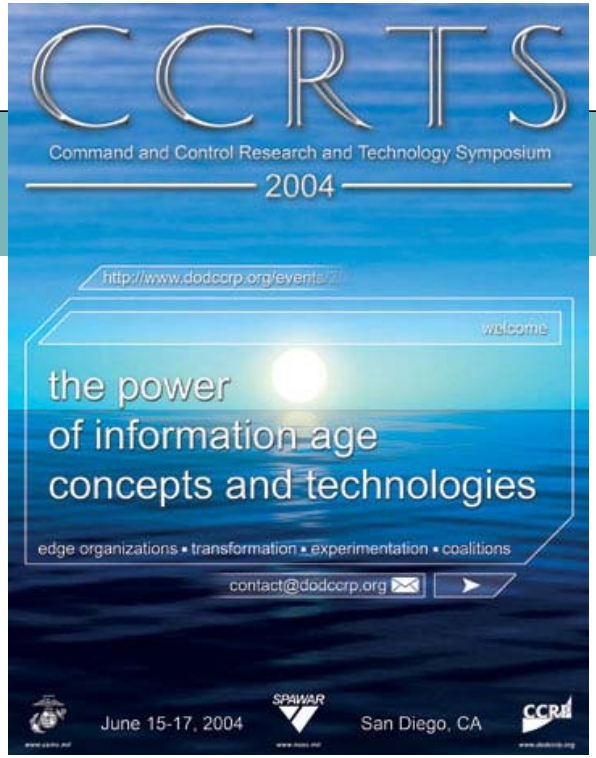


An Employee-Owned Company

Identity Management: Role Based Access Control for Enterprise Services

16 June 2004

Rick Kooker, PMP

Stephan Kane, PMP

Information Management Evolution

SAIC®
An Employee-Owned Company

- **1960's-1990's Challenges**
  - Lacked bandwidth
  - Lacked computing power
  - Lacked timely access to information
- **2000's Challenges**
  - Data and user overload
  - "BLUE on BLUE" challenge
  - Larger Domains (audiences) with no additional funding (NMCI)
  - Decentralized decision making
  - DoD "Transformation" and "JOINT-ness"

Cyber Identity

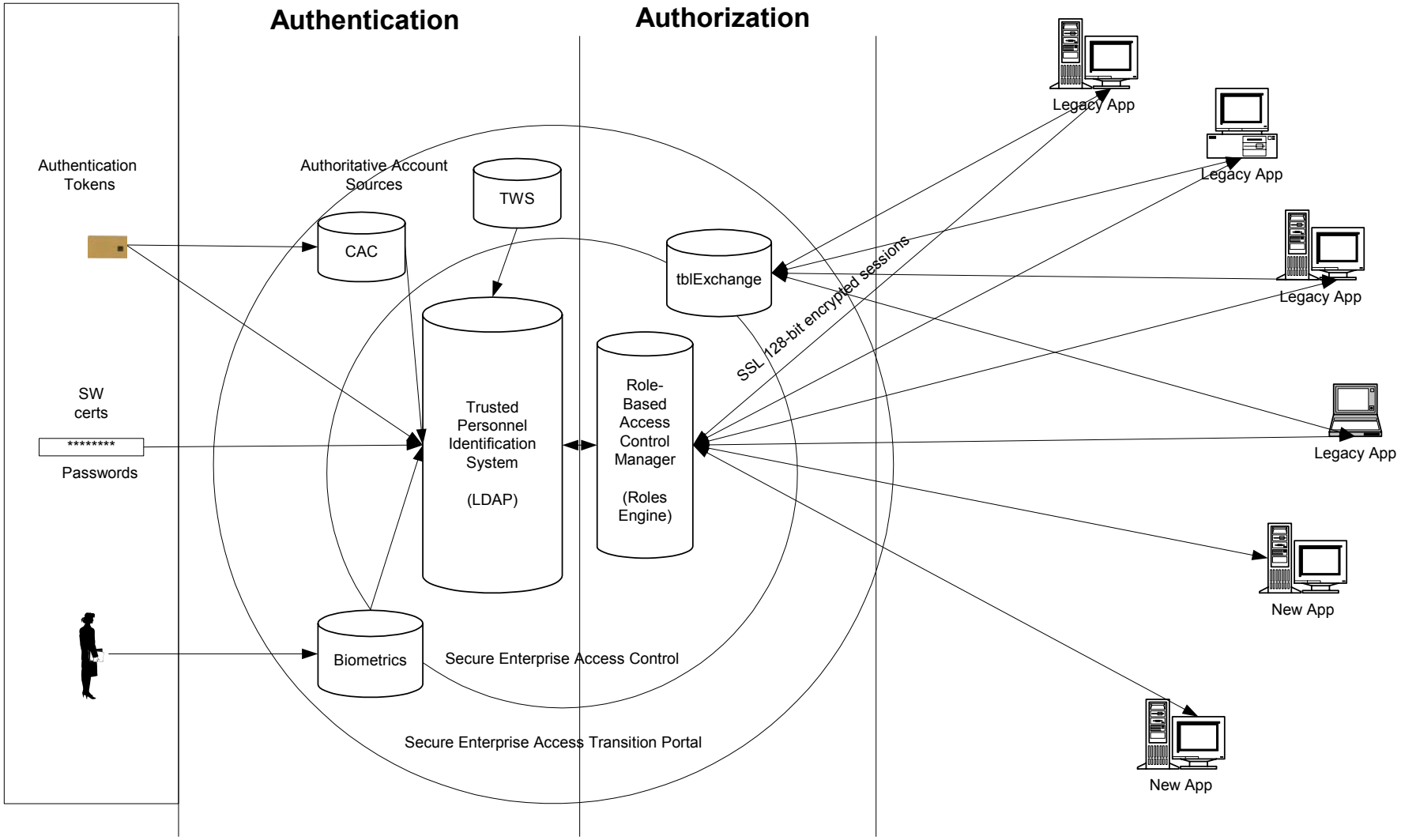
- Critical feature for future of network computing
- Must confirm with confidence
  - Validity of online transactions
  - Identity of individuals involved in those exchanges
- Must precisely verify who you are dealing with online
- Protect against unauthorized access to mission-critical systems and data
- ***Critical for Web Services***

Maintenance of Cyber Identity

An Employee-Owned Company

- Who do I let see my data? Need to Know ?
- Who is accessing my data via Web Services?
- Privacy Act Issues
- Management of relationship of individual user to systems and network and/or Web service

Traditional Architecture



Issues and Challenges

- NIST RBAC Definition
- ID Management Solutions (IdM)
- DoD RBAC Work to Date
- Expanded DoD and Commercial Efforts

Notable Ongoing ERBAC Efforts

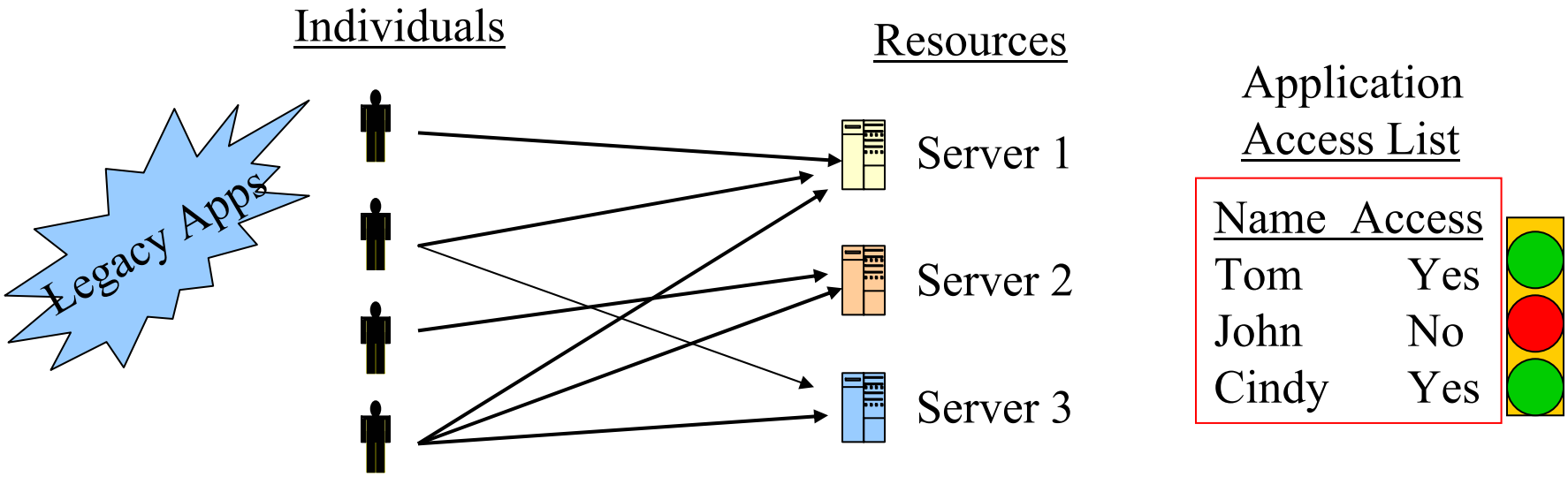
- NIST American National Standard on Role Based Access Control - ANSI INCITS 359-2004 (approved 19 Feb 2004)
- In OASIS, the XACML technical committee is developing an RBAC profile for expression of authorization policies in XML
- Computer Associates' eTrust
- SYSTOR AG's Sam Jupiter
- Netegrity's Business Layers Day One
- OpenNetworks' Directory Smart provisioning software in conjunction with Microsoft's Active Directory
- In-house efforts by Chevron, Anthem Blue Cross/Blue Shield, and State Farm
- Many solutions are being implemented in conjunction with provisioning efforts for new network hardware and software
- Adaptation of the CA eTrust suite to a DoD application is contained in Richard Fernandez' paper 196 for CCRTS

Types of Access Control

- Discretionary (DAC)
- Mandatory (MAC)
- Role-Based (RBAC)

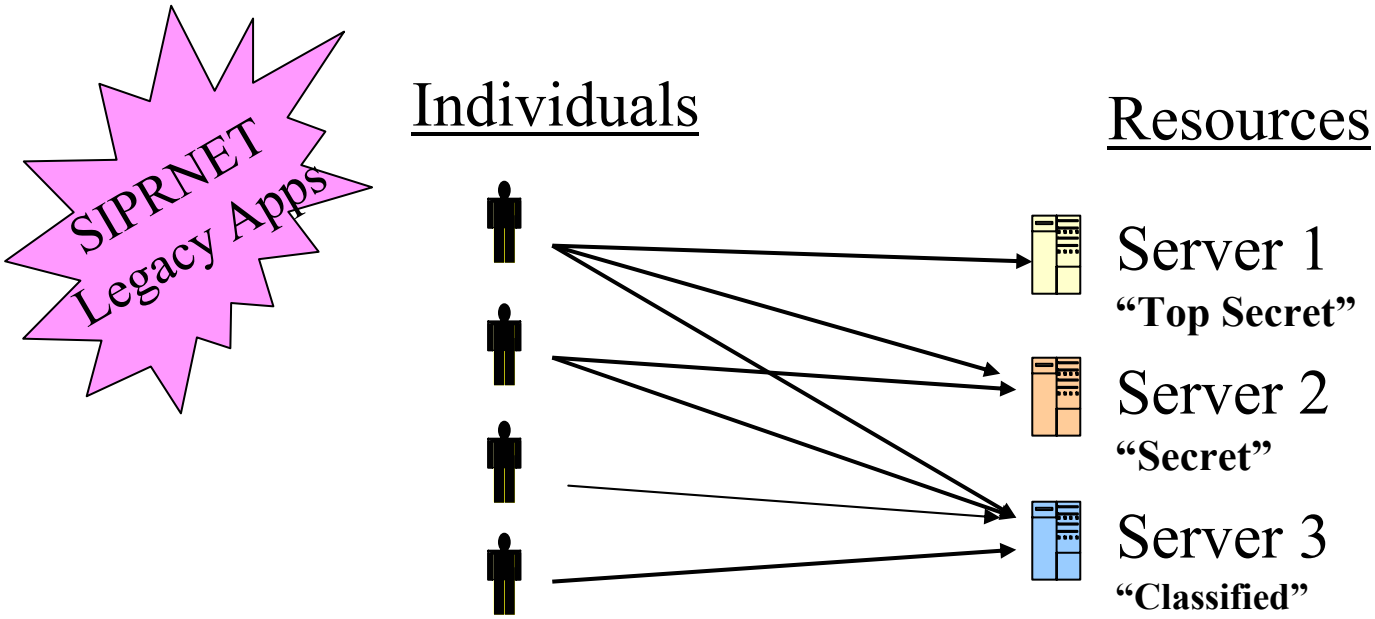
Discretionary AC

Restricts access to objects based solely on the identity of users who are trying to access them.



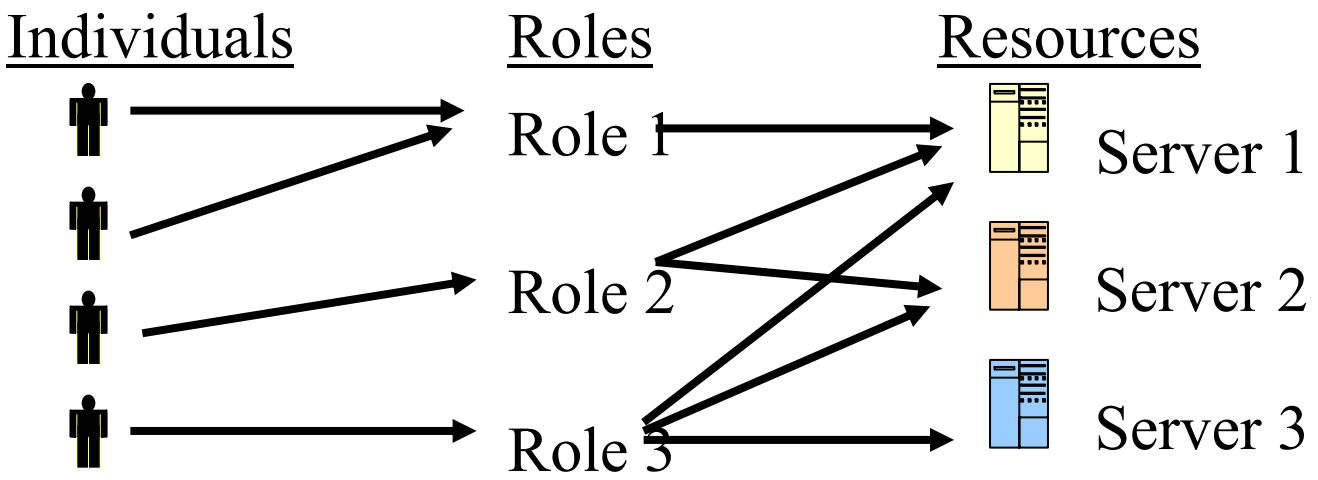
Mandatory AC

Restricts access to data/information based on matching the security level of data being accessed and the identity of the user.



Role-Based AC

Restricts access to data/information based on matching the security level of data being accessed, the identity of the user and the role being performed by the user.



Users change frequently, Roles not as often..

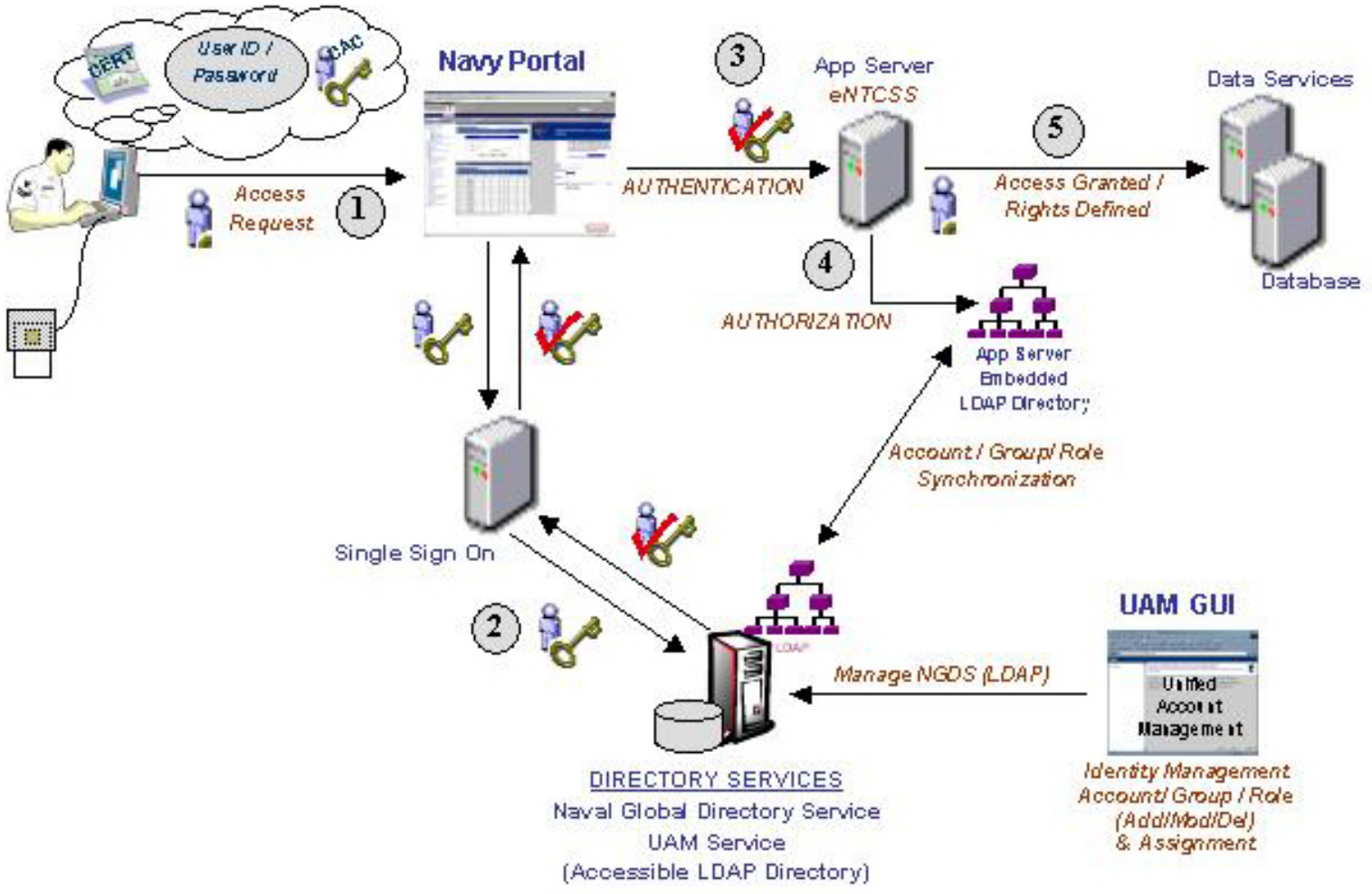
Role Based Access Factors

An Employee-Owned Company

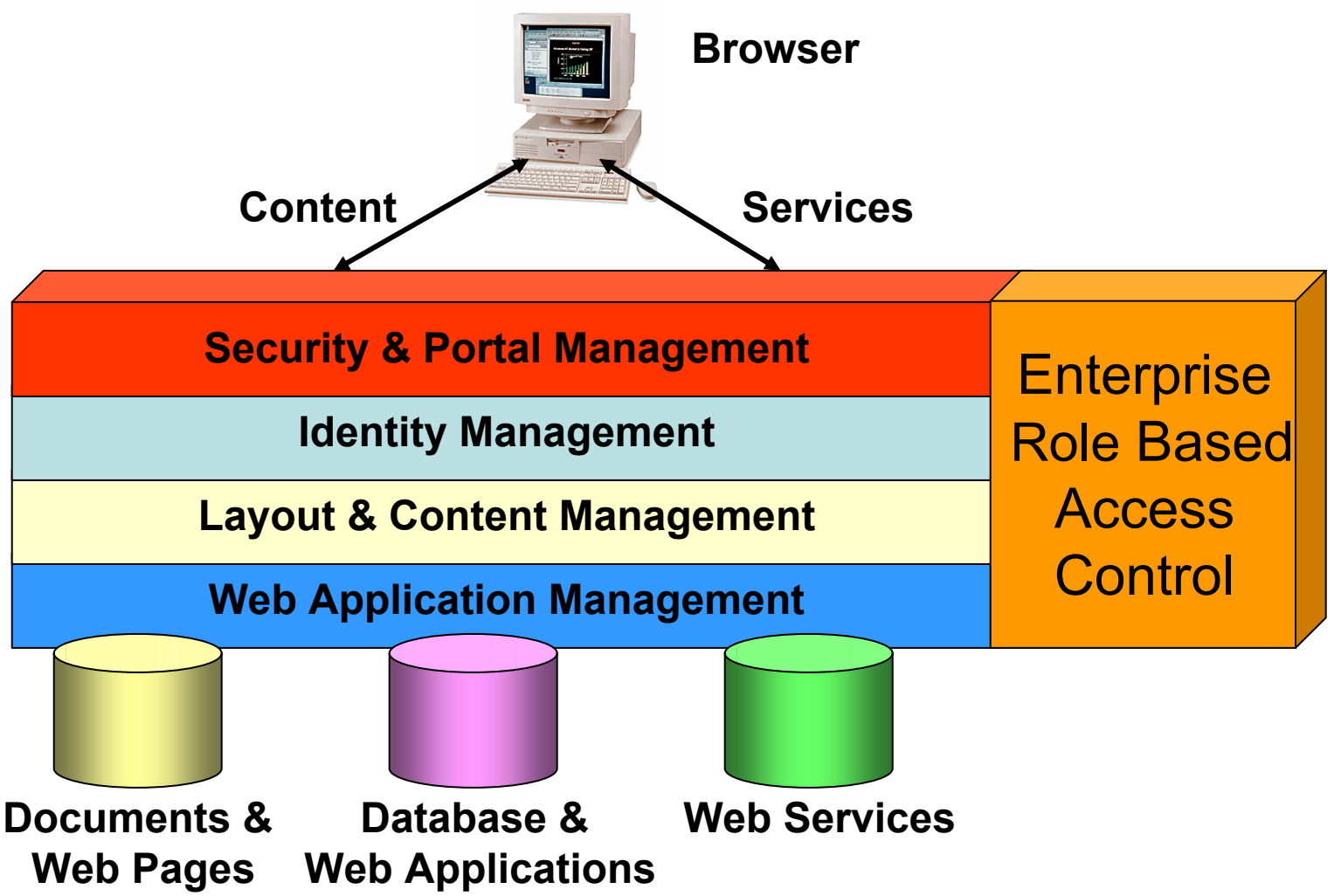
- People
- Functions/processes/rules
  - PMI, SEI-CMMI, BPM
- Data
- Time
- Situation

Access Control Architecture Example

An Employee-Owned Company



Portal/SOA Architectures



Specific Requirements

An Employee-Owned Company

- **Security administration is costly and error prone**
  - 1000's of application access control lists and "forms-based logins"
  - User need to know must be individually determined by app owner
  - "Semi-automated self-sign up registration, email back password" may introduce security risks
  - Rarely are users forced to update USERIDs/passwords
  - There is no process for data/application owners or CDA's to validate access requests from Web services
- **What is needed**
  - Automated, secure, accurate system to 'vet' users by role
  - Flexible role creation and modification
  - Rapid yet completely trustworthy PKI/biometrically enabled Single Sign On
  - Formal enterprise architecture and project, change, and business process management

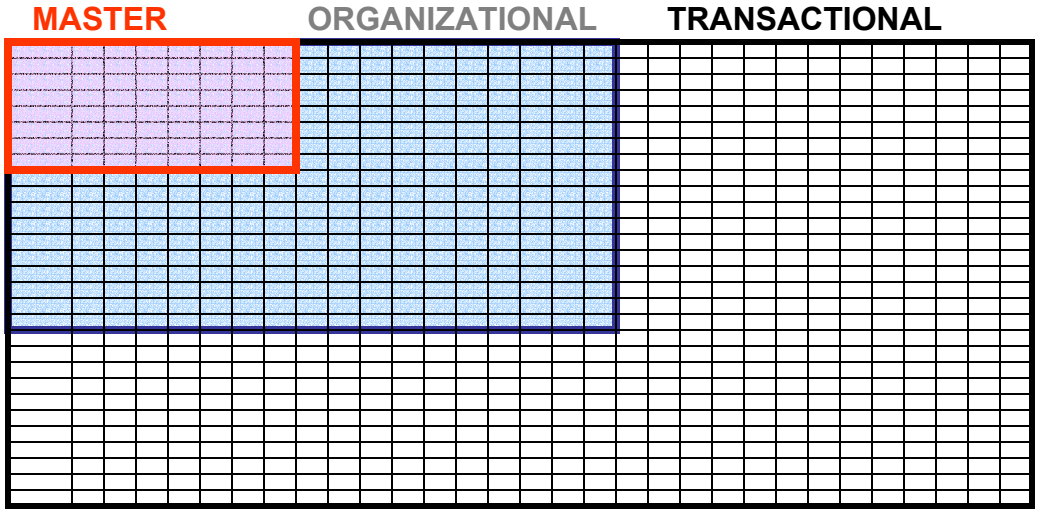
Role Basics ("Rosetta Stone")

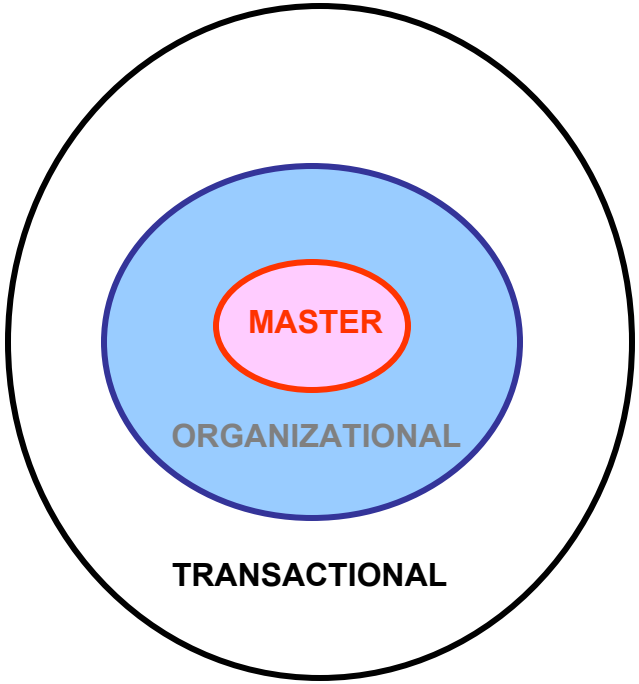
An Employee-Owned Company

Master - Authoritative, objective data objects (name, SSN, DOB, etc.)

Organizational – Local data objects (Command, NEC, Billet, Phone#, etc.)

Transactional – Self input data objects





"VIN" Code

Sample First Digit Choices

A = Active Duty NAVY
B = Reserve NAVY
C = GS
D = Contractor
E = Foreign National
F = Active Duty AF
G= Reserve AF
H=Active Duty ARMY
I= Reserve ARMY
J=Active Duty Marine
K=Reserve Marine
L=Active Duty CG
Etc., etc., etc.,

Essential Provisions of an ERBAC

An Employee-Owned Company

- Should be added to the nine (9) Core Enterprise Services currently listed for NCES
- DoD should fund and maintain a DoD ERBAC office as part of the GIG Enterprise Architecture (EA) effort with an ERBAC representative at every major Joint and Service Echelon 2 and above Command
- Must be one of the major pillars of the Operational portion of the C4ISR Enterprise Architecture (Fn, NCES, etc.)
- Process of defining required roles/policies/rules should be based on a thorough analysis of how the end user operates the system and should include input from all stakeholders

Conclusion

- DoD not realizing promised ROI for IT
- Technology to create an ERBAC system is being implemented today
- ERBAC makes Enterprise Network Centric C2 possible

Next Steps

- Increase DoD wide awareness and actions to resource a solution
- Obtain DoD-wide consensus on ERBAC policy and processes
- Establish a common vocabulary for Role-Based Access Control for use in the DoD Enterprise
- Present a Framework for Role-Based Access Control for both Physical and Virtual Domains

Contact Information

- Rick Kooker

  kookerf@saic.com (808) 833-8661
- Stephan Kane

  kanest@saic.com (808) 833-8658

  3049 Ualena Street, Suite 1100

  Honolulu, HI 96819