Directory Technologies for PKI Repositories

Sharon Boeyen
Entrust Technologies

©1998 Entrust Technologies, inc. Proprietary

Outline

- Overview
  - PKI Repository
  - Technology selection considerations
  - Status of Directory functionality - standards
- Sample directory technology solutions
  - Small scale PKI - single directory server solution
  - Larger scale PKI - multi-server directory solution
  - Inter-enterprise PKI - multi technology solution
- Summary

©1998 Entrust Technologies, inc. Proprietary

PKI Repository - Primary Task

- Publish and provide access to:
  - User public-key certificates
  - CA public-key certificates
  - CA cross certificates
  - Certificate Revocation Lists (CRL)
  - Other related info

©1998 Entrust Technologies, inc. Proprietary

Technology Selection Considerations

- PKI scalability
  - Single site or distributed environment
  - Referral, chaining, replication
- Security issues
  - Authentication, access control, privacy
- PKI and repository interoperability
  - Protocols, schema specification, etc.

©1998 Entrust Technologies, inc. Proprietary

Directory Functionality - Status

Referral

Multiple Language

Replication

Strong Authentication

Access Control

Signed Operations

Chaining

Distributed Admin

X.500 ('93 2nd edition)
LDAP ('98 version 3)

X.500 & LDAP specified

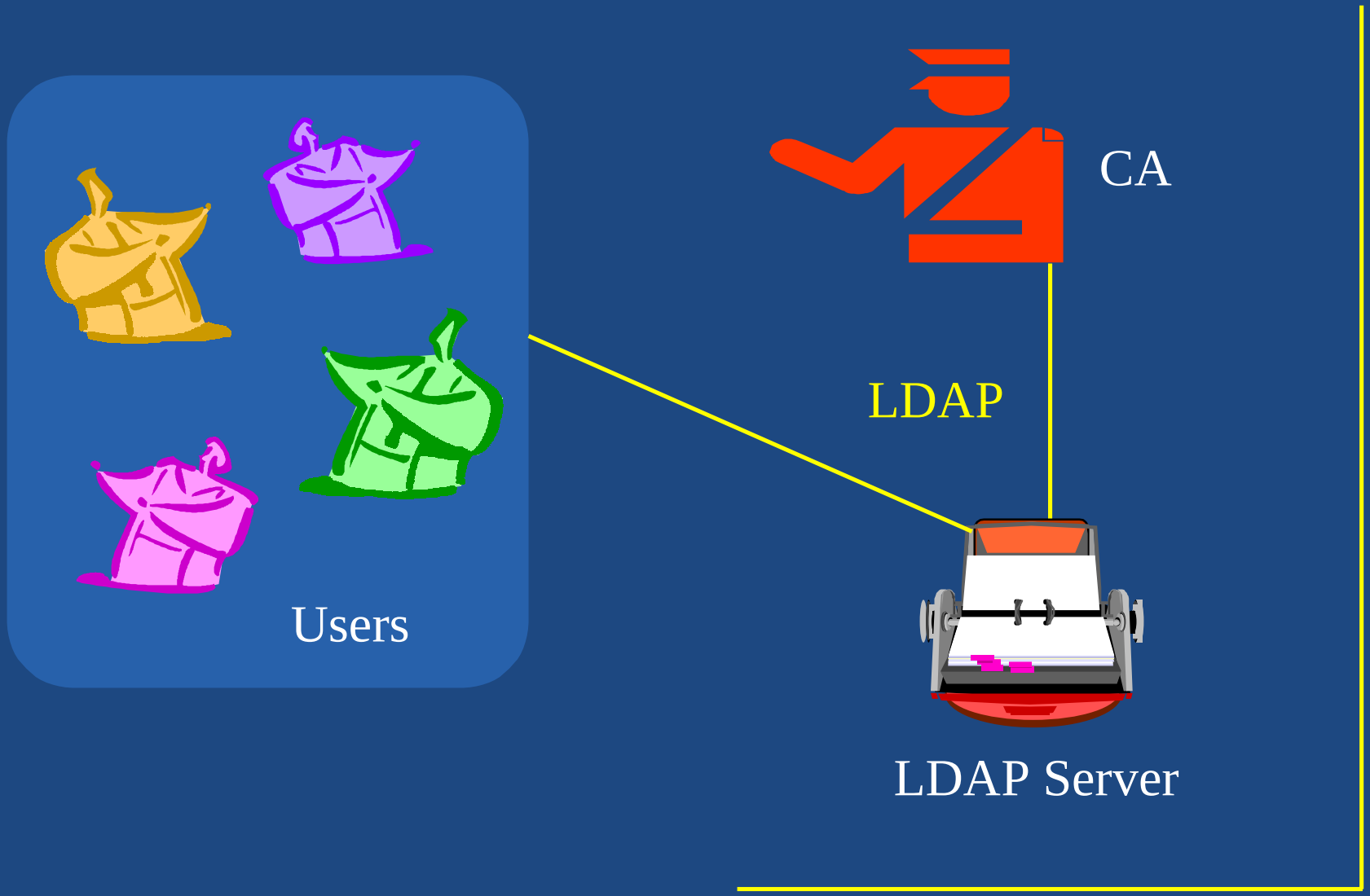
X.500 specified
LDAP partially specified

X.500 specified
LDAP planned/initiated

X.500 specified
no LDAP plans

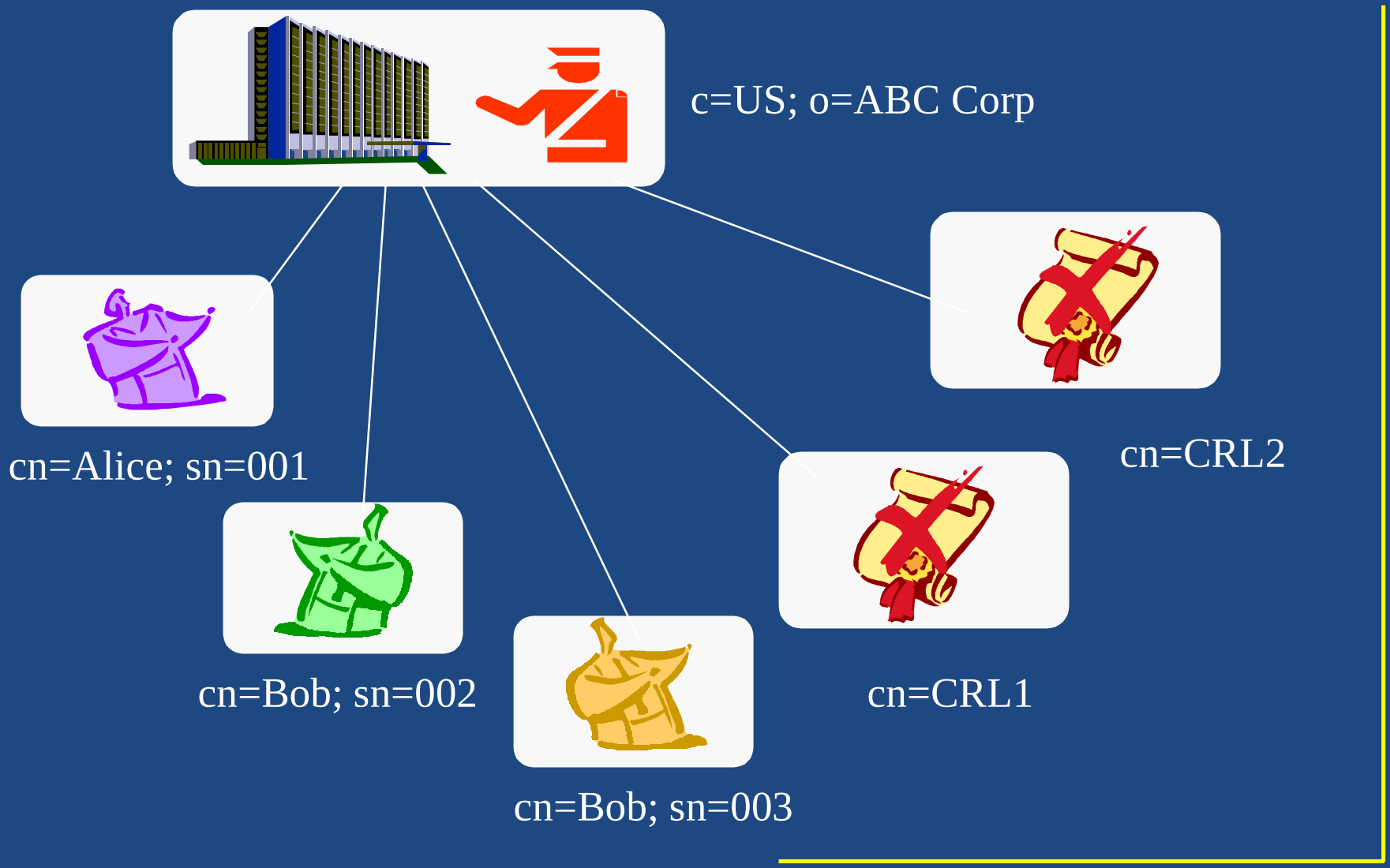
©1998 Entrust Technologies, inc. Proprietary

Small Scale PKI Architecture



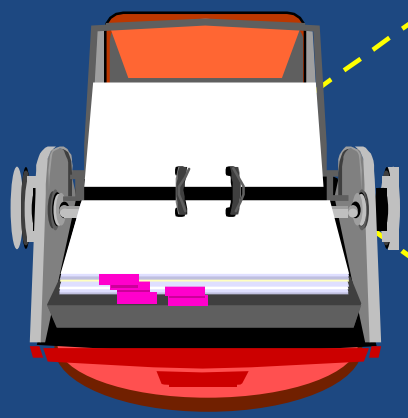
©1998 Entrust Technologies, inc. Proprietary

Sample DIT Structure



©1998 Entrust Technologies, inc. Proprietary

CA Entry - Sample Structure

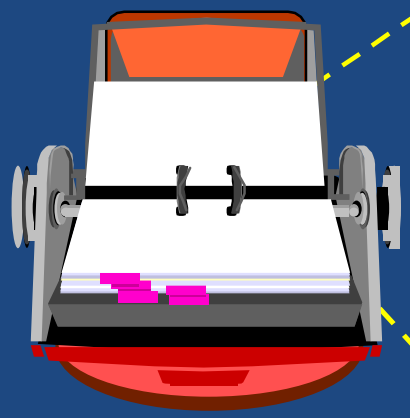


c=US;
o=ABC Corp

- **PKI CA**
  - **CA certificate**
- **Organization**
  - organization name
  - postal address
  - telephone number
  - description
  - etc.

©1998 Entrust Technologies, inc. Proprietary

User Entry - Sample Structure

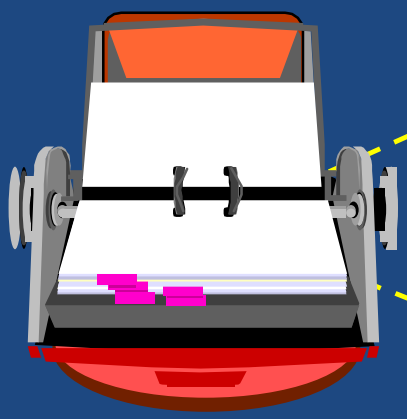


c=US
o=ABC Corp;
cn=Alice; sn=001

- **PKI User**
  - user certificate
- **Organizational Person**
  - common name
  - email address
  - telephone number
  - ...
  - etc.
  - serial number

©1998 Entrust Technologies, inc. Proprietary

CRL Distribution Point Entry - Sample Structure



c=us;

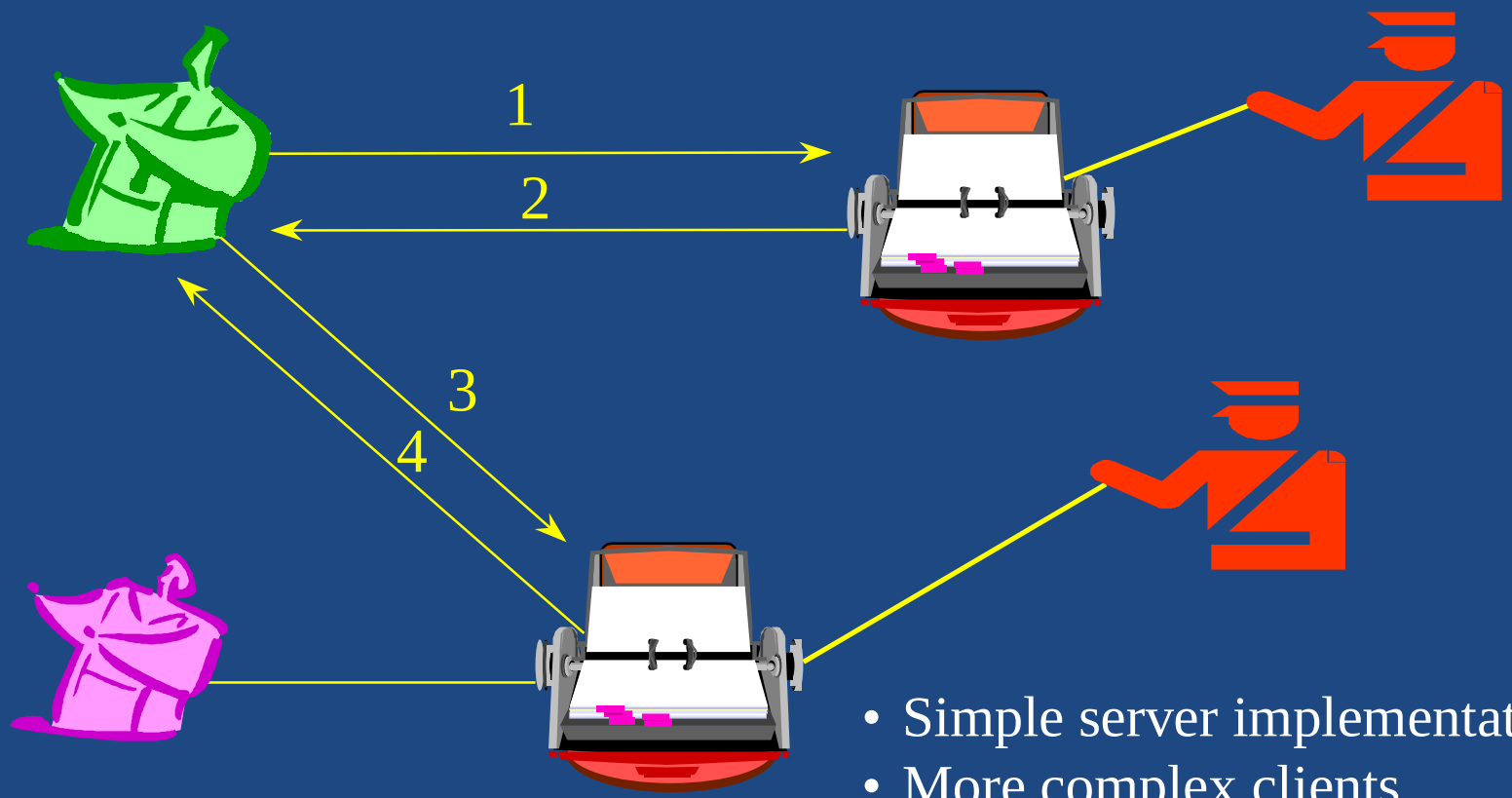
o=ABC Corp;

cn=CRL1

- **CRL Distribution Point**
  - common name
  - **CRL**

©1998 Entrust Technologies, inc. Proprietary

Large Scale PKI - Referral

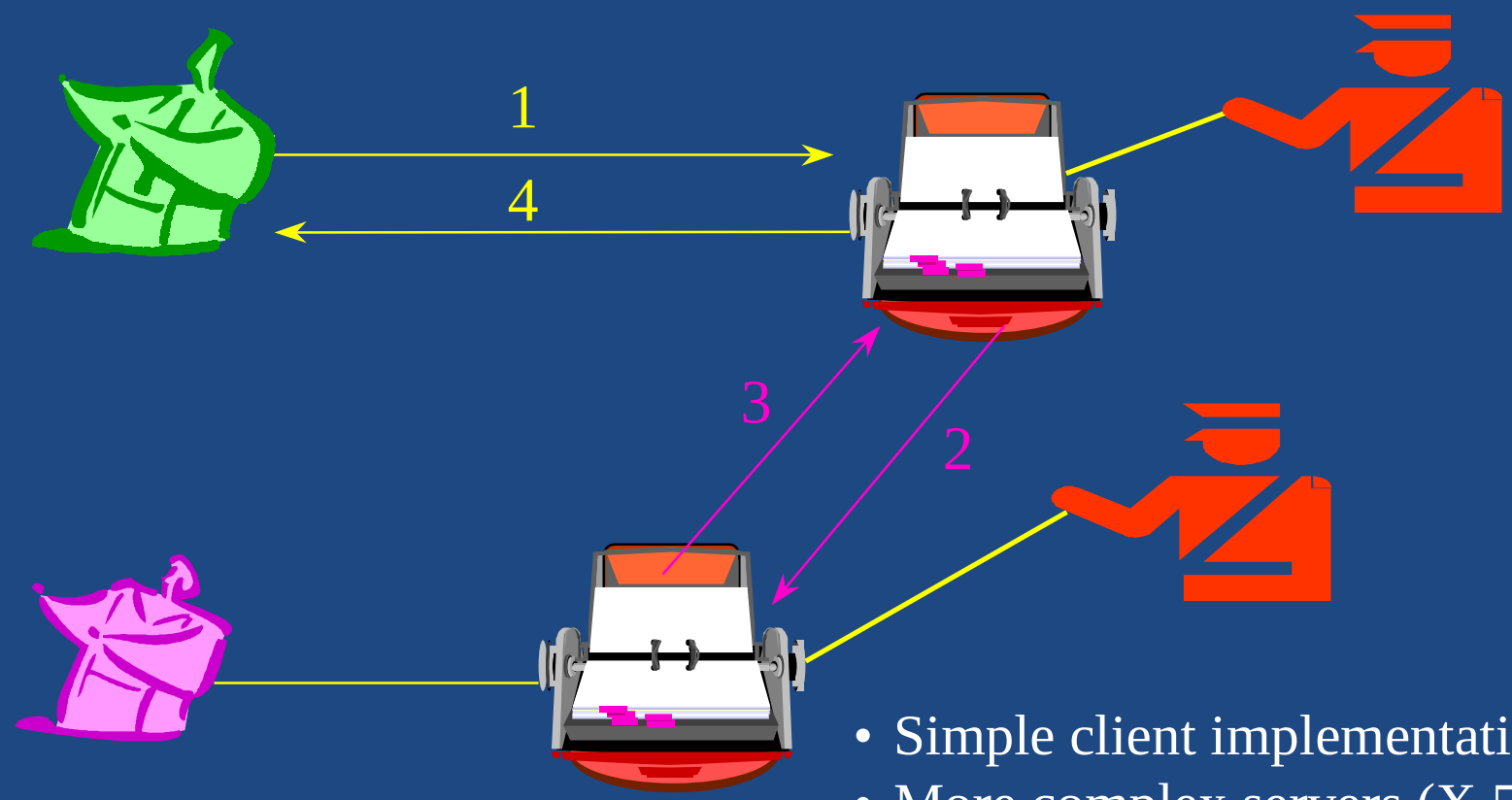


- Simple server implementation
- More complex clients
- No user transparency
- Limited scalability without knowledge management

——— LDAP

©1998 Entrust Technologies, inc. Proprietary

Large Scale PKI - Chaining



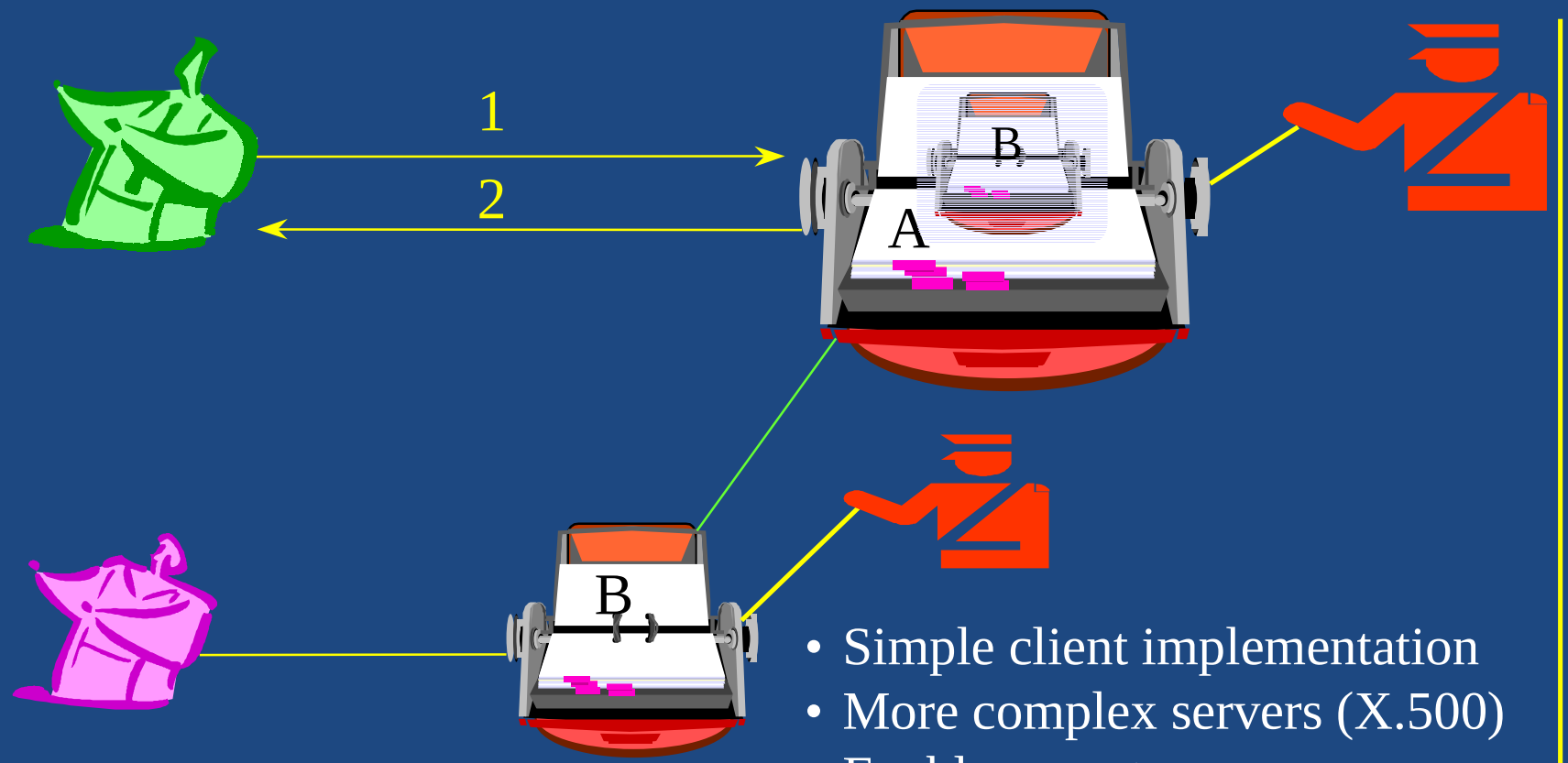
- Simple client implementation
- More complex servers (X.500)
- Enables user transparency
- Unlimited scalability with good knowledge management

LDAP

DSP

©1998 Entrust Technologies, inc. Proprietary

Large Scale PKI - Replication

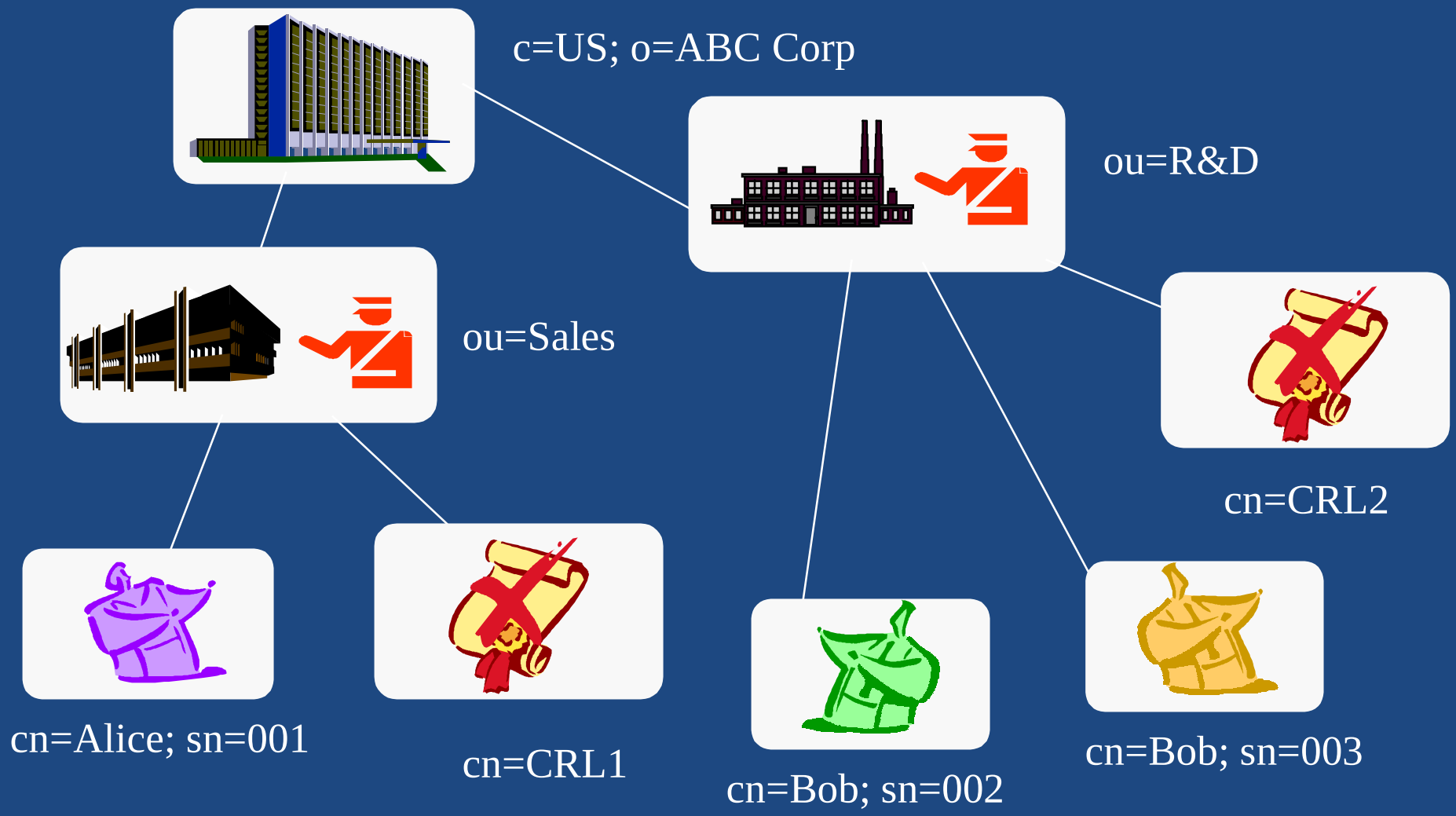


- Simple client implementation
- More complex servers (X.500)
- Enables user transparency
- Reduces latency on operations
- Unlimited scalability with knowledge management

LDAP
DISP

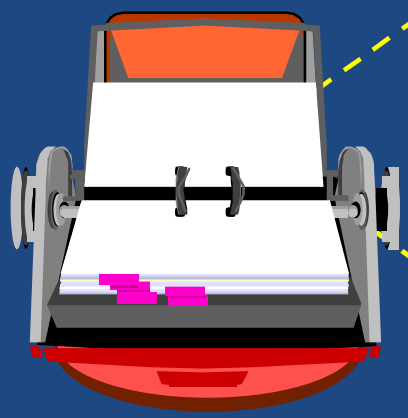
©1998 Entrust Technologies, inc. Proprietary

Sample DIT Structure



©1998 Entrust Technologies, inc. Proprietary

CA Entry - Sample Structure

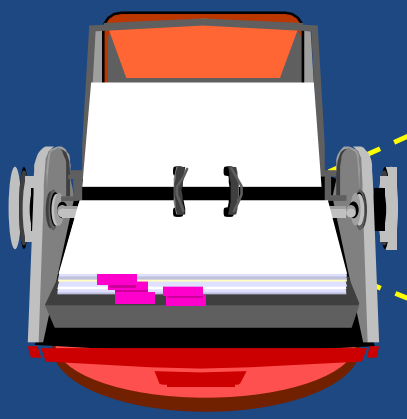


c=US;
o=ABC Corp;
ou=Sales

- **PKI CA**
  - CA certificate
  - **cross-certificate pair**
- **Organization**
  - organization name
  - postal address
  - telephone number
  - description
  - etc.

©1998 Entrust Technologies, inc. Proprietary

CRL Distribution Point Entry - Sample Structure

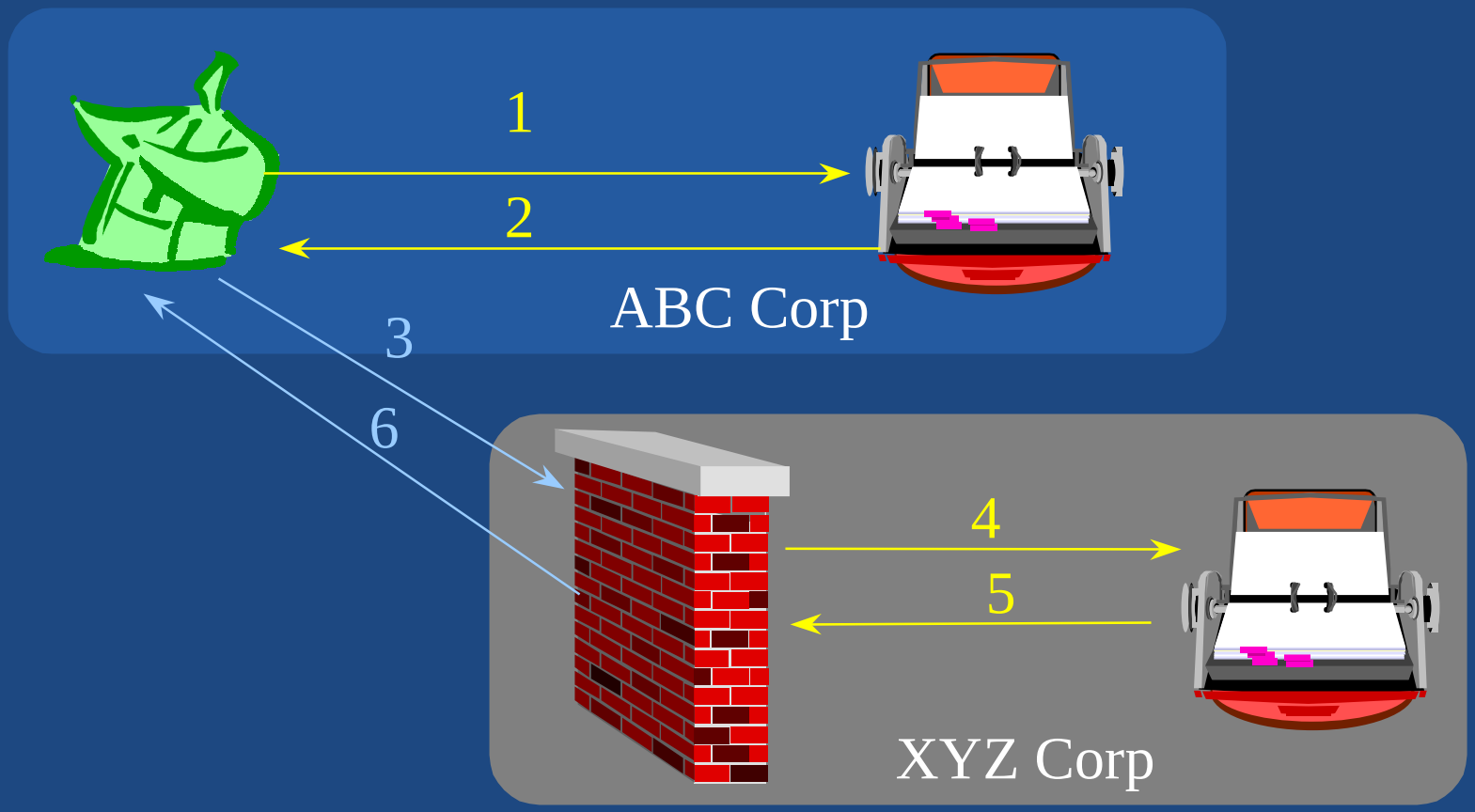


c=us;
o=ABC Corp;
ou=Sales;
cn=CRL1

- **CRL Distribution Point**
  - common name
  - CRL
  - **ARL**

©1998 Entrust Technologies, inc. Proprietary

Inter-enterprise PKI - HTTP



LDAP

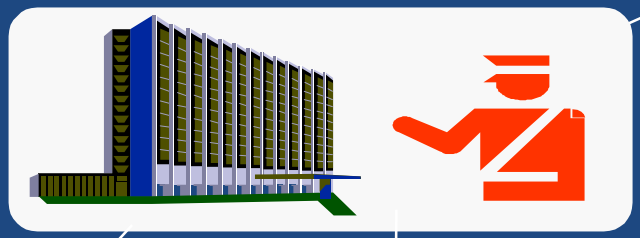
HTTP

- LDAP referral to HTTP URL for firewall proxy
- Proxy/user - HTTP : Proxy/directory - LDAP
- No direct external repository access

©1998 Entrust Technologies, inc. Proprietary

Sample DIT Structure

c=US



o=ABC Corp

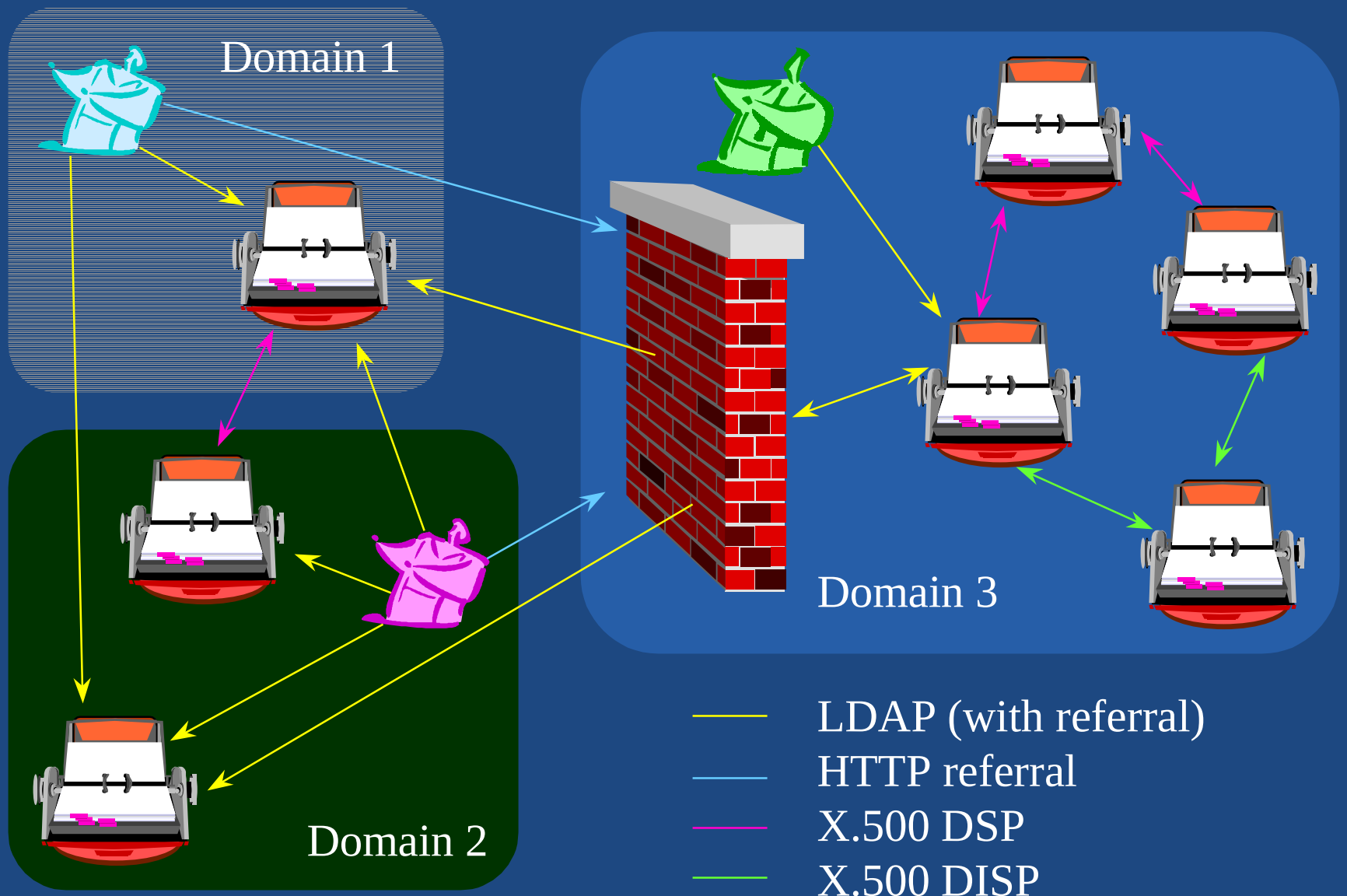
cn=Alice; sn=001

cn=CRL1

o=XYZ Corp
- referral only
- contains http url
  to XYZ firewall proxy

©1998 Entrust Technologies, inc. Proprietary

Interoperability Example



©1998 Entrust Technologies, inc. Proprietary

Summary

- X.500
  - Currently satisfies all PKI repository requirements
  - Vendor support less widespread than for LDAP
- LDAP
  - ***The*** directory access protocol of choice
  - Some key features yet to be defined
- Together
  - Can currently provide PKI repositories which are:

SCALABLE, INTEROPERABLE &

STANDARDS-BASED

©1998 Entrust Technologies, inc. Proprietary