IBM Systems and Technology Group

Vanguard Security Solutions & RACF User Training
Session RTB 15
June, 2008

Introduction to Identification and Authentication Mechanisms

Rich Guski CISSP
IBM Senior Technical Staff Member
zSeries Software Security Architecture

Abstract

The concepts of Identification and Authentication as well as the related concept known as identity context form an important cornerstone of any modern computing resource security environment. If you are new to the computer security discipline, and you would like to learn some fundamentals about these concepts and their place "in the larger scheme of things", this is a presentation you should plan to attend.

Trademarks

See url http://www.ibm.com/legal/copytrade.shtml for a list of IBM trademarks

The following are trademarks or registered trademarks of other companies.

Intel is a registered trademark of the Intel Corporation in the United States, other countries or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC

BSAFE

Identrus

IdenTrust

Vanguard Products

Other company, product, and service names may be trademarks or service marks of others.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

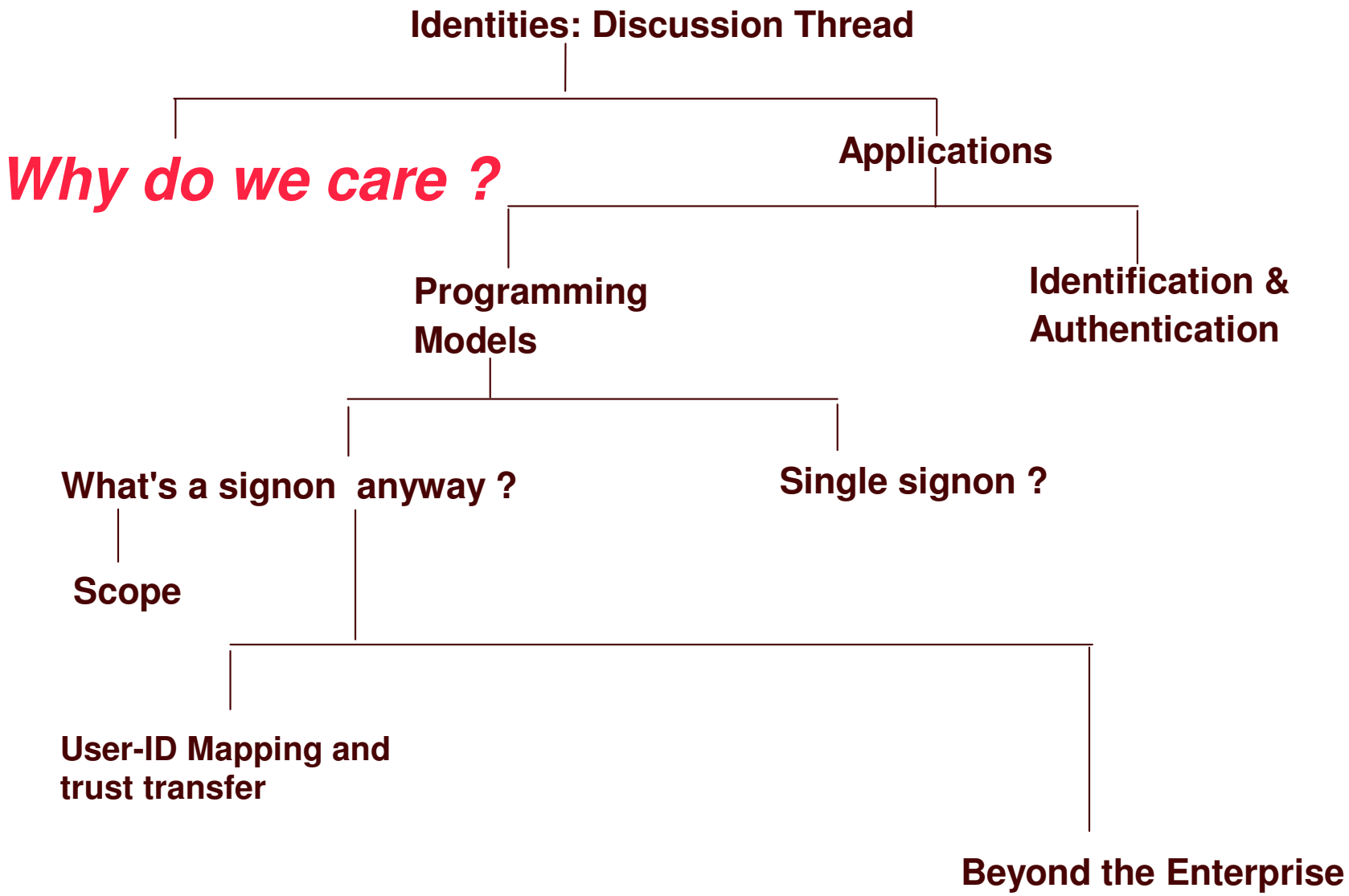
Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.



Identities: why do we care ?

We didn't always care about identities

Started to care when computer applications began to be used by multiple users

- Applications needed to differentiate one user from another, examples:
  - maintain logs of who did what (e.g. who wrote over maclib)
  - separate regular user from administrative user
  - associate different users with different sets of attributes
  - establish sets (groups) of users with common attributes
  - etc..
- Later, the need was recognized to allow certain users to access certain resources, while disallowing others; the birth of *access control*

Access Control (who has access to what ?)

Who = Identity, expressed in a way that is meaningful (locally and-or globally) and authenticated

Access = Created, updated, read, executed, copied, deleted, etc.

What (examples)

- Application function:
  - ✓ methods, procedures, unusual privilege, limits, restrictions, etc.
- Information:
  - ✓ files
  - ✓ RDMS; views, tables, etc.
  - ✓ name spaces (example: catalog entries)
- Network:
  - ✓ TCPIP resources
    - IP addresses, admin functions, servers, etc.
- Platform functions and resources:
  - ✓ Console commands, administration, accounting, logging, auditing, etc.
  - ✓ Executables
    - programs, procedures, methods, transactions, applications, etc.
  - ✓ Hardware functions (example: Crypto)

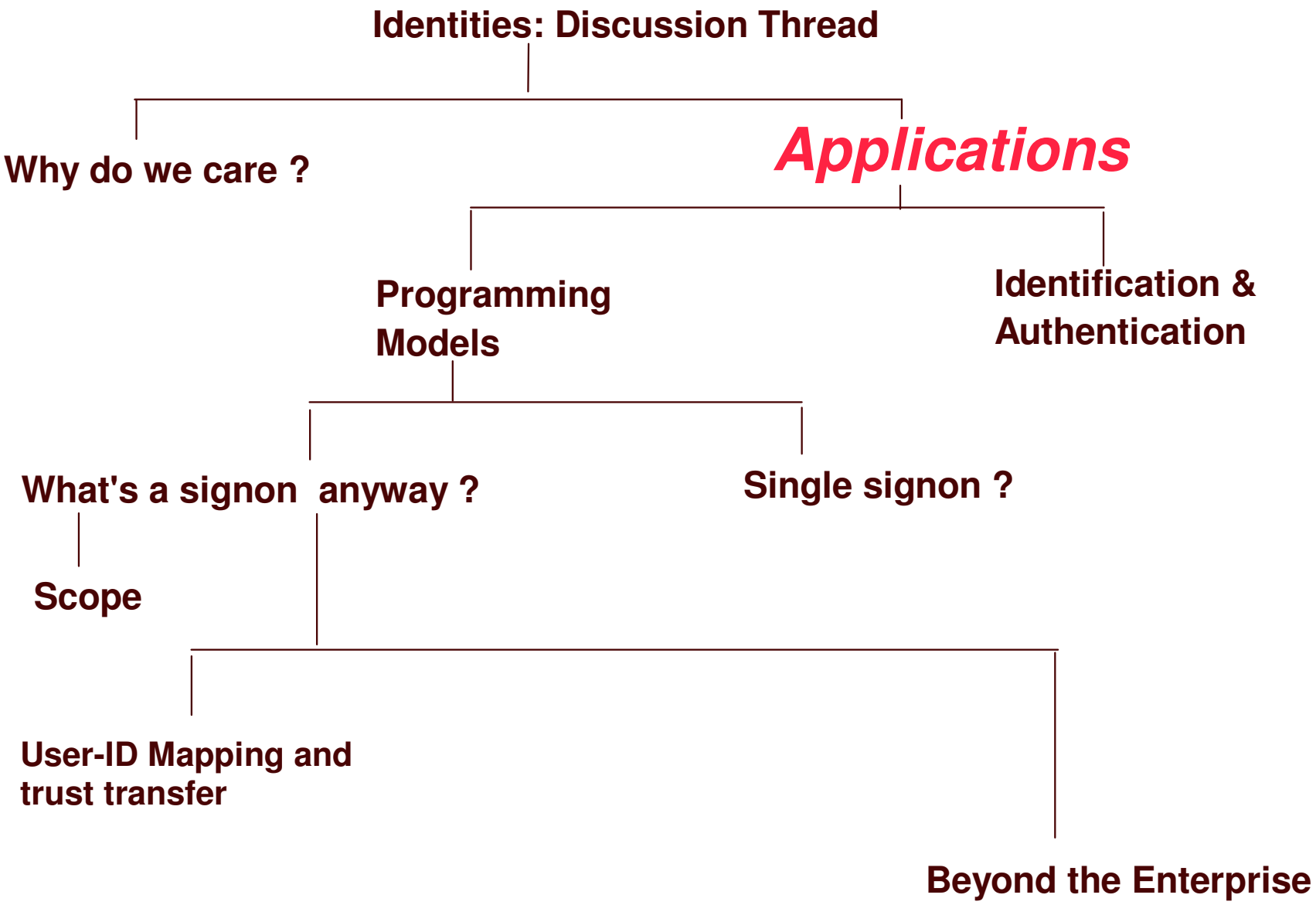
Auditing (who accessed what, when and how ?)

Who = Identity, expressed in a way that is meaningful (locally and-or globally) and authenticated

Access = Created, updated, read, executed, copied, deleted, etc.

What (examples)

- Application function:
  - ✓ methods, procedures, unusual privilege, limits, restrictions, etc.
- Information:
  - ✓ files
  - ✓ RDMS; views, tables, etc.
  - ✓ name spaces (example: catalog entries)
- Network:
  - ✓ TCPIP resources
    - IP addresses, admin functions, servers, etc.
- Platform functions and resources:
  - ✓ Console commands, administration, accounting, logging, auditing, etc.
  - ✓ Executables
    - programs, procedures, methods, transactions, applications, etc.
  - ✓ Hardware functions (example: Crypto)



Applications

Identities are used by "applications"...

Platform components (platform inclusive "applications"):

- Contents Supervision
- z/OS data management (DFSMS)
- TSO
- JES
- Communications Server
- etc.

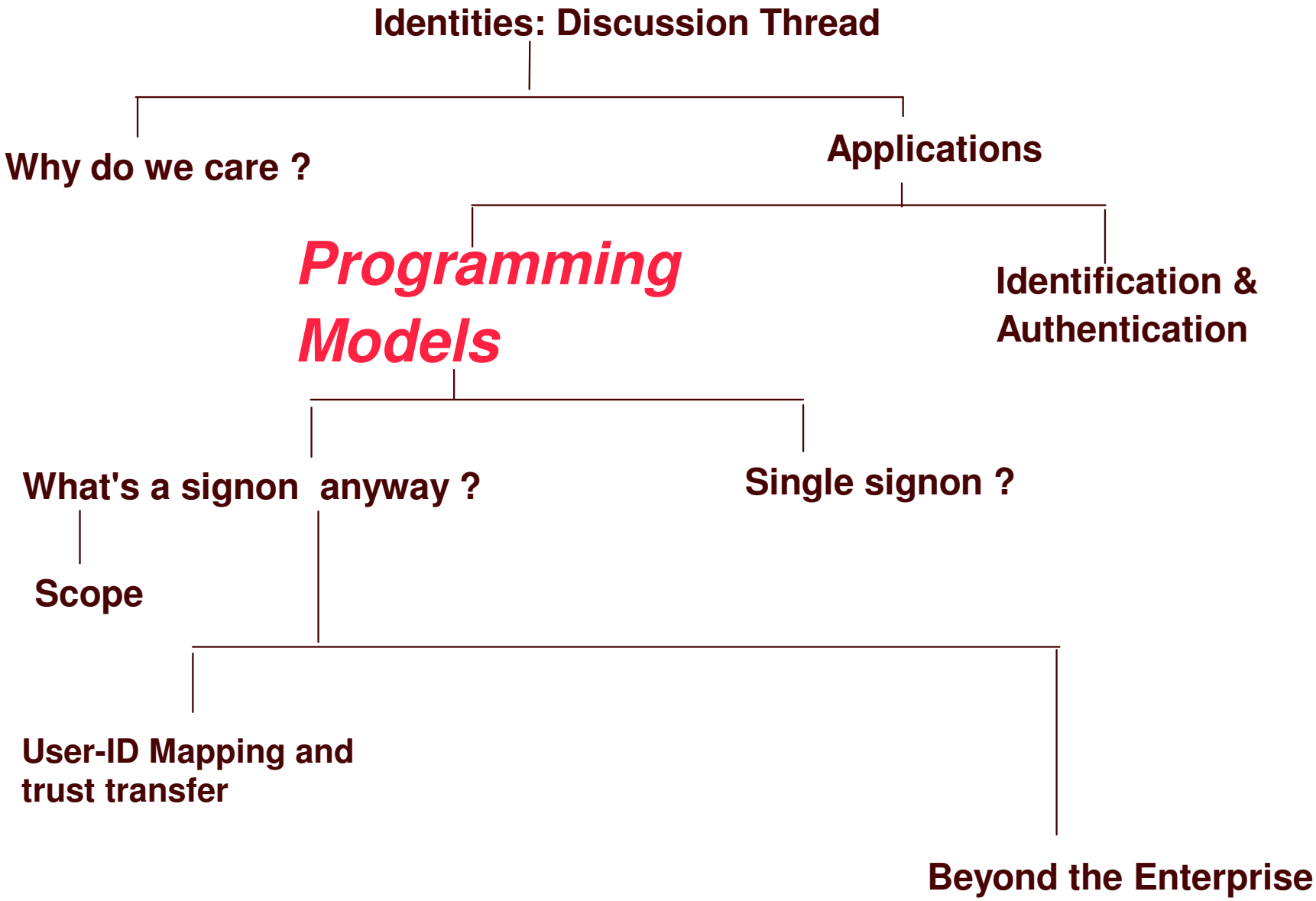
"Hosting environments" that run on a platform:

- CICS
- IMS
- SAP
- WebSphere Application Server (WAS)
- etc.

Other applications:

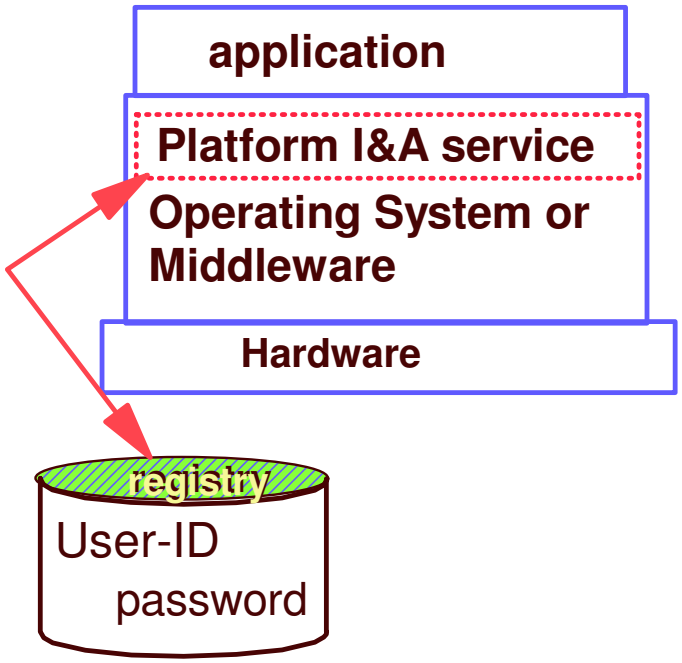
- DB2
- HTTP Server

Any-all applications that are authorized via security administration services to perfom identity manipulation must be considered security sensitive

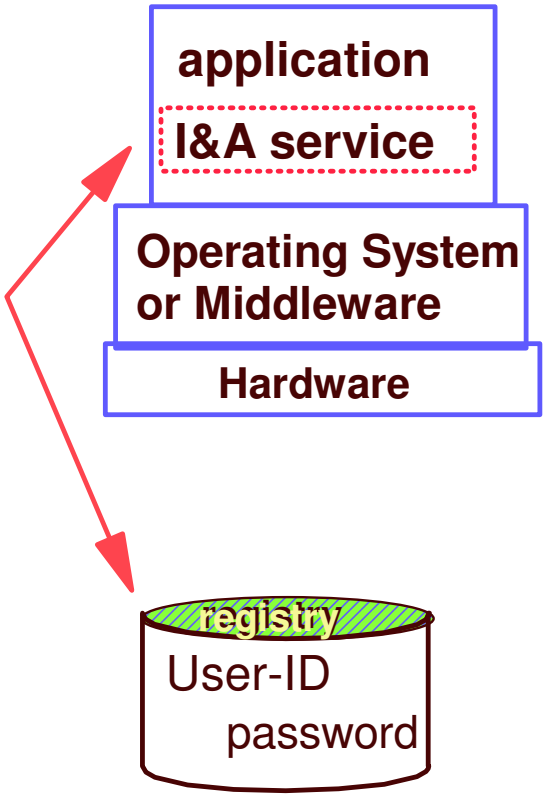


Typical I&A programming models

I&A = User Identification and Authentication

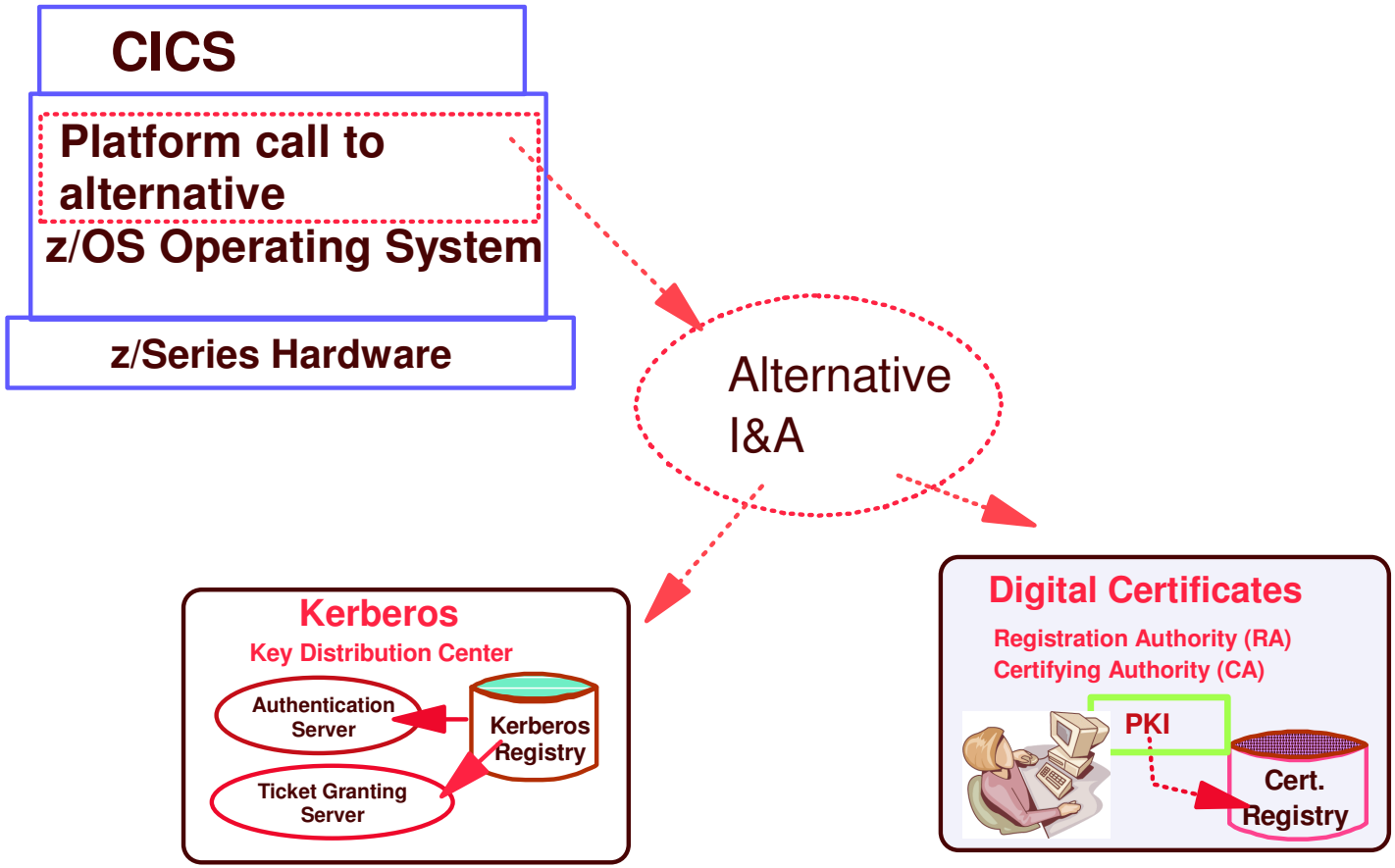


Might use platform I&A,

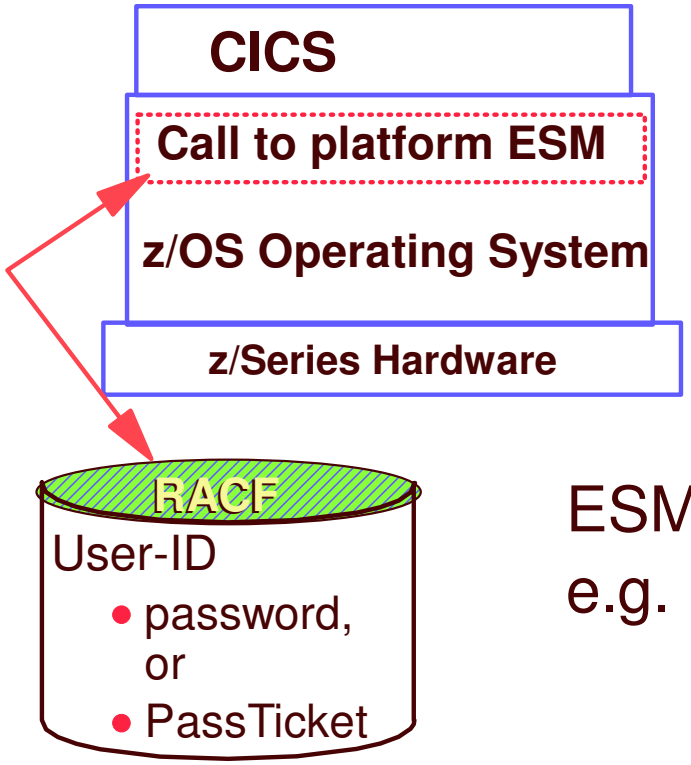


or, it's own I&A

Example: use of alternative I&A function or service

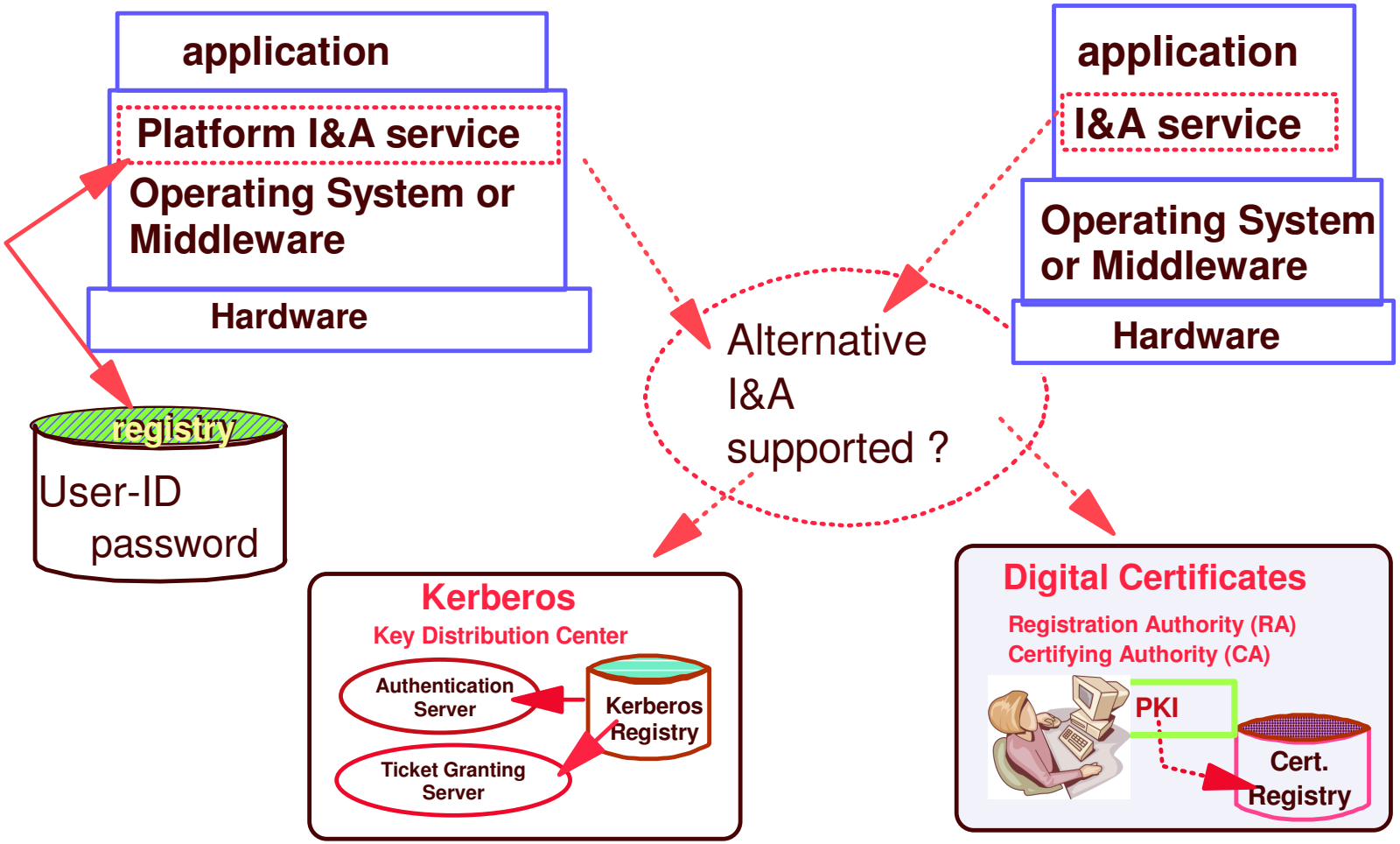


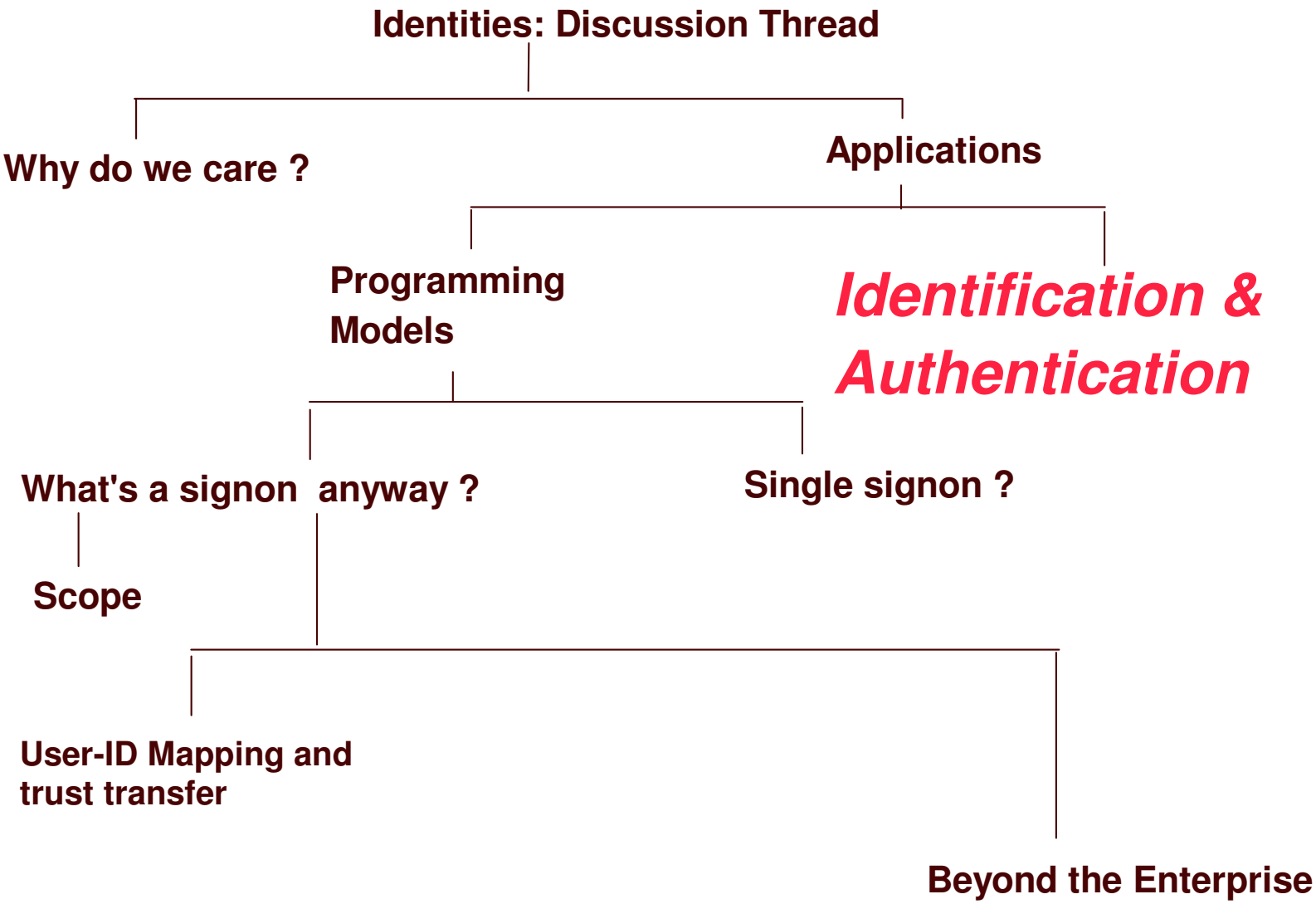
Example: use of platform service



ESM = external security manager
e.g. RACF

Summary of I&A programming models

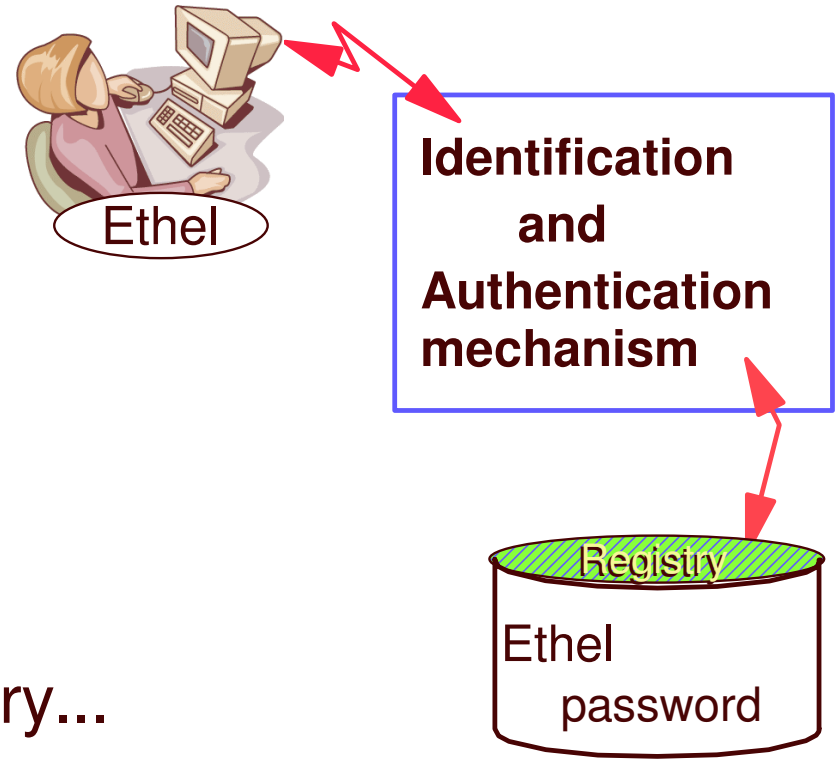




User Identification and Authentication

User asserts who he/she is, and proves it

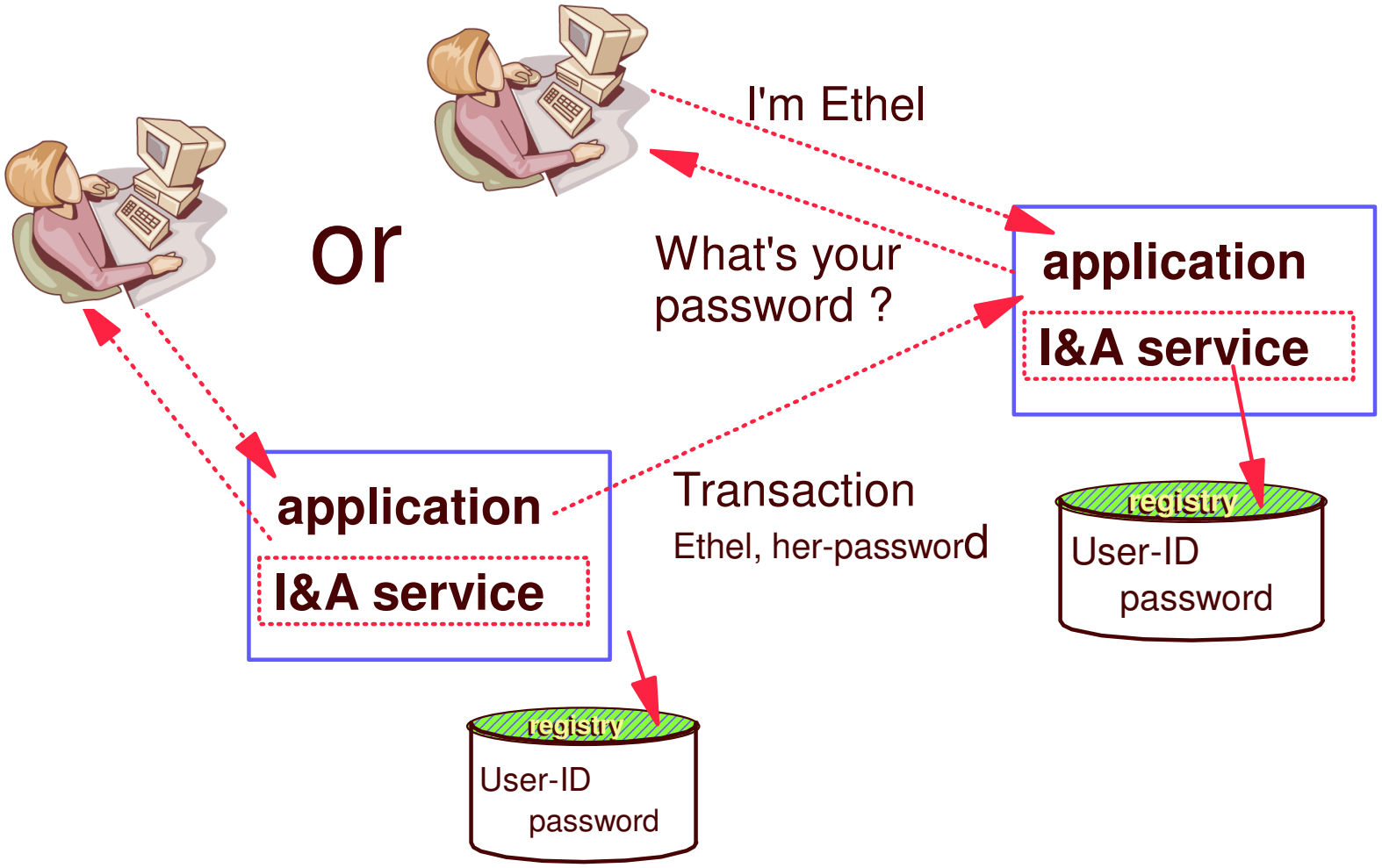
- Popular technologies include:
  - ✓ Digital Certificates & PKI
    - Lotus Notes
    - RACF option
  - ✓ Kerberos
    - RACF option
  - ✓ UserIDs and passwords
    - RACF
    - LDAP Bind
    - UNIX-Linux signon
    - many others...



Authentication processes vary...

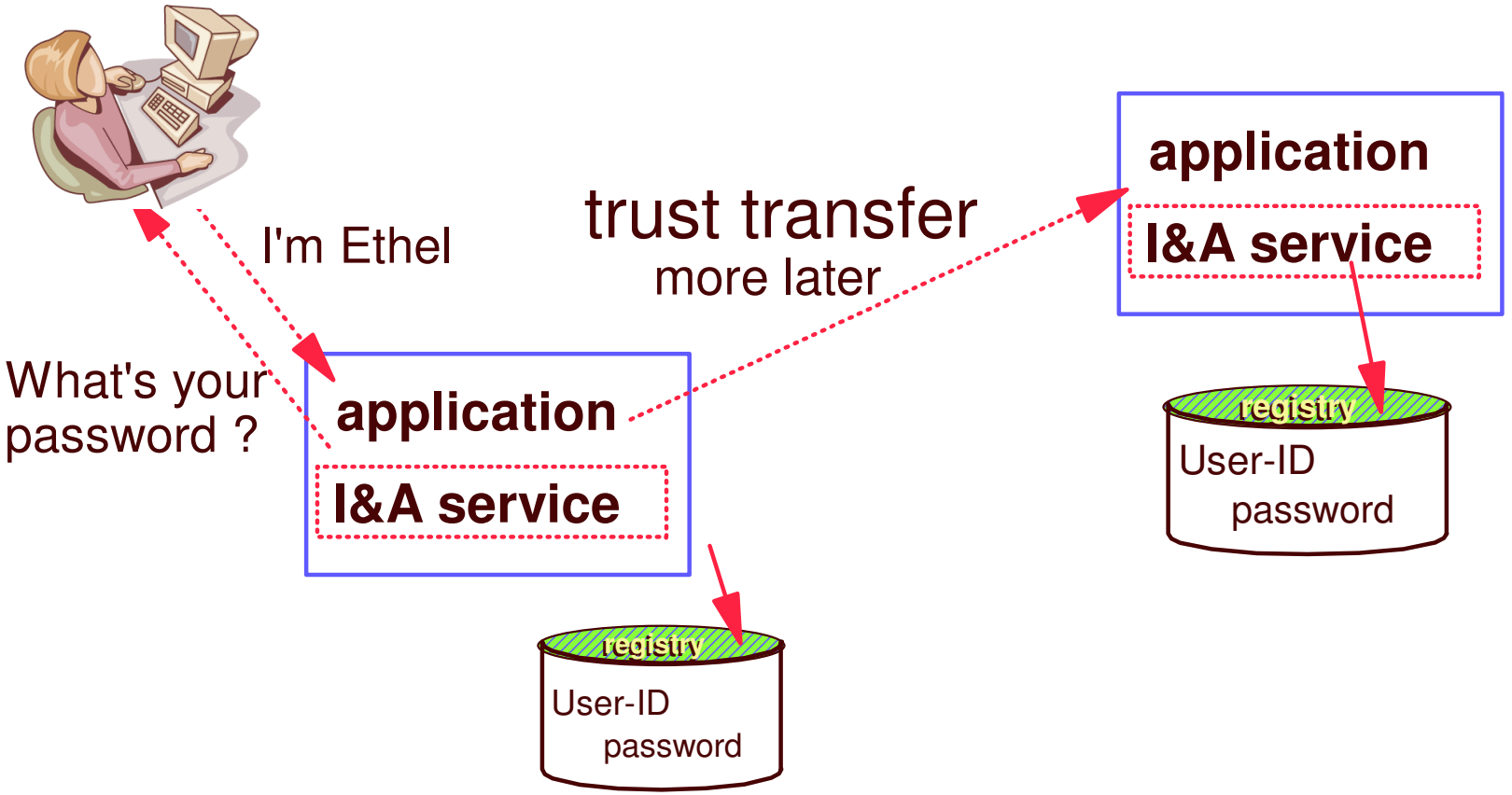
Userid - Password

(e.g. RACF, LDAP Bind, etc.)

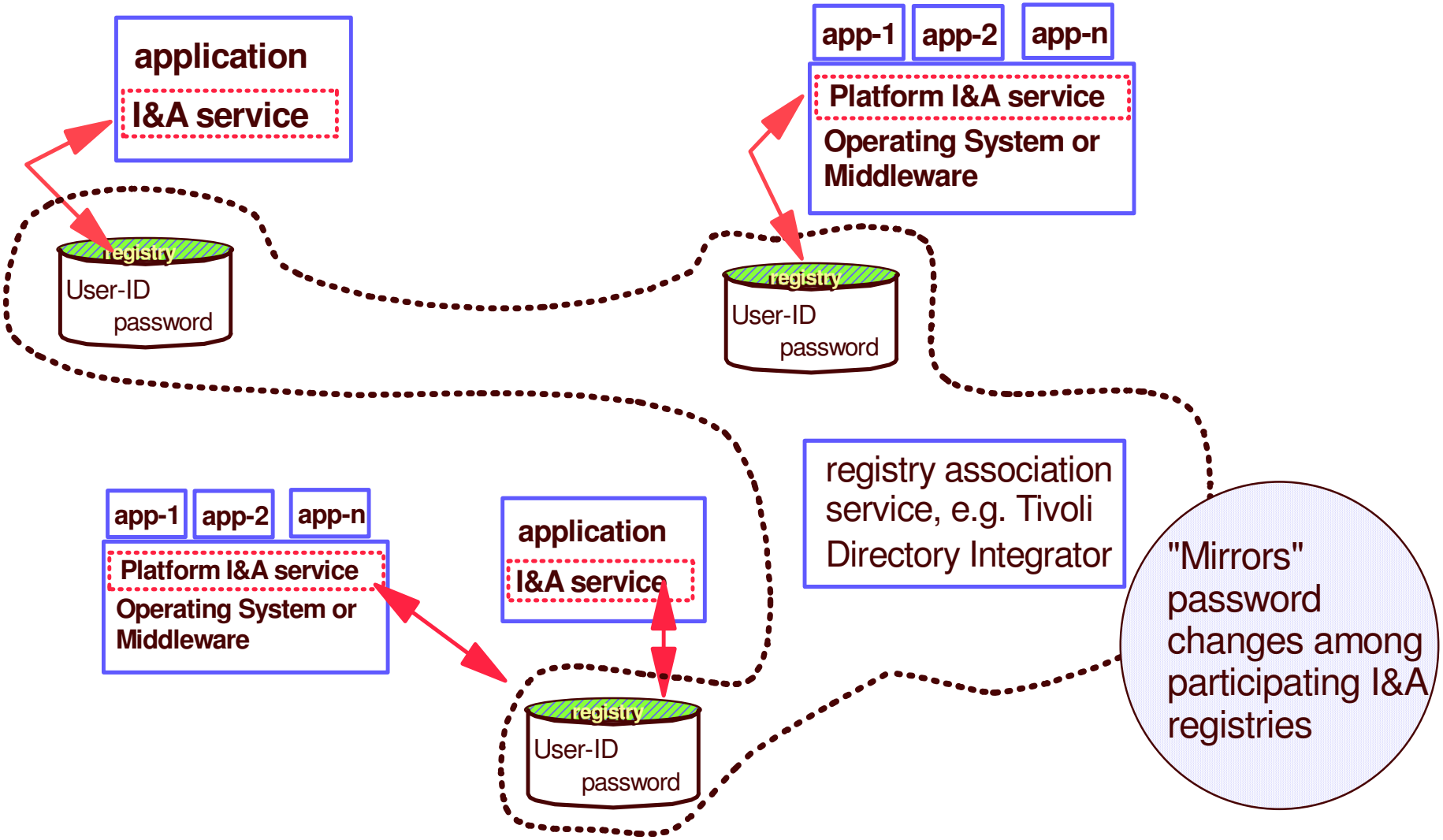


Userid - Password

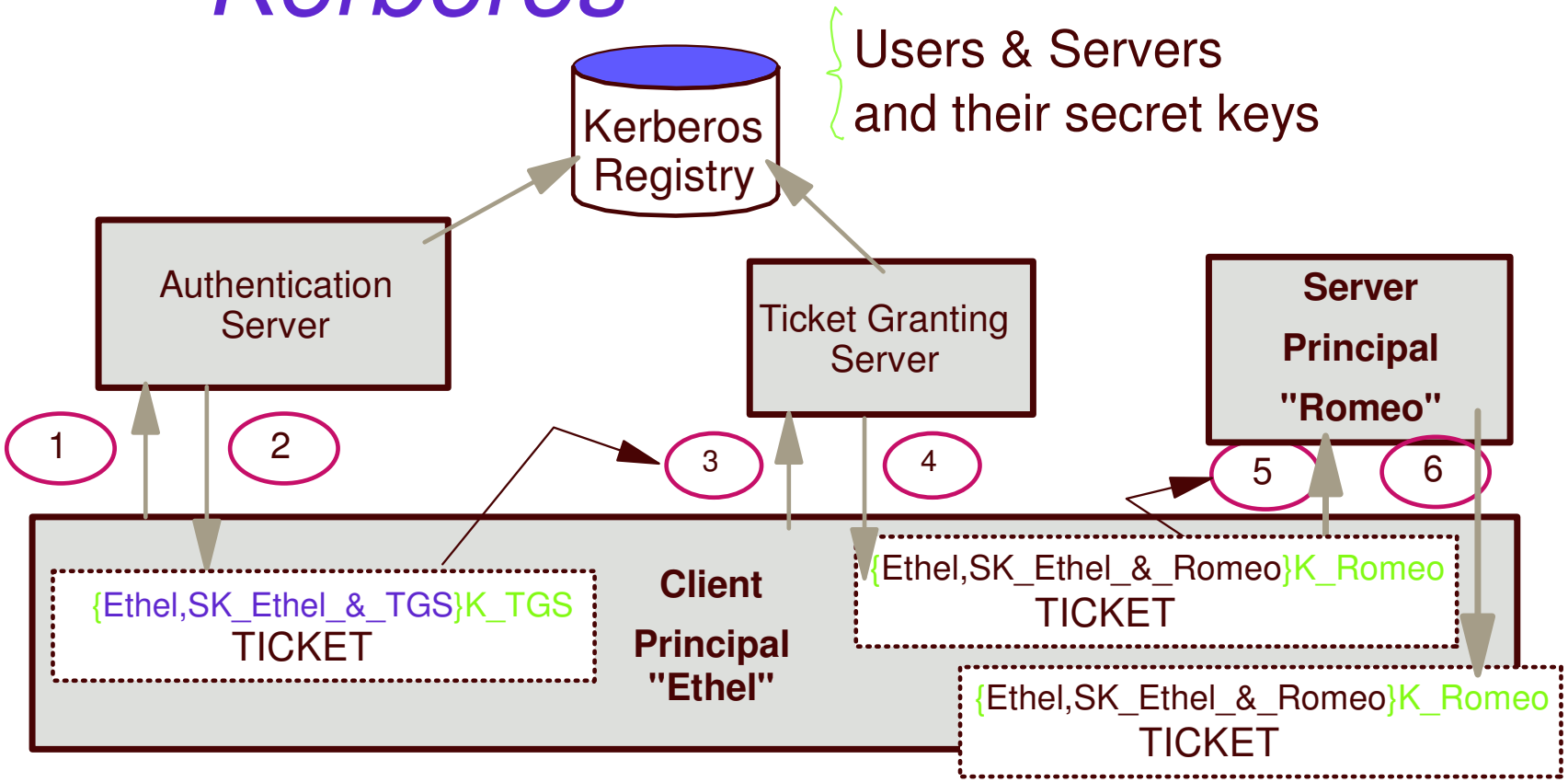
(e.g. RACF, LDAP Bind, etc.)



Password "synchronization"



Kerberos



1. Ethel's request for authentication to Kerberos Authentication Server
2. {Ticket-Ethel-to-TGS,SK_ Ethel & TGS}K_Ethel
3. {Ethel authenticator}SK_Ethel_&_TGS,Ticket-Ethel-to-TGS
4. {Ticket-Ethel-to-Romeo,SK-Ethel & Romeo}SK_Ethel_&_TGS
5. {Ethel authenticator}SK-Ethel & Romeo,Ticket-Ethel-to-Romeo
6. {Server response to client}SK_Ethel_&_Romeo

Note:
Nonces and Time-stamps not shown for clarity.

Digital Certificates...

Certifying Authority (CA)

Ethel's Digital Certificate looks something like this.

Ethel's name +

Ethel's public-key +

Standards:
CCITT X.509 + PKCS + PEM

Name of CA, e.g., Verisign | Expiration date | Serial number +

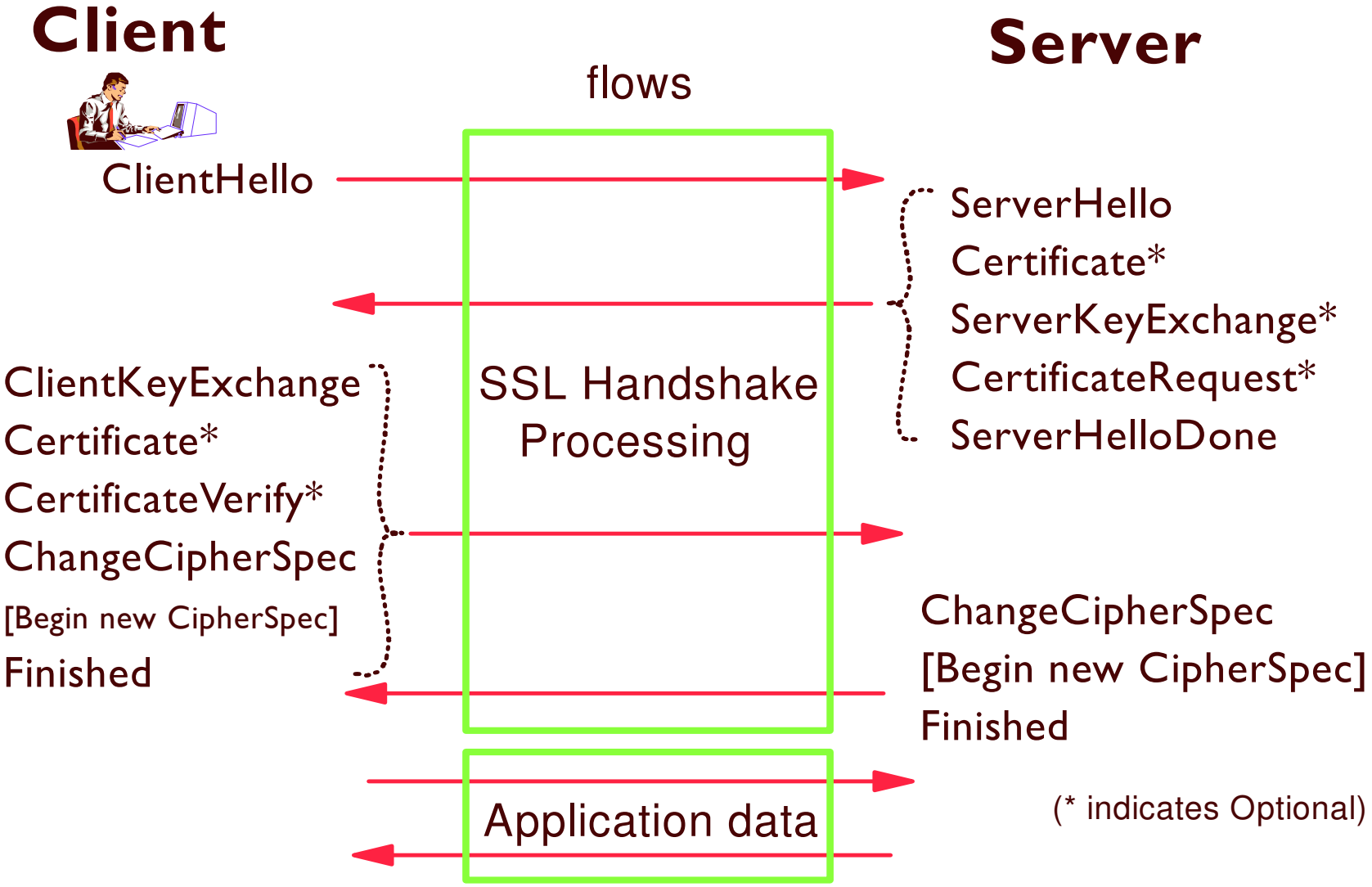
MD5 hash of above, encrypted with private-key of CA

Added by CA

(Signature of CA)

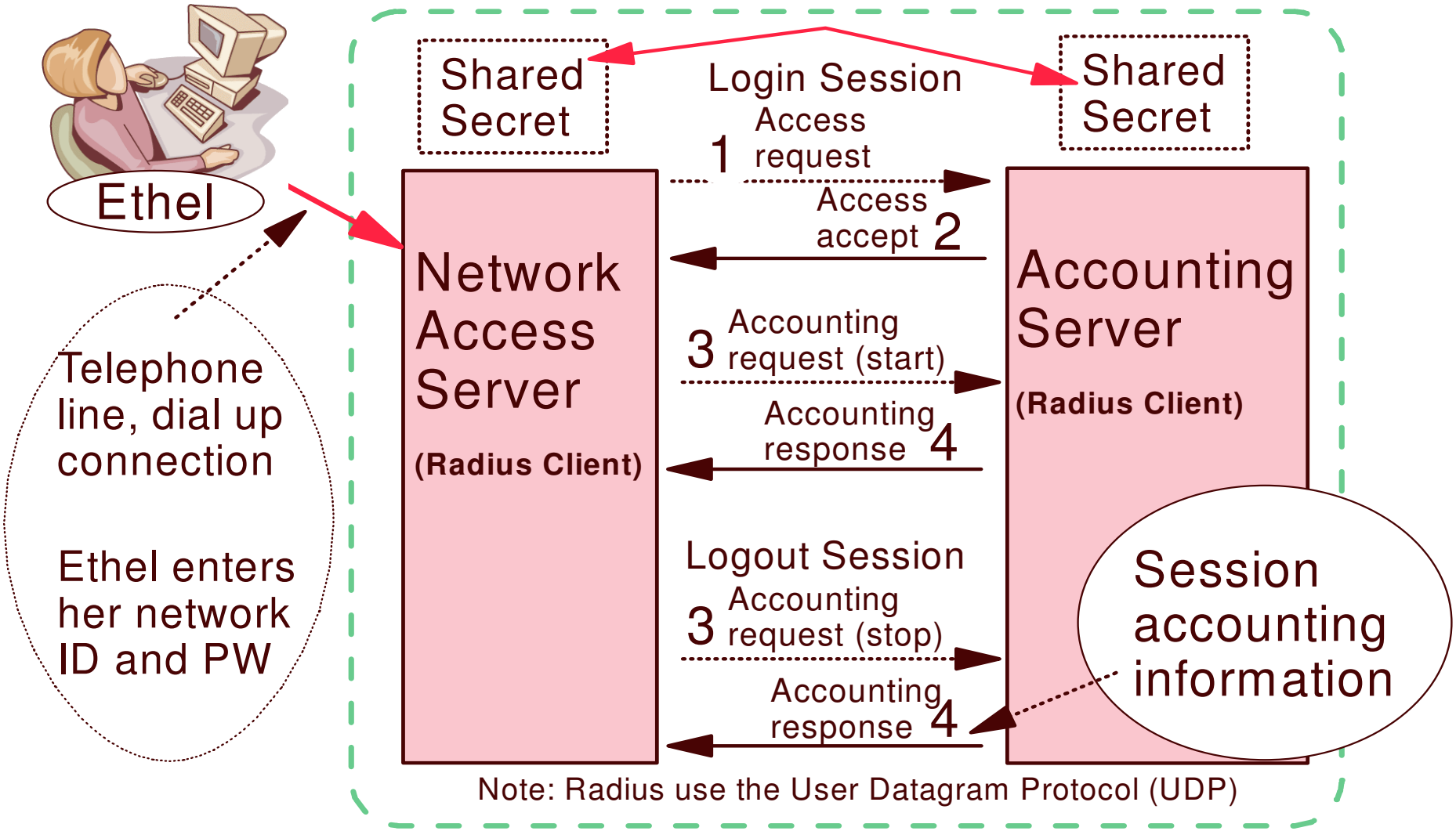
Certificate is not encrypted, merely 'signed' by the CA

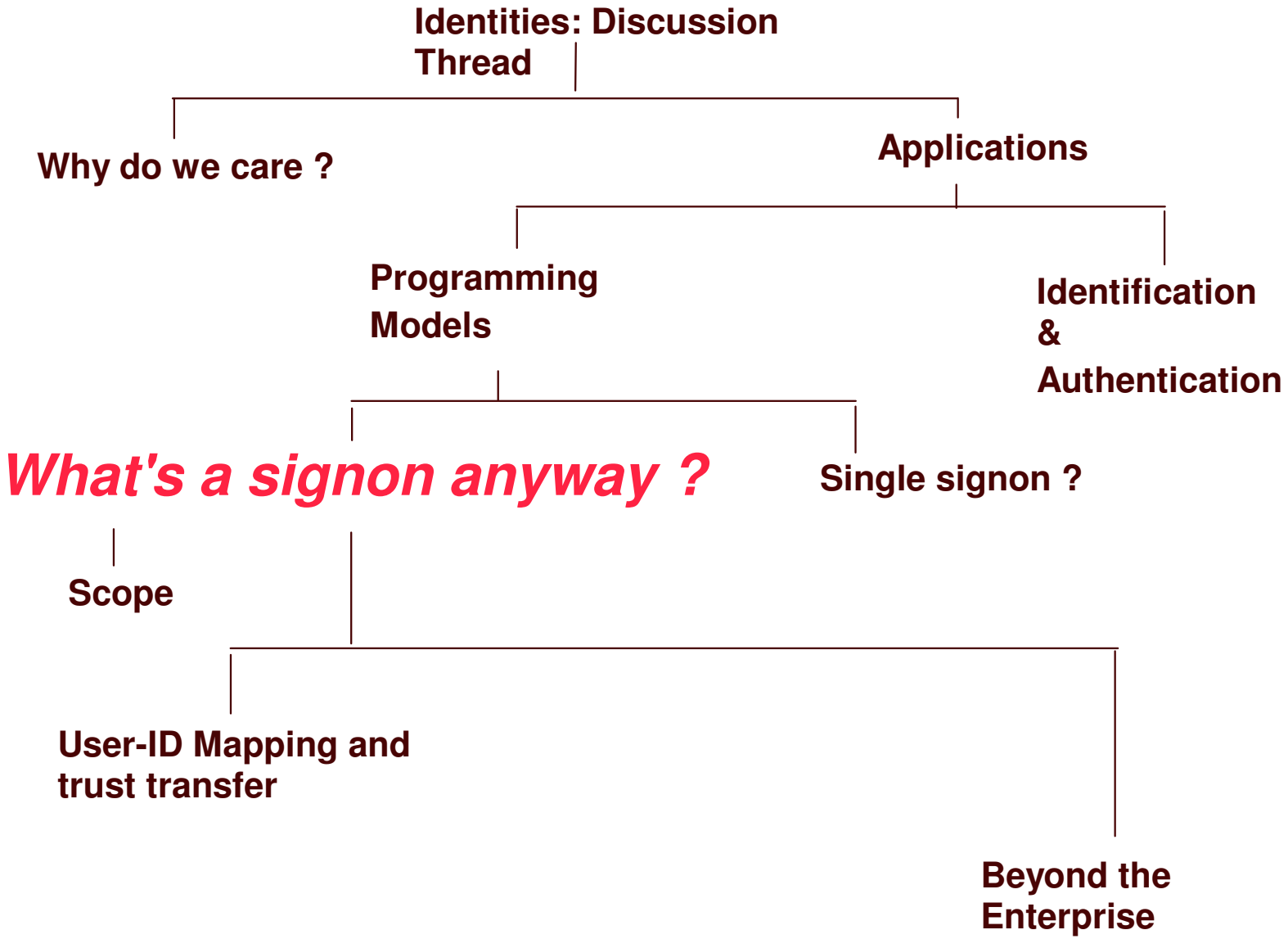
Digital Certificate use example: SSL



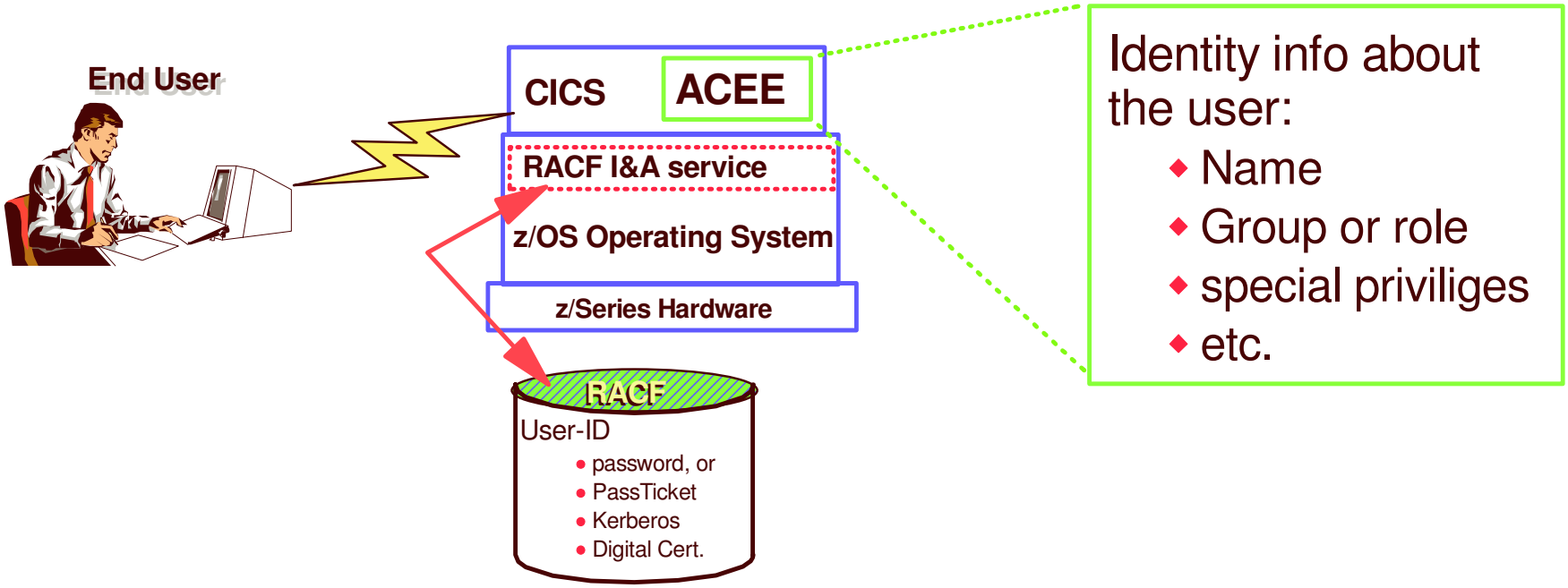
RADIUS Protocol

(Remote Authentication Dial-In User Service)

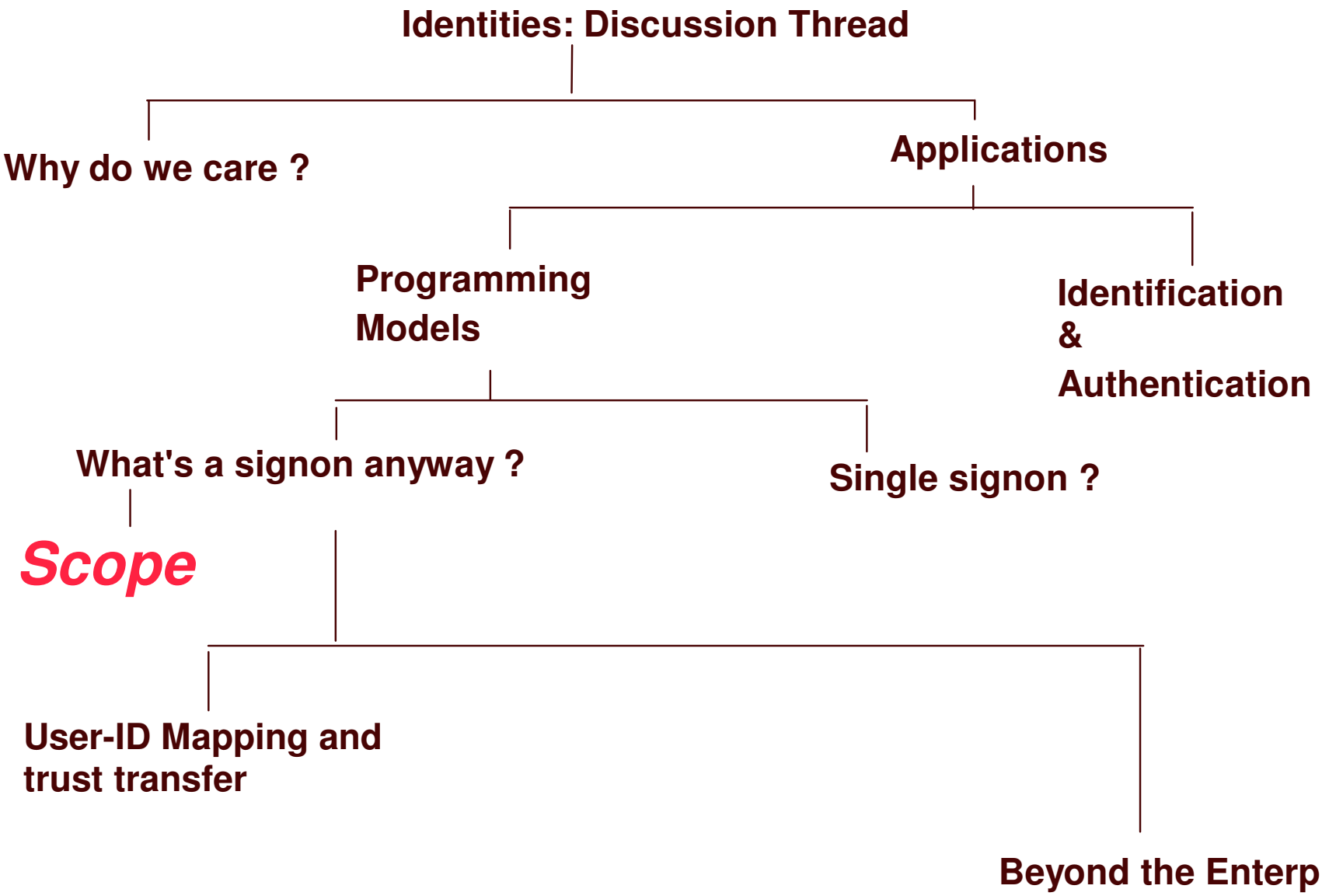




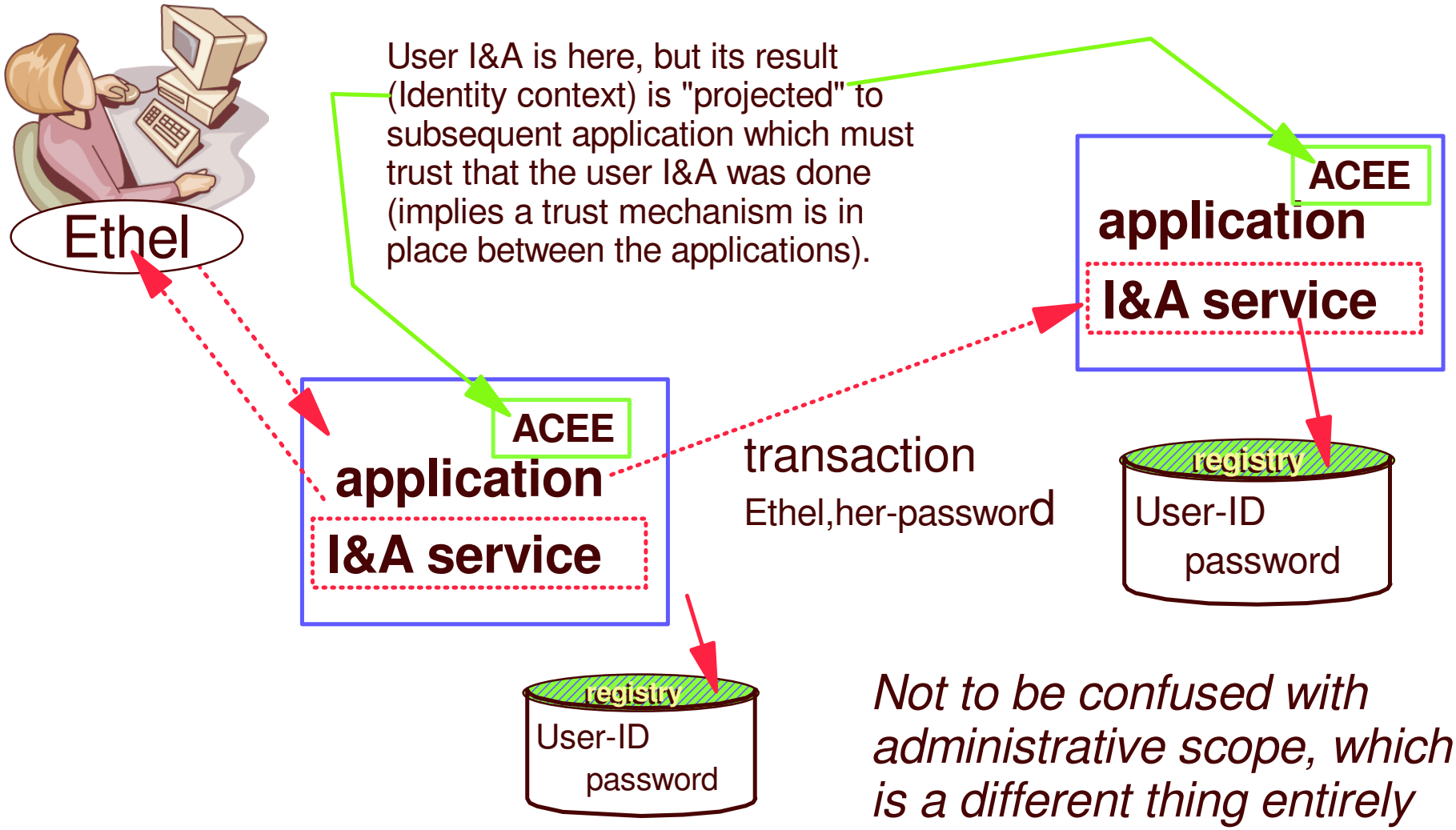
Result of a successful signon ?



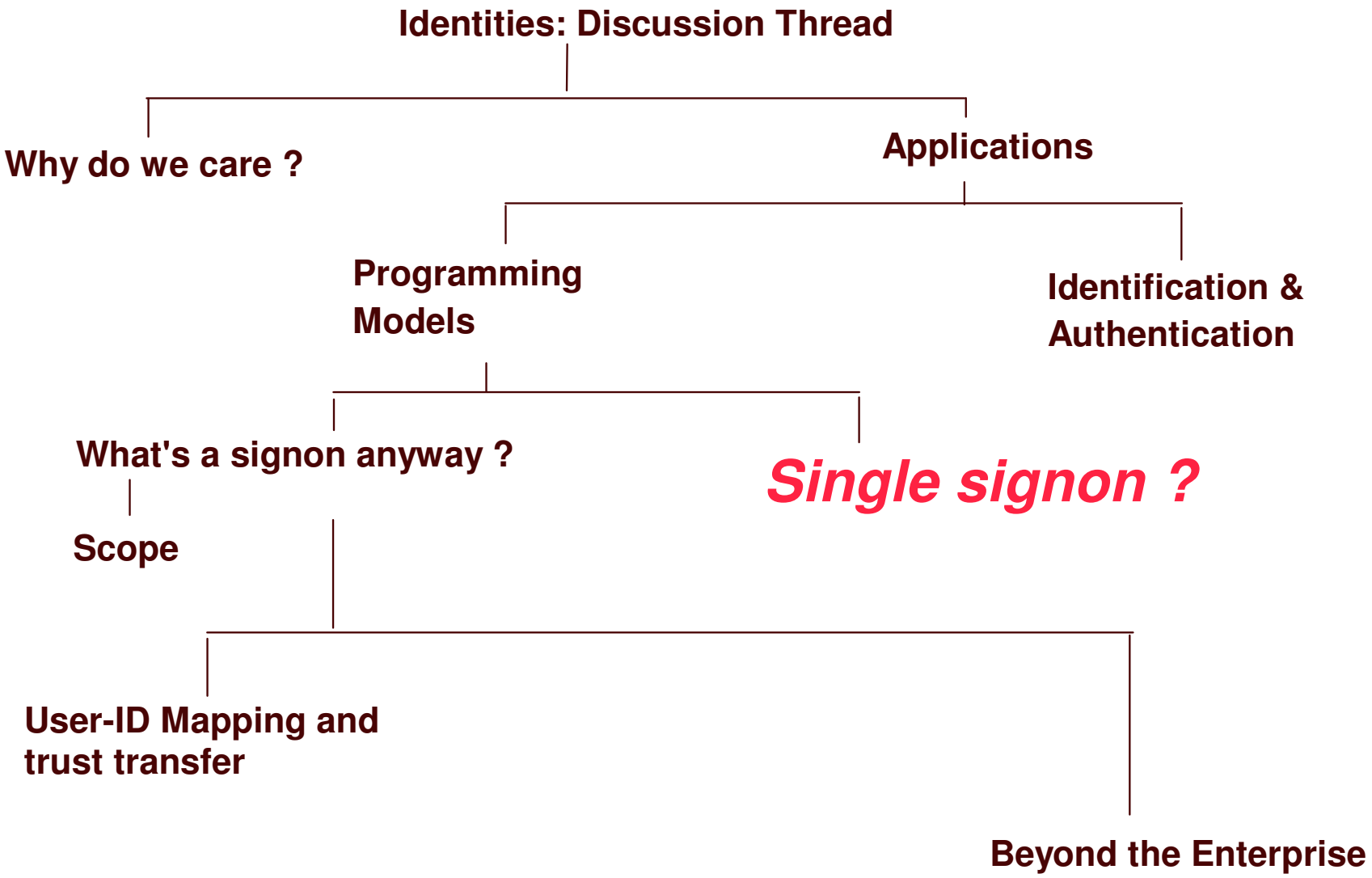
An "identity context" is constructed (either by the app or the I&A service) and maintained by the application during run-time, example: RACF Accessor Control Environment Element (ACEE). It is meaningful ONLY within the context of this application and other run-time security services that will consume it.



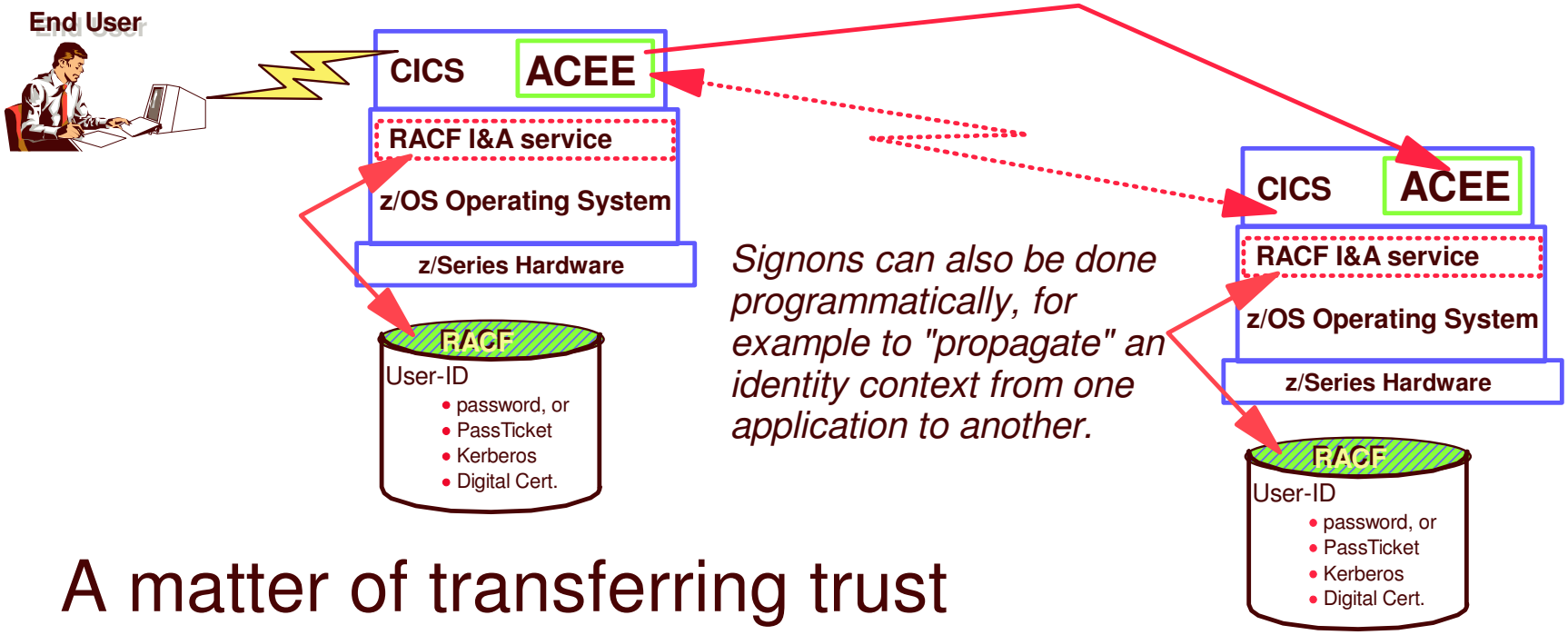
User I&A Scope



Not to be confused with administrative scope, which is a different thing entirely



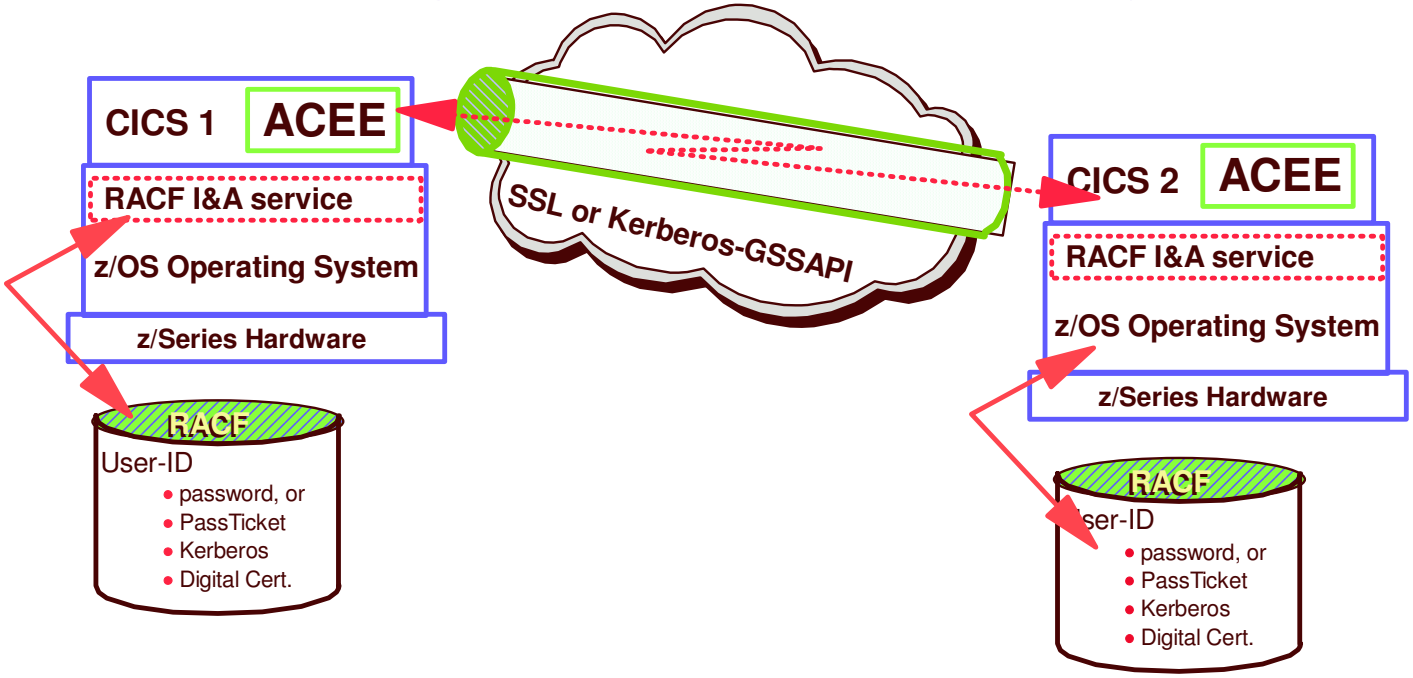
Single Signon explained



A matter of transferring trust

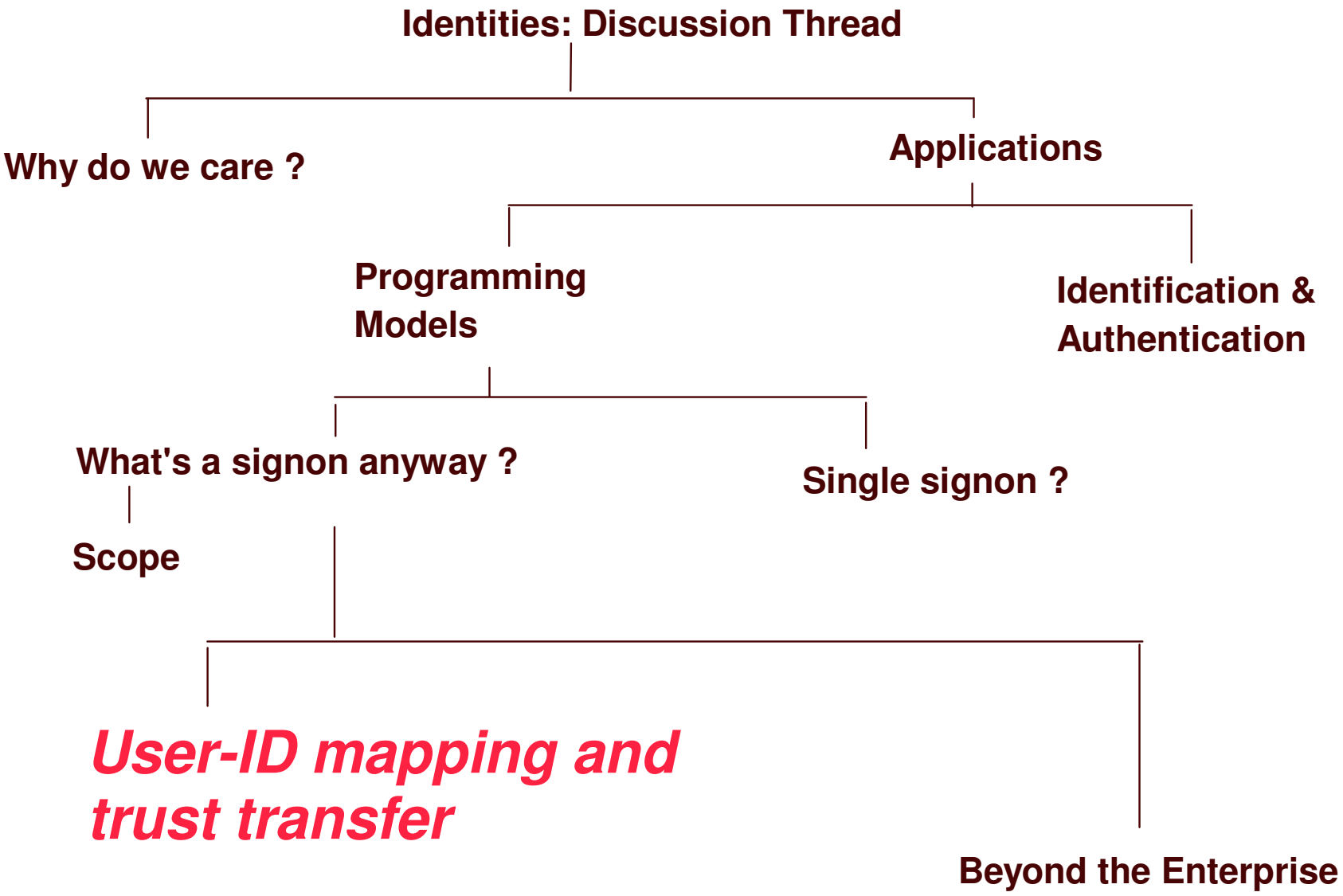
Scenario is, two (or multiple) applications, one of which actually authenticates the user, are required to process the user's request. Second app "trusts" the authenticating app to securely propagate user's identity to the second app without requiring the user to re-authenticate; identity context is created within the second application.

Transferring Trust Securely



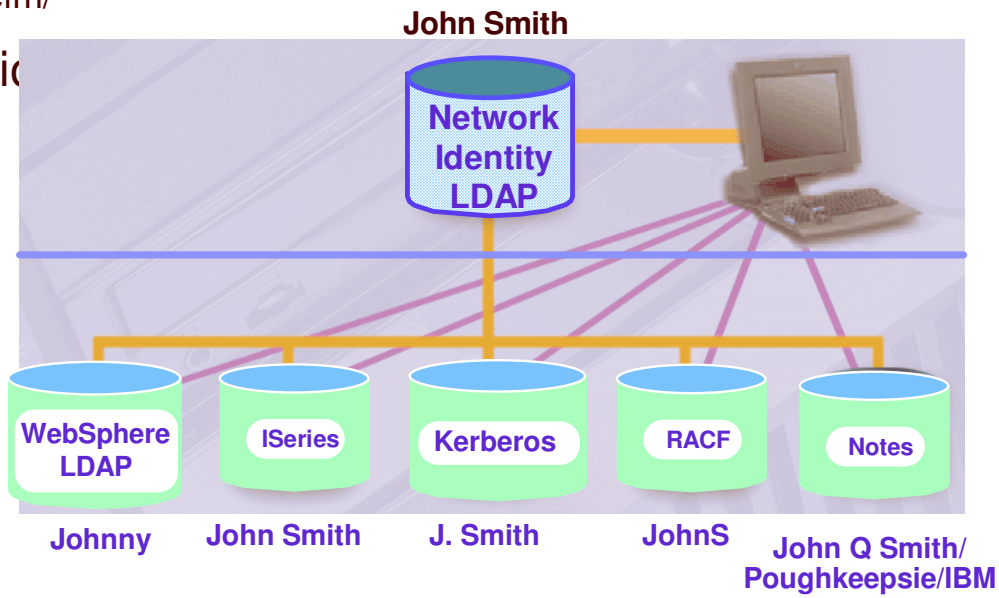
- ✓ Applications, instantiated as "servers", have identities, and must trust each other for identity propagation (single signon) of their ***end-user clients*** to be allowed.
- ✓ Communication path between them must be secure (trustworthy).
- ✓ Second server's I&A service must be capable of accepting user signon requests from another -trusted- server without requiring user re-authentication (password).

But, how do you know that a given user-ID refers to the same person from one registry domain to another, and what if the same person is represented by a different user-ID in another registry domain ?



Enterprise Identity Mapping (EIM) *Available since* ***z/OS V1R4***

- **Help manage the relationship between identities in multiple system and application registries**
- **Enterprise Identity Mapping**
  - EIM is designed to allow interoperation between differing security models
  - For more information,
    see: www.ibm.com/servers/eserver/security/eim/
  - DB2 exploits EIM in DB2 V9 in relati
    suppport

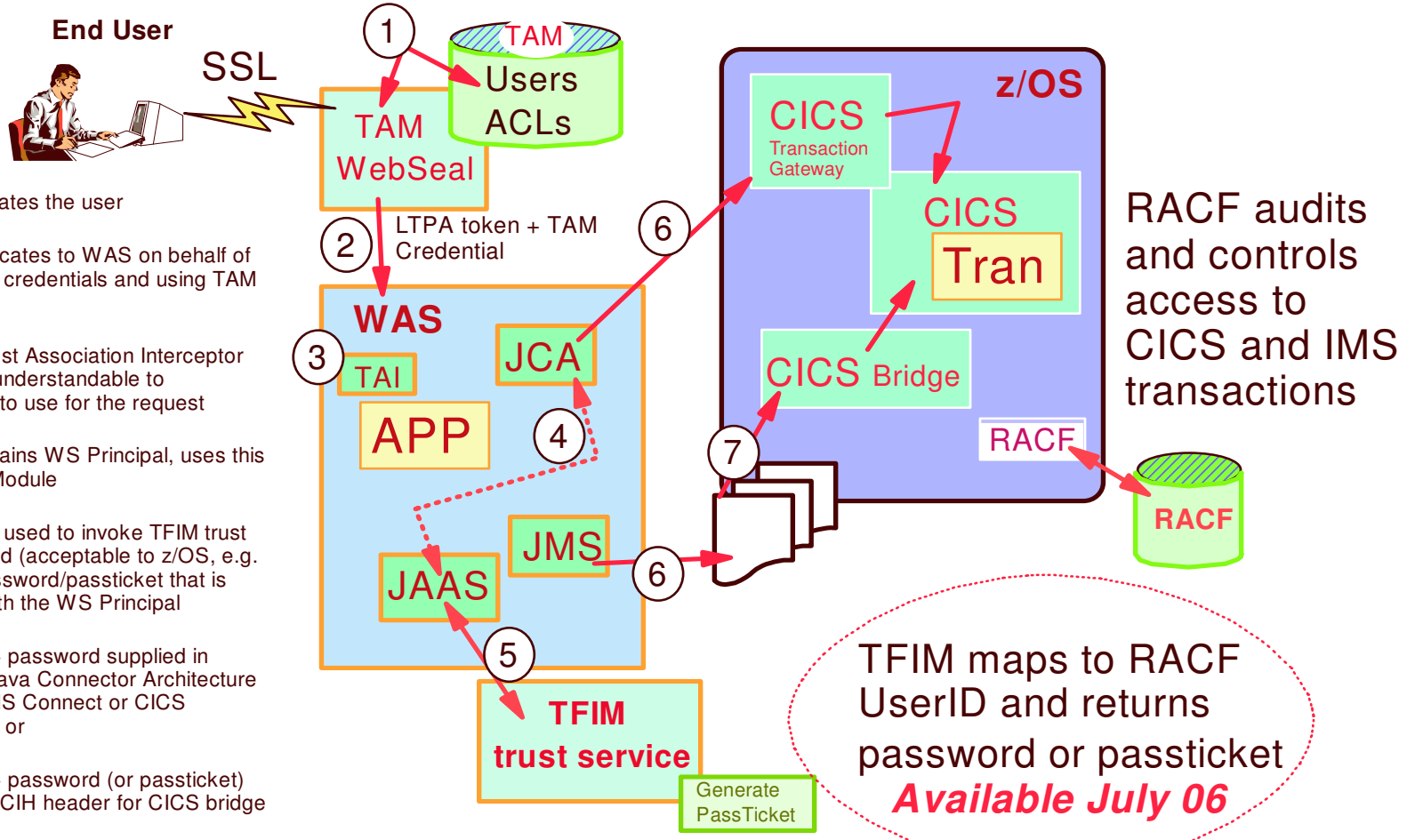


Tivoli Federated Identity Manager 6.1, (GAed July 06) introduced new z/OS-related features

- **Security Token Services (STS) run-able on z/OS (runs as a WAS for z/OS application)**

- **PassTicket Generation/Validation module**
  - Allows for creation/validation of usernametoken security tokens which consist of userid+PassTicket values
  - When running on z/OS, utilizes RACF-specific functions
  - When running on other platforms, requires PassTicket shared secret configuration between FIM server system and RACF

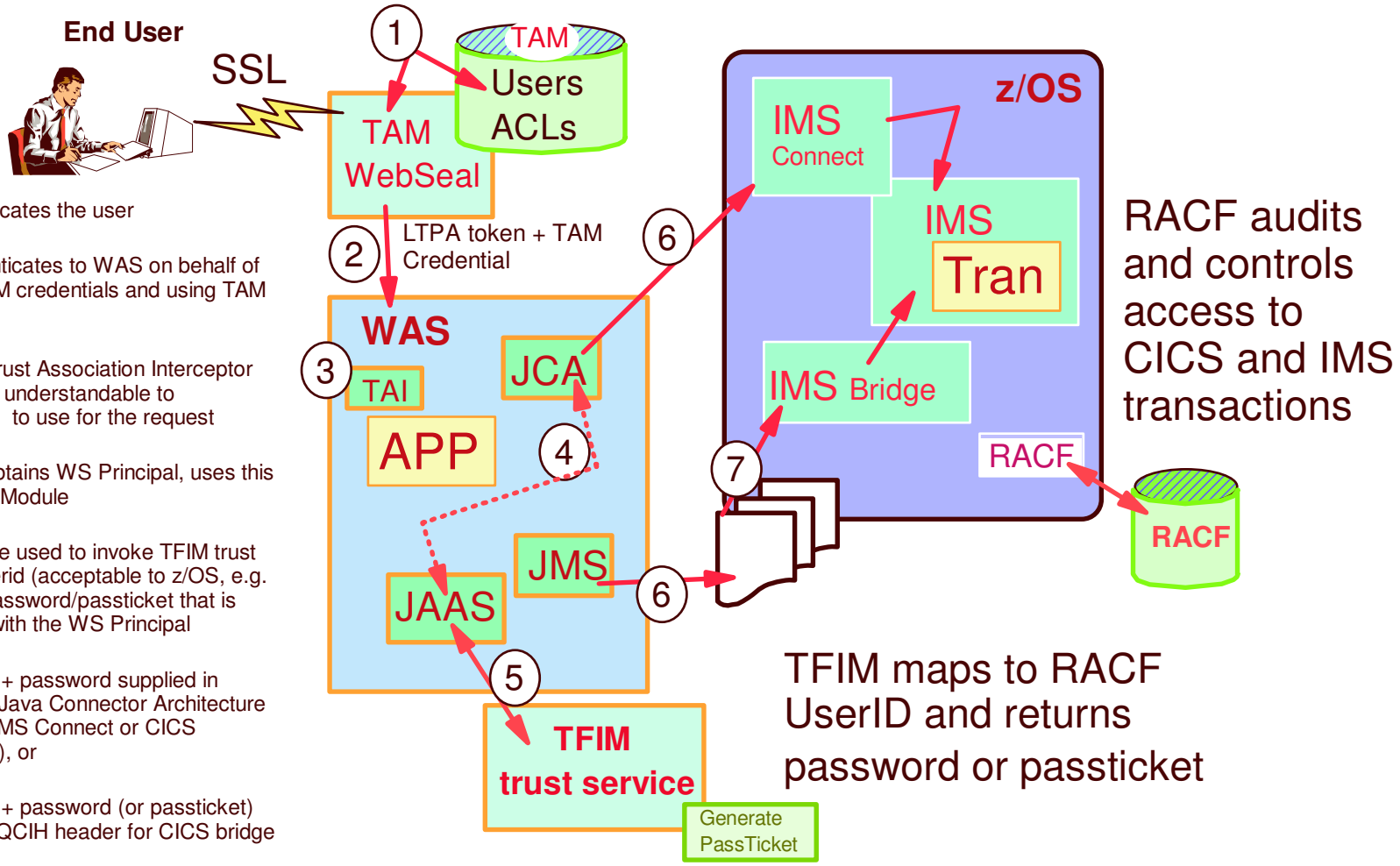
CICS flow using TFIM for PassTickets



Readable version of previous ledger

1) WebSeal authenticates the user
2) WebSEAL authenticates to WAS on behalf of the user, passing TAM credentials and using TAM TAI
3) In WAS, a TAM Trust Association Interceptor (TAI) returns a userid understandable to WebSphere for WAS to use for the request
4) JCA Connector obtains WS Principal, uses this to invoke JAAS LoginModule
5) JAAS LoginModule used to invoke TFIM trust service to get a userid (acceptable to z/OS, e.g. RACF userID) and password/PassTicket that is associated by TFIM with the WS Principal
6) Mainframe userid + password supplied in Connection Spec for Java Connector Architecture connection (through IMS Connect or CICS Transaction Gateway), or
7) Mainframe userid + password (or PassTicket) supplied in MQMD/MQCIH header for CICS bridge connection

IMS Flow illustrated *(similar to CICS)*



(1) WebSeal authenticates the user

(2) WebSEAL authenticates to WAS on behalf of the user, passing TAM credentials and using TAM TAI

(3) In WAS, a TAM Trust Association Interceptor (TAI) returns a userid understandable to WebSphere for WAS to use for the request

(4) JCA Connector obtains WS Principal, uses this to invoke JAAS LoginModule

(5) JAAS LoginModule used to invoke TFIM trust service to get the userid (acceptable to z/OS, e.g. RACF userID) and password/passticket that is associated by TFIM with the WS Principal

(6) Mainframe userid + password supplied in Connection Spec for Java Connector Architecture connection (through IMS Connect or CICS Transaction Gateway), or

(7) Mainframe userid + password (or passticket) supplied in MQMD/MQCIH header for CICS bridge connection

RACF audits and controls access to CICS and IMS transactions

TFIM maps to RACF UserID and returns password or passticket

Certificate Mapping to RACF Identity

via Certificate Name Filtering (CNF) in RACF

- Two ways to establish mapping:

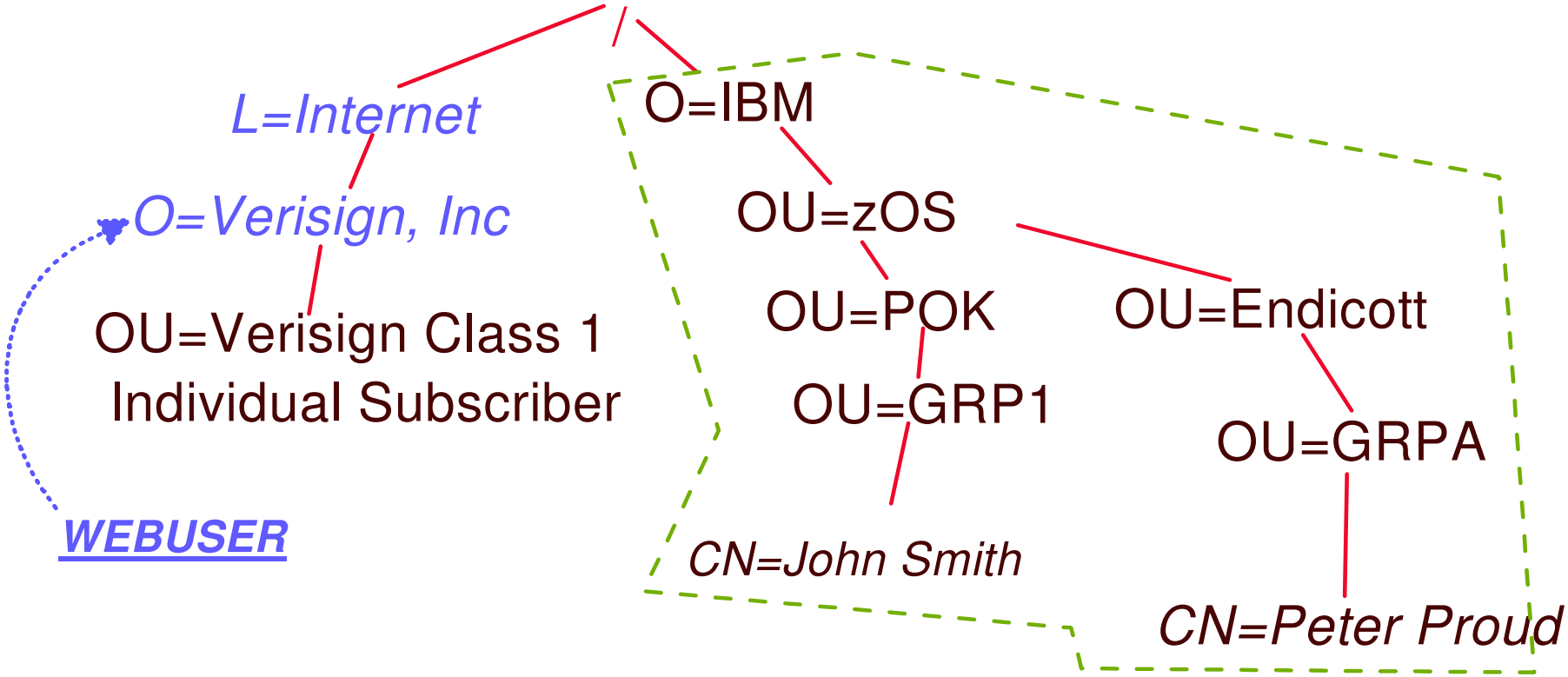
1. Certificates can be individually defined to RACF

2. Filter 'rules' based on Distinguished Name can select the userid to assign for a particular certificate
   - Certificate "subject" and "issuer" name considered, plus "*criteria*"
     - *Criteria allows one Digital Certificate to be used for multiple applications*
   - More granular access control and accountability, and easier handling of expired certificate situation
   - RACF Dig Cert Mapping can scale to very large numbers

Example: Mapping, Certs to Userid

Map all Verisign issued certificates to user WEBUSER.
Subject doesn't matter

RACDCERT MAP IDNFILTER('O=Verisign, Inc.L=Internet') ID(WEBUSER)



Example 2

Map all 'Your z PKI' issued certificates to User IDs based on the target application, subject doesn't matter

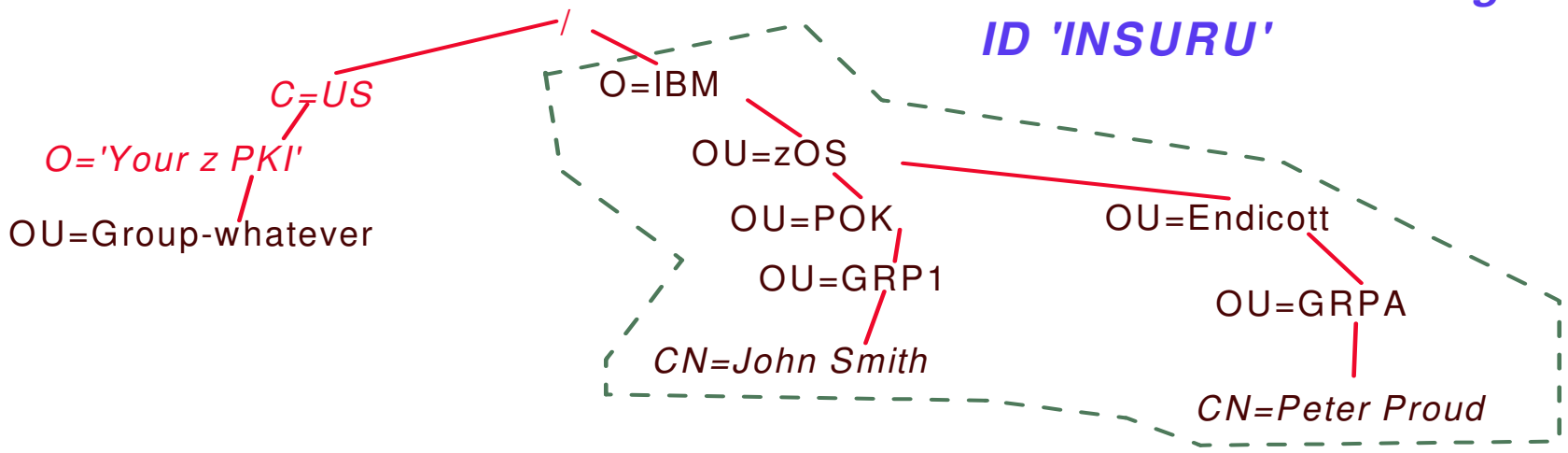
DIGTCRIT Class Profiles:

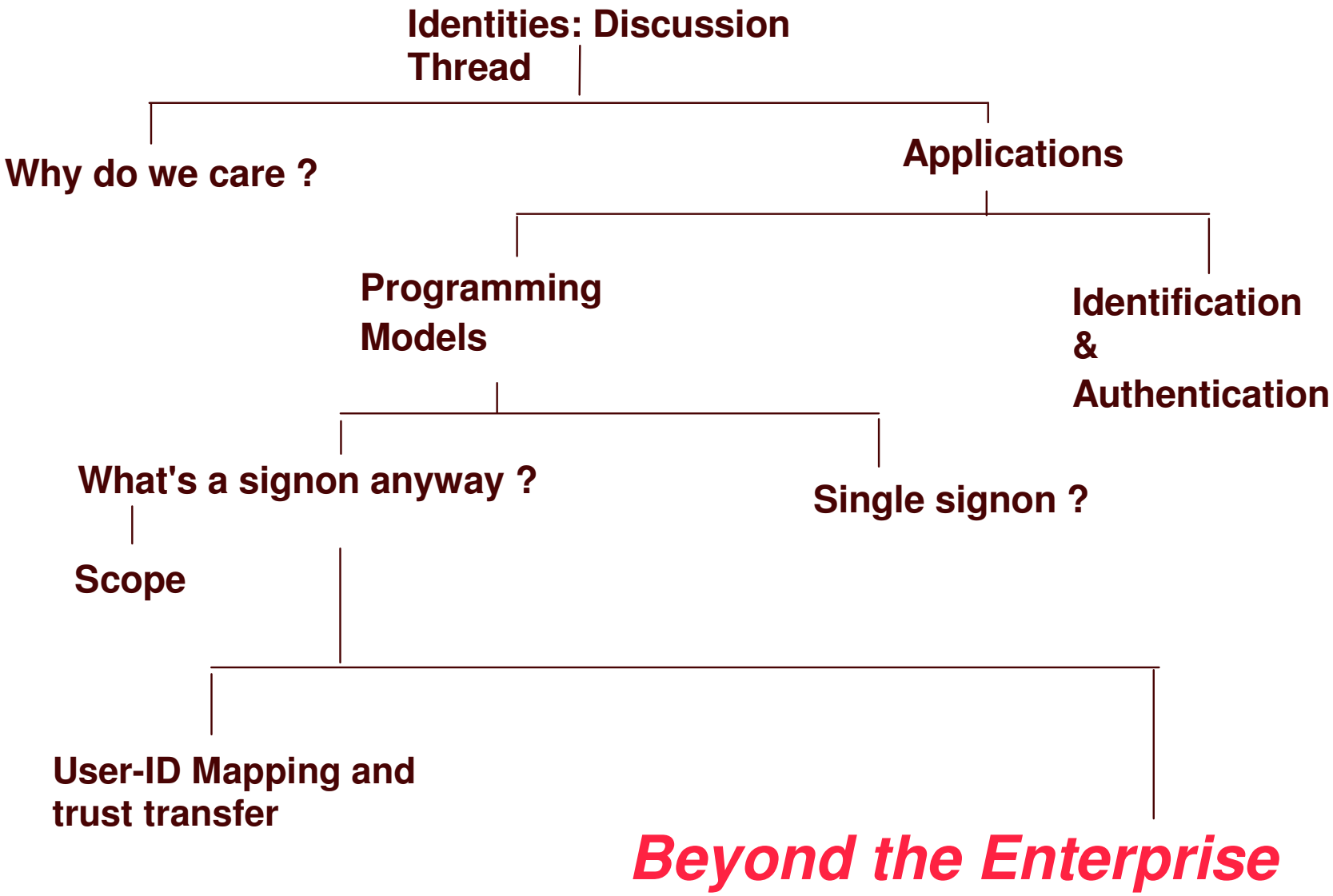
- **RDEF DIGTCRIT APPLID=WEBBANK APPLDATA(BANKU)**
- **RDEF DIGTCRIT APPLID=WEBINSUR APPLDATA(INSURU)**

RACDCERT IDNFILTER('O=YourZPKI.L=Internet') MULTIID CRITERIA(APPLID=&APPLID) TRUST

MAP

Result: any users with a 'Your z PKI' certs accessing application 'WEBBANK' are assigned ID 'BANKU' while those accessing application WEBINSUR are assigned ID 'INSURU'





Tivoli Federated Identity Manager (TFIM)

Cross-Domain Security for Web Services and Credential Transform

Components

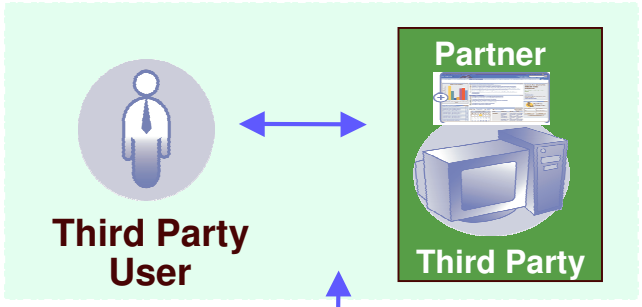
Federated Single Sign-on
(SAML, Liberty, WS-Federation)

Federated User Provisioning
(WS-Provisioning)

Web Services Security Management
(WS-Security, WS-Trust)

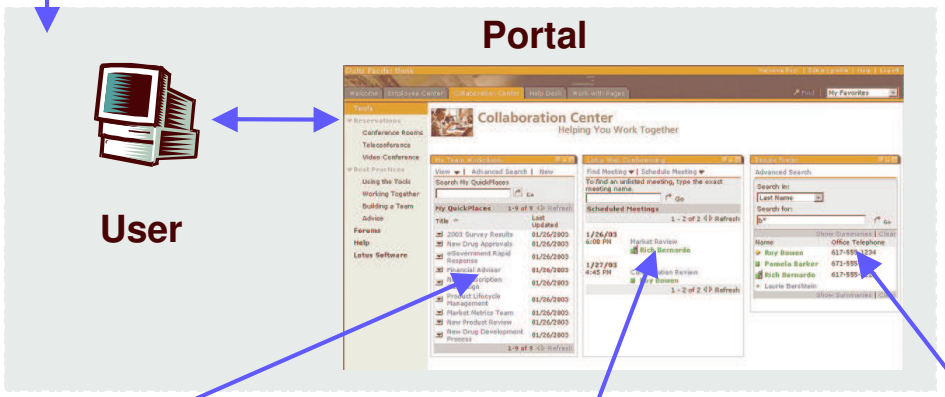
z/OS PassTicket generation support added; GA July 06

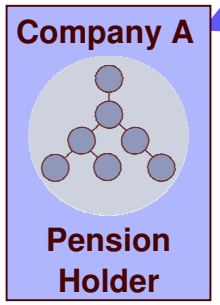
Tivoli Federated Identity Manager

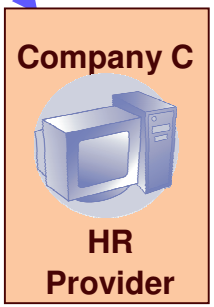


Typical Scenarios

- Multiple enterprises or multiple businesses within an enterprise
- Goal: share user information among trusted partners in a transaction







Wrap-up

- Identities have meaning between a given application and the security identification & authentication (I&A) service that the application uses
- User-ID mapping functions, such as RACF Certificate Name Filtering, can be used to translate an identity known in one registry domain to an identity known some other registry domain
- In order to facilitate single signon between applications, trust in the end-user must be securely transferable between the applications
- Web Security Services expand the concept of identity mapping beyond the enterprise, and as such will be critical infrastructure in support of on-demand computing
- Future: A strategic direction for z/OS is enterprise computing infrastructure simplification. Improved handling of multiple identities is a key component of this strategy

z/OS Security Information on the Web

- **z/OS Web Sites**
  - http://www.**ibm.com**/servers/eserver/zseries,
  - http://www.i**bm.com**/servers/eserver/zseries/zos

- **RACF Home Page**
  http://www.ibm.com/RACF
  - Latest release information on RACF
  - Links to announcement letters
  - Sample code
    - DBSYNC to compare/sync. two RACF databases
    - RACFICE to create audit/analysis reports
    - OS390ART for a Web-based reporting tool
    - RACTRACE tracing facility
    - RACFDB2 Conversion Utility
    - PKIServ (replacement for CA Servlet)
  - Frequently Asked Questions
  - RACF user group information
  - RACF-L information

IBM System z Security

- http://www.ibm.com/systems/z/security/

IBM Systems Journal articles on z/OS Security, via the Web at http://www.research.**ibm.com**/journal

- Search for "Security on z/OS: Comprehensive, current, and flexible" , and
- "Using RACF to Secure DB2 Objects"

Not z/OS, but included anyway, on RADIUS protocol
http://ing.ctit.utwente.nl/WU5/D5.1/Technology/radius/