



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

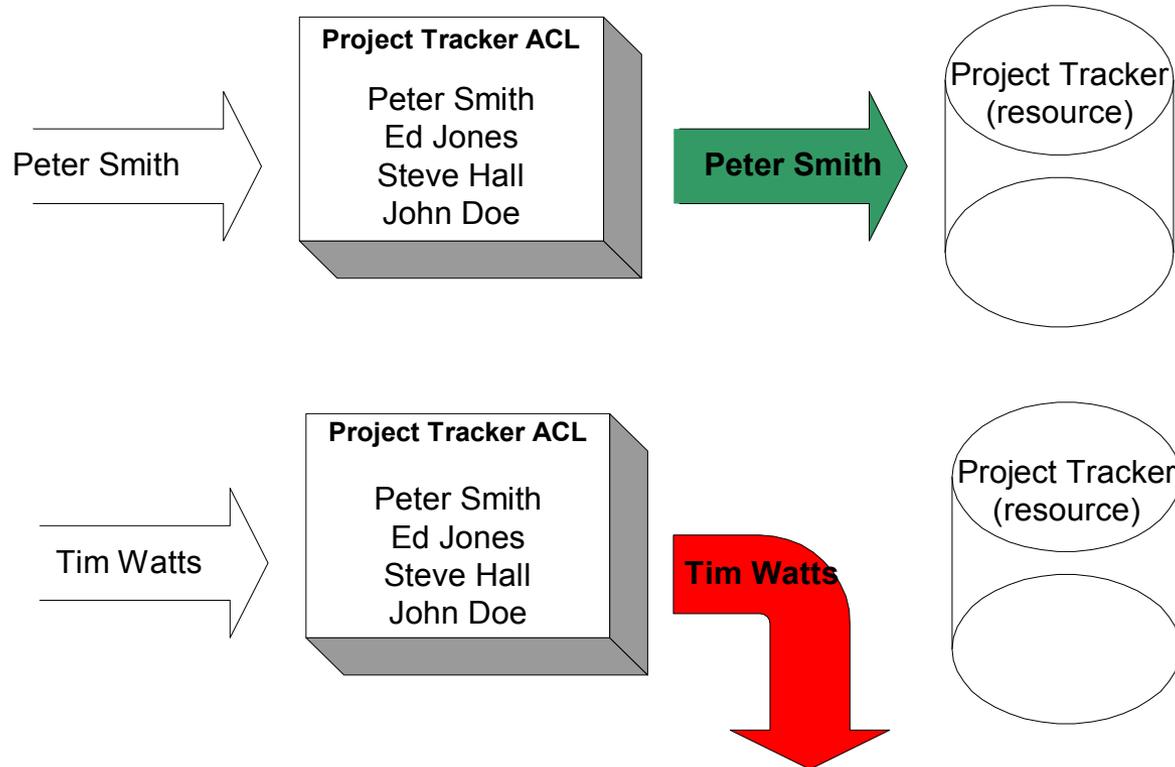
(808) 474-9270

Richard.R.Fernandez@navy.mil



Access Control Lists (ACL)

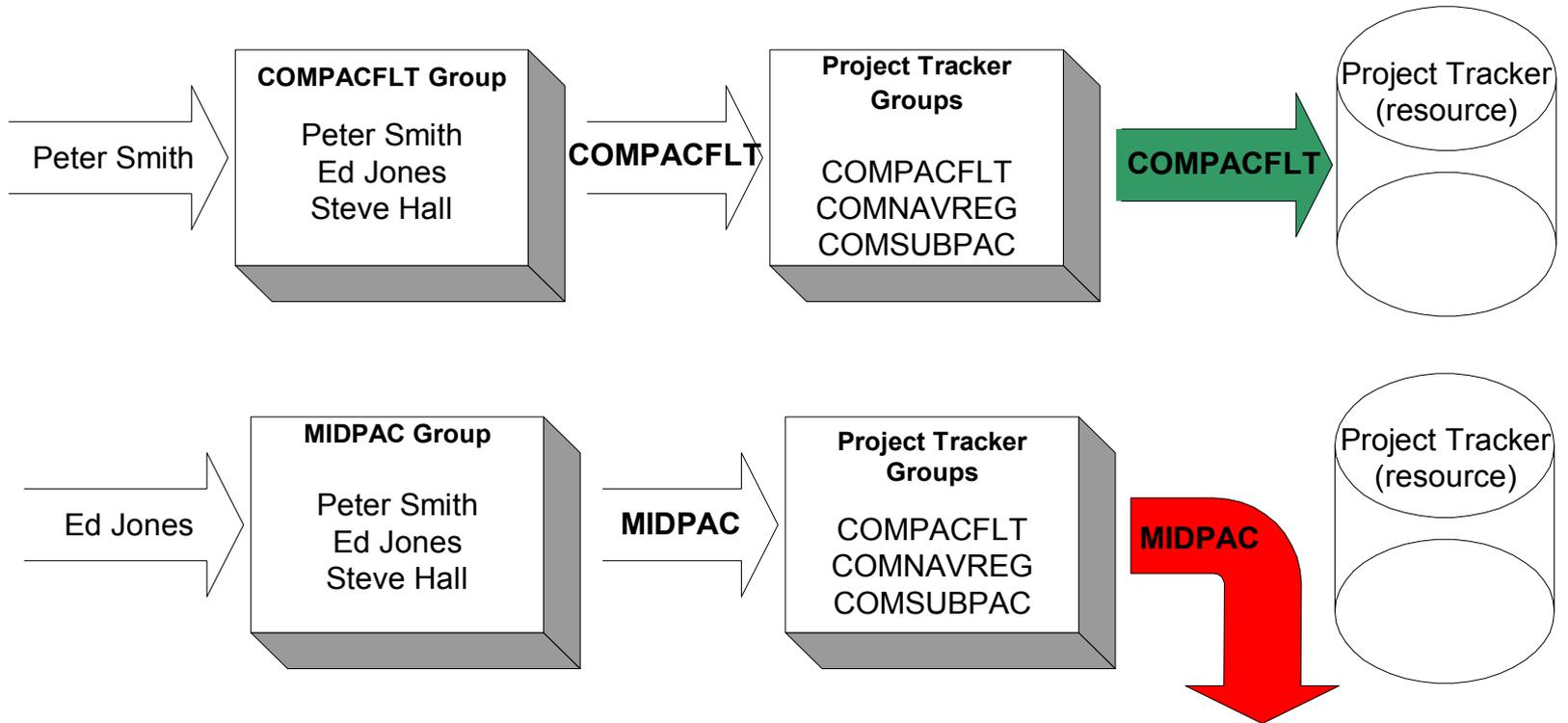
User name or unique identifier associates access to resources





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.

<u>Categories</u>	<u>COMPACFLT</u>	<u>USNR</u>
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

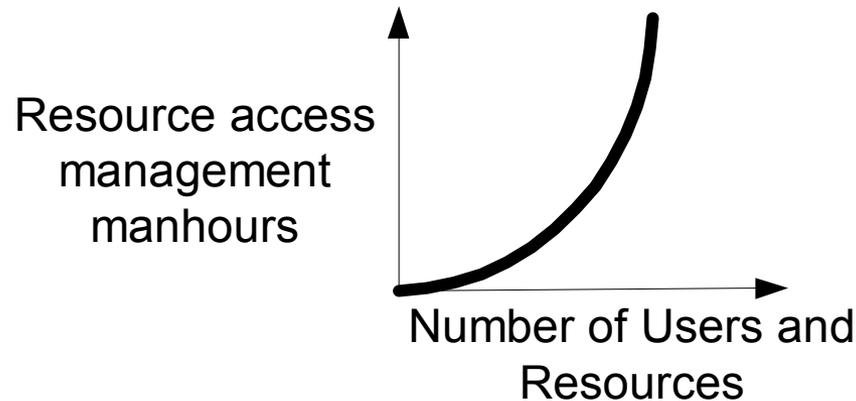


Problems with ACLs and Groups

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) 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.*



Access control comparison

How access control solutions can simultaneously evaluate user characteristics.

User Characteristics

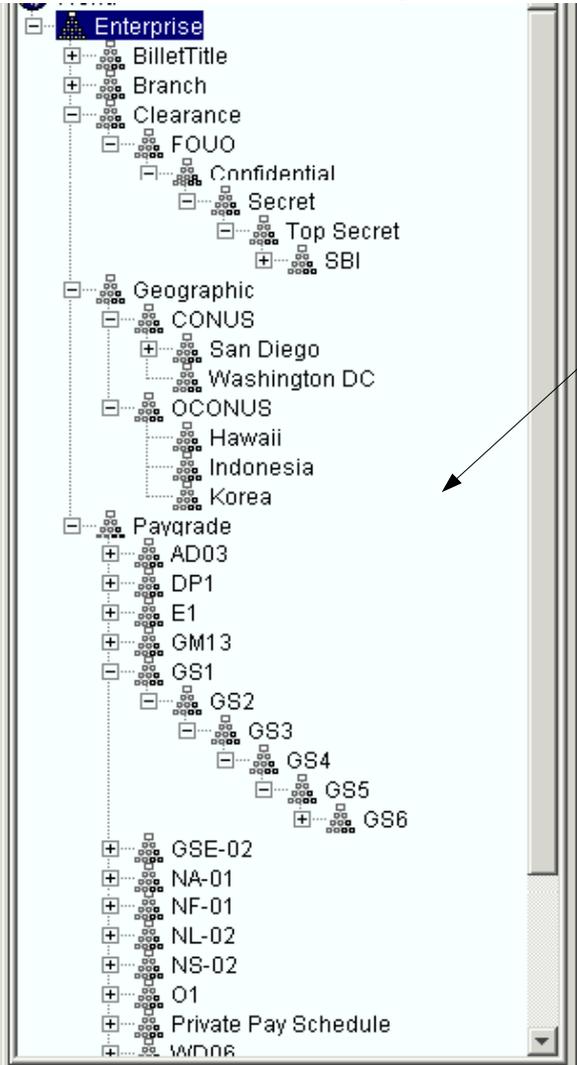
	Number of user characteristics evaluated	Hierarchal evaluation of user characteristics
ACLs	0	No
Groups	1	Yes/No
NIST RBAC	1	Yes
SEAC RBAC	Unlimited	Yes

Note: A hierarchal structure offers inheritance capabilities.



How the SEAC RBAC works

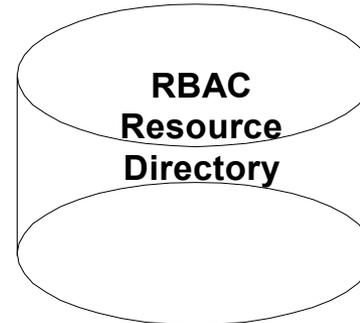
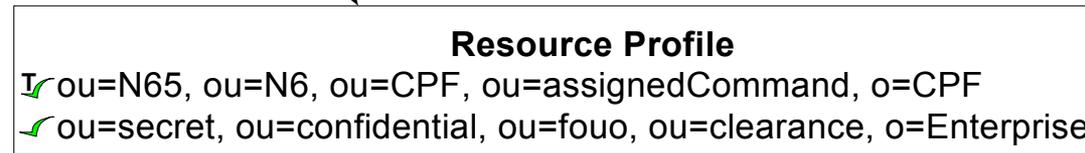
Customer Meta-Database (Reference Directory)



Step 1:

Resource manager establishes a set of conditions to access a resource.

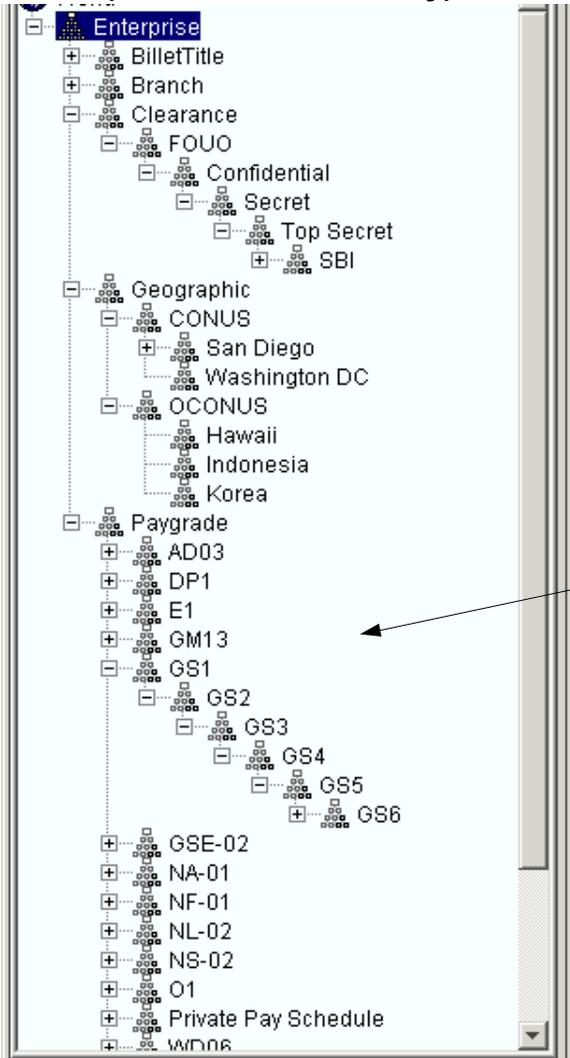
These set of conditions represent a **resource profile**.





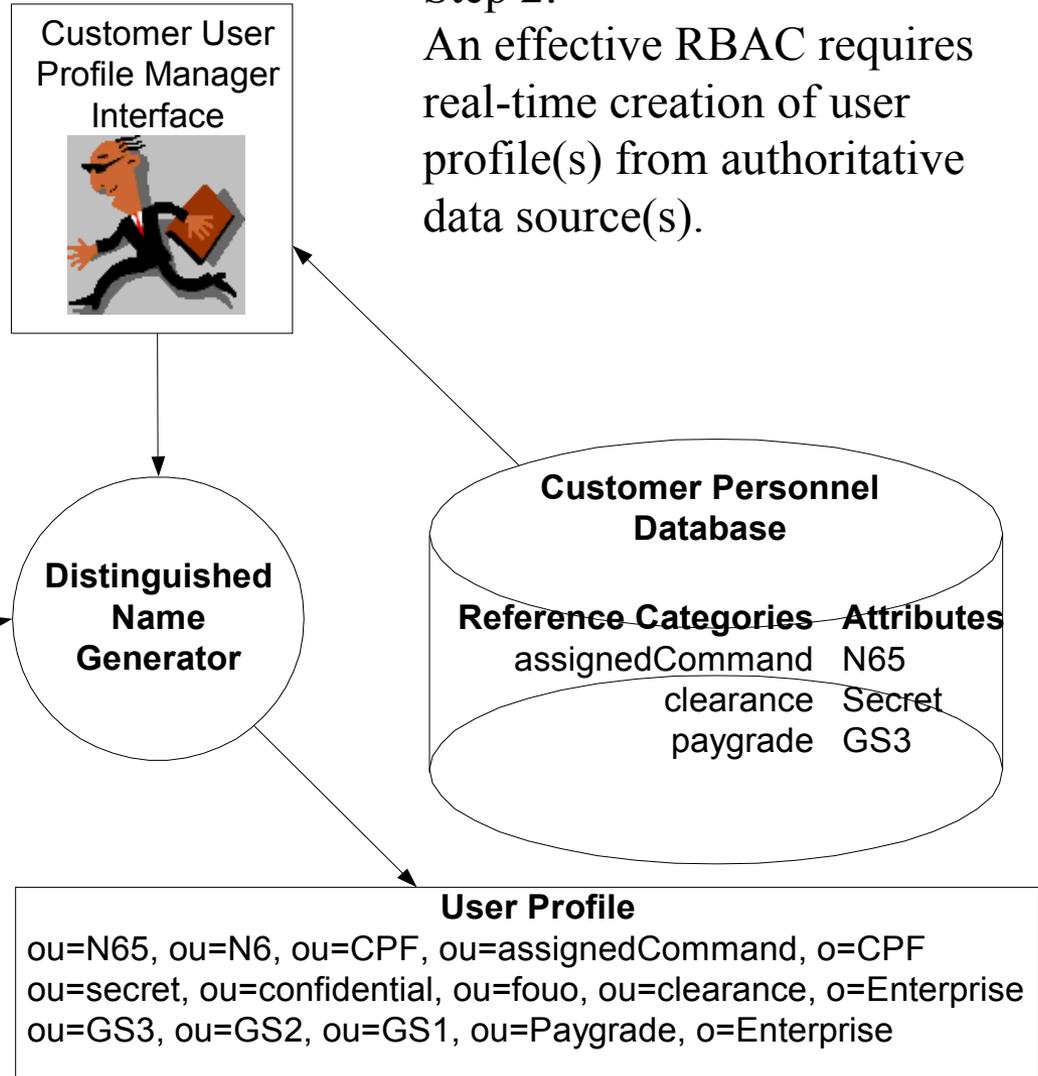
How the SEAC RBAC works

Customer Meta-Database (Reference Directory)



Step 2:

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

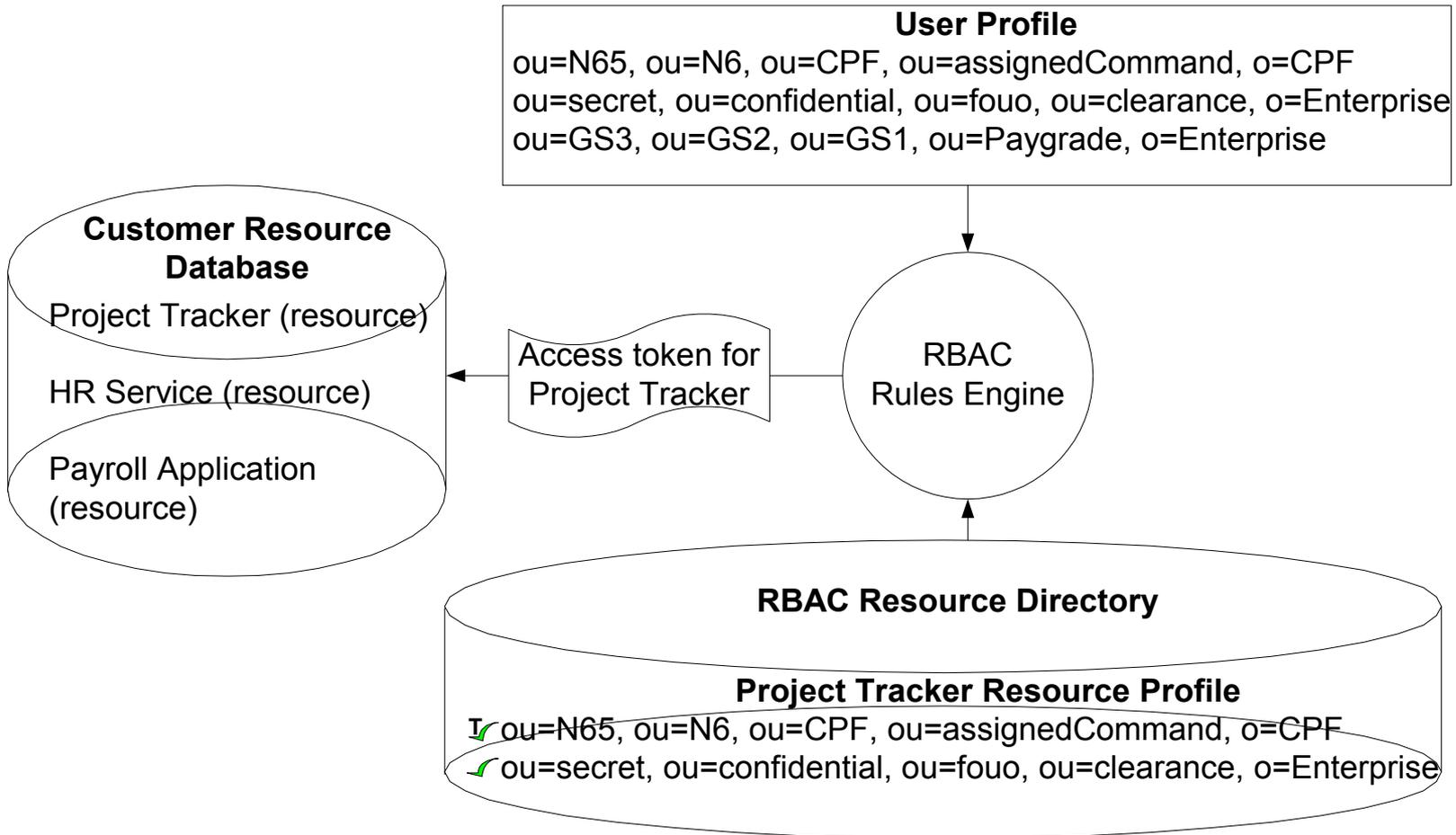




How the SEAC RBAC works

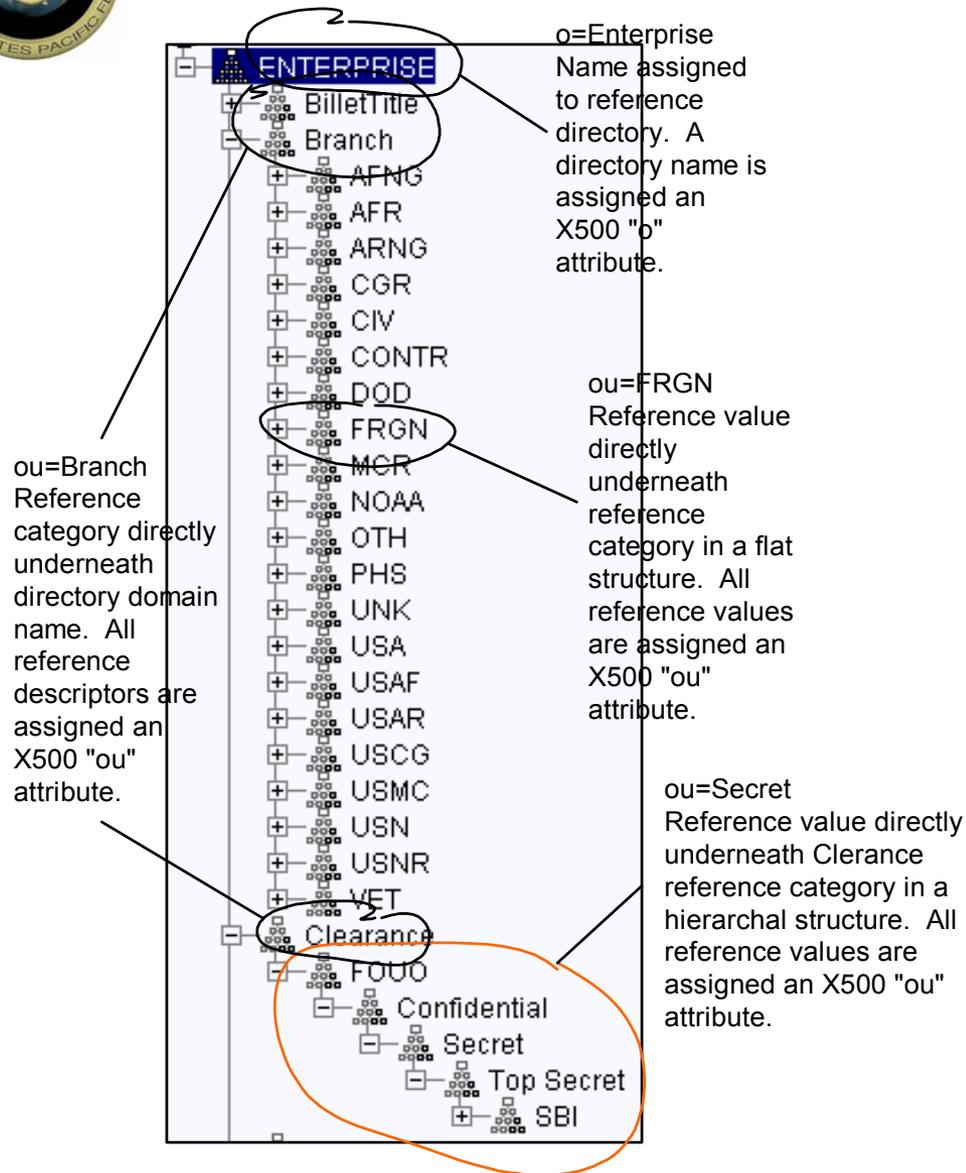
Step 3:

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





Reference directory standard specifications



- 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	CPF N6 Users T ✓ CPF N6 T ✓ GS12 Mon & Thurs 0800 -1300	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

	CPF Guest	CSP Guest	CNR Guests
INFOCON A	Guest	Deny	Deny
User	Deny	Deny	Deny
Admin	Deny	Deny	Deny
INFOCON B	Guest	Deny	Deny
User	Deny	Deny	Deny
Admin	Deny	Deny	Deny
INFOCON C	Guest	Deny	Deny
User	Deny	Deny	Deny
Admin	Deny	Deny	Deny
INFOCON D	Guest	Deny	Deny
User	Deny	Deny	Deny
Admin	Deny	Deny	Deny

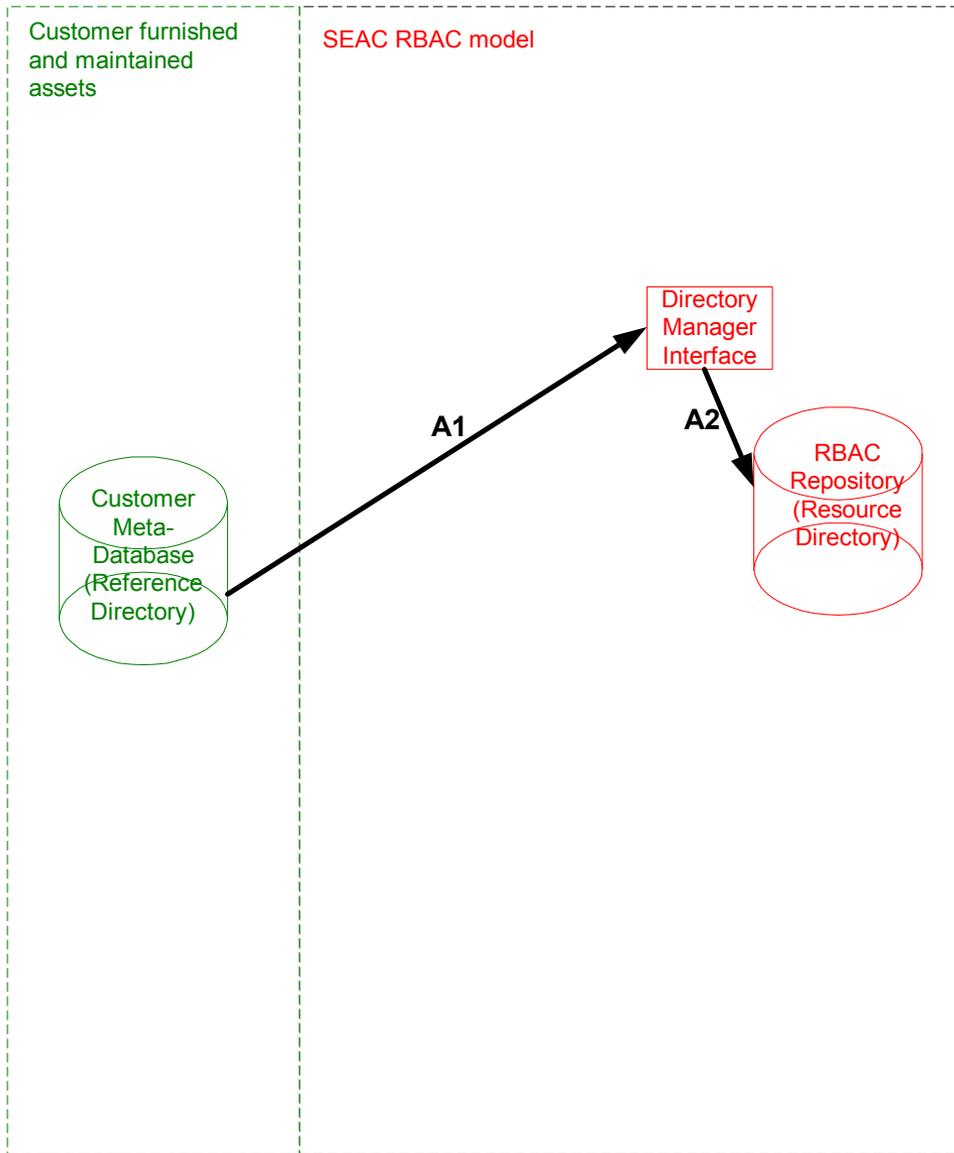
During INFOCON C

	CPF Guest	CSP Guest	CNR Guests
INFOCON A	Guest	Deny	Deny
User	Deny	Deny	Deny
Admin	Deny	Deny	Deny
INFOCON B	Guest	Deny	Deny
User	Deny	Deny	Deny
Admin	Deny	Deny	Deny
INFOCON C	Guest	Deny	Deny
User	Deny	Deny	Deny
Admin	Deny	Deny	Deny
INFOCON D	Guest	Deny	Deny
User	Deny	Deny	Deny
Admin	Deny	Deny	Deny

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



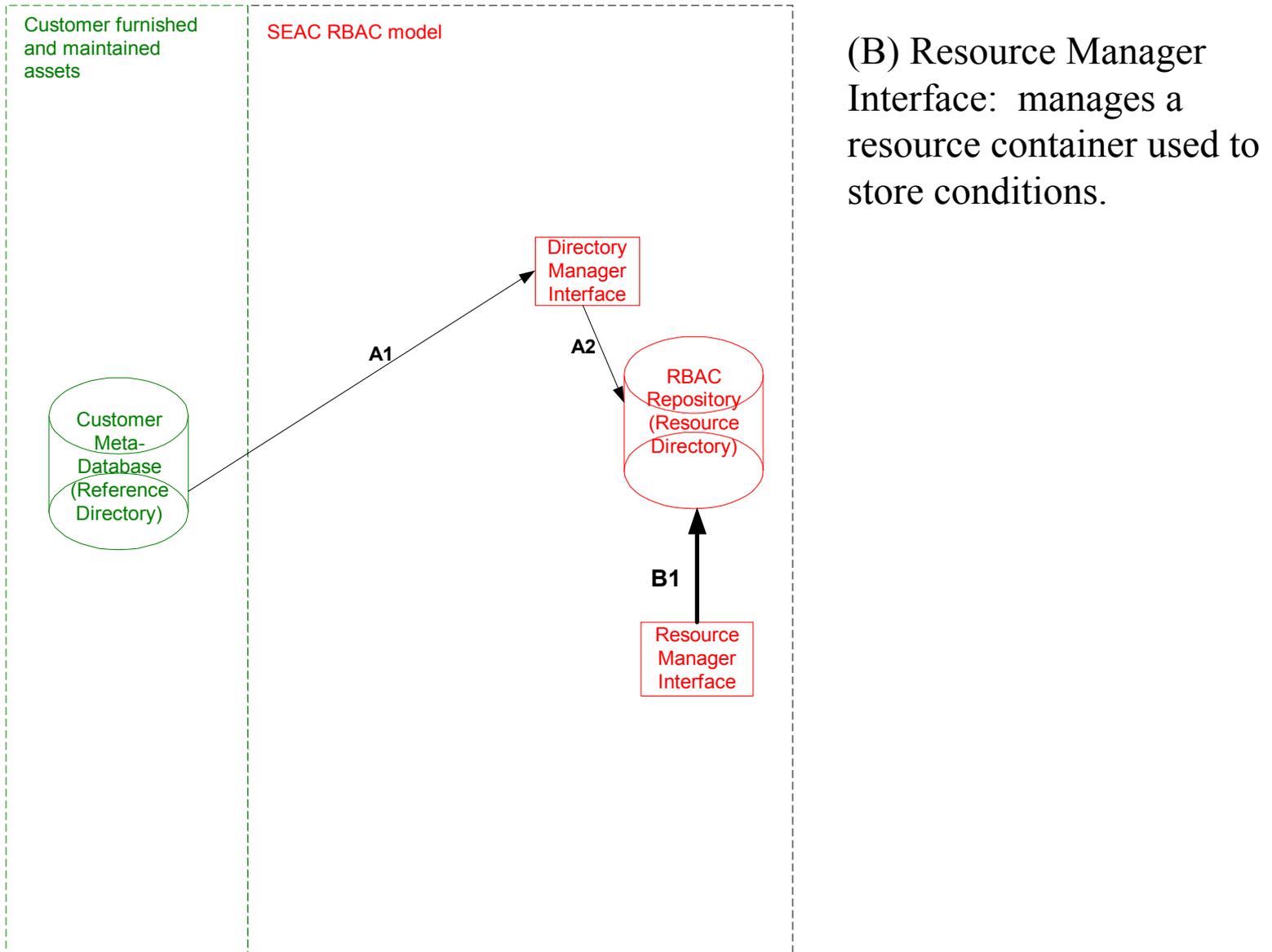
SEAC RBAC - Model



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

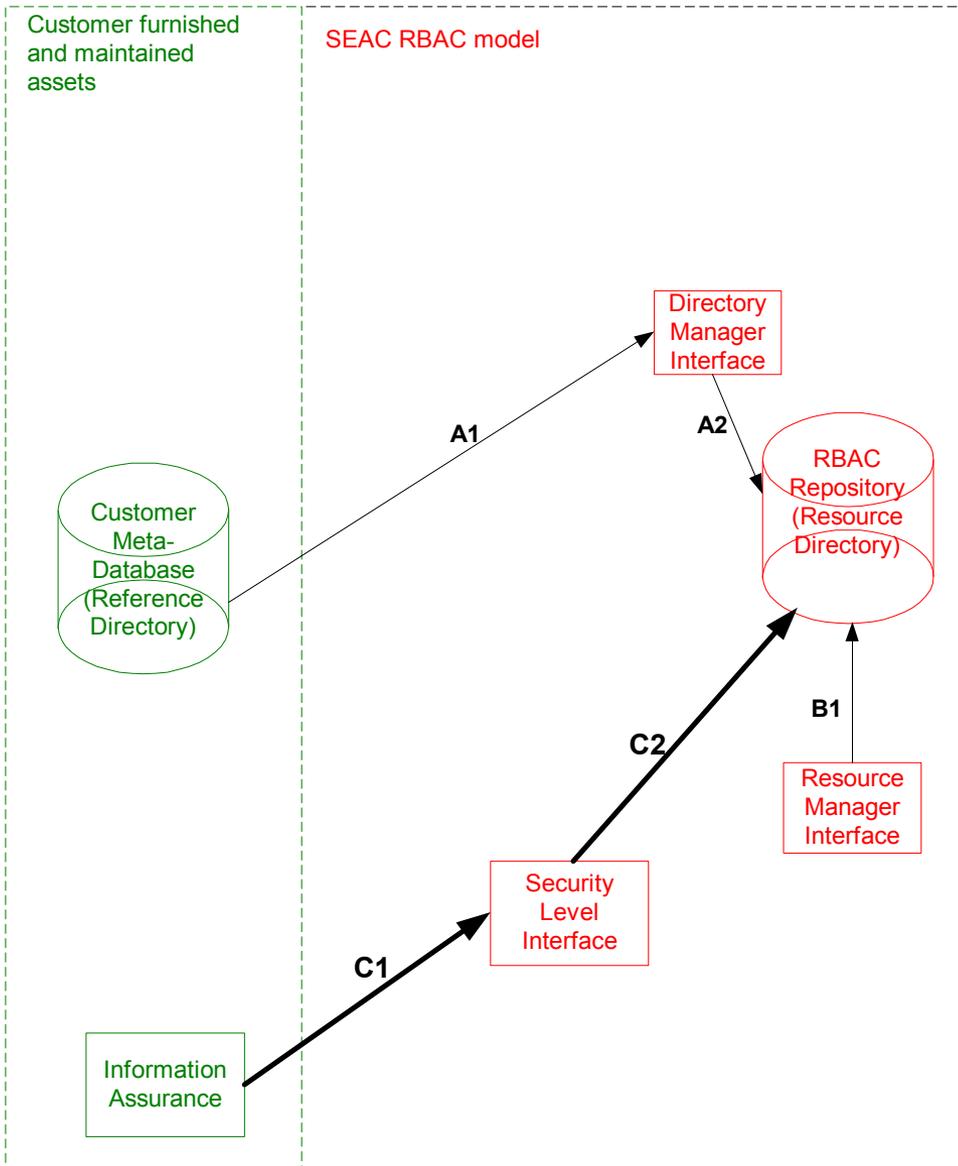


SEAC RBAC - Model





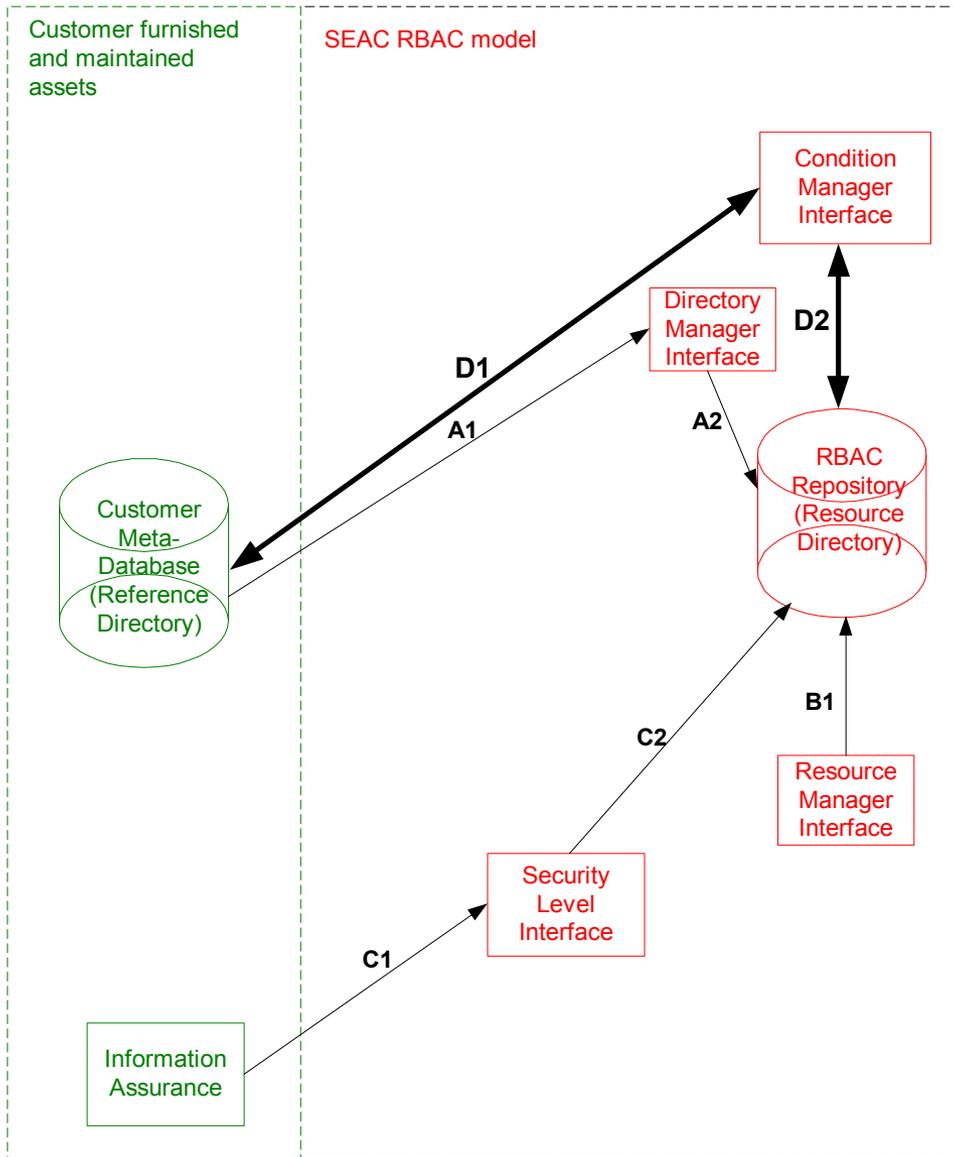
SEAC RBAC - Model



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



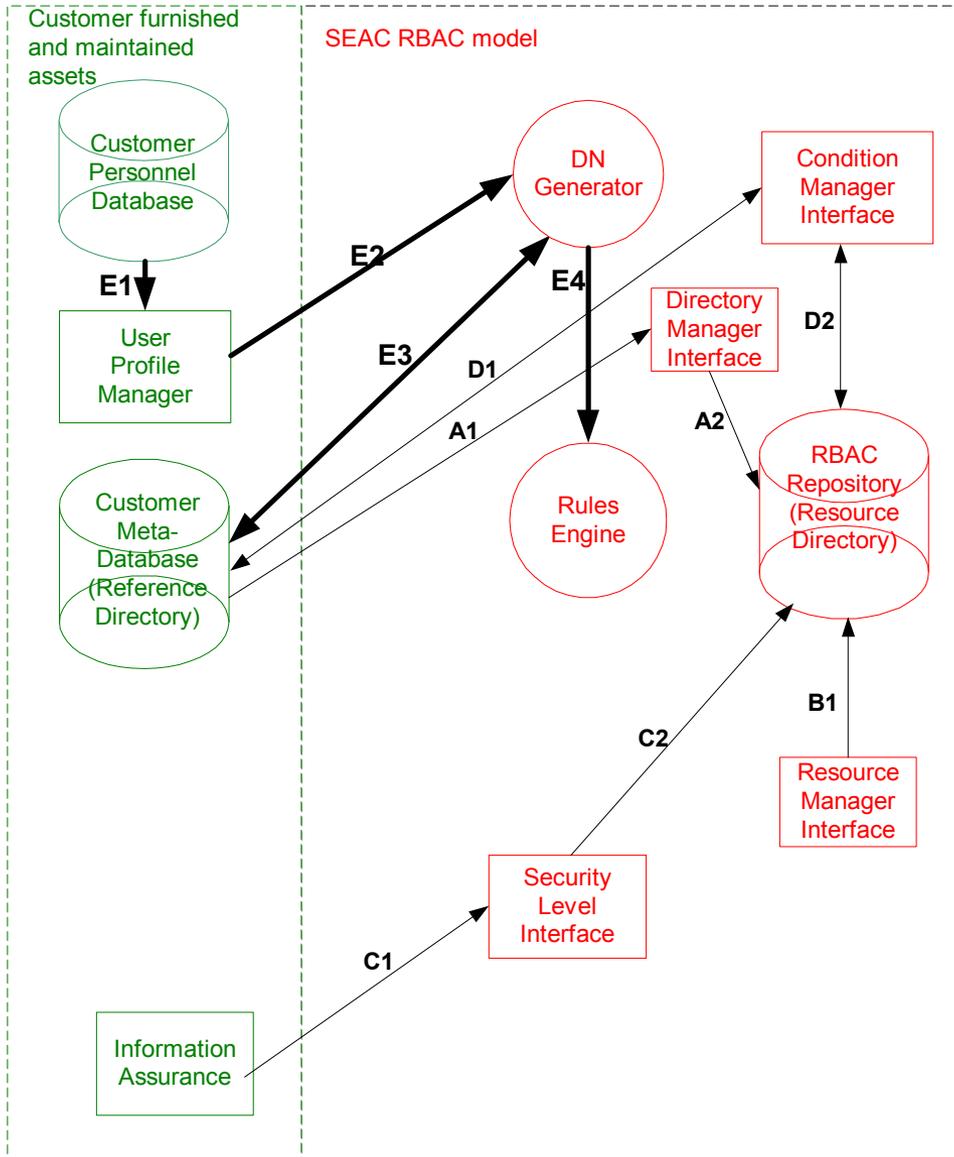
SEAC RBAC - Model



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



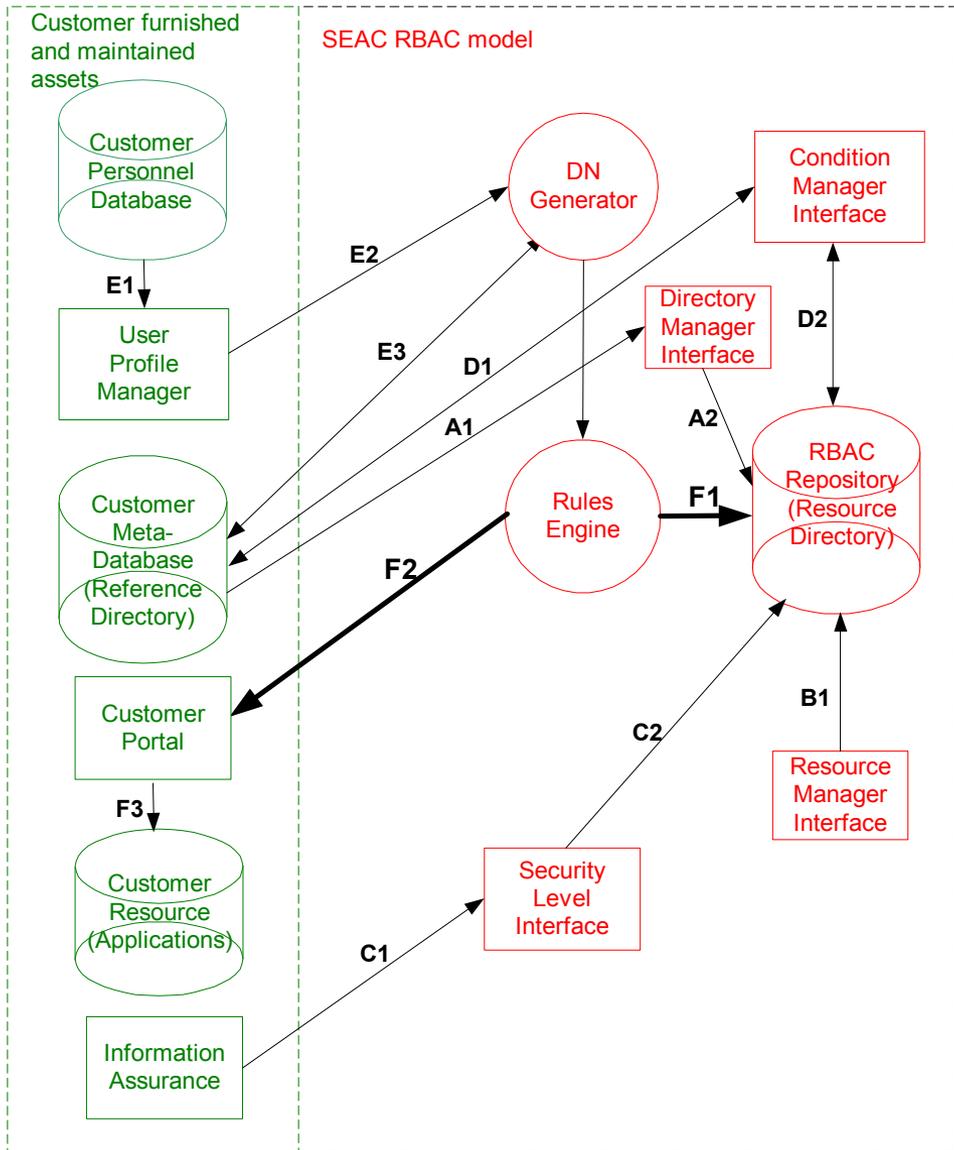
SEAC RBAC - Model



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



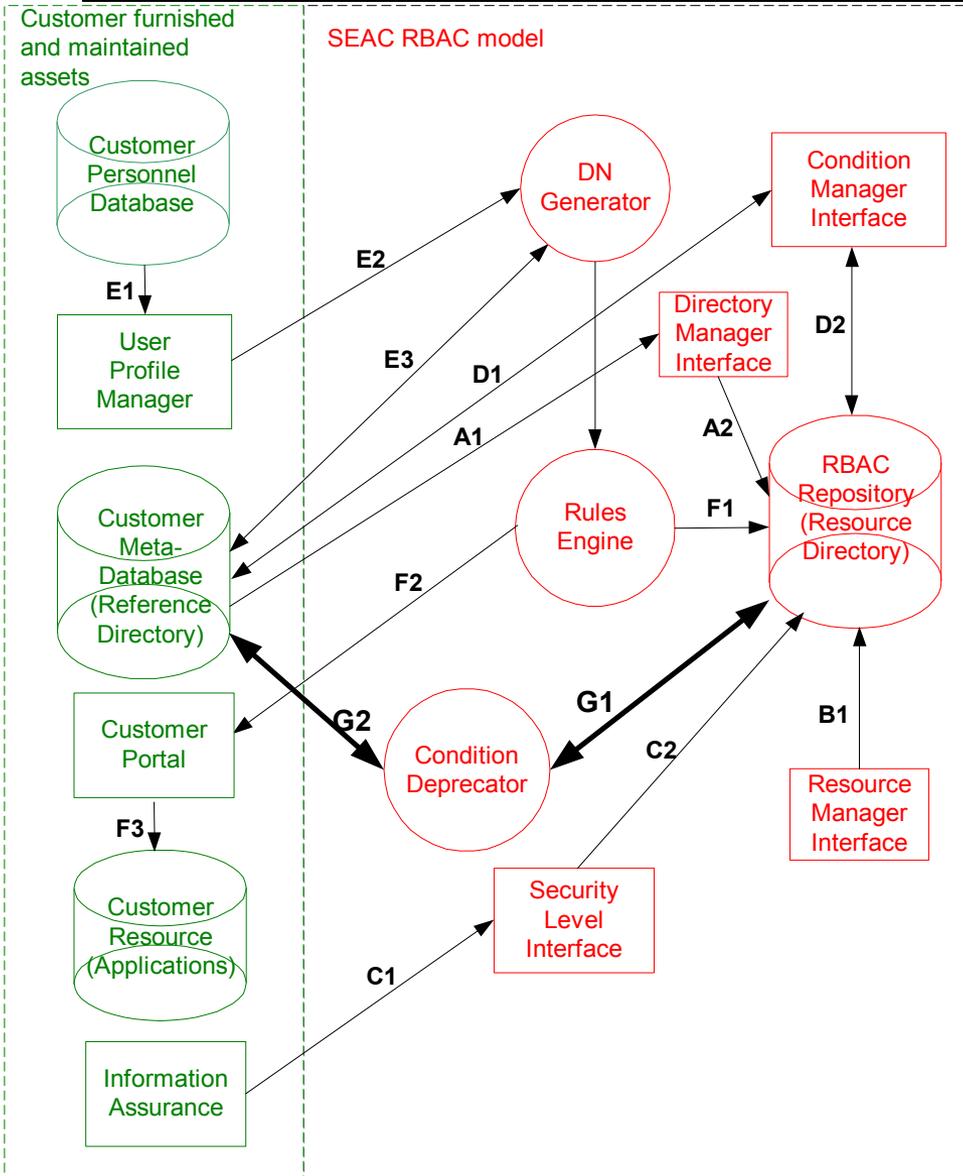
SEAC RBAC - Model



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



SEAC RBAC - Model

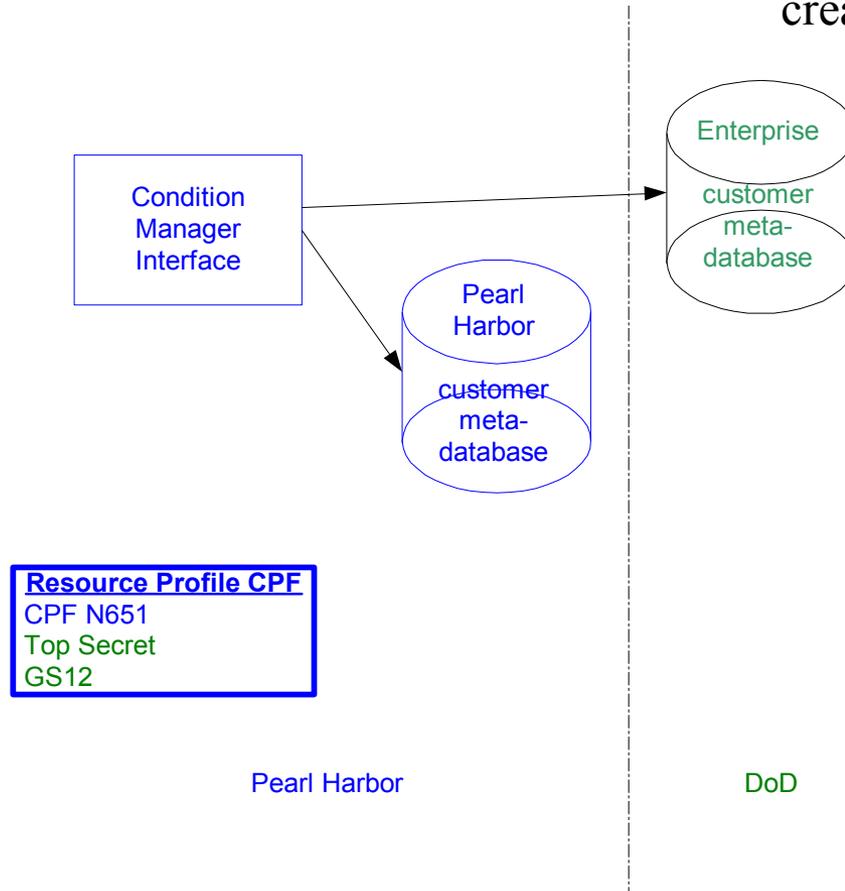


(G) Condition deprecation: scans reference directories and compares resource profiles for any changes.



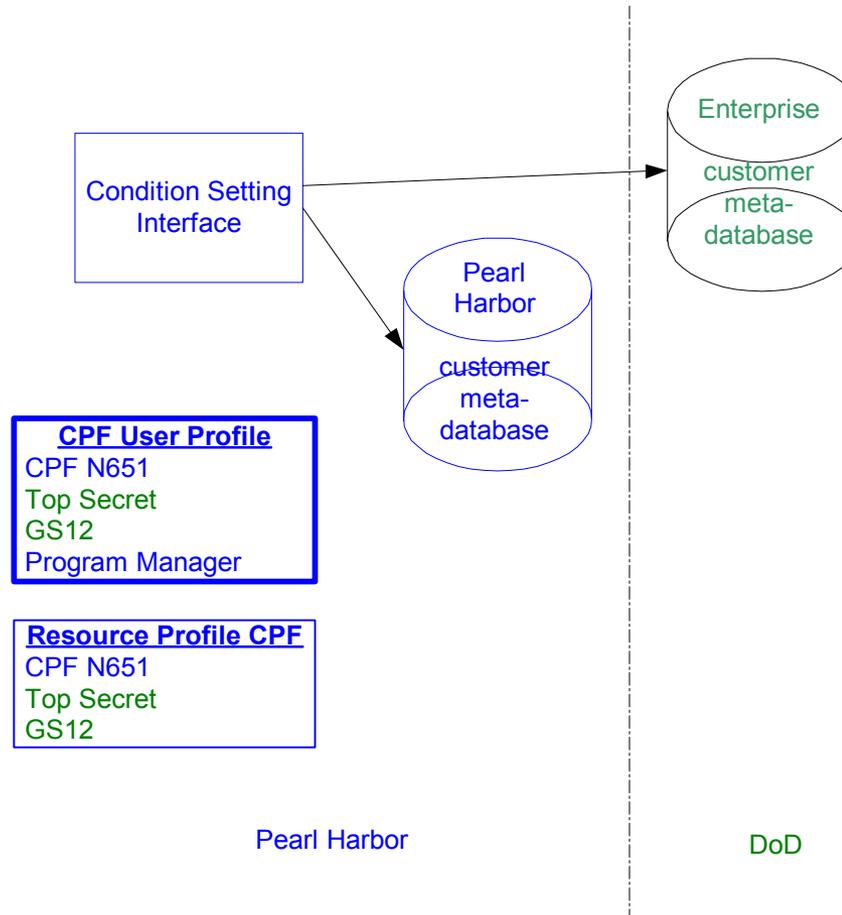
SEAC RBAC - Interoperability

Pearl Harbor: resource profile created for local resource access.





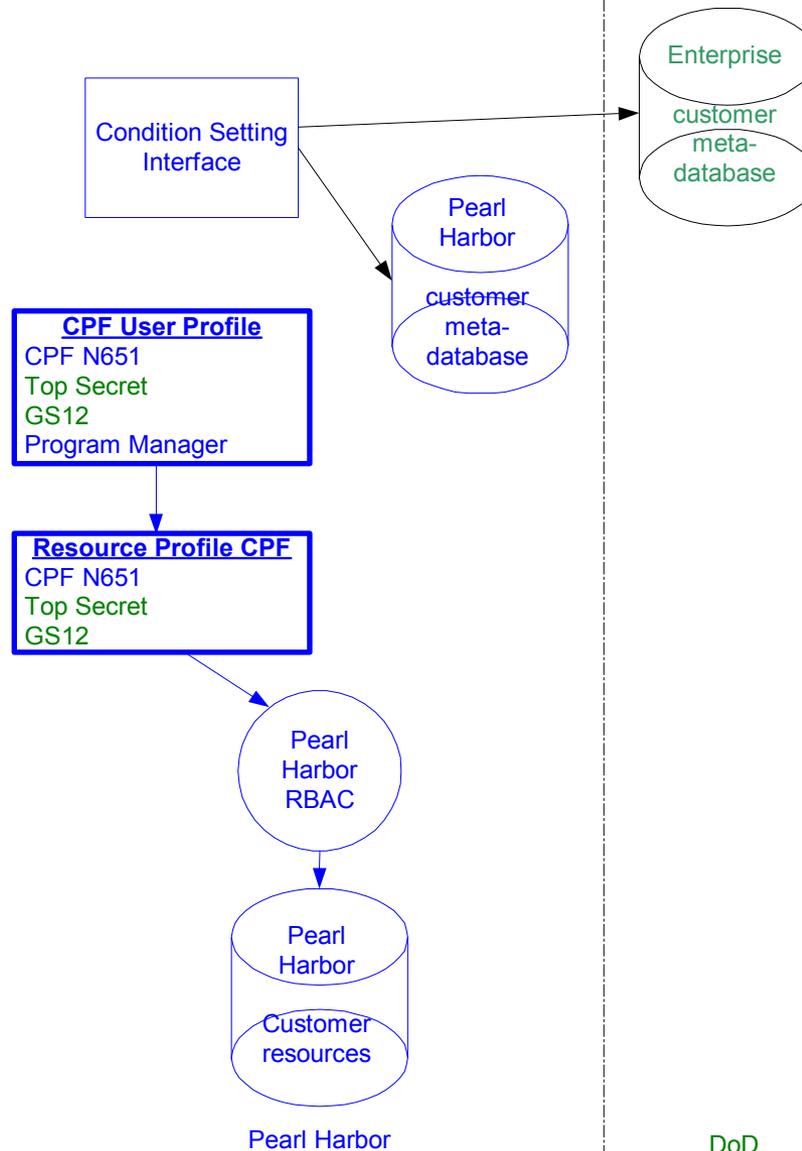
SEAC RBAC - Interoperability



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



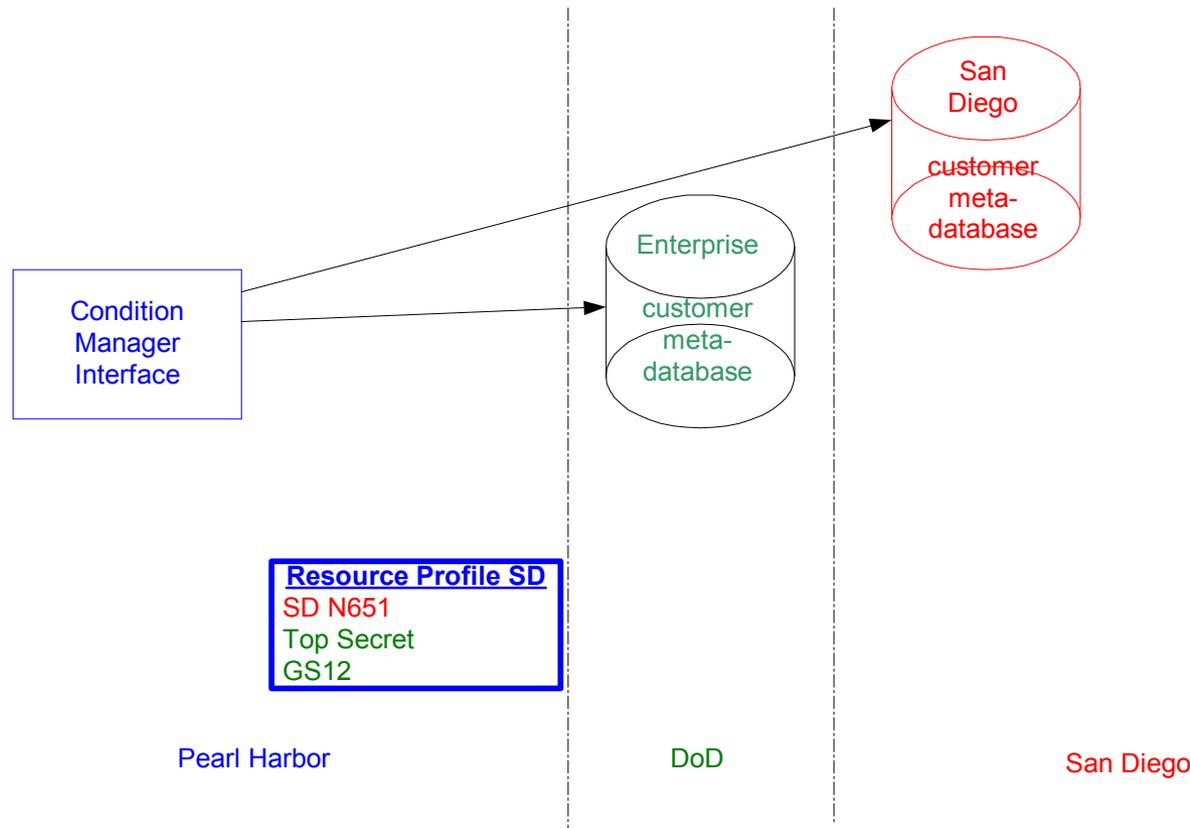
SEAC RBAC - Interoperability



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



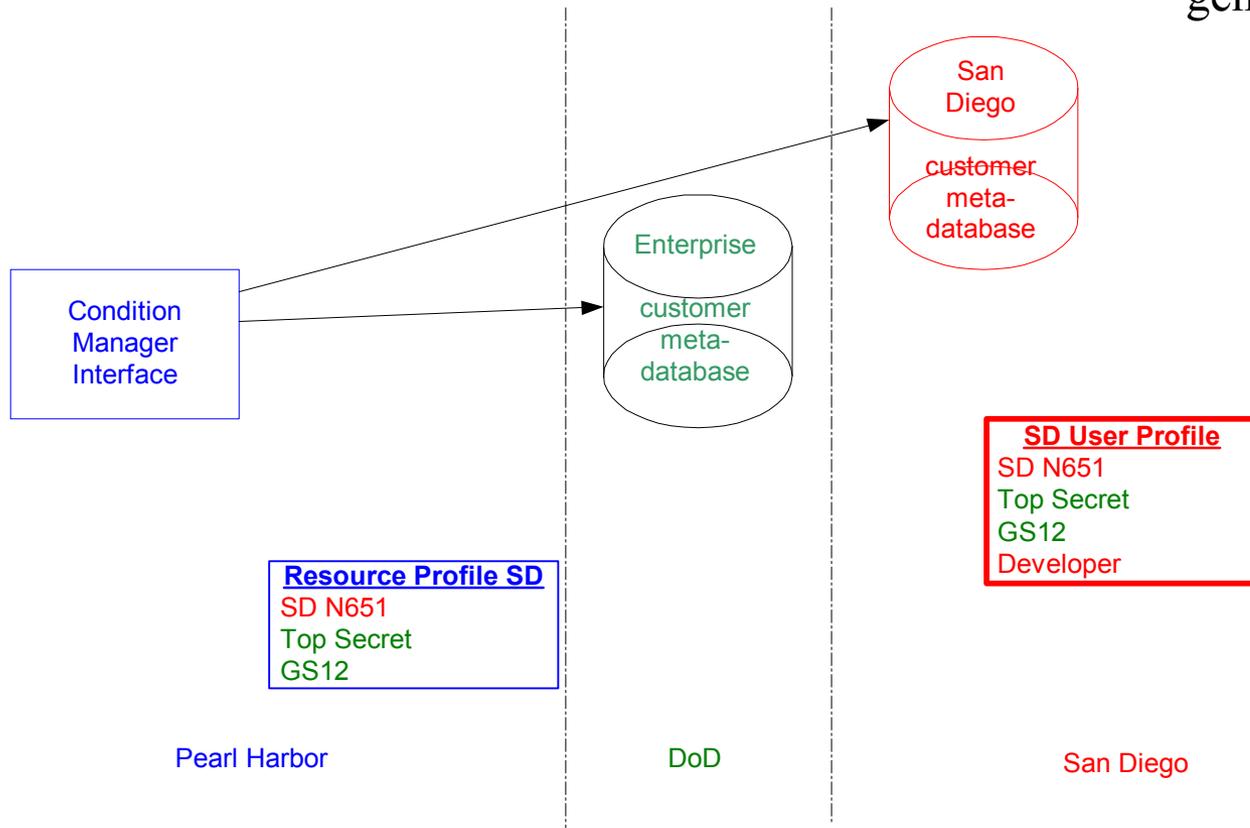
SEAC RBAC - Interoperability



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



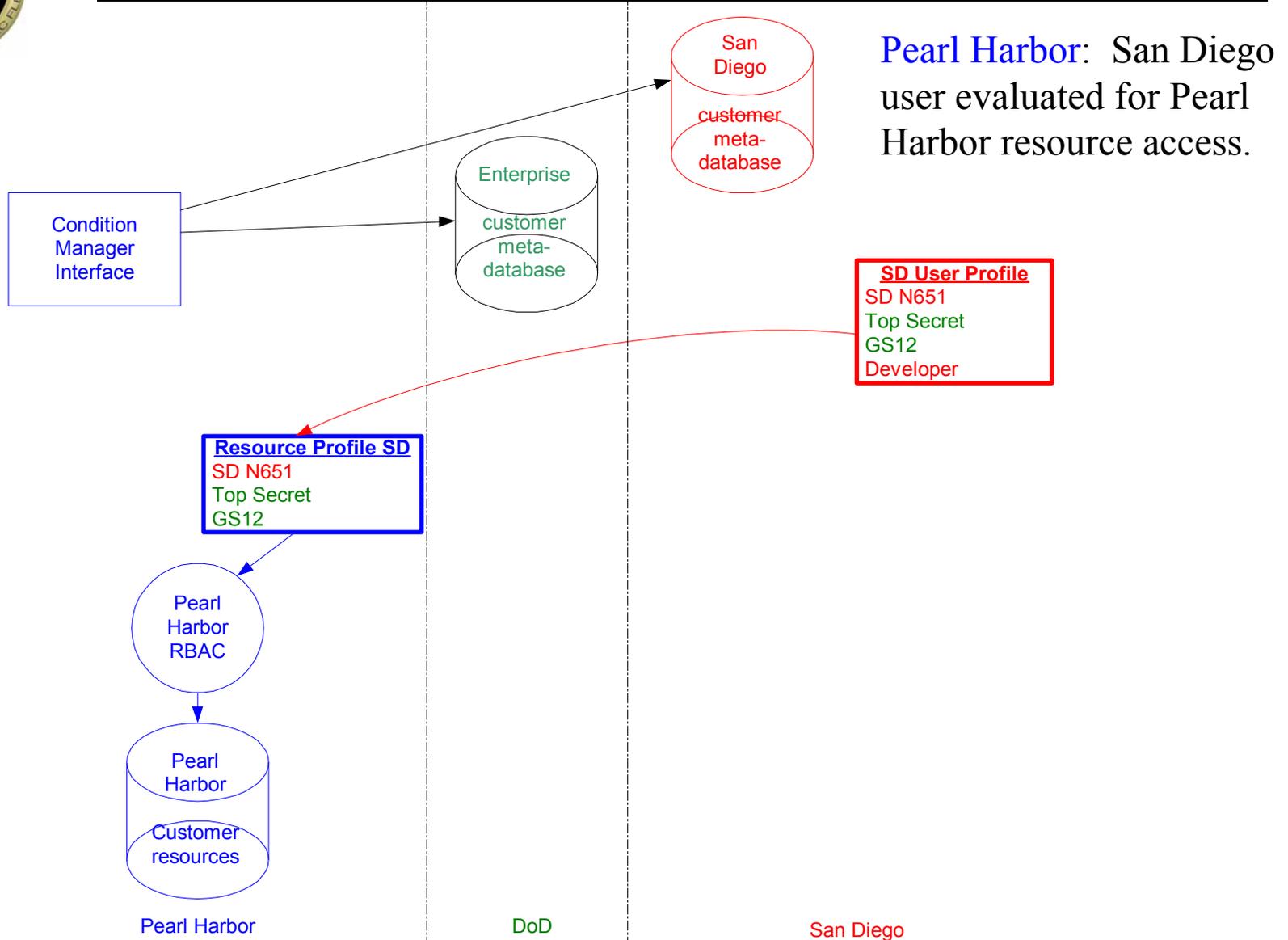
SEAC RBAC - Interoperability



San Diego: user profile generated.



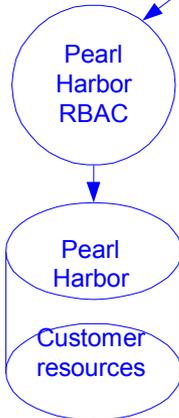
SEAC RBAC - Interoperability



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

SD User Profile
SD N651
Top Secret
GS12
Developer

Resource Profile SD
SD N651
Top Secret
GS12



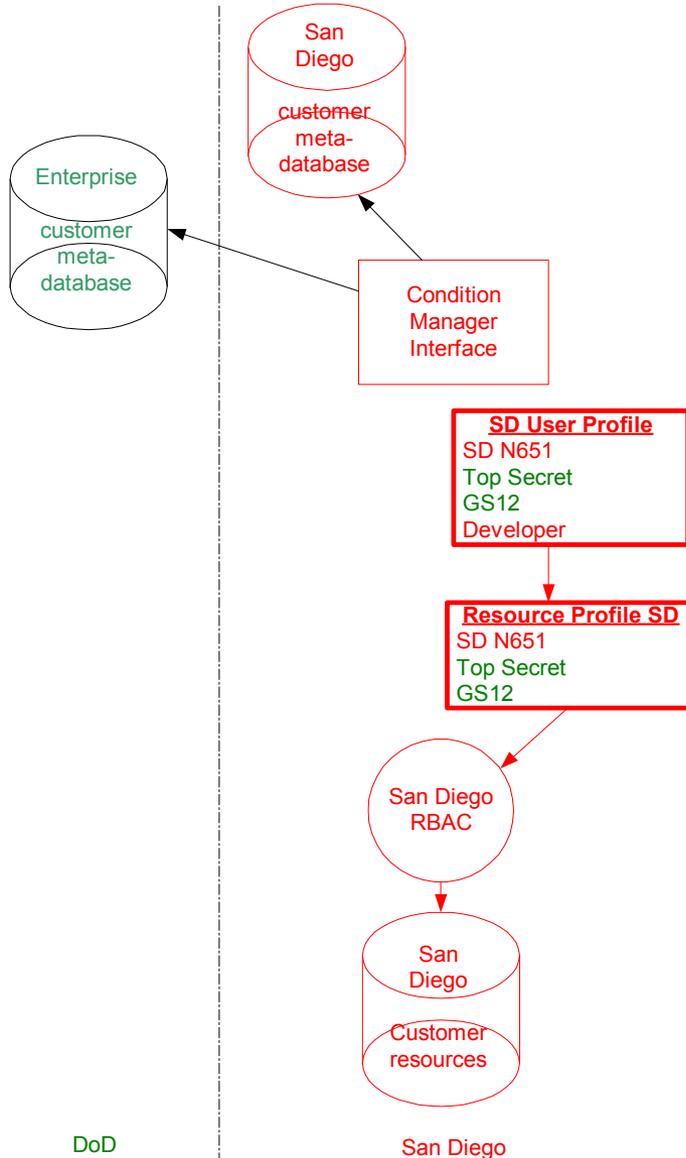
Pearl Harbor

DoD

San Diego



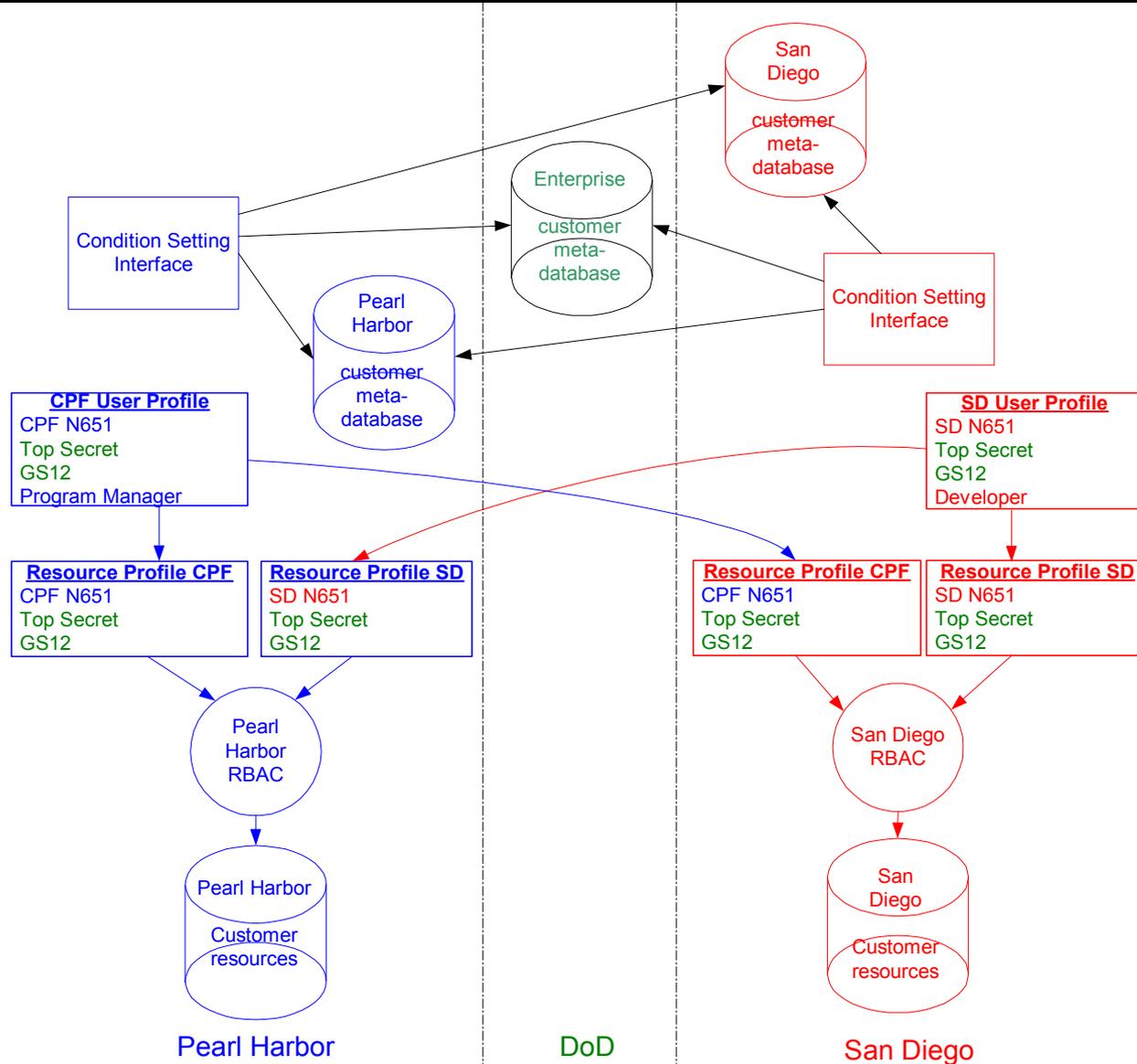
SEAC RBAC - Interoperability



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



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.

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.