Web Application Security Infrastructure

Web Application Security Infrastructure

Reverse Proxies, Attack Surfaces and Single-Sign-On

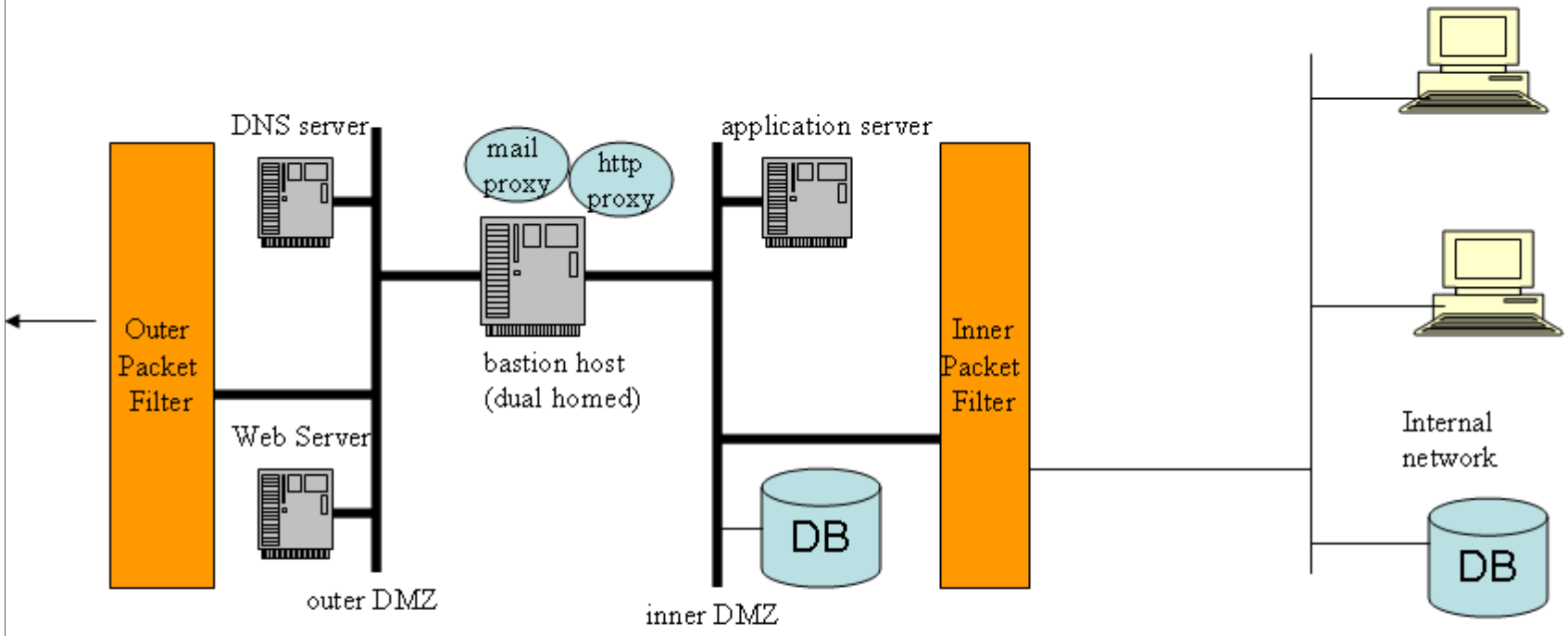
Goals

- Explain typical web application infrastructures and how they are secured using reverse proxies
- Show how attack surfaces of web apps can be reduced
- Raise developer awareness for the dependencies of application architectures on infrastructure
- Demonstrate Single-Sign-On options and approaches

Overview

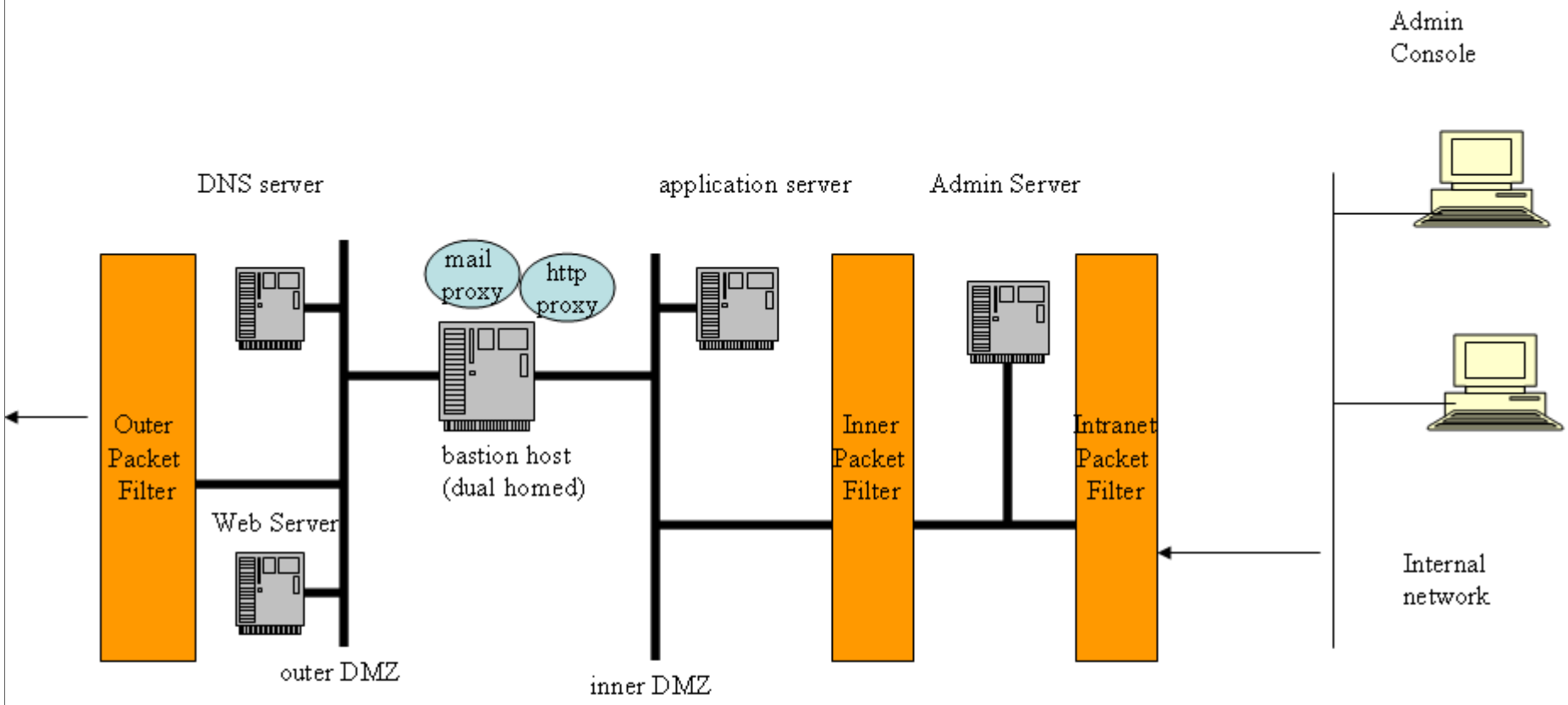
- DMZ and Firewall Organization
- The Architectural Role of Reverse Proxies
- Attack Surface Reduction
- SSO Approaches
- Virtual Organizations

Firewall and DMZ Topologies

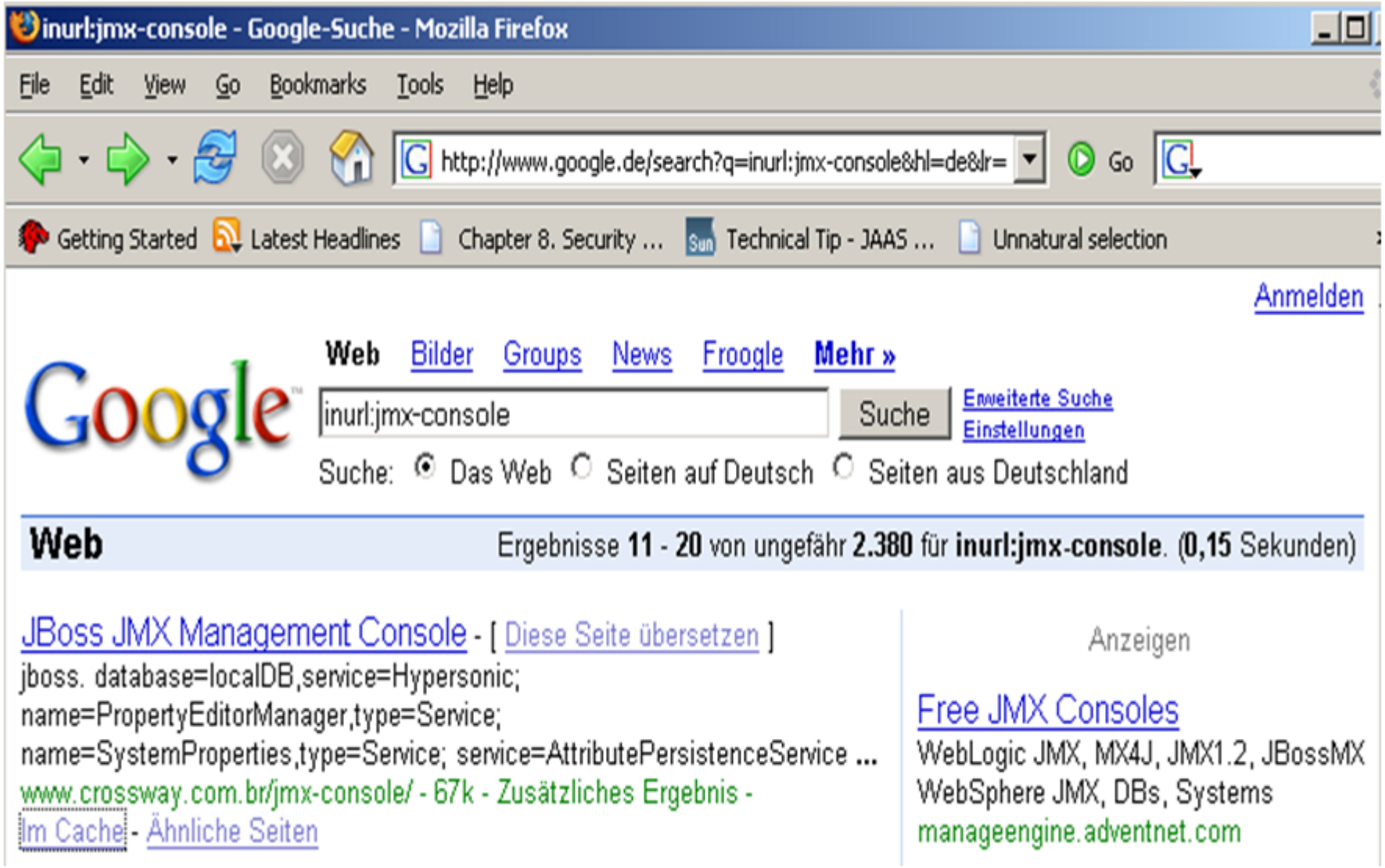


A simple DMZ. Topology and security policies define:

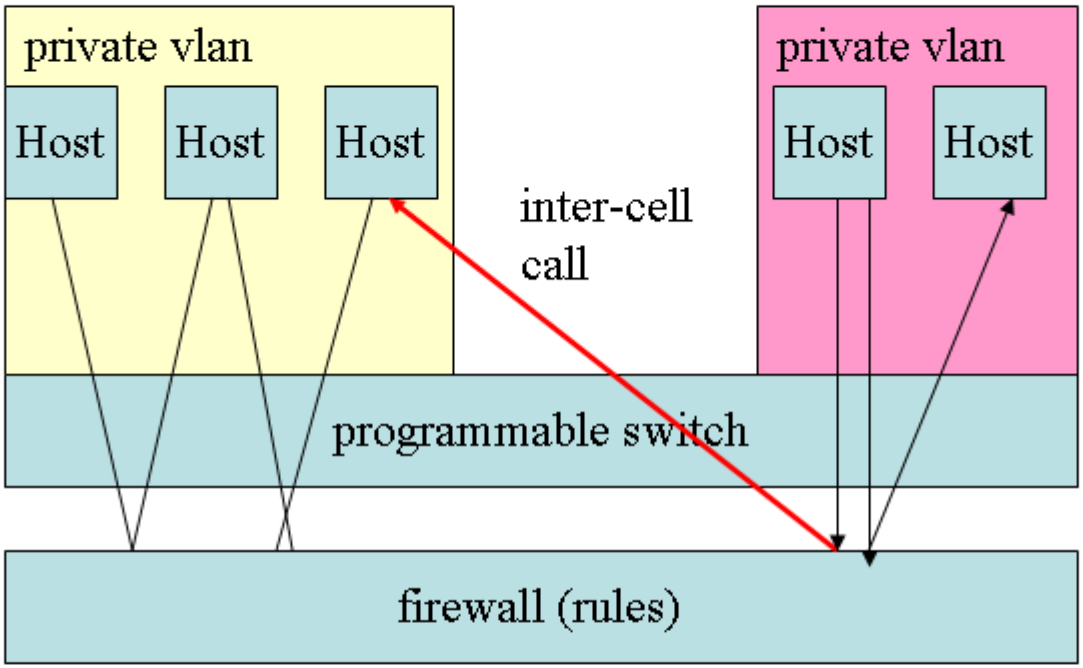
- what kind of protocols are allowed in which zone
- required changes of protocols
- when do we require authentication?
- who can access those zones from where?
- are there zones with different security requirements?



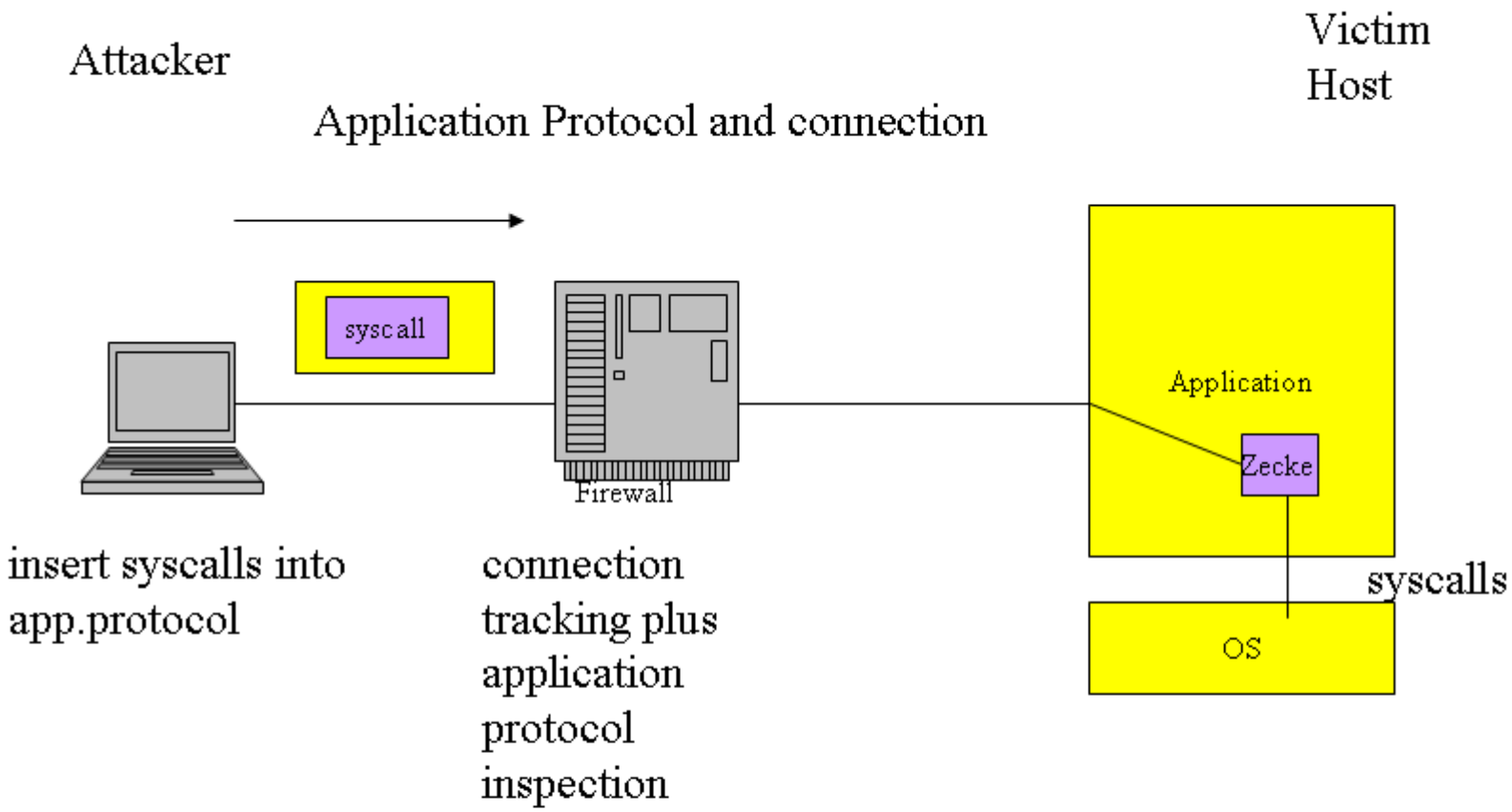
The problem of administrative access! Is interactie access allowed? Do we require an admin proxy inside of zones?



Use google to find unsafe administration entries!



Granular isolation using private vlan technology



Penetrate the firewall using application protocols

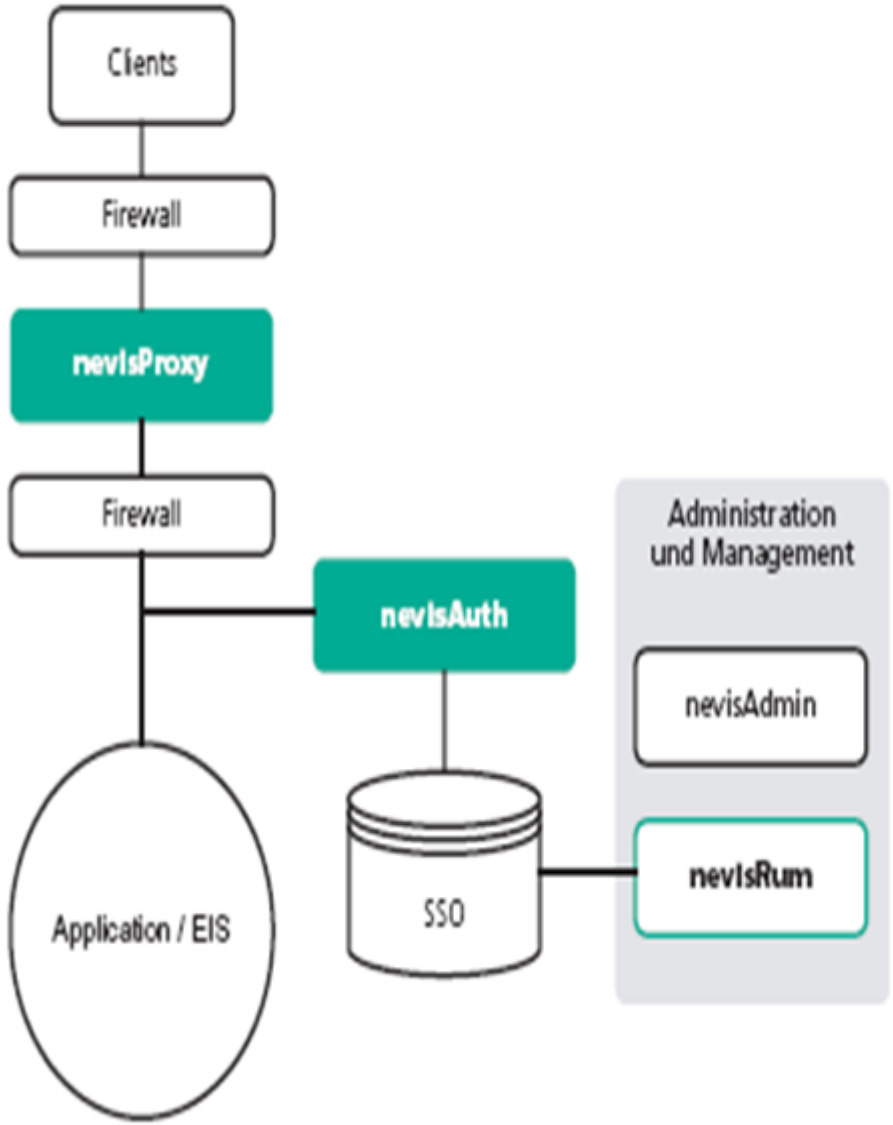
Reverse Proxies

The Architectural Role of RPs for Web Application Security

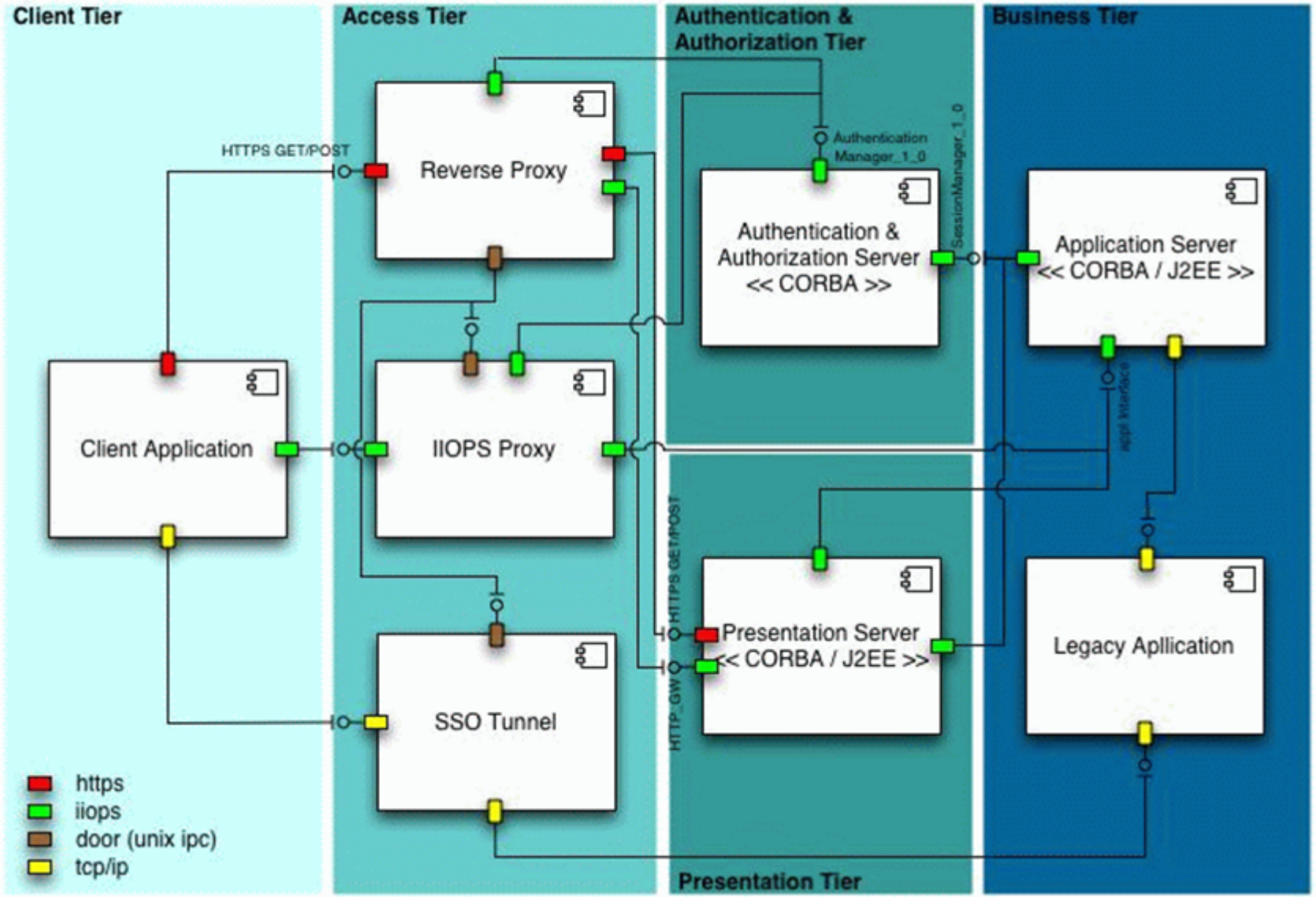
Reverse Proxy Responsibilities

- Deny access to un-authenticated requests coming from the Internet
- Determine identity and location of a request.
- Accecpt identity tokens for token-based secure delegation.
- Control Session Handling
- Control Internet access from inside
- Logging and Filtering

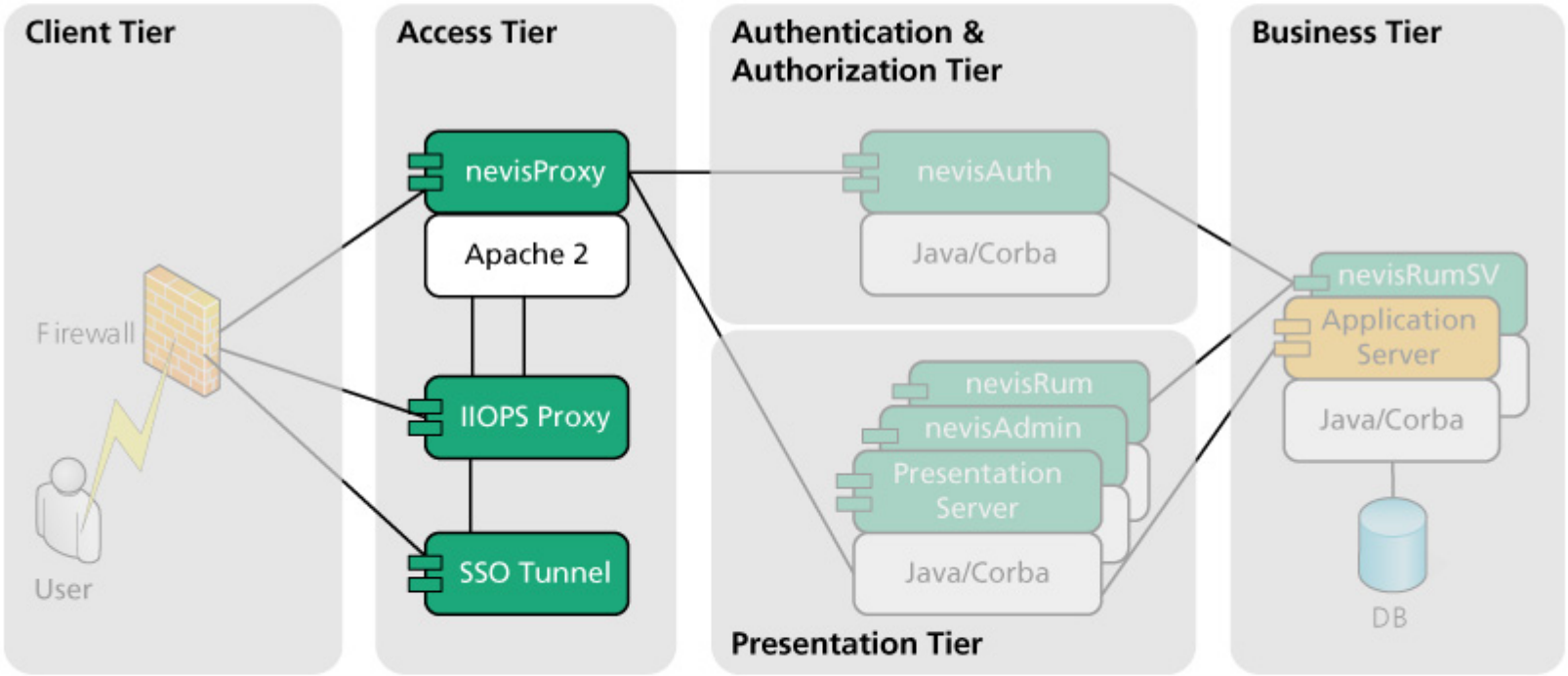
Example: Nevis-Web Architecture



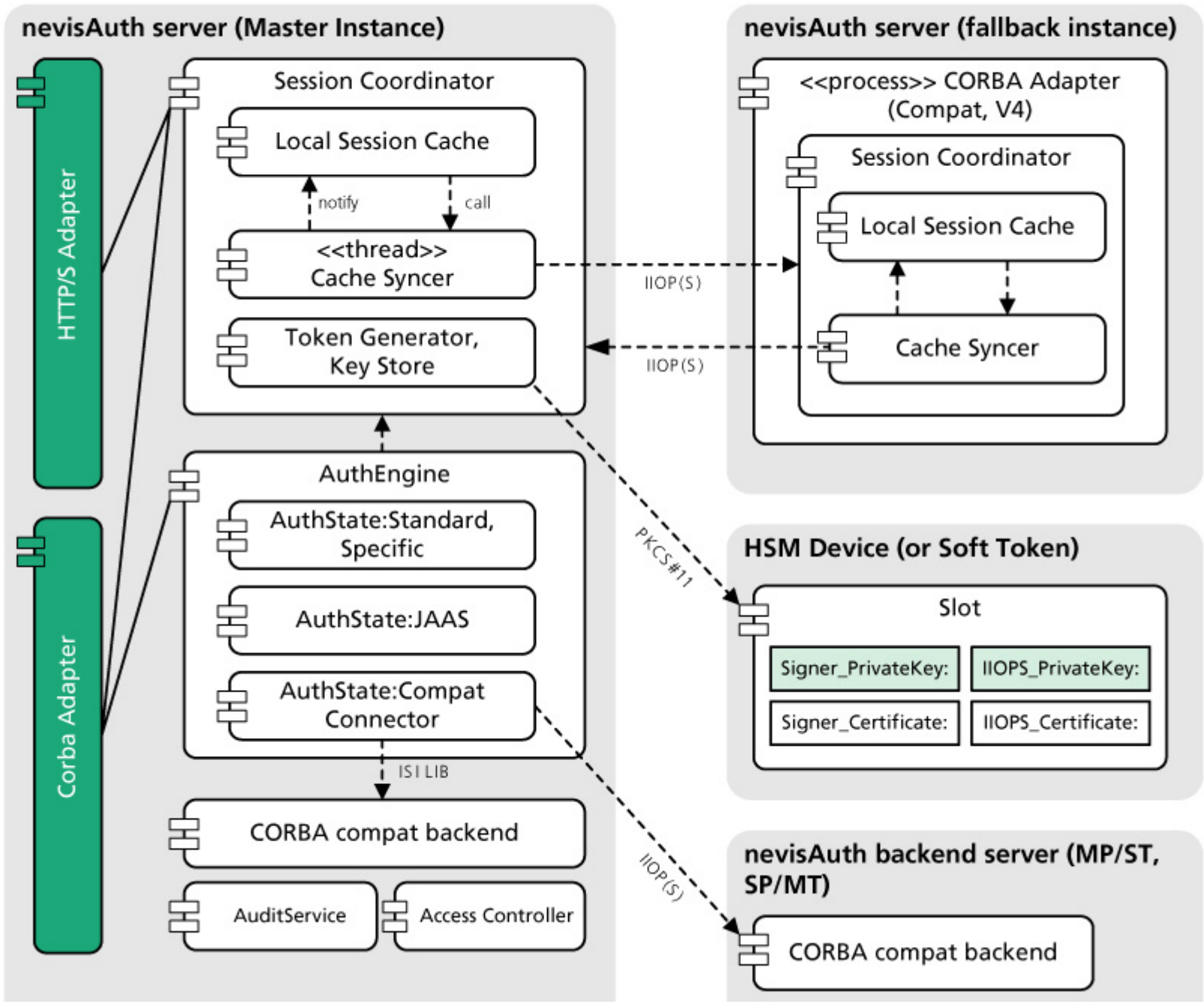
Protocols and Layers

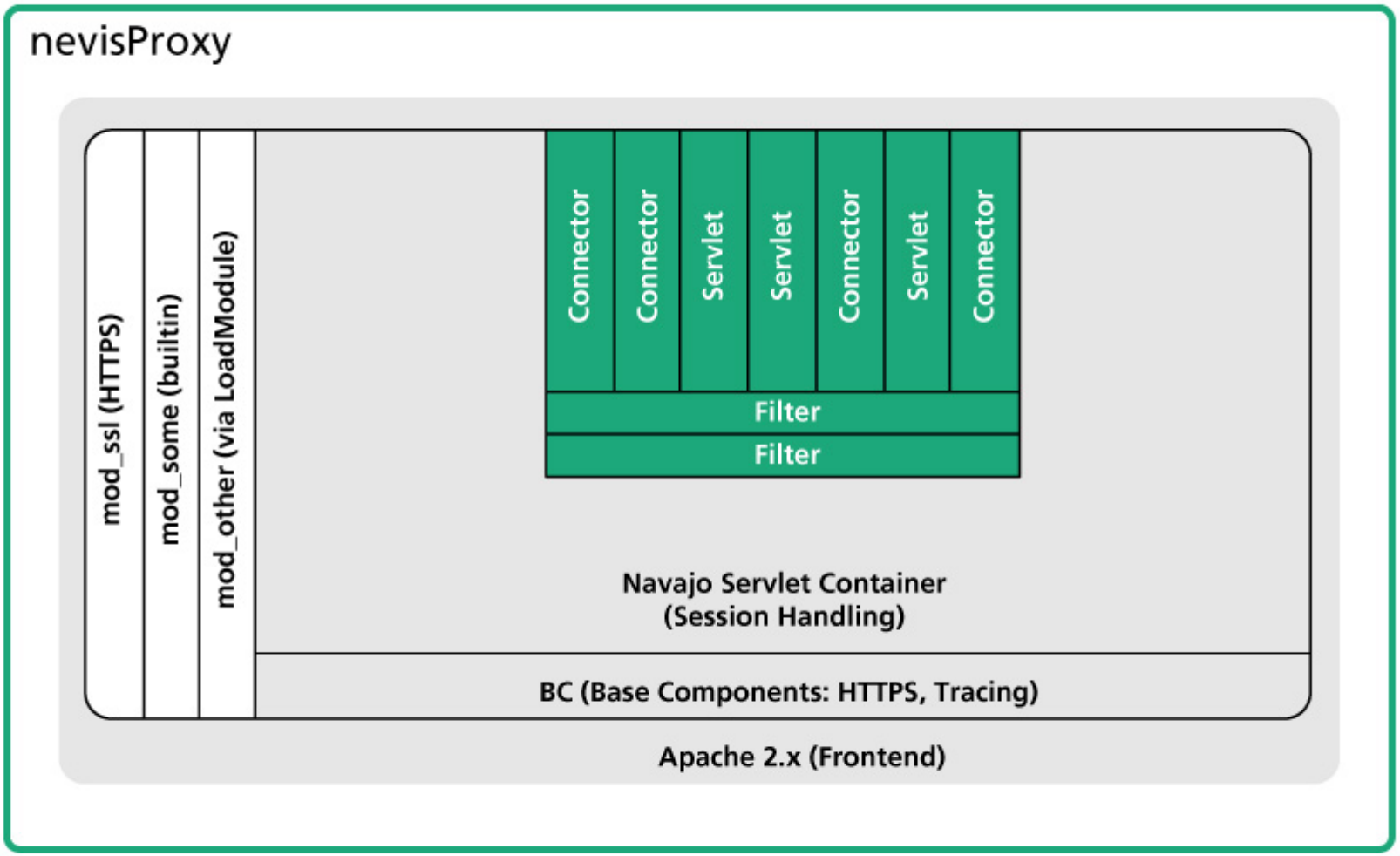


nevisProxy

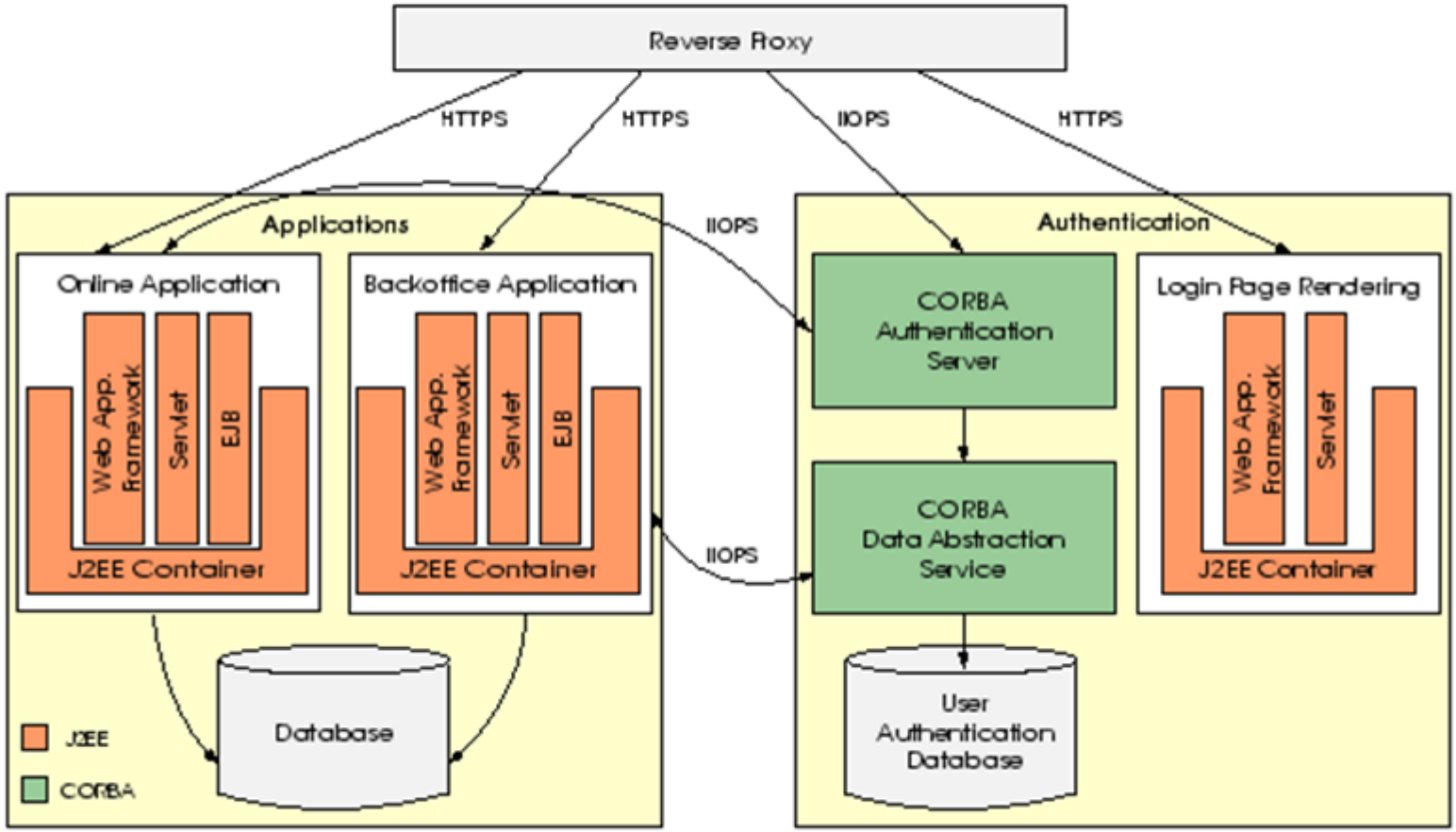

Client Tier
Access Tier
Authentication &
Authorization Tier
Business Tier
nevisProxy
Apache 2
IIOPS Proxy
SSO Tunnel
nevisAuth
Java/Corba
nevisRum
nevisAdmin
Presentation
Server
Java/Corba
Presentation Tier
nevisRumSV
Application
Server
Java/Corba
DB
Firewall
User

nevisAuth

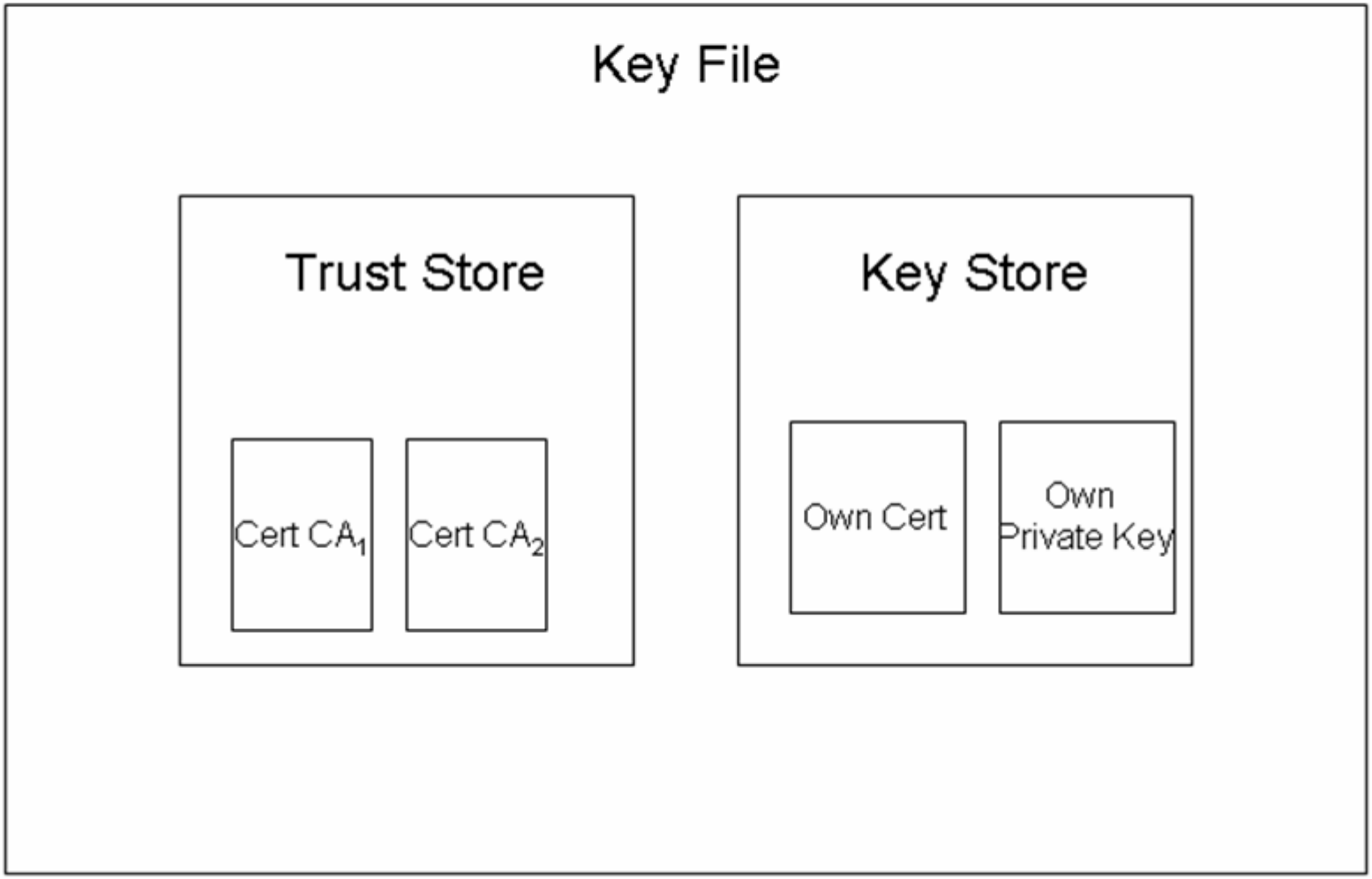

nevisAuth server (Master Instance)
HTTP/S Adapter
Corba Adapter
Session Coordinator
Local Session Cache
notify
call
<<thread>>
Cache Syncer
Token Generator,
Key Store
AuthEngine
AuthState:Standard,
Specific
AuthState:JAAS
AuthState:Compat
Connector
ISI LIB
CORBA compat backend
AuditService
Access Controller
IIOP(S)
IIOP(S)
PKCS#11
IIOP(S)
nevisAuth server (fallback instance)
<<process>> CORBA Adapter
(Compat, V4)
Session Coordinator
Local Session Cache
Cache Syncer
HSM Device (or Soft Token)
Slot
Signer_PrivateKey:
IIOPS_PrivateKey:
Signer_Certificate:
IIOPS_Certificate:
nevisAuth backend server (MP/ST,
SP/MT)
CORBA compat backend


nevisProxy
mod_ssl (HTTPS)
mod_some (builtin)
mod_other (via LoadModule)
Connector
Connector
Servlet
Servlet
Connector
Servlet
Connector
Filter
Filter
Navajo Servlet Container
(Session Handling)
BC (Base Components: HTTPS, Tracing)
Apache 2.x (Frontend)

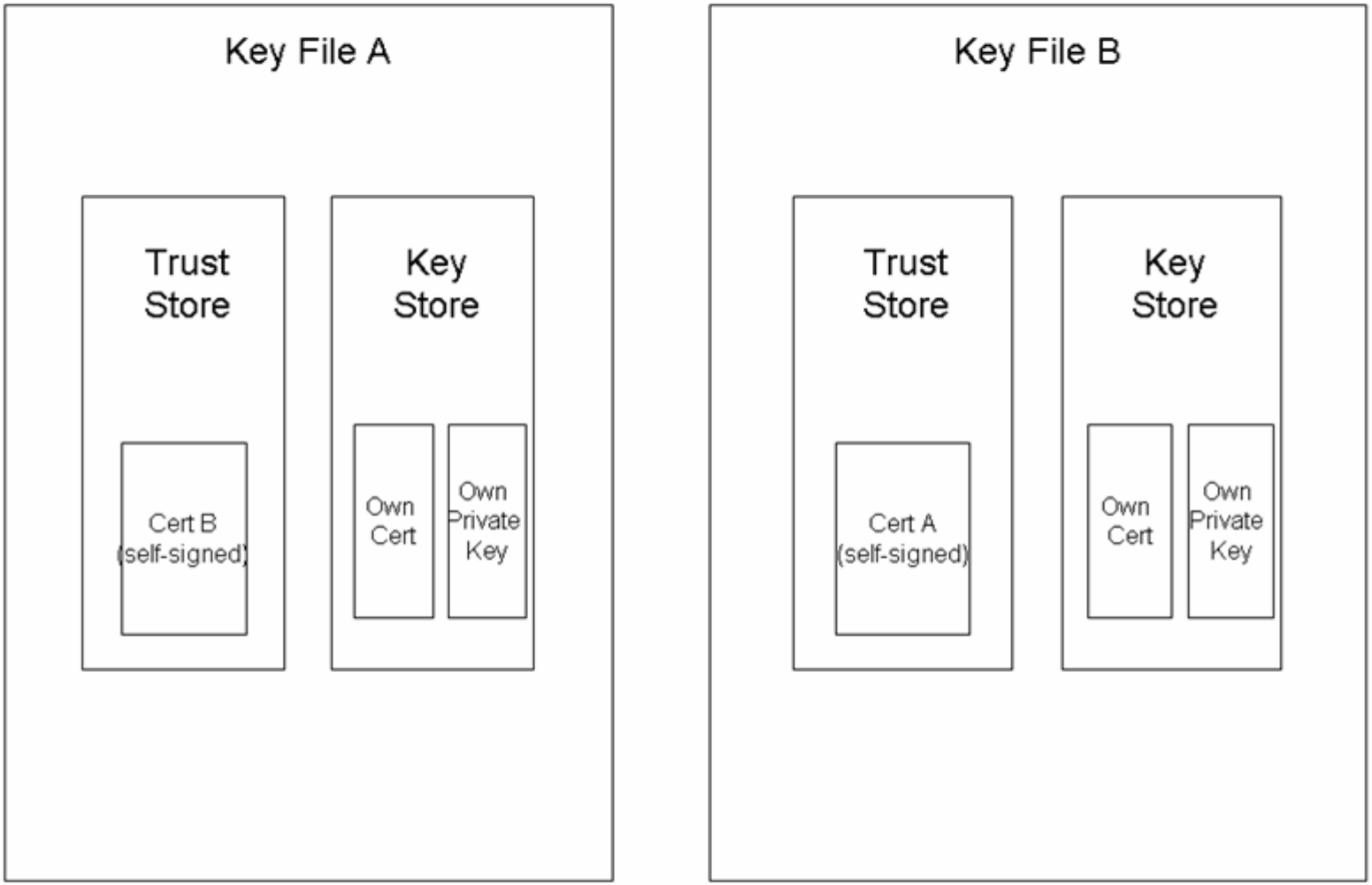
Backend Connections



Mutual Authentication Issues



Two Nodes



Are you aware of the implications of putting a root cert into your trust store?

Sessions and Timeouts

Session Mechanisms

- a TCP sequence number which is incremented with every request
- some arbitrary piece of data which accompanies every request. (Cookie oder spezielle URL)
- a SSL SessionID

The Timeout Problem

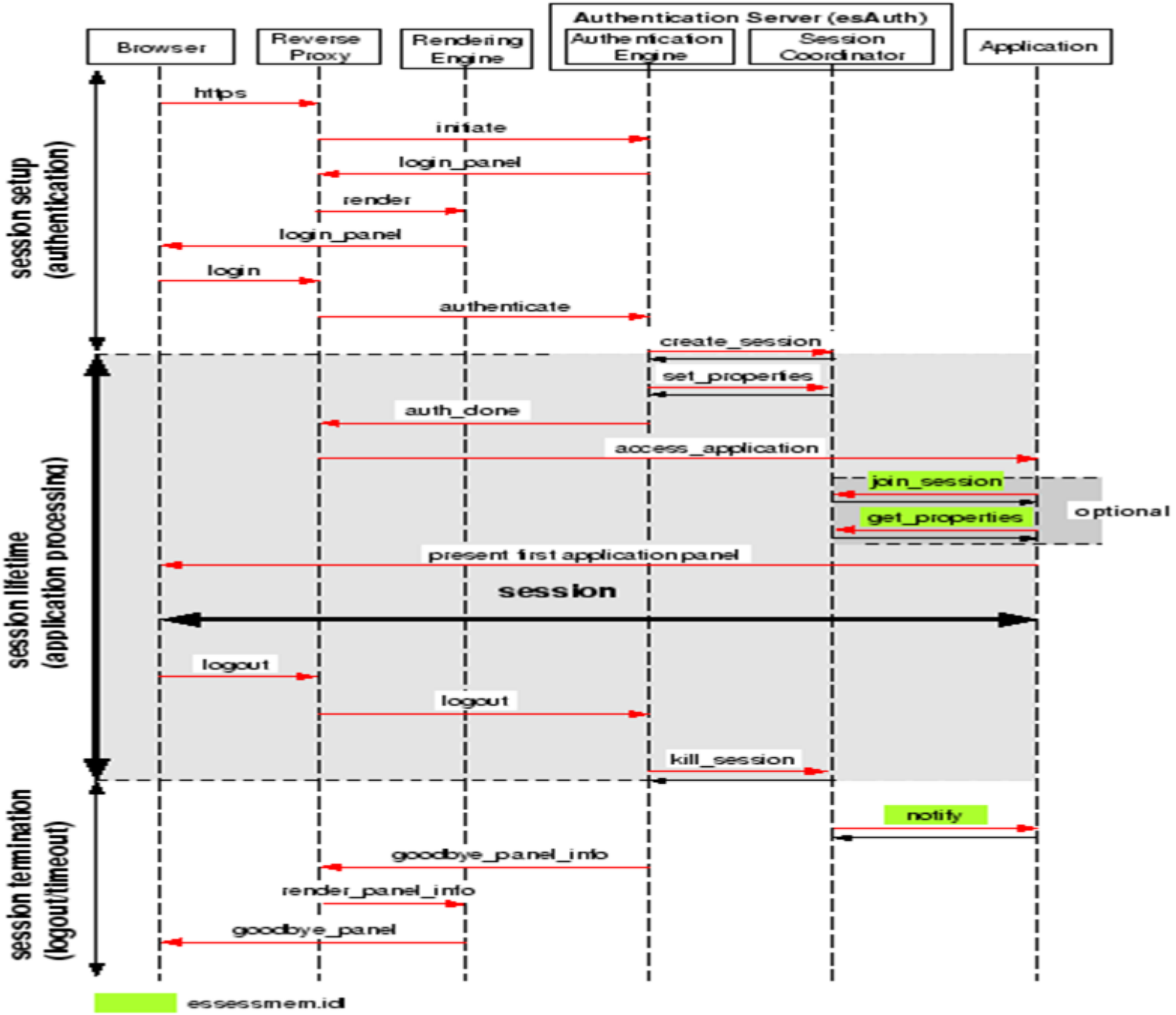
1. **A customer logs into an e-business application**
2. **The reverse proxy checks the credentials and generates an authenticated SSL session with the user agent and forwards the request to the app server.**
3. **The application server generates a session and an associated cookie which represents the proven identity of the customer (principal).**
4. **A hour goes by without an action by the customer. The timeouts expire. Now does the customer click on „logout“.**
5. **A „you need to log-in to logout“ message.**

The timeout mechanism and especially different timeouts active in a system can cause confusing behavior. Which timeout should expire first? What is a good value for a timeout?

Session Management

- **Is the mechanism for session management tried and proven? (SessionIDs, SSL-Sessions etc.)**
- **Does the application keep state internally? If yes: authenticated requests only?**
- **Does the application expect „Sticky Sessions“ (all requests of a customer end at the same application server?)**
- **Ist the sticky session mechanism compatible with the load-balancing infrastructure?**
- **Does the application require or expect session failover to other machines in the cluster or server complex? Are those machines defined?**
- **Does the load-balancer support pairs of machines in clusters?**
- **Is the session size well known and tracked with respect to performance?**

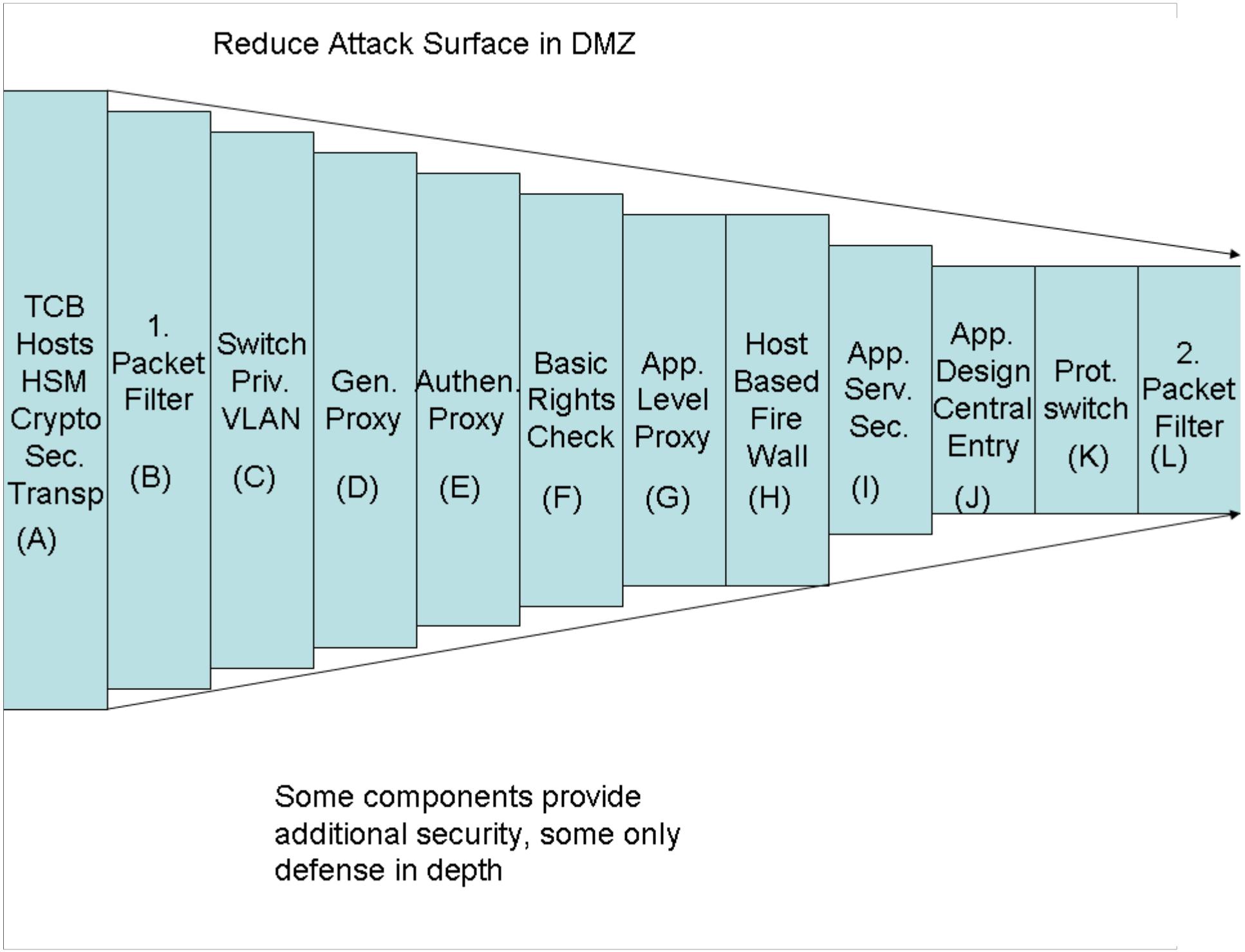
- **Is the max. session timeout in complicance with business and security requirements? Does transport level security support this value?**
- **Can the application detect the end of a session and what kind of event interfaces are available to send out or get notifications?**


Authentication Server (esAuth)
Browser
Reverse Proxy
Rendering Engine
Authentication Engine
Session Coordinator
Application
session setup (authentication)
https
initiate
login_panel
render
login_panel
login
authenticate
create_session
set_properties
auth_done
access_application
join_session
get_properties
optional
present first application panel
session
session lifetime (application processing)
logout
logout
kill_session
notify
goodbye_panel_info
render_panel_info
goodbye_panel
session termination (logout/timeout)
essessmem.idl

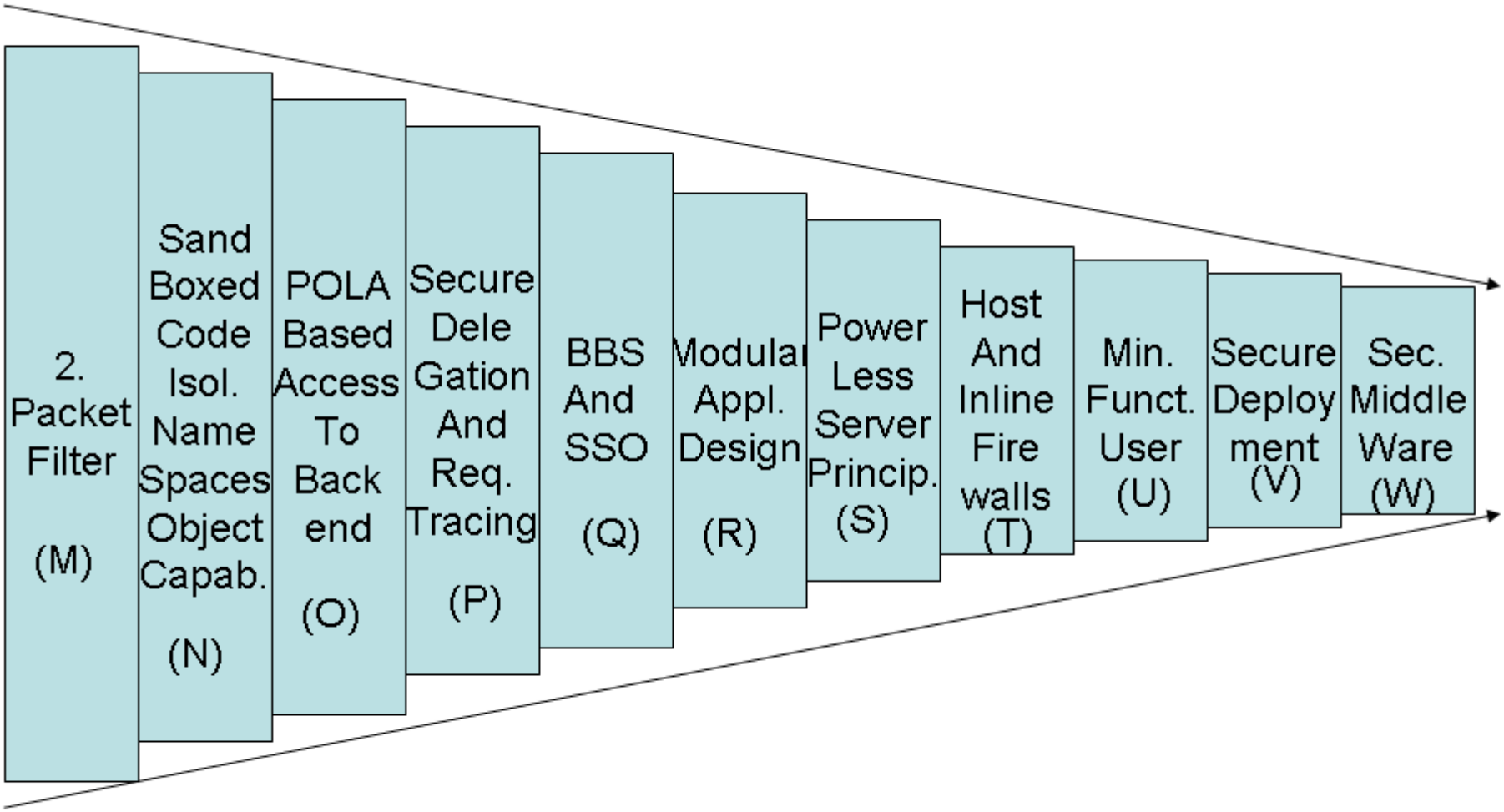
Attack Surface Reduction

Questions

- What can a simple generic proxy really do?
- What parts of your web app are really visible to the outside?
- What is changed by authentication?

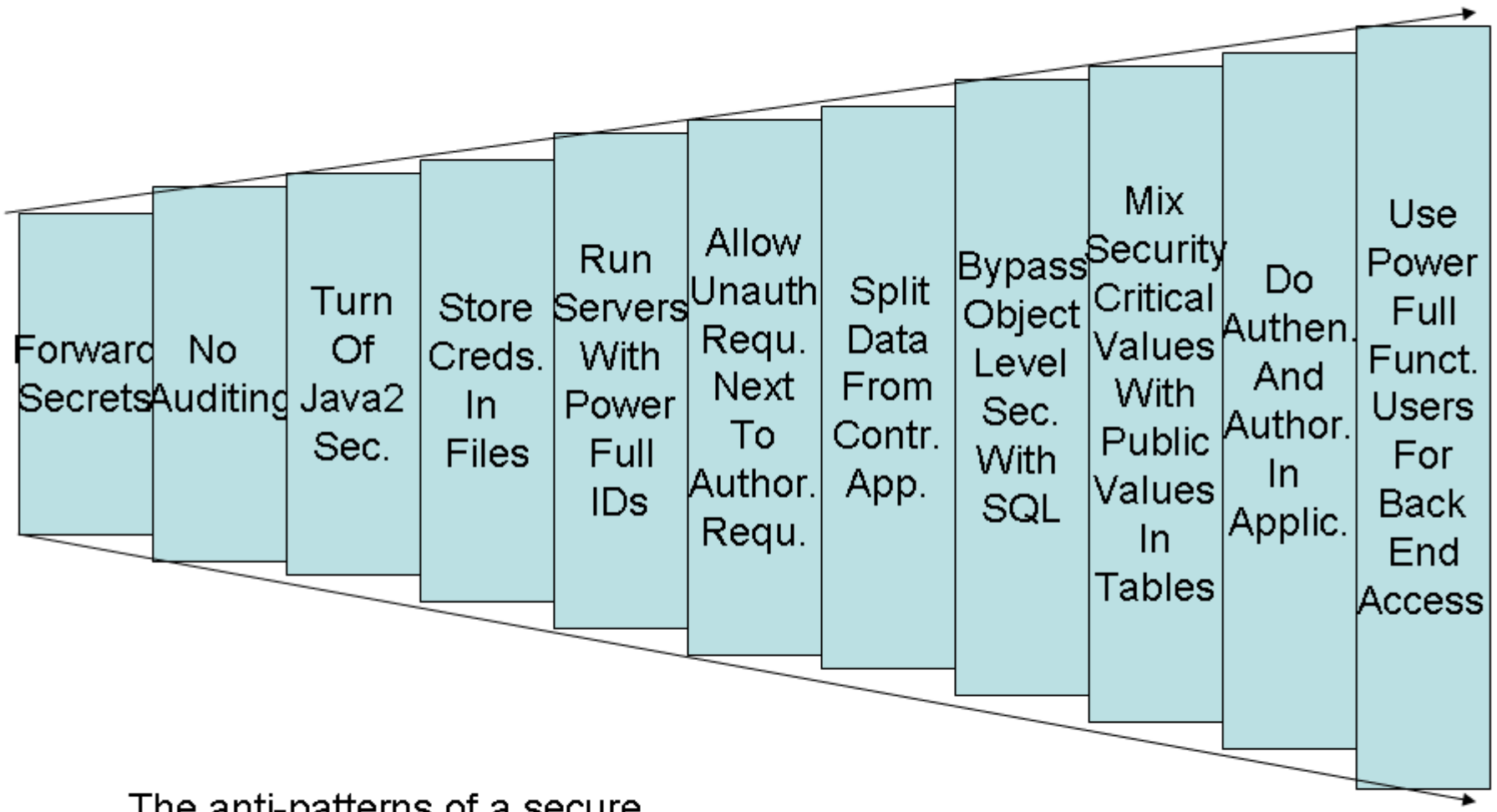

Reduce Attack Surface in DMZ
TCB Hosts HSM Crypto Sec. Transp (A)
1. Packet Filter (B)
Switch Priv. VLAN (C)
Gen. Proxy (D)
Authen. Proxy (E)
Basic Rights Check (F)
App. Level Proxy (G)
Host Based Fire Wall (H)
App. Serv. Sec. (I)
App. Design Central Entry (J)
Prot. switch (K)
2. Packet Filter (L)
Some components provide additional security, some only defense in depth

Reduce Attack Surface in Intranet



Code access security is a powerful technique to reduce damage in application servers

Increase Attack Surface in Intranet



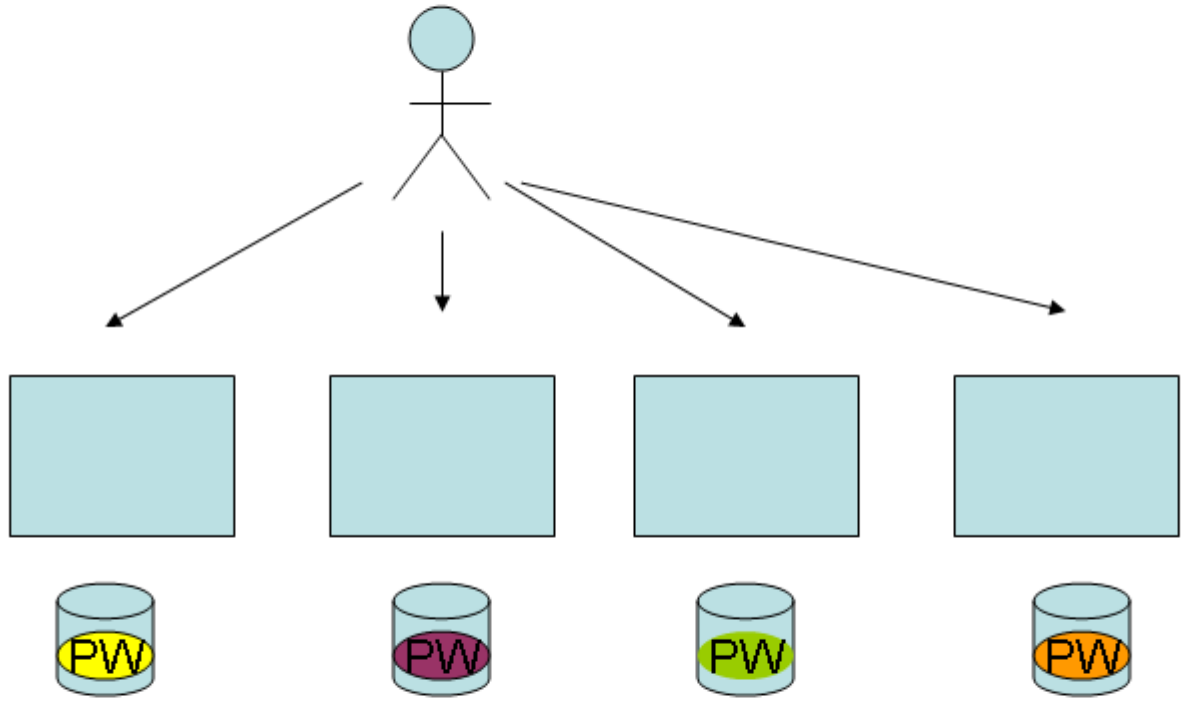
The anti-patterns of a secure infrastructure

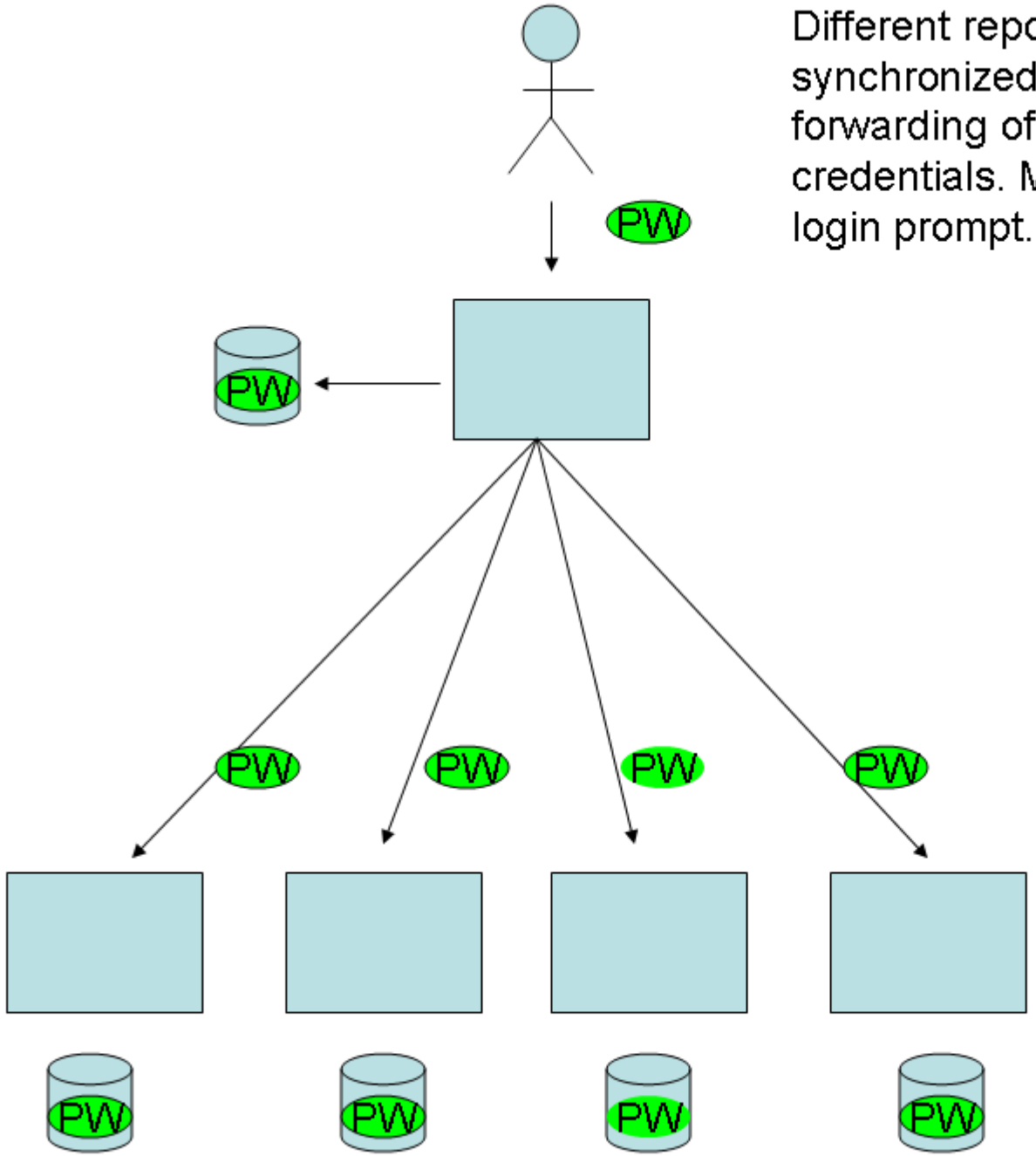
SSO-Variations

Or: pick your own SSO

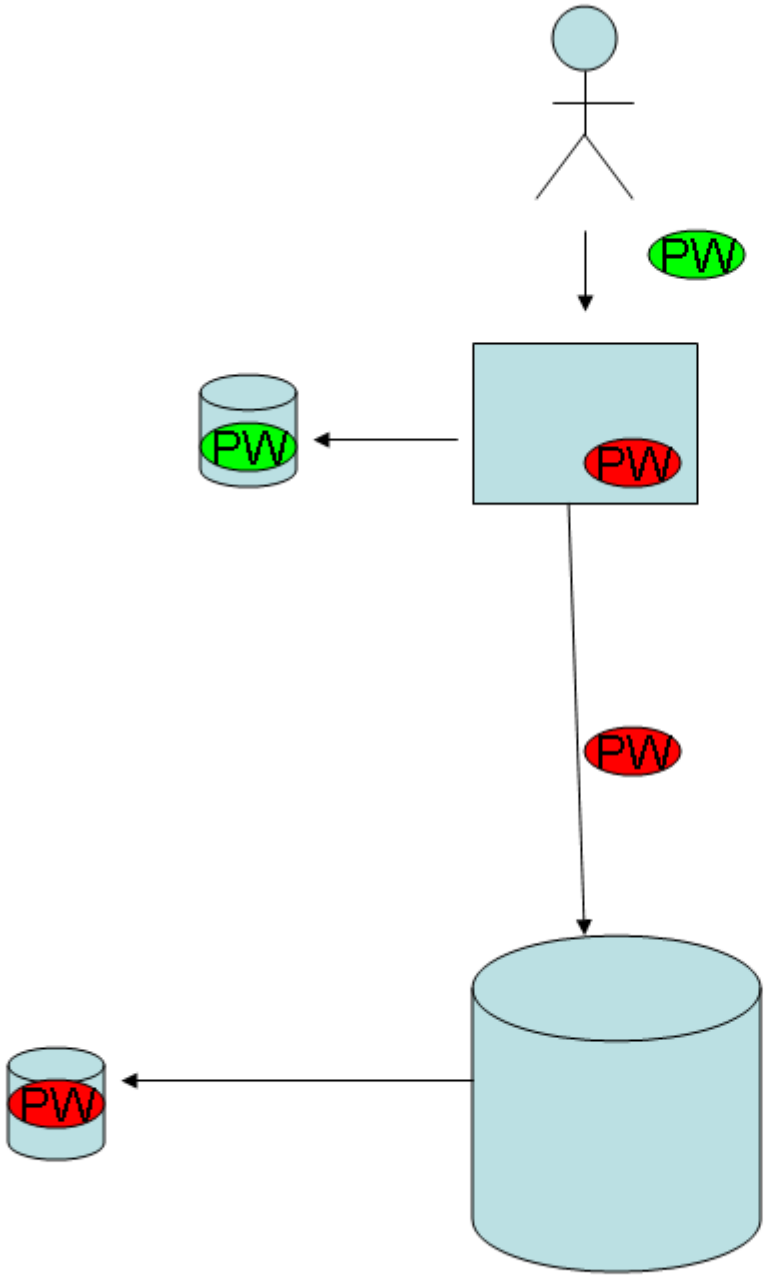
no SSO

Different repositories, passwords and many prompts

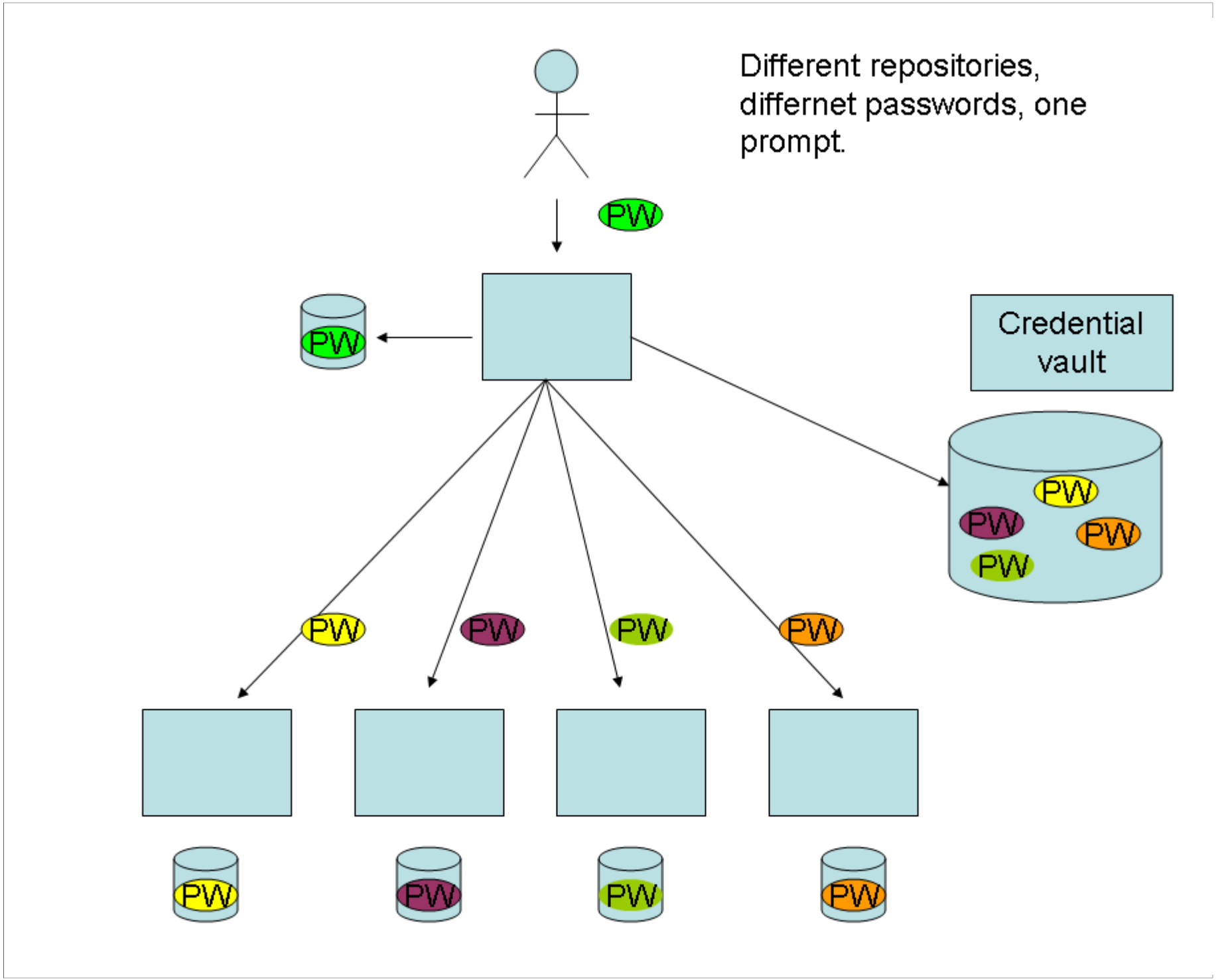


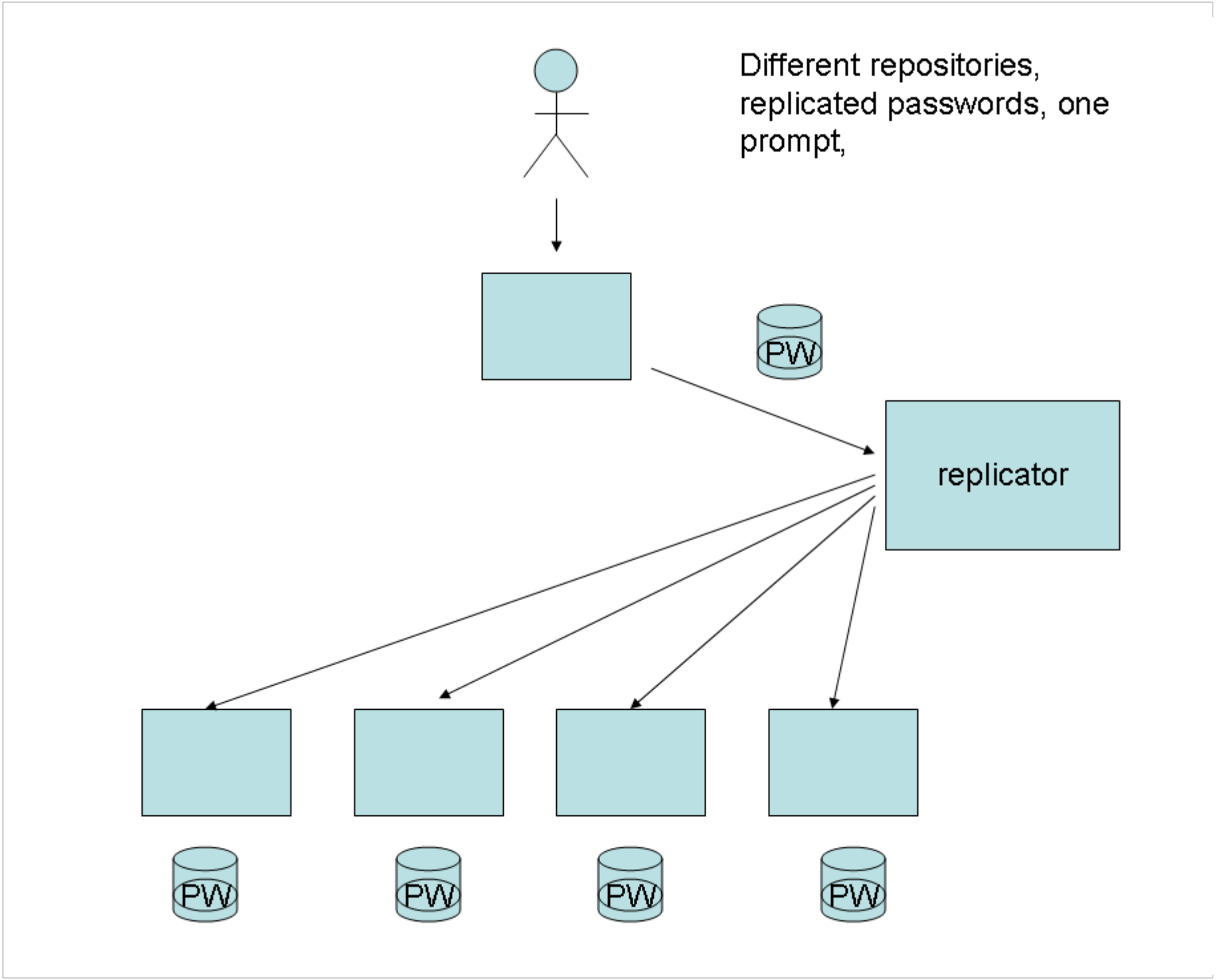


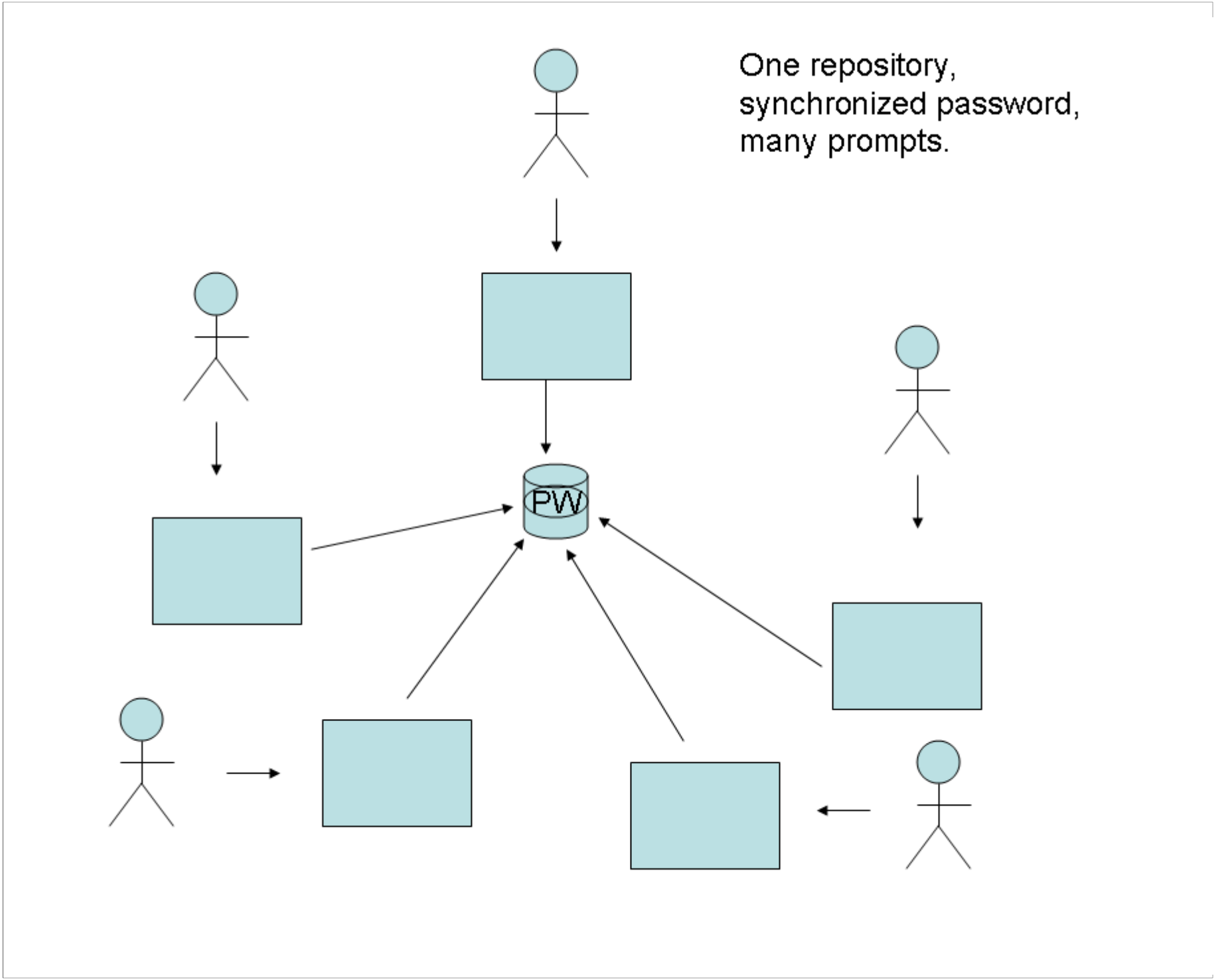
Different repositories, synchronized passwords, forwarding of authentication credentials. Many or one login prompt.

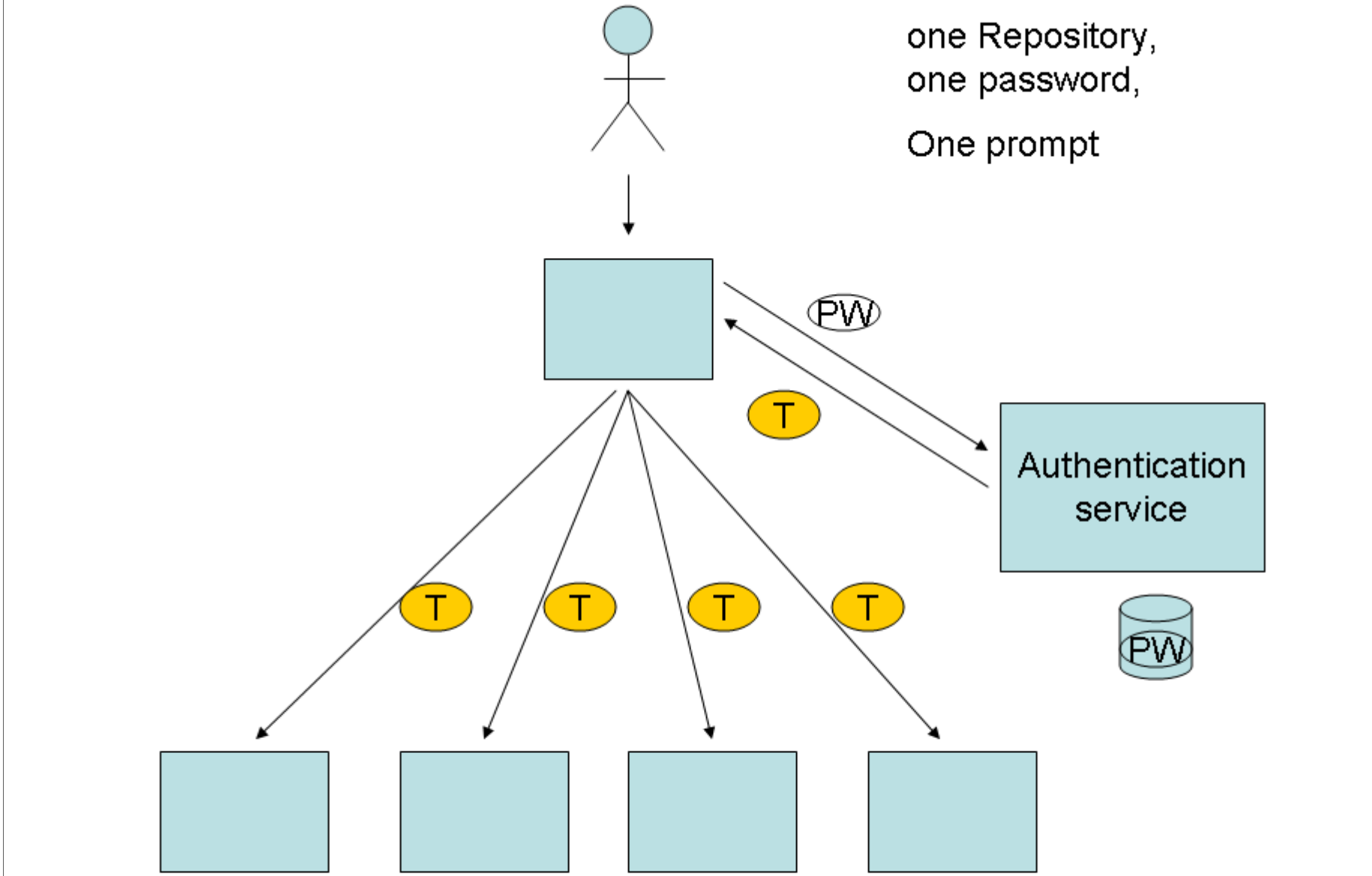


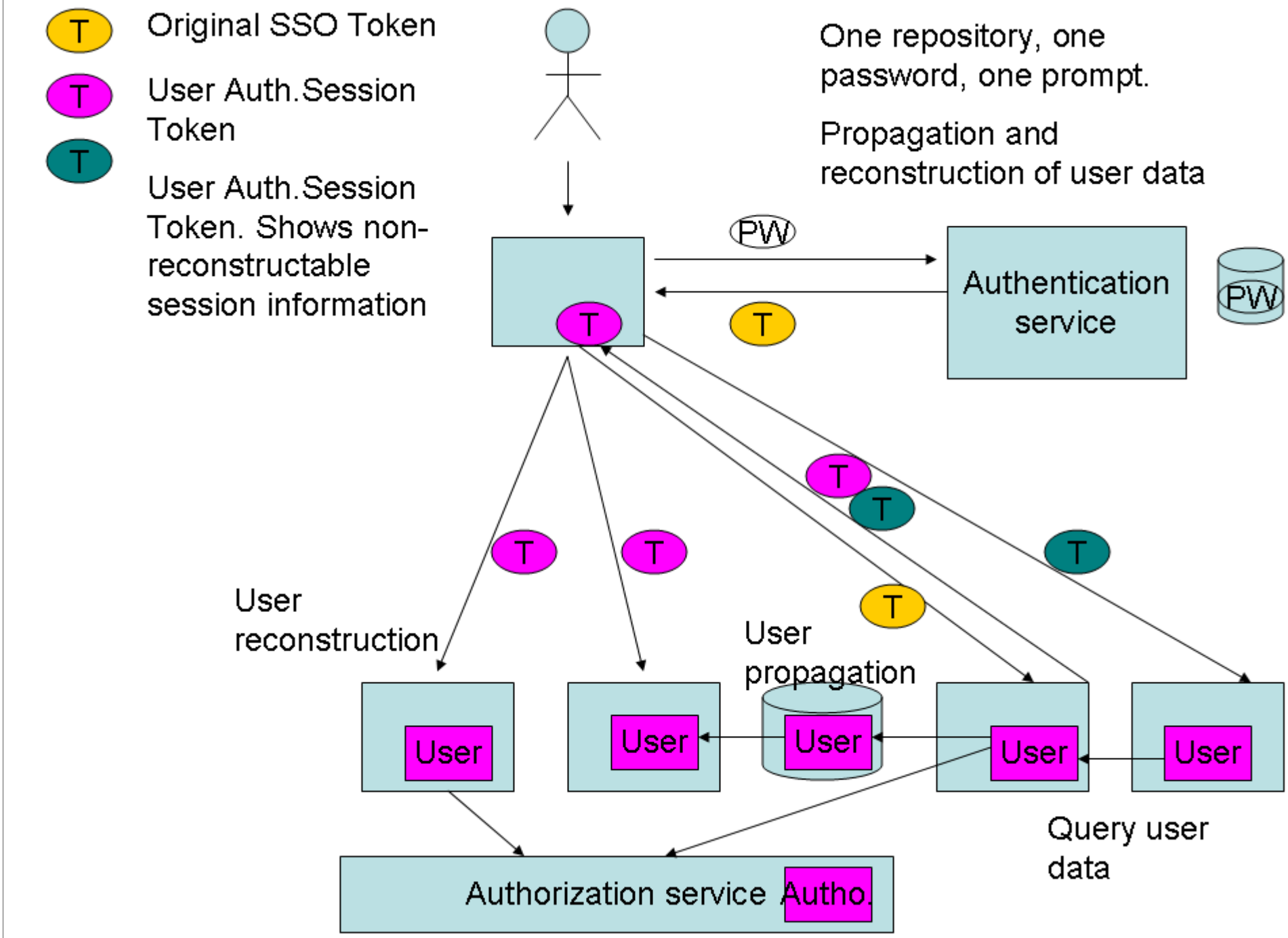
Different repositories, one user prompt, use of a functional user with fixed password

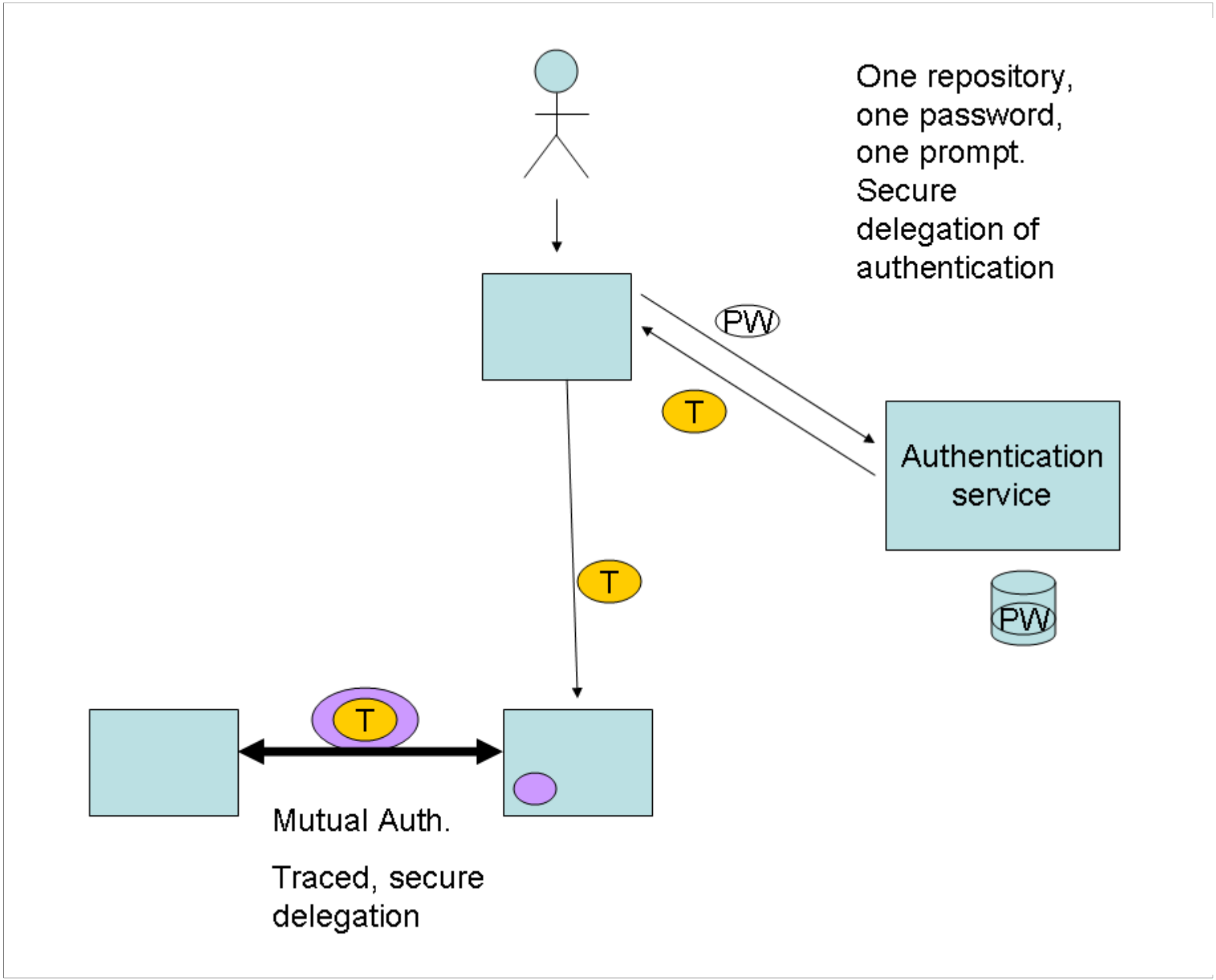

Different repositories, differnet passwords, one prompt.
PW
PW
Credential vault
PW
PW
PW
PW
PW
PW
PW
PW
PW
PW
PW


Different repositories, replicated passwords, one prompt,
PW
replicator
PW
PW
PW
PW

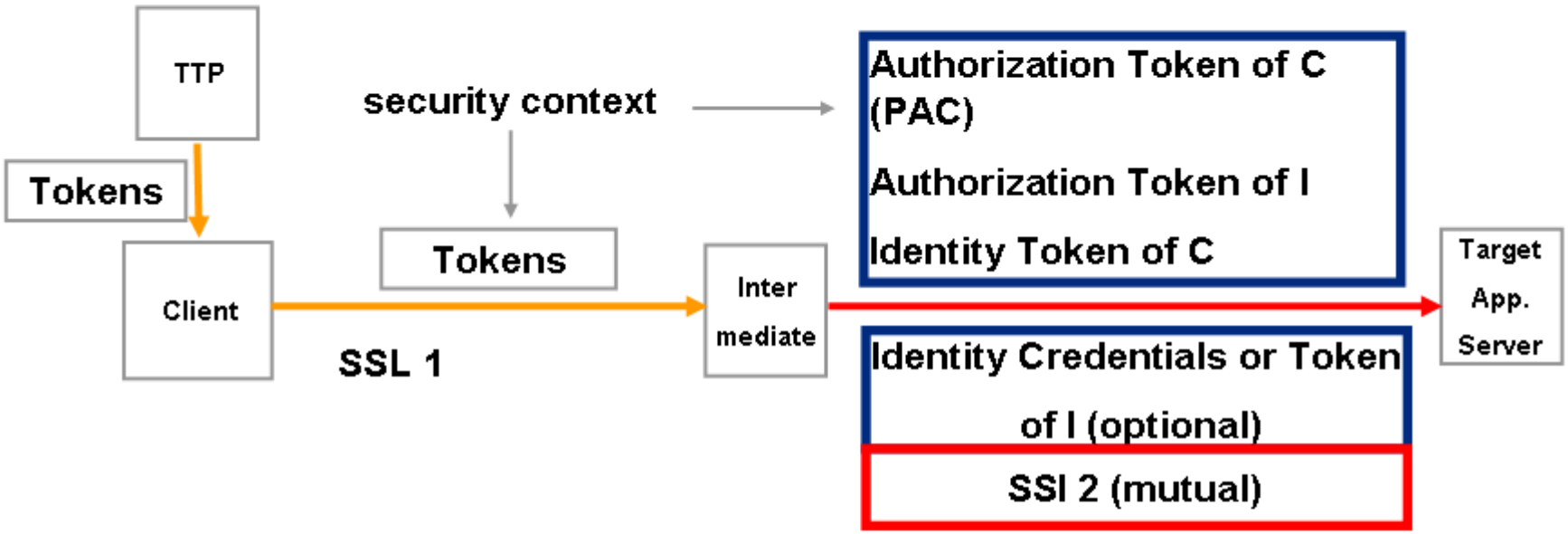

One repository,
synchronized password,
many prompts.
PW


one Repository,
one password,
One prompt
PW
T
Authentication service
T
T
T
T
PW


T
Original SSO Token
T
User Auth.Session Token
T
User Auth.Session Token. Shows non-reconstructable session information
One repository, one password, one prompt.
Propagation and reconstruction of user data
PW
Authentication service
PW
T
T
T
T
T
T
T
T
User reconstruction
User propagation
User
User
User
User
User
Authorization service
Autho.
Query user data


One repository,
one password,
one prompt.
Secure
delegation of
authentication
PW
T
Authentication
service
PW
T
T
Mutual Auth.
Traced, secure
delegation

CORBA CSIv2 Mechanism



Mobile Security

Slides from Jürgen Butz

- Mobile Endgeräte
  - Laptop
  - PDA
  - Smartphone
  - Mobiltelefon

- Aktive Datenspeichergeräte
  - IPod, portable Playstation,
  - USB-Mp3-Player

- Passive Datenspeichergeräte
  - Diskette
  - USB-Stick
  - CD/DVD

- Andere mobile Geräte
- z.B. Handscanner, Drucker, Keylogger usw.

Aus: Jürgen Butz, Sicherheitsaspekte mobiler Geräte, [Butz07]

- Mobile Geräte werden oft in Taxen vergessen was folgende Statistik belegt:

  Global Survey of 900 Taxi Drivers

  Based on the large size of the Chicago company's fleet, the statistics indicate a staggering 85,619 mobile phones, 21,460 PDAs/Pocket PCs, and 4,425 laptops left in the firm's licensed cabs during the six months covered in the study. Only London, with 0.21 laptop PCs lost per cab versus the Chicago firm's 0.18, was higher in any category.

  [Quelle: Pointsec: Global Survey of 900 taxi drivers – Mai 2006]

- Laut einer Analyse von Gartner sind 57% aller erfolgreichen Netzwerkangriffe auf einen Notebook-Diebstahl zurückzuführen

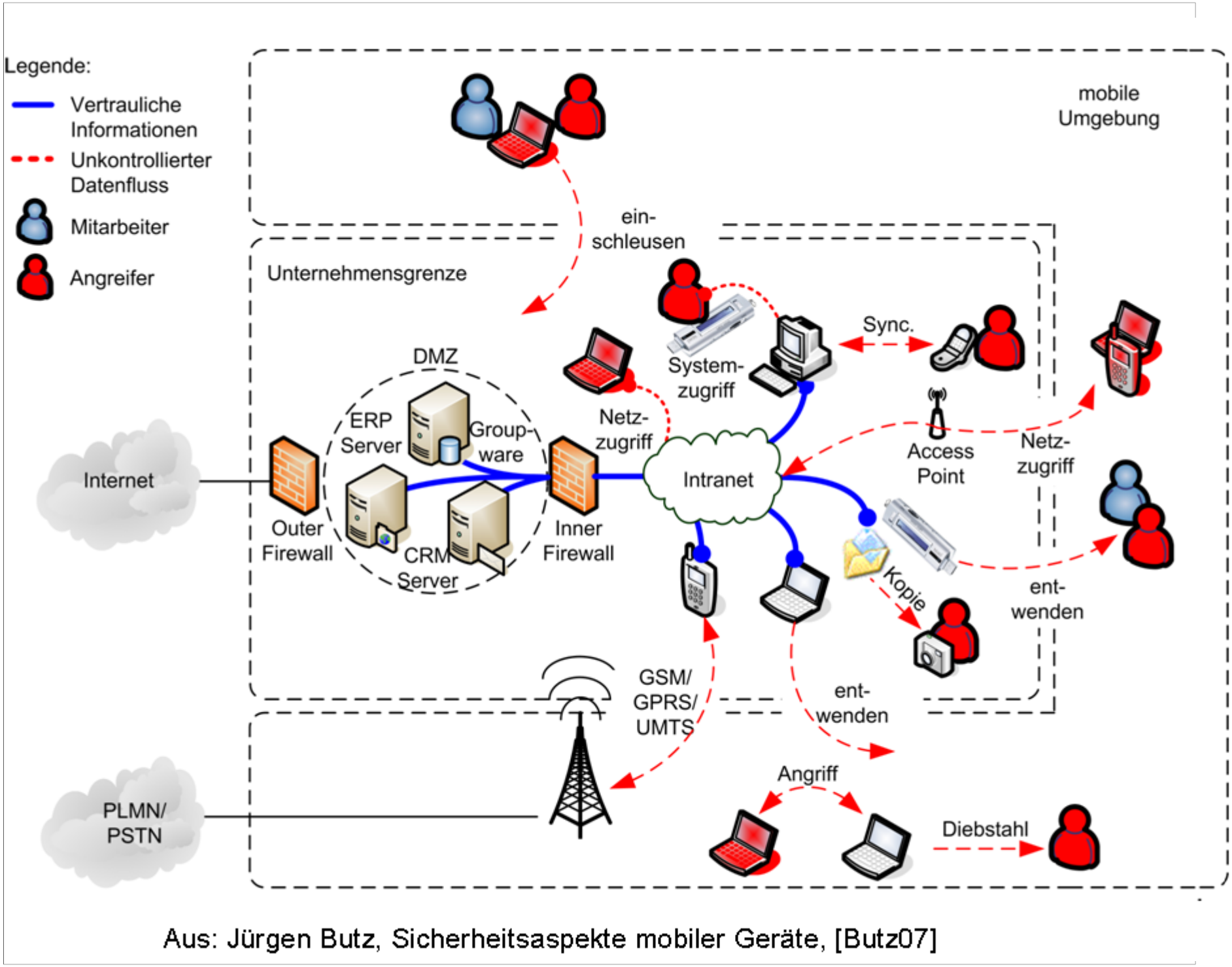
  [Quelle: ix-Extra 10/2006]

- USB-Sticks von US-Armee entwendet

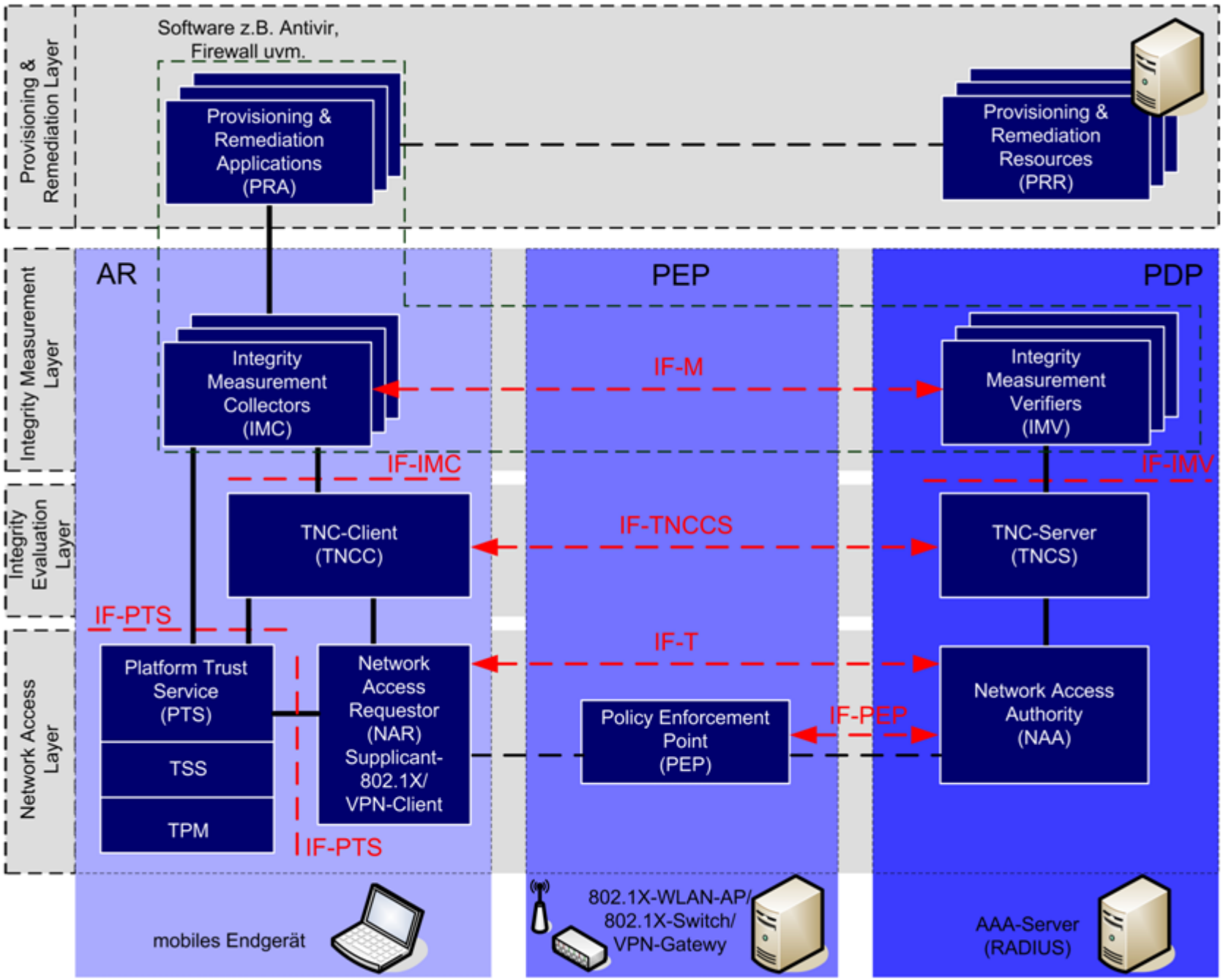
[Quelle: http://www.n24.de/wirtschaft/multimedia/index.php/n20060418102128000002]

➡ Schutz *der* mobilen Geräten!

Aus: Jürgen Butz, Sicherheitsaspekte mobiler Geräte, [Butz07]



Aus: Jürgen Butz, Sicherheitsaspekte mobiler Geräte, [Butz07]



Aus: Jürgen Butz, Sicherheitsaspekte mobiler Geräte, [Butz07]

Erweiterungsschnittstellen

SD/IO Adapter:

WLAN, Bluetooth, Modem, Kammera, Scanner, Audio Aufnahmegerät

CF Adapter:

WLAN, analoges Modem, PCMCIA

PCMCIA Karte:

serieller Schnittstelle, Ethernet LAN Adapters, Bluetooth cards, ISDN-Modem Cards, Brenner, Speicherkarten Adapter, GSM, GPRS, UMTS

USB Host Adapter:

S-ATA, Festplatten, Brenner Anschluss, Bluetooth, IrDA

RS232 Adapter:

Bluetooth, Modems, RJ45 LAN, WLAN

Aus: Jürgen Butz, Sicherheitsaspekte mobiler Geräte, [Butz07]

Virtual Organizations

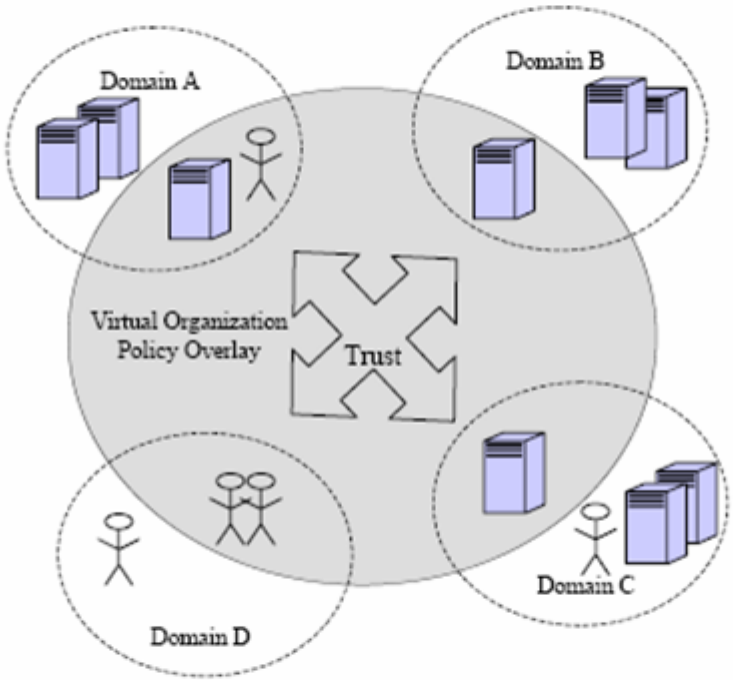


Figure 1. A virtual organization policy domain overlay pulls together participants from disparate domains into a common trust domain.

From: globus.org

Latest Trends: Cloud Security

- Infrastructure as a Service
- Plattform as a Service
- Software as a Service.

Possible security problems between:

-Client and cloud provider (data theft and loss, processing exposure, availability)

-Between clients (isolation problems with VMs, availability and performance, covered channel exposures)

- Cloud provider and cloud provider?

- Client and outside victims (DDOS)

Master Topics:

- Securing Servers
- Code Access Security
- Isolation with capabilities
- Object based infrastructure security
- Plattform security with inversion of control
- Virtualization and security
- Secure languages and code