Intro to Authentication

James Farricker

January, 2016

Definitions

Authentication:

Verification of an entity's (person, server or object) identity

Authorization:

Granting an entity access to services or information

Authentication / Authorization

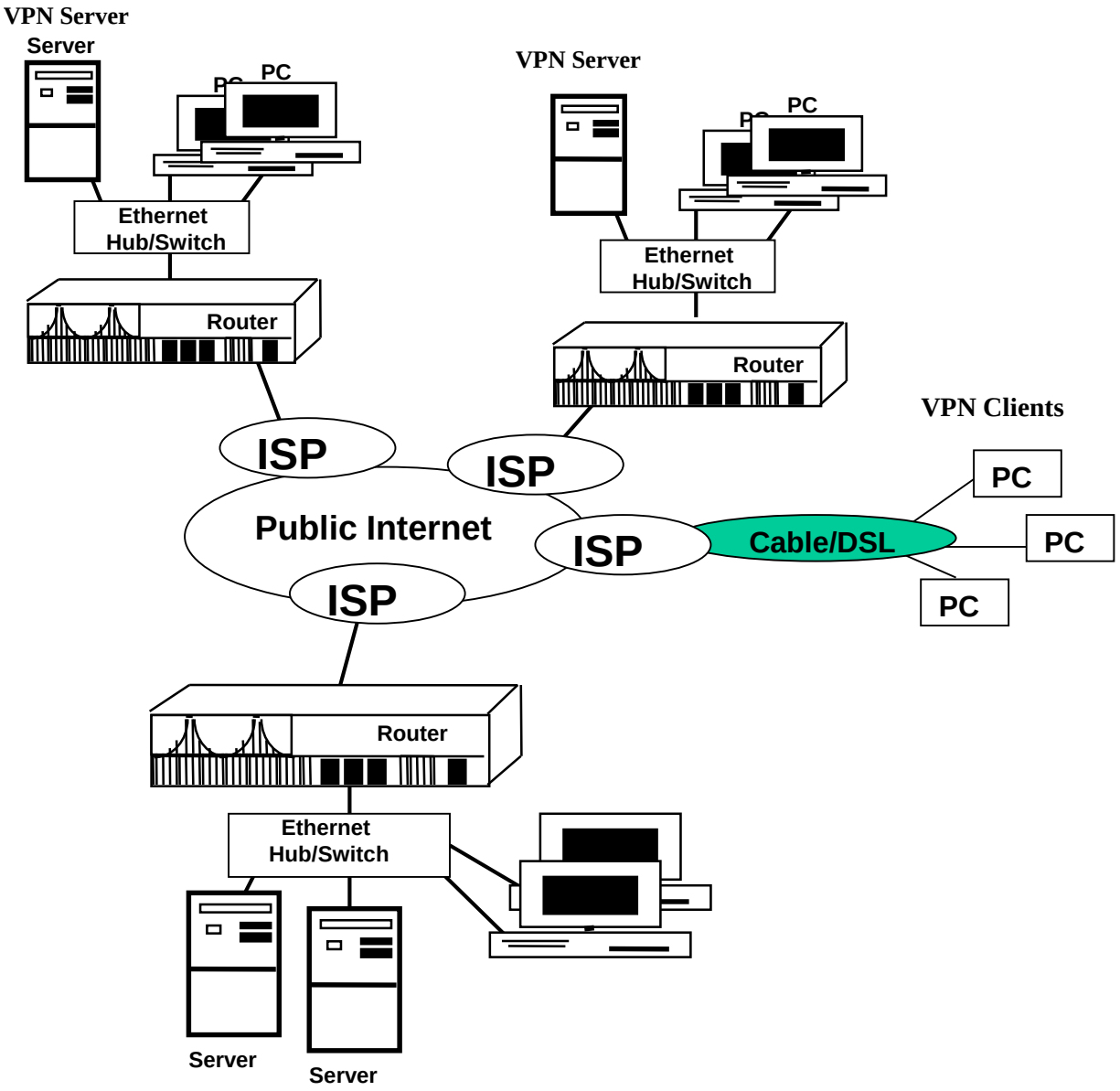
- Some Companies have multiple authentication /access control schemes. What are some authentication methods ?:

- Each authentication scheme has a unique set of challenges

  Why are biometrics (retina scan, fingerprint) controversial ?

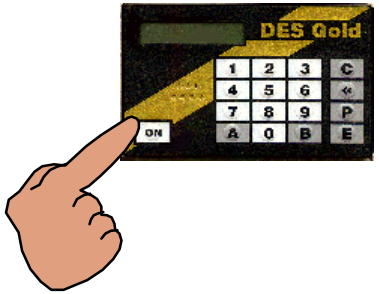
- Users often need multiple passwords to access the business applications and data assets they require

Remote Access



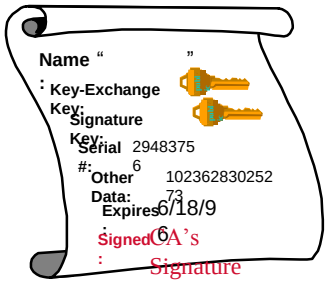
Remote Access - Authentication

DES Gold token cards - used to authenticate remote users and wireless users

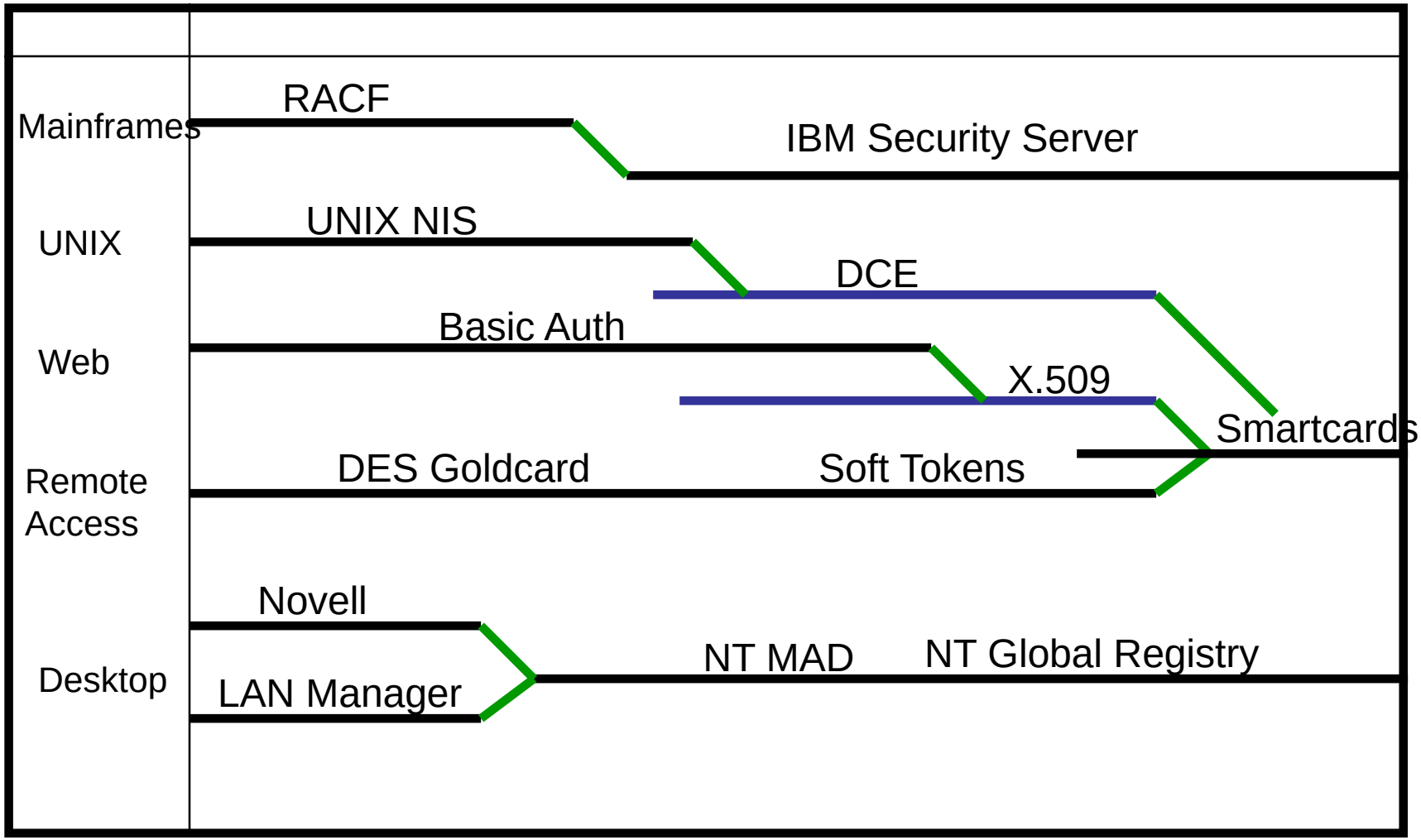


Smart card is the size of a standard plastic " credit card " with an embedded computer chip holding various types of information in electronic form with sophisticated security mechanisms.

X.509 Digital Certificates - A component of the ITU (CCITT) and ISO/IEC defined standards
It defines the standards and format to be employed for public-key certificate distribution for authentication and/or digital signatures.



Authentication Migration



Smart Cards

What is a Smart Card ?

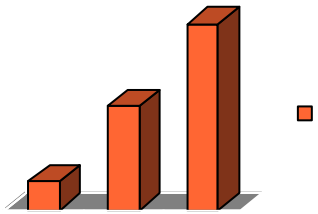
- The smart card is the size of a standard plastic " credit card " with an embedded computer chip. The chip holds various types of information in electronic form

  with sophisticated security mechanisms.

Current applications

- Pay TV
- Pay phones
- Health care records
- Electronic purse
- Transportation
- System Security

Smart Card Market Growth



Smart Cards

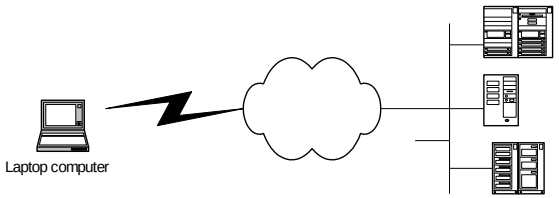
Why Smart Cards ??

- X.509 certificates project
- External Access “Strong authentication”
- Identification / Badging

“Smart Badge”

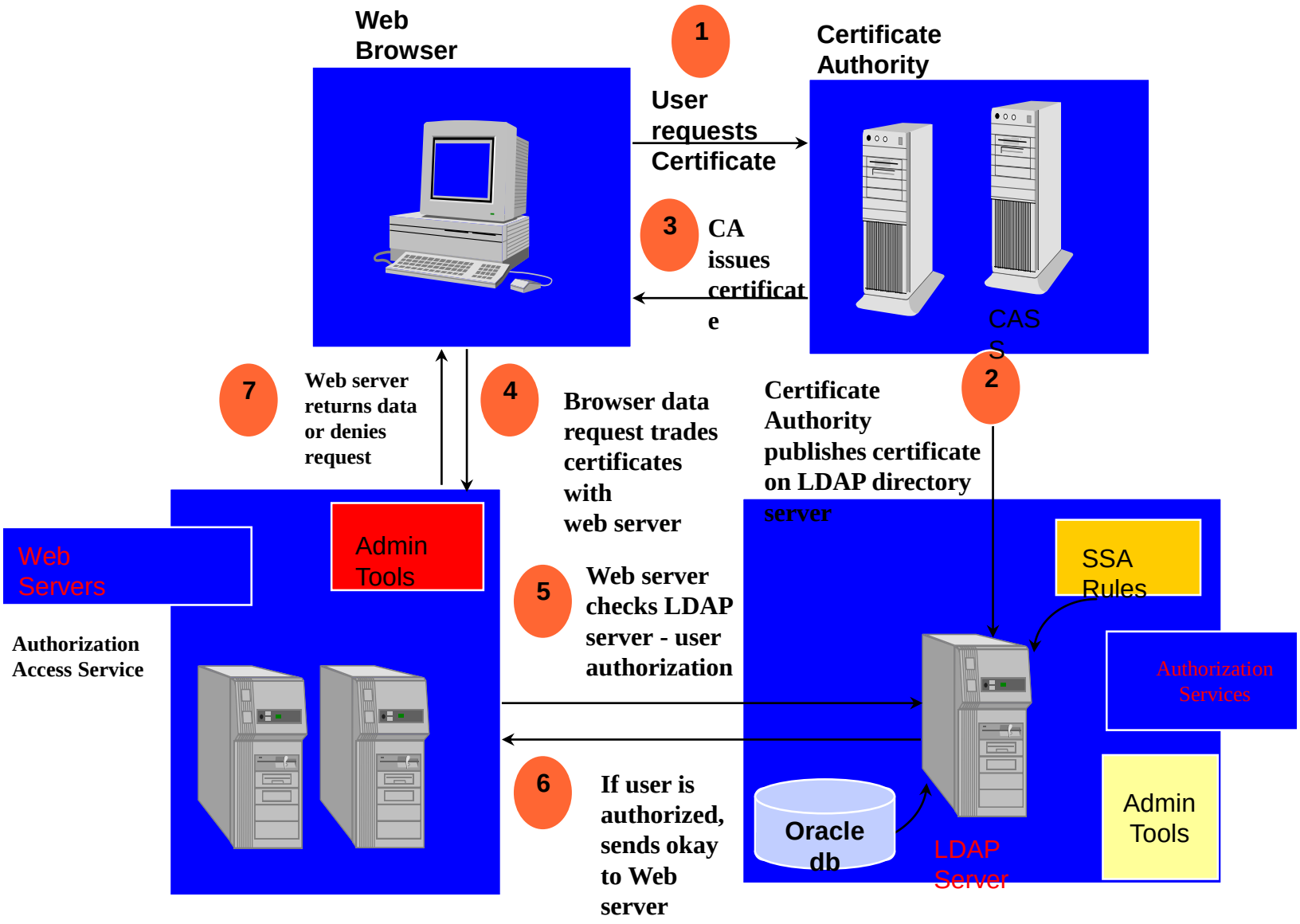
Benefits

- Compliments / Enhances X.509 certificate authentication architecture
- Makes certificates portable
- Strong Authentication “Something you have and Something you know”
- Multi-level access control to information stored on card
  - Who can access (everybody, the card holder, specific 3rd party)
  - How can information on the card be accessed (Read, added to, modified or erased)
- Integrated device support in common software applications (Netscape, MS Internet Explorer, MS Windows NT)



Access Authentication

Remote Access - Authentication



General Strategies

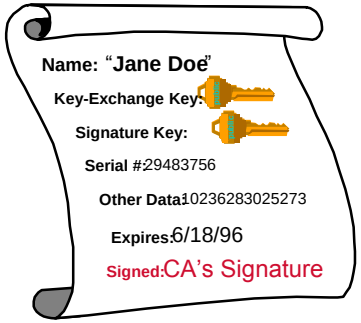
Implement Security Certificate Infrastructure

To enable:

- Electronic Commerce
- Secure web based transaction processing
- Digital signatures
- Secure E-Mail interchange and Exchange (S/MIME compliant)

What is a Certificate?

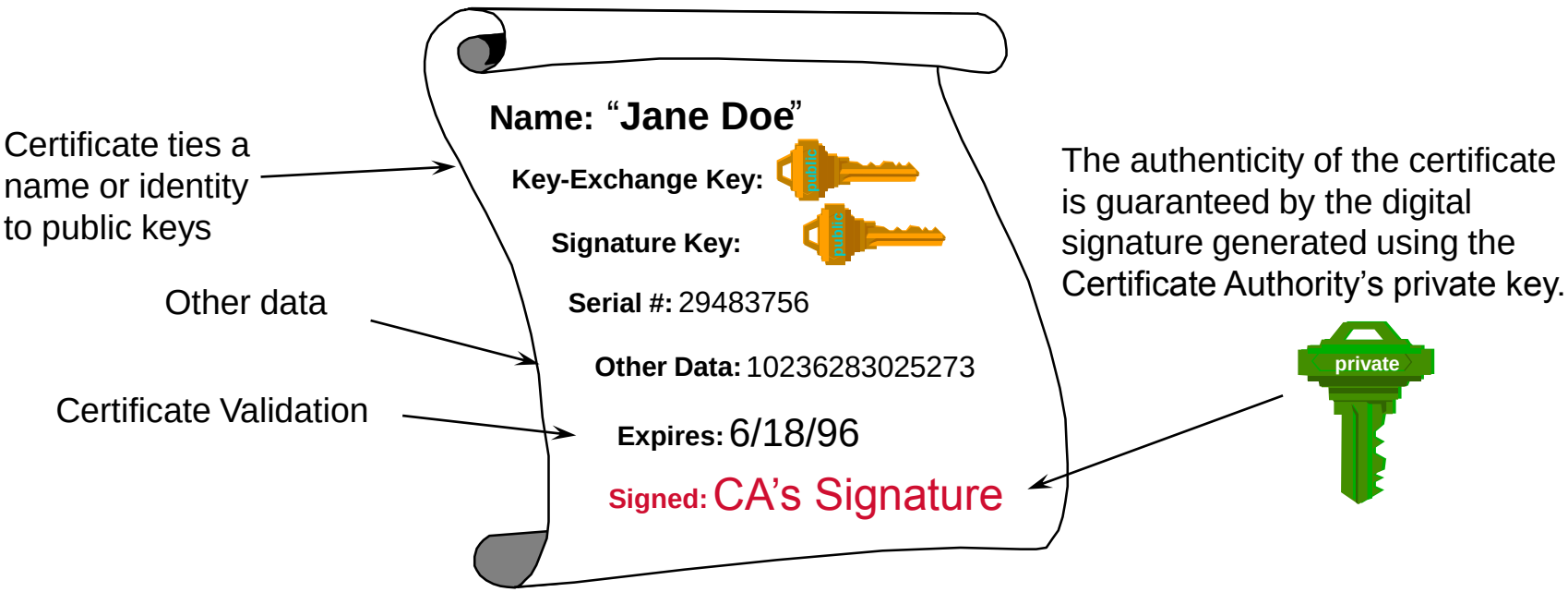
- Security certificates are data files
- Netscape and Microsoft web browsers store certificates in a password protected area on the user's desktop



- More trusted than passwords (strong authentication)
- They can be carried on floppies
- They can be carried in Smart Cards
- They are used to authenticate identity and establish encrypted communications

What is a Certificate?

Binds a public key to an identity



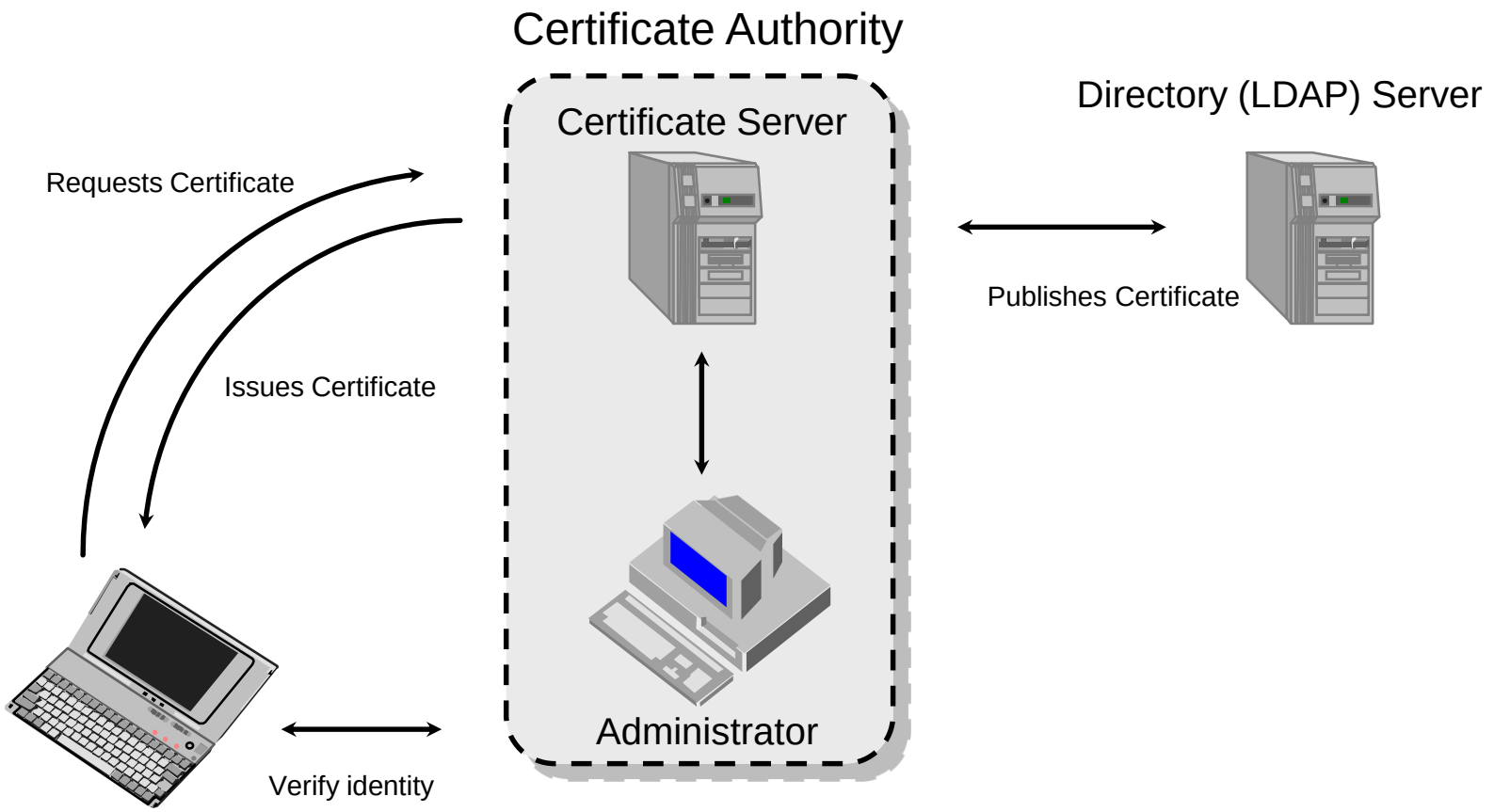
What Is a Certification Authority?

It is the service (software, servers, policies, procedures and support staff) which issues X.509 security certificates.

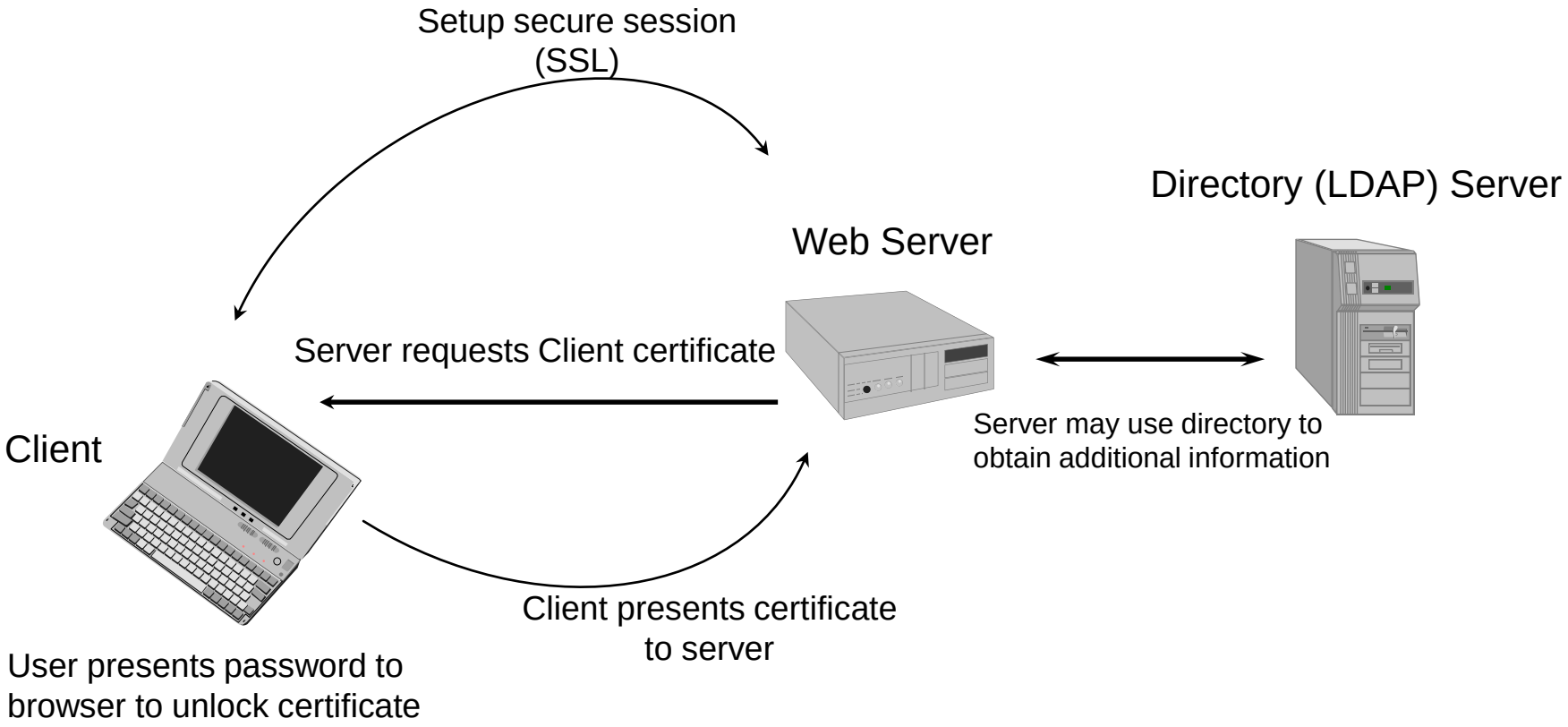
Primary responsibility of the Certificate Authority is to assure the identity of the person receiving the certificate.

The Authority is also responsible for revoking certificates.

Obtaining a Client Certificate



How to Use a Certificate



How have modern authentication methods changed the focus of hackers/intruders/attacks ??