CSI – Common Security Infrastructure
GTP Next Generation

www.fmgtp.se

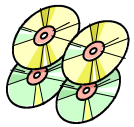
Agenda

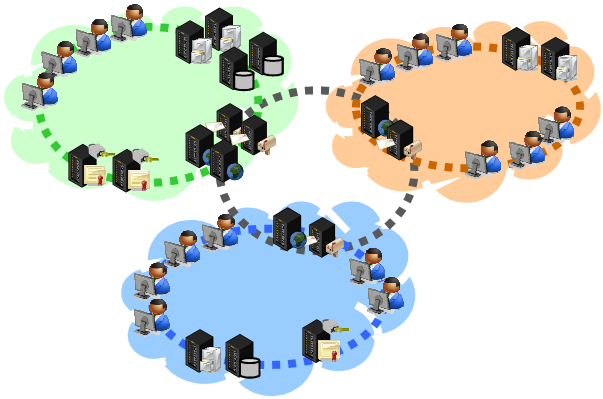
- Introduktion
- Demonstration
- Q&A

Introduktion

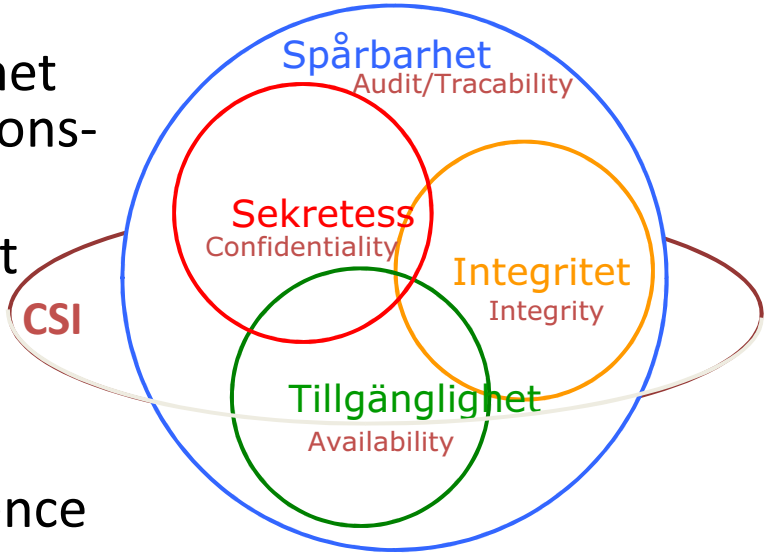
CSI – Common Security Infrastructure

- Teknisk IT-infrastruktur med samverkande säkerhetskomponenter som ger en säker driftsmiljö för nätverks- och tjänste-baserade tillämpningar
- Programvaruprodukt –
  - CD/DVD media
  - färdig CSI säkerhetsserver att koppla in på nätet





- Säkerhetsprodukter för att uppfylla krav på sekretess, integritet, tillgänglighet och spårbarhet i verksamhetsfunktioner för alla slags informations- och ledningssystem
- Kan användas för H/TS, H/S, H/C, H/R och öppet – konfigurerbara mekanismer för olika behov
- Standardprodukt – färdig att använda
- Modern operativsystemoberoende säkerhetsarkitektur (IRMA, Independent Reference Monitor Architecture) – för hög assurans



CSI Functions

- Single Sign-On - PKI
- Mutual authentication
- Access control
- Delegation of credentials
- Communications encryption
- Pluggable security tokens and algorithms
- Unified administration
- Identity Management
- Integrity control
- Security logs/audit, collection of logs
- Log analyses (automatic and manual)
- Secure program/service start/activation
- Surveillance and control
- Common message console
- Secure remote terminals (telnet, Citrix and Windows Terminal Services)
- Secure web access, email and other communication in TCP/IP networks

CSI - Network Centric Security

Common Security Infrastructure

CSI PKI

Identity Agents

Identity Management meta catalogue

Trusted CA (multiple) that manages certificates and Certificate Revocation Lists

Maintain audit of events based on strong authentication and authorization

CSI Single Sign-On

Authentication

CSI Policy Manager

CSI advanced Kerberos engine

CSI Security logging

Other logs

End to End encryption

CSI Access Control

Domain - protected information & resources

CSI runtime Configuration Control

CSI Event Handling

CSI Integrity

Web Server

Mail Server

Custom/ Bespoke Apps

Legacy Terminal Apps

Secure Info-store

Other Network Services

Windows, Unix, Virtualization

Dynamic access decisions based on relationship between user (subject) and data (object)

Ensure that the right people access the right resources with authentication and authorization policies

CSI tjänster i nätverk

Single
Sign-On

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

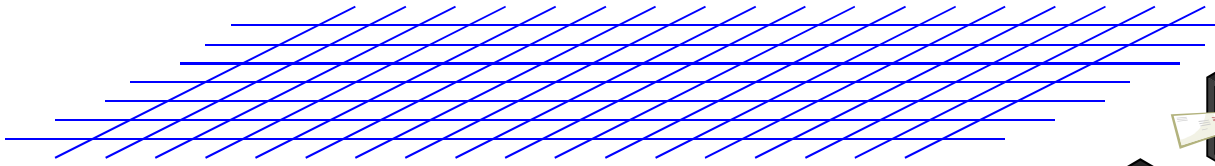
Office

Fil-
åtkomst

E-Post

WEB

Terminal
emulering



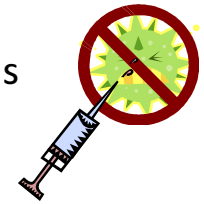
Filserver

Mailserver

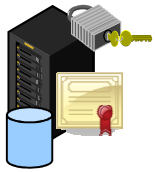
Webserver

CSI Tjänster i ”nätet”

Antivirus



Säkerhets-
Server

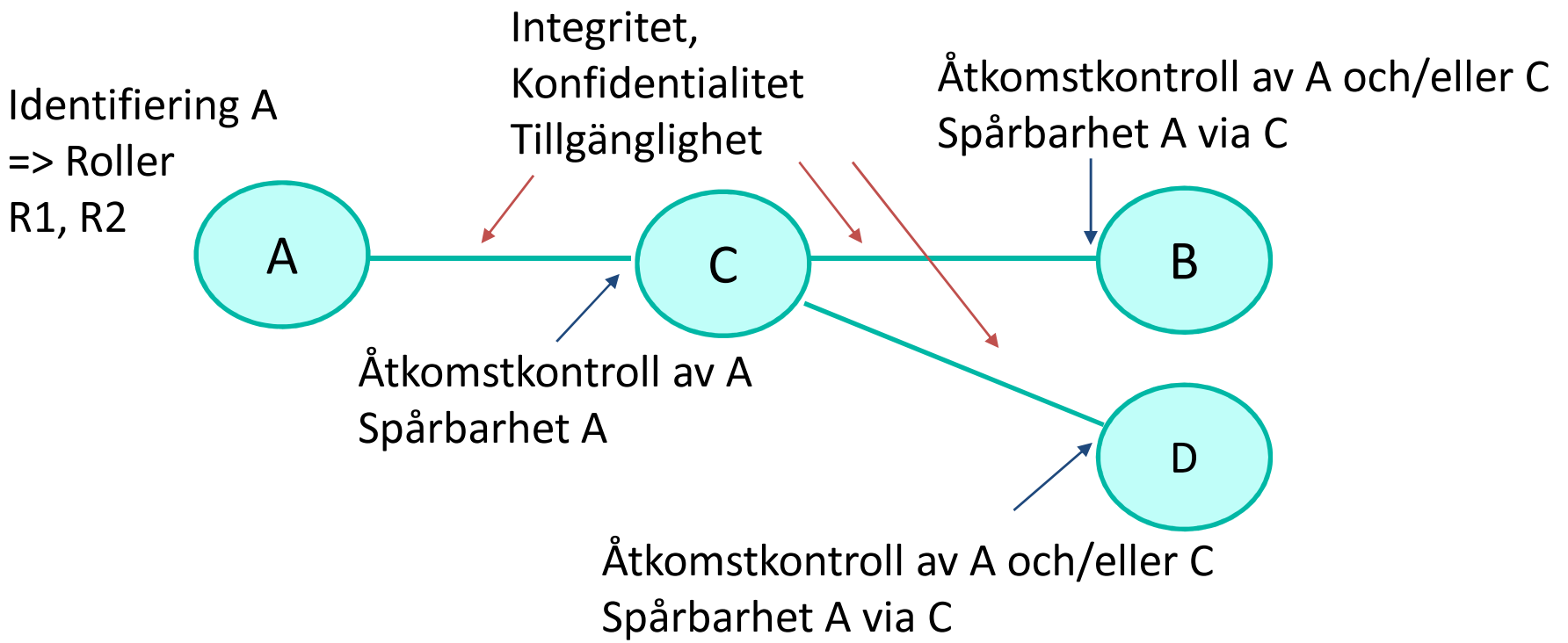


Identity Management – SSO, PKI
Nyckeldistribution
Kryptering (olika alg, symm/asym)
Integritet
Åtkomstkontroll
Loggning
Övervakning/Styrning
Kapsling säk-/arvsprotokoll

Installations-
Media
(installations server)

Mobilitet

Enhetlig, sammanhållen säkerhetsarkitektur

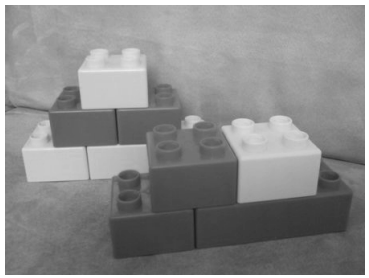


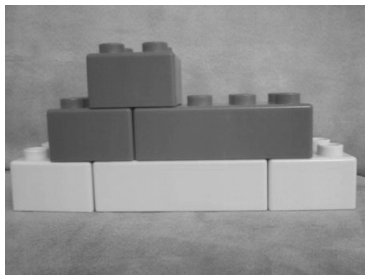
- Designenheter – komponenter, gränsytor, tjänster, processer, operationer, informationsobjekt.
- Säkerhetsobjekt – {Subjekt, Objekt} -- Principaler, Behörigheter, Åtkomstregler.
- Alla Subjekt (processer - A, B, C) identifieras ömsesidigt sinsemellan
- För all åtkomst {Subjekt} –> {Subjekt, Objekt} sker åtkomstkoll och loggning
- All samverkan {Subjekt} -> {Subjekt, Objekt} skyddas med unik sessionsnyckel {integritet, konfidentialitet}$SK_{p1,p2}$

Komponenter som passar ihop

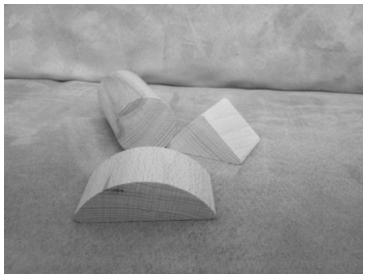
- Välj komponenter efter behov
- Konfigurera mekanismer efter behov
- Alla säkerhetskomponenter passar ihop
- Säkerhetsarkitektur – inkl ”säkerhetsbuss” – oberoende av operativsystem (IRMA)
- Assuransarkitektur – hantera ”osäkerhet” i Windows

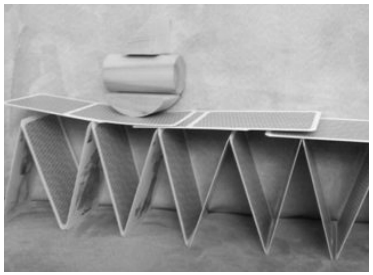
CSI





XYZ?





CSI Highlights

- Protection in depth – information / resource centric, assume “dimensioning” threat to be the “insider”
- Reviewed and recommended for use up to Top Secret and proven in use by SwAF GTP
- High assurance - Independent Reference Monitor Architecture - IRMA
- Flexible, “pluggable” security mechanisms – authentication tokens, encryption mechanisms, application protocols support
- Configurable, descriptive security configuration – identity management, PKI, role and rule based access control, encryption
- Collaboration – multiple and concurrent security authorities and mechanisms in parallel

CSI jämfört med GTP

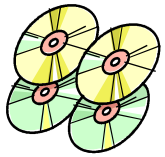
- Fler systemmiljöer WindowsXP – Windows7, UNIX …
- Inga ”förbestämda” versioner av Office, Windows etc som i GTP
- Flexibilitet – fler valmöjligheter komponenter/mekanismer
- Ökad pluggbarhet – olika token, mekanismer, säkerhets-/ kommunikations –bussar att välja mellan
- Standardprodukt – färdig att installera, ingen egen utveckling behövs
- Enkelhet
  - CSI komponenter installeras som standarprogram
  - användning inkl säkerhet konfigureras (ingen egen utveckling behövs)
  - färdig ”appliance” säkerhetsserver för drift och som installationsserver
- Komponenter för olika krav - öppet, kommersiell sekretess, Hemligt/R, H/C, H/S, H/TS
- Versionsuppdatering av tidigare granskade GTP 3 och GTP 4

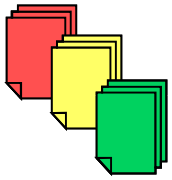
Säkerhetslösning för FM krav (ex KSF)

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)	✓	

CSI – NISP, NCOE/NC3TA, FMLS TS TA/RA, IRMA

CSI

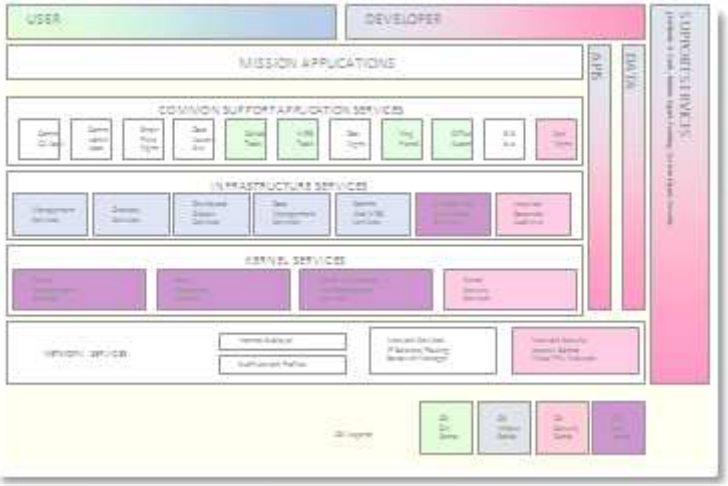




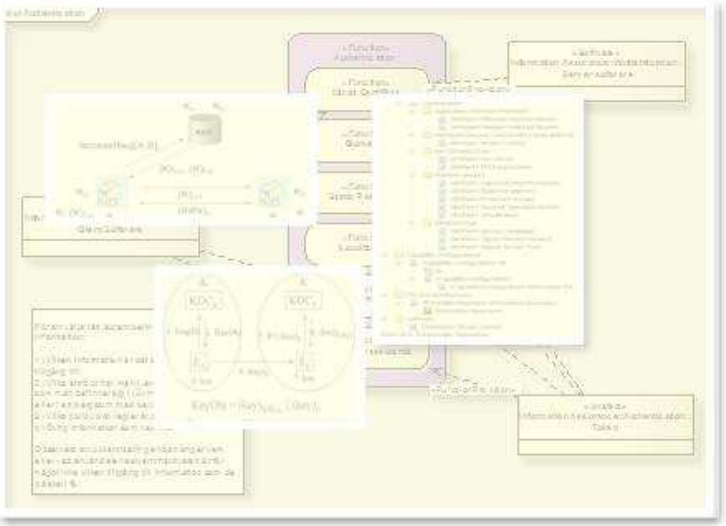
CSI – NISP IA

GTP product		NISP keyword
Security		IA - Information Assurance
Sec_	Secure Login	Single Sign On
SFA	Secure File Archive	Single Sign On
SysA	System Administration	User Mgmt, (Single-Sign On, Auditing)
SecS	Security Services	Confidentiality
SUS	Start-Up Service	Availability
RTCS	RunTime Configuration Services	Availability
SSMS	System Surveillance & Mgmnt Services	Manageability
LogS	Log Services	Auditing
ComE	Communications Encapsulation	Confidentiality
IntG	Integrity Guar	Integrity
CMC	Common Message Console	Manageability
AKE	Advanced Kerberos Engine	Confidentiality, (Single Sign-On, Integrity, Non Repudiation, Timestamping)
AV	AntiVirus	Malicious Code Detection
CHS	Conflict Handling Services	Availability
LNS	Logical Name Services	Availability
TNS	TeS Install & Verify	Manageability
Port Services		
SFS	Secure File Server	STO - Storage
Mail	Mailserver	MSG - Messaging
Web	Webserver	COL - Collaboration
HR Support		
GTS	Game Time Services	
RoleS	Role Services	

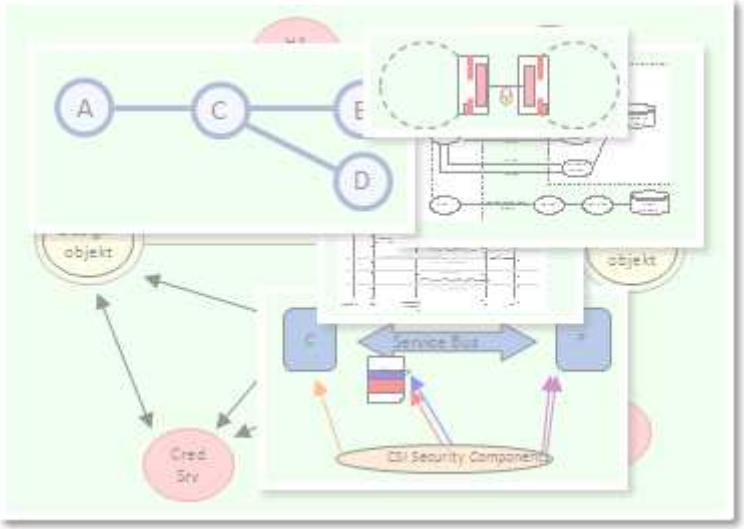
CSI - NCOE/NC3TA



CSI – FMLS TS RA/TA



CSI – IRMA



Demonstration

CSI SSO – olika token mm, samma funktion

(”Behörighetskontroll”)

Client (SA)

Single
Sign-On

CSI Security-server

Inloggning olika kort/-läsare till:
- CSI – nätverket, systembussen
- Aktuell COTS – Windows etc.

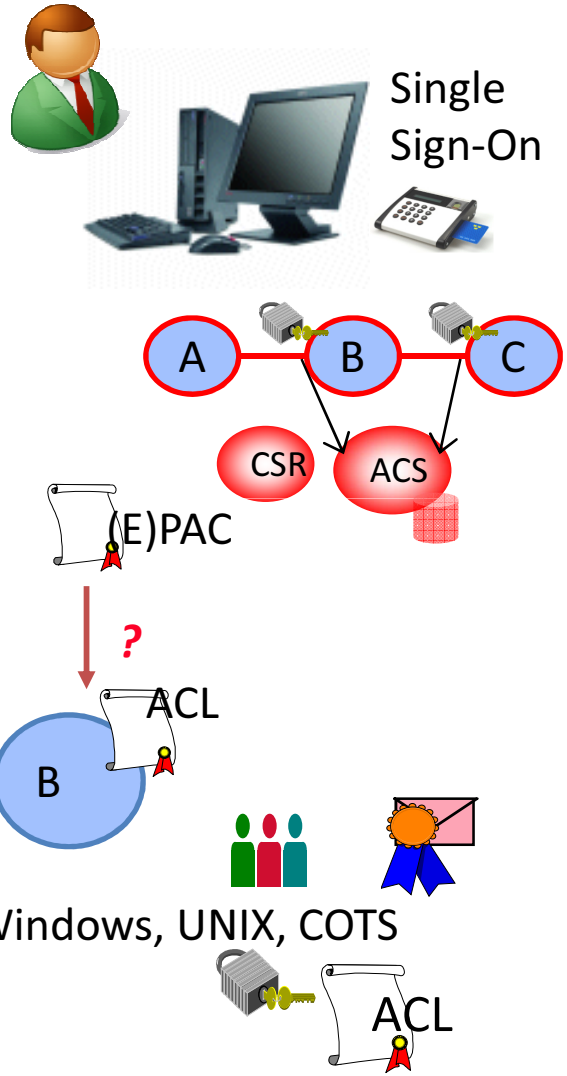
Olika kort/läsare ger olika egenskaper …

Administration:
- Registrera godkända CA
- Registrera Användare och Roller/behörigheter

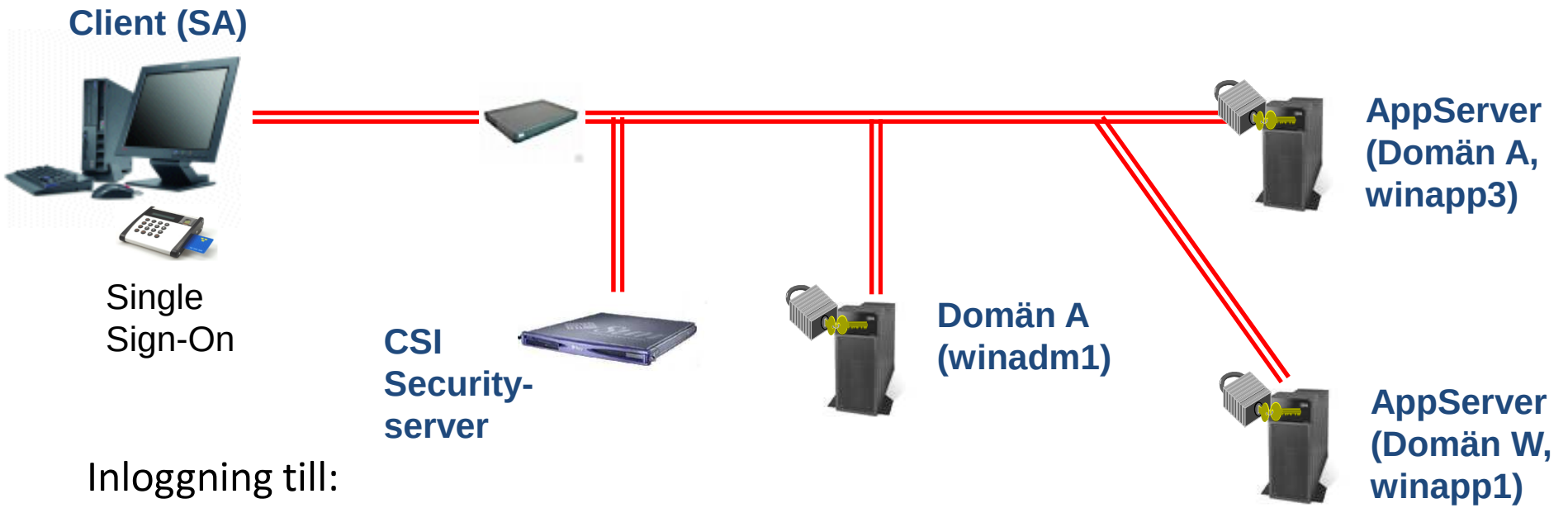
Labbmoln …
- Windows XP – Windows 7
- Windows server 2003 R2 – 2008 R2
- Olika Windows domäner (AD resp StandAlone/ WorkGroup)
- UNIX servrar
- COTS (ex IIS, Sharepoint) och OpenSource (ex Apache, Alfresco)

Behörighetskontroll

- SSO (Single-Sign-On)
  - Windows (domän eller ”stand-alone”), UNIX, COTS
  - Windows GINA resp CredProv + SSPAP, UNIX PAM
  - Agenter för olika COTS/systemmiljöer
  - Fjärrterminal – Citrix, WTS, telnet etc.
- Stöd för olika ”token”
  - Stark autentisering med FM TAK2
  - Förstärkt inloggning med FM TEID
  - Annat: Aktiva kort, 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: Identity Management, PKI, flera CA, policies, attribut, Windows, UNIX, COTS
  - SecAdm: åtkomstregler, policies, delegering, …



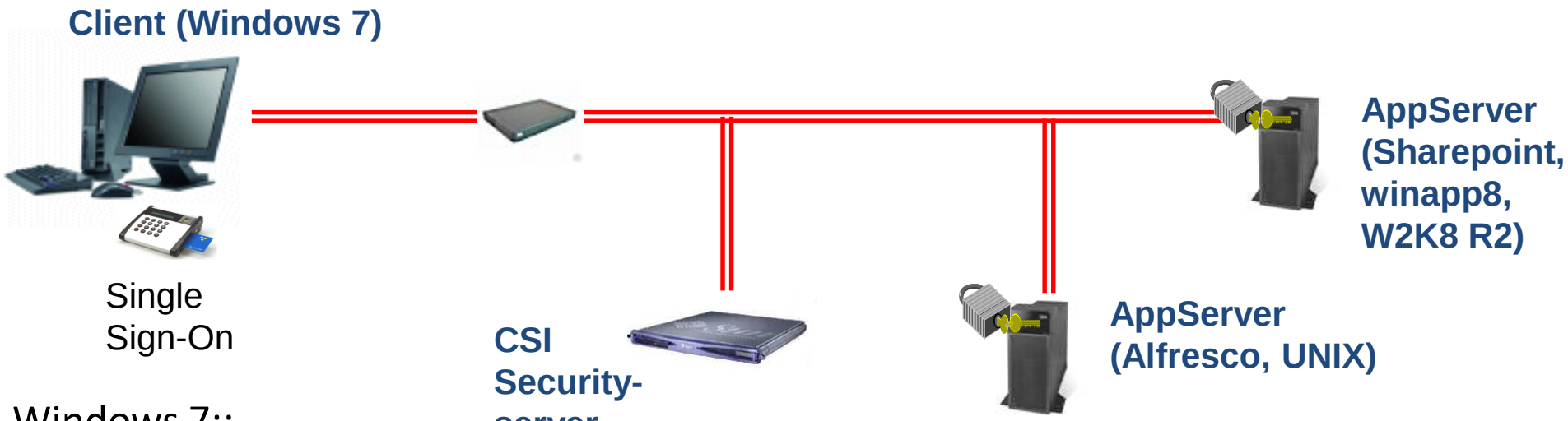
CSI SSO – i flera steg - terminal services, flera domäner



Inloggning till:

- CSI – nätverket, systembussen
- Steg 1 – Client OS (WXP resp Windows 7)
- Servertjänster – Mail, Web (Telnet, …) - skyddad kommunikation (ComE)
- Steg 2 – Terminal Services (winapp3) - skyddad kommunikation (ComE)
- Steg 3 – Terminal Services (winapp1) - skyddad kommunikation (ComE)

CSI Collaboration – “end-to-end security”

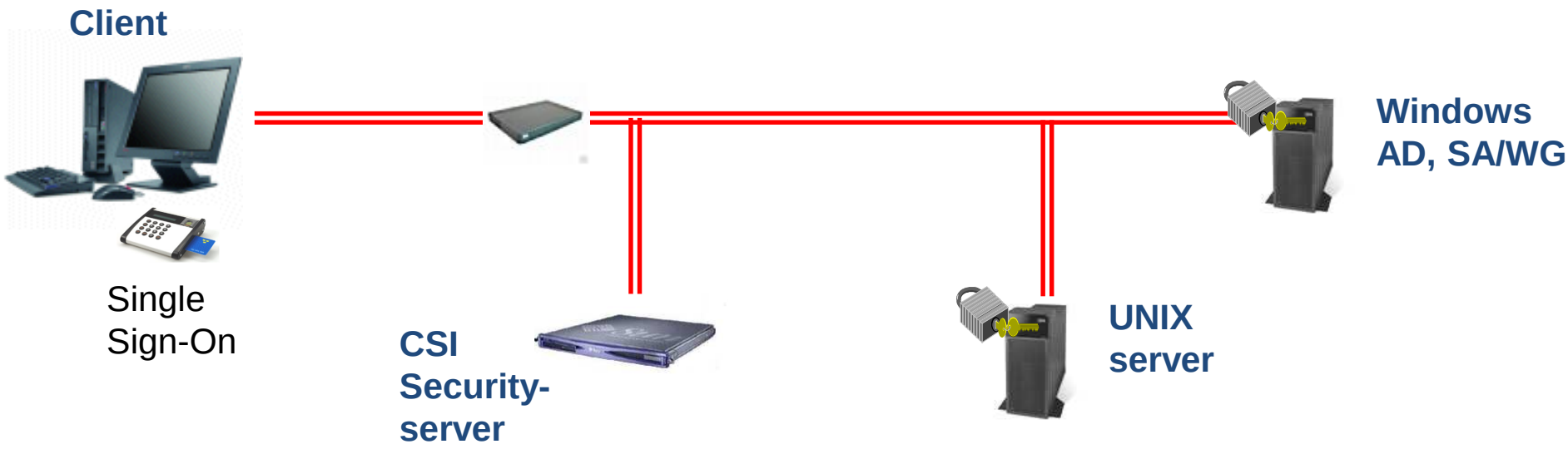


Windows 7::

- SSO med TAK2 (”Calvin”), TEID (”Bender”)
- Windows – Windows 7
- Terminal Services, Mail, Web, Telnet, …
- MS Sharepoint på Windows Server - skyddad kommunikation (ComE)
- Alfresco (”open-source sharepoint”) på UNIX server - skyddad kommunikation
- Steg 3 – Terminal Services (winapp1), skyddad kommunikation (ComE)

CSI SSO (SecL ”GUI”), CSI Communications (ComE),
CSI Delegation, CSI AccessControl, CSI LogAnalysis

CSI Management

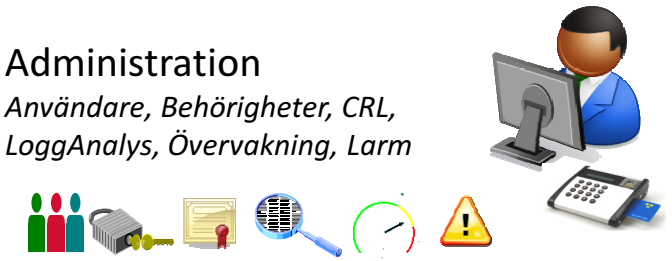


Management:

- CSI Identity Management och PKI (SysA GUI)
  Administrera PKI, Personer, konton, Windows (Clients, Servers AD, Servers SA/WG), UNIX servers, …
- CSI LoggAnalys, Övervakning, Larm
- CSI Access Control (SecAdm GUI) – behörigheter, roller, …
- . . .

Administration

Användare, Behörigheter, CRL, LoggAnalys, Övervakning, Larm



- Hur konfigureras stöd för olika aktiva kort och CA?
- Hur kom det sig att ”vissa” ”kom åt” applikationer/tjänster såsom Web, telnet etc?

Säkerhetsloggning

Användare
Program
Nod

Loggning
Autentisering

Konsument

Producent/
Konsument

Producent

Loggning
Administrativa
åtgärder

Tillämp-
ning

Windows
Loggar

Windows
Server
Loggar

Unix
Loggar

Nätverks-
utrustning
Loggar

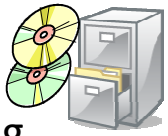
Urval relevanta
Tillämpnings-
loggar

Insamling

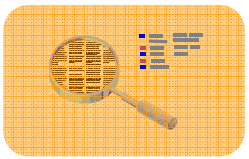
Loggning
Åtkomst-
kontroll

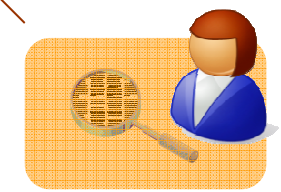
Applikations-
loggning

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

Skydd mot Skadlig Kod

Antivirus

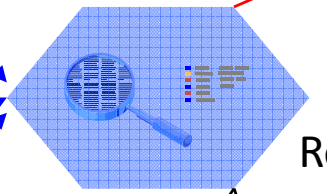
IntG Integritets-vakt

Larm

Administratör

Gemensam Meddelande Hantering (CMC)

Insamling loggar



Regelbaserad Bakgrunds-analys

Operativsystem Loggar

Router/ Brandväggs-loggar

Begära förberedd åtgärd i viss nod av StartTjänst (SUS)

Automatisk Åtgärd centralt

- Antivirus – mot ”vanlig” skadlig kod
- Integritetsvakt – mot ny/speciell (Zero Day) skadlig kod
- Insamlade loggar från Operativsystem och brandväggar/routrar
- Regelbaserad Samanalys
- Larm eller automatisk åtgärd
- Överföringen är skyddad
- Konfigurationsstyrning

Summering

- CSI tillhandahåller säkerhet från användaren hela vägen till resursen, även i flera led
- CSI säkerhet griper in och ger automatiskt effekt i alla applikationer och tjänster i nätet oberoende av operativsystem
- Flexibelt – välj funktioner/komponenter efter kravbild
- Alla komponenter/tjänster passar ihop – gemensam säkerhetsarkitektur
- IRMA – operativsystemoberoende säkerhetsarkitektur för hög assurans
- Assuransarkitektur – slipper ”lita” på (dvs hindras av) svaga OS (Windows) och kan använda färdigutvecklad och beprövad inköpt programvara även om den inte har ”rätt” (svenska) säkerhetsfunktioner
- Pluggbart – olika mekanismer för olika behov, gränssnitt/standards
- Enkelhet – installera, konfigurera och kör - ingen utveckling behövs för användning
- Stämmer med flertal initiativ av sortering/indelning/modellering på säkerhetsområdet
- Avsett för FM krav – löser säkerhet på ”riktigt” (inte genom alternativa åtgärder), granskat och praktiskt beprövat
- Stöder såväl nuvarande som framtida OS, ex Windows XP – Windows 7, en följd av arkitekturen

Q&A