Security Analysis

Security Analysis

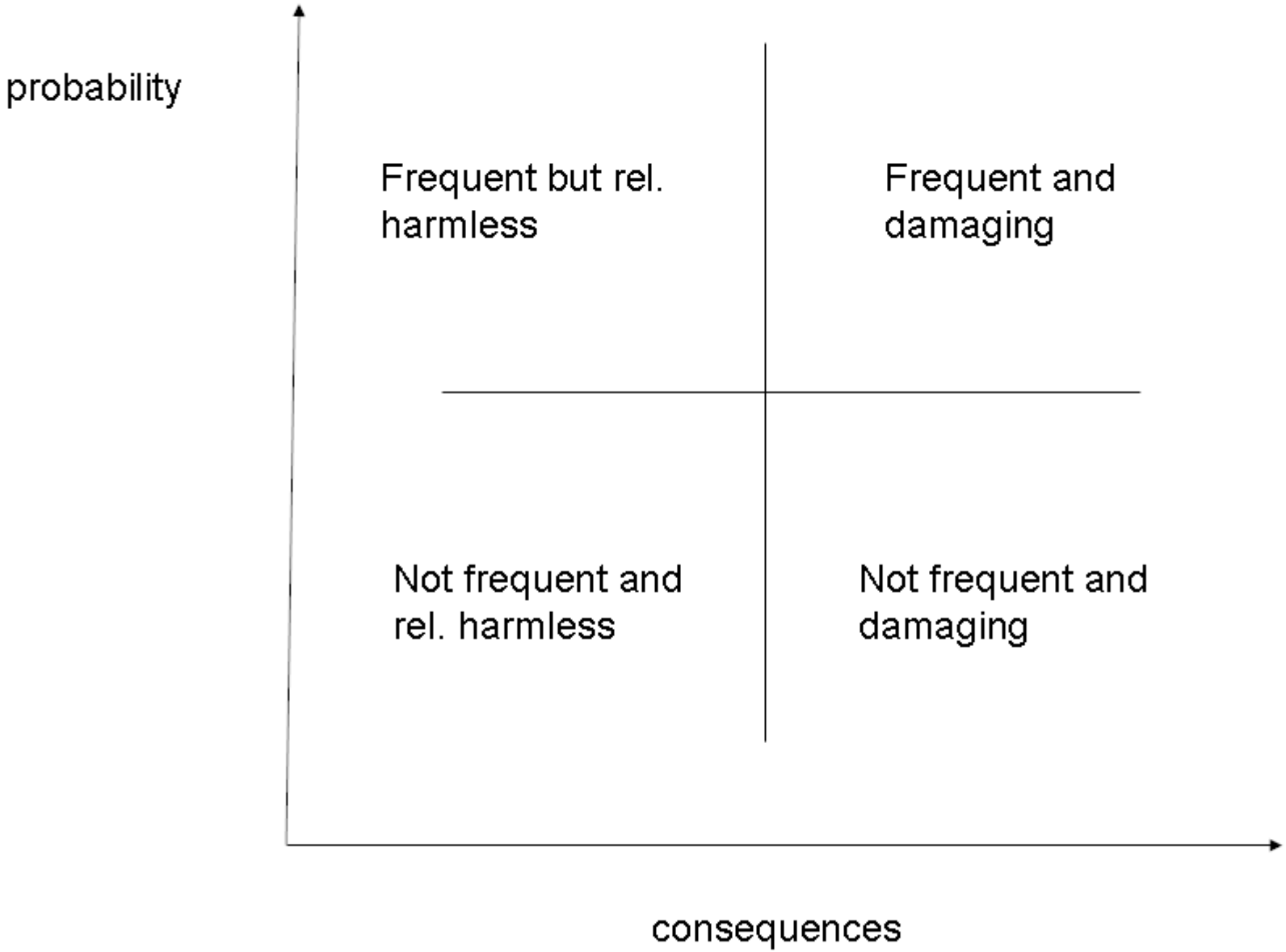
Principles, Failure Analysis and Architectural Validation

Overview

1. Basic Principles of Security Analysis (risc, concepts and threat models, topologies and architecture, connectivity, people problem)
2. Analysis of Failures (Societe General, OBSOC, Cisco)
3. Architectural Validation (Observation System, Enterprise Search Plattform)

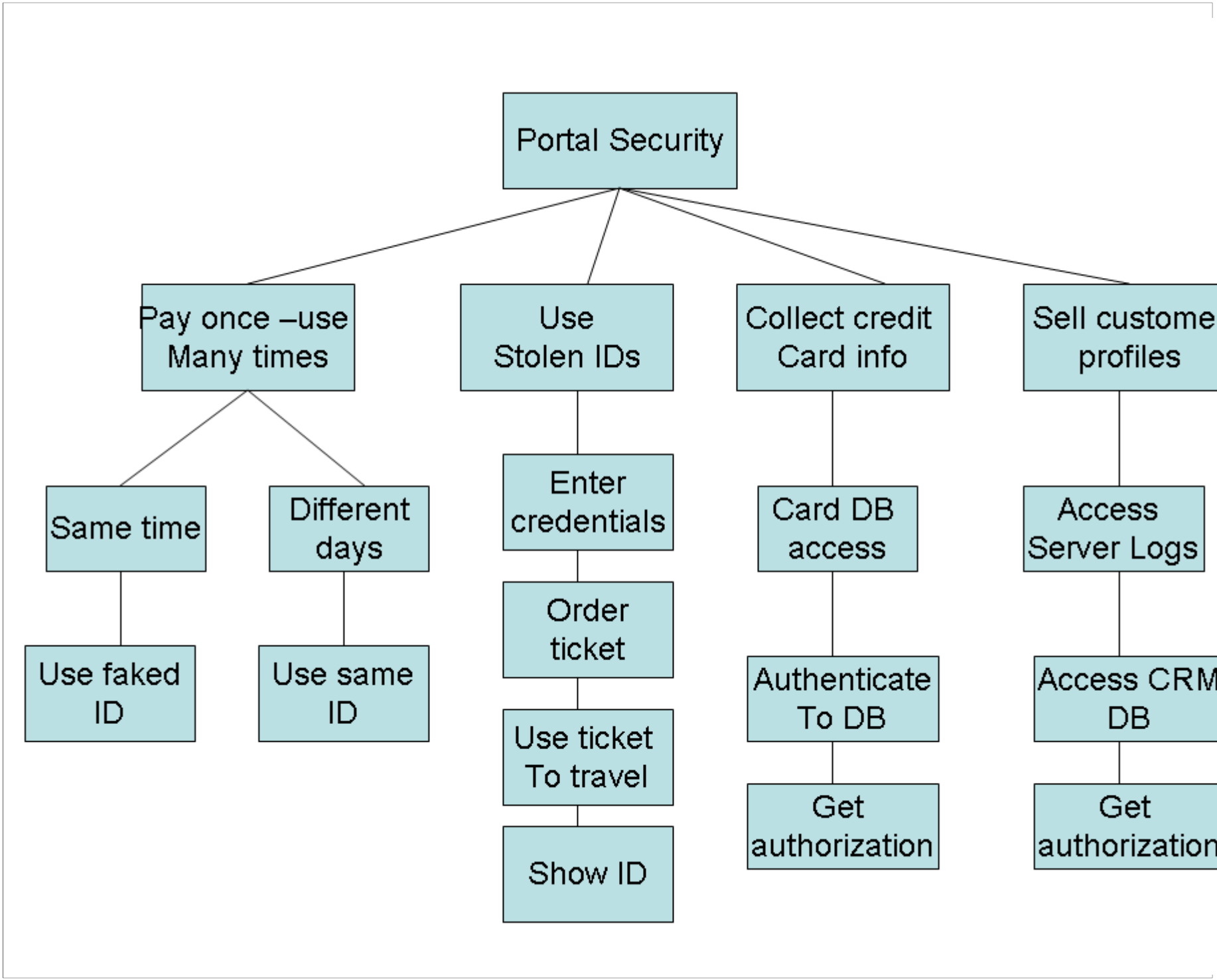
Basic Principles of Security Analysis

- Risk and Risk Analysis


probability
Frequent but rel. harmless
Frequent and damaging
Not frequent and rel. harmless
Not frequent and damaging
consequences

Threat	Frequence	Damage	Result
Forged tickets	Rare	small	Accept risc
Stolen Cards	More often	Small	Accept risc
DOS Attack on Service	Frequent	Small	Accept risc

Attack	Attacker	Difficulty	Gain	Risc	Priority
Forged ticket	anybody	easy	Small	high	low
DOS	Script kiddy	Easy	None/ fame	High	high
Stolen ID	Professional	Medium	Small	medium	medium

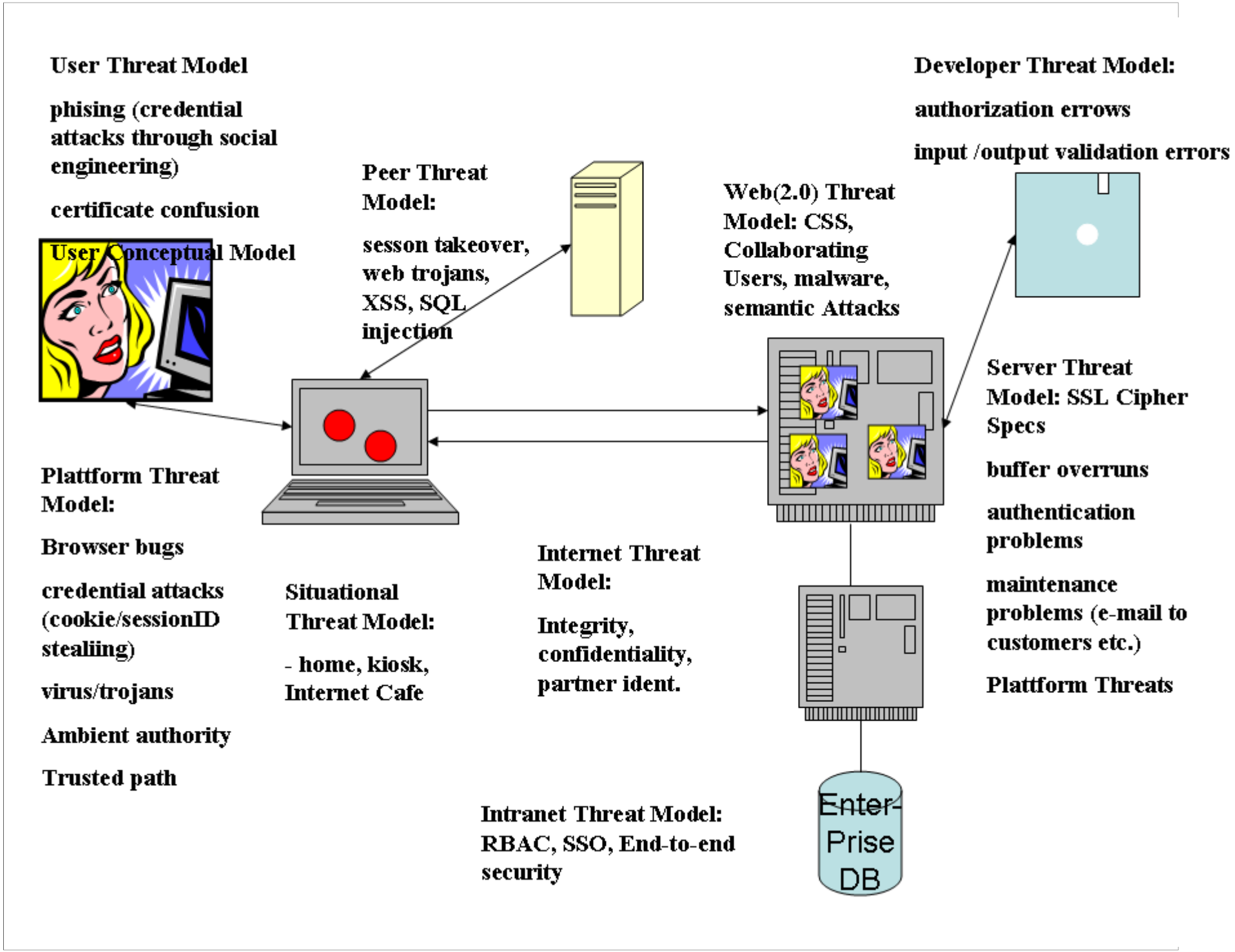

Portal Security
Pay once –use Many times
Use Stolen IDs
Collect credit Card info
Sell customer profiles
Same time
Different days
Enter credentials
Card DB access
Access Server Logs
Use faked ID
Use same ID
Order ticket
Authenticate To DB
Access CRM DB
Use ticket To travel
Get authorization
Get authorization
Show ID

Security Meta-Pattern

- Spatial Transformation of things (mobility, ownership)
- Moral Transformations of Participants (from employee to attacker)
- ?

Basic Principles of Security Analysis

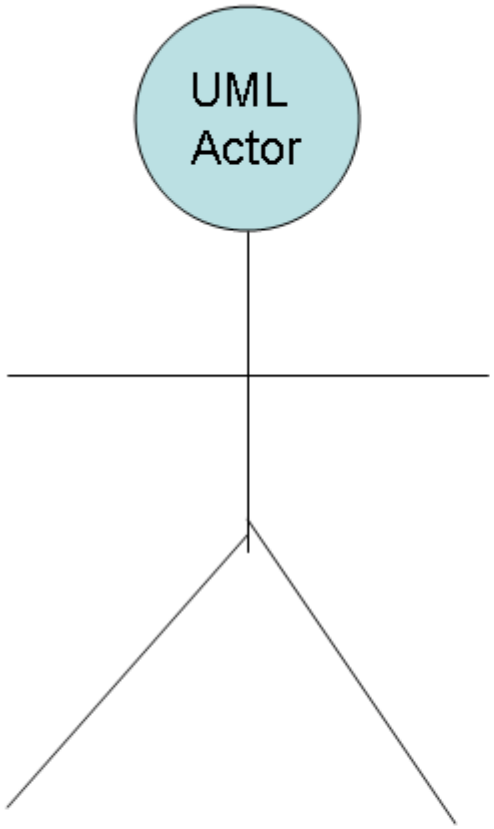
- Threat Models


User Threat Model
phising (credential attacks through social engineering)
certificate confusion
User Conceptual Model
Peer Threat Model:
sesson takeover, web trojans, XSS, SQL injection
Developer Threat Model:
authorization errows
input /output validation errors
Web(2.0) Threat Model: CSS, Collaborating Users, malware, semantic Attacks
Server Threat Model: SSL Cipher Specs
buffer overruns
authentication problems
maintenance problems (e-mail to customers etc.)
Plattform Threats
Plattform Threat Model:
Browser bugs
credential attacks (cookie/sessionID stealiing)
virus/trojans
Ambient authority
Trusted path
Situational Threat Model:
- home, kiosk, Internet Cafe
Internet Threat Model:
Integrity, confidentiality, partner ident.
Intranet Threat Model:
RBAC, SSO, End-to-end security
Enter-Prise DB

User Conceptual Models

New Design Patterns for Representation of Security Information needed

The „Personal Message“ is ALL a user has to guarantee that the message is from VISA. It could still be a MIM attack but I doubt that most user will even understand the importance of this field.



Humanity seen by IT

-No sex

-No age

-No culture

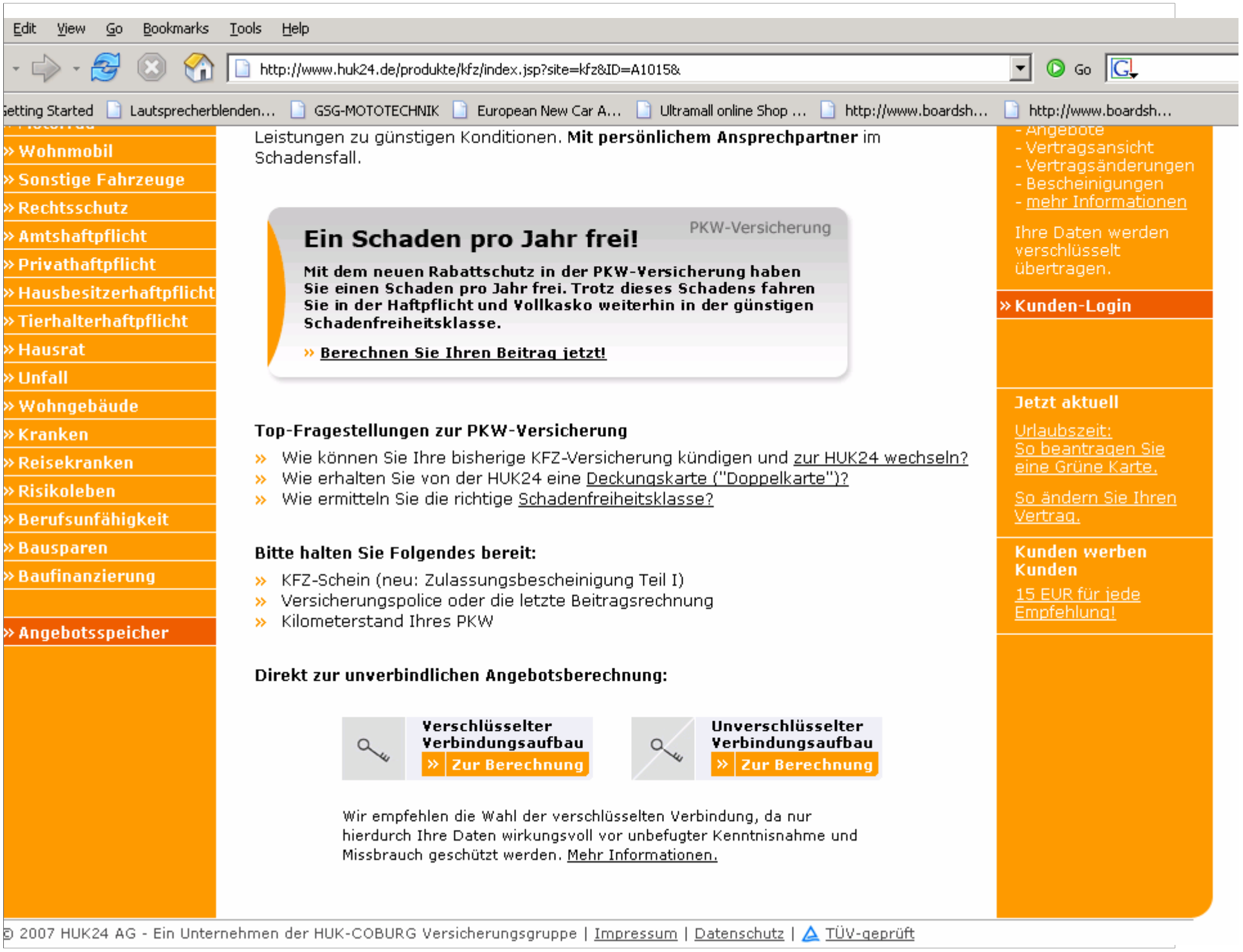
-No education

-No situation

-No mood

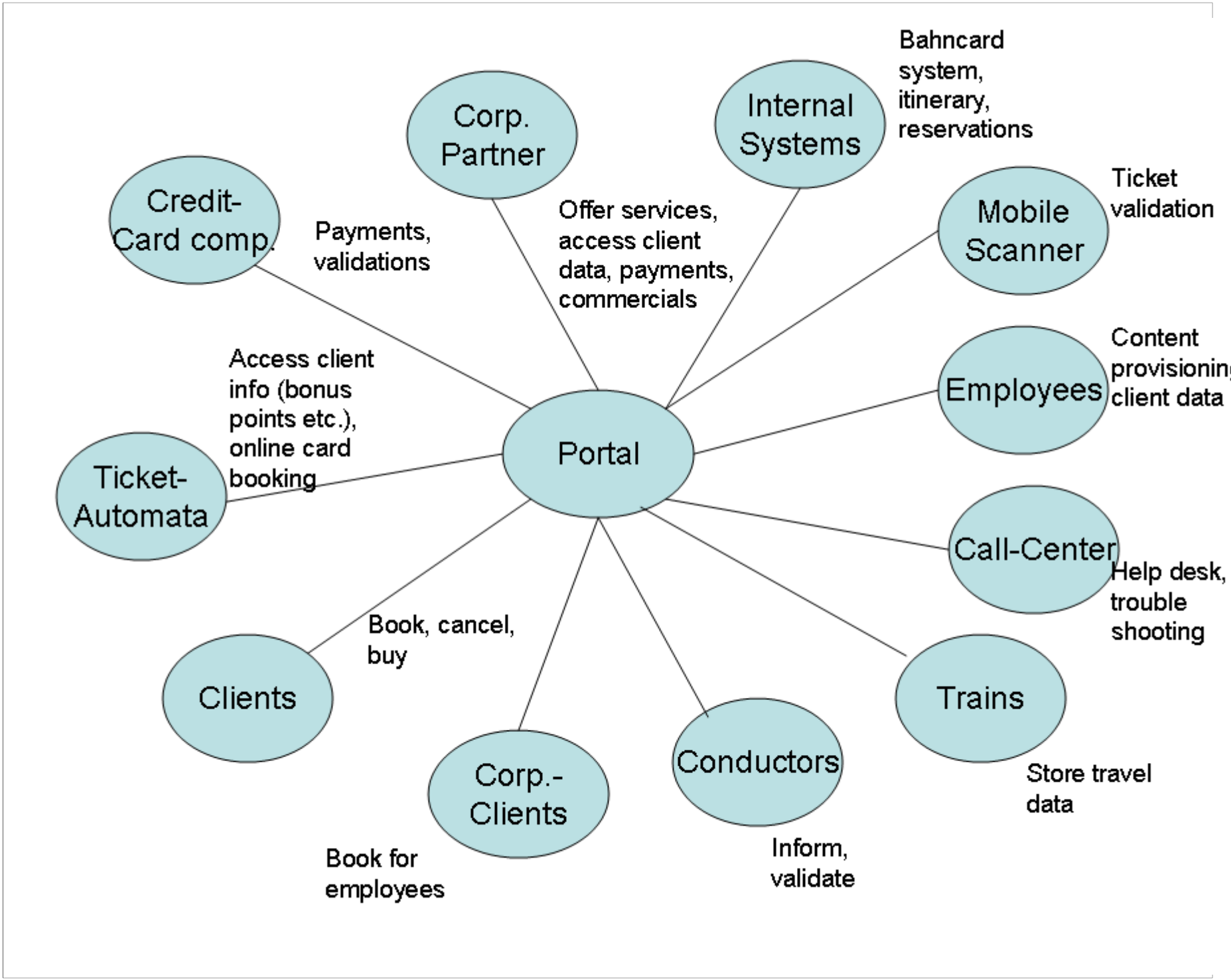
-No preferences

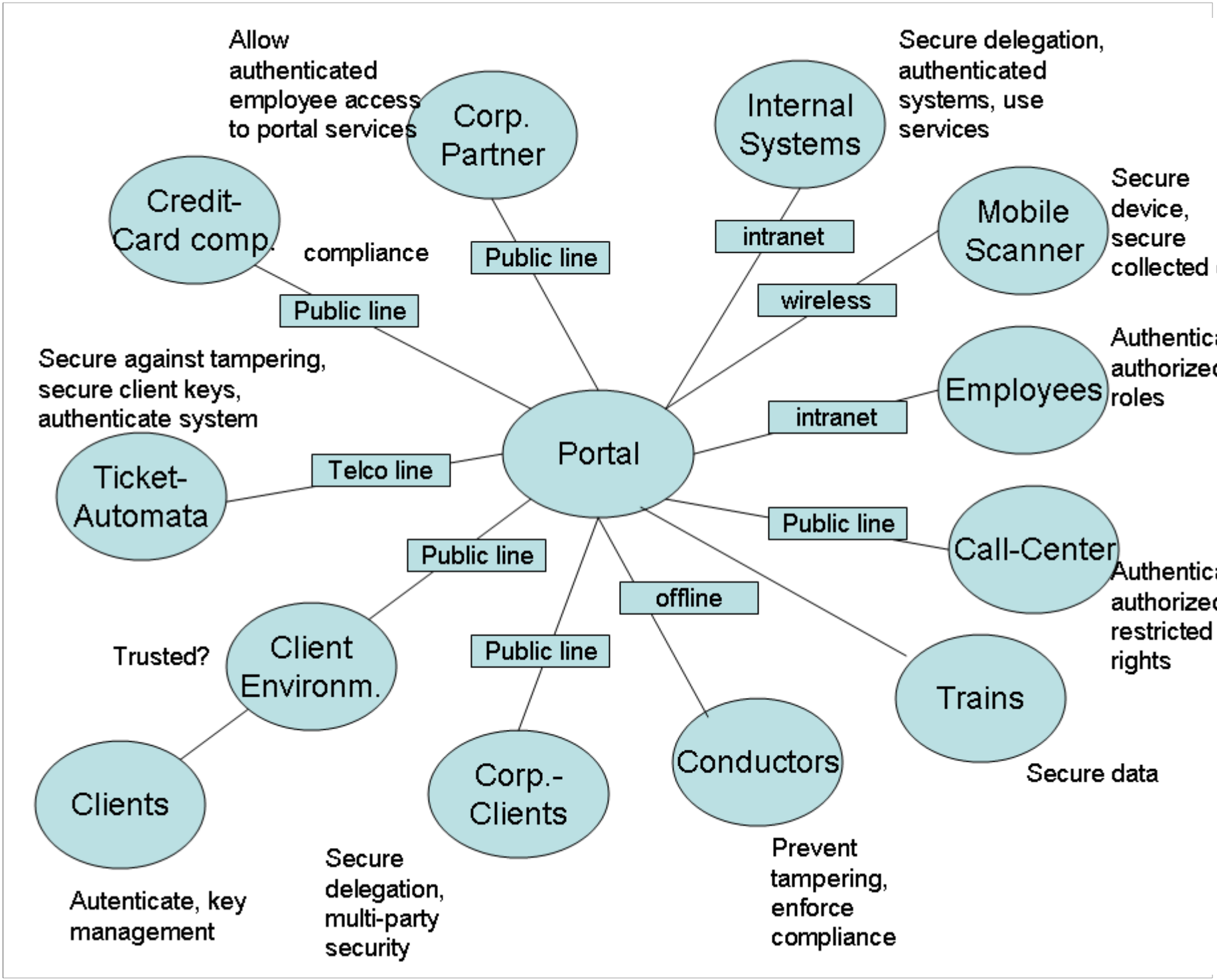
And so on…

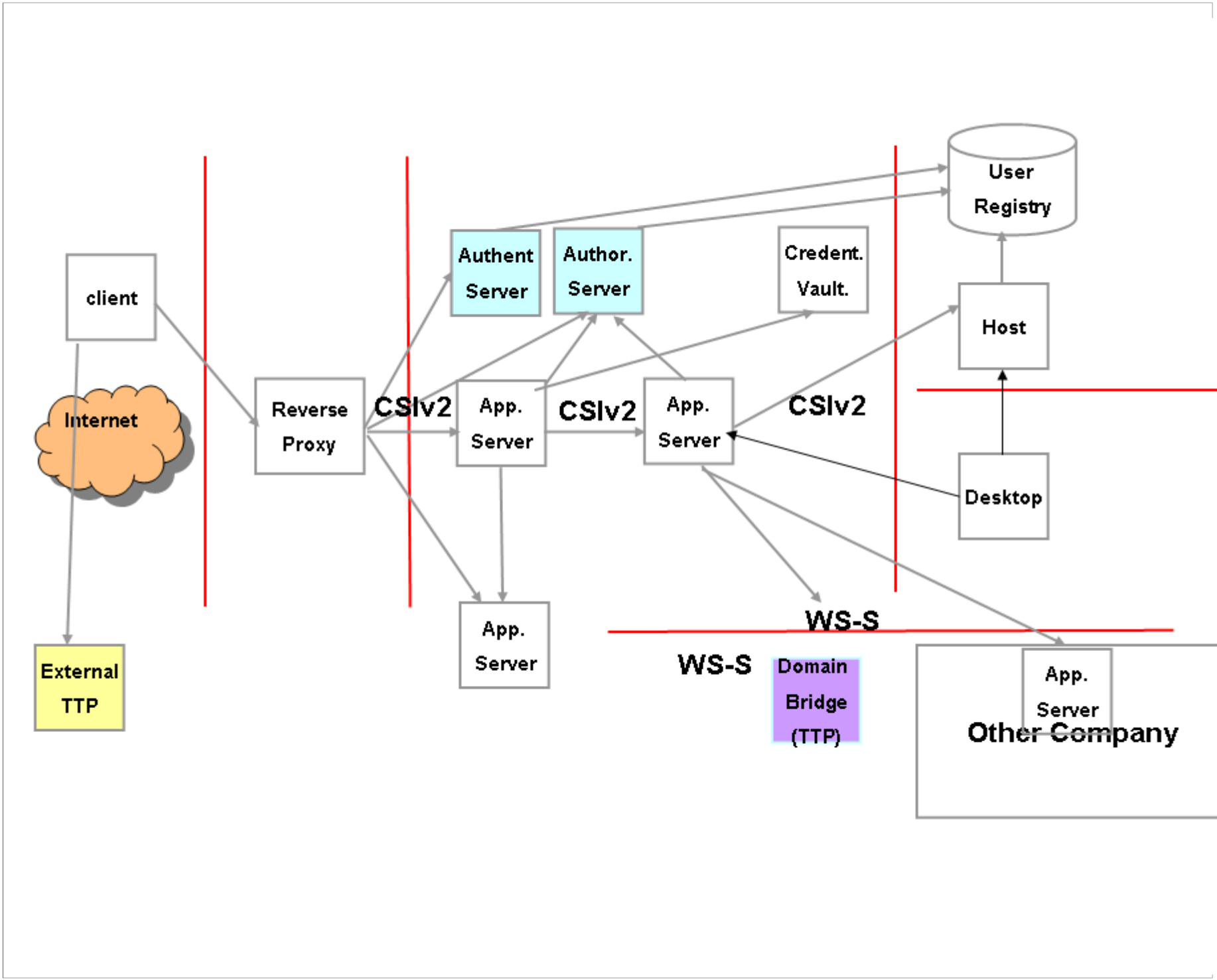

Edit View Go Bookmarks Tools Help
http://www.huk24.de/produkte/kfz/index.jsp?site=kfz&ID=A1015&
Go
Getting Started
Lautsprecherblenden...
GSG-MOTOTECHNIK
European New Car A...
Ultramall online Shop ...
http://www.boardsh...
http://www.boardsh...
» Wohnmobil
» Sonstige Fahrzeuge
» Rechtsschutz
» Amtshaftpflicht
» Privathaftpflicht
» Hausbesitzerhaftpflicht
» Tierhalterhaftpflicht
» Hausrat
» Unfall
» Wohngebäude
» Kranken
» Reisekranken
» Risikoleben
» Berufsunfähigkeit
» Bausparen
» Baufinanzierung
» Angebotsspeicher
Leistungen zu günstigen Konditionen. Mit persönlichem Ansprechpartner im Schadensfall.
PKW-Versicherung
Ein Schaden pro Jahr frei!
Mit dem neuen Rabattschutz in der PKW-Versicherung haben Sie einen Schaden pro Jahr frei. Trotz dieses Schadens fahren Sie in der Haftpflicht und Vollkasko weiterhin in der günstigen Schadenfreiheitsklasse.
» Berechnen Sie Ihren Beitrag jetzt!
Top-Fragestellungen zur PKW-Versicherung
» Wie können Sie Ihre bisherige KFZ-Versicherung kündigen und zur HUK24 wechseln?
» Wie erhalten Sie von der HUK24 eine Deckungskarte ("Doppelkarte")?
» Wie ermitteln Sie die richtige Schadenfreiheitsklasse?
Bitte halten Sie Folgendes bereit:
» KFZ-Schein (neu: Zulassungsbescheinigung Teil I)
» Versicherungspolice oder die letzte Beitragsrechnung
» Kilometerstand Ihres PKW
Direkt zur unverbindlichen Angebotsberechnung:
Verschlüsselter Verbindungsaufbau
» Zur Berechnung
Unverschlüsselter Verbindungsaufbau
» Zur Berechnung
Wir empfehlen die Wahl der verschlüsselten Verbindung, da nur hierdurch Ihre Daten wirkungsvoll vor unbefugter Kenntnisnahme und Missbrauch geschützt werden. Mehr Informationen.
- Angebote
- Vertragsansicht
- Vertragsänderungen
- Bescheinigungen
- mehr Informationen
Ihre Daten werden verschlüsselt übertragen.
» Kunden-Login
Jetzt aktuell
Urlaubszeit: So beantragen Sie eine Grüne Karte.
So ändern Sie Ihren Vertrag.
Kunden werben Kunden
15 EUR für jede Empfehlung!
© 2007 HUK24 AG - Ein Unternehmen der HUK-COBURG Versicherungsgruppe | Impressum | Datenschutz | TÜV-geprüft

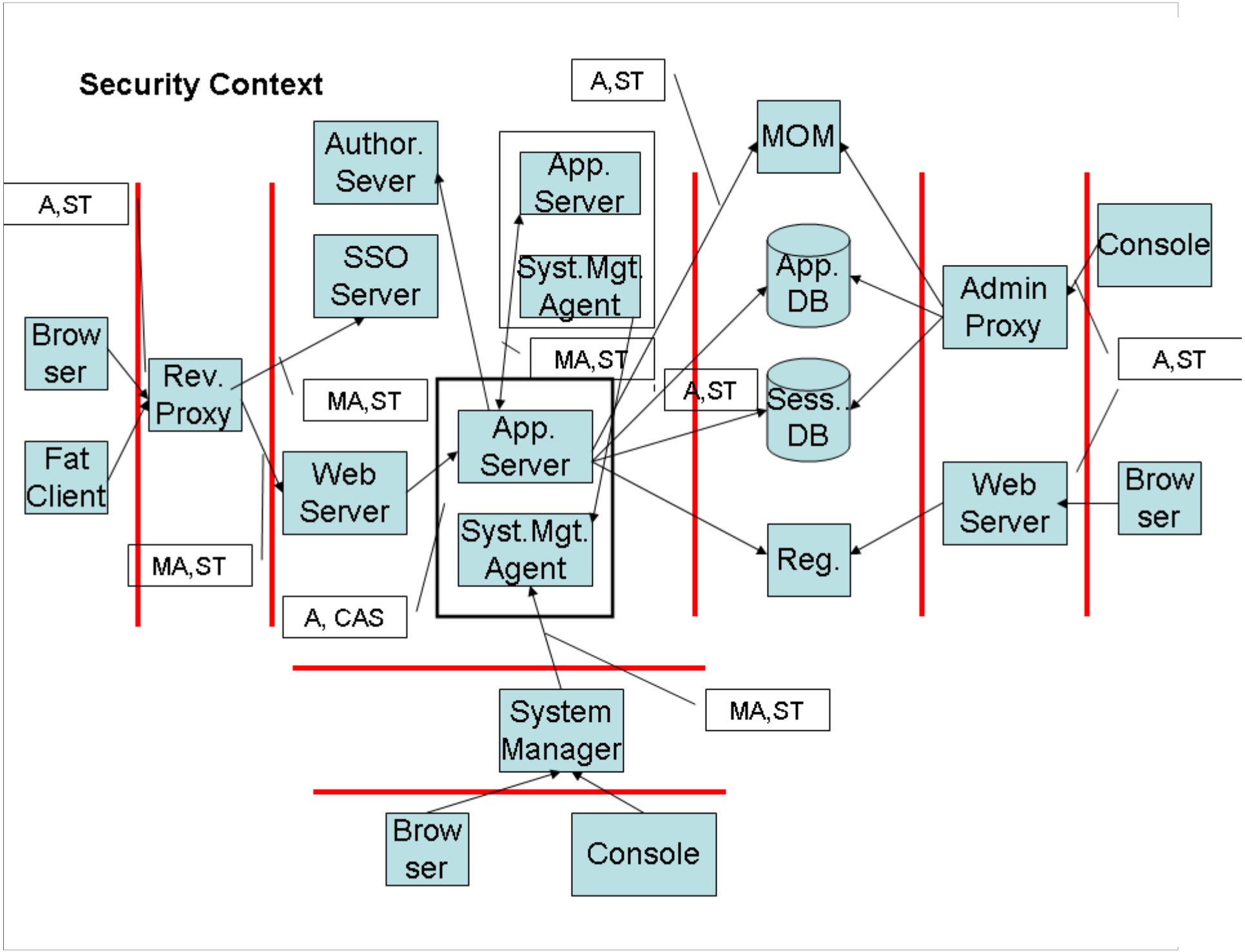
Basic Principles of Security Analysis

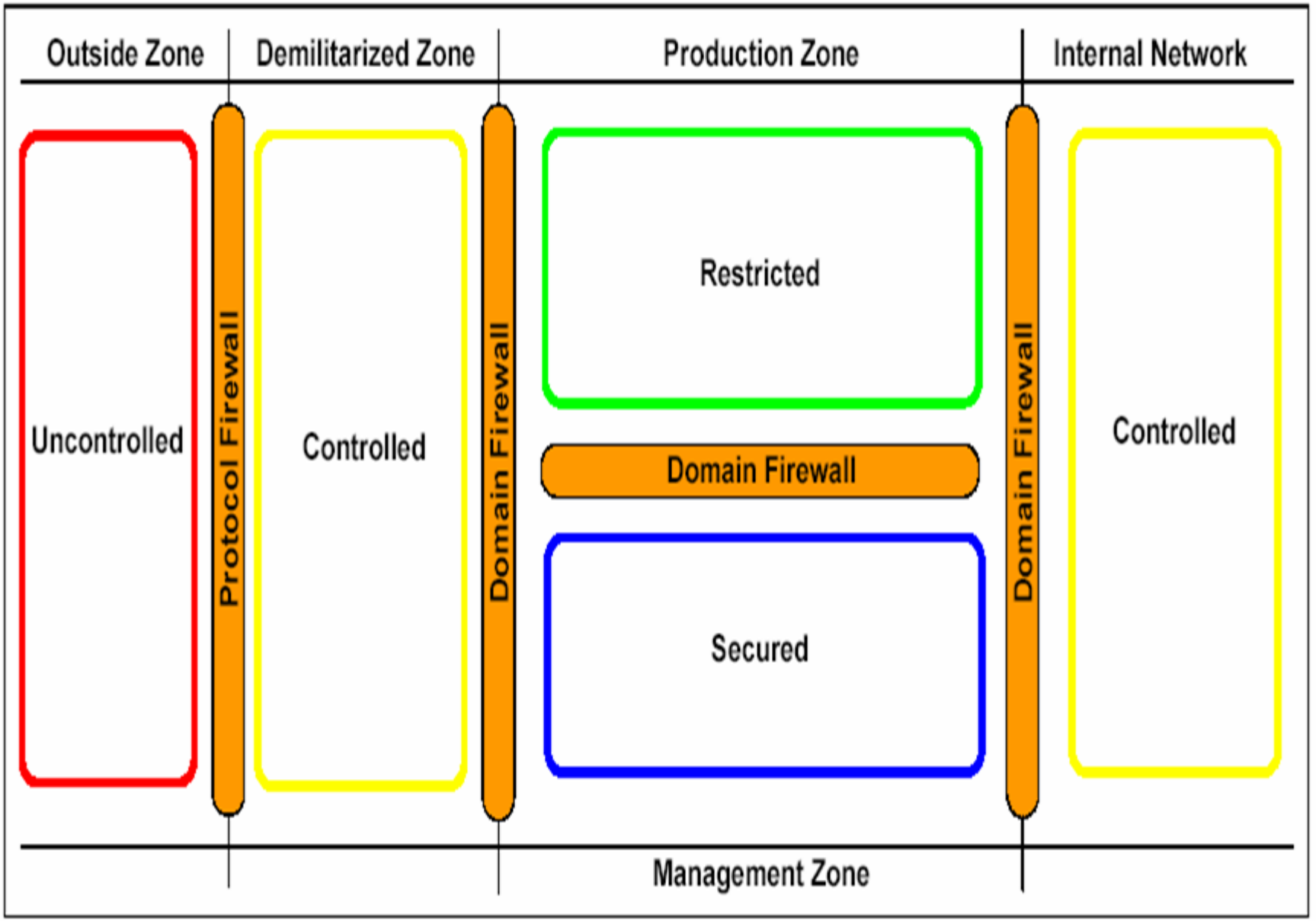
- Topology and Architecture

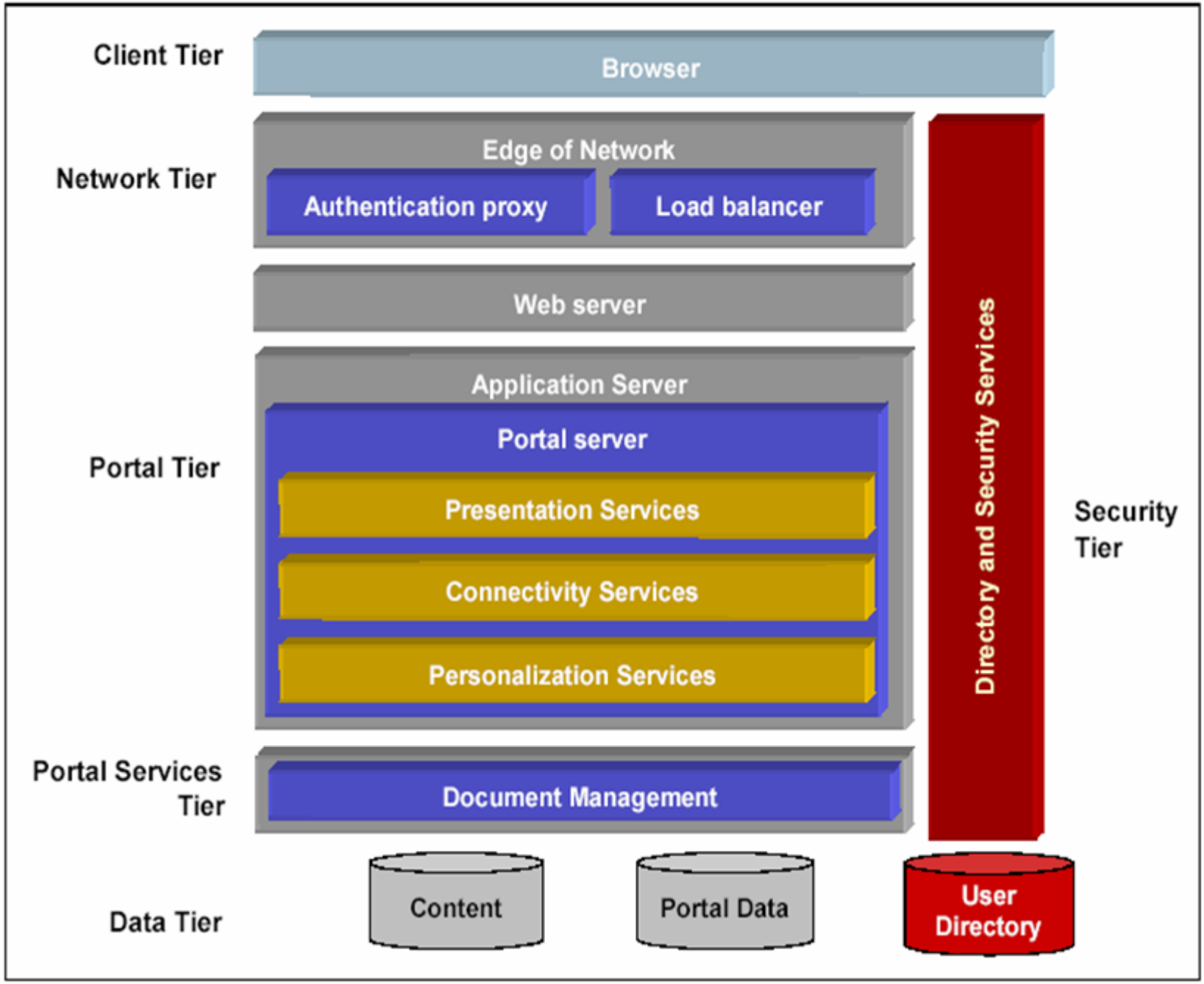

Bahncard system, itinerary, reservations
Corp. Partner
Internal Systems
Credit-Card comp.
Payments, validations
Offer services, access client data, payments, commercials
Mobile Scanner
Ticket validation
Access client info (bonus points etc.), online card booking
Employees
Content provisioning, client data
Ticket-Automata
Portal
Call-Center
Help desk, trouble shooting
Book, cancel, buy
Clients
Trains
Corp.-Clients
Conductors
Store travel data
Book for employees
Inform, validate

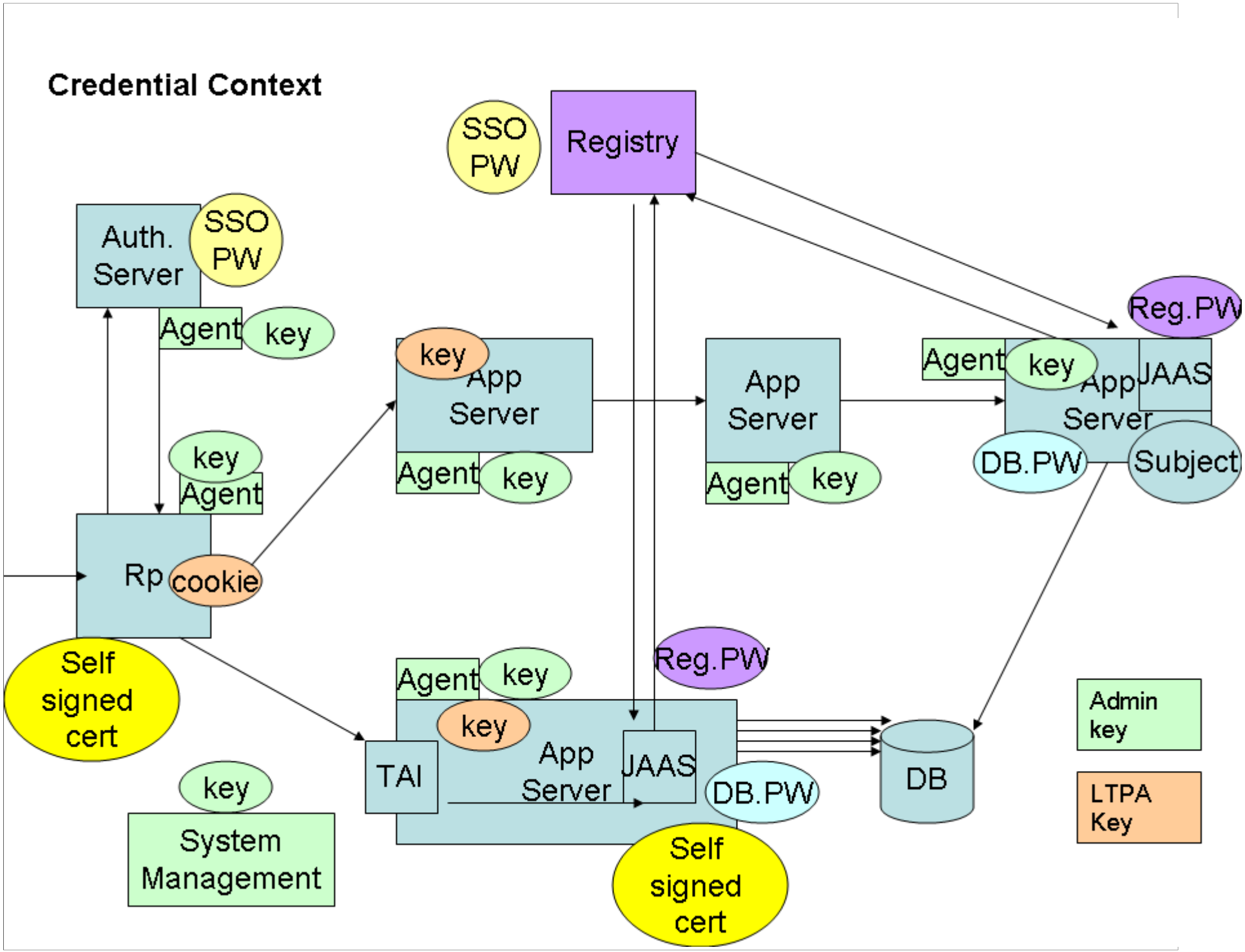

Allow authenticated employee access to portal services
Corp. Partner
Internal Systems
Secure delegation, authenticated systems, use services
Credit-Card comp.
compliance
Public line
Public line
intranet
wireless
Mobile Scanner
Secure device, secure collected data
Secure against tampering, secure client keys, authenticate system
Portal
intranet
Employees
Authenticate, authorized, roles
Ticket-Automata
Telco line
Public line
Public line
Call-Center
Authenticate, authorized, restricted rights
offline
Trusted?
Client Environm.
Public line
Trains
Clients
Corp.-Clients
Conductors
Secure data
Autenticate, key management
Secure delegation, multi-party security
Prevent tampering, enforce compliance


User Registry
Authent Server
Author. Server
Credent. Vault.
client
Host
Internet
Reverse Proxy
CSIv2
App. Server
CSIv2
App. Server
CSIv2
Desktop
App. Server
WS-S
WS-S
Domain Bridge (TTP)
External TTP
App. Server
Other Company


Security Context
A,ST
Author.
Sever
App.
Server
MOM
A,ST
SSO
Server
Syst.Mgt.
Agent
App.
DB
Console
Brow
ser
Rev.
Proxy
MA,ST
Admin
Proxy
A,ST
MA,ST
A,ST
Sess.
DB
Fat
Client
Web
Server
App.
Server
Web
Server
Brow
ser
Syst.Mgt.
Agent
Reg.
MA,ST
A, CAS
System
Manager
MA,ST
Brow
ser
Console


Outside Zone
Demilitarized Zone
Production Zone
Internal Network
Uncontrolled
Protocol Firewall
Controlled
Domain Firewall
Restricted
Domain Firewall
Secured
Domain Firewall
Controlled
Management Zone


Client Tier
Browser
Network Tier
Edge of Network
Authentication proxy
Load balancer
Web server
Portal Tier
Application Server
Portal server
Presentation Services
Connectivity Services
Personalization Services
Portal Services Tier
Document Management
Directory and Security Services
Security Tier
Data Tier
Content
Portal Data
User Directory


Credential Context
SSO PW
Registry
Auth. Server
SSO PW
Agent
key
key
App Server
Agent
key
App Server
Agent
key
Reg.PW
Agent
key
App Server
JAAS
DB.PW
Subject
key
Agent
Rp
cookie
Self signed cert
Agent
key
key
TAI
App Server
JAAS
Reg.PW
DB.PW
DB
key
System Management
Self signed cert
Admin key
LTPA Key

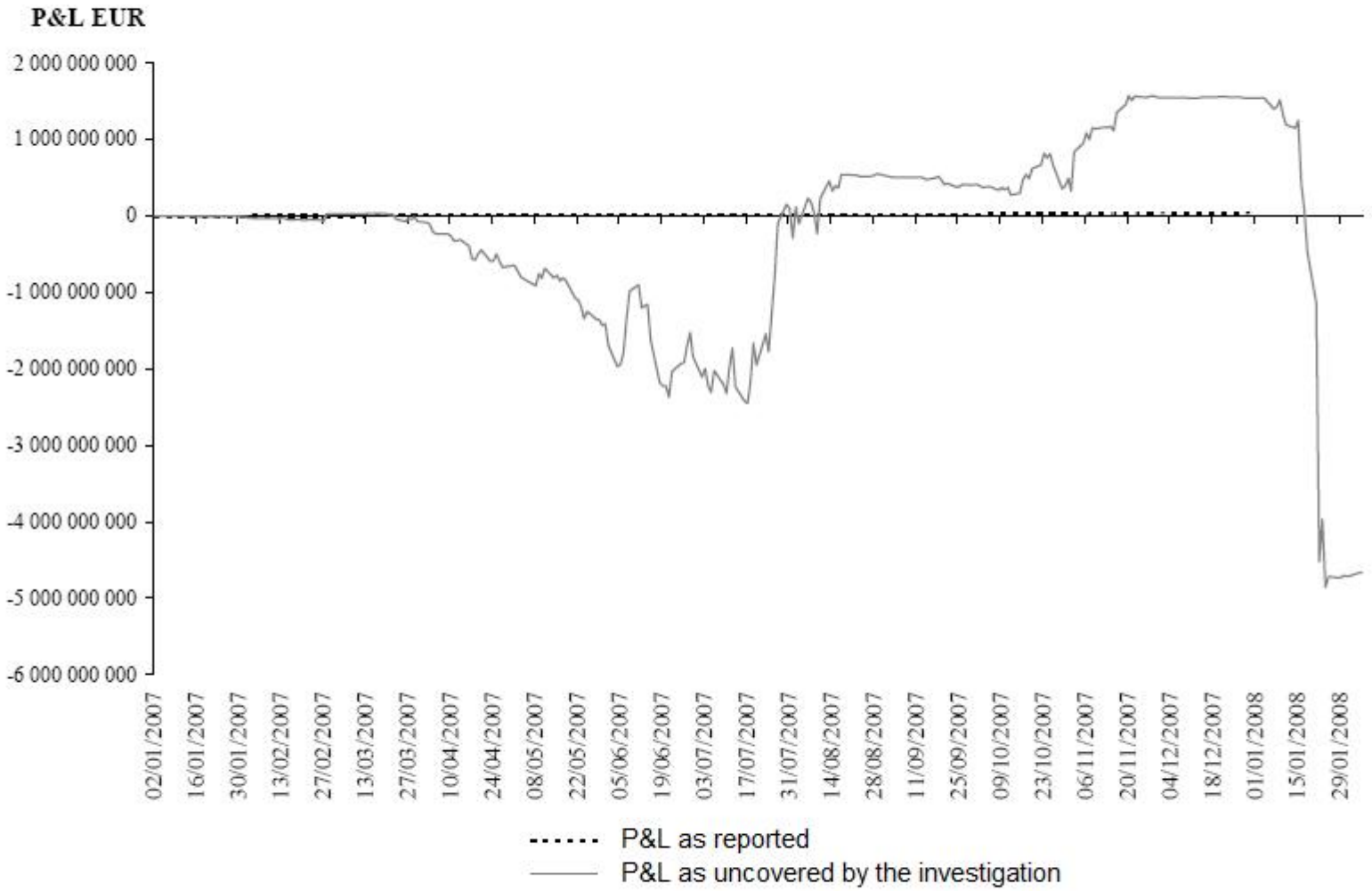
Failure Analysis

Societe General, OBSOC, Cisco

The Architecture of a 7.9 Billion $ Loss

- Junior Broker invests 73 Billion Dollar in Stocks and makes a 4.9 Bill. Euro Loss
- No embezzlement
- Management claims to be innocent
- Case resembles Barcley debacle (Singapore)
- Was it an IT-Security or management Problem?

Jean-Jacques Dubray on infoq.com


P&L EUR
2 000 000 000
1 000 000 000
0
-1 000 000 000
-2 000 000 000
-3 000 000 000
-4 000 000 000
-5 000 000 000
-6 000 000 000
02/01/2007
16/01/2007
30/01/2007
13/02/2007
27/02/2007
13/03/2007
27/03/2007
10/04/2007
24/04/2007
08/05/2007
22/05/2007
05/06/2007
19/06/2007
03/07/2007
17/07/2007
31/07/2007
14/08/2007
28/08/2007
11/09/2007
25/09/2007
09/10/2007
23/10/2007
06/11/2007
20/11/2007
04/12/2007
18/12/2007
01/01/2008
15/01/2008
29/01/2008
P&L as reported
P&L as uncovered by the investigation

How it was done

- Entry followed by cancellation of fake operations hiding the risks and the P&L. *The trader entered one or several fake operations in the systems so that they could be taken into account in risk calculation and value of the portfolio.... we have identified 947 transactions of this type.*
- Entry of fake compensated transaction (buy/sell) for identical quantities for different prices "outside the market", *with the goal to mask the P&L when transactions become effective... we have identified 115 transactions of this type*
- Entry of provisions that would temporarily cancel his P&L. *The trader used the ability to correct model biases, normally reserved to trader-assistants -without access rights to prevent traders to enter them-, to enter positive or negative provisions [in the middle-office system] to modify the calculated value [of a position] by the front-office system. We have identified 9 operations of this type.*

Who is responsible?

- First company report: the top management
- Second company report: middle management, helpers
- Kerveils lawyer jokes: in the third company report the cleaning ladies will be blamed for the desaster…

What PWC recommends

- using biometric authentication instead of Windows authentication for the most sensitive applications
- forbidding any transaction from the front-office onto middle-office applications
- considering forbidding any XL connection where the password is stored in the spreadsheet
- secure reporting applications (the report notes that many reporting feeds have been insufficiently tested)
- check if the workstation matches the potential user of an application

Questions for Risk Mitigation

- Does the action work towards the intended goal?
- Is the action in a reasonable relation to the risk it prevents or mitigates?
- Are there strong negative side-effects?
- Does the action calm down the nerves or does it really help?
- Are the people who recommend the action the same that will profit by seeing it implemented?
- Is it a „cover your ass“ action to avoid responsibility?

IT-Architecture

- Is a synchronous client-server system (DB backed) the right solution?
- How could an asynchronous, event based system detect fraud?

Architectural Validation

Observation System Analysis

-Use of security related meta-pattern (transformations like division, maliciousness)

-Results of Mobility

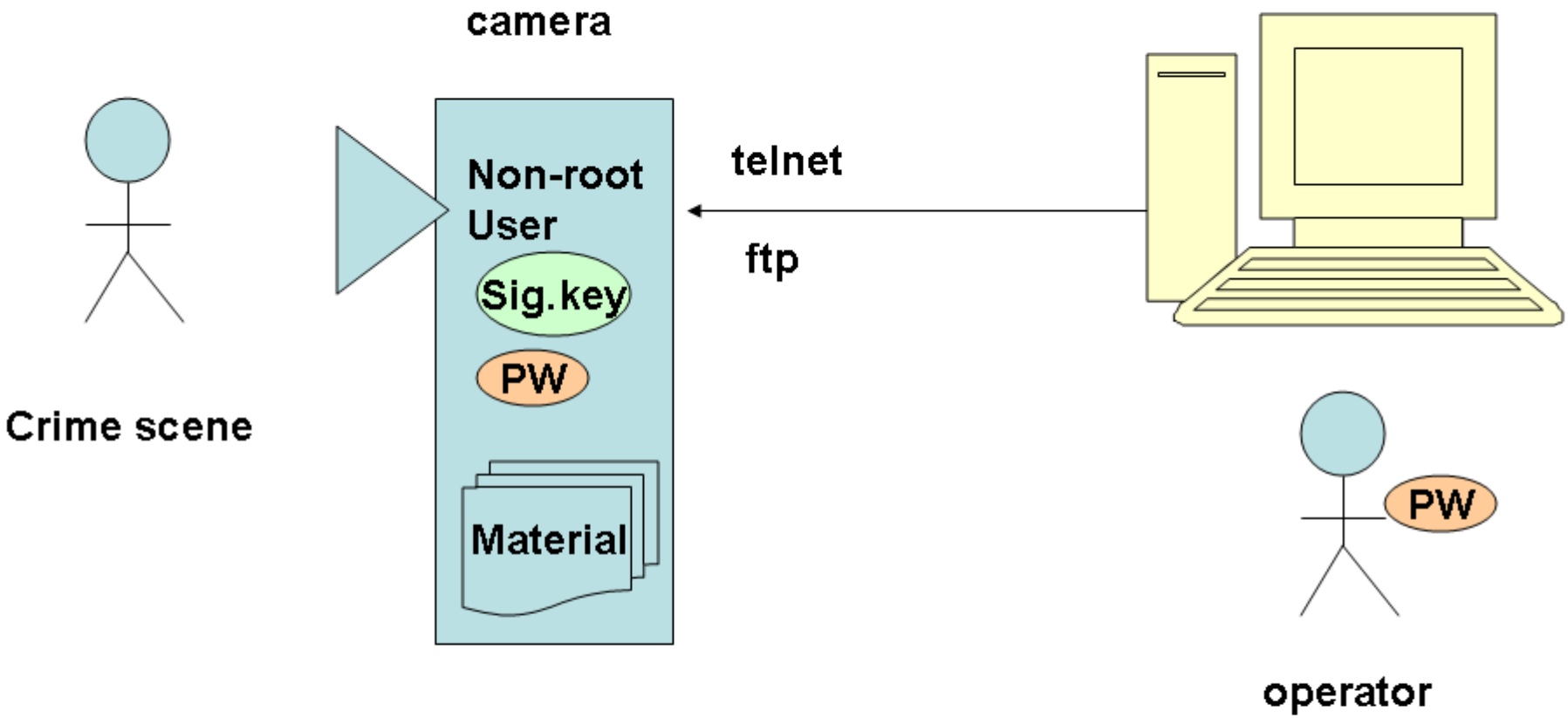
-Non repudiation problems

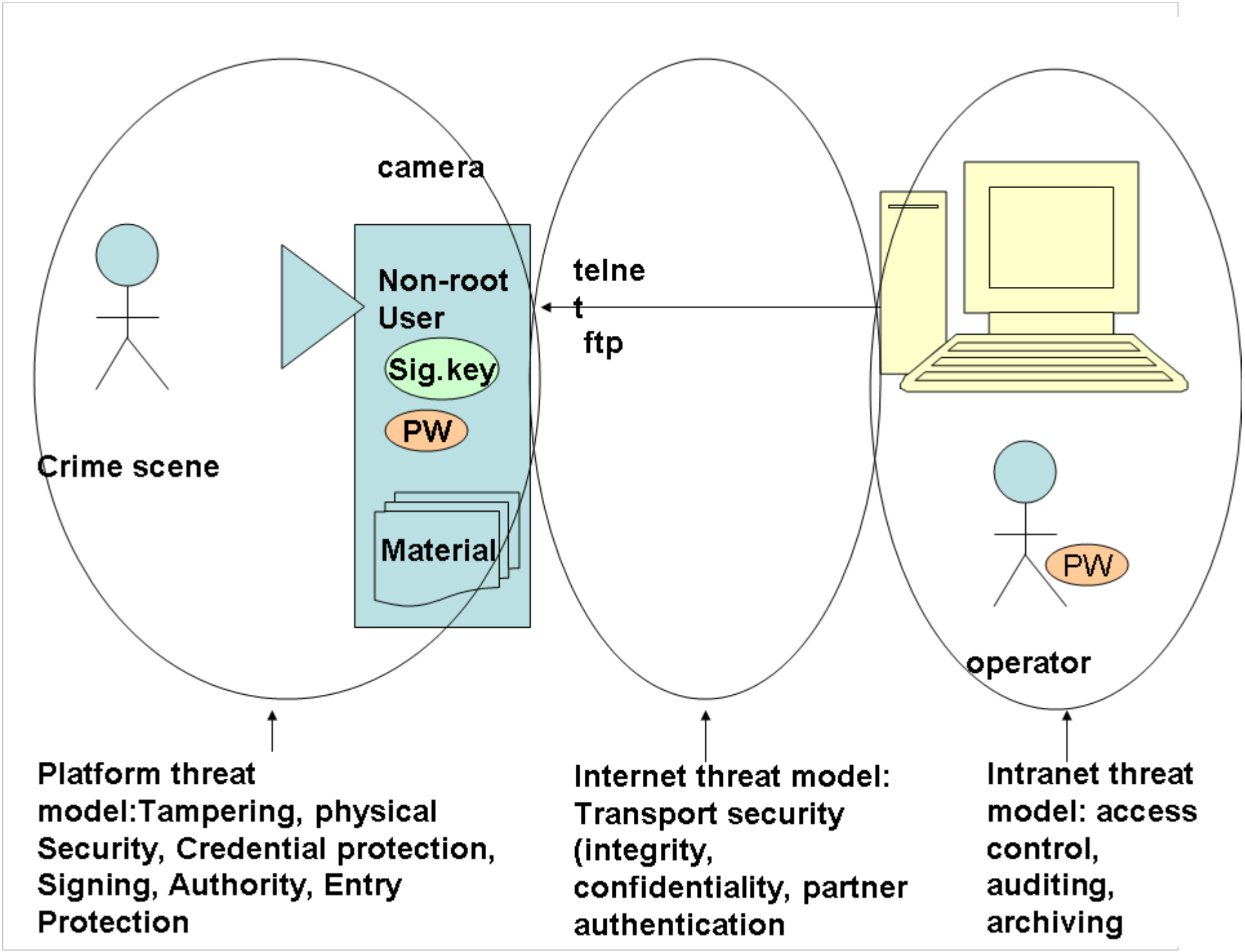
-Legal Aspects

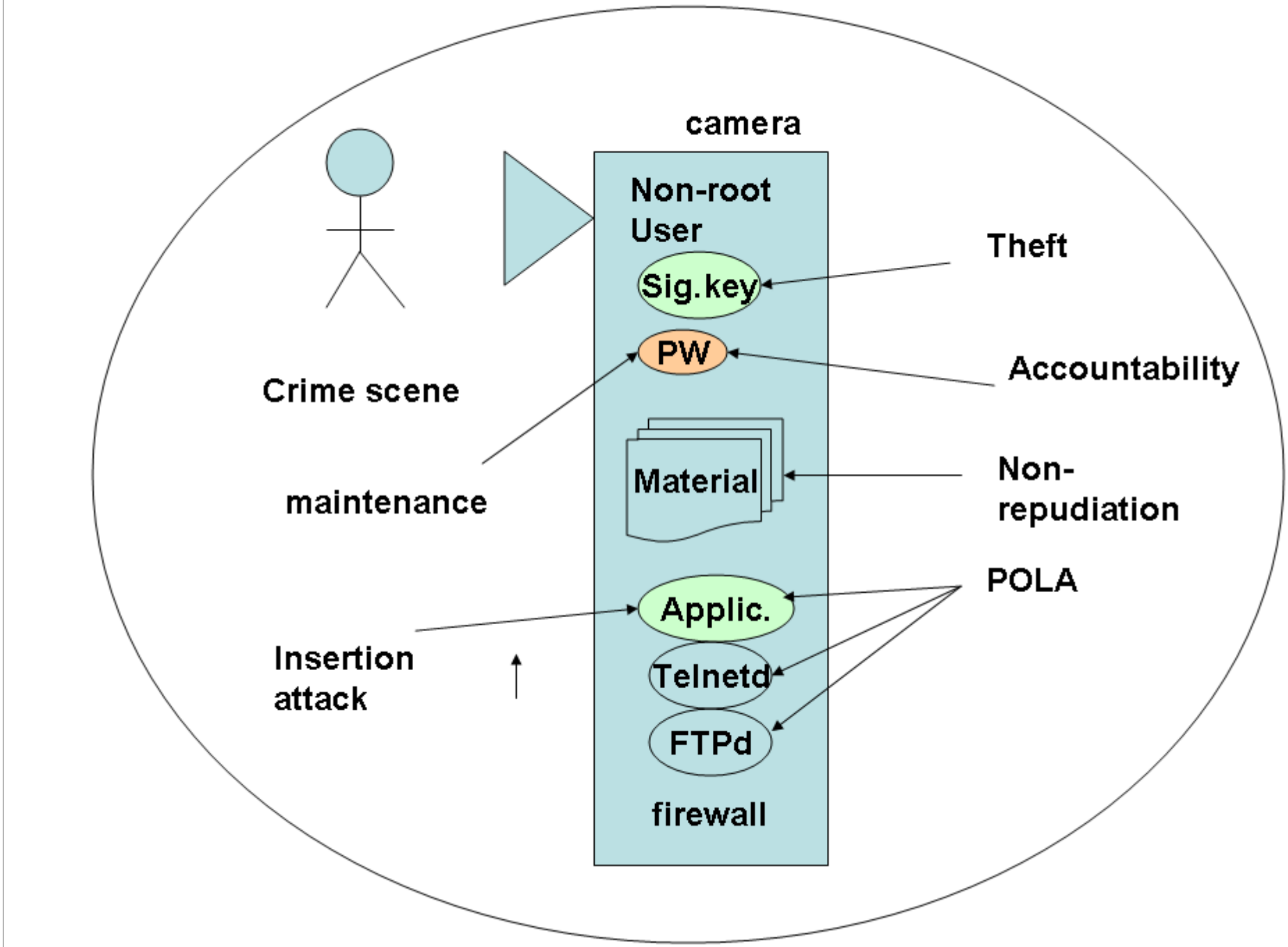
-Key Management Problems

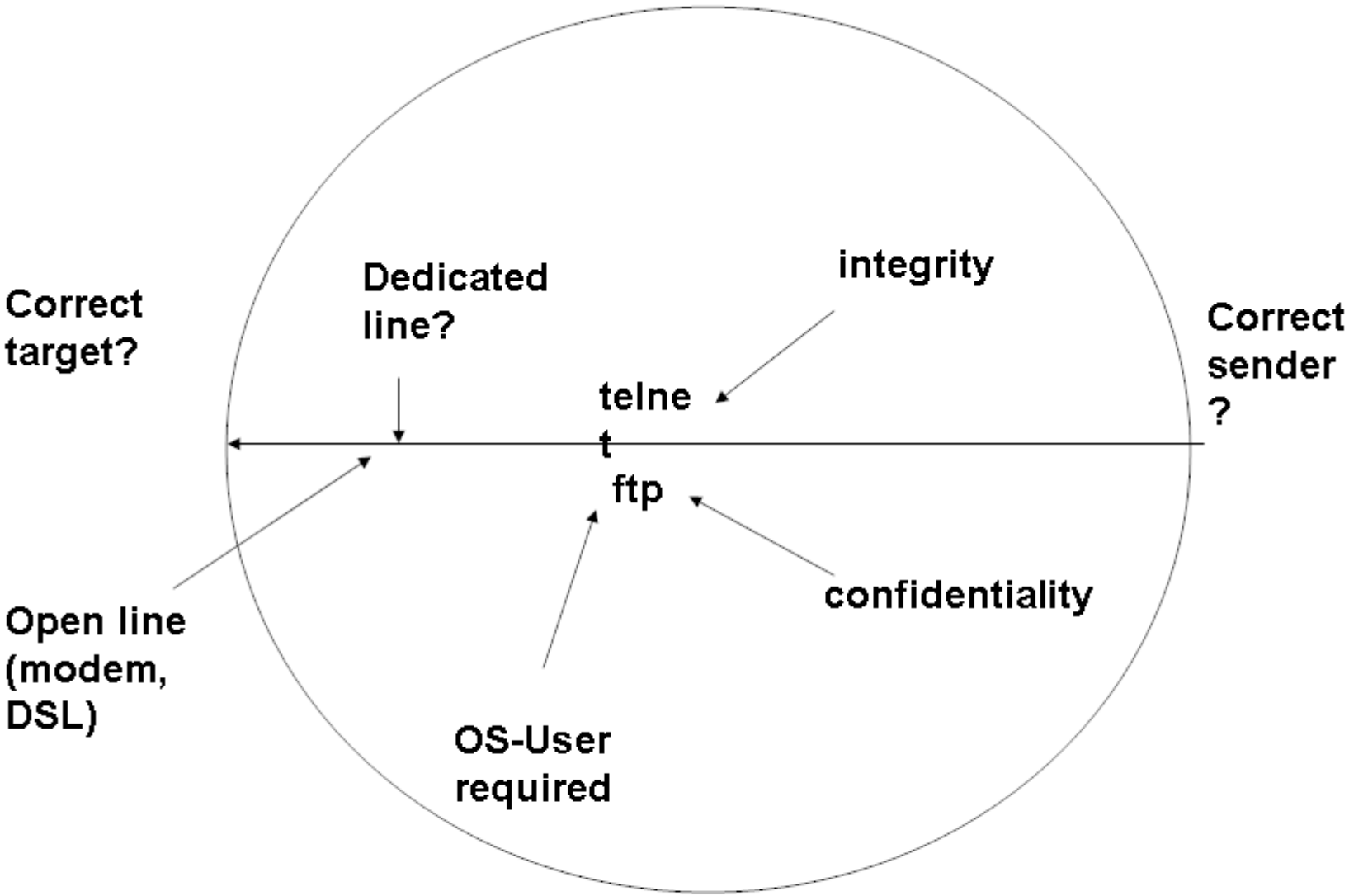
- POLA

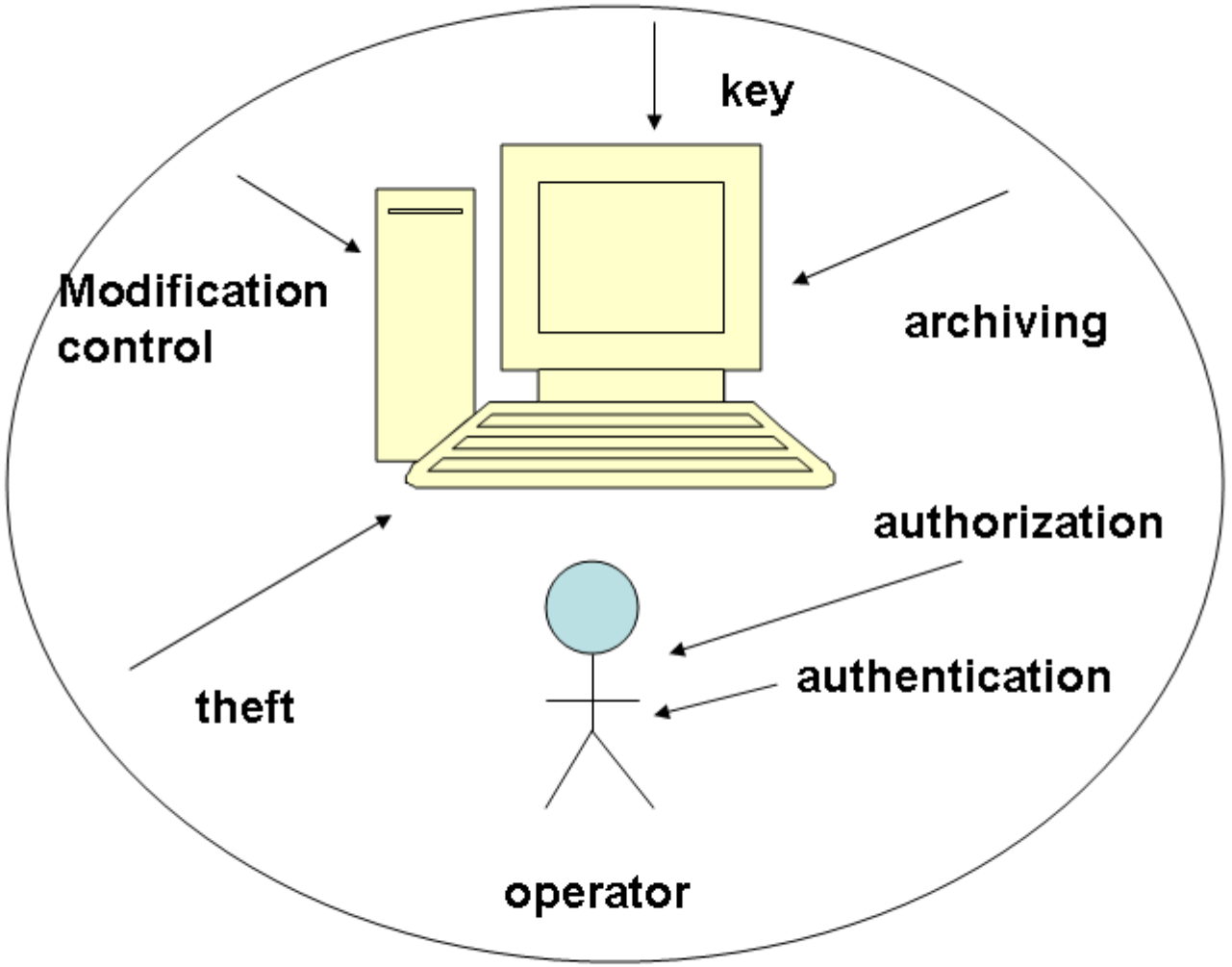
- Data Security and safety (backup etc.)


camera
Non-root
User
Sig.key
PW
Material
telnet
ftp
Crime scene
PW
operator

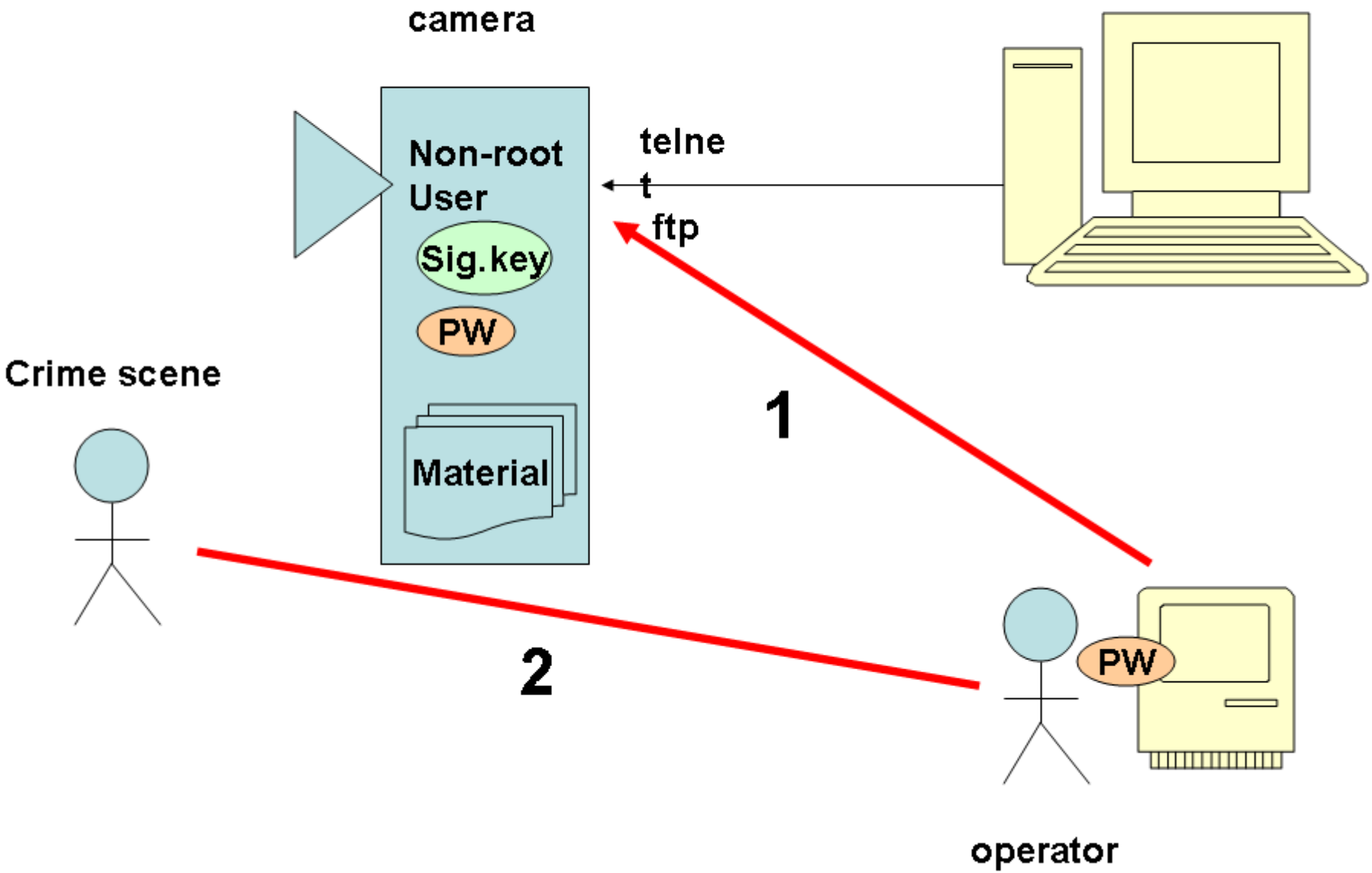

camera
Non-root
User
Sig.key
PW
Material
Crime scene
telne
t
ftp
PW
operator
Platform threat model:Tampering, physical Security, Credential protection, Signing, Authority, Entry Protection
Internet threat model: Transport security (integrity, confidentiality, partner authentication
Intranet threat model: access control, auditing, archiving


camera
Non-root User
Sig.key
PW
Material
Applic.
Telnetd
FTPd
firewall
Crime scene
maintenance
Insertion attack
Theft
Accountability
Non-repudiation
POLA

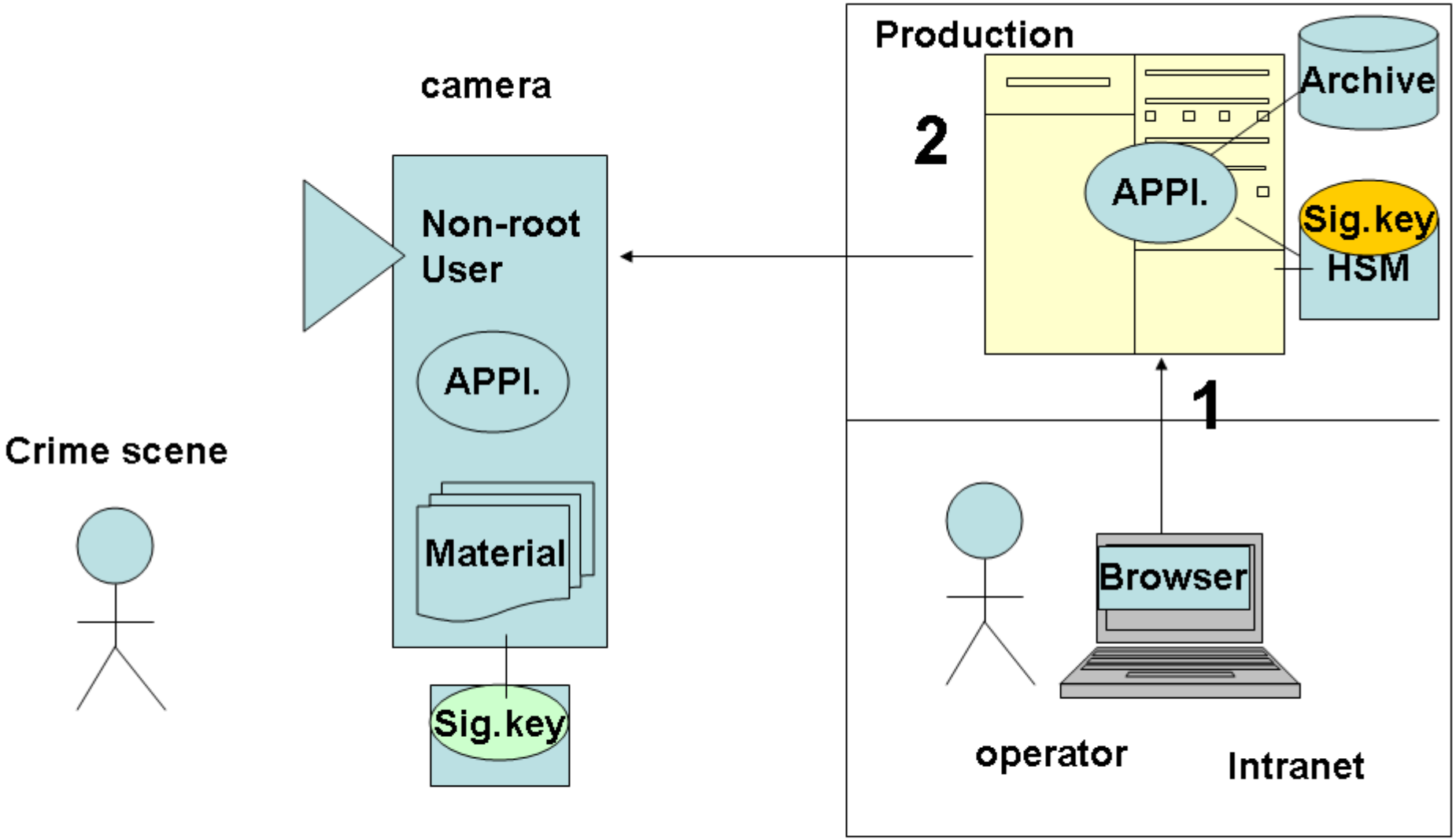

Correct target?
Dedicated line?
integrity
Correct sender ?
telnet
ftp
Open line (modem, DSL)
OS-User required
confidentiality


key
Modification
control
archiving
authorization
theft
authentication
operator

Transformations: spatial and moral



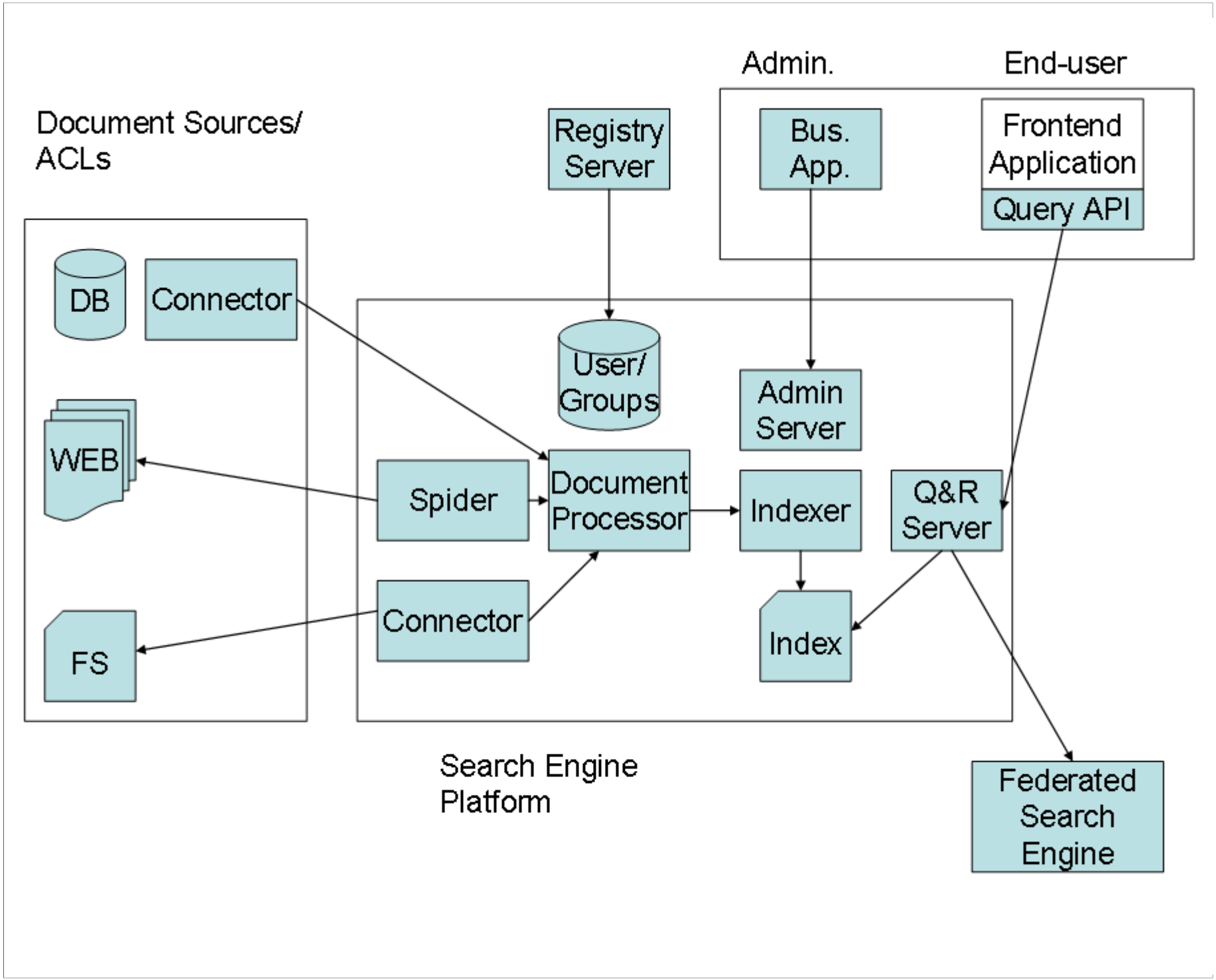
Transformations: spatial and type

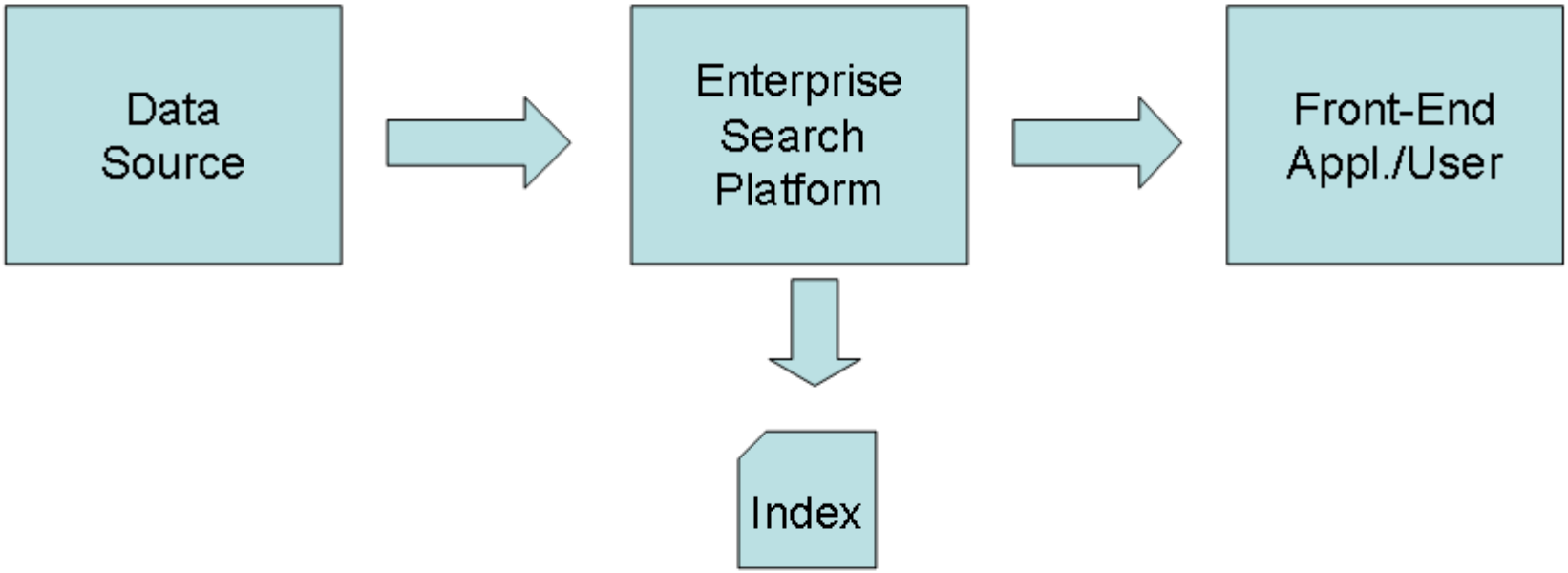


Architectural Validation

Enterprise Search Platform

- the importance of backend security)
- Access to platform
-Privacy
-Authentication and Access Control Problems


Admin.
End-user
Document Sources/
ACLs
Registry
Server
Bus.
App.
Frontend
Application
Query API
DB
Connector
User/
Groups
Admin
Server
WEB
Spider
Document
Processor
Indexer
Q&R
Server
Connector
Index
FS
Search Engine
Platform
Federated
Search
Engine


Data Source
Enterprise Search Platform
Front-End Appl./User
Index

Signs and Minds

- Infoq.com articles on societe general desaster
- Datenschleuder on OBSOC desaster