GTP Info KP

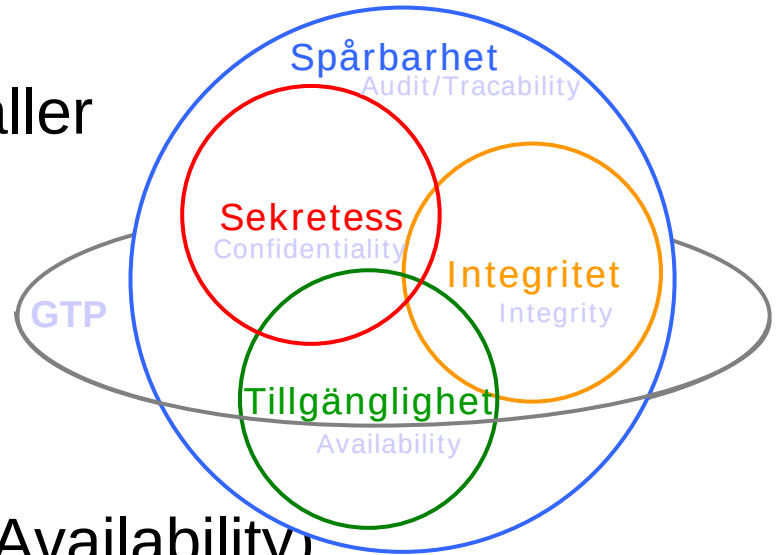
081113

Jaan Haabma
Jaan.haabma@basesoft.se

P-O Risberg
per-ola.risberg@logica.com

FM GTP 3

- GTP - FM Generell Teknisk Plattform
- En IT-infrastruktur som bl a tillhandahåller säkerhet för nätverksbaserade tillämpningar (”SOA”)
  - såväl COTS som specialutvecklade
- Säkerhet - ”CIA” + spårbarhet
  - (C - Confidentiality, I - Integrity, A - Availability)
- Kryptoverifierad, Säkerhetsgranskad mot KSF H/TS
- MUST yttrande --H/TS
- Kan användas för H/TS, H/S, H/C, H/R och öppet
  – konfigurerbara mekanismer för olika behov
- Fritt tillgänglig inom FM och FMV



Säkerhetslösning för FM krav

• Behörighetskontroll	✓
• Inloggning	✓
• Autentisering	✓
• Åtkomstkontroll	✓
• Säkerhetsloggning	✓
• Skydd mot obehörig avlyssning	✓ RÖS, KRY utrustning mm kan behövas
• Intrångsskydd	✓ Brandvägg mm förutsätts för extern komm.
• Intrångsdetektering	✓ Regler förutsätts vara definierade
• Skydd mot skadlig kod	✓
• Funktioner för tillgänglighet	✓
• Funktioner för riktighet (Integritet)	✓
• Stark Autentisering (TAK2)	✓
• Förstärkt inloggning (TEID)	✓
• Framtagen enligt Common Criteria EAL4+	✓
• Kryptoverifierad H/S, H/TS	✓
• Lösning granskad separat mot MUST krav, H/TS	✓
• Yttrande från MUST avseende produkten finns	✓
• Använd i ackrediterade system H/TS, H/S	✓
• Lösning huvudsakligt skydd i ackrediterat system	✓

Funktioner

Single
Sign-On

Administration
Användare, Behörigheter, CRL,
LoggAnalys, Övervakning, Larm

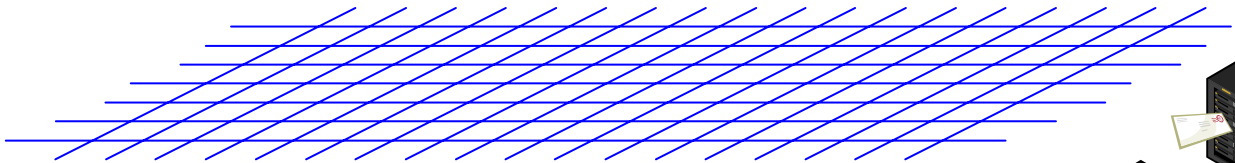
Office

Fil-
åtkomst

E-Post

WEB

Terminal
emulering



GTP Tjänster i ”nätet”

Filserver

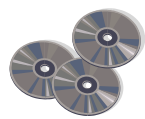
Mailserver

Webserver

Antivirus

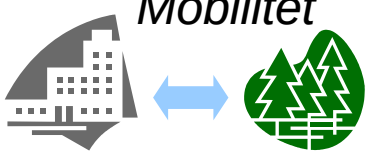
**Säkerhets-
Server**

PKI - SSO
Nyckeldistribution
Kryptering (olika alg, symm/asym)
Integritet
Åtkomstkontroll
Loggning
Övervakning/Styrning
Kapsling säk-/arvsprotokoll



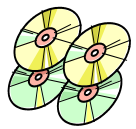
Installations-
Media
(installations server)

Mobilitet



Administrationsmeny

”Deployment”



Steg 2

GTP programvara / komponenter
installeras i de klienter och servrar som skall skyddas

Steg 1

Säkerhetsserver
(appliance)
kopplas in på nätverket

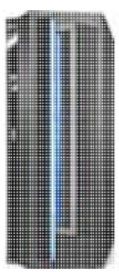
Steg 3a
(Option)

Mellandator
(appliance)
skyddar legacy system

Steg 3b
(Option)

Tillämpnings-server
(SFS, mail, web, …)
ger ytterligare tjänster

Windows Server
eller
Unix server



Legacy
System

Steg 4 Konfigurera säkerhetspolicies

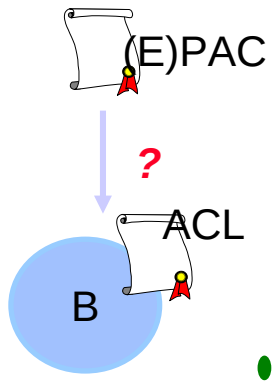
GTP Komponenter

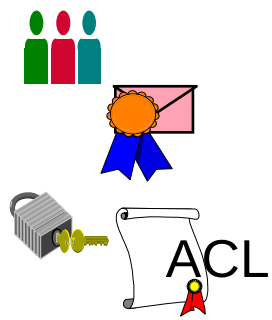
Exempel: Behörighetskontroll och Säkerhetsloggning

Tiden medger inte genomgång av komponenter för övriga GTP säkerhetsfunktioner.

Behörighetskontroll

- SSO (Single-Sign-On)
  - Windows (domän eller ”stand-alone”), UNIX, COTS
  - Windows GINA, UNIX PAM, agenter för olika COTS/system
  - Fjärrterminal – Citrix, WTS, telnet etc.
- Stöd för olika ”token”
  - Stark autentisering med FM TAK2
  - Förstärkt inloggning med FM TEID
  - Annat: lösen, ”mjuka” certifikat, …
- Åtkomstkontroll
  - Delegering, impersonifiering, tjänste-kedjor
  - Olika policies: separation av ansvar, roller/grupper etc.
  - Ömsesidig autentisering (alla subjekt – objekt/subjekt i nätet)
- Administration
  - SysA: PKI, olika CA, policies, attribut, Windows, UNIX, COTS
  - SecAdm: åtkomstregler, policies, delegering, …





Säkerhetsloggning

Användare
Program
Nod

Loggning
Autentisering

Konsument

Producent/
Konsument

Producent

Loggning
Administrativa
åtgärder

Loggning
Åtkomst-
kontroll

Applikations-
loggning

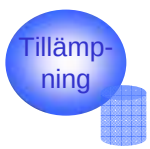
Windows XP
Loggar

Windows
2003server
Loggar

Insamling

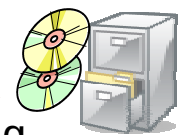
Unix
Loggar

Nätverks-
utrustning
Loggar

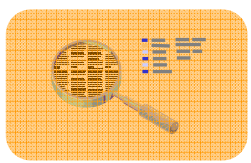


Urval relevanta
Tillämpnings-
loggar

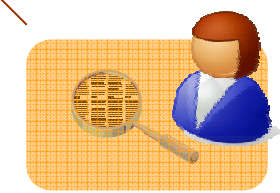
LogS
logg-
server



Arkivering



Regelbaserad
Automatisk
Analys



Manuell Analys
SQL-frågor
Rapporter

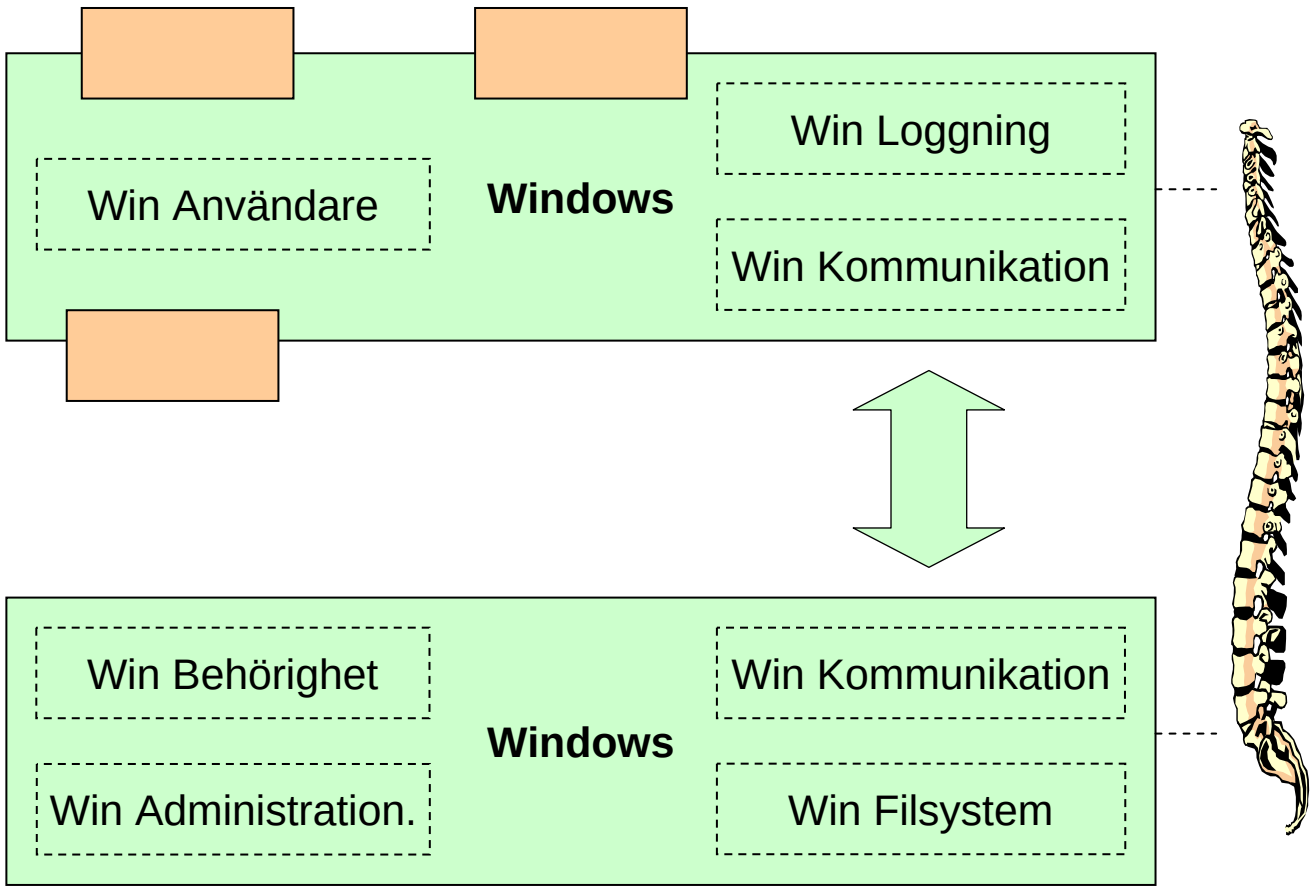
- Loggning av säkerhetshändelser
- Applikations logg
- Insamling av loggar
- Automatisk och manuell analys
- Arkivering
- Överföringen är skyddad
- Loggar är integritets-övervakade

Säkerhetsarkitektur

Säkerhetsfunktion i produkter

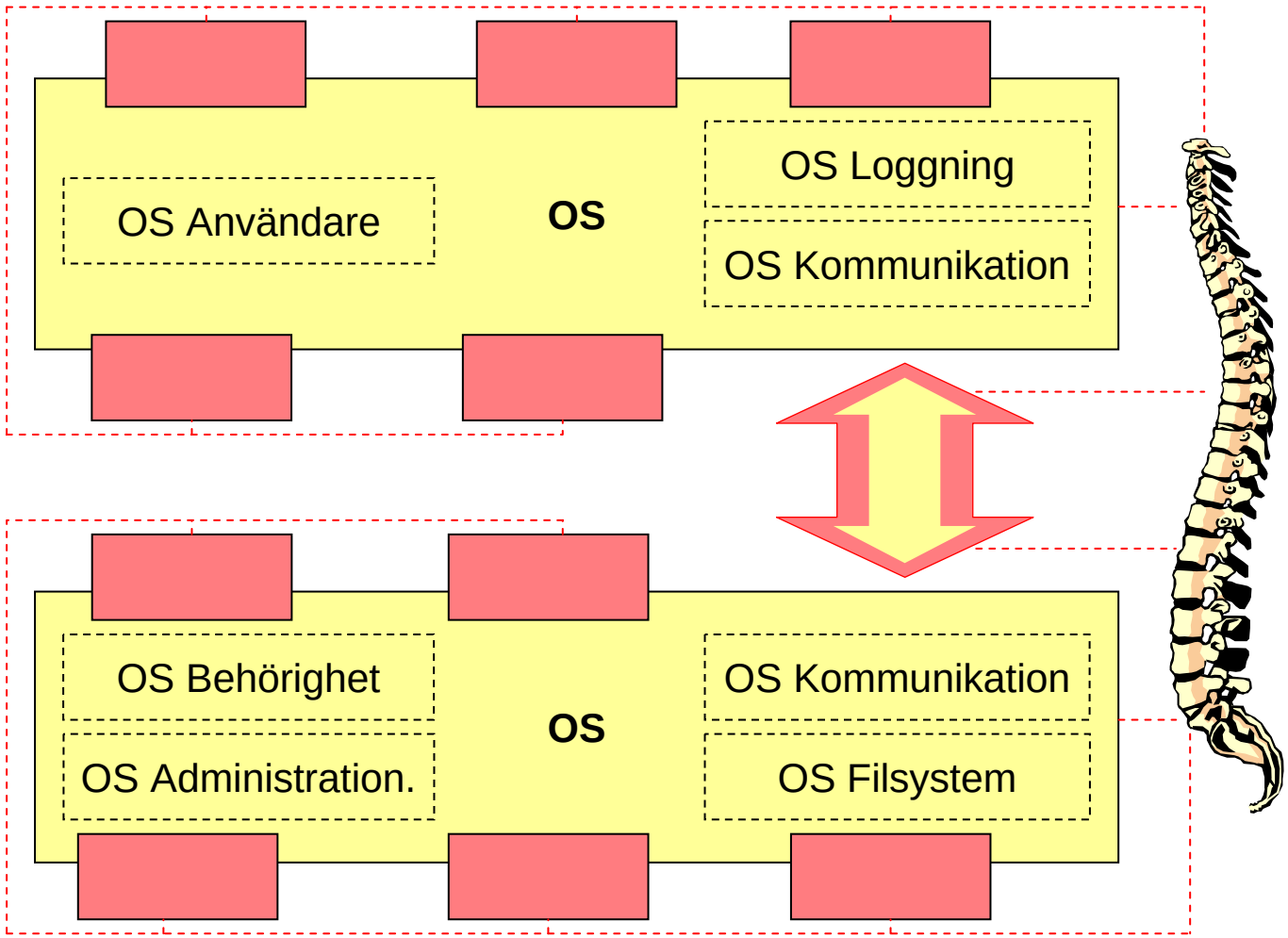
- Behörighetskontroll
  - SSO (Single-Sign-On, PKI, TAK/TEID…)?
    - GTP
  - Inloggning (OS – Windows, UNIX, …)?
    - SITS (ts, tty/aix), SD (windows), CUAP (windows), GTP (infrastruktur, windows, ts, unix)
  - Autentisering (subjekt – objekt/subjekt)?
    - GTP
  - Åtkomstkontroll (subjekt – objekt/subjekt)?
    - GTP
- Säkerhetsloggning
  - …
- Skydd mot skadlig kod
  - …
- Intrångsskydd, Intrångsdetektering
  - …
- Funktioner för tillgänglighet, riktighet (Integritet)
  - …

Exempel – integration i Windows



- Windows utgör säkerhetsbärande ”ryggrad” – säkerhetsarkitektur.
- Integration i Windows medför beroende av Windows säkerhets-mekanismer.
- Begränsar vilken assurans som kan uppnås.
- Begränsar vilka informationsklasser som kan stödas.
- Stöder endast Windows.

Exempel – OS oberoende säkerhetsarkitektur



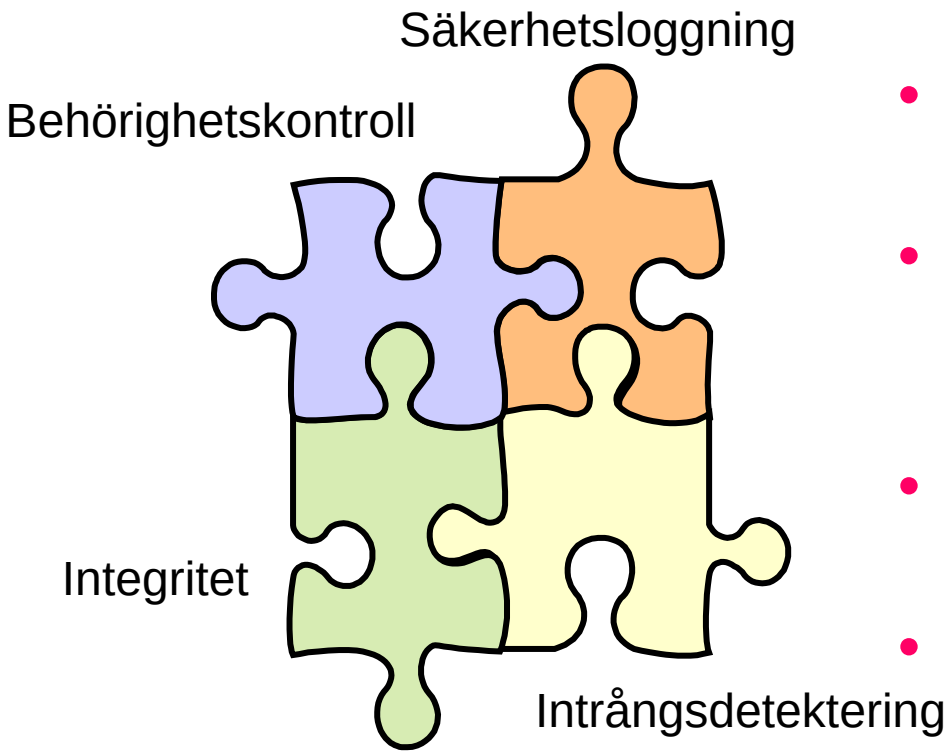
- Separata säkerhetsmonitorer och kommunikation bygger upp säkerhetsfunktioner.
- OS-neutral säkerhetsbärande ”ryggrad” – säkerhets-arkitektur (IRMA).
- Integrerar mot OS, men är inte beroende av OS säkerhets-mekanismer
- Hög assurans kan uppnås.
- Även högre informationsklasser kan stödas.
- Stöder olika OS.

Säkerhetsarkitektur – IRMA

Independent Reference Monitor Architecture

- TCB (Trusted Computing Base)
  - Litet, avgränsat, oberoende referensmonitorer, granskningsbart, integrationspunkter…
  - Tjänsteorienterat, avgränsade komponenter med tydlig funktion och specificerade gränsytor, … SOA
- Säkerhetsfunktioner
  - Behörighetskoll – Identifiering (inte bara inloggning, utan ömsesidig auth subjekt-/objekt/subjekt mm), åtkomstkontroll, säkerhetsloggning, …
  - Även övriga säkerhetsfunktioner enligt KSF plus Integritet och Tillgänglighet
    - Säkerhetsloggning, Skydd mot skadlig kod, Intrångsskydd, Intrångsdetektering, Skydd mot skadlig kod, Funktioner för tillgänglighet, Funktioner för riktighet (Integritet)
- Tjänster
  - Säkerhetsfunktioner i nätet enligt SOA …
- Komponenter
  - COTS/GOTS – Windows, TTP (Citrix), WTS, KrAPI
  - GTP – SecL, SysA, LogS, …

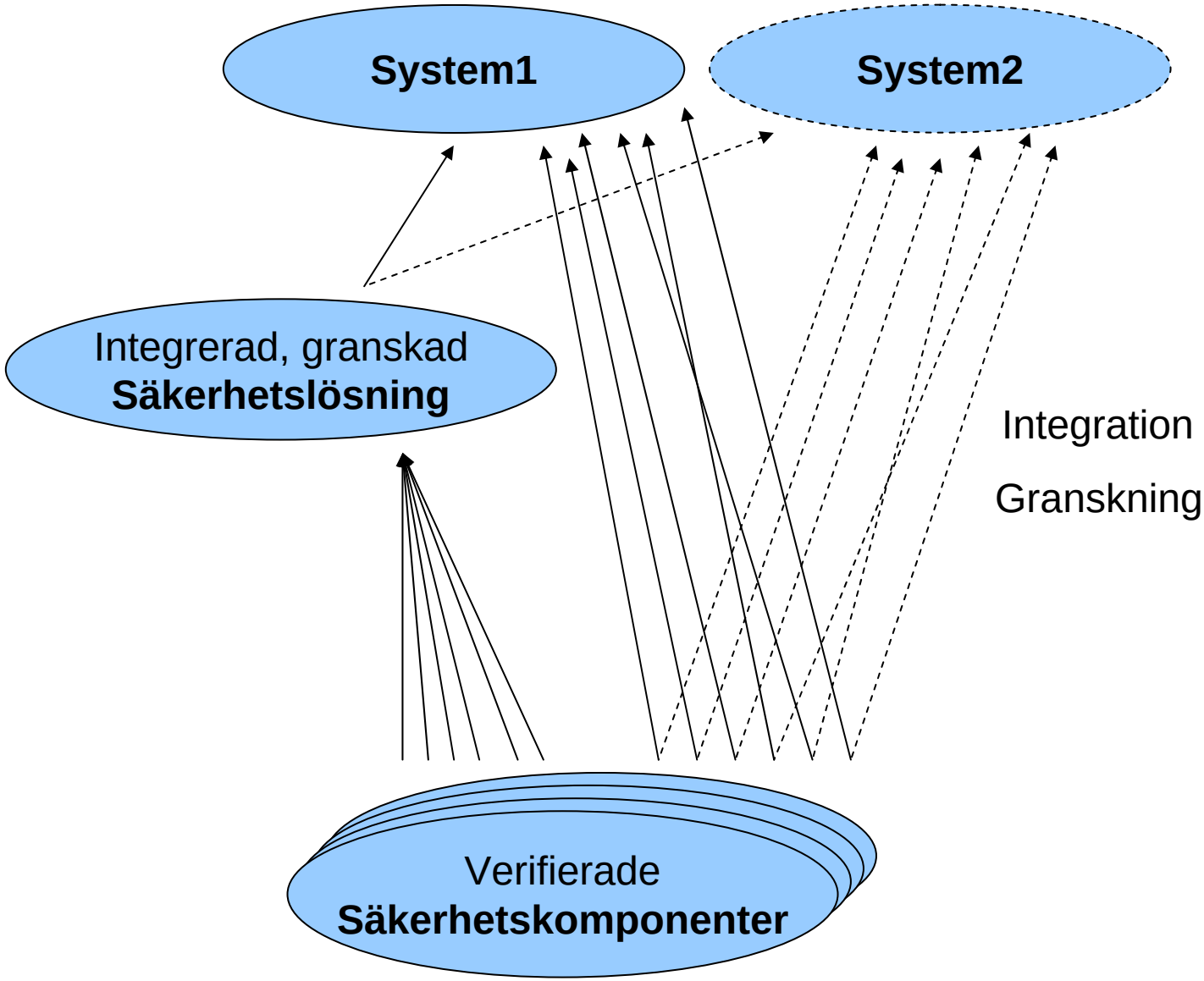
GTP säkerhetskomponenter



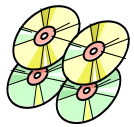
- GTP kan nyttjas i alla system som har Windows eller UNIX.
- GTP har en från Windows/ UNIX/etc. oberoende ”säkerhetsmotor”.

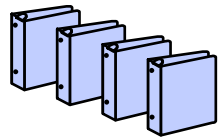
- GTP har en väldefinierad generell säkerhetsarkitektur (IRMA)
- GTP kan användas som integrationsplattform eller komponentvis
- De GTP komponenter/ tjänster som väljs passar ihop från början!
- Respektive GTP tjänst/ komponent har var och en, en väldefinierad roll i arkitekturen och tillhandahåller väldefinierade tjänstegränsytor för användning och integration.

Säkerhetslösning eller säkerhetskomponenter?

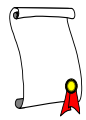


Sammanfattning





- Programvara
- Dokumentation
- Tekniskt Ackrediteringsunderlag (TAU)
- Kryptoverifierat, Säkerhetsgranskat, MUST yttrande



- Stöd/support
  - Produktsupport (produktleverantör Logica/Basesoft)
  - Ramavtal för enkelt avrop av GTP-tjänster

- Kontaktinfo:
  - Anders Wretö, FMV anders.wreto@fmv.se
  - Barbro Norlander, FMV barbro.norlander@fmv.se
  - P-O Risberg, Logica per.ola.risberg@logica.com
  - Jaan Haabma, Basesoft jaan@basesoft.se

SLUT