STADSNÄTS
FÖRENINGEN

Robust & Säker IoT

Vägledning för robust och säker IoT

Informationsmöte om avvecklingen av 2G och 3G nät

MAJ 2023

Jimmy Persson, Utveckling- och säkerhetschef

TLP:CLEAR

STADSNÄTS FÖRENINGEN

Informationsäkerhetsklassning

TLP:CLEAR

Mottagare kan sprida detta till världen, det finns ingen gräns för spridning.

Källor kan använda TLP:CLEAR när informationen medför minimal eller ingen förutsägbar risk för missbruk, i enlighet med tillämpliga regler och förfaranden för offentliggörande.

TLP:CLEAR-information kan delas utan begränsning, under förutsättning att standardregler för upphovsrätt följs.

TLP:CLEAR

Jag ska tala om …..

- Vägledningen Robust och Säker IoT
- Från behov till etablera och använd IoT
- Exempel på tjänster

Robust & Säker IoT

Sveriges Kommuner och Regioner

TLP:CLEAR

Bakgrund

- Samhällets beroende av tjänster baserade på lösningar, utrustningar och system för Internet of Things (IoT) ökar i en allt snabbare takt.

- IoT finns i **många delar av samhället**: i hemmet, i offentlig verksamhet och inom industrin.

- **Beroendet till IoT** gör att hanteringen av utrustningar och system för IoT, och den infrastruktur som de kopplas upp till, **måste vara robust och säker**.

- Detta gäller även tillverkningen av utrustning samt leveranskedjan till slutanvändaren.

- Det finns därför **ett behov av en vägledning** som kan **stödja aktörerna i att höja säkerhetsnivån inom IoT**.

- Minimikraven i denna vägledning är menade som **stöd** att få en **grundläggande nivå gällande IoT-säkerhet**.

TLP:CLEAR

Syfte

Vägledningen **innehåller minimikrav** avseende åtgärder för **robusthet och säkerhet för IoT**.

Enskilda systemägare tillämpar vägledningen efter egna instruktioner, processer och byggbeskrivningar och **kan ha krav som är högre eller krav som inte framgår här**.

Syftet med vägledningen är att:

- Definiera branschgemensamma **begrepp och uttryck**
- Beskriva hur **ENISA** definierar säkerhet IoT- lösningar
- Beskriva **minimikrav avseende säkerhetsåtgärder** för IoT-lösningar
- Beskriva en metod samt tillhandahålla verktyg för analys av minimikrav avseende **säkerhetsåtgärder** för IoT
- Beskriva en metod samt tillhandahålla verktyg för **riskhantering**
- Utgöra underlag för **utbildning, kompetensutveckling** och **fortbildning**

Målgrupp

- Vägledningen riktar sig till aktörer **som i olika roller** utvecklar, levererar, tillhandahåller, underhåller och driftar utrustningar, tjänster och system för IoT-tillämpningar.

- Vägledningen riktar sig också till aktörer som bedriver **utbildning** inom IoT området samt till aktörer som svarar för **upphandling och kravställning** på tjänster och utrustning.

Roller inom IoT

Utbildning

Upphandling

Kravställan

TLP:CLEAR

Standarder

Vägledningen utgår från **standarder och regelverk** inom de olika delområden som berörs i vägledningen till exempel:

- **ENISA** Good practices for IoT and Smart Infrastructures
- **ENISA** Baseline Security Recommendations for IoT
- **MSB** 245, 2011 MSB:s vägledning för risk- och sårbarhetsanalyser
- **MSB** 2017-1554 NCS3 Studie – IoT-relaterade risker och strategier
- **ISO/IEC** 30141 Internet of Things Reference architecture
- **ISO/IEC** 15408–1:2009 Generella säkerhetsmodeller
- **ISO/IEC** TR 15446:2017 Vägledning för produktion av skyddsprofiler och säkerhetsmål
- **ISO/IEC** 31010:2019 Risk management - Risk assessment techniques

enisa THE EU CYBERSECURITY AGENCY

MSB Myndigheten för samhällsskydd och beredskap

ISO IEC

Robust & Säker IoT

TLP:CLEAR

Identifierade brister och utmaningar inom IoT enligt ENISA

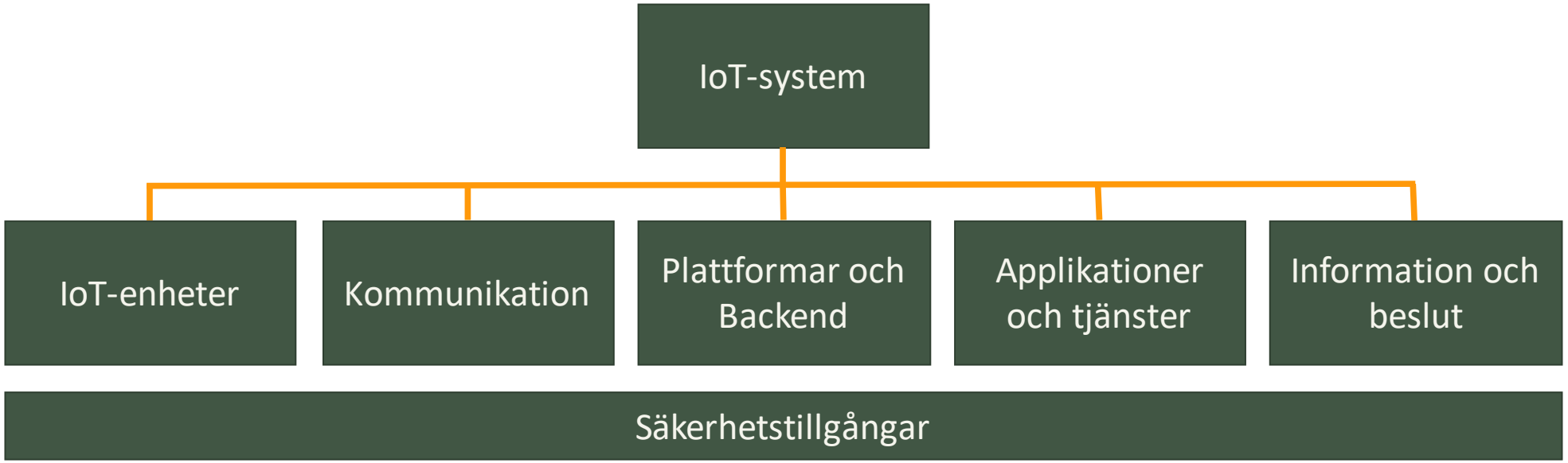
Robust & Säker IoT

- **Fragmentering** i befintliga säkerhetsmetoder och regler.
- Brist på medvetenhet och **kunskap.**
- **Osäker design** och / eller utveckling
- Bristande **interoperabilitet** mellan olika IoT-enheter, plattformar och ramverk
- Brist på **ekonomiska incitament**
- Brist på korrekt **produktlivscykelhantering**

TLP:CLEAR

IoT-system en översikt

Schematisk bild över tillgångar/komponenter (assets groups) i ett IoT-system



TLP:CLEAR

IoT-enhet / andra typer av IoT

Robust & Säker IoT

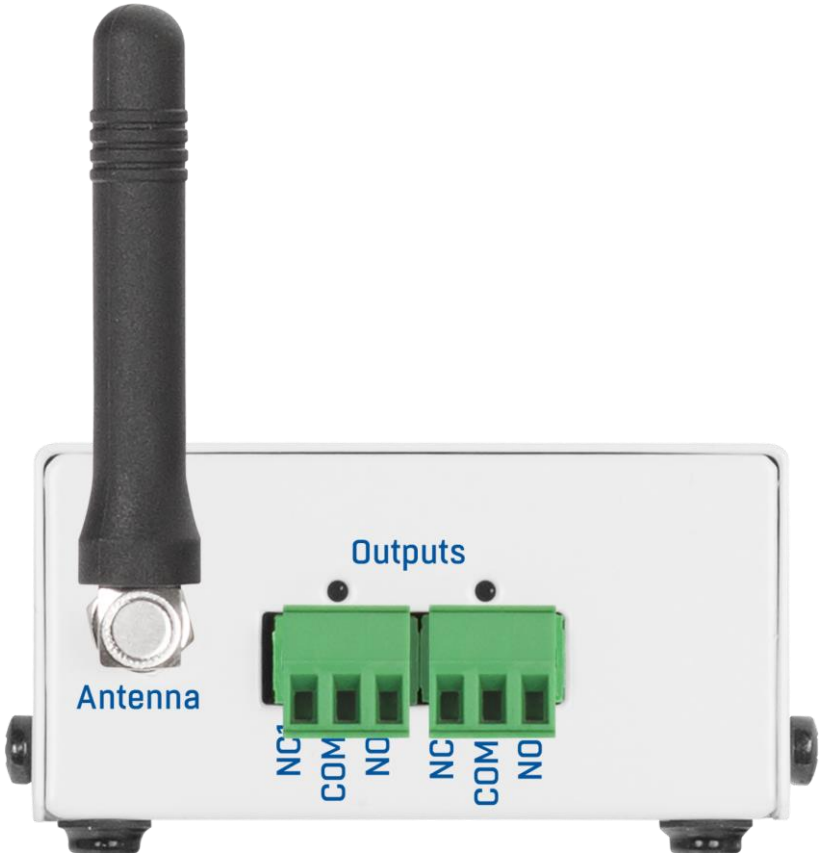
Enhet som interagerar med fysiska enheter och andra digitala enheter i ett IoT-system genom att avkänna och aktivera funktioner i dessa.

Observera att en IoT-enheten är en fysisk enhet såväl som en digital enhet - detta är viktigt då vissa av de fysiska egenskaperna hos IoT-enheten spelar en roll vid användningen inom ett IoT-system, såsom dess läge, eller dess rörelse och acceleration.

Sensor

Ställdon
(Actuator)

Strömförsörjning



TLP:CLEAR

Kommunikation

- **Passiv Infrastruktur:** Ledningsnät: fiber-, koppar- och koaxialkablar.
- **Aktiv Infrastruktur (Kommunikationsnät):** Kommunikationsnät som medger att olika noder i ett IoT-system kan utbyta data och information över en datalänk. Det finns olika typer av kommunikationsnät beroende på tillämpningsområde vilket bland annat inkluderar (W)LANs, (W)PANs, PANs och (W)WANs.
- **Routers:** Nätkomponenter som skickar datapaket mellan olika kommunikationsnät i IoT Ekosystemet.
- **Gateways:** Nätnoder som används som gränssnitt mot andra kommunikationsnät i IoT miljön som använder andra typer av protokoll. Gateways kan innehålla protokolltransformering, funktioner för isolering av fel etc. för att stödja system-interoperabilitet.
- **Protokoll:** Definierar regler för hur kommunikation mellan IoT-enheter ska utföras över en specifik kommunikationskanal. Det finns många olika protokoll för trådlös alternativt trådbunden kommunikation. Exempel på kommunikationsprotokoll för IoT är ZigBee, MQTT, CoAP, BLE, etc.

TLP:CLEAR

Plattform och backend

Plattform

Hantering/management av Enheter och Kommunikationsnät

Hanteringen/management av IoT-systemets enheter och kommunikationsnät inkluderar uppdatering av mjukvara för OS, firmware och applikationer. Det omfattar också spårning och monitorering av enheter och kommunikationsnät, insamling och lagring av loggar som i ett senare skede kan användas för diagnostik.

Enhetsanvändning

Övergripande uppföljning av IoT- systemets enheter och kommunikationsnät för att förstå aktuellt status, användarmönster, prestanda etc.

Backend

Web-baserade tjänster

Detta är tjänster inom World Wide Web, vilka stödjer ett web-baserat gränssnitt för web-användare eller för webanslutna applikationer. Detta innebär att web-teknologi kan användas inom IoT för Människa till Maskin-kommunikation (H2M) och för Maskin till Maskin-kommunikation (M2M).

Moln-infrastruktur och tjänster

Inom IoT, kan moln-backend användas för att aggregera och processa data från spridda enheter och för att stödja beräkningskapacitet, lagring, applikationer, tjänster etc.

Det finns ca 300 plattformar att tillgå!

INDENTIVE

Actility

Microsoft Azure

IBM

amazon

Jasper

GE

icontrol NETWORKS

xively

ThingWorx

BlackBerry

Ayla Networks

ZATAR

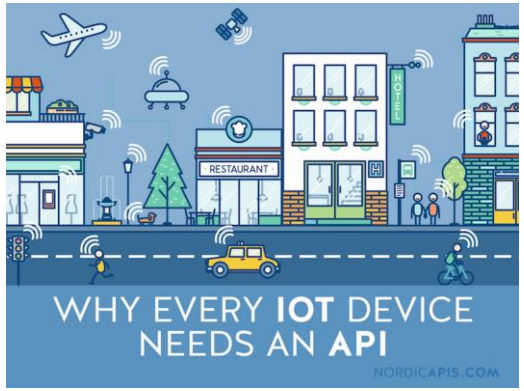
PubNub

SAMSUNG SmartThings

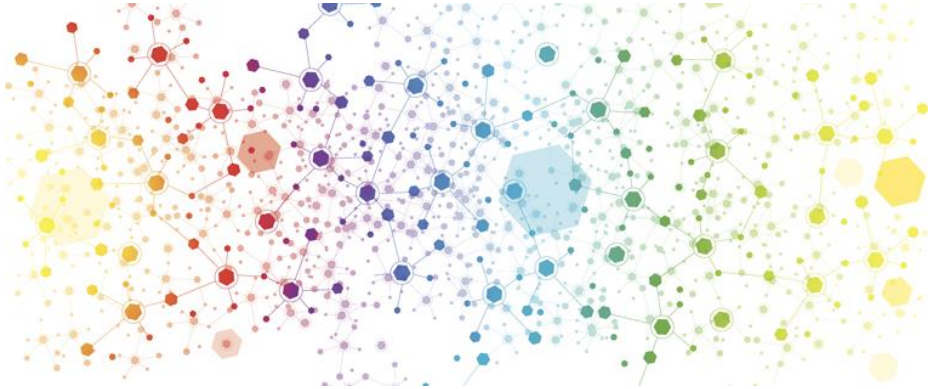
TLP:CLEAR

Applikationer och tjänster

- **Program för användartillämpningar**
- **Leverans-API (Application Programming Interface)**
- **Dataanalys och visualisering**



Efter att data har samlats in och processats kan den framtagna informationen analyseras och visualiseras för att identifiera nya mönster (eng. pattern), effektivisering av drift etc.



Dataanalys och visualisering

IBM Watson

Google AI

Microsoft
Cognitive Services

TLP:CLEAR

Säkerhetstillgångar

Denna grupp omfattar tillgångar som är specifikt fokuserade på säkerheten för IoT-enheter, kommunikationsnät och information

- Tillgångarna inkluderar främst **Brandväggar och preventiv detektering**
- Brandväggar för Web Applikationer (**WAF**)
- programvara för skydd av cloud access (cloud access security broker/**CASB**)
- system för intrångsskydd (Intrusion Prevention System/**IPS**)
- system för hantering av **autentisering/rättigheter**

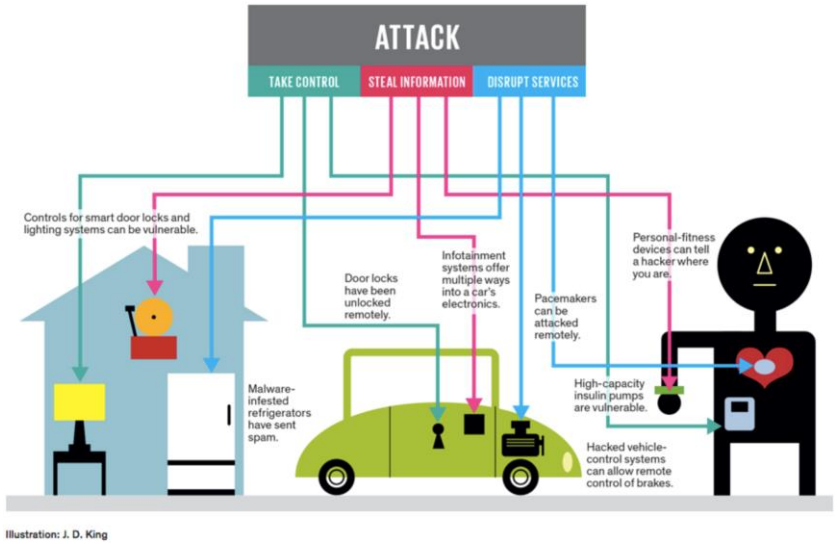
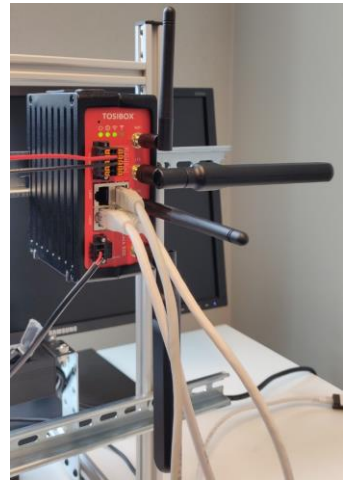
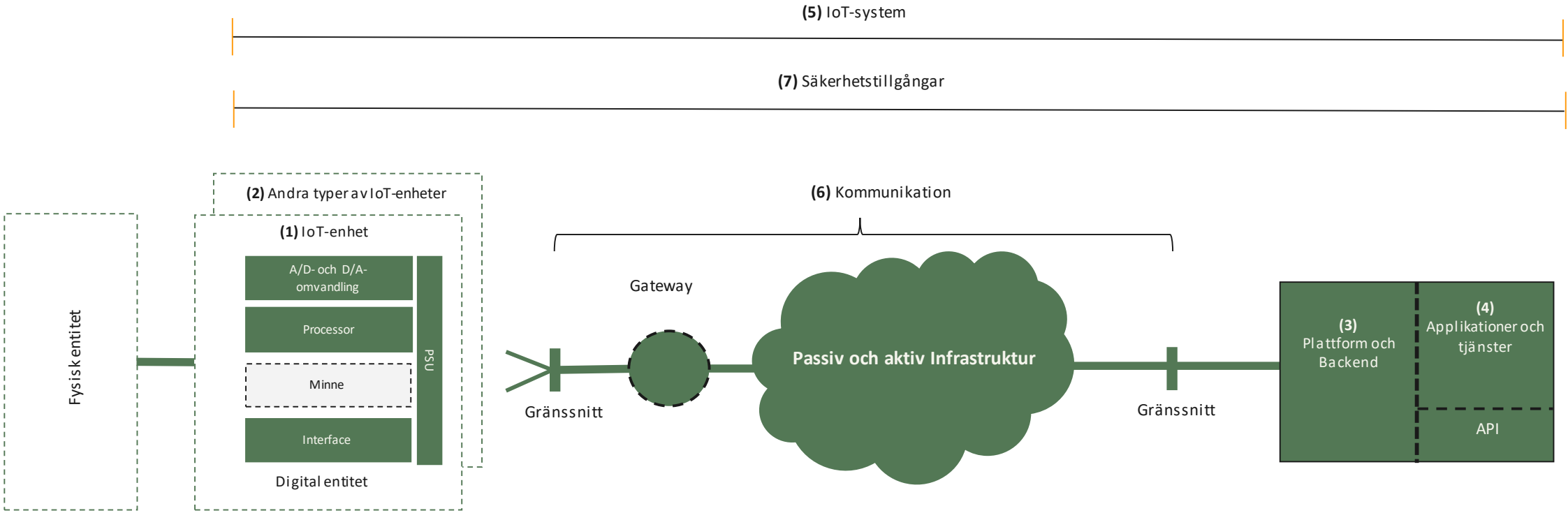


Illustration: J. D. King



TLP:CLEAR

IoT-system: Generisk referensmodell



Det finns sju roller inom ett IoT-system som en hållbar affärsmodell och ett säkerhetsarbete måste hantera

TLP:CLEAR

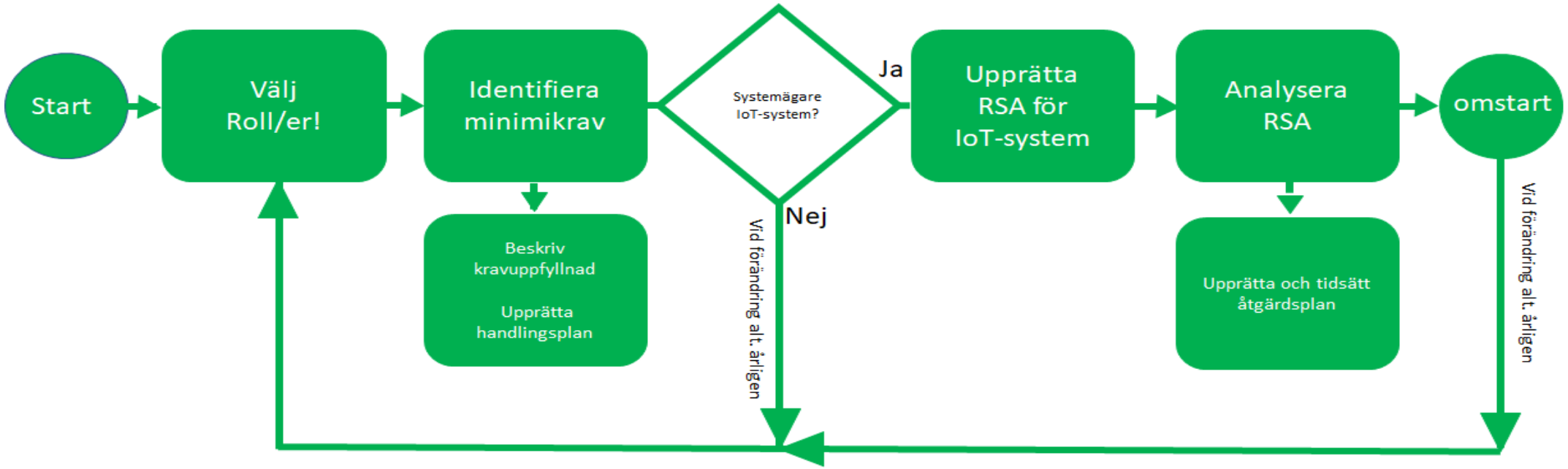
Sju roller inom IoT-systemet

	Roller	Beskrivning
R1	R1	**R1 – Roller för IoT enheter**
	R1.1	*Utvecklar och tillverkar IoT-enheter*
	R1.2	*Levererar IoT enheter*
R2	R2	**R2 – Roller för andra typer av IoT-enheter**
	R2.1	*Utvecklar och tillverkar andra typer av IoT-enheter*
	R2.2	*Levererar andra typer av IoT enheter*
R3	R3	**R3 – Roller för funktionsplattformar och backend**
	R3.1	*1. Utvecklar och ”tillverkar” funktionsplattformar med backendfunktioner. Levererar plattformar med backendfunktioner*
	R3.2	*2.Tillhandahåller, underhåller och driftar funktionsplattformar med backendfunktioner*
R4	R4	**R4 – Roller för applikationer och tjänster**
	R4.1	*1. Utvecklar och ”tillverkar” IoT-applikationer och IoT- tjänster. Levererar IoT-applikationer och IoT- tjänster*
	R4.2	*2. Tillhandahåller, underhåller och driftar IoT-applikationer och IoT- tjänster*
R5	R5	**R5 – Roller för IoT- system**
	R5.1	*1. Utvecklar (t.ex. design, arkitektur, integration, konfiguration) . Levererar IoT-system*
	R5.2	*2. Systemägare*
R6	R6	**R6 – Roller för kommunikation**
	R6.1	*1. Utvecklar kommunikationsnät och tjänster. Levererar kommunikationsnät och tjänster*
	R6.2	*2. Tillhandahåller, underhåller och driftar kommunikationsnät och tjänster*
R7	R7	**R7 – Roller för Säkerhetstillgångar**
	R7.1	*Utvecklar och tillverkar säkerhetstillgångar*
	R7.2	*Levererar säkerhetstillgångar*

Robust & Säker IoT

TLP:CLEAR

Metod för kravanalys och Riskhantering



TLP:CLEAR

Säkerhetsområden och kategorier

Säkerhetsområden – 11 områden

1. **Styrning av säkerheten i informationssystem och riskhantering (Information System Security Governance & Risk Management)**
   Innehåller säkerhetsåtgärder avseende riskanalys, policy, ackreditering, indikatorer och revision samt säkerhetsresurser för informationssystem.

2. **Systemhantering (Ecosystem Management)**
   Innehåller säkerhetsåtgärder avseende kartläggning av ekosystem och ekosystemrelationer.

3. **IT-säkerhetsarkitektur (IT Security Architecture)**
   Innehåller säkerhetsåtgärder avseende systemkonfiguration, förvaltning av tillgångar, systemseparering, trafikfiltrering och kryptografi.

4. **Administration av IT-säkerhet (IT Security Administration)**
   Innehåller säkerhetsåtgärder avseende administrationskonton och administrationsinformationssystem.

5. **Identitets-och åtkomsthantering (Identity and access management)**
   Innehåller säkerhetsåtgärder avseende autentisering, identifiering och åtkomsträttigheter.

6. **Underhåll av IT-säkerhet (IT security maintenance)**
   Innehåller säkerhetsåtgärder avseende underhållsrutiner för IT-säkerhet och fjärråtkomst.

7. **Fysisk- och miljömässig säkerhet (Physical and environmental security)**
   Innehåller fysisk säkerhet och miljöfaktorers påverkan på driftsäkerhet.

8. **Loggning (Detection)**
   Innehåller säkerhetsåtgärder avseende detektering, loggning och loggkorrelation och analys.
9. **Hantering av datasäkerhetsincidenter (Computer security incident management)**
   Innehåller säkerhetsåtgärder avseende analys och hantering av informationssystemets säkerhetsincidenter samt incidentrapport.

10. **Driftsäkerhet (Continuity of Operations)**
    Innehåller säkerhetsåtgärder för hantering av kontinuitet och katastrof.

11. **Krishantering (Crisis Management)**
    Innehåller säkerhetsåtgärder avseende krishanteringsorganisation och process.

Säkerhetskategorier – 3 kategorier

Säkerhetkategorier enligt ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,* utgörs av:

- Säkerhetspolicys (PS)
- Organisation, personal och processmätvärden (OP)
- Tekniska åtgärder (TM)

Säkerhetspolicys

Avser policys som riktar sig mot informationssäkerhet och syftar till att göra den mer konkret och robust.
Policys ska vara tillräckliga för organisationens verksamhet och ska innehålla väl dokumenterad information.
I det här sammanhanget har good practice används som utgångspunkt.
När säkerhets- och integritetsskydd hänför sig till design bör säkerhetsåtgärderna återspegla de särdrag och det sammanhang där IoT-enheten, eller systemet, kommer att användas. Därför kan säkerhet genom design hänvisa till olika specifikationer när en IoT-enhet används i hemmiljö, jämfört med en IoT-enhet i en kritisk infrastruktur.

Organisation, personal och processmätvärden

Alla organisationer ska ha organisatoriska kriterier för hantering av informationssäkerhet.
Personalpraxis ska främja god säkerhet, säkerställa hanteringen av processer och en säker hantering av information i organisationen.
Organisationer bör se till att entreprenörer och leverantörer är ansvariga för givna funktioner.
I händelse av en incident i organisationens säkerhet ska organisationen vara förberedd med tydliga roller för ansvar, utvärdering och åtgärder.

Tekniska åtgärder

För att minska sårbarheten i det tekniska systemet ska säkerhetsåtgärder och god praxis implementeras och omfatta systemets tekniska element.
Tekniska mätvärden ska ge nödvändiga indata för de tekniska åtgärder som krävs för att bevara och skydda informationssäkerheten.
Vid tillämpning av dessa tekniska åtgärder bör man ta hänsyn till särdragen i IoT-ekosystemet. Det innebär till exempel att vid ett stort antal involverade enheter och produkter kan vissa åtgärder behöva utföras med specialiserade arkitektoniska komponenter, t.ex. gateways.

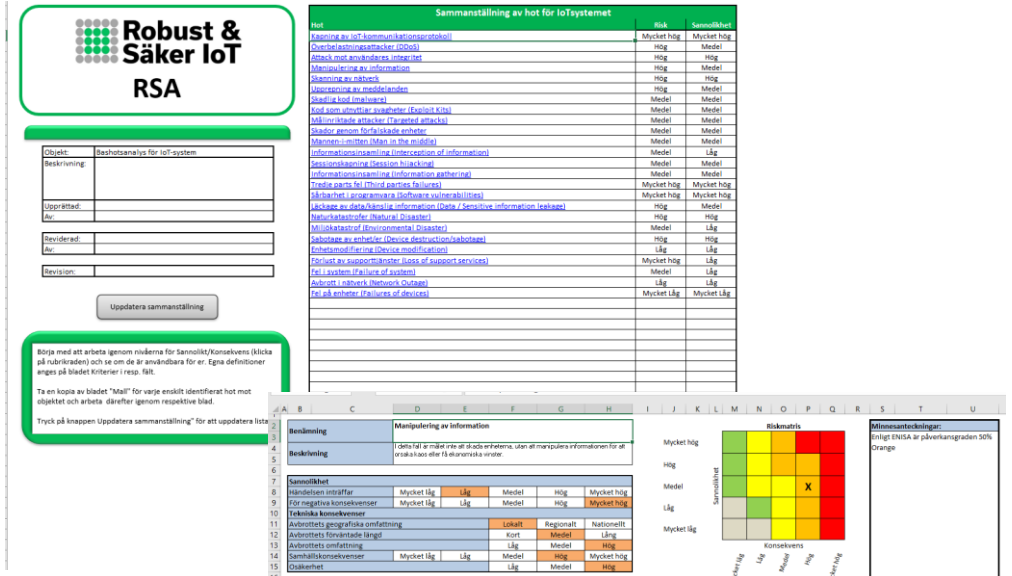
Kravanalys

Säkerhetsområde	Huvudkategori	Delkategori	Index	Åtgärd	Roll1	Roll2	Roll3	Roll4	Roll5	Roll6	Roll6
3	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom design	**GP-PS-05**	GP-PS-05: Arkitekturen ska utformas i segment/delar som kapslar in element i händelse av attacker.	R1	R2	R3	R4	R5	R6	R7.1
2	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom design	**GP-PS-02**	GP-PS-02: Möjligheten att integrera olika säkerhetspolicyer (inkl. roller och ansvar) och tekniker för en konsekvent säkerhetskontroll av olika enheter och användarnät i ett IoT-system ska säkerställas.			R3.2	R4.2	R5.2	R6.2	
6	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom design	**GP-PS-06 A**	GP-PS-06 A: Testplaner för att verifiera att en produkt som installeras i ett system fungerar som förväntat ska implementeras. Testplanerna ska också omfatta felaktig beteende t.ex handhavandefel.	R1	R2	R3.1	R4.1	R5.1	R6.1	R7
6	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom design	**GP-PS-06 B**	GP-PS-06 B: Penetrationstester ska användas för att identifiera felaktig inmatningshantering, bypassförsök vid autentisering och för övergripande säkerhetsstatus.			R3.2	R4.2	R5.2	R6.2	
6	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom design	**MK 1**	MK 1: Använd separata miljöer för utveckling, testning och produktion så att operativa verksamhetsprocesser och produktionsdata inte påverkas vid fel i utvecklings- och testprocessen	R1	R2	R3.1	R4.1	R5.1	R6.1	R7
3	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom design	**GP-PS-04**	GP-PS-04: Vid utformning av lösningar för energibesparing ska säkerheten inte äventyras.	R1	R2			R5.1		
3	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom design	**GP-PS-03**	GP-PS-03: Vid utformningen av säkerhetslösningar ska risken för människors säkerhet vägas in.	R1	R2	R3.1	R4.1	R5.1	R6.1	R7
2,3	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom design	**GP-PS-01**	GP-PS-01: Säkerheten för hela IoT-systemet ska hanteras genom ett konsekvent förhållningssätt enligt kapitel *Analysprocessen* under hela livscykeln. Detta görs på alla nivåer av enhet/applikationsdesign och utveckling samt omfattar också säkerhetsaspekterna under utveckling, tillverkning och implementering.					R5		
6	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom design	**GP-PS-07 A**	GP-PS-07 A: Kodgranskning ska genomföras under implementationen, detta bidrar till att minska buggar i en slutlig version av en produkt.	R1	R2	R3.1	R4.1	R5.1	R6.1	R7
6	7.1 Säkerhetspolicy (PS)	7.1.1 Säkerhet genom	**GP-PS-07 B**								

TLP:CLEAR

Risk- och sårbarhetsanalys
Metod och verktyg

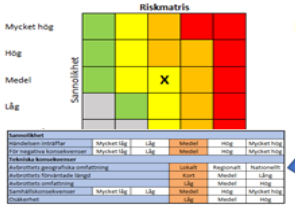
- Välj och beskriv analysobjekt
- Identifiera hot
- Gruppera ock klassificera hot
- Genomför en riskanalys
- Sammanställning och rapport
- Handlingsplan – åtgärdslista
- Riskhantering enligt åtgärdsplan
- Kontinuitetsplanering



Bashot byggda på empirisk kunskap och faktainsamling

Basinput till RSA

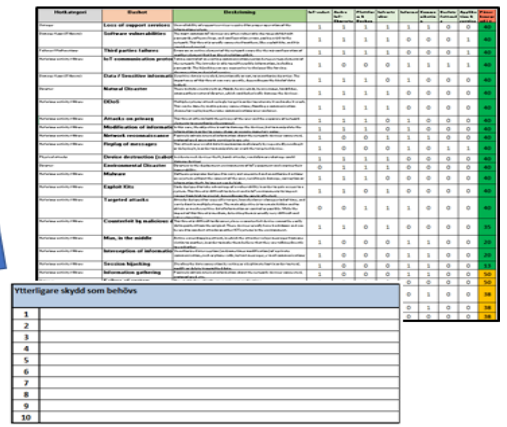
Risk- och sårbarhetsanalys för Robust & säker IoT



Resultat RSA

Restpunkter

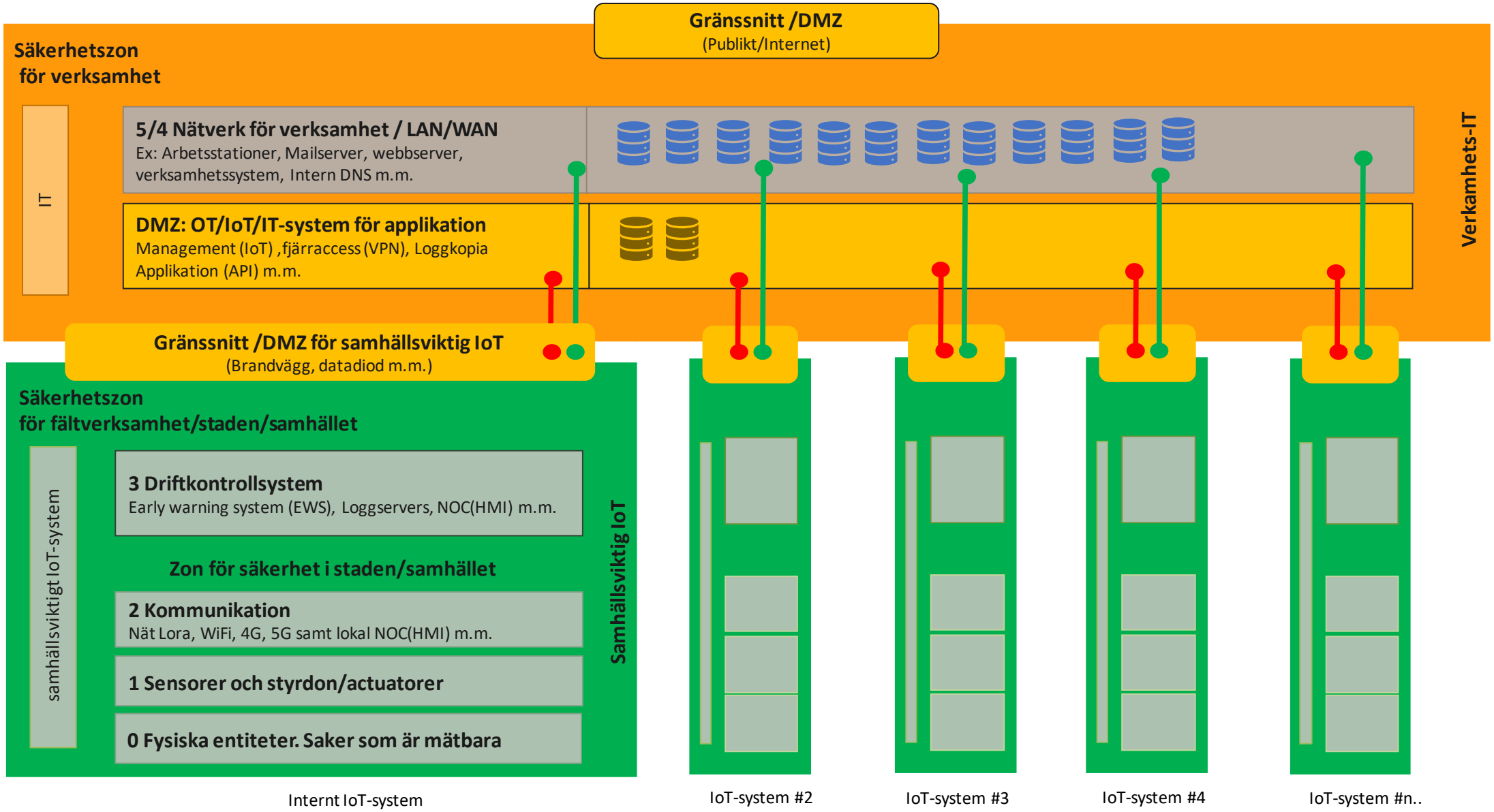
Säkerhetsläget efter RSA



Åtgärdsplan

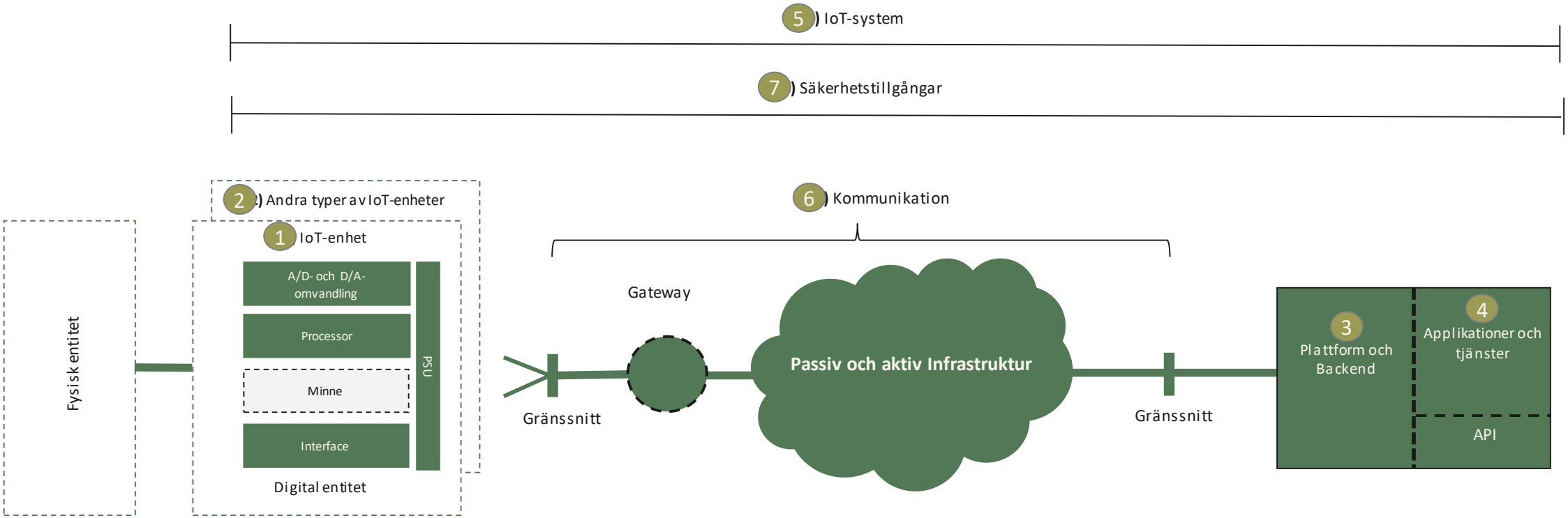
TLP:CLEAR

IoT-Arkitektur baserat på purdue för samhällsviktig IoT



TLP:CLEAR

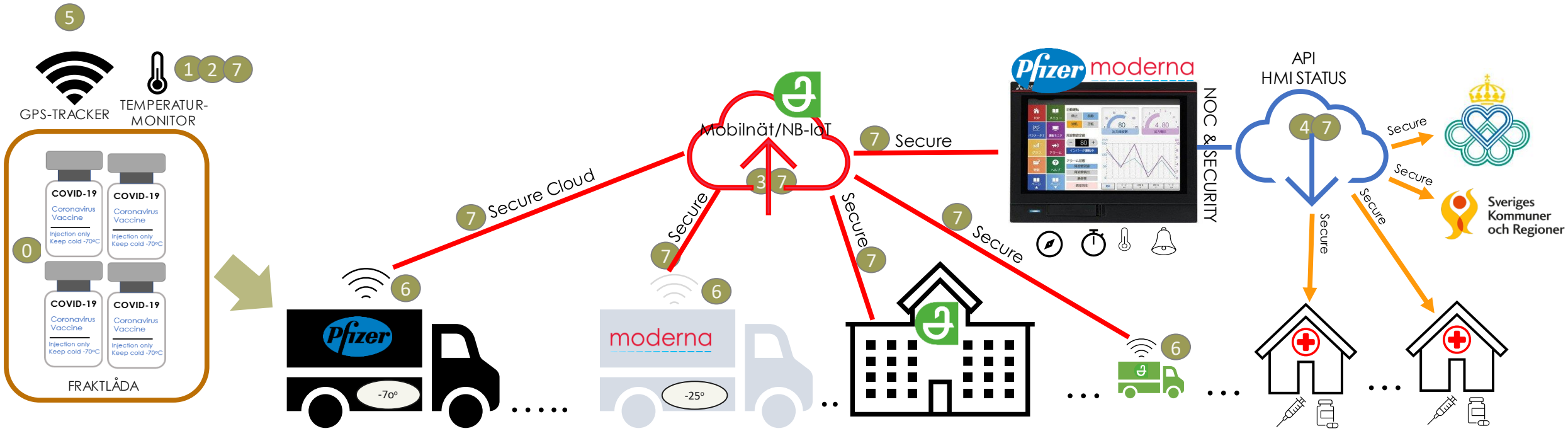
Exempel på tjänster
IoT-system: Generisk referensmodell

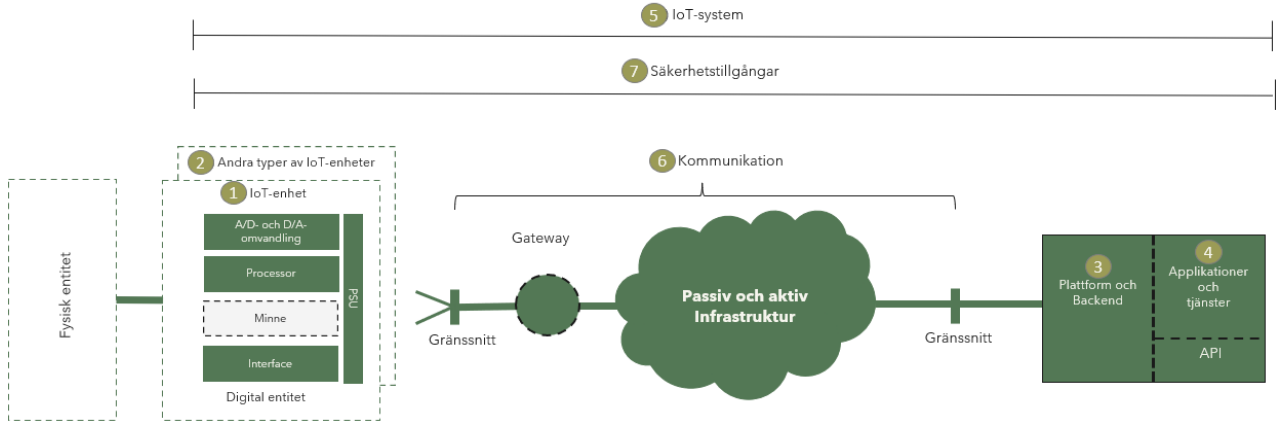


TLP:CLEAR

Exempel på IoT-tjänst

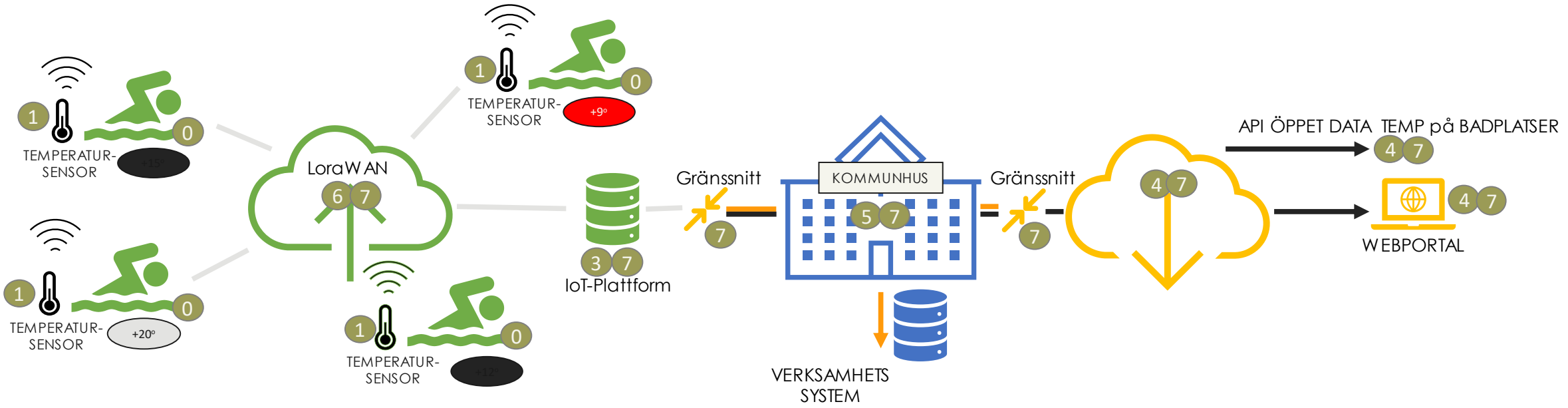
Övervakning av vaccintransport med temperaturbevakning, larm och position

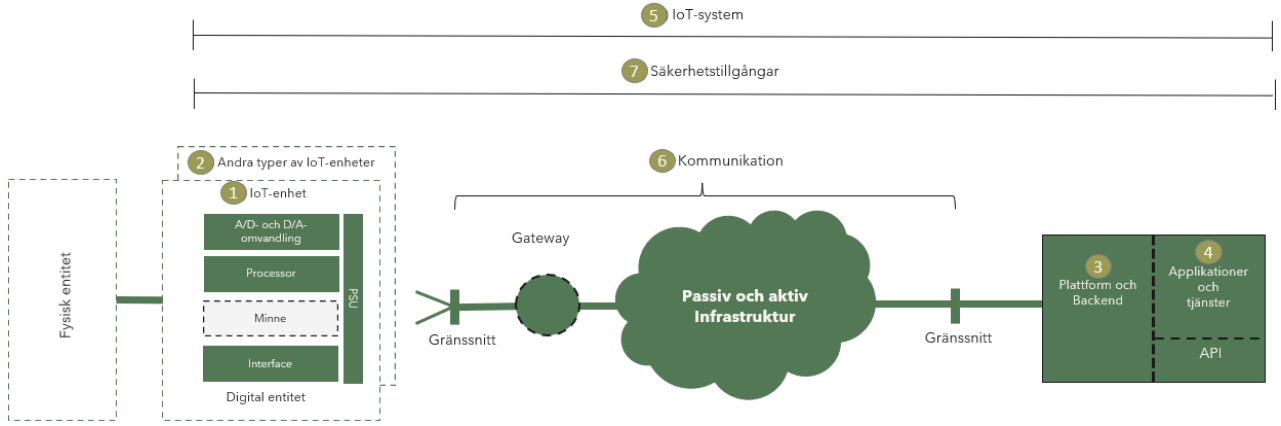




TLP:CLEAR

Exempel på IoT-tjänst:
Badtjänst

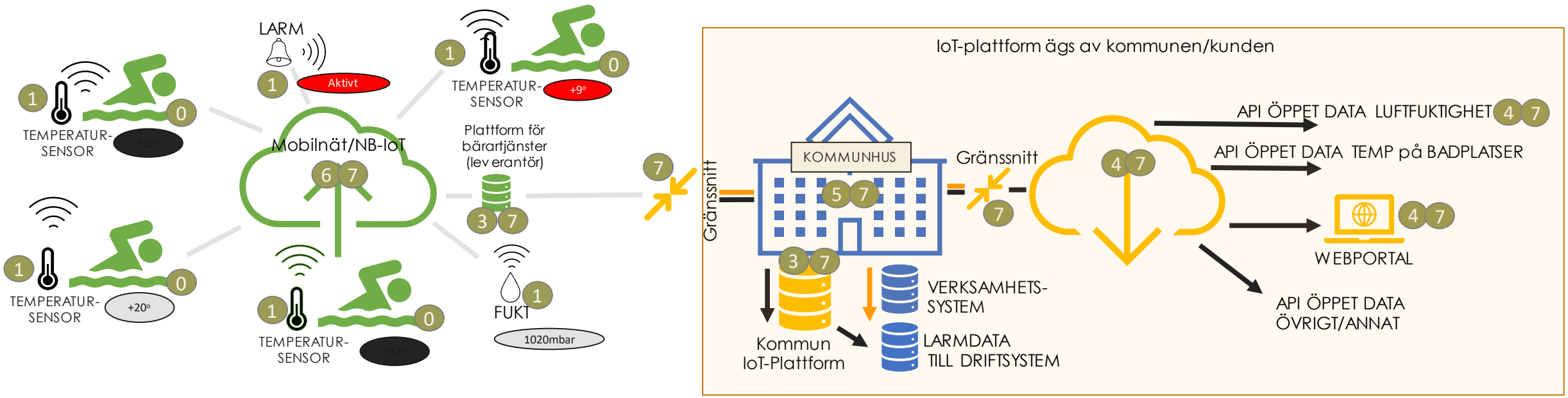


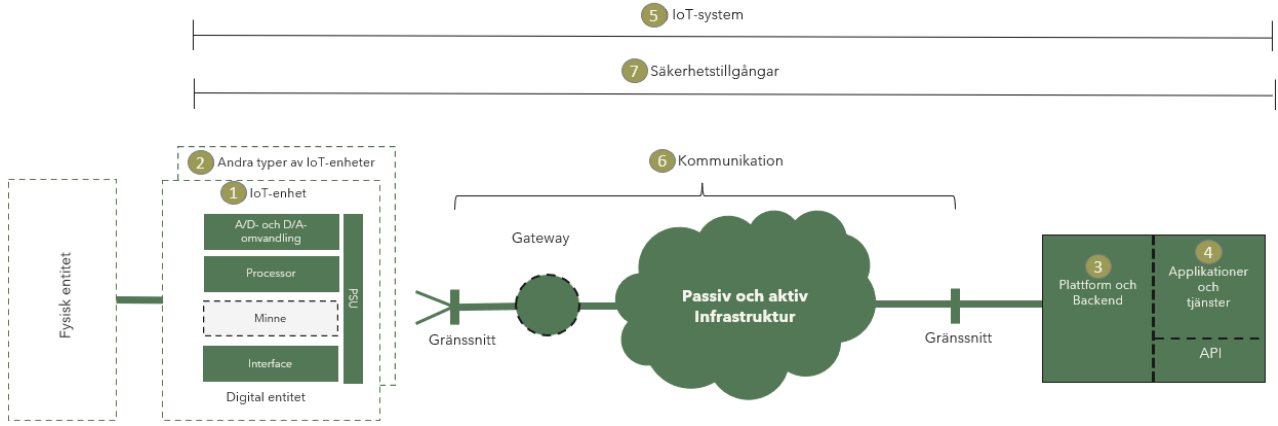


TLP:CLEAR

Exempel på IoT-tjänst

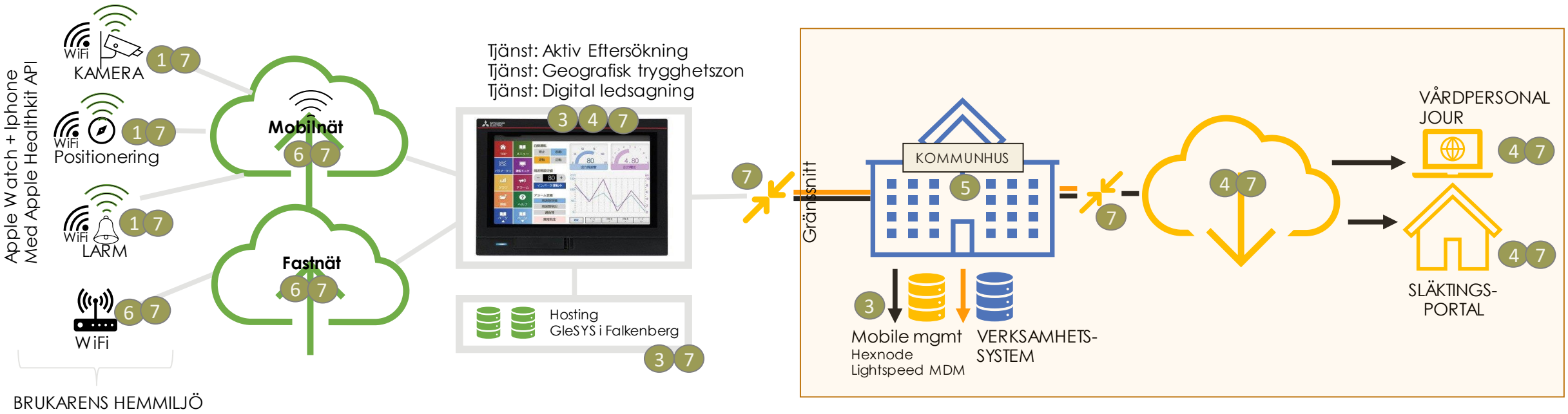
Transport av mätvärden

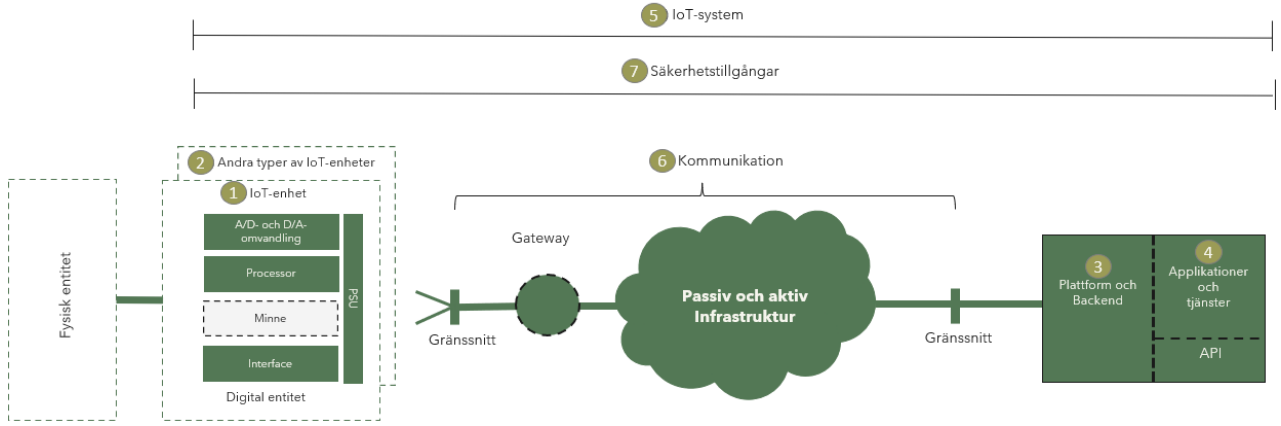




TLP:CLEAR

Exempel på IoT-tjänst
Stödvård I hemmet





TLP:CLEAR


STADSNÄTS
FÖRENINGEN