



Conference

PVI architecture, functionalities, and integration with WMS

# Building an Infrastructure for Product Authentication

Lessons learned from the SToP project



Information Society  
Technologies

Harald Vogt, SAP Research

27 May 2009



## Observations:

- The counterfeiting problem is **serious**, but hard / impossible to **quantify**
- Raising the threshold for market entry of counterfeits will decrease the demand and increase the associated risks
- Technical means alone are insufficient

## Why do SToP?

- One ingredient within a broad strategy
- Protection of customer/patient health and safety
- Protection of product value (e.g. “experience”)
- **Control** for players within the supply chain

## Changing market structures



### Regulated markets

- High threshold for market entry
- Known players
- Stable trading relationships
- Long-term contracts
- Common standards (e.g. quality)

### Open (globalized) markets

- Low threshold for market entry & exit
- Dynamic peers
- Ad hoc trading relationships
- Short-term contracts
- Outsourcing
- Differing, non-enforced standards

# Providing Product (Item) Integrity



## ■ Method 1: **Relying on the infrastructure**

- Supplier certification
- Contract enforcement
- Trust (in internal & external entities)
- Market regulation & observation

**Increasingly difficult in globalized markets; opportunities might be missed!**

## ■ Method 2: **End-point intelligence**

- Only end-to-end trust relationship required
- Integrity verification required
- Challenge: Maintain early response

**Possibly the only way in the new economy; profit from flexibility!**

Presumably **300+ products** being offered...

- *Differing in* product suitability (material-dependent)
- *Differing in* requirements for services and data
- *Differing in* checking devices and procedures
- *Differing in* level of security (incl. certification, resistance)
- *Differing in* process integration (production and checking)

- What are your selection criteria of security features?
  - Technology required for application, verification
  - Materials compatibility
  - License costs
  - Visibility / concealment
  - Data capabilities
  - Ease of verification
  - Durability

# Do you need a security feature?



## ■ Some observations

- Sometimes the mere *mentioning* of a security feature seems to work
- Easy-to-produce features are being copied badly; fakes can be easily spotted – but are on sale anyway
- Who do you (mis)trust? Will a security feature help? Do you trust your customers?

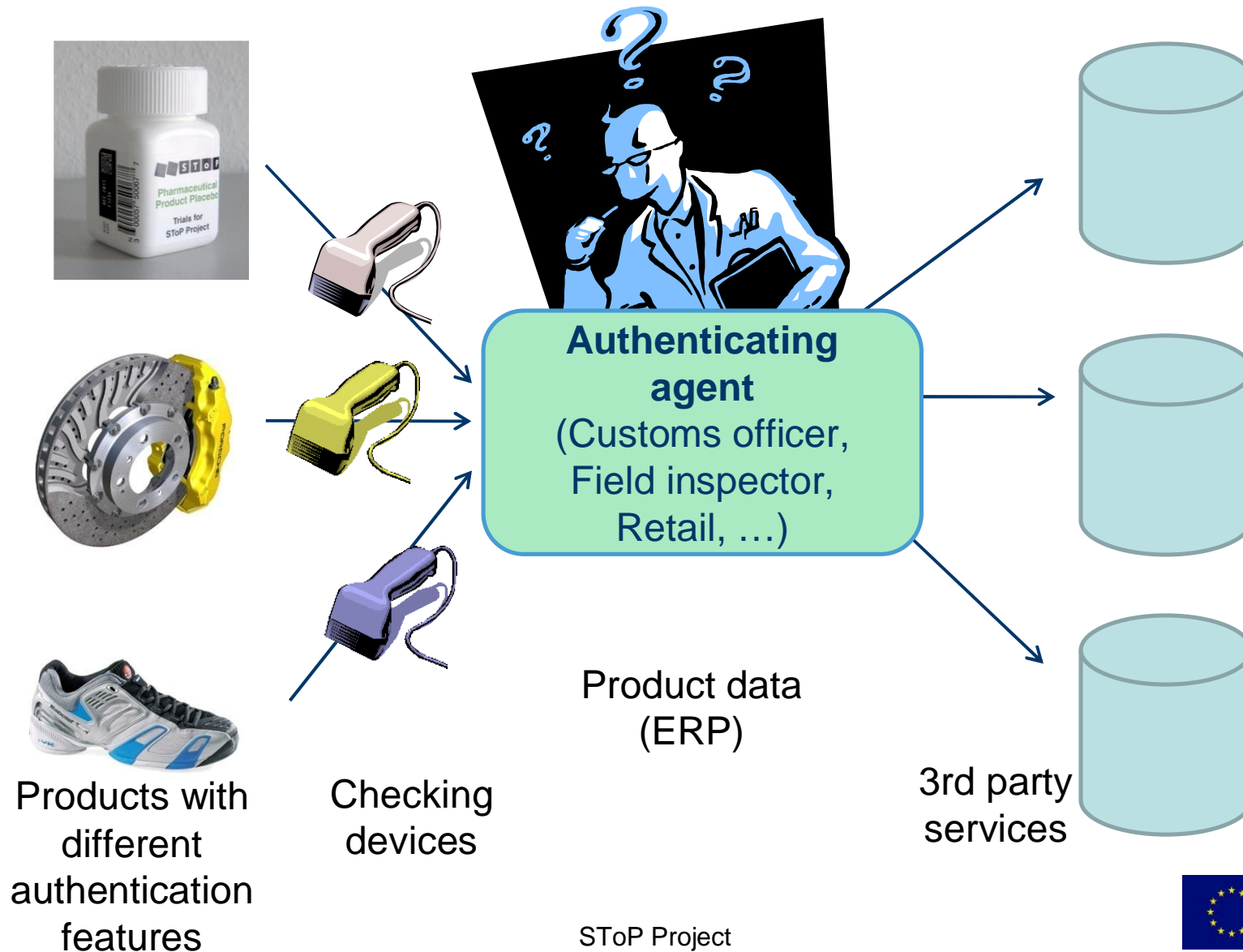
# Do you need a generic approach?



## Complexity

- # product types
- # vendors
- # verifiers
- # security features
- # authentication equipment
- # back-end systems
- # access rights
- # types of information being transmitted
- # industries with individual requirements
- # requirement evolution

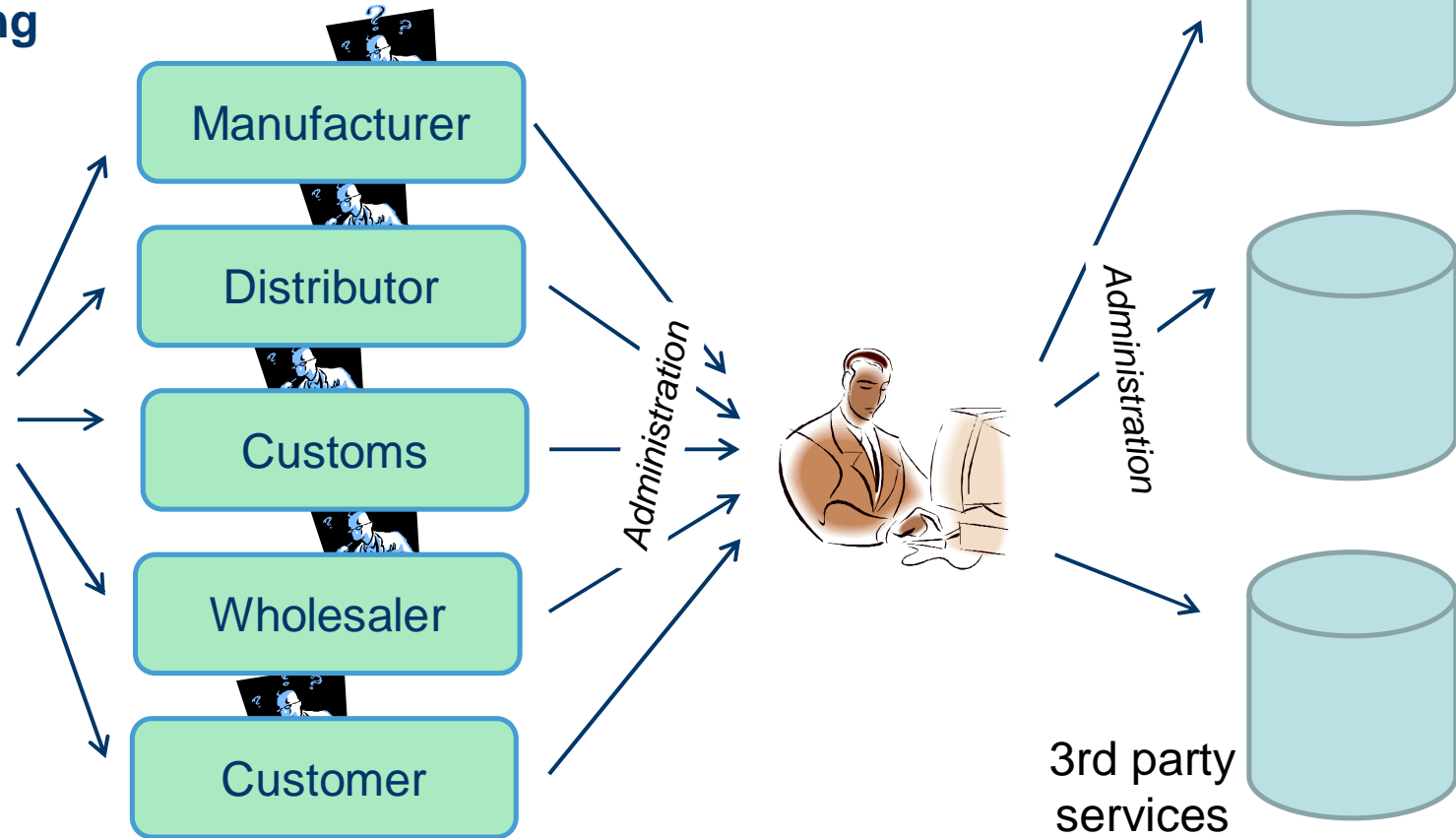
# Verifier's Point of View



# Brand Owner's Point of View



- Heterogeneous „authentication landscape“ requires
  - Management of users (devices, authorization)
  - Management of features (identification, feature data)
  - Specific view & application integration
  - Reporting
  - ...



## Pharma

**Objective:** Patient safety

**Object of authentication:**  
Packaging (Level 1+2)

**Automation:** up to 400 units  
per minute

**Check locations:**  
Manufacturing, Wholesaler,  
Customs; Pharmacy, Patient

**Environment:** High  
temperatures while packaging  
(blister)

**Regulation:** legal  
requirements (e-pedigree)

**Extra:** Logistics integration

## Aviation

**Objective:** Safety

**Object of authentication:** Line  
Replacable Units (LRU)

**Automation:** Mobile check  
devices; checking automated

**Check locations:** Suppliers,  
Maintenance

**Environment:** RFID  
mandatory; Maintenance data  
on tag

**Regulation:** Industry standards;  
Verified airworthiness

**Extra:** Synchronisation of tag  
data with backend server

## Luxury goods

**Objective:** Brand protection,  
„user experience“

**Object of authentication:**  
Watches, jewelry, accessories,  
glasses, wine, etc.

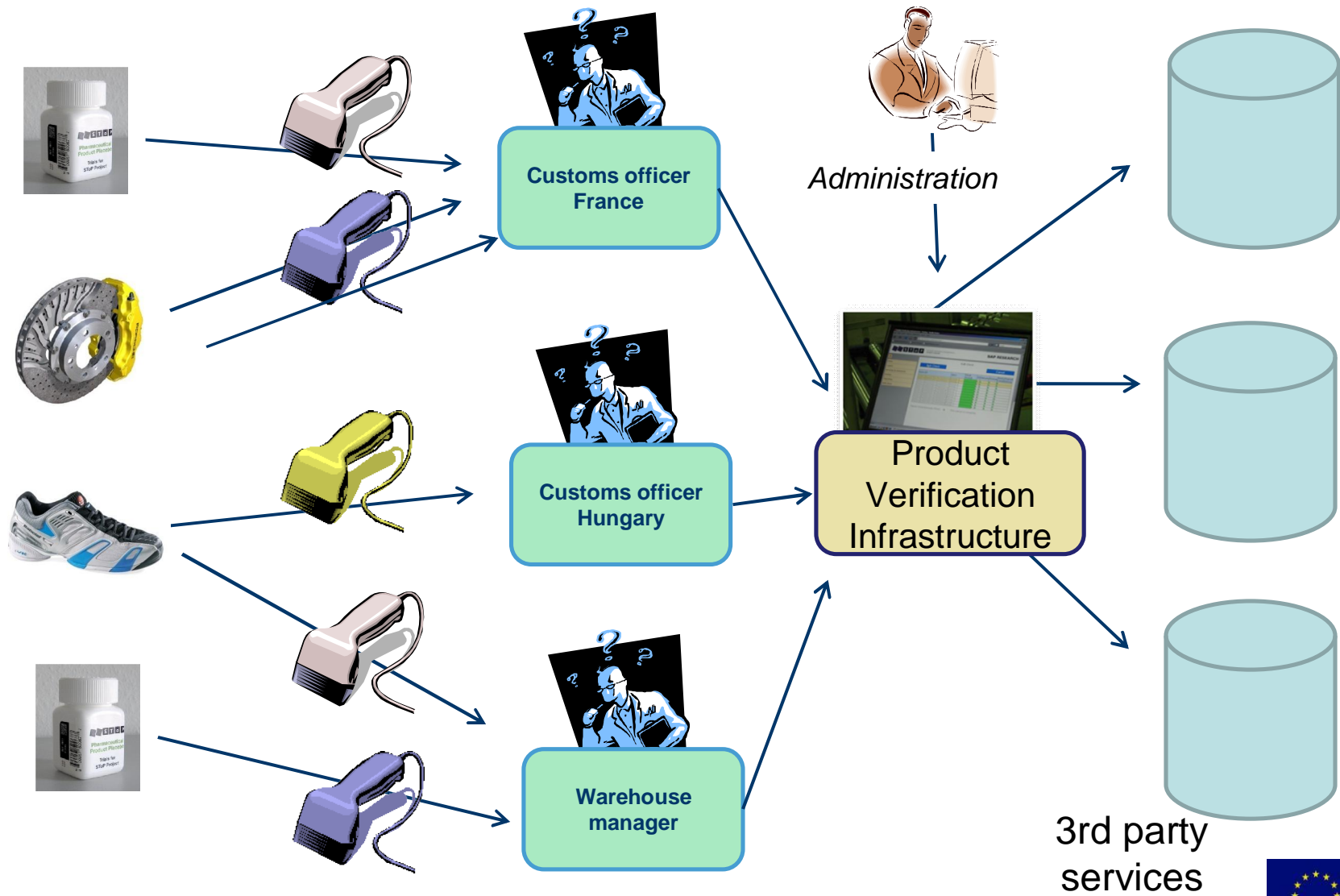
**Automation:** Manual, semi-  
automatic

**Check locations:**  
Manufacturing, Service,  
Customs, Retailer, Field  
inspector

**Environment:** No impact on  
visual design, robustness

**Extra:** Coupling with SCM and  
T&T

# Let the PVI do the work!



# PVI Objectives



Platform for product authentication:

- Interface between application/business processes and technology
- Abstract from technology requirements
- Broad support of both inspection devices and user roles



*User*

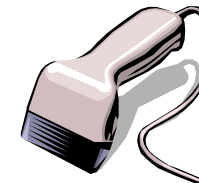
Application



Platform

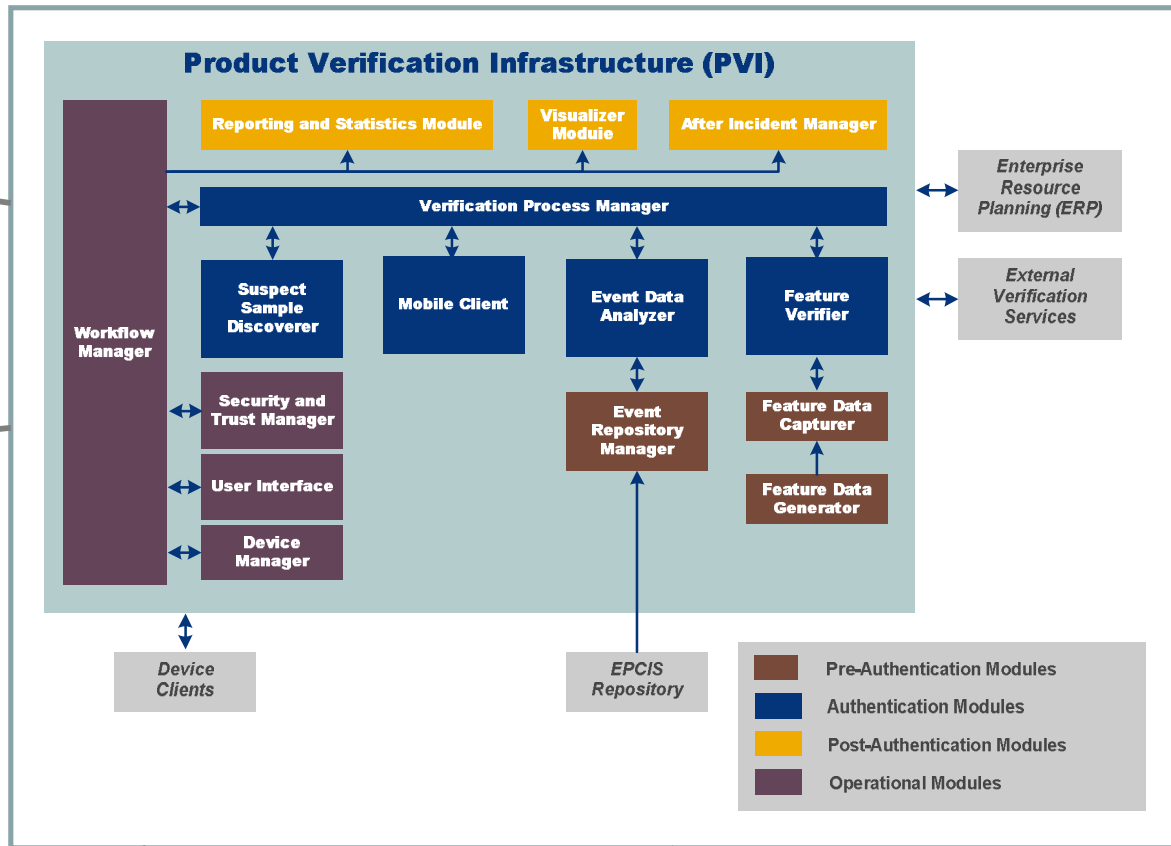
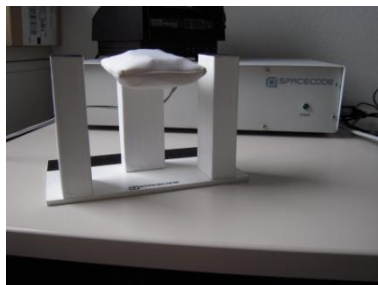


Technology



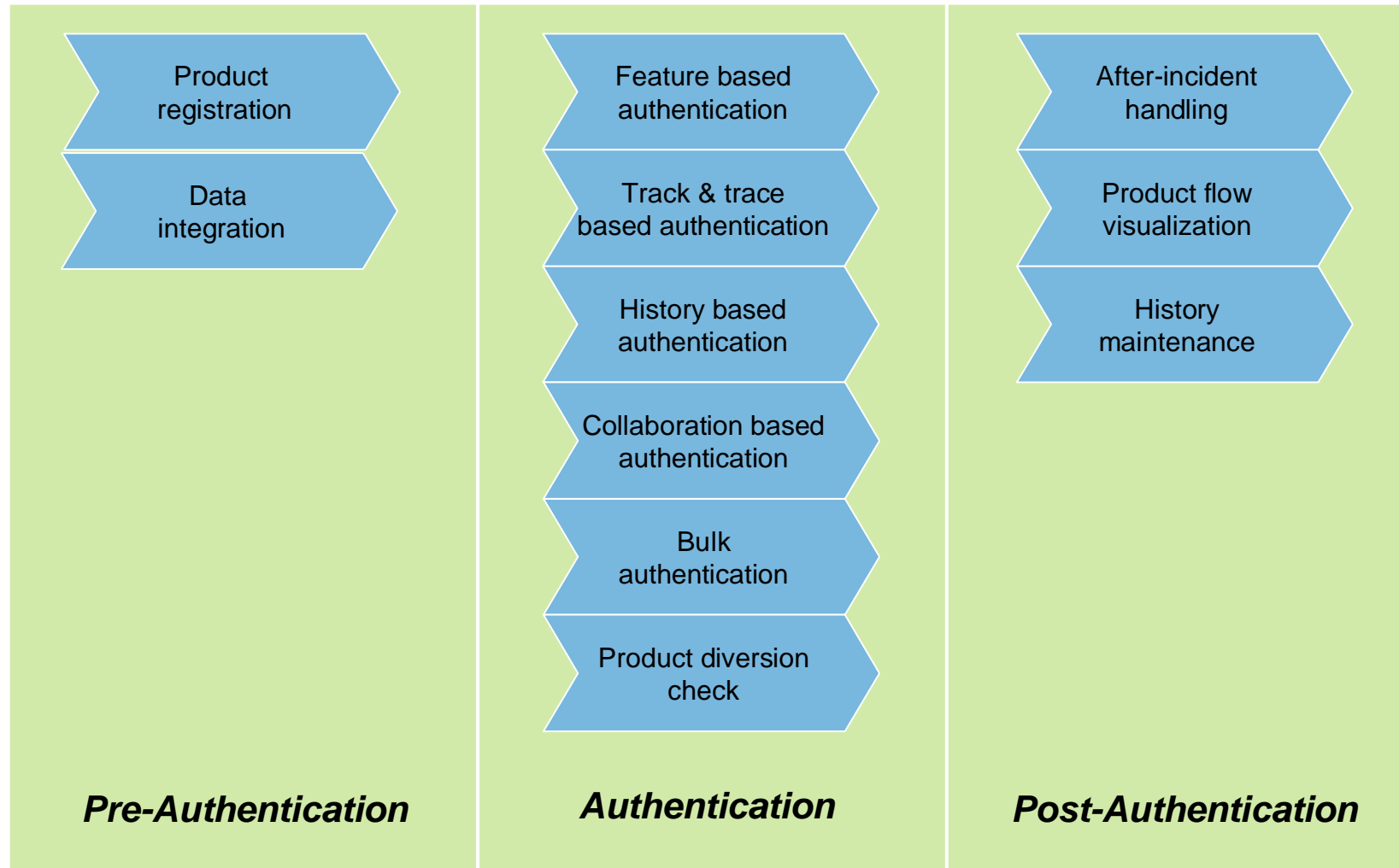
*Product*

# SToP Platform

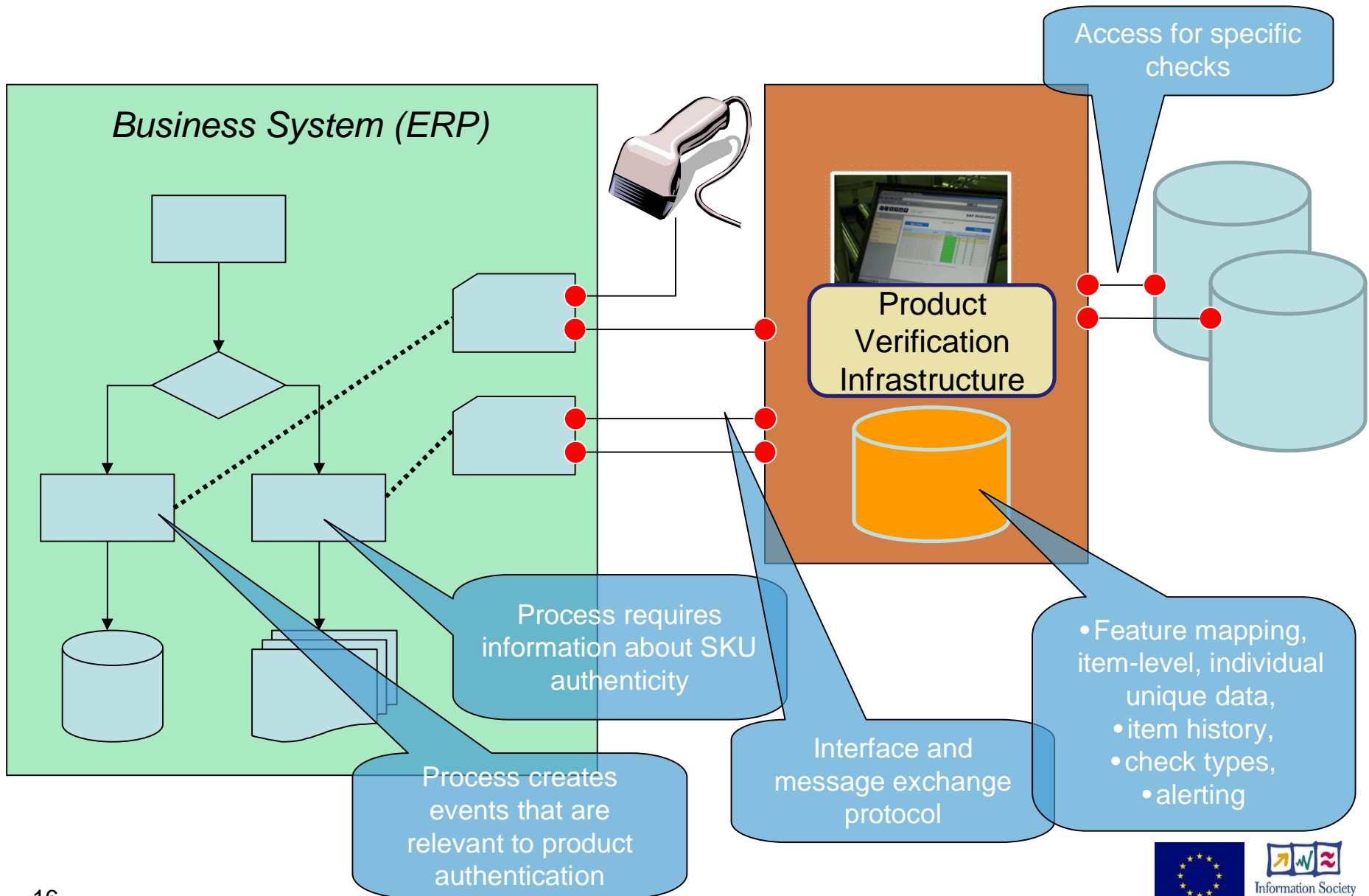


# PVI Supported Processes

*Implementation of functional requirements*



# PVI Integration with Business Systems



# Scenario: Mystery Shopper



Mystery Shopper

Mobility  
Minimal UI  
Multiple Features

Remote Product Authentication

Connection to Enterprise System  
Desktop Integration  
Awareness of Authentication Attempts  
Full Control, After Incident Management



Manufacturer's Back Office

The Mystery Shopper hunts for counterfeits in a store.

# Trial Prototypes



- Luxury goods
  - Warehouse process (packing)
  - Retail process (service)
- Pharmaceutical products
  - Pharmacy goods received
- Logistics
  - Warehouse process (receiving, shipping, ...)
- Aviation
  - Service history



# Aviation Trial



Initialize

Untagged Parts	
Manu ID	Part ID
DESAP	PART10000000002
DESAP	PART10000000003
FRAIR	PART10000000001
FRAIR	PART10000000002

Original Part Infos

Original Part ID: 1234567890  
Part Description: FOR TEST  
Lot ID: 1234  
Manufacture Data: 2008-10-10  
Expiration Data: 2008-10-22  
Fabricator ID: DESAP  
Intern Customs ID: USER02  
Export Control ID: 0A001  
Hazardousmaterial: NAICAO  
Country ID: DE  
Nato Stack ID: NNNNNNNNNNNN  
Weight: 12 MG

Other Informations

Software Indicator: Y ET dev Indicator: N  
Tag ID: 987654321  
Tracking ID: TRACK001  
Remarks: THIS IS A TEST

Please Input complete Infos

Finish Cancel



# Pharmacy Trial



# Conclusion



- Product verification infrastructure requires dedicated functionality and management processes
- PVI must be partially open to allow access by external parties
- Security feature technology change is part of ordinary business
- SaaS approach seems feasible



# Thank you!

**Dr. Harald Vogt**

SAP AG

SAP Research

Vincenz-Priessnitz-Str. 1

76131 Karlsruhe

Germany

Phone: +49 6227 7 52551

Mobile: +49 151 5711 8766

E-Mail: [harald.vogt@sap.com](mailto:harald.vogt@sap.com)

