COMPACFLT - EDAC

Enterprise Dynamic Access Control (EDAC)

Point of Contact:

Richard Fernandez

fernandr@spawar.navy.mil

SPAWAR
Systems Center
San Diego

COMPACFLT - EDAC

For licensing information contact:
Stephen Lieberman
Voice: (619) 553-2778
Mobile: (619) 606- 5940
Email: stephen.lieberman@navy.mil

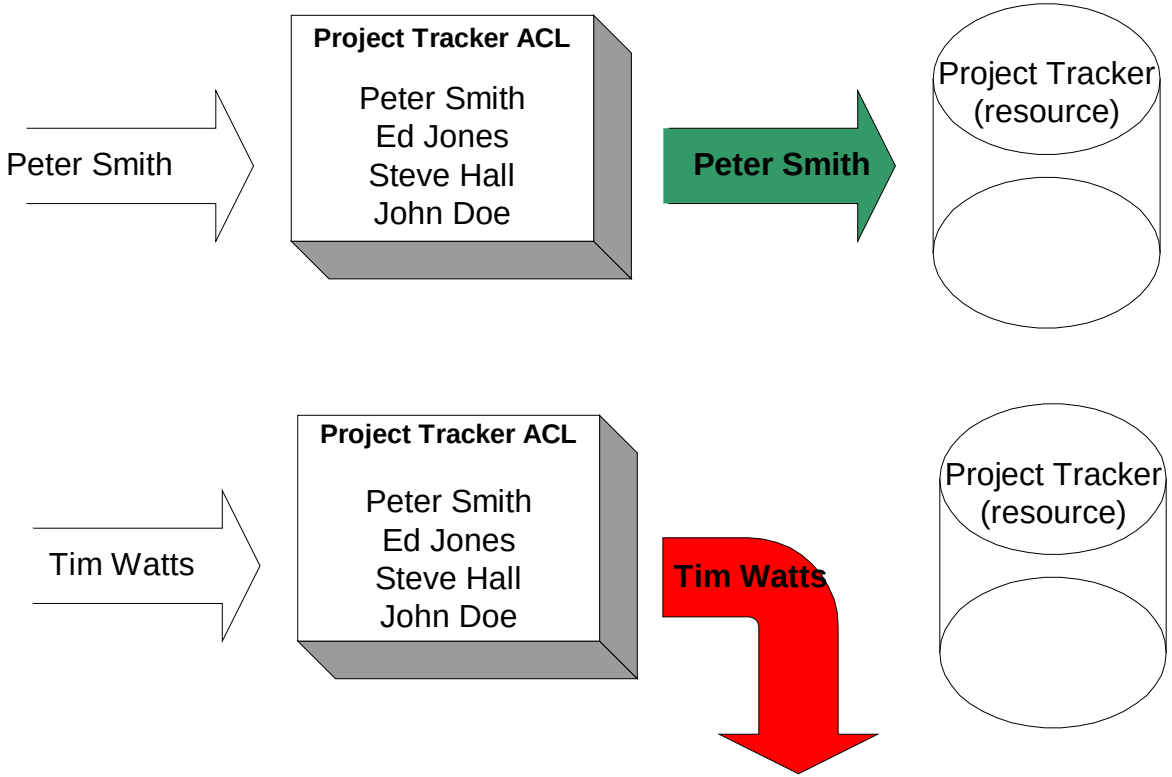
For comments regarding this product contact:
Richard Fernandez
Voice: (808) 474-9270
Email: richard.r.fernandez@navy.mil

Outline

- Access control background
  - Access control lists
  - Groups
  - NIST RBAC standard
- SEAC RBAC
  - Customer furnished and maintained assets
  - How it works
  - Product overview
  - Interoperability

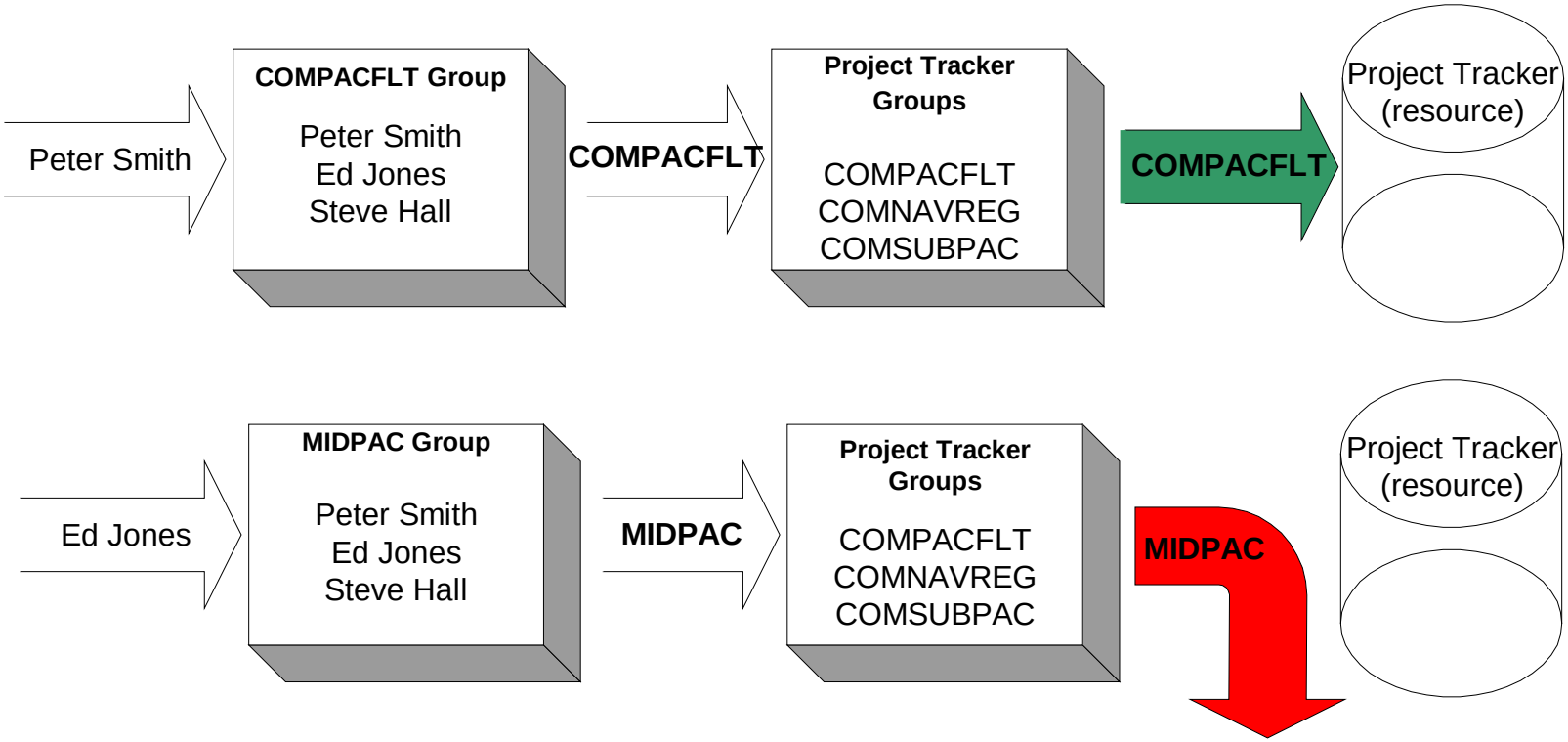
Access Control Lists (ACL)

User name or unique identifier associates access to resources



Groups

User associated to a group and group associated to resources



Essentials for resource access

Necessary requirement to access resources:

- Not a user name
- Not a unique identifier
- Not a group association

- List of user characteristics

What are user characteristics

User characteristics (user profile)

- Where client works: **organization**
- What security credentials: **clearance**
- What pay category: **pay grade**
- What branch : **service**
- What vocation: **job function**
- etc

Examples of User Profiles

- User profile is a unique list of user characteristics.
- A client may have more than one user profile.
- User attributes should be compiled from an authoritative data source(s) on a real-time basis.

Categories	COMPACFLT	USNR
Organization:	CPF N65	Naval Intel
Clearance:	Secret	Top Secret
Paygrade:	DP3	02
Service:	DoD	DoNR
Function:	Program Manager	Intelligence

Impact on resource access

The following can affect resource access:

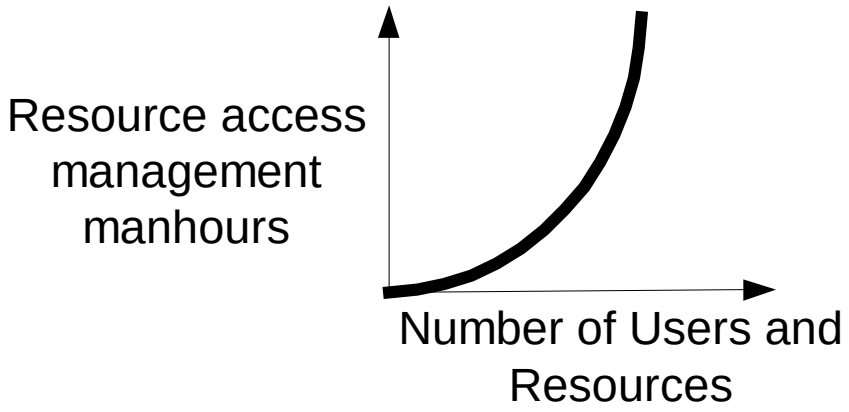
- Transfer to another organization
- Loss of security clearance
- Change in job title
- Job promotion

Problems with ACLs and Groups

Maintaining an updated ACL or group is time consuming.

Situation worsens when:

- Number of users increase
- Number of resources increase



NIST RBAC compliance

Because of ACL and group limitations:

The National Institute of Standards and Technology (NIST) RBAC is an American National Standard - ANSI INCITS 359-2004 (approved 19 Feb 04)

NIST RBAC standard

Definitions:

Users and Roles: "…*access decisions are based on the roles that individual users have as part of an organization.*
"Access rights are grouped by role name…

Role hierarchies: *"Under RBAC, roles can have overlapping responsibilities and privileges;*

Roles and Operations: *"Organizations can establish the rules for the association of operations with roles.*

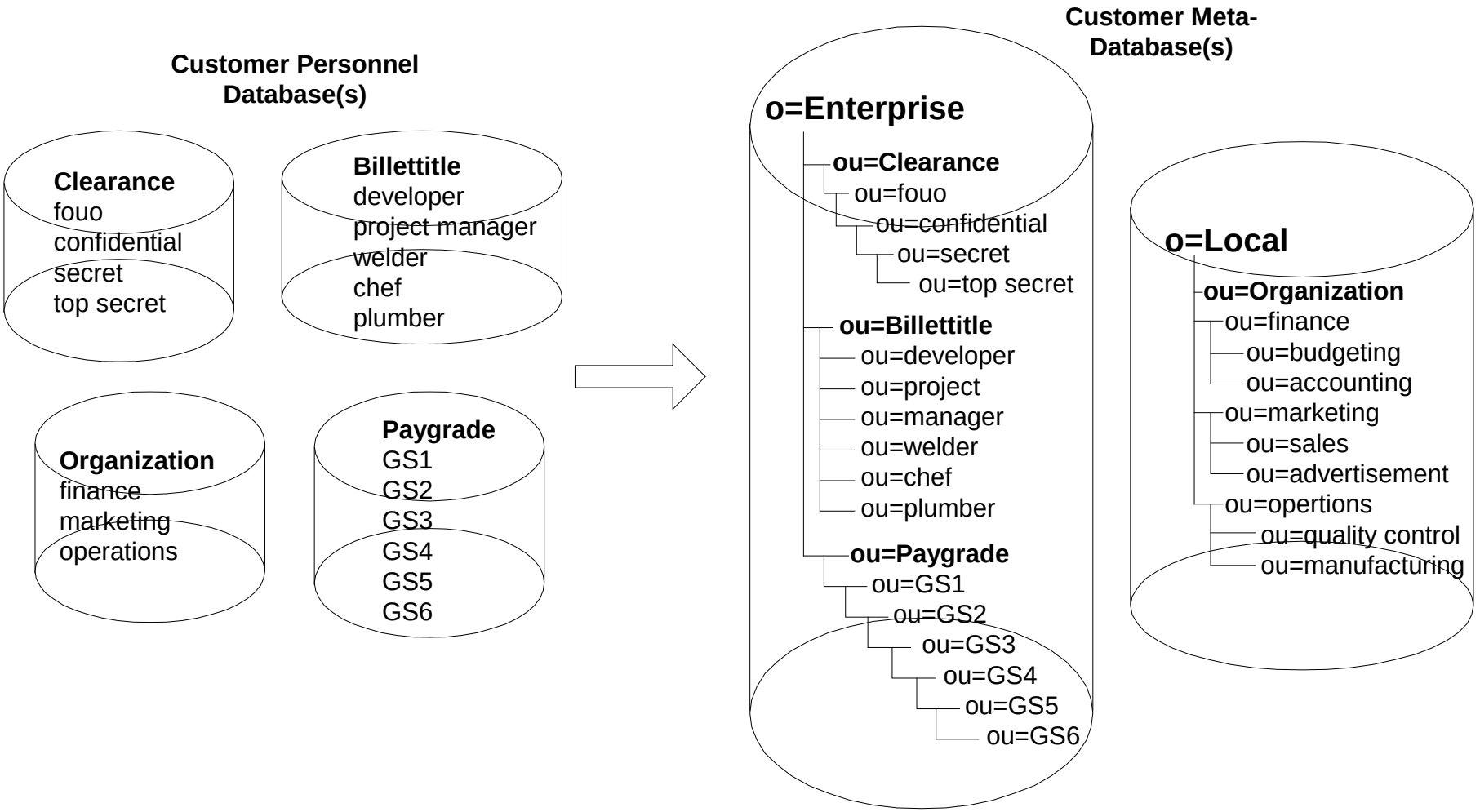
Access control comparison

How access control solutions can simultaneously evaluate user characteristics.

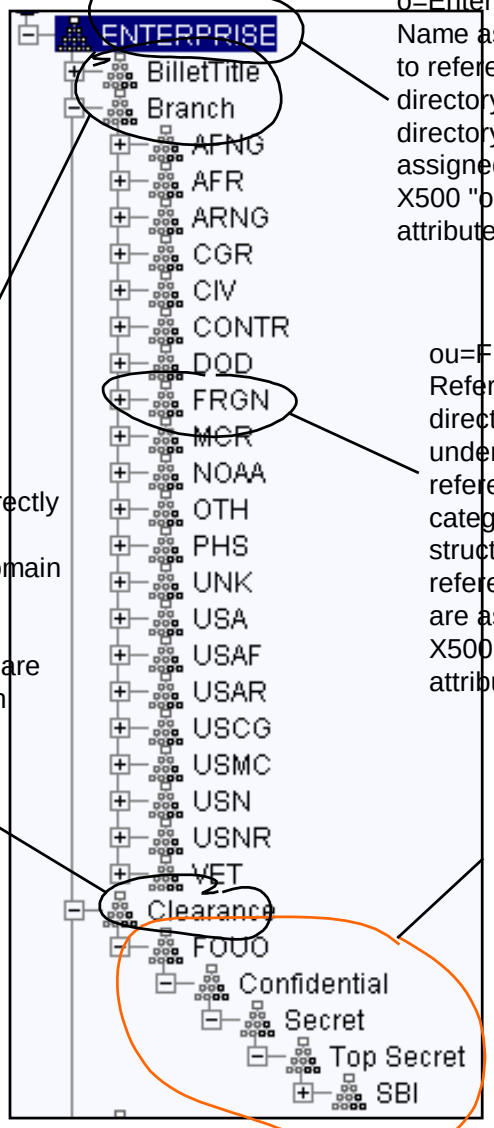
	Simultaneous evaluation of multiple object characteristics & environmentals	Simultaneous evaluation of multiple object characteristic & environmental hierarchies	Real-time detection of object characteristic changes, thus affecting resource access
ACLs	0	No	No
Groups	1	No	No
EDAC	Unlimited	Yes	Yes

Customer meta-database background

Relational database data duplicated on a directory service.



Customer meta-database specifications



o=Enterprise
Name assigned to reference directory. A directory name is assigned an X500 "o" attribute.

ou=FRGN
Reference value directly underneath reference category in a flat structure. All reference values are assigned an X500 "ou" attribute.

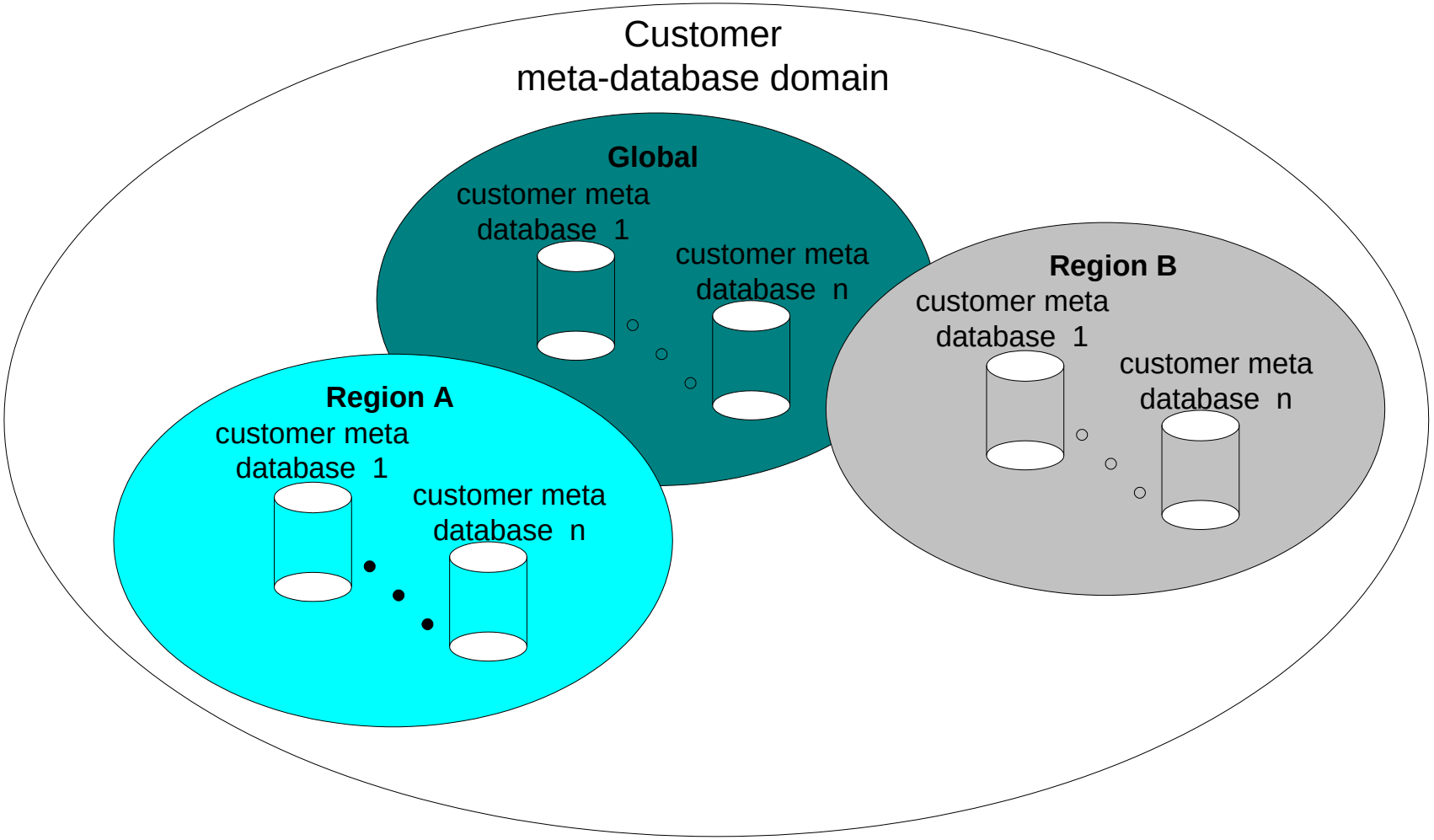
ou=Branch
Reference category directly underneath directory domain name. All reference descriptors are assigned an X500 "ou" attribute.

ou=Secret
Reference value directly underneath Clerance reference category in a hierarchal structure. All reference values are assigned an X500 "ou" attribute.

- Customer meta-database
- LDAP v 3/DSML directory
- X500 class objects
  - organization
  - organizationalUnit
- Scalable
  - unlimited entries
  - modifications allowed
- Structure designation
  - domain
  - reference category
  - values
- Structure
  - flat
  - hierarchal
- Maintained
  - local commands
  - regional commands

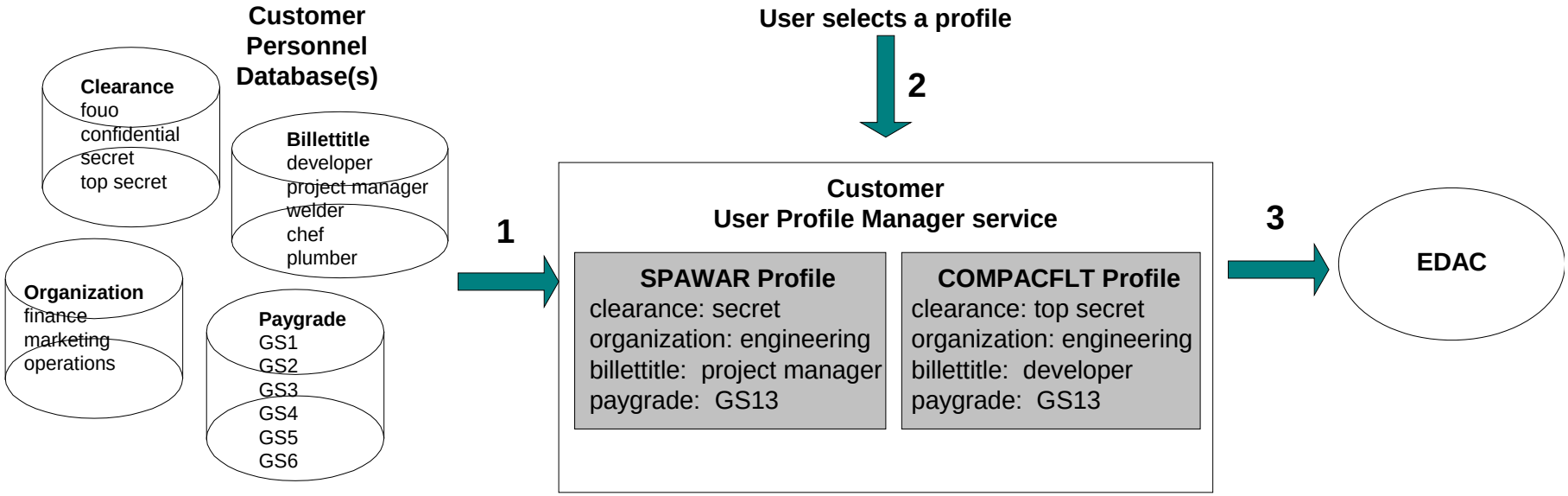
Customer meta-database domain

Domain consist of global and regional directories.



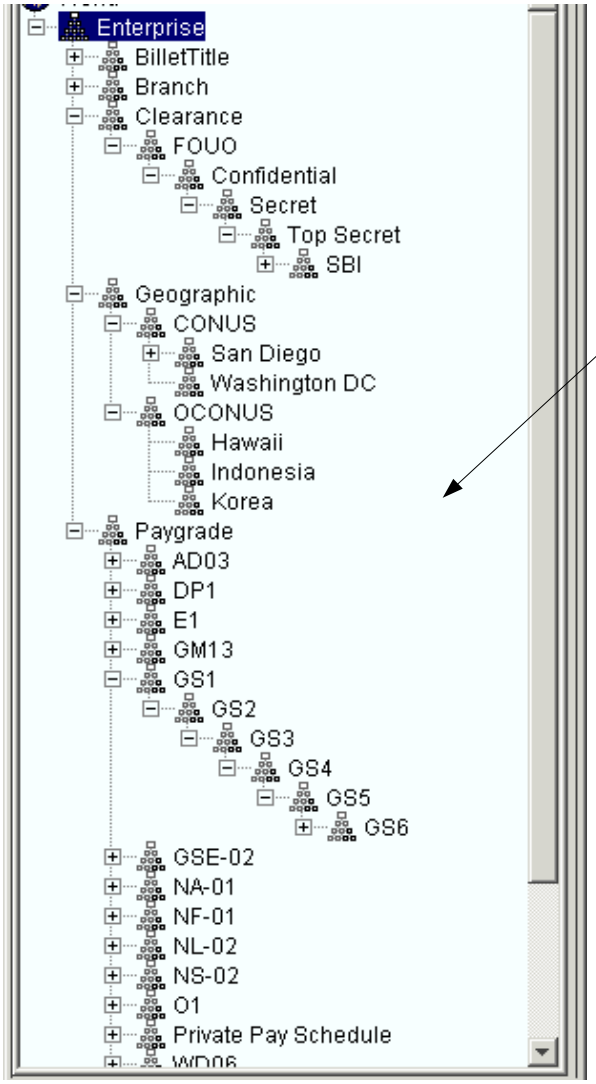
User Profile Manager

User selects a profile to determine resource access.
Mgmt constraints on user profile selections



How the EDAC works

Customer Meta-Database



RBAC Condition Manager

Step 1:
Resource manager establishes a set of conditions to access a resource.

These set of conditions represent a **resource profile.**

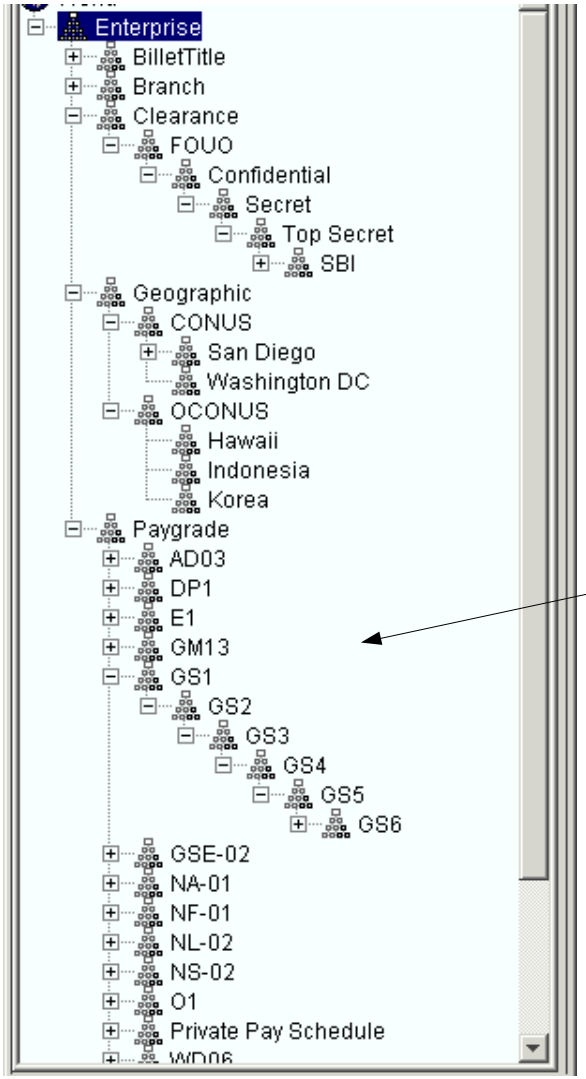
Resource Profile

- ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
- ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise

RBAC Resource Directory

How the EDAC works

Customer Meta-Database



Customer User Profile Manager Interface

Step 2:
An effective RBAC requires real-time creation of user profile(s) from authoritative data source(s).

Structure Format Service

Customer Personnel Database

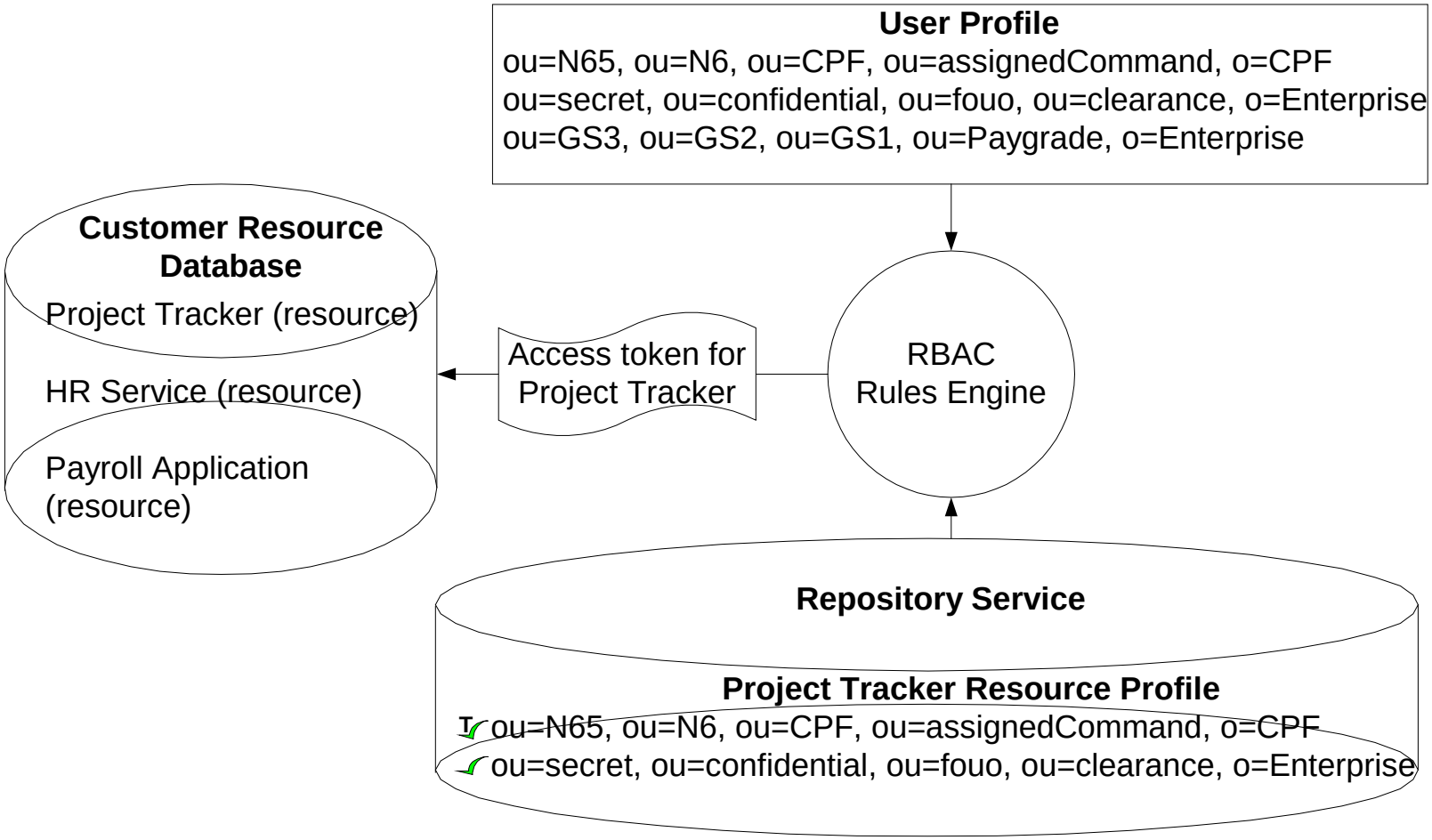
Reference Categories	Attributes
assignedCommand	N65
clearance	Secret
paygrade	GS3

User Profile

ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise
ou=GS3, ou=GS2, ou=GS1, ou=Paygrade, o=Enterprise

How the EDAC works

Step 3:
The RBAC Rules Engine compares User and Resource Profiles to determine resource access.

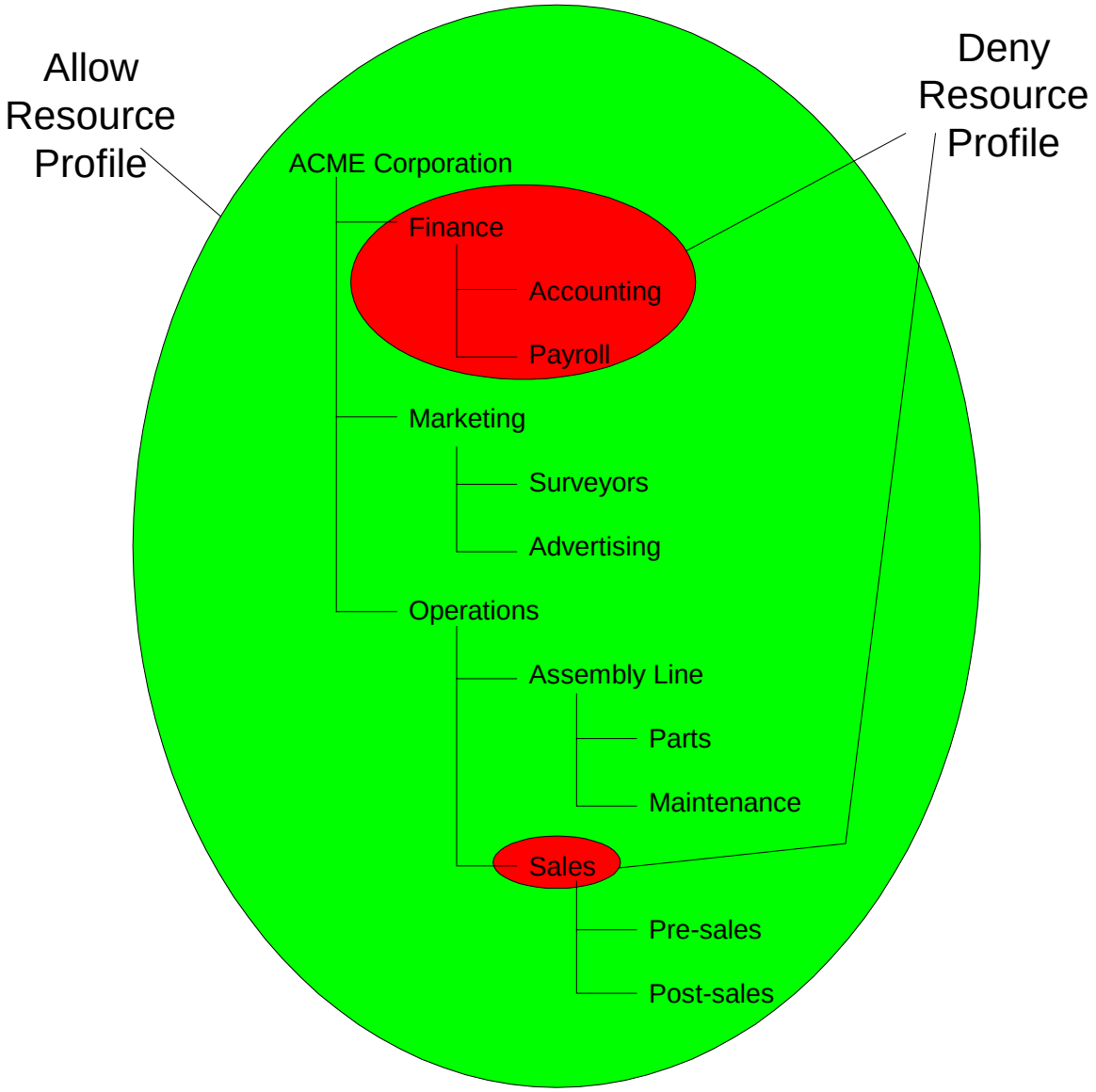


EDAC – Resource profiles

Resource Roles for Project Tracker	Resource Profiles		
Guest	CPF Guest T COMPACFLT	CSP Guest T COMSUBPAC DoD	CNR Guests T COMNAVREG Tuesdays 1700 -2300
User Mon & Thurs 0800 -1300	CPF N6 Users T CPF N6 T GS12	Deny Contr Users T CPF N6 Secret CONTR	
Administrator	CPF Admin CPF N65 T TS	Deny CPF N65 Admin T CPF N65 CONTR Mon & Thurs 0800 -1300	

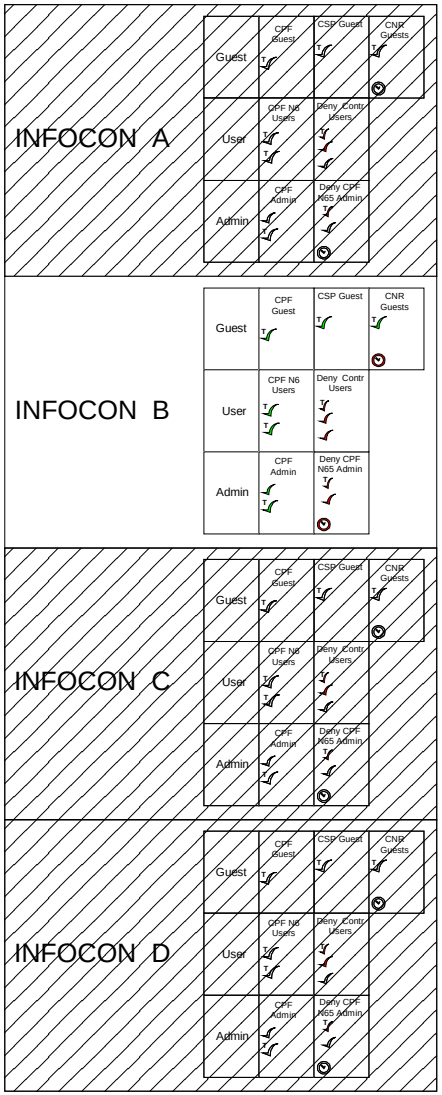
- Resource roles
- Allow & Deny profiles
- Exact and subtree conditions
- Time constraints

EDAC – Resource profiles

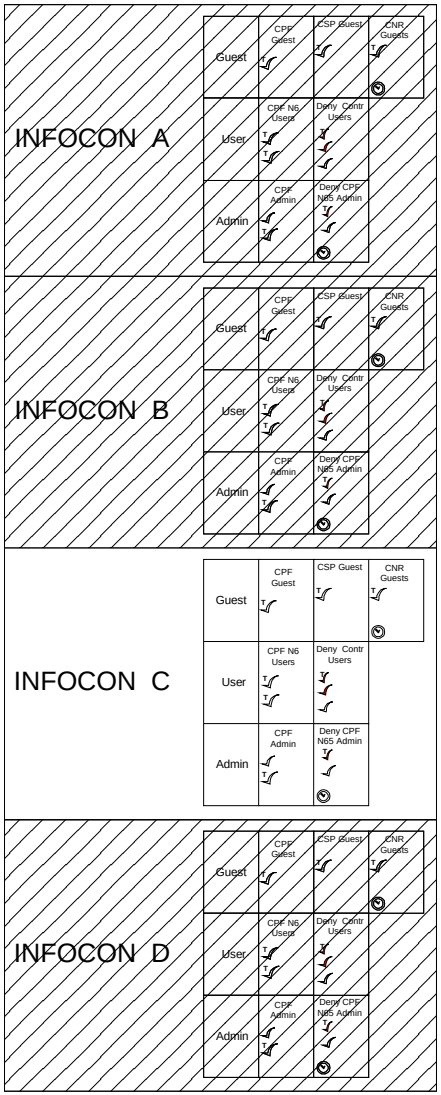


EDAC – Security levels

During INFOCON B



During INFOCON C



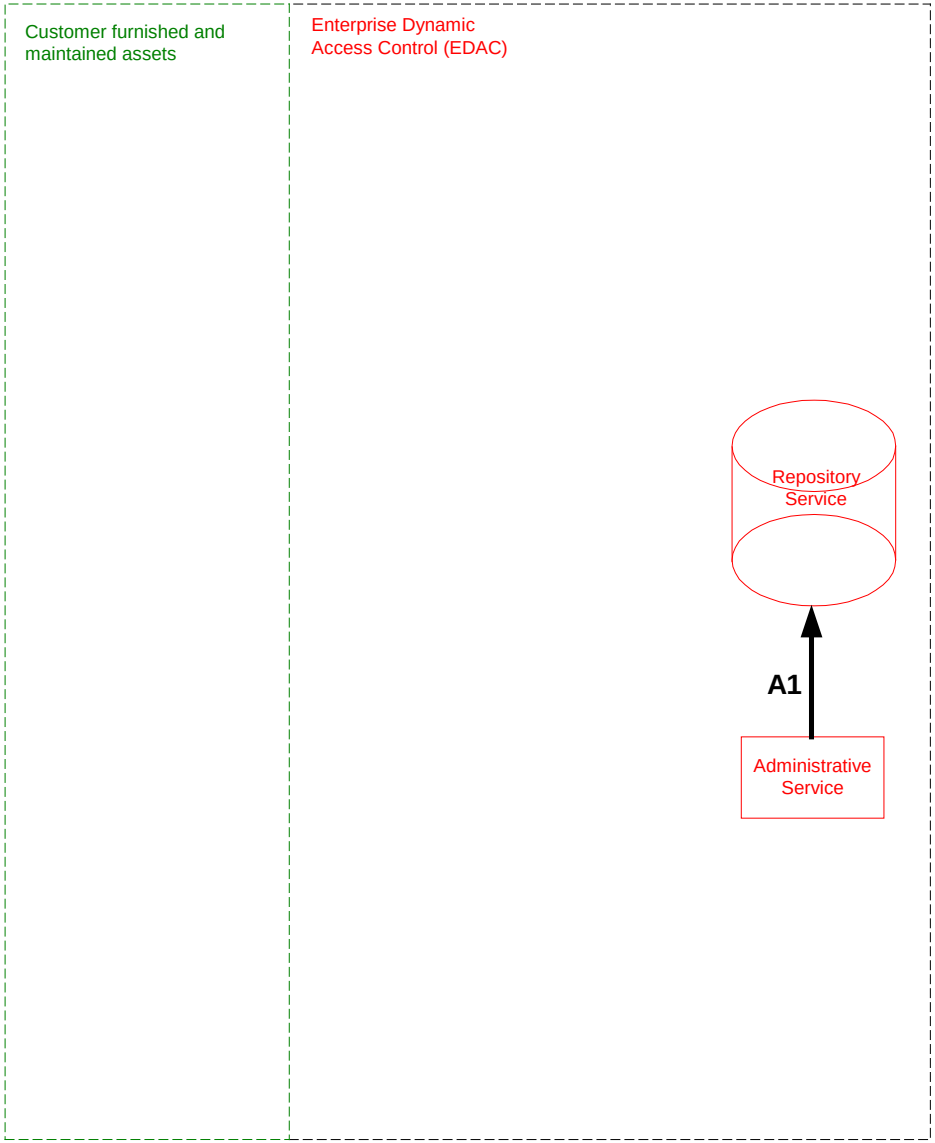
- Pre-configure conditions under each security level.
- RBAC Rules Engine evaluates only conditions for prevailing security level.

EDAC – Model

EDAC standard initiative:

- Interchangeable modular access control components
- Minimum salient features
- Protocol between components
- Standard tie-ins between customer assets and access control system

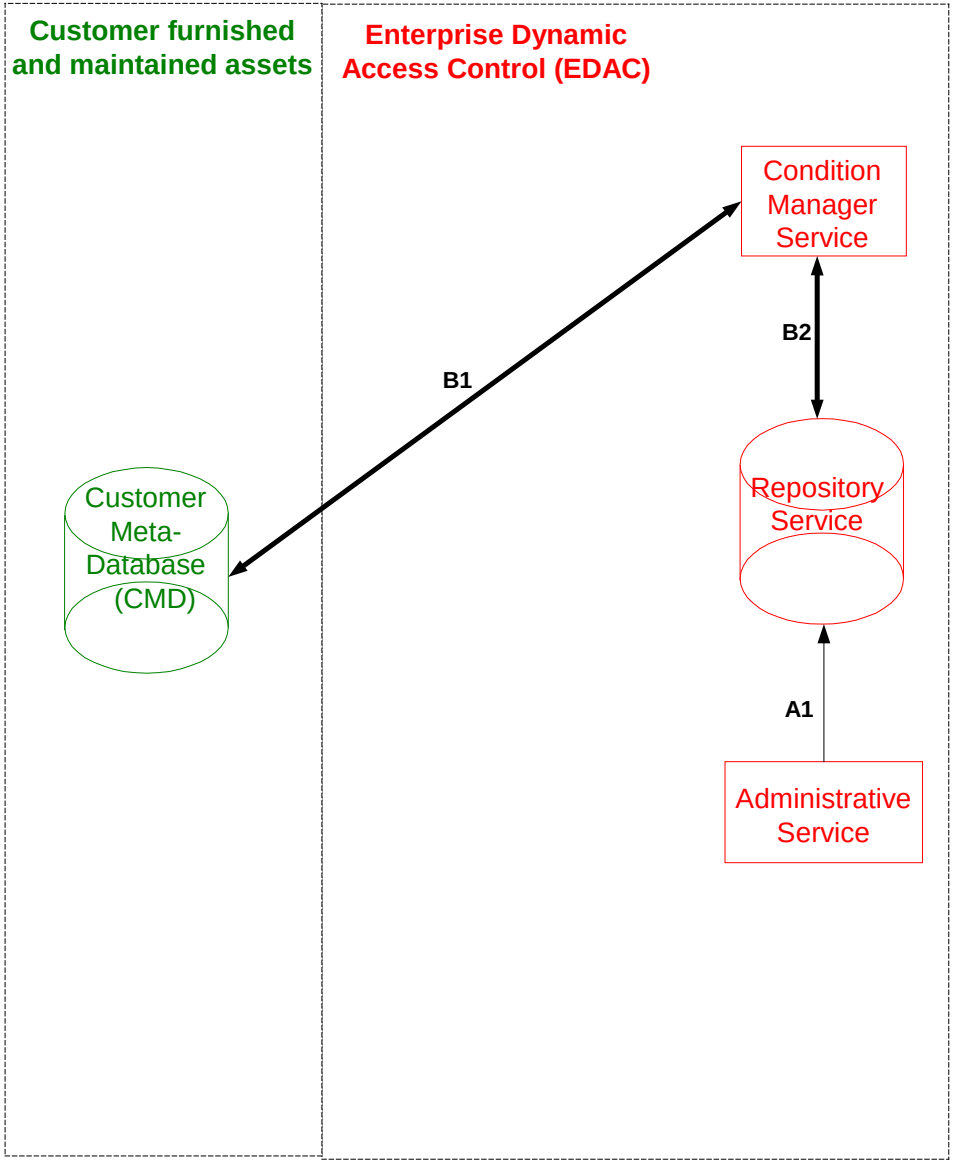
EDAC - Model



EDAC Process

(A) Administrative Service - establishes resource containers, CMD referrals, RM accounts.

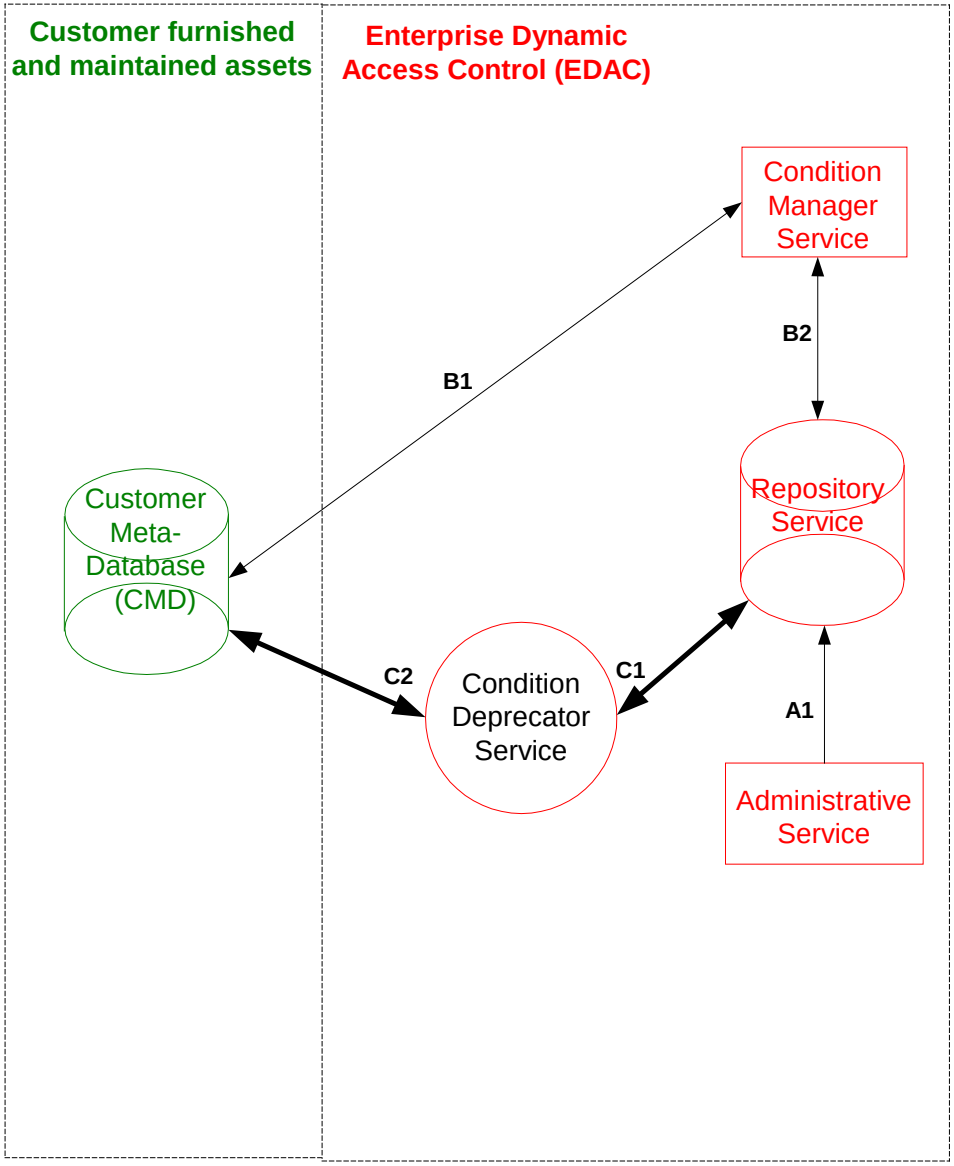
EDAC - Model



EDAC Process

(B) Condition manager Service - Establishes and edits conditions to access resources.

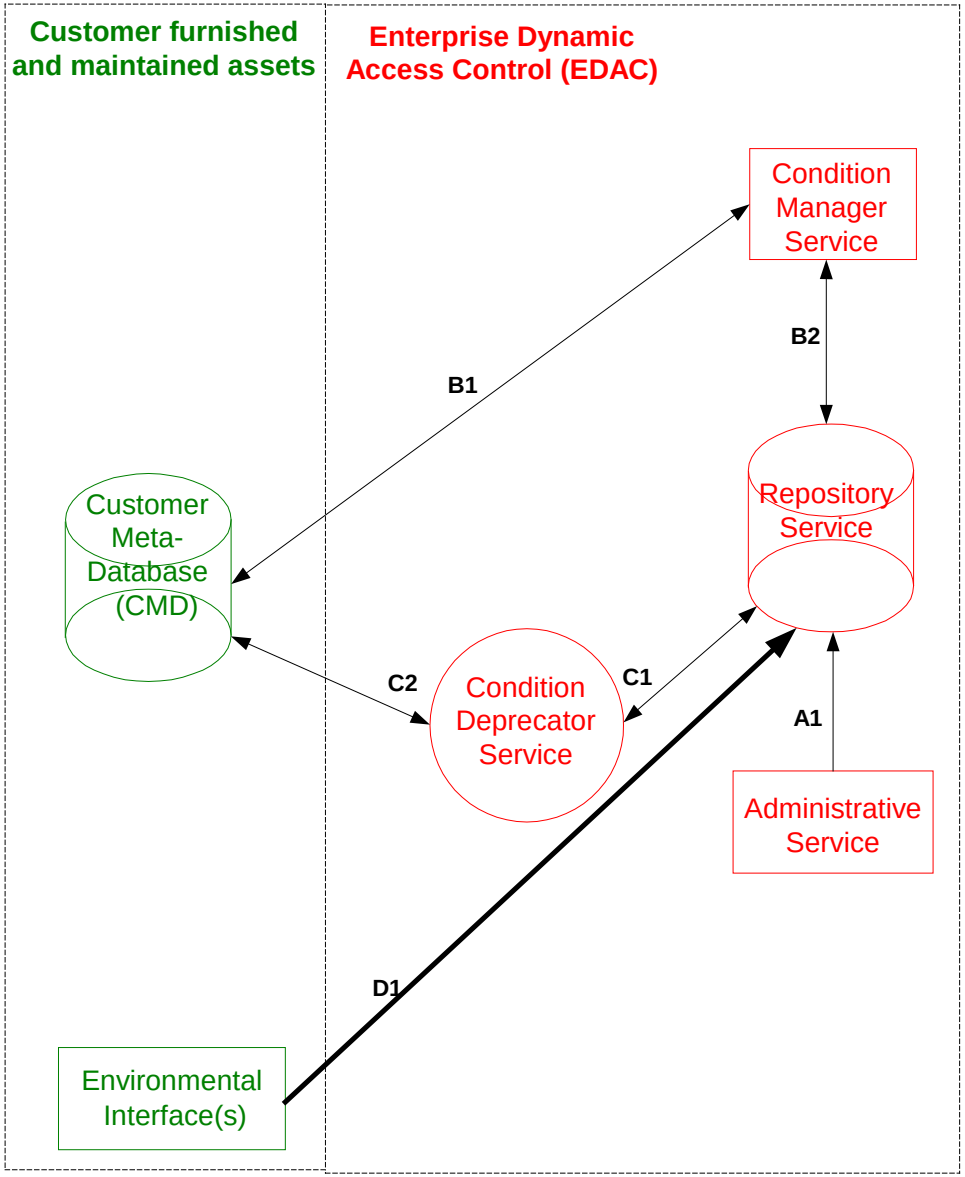
EDAC - Model



EDAC Process

(C) Condition deprecator Service - listens for CMD content changes and flags unmatched or unreachable conditions.

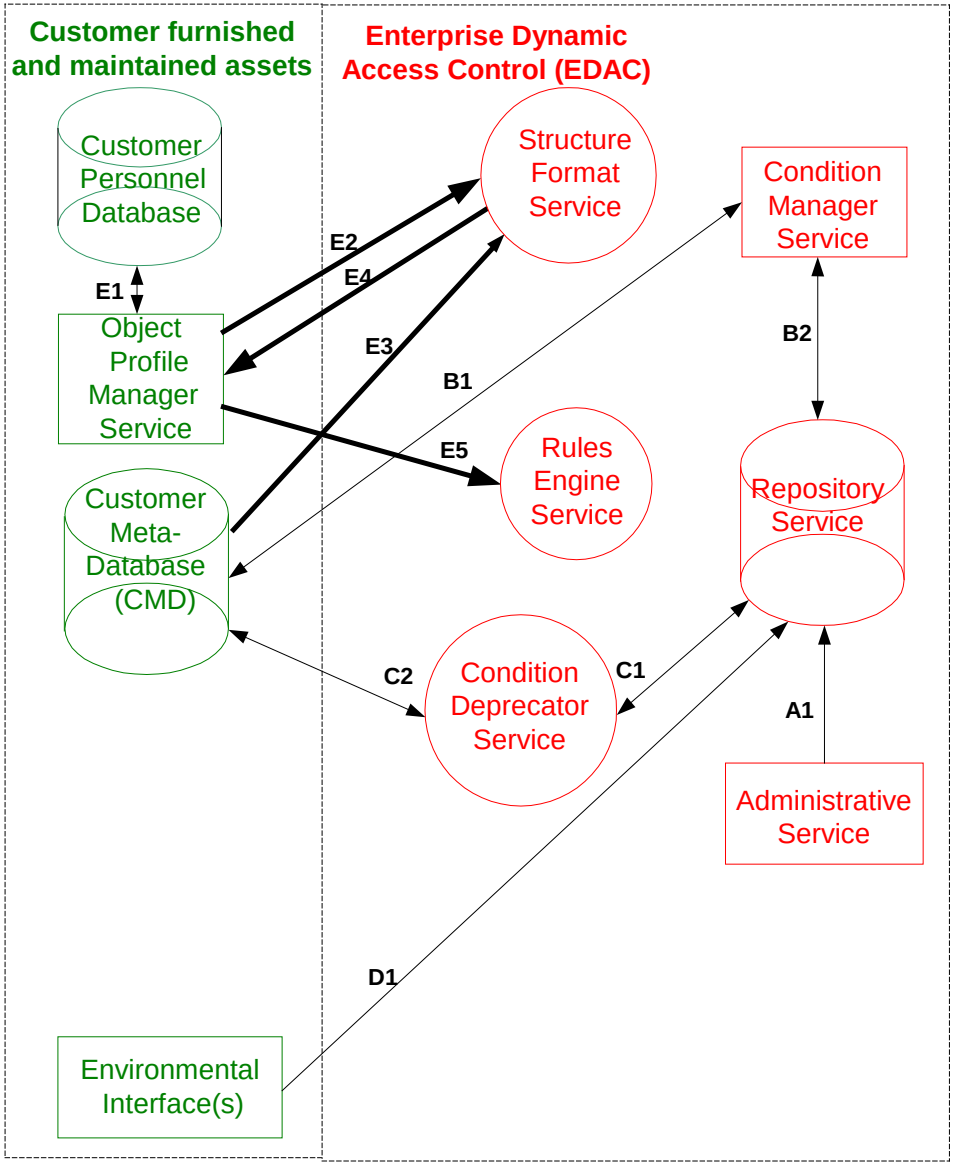
EDAC - Model



EDAC Process

(D) Customer Environmental Interface - furnishes environmental updates.

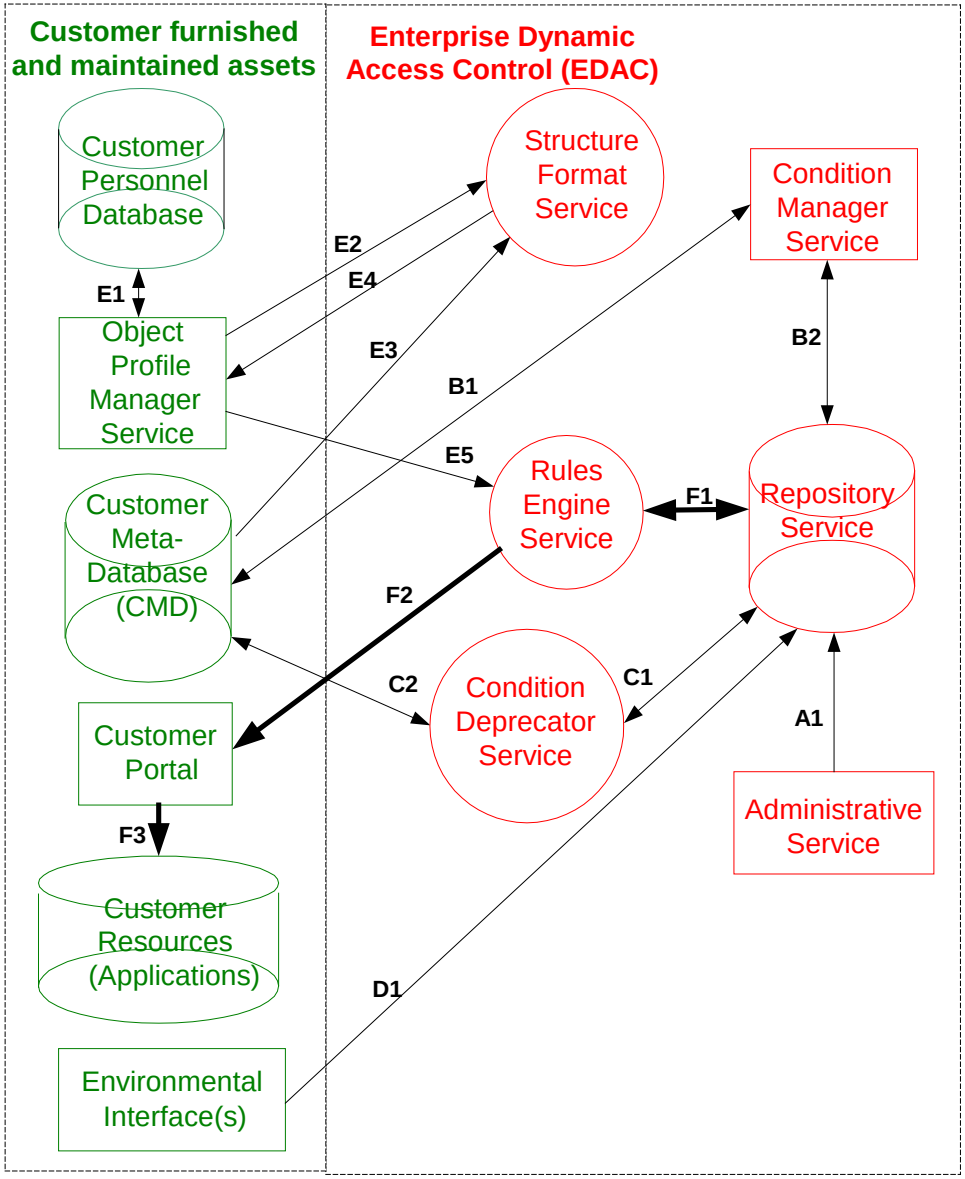
EDAC - Model



EDAC Process

(E) Customer Object profile manager Service - object characteristic compilation, selection and formatting.

EDAC - Model



EDAC Process

(F) Rules Engine Service - evaluates object and conditions to determine object resource access.

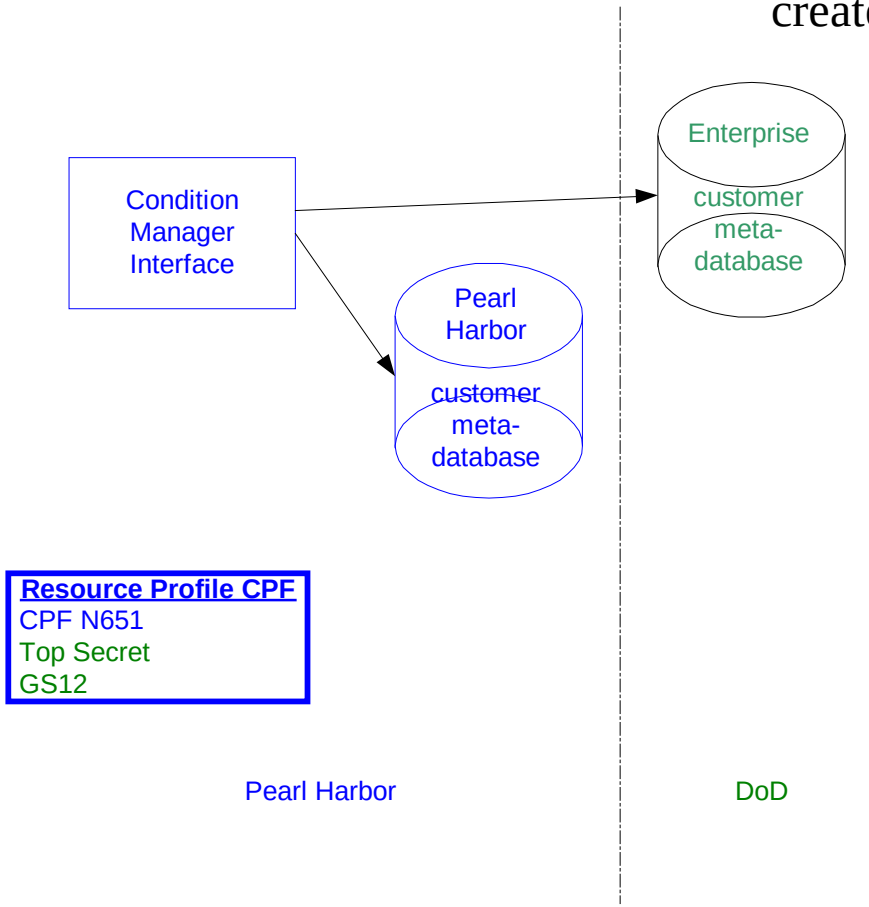
EDAC – Interoperability

EDAC interoperable among regions:

- Set conditional access for remote users
- Domain customer meta-databases

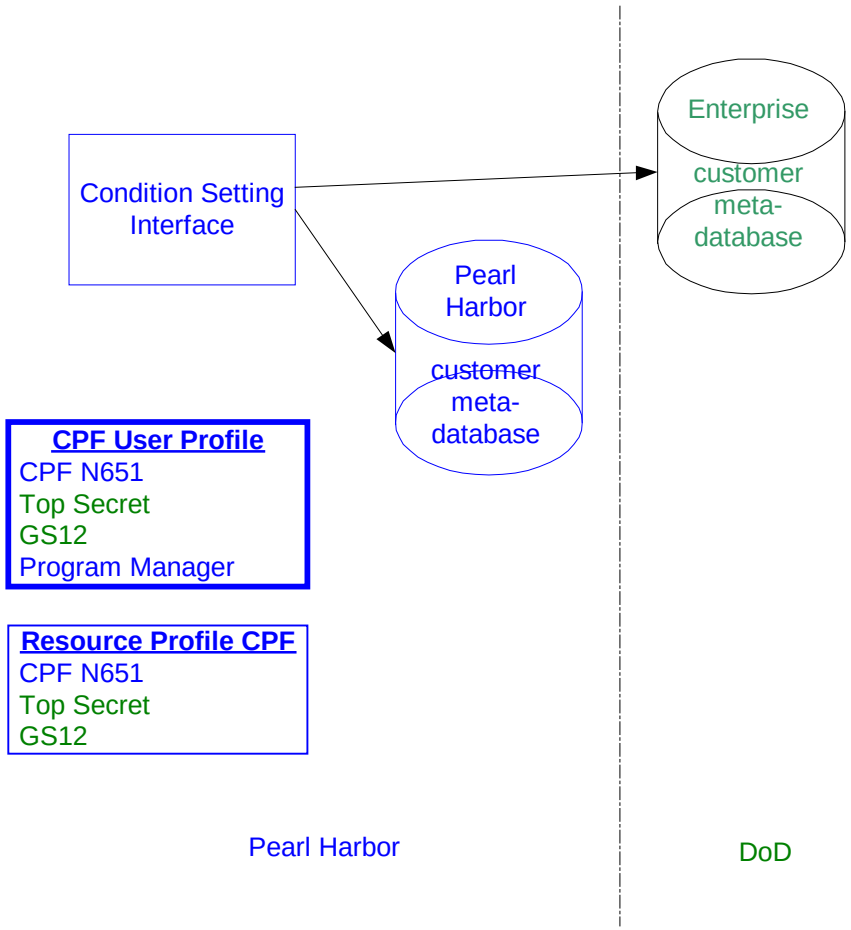
EDAC - Interoperability

Pearl Harbor: resource profile created for local resource access.

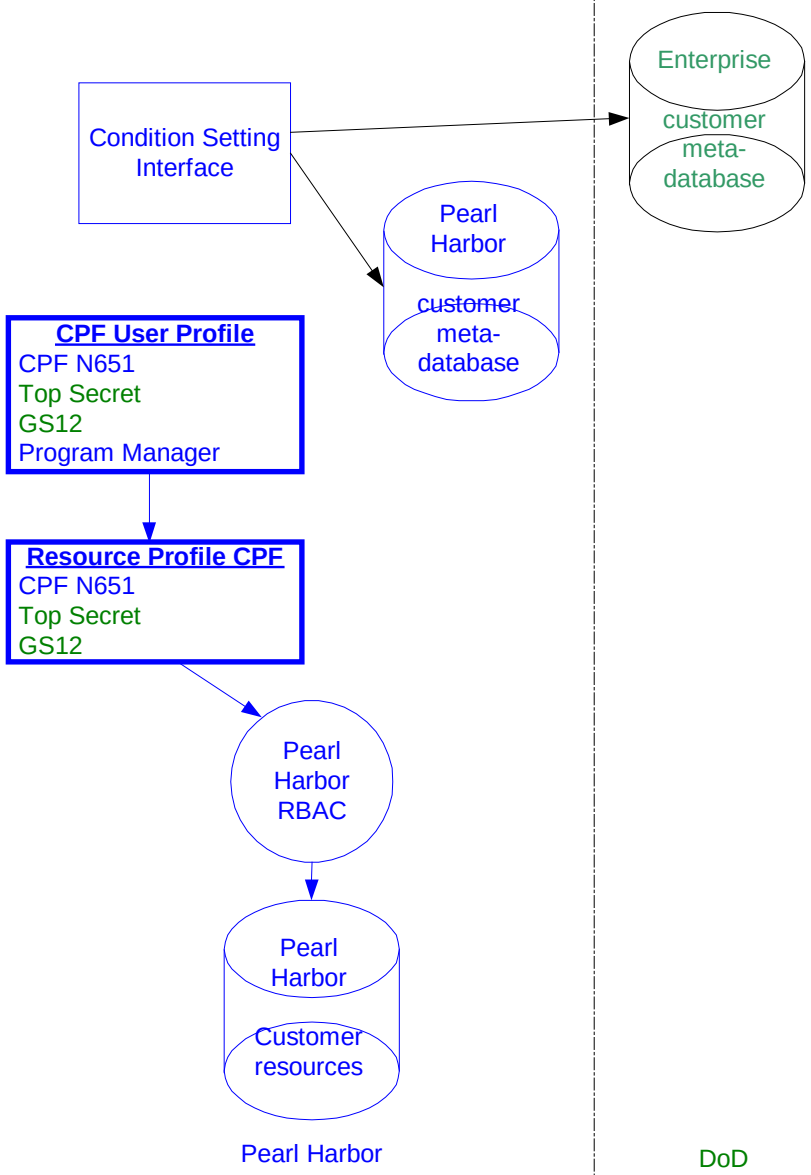


EDAC - Interoperability

Pearl Harbor: local user profile is generated to access a local resource.

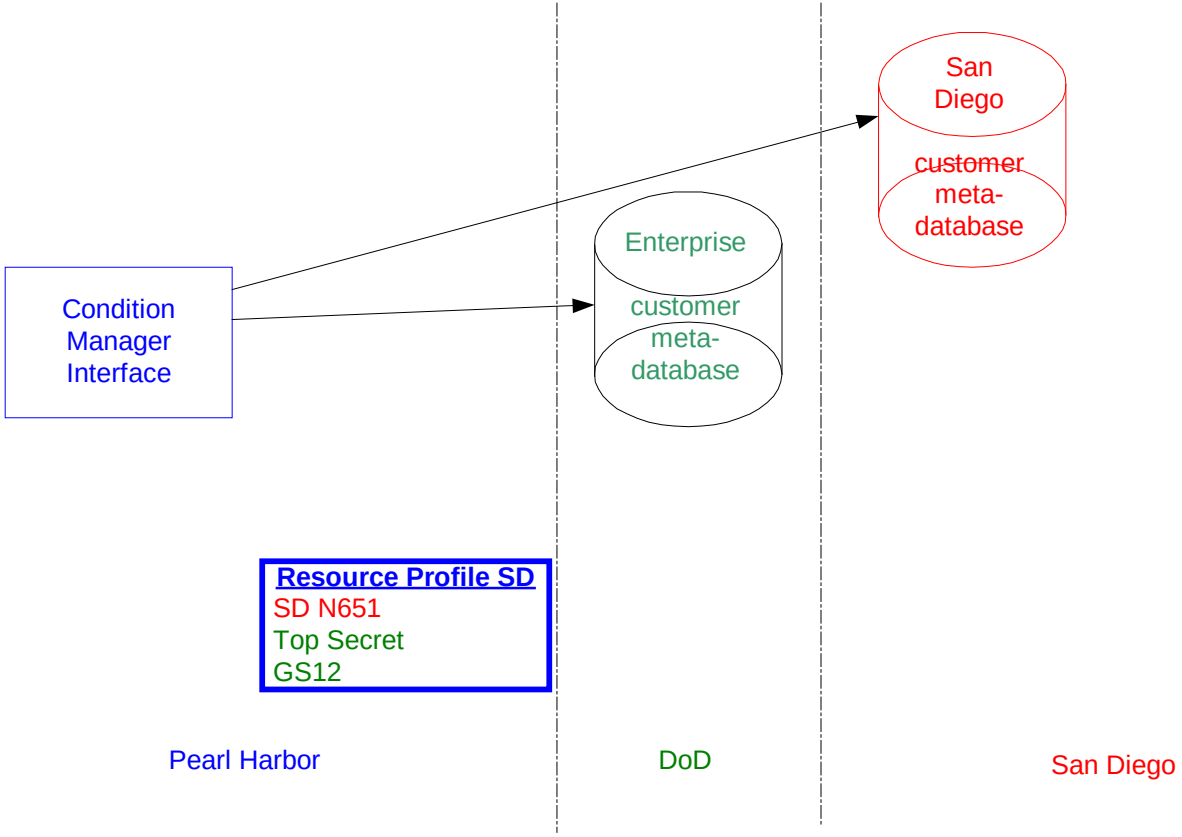


EDAC - Interoperability



Pearl Harbor: user and resource profiles are evaluated by rules engine to determine local resource access.

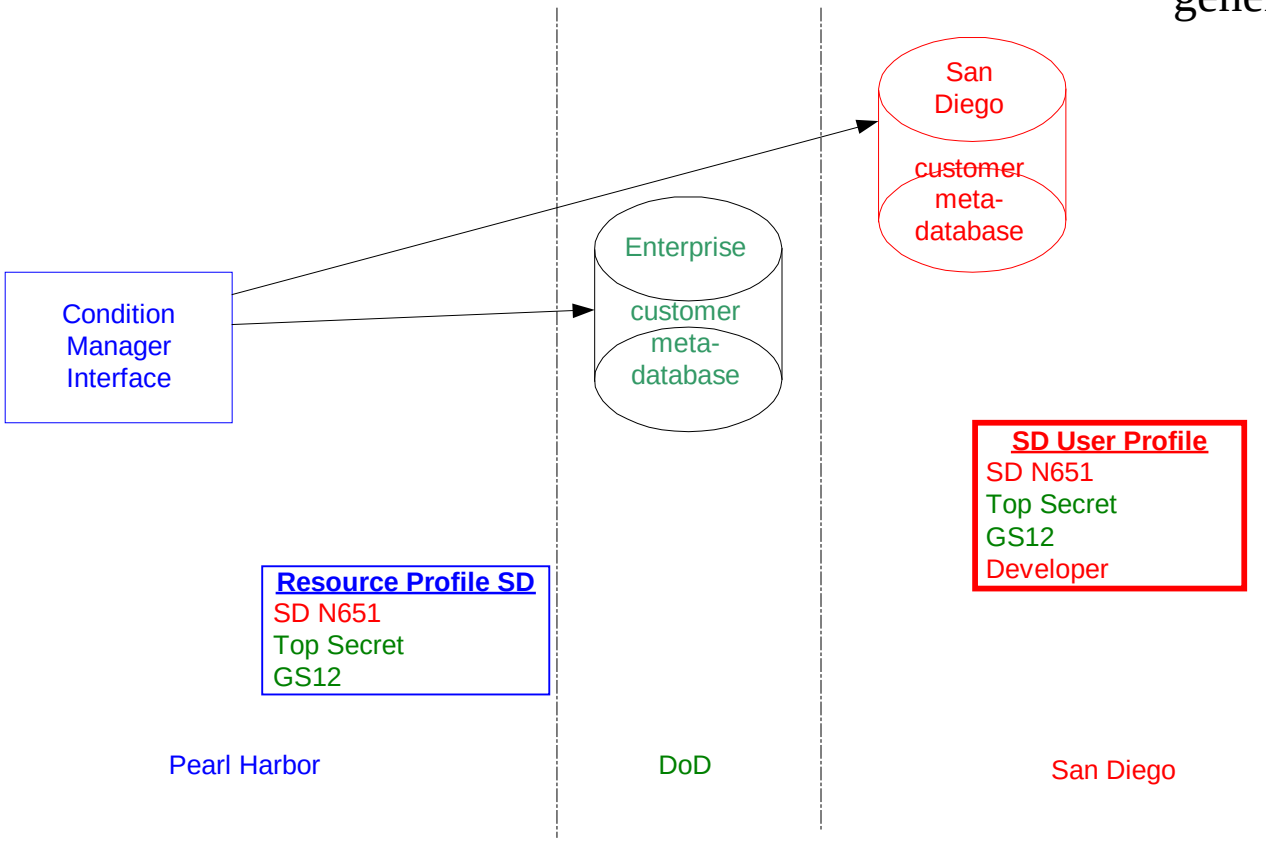
EDAC - Interoperability



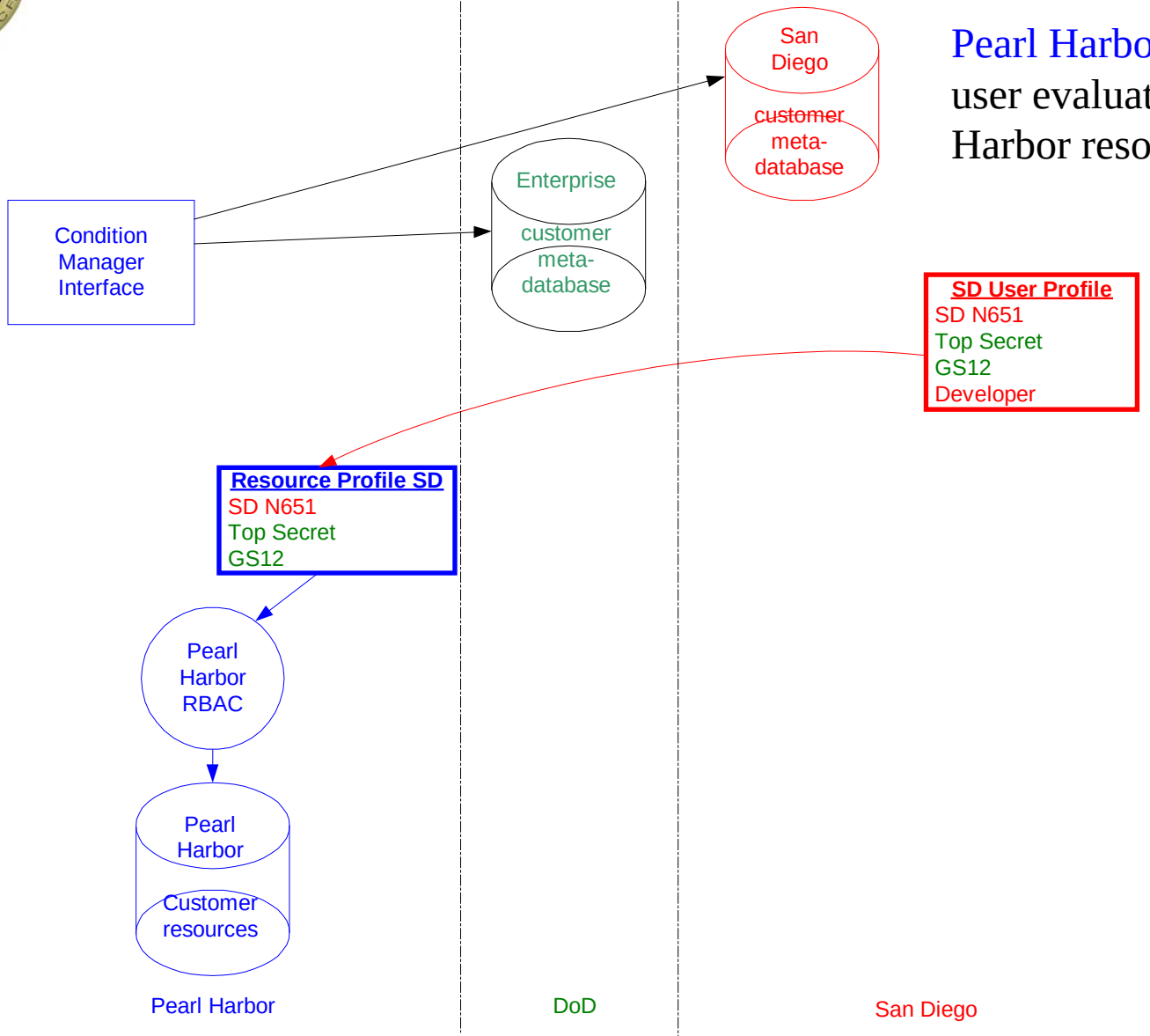
Pearl Harbor: A resource profile to allow remote users access to local resources.

EDAC - Interoperability

San Diego: user profile generated.

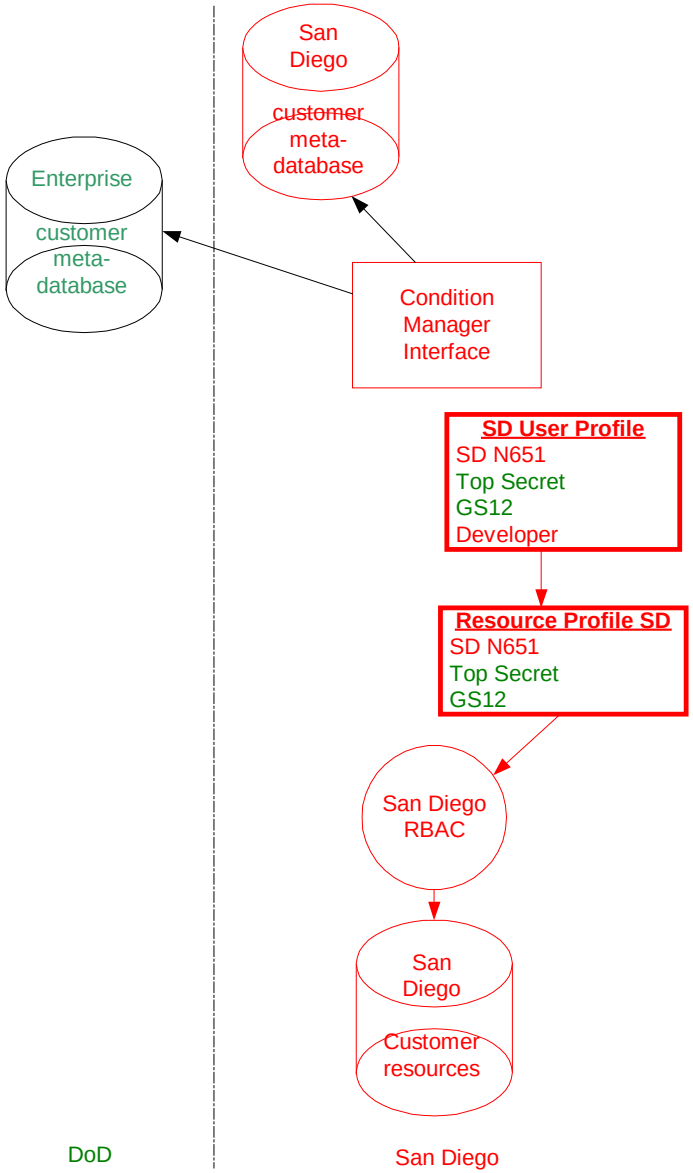


EDAC - Interoperability



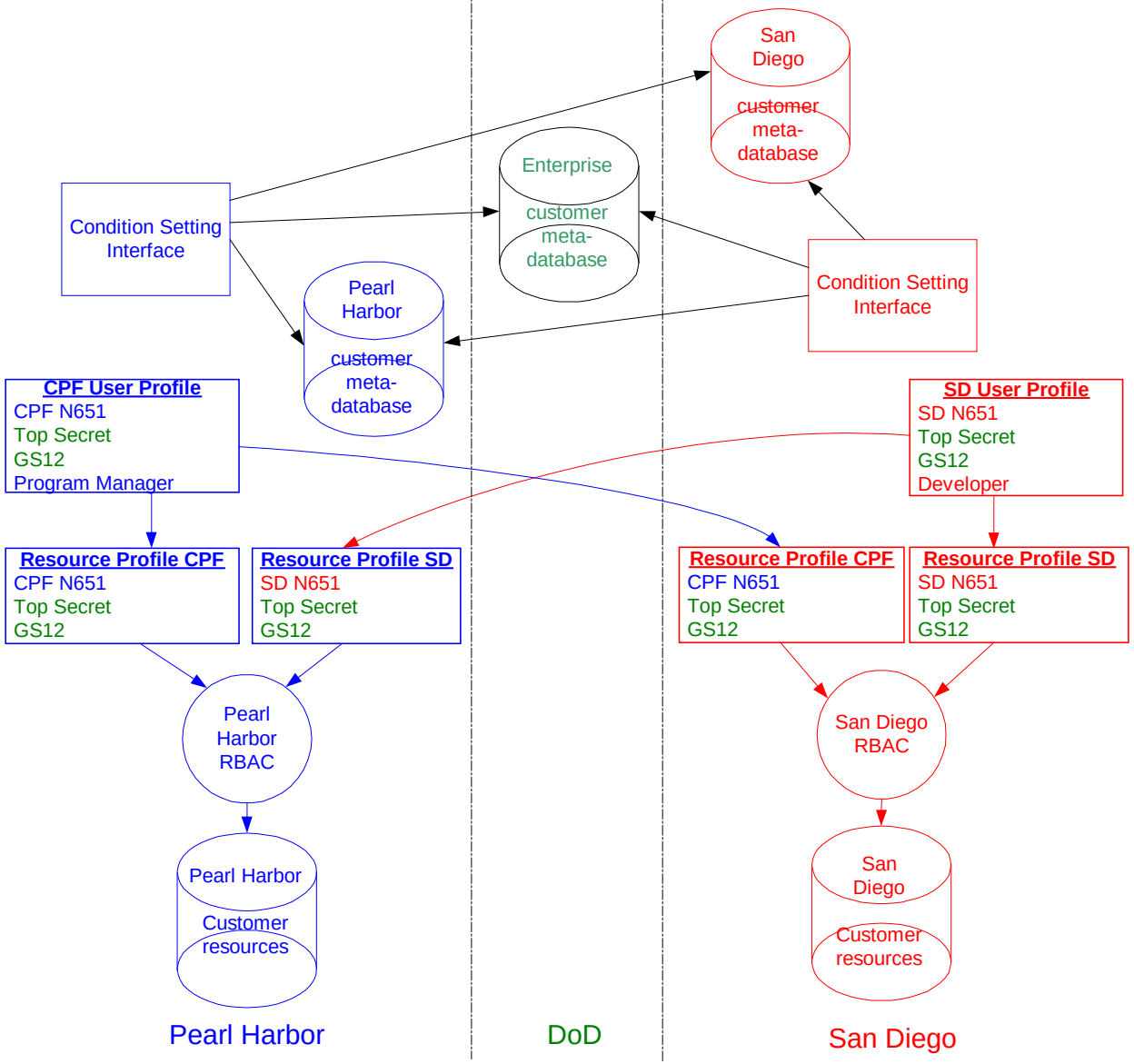
Pearl Harbor: San Diego user evaluated for Pearl Harbor resource access.

EDAC - Interoperability



San Diego: same user evaluated for San Diego resource access.

EDAC – Interoperability



San Diego, CA 92152-5001