

Who's That Knocking at My Door?



Authentication & Authorization Technologies

LACASIS Workshop
September 15, 2000

Terry Ryan
Associate University Librarian for Info Technology
UCLA Library
tryan@library.ucla.edu

Three Parts of Access Control

- § Who are you, and how do I know you are who you say you are? = **AUTHENTICATION**
- § What attributes do you have, what role are you playing? =
IDENTITY/DIRECTORY/DEMOGRAPHICS
- § Based on that, what will I let you do? =
AUTHORIZATION

How do you identify yourself, and prove it?

- § Something you know (a password)
- § Something you have (Library card with barcode)
- § Something you are (fingerprint, iris scan)

Traditional solution: User ID & Password



- Each application keeps a list of users
- Each user associated with a password
- If you know your password, application knows you are you
- User ID tied to info used for authorization decision

What's good about User ID & Password?



- § Very well understood by users
- § Most applications come with capability built in
- § If you control your application, can implement independently

What's wrong with User ID & Password?



- § Password proliferation
- § No longer truly secure
- § If you must -- encrypt

Beyond Passwords: Three Common Approaches



- § IP Authentication
- § Kerberos
- § X.509 Certificates

IP Authentication



- § Application keeps a list of IP addresses
- § If you come from a valid IP location, you have access
- § Authenticates a location, not a user

What's good about IP Authentication



- § Good match to enterprise-wide licenses
- § Easy to implement in most Web servers
- § Transparent to users

What s not so good about IP Authentication



- § Works best when entire enterprise should be authorized
- § Maintaining IP lists can be challenging
- § For remote use, must use Proxy Server
- § Low level of security

Kerberos



- ☞ Trusted third-party authentication system
- ☞ Everyone registered in a single Kerberos server
- ☞ Log on to Kerberos server and it gives you a short-lived ticket
- ☞ Same ticket tells all applications that you are you

What's good about Kerberos



- Still a password, but only one and encrypted
- Authenticates systems as well as people
- Enables strong security
- Well tested, good track record of implementations

What s not so good about Kerberos



- § Need to install clients or proxy
- § Applications must become kerberized
- § Requires a single central registration authority
- § Requires organizational commitment

What s not so good about Kerberos



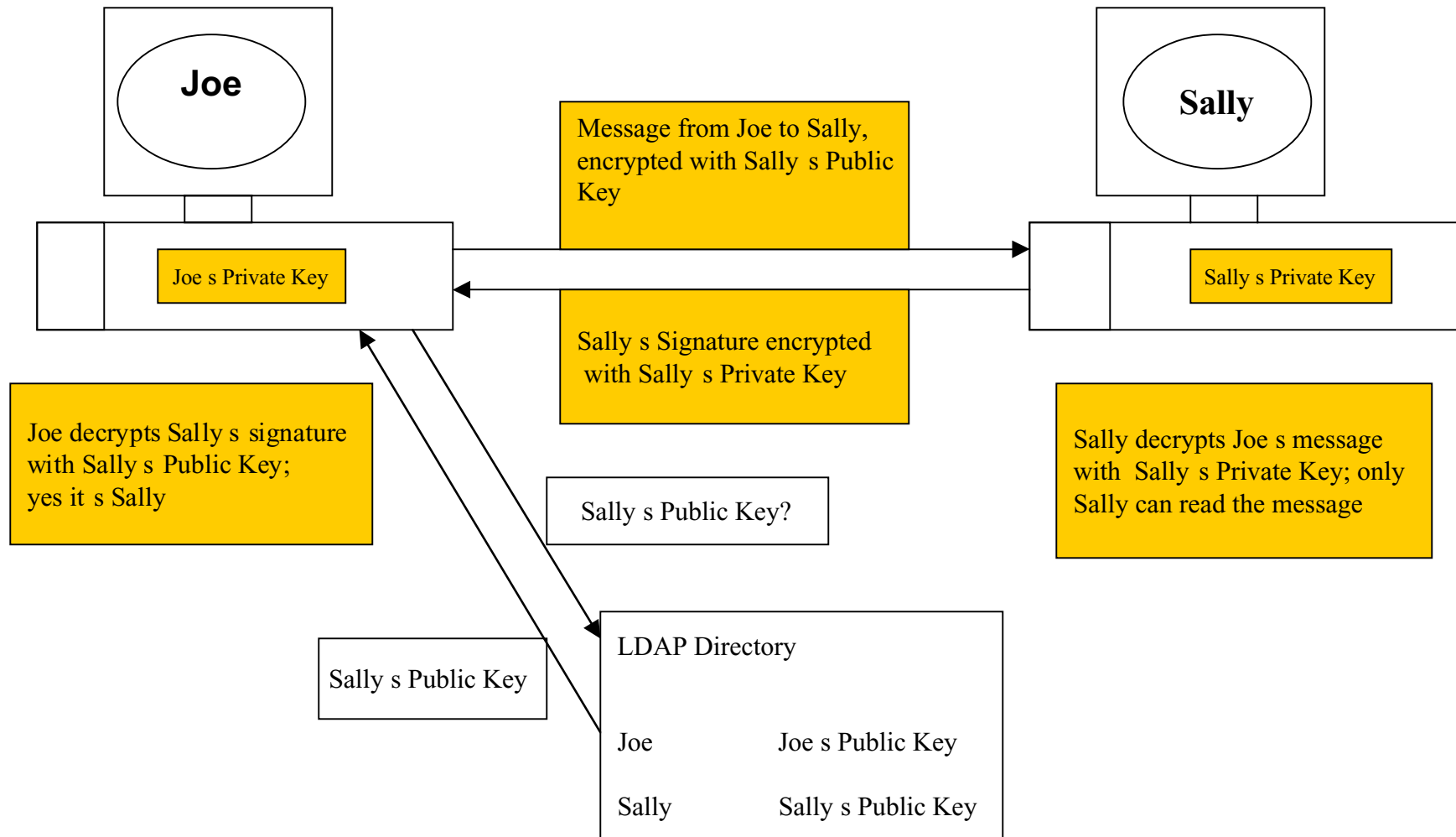
- § Most appropriate for use within an enterprise
- § Some security compromises
- § Not extensible to digital signatures, document authentication

X.509 Public key certificates

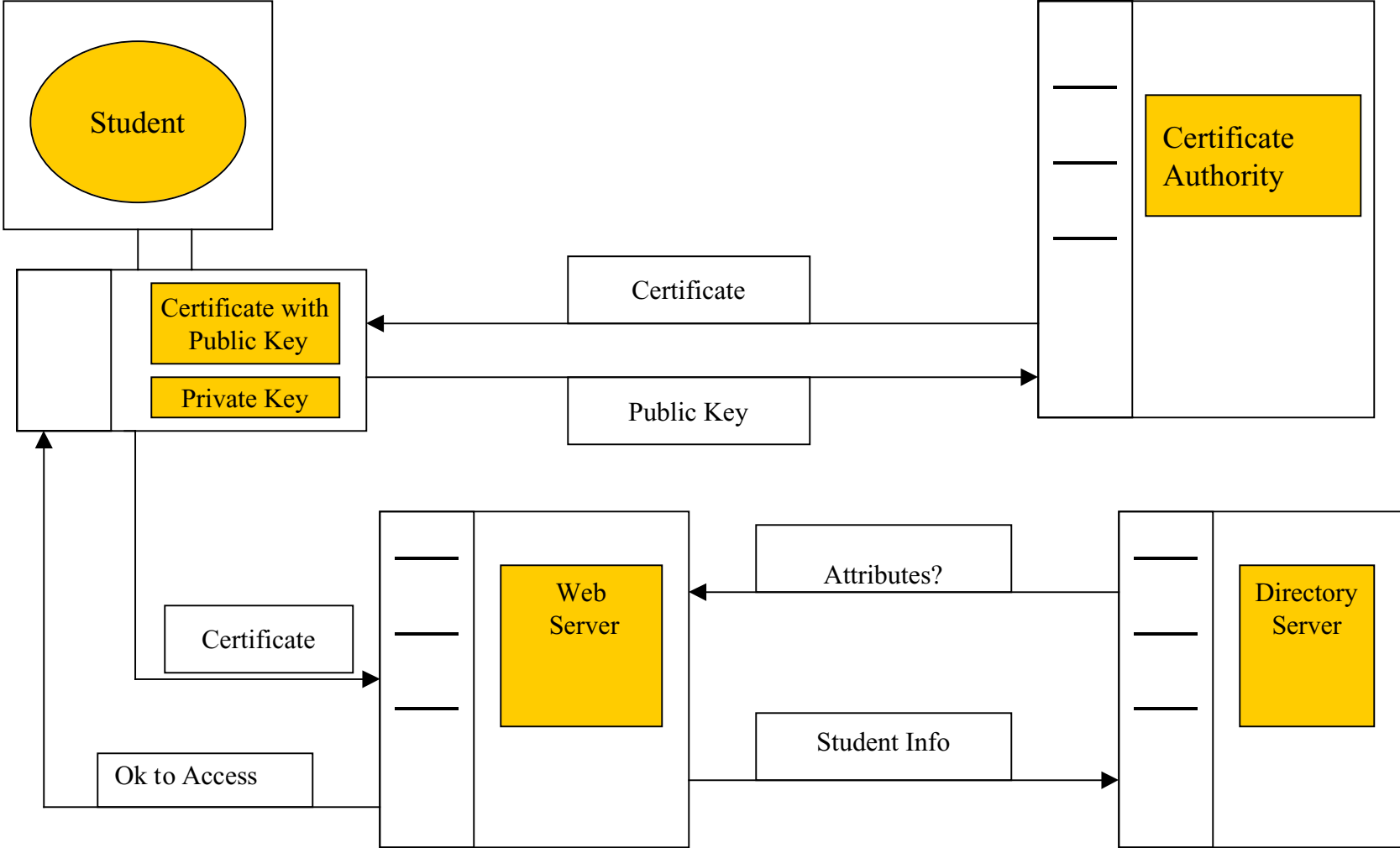


- § Based on public key/private key model
- § Part of a Public Key Infrastructure (PKI)
- § Part of the IETF Directory standards

Public Key/Private Key



Certificates



Sample Certificate Payload



Version: 2 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5withRSAEncryption
Issuer: C=US, SP=California, L=Oakland, O=University of California,
OU=UC Davis
Validity:
Not Before: Jul 31 12:00:00 1997 GMT
Not After: Jul 31 12:00:00 1998 GMT
Subject: C=US, SP=CA, L=Oakland, O=University of California, OU=UC Davis,
CN=J. P. Student/Email=jpstudent@ucdavis.edu
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public Key: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00
Exponent: 65537 (0x10001)
X509v3 extensions:
Netscape CA Revocation Url: <http://ca.ucdavis.edu/ca-crl.pem>
Netscape Comment: Any comment you wish to be
displayed in the netscape certificate info dialog
Signature Info:
Signature Algorithm: md5withRSAEncryption
Signature: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

What's good about Certificates



- § Standards-based
- § Authenticates systems as well as people
- § Enables strong security
- § Support for certificates is embedded in major Web servers and Web browsers

What's good about Certificates



- § Can be used by unaffiliated services (potentially, e-resource providers)
- § PKI also supports digital signatures & document authentication
- § When only one certificate, transparent to user

What s not so good about Certificates



- § Requires a single central registration authority
- § Requires organizational commitment & resources
- § Applications must become certificate aware

What s not so good about Certificates



- § Must work out policies and procedures up front
- § Public workstations are a challenge
- § Getting and managing certificates can be hard for users

Who's using Certificates



- § Banks, stock traders, etc
- § Federal Government (ACES: Access Certificates for Electronic Services)
- § University of California

Useful bookmarks



- § <http://gits-sec.treas.gov> Federal Public Key Infrastructure Steering Committee
 - § Access with Trust, Sept 1998
 - § The Evolving Federal Public Key Infrastructure, June 2000
- § <http://www.ucop.edu/irc/auth/> University of California Common Authentication Project