



Defense Information Systems Agency

Department of Defense

Cyber Security, Information Assurance

Richard Hale
Chief Information Assurance Executive
Defense Information Systems Agency
April 8, 2008



Bad Guys

Bad Guy Motivation:
Gain Military Advantage by...

**Knowing what
we're going to do**
or what we're likely
to do

**Making our
weapons work in
unexpected ways**

**Causing us to lose faith in
each other**

**Slowing
our
decision
cycle**

Etc.

**Fuzzing up our view of
reality**

- By changing information
- By participating directly in
our decisions (by
masquerading as us)

Sophisticated Adversaries

aka *Really Capable Bad Guys*

- Have a military or intelligence mission in mind
- Will plan and select the plan with the best combination of effectiveness, (low) risk to the adversary, and cost
- Are very patient, analytical, methodical, and quiet
- Have advanced resources and tradecraft
- Can select the attack method, the target, the time, and the place

What's Our Business?

...Twin Goals for
Cyber Security/Information Assurance

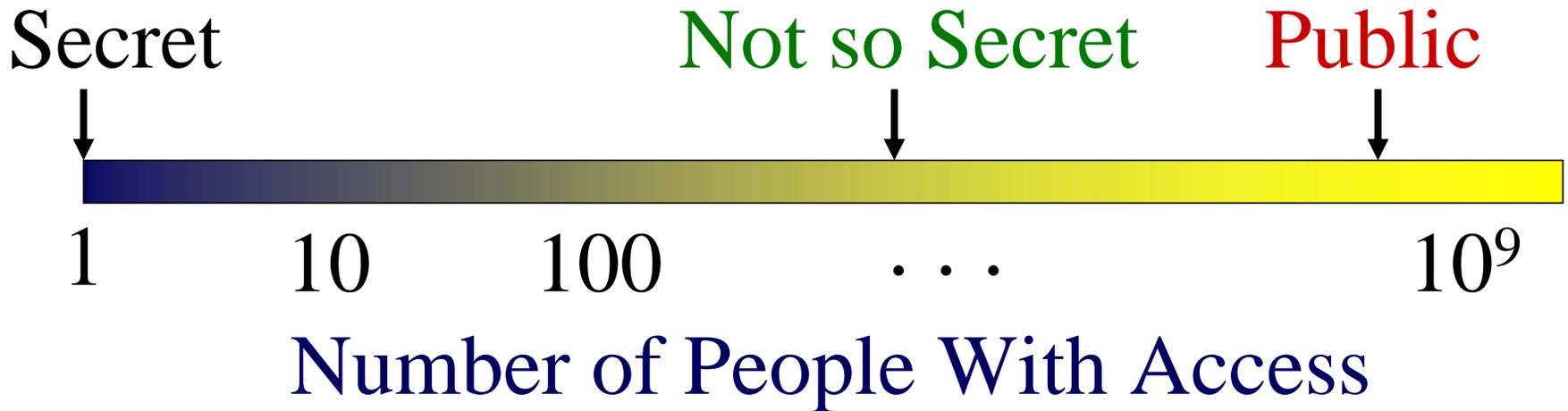
**1. Ensuring that our customers
can depend on information
and on the information
infrastructure in the face of
physical and cyber attack**

(Mission Assurance, or, *we're all
really dependability experts*)

**2. Ensuring that our customers
can keep a secret (when they
want to)**

**... and doing both while
*sharing as broadly as possible***

Keeping a Secret (While Sharing Broadly)



My Customers

Anyone in DoD, and anyone involved in a mission important to DoD

We often don't know in advance with whom DoD will be working

My Oversimplification of How DoD Is Pursuing These IA (and sharing) Goals

Part 1

Limit exposure of vulnerabilities by

- ***Removing*** as many of these vulnerabilities as possible (e.g. **encrypt** when appropriate, **configure** things securely, **remove** unnecessary functions, eliminate passwords)
- ***Layering protections*** that incrementally limit the population with access to a given vulnerability (defense-in-depth)
- ***Designing*** what DoD looks like to partners, to the public, to adversaries

Part 2

- Drive-out anonymity** (and enable net-centricity and improve sharing) by broad use of non-spoofable cyber identity credentials (aka **PKI**)
- Minimize whole classes of worries; brings accountability, *worries some classes of bad guys*

Build and operate an **attack detection and diagnosis** capability that allows rapid, sure, **militarily useful reaction** to cyber attacks

Improve joint, coalition, interagency, & industry partner cyber operations/ NETOPS so the above is possible

The Basics: Secure Configuration

(Or...configuring *everything* securely,
keeping everything configured
securely, and ensuring the right people
know this is so, or not so)

1. Define: Configuration guides with NSA, NIST, industry, military services, DISA

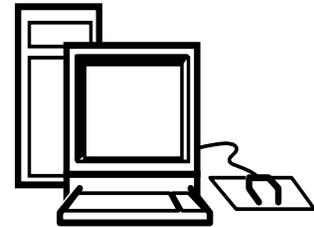
2. Buy it pre-configured

3. Configure it (Automate)

4. Measure it (Automate)

5. Change it (Automate)

6. Report it (Automate)



Big win:

(NSA/NIST/AF/DHS/DISA/Microsoft/OMB):

Federal Desktop Core Configuration

Security Content Automation Protocol

SCAP

- **Name for family of cyber security data standards**
 - Configuration description
 - Configuration measurement
 - Vulnerability
 - Etc.
- **NIST in the lead in defining; many are used now**
- **Goals is to improve sharing and improve automation**
 - Ex. “STIG” content can be machine readable and consumed by any compliant tool
 - DoD can purchase automation tools from any vendor that complies

Information Sharing in the Federal Government

Or, ***What System-High Wrought***

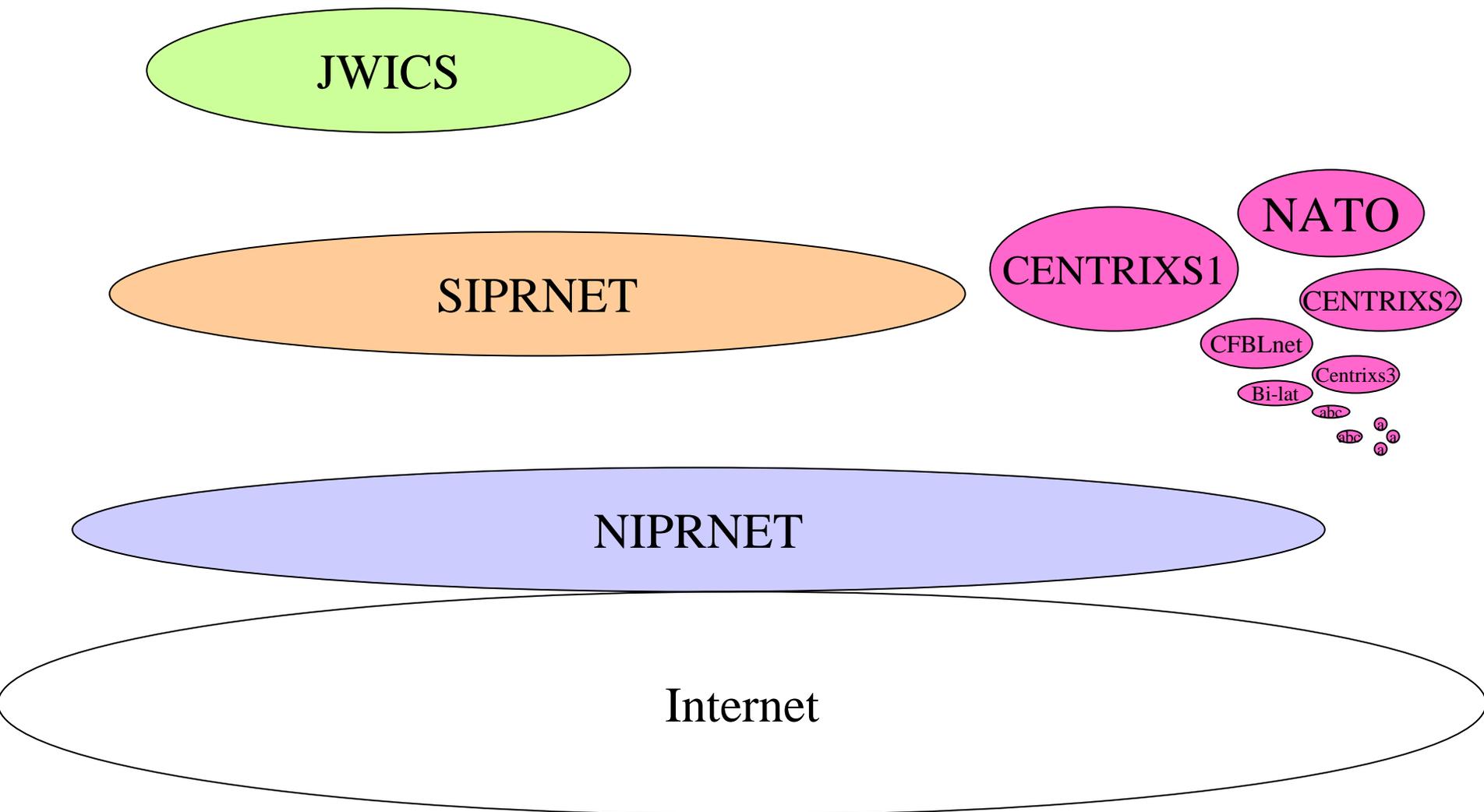
JWICS

SIPRNET

NIPRNET

Internet

Sharing With Allies



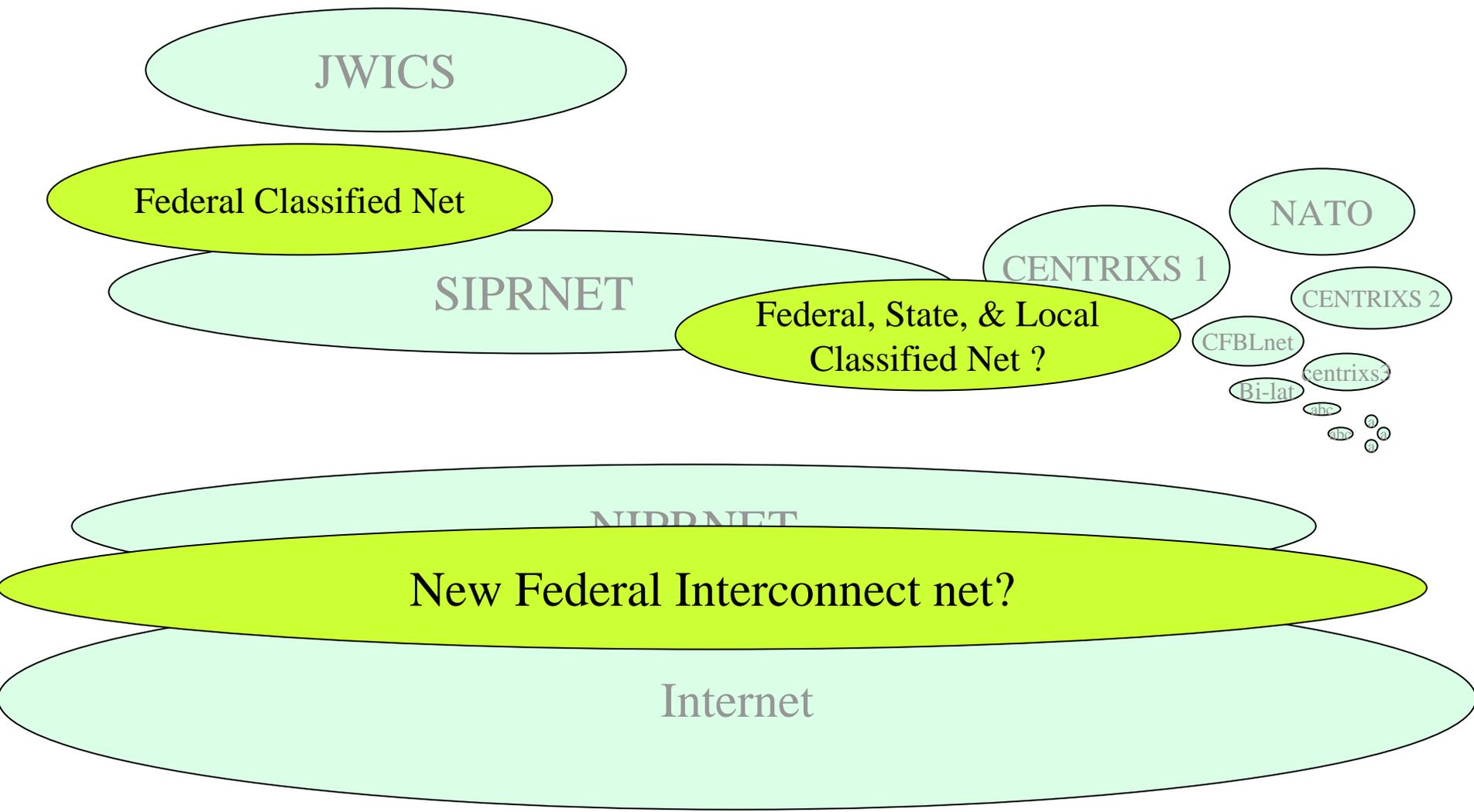
Q. Does all of this stuff really require system-high separation?

A. (My theory, although many others have concluded the same thing.)

Nope. Some of these networks can be treated as *separate communities within a single network infrastructure*

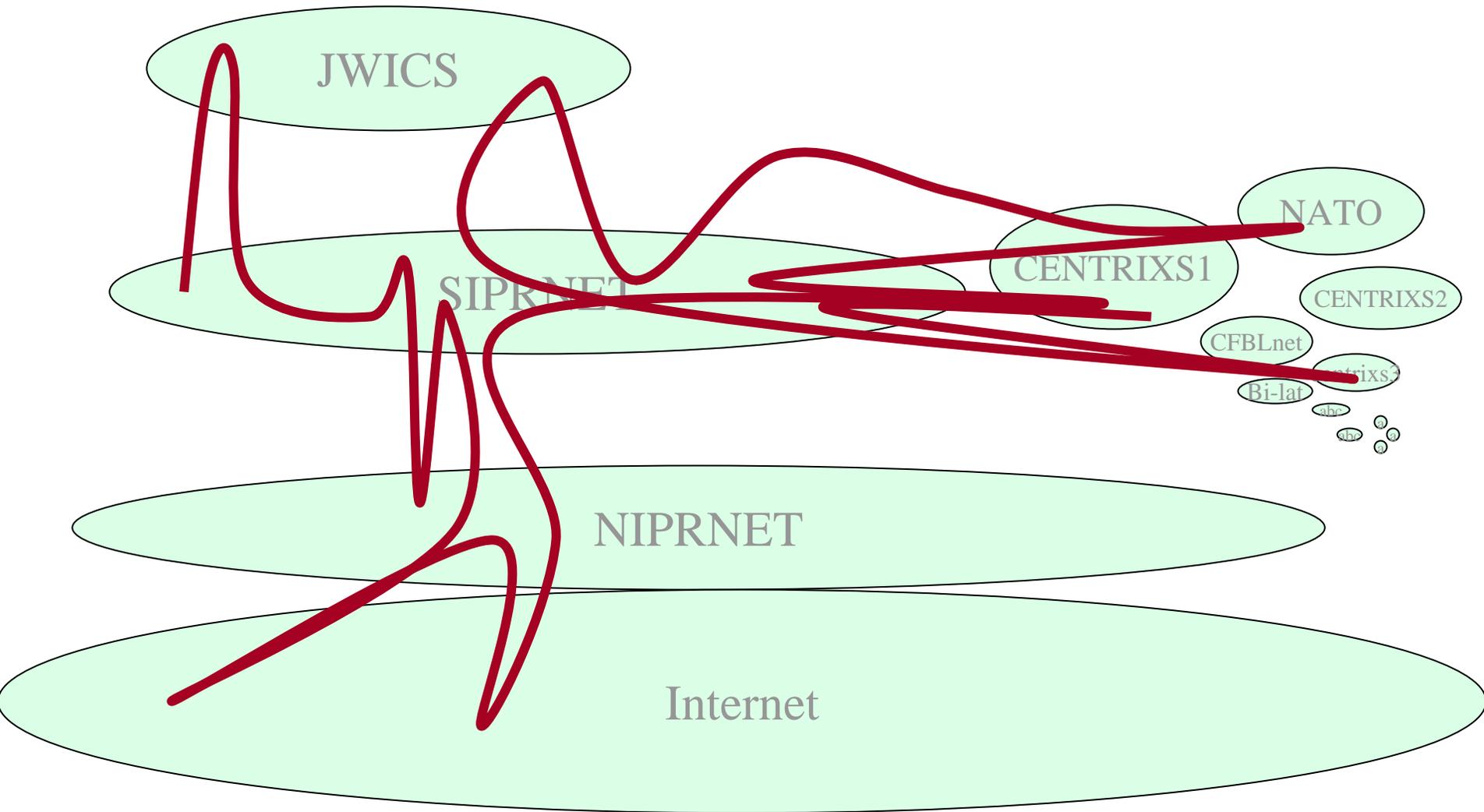
The CCER. The JCS & COCOMs & NII have asked DISA & NSA, to develop and deploy a method of consolidating several of the large CENTRIXS
– **CENTRIXS cross enclave requirement (or CCER)**

Sharing in the Interagency



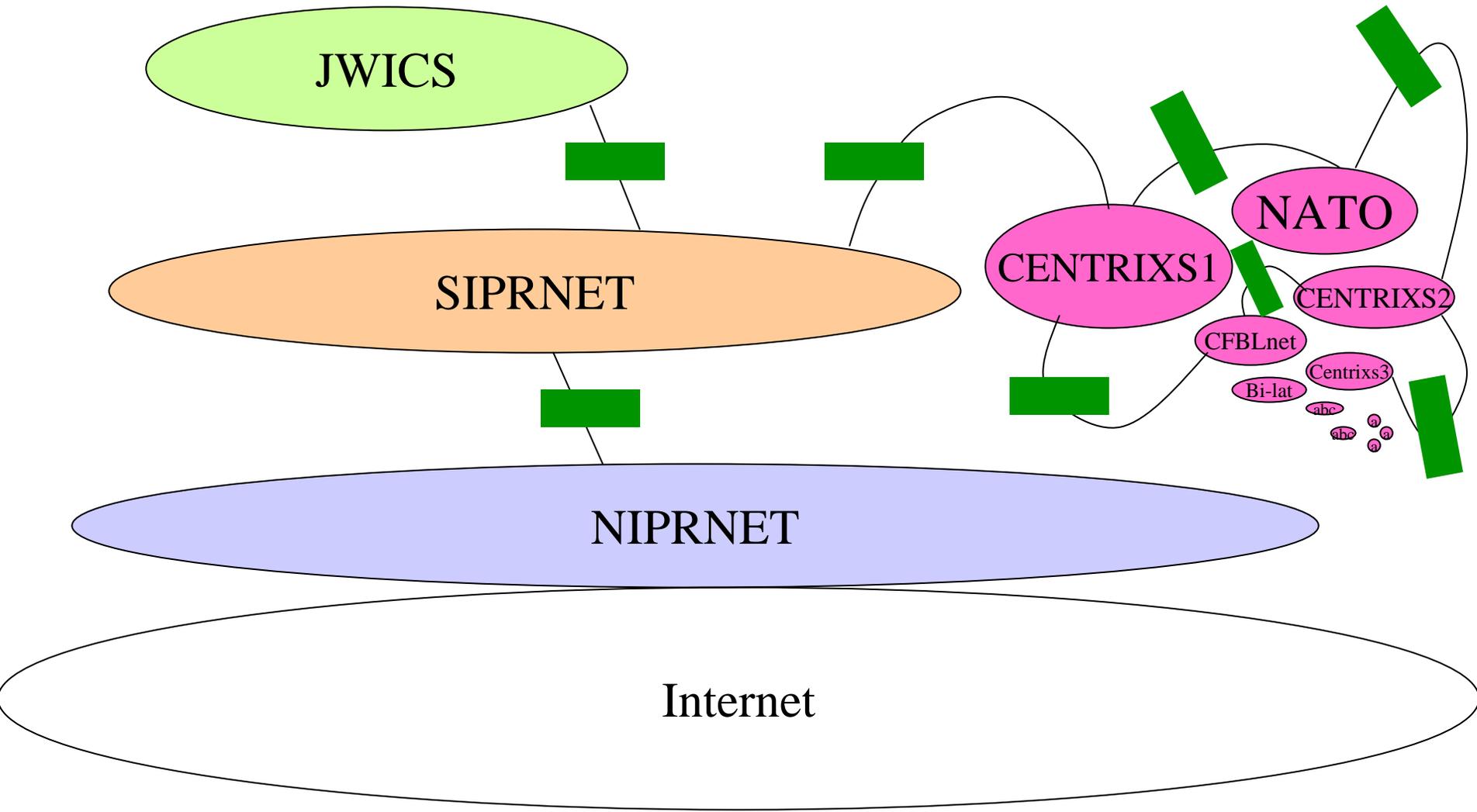
A Typical Netcentric Mission Thread

(or, sharing in spite of system high)



How Exactly Does *That* Sharing Work?

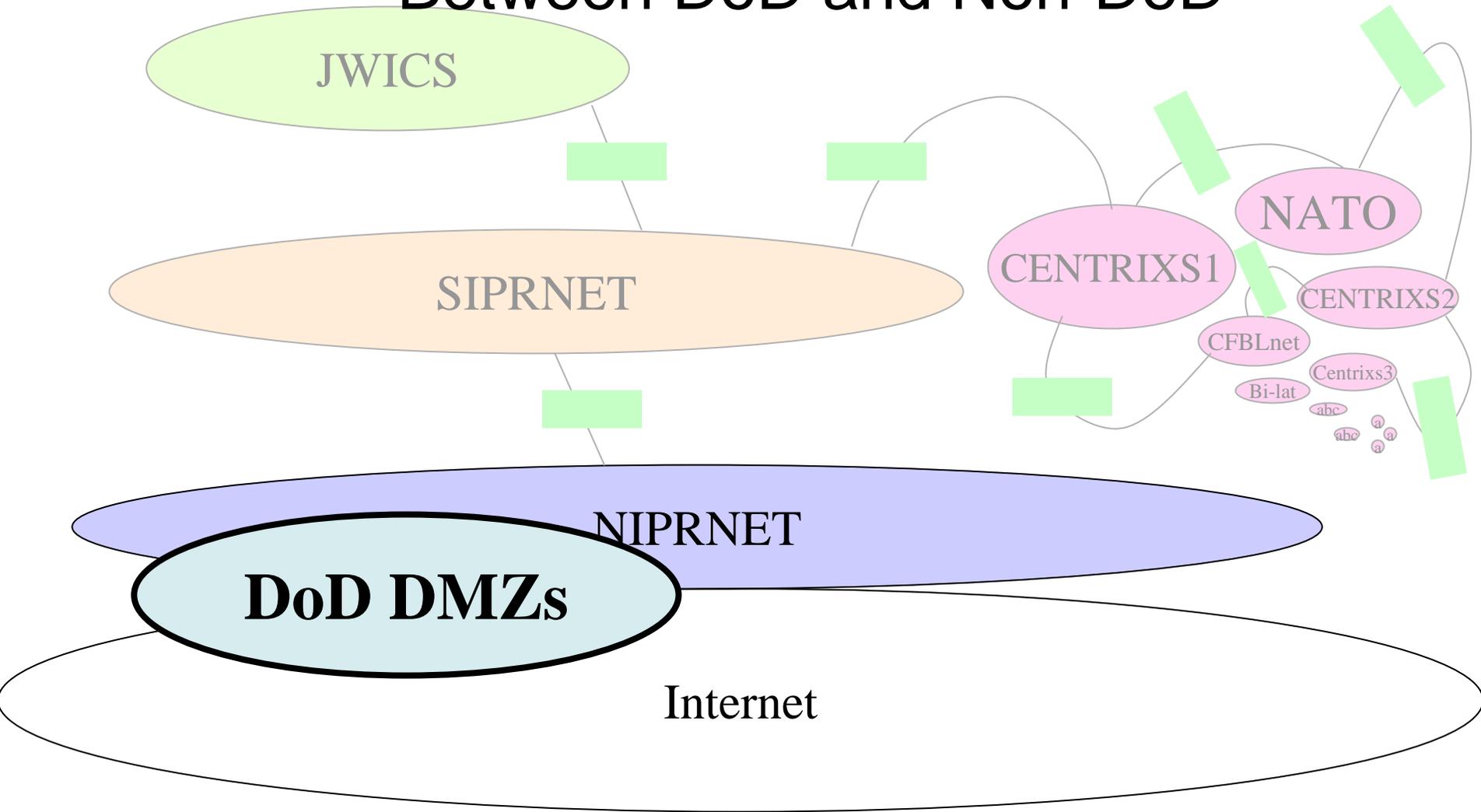
Sharing Part 1: That's What We Do With All That Cross Domain Stuff



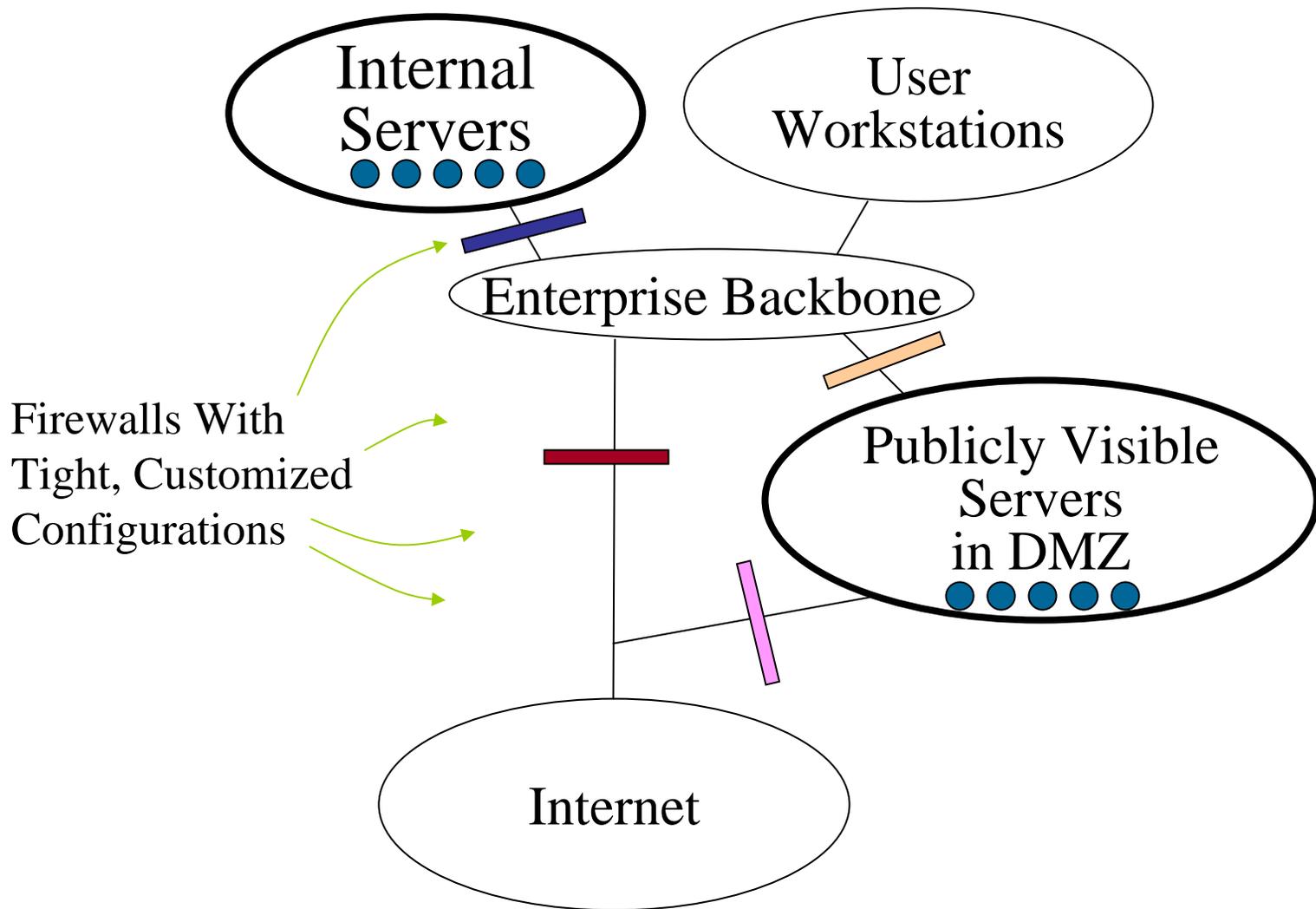
The Unified Cross Domain Management Office

- Intelligence Community and DoD effort to manage cross domain efforts
 - Approve standard products
 - Help customers find existing or modifiable technologies before developing more
 - Oversee the provision of *cross-domain as a network service*
 - Monitor technology development
 - Improve MLS certification and accreditation process
 - *As part of overall IC/DoD C&A re-engineering*

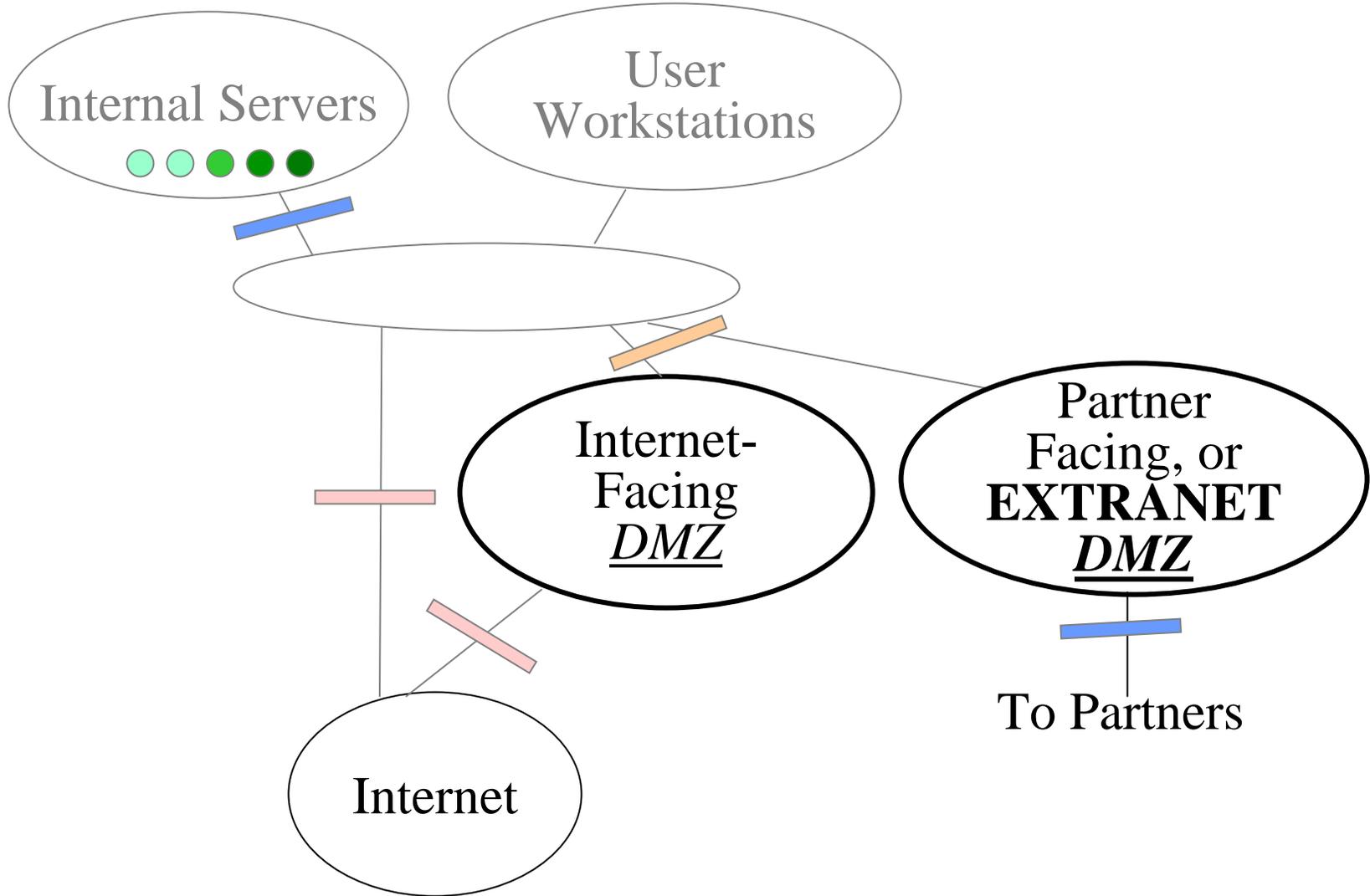
Sharing Part 2: Better DMZs Between DoD and Non-DoD



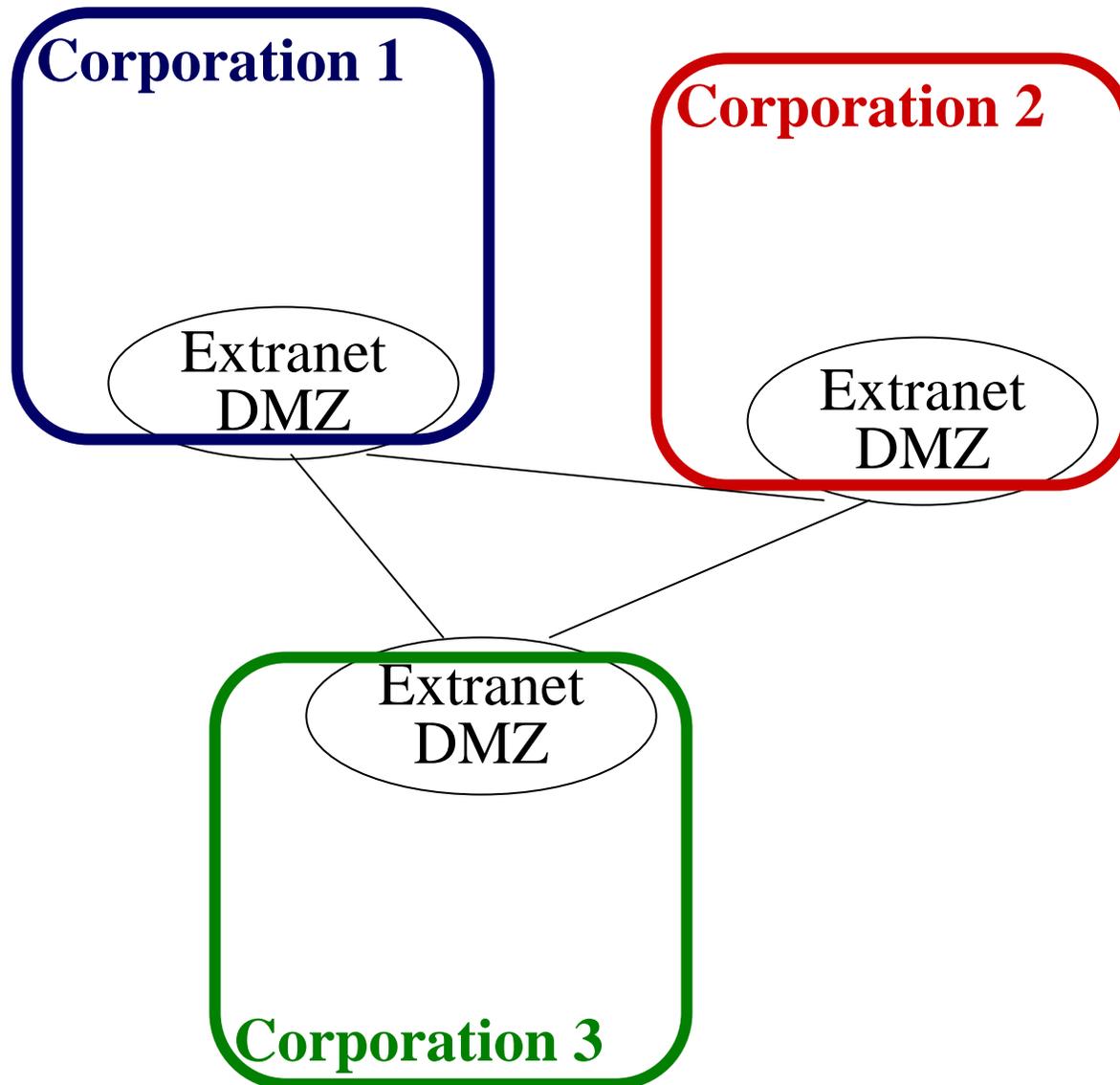
DoD DMZs



Sometimes There Is A Separate DMZ For Close Partners

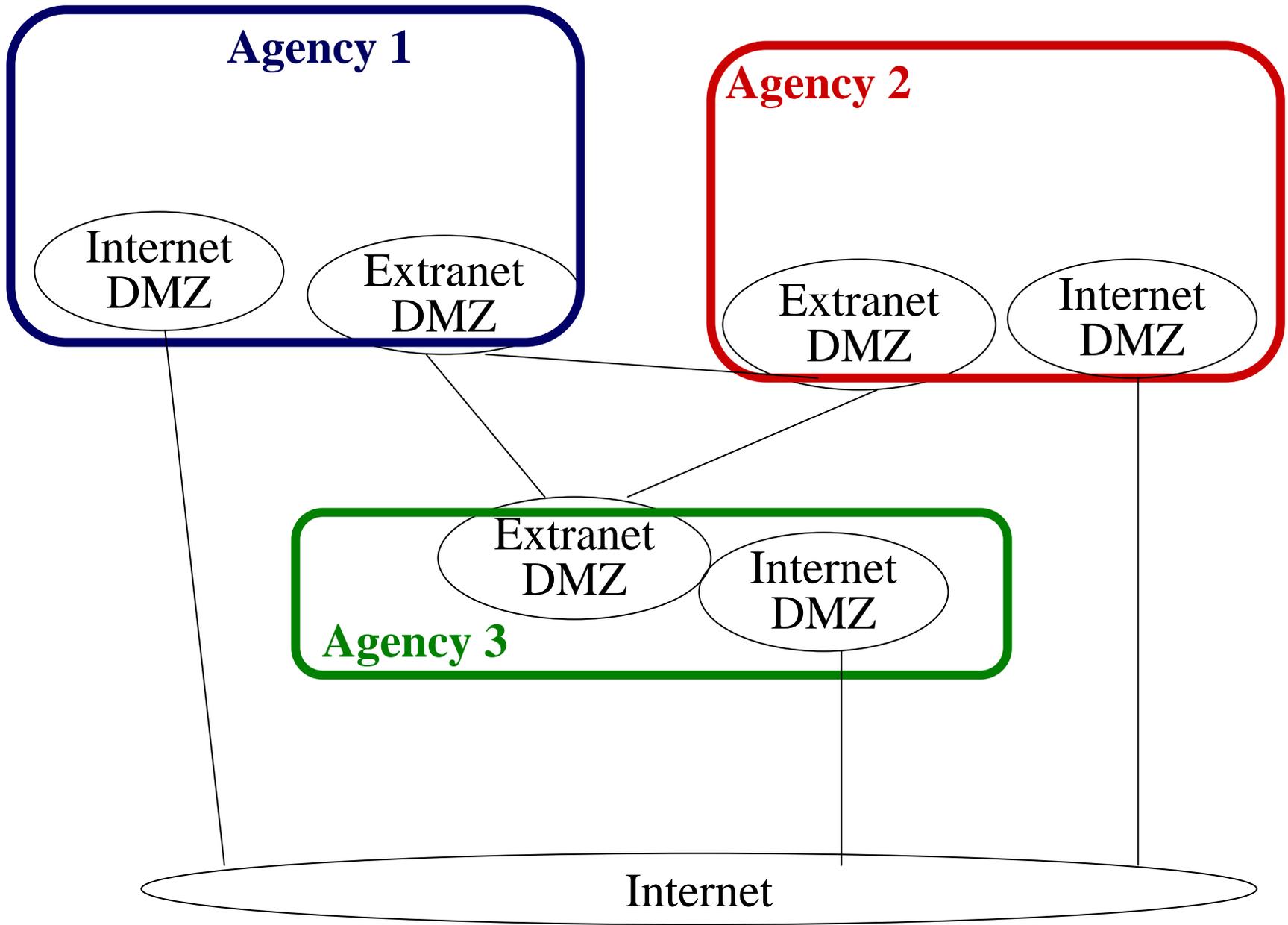


The Extranet DMZs May Be Attached to a Private Network, or *Extranet*



Unclassified Sharing in the Interagency?

One Result of the Trusted Internet Connection Initiative?



Other TIC Thoughts Based on DoD Lessons

- DoD has evolved various connection approval, compliance assessment, enforcement, and exception processes
 - These will likely need to be replicated in the inter-agency
 - Compliance enforcement must have teeth
- Partners *ALWAYS* have internet connections so connect to them via partner/extranet DMZs and monitor these as you would an internet connection
- Clear lines of authority for management of the connections is essential
- Sharing the attack detection and diagnosis data from the connection points is essential

A Little Bit About Driving Out
Anonymity:

PKI and Cyber Identity Credentials
(DoD PKI and Other PKIs)

**First, a bit about Bad Guys and
Directories**
(and why we have Public Key
Infrastructures)

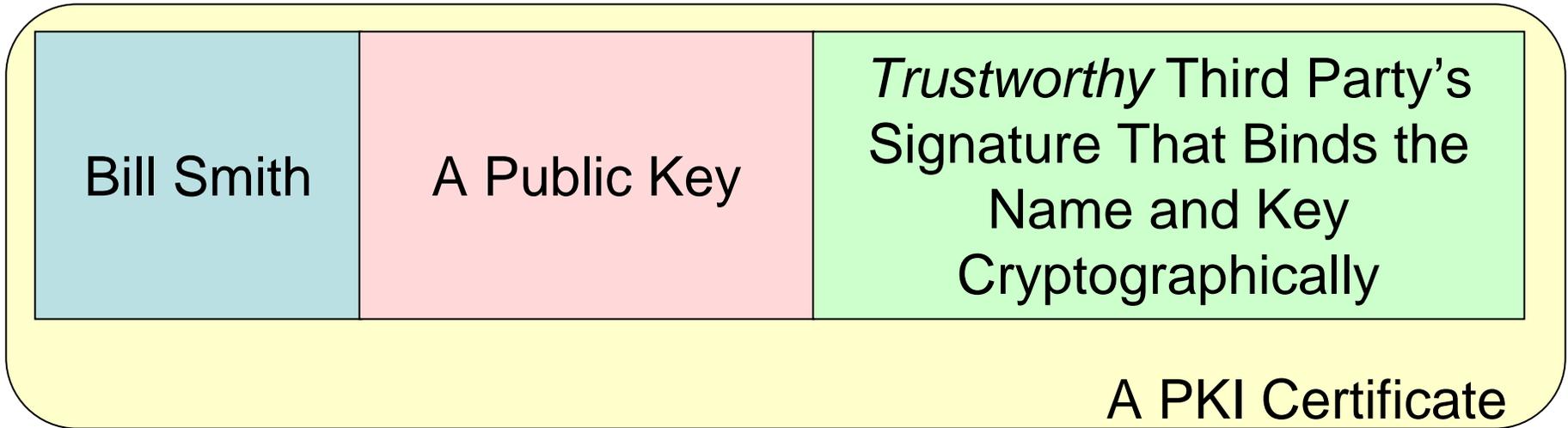
Publishing Public Keys: the old days

...One public key looks pretty much like any other

The Directory

| | |
|------------|--------------|
| Bill Smith | A Public Key |
| John Smith | A Public Key |
| Sam Smith | A Public Key |

Publishing Public Keys: Now



Increased *assurance* that Bill's public key is really his, and not John's or Sam's

An Important Detail...

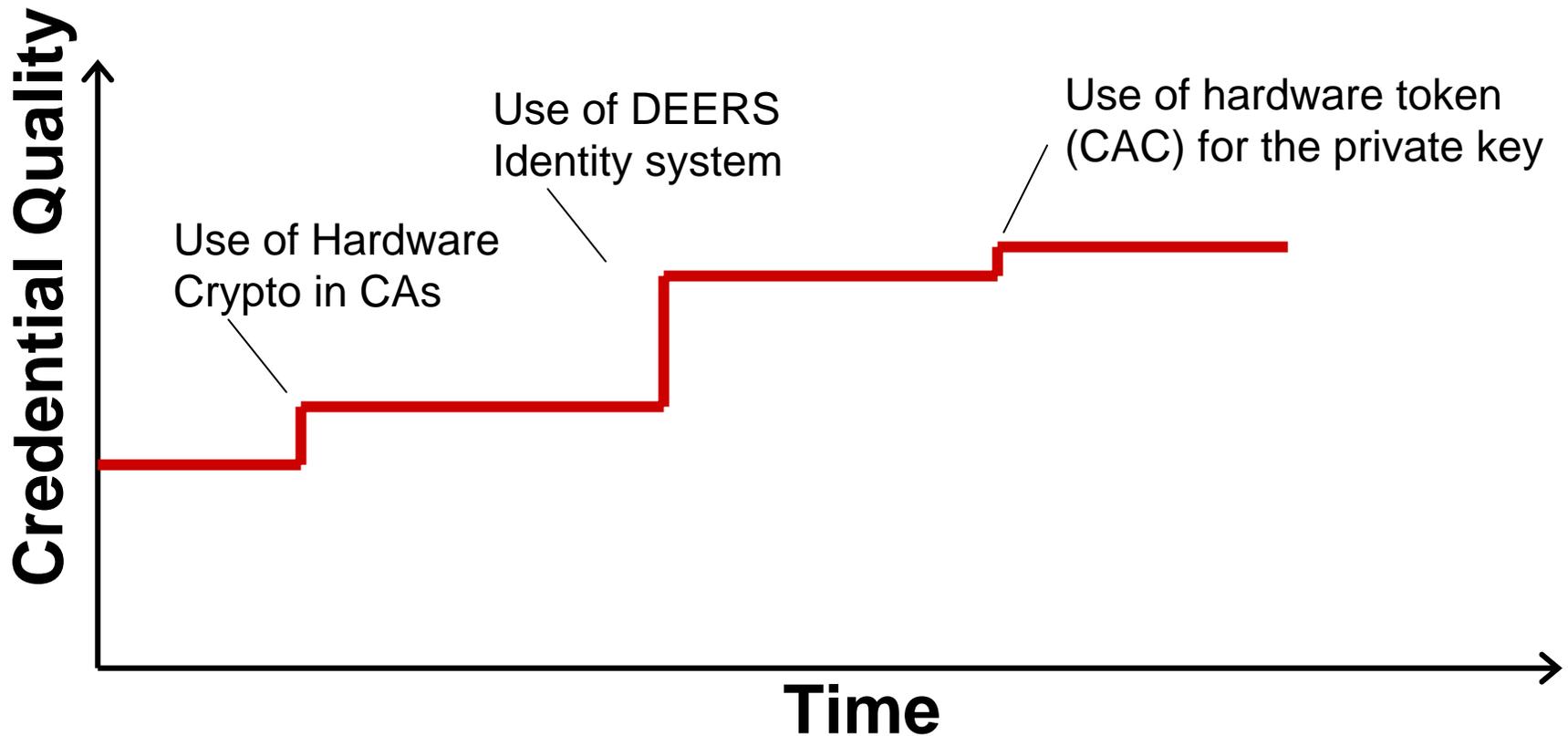
- Bill still needs to protect the other piece of the credential...the *private key*

The DoD PKI

- Primarily identity credentials for people (for now)
- Issuance tied to the pool of people identity in DoD...DEERS
- Single trust root, although credentials issued by many subordinate certificate authorities
- **Asserts very little other than the tie between a name and a public key**
 - **Must find those other tidbits about Richard Hale from other sources**
- Private keys (mostly) stored on the Common Access Card, or CAC
- Credential quality depends on many, many things...

DoD PKI Credential Quality

(How Much Can I Trust This Credential I've Been Presented?)



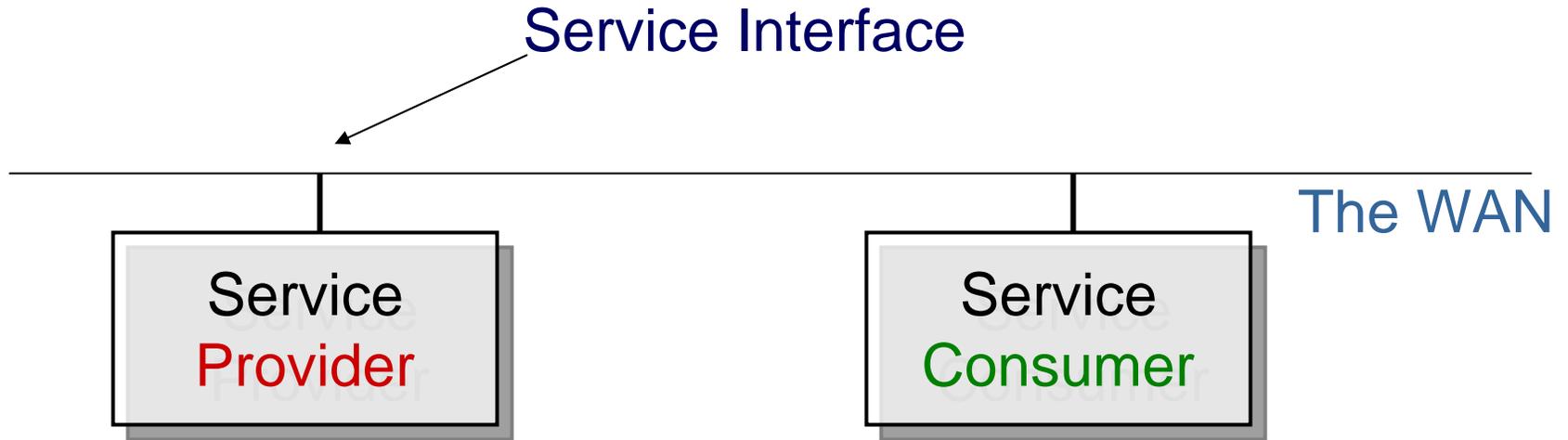
Lots of Assurance Increases in the Works for DoD & Other PKIs

- Improved cryptography (elliptic curve)
- Stronger protection of private keys, alternate tokens
- Better identity vetting of individuals before issuing a credential
- Stronger protocols between the certificate authority and the place the keys are generated
- More auditing
- Etc., etc., etc.

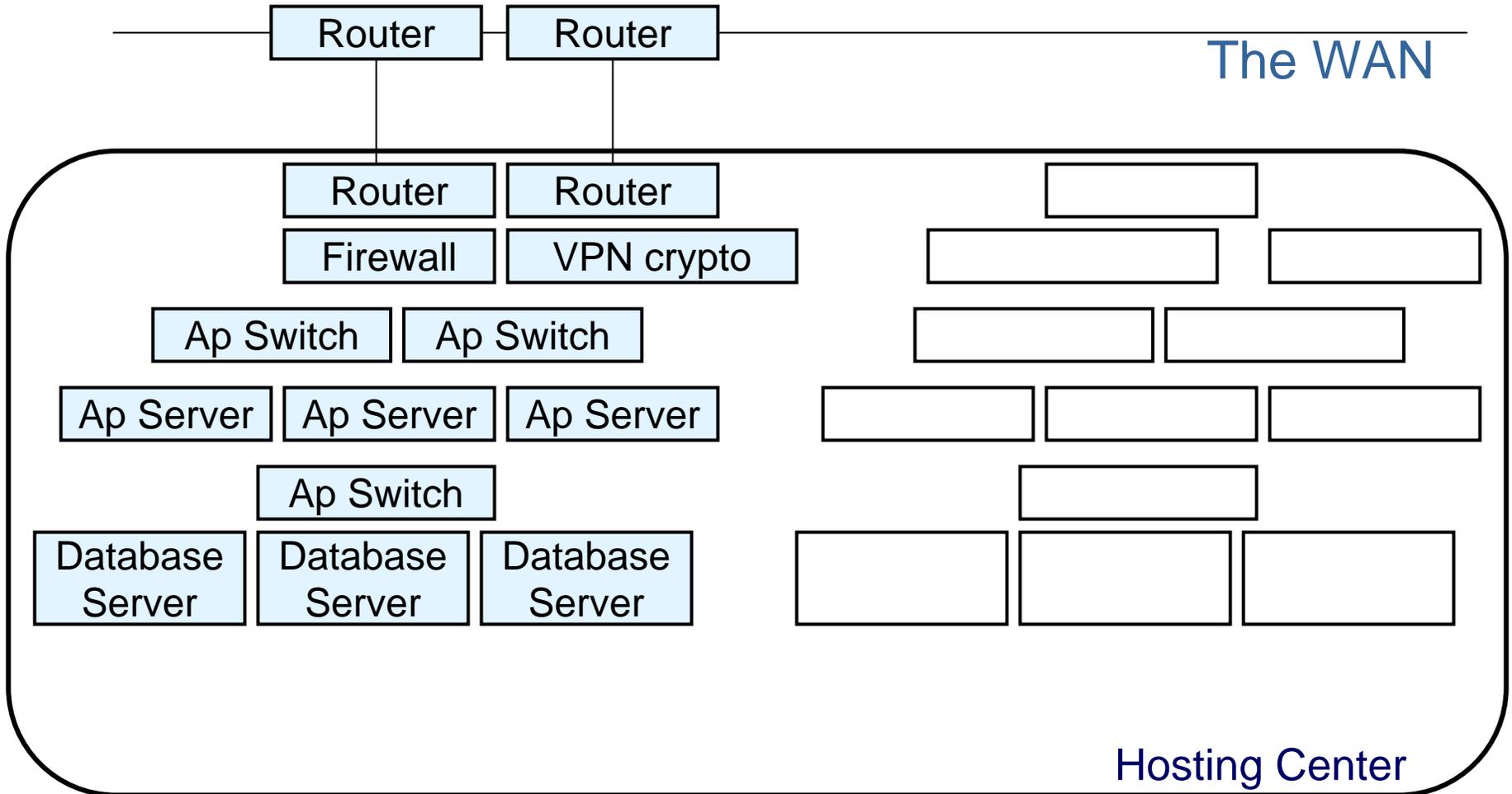
Sharing & Application Agility: *The Service Oriented Architecture*

*(We'll come back to my cyber identity credential,
and some of its uses)*

The Simple View of the SOA



What's Behind the Service Interface?



Dependable SOA Poses a Question

- **Each service consumer *relies* on some sort of statement by the service provider on the service being consumed**
- **Provider asserts things like**
 - Reliability of the service (in the face of equipment failure, circuit failure, natural disaster, cyber attack, whatever)
 - Accuracy of information
 - Performance, etc.

How does the consumer know whether to believe the claims?

Answers?

- Traditionally, a contract between supplier and consumer defines the terms of service
- In DoD and the IC, this isn't exactly how we work
- But, we could invent a scheme of point-to-point MOAs. But, this doesn't scale, even if we could figure out enforcement
- But, important missions, people's lives, and all sorts of things may depend on the service

So, I think *a third party* must verify the service providers' claim, then publish the findings

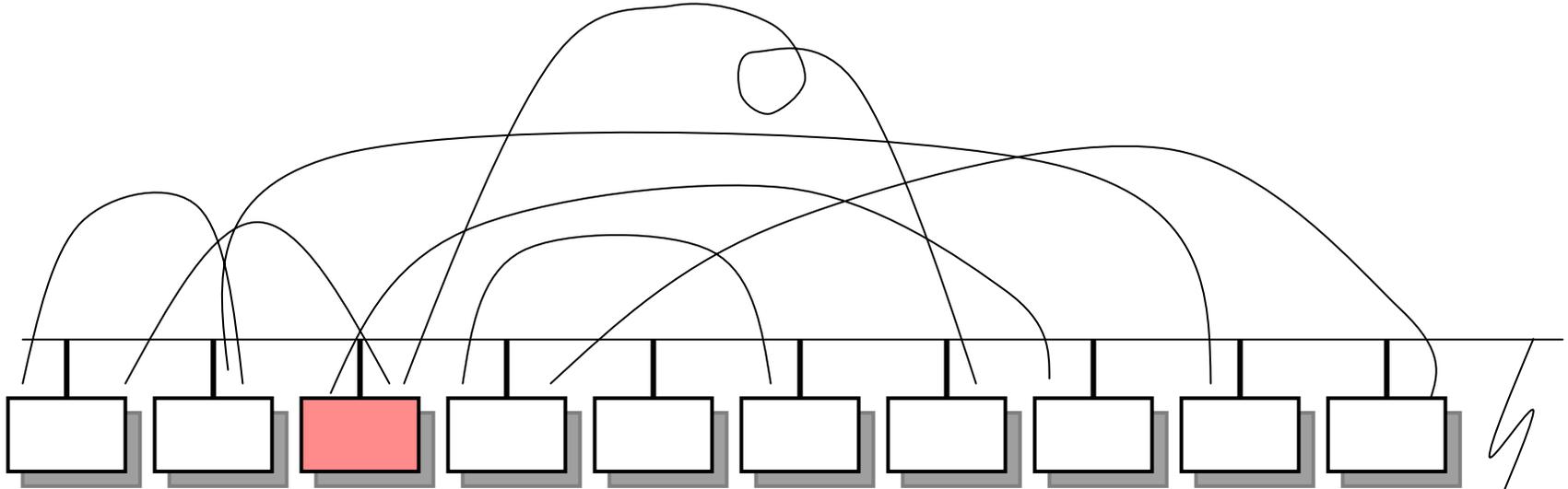
– (a Certifier, a Tester?)

Who Spot Checks These Claims?

- To ensure the service provider is continuing to satisfy the claims on which our consumer is depending
- Certifier?
- Tester?
- Blue Team? (Acting on behalf of both the consumer *and* the provider?)

Isn't This a Lot of Trouble Over
Something That's Not That Hard?

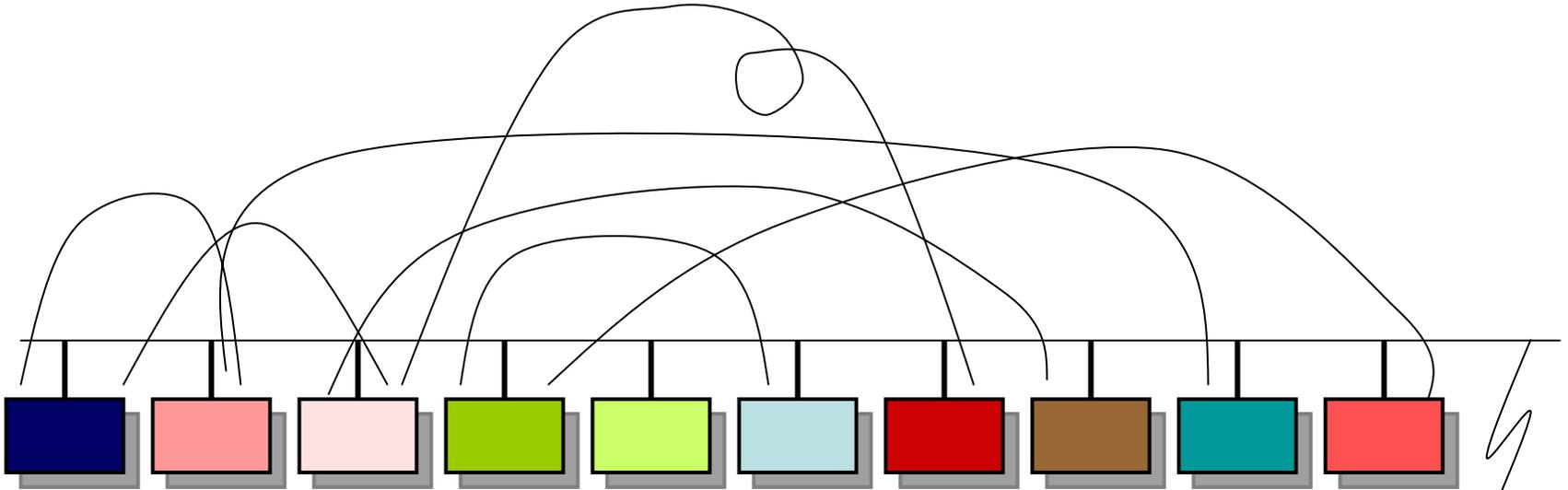
Composition of Services into an Application



Our service is a participant in a composed application serving a soldier in the field



Many Service Providers



“Dependability in the Face of Cyber Attack”



Back to Sharing While Keeping a Secret

If We Have Thousands of Services, Can an Access-Control-List Access Model Work?

Enter ... ***Attribute-Based Access Control***

- Important in the SOA going forward
 - Scale
 - Policy flexibility (*share information with unanticipated person without having to give the person an account*)

Before:

Allowing me to access information,
Allowing me to act in a certain role,
Doing business with me, etc.

Step 1. **Determine that it's *really* me**

Step 2. ***Then, learn things about the real me***
before deciding to take a risk on me

Step 1: I present my PKI credential and use my private key to authenticate.

Then, all that stuff *about* me comes into play

Who Knows, Who Tells the Things About Me?

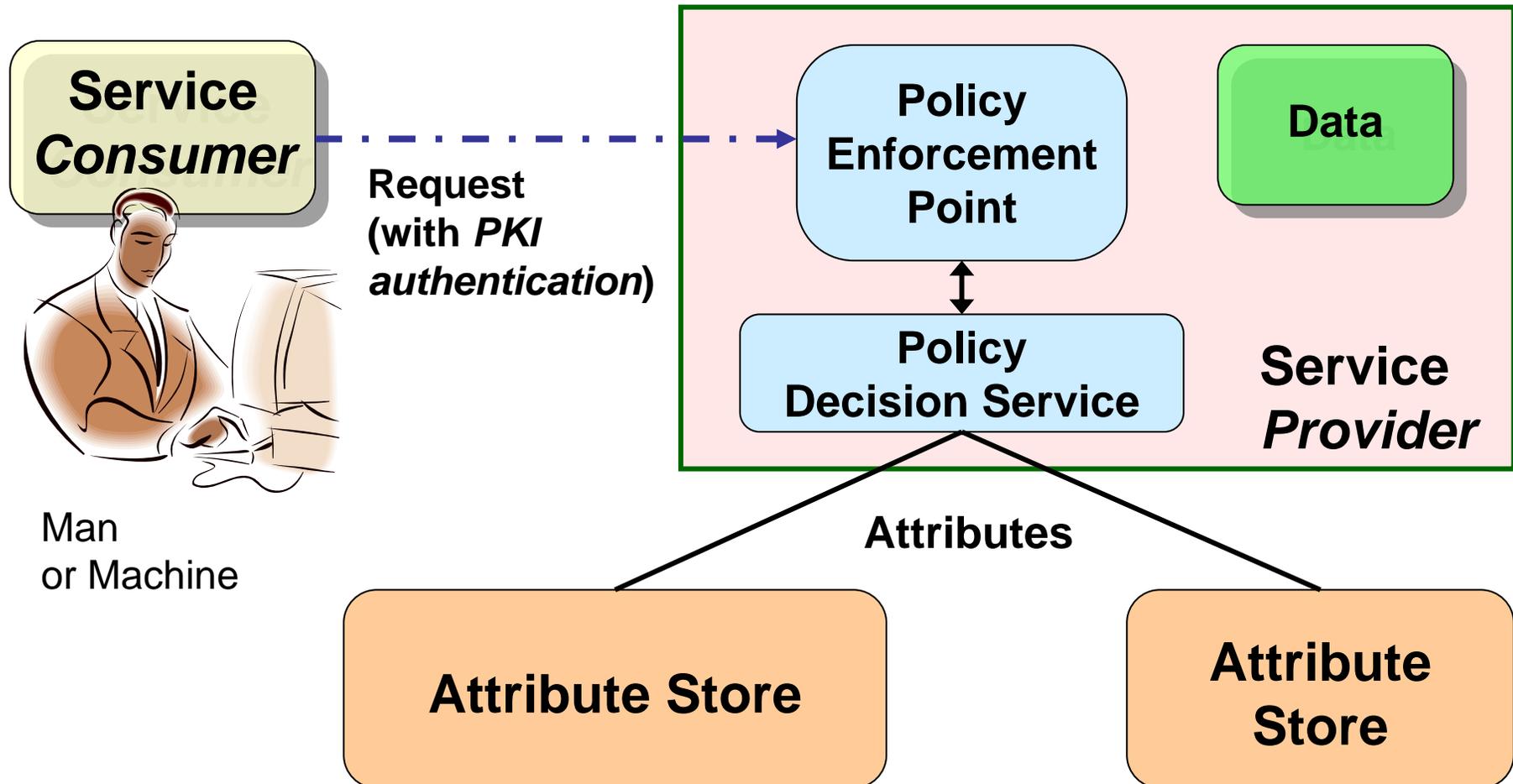
I Do

But if you don't know me, will you *trust* what I say?

Others Do

You *might* trust some of what *others* say about me (**attributes** about me)

Attribute-Based Access Control



Are Those Attributes Worthy of The
Service Provider's Trust?

Attributes and the Directory Problem

- Tight tie between me and my public key provided by my PKI cert (and by careful design of the issuance process)
- **Where's the tight tie between me (my name or some other unique identifier) and an attribute about me?**
- **Who is authoritative** for particular information about me?

How does a relying party know that my credit score, my clearance, my role, my grades, are really mine?

Incident & Attack Detection, Diagnosis, and Reaction

The Computer Network Defense Process

- **Detect** the incident or attack or problem (hopefully before it's launched)
- **Diagnose** what's going on
- **Develop militarily useful courses of action**
- **Pick** one
- **Execute** it
- Then **follow up**

All in militarily useful time

Realistic NETOPS Tactics, Techniques, Strategies

- This may (at any time) be a war fight
- Development of effective NETOPS war fighting tactics, etc. must be done by considering realistic adversaries
- Then we must *practice* these (and practice, practice, practice these)
- Practice at all levels of organizations, from individuals to small groups to ops centers to multiple ops centers...
 - You get the idea

This Also Requires Broad Sharing

- Sharing of raw sensor data, partial incident data, and more fully analyzed incidents is also critical
 - If we're to do this fast, and broadly across government and industry
 - **So, IMHO we've got to set standards for protecting this stuff so we're all willing to share...**

DoD Sets Standards and Accredits Computer Network Defense Service Providers

- The Interagency, industry, others will likely have to do this too

To Summarize...

1. Dependability in the Face of Cyber Attack

2. Keeping a Secret

Both While Simultaneously Sharing
Information Broadly



www.disa.mil

iase.disa.mil