agent, which asks the Access Manager to validate the end-user's credentials. If the end-user has not previously authenticated (does not have a proper SSO token browser cookie), he is redirected to the Access Manager for authentication. After credentials are

provided, the Access Manager redirects the end-user back to the Policy Agent.

When the Policy Agent returns control to the application, it also returns several standardized data objects, including *REMOTE_USER*. The Policy Agent sets the same environmental variables that are set by a web server using basic authentication, so for the application being protected, it does not generally matter whether HTTP *basic* authentication or Policy Agent authentication is used. The underlying application can then use the environment provided by the Policy Agent for further authentication and authorization.

A simple application that previously used *basic* authentication can easily be configured to use the Policy Agent, which is installed as a separate component onto a web server or application server. In the case of Sun Web Servers, the name of the shared library containing the Policy Agent executable is added to the *magnus.conf* file. A configuration file is simultaneously created on the web server that simply defines *which* URLs are to be protected by the Policy Agent. The native web server access control list is modified to disable protection of the resource.

The specific access control list for the URL is maintained by the Access Manager. The Sun JES includes a graphical user interface to manage access control lists.

Complex web applications — typically larger open-source projects and commercial products — require code modification and customization to integrate into a Policy Agent environment. A direct API is available for applications needing to forego the Policy Agent and communicate directly with the Access Manager. The amount of effort required to integrate a product into the Access Manager SSO environment depends heavily on the complexity and implementation of the application.

A significant advantage of using the Access Manager to provide authentication to a large number of applications is consolidation of authentication. Assuming a modest application inventory, it would be challenging to upgrade each application to accept a new form of

authentication credentials. For example, if a site were to move from username and password to certificates as its primary authentication mechanism, each application must be modified to accept this new credential. By using the Access Manager, credential changes only need to be made in one location. Applications using Policy Agents or the Access Manager API do not need to be altered. Once an application is integrated into the Access Manager environment, little else needs to be done to accommodate new authentication mechanisms.

Policy Agents are available from Sun Microsystems and third-party vendors for a wide variety of web resource environments, such as the commercial Java application servers (IBM WebSphere, BEA WebLogic, Oracle Application server, and Redhat JBoss), Microsoft Internet Information Server (IIS), Apache, and Tomcat, among others. The Agents allow third-party web providers to be integrated into a centralized authentication infrastructure. The Access Manager API can be used directly to integrate almost any application, provided source code is available. Commercial software vendors have been willing to modify their products to integrate into SSO solutions.

Browsers

Browser compatibility is a significant issue in enabling a successful portal. Argonne's portal components have been tested with Microsoft's Internet Explorer, Firefox, and Mozilla.

Multiple browsers (including Internet Explorer, Mozilla, and Firefox) can use the University of Michigan's KX.509 certificates. Mozilla and Firefox require the *kpkcs11* component of the KX.509 suite to be installed on the client workstation.

The *kpkcs11* component implements the RSA PKCS#11 standard to enable applications such as web browsers to access certificates stored by *kx509*. The Windows version is a dynamic link library (dll), and the Unix version is a shared library. These executables emulate security devices (e.g., smart cards) to Mozilla or Firefox.

Authentication Process

Workstation Login

Workstation login that results in users having a personal certificate can be conducted in three ways:

- With a user name and password using auto-enroll certificates,
- With a user name and password using KX.509 certificates (manual), or
- With a smart card.

The highlight of all logins is that, at the end of login, the user has *both* a Kerberos credential

issued by the domain controller *and* a certificate issued by either Microsoft Enterprise Certificate Services or the KX.509 package. The user can immediately access resources that request *either* form of authentication.

Figure 7 summarizes authentication credential flow from user workstation login to application admission.

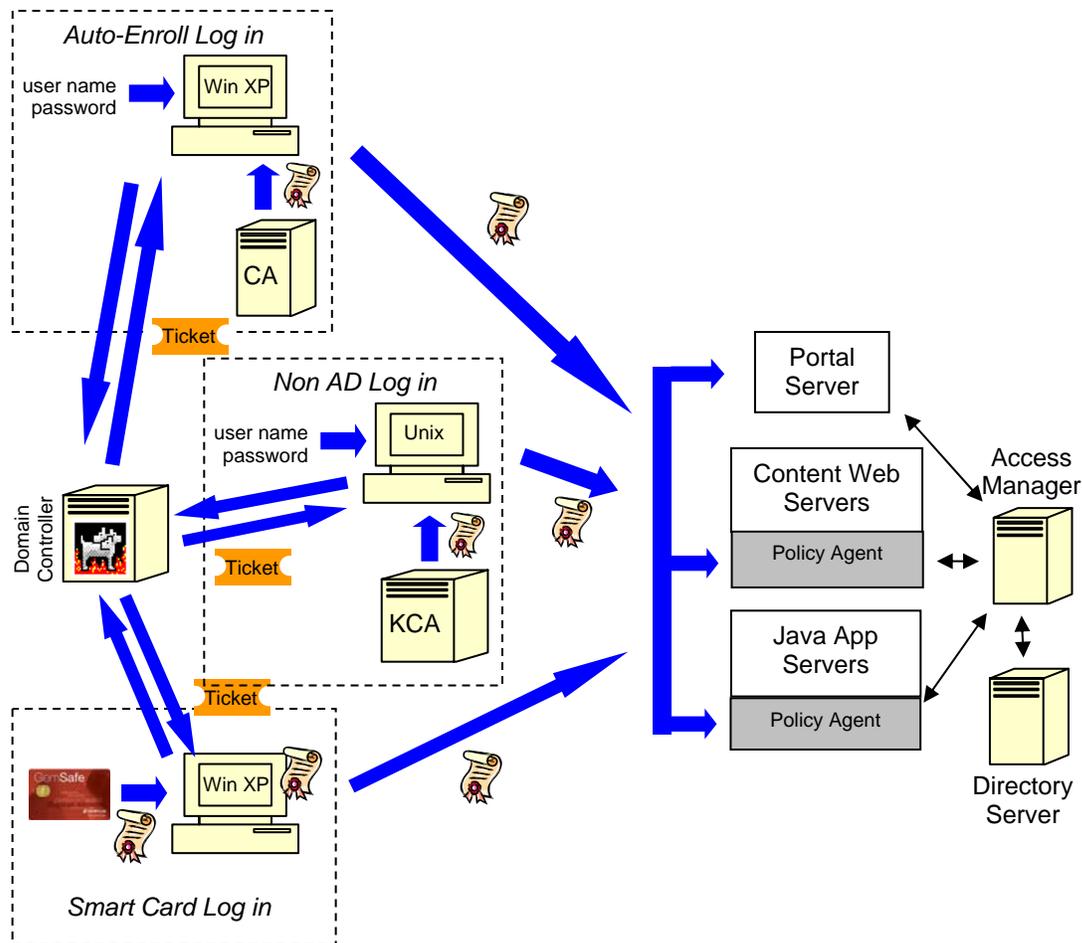


Fig.7: Authentication Communication From Logon to Application

User Name and Password

In this mode, the users log in to their workstations by using their user name and password and then acquire a certificate.

Certificate acquisition may be automatic and invisible when using auto-enroll or manual when using the KX.509 process.

- *Auto-Enrollment*

Users initiate a standard Microsoft Windows domain login by providing their user name and password. At login, the user obtains Kerberos credentials. As part of the login process, Group Policy settings are evaluated (including the policies for auto-enrolled certificates). If there is no certificate or if it has expired, an auto-enroll certificate is obtained. The process is completely transparent; users are unaware of the auto-enroll certificate process, and no action is required on their part to obtain or renew a certificate.

Auto-enroll certificates are usable only as long as the associated Windows domain account is enabled. In a non-Roaming Profile environment, a user logging onto another Microsoft workstation obtains a new auto-enroll certificate. In a Roaming Profile environment, the certificate is transmitted with the user profile.

- *Dynamic KX.509 Certificates*

Kerberos Login. If the desktop computer conducts a Kerberos login, the user receives a Kerberos ticket as part of the login process. The user then manually requests a short-term certificate by running the kx509 client program on his/her desktop computer.

The kx509 program uses Kerberos to authenticate to one of the KCA servers. The program generates a public/private key-pair and sends the public key to the KCA server. The KCA server returns a certificate good for the lifetime of the Kerberos ticket used in the request — typically 12 hours or less. The certificate and private key are stored on the local computer.

Non-Kerberos Login. If the desktop computer does not conduct a Kerberos login, users must manually obtain a Kerberos ticket using kinit. Users request a short-term certificate by running the kx509 client program on their desktop computers, as they would if they had performed a Kerberos login.

- *Smart Card*

The insertion of a smart card is automatically recognized by Microsoft Windows Graphical Identification and Authentication (GINA). Windows immediately prompts the user for the Personal Identification Number (PIN) that permits use of the private key functions of the card.

The client workstation uses the PKINIT component of the Kerberos protocol to obtain Kerberos credentials. The *User Principal Name* contained in the *Subject Alternate Name* field of the certificate enables the domain controller to select the user for which a session should be initiated.

Validation of the user's certificate by the domain controller is included in the login process. The controller validates the certificate chain and inspects the CRL of Microsoft Enterprise Certificate Services.

Smart card login is quick and easy for users. In the Argonne smart card pilot program, several non-technical users have been issued smart cards. They use the cards routinely with no complaint (even though they are optional).

Access Manager Authentication

The end-user portal authentication experience is straightforward. All web and application resources that are protected by a Policy Agent rely on the Access Manager to provide authentication and authorization. Therefore, accessing any protected resource results in the same experience.

The only variation is whether the client has previously authenticated to the Access Manager and still owns a valid session.

The general end-user experience can be described as follows:

1. The user starts a new browser and points it at <https://www.anl.gov/protected/>.

2. The Policy Agent uses information from a requested cookie and the Access Manager to determine whether access can be granted.
3. If access can be granted, the user is granted access to the resource.
4. If access cannot be granted (no session), the user is redirected to the Access Manager to provide credentials.
5. The user provides a certificate to the Access Manager.
6. The user is redirected to the protected resource, and the process resumes at Step 2

By default, Internet Explorer will automatically present a certificate in the certificate store to a web site that requests one, assuming that only one certificate is present. Most Argonne users have only the auto-enroll certificate available in their certificate store. Therefore, when such users contact the Access Manager for authentication, the authentication process begins immediately; no user action is required. The Access Manager accepts the certificate and creates a user session.

Authentication is virtually the same if the certificate is contained on a smart card. The only difference is that the user is prompted for the PIN so that the private key functions of the card may be used.

During an average business day at Argonne, roughly 1,000 users will authenticate to the Access Manager. Half of these users authenticate by using a certificate.

Conclusions

Argonne National Laboratory's deployment of a certificate-enabled infrastructure and portal technology addresses the two vexing challenges associated with enabling certificates for authentication:

- Providing certificates to users, and
- Enabling applications to accept certificates for authentication.

The result is that Argonne employees routinely and transparently use certificates to access Laboratory applications.

Argonne succeeded in this endeavor by successfully leveraging and integrating a number of authentication and related technologies to use certificates in a real-world, end-user environment. Certificate deployment was accomplished by using two types of technology:

- Short-term user certificates issued via Microsoft's auto-enroll technology or the University of Michigan's KX.509 suite, and
- Long-term user certificates contained on smart cards.

We enabled the applications to accept certificates by adopting the Sun Java Enterprise System. The Microsoft, Sun Microsystems, and University of Michigan products demonstrate daily that certificate authentication — even end-to-end certificate authentication — is doable today.

Argonne has accrued several specific benefits through its certificate-enabled infrastructure, as described below.

Benefits

Approach Enables Single Sign-On for Users

In Argonne's authentication infrastructure, one authentication credential provides access to many applications. Successfully obtaining a Kerberos ticket permits the user to obtain a certificate (auto-enroll, KX.509). On the other hand, possessing a valid certificate allows the user to obtain a Kerberos ticket (smart card). At the completion of login, the user possesses both types of credentials and can immediately interact with downstream applications requiring either authentication technology.

Short-Term Certificates Eliminate User Certificate Management Burdens

The Microsoft auto-enroll and the University of Michigan KX.509

technologies provide a quick and simple way to issue certificates to users and thereby accelerate certificate deployment. These tools eliminate many of the burdens of certificate management for the user — such as issuance, private key management, and renewal. Overnight, users can be certificate-enabled.

Short-Term Certificates Jump Start Application Certificate Enablement

Organizations should consider using Microsoft's auto-enroll technology to allow rapid deployment of applications that use certificate authentication. Auto-enroll technology allows certificate deployment to be decoupled from application enablement. Organizations can benefit from certificate-enabled application without having to address the burdensome aspects of certificate deployment.

With auto-enroll technology, organizations can prepare their applications now for HSPD-12 certificate availability.

Approach Provides Universal Application Access

Argonne has made use of proprietary, open-source, and standard protocols and technologies to enable employees using various desktop operating systems to access Laboratory applications by using certificates. Whether the end-user is running Windows, Linux, Solaris, or Macintosh, there is a method to acquire a certificate and import it into a browser for use in portal applications.

Applications Are Authentication-Neutral

The applications provided in the portal are authentication neutral. The application authentication process is centralized through the Sun Access Manager, which provides the flexibility to support future authentication mechanisms without making changes to the applications that depend on authentication. A certificate can be used for authentication just as easily as a user name and password. The application only knows that the user has authenticated. The manner

in which authentication occurred is not critical.

Approach Allows End-to-End Certificate Authentication

Via smart cards, Argonne is providing end-to-end SSO based on certificates. That is, users rely totally on certificates for authentication; they never present a user name and password. Indeed, in the future, users will not have passwords.

Smart Cards Allow Functional Certificate Portability

Adding smart cards to a certificate instantly enables certificate portability. Microsoft Windows manages smart-card-stored certificates as seamlessly as it manages internally stored certificates. Users find that smart cards have a negligible impact on workplace efficiency and permit certificate authentication from any workstation. In a properly equipped environment, the certificate is as portable as the user name and password.

Approach Increases HSPD-12 Readiness

An outcome of smart card deployment, as required by HSPD-12, is that users possess portable long-lived certificates. The deployment of portal technology has positioned Argonne for the availability HSPD-12-compliant smart cards and certificates. The versatility of X.509 authentication included in the Sun Access Manager enables Argonne to readily accept an HSPD-12 certificate for application authentication.

Lessons Learned

Two-Factor Authentication Can Enable SSO

Two-factor authentication requirements that require smart cards (e.g., HSPD-12) can be a vehicle for user certificate deployment. Argonne's smart card deployment has shown that users can readily employ smart cards for client authentication and subsequently use the same smart card for application access. Smart cards and their supporting software readily interact with

browsers. The user impact of performing a smart card login is negligible.

Auto-Enroll Certificates Complement Smart Cards

Argonne has realized the benefits of issuing auto-enroll certificates to users who log in with smart cards, especially users who must frequently authenticate to applications. Application authentication via certificates requires access to the private key. Repeated presentation of the smart card becomes burdensome to the user. Issuing an auto-enroll certificate to smart card users permits two-factor authentication for the initial login without requiring two-factor authentication for each successive application.

Automation Is Key to Certificate Usage

As noted above, Argonne's Administrative Systems Portal processes 500 certificate authentications per day. Argonne's KX.509 KCA servers issue fewer than two short-term certificates per day. The vast majority of application certificate authentications rely on auto-enroll certificates.

So, although only two commands (kinit and kx509) are required by users to enable certificate authentication — and thus SSO — from Linux and Mac desktops to Argonne's Administrative Portal, these users continue to rely on user name and password. It is clear that certificate acceptance is achieved through automation of certificate issuance and management.

Issues

Undesirable SSO

The concept of using a certificate instead of a user name and password for authentication is new to many users. Confusion can arise when a user wishes to access an application as another user. For example, a Human Resources representative may wish to have an employee who is sitting in his or her office log in to an application. When the application is accessed, the Human Resources representative is automatically logged in because the certificate contained in the user's profile is automatically

presented by Microsoft's Internet Explorer to the Sun Access Manager. As a result, Argonne Human Resources representatives do not receive auto-enroll certificates.

User education is therefore an important part of certificate rollout. Confusion may arise unless an employee understands how authentication is occurring and how to change default browser behavior.

System Administrator Skills

Similarly, system administrators are generally unfamiliar with certificates and public key infrastructure concepts. Technical staff charged with maintaining the desktop environment and supporting users may not understand the roles of certificate authorities, certificates, and smart cards. Too often, system administrators equate the smart card PIN to the user's password.

The challenges that system administrators face will increase with the adoption of HSPD-12 smart cards for authentication. Today at Argonne, the certificate authority is local, and certificate issues can be addressed by on-site staff. As Argonne accepts externally signed certificates for authentication, its staff must be prepared to work with external service providers to address real-time authentication issues. During Argonne's smart card pilot program, staff experienced the absence of a valid CRL, which disables Microsoft smart card login. Under HSPD-12, organizations will have to depend on external information sources for authentication.

Smart Card Certificate Requirements

The current requirement that the *Subject Alternate Name* field of the smart card certificate contain the *User Principal Name* of the user prevents the card from being used for desktop logins in other Windows domains. As described earlier, the UPN is username@domain, and a domain controller cannot normally establish a session for a user of another domain. Microsoft is expected to remove the requirement for the

UPN in the next version of Microsoft Windows.

Related Work

PIV Smart Card Support

Argonne National Laboratory sees great value in having a broadly trusted and interoperable identity credential as envisioned by HSPD-12. The Laboratory has obtained NIST SP 800-73-1-compliant smart cards from vendors and has developed enhancements to the Open Source Smart Card Project (OpenSC) to enable Linux and Mac platforms to use the certificates contained on these cards. These PIV enhancements have been donated to OpenSC.

OpenSC provides a PKCS#11 interface, thus making the smart card available for Kerberos login via PKINIT. For example, the Heimdal Kerberos with PKINIT enables smart card login for open systems such as Linux.

Acknowledgements

This work was produced with funding from the U.S. Department of Energy's Office of Science under Contract Number DE-AC02-06CH11357.

The authors would like to thank Gemalto, MobileMind, and Oberthur for providing sample PIV cards.

References

Butler, R., D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, and V. Welch, "A National-Scale Authentication Infrastructure," *IEEE Computer*, 33(12):60–66, December 2000.

Doster, W., M. Watts, and D. Hyde, "The KX.509 Protocol," University of Michigan, Ann Arbor, MI, 2001 (<http://www.citi.umich.edu/techreports/reports/citi-tr-01-2.pdf>).

Foster, I., and C. Kesselman, "Globus: A Metacomputing Infrastructure Toolkit." *Intl J. Supercomputer Applications*, 11(2):115–128, 1997.

Heimdal Kerberos Implementation (<http://www.pdc.kth.se/heimdal/>), October 5, 2006.

Komar, B., "Microsoft Windows Server 2003 PKI and Certificate Security," Microsoft PKI Team, Microsoft Press, Redmond, WA, 2004.

Microsoft Corporation, "2821A: Designing and Managing a Microsoft Windows Public Key Infrastructure," Microsoft Official Curriculum 2821A, Redmond, WA, 2003.

Neuman, B.C., and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications*, 32(9):33–38, September 1994.

Open Smart Card Project (<http://www.opensc-project.org/>), October 5, 2006.

RSA Laboratories, *PKCS #11 v2.20: Cryptographic Token Interface Standard*, Bedford, MA, June 2004.

Sun Documentation (<http://docs.sun.com/>, <http://docs.sun.com/app/docs/prod/entsys.05q4#hic>).

Sun Java Enterprise Server 2005Q4, (<http://www.sun.com/software/javaenterprisystem/index.xml>).

U.S. Department of Homeland Security, *Homeland Security Presidential Directive (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors* (<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>), August 27, 2004.

Zhu, L., and B. Tung, *RFC 4556 Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)*, The Internet Society, June 2006.

¹ Microsoft offers both Standard Certificate Services and Enterprise Certificate Services. All of the Microsoft functionality discussed in this paper is achieved via the Enterprise Certificate Services.

² The selection of smart cards and corresponding middleware is in itself a research undertaking and so outside the scope of this paper. The smart card market is fragmented and proprietary. Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard 201 (FIPS-201) will enable significant improvement in the standardization and interoperability of smart cards.

³ The Access Manager uses an internal list of trusted root certificates to validate user certificates; it does not rely on root certificates contained in Active Directory.