

Risker med virtualisering av IT-system

Daniel Eidenskog

Virtualisering av IT-system

- Rötter i 1960-talet
- Skapa en virtuell miljö för en mjukvara
- Olika drivkrafter
 - Separation
 - Hårdvaruoberoende
 - ...

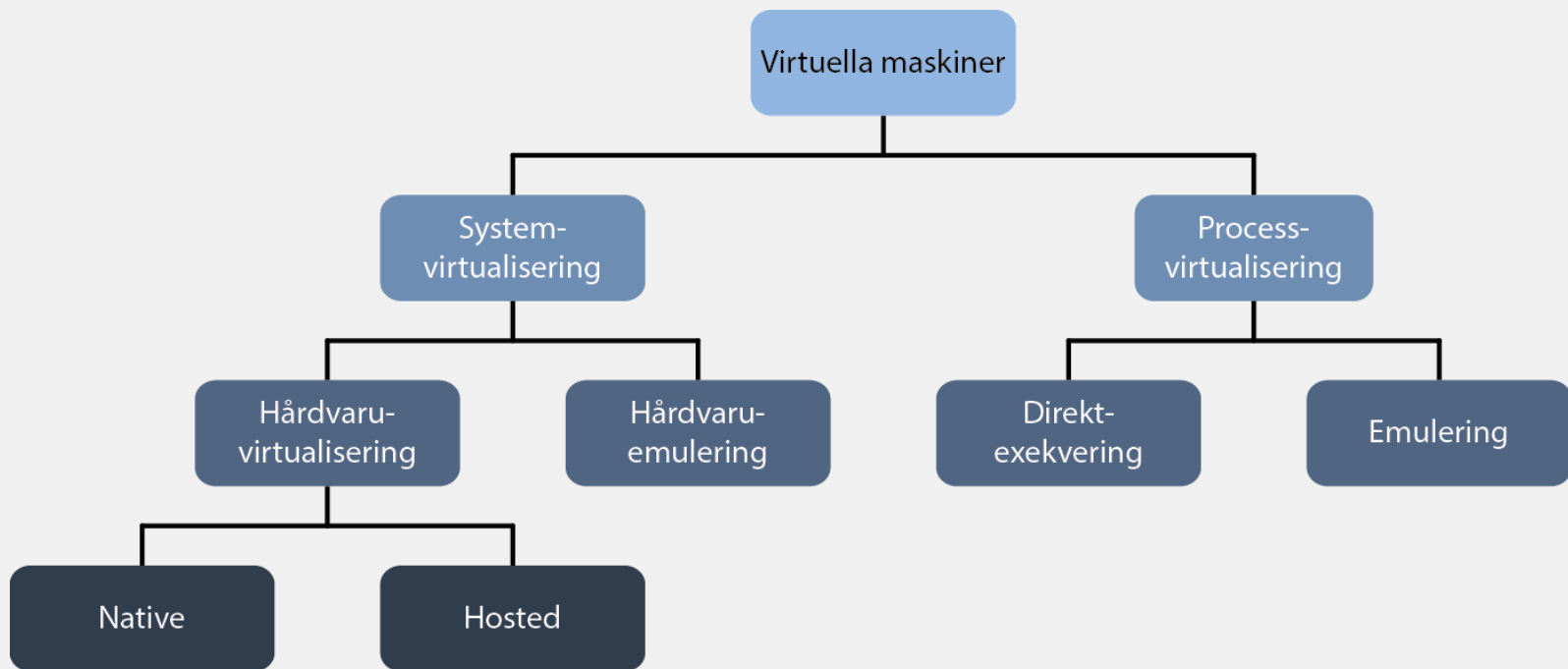


Bild: NASA

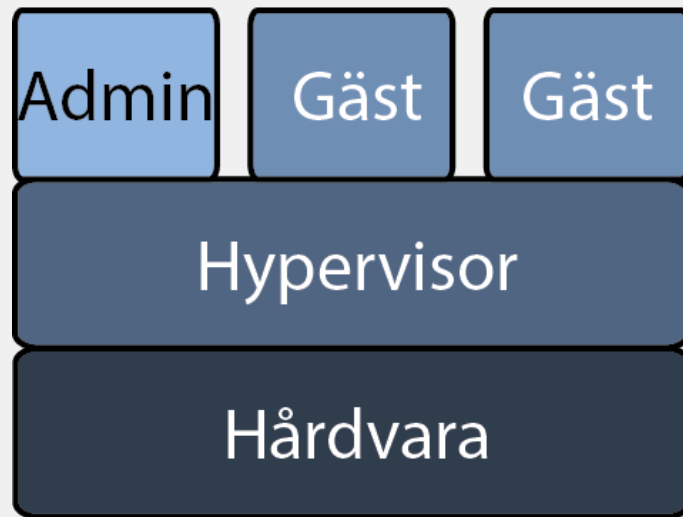
Vad är virtualisering?

- Ofta mjukvara som beter sig som hårdvara
 - "Virtualization is the process of creating a software-based (or virtual) representation of something rather than a physical one." (VMware)
- Abstraktionsteknik som frikopplar gästmiljön från värdmiljön

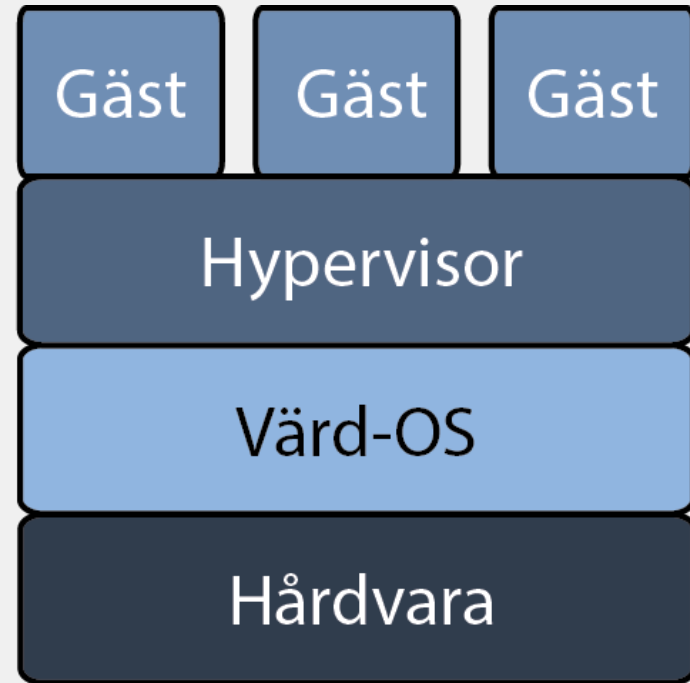
Taxonomi



Typer av systemvirtualisering



a) Native / Typ 1



b) Hosted / Typ 2

Fördelar med systemvirtualisering

- Isolering av applikationer
- Samlokalisering av servrar
- Hårdvaruoberoende
- Lastbalansering
- Enklare återställning
- Energibesparing
- Platsbesparing
- Enklare att bygga testmiljöer
- ...



Bild: Wikimedia Commons / Victorgrigas

Metod

- Litteraturstudie
- Sökning för att få fram översikter
 - Sökning gav 380 artiklar
 - Manuellt urval 15 artiklar
 - G. Pék, L. Buttyan och B. Bencsath (2013). “A survey of security issues in hardware virtualization”. ACM Computing Surveys 45(3).
- Systematisk genomgång av sårbarheter
 - Fokus på verkliga exempel



Administrativa risker

- Ansvarsfördelningen kan bli mindre tydlig
 - Större sammanblandning av samlokaliserade system
 - Systemadministratörer med större tillgång
 - Lätt att skapa för breda roller
- Systemkomplexitet kan ge oöverskådliga effekter av olika åtgärder
- Lätt att kopiera virtuella maskiner vilket kan ge följdrisker
 - Migration, kloner, säkerhetskopior, ...

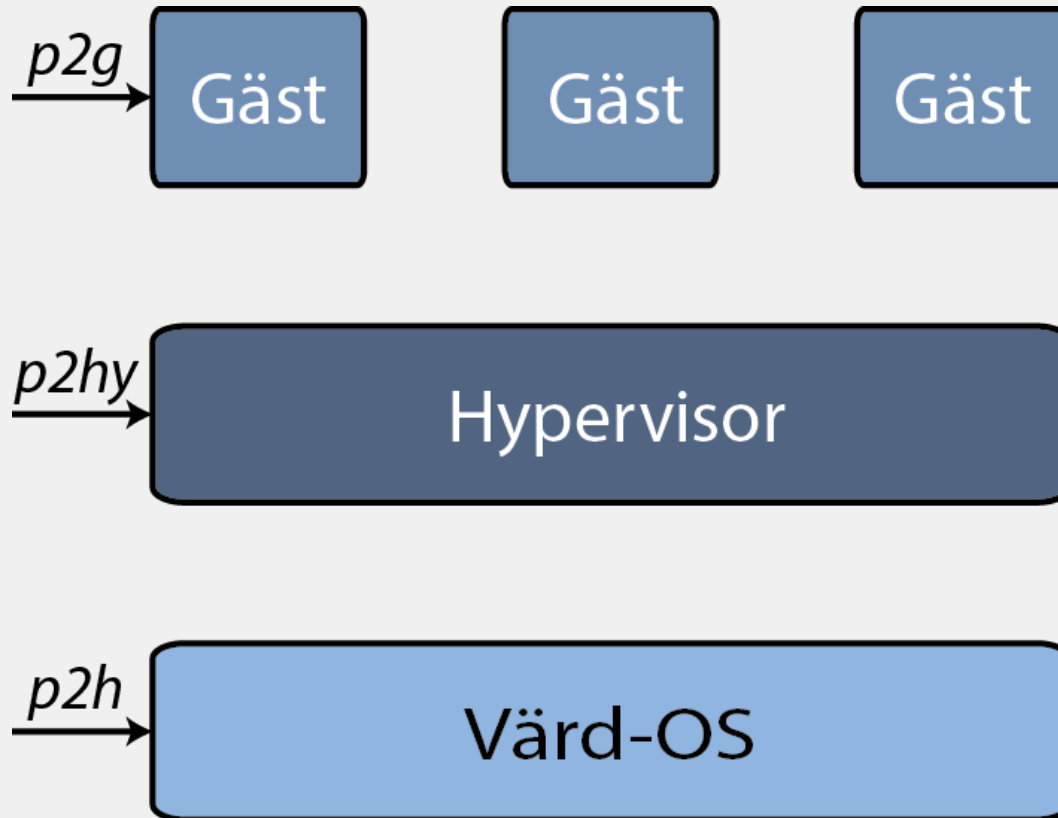
Tekniska risker

- Nya lager med mjukvara
 - Hypervisorn är en felkritisk systemdel i separationen
 - Större komplexitet
 - Mycket svårt att undvika sårbarheter
- Samlokalisering
- Beroenden mellan virtuella maskiner
- Vissa säkerhetsåtgärder kan fungera sämre i en virtualiserad miljö
 - Antivirus, IDS

Sårbarheter och angrepp

- De gamla sårbarheterna och angreppsvägarna finns kvar
- Angriparen kan finnas i den fysiska maskinen
- Sårbarhetskedjor
 - Exempel: externt angrepp mot en tjänst i gäst, eskalering av privilegier, angripa hypervisor, ta över målgästen
 - Inte ovanligt att utnyttja kedjor av sårbarheter

Externa angrepp

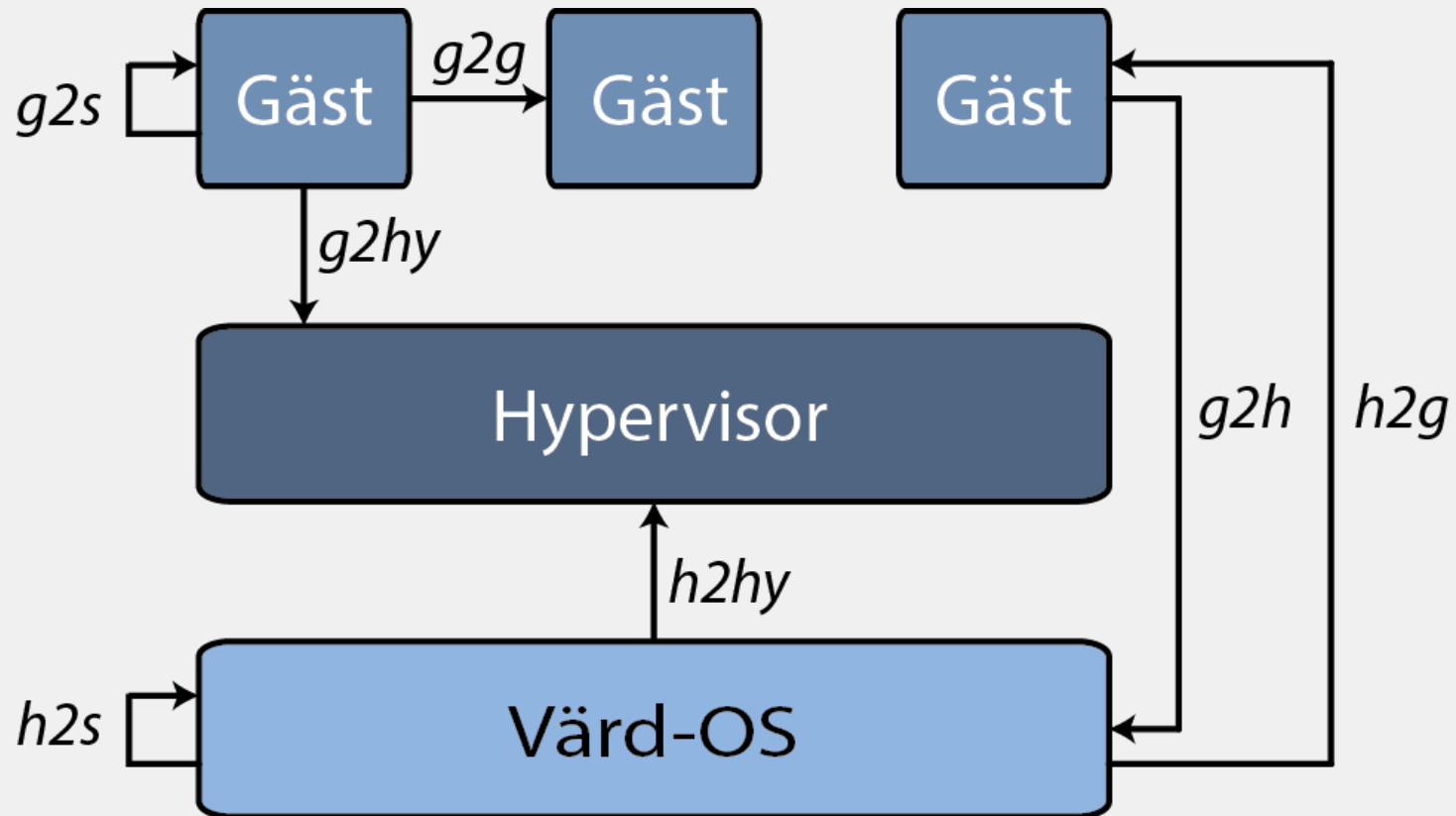


Externa angrepp

- Alla "gamla" sårbarheter finns kvar i operativsystem och övrig mjukvara
- Hypervisorn med administrationsfunktioner kan innehålla nya sårbarheter



Interna angrepp



Exempel på kända sårbarheter

- (g2g) Informationsextraktion – vilka applikationer som körs, kryptonycklar
- (g2hy) Brist i nätverksdrivrutin ger möjlighet att exekvera godtycklig kod
- (g2h) Brist i videodrivrutin ger tillgång till världens minne (Cloudburst)
- (g2s) Eskalering av privilegier genom brist i hanteringen av Virtual-8086-läge

Exempel på kända sårbarheter

- (h2g) Åtkomst till gästernas minne
- (h2hy) Exekvering av godtycklig kod genom DMA-överföringar mot nätverkskort
- (h2s) Eskalering av privilegier genom verktyg för att hantera virtualiseringsmiljön

Diskussion

- Virtualisering är en beprövad och kraftfull teknik med många fördelar
- Risker tillkommer i virtualiserad miljö
 - Nya funktionella områden
 - Nya angreppsytor och sårbarheter
 - Kan bli större konsekvenser vid angrepp
- Fördelar och riskerna måste vägas mot varandra
 - Vissa risker kan vara begränsande
 - Separationen blir svagare i virtualiserad miljö

Sammanfattning

- Virtualisering kan ge både bra och dåliga effekter på IT-säkerheten
 - "[Virtualization] isn't an additional security layer, it's just another layer to find bugs in"
 - Sekretess är inte den enda säkerhetsaspekten
- Virtualisering är användbart på alla säkerhetsnivåer – så länge det används på rätt sätt
- Var medveten om riskerna

Frågor?



IT-krig och Cyberhot

Aktörer, mål, förmåga

T-LD1004-TT

- 18/8 FBI varnar för att två delstaters valdatabaser hackats och data stulits.
- 29/8 Enligt Yahoo! News är det Illinois och Arizona som drabbats
 - "upp till 200 000" väljares data har stulits
 - Minst ett av IP-numren som användes i angreppet har kopplingar till ryska hackingforum
 - Enligt Rich Barger, ThreatConnect, liknar angreppet andra som tillskrivits Ryssland, till exempel angreppet mot WADA-CAS,

Eller?

- 29/8 The Washington Post anger att FBI informerat Arizona att "Ryssland låg bakom angreppet" vilket beskrivs som ett trovärdigt och signifikant hot. "En 8 på en skala från 1 till 10"
- I samma artikel påstås det att angriparna i själva verket bara lyckats komma över " the username and password of a single election official in Gila County"

Vad är sant?

- Vad har egentligen hänt?
 - Alla aktörer¹ har en agenda
 - Kan vi lita på aktörernas kompetens?
 - Även om aktörerna är kompetenta och talar sanning, kan de hitta tillräckligt med spår för att veta vad som hänt?

¹ Som uttalat sig i media. Inte bara angripare.

Vem var angriparna?

Cybersoldater

- USCYBERCOM, Före detta 16:de Avdelningen KGB, PLA Enhet 61398, Enhet 8200
- Professionella kompetenta grupper med stora resurser
- Agerar för att främja sin nations intressen
- Angriper system för att ta information, säkra framtida tillgång, propaganda, psyops, övning, m fl

”Oberoende” Hacktivister

- Politiskt motiverade
- Normalt små resurser, men inte alltid
- Stor variation i kompetens
- EHAP, Anonymous, Telecomix, Honker Union, Palestinian Cyber Army, RedHack, Tahr Andishan, Syrian Electronic Army.....
- Angriper alla som de uppfattar som associerade med ”fienden”

Opportunistbrottslingar

- Gottfrid Svartholm Warg
 - Anakata
- Pirate Bay
- Datorintrång mot Logica, Nordea, CSC

Yrkesbrottslingar

- Professionella brottslingar.
- Tar över datorer,
 - Säljer stulen data
- Använder de hackade datorerna
 - Intrång, utpressning,
 - Uthyrning, försäljning
- Agerar inte alltid professionellt
 - Angriper ett annat land när deras eget är i krig med det.
 - Angriper Scientologerna för att en online-kompis ber honom.

Den lurade

- En anställd som luras att göra något som försätter systemet i ett osäkert läge.
 - Ansluter en dator/smartphone som smittats någon annanstans
 - Angriparens programvara agerar autonomt och börjar angripa systemet
- Annat exempel: "Barnens leksaker"

Hämnaren

- En datorkonsult får inte en anställning han sökt på ett reningsverk.
- Han spenderar större delen av tre månader, kvällar och helger med att hacka styrsystemet på reningsverket.
- ..inklusive (minst) tre fysiska inbrott för att sabotera rörsystemen.
- Han åstadkommer stora utsläpp av avloppsvatten vilket leder till stora skador på djur och natur i området.

Förrädaren

- Chelsea Manning, Edward Snowden,
- En person i er organisation som anfaller er.
- Mycket farlig i förhållande till sin kompetens eftersom de redan har tillgång till systemen och kännedom om dem.

Relevant för er:

- Egen spaningskapacitet i näten
 - Vem gör vad i era system?
- Egen forensikkompetens
 - Hur ta reda på vad som hänt?
 - Hur bevisa det i domstol?
- Incidentberedskap
 - Teknisk nivå
 - Management/business-nivå
 - Omvärldsbevakning

Slut



Klassificering av IT-utrymmen

Björn Åkesson, FMTIS



Inledning

- AG Hall – samarbete mellan FM och FMV
- Direktiv för klassificering av försvarsmaktens IT-utrymmen
- Typnivåer beskriver förväntad tillgänglighet över tid



Beroenden

- Försvarmaktens förmåga beroende av IT-stöd
- Hur säkerställer vi detta oavsett beredskapsgrad?
- Ska det fungera i kris och krig måste det fungera idag!



Tillgänglighet

- Tillgänglighet definieras här som:
Oavbruten tillgång till IT-stödet över tid
 - Planerade och oplanerade avbrott
 - 100% är inte möjligt
 - 99% – 90 timmar per år utan tillgång
 - 99,999% – drygt 5 minuter per år utan tillgång
 - 1 timmes avbrott medför att ”fem nior” inte uppfylls förrän 12 år senare





Säkerställ IT-stödets tillgänglighet!

- Logisk och fysisk säkerhet
- Robusta kommunikationer
- Robusta IT-utrymmen
- Bemanning
- *IT-systemets konstruktion*



Vad är ett IT-utrymme?

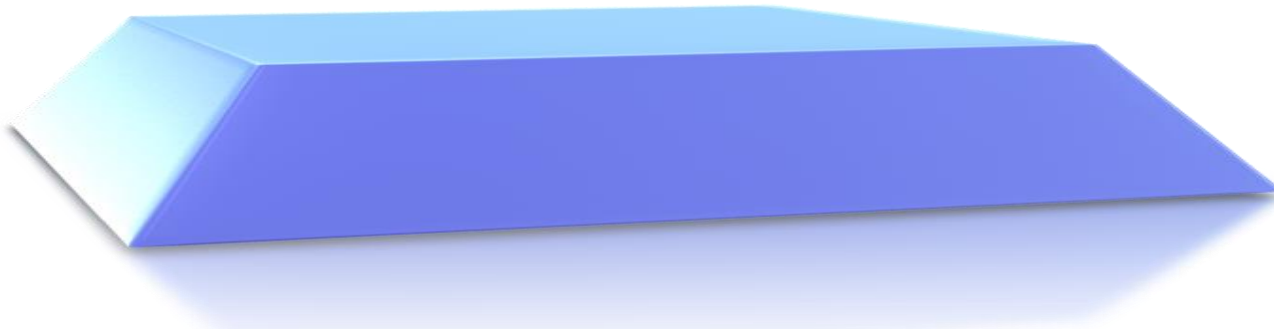
- En lokal avsedd för uppställning och drift av IT-utrustning
- Kärt barn...
 - Datahall
 - Datorhall
 - Datorcentral
 - Datacenter
 - Datorrum
 - "Skrubb..."
- Gemensam benämning: IT-utrymme





Bottenplattan

- Funktion i kris och krig
- Vilka IT-system måste vara tillgängliga?
- Var finns dessa IT-system?
 - Vilken tillgänglighet erbjuder dessa IT-utrymmen?



Kärnan i budskapet

- Rätt system på rätt ställe!
- Hur vet vi vad som är rätt ställe?





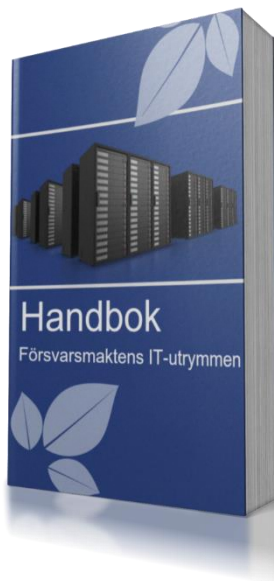
Sammanhang

- Infra Ny - Försvarmaktens gemensamma LAN-modell
- UIT – Central drift samt IT-driftprocesser (ITIL)
- Konsolidering av IT-system
- SÅKK – Säkerhetshöjande åtgärder
- Klassificering av IT-utrymmen



AG Hall

- HKV PROD LEDUND uppdrag
 - Ta fram handbok för kravställning, projektering, etablering, vidmakthållande och avveckling av IT-utrymmen
- Deltagare från FMV, FMTIS och snart även FORTV



Klassificeringsdokumentet

- Fastställt direktiv
- Målgrupp:
 - Strateger, beställare, konstruktörer
 - Leverantörer av IT-utrymmen och IT-system
 - Nyttjare av IT-utrymmen
 - Drift- och underhållsorganisationer

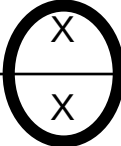
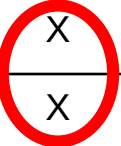
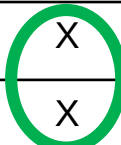


Typindelning i 5 nivåer

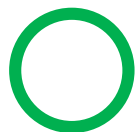
- Typ 1 – Enklare icke-redundant IT-utrymme
- Typ 2 – IT-utrymme med redundanta komponenter
- Typ 3 – Möjliggör service och underhåll av IT-utrymme under drift
- Typ 4 – Feltolerant IT-utrymme
- Typ 0 – Allt övrigt som inte uppfyller kraven för typ 1 eller högre
Planeras för uppgradering eller avveckling
- Kostnader ökar kraftigt med högre typnivåer



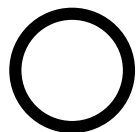
Matris utrymme/typnivå

Tillgänglighetskrav						
Lokaltutformning	Typ 0	Typ 1	Typ 2	Typ 3	Typ 4	...
Datorcentral		---	---			
Datorhall		---				
Datorrum		X		X	X	
KK-rum/nodrum		X	X	X	X	
IT-skåp (FM-specifikation)		X		---	---	
IT-container		X				
Övrigt utrymme	X	---	---	---	---	

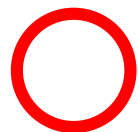
*: Ställer ytterligare krav på omkringliggande utrymmen.



= UDaC



= DaC



= HDaC

Beskrivande parametrar

- Elkraft
- Kyla
- Driftmiljöövervakning
- Brandskydd och släcksystem
- Bemanning
- Placering
- Tillträdesbegränsning
- Uthållighet
- Sekretess
- Skyddsnivåer
- Rutiner och processer





Tillgänglighet

	Typ 1	Typ 2	Typ 3	Typ 4
Tillgänglighet/år (%)	95%*	99,5%	99,9%	99,99%
Avbrottstid/år	100h*	40h	10h	1h
Hindertid	< vecka	< dag	< timme	< minut
Uthållighet vid funktionsbortfall	Ej def.	Timme - dagar	Dag - veckor	Vecka - månader
Skada innebär funktionsavbrott	Ja	Ja	Ja	Nej
Underhåll utan driftavbrott	Nej	Nej	Ja	Ja

*: För Typ 1 avses kontorstid (detta krav är väsentligt lägre än övriga som räknas på kalendertid).



Elkraft

	Typ 1	Typ 2	Typ 3	Typ 4
A-kraft	Ja	Ja	Ja	Ja
B-kraft	Nej	Ja	Ja	Ja
C-kraft	Nej	Ja	Ja	Ja
Flera möjliga försörjningsvägar (passiv reserv)	Nej	Nej	Ja	-
Flera samtidigt aktiva försörjningsvägar	Nej	Nej	Nej	Ja
Service- och supportavtal	Nej	Ja	Ja	Ja
Rutiner för kontroll av reservkraftfunktion inklusive tillgång till drivmedel	Nej	Ja	Ja	Ja



Kyla

	Typ 1	Typ 2	Typ 3	Typ 4
Ventilation	Ja	Ja	Ja	Ja
Fastighetens klimatkyla	Ja	Nej	Nej	Nej
Dedicerade kylaggregat	Nej	Ja	Ja	Ja
Flera möjliga försörjningsvägar (passiv reserv)	Nej	Nej	Ja	-
Flera samtidigt aktiva försörjningsvägar	Nej	Nej	Nej	Ja
Erforderlig kylkapacitet även vid fel på del av systemet	Nej	Nej	Ja	Ja
Service- och supportavtal	Nej	Ja	Ja	Ja
Rutin för kontroll av försörjningskedja	Nej	Ja	Ja	Ja
Rekommenderad temperatur vid luftintag till IT-utrustning	22-24 C°	22-24 C°	22-24 C°	22-24 C°
Relativ luftfuktighet	30-50%	30-50%	30-50%	30-50%

Bemanning

- Tillgänglighet kräver personal
- Högre typnivåer – utbildad personal dygnet runt
- Personalkategorier:
 - Lokal IT-drift/övervakning
 - Central IT-drift/övervakning
 - Fastighetsdrift
 - Lokal bevakning
 - Central bevakning



Fortsatt arbete

- Vidareutveckla klassificeringsdirektivet
- Handbok IT-utrymmen
- Definiera vad som styr tillgänglighet för IT-system
- Stödja kravställning på design av IT-system
 - Krigets krav
 - Georedundans
- Krav på komponentval
 - Beprövade och tillförlitliga
 - Tillgång till service och reservdelar
 - Standardiserade pusselbitar
- Gemensam FM-nomenklatur



Slutord

- Omvärldsläget förändras
 - Tillgänglighetskraven på IT-stödet ökar
 - IT-utrymmen allt viktigare
- Nu finns en måttstock
- Kärnan i budskapet – Rätt IT-system på rätt ställe







Tack!





Klassificering av IT-utrymmen

Björn Åkesson, FMTIS

Objektbaserad säkerhet

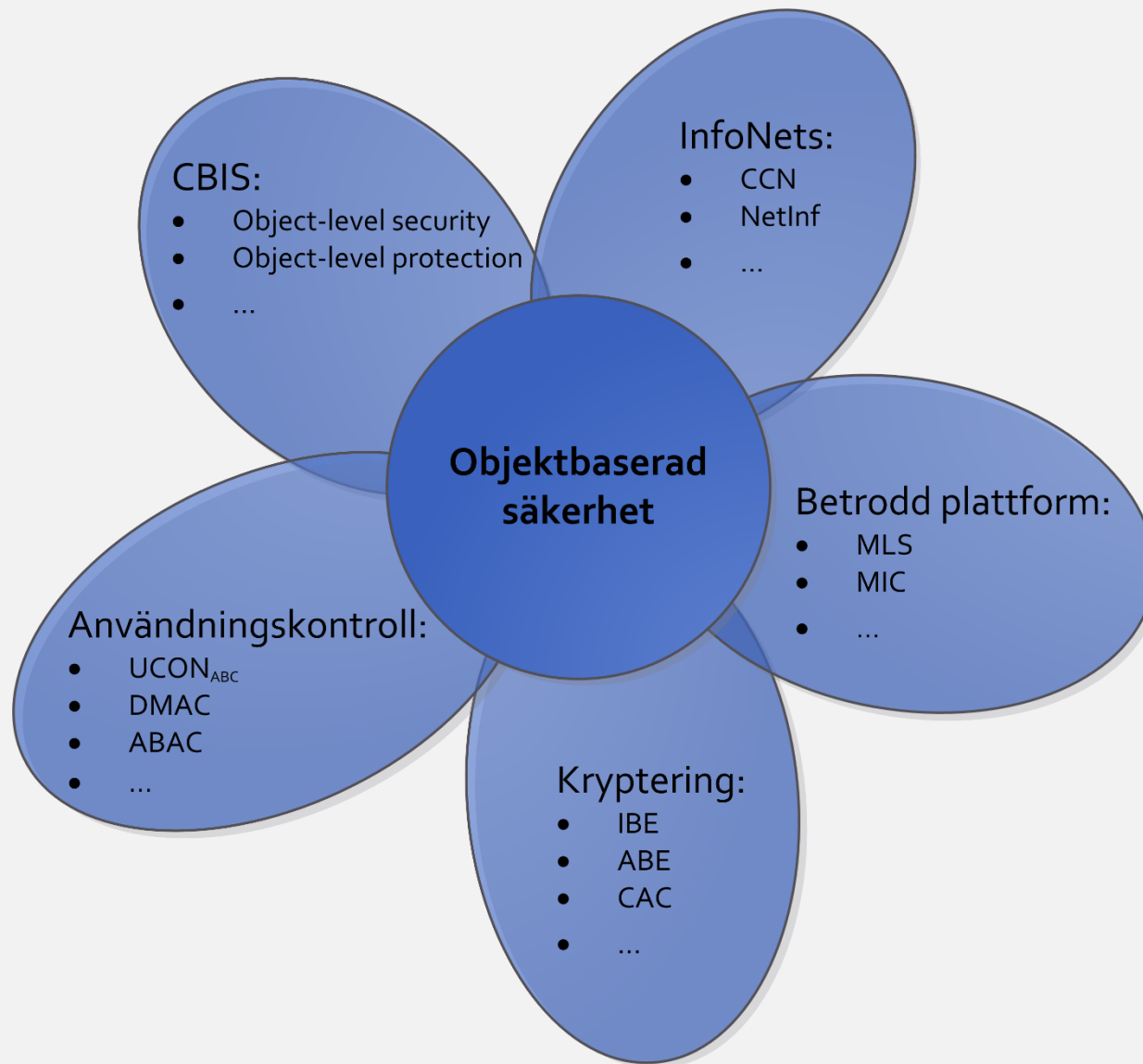
Bakgrund och nuläge

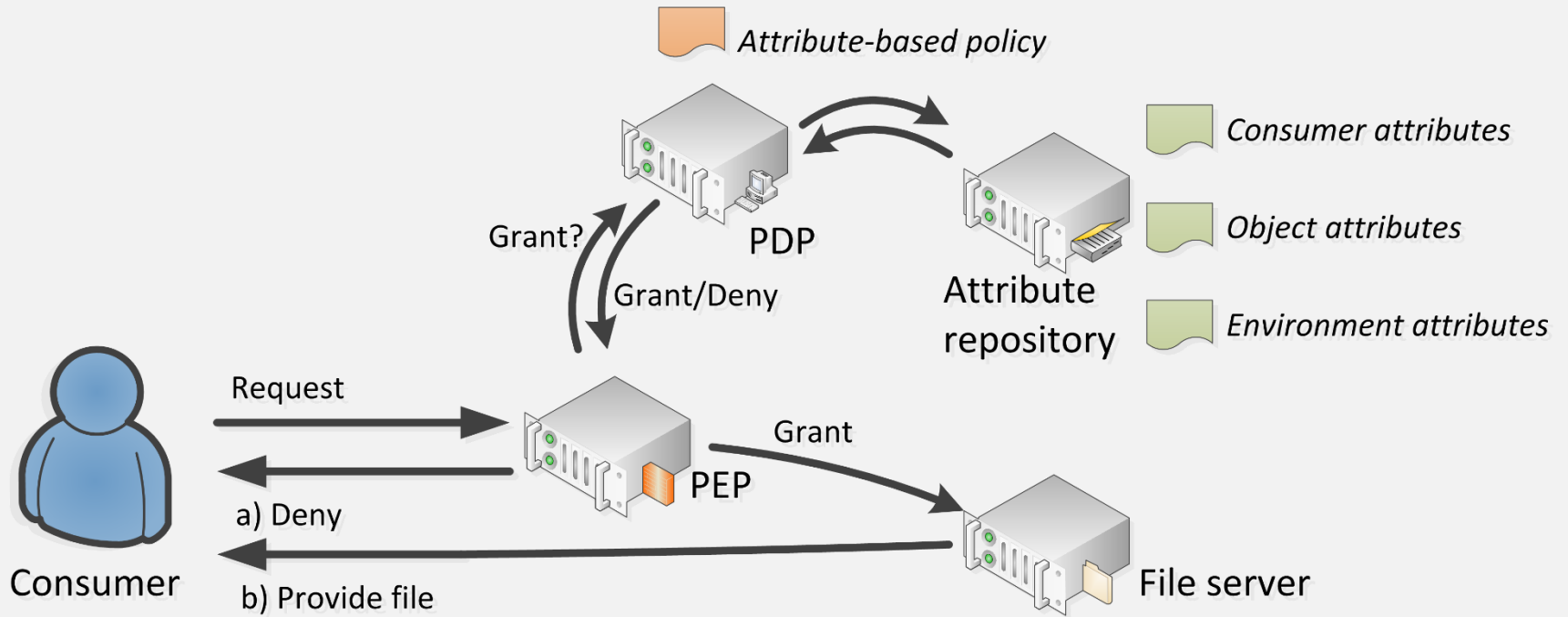
Lars Westerdahl

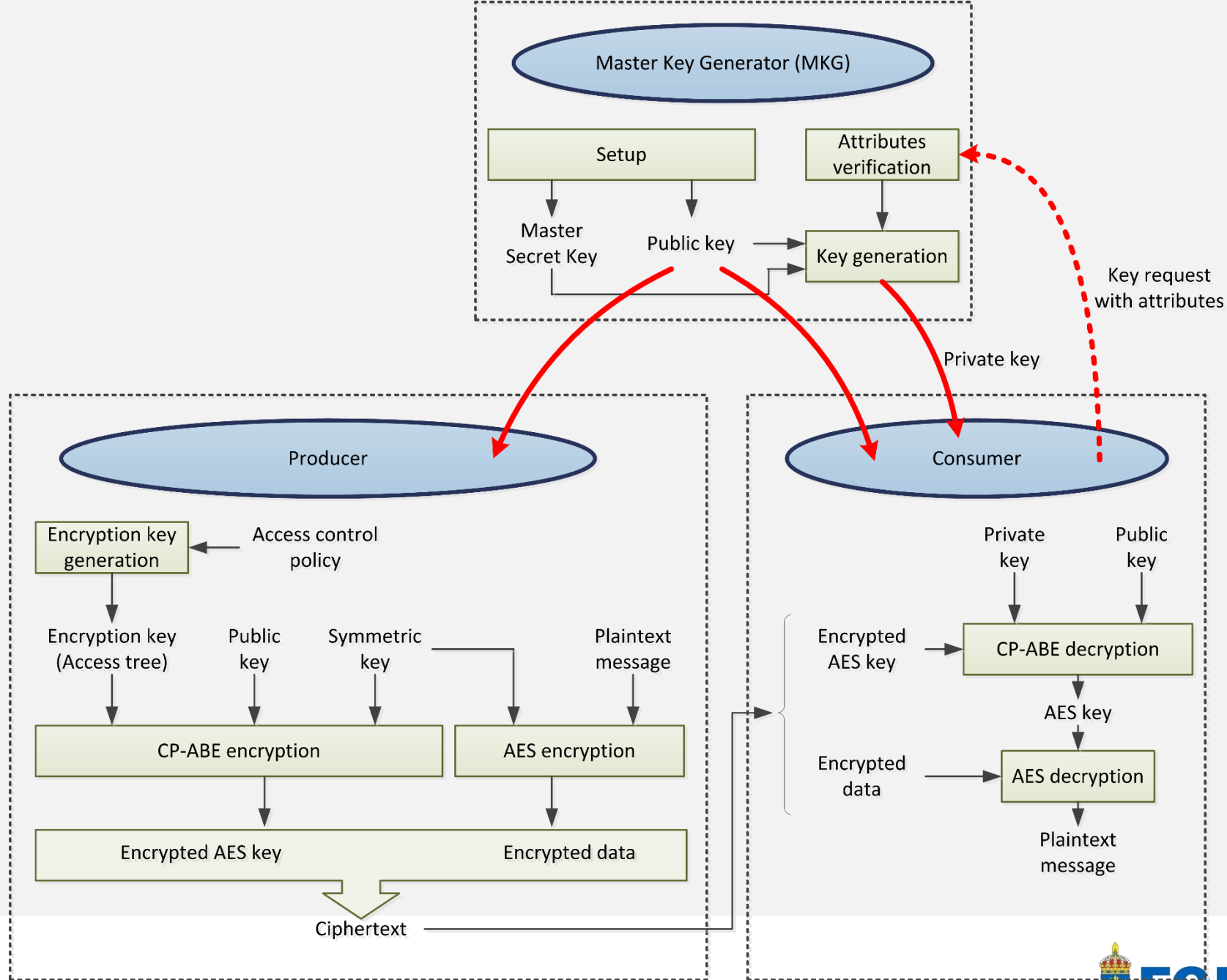
3 november 2016

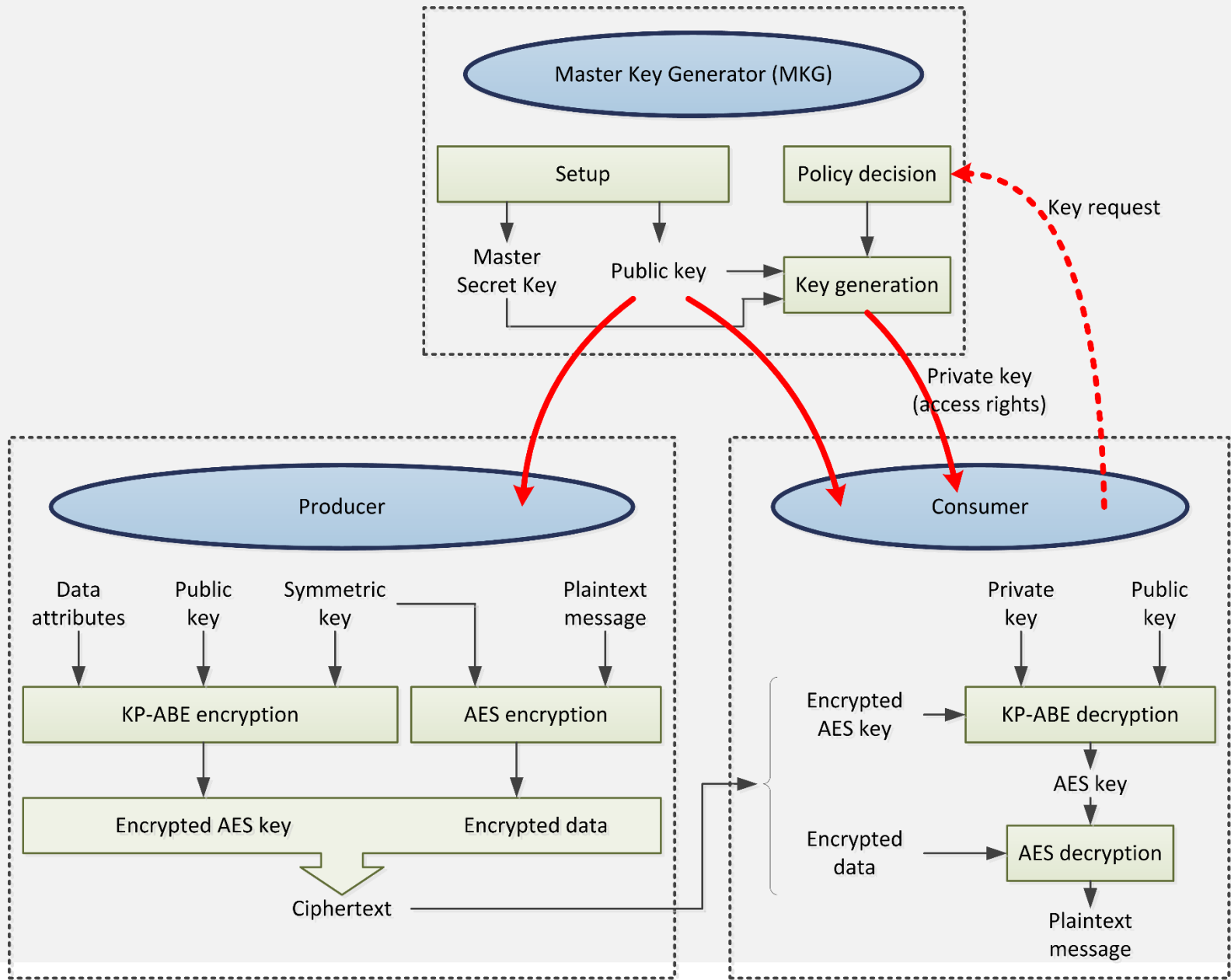














NATO Communications and Information Agency
Agence OTAN d'information et de communication







