COMPACFLT SEAC RBAC

Commander, Pacific Fleet (COMPACFLT)
Secure Enterprise Access Control (SEAC)
Role Based Access Control (RBAC)

Point of Contact:
Richard Fernandez
(808) 474-9270

The information contained herein is considered U.S. Government Proprietary and may be related to one or more U.S. Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SD 541, June 2004
SSC San Diego
San Diego, CA 92152-5001

Approved for public release; distribution is unlimited.

COMPACFLT SEAC RBAC

The SEAC RBAC is available at:
http://www.spawar.navy.mil/sti/publications/pubs/td/3182/td3182con.pdf

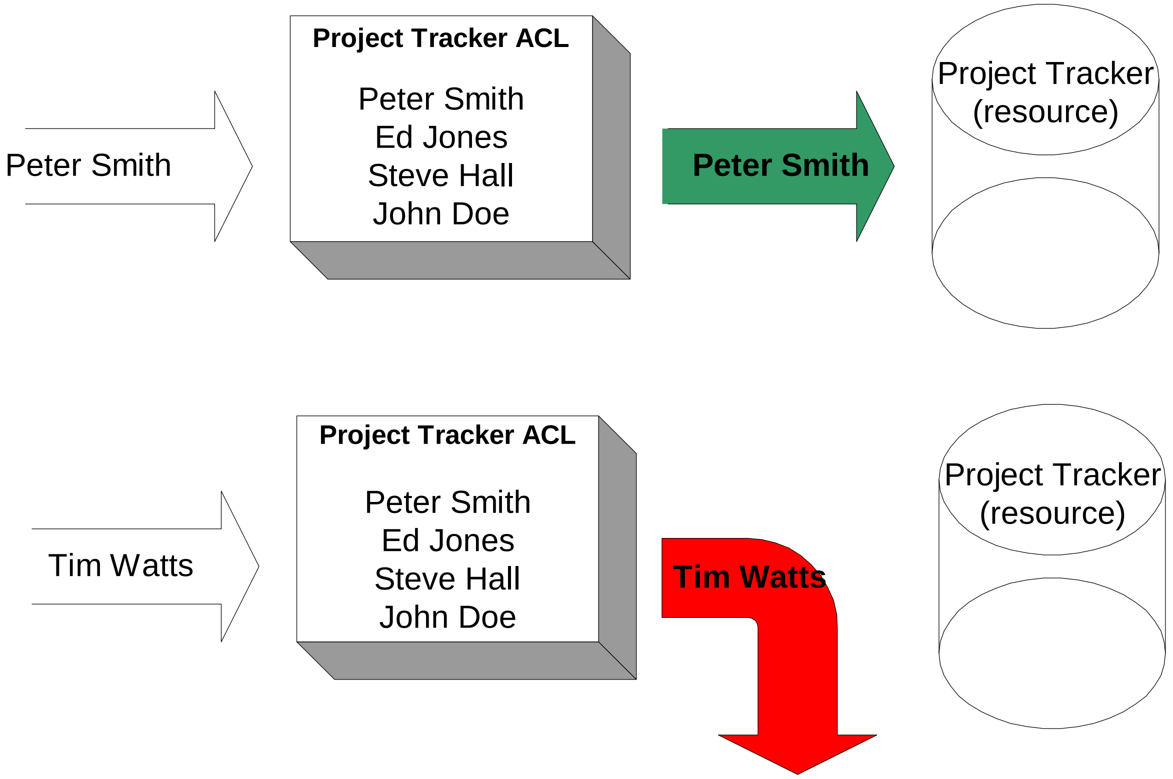
References:
http://csrc.nist.gov/rbac/

For comments contact:
Richard Fernandez
(808) 474-9270
Richard.R.Fernandez@navy.mil

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

Access Control Lists (ACL)

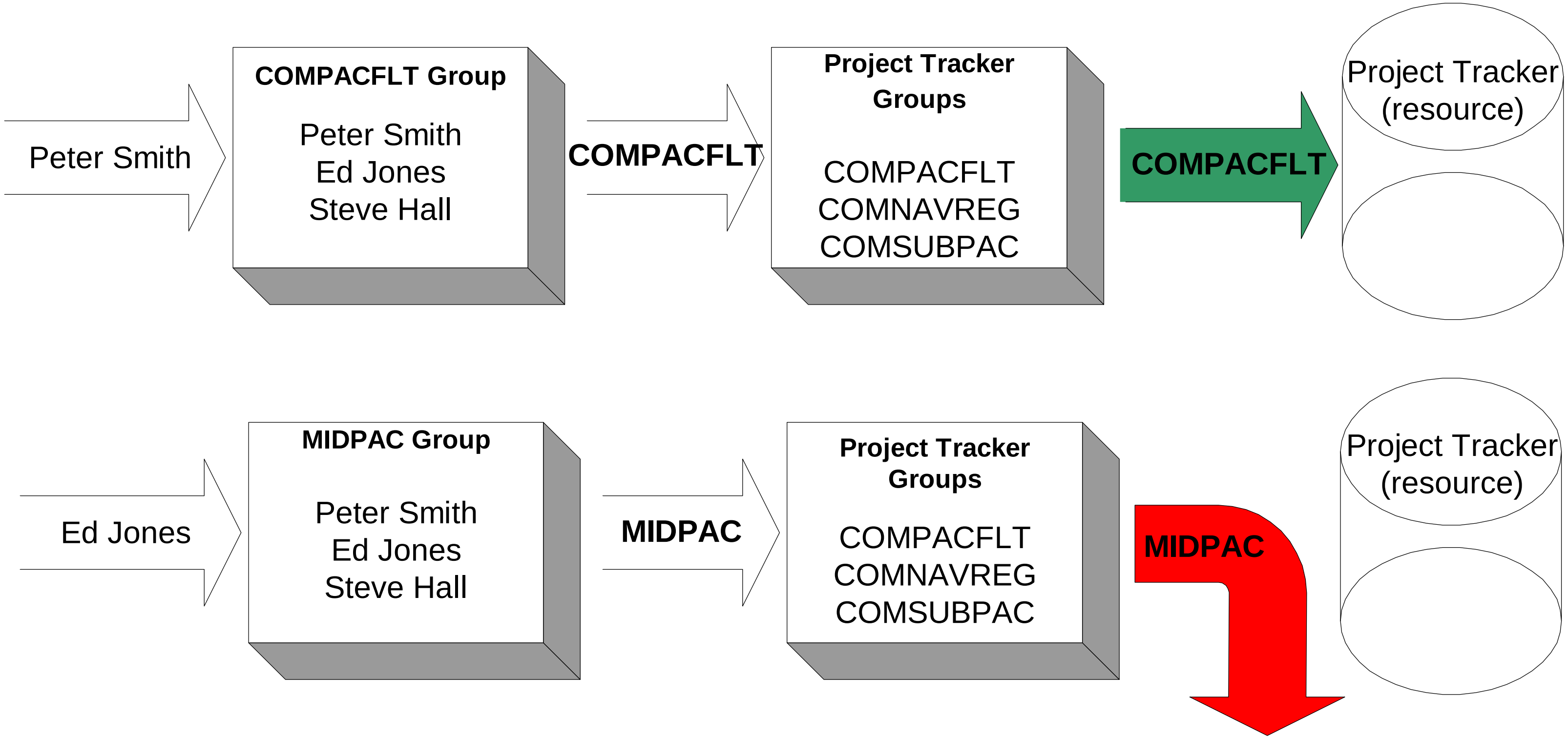
User name or unique identifier associates access to resources



The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

Groups

User associated to a group and group associated to resources



The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

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:

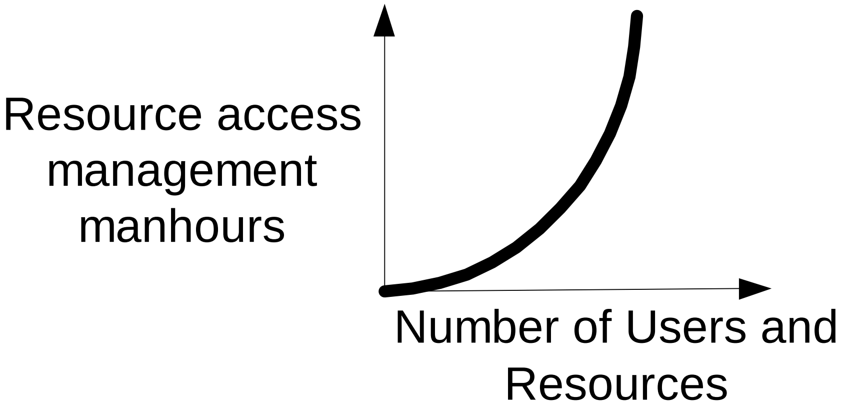
- Transfer to another organization
- Loss of security clearance
- Change in job title
- Job promotion

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



The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

NIST RBAC compliance

Because of ACL and group limitations:

The National Institute of Standards and Technology (NIST) has declared RBAC 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.*

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

Access control comparison

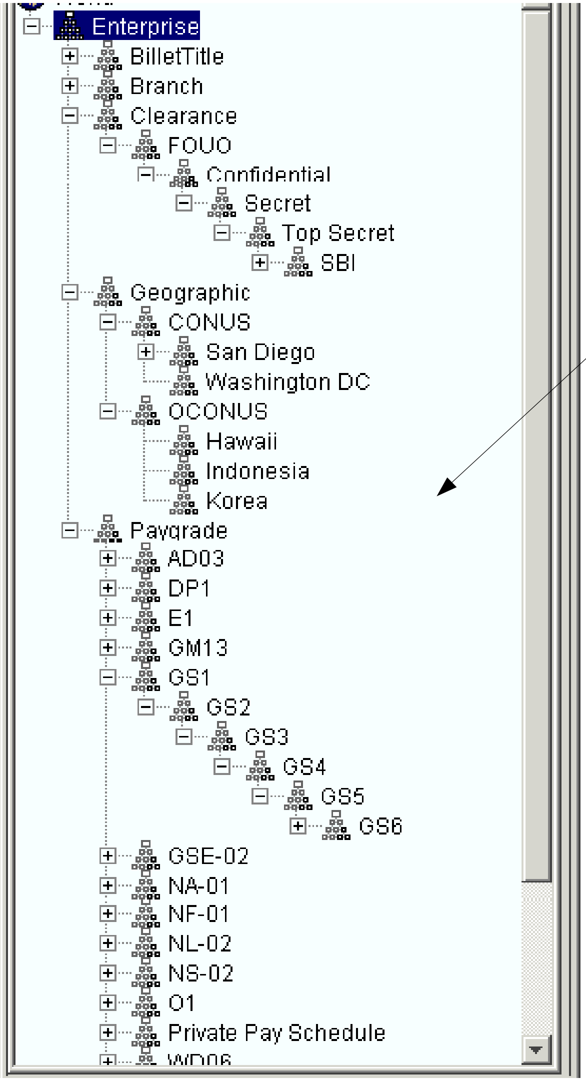
How access control solutions can simultaneously evaluate user characteristics.

	User Characteristics	
	Number of user characteristics evaluated	Hierarchal evaluation of user characteristics
ACLs	0	No
Groups	1	Yes/No
NIST RBAC	1	Yes
SEAC RBAC	Unlimited	Yes

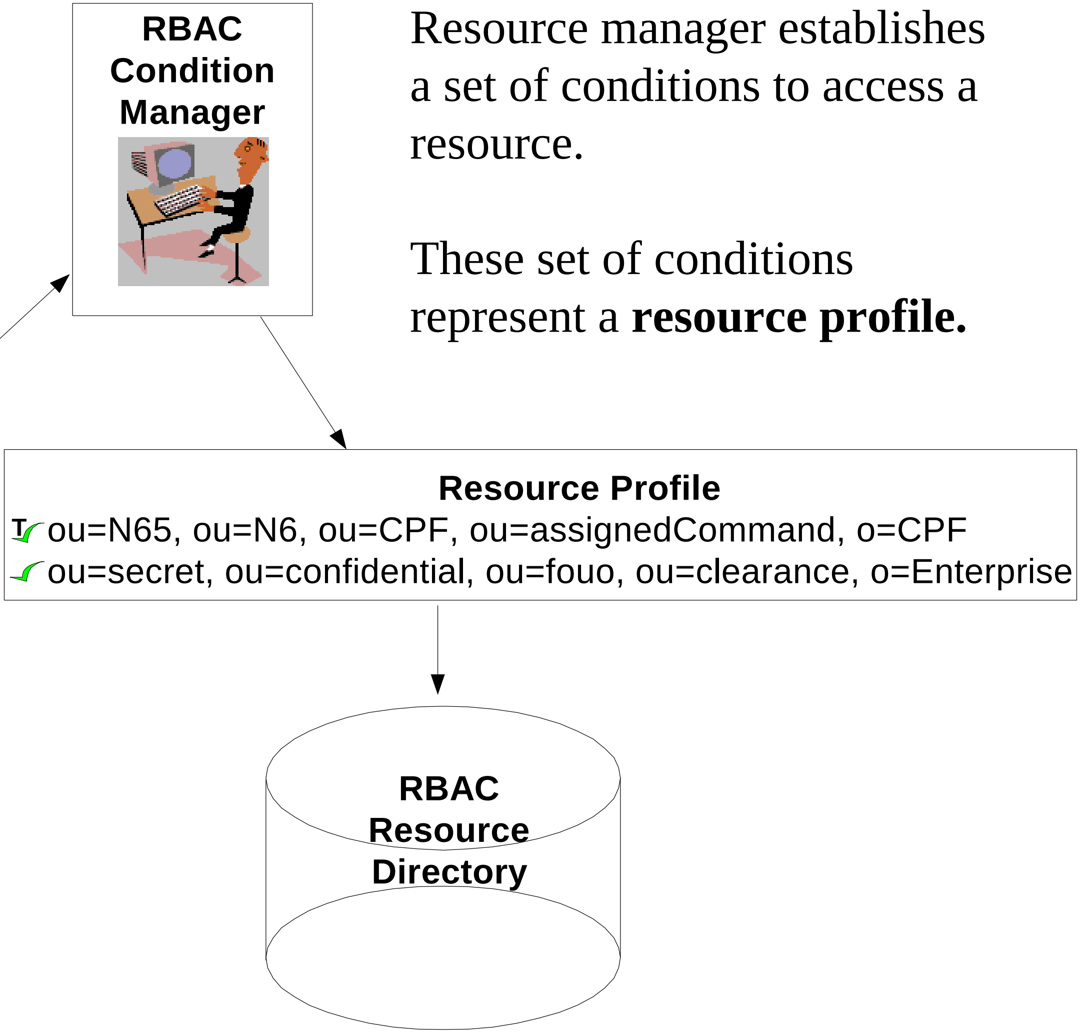
Note: A hierarchal structure offers inheritance capabilities.

How the SEAC RBAC works

Customer Meta-Database (Reference Directory)



- 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

T✓ ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF

✓ ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise

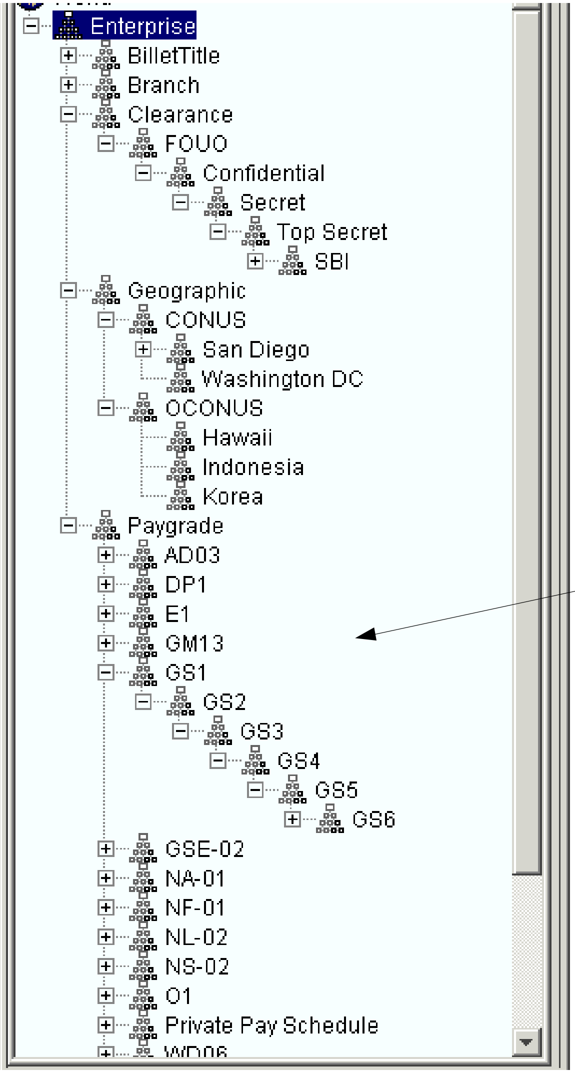
Step 1:
Resource manager establishes a set of conditions to access a resource.

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

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

How the SEAC RBAC works

Customer Meta-Database (Reference Directory)



- 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

Customer User Profile Manager Interface

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

Distinguished Name Generator

Customer Personnel Database

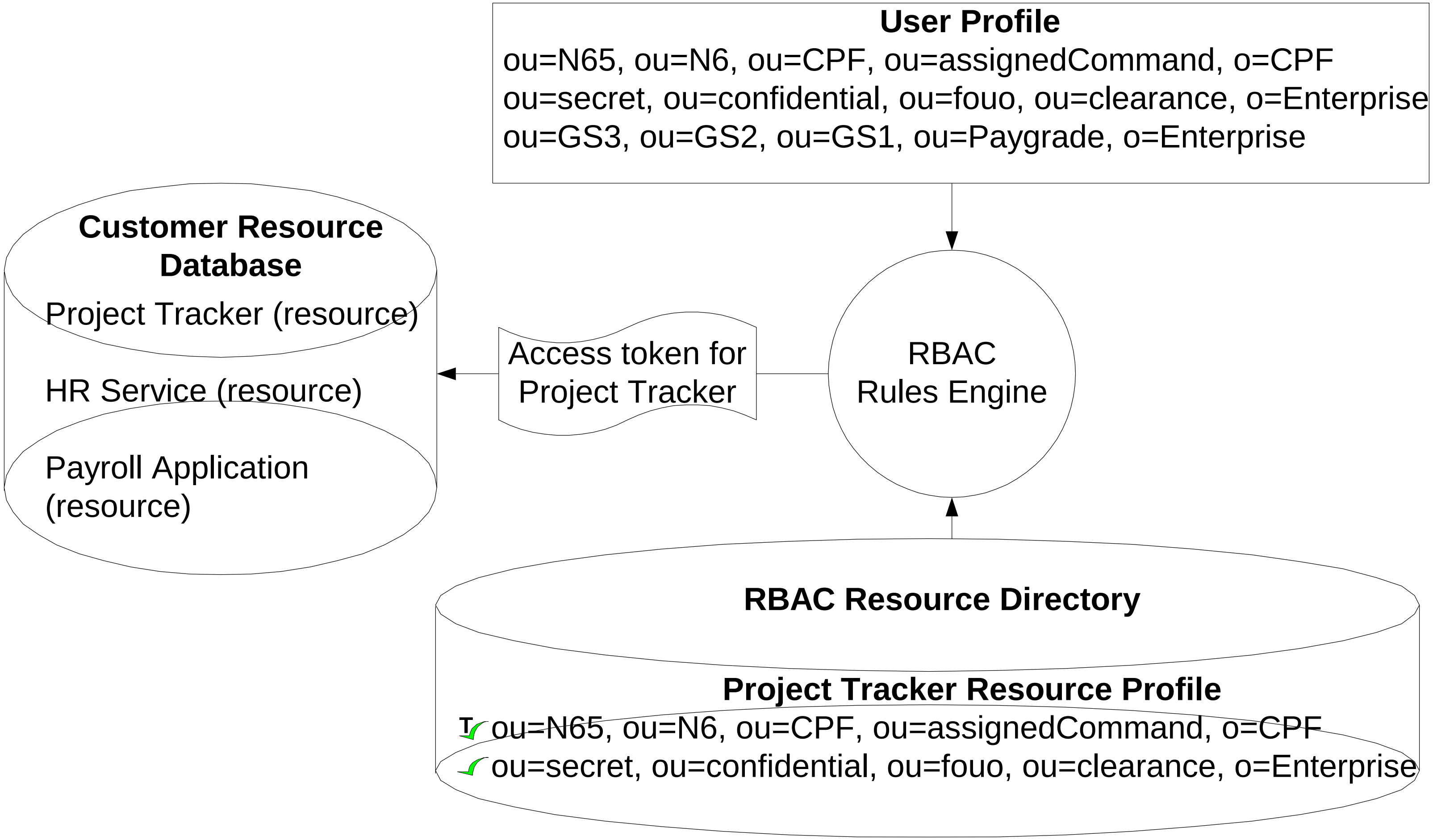
Reference Categories	Attributes
assignedCommand	N65
clearance	Secret
paygrade	GS3

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

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

How the SEAC RBAC 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

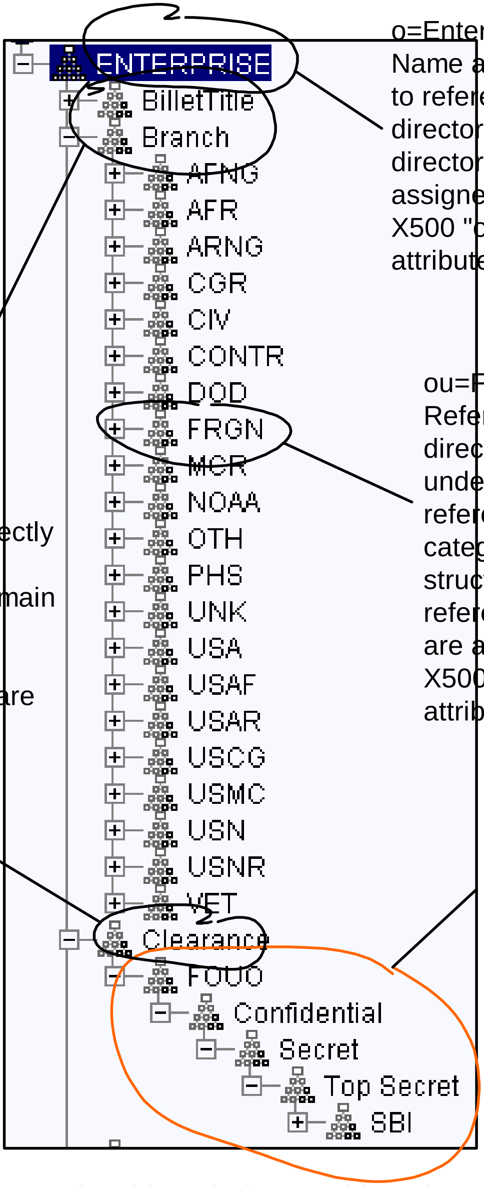
RBAC Rules Engine

RBAC Resource Directory

Project Tracker Resource Profile

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

Reference directory standard specifications



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

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

ou=FRGN
Reference value directly underneath reference category in a flat structure. All reference values 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

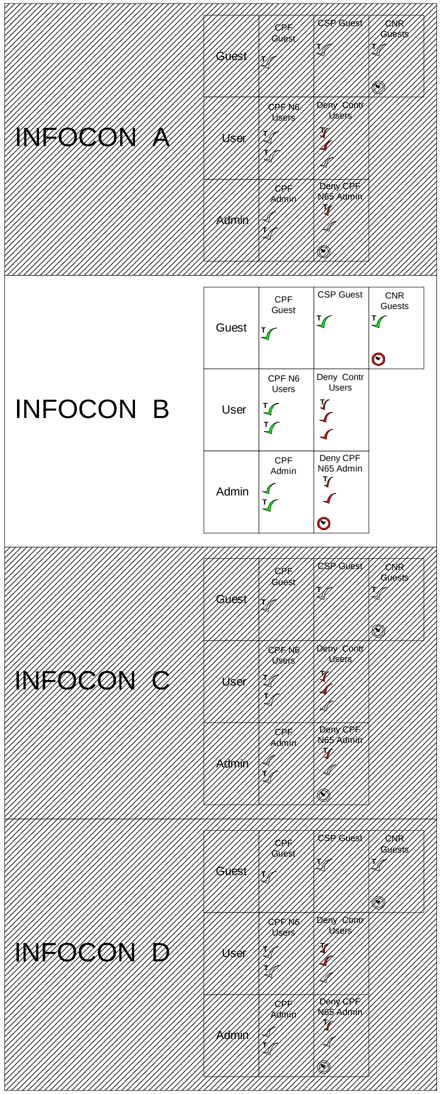
SEAC RBAC – Resource profiles

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	

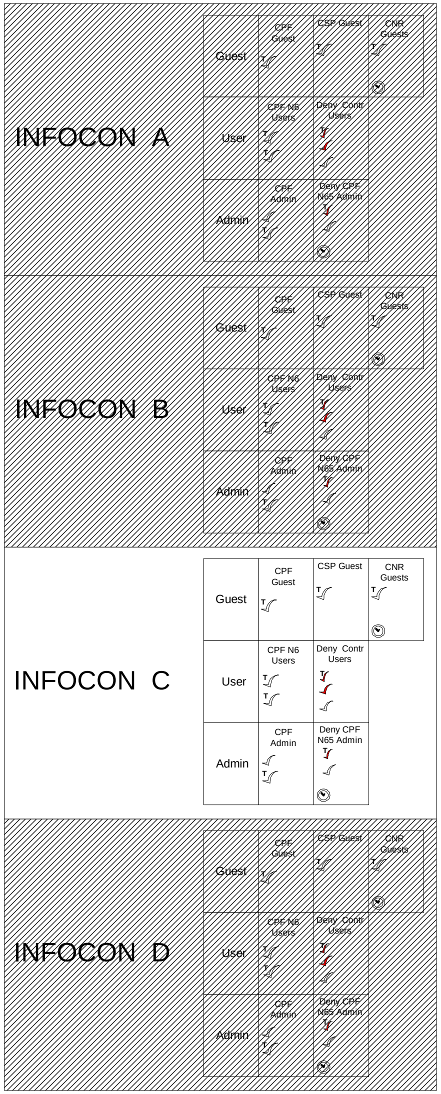
- Resource roles
- Allow & Deny profiles
- Exact and subtree conditions
- Time constraints

SEAC RBAC – Security levels

During INFOCON B



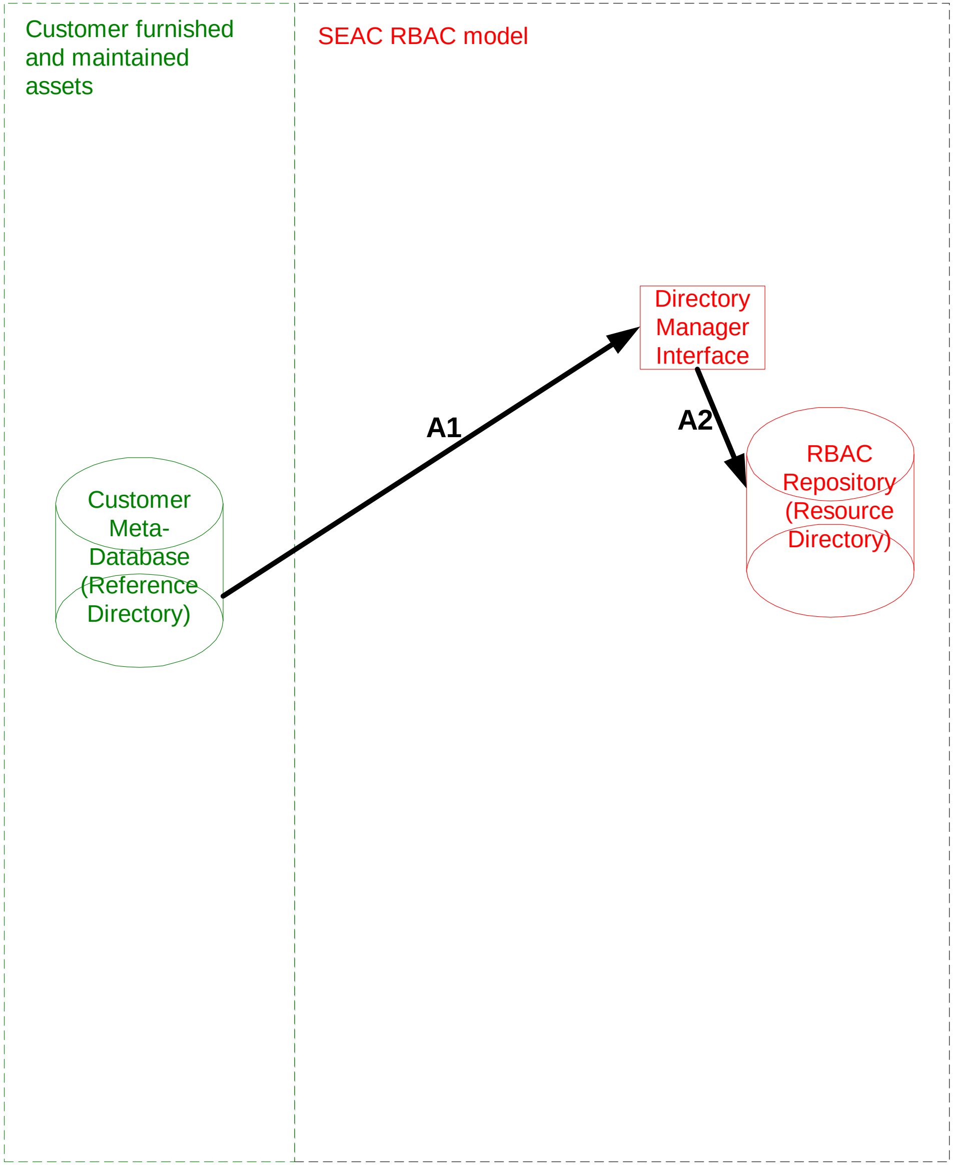
During INFOCON C



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

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

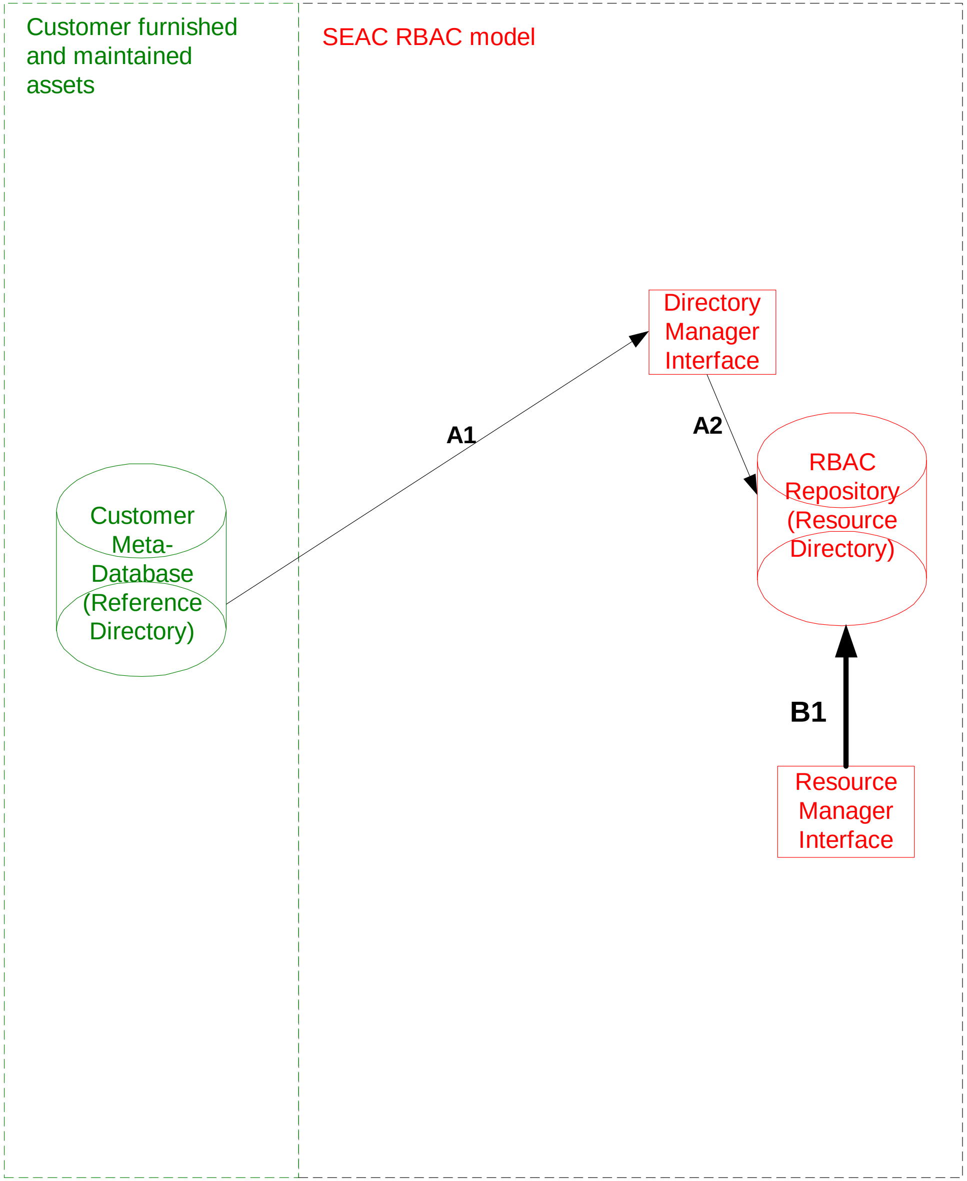
SEAC RBAC - Model


Customer furnished and maintained assets
SEAC RBAC model
Directory Manager Interface
A1
A2
RBAC Repository (Resource Directory)
Customer Meta-Database (Reference Directory)

(A) Directory Manager Interface: manages reference directory referrals.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SEAC RBAC - Model

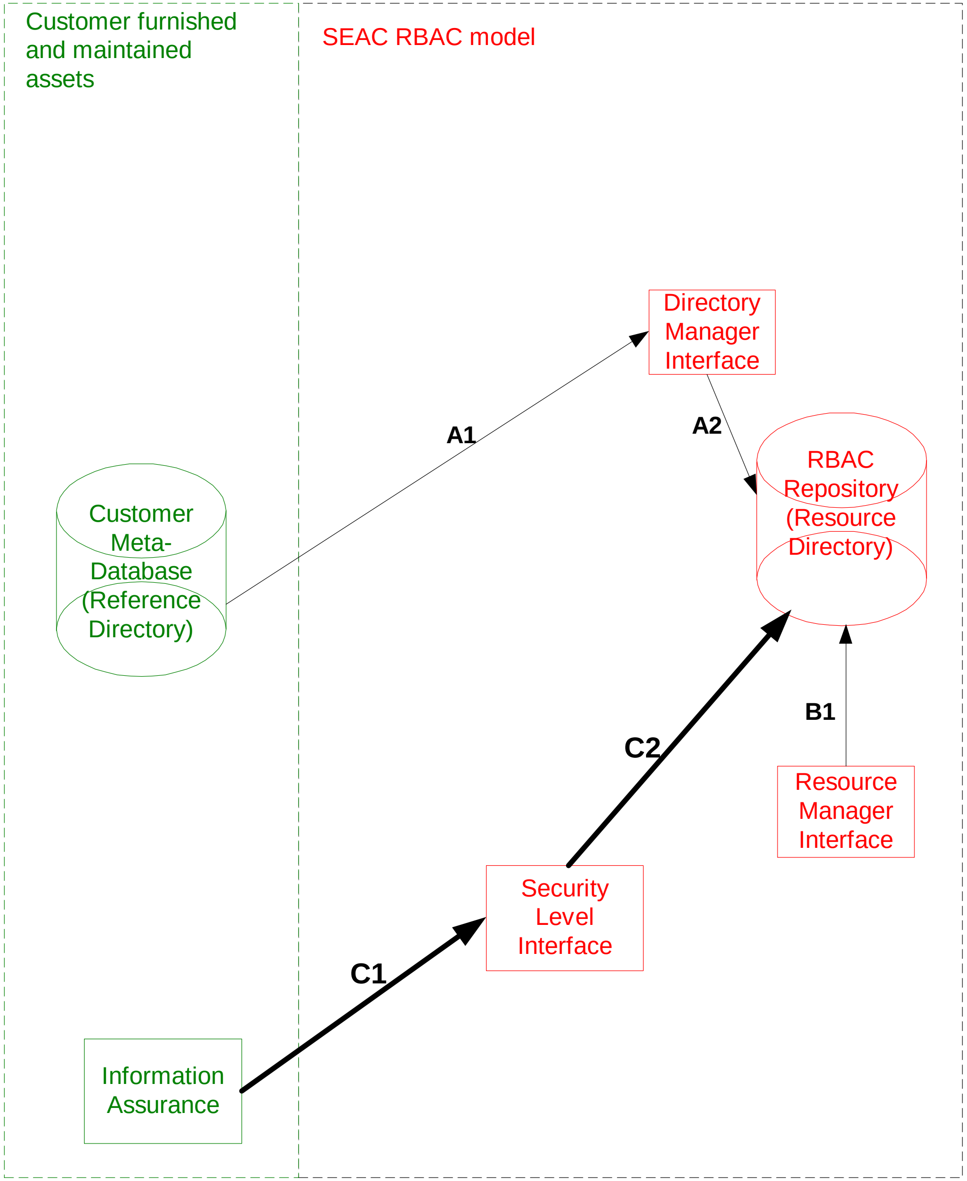


Customer furnished and maintained assets
SEAC RBAC model
Directory Manager Interface
A1
A2
RBAC Repository (Resource Directory)
Customer Meta-Database (Reference Directory)
B1
Resource Manager Interface

(B) Resource Manager Interface: manages a resource container used to store conditions.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

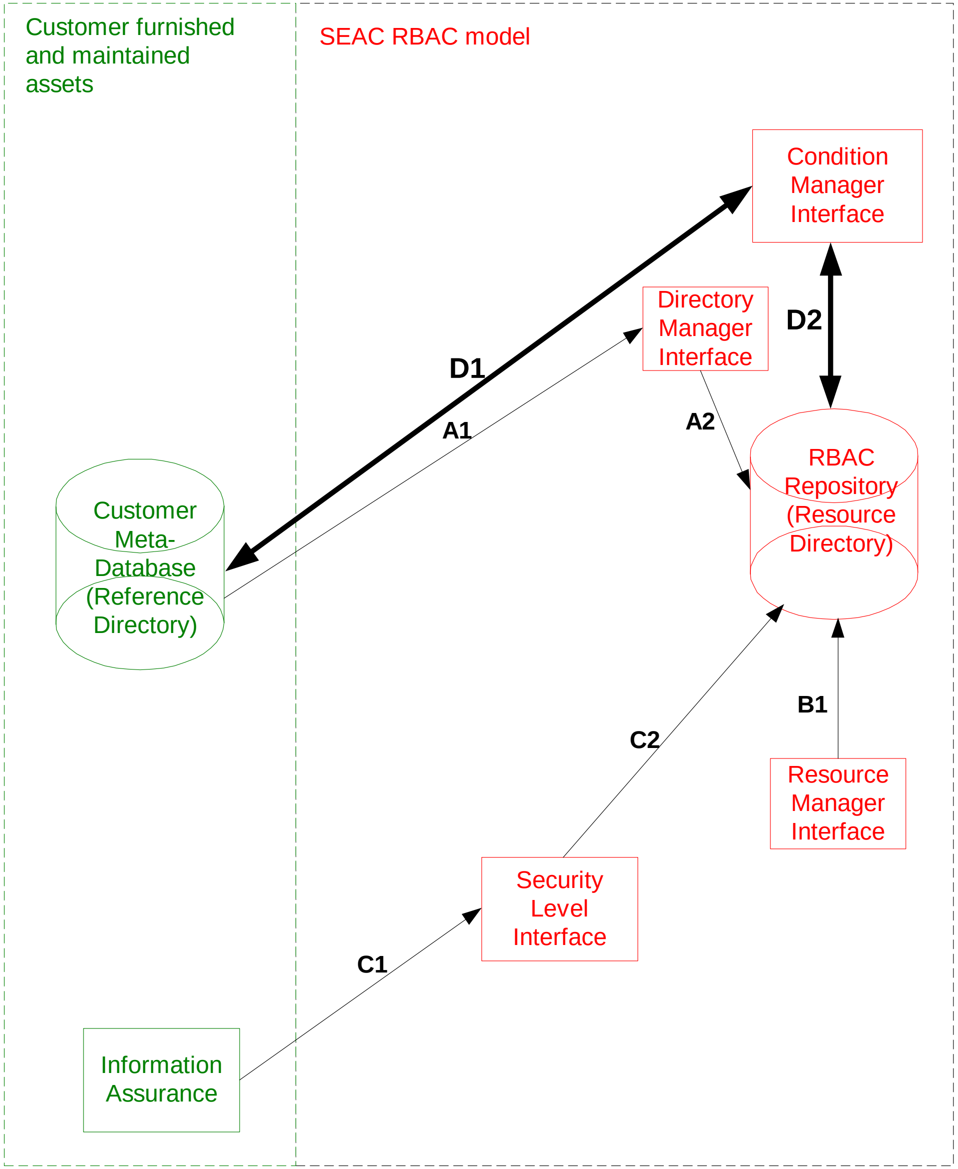
SEAC RBAC - Model


Customer furnished and maintained assets
SEAC RBAC model
Directory Manager Interface
A1
A2
RBAC Repository (Resource Directory)
Customer Meta-Database (Reference Directory)
B1
C2
Resource Manager Interface
Security Level Interface
C1
Information Assurance

(C) Security Level Interface: establishes prevailing security level.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

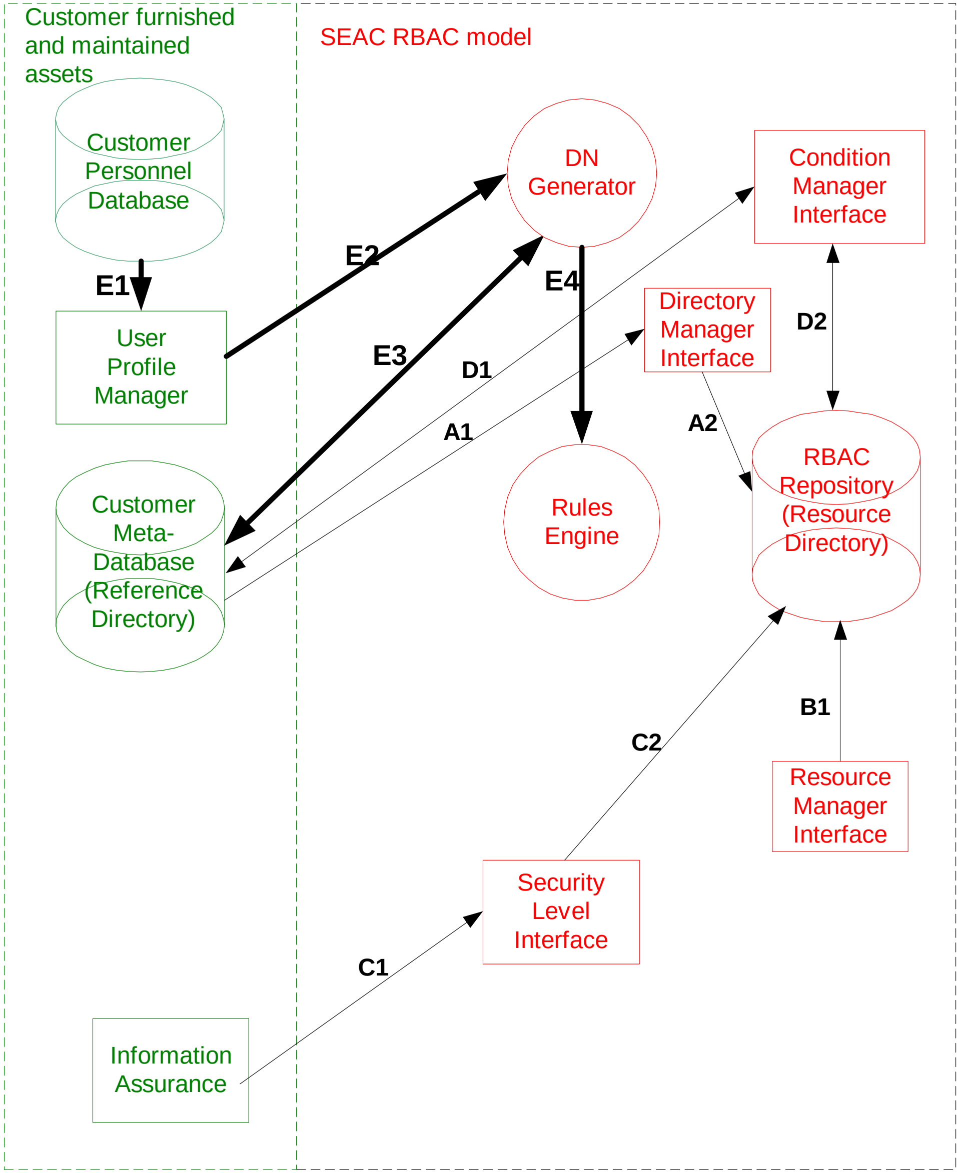
SEAC RBAC - Model


Customer furnished and maintained assets
SEAC RBAC model
Condition Manager Interface
Directory Manager Interface
D2
D1
A1
A2
RBAC Repository (Resource Directory)
Customer Meta-Database (Reference Directory)
B1
C2
Resource Manager Interface
Security Level Interface
C1
Information Assurance

(D) Condition Manager Interface: establishes conditions to access resources.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SEAC RBAC - Model

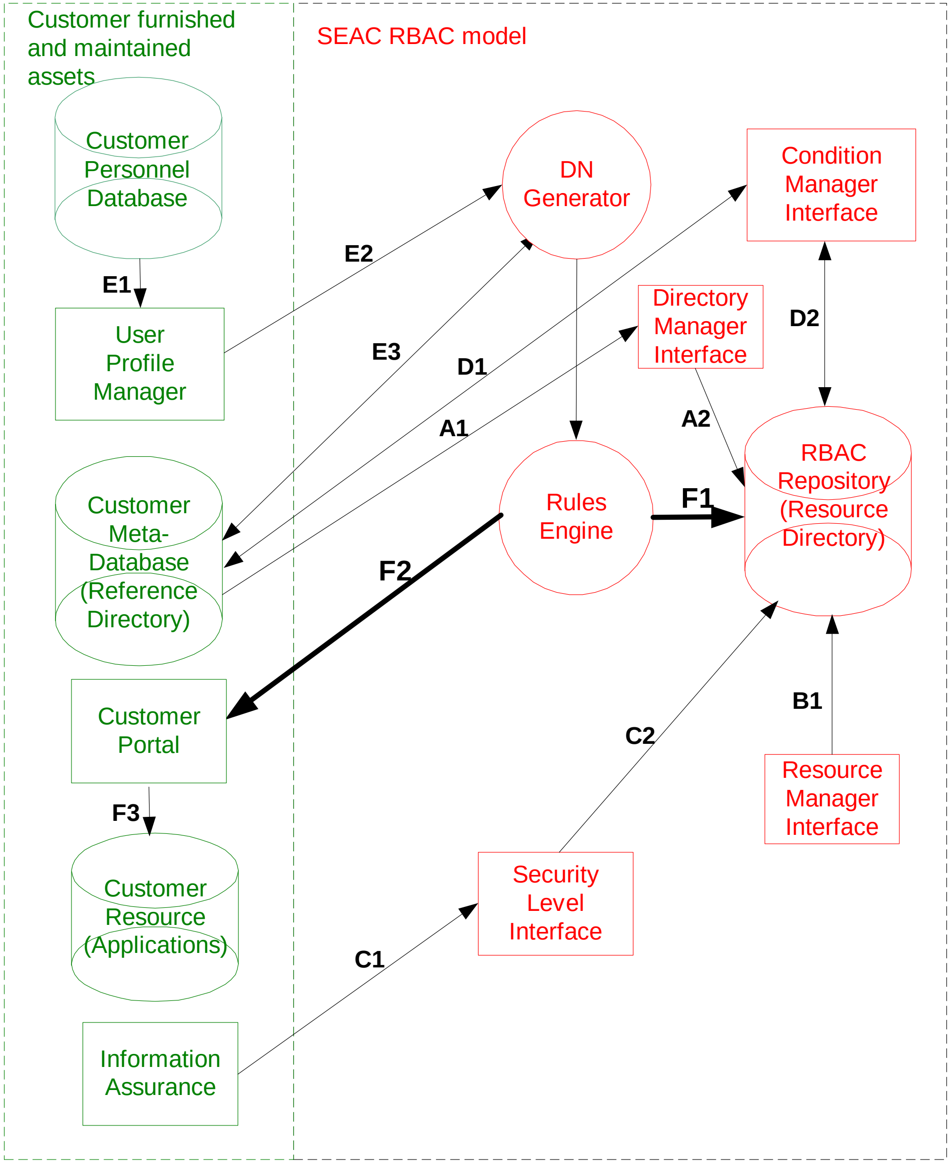


Customer furnished and maintained assets
SEAC RBAC model
Customer Personnel Database
E1
User Profile Manager
E2
DN Generator
E3
E4
Condition Manager Interface
Directory Manager Interface
D1
D2
A1
A2
Customer Meta-Database (Reference Directory)
Rules Engine
RBAC Repository (Resource Directory)
B1
C2
Resource Manager Interface
Security Level Interface
C1
Information Assurance

(E) User profile manager: user profile selection and DN formatting.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SEAC RBAC - Model

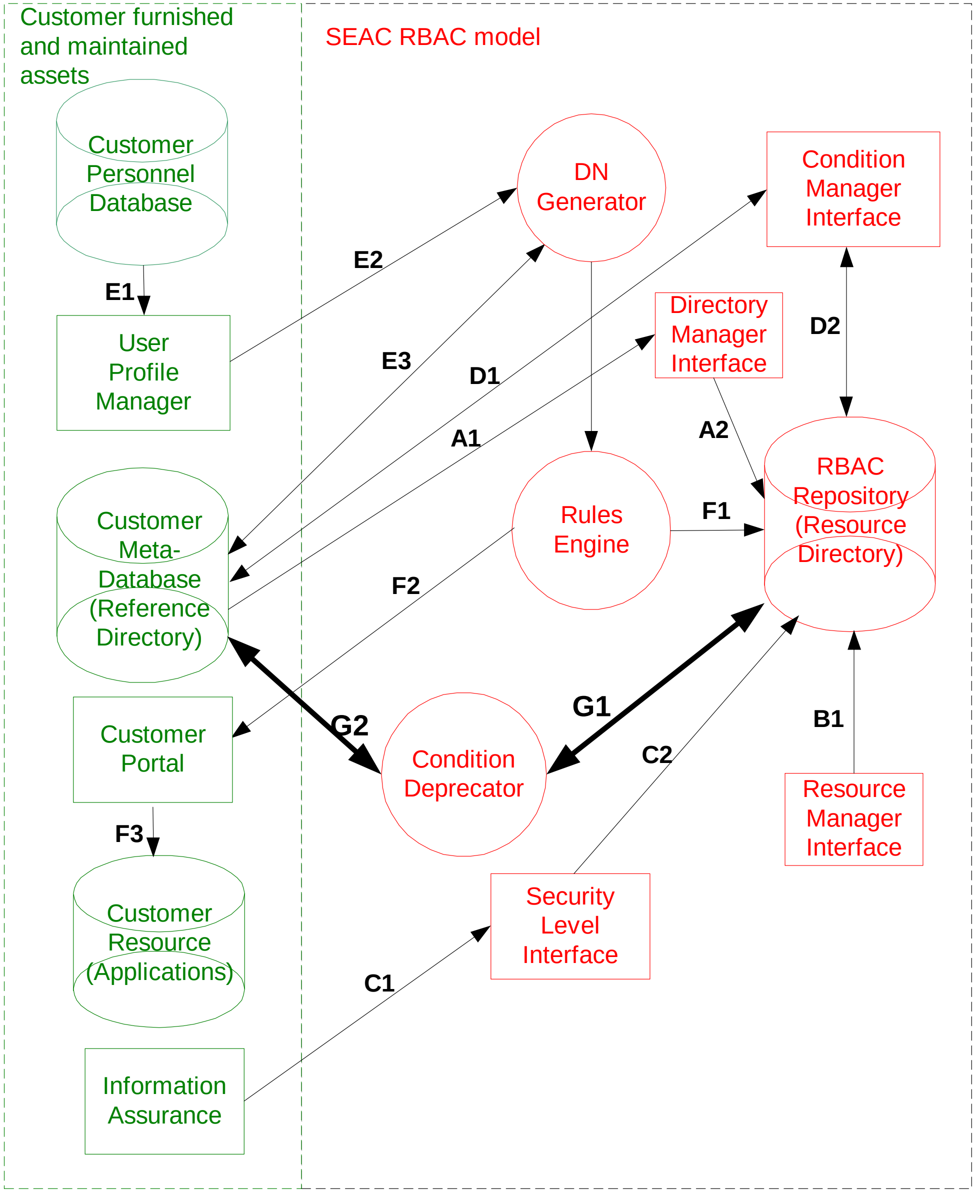


Customer furnished and maintained assets
SEAC RBAC model
Customer Personnel Database
E1
User Profile Manager
E2
DN Generator
Condition Manager Interface
E3
D1
Directory Manager Interface
D2
A1
A2
Customer Meta-Database (Reference Directory)
Rules Engine
F1
RBAC Repository (Resource Directory)
F2
Customer Portal
B1
C2
Resource Manager Interface
F3
Customer Resource (Applications)
Security Level Interface
C1
Information Assurance

(F) Rules Engines: evaluates user and resource profiles to determine resource access.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SEAC RBAC - Model

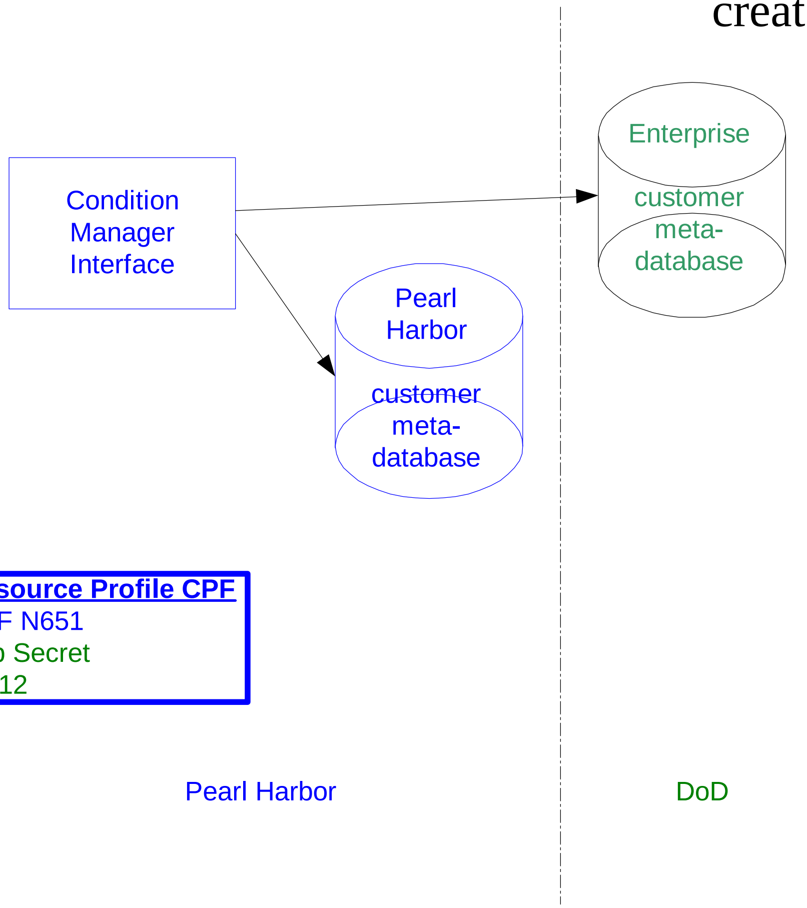

Customer furnished and maintained assets
SEAC RBAC model
Customer Personnel Database
E1
User Profile Manager
E2
DN Generator
E3
D1
Condition Manager Interface
Directory Manager Interface
D2
A1
A2
Customer Meta-Database (Reference Directory)
Rules Engine
F1
RBAC Repository (Resource Directory)
F2
Customer Portal
G2
Condition Deprecator
G1
C2
B1
F3
Resource Manager Interface
Customer Resource (Applications)
Security Level Interface
C1
Information Assurance

(G) Condition deprecation: scans reference directories and compares resource profiles for any changes.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SEAC RBAC - Interoperability

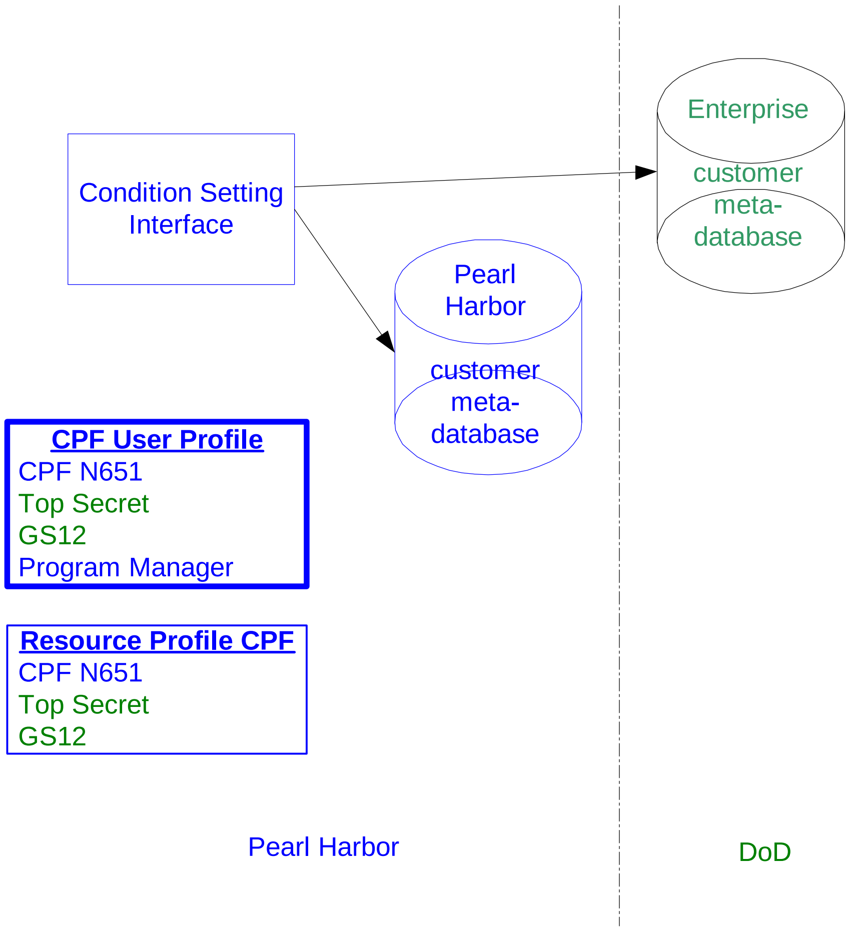
Pearl Harbor: resource profile created for local resource access.



Resource Profile CPF
CPF N651
Top Secret
GS12

SEAC RBAC - Interoperability

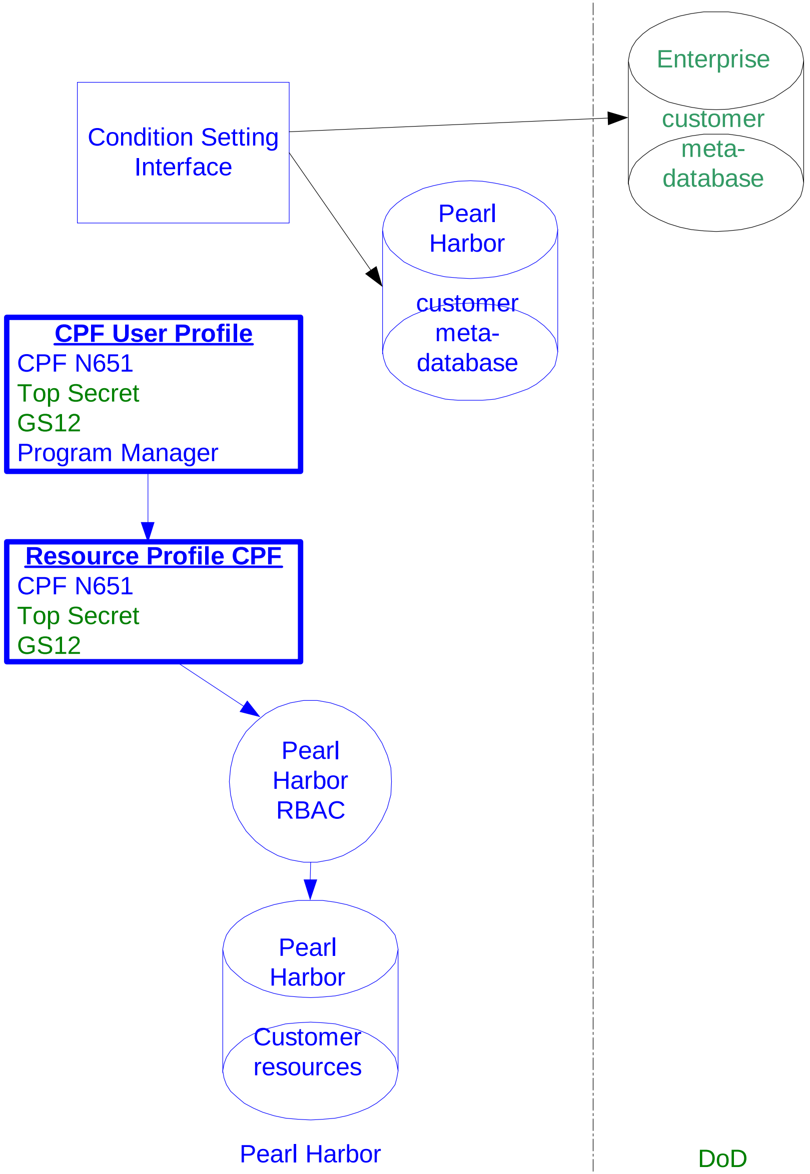
Pearl Harbor: local user profile is generated to access a local resource.



CPF User Profile
CPF N651
Top Secret
GS12
Program Manager

Resource Profile CPF
CPF N651
Top Secret
GS12

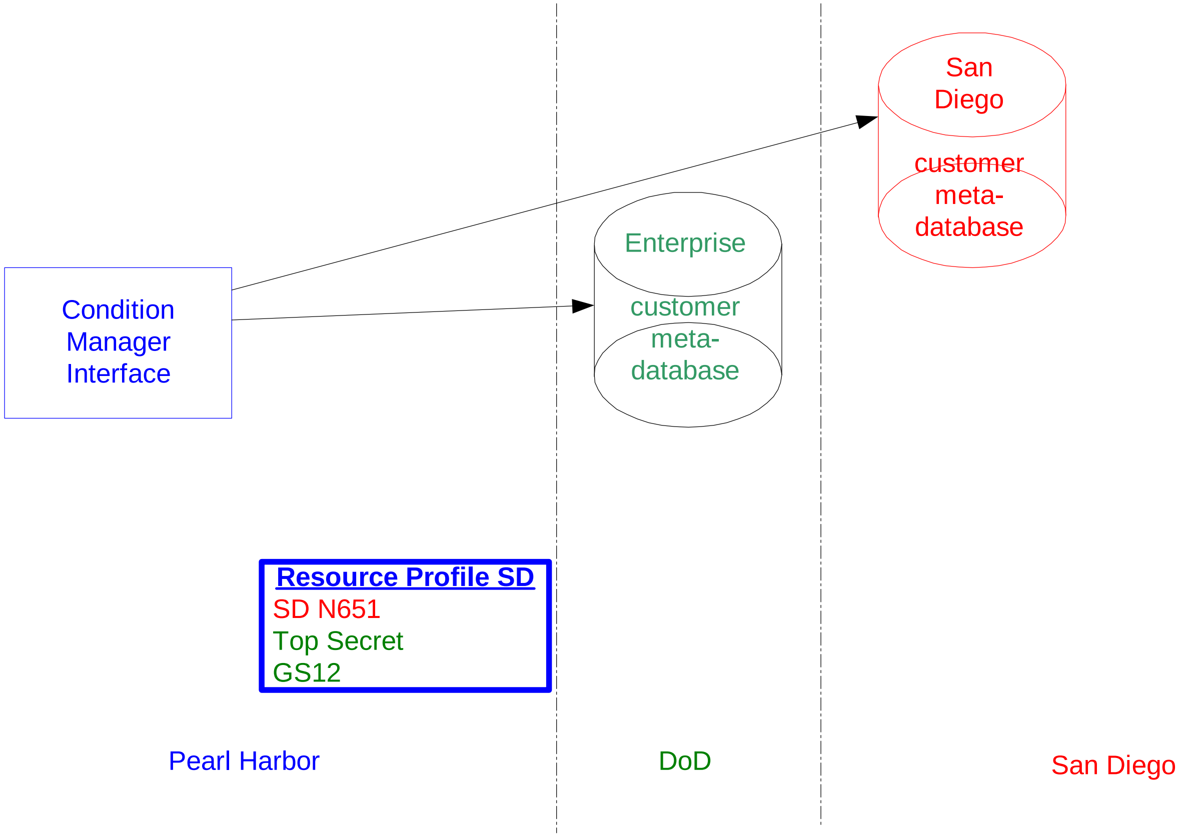
SEAC RBAC - Interoperability



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

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SEAC RBAC - Interoperability



San Diego customer meta-database

Enterprise customer meta-database

Condition Manager Interface

Resource Profile SD
SD N651
Top Secret
GS12

Pearl Harbor

DoD

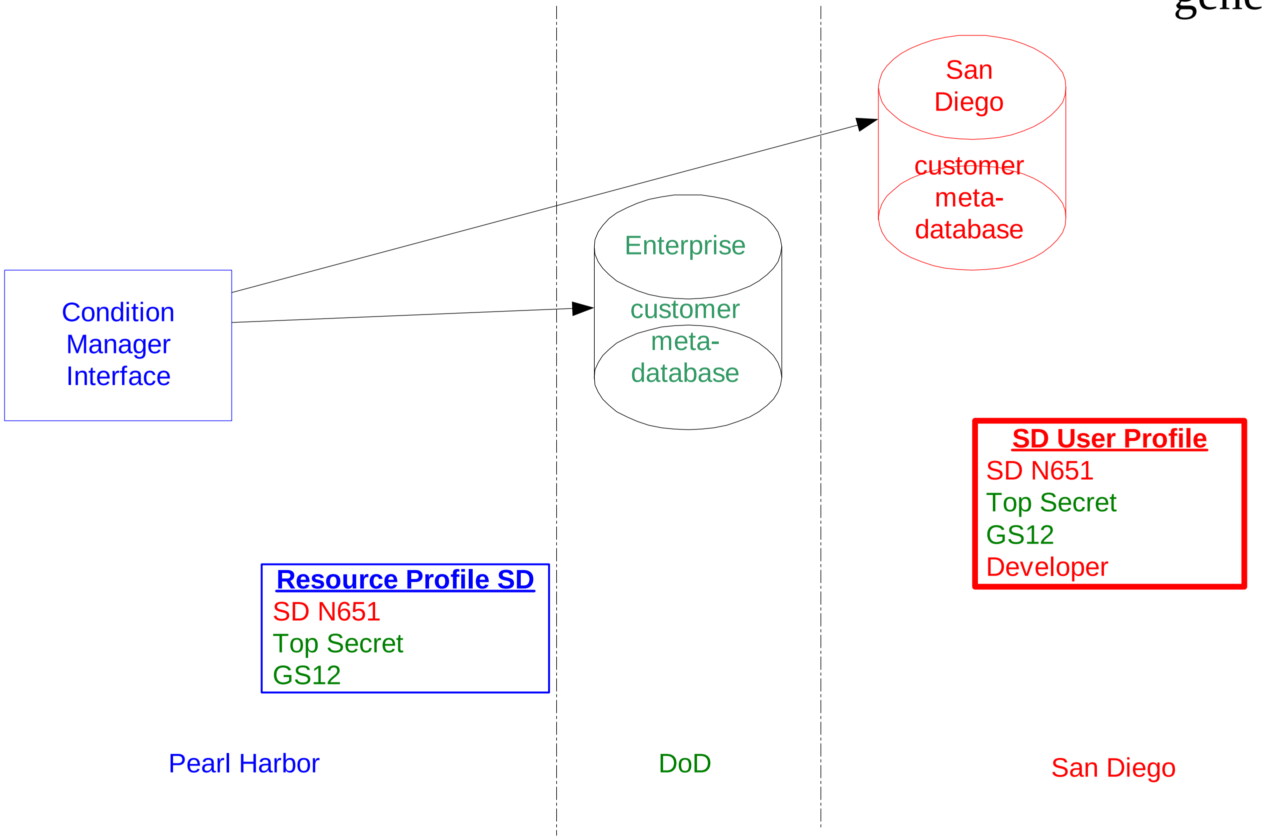
San Diego

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

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SEAC RBAC - Interoperability

San Diego: user profile generated.



Condition Manager Interface

Enterprise customer meta-database

San Diego customer meta-database

SD User Profile
SD N651
Top Secret
GS12
Developer

Resource Profile SD
SD N651
Top Secret
GS12

Pearl Harbor

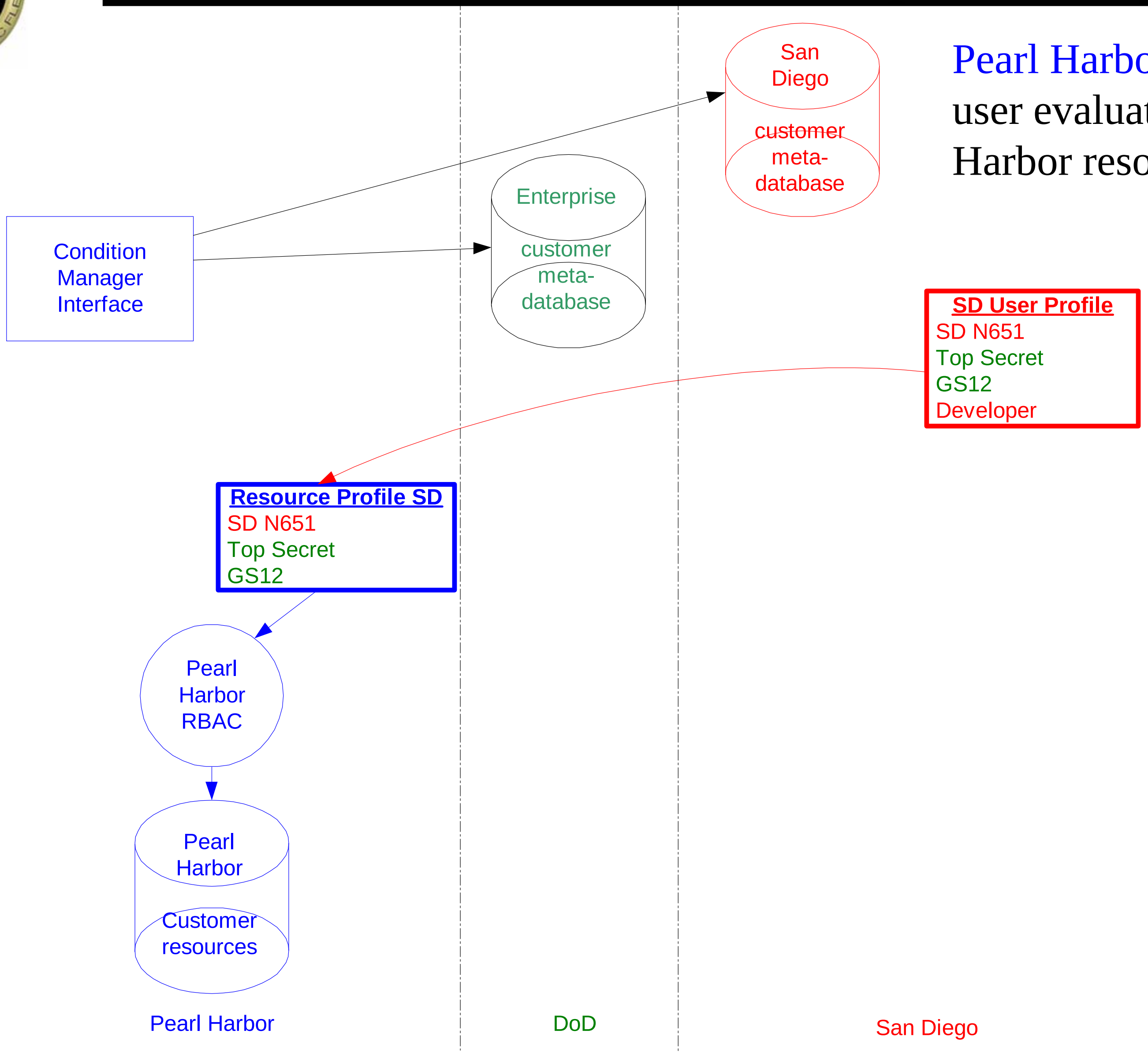
DoD

San Diego

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

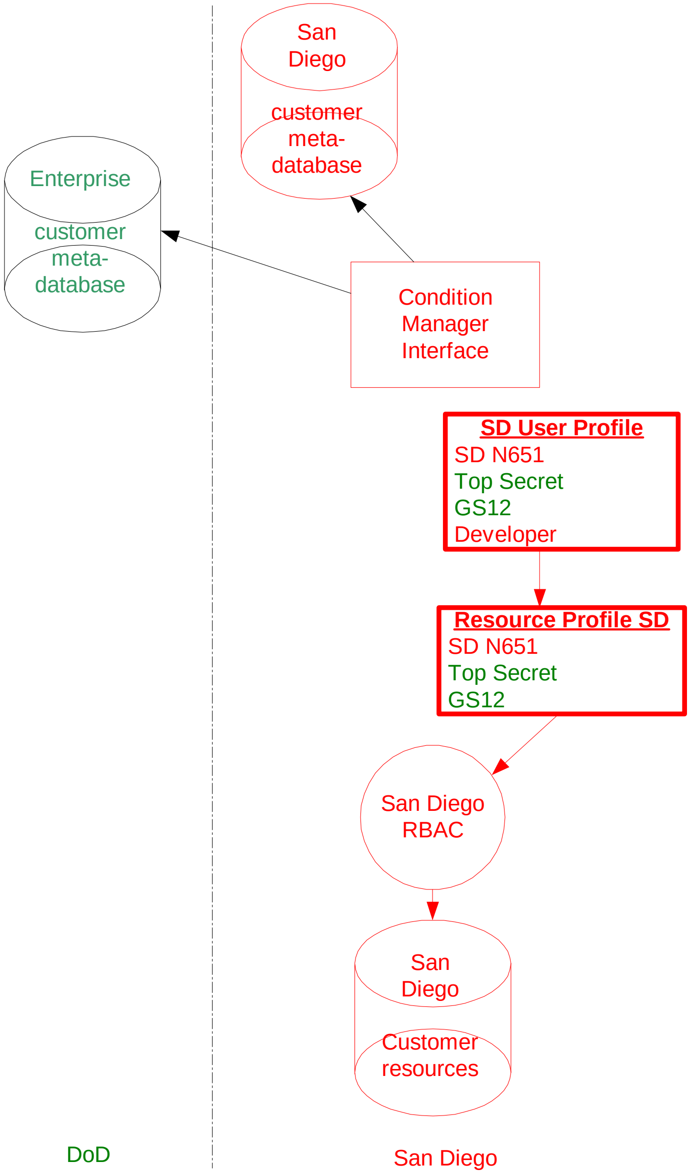
SEAC RBAC - Interoperability

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



The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

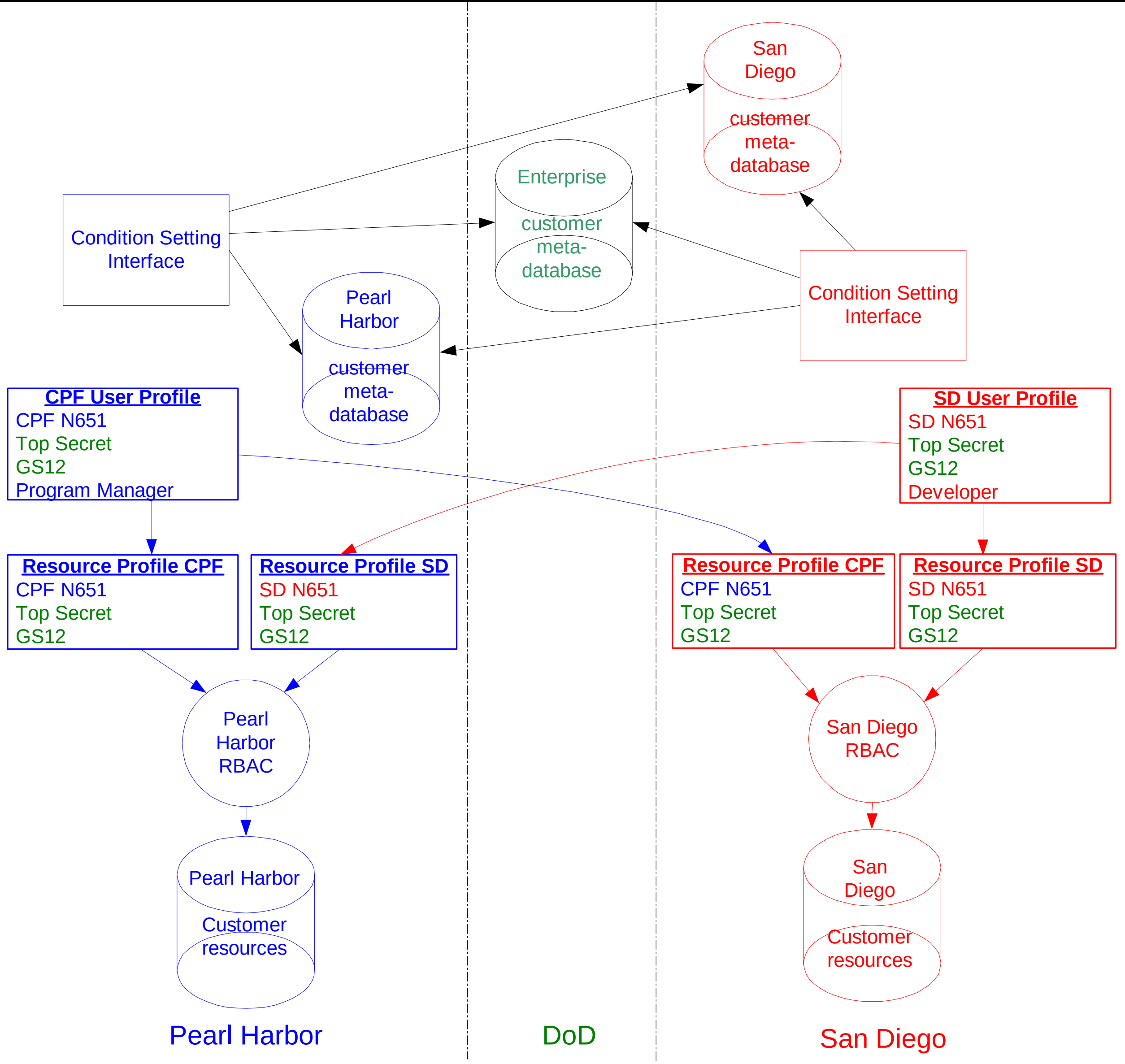
SEAC RBAC - Interoperability


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

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

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SEAC RBAC – Interoperability



The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SD 541, June 2004

SSC San Diego

San Diego, CA 92152-5001