PI Server Security

Bryan S. Owen
Omar A. Shafie

What is Security?

- se·cu·ri·ty
  - Pronunciation: \si-kyu̇r-ə-tē\
  - Function: noun
 - Date: 15th century

1. The quality or state of being secure:
   a) freedom from danger : safety
   b) freedom from fear or anxiety
   c) freedom from the prospect of being laid off

Source: Webster's Online Dictionary

PI Infrastructure Helps

- Information as a Survival Tool
  - Compete using a real-time data infrastructure
  - Collaborate across disparate systems
- Critical Infrastructure Protection
  - Defense in Depth for your systems

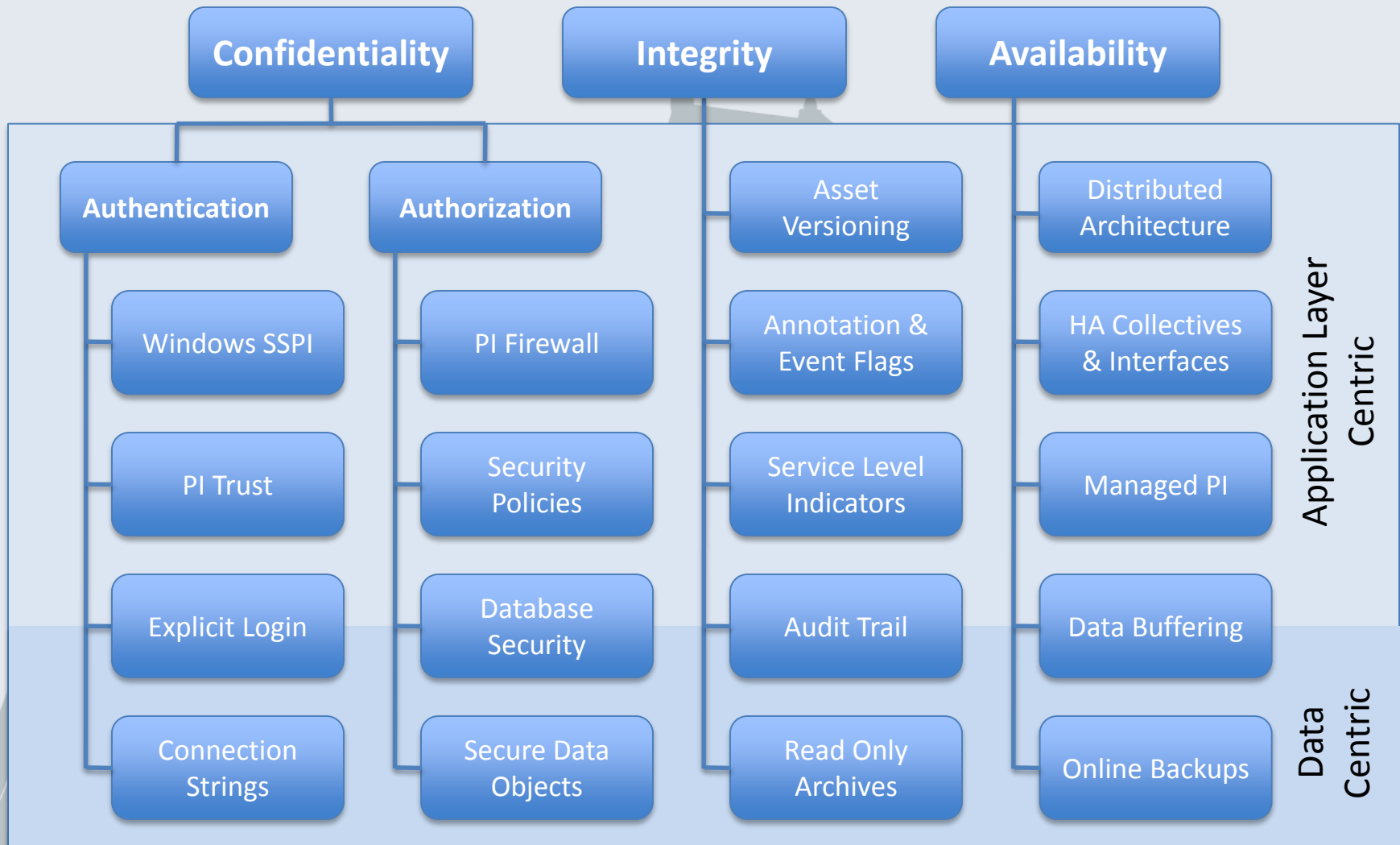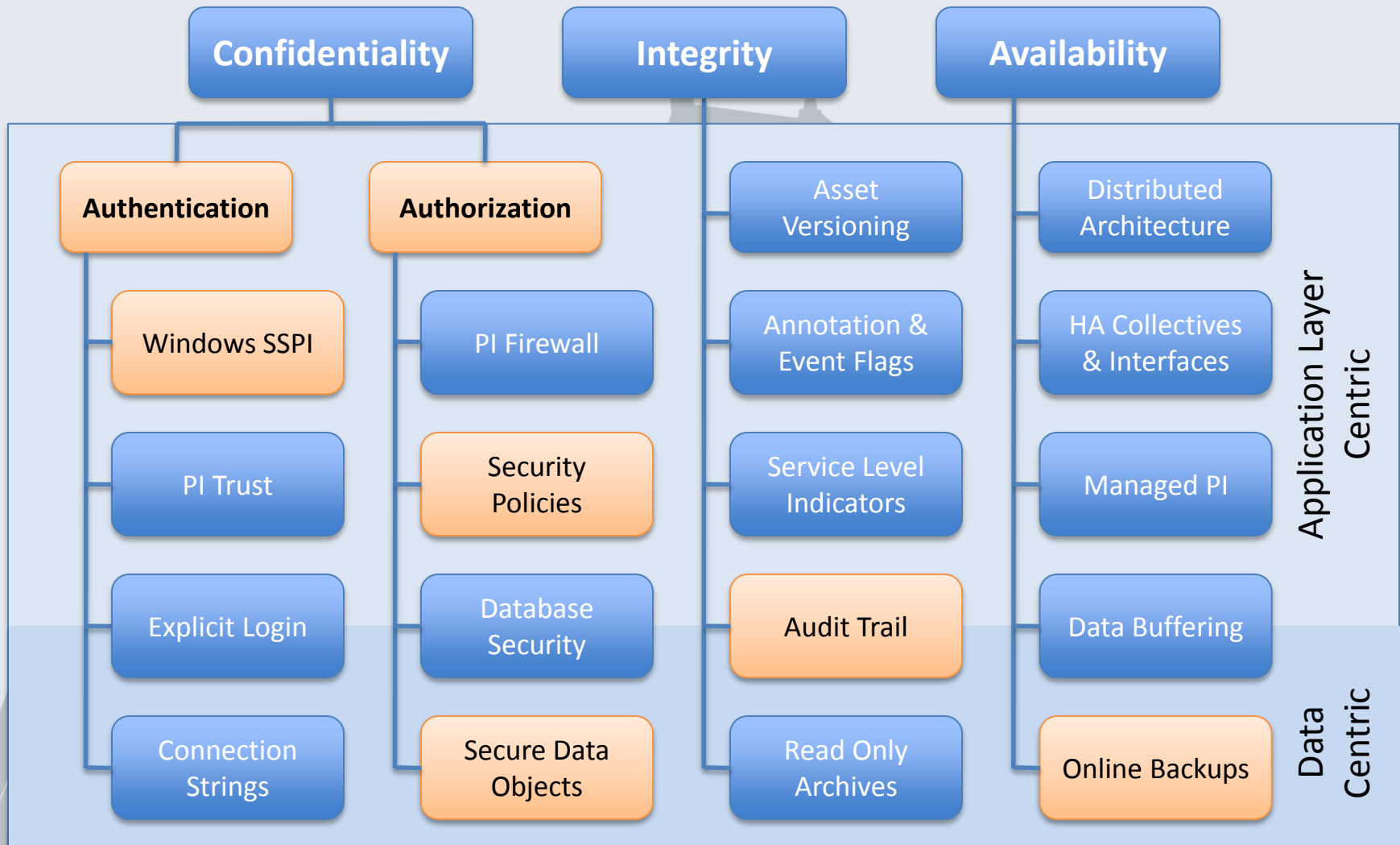| Zone	Network Depth	Software Depth
4	External	Network
3	Corporate	Operating System
2	Internal	Application
1	Critical	Data
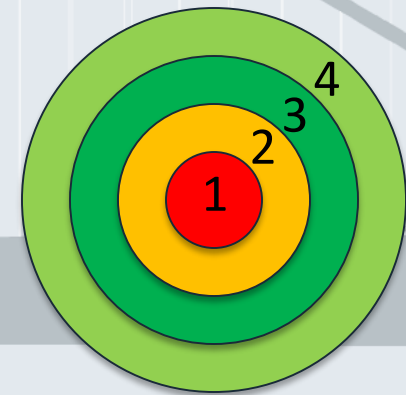
What's New in PI Server?

- Enhanced Security
  - Increased Control and Flexibility
- Less Maintenance
  - Security Features
  - Stability
- Better Manageability
  - System Management Tools (SMT)
  - Backward Compatible
- Lifecycle Support
  - 64bit and Windows 2008 (incl. Server Core)

CERTIFIED FOR
Windows
Server®2008

Security Feature Map

Confidentiality

Integrity

Availability

Authentication
- Windows SSPI
- PI Trust
- Explicit Login
- Connection Strings

Authorization
- PI Firewall
- Security Policies
- Database Security
- Secure Data Objects

- Asset Versioning
- Annotation & Event Flags
- Service Level Indicators
- Audit Trail
- Read Only Archives

- Distributed Architecture
- HA Collectives & Interfaces
- Managed PI
- Data Buffering
- Online Backups

Application Layer Centric

Data Centric

OSIsoft. 2009 USERS CONFERENCE SAN FRANCISCO

Security Feature Topics

Confidentiality		Integrity	Availability

Authentication	Authorization	Asset Versioning	Distributed Architecture
Windows SSPI	PI Firewall	Annotation & Event Flags	HA Collectives & Interfaces
PI Trust	Security Policies	Service Level Indicators	Managed PI
Explicit Login	Database Security	Audit Trail	Data Buffering
Connection Strings	Secure Data Objects	Read Only Archives	Online Backups

Application Layer Centric

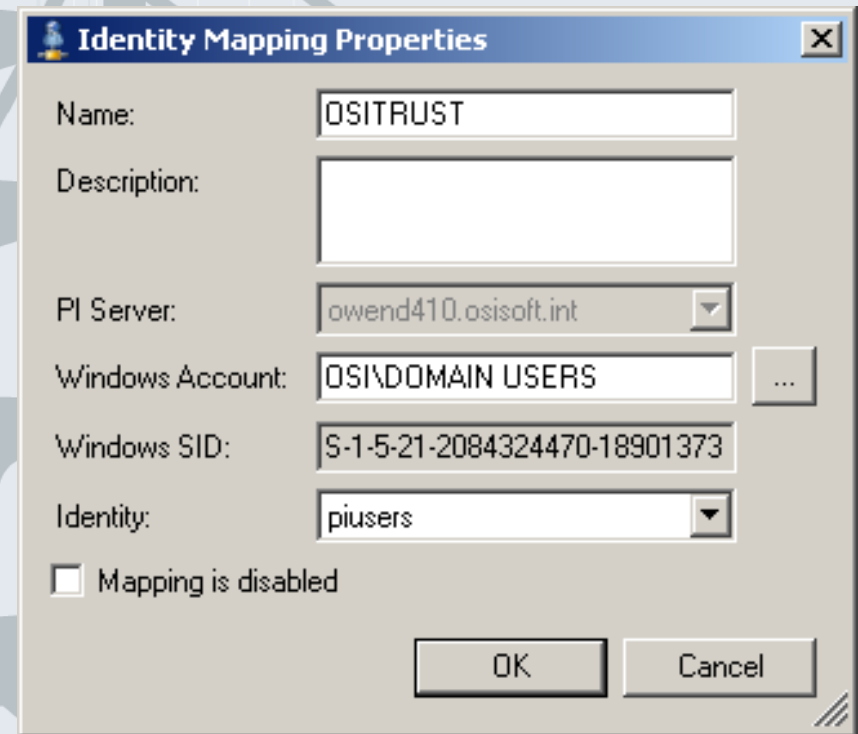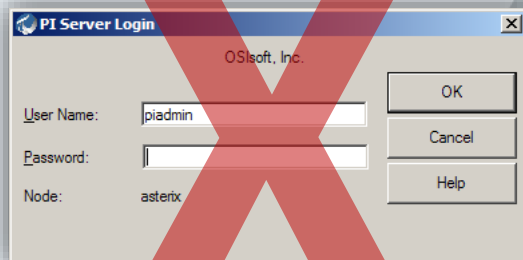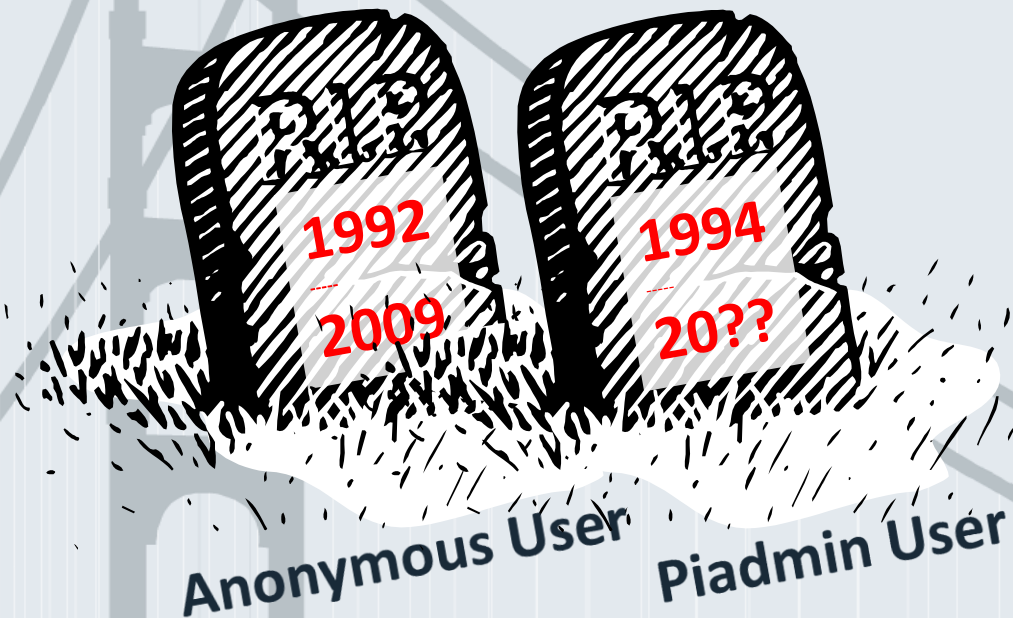Data Centric

Authentication

- ## Single Sign On – Windows Security (Kerberos)
  - ### One time mapping for Active Directory Groups
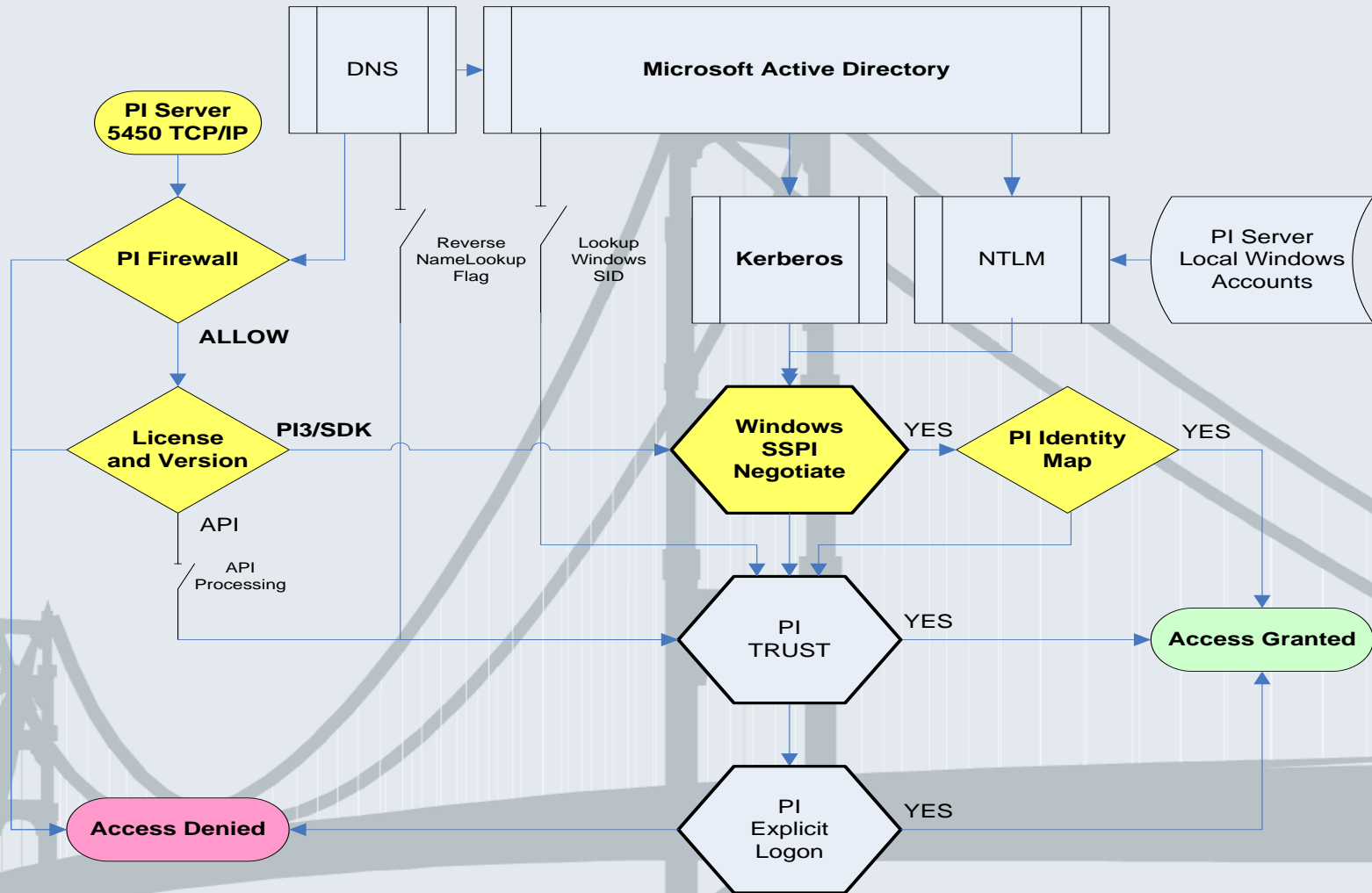
    …Just 5 mouse clicks

Authentication Policy

- Policies to Allow and Prioritize Methods
  - Windows SSPI
  - PI Trust
  - Explicit Login
- Granular Scope
  - Server
  - Client
  - Each Identity

1992
2009

1994
20??

Anonymous User

Piadmin User

Authentication Path

Authentication Summary

- Most Secure if PI Server is a Domain Member
  - Not required
- Manage Users and Groups
  - Centrally in Windows
  - One time association in PI
- Explicit Login and Trust
  - You have control

AUTHORIZATION

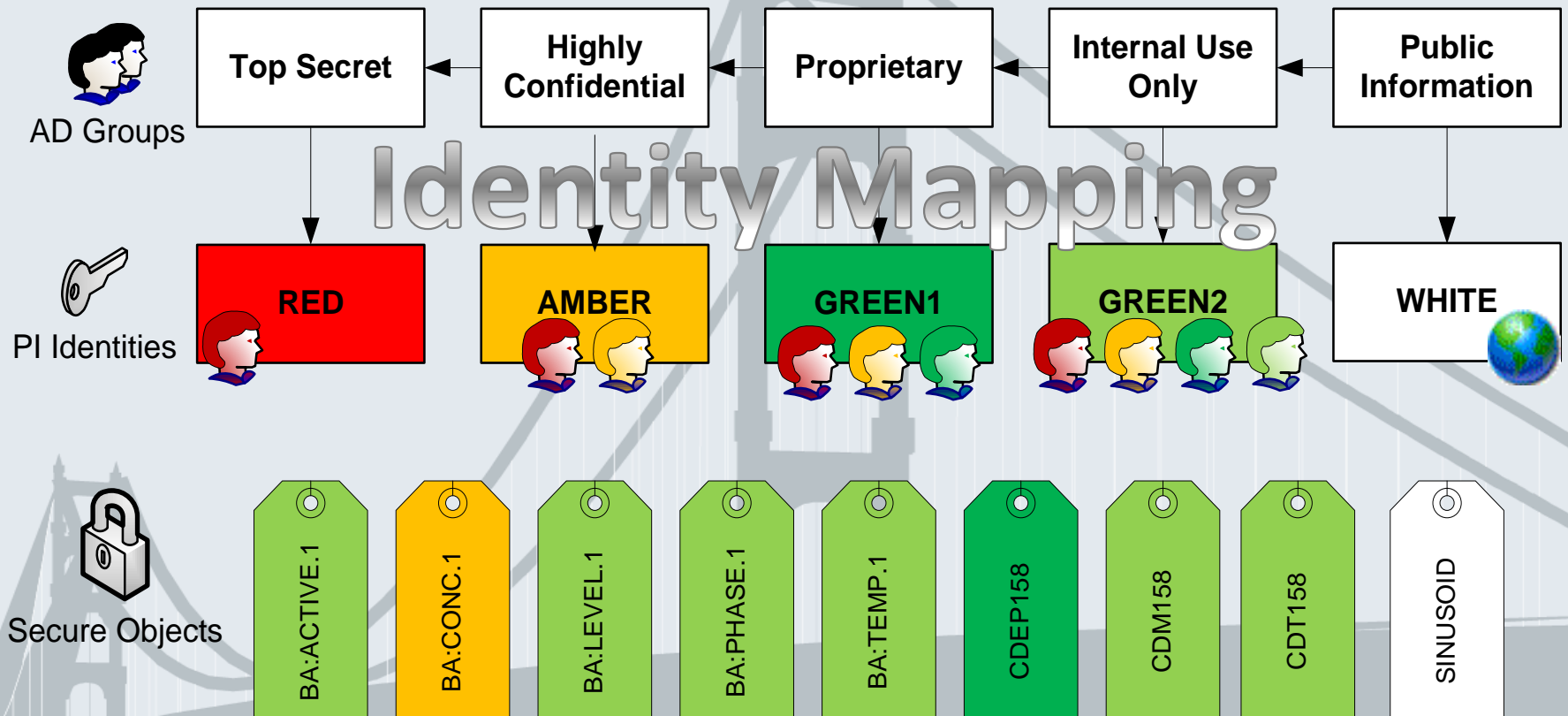## [-10400] NO READ ACCESS - SECURE OBJECT

Is Your Data Protected?

- Maybe…
  - Access is <u>ALWAYS</u> granted with piadmin
  - Factory setting allows world read access

- You <u>MUST</u> make changes!

- Default permission is configurable
  - Points: inherit from PIPOINT DBSecurity
  - Modules: inherit from parent

Standard Data Protection Example

ISO/IEC27000 mapped to G8 Traffic Light Protocol

AD Groups

Top Secret ← Highly Confidential ← Proprietary ← Internal Use Only ← Public Information

Identity Mapping

PI Identities

RED | AMBER | GREEN1 | GREEN2 | WHITE

Secure Objects

BA:ACTIVE.1 | BA:CONC.1 | BA:LEVEL.1 | BA:PHASE.1 | BA:TEMP.1 | CDEP158 | CDM158 | CDT158 | SINUSOID

History of Authorization Settings

- PI 2
  - Security by Display
    - Set permission level for each user and application (0-255)
    - Rights divided into 3 sub ranges
  - Security by Client Node (Read, Write, Login Policy)
- PI 3
  - Security by Point
    - PtOwner, PtGroup, PtAccess
    - DataOwner, DataGroup, DataAccess

In 2009…

How many configuration attributes per point?

2

- Access Control List (ACL) can be as long or short as needed

  D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)

  PtSecurity: Antarctica: A (r,w) | Americas: A (r) | Asia-Pacific: A (r) | Europe: A (r)

Point Builder - PI System Management Tools

File　View　Tools　Help

1 point

Point	Point Security	Data Security	
SINUSOID	Asia-Pacific: A(r)	Antarctica: A(r,w)	Americas: A(r)	Europe: A(r)	Green: A(r)	

General　Archive　Classic　Security　System

Data Access

Identities:

👤 Green

[Add...]　[Remove]

Permissions for Green	Allow
Read	☑
Write	☐

Point Access

Identities:

👤 Asia-Pacific　👤 Americas
👤 Antarctica　👤 Europe

[Add...]　[Remove]

Permissions for Antarctica	Allow
Read	☑
Write	☑

piadmin

What else in 2009?

- PI Network Manager
  - Stability and hardened stack
  - Performance
  - Enhanced SMT plug-in
- Message Log Subsystem
  - Filter by severity
    - Critical, Error, Warning, Informational, Debug
- Audit Trail
  - Windows user preserved

Also coming...

- Backup
  - Performs incremental backup
  - Checks integrity
  - Maintains "Last Known Good"
  - New SMT plug-in
    - On demand copy backup
   - Viewing backup history

Our Commitment to You

- Ongoing focus of Security Development Lifecycle
  - Help you with Best Practices
    - Reduce effort and improve usability
  - Eliminate Weakest Code
    - Cumulative QA effort with every release
  - Collaborate with Security Experts
    - Industry, Government, Academia, Customers

Basic	Standardized	Advanced	Dynamic
Security is reactive Customer risk is undefined	Security is proactive Customer risk is understood	Security is integrated Customer risk is controlled	Security is specialized Customer risk is minimized

Call To Action

- Protect our Critical Infrastructure
  - Use PI for Defense in Depth
  - We are all stakeholders
  - Patch management is important
    - Vulnerability in PI Network Manager (18175OSI8)

- See for yourself how security is easier than ever before
  - Come try SMT with the PI Server beta
  - Plan your upgrade today!
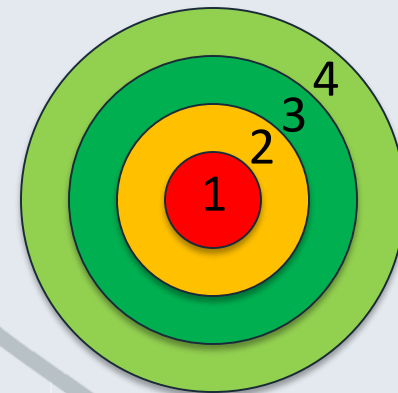
Being Secure Is…

- More than regulations and features
    - Technology can help
- A state of mind, knowing
    - Your systems
    - What to do
    - Who you trust
    - OSIsoft wants to earn your trust