# Public Key Infrastructure:

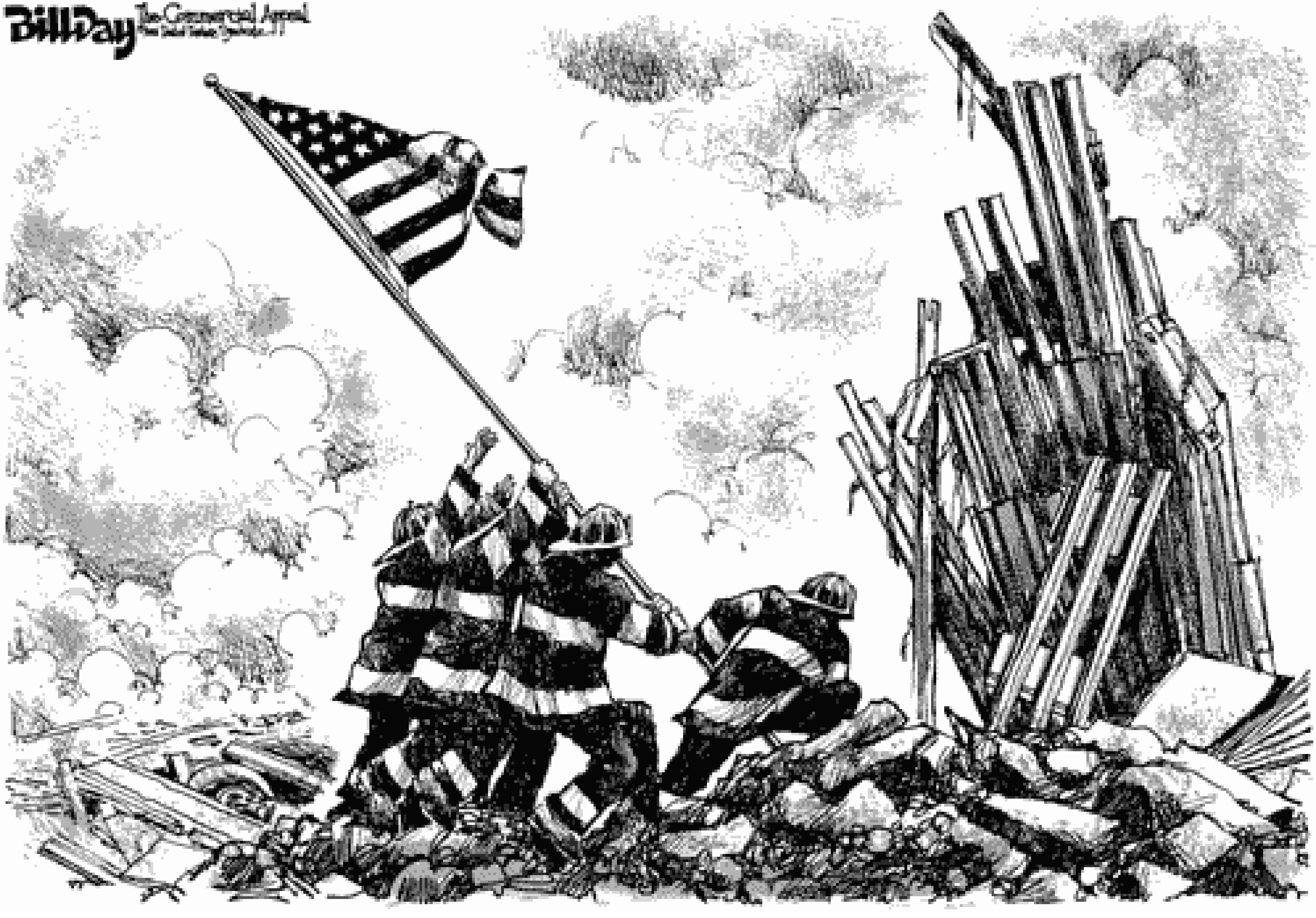
## The Enabler for DoD e-Bus

*A Presentation for PKI in Today's Government: A Matter of Trust*

R. Michael Green
Director, DoD PKI PMO
(410) 854-4900
rmgree2@missi.ncsc.mil

Becky Harris
Deputy Director
(703) 681-0271
Harrisb@ncr.disa.mil

29 November 2001


Bill Day
The Commercial Appeal

Awakening a sleeping giant
9·11
MacGregor
©2001
THE ARGUS-PRESS

# IA Essentials - The Dawn of e-Gov

## *PKI, The Enabler*

**Today's Objective:**

**Discuss Current DoD Status**
**Review Federal Efforts**
**Highlight Future Activities**

**<u>The Goal</u>**: To ***enhance the business processes*** and ***improve the IA posture*** of the DoD through widespread use of PKI-enabled applications.

The DoD PKI PMO

www.c3i.osd.mil/org/sio/ia/pki/index.html

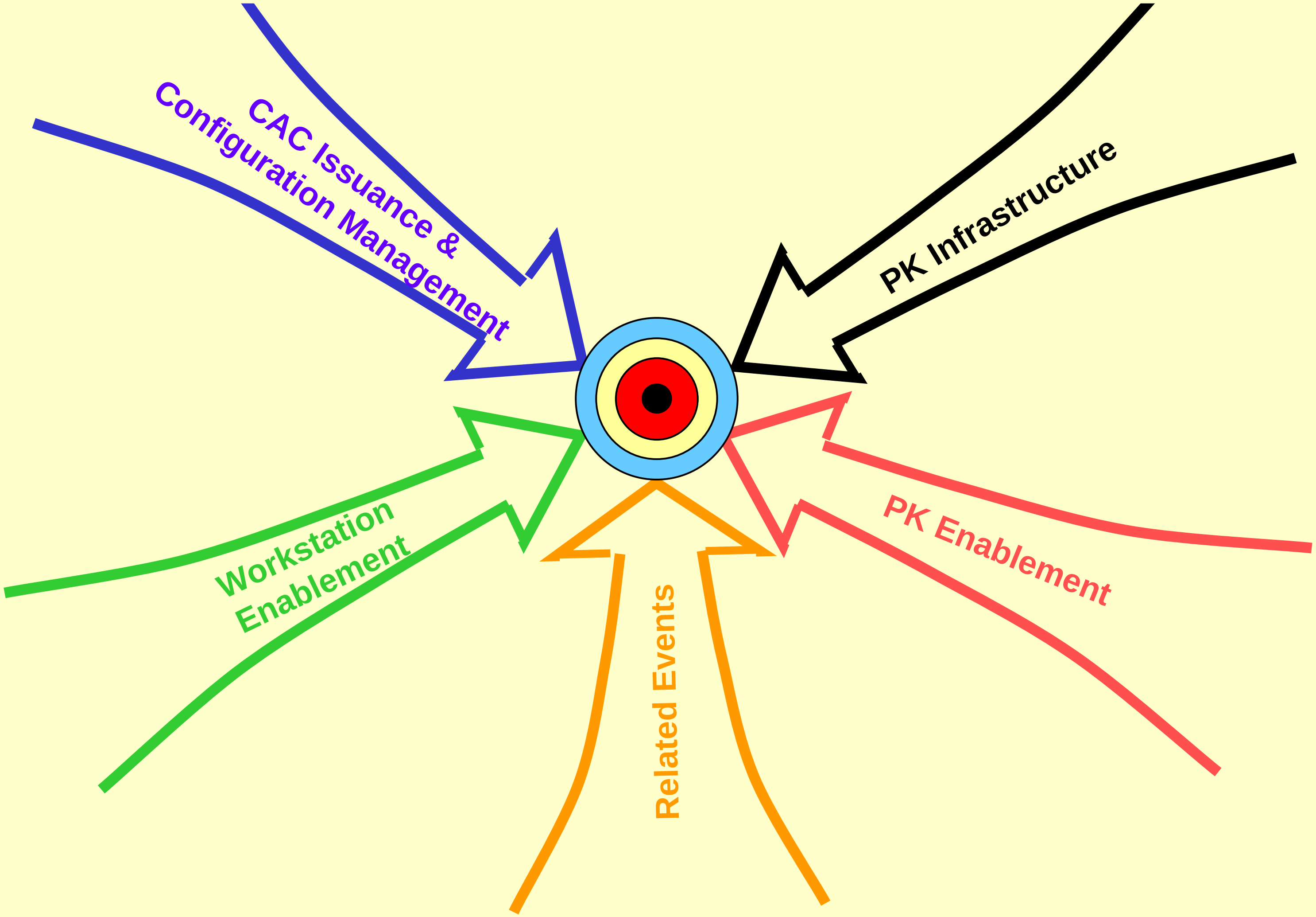
**R. Michael Green**

**Director, DoD PKI PMO**

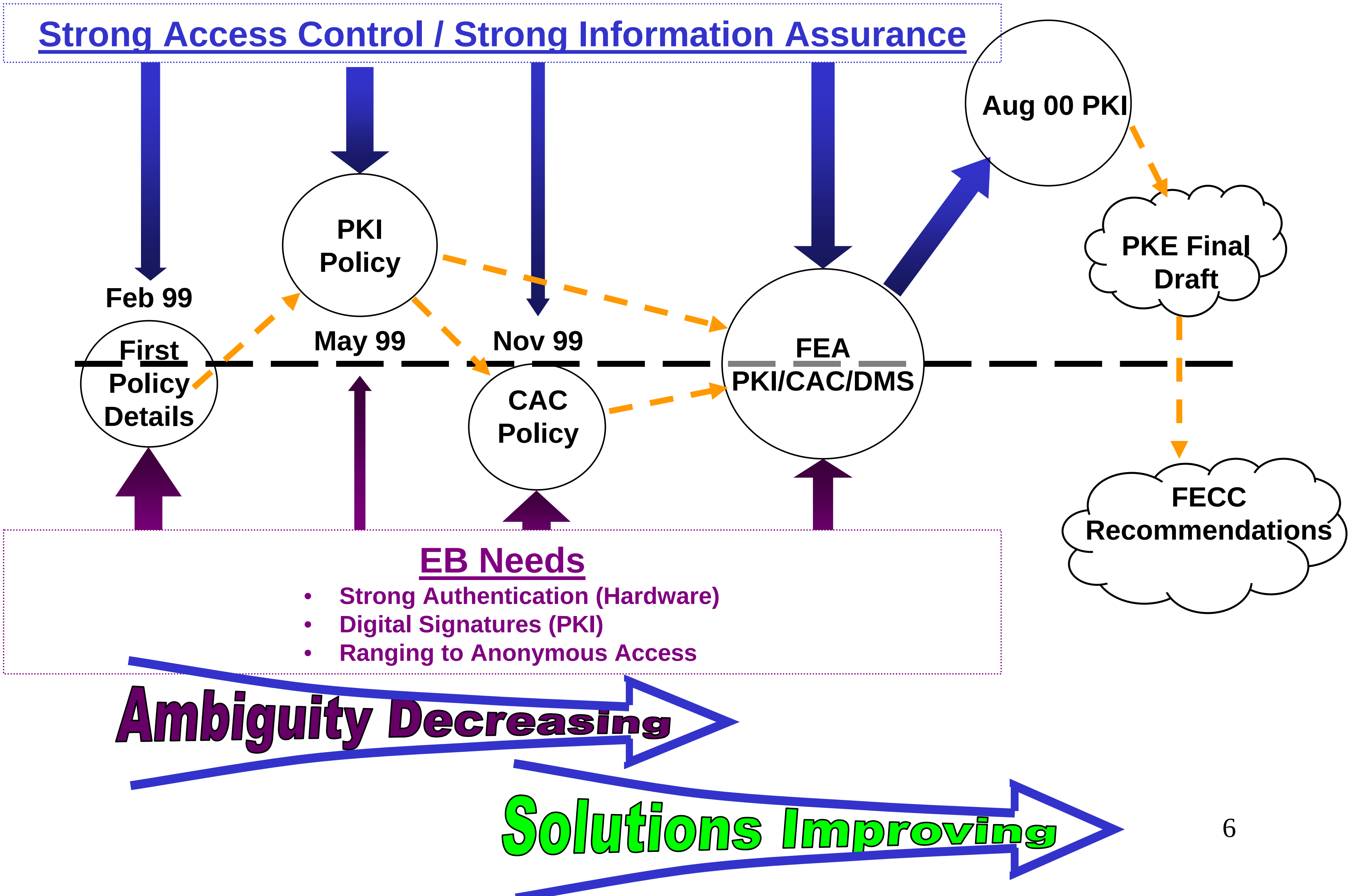
**410-854-4900**

**29 November 2001**

# DoD PK-Capability Requires Coordinated Convergence



# DoD PK Capability Recent Journey



Strong Access Control / Strong Information Assurance

Feb 99

First Policy Details

PKI Policy

May 99

Nov 99

CAC Policy

FEA PKI/CAC/DMS

Aug 00 PKI

PKE Final Draft

FECC Recommendations

EB Needs

- Strong Authentication (Hardware)
- Digital Signatures (PKI)
- Ranging to Anonymous Access

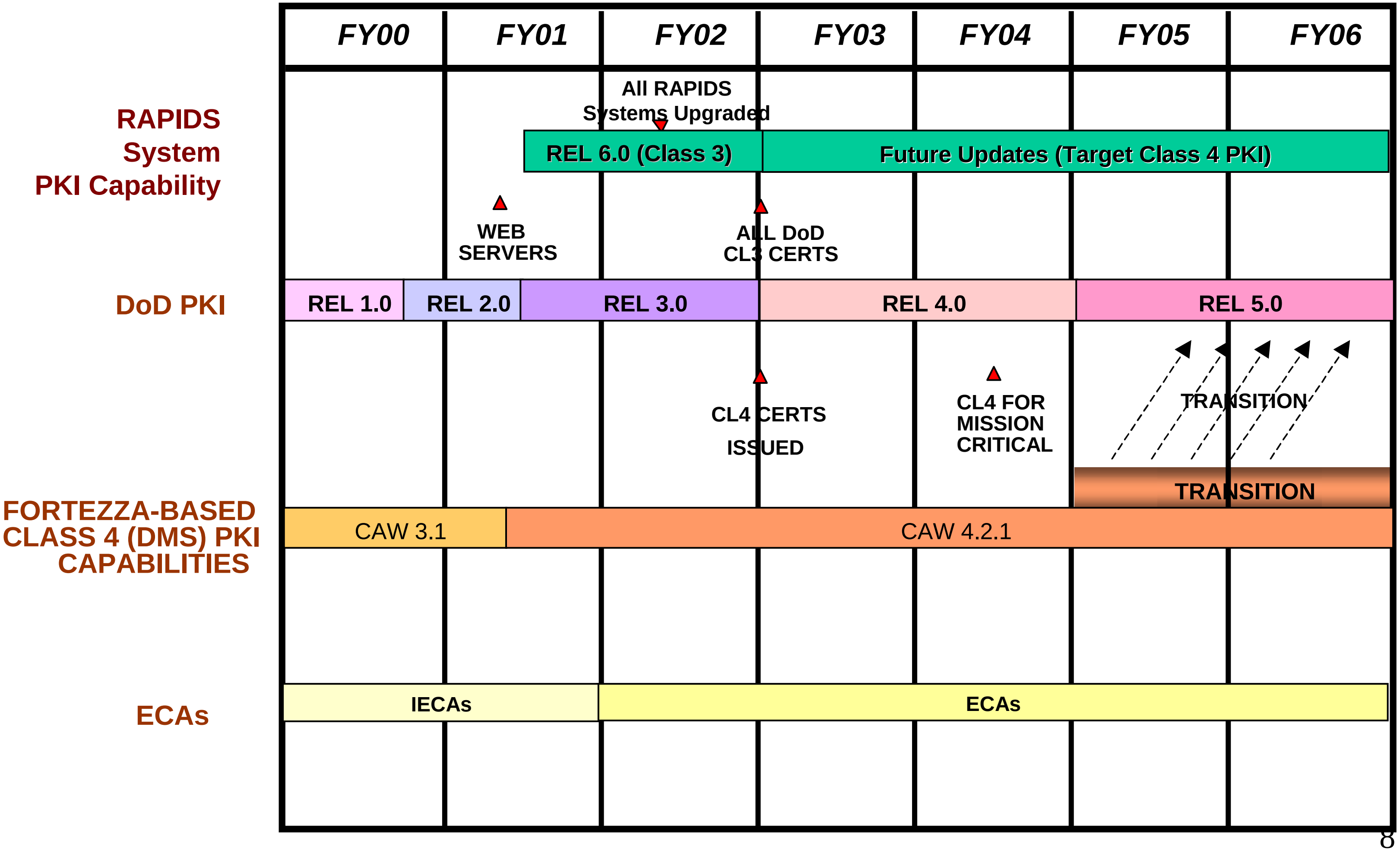
Ambiguity Decreasing

Solutions Improving

# Current PKI Milestones

- Approved (8/12/00) DoD PKI Defined Milestones
  - Private Web Servers PKI Enabled by **Dec 00**
  - Complete Class 3 Infrastructure In Place By **Dec 01**
  - All DoD Personnel Issued Class 3 Certificates by **Oct 02**
  - All DoD E-Mail Must be Signed With a Class 3 Certificate by **Oct 02**
  - All Private Web Servers Must Do Client-Side Authentication by **Oct 02**
  - Begin Issuing Class 4 Certificates by **Oct 02**
  - Protection of Mission Critical Systems Must Migrate from Class 3 to Class 4 by **Dec 03**

# DOD PKI Schedule



FY00 FY01 FY02 FY03 FY04 FY05 FY06

RAPIDS System PKI Capability

All RAPIDS Systems Upgraded

REL 6.0 (Class 3)

Future Updates (Target Class 4 PKI)

WEB SERVERS

ALL DoD CL3 CERTS

DoD PKI

REL 1.0

REL 2.0

REL 3.0

REL 4.0

REL 5.0

CL4 CERTS ISSUED

CL4 FOR MISSION CRITICAL

TRANSITION

TRANSITION

FORTEZZA-BASED CLASS 4 (DMS) PKI CAPABILITIES

CAW 3.1

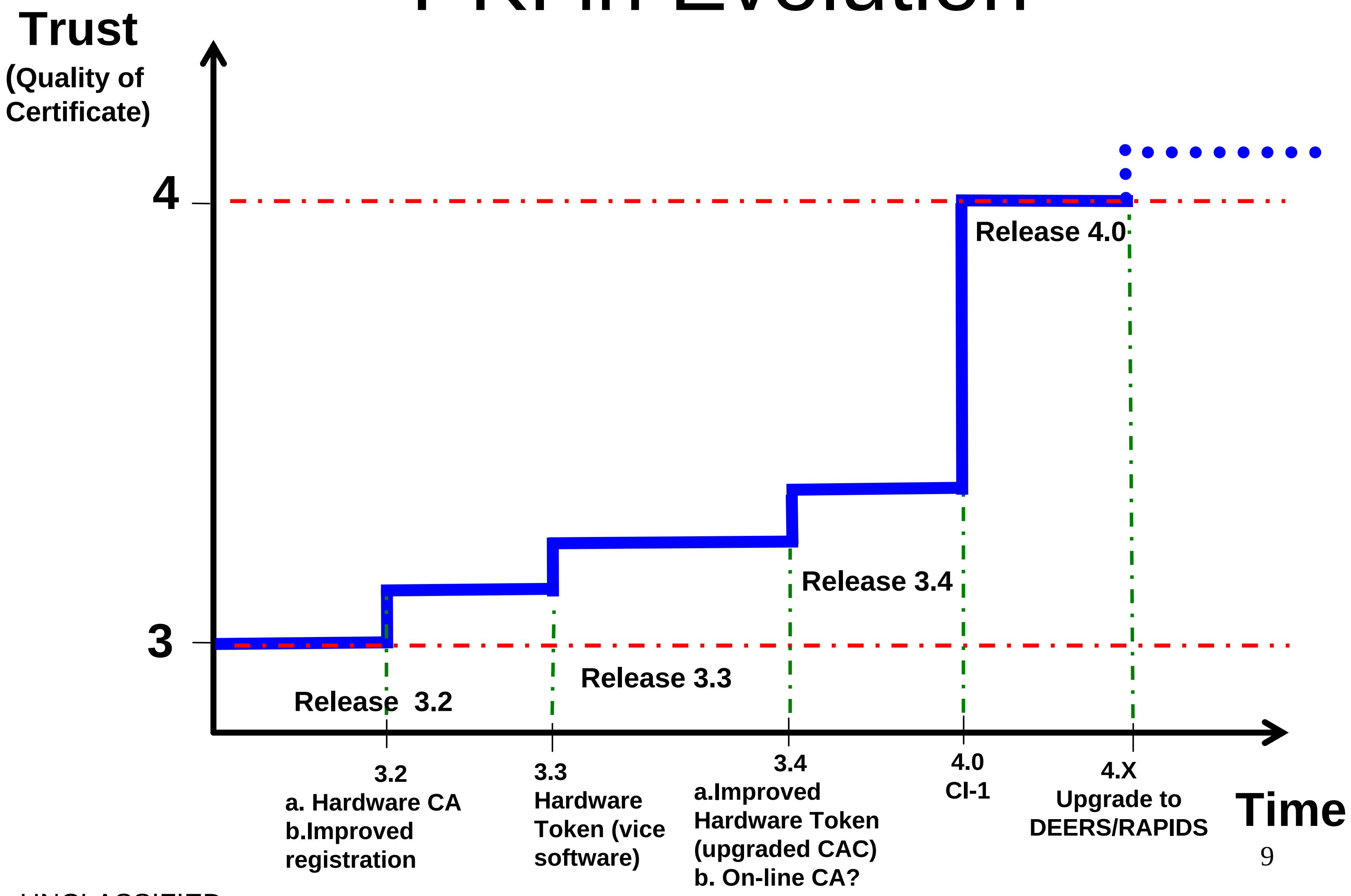
CAW 4.2.1

ECAs

IECAs

ECAs

# PKI in Evolution



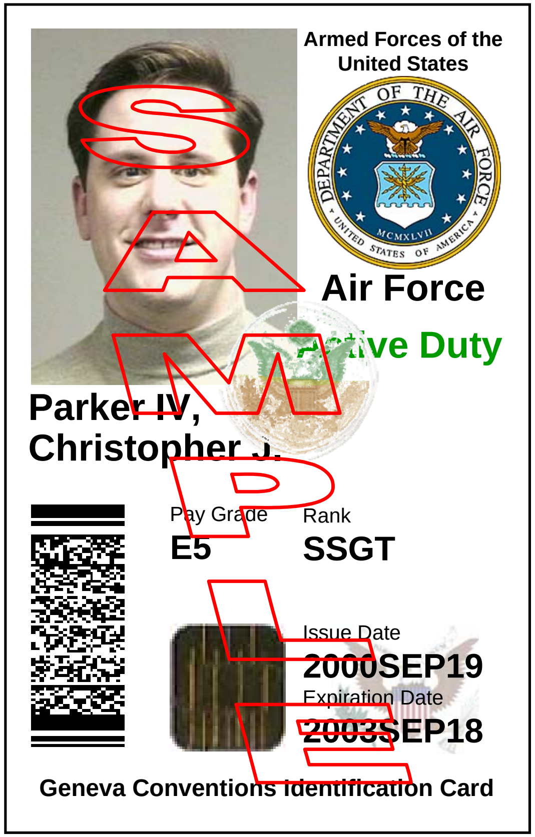
# *General Status*

- Making Good Progress
- Excellent Support of Services & Agencies
- Class 3 DoD PKI Fully Operational
- CAC Integration with PKI “Achieved”/Rel. 3.0
- Token/Smart Card Strategy laid out
  - 3+ Million Cards
- Target Class 4 Acquisition Complete
  - System Integrator Awarded November 9th
- Private Web Server Protection Complete

# Class 4 Tokens/Smart Cards

- GSA Contract award 19 May ‘00 - 5 Vendors
  - ACO will use to Procure Class 3 & Class 4
  - Primes developing interop spec
  - PMO & ACO/DMDC participating
- SSAB, SCSCG and SCCMCB Participation
- FIPS 140-1 Level 2 Testing & Certification (August ’01)
- FIPS Certified Schlumberger Cards faster by 25%
- Class 4 Security Requirements
  - Sept ‘00: Protection Profile Complete
  - Industry Vetting/DoD Coordination; Mar ‘01: Formal Release
  - July ‘01: Industry Mods and Cert.
  - Mid ’03(??): Initial Class 4 Procurements

# Active Duty Card (Front and Back)



Armed Forces of the United States

Air Force

Active Duty

Parker IV,
Christopher J.

Pay Grade
E5

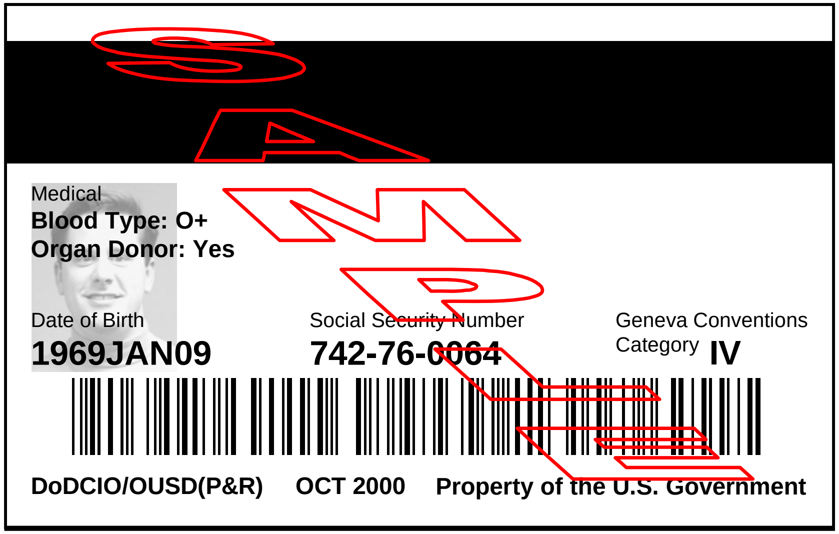
Rank
SSGT

Issue Date
2000SEP19

Expiration Date
2003SEP18

Geneva Conventions Identification Card

DEPARTMENT OF THE AIR FORCE
UNITED STATES OF AMERICA
MCMXLVII



Medical
Blood Type: O+
Organ Donor: Yes

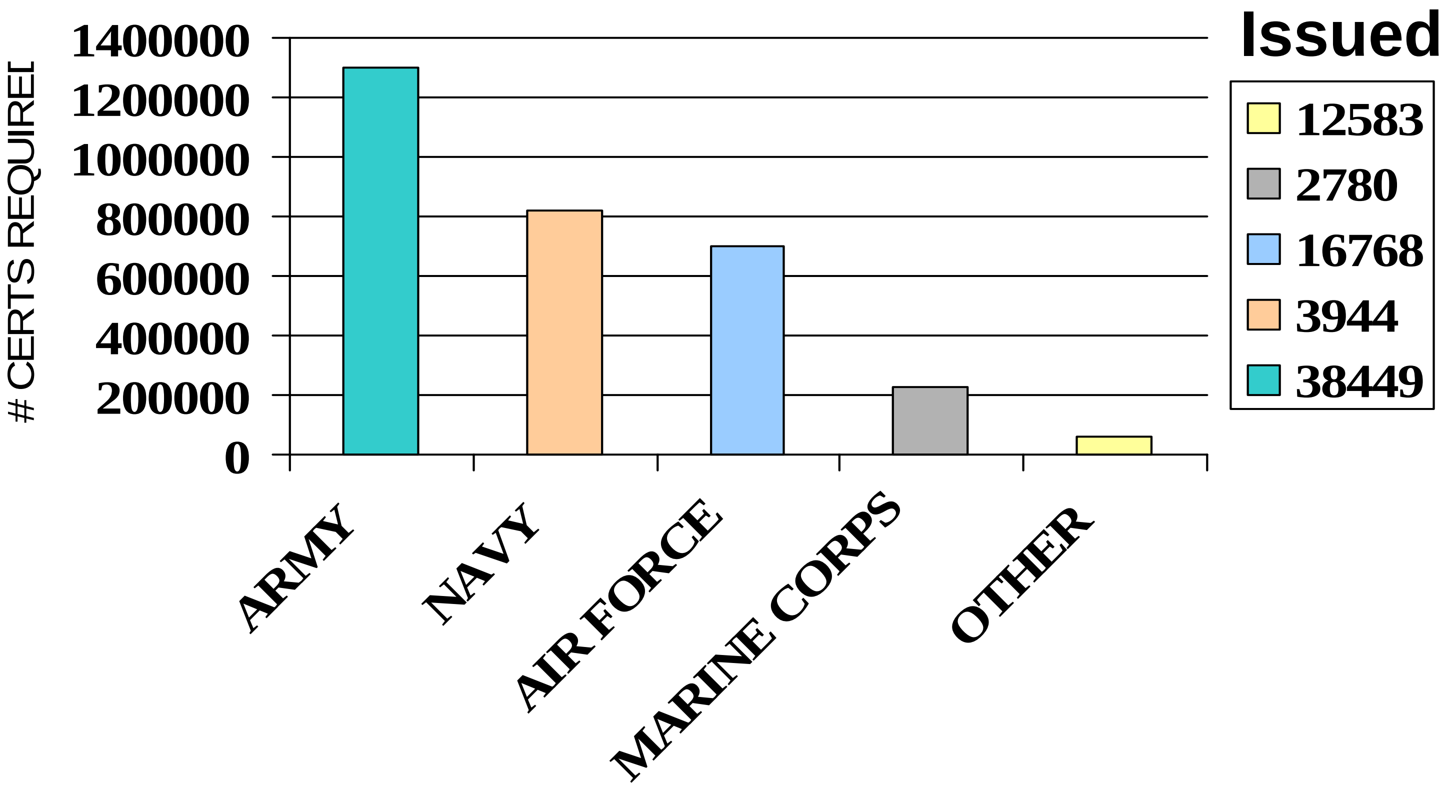
Date of Birth
1969JAN09

Social Security Number
742-76-0064

Geneva Conventions Category IV

DoDCIO/OUSD(P&R) OCT 2000 Property of the U.S. Government

# Certs Required/Issued



| | | |
|---|---|---|
| *Total Req'd* | *3,109,983* | |
| *Total Issued* | *74,524* | *June '01* |
| *Total CACs* | *94,712* | *Nov '01* |

# Private Web Server Cert Status

*** Contacting Commands for Exact Numbers**

**** Waivered (3 cannot recognize DoD Certs, 4 Don’t Support SSL)**

***** SSL-enabled with non-DoD Certs**

| | Private Web Servers | Issued | Activated (SSL Enabled) | Not Issued | % Complete | Completion Date |
|---|---|---|---|---|---|---|
| Navy | 2200(est)* | 2133 | 2133 | 67(est) | 97% | --- |
| Army | 2117 | 2080 | 2080 | 37** | 98% | --- |
| AF | 2061 | 1966 | 1966 | 95 | 95% | Tracking Daily |
| Marines | 253 | 191 | 253 | 62*** | 100% | --- |
| Other | 1255 | 1048 | 1048 | 207 | 84% | Incomplete Data |
| Total | 7886 | 7418 | 7480 | 468 | 95% | |

May ‘01

# PKI Milestone Review

- Approved (8/12/00) DoD PKI Defined Milestones
  - 🟢 Private Web Servers PKI Enabled by Dec 00
  - 🟡 Complete DoD PKI Registration Infrastructure In Place By Dec 01
  - 🟡 All DoD Personnel Issued DoD PKI Certificates by Oct 02
  - 🟡 All DoD E-Mail Must be Signed With a DoD PKI Certificate by Oct 02
  - 🟡 All Private Web Servers Must Do Client-Side Authentication by Oct 02
  - 🟡 Begin Issuing Class 4 Certificates by Oct 02
    - IOC – Nov 02
    - FOC – Jan 04
  - 🟢 Protection of Mission Critical Systems Must Migrate from Class 3 to Class 4 by Dec 03

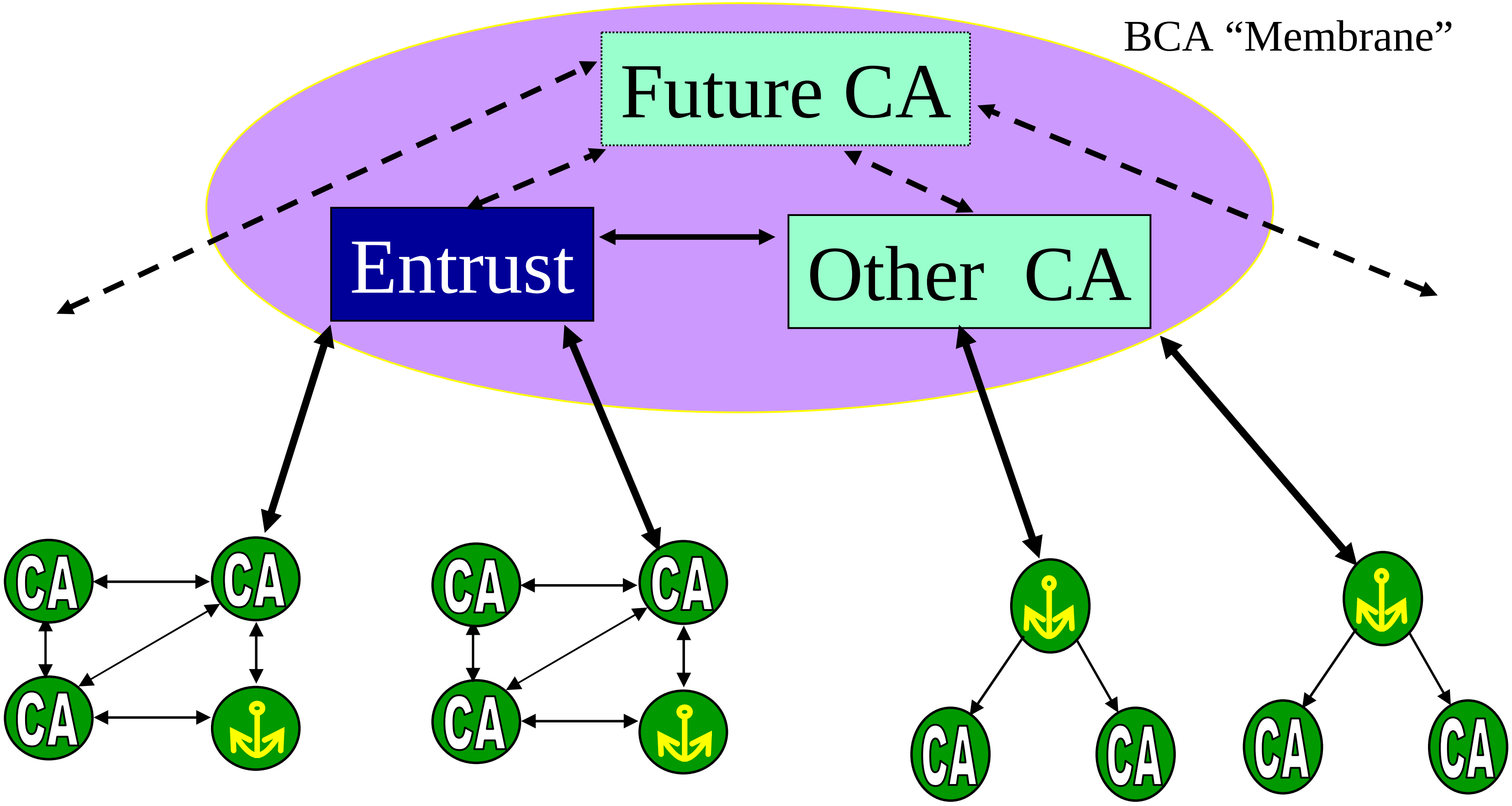
# Federal PKI, Interim External Certification Authority (IECA) & ACES

- Four Vendors Approved/Operating As IECAs
  - *Operational Research Consultants (ORC)     *Verisign
  - *Digital Signature Trust (DST)     *General Dynamics
- Small Number of Certificates Sold To Date (100s)
  - Low Quantities and High Liability Drove Cost Up
    - Waivers Reduced Quantities Significantly
- Current Activities
  - DMS/MGS purchased 200 CERTS
  - DISA/NSA Providing Seed Money ($100K+) to Apps to Jumpstart Program
  - Re-writing ACES Cert Policy to reconcile DoD differences

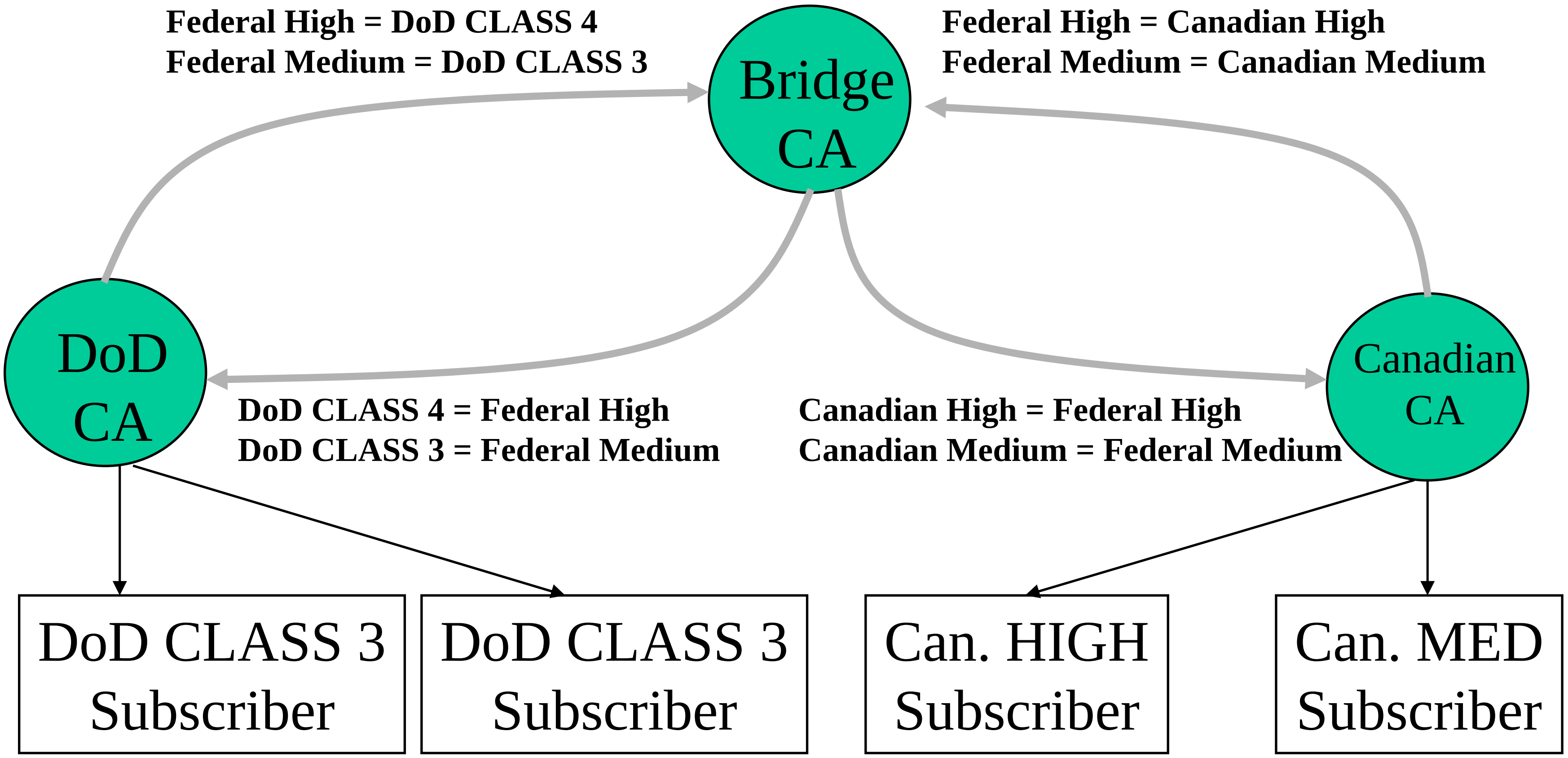
# Federal Bridge CA

- “Connects” multiple PKIs by cross-certification of “Bridge CA” with agency “Principal CAs” (e.g., DoD root CA)
- Federal Policy Authority evaluates agency certificate policies against federal Rudimentary, Basic, Medium and High Certificate Policies
- Federal PKI directory “connects” agency directory systems
- Applications obtain certificates and CRLs through distributed directory system, and check certificate validity

# Federal Bridge CA



# Policy Mapping



Federal High = DoD CLASS 4
Federal Medium = DoD CLASS 3
Bridge CA
Federal High = Canadian High
Federal Medium = Canadian Medium
DoD CA
DoD CLASS 4 = Federal High
DoD CLASS 3 = Federal Medium
Canadian High = Federal High
Canadian Medium = Federal Medium
Canadian CA
DoD CLASS 3 Subscriber
DoD CLASS 3 Subscriber
Can. HIGH Subscriber
Can. MED Subscriber

# Bridge CA (BCA) Status

- Ready and Open for Business
- Cross-Certification Approval Process
  - Technical
    - Cross-Certification
    - Directory Interoperation
  - Policy
    - Agency policy compared to Federal policy
    - Compliance Audit
- Agencies submitting applications:
  - NASA
  - GSA ACES
  - NSF
  - DoD
  - Others considering
- Much State Government and International Interest

# *ISSUES*

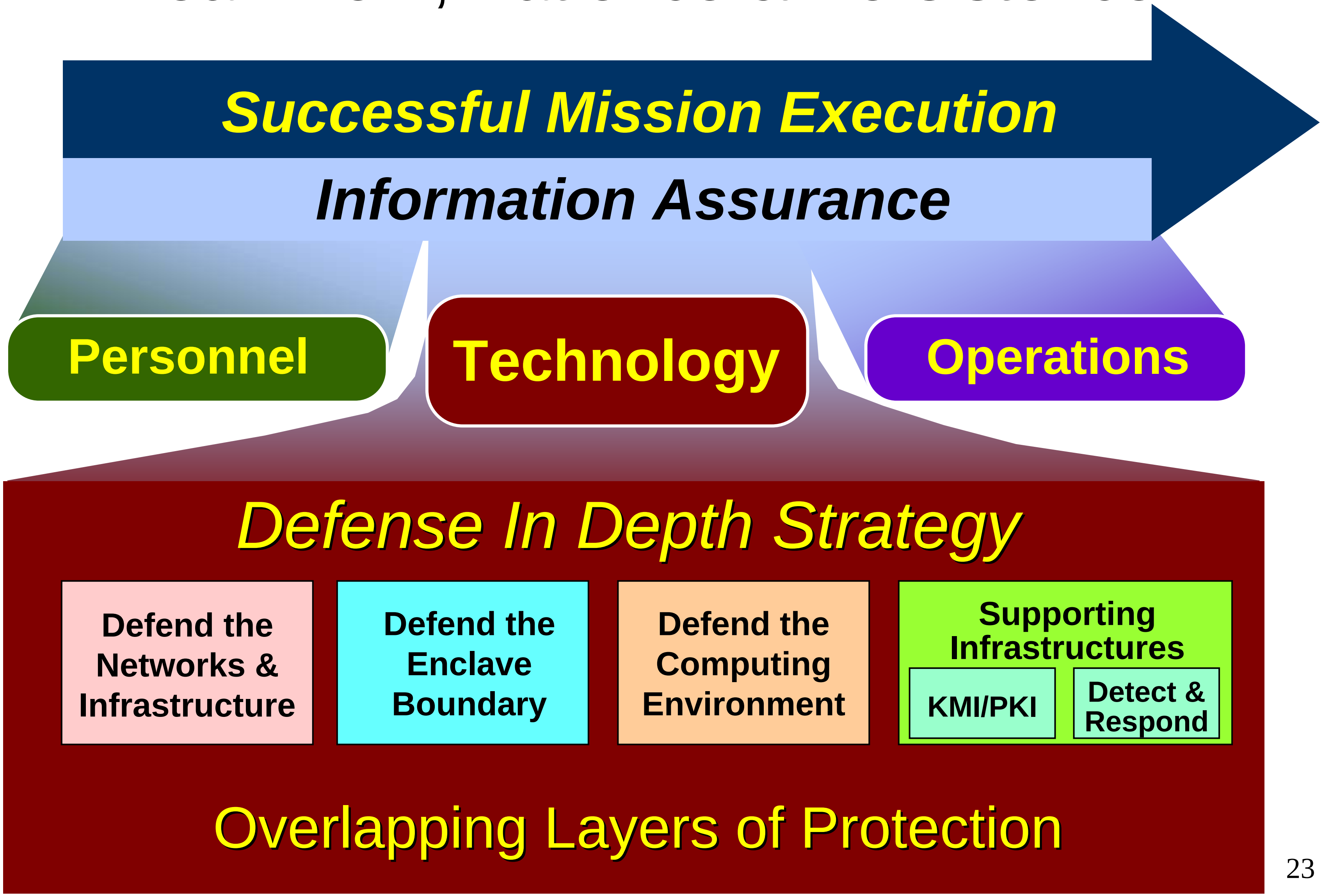
- Meeting the Commercial Environment at the Right Assurance Level (FECC)
- Higher Assurance Smart Cards
- Middleware to Allow Smart Cards to work with Readers and Operating Systems
- Evaluated Applications that can process our Certificates with little User Involvement

# FUTURE  PKI Activities

- DoD Policy Rewrite/Milestone Review
- Tactical Requirements Collection/Impl. Plan
- SIPRNET Plan
- MS Logon Agreement/Rel. 3.0.1
- Code Signing/Rel. 3.1
- Smart Card Readers and Middleware
- PK-Enabled Applications
- Private Web Server Certs/Client Side Auth.

# Defense In Depth for Technology

## Teamwork, Patience & Persistence



***Successful Mission Execution***

***Information Assurance***

**Personnel**

**Technology**

**Operations**

*Defense In Depth Strategy*

**Defend the Networks & Infrastructure**

**Defend the Enclave Boundary**

**Defend the Computing Environment**

**Supporting Infrastructures**

**KMI/PKI**

**Detect & Respond**

Overlapping Layers of Protection

# BACKUPS

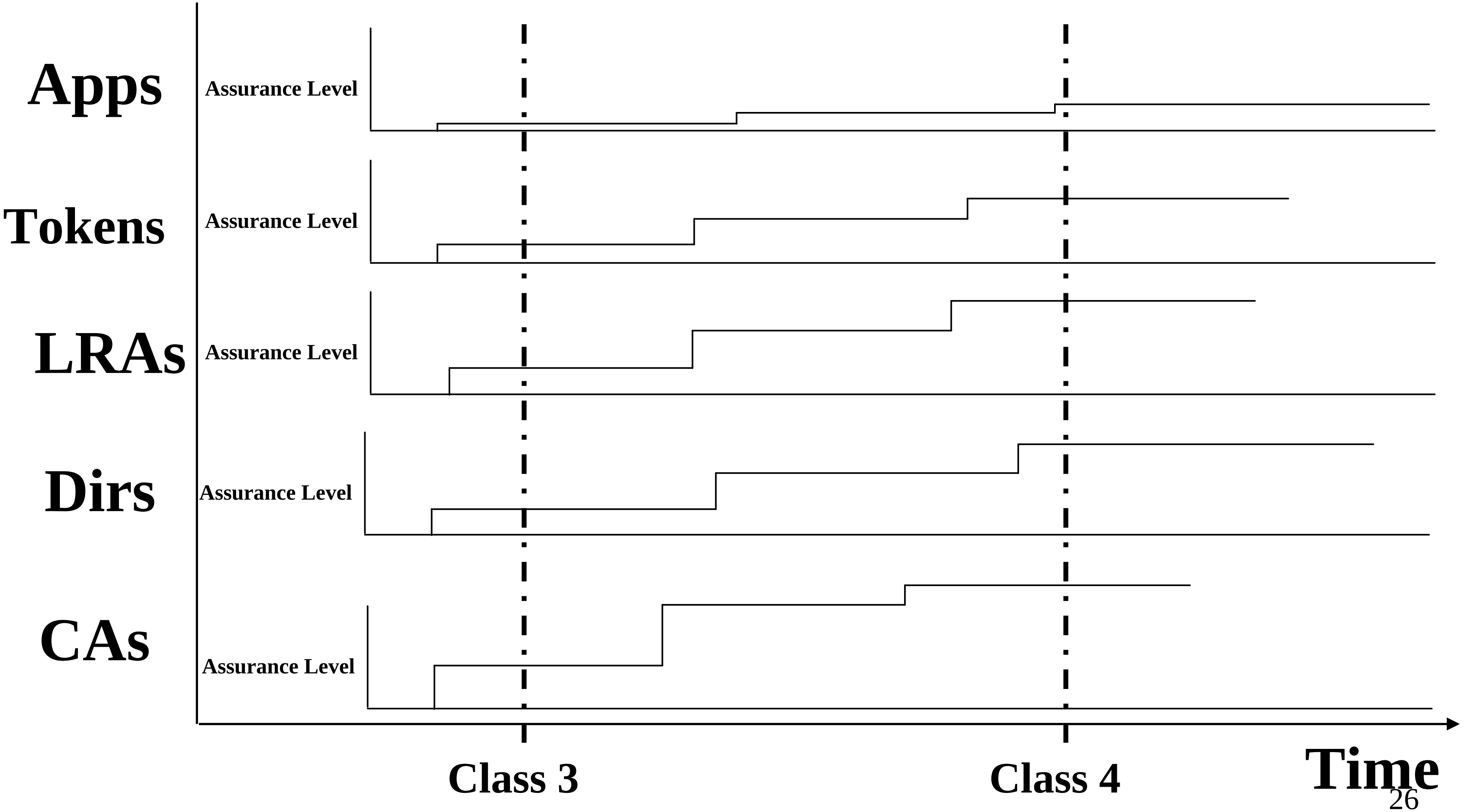
# History: Where We've Been/What We've Learned

- The MISSI/Fortezza Experience (with DMS)
  - It's Hard To Make Smart Choices Ahead of the Market (PCMCIA)
  - The Best Choice Isn't Always the Right Choice (Standards)
  - It's the "other" things that get you (Mid-ware, Reader Interfaces)
  - Decentralized CAs - Expensive to support
- There's More to PKI than just Infrastructure
  - It's a System Stupid: Apps, Smart Cards, Readers, Directories
- You Can't Expect Too Much From the User
  - Make it user-friendly
- We Must Depend on Industry to Maintain the Apps (COTS)

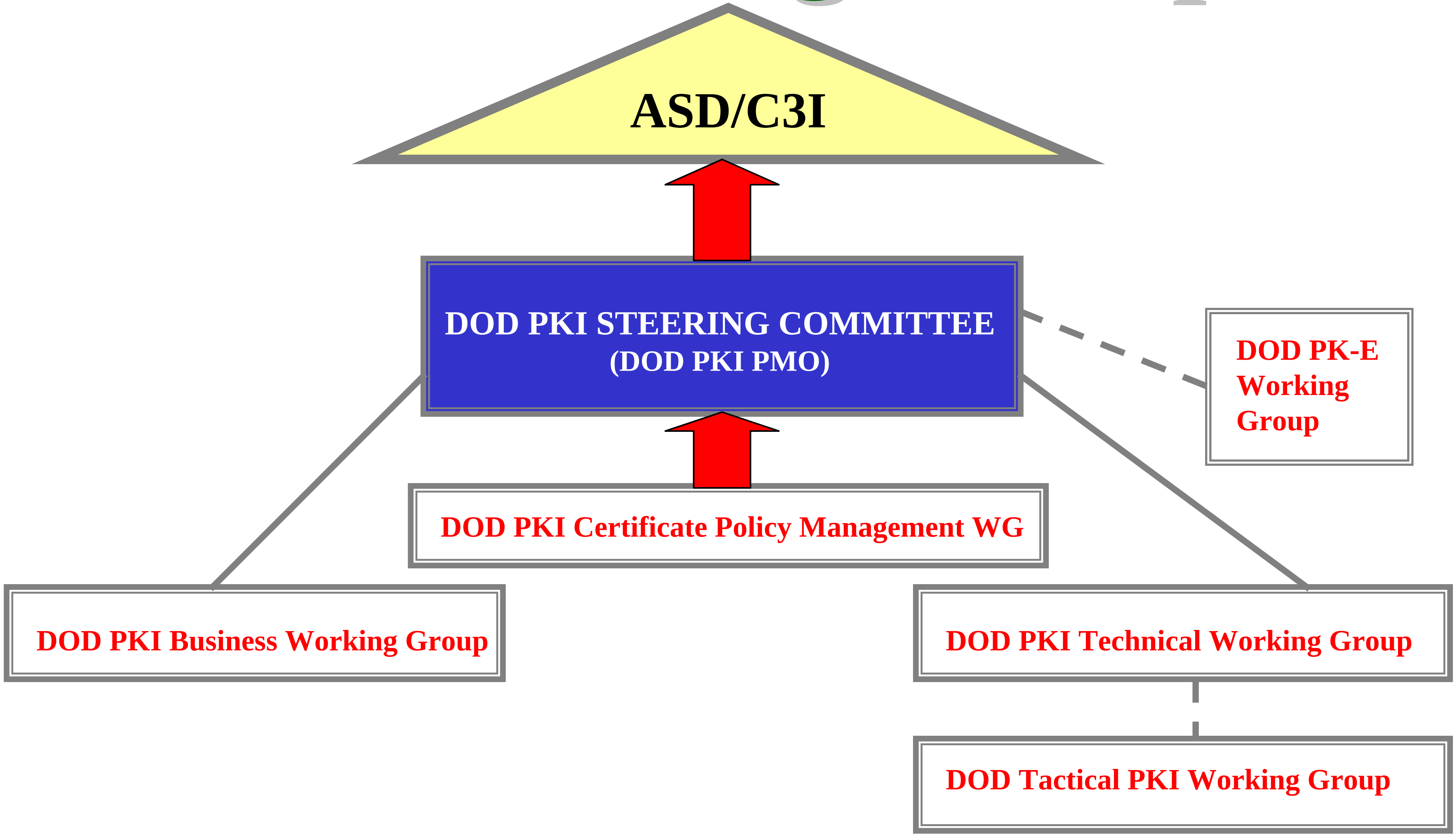
# The Challenge - It's a hard problem

## Event Driven Security

### Robustness Growth



# PKI Working Groups



ASD/C3I

DOD PKI STEERING COMMITTEE
(DOD PKI PMO)

DOD PK-E Working Group

DOD PKI Certificate Policy Management WG

DOD PKI Business Working Group

DOD PKI Technical Working Group

DOD Tactical PKI Working Group