COMPACFLT - EDAC

Enterprise Dynamic Access Control (EDAC)

Point of Contact:

Richard Fernandez
(808) 474-9270

Approved for public release; distribution is unlimited.

Report Documentation Page		Form Approved OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JUN 2005**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2005**
4. TITLE AND SUBTITLE **Enterprise Dynamic Access Control (EDAC) (Briefing Charts)**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Space and Naval Warfare Systems Center San Diego,Code 20012,San Diego,CA,92152**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES **The original document contains color images.**		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**40**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

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
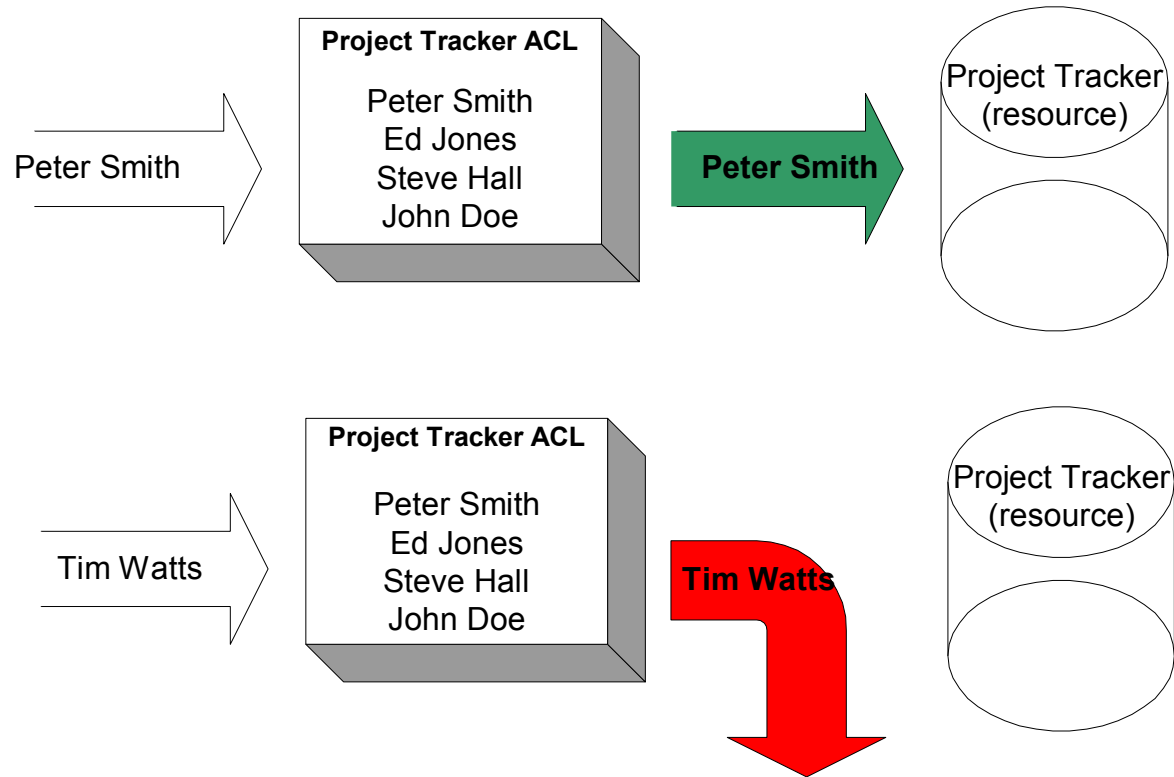- Customer furnished and maintained assets
- How it works
- Product overview
- Interoperability
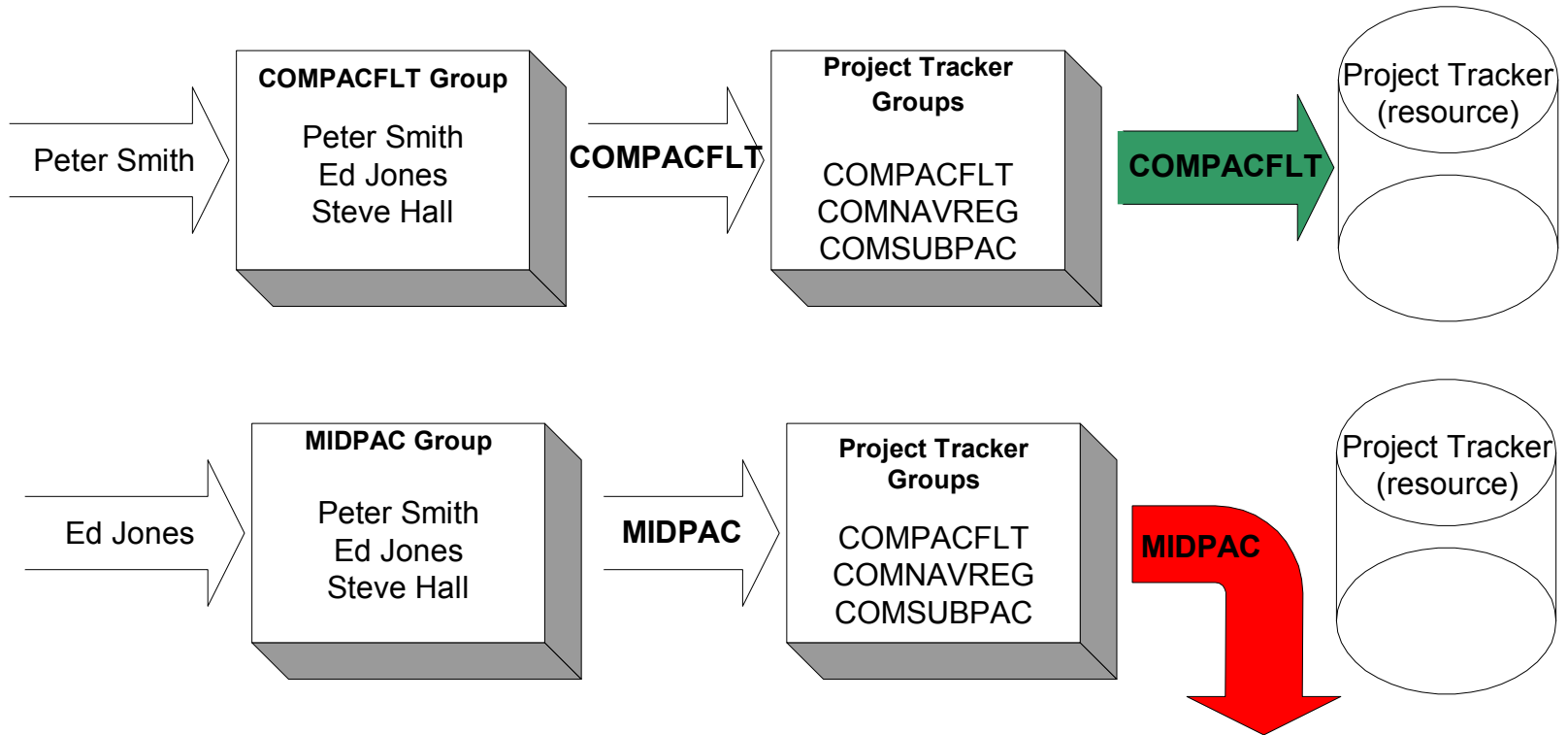
Access Control Lists (ACL)

User name or unique identifier associates access to resources

Project Tracker ACL

Peter Smith
Ed Jones
Steve Hall
John Doe

Peter Smith → **Peter Smith** → Project Tracker (resource)

Project Tracker ACL

Peter Smith
Ed Jones
Steve Hall
John Doe

Tim Watts → **Tim Watts** → Project Tracker (resource)

Groups

User associated to a group and group associated to resources

Peter Smith →

COMPACFLT Group

Peter Smith
Ed Jones
Steve Hall

→ **COMPACFLT** →

Project Tracker Groups

COMPACFLT
COMNAVREG
COMSUBPAC

→ **COMPACFLT** →

Project Tracker
(resource)

Ed Jones →

MIDPAC Group

Peter Smith
Ed Jones
Steve Hall

→ **MIDPAC** →

Project Tracker Groups

COMPACFLT
COMNAVREG
COMSUBPAC

MIDPAC

Project Tracker
(resource)

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
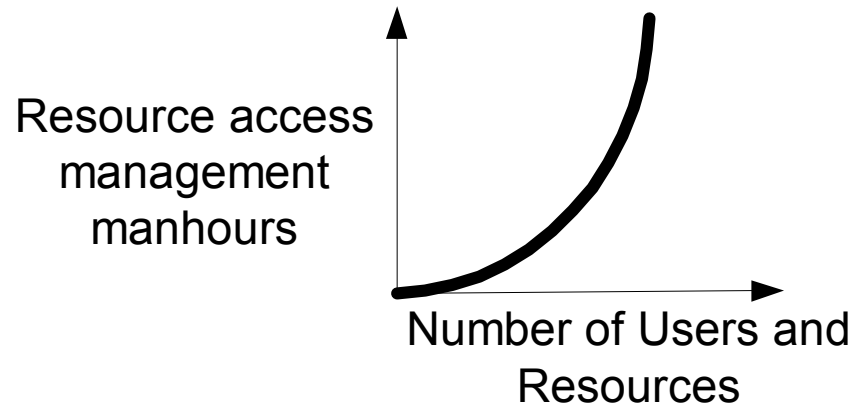- Change in job title
- Job promotion

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

Resource access management manhours (vertical axis)

Number of Users and Resources (horizontal axis)

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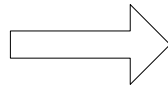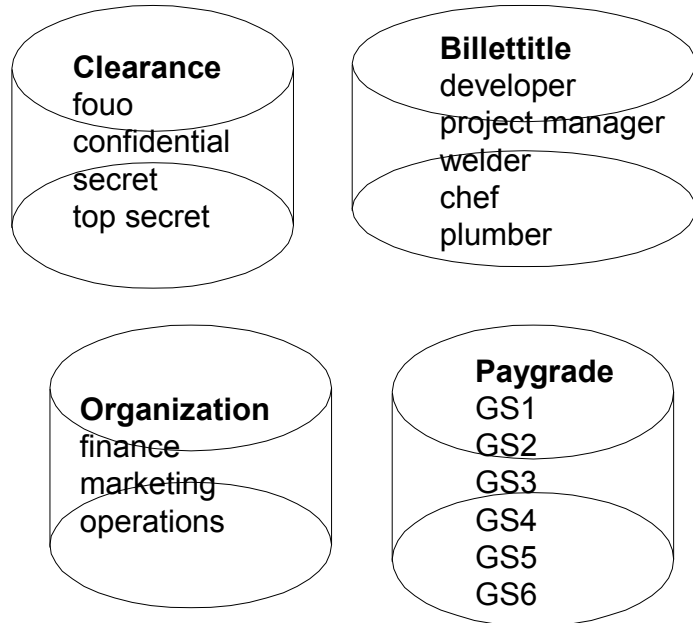
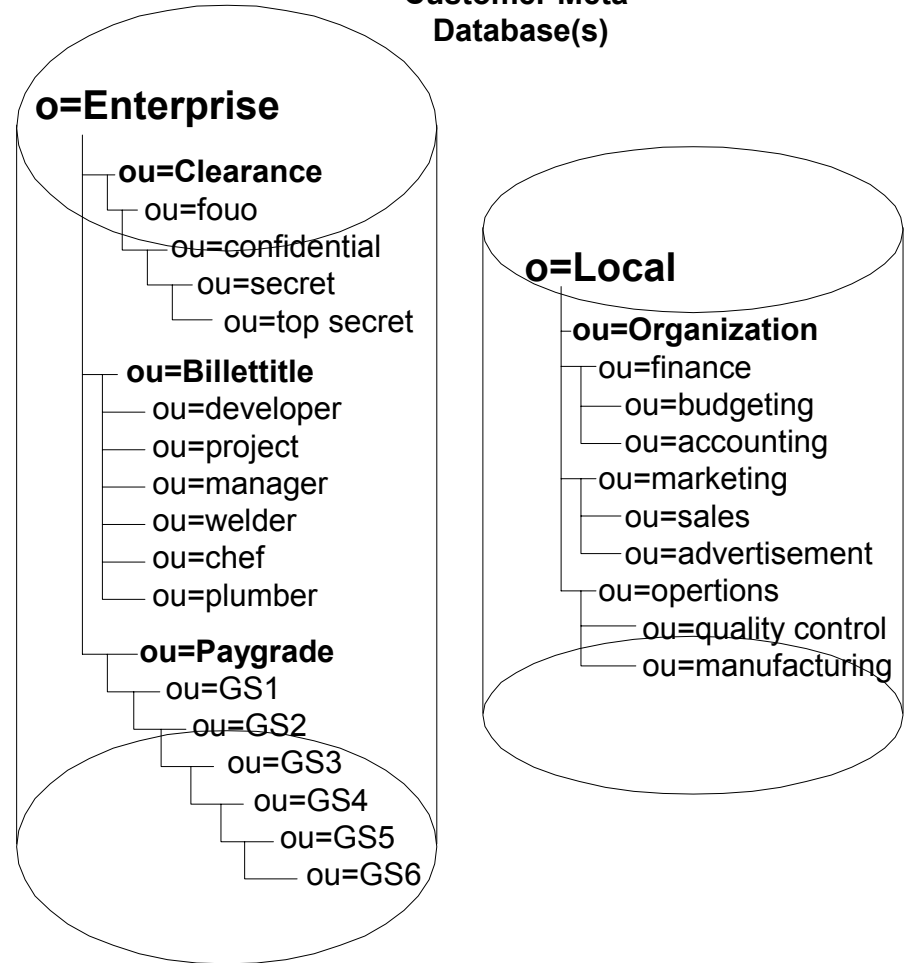|	Simultaneous evaluation of multiple object characteristics & environmentals	Simultaneous evaluation of multiple object characteristic & environmental hierarchies	Real-time detection of object characteristic changes, thus affecting resource access
ACLs	0	No	No
Groups	1	No	No
EDAC	Unlimited	Yes	Yes

Customer meta-database background

Relational database data duplicated on a directory service.
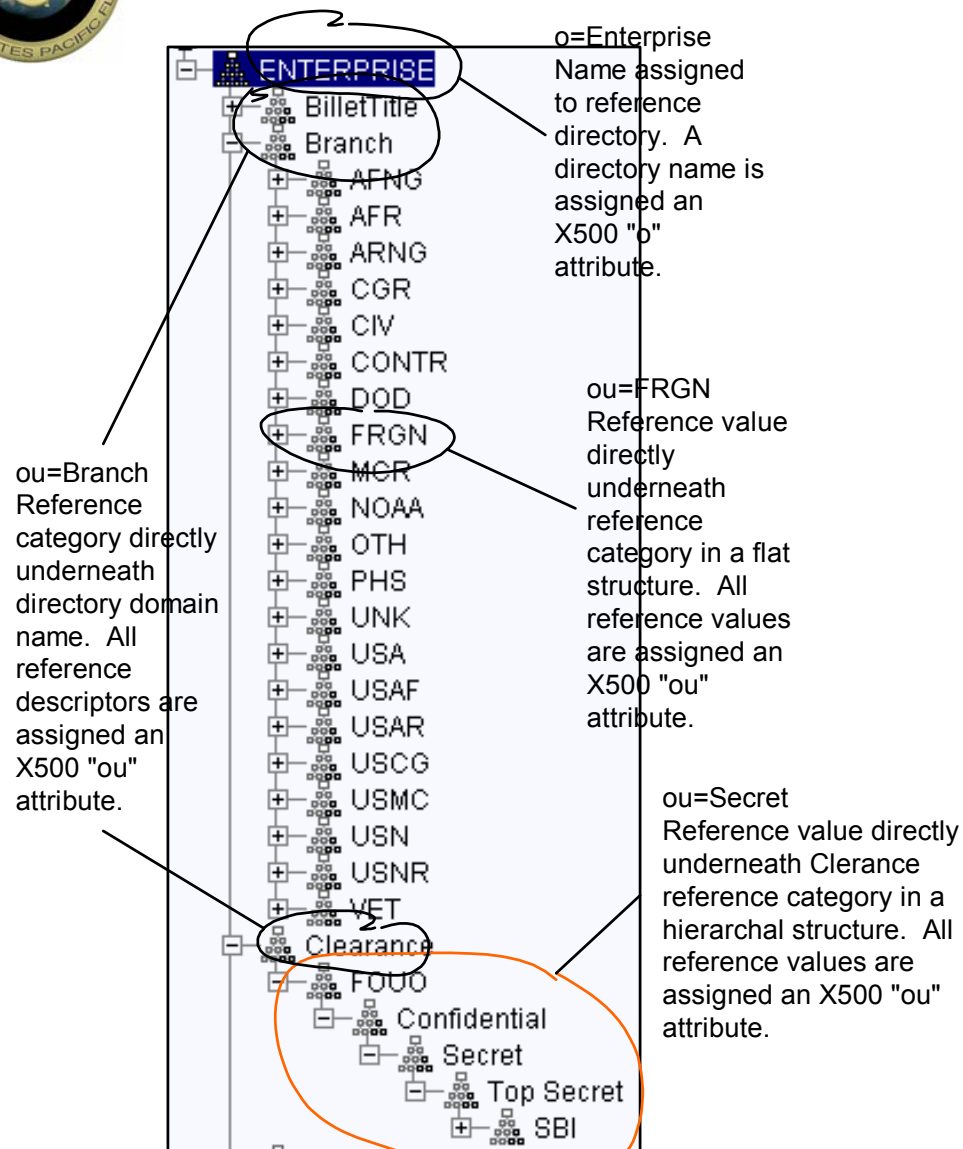
Customer Personnel Database(s)

Customer Meta-Database(s)

Clearance
fouo
confidential
secret
top secret

Billettitle
developer
project manager
welder
chef
plumber

Organization
finance
marketing
operations

Paygrade
GS1
GS2
GS3
GS4
GS5
GS6

o=Enterprise

ou=Clearance
ou=fouo
ou=confidential
ou=secret
ou=top secret

ou=Billettitle
ou=developer
ou=project
ou=manager
ou=welder
ou=chef
ou=plumber

ou=Paygrade
ou=GS1
ou=GS2
ou=GS3
ou=GS4
ou=GS5
ou=GS6

o=Local

ou=Organization
ou=finance
ou=budgeting
ou=accounting
ou=marketing
ou=sales
ou=advertisement
ou=opertions
ou=quality control
ou=manufacturing

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
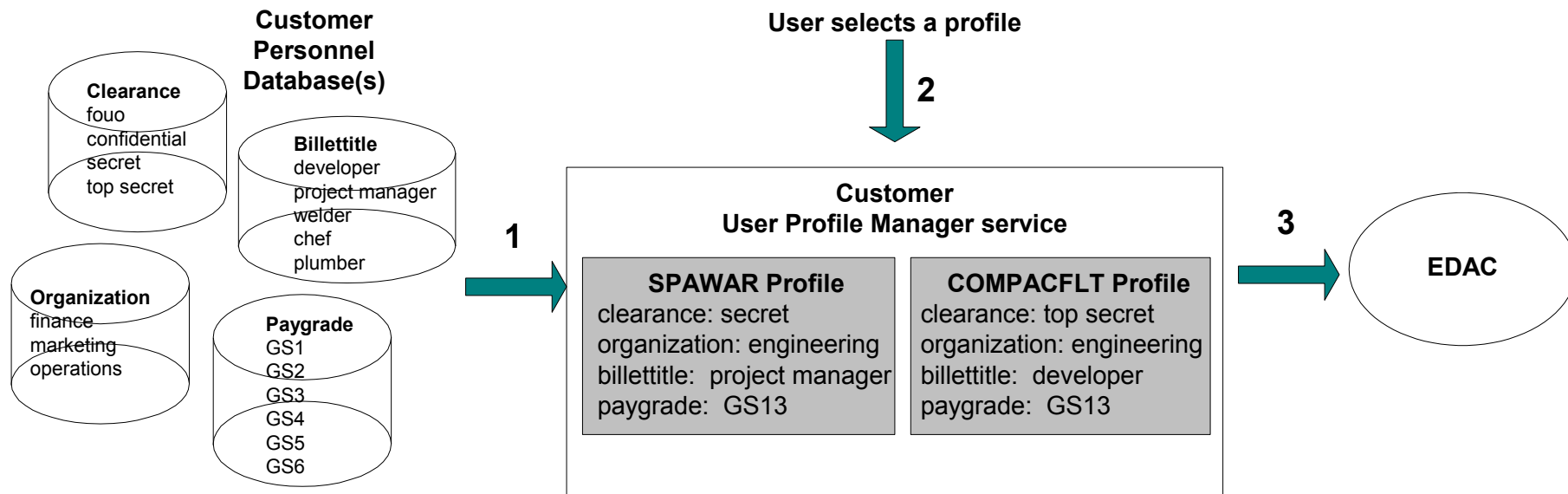 - regional commands

Customer meta-database domain

Domain consist of global and regional directories.
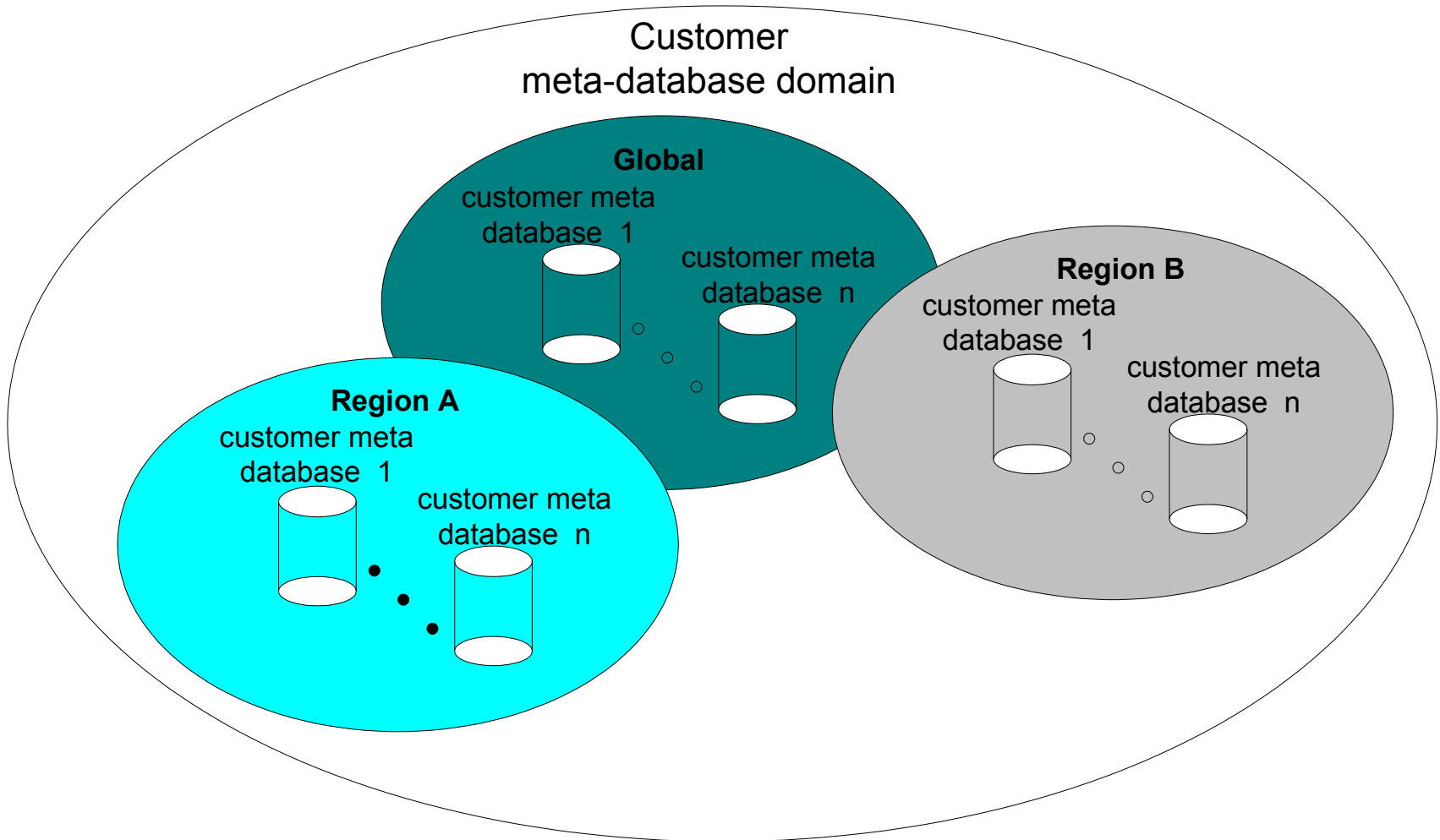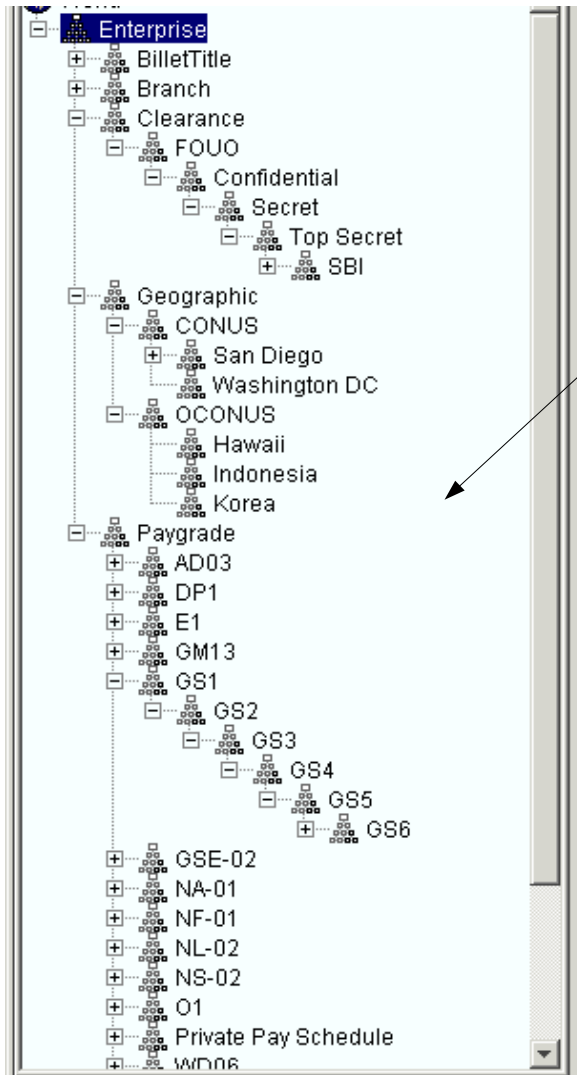
User Profile Manager

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

Customer Personnel Database(s)

Clearance
fouo
confidential
secret
top secret

Billettitle
developer
project manager
welder
chef
plumber

Organization
finance
marketing
operations

Paygrade
GS1
GS2
GS3
GS4
GS5
GS6

User selects a profile

2

1

**Customer
User Profile Manager service**

SPAWAR Profile
clearance: secret
organization: engineering
billettitle: project manager
paygrade: GS13

COMPACFLT Profile
clearance: top secret
organization: engineering
billettitle: developer
paygrade: GS13

3
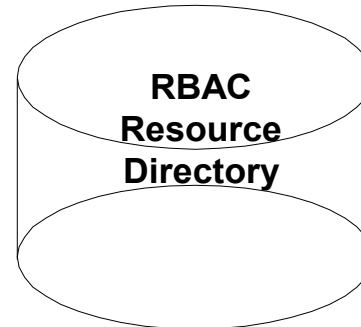
EDAC

How the EDAC works

Customer Meta-Database

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

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

RBAC Condition Manager

Enterprise
- BilletTitle
- Branch
- Clearance
  - FOUO
    - Confidential
      - Secret
        - Top Secret
          - SBI
- Geographic
  - CONUS
    - San Diego
    - Washington DC
  - OCONUS
    - Hawaii
    - Indonesia
    - Korea
- Paygrade
  - AD03
  - DP1
  - E1
  - GM13
  - GS1
    - GS2
      - GS3
        - GS4
          - GS5
            - GS6
  - GSE-02
  - NA-01
  - NF-01
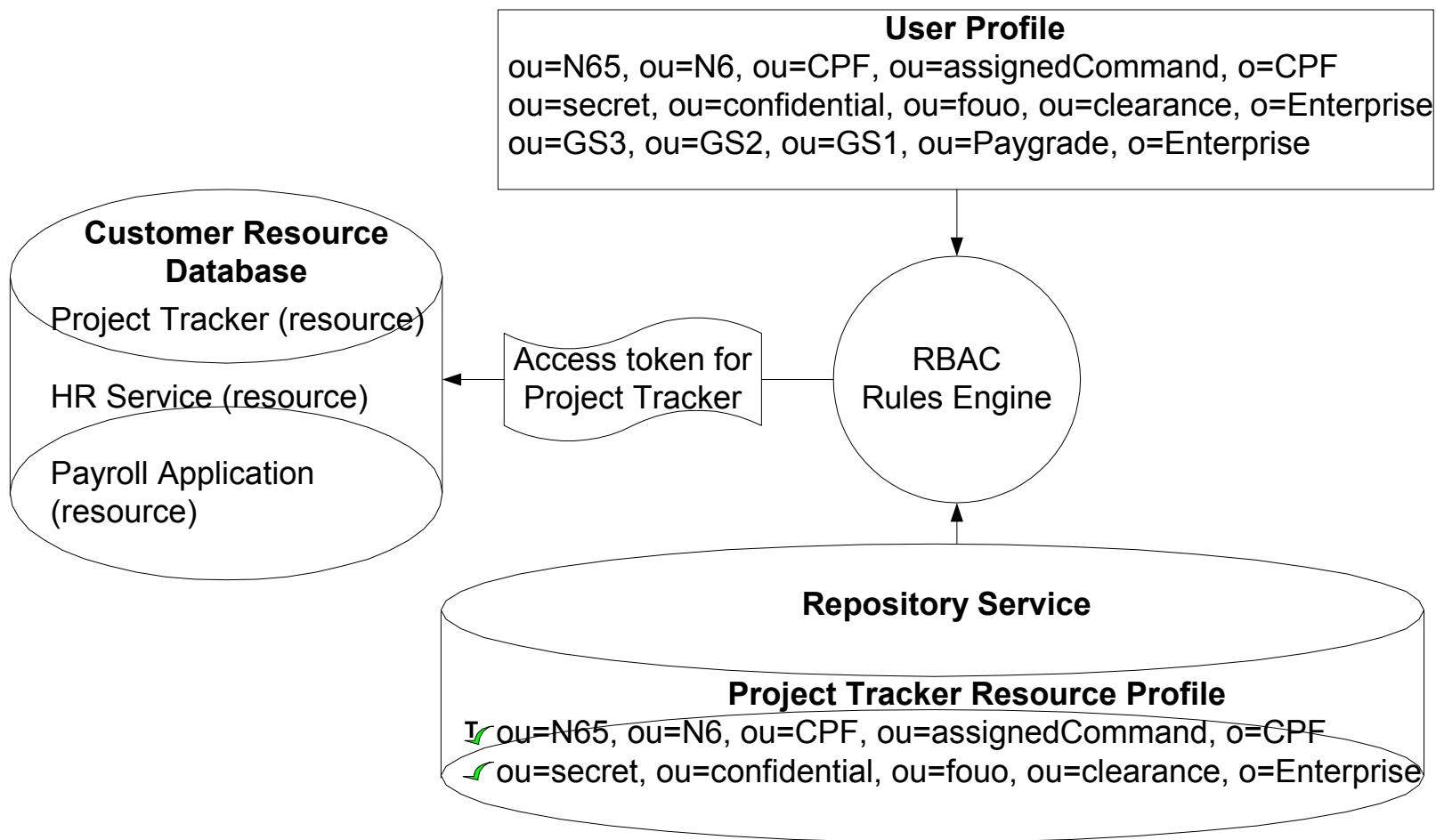 - NL-02
  - NS-02
  - O1
  - Private Pay Schedule
  - WD06

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

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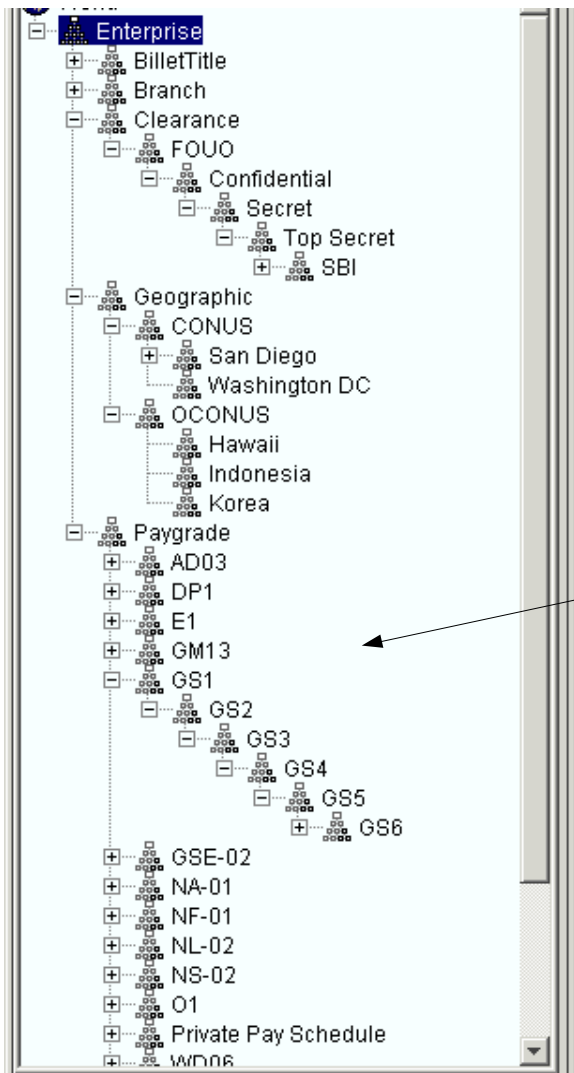
Customer User Profile Manager Interface

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

Meta-database tree contents:
- Enterprise
  - BilletTitle
  - Branch
  - Clearance
    - FOUO
      - Confidential
        - Secret
          - Top Secret
            - SBI
  - Geographic
    - CONUS
      - San Diego
      - Washington DC
    - OCONUS
      - Hawaii
      - Indonesia
      - Korea
  - Paygrade
    - AD03
    - DP1
    - E1
    - GM13
    - GS1
      - GS2
        - GS3
          - GS4
            - GS5
              - GS6
    - GSE-02
    - NA-01
    - NF-01
    - NL-02
    - NS-02
    - O1
    - Private Pay Schedule
    - WD06

How the EDAC works

Step 3:
The RBAC Rules Engine compares User and Resource Profiles to determine resource access.
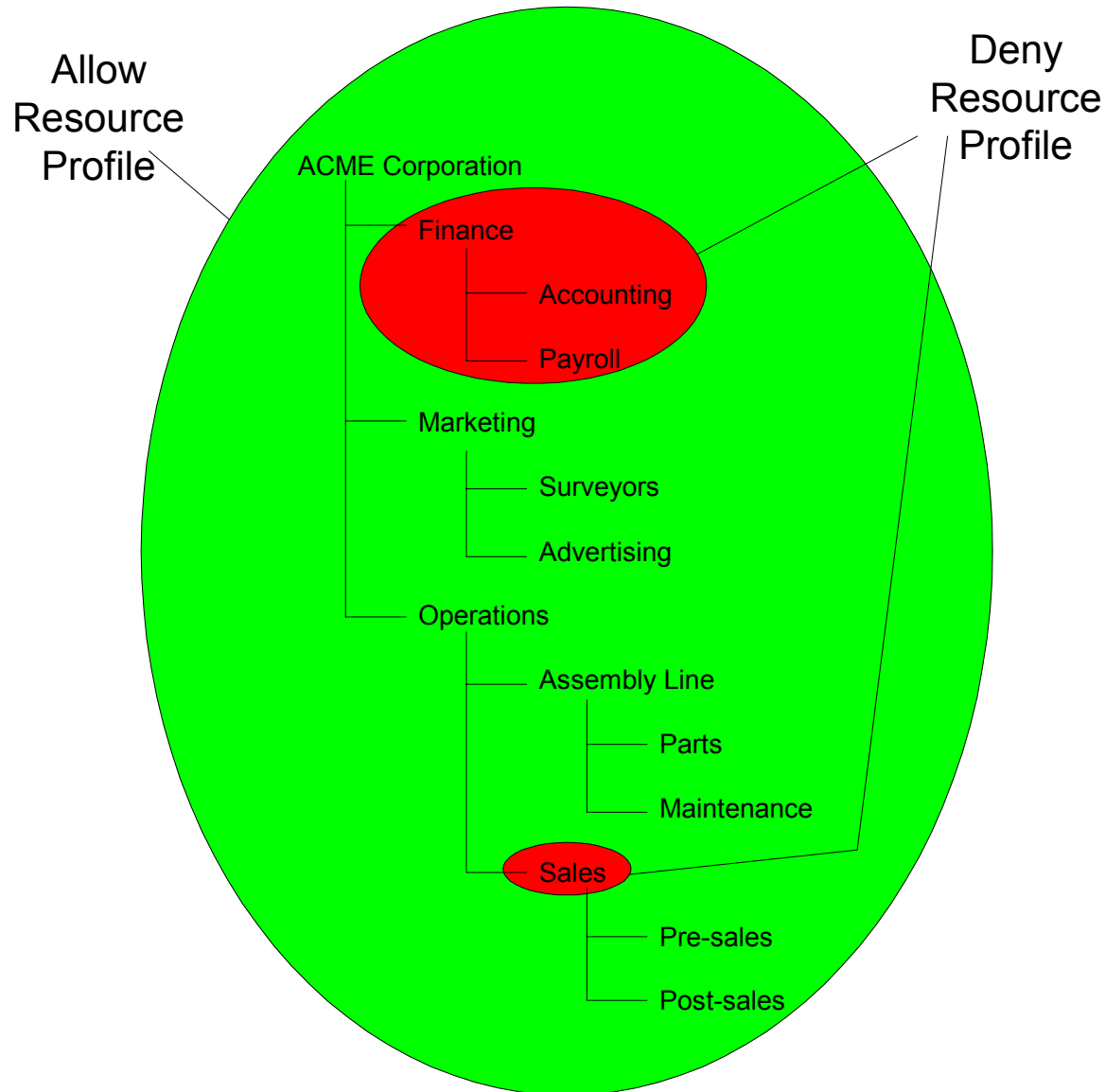
User Profile
ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise
ou=GS3, ou=GS2, ou=GS1, ou=Paygrade, o=Enterprise

Customer Resource Database

Project Tracker (resource)

HR Service (resource)

Payroll Application (resource)

Access token for Project Tracker

RBAC Rules Engine

Repository Service

Project Tracker Resource Profile
ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise

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

Allow Resource Profile

Deny Resource Profile

ACME Corporation

- Finance
  - Accounting
  - Payroll
- Marketing
  - Surveyors
  - Advertising
- Operations
  - Assembly Line
    - Parts
    - Maintenance
  - Sales
    - Pre-sales
    - Post-sales

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

Enterprise Dynamic Access Control (EDAC)
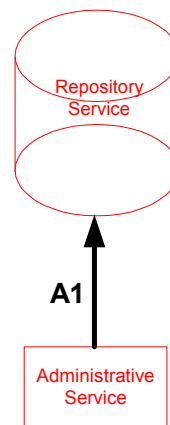
EDAC Process

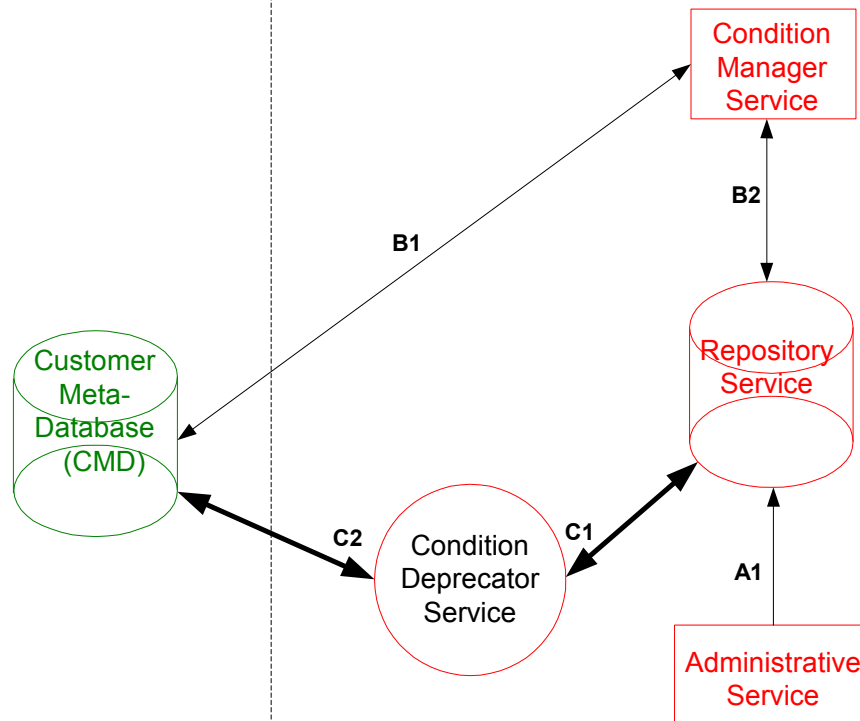(A) Administrative Service - establishes resource containers, CMD referrals, RM accounts.

Repository Service

A1

Administrative Service

EDAC - Model

**Enterprise Dynamic
Access Control (EDAC)**
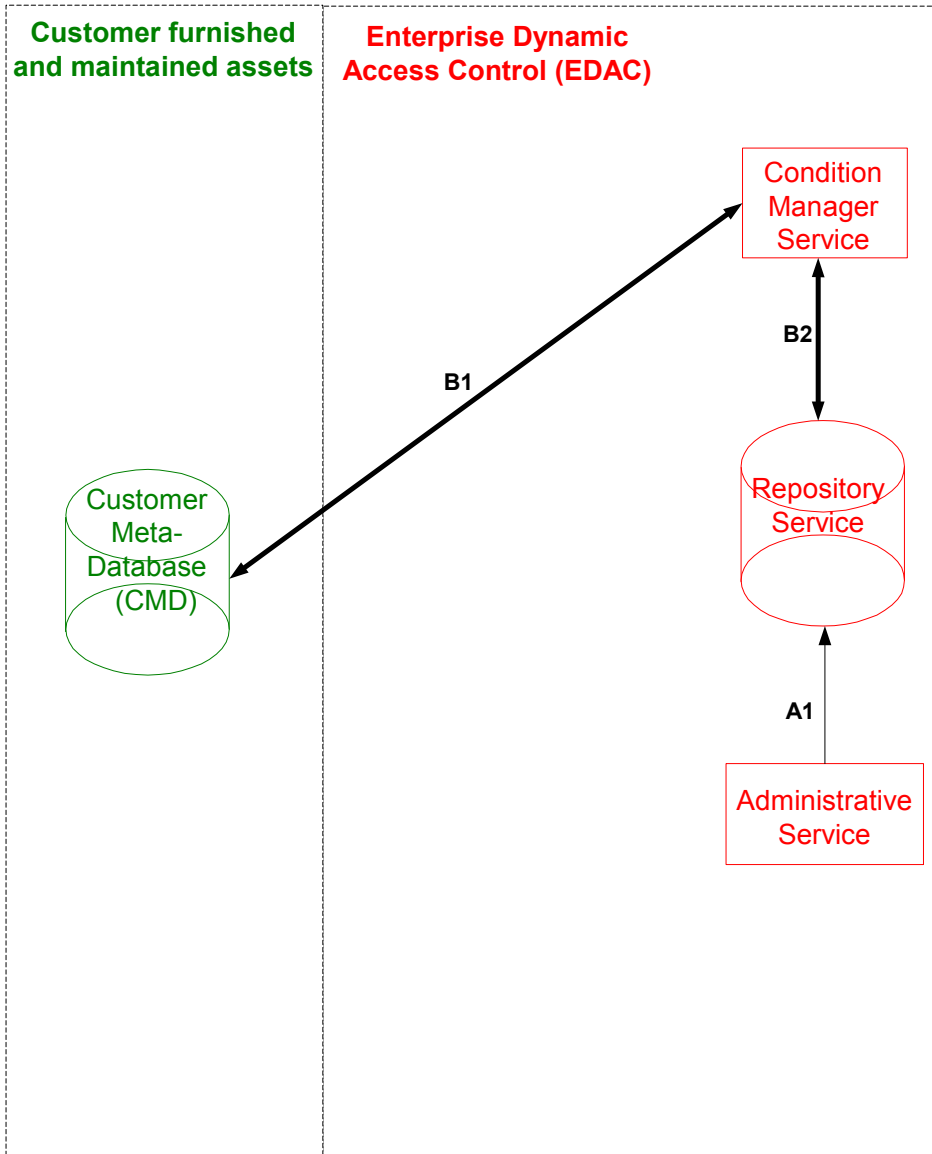
EDAC Process
(B) Condition manager
Service - Establishes
and edits conditions to
access resources.

Condition
Manager
Service

B2

Repository
Service

B1

Customer
Meta-
Database
(CMD)

A1

Administrative
Service

EDAC - Model

Customer furnished and maintained assets

Enterprise Dynamic Access Control (EDAC)

Condition Manager Service

B2

B1

Customer Meta-Database (CMD)

Repository Service

C2

Condition Deprecator Service

C1

A1

Administrative Service

EDAC - Model

Customer furnished and maintained assets

Enterprise Dynamic Access Control (EDAC)
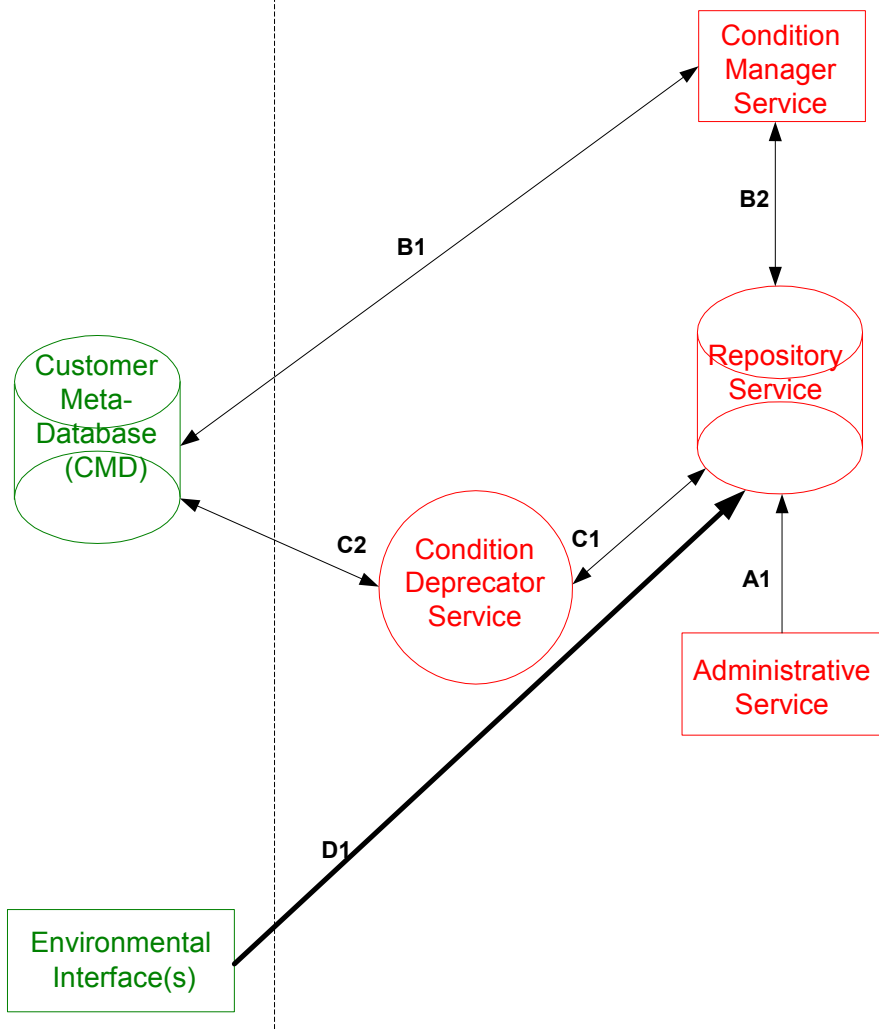
EDAC Process
(D) Customer Environmental Interface
- furnishes environmental updates.

Condition Manager Service

Customer Meta-Database (CMD)

Repository Service

B1

B2

C2

Condition Deprecator Service

C1

A1

Administrative Service

D1

Environmental Interface(s)

EDAC - Model

Customer furnished and maintained assets

Enterprise Dynamic Access Control (EDAC)

- Customer Personnel Database
- Object Profile Manager Service
- Customer Meta-Database (CMD)
- Environmental Interface(s)

- Structure Format Service
- Condition Manager Service
- Rules Engine Service
- Repository Service
- Condition Deprecator Service
- Administrative Service

E1, E2, E3, E4, E5, B1, B2, C1, C2, A1, D1

EDAC Process

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

EDAC - Model
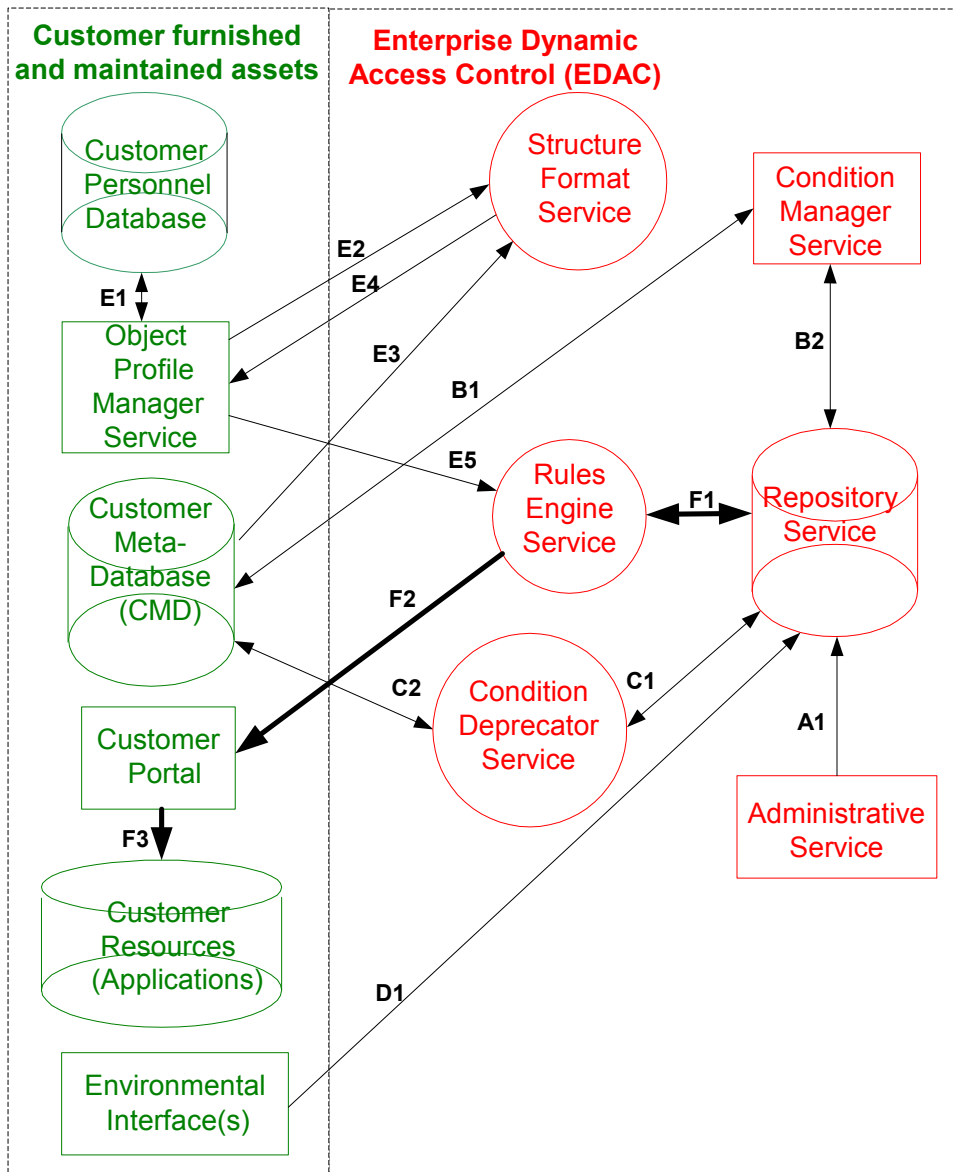
EDAC Process

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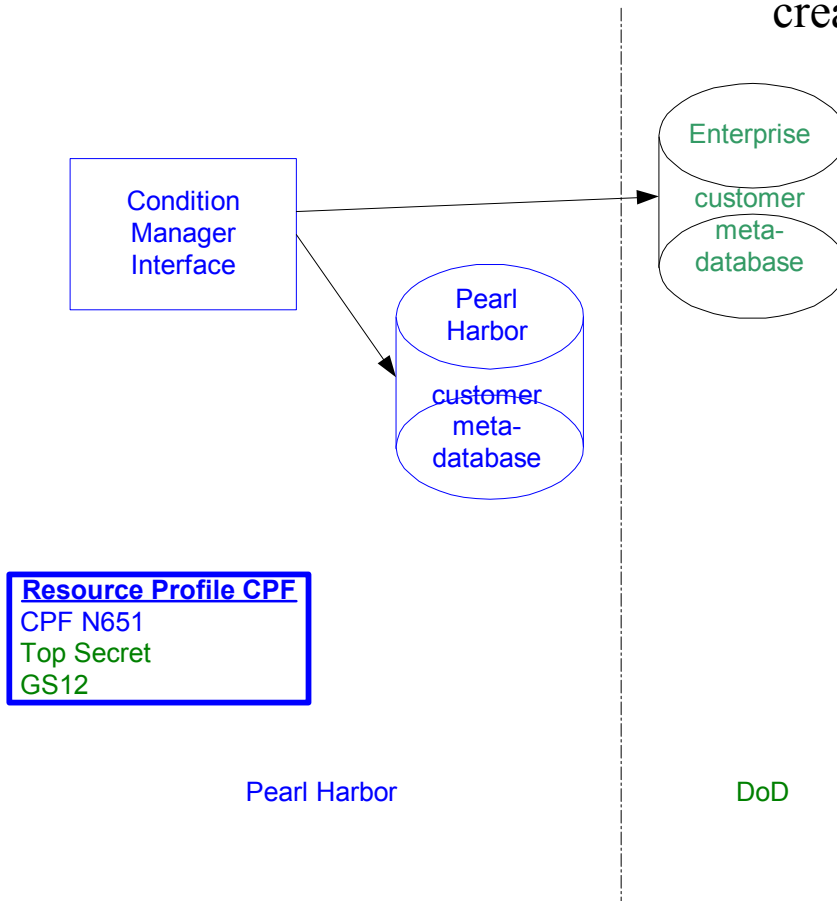
EDAC – Interoperability

EDAC interoperable among regions:

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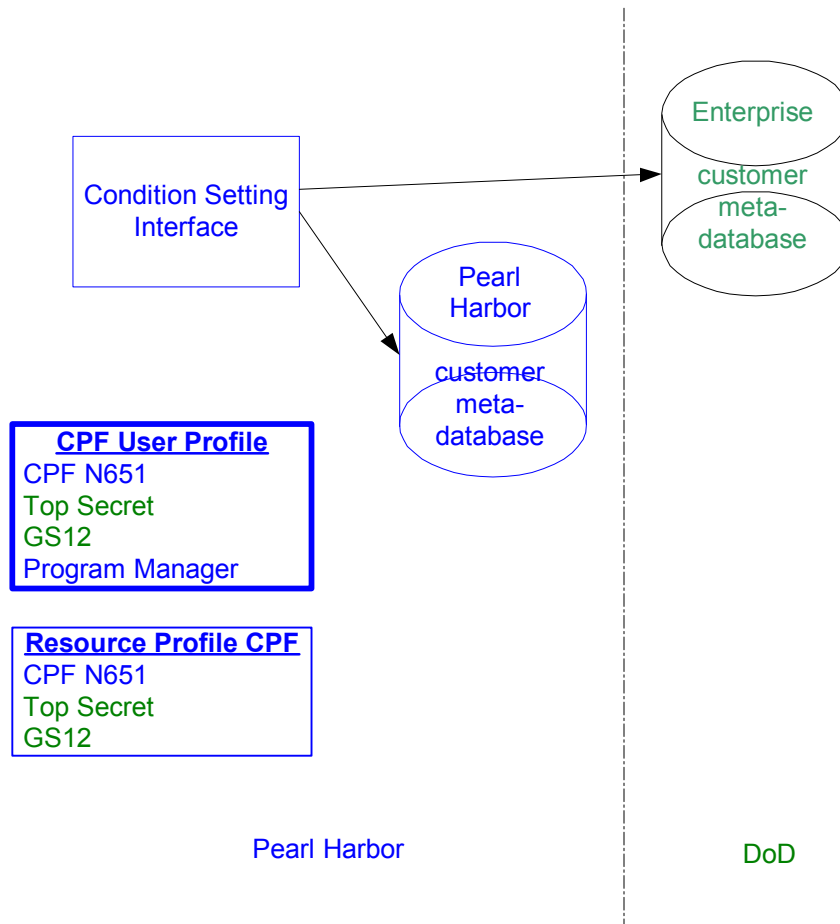- Domain customer meta-databases

EDAC - Interoperability

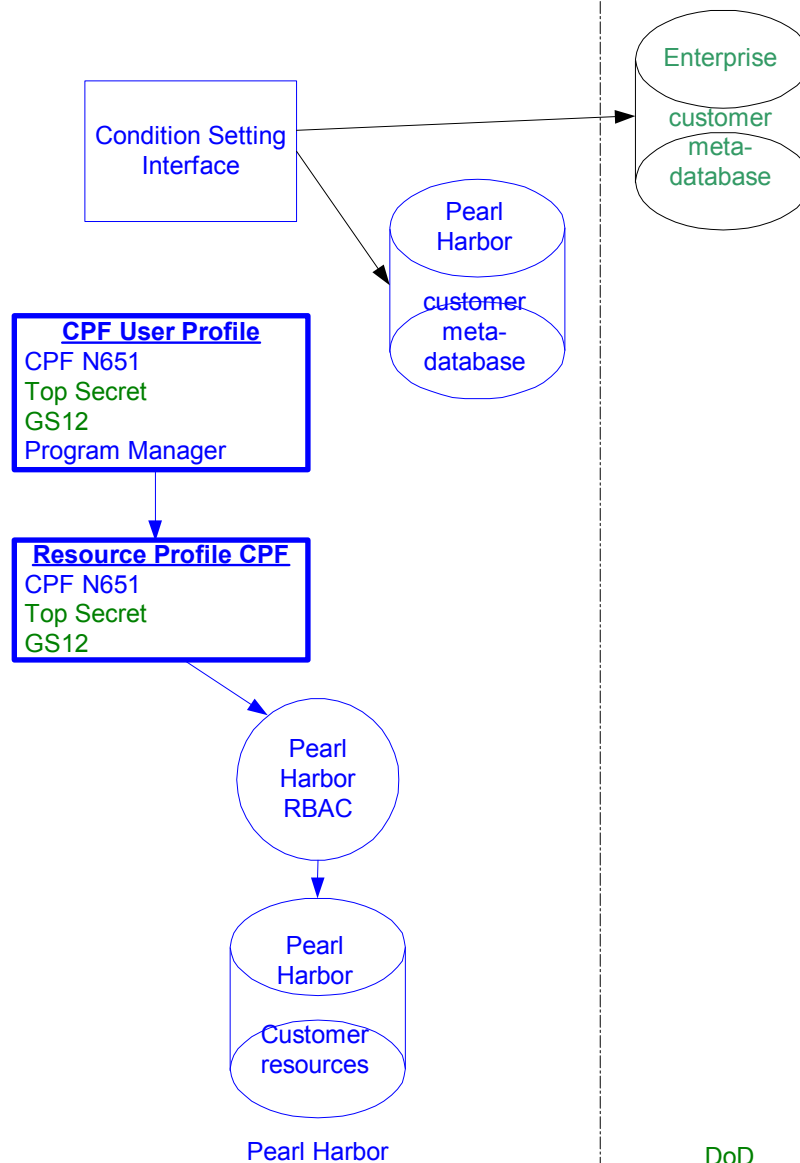Pearl Harbor: resource profile created for local resource access.

Condition Manager Interface

Enterprise customer meta-database

Pearl Harbor customer meta-database

Resource Profile CPF
CPF N651
Top Secret
GS12

Pearl Harbor

DoD

EDAC - Interoperability

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

Enterprise customer meta-database

Condition Setting Interface

Pearl Harbor customer meta-database

CPF User Profile
CPF N651
Top Secret
GS12
Program Manager

Resource Profile CPF
CPF N651
Top Secret
GS12

Pearl Harbor

DoD

EDAC - Interoperability

Condition Setting Interface

Enterprise customer meta-database

Pearl Harbor customer meta-database

CPF User Profile
CPF N651
Top Secret
GS12
Program Manager

Resource Profile CPF
CPF N651
Top Secret
GS12

Pearl Harbor RBAC

Pearl Harbor Customer resources

Pearl Harbor

DoD

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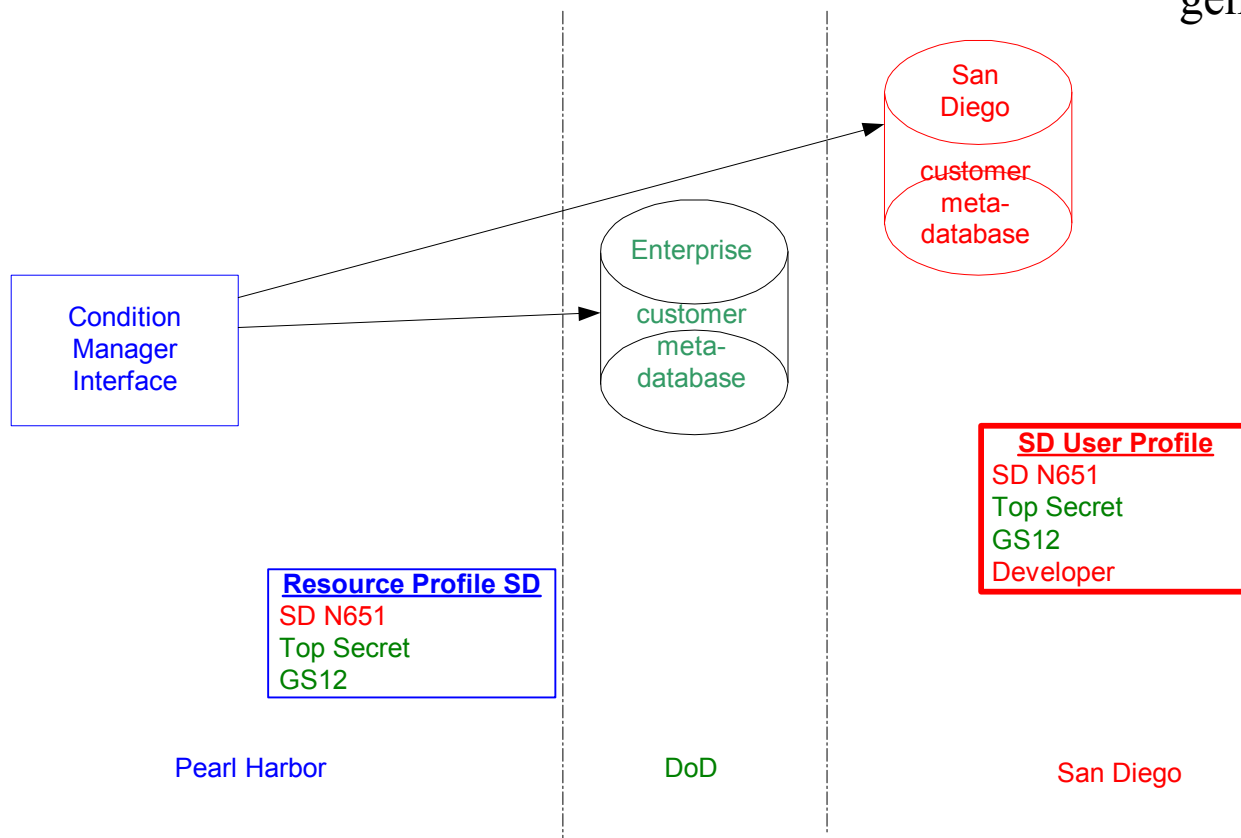
EDAC - Interoperability

San Diego

~~customer~~
meta-
database

Enterprise

customer
meta-
database

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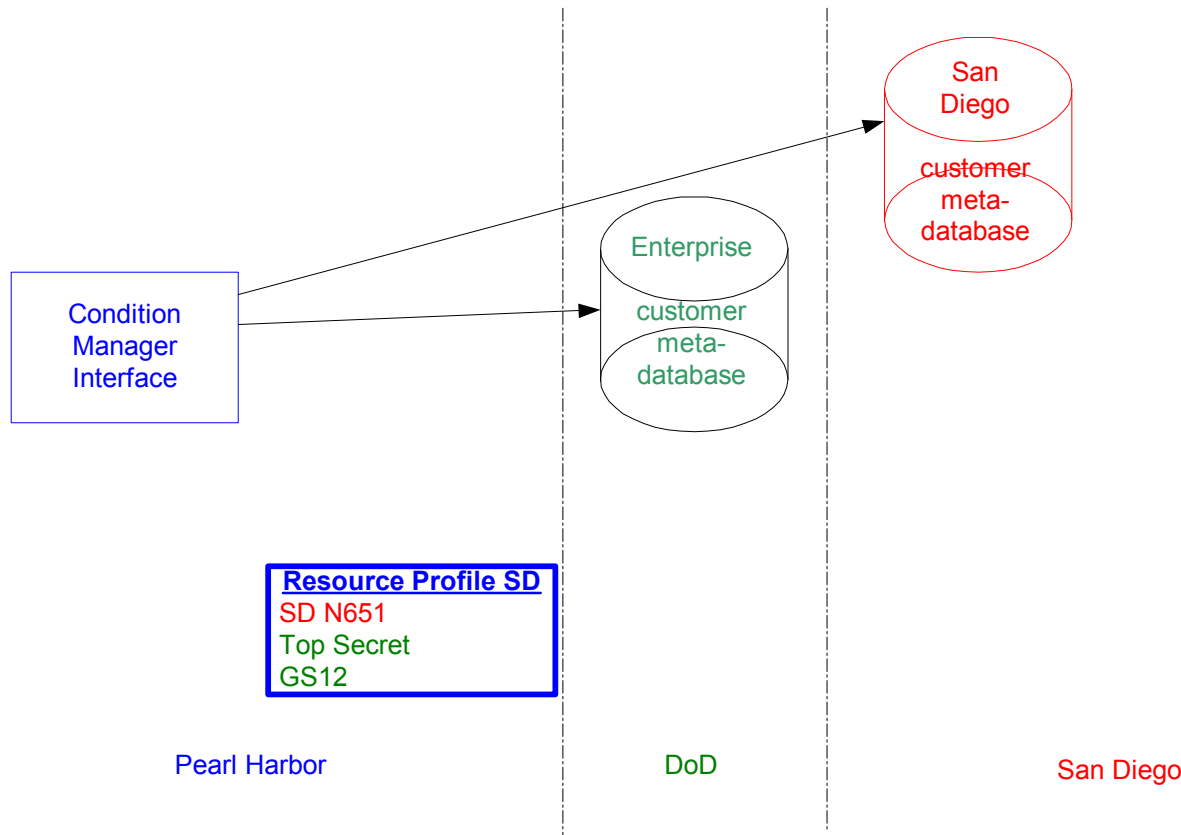
Pearl Harbor: A resource profile to allow remote users access to local resources.

Resource Profile SD
SD N651
Top Secret
GS12

Pearl Harbor

DoD

San Diego

EDAC - Interoperability

San Diego: user profile generated.

San Diego
~~customer~~
meta-
database

Enterprise
customer
meta-
database

Condition
Manager
Interface

SD User Profile
SD N651
Top Secret
GS12
Developer

Resource Profile SD
SD N651
Top Secret
GS12

Pearl Harbor

DoD

San Diego

EDAC - Interoperability

San Diego
~~customer~~
meta-database

Enterprise
customer
meta-database

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

Condition Manager Interface

SD User Profile
SD N651
Top Secret
GS12
Developer

Resource Profile SD
SD N651
Top Secret
GS12

Pearl Harbor RBAC

Pearl Harbor
Customer resources

Pearl Harbor   DoD   San Diego

EDAC - Interoperability

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

San Diego customer meta-database

Enterprise customer meta-database

Condition Manager Interface

SD User Profile
SD N651
Top Secret
GS12
Developer

Resource Profile SD
SD N651
Top Secret
GS12

San Diego RBAC

San Diego Customer resources

DoD

San Diego

EDAC – Interoperability

San Diego, CA 92152-5001