

Single Point Security

The Unisys Vision

Bill Buffam, Software Architect, Unisys Corp.

buffam@tr.unisys.com

Conventions



denotes a “you are here” slide



denotes a handout-only slide



Single Point Security

- **the problem**
- requirements for a solution
- the security spectrum
- Single Point Security function set

The Multiple Multiple Problem

- multiple servers
- multiple operating systems
- multiple client/server applications
- multiple security systems
- multiple locations

Has led to ...

- 2nd order multiple multiple problems
 - multiple userids
 - multiple passwords
 - multiple security repositories
 - multiple security administrators

Which caused ...

- decreased productivity
 - forgotten passwords
 - disabled accounts
- increased security risks
 - post-its on the monitor
 - security features disabled because they're too hard to administer
- increased costs
 - end-user downtime
 - labor intensive administration

Aggravated by ...

- change, change, and more change
 - business reorganizations
 - changing job roles
 - employee turnover
 - company growth
 - business re-engineering
 - new application roll-out



Single Point Security

- the problem
- **requirements for a solution**
- the security spectrum
- Single Point Security function set

Business Requirements

“Until we can focus our IT activities on business processes, management of the enterprise will continue to be expensive and complicated for companies like Smith Barney. We require a consistent view of the entire organization ...”

– Mel Taub, Sr Executive VP, Smith Barney

Translating Business Requirements to Technical Requirements

- mapping business processes onto IT configuration is labor-intensive and error prone
therefore
- the keys to effective configuration are
 - automation
 - raising the level of abstraction

Security Functional Requirements

- provide industry-leading security products and services to allow customers to implement an effective security environment
 - consistent with their requirements
 - satisfactory to their auditors

Supporting Requirements

- **scalable solution**
- flexibility
 - easy to customize
 - policy driven
- extensible
 - easy to include new managed platforms
 - administrator-defined policy actions

Scalable Solution

- enterprise capable
 - coherent enterprise view from single point
 - delegation to local administrators
 - delegation to *non-IT* personnel
- tractable at department level
 - small environments must be manageable without overwhelming complexity
 - every enterprise roll-out starts at the departmental level

Supporting Requirements

- scalable solution
- flexibility
 - easy to customize
 - **policy driven**
- extensible
 - easy to include new managed platforms
 - **administrator-defined policy actions**

Policy-related requirements

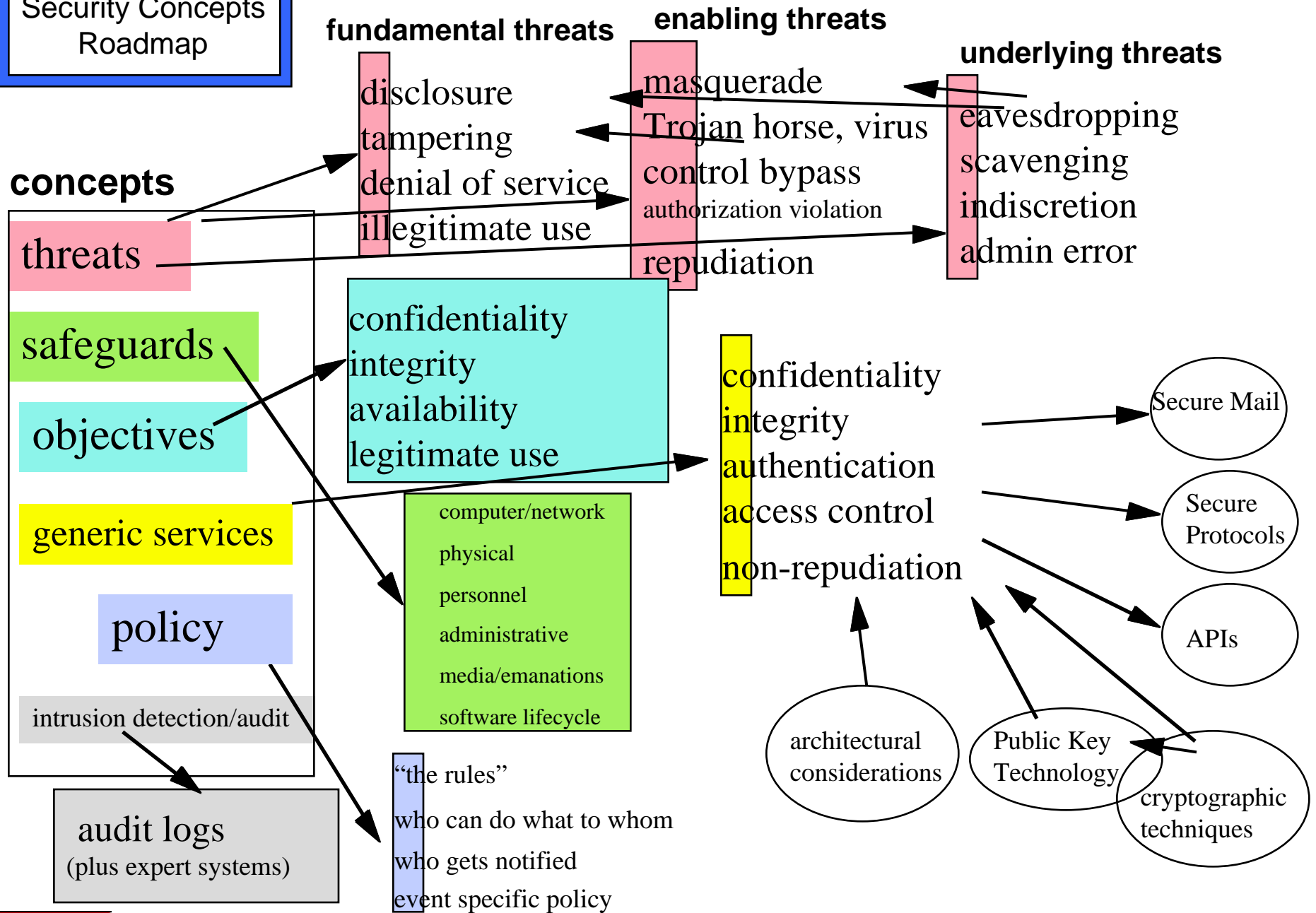
- define how and where security policies are applied and enforced
- provide the means for the convenient expression of such policies
- provide the underlying mechanisms that carry out such policies
- provide best-practices default policies bundled with delivered product



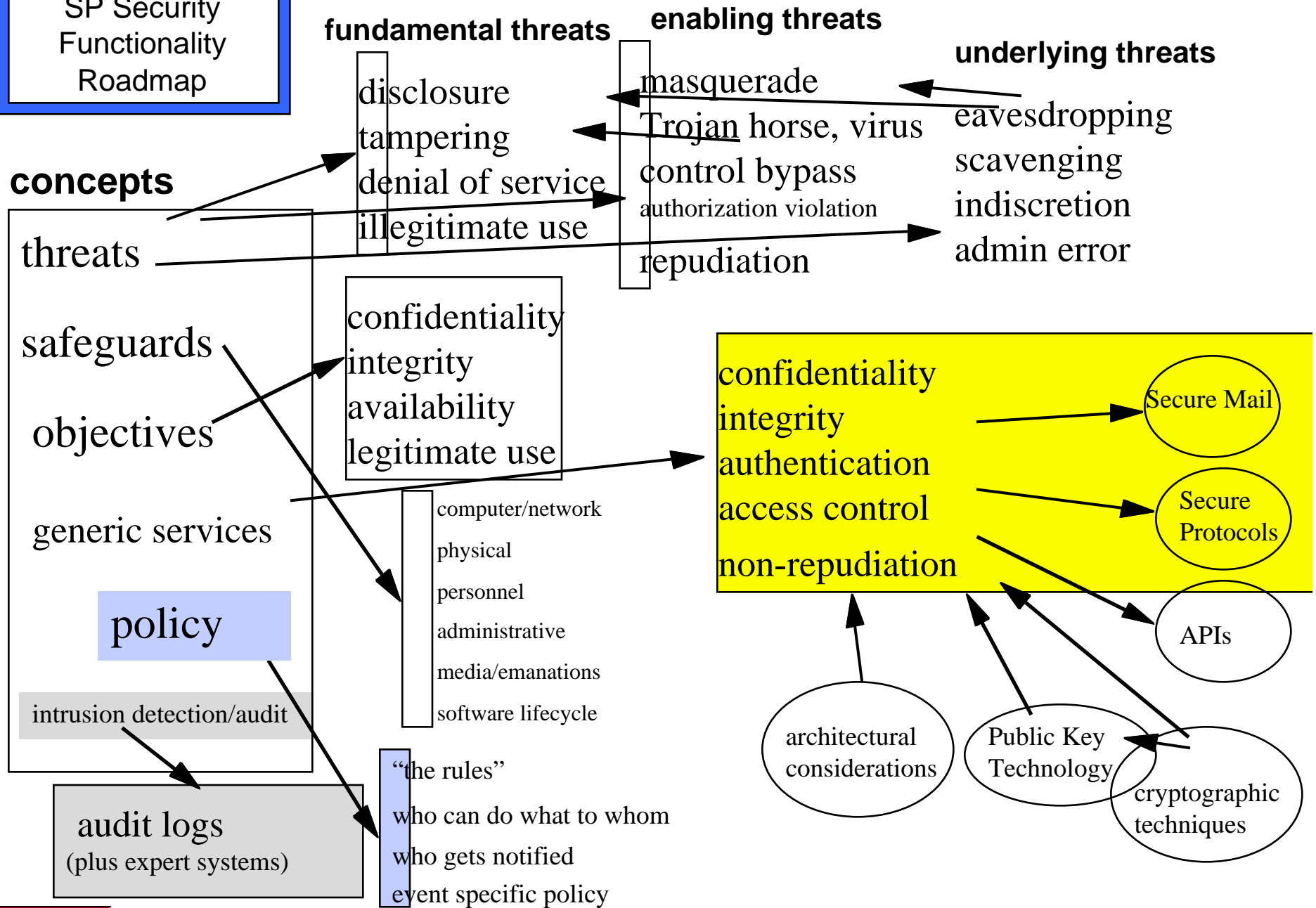
Single Point Security

- the problem
- requirements for a solution
- **the security spectrum**
- Single Point Security function set

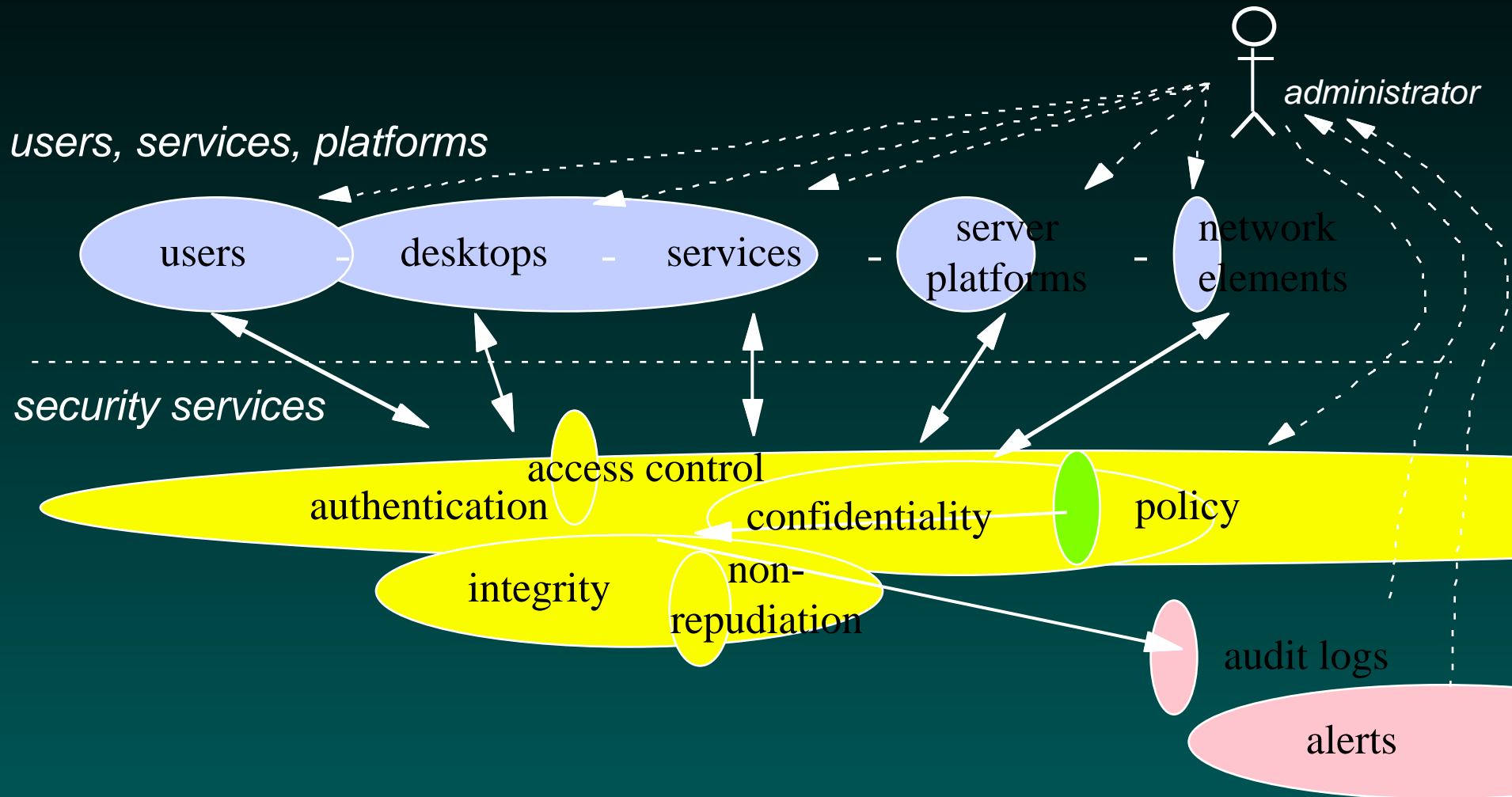
Security Concepts Roadmap



**SP Security
Functionality
Roadmap**



Security-related administration

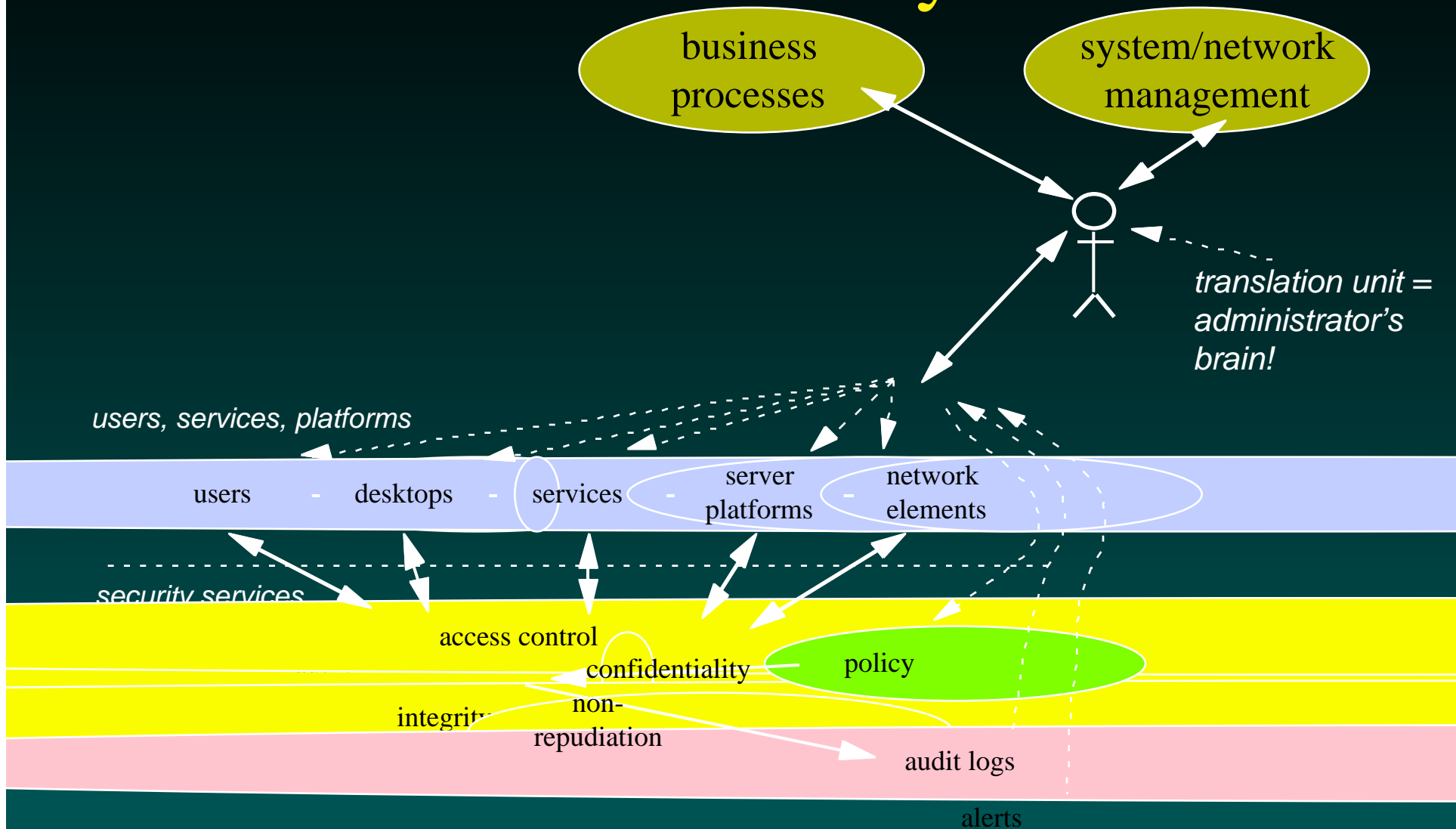




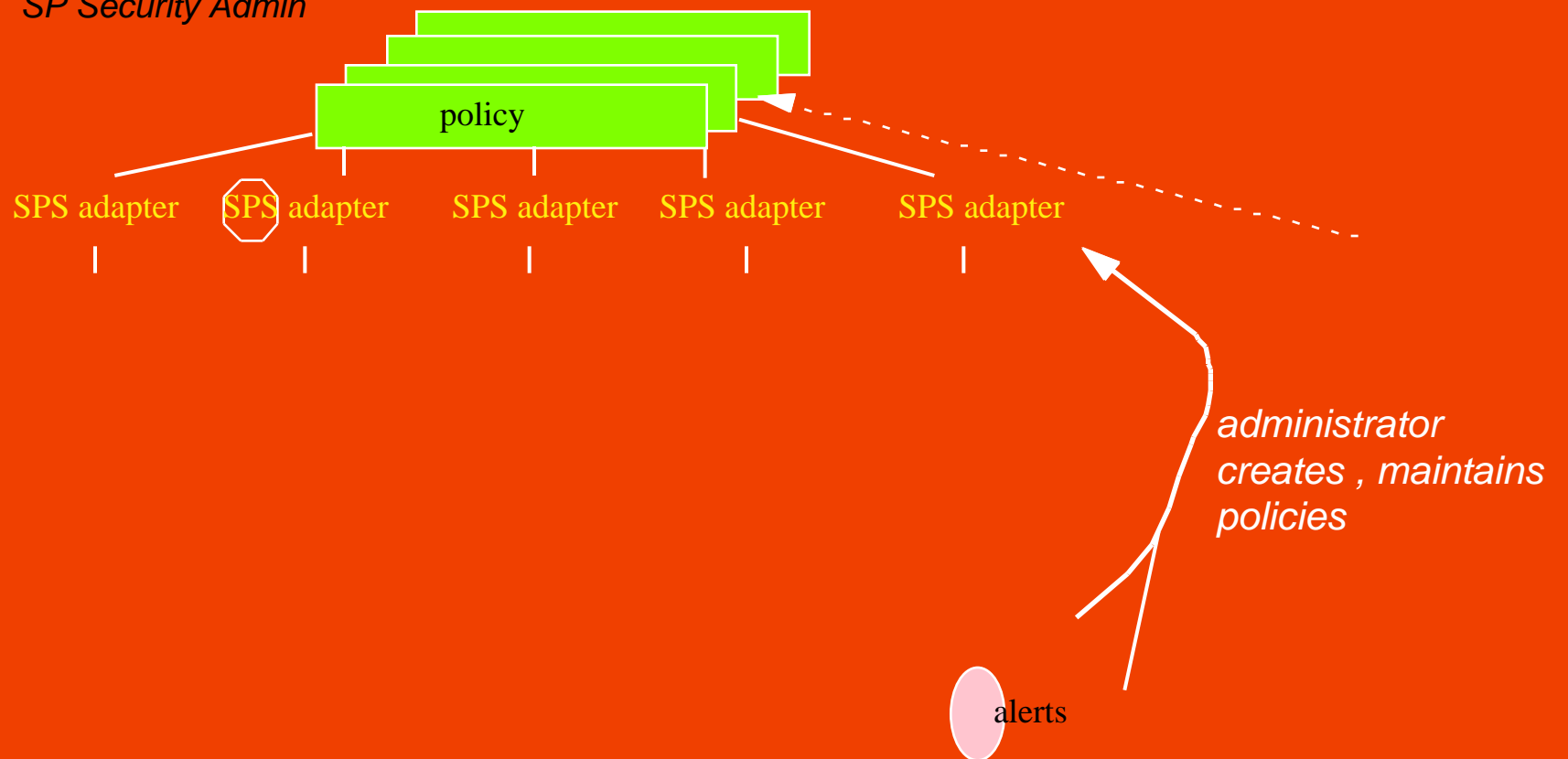
Single Point Security

- the problem
- requirements for a solution
- the security spectrum
- **Single Point Security function set**

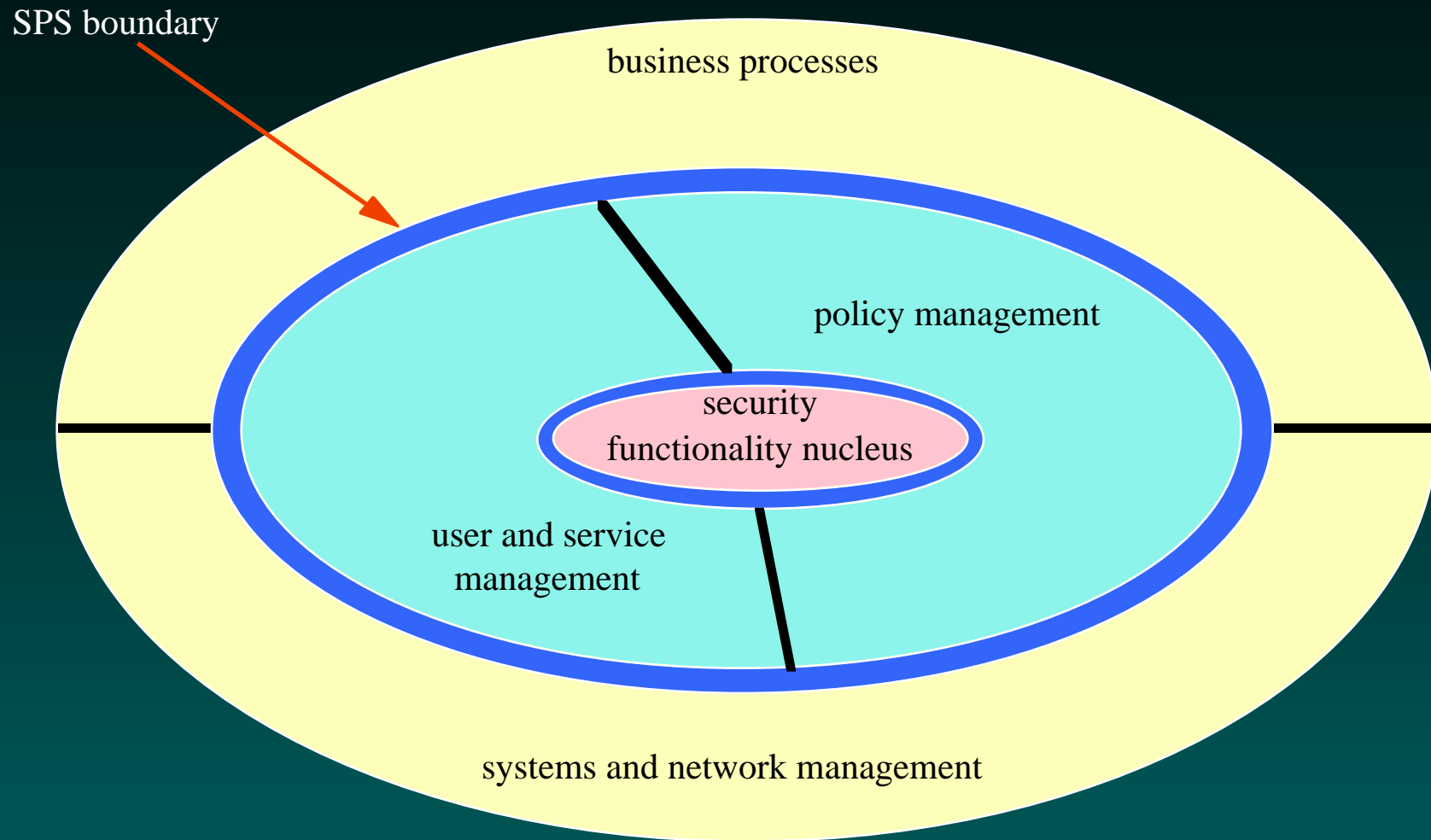
Security-related administration - the hard way



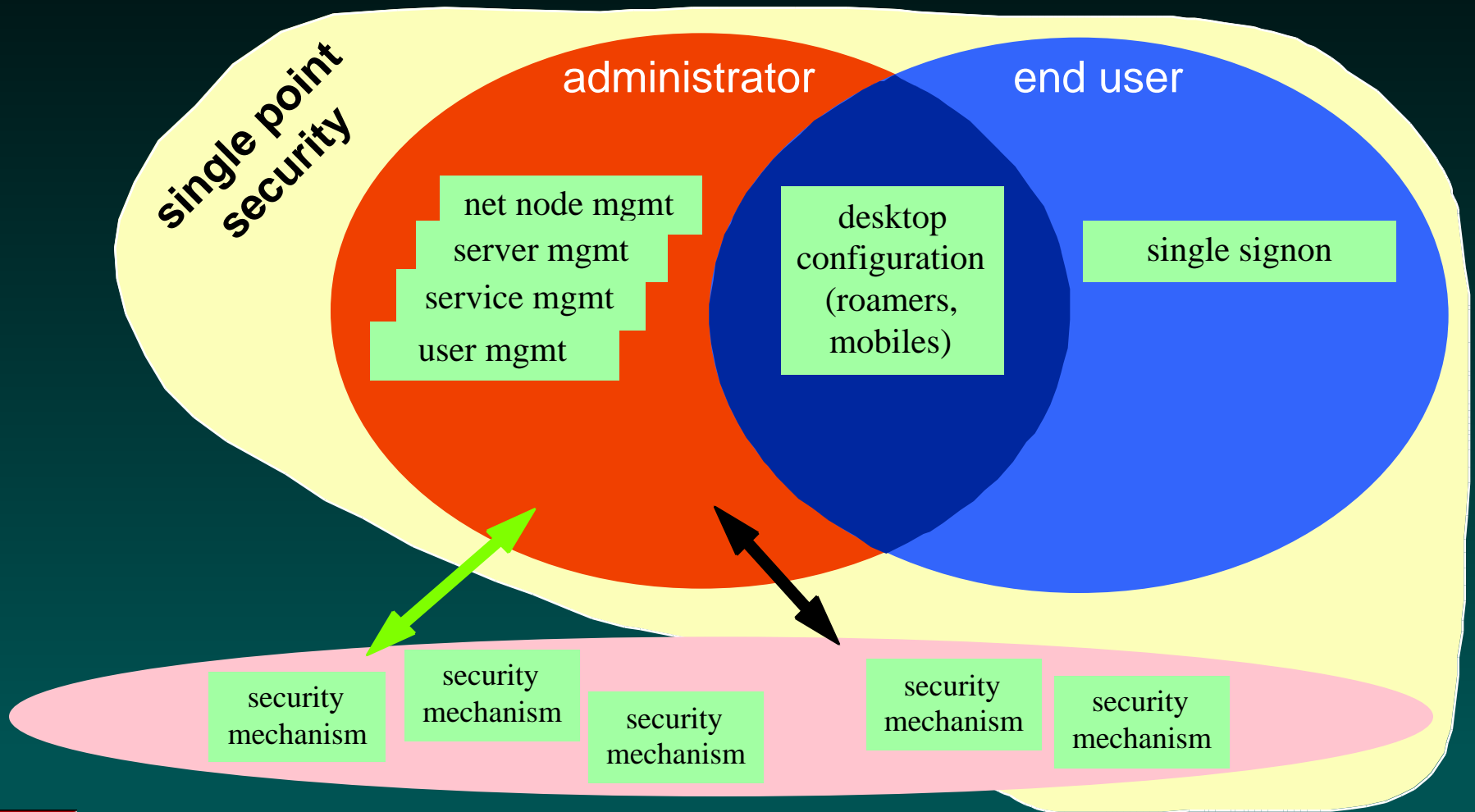
SP Security Admin



Concentric bands of administration abstraction (through exposed interfaces)



Single Point Security Functionality



SPS Function Set

- SPS is *primarily* about effective and powerful security *administration*
 - of heterogeneous security mechanisms
 - OS-embedded
 - third party
 - Unisys-supplied
- SPS supplies security mechanisms
 - where suitable ones may not otherwise exist
 - where adaptation is required for cohesive product integration
 - where there's a business opportunity for Unisys

Why this set of functions?

- administration
 - facilitate *accuracy of configuration* in the multiple-multiple situation
 - security depends on accuracy of configuration
 - difficult administration encourages turning off security features
 - user management
 - central to security administration
 - long-lived value

Why this set of functions?

- desktop configuration
 - a natural adjunct to user management
 - manage users implies manage their desktops
 - “roaming” capability required in some environments
 - one user can use many different PCs
 - user-specific environment comes to user regardless of which PC he uses
 - “mobile” capability
 - one user with one machine connecting from various points on the network

Why this set of functions?

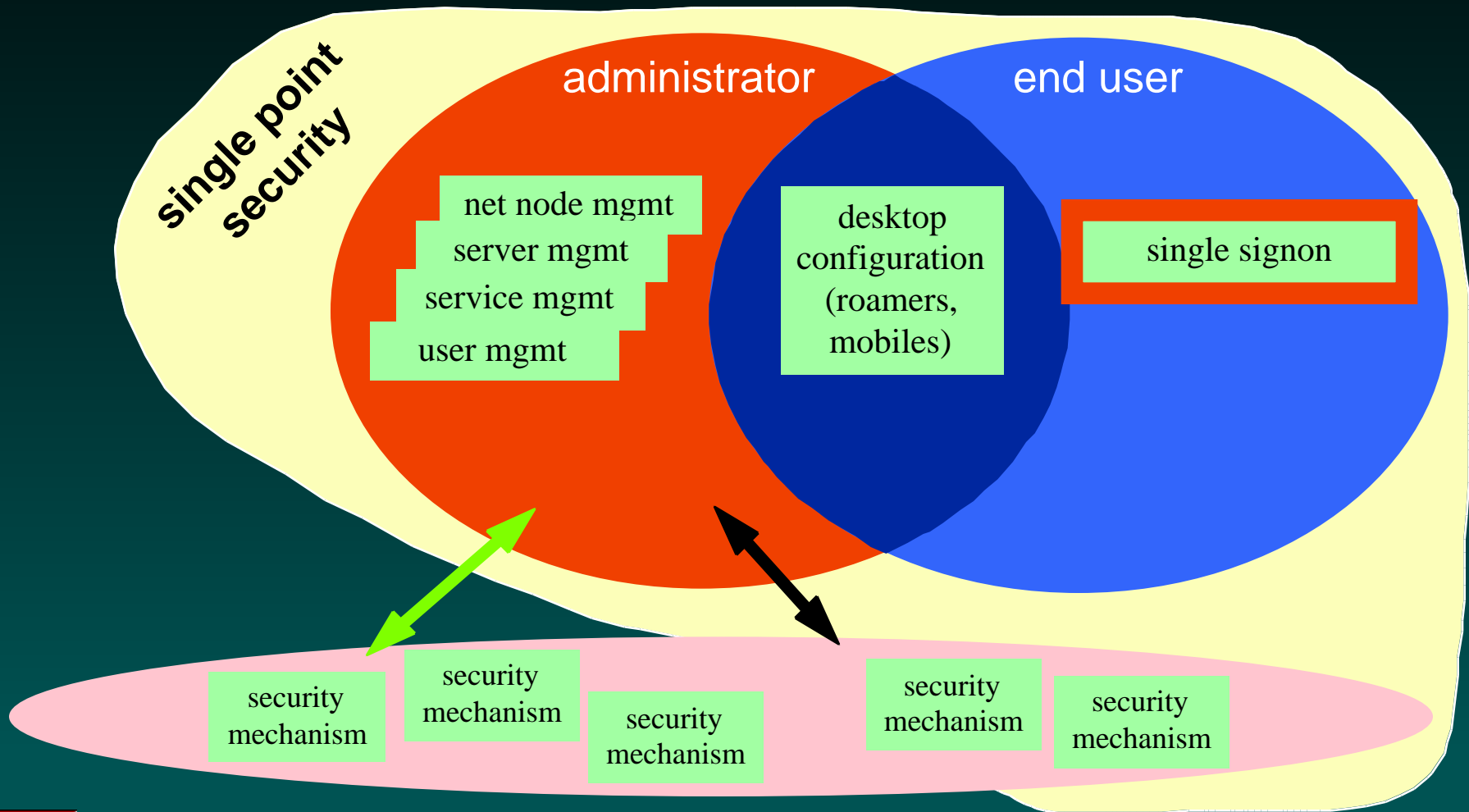
- single sign-on
 - urgently required in legacy environments
 - will be years before application environments get re-engineered around GSS mechanisms
 - no widespread agreement that GSS is the way to go
 - GSS alternatives immature
 - therefore single sign-on will require mixture of legacy and GSS-style techniques for foreseeable future

Why this set of functions?

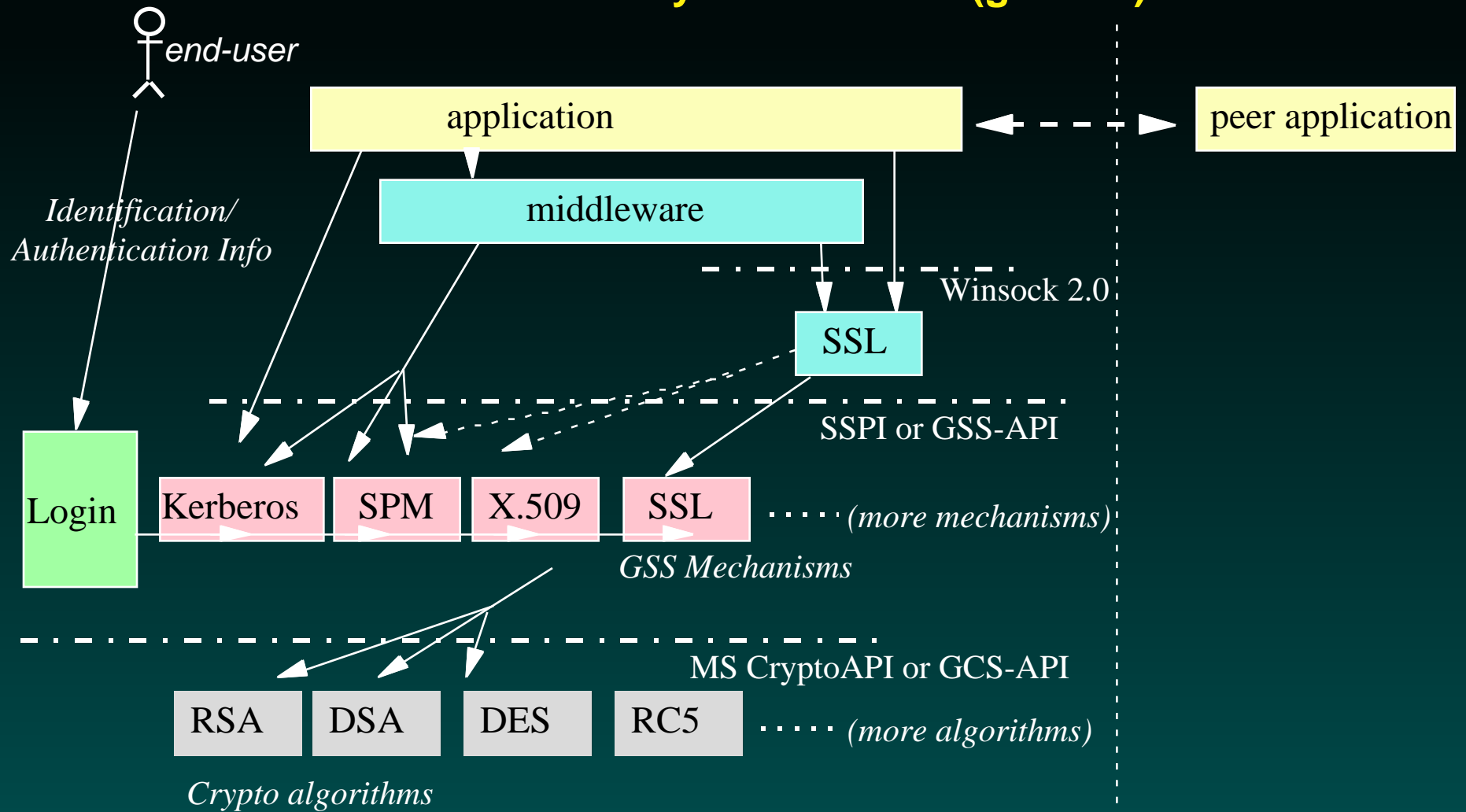
- security mechanisms
 - where suitable ones may not otherwise exist
 - where adaptation is required for cohesive product integration
 - where there's a business opportunity for Unisys



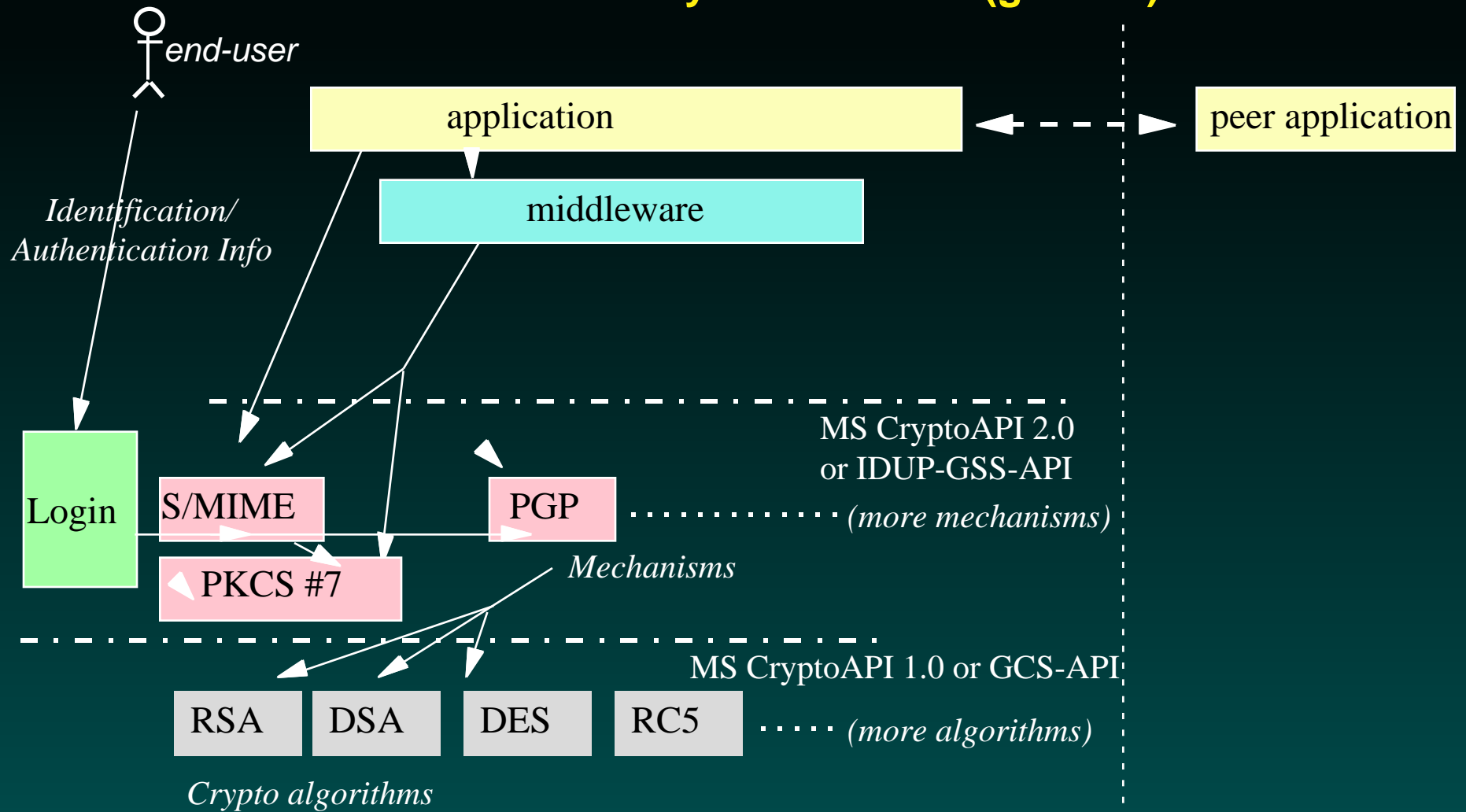
Single Point Security Functionality



Session-oriented security environment (generic)



Store-and-forward security environment (generic)



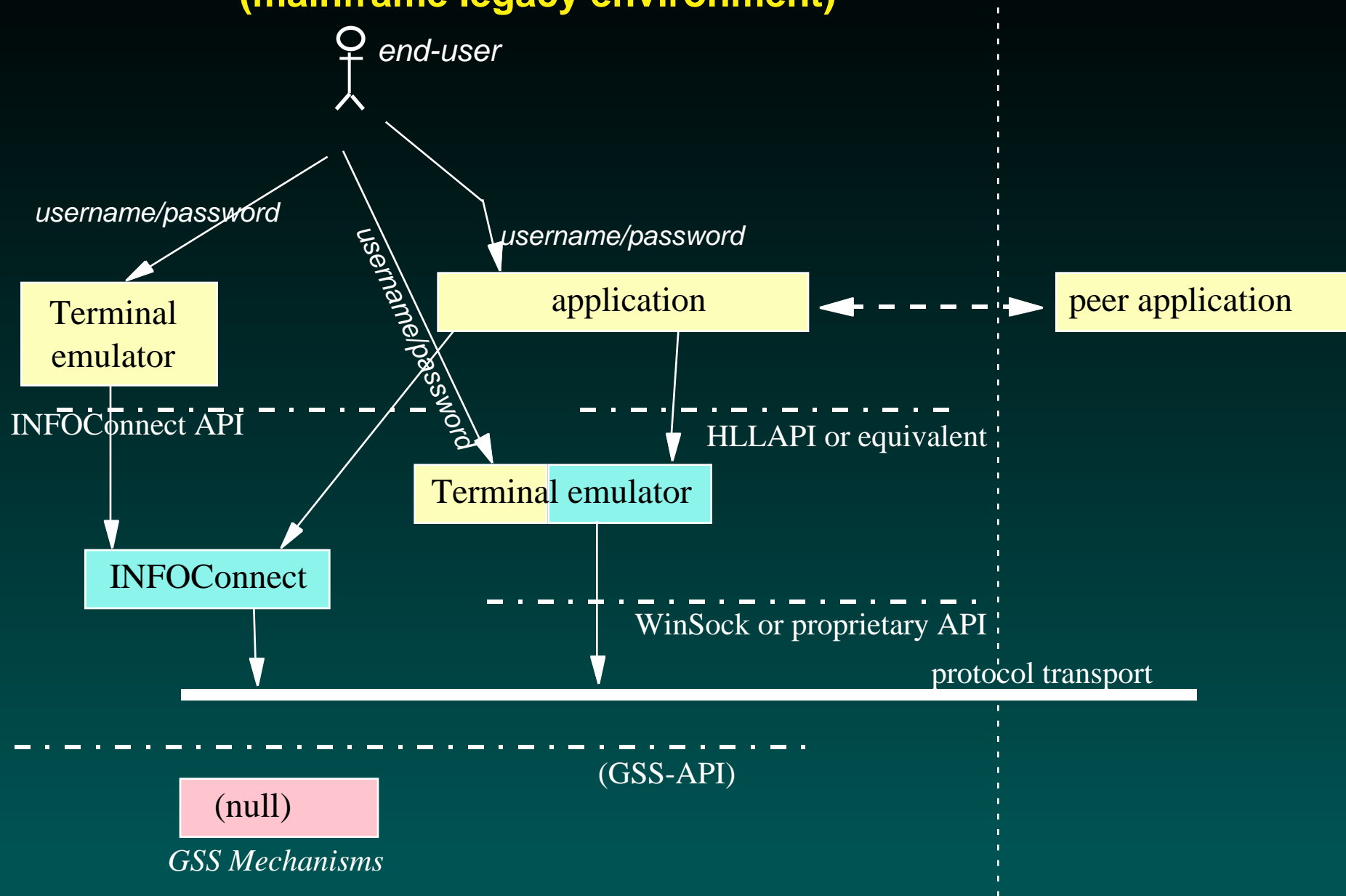
Single Signon Evolution

- “end game” (Utopia) is a state where:
 - multiple GSS mechanisms provide
 - single sign-on (authentication)
 - encryption and integrity

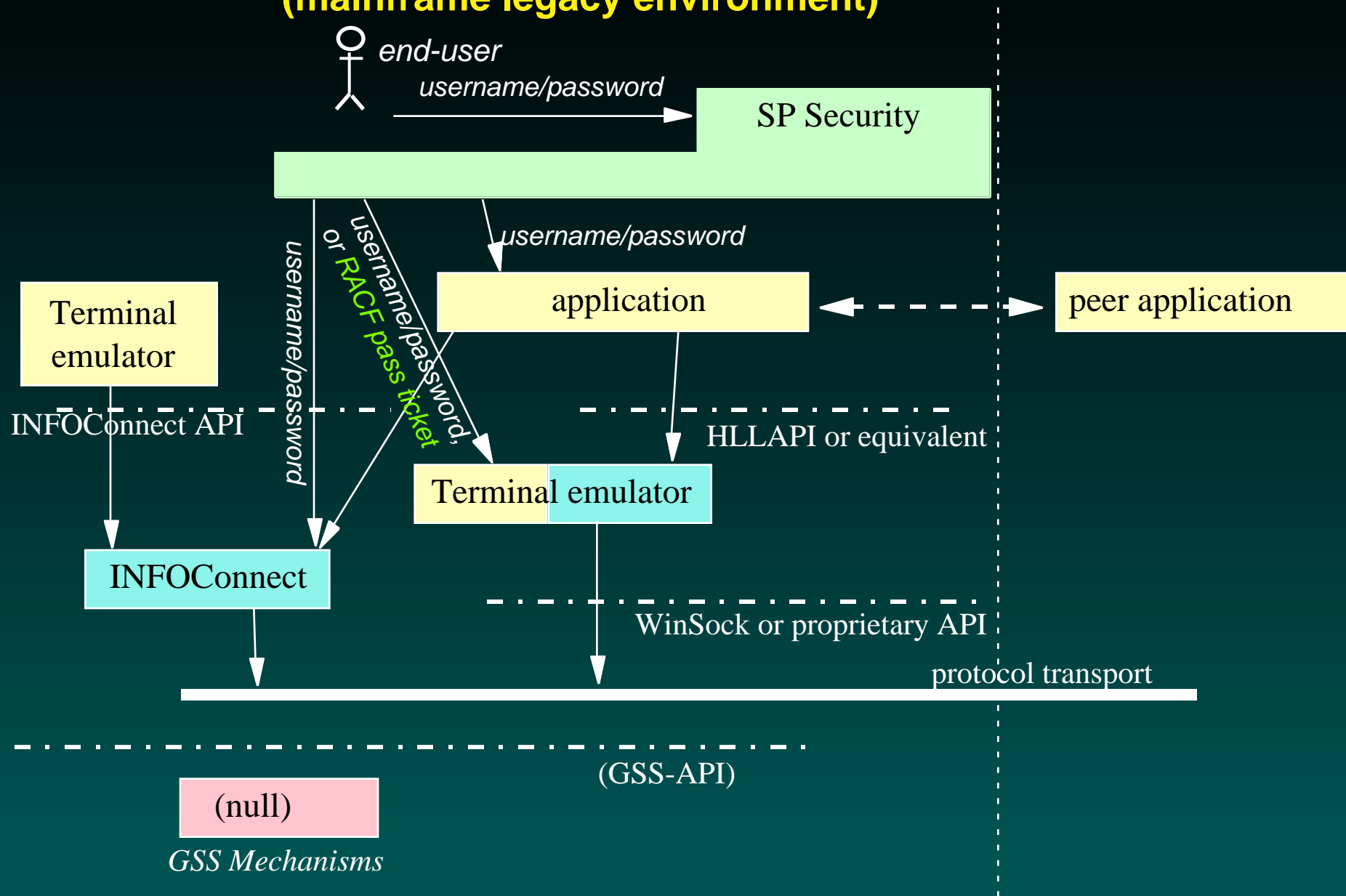
Single Signon Evolution

- “middle game” much more chaotic
 - client/server applications often using ad hoc authentication mechanisms
 - mainframe terminal environments still in use
 - complete with legacy ad hoc authentication methods

Signing on: Session-oriented security environment (mainframe legacy environment)



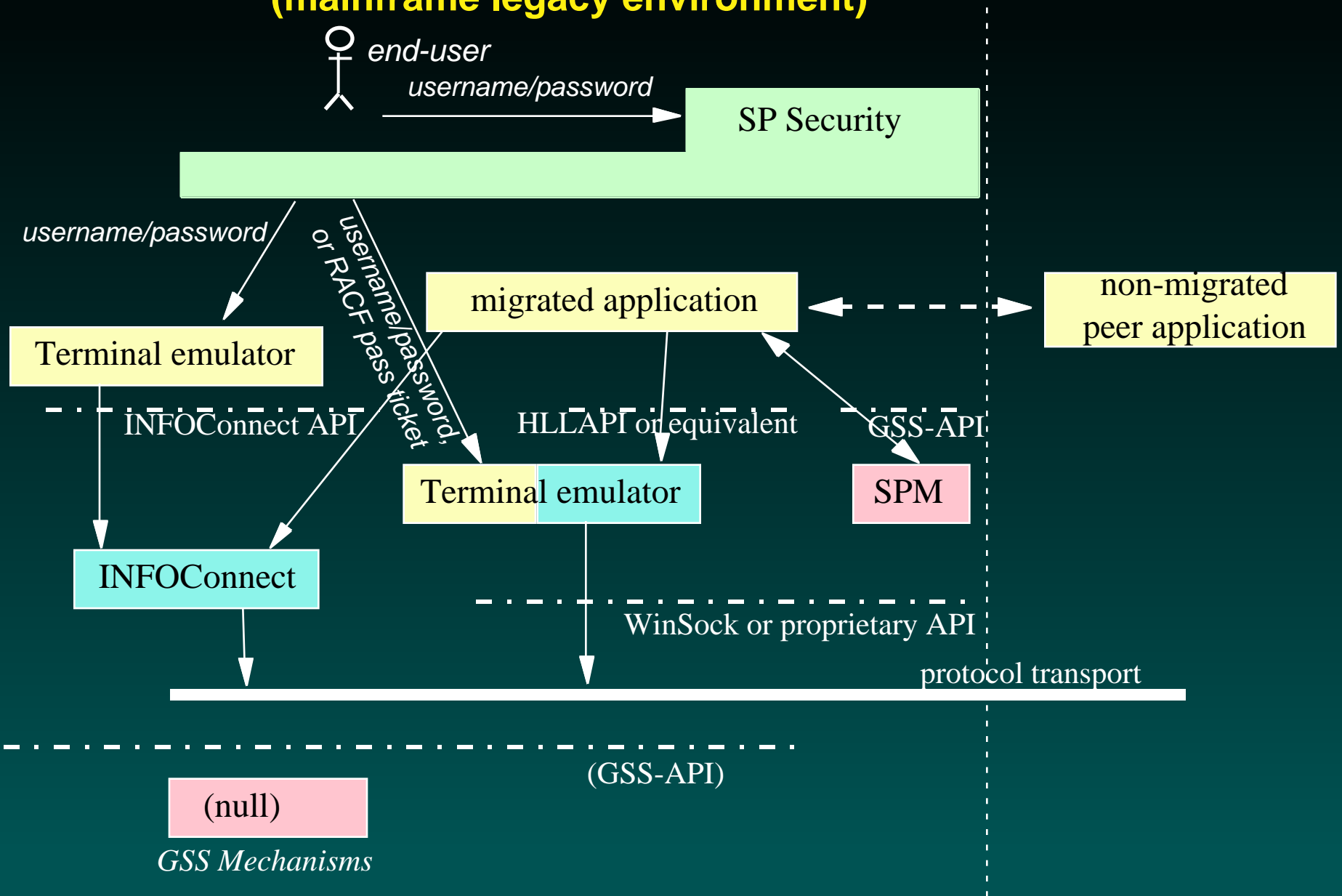
Single SignOn: Session-oriented security environment (mainframe legacy environment)



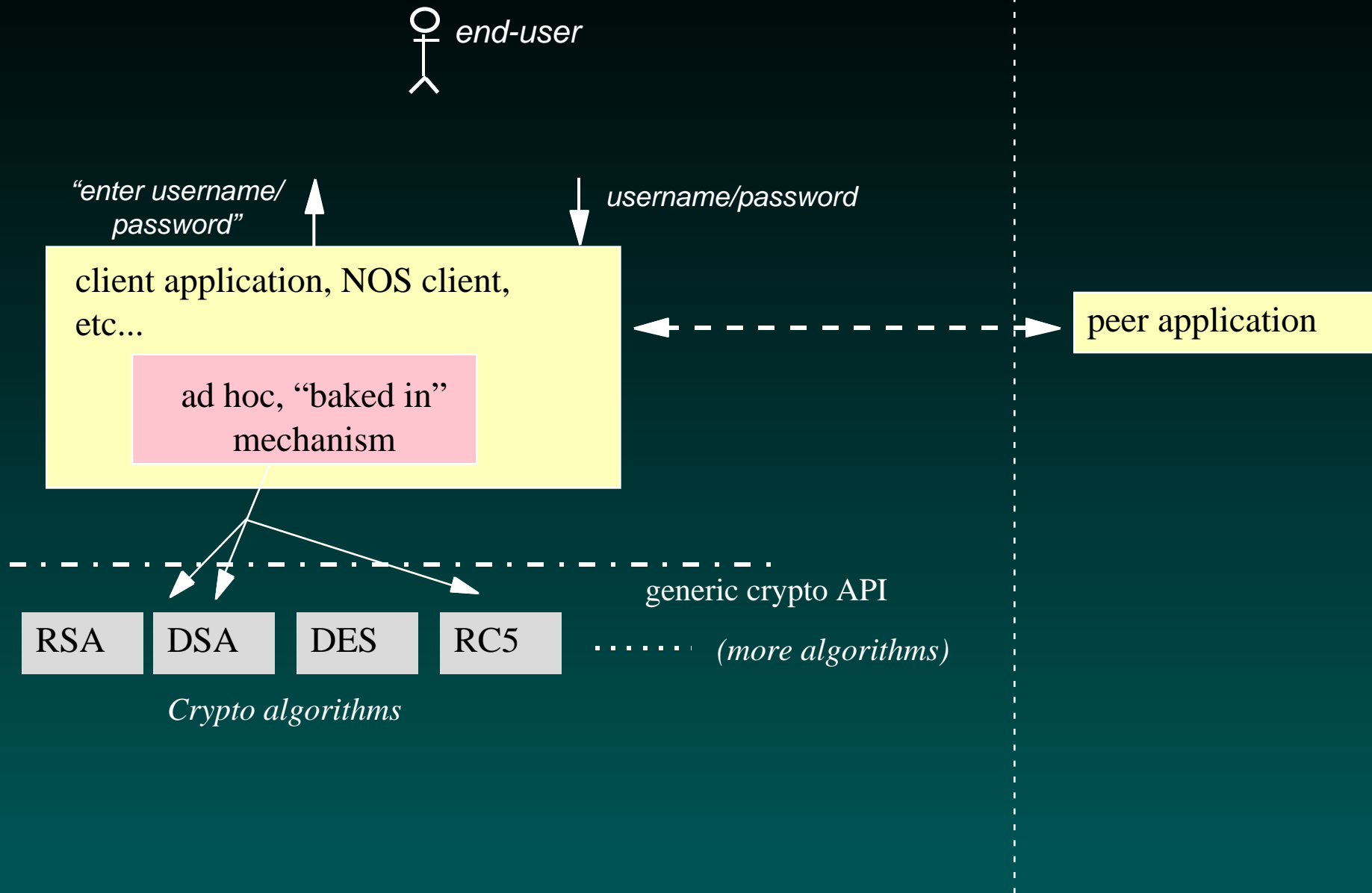
Attributes of mainframe legacy environment

- middleware consists of Terminal Emulator and INFOConnect.
- identification/authentication (usually) not performed on the desktop
 - info gathered from user, sent to server
 - transmitted in the clear
 - validated by server
- each server (or server platform) maintains username/password.

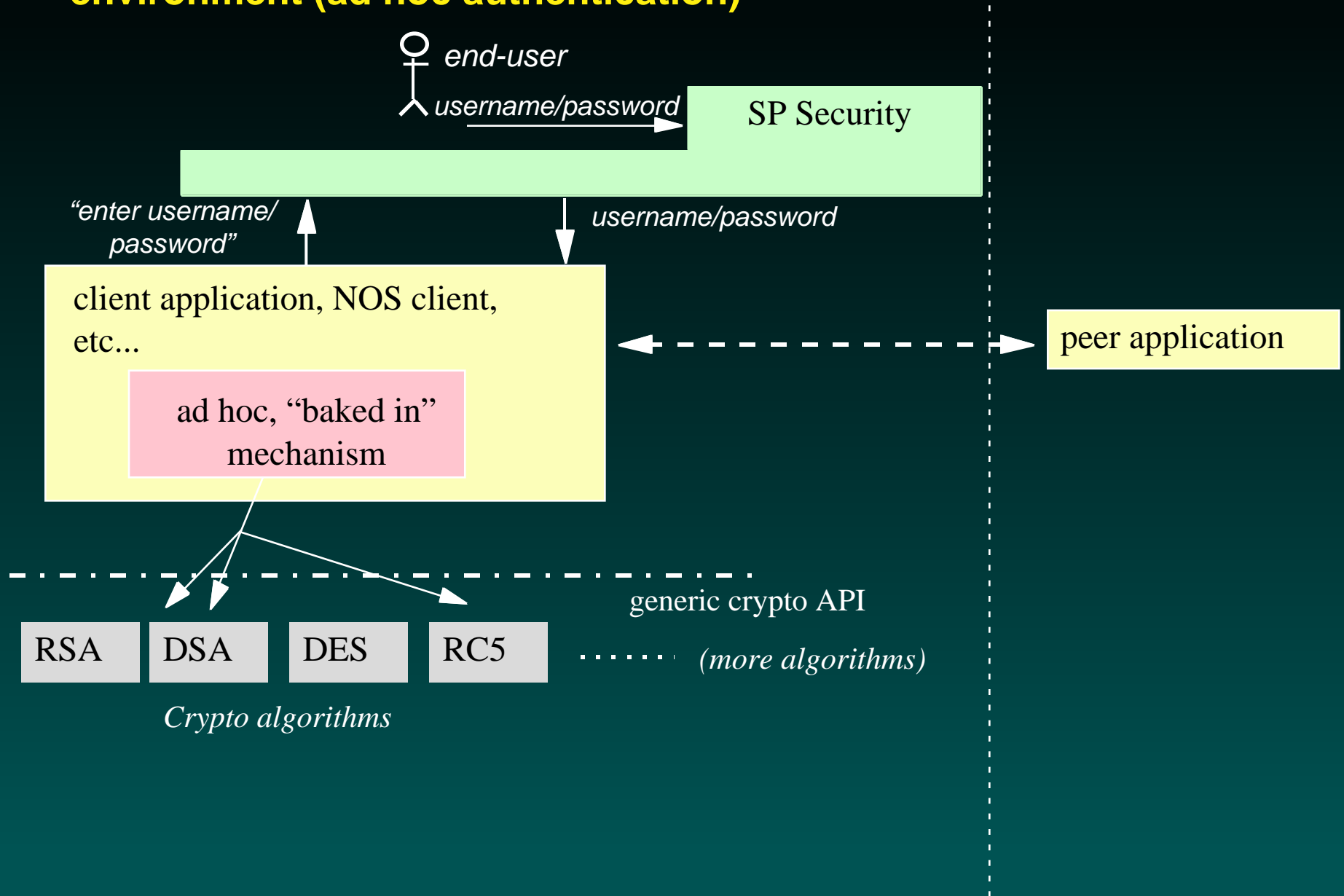
Single SignOn: Session-oriented security environment (mainframe legacy environment)



Signing on: Session-oriented security environment (ad hoc authentication)

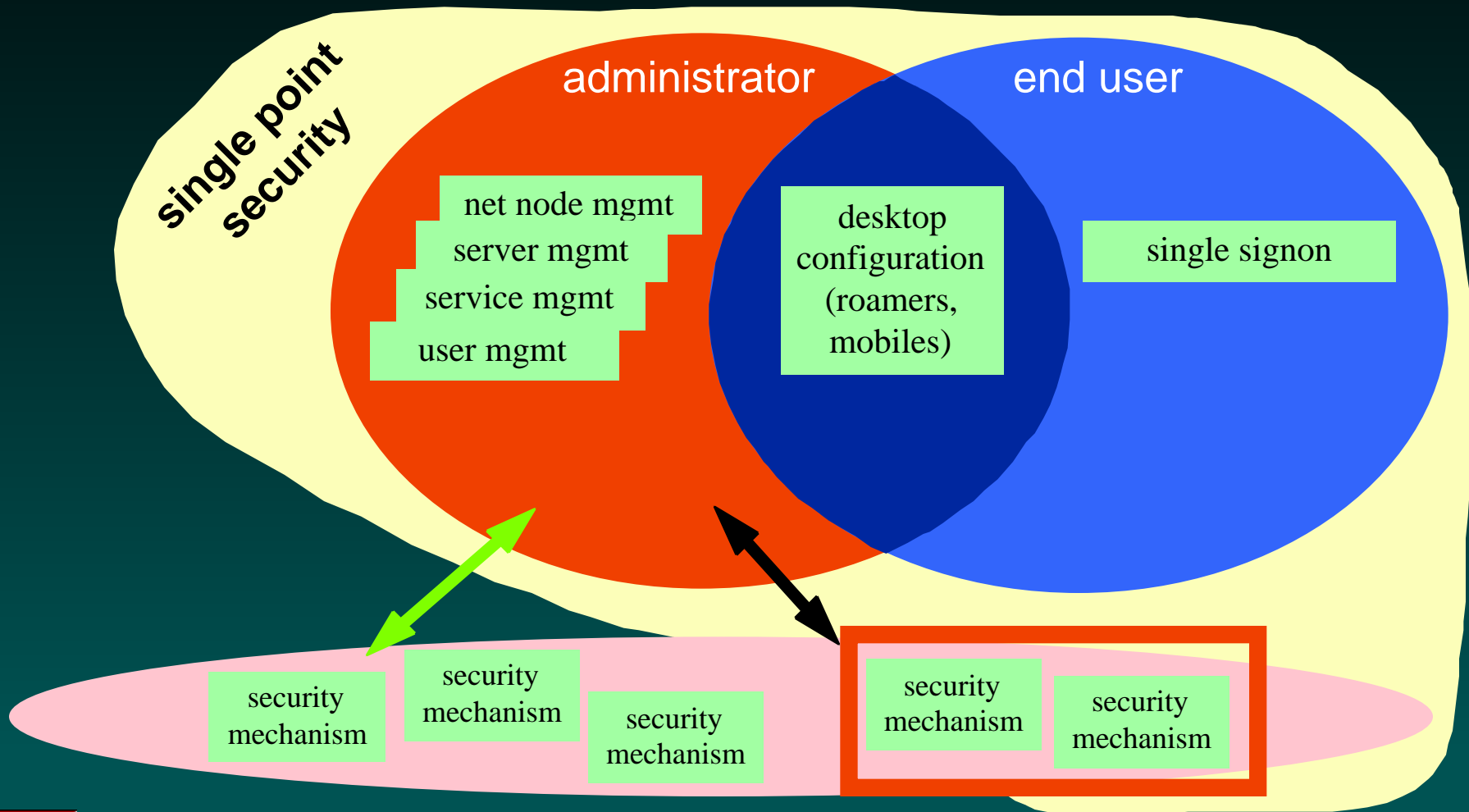


Single SignOn: Session-oriented security environment (ad hoc authentication)





Single Point Security Functionality

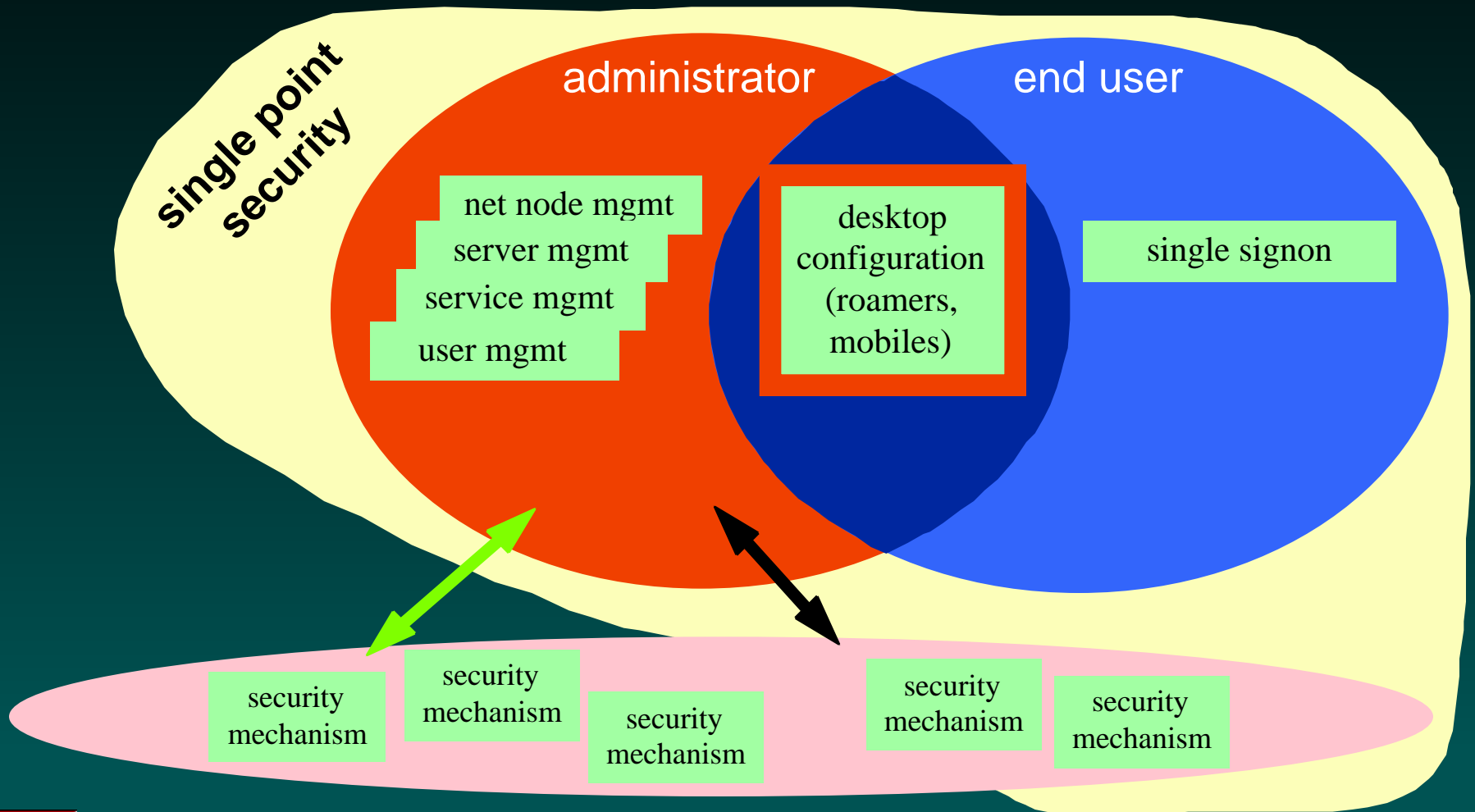


Security Mechanisms

- OS add-ons
 - smart card sign-on
 - Fischer Watchdog
 - access control for DOS, Win 3.x, Win95
 - optional encryption
 - Memco SeOS
- Kerberos
 - Win 3.x, Win95
 - Unisys enterprise servers
- additional mechanisms on enterprise servers



Single Point Security Functionality

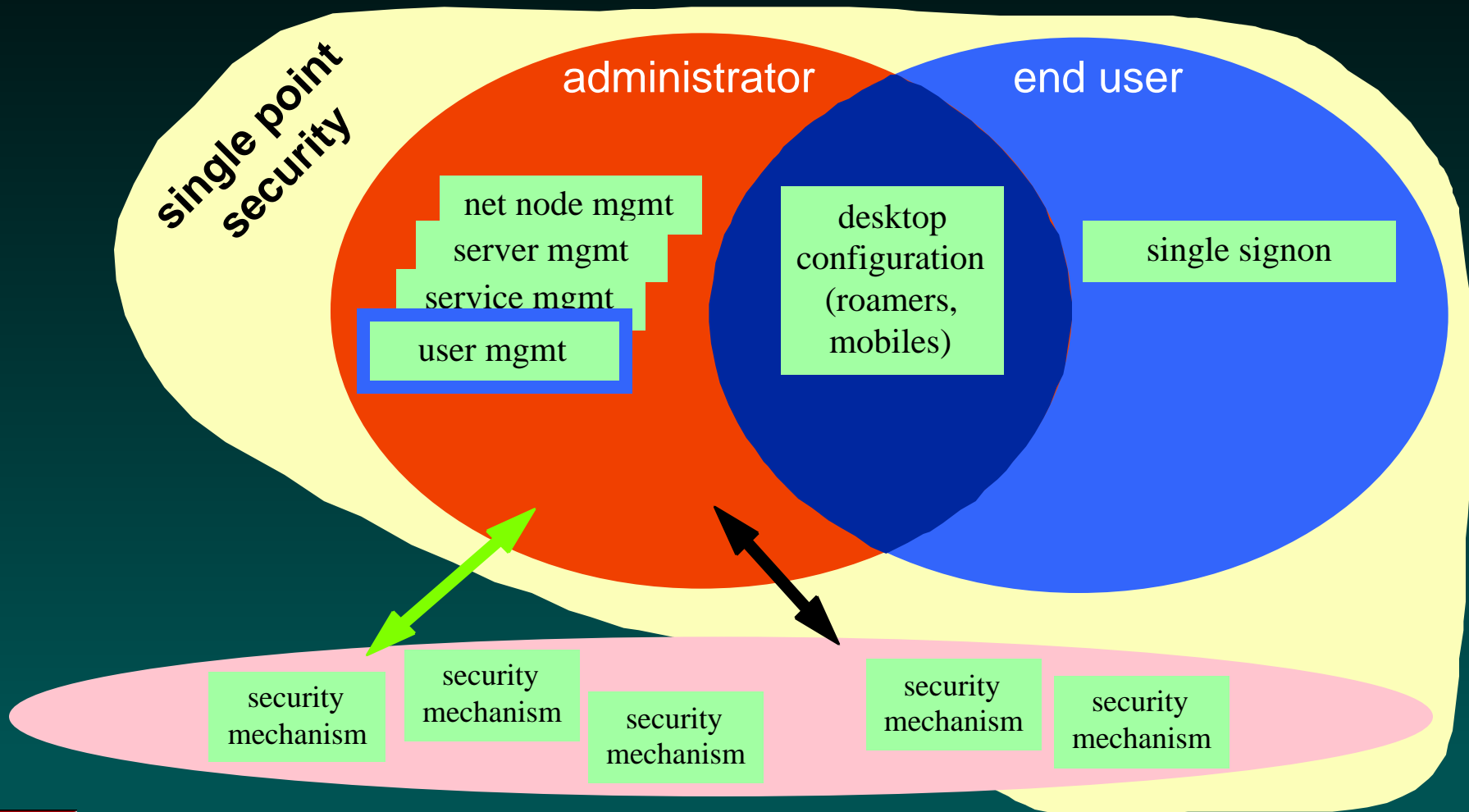


Desktop Configuration

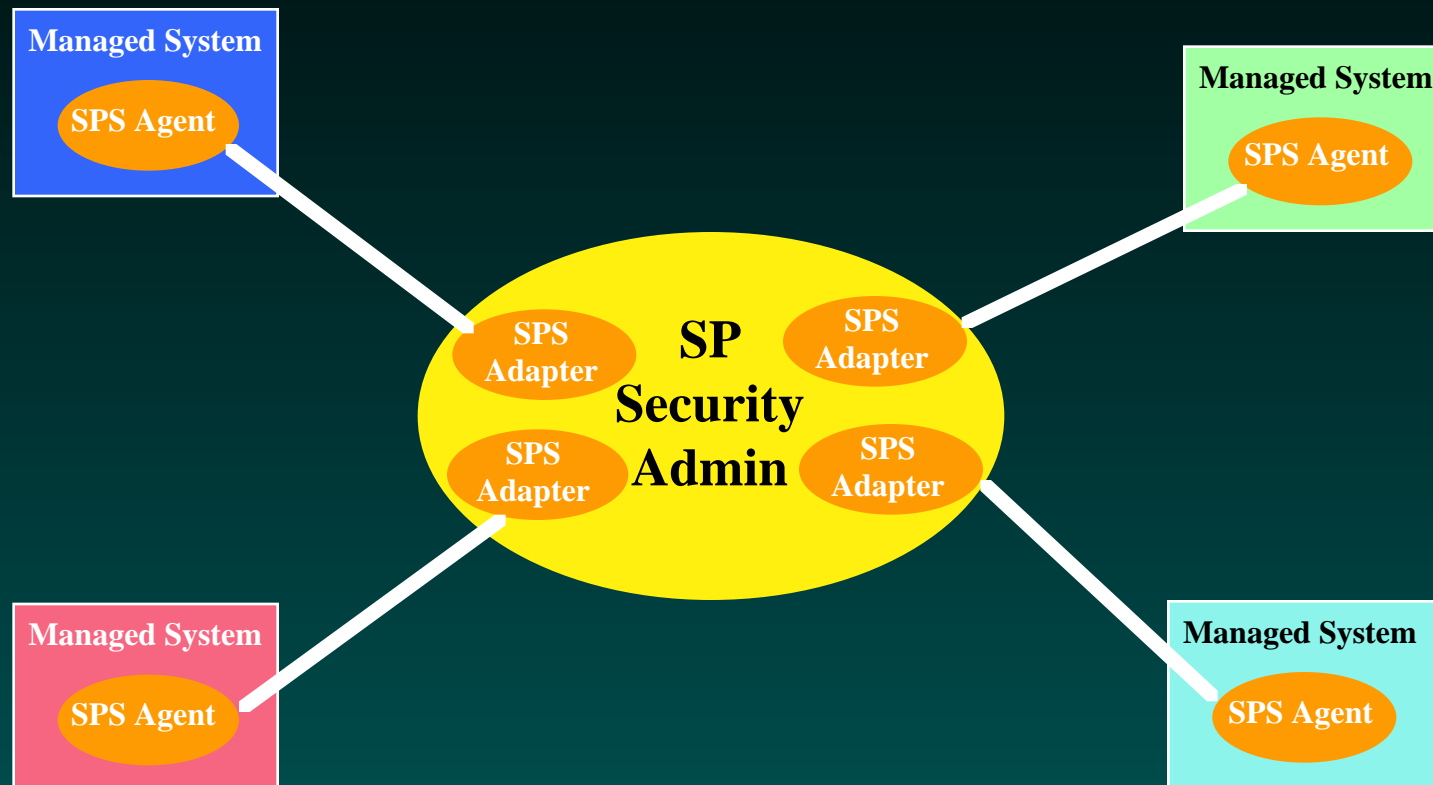
- user's desktop configured to his profile
 - a form of access control (optional)
 - user only sees authorized services
- software distribution
 - generate scripts for Microsoft SMS



Single Point Security Functionality



SPS User Management

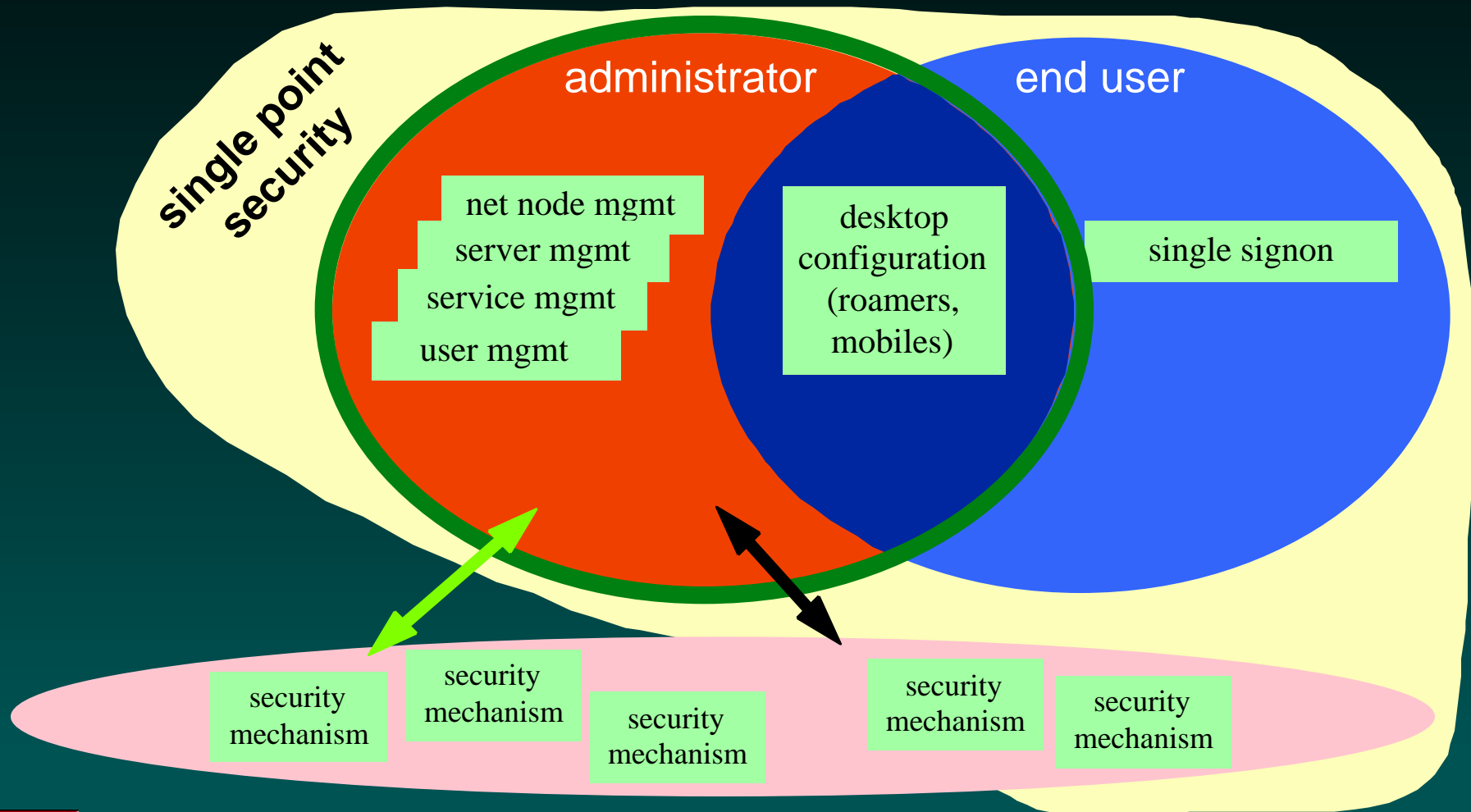


Managed System Examples

- operating systems
 - mainframes
 - file servers
- groupware
- databases
- vertical applications
- etc...



Single Point Security Functionality



SPS Administration

- requirements:
 - enterprise scale solution
 - easy to administer
 - flexible - easy to customize
 - extensible - easy to include new managed platforms



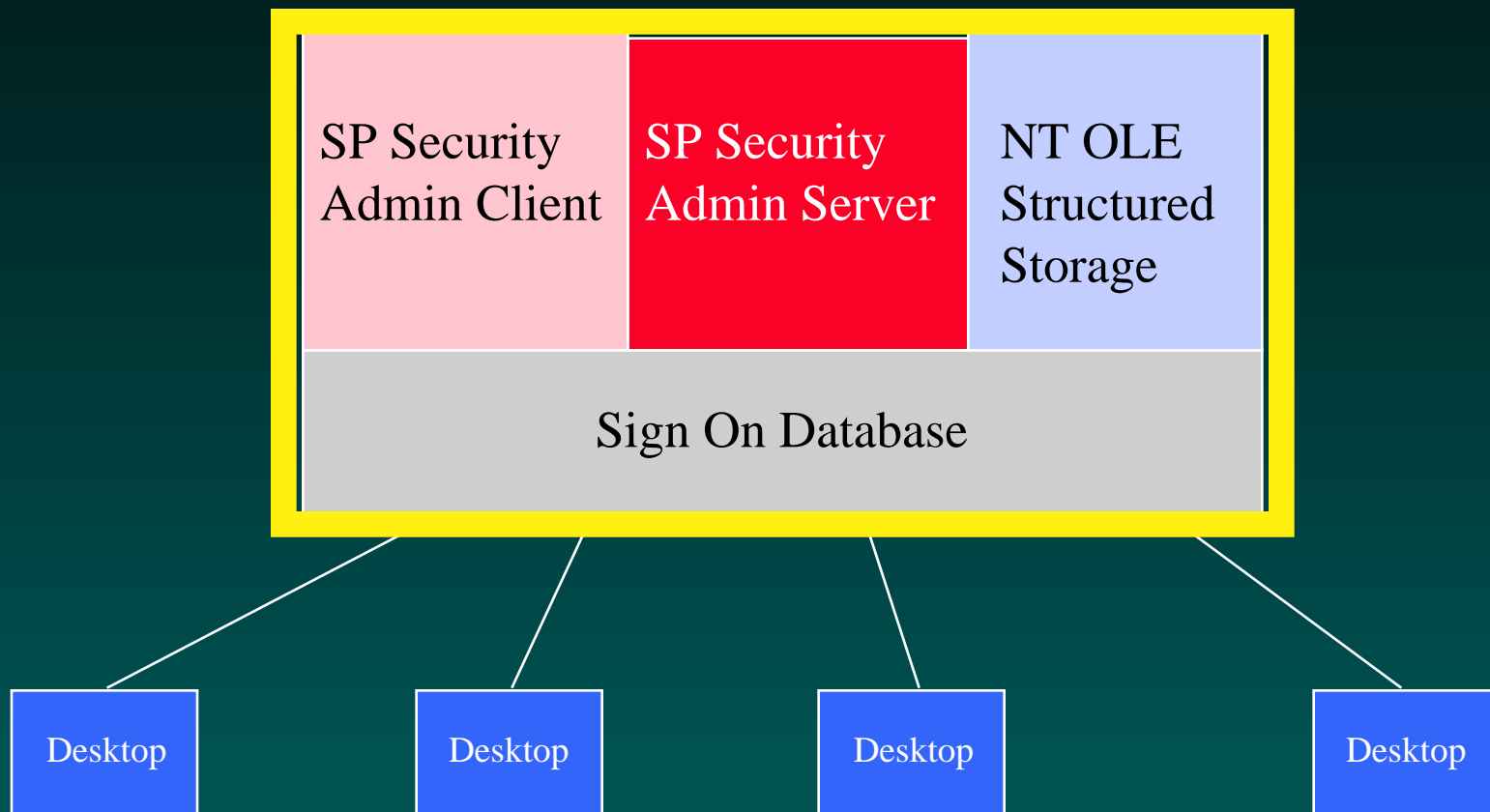
SPS Administration

- requirements:
 - **enterprise scale solution**
 - easy to administer
 - flexible - easy to customize
 - extensible - easy to include new managed platforms

SP Security Administration

Departmental Version

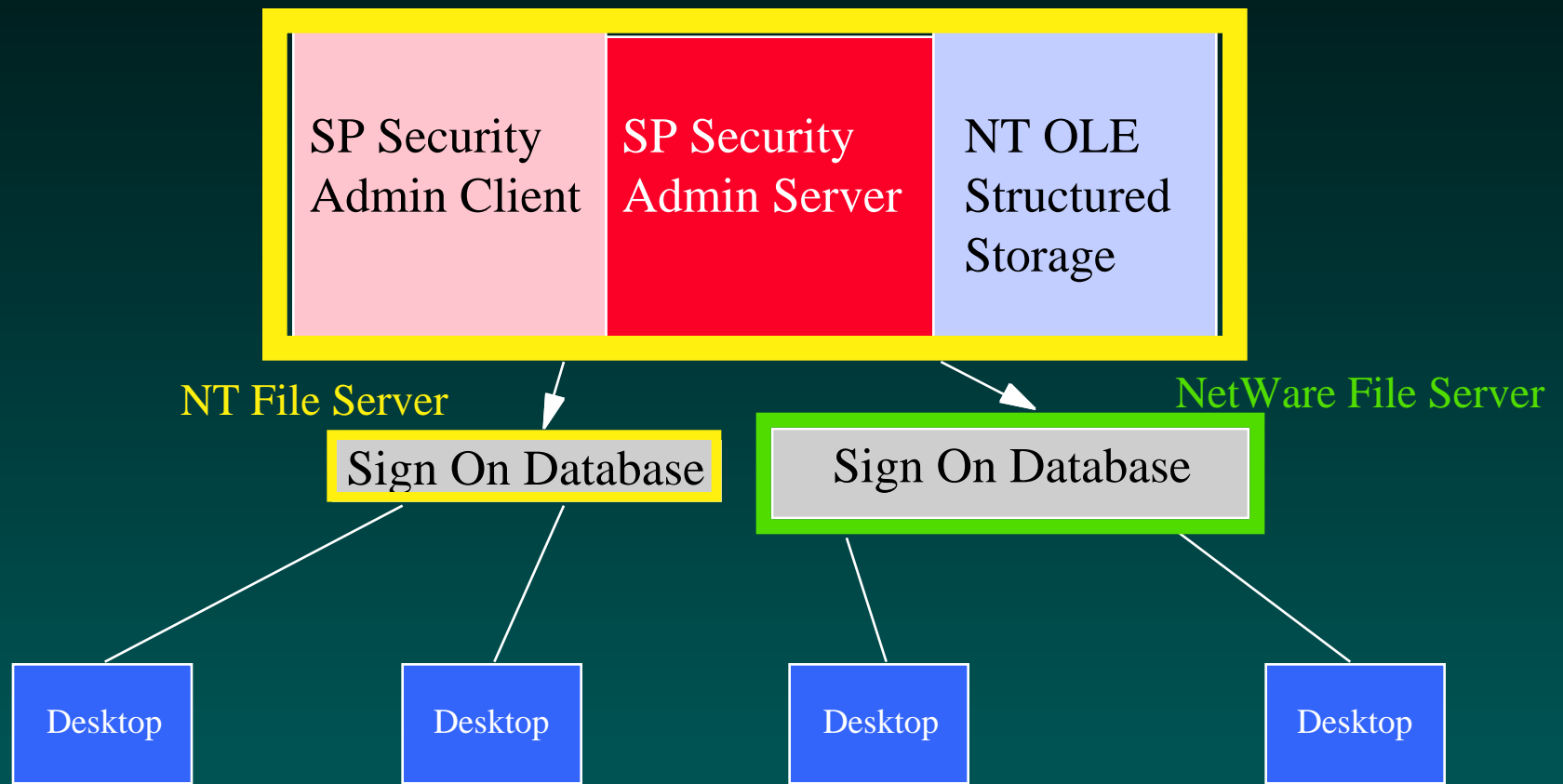
NT 4.0 Server



SP Security Administration

Departmental Version

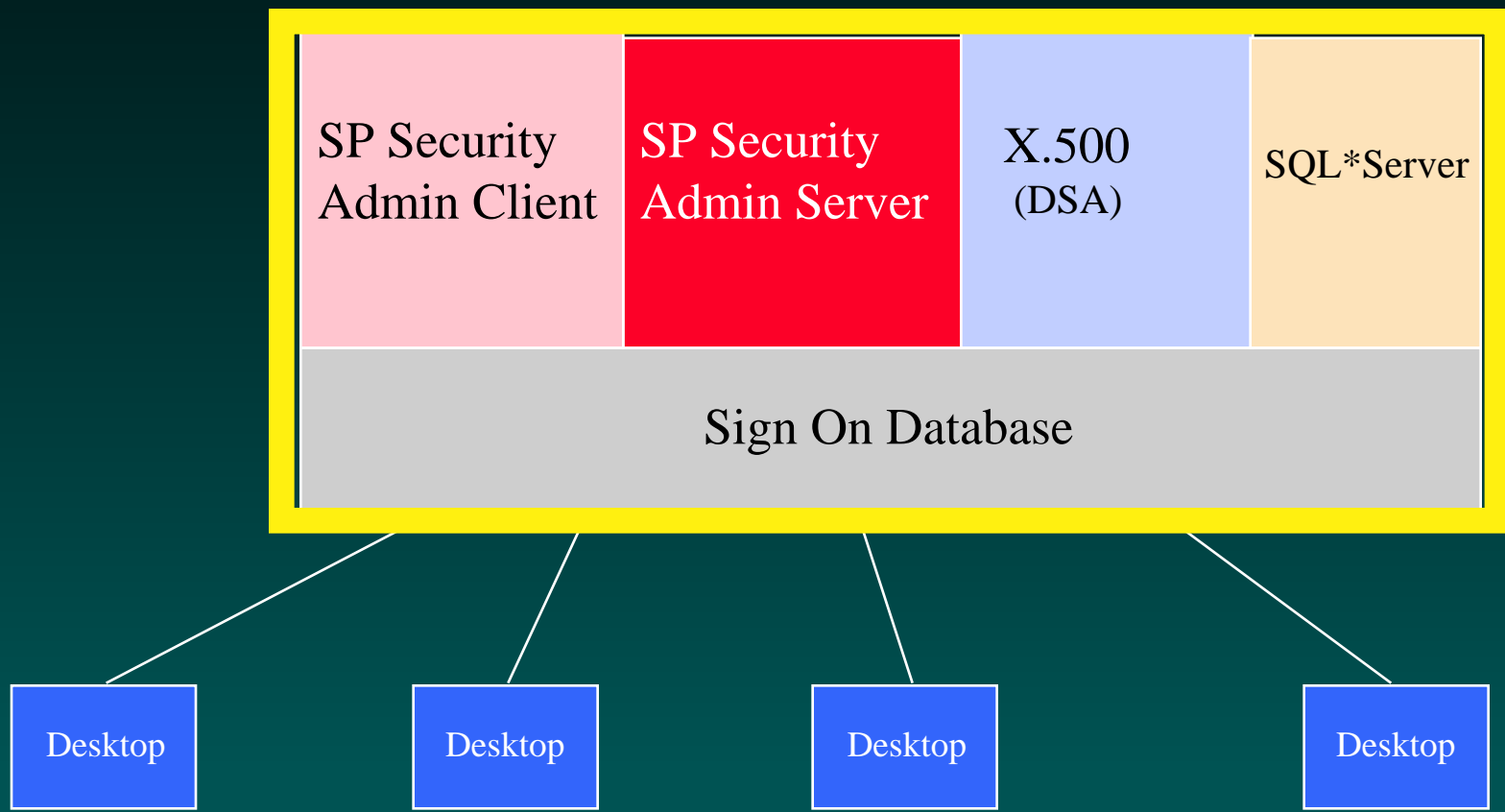
NT 4.0 Server



SP Security Administration

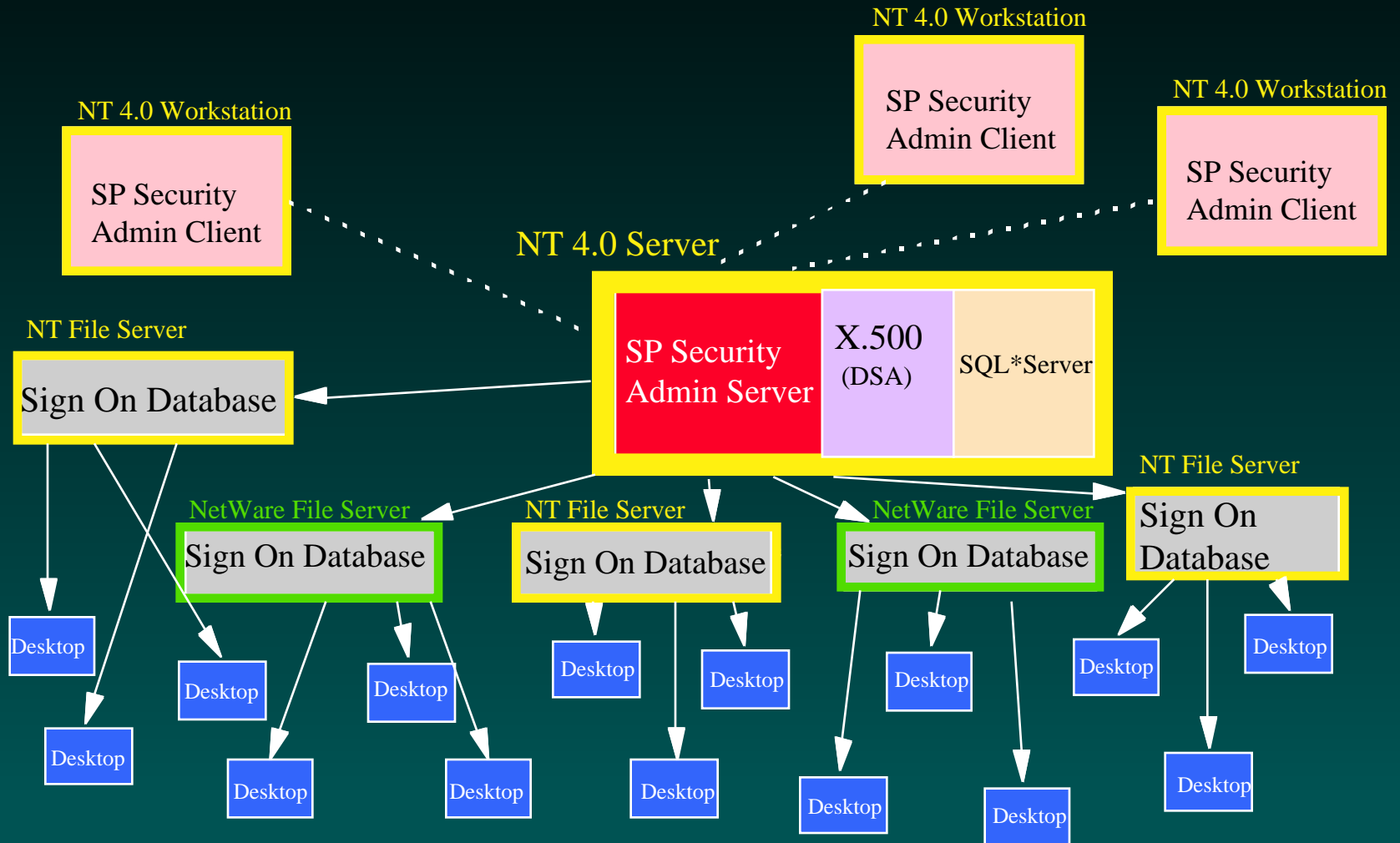
Enterprise Version

NT 4.0 Server



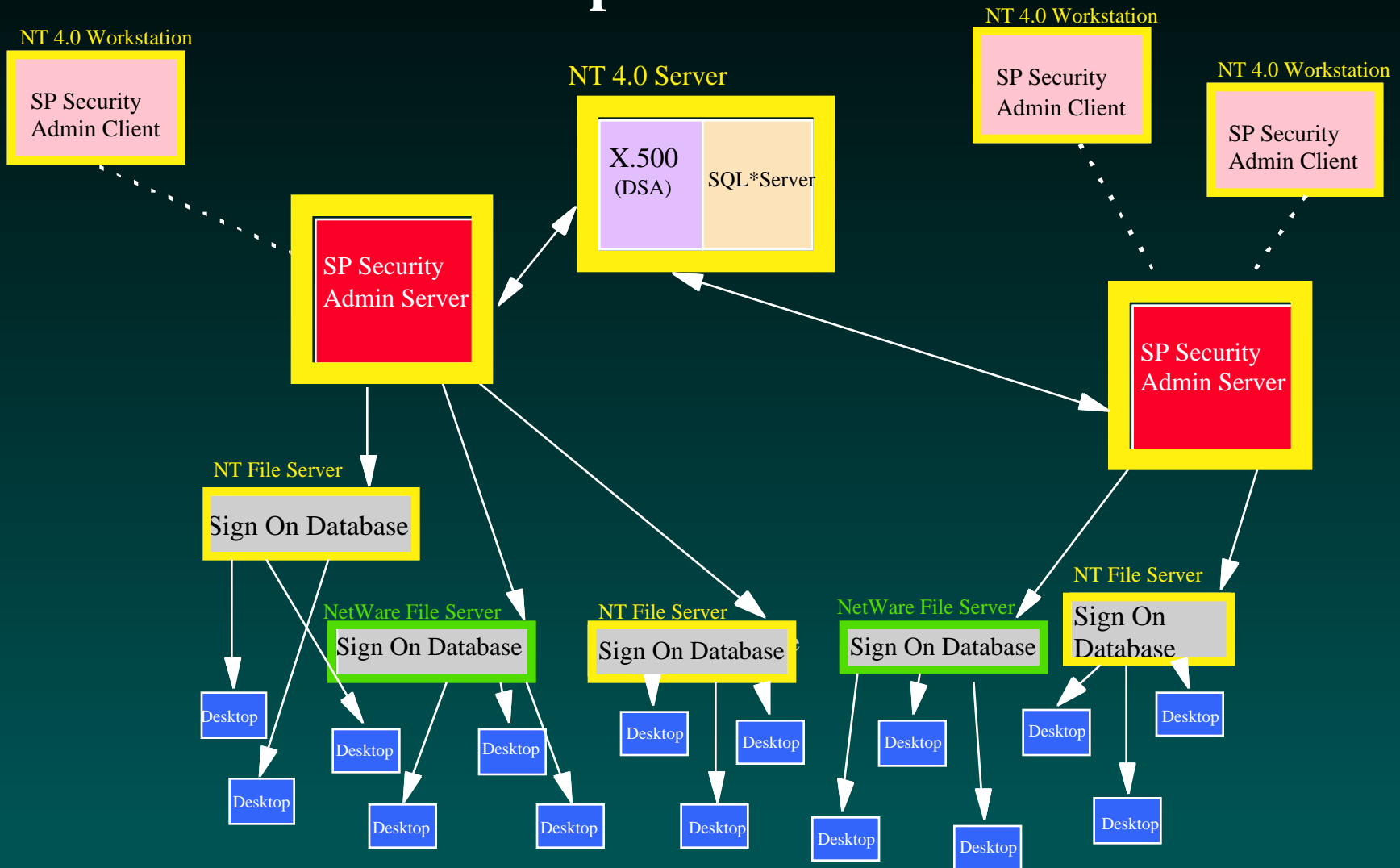
SP Security Administration

Enterprise Version



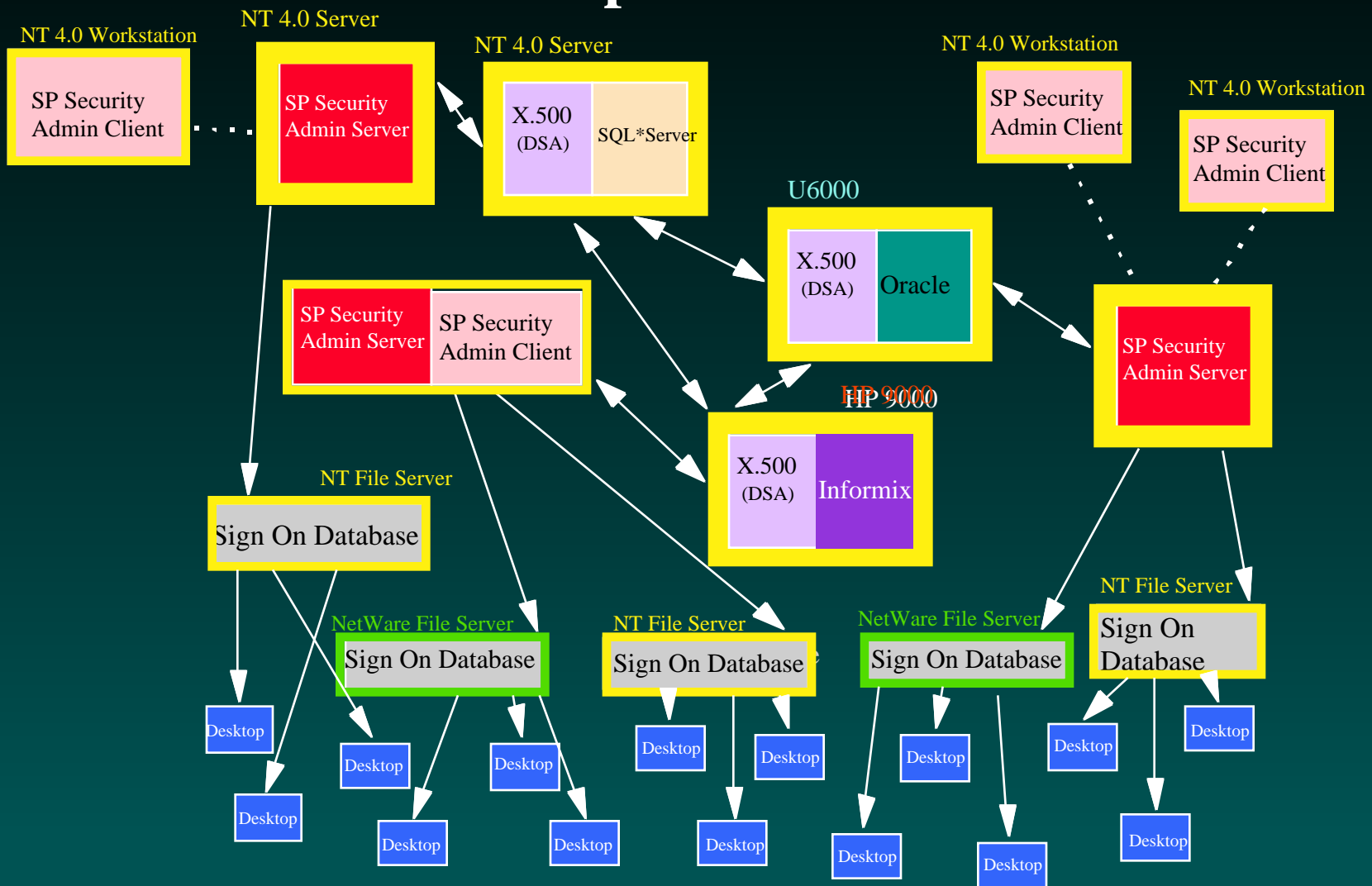
SP Security Administration

Enterprise Version

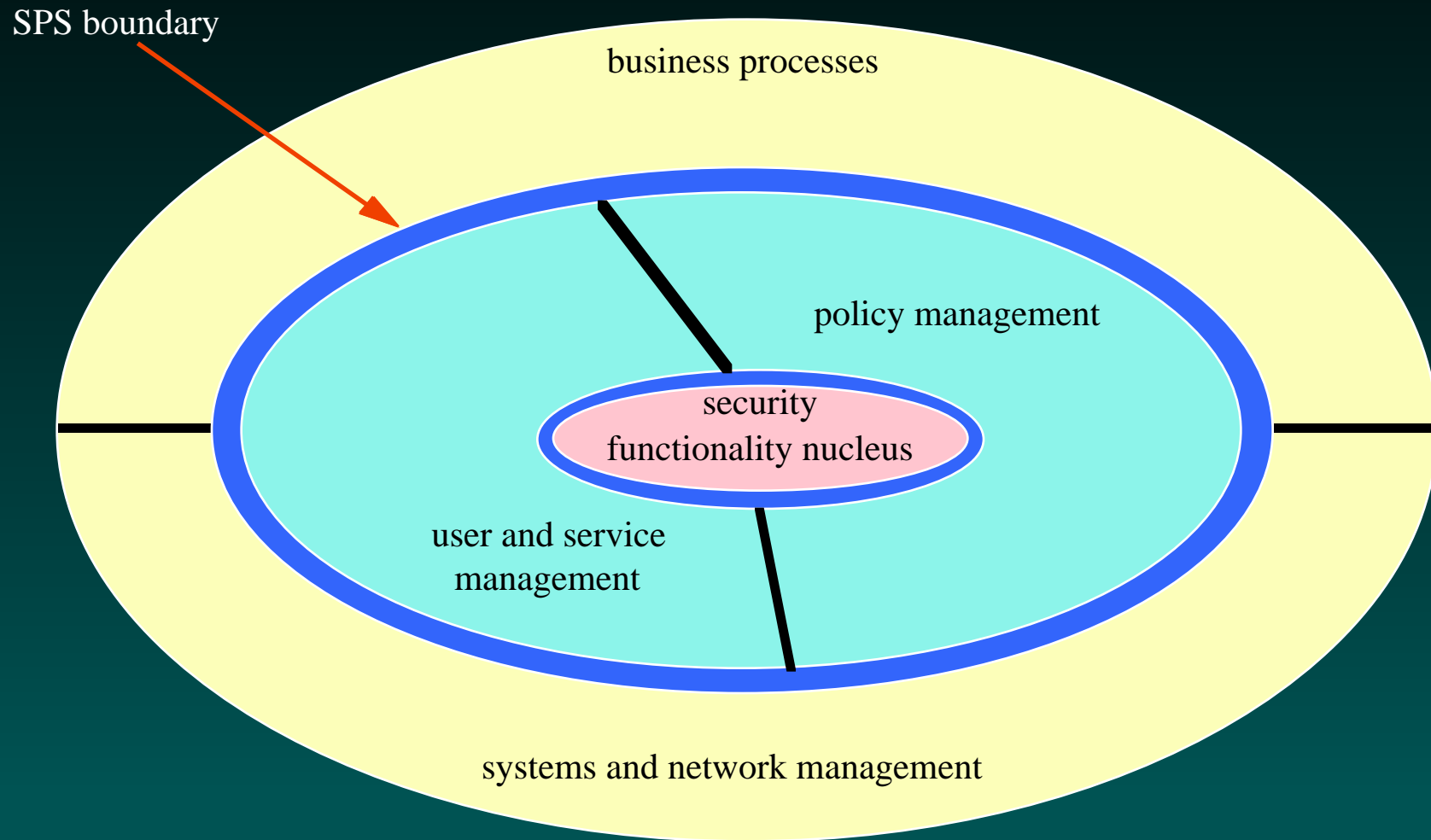


SP Security Administration

Enterprise Version

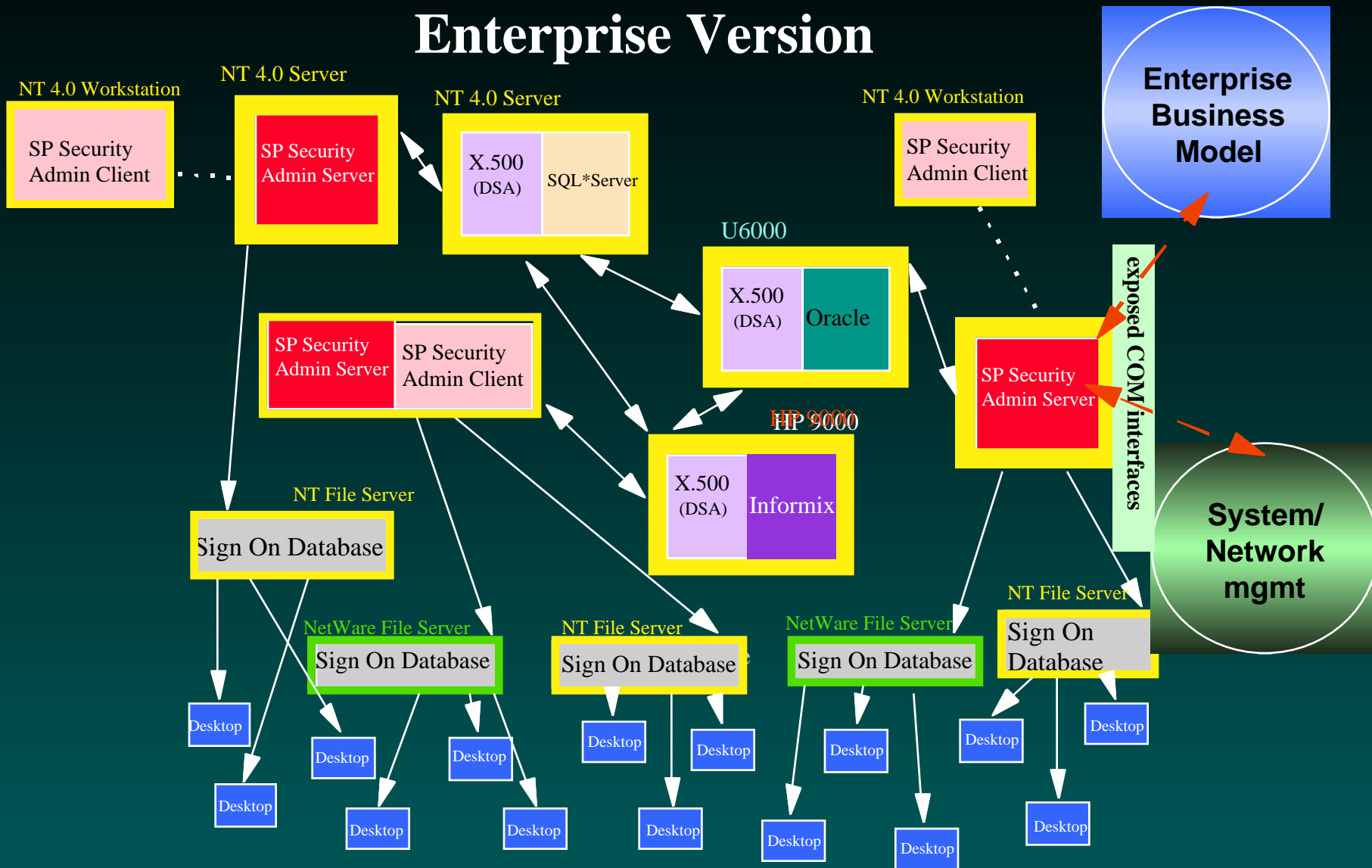


Concentric bands of administration abstraction (through exposed interfaces)



SP Security Administration

Enterprise Version





SPS Administration

- requirements:
 - enterprise scale solution
 - **easy to administer**
 - flexible - easy to customize
 - extensible - easy to include new managed platforms

Easy to Administer

- policy objects
- “chunking concepts”
- “task” concept
 - built-in recovery
- familiar GUI



Easy to Administer

- **policy objects**
- “chunking concepts”
- SPS model
- “task” concept
 - built-in recovery
- familiar GUI

SP Security Administration

- policy administration

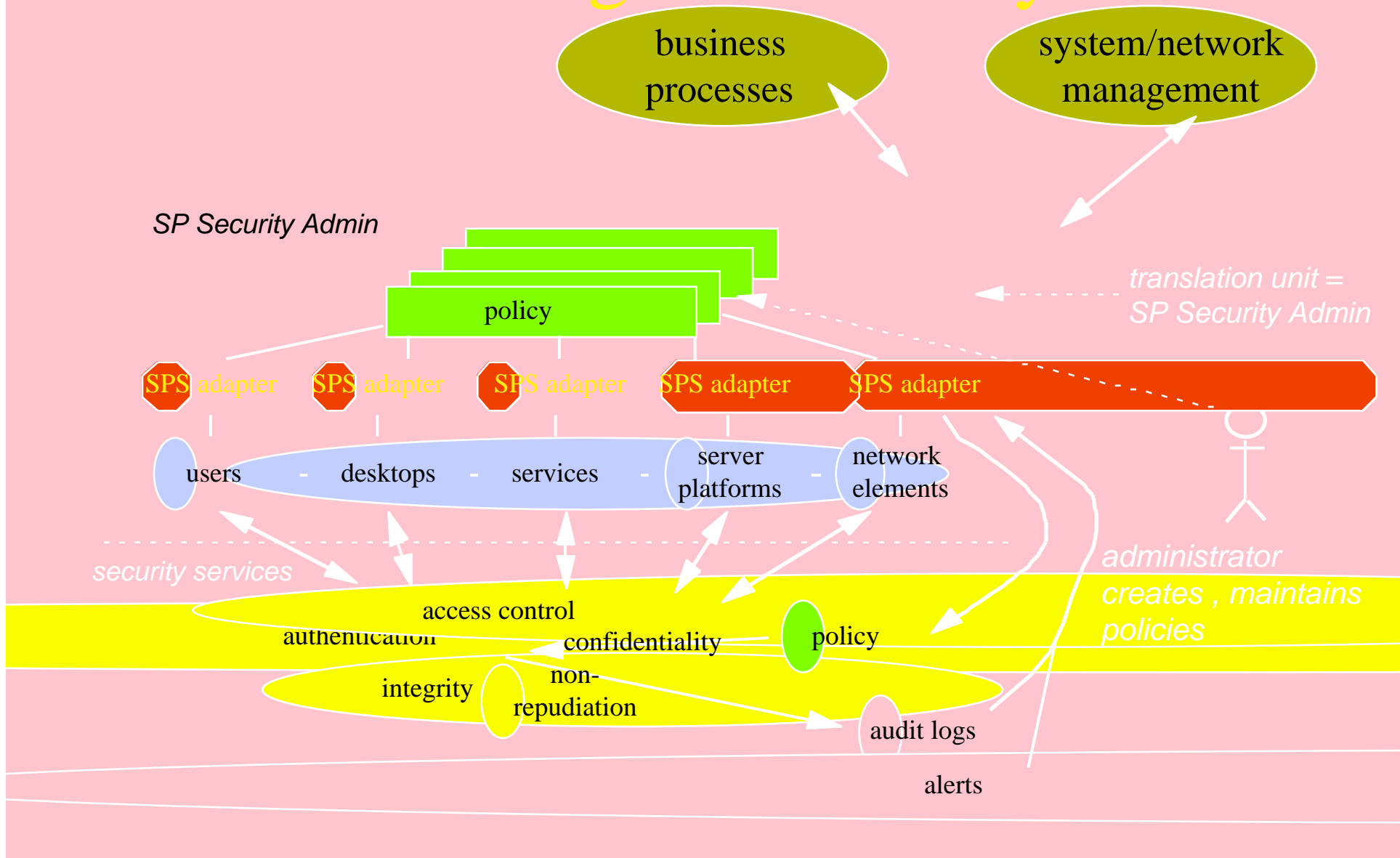
*a **policy** is a definition (or customization) of behavior for this instance of the SP Security solution.*

- policy set by :
 - default - shipped with the product
 - admin user interface
 - policy scripts
- policy defined at domain level
- policy administration a specific administrator privilege

Policy as a point of leverage

- policy constructed at higher level of abstraction
- once thought out and constructed, can be applied in many situations
 - and adapted for others
- senior administrator constructs/maintains policy
- junior administrators can invoke policies

Security-related administration - the Single Point way



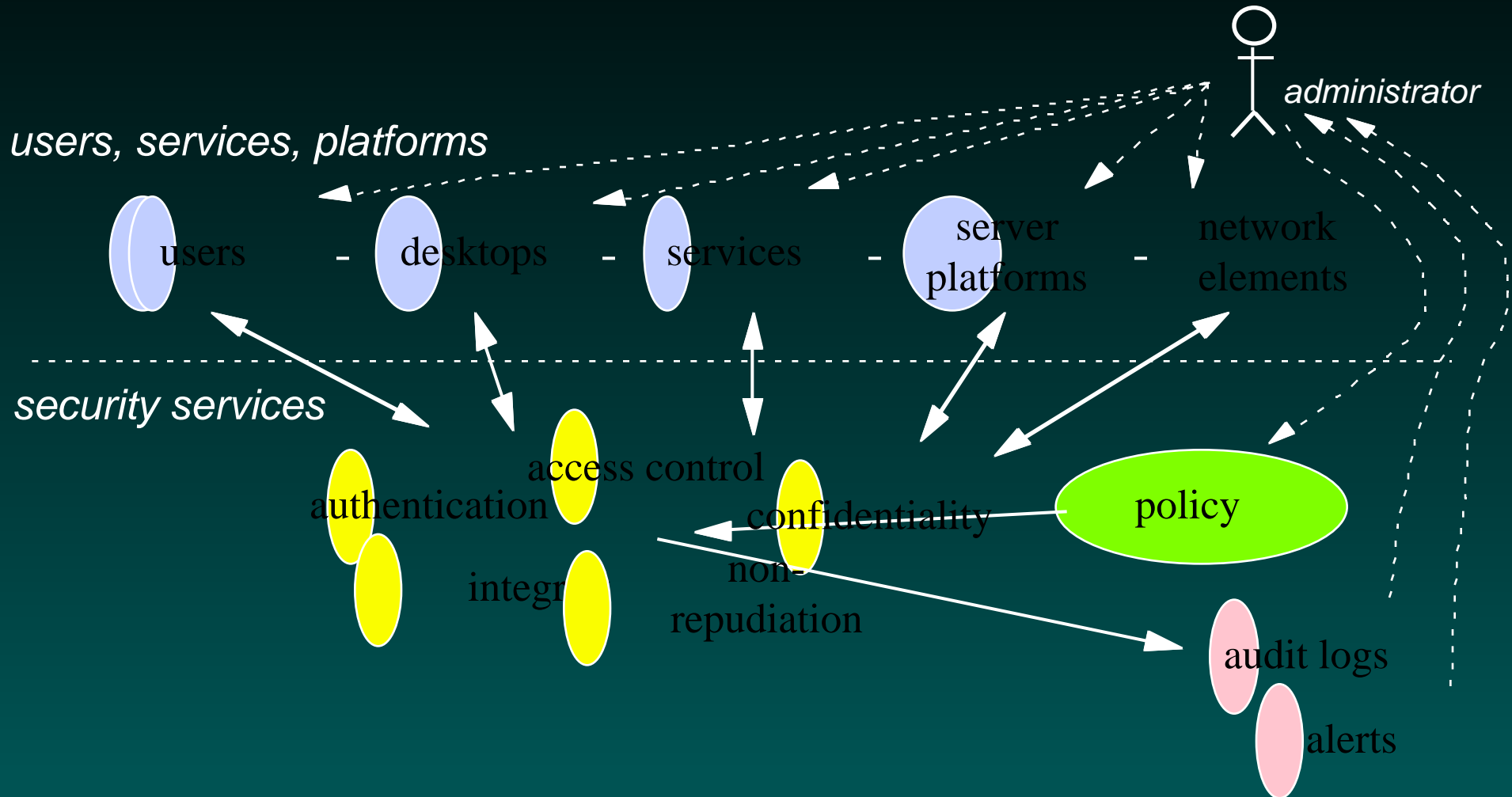
SP Security Administration

entities the Administrator can Control

- users
- desktops
- services
- servers
- network elements
- security mechanisms



Security-related administration





Easy to Administer

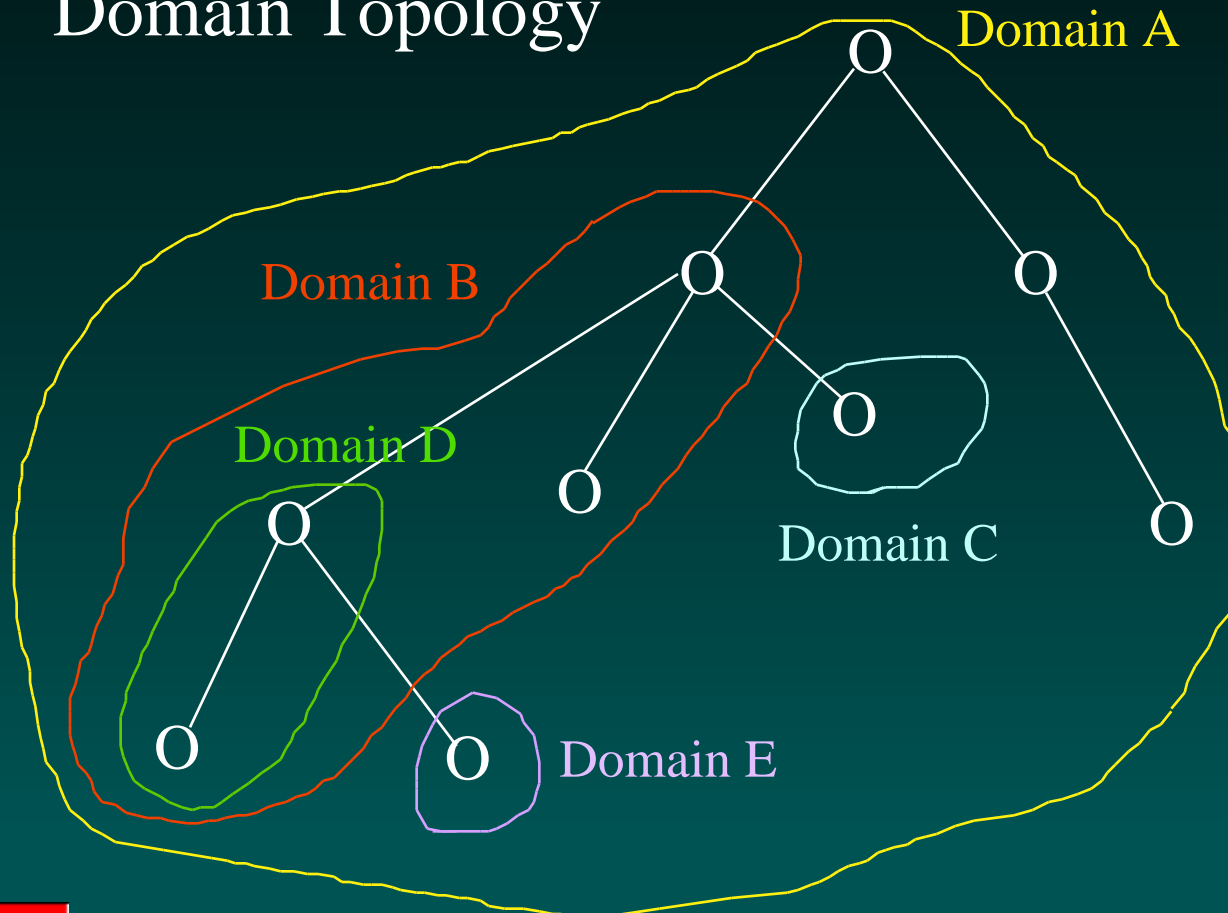
- policy objects
- **“chunking concepts”**
- SPS model
- “task” concept
 - built-in recovery
- familiar GUI

SP Security Chunking Concepts

- concepts to raise level of abstraction - permits “chunking” of information for increased intellectual manageability
 - domains
 - user groups
 - roles
 - service groups
 - administrators
 - administrator groups
 - tasks

SP Security Domains

Domain Topology





Easy to Administer

- policy objects
- “chunking concepts”
- **SPS model**
- “task” concept
 - built-in recovery
- familiar GUI

SPS Model

- model constructed around “chunking concepts”
- provides scalability and leverage
- a *single* (although distributed) repository

SPS Model Examples

- add service to service group
 - potentially rolls out new application to entire enterprise
- change relationship between service group and user group
 - changes services available to all users in group



Easy to Administer

- policy objects
- “chunking concepts”
- SPS model
- **“task” concept**
 - built-in recovery
- familiar GUI

SPS “Task” concept

- tasks adjust managed system configuration to reflect the model
- tasks scheduled by administrator
 - review, validate changes to the model
 - avoid race conditions
 - avoid disruption to ongoing operations

SP Security Task Recoverability

- all committed tasks parsed into discrete action request lists and maintained in persistent storage
- recoverable to individual action request
- session histories kept for every transaction
 - between admin client and server
 - between servers
 - between server and X.500
- status of tasks available for audits and tracking



Easy to Administer

- policy objects
- “chunking concepts”
- SPS model
- “task” concept
 - built-in recovery
- **familiar GUI**

SP Security Administrator GUI

- administrator User Interface fully integrated with NT Explorer
 - SP Security Standard View
 - list, tree views
 - filters, searches



SPS Administration

- requirements:
 - enterprise scale solution
 - easy to administer
 - **flexible - easy to customize**
 - extensible - easy to include new managed platforms

SPS Flexibility

- a major design goal:
 - *lower the cost of entry to customization*
 - for customers
 - for third party ISVs and integrators
- object model
 - generic objects
 - standard objects
 - custom objects

SPS Object Model

- generic, standard, custom
- generic
 - e.g. user, usergroup, role
- standard
 - e.g. default policies
- custom
 - e.g. enterprise-specific policies

SPS Object Model

- flexibility through
 - building on (deriving from) standard objects
 - creating new objects (of generic type)
 - creating new generic types

Generic/Standard/Custom

Analogous examples from Microsoft Excel

- generic
 - worksheet, cell, function, macro, formula, etc.
- standard
 - e.g. function: sqrt, log, tan, concatenate, etc.
- custom
 - user-defined functions

Why use SPS Administration?

(Why use Excel rather than calculator?)

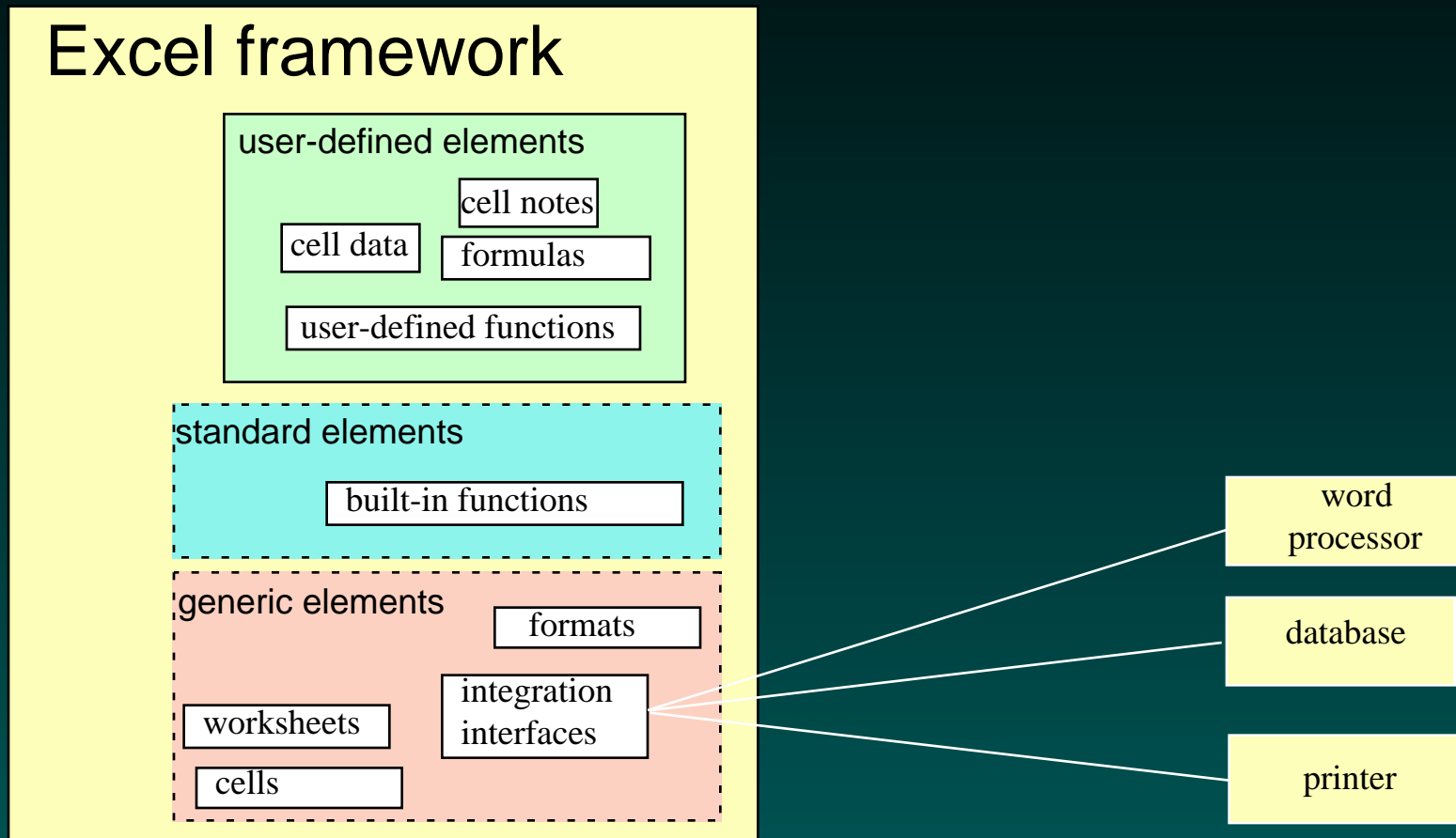
calculator

- manual data entry
- repeated data entry
- repeated calculations
- errors
- manual recording and transport of output

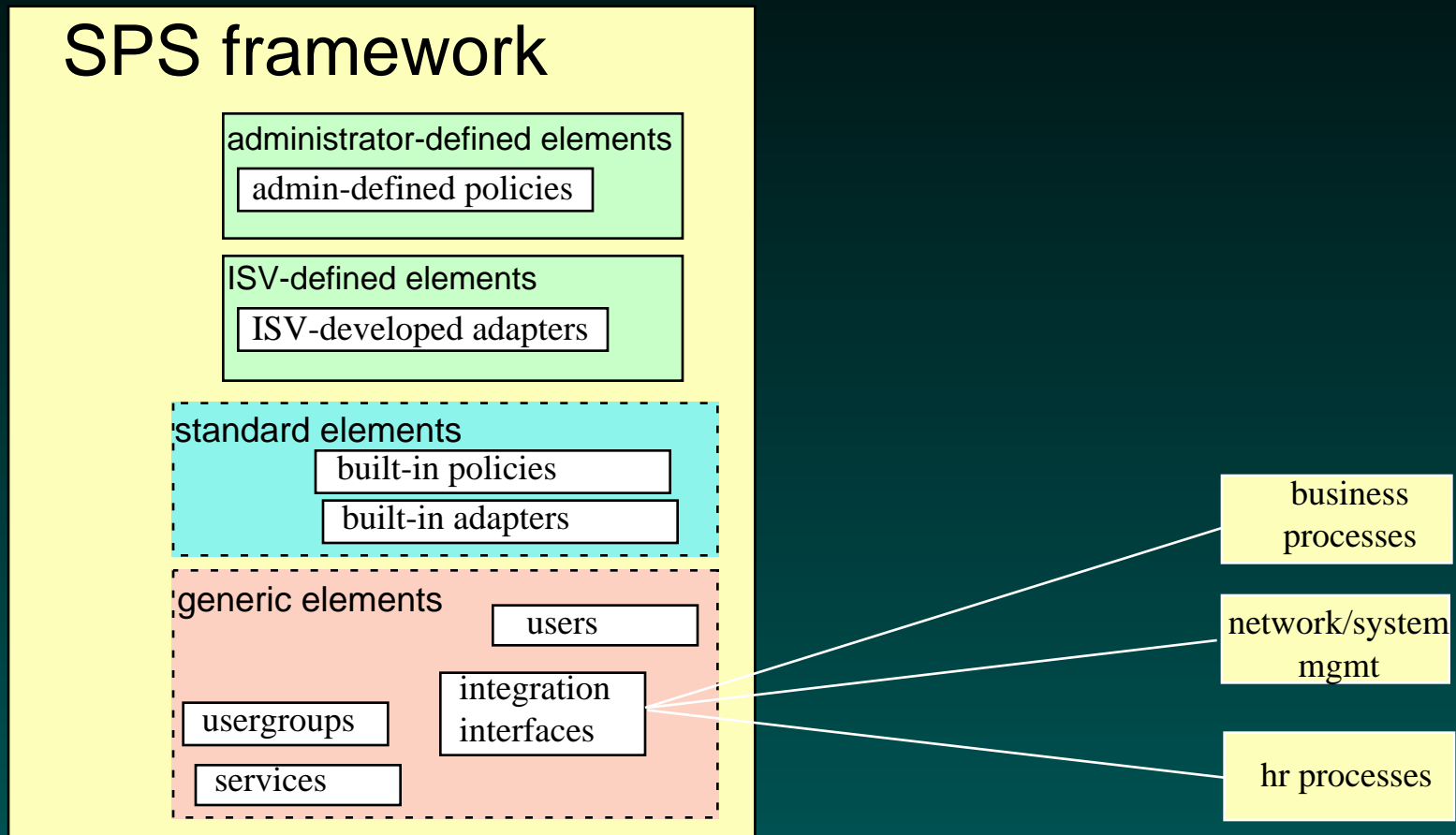
Microsoft Excel

- prebuilt framework for organization
 - worksheets, cells, formats, notes, etc.
- one time data entry
- data import from other sources
- data export to other sources
 - database, word processor, printer, etc.
- persistently remembered procedures
- etc.

Why use Microsoft Excel?



Why use SPS Administration?





SPS Administration

- requirements:
 - enterprise scale solution
 - easy to administer
 - flexible - easy to customize
 - **extensible - easy to include new managed platforms**

SPS Extensibility

- exposed COM interfaces
- Explorer-based GUI
 - Internet integration
- NT based
 - easily integrate third party products

SP Security Administration

Development Tool Kit :

- policy scripts
 - defaults based on best practices
 - use industry standard scripting tools, such as Java, VB
 - customer (and third parties) can do things not yet thought of
- published OLE interface specifications for ISVs
(for automation & adapter development)
- task oriented Wizards

Summary

- Unisys Single Point Security
 - tames the complexity problem in security administration
 - massively scalable
 - infinitely flexible and extensible
 - addresses today's situation
 - designed to grow and adapt to tomorrow's situation