lönsamt, **lätt** och **roligt**
att testa
informationssäkerhet i
system**!**

Rosemarie Arnmark

- Dataingenjör KTH
- Informations- ITsäkerhet DSV Stockholms Universitet
- Systemanalytiker
- Testexpert och testledare
- Nätverksledare på DFS

Dyrt

lång tid, många intressenter, många möten

Svårt

krångliga testfall, osäkra resultat

Tråkigt

omständligt, testdata svårt, omkörning svårt

Viktiga säkerhetsbegrepp

Safety / Systemsäkerhet

Skydd av människa, maskin och miljö

Security / IT-säkerhet (Datasäkerhet)

Skydd av information

- Tillgänglighet
- Skydd mot otillbörlig access
- Konsistent information
- Spårbarhet
- Oavvislighet

Viktiga säkerhetsbegrepp

Informationssäkerhet

- *Hela* bilden, *all* information
- Ex. lokalaccess, regelverket m.m.

IT-säkerhet

- data-system
- mjukvara *samt* hårdvara

FRÅGA:

Hur får vi test av IT-säkerhet **lönsamt**, **lätt** och **roligt**?

SVAR:

3 **olika** systemanalyser, med **olika** fokus!

3 systemanalyser, med *olika* fokus

1. **Produktionssystemet, ur alla aspekter**

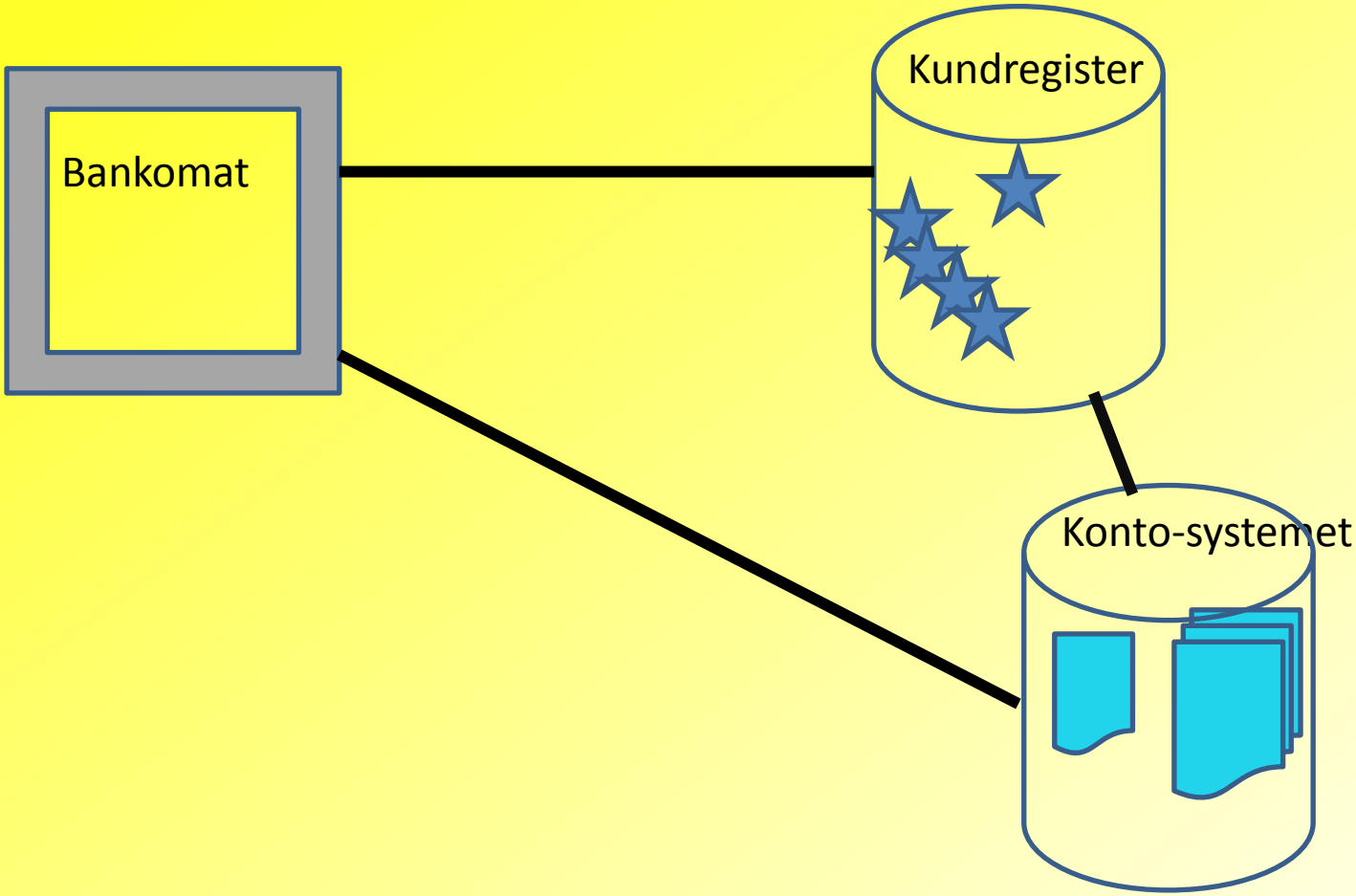
2. **Testsystemet,** skillnader mot produktionssys

3. **Informationssäkerheten** analyseras

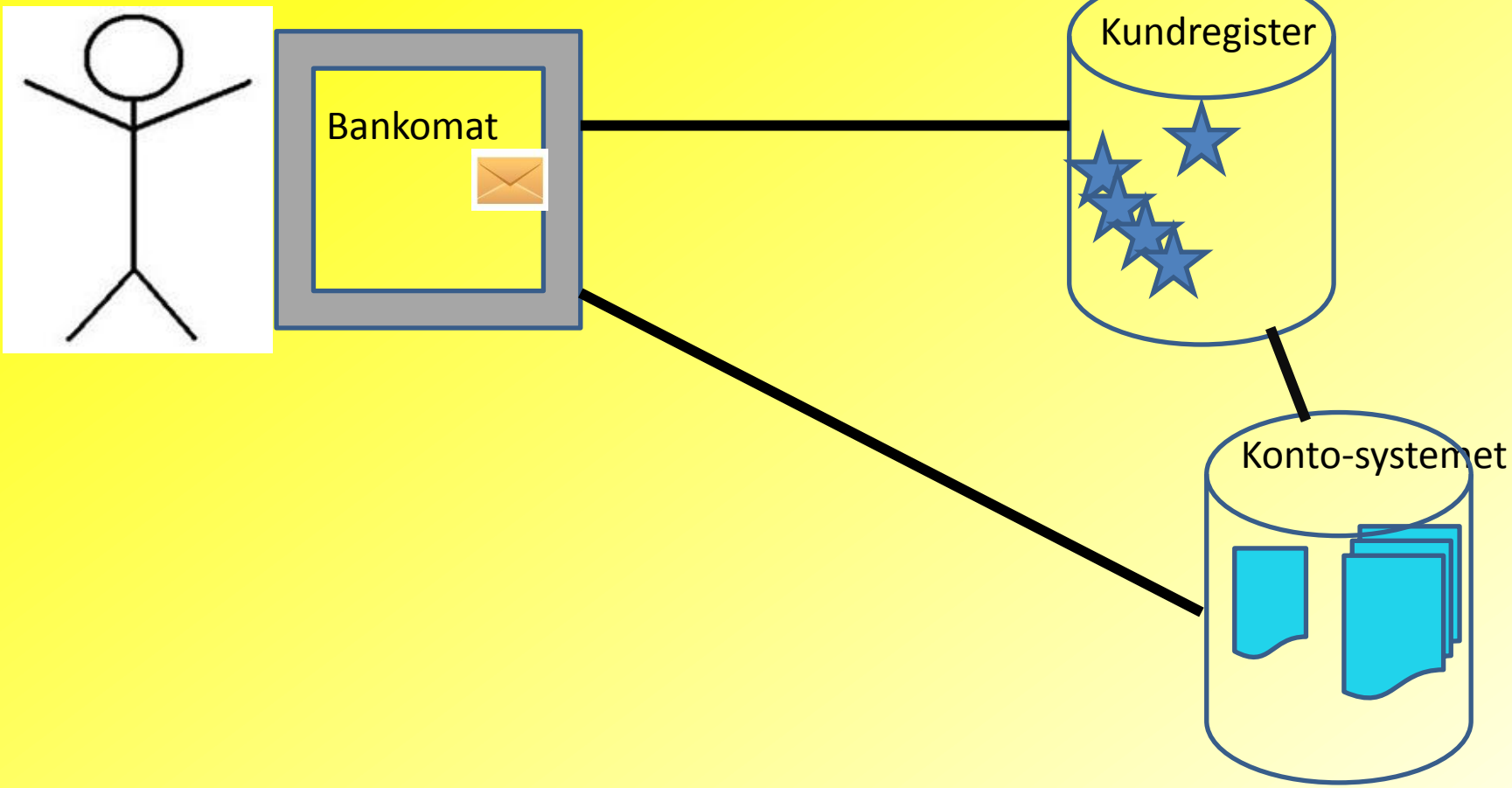
Systemanalys 1: Produktionssystemet

Bankomatexempel

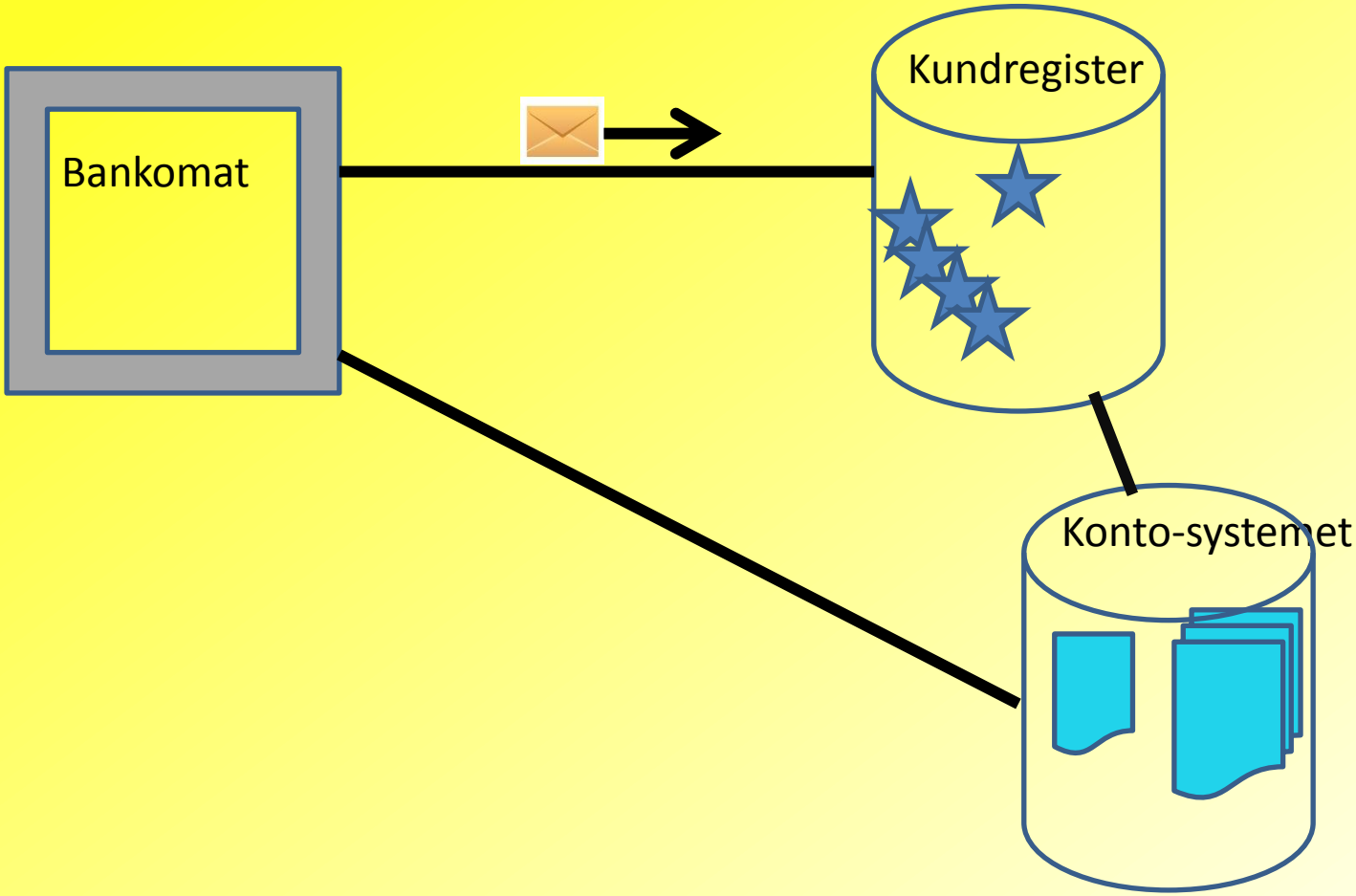
Bankomatexempel



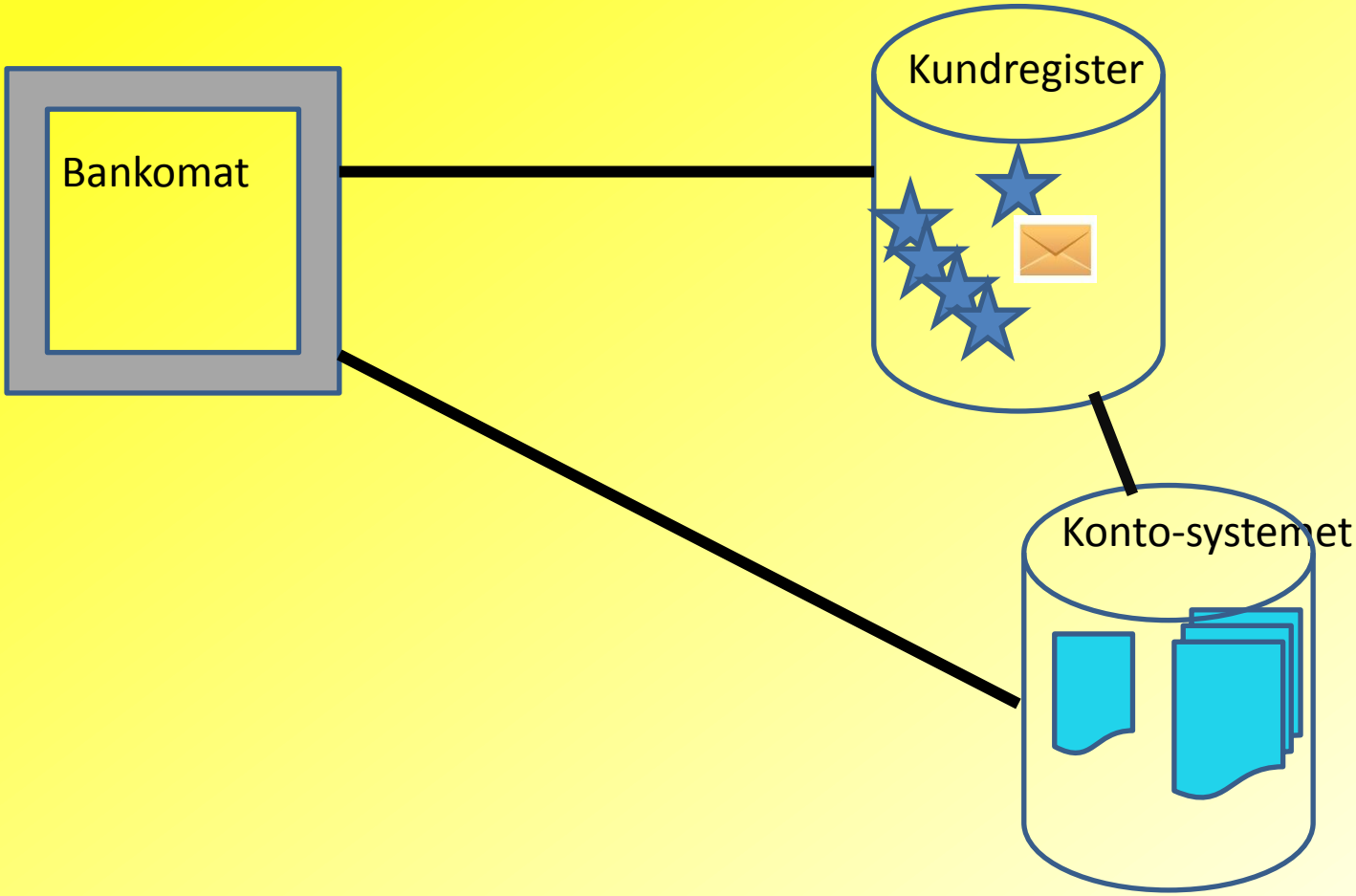
Bankomatexempel



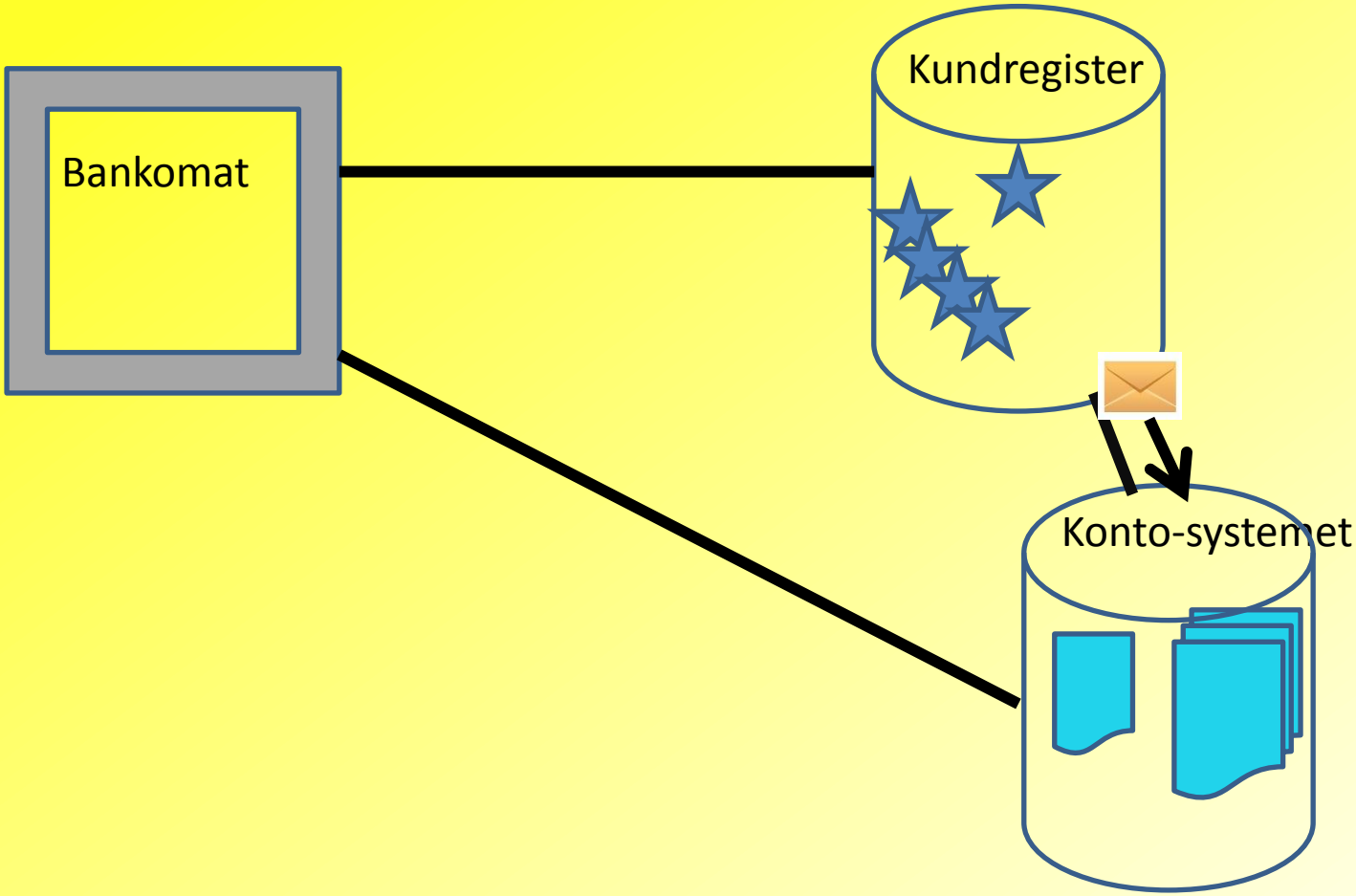
Bankomatexempel



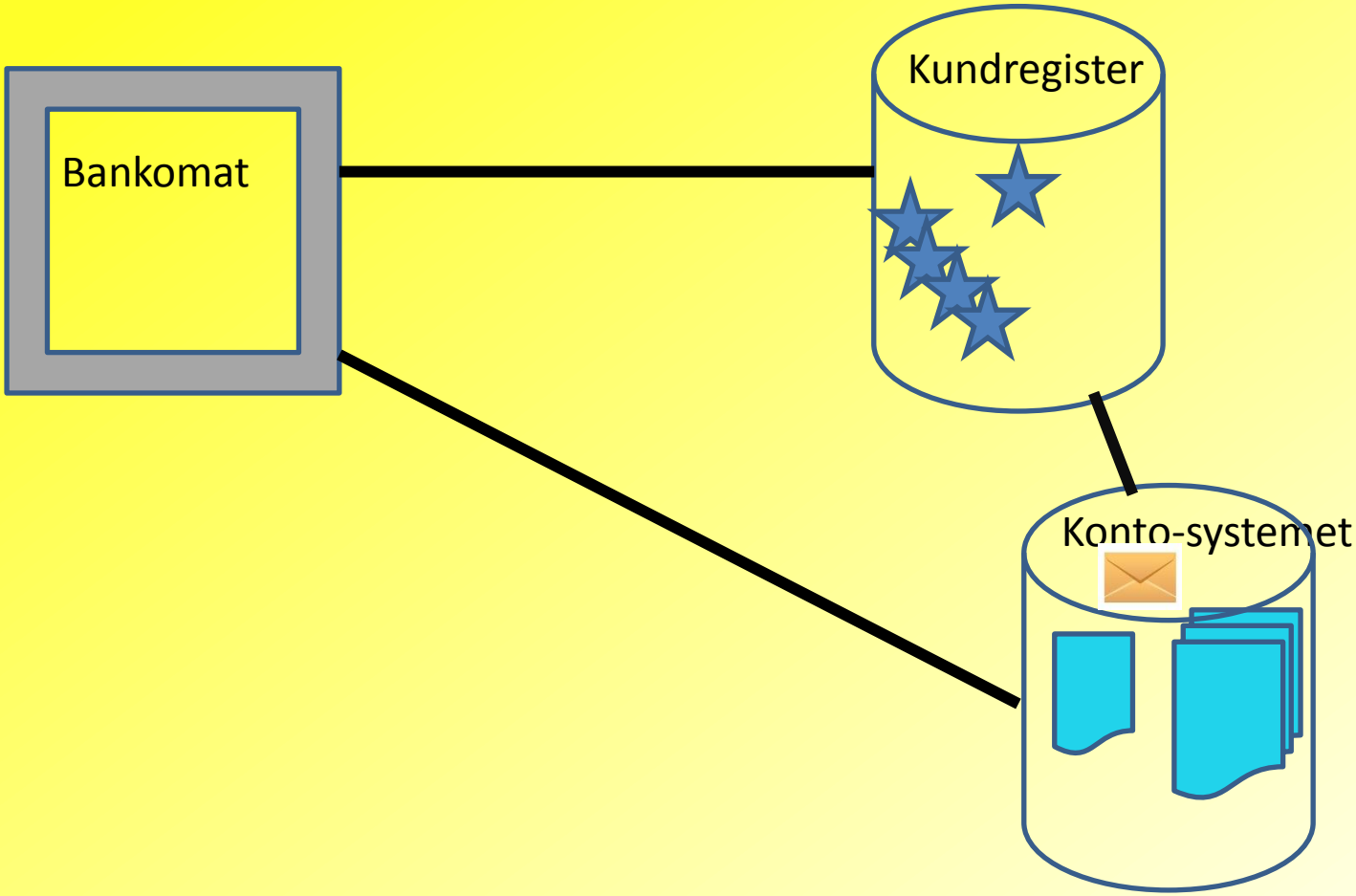
Bankomatexempel



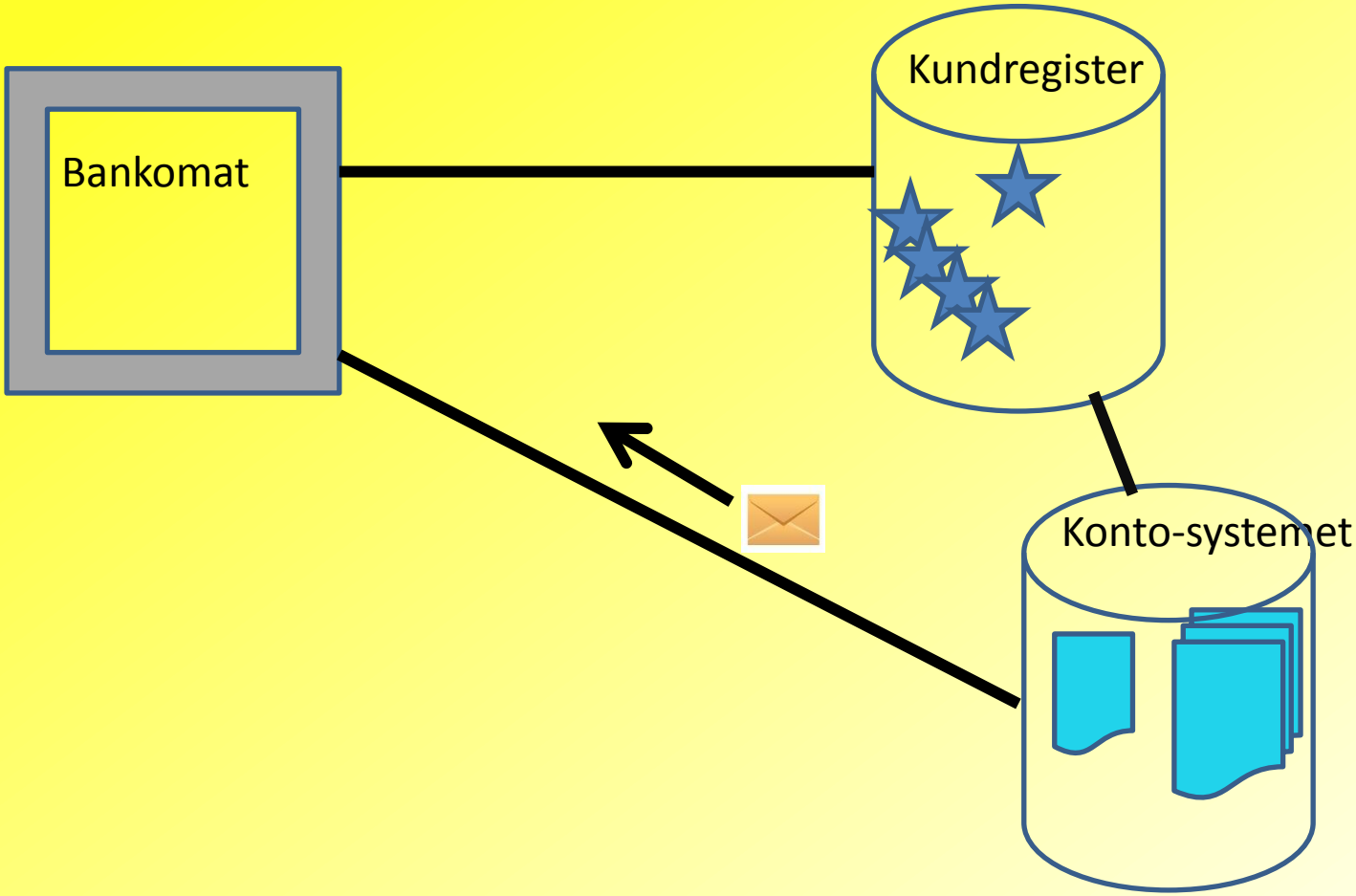
Bankomatexempel



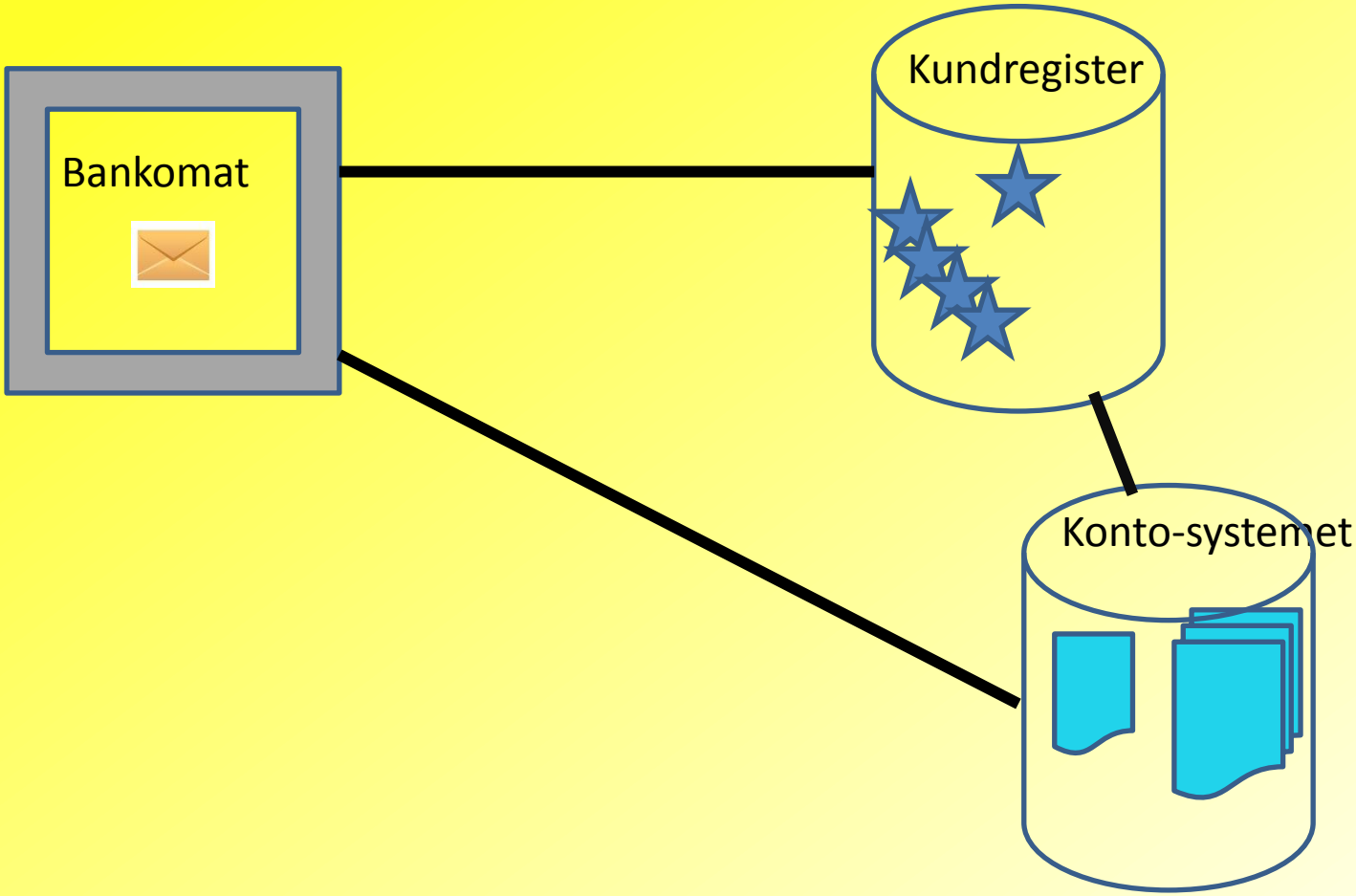
Bankomatexempel



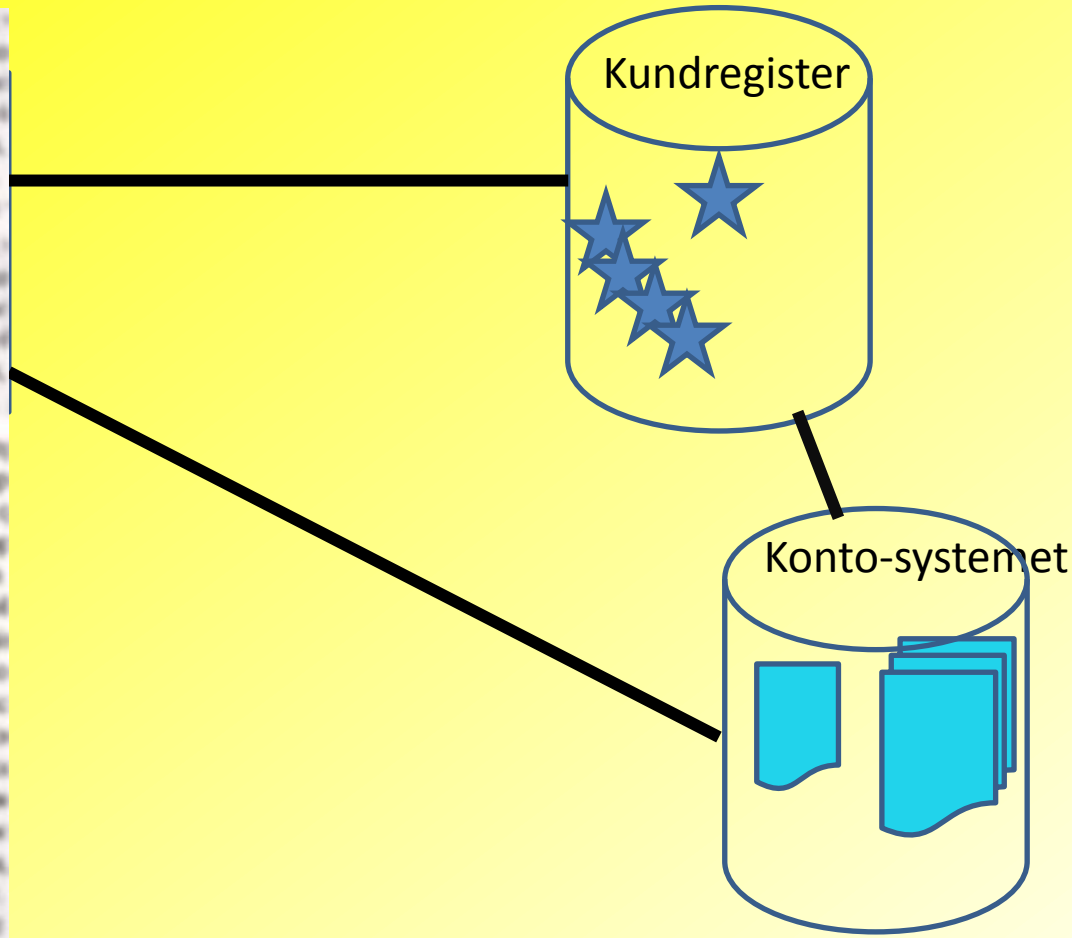
Bankomatexempel



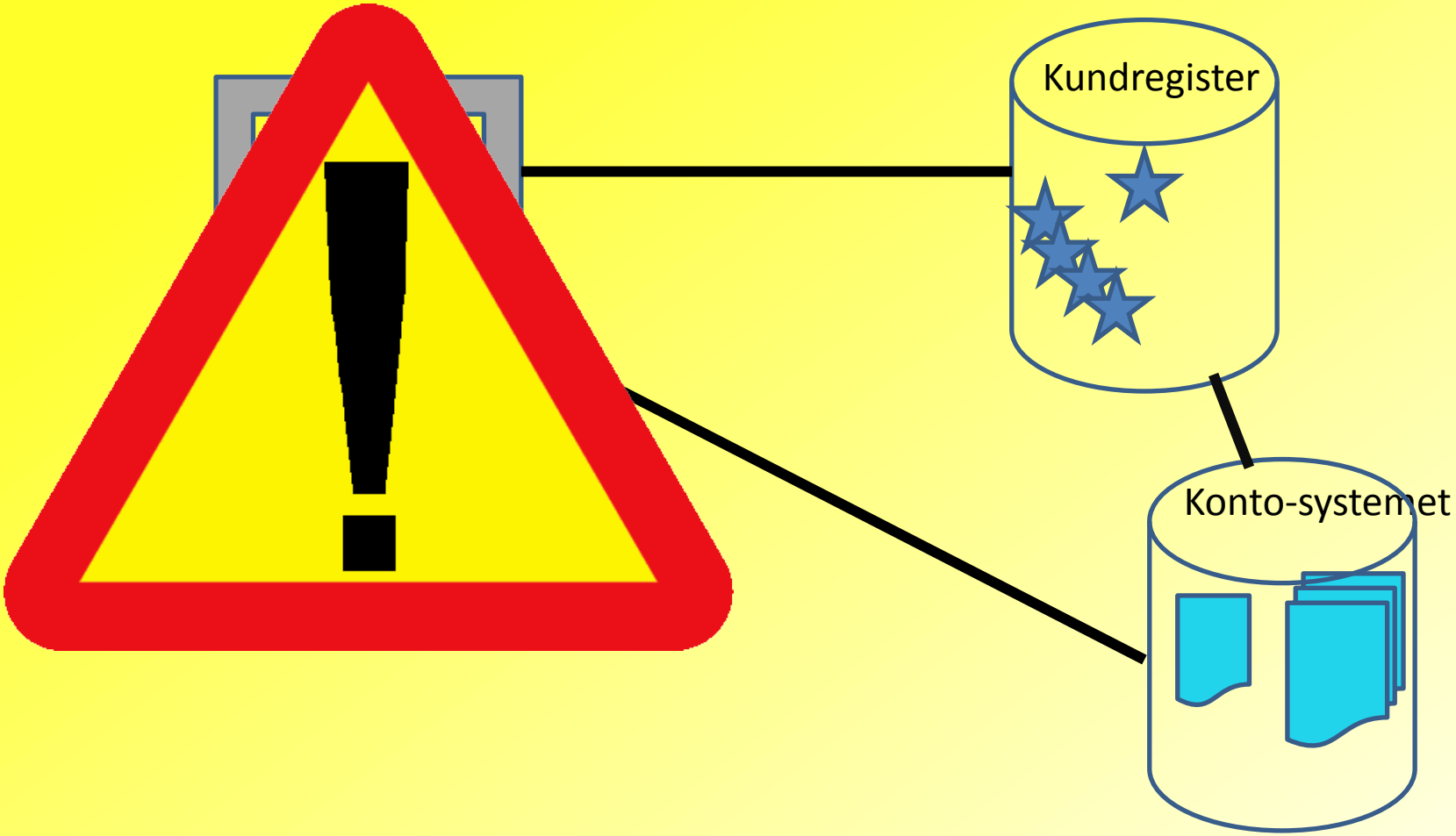
Bankomatexempel

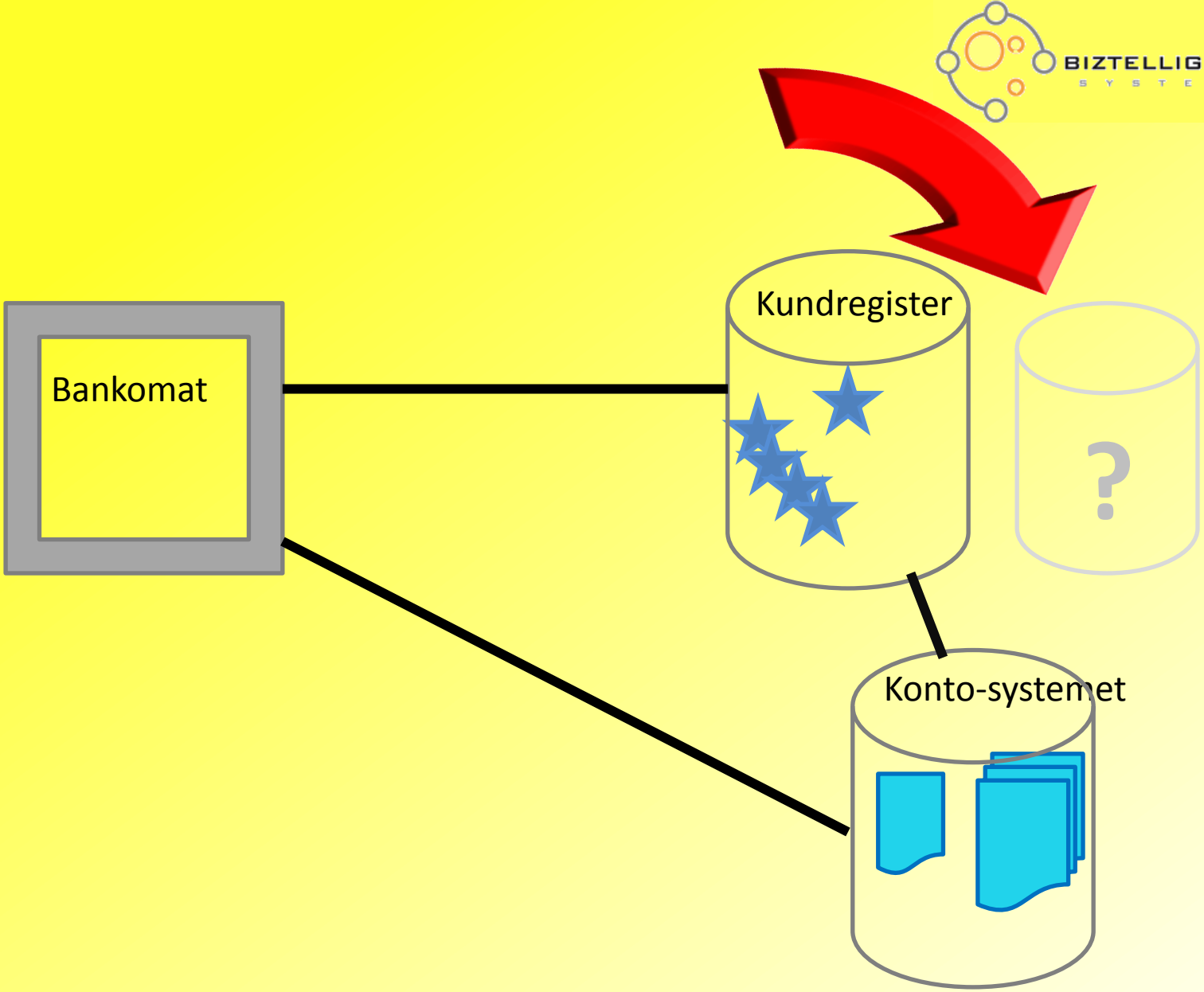


Bankomatexempel



Bankomatexempel




BIZTELLIGENT
SYSTEMS
Bankomat
Kundregister
?
Konto-systemet

KOSTNAD?

Planerad testomgång			Timmar	Kronor
	nyckelresurser		40	40.000
	projektmedlemmar		60	60.000
			Summa	100.000
OPLANERADE KOSTNADER				
Utredning fel				
	nyckelresurser		30	30.000
	projektmedlemmar		20	20.000
Felrättning				
	nyckelresurser		60	60.000
	projektmedlemmar		15	15.000
Ställtid/väntetid				
	projektmedlemmar	två veckor, 5 personer, avrundning	300	300.000
Releasearbete				
	nyckelresurser		20	20.000
Omkörning testfall				
	nyckelresurser		40	40.000
	projektmedlemmar		40	40.000
Tot för projekt X				**525.000**
Hur mycket kostade felet för de andra projekten?				

Systemanalys 2: Testsystemet

Fokus på *skillnad* mellan testsystem och produktionssystem

Alla skillnader behöver vara kända.

Skillnader **behöver** inte innebära problem.

När vi inte vet **exakta** skillnader, då har vi problem!

Exempel på skillnader

- Alla kopplingar ”ut”
- Dyrt med exakta kopior
- Konfiguration, kodversioner, systemkopplingar . . .

Systemanalys 1 och 2:

1. Analysera **alla aspekter** av **produktionssystemet!**

2. Analysera **skillnaderna mot testsystemet!**

Systemanalys 3

Analys av IT-säkerheten i systemet, för att:

1. **Kartlägga funktioner och data som har IT-säkerhetsrelevans**

2. **Prioritera och riskklassa för att kunna satsa mest och tidigast på viktigast/mest kritiskt**

Systemanalys 3

- **Analys av IT-säkerhetsfunktioner kan vem som helst göra**

- **Prioritering och klassning måste göras av alla gemensamt**

(Använda Common Criteria som stöd)

Common Critera

- Common Criteria: internationellt erkänd standard för IT-säkerhet

(FMV Svenskt Certifieringsorgan)

- I detta sammanhang tänkt som ***stöd*** för **identifiering av säkerhetsfunktioner**

(bestämma företagets skyddsklass)

Table of contents

8 CLASS FAU: SECURITY AUDIT 29
8.1 Security audit automatic response (FAU_ARP) 30
8.2 Security audit data generation (FAU_GEN) 31
8.3 Security audit analysis (FAU_SAA) 33
8.4 Security audit review (FAU_SAR) 37
8.5 Security audit event selection (FAU_SEL) 39
8.6 Security audit event storage (FAU_STG) 40

9 CLASS FCO: COMMUNICATION 43
9.1 Non-repudiation of origin (FCO_NRO) 44
9.2 Non-repudiation of receipt (FCO_NRR) 46

10 CLASS FCS: CRYPTOGRAPHIC SUPPORT 48
10.1 Cryptographic key management (FCS_CKM) 49
10.2 Cryptographic operation (FCS_COP) 52

11 CLASS FDP: USER DATA PROTECTION 54
11.1 Access control policy (FDP_ACC) 57
11.2 Access control functions (FDP_ACF) 59
11.3 Data authentication (FDP_DAU) 61
11.4 Export from the TOE (FDP_ETC) 63
11.5 Information flow control policy (FDP_IFC) 65
11.6 Information flow control functions (FDP_IFF) 67
11.7 Import from outside of the TOE (FDP_ITC) 72
11.8 Internal TOE transfer (FDP_ITT) 74
11.9 Residual information protection (FDP_RIP) 77
11.10 Rollback (FDP_ROL) 79
11.11 Stored data integrity (FDP_SDI) 81
11.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT) 83
11.13 Inter-TSF user data integrity transfer protection (FDP_UIT) 84

12 CLASS FIA: IDENTIFICATION AND AUTHENTICATION 87
12.1 Authentication failures (FIA_AFL) 89
12.2 User attribute definition (FIA_ATD) 91
12.3 Specification of secrets (FIA_SOS) 92
12.4 User authentication (FIA_UAU) 94
12.5 User identification (FIA_UID) 99
12.6 User-subject binding (FIA_USB) 101

13 CLASS FMT: SECURITY MANAGEMENT 103
13.1 Management of functions in TSF (FMT_MOF) 105
13.2 Management of security attributes (FMT_MSA) 106
13.3 Management of TSF data (FMT_MTD) 110
13.4 Revocation (FMT_REV) 113
13.5 Security attribute expiration (FMT_SAE) 114
13.6 Specification of Management Functions (FMT_SMF) 115
13.7 Security management roles (FMT_SMR) 116

14 CLASS FPR: PRIVACY 118
14.1 Anonymity (FPR_ANO) 119
14.2 Pseudonymity (FPR_PSE) 120
14.3 Unlinkability (FPR_UNL) 122
14.4 Unobservability (FPR_UNO) 123

15 CLASS FPT: PROTECTION OF THE TSF 126
15.1 Fail secure (FPT_FLS) 128
15.2 Availability of exported TSF data (FPT_ITA) 129
15.3 Confidentiality of exported TSF data (FPT_ITC) 130
15.4 Integrity of exported TSF data (FPT_ITI) 131
15.5 Internal TOE TSF data transfer (FPT_ITT) 133
15.6 TSF physical protection (FPT_PHP) 136
15.7 Trusted recovery (FPT_RCV) 139
15.8 Replay detection (FPT_RPL) 142
15.9 State synchrony protocol (FPT_SSP) 143
15.10 Time stamps (FPT_STM) 145
15.11 Inter-TSF TSF data consistency (FPT_TDC) 146
15.12 Testing of external entities (FPT_TEE) 147
15.13 Internal TOE TSF data replication consistency (FPT_TRC) 148
15.14 TSF self test (FPT_TST) 149

16 CLASS FRU: RESOURCE UTILISATION 151
16.1 Fault tolerance (FRU_FLT) 152
16.2 Priority of service (FRU_PRS) 154
16.3 Resource allocation (FRU_RSA) 156

17 CLASS FTA: TOE ACCESS 158
17.1 Limitation on scope of selectable attributes (FTA_LSA) 159
17.2 Limitation on multiple concurrent sessions (FTA_MCS) 160
17.3 Session locking and termination (FTA_SSL) 162
17.4 TOE access banners (FTA_TAB) 165
17.5 TOE access history (FTA_TAH) 166
17.6 TOE session establishment (FTA_TSE) 167

18 CLASS FTP: TRUSTED PATH/CHANNELS 168
18.1 Inter-TSF trusted channel (FTP_ITC) 169
18.2 Trusted path (FTP_TRP) 171

Common Criteria,
Security functional components

Table of contents

8 CLASS FAU: SECURITY AUDIT 29
8.1 Security audit automatic response (FAU_ARP) 30
8.2 Security audit data generation (FAU_GEN) 31
8.3 Security audit analysis (FAU_SAA) 33
8.4 Security audit review (FAU_SAR) 37
8.5 Security audit event selection (FAU_SEL) 39
8.6 Security audit event storage (FAU_STG) 40

9 CLASS FCO: COMMUNICATION 43
9.1 Non-repudiation of origin (FCO_NRO) 44
9.2 Non-repudiation of receipt (FCO_NRR) 46

10 CLASS FCS: CRYPTOGRAPHIC SUPPORT 48
10.1 Cryptographic key management (FCS_CKM) 49
10.2 Cryptographic operation (FCS_COP) 52

11 CLASS FDP: USER DATA PROTECTION 54
11.1 Access control policy (FDP_ACC) 57
11.2 Access control functions (FDP_ACF) 59
11.3 Data authentication (FDP_DAU) 61
11.4 Export from the TOE (FDP_ETC) 63
11.5 Information flow control policy (FDP_IFC) 65
11.6 Information flow control functions (FDP_IFF) 67
11.7 Import from outside of the TOE (FDP_ITC) 72
11.8 Internal TOE transfer (FDP_ITT) 74
11.9 Residual information protection (FDP_RIP) 77
11.10 Rollback (FDP_ROL) 79
11.11 Stored data integrity (FDP_SDI) 81
11.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT) 83
11.13 Inter-TSF user data integrity transfer protection (FDP_UIT) 84

12 CLASS FIA: IDENTIFICATION AND AUTHENTICATION 87
12.1 Authentication failures (FIA_AFL) 89
12.2 User attribute definition (FIA_ATD) 91
12.3 Specification of secrets (FIA_SOS) 92
12.4 User authentication (FIA_UAU) 94
12.5 User identification (FIA_UID) 99
12.6 User-subject binding (FIA_USB) 101

13 CLASS FMT: SECURITY MANAGEMENT 103
13.1 Management of functions in TSF (FMT_MOF) 105
13.2 Management of security attributes (FMT_MSA) 106
13.3 Management of TSF data (FMT_MTD) 110
13.4 Revocation (FMT_REV) 113
13.5 Security attribute expiration (FMT_SAE) 114
13.6 Specification of Management Functions (FMT_SMF) 115
13.7 Security management roles (FMT_SMR) 116

14 CLASS FPR: PRIVACY 118
14.1 Anonymity (FPR_ANO) 119
14.2 Pseudonymity (FPR_PSE) 120
14.3 Unlinkability (FPR_UNL) 122
14.4 Unobservability (FPR_UNO) 123

15 CLASS FPT: PROTECTION OF THE TSF 126
15.1 Fail secure (FPT_FLS) 128
15.2 Availability of exported TSF data (FPT_ITA) 129
15.3 Confidentiality of exported TSF data (FPT_ITC) 130
15.4 Integrity of exported TSF data (FPT_ITI) 131
15.5 Internal TOE TSF data transfer (FPT_ITT) 133
15.6 TSF physical protection (FPT_PHP) 136
15.7 Trusted recovery (FPT_RCV) 139
15.8 Replay detection (FPT_RPL) 142
15.9 State synchrony protocol (FPT_SSP) 143
15.10 Time stamps (FPT_STM) 145
15.11 Inter-TSF TSF data consistency (FPT_TDC) 146
15.12 Testing of external entities (FPT_TEE) 147
15.13 Internal TOE TSF data replication consistency (FPT_TRC) 148
15.14 TSF self test (FPT_TST) 149

16 CLASS FRU: RESOURCE UTILISATION 151
16.1 Fault tolerance (FRU_FLT) 152
16.2 Priority of service (FRU_PRS) 154
16.3 Resource allocation (FRU_RSA) 156

17 CLASS FTA: TOE ACCESS 158
17.1 Limitation on scope of selectable attributes (FTA_LSA) 159
17.2 Limitation on multiple concurrent sessions (FTA_MCS) 160
17.3 Session locking and termination (FTA_SSL) 162
17.4 TOE access banners (FTA_TAB) 165
17.5 TOE access history (FTA_TAH) 166
17.6 TOE session establishment (FTA_TSE) 167

18 CLASS FTP: TRUSTED PATH/CHANNELS 168
18.1 Inter-TSF trusted channel (FTP_ITC) 169
18.2 Trusted path (FTP_TRP) 171

Ägandeskap och förvaltning

. . . av analyserna

- Produktionssystemet: arkitekt/systemägare . .
- Testsystemet: testavdelningen!
- IT-säkerheten: beslutas av företaget

Ansvar

Vi har alla ett ansvar för att systemanalyserna

- Är relevanta (granska)
- Är korrekta (gör egna systemanalyser)
- Är begripliga och kända!

Sammanfattning

1. **Produktionssystemets** alla aspekter exempelvis *både* fysisk och logisk struktur

2. **Testsystemets** skillnader mot produktionsys

3. **Informations-säkerheten** kartlagd, prioriterad och riskklassad (funktioner och data)

Lönsamt

effektivt, återanvändbart, tillgängligt, prioriteringar klara, förvaltningsbart

Lätt

fastställt, tydliga testfall, begripligt

Roligt

testdata lätt, omtestning tydligt, tydliga testfall, alla ”med i båten”

FRÅGOR?

Mail: rosemarie.arnmark@biztelligent.se

Hemsida : www.arnmark.se (OBS! Pågående omläggning är klar vecka 48)

Du hittar bland annat olika tipslistor, ex Kravställarens resp. Testledarens hetaste tips, Vanligaste myterna med mera.