OSIsoft®

USER CONFERENCE

2008

AMSTERDAM

Empowering Business in **Real Time.**

PI Infrastructure for the Enterprise.

OSIsoft®
USER CONFERENCE
2008
AMSTERDAM

Windows Integrated Security for the PI Server

Hans-Herbert Gimmler
Rulik Perla

© 2008 OSIsoft, Inc. | Company Confidential

PI Server Security? Why?

- PI is a system you trust!
  - To maintain the quality of your product
  - To facilitate the safety of your operations
  - To drive innovation and investment
- Anywhere, anytime access adds value… but:
  - Who has access?
  - What can they do?
- The keys: Authentication and Authorization

© 2008 OSIsoft, Inc. | Company Confidential

Objectives

Respond to your requests for:

1. More flexible access control
2. More secure authentication methods
3. Leverage Windows for account administration
4. Single sign-on (no explicit PI Server login required)

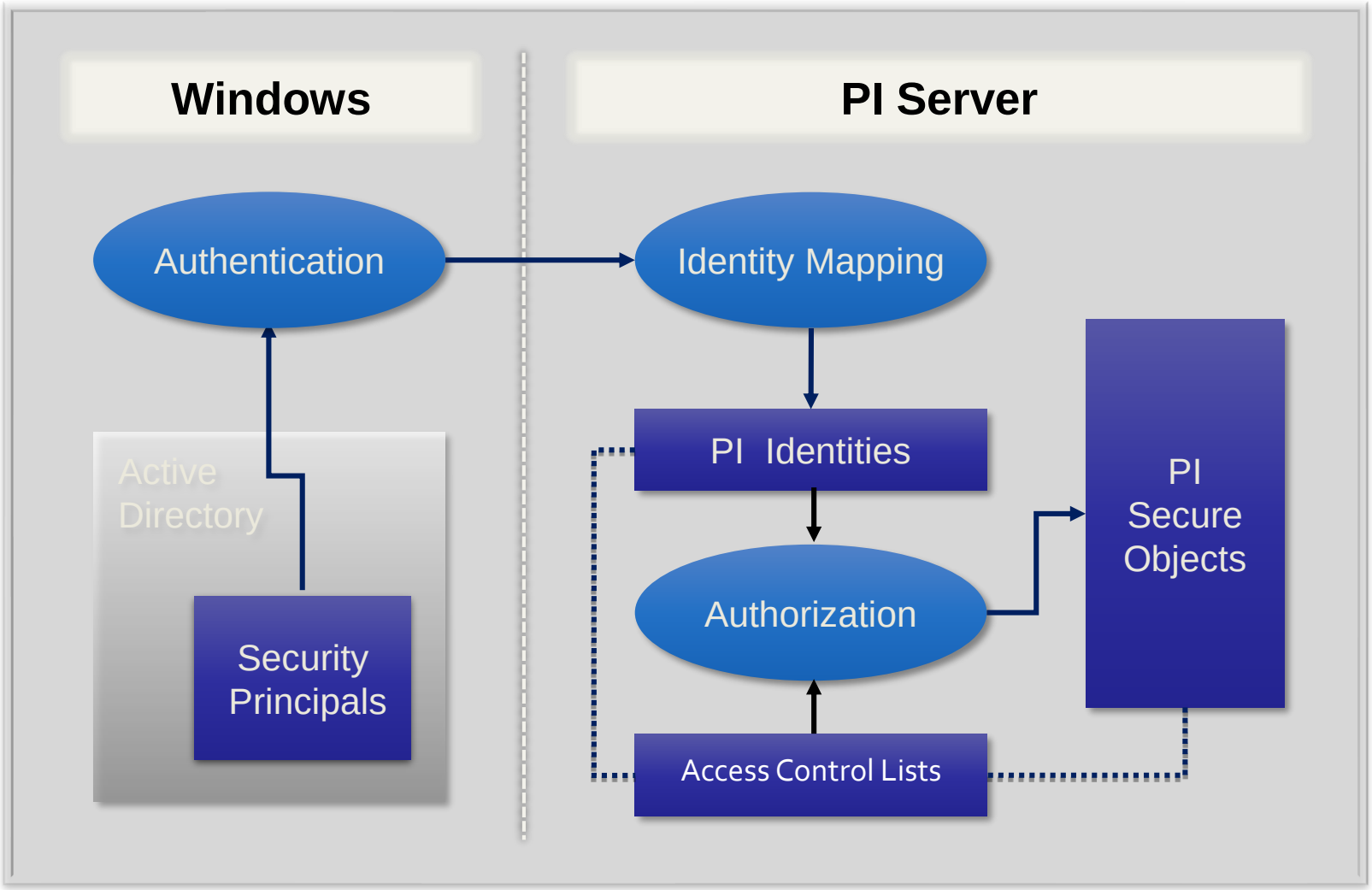
© 2008 OSIsoft, Inc. | Company Confidential

Architectural Overview

- Our Current Security Model
  - Choice of access rights: read, write
  - A single owner (per object)
  - A single group association
  - And then everyone else . . . “world”
- The New Model
  - Support for Active Directory and Windows Local Users/Groups
  - Mapping of authenticated Windows principals to “PI Identities”
  - Access Control Lists for points, etc.

© 2008 OSIsoft, Inc. | Company Confidential

WIS in a Nutshell



© 2008 OSIsoft, Inc. | Company Confidential

And more simply: Keys and Locks

Authentication

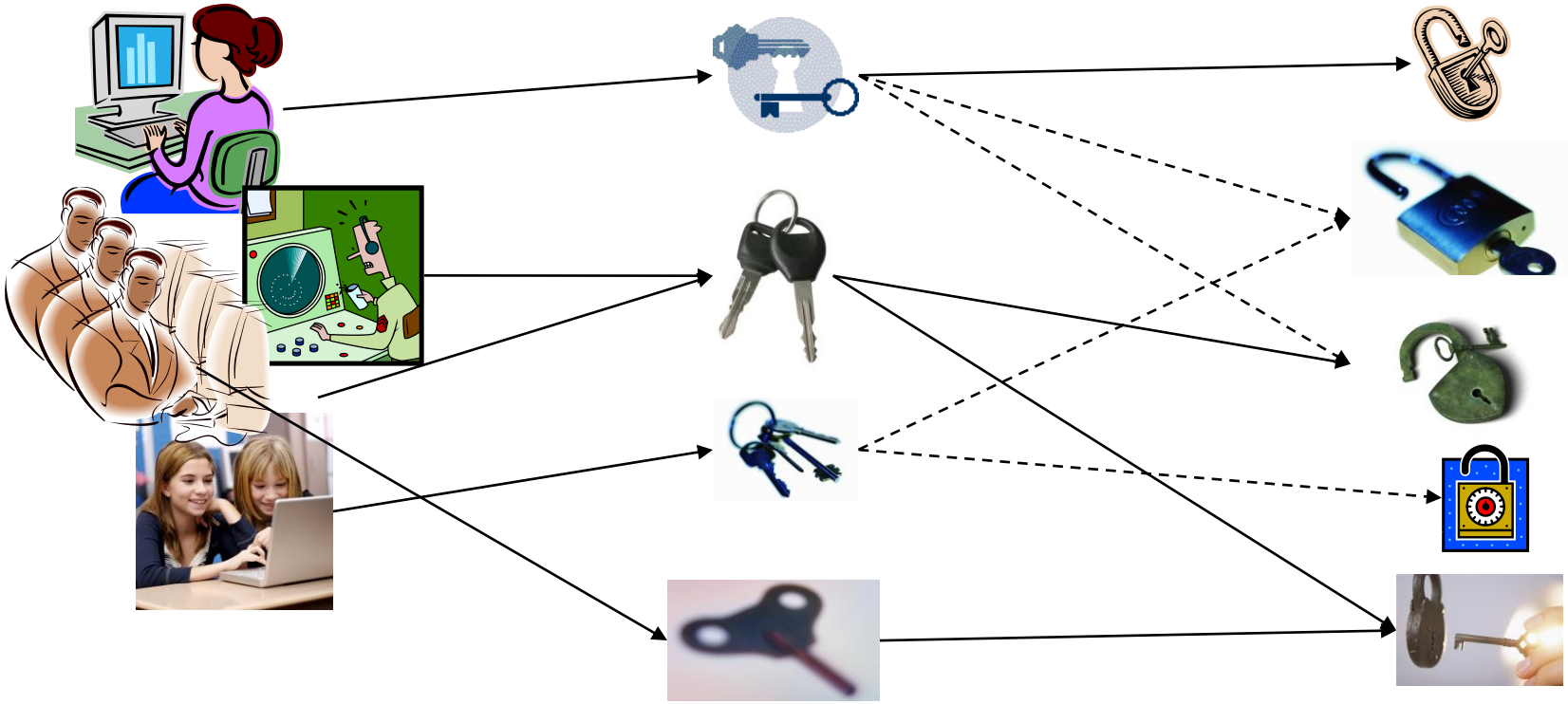
Authorization

ID Mapping

Users and Groups

PI-Identities

PI secure Objects



© 2008 OSIsoft, Inc. | Company Confidential

User Authentication

- Until Now
  - Explicit Login: validation against PI internal user database
  - Trust Login: validation of user's Security Identifier (SID)
- PI Server 2008 Release
  - Authentication through Microsoft Security Support Provider Interface (SSPI) – Negotiate protocol
  - Principals from Active Directory
  - Principals from local system
  - Configurable authentication modes (client-side and server-side)

© 2008 OSIsoft, Inc. | Company Confidential

PIIdentities

- Purpose
  - Link Windows principals with PI Server objects
- What are PI Identities?
  - A representation of an individual user, a group, or a combination of users and groups
  - All PIUser's and PIGroup's become PIIdentities
- Why?
  - To maximize flexibility for controlling user access to secure objects within the PI Server

© 2008 OSIsoft, Inc. | Company Confidential

PIIdentities (cont'd)

- 3 Types: PIUser, PIGroup, and PIIdentity
- All existing PIUser's and PIGroup's are included
  - piadmin, pidemo
  - piadministrators (renamed piadmin), piusers (plural)
- Best viewed as "roles" or "categories"
  - Similar to SQL Server logins
  - Suggested categories (as pre-defined defaults):
    - PIWorld, PIEngineers, PIOperators, PISupervisors
  - Customizable according to your needs
    - Add new Identities
    - Rename existing Identities
    - Disable Identities

© 2008 OSIsoft, Inc. | Company Confidential

PI Identity Mappings & Trusts

- Mappings
  - 1 Principal (AD/Windows group) to 1 PI Identity
    - Example: COMPANY\Supervisors to PISupervisors
  - Authenticated users have 1..N PI Identities
    - A user typically belongs to many (nested) groups
- Trusts
  - A trust points to 1 and only 1 PIIdentity
  - Enhancement: map to any PI Identities, not just PIUsers

© 2008 OSIsoft, Inc. | Company Confidential

PI Secure Objects: Authorization

- Main objects: Points and Modules
- Ownership Assignments
  - Objects are “co-owned” by PI identities
  - Any PIIdentity is eligible
  - Multiple ownership is now supported
    - not just 1 PIUser and 1 PIGroup
- Access Control Lists
  - Every secure object has at least 1 (points have 2)
  - The replacement owner, group, and access (“o:rw g:rw w:rw”)
  - Each identity in the list has its own set of access rights
  - ACLs compatible with the existing security model have 3 identities
    - 1 PIUser, 1PIGroup, and PIWorld (any order)

© 2008 OSIsoft, Inc. | Company Confidential

Making the Transition

- Existing security still supported
  - On upgrade: no loss of configuration, no migration
  - Downgrade only by restoring from backup
- Existing SDK applications
  - Preserve existing behavior
    - Can still connect via explicit logins or trusts
  - Single sign-on after SDK and server upgrade
    - No configuration or code changes to client applications!

© 2008 OSIsoft, Inc. | Company Confidential

Summary

- Windows Integrated Security Means
  1. More flexible configuration
  2. More secure PI Server
  3. Less maintenance
  4. Preserving customer investment

- We welcome your feedback!

© 2008 OSIsoft, Inc. | Company Confidential

Thank You

© 2008 OSIsoft, Inc. | Company Confidential