Single Sign On In A CORBA-Based Distributed System

Igor Balabine

IONA Security Architect

Outline

- A standards-based framework approach to the Enterprise application security
- Security framework example: IONA Security Framework (iSF)
- Security framework based SSO solutions
- Summary

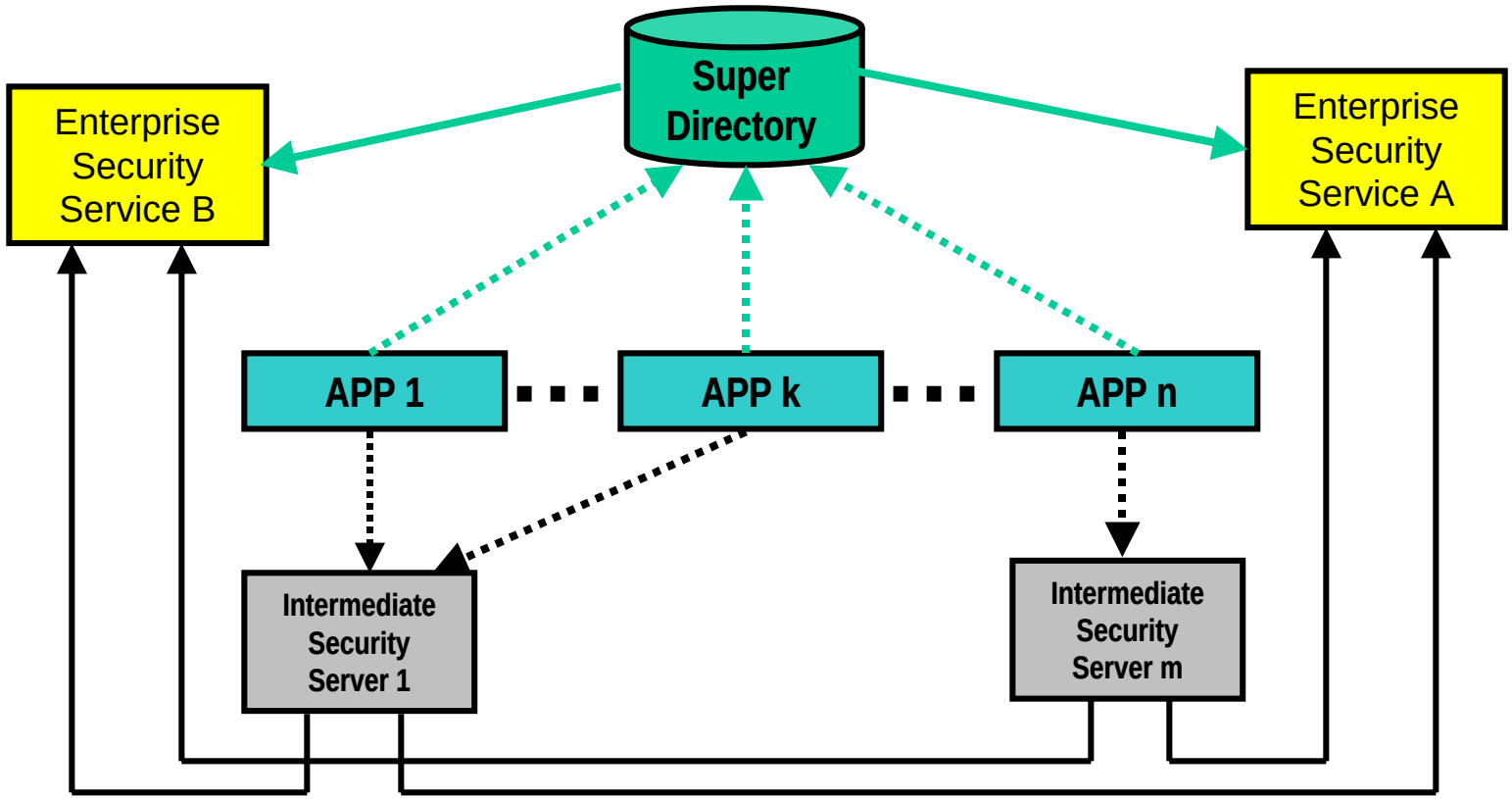
Why A Security Framework?

Security Framework:

- insulates middleware applications from the diverse and changing enterprise security infrastructures.
- provides a uniform, vendor-neutral, standards-based approach to communicating security-related requests across the enterprise.
- provides applications a single access point to multiple security services such as authentication, authorization, SSO, PKI, management, and notification services.

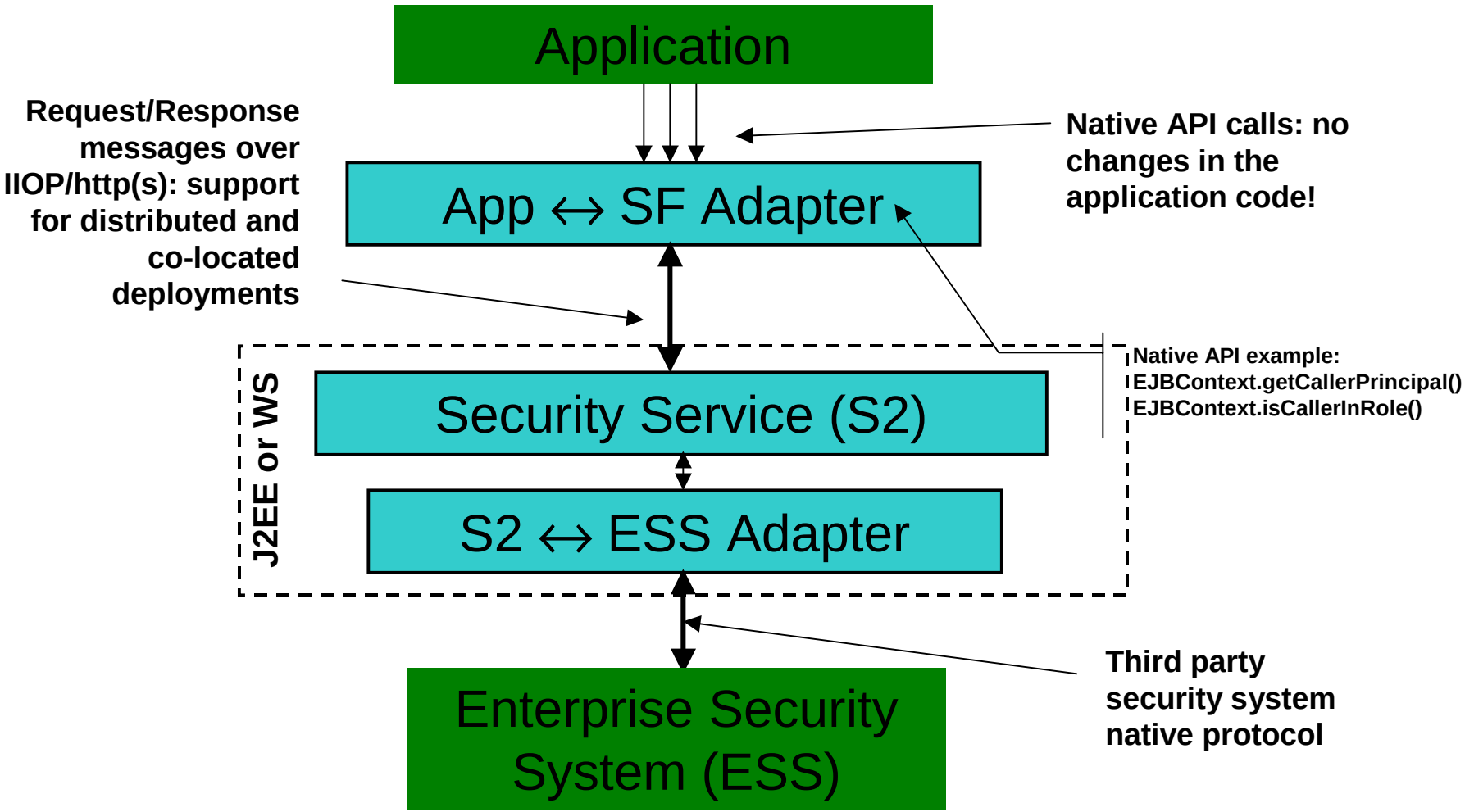
Security Framework binds applications with any enterprise security infrastructure!

Security Framework vs Super-Directory



Security framework approach avoids performance bottlenecks suffered by a centralized approach such as Super Directory !

Security Framework Architecture



Authentication and Authorization Services

- Authentication and authorization services are supported via dedicated adapters.
- Internal protocol: SAML – satisfies purposes and allows extensibility. Could be easily replaced if necessary if internal interface in the application SDK is generic.
- Required authorization models: coarse grain – RBAC (e.g. J2EE, Web Services), fine grain – DAC (e.g. CORBASEC, B2Bi).

SAML protocol allows communicating arbitrary security assertions between applications and the Security Server!

PKI Services

- PKI services are supported via dedicated adapters.
- Internal protocol: XKMS – powerful and extensible. Endorsed by industry leaders (Verisign, Entrust, Microsoft).
- Common use: integration with certificate stores.
- Advanced use: certificate validation services.

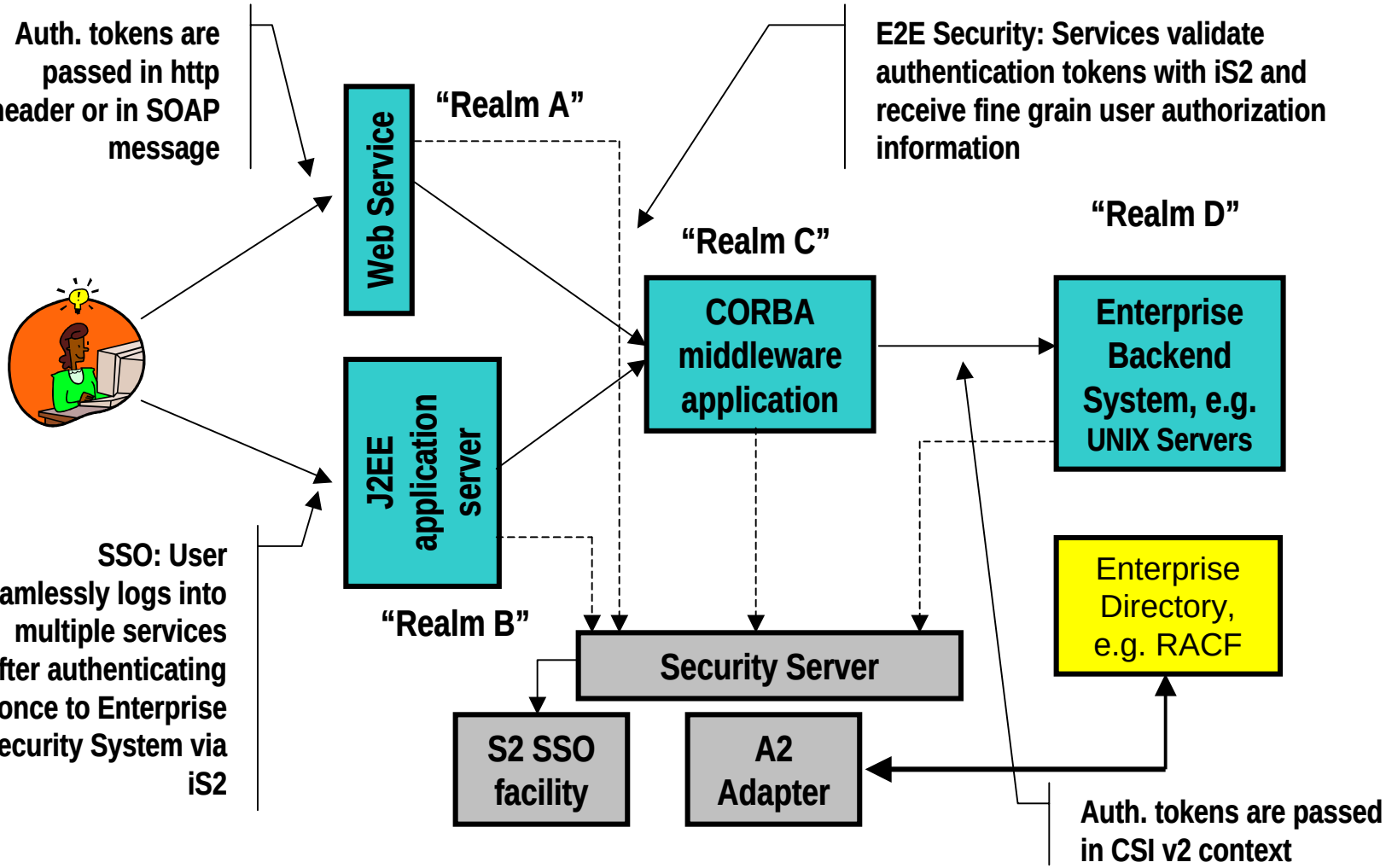
Many PKI vendors are expected to adopt XKMS: in such installations S2 PKI adapter becomes (almost) a pass through!

Framework Administration

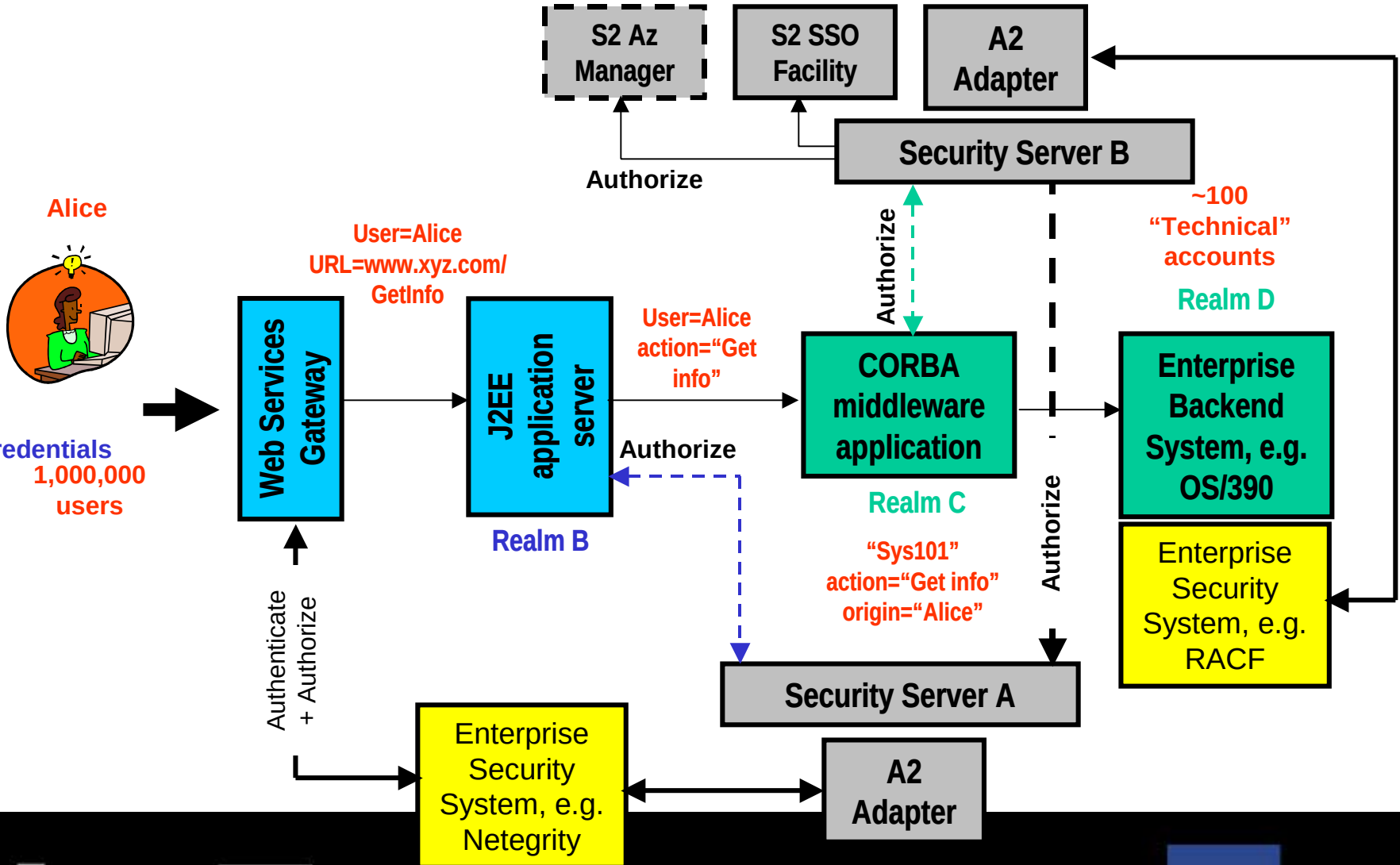
- Solutions integrated with 3rd party systems are managed using native administrative tools, e.g. SiteMinder console for an enterprise which uses Netegrity SiteMinder.
- Framework provides out of the box facilities for Single Sign-On and authorization (RBAC and DAC) services for environments devoid of such functionality, e.g. Windows Domain.
- Framework Auditing Component co-located with the Security Server (S2) provides logs in standard formats (syslog, NT Event Log, Snort) easily consumable by event monitoring systems.

Framework offloads administrative tasks to 3rd party tools where possible and provides components to manage custom security information!

Single Sign-on and End-to-End Security

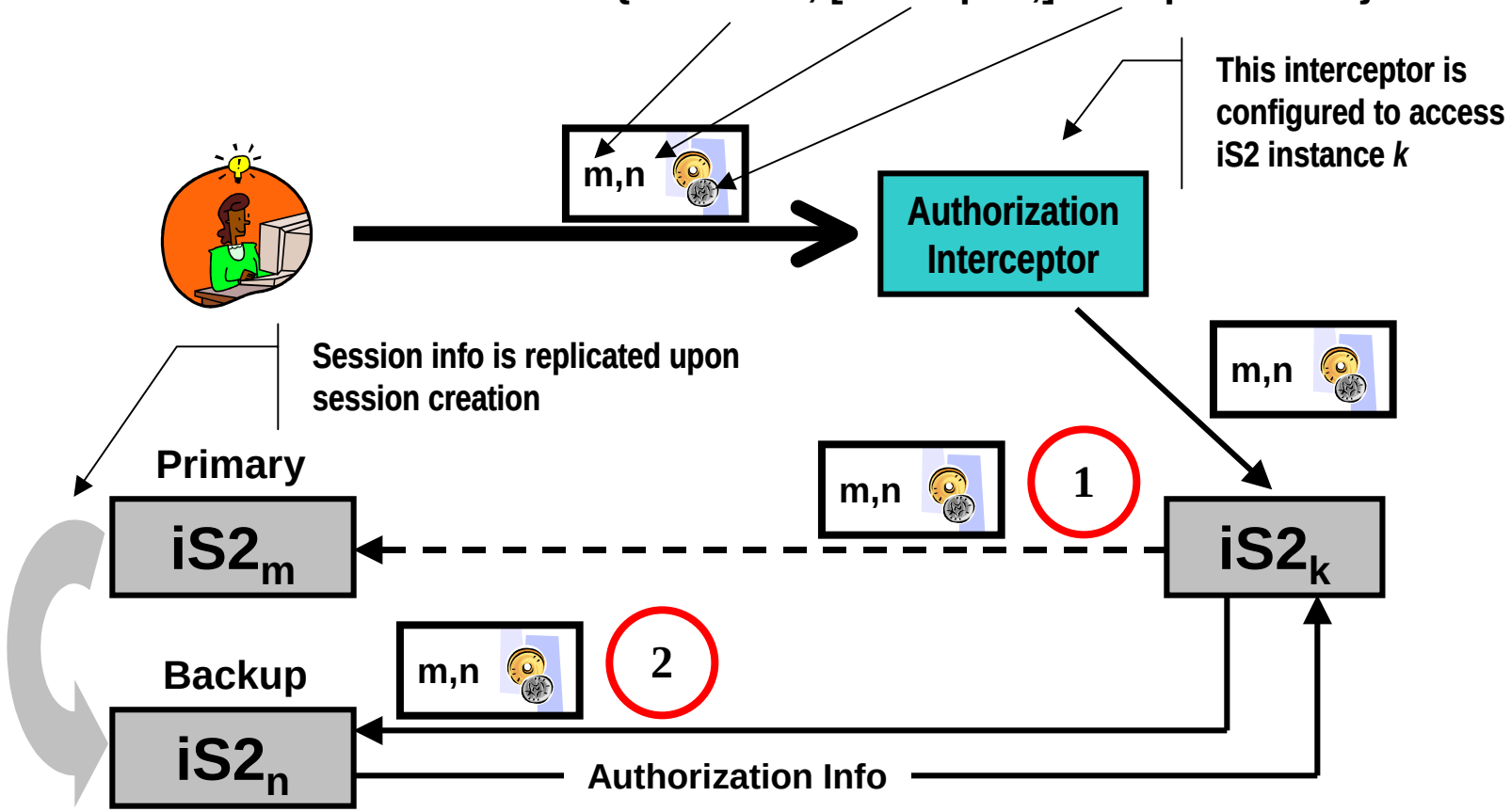


Crossing The Chasm…



Framework Scalability and Fail-over

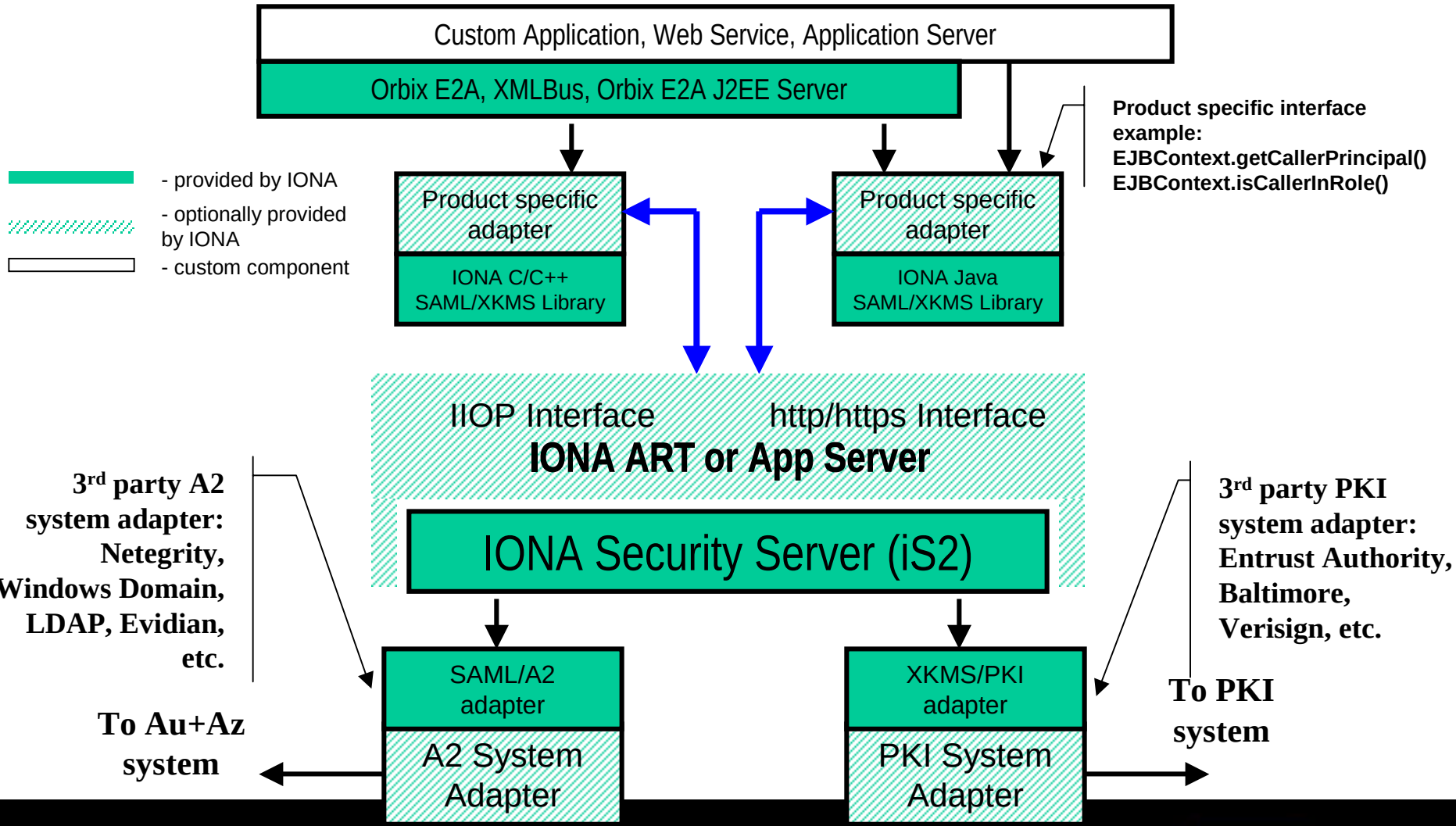
Authentication Token structure: { issuer id, [backup id,] <unique value>}



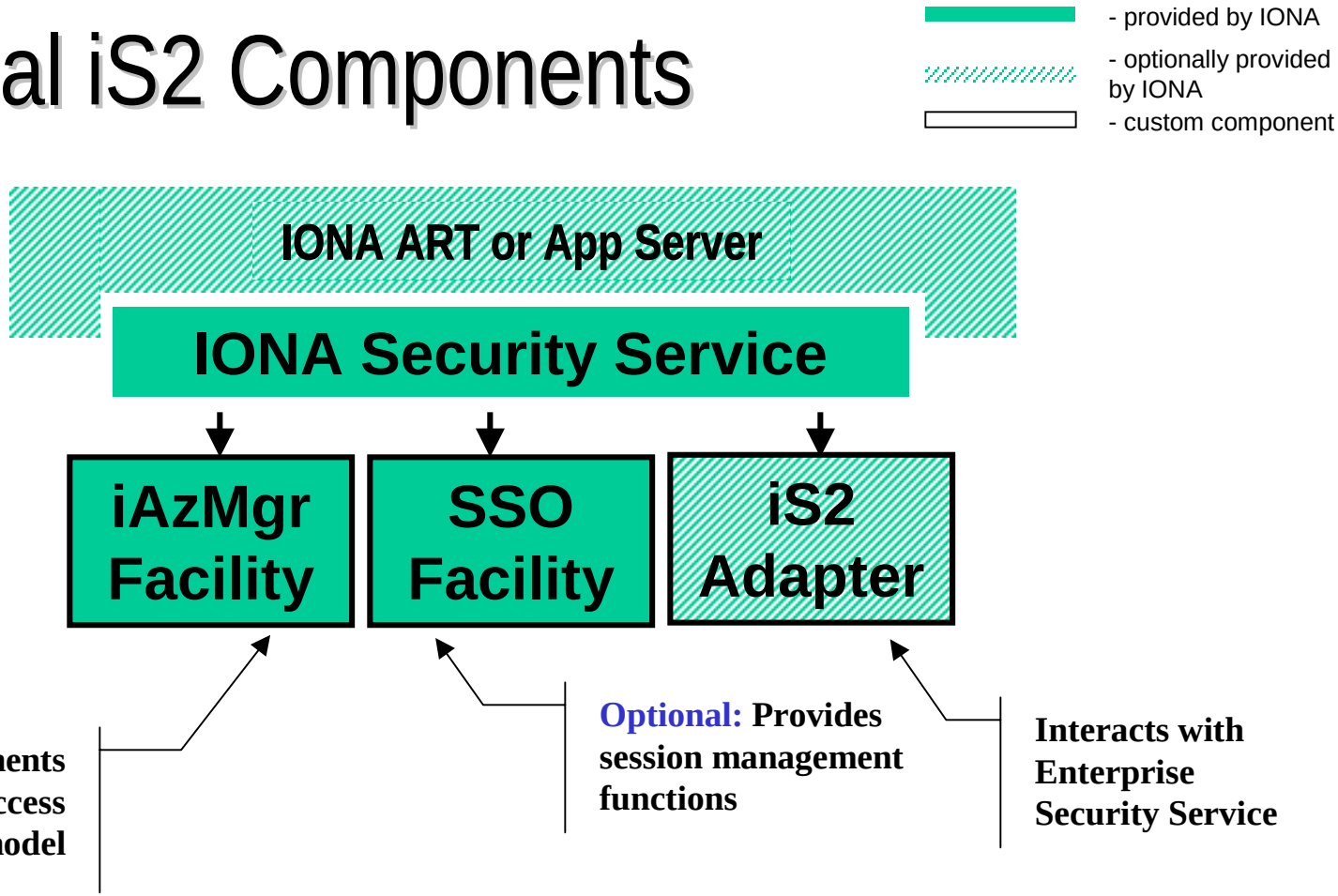
Security framework clustering schema guarantees that principal's authorization information is no more than two hops away!

Security Platform Example: IONA Security Framework (iSF)

IONA Security Framework Components



Optional iS2 Components



iSF provides optional built-in components which augment the existing ESS functionality or provide mechanisms absent in the existing ESS!

Single Sign On (SSO) Facility

- Provides session management features to iS2 client applications.
- Issues authentication tokens which clients can use for subsequent access to the services provided by iS2 client applications.
- Authentication token is valid for a certain period configured by SysAdmin.
- Authentication token expires if idle period between two subsequent service requests exceeds maximum configured by SysAdmin.

iS2 SSO facility provides single sign on functionality across Enterprise security domains!

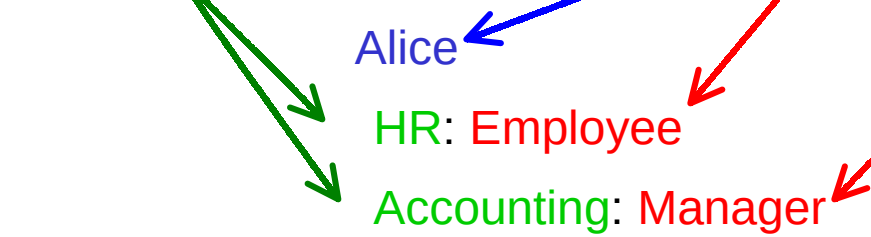
iS2 Authorization Manager

- iAzMgr keeps information which supports implementation of the Role Based Access Control (RBAC) model by IONA or third party products.
- iAzMgr stores information about Principals, Roles and privilege scopes called “Realms”.
- iAzMgr answers a simple question: “Which ***Roles*** are assigned to this ***Principal*** in a given ***Realm***?”
- iAzMgr database of Principals, Roles and Realms is stored in an abstract repository accessed via JDBC.

iAzMgr keeps authorization information in environments devoid of robust authorization facilities such as Windows Domain!

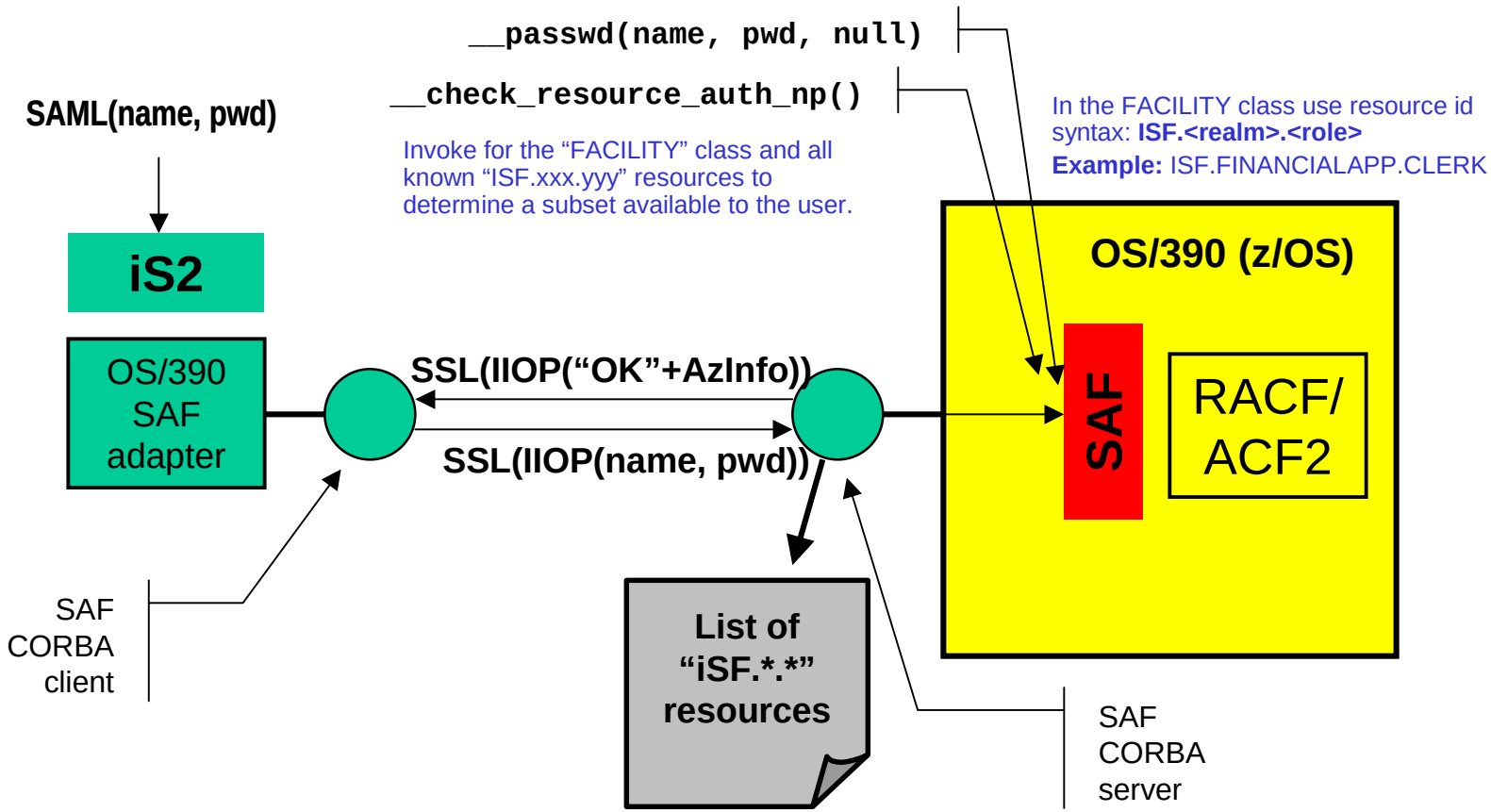
iAzMgr Feature: Scoped Roles

Realm	Role	Principal
HR	Employee	Alice
Engineering	Manager	Bob
Accounting	Administrator	Carol
	Operator	



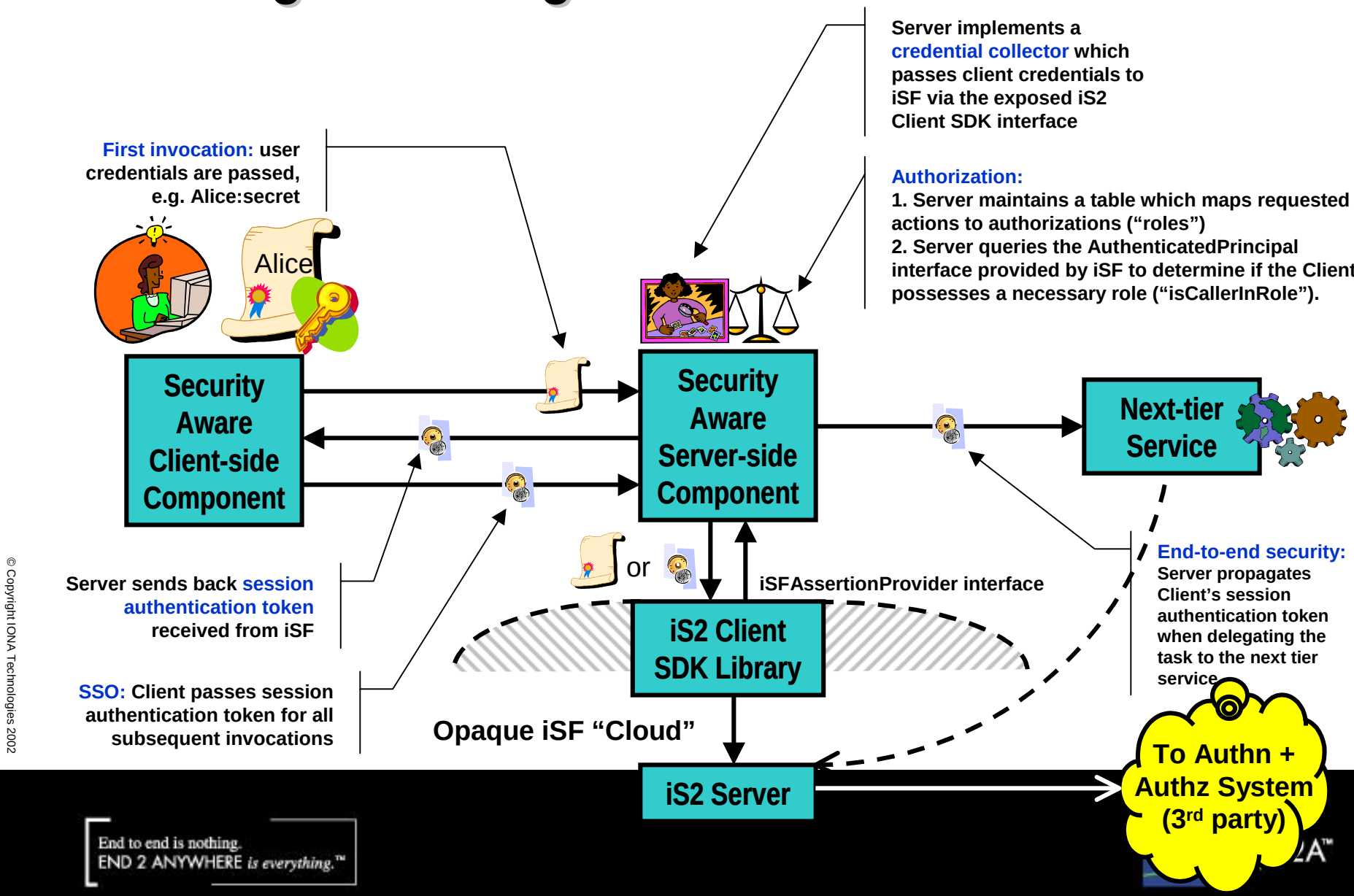
iSF implements a superset of the proposed NIST RBAC standard compatible with the J2EE requirements!

iSF Adapter Example: OS/390 SAF



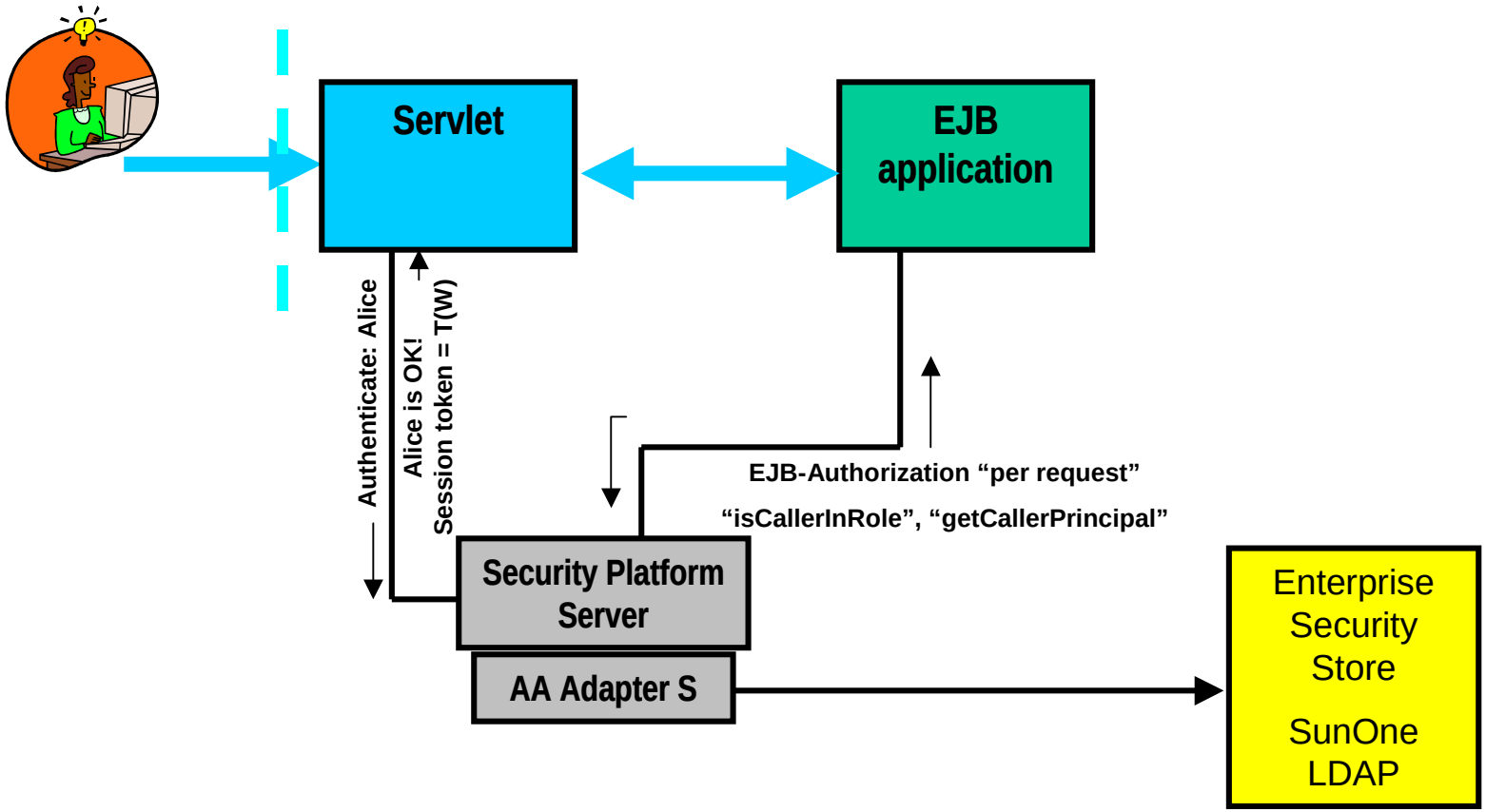
A "smart" iSF adapter allows to use RACF as a RBAC repository!

Putting It All Together

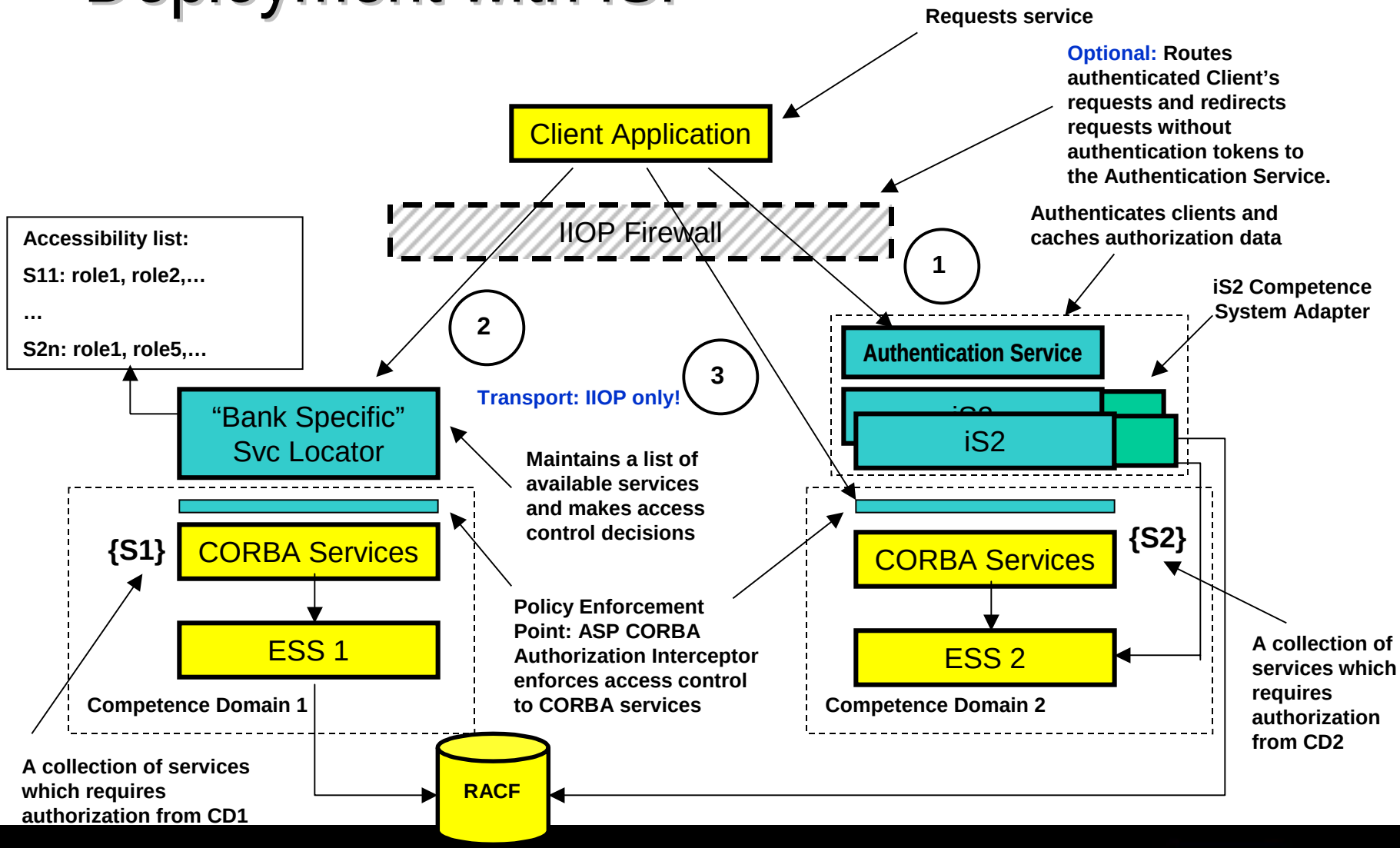


Security Framework Based SSO Solutions

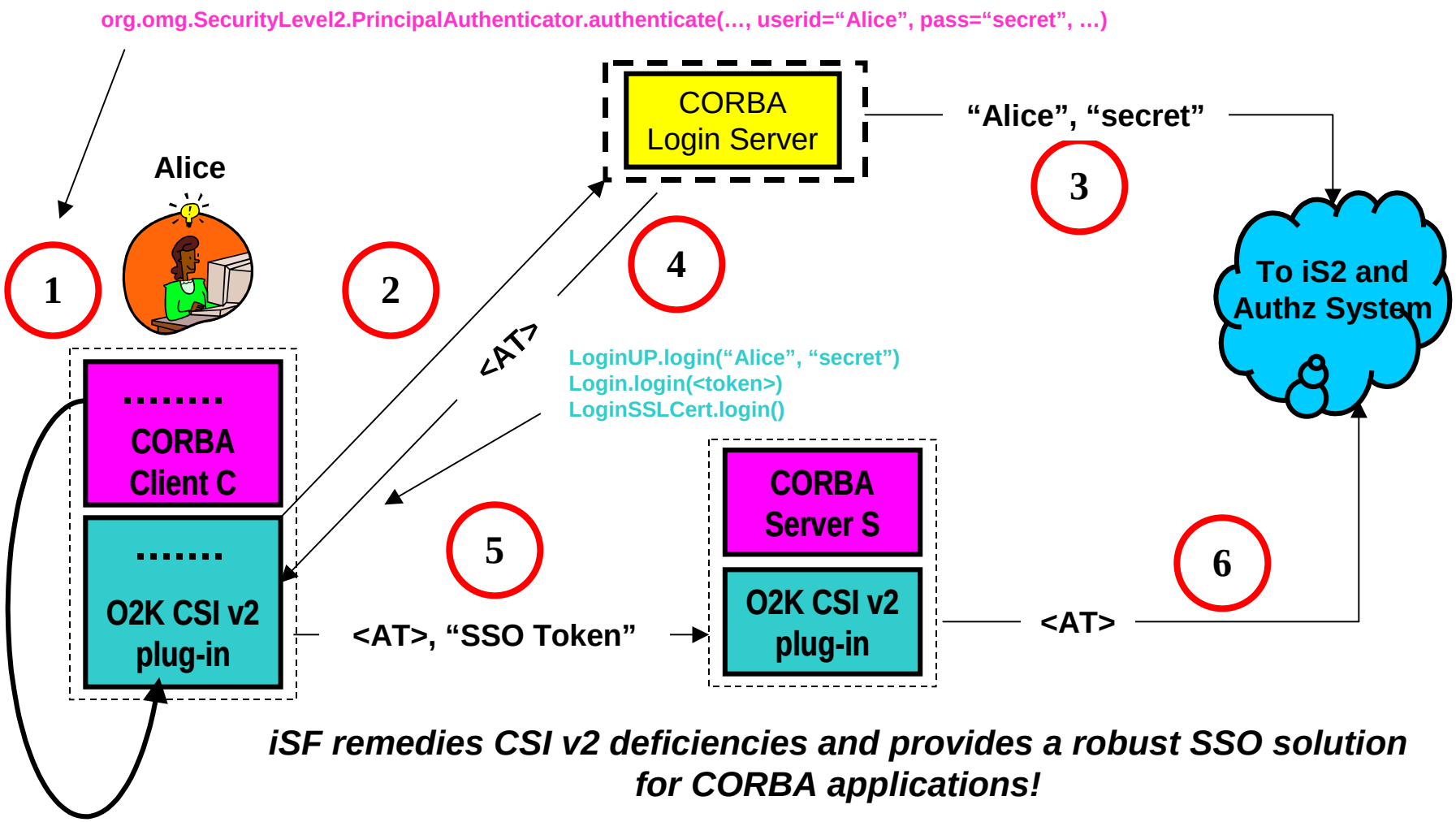
“A Spanish subsidiary of a Swiss Insurance”



Deployment with iSF



SSO For CORBA Clients

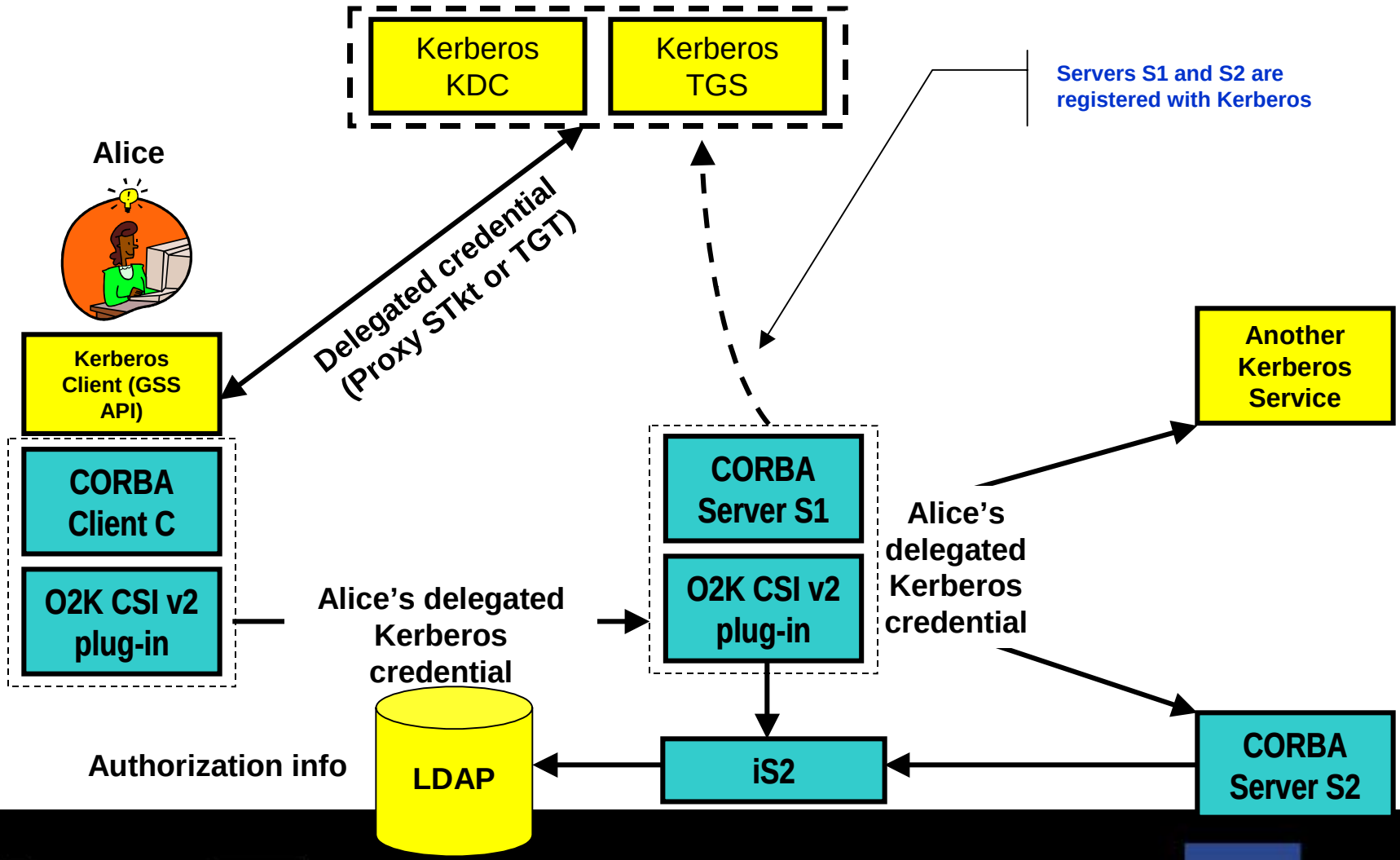


iSF remedies CSI v2 deficiencies and provides a robust SSO solution for CORBA applications!

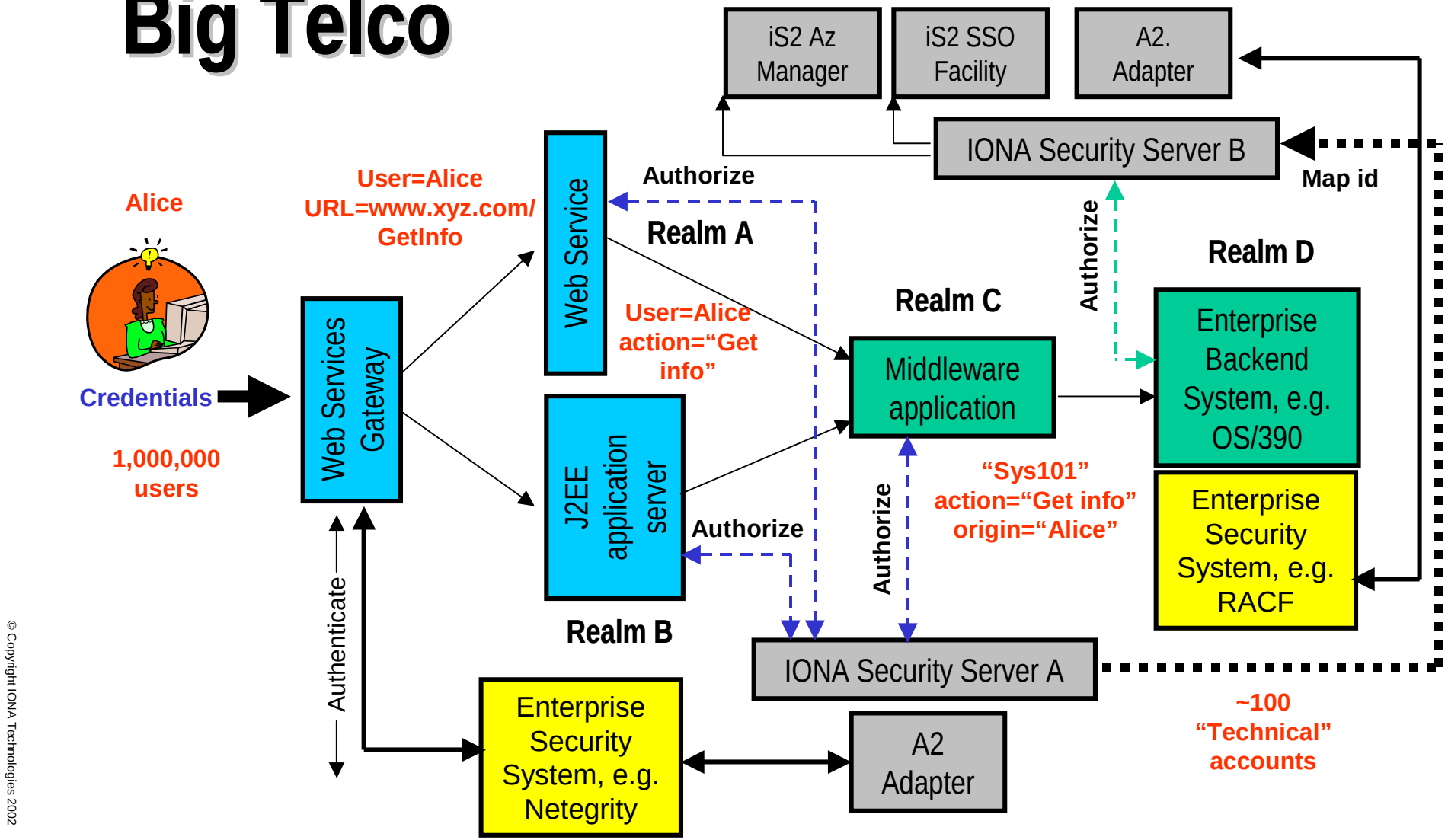
“A Government Agency”

- Requirements:
  - Use Kerberos credentials to authenticate and authorize requests to non-Kerberized services
  - Support secure invocation of Kerberized services by non-Kerberized CORBA applications using delegated Kerberos credentials
- Solution:
  - Use CSI v2 context for transmitting Kerberos service request tokens
  - Use iSF to authorize Kerberos users for invoking non-Kerberos services

“Government Agency” Deployment



Big Telco



Summary - Security Platform benefits

- Security Framework approach provides applications a robust integration broker layer with Enterprise wide security services.
- Framework based architecture is flexible and allows integration with diverse security solutions from Windows domain to OS/390 RACF.
- Security framework covers important aspects of security such as authentication, authorization, SSO and PKI services.

Additional Information

IONA Security Framework (iSF) and its application to providing security services to J2EE, CORBA applications and Web Services is described in the “Orbix E2A Security” white paper.

You may download it at

http://www.iona.com/whitepaper.htm