Avtal Robust & säker IoT version 1.0

2021-03-10

Per Lindström
Kommersiell Produktchef
per.lindstrom@ssnf.org
08-214 606

Avtal Robust & Säker IoT

Ett helt nytt öppet avtal för
robust & säker IoT

Framtaget i samverkan!

Version 1.0 lanserad 1 mars 2021

Dagens innehåll

- Avtalsmodell och innehåll – Per Lindström
- Teknisk och arkitektonisk design – Jimmy Persson
- Viktiga avtalsaspekter – Robert Wälikangas

Bakgrund

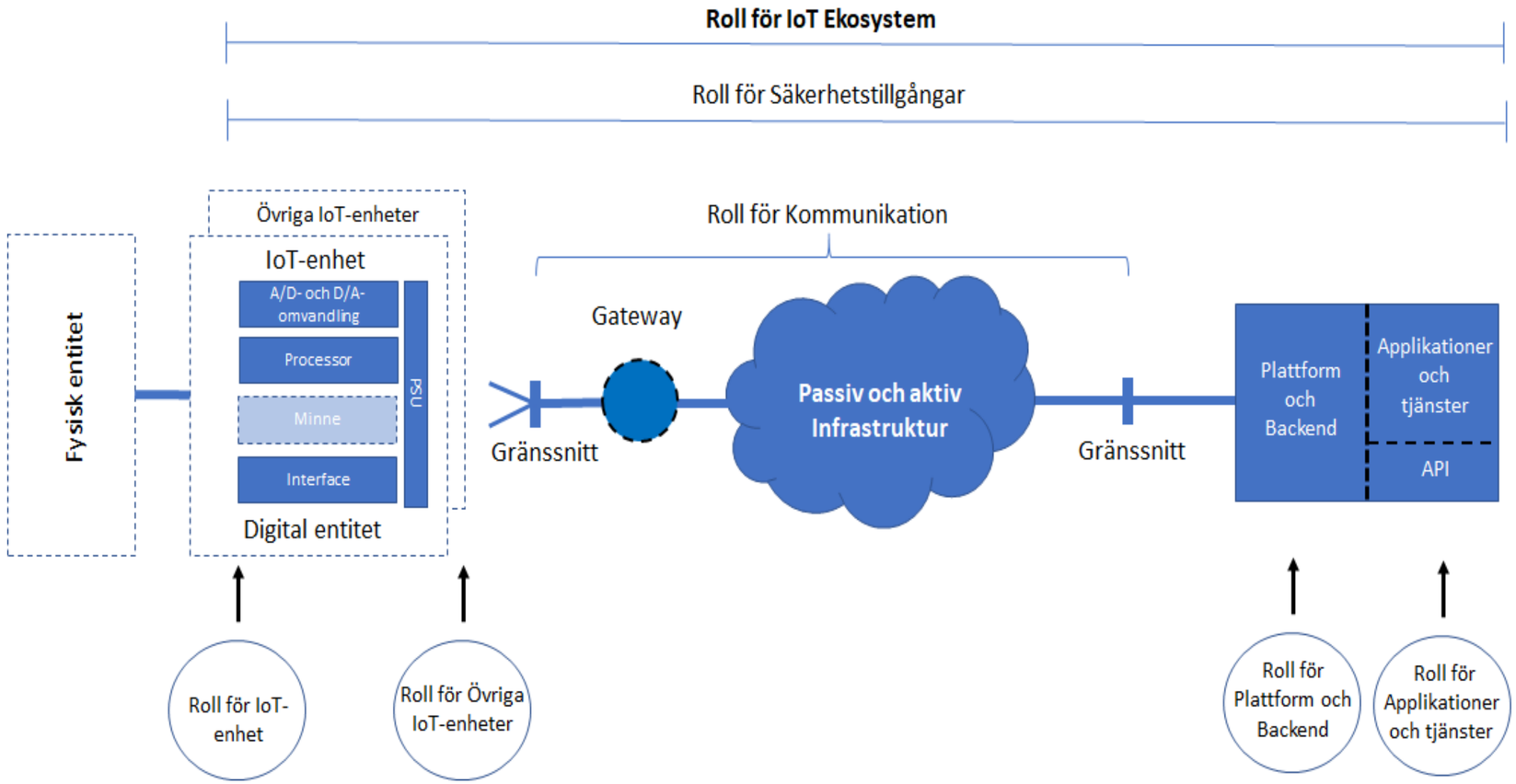
Robust & Säker IoT

- Samhällets beroende av tjänster för IoT ökar
- **Beroendet till IoT** gör att hanteringen av utrustningar, system och infrastruktur för IoT **måste vara robust och säker**.
- Det har saknats ett **avtalspaket för IoT** som möter marknadens behov och är anpassad för SKR:s process **KLASSA för IoT**
- **Ett standardavtal** med modulär avtalsmodell ger möjlighet att **förenkla avtal kring IoT- tjänster** och utöka utbudet av komplexa tjänster
- Avtalet öppnar för en **branschgemensam** syn på **allmänna villkor, servicenivåer** och **felhantering**

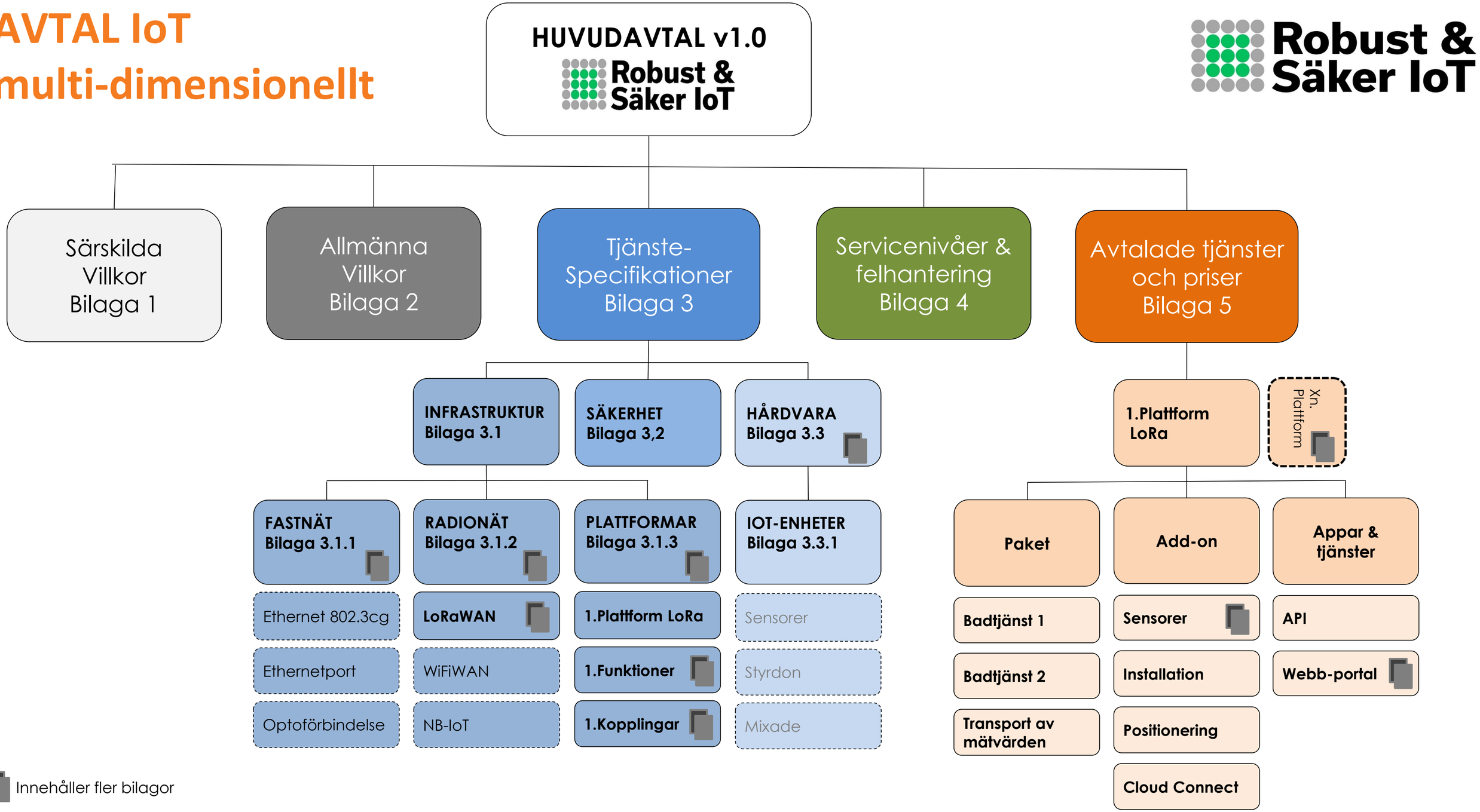
Vägledning för Robust & Säker IoT - grund för avtalspaket

Robust & Säker IoT

Vägledning för Robust & Säker IoT beskriver ett ekosystem för IoT-roller som gäller för olika roller som t.ex. utvecklare, tillverkare, leverantör av produkter och tjänster, integratörer

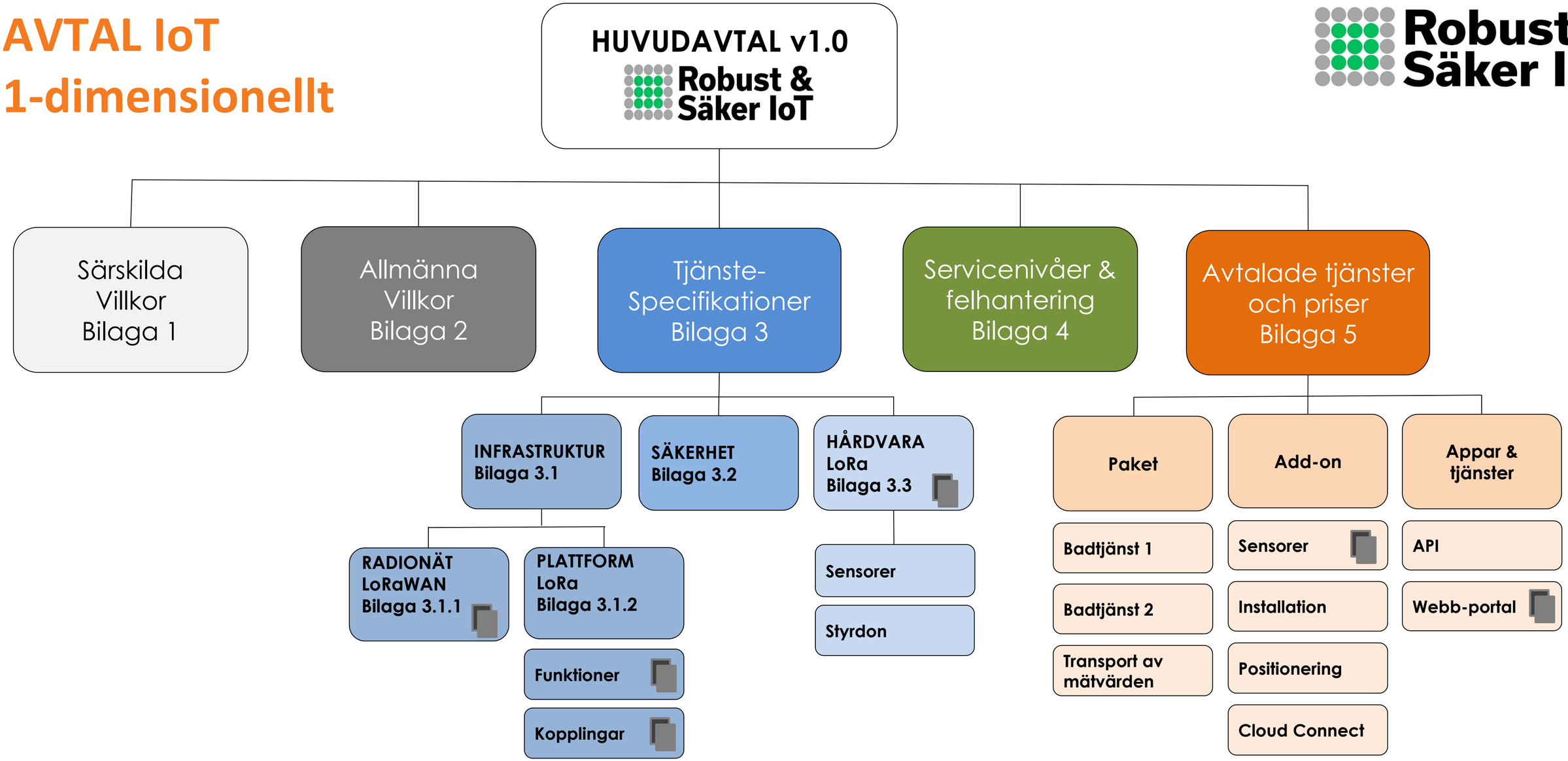


AVTAL IoT
multi-dimensionellt



Innehåller fler bilagor

AVTAL IoT
1-dimensionellt

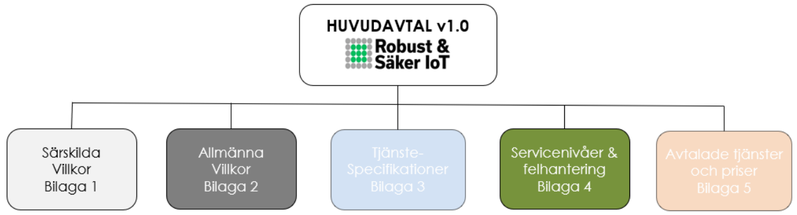


Innehåller fler bilagor

Avtalsdokument Robust & säker IoT 1.0

Huvudavtal

- Huvudavtal tecknas mellan parterna som ramverk



Särskilda villkor

- Innehåller eventuella avvikelser från standardvillkor

Allmänna villkor

- Allmänna villkor kan förändras över tid med en godkännandeprocess utan att teckna om huvudavtalet

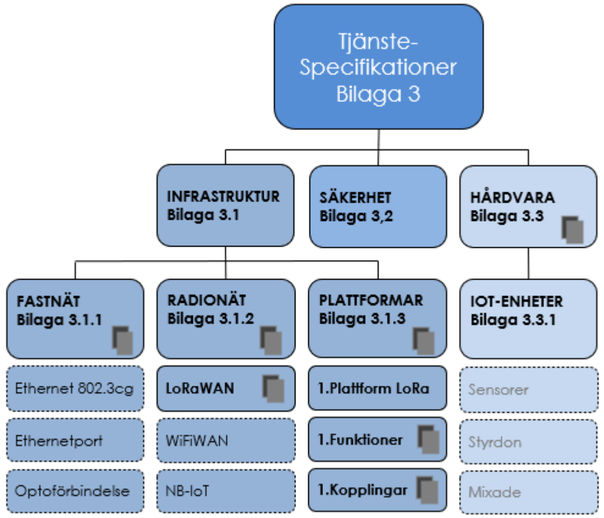
Servicenivåer & felhantering

- Gemensam bilaga för SLA och felhanteringsrutiner

Tjänstespecifikationer

Robust & Säker IoT

Uppdelad i Infrastruktur, Säkerhet och Hårdvara



Infrastruktur

- Beskriver ingående nät (fastnät, radionät) och plattformar (tex LoRaWAN, Wifi)

Säkerhet

- Beskriver säkerhetsarbete för informationssäkerhet driftsäkerhet och arkitektur.

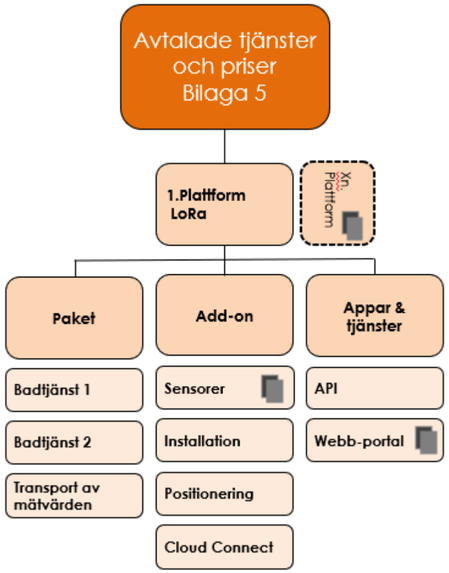
Hårdvara

- Tekniska specifikationer av produkter som tillhandahålls av nätägare och systemägaren av IoT-system.

Avtalade tjänster och priser

Robust & Säker IoT

Tjänster som kan tillhandahållas inom Avtalet



Erbjudande uppdelat per plattform

- LoraWAN finns med som exempel

Paketerade Tjänster

- Badtjänst och Transport av mätvärden finns med som enkla **LoraWAN**-exempel med förslag på prismodell

Add-on (tillägg)

- Sensorer, installation, etc

Appar & tjänster

- Webb-portal, API

Arbetsgrupp som medverkat

Robust & Säker IoT

SVENSKA STADSNÄTS FÖRENINGEN

ServaNet DITT LOKALA FIBERNÄT

sandnet

pingday.

IoTOPEN

utsikt bredband

VARBERG ENERGI

EL & STADSN

Corporate Fiber

AFFÄRS VERKEN

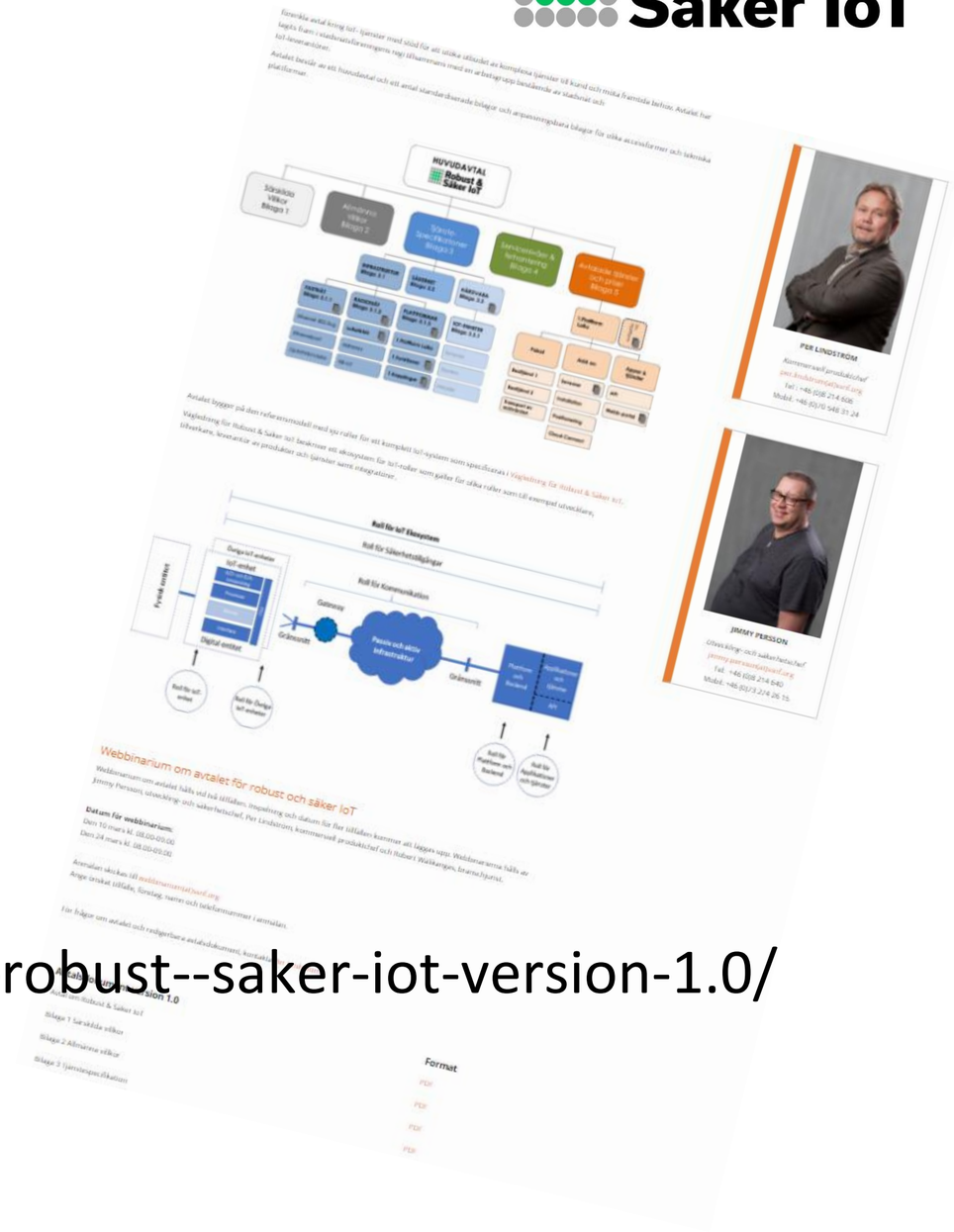
itn IT NORRBOTTEN

netmore

Göteborg Energi

DIGITAL NORDIX Connectivity as-a-service

Avtalsdokument
Robust & säker IoT 1.0



Avtalsdokument finns tillgängliga på Stadsnätsföreningens webbplats

https://www.ssnf.org/nat-i-varldsklass/avtal/nyhet-avtal-robust--saker-iot-version-1.0/

Tack så mycket för mig. Frågor?

Per Lindström
Kommersiell Produktchef
per.lindstrom@ssnf.org
08-214 606

Samhällsviktig IoT Teknisk och arkitektonisk design

AVTAL ROBUST & SÄKER IOT V1.0: TJÄNSTESPECIFIKATION BILAGA 3.2 SÄKERHET

MARS 2021

Jimmy Persson
Utveckling- och säkerhetschef
Jimmy.persson@ssnf.org
08-214 640

TLP:WHITE

Informationsäkerhetsklassning

TLP:WHITE

TLP:WHITE = Ingen begränsning kring hur informationen får delges och spridas.

Ingen begränsning kring hur informationen får delges och spridas. Informationsägare kan använda TLP:WHITE när delning av informationen medför liten eller ingen förutsägbar risk för felanvändning, i enlighet med tillämpliga regler och förfaranden för offentliggörande. Med förbehåll för vanliga upphovsrättsregler kan information märkt med TLP:WHITE delas utan restriktioner.

Jag ska tala om …..

- Purdue*, IoT-säkerhet och samhällsviktighet
- Referensmodell för IoT
- **CASE:** Badtemperaturtjänst
- **CASE:** Transport av mätvärden
- **CASE:** Stödvård i hemmet

IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

* Purdue Enterprise Reference Architecture (PERA) is a 1990s reference model for enterprise architecture, developed by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing

Robust & Säker IoT

TLP:WHITE

Hantverket inom IoT-Säkerhet

Hantverket i säkerhetsarbetet handlar bland annat om att ge enkel åtkomst till data för de i organisationen som behöver det för att göra sitt jobb.

Men samtidigt **skydda data och information** genom att förhindra tillgång från utomstående som inte ska se, ändra eller ta bort data och information..

IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

TLP:WHITE

IoT-Säkerhet: Råd på vägen

- Beakta **dataskydd** och datasäkerhet (GDPR)
- Standarder för **IoT-säkerhet skiljer sig från de för IT-säkerhet** eftersom verksamhetssystemens behov skiljer sig från behoven för IoT-system.
- Rekommendationen är att **hålla systemarkitekturen för IoT enkel.** Det blir komplext över tid ändå.
- **Paketera inte ihop** verksamhetssystem med IoT-system.
- Tätt kopplade system är **svåra att hantera.**

IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

TLP:WHITE

Purdue Enterprise Reference Architecture (PERA)

Nivå 0 är de fysiska processerna i företaget

Nivå 1 är sensorer och andra anordningar som mäter och direkt påverkar de fysiska processerna

Nivå 2 är styrsystem och användargränssnitt

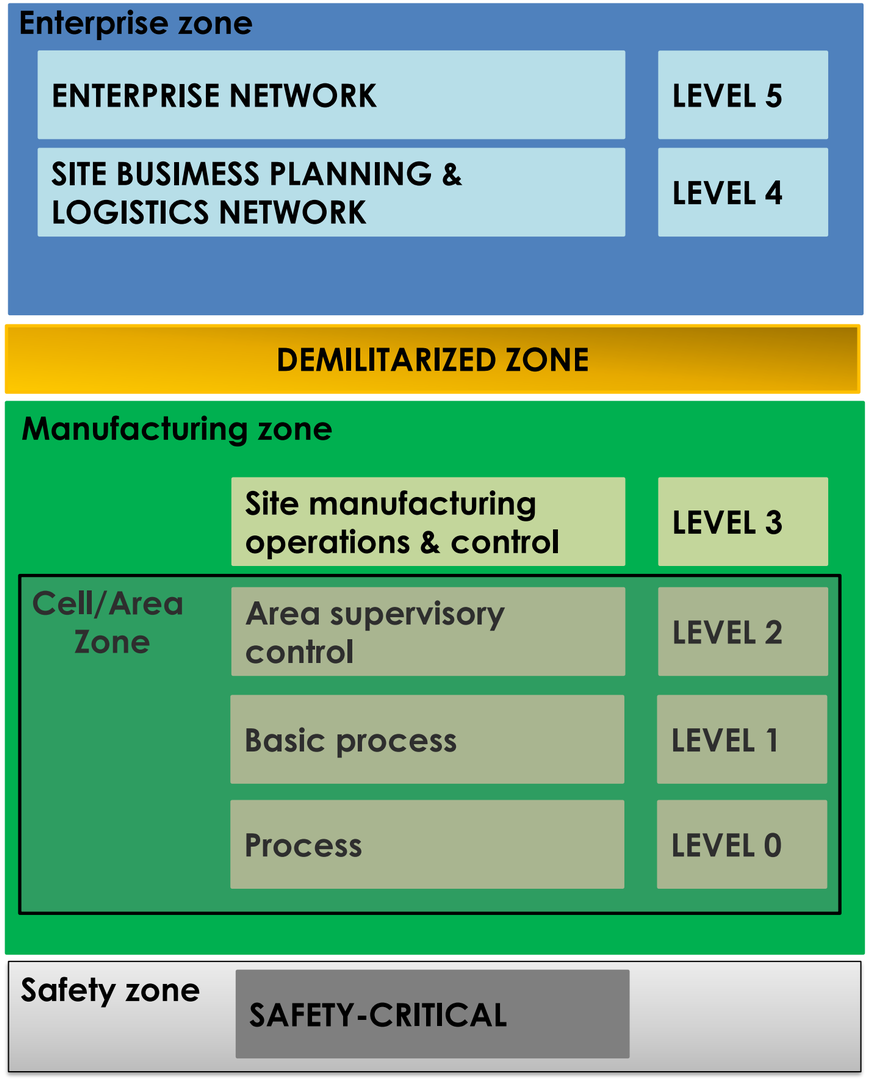
NIVÅ 3 är system som hanterar tillverkningsprocessen

NIVÅ 4 är affärssystem och logistik

NIVÅ 5 är företagets nätverk och övriga system

DEMILITARIZED ZONE gränssnittet mellan verksamhetssystem och IoT-systemet. Regler och kontroll

SAFETY ZONE är säker zon för maskiner, apparater m.m.



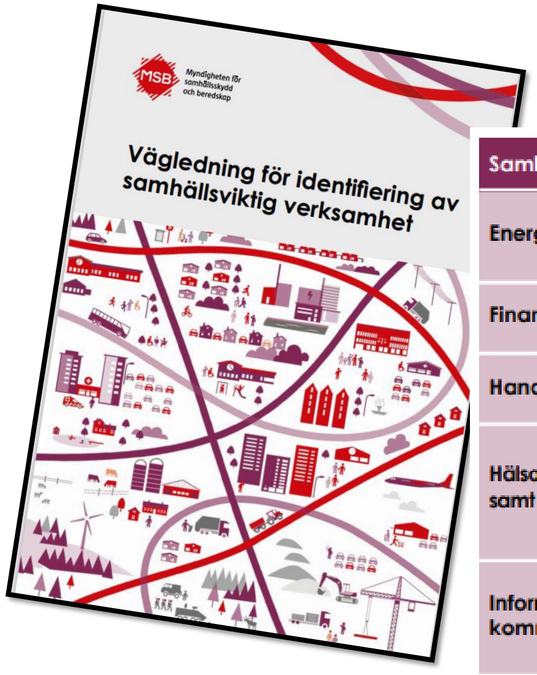
* Purdue Enterprise Reference Architecture (PERA) is a 1990s reference model for enterprise architecture, developed by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing. http://www.pera.net

TLP:WHITE

Samhällsviktig Verksamhet

"Med samhällsviktig verksamhet avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet."

Källa: MSB Definition av samhällsviktig Verksamhet



Samhällssektor	Exempel på viktiga samhällsfunktioner
Energiförsörjning	Produktion av el, distribution av el, produktion och distribution av fjärrvärme, produktion och distribution av bränslen och drivmedel.
Finansiella tjänster	Betalningar, tillgång till kontanter, centrala betalningssystemet, värdepappershandel.
Handel och industri	Bygg- och entreprenadverksamhet, detaljhandel, tillverkningsindustri.
Hälso- och sjukvård samt omsorg	Akutsjukvård, läkemedels- och materielförsörjning, omsorg om barn, funktionshindrade och äldre, primärvård, psykiatri, socialtjänst, smittskydd för djur och människor.
Information och kommunikation	Telefoni (mobil och fast), internet, radiokommunikation, distribution av post, produktion och distribution av dagstidningar, webbaserad information, sociala medier.
Kommunalteknisk försörjning	Dricksvattenförsörjning, avloppshantering, renhållning, väghållning.
Livsmedel	Distribution av livsmedel, primärproduktion av livsmedel, kontroll av livsmedel, tillverkning av livsmedel.
Offentlig förvaltning	Lokal ledning, regional ledning, nationell ledning, begravningsverksamhet, diplomatisk och konsulär verksamhet.
Skydd och säkerhet	Domstolsväsendet, åklagarverksamhet, militärt försvar, kriminalvård, kustbevakning, polis, räddningstjänst, alarmeringstjänst, tull-kontroll, gränsskydd och immigrationskontroll, bevaknings- och säkerhetsverksamhet.
Socialförsäkringar	Allmänna pensionssystemet, sjuk- och arbetslöshetsförsäkringen.
Transporter	Flygtransport, järnvägstransport, sjötransport, vägtransport, kollektivtrafik.

Tabell 1. Exempel på samhällssektorer och viktiga samhällsfunktioner

TLP:WHITE

IoT-Arkitektur baserat på purdue för samhällsviktig IoT

Traditionell Purdue-arkitektur för industriell styrning

Enterprise zone

ENTERPRISE NETWORK	LEVEL 5
SITE BUSIMESS PLANNING & LOGISTICS NETWORK	LEVEL 4

DEMILITARIZED ZONE

Manufacturing zone

	Site manufacturing operations & control	LEVEL 3
Cell/Area Zone	Area supervisory control	LEVEL 2
	Basic process	LEVEL 1
	Process	LEVEL 0

Safety zone — SAFETY-CRITICAL

Purdue-arkitektur för samhällsviktig IoT

Gränssnitt /DMZ
(Publikt/Internet)

Säkerhetszon för verksamhet

IT

5/4 Nätverk för verksamhet / LAN/WAN
Ex: Arbetsstationer, Mailserver, webbserver, verksamhetssystem, Intern DNS m.m.

DMZ: OT/IoT/IT-system för applikation
Management (IoT) ,fjärraccess (VPN), Loggkopia Applikation (API) m.m.

Verksamhet-IT

Gränssnitt /DMZ för samhällsviktig IoT
(Brandvägg, datadiod m.m.)

Säkerhetszon för fältverksamhet/staden/samhället

Samhällsviktig IoT

3 Driftkontrollsystem
Early warning system (EWS), Loggservers, NOC(HMI) m.m.

Zon för säkerhet i staden/samhället

2 Kommunikation
Nät Lora, WiFi, 4G, 5G samt lokal NOC(HMI) m.m.

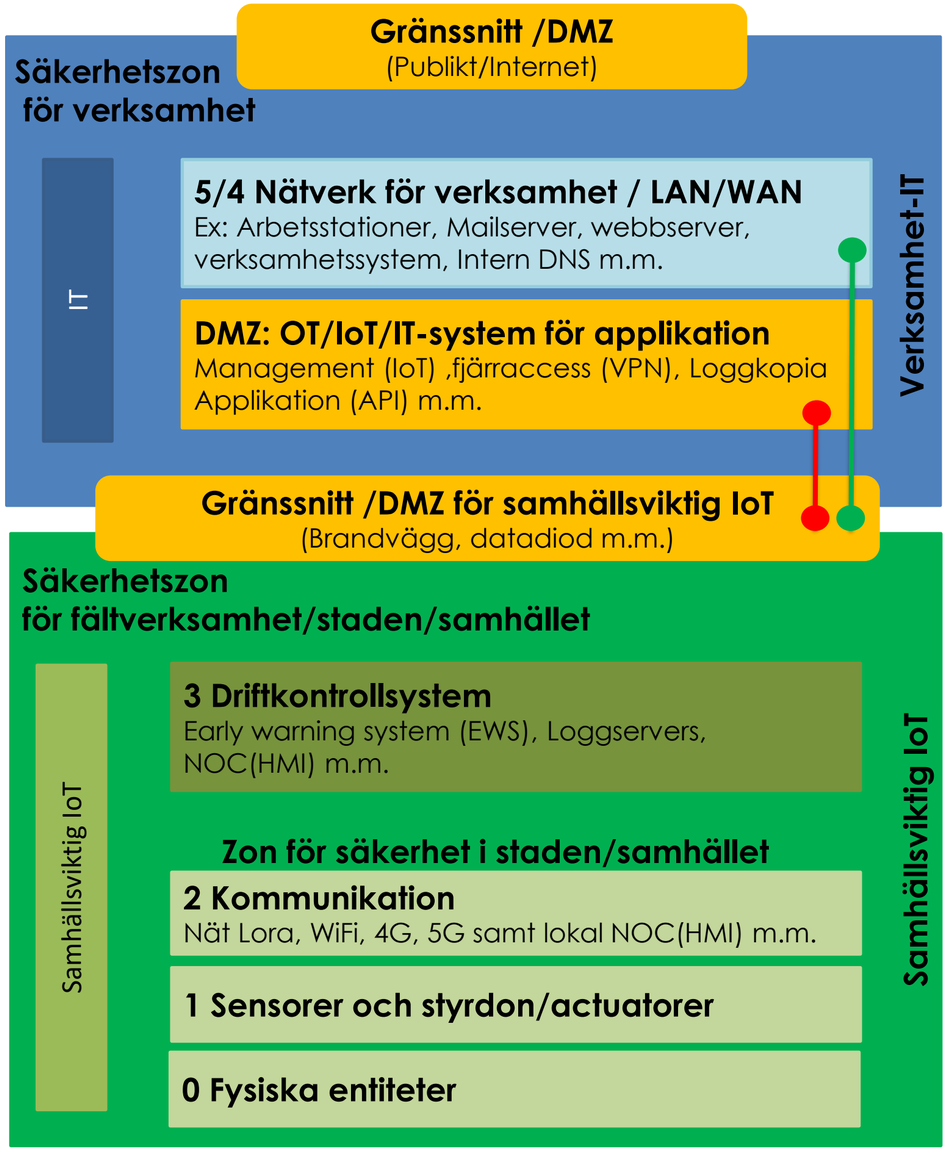
1 Sensorer och styrdon/actuatorer

0 Fysiska entiteter. Saker som är mätbara

Samhällsviktig IoT

TLP:WHITE

IoT-Arkitektur baserat på purdue för samhällsviktig IoT



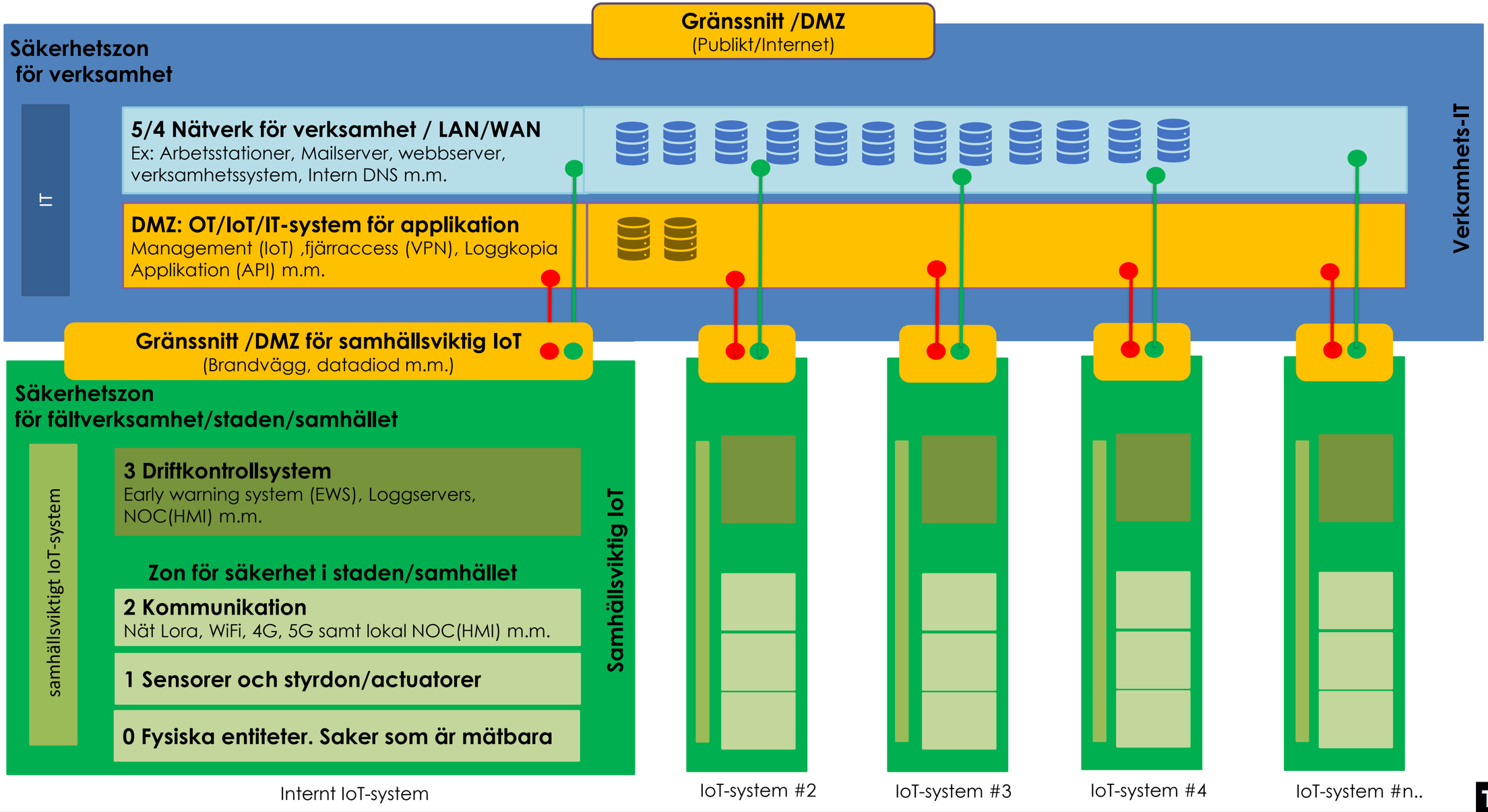
Begreppet Samhällsviktig IoT innefattar:

- IoT för den smarta staden
- Traditionell styr- och regler
- Operational technology (OT)
- Industriell IoT (IIoT)
- Kritisk IoT

Fysisk entitet är:
Är något mätbart.

TLP:WHITE

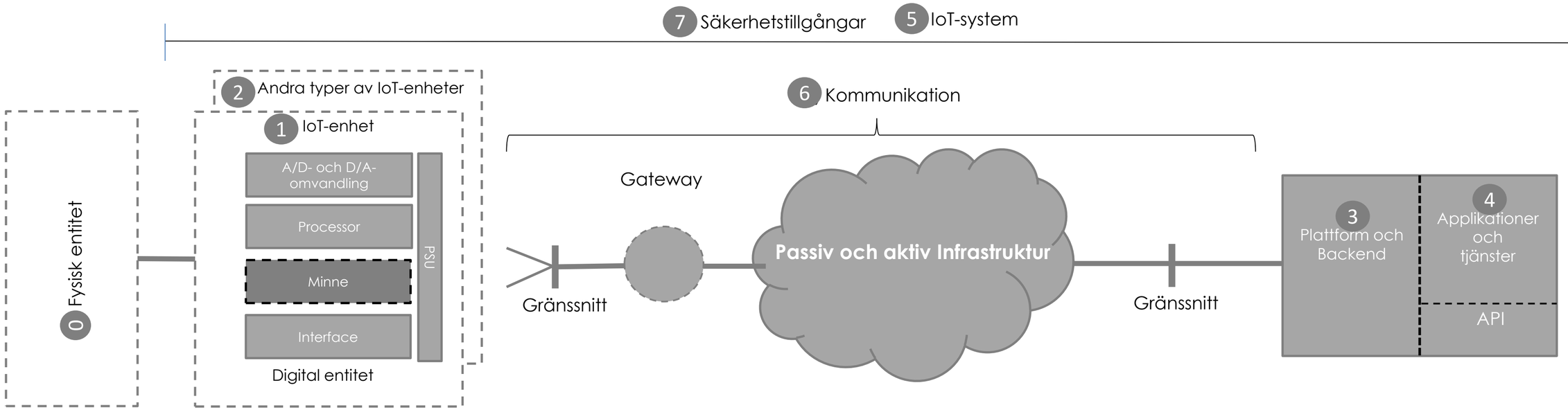
IoT-Arkitektur baserat på purdue för samhällsviktig IoT



TLP:WHITE

IoT-system: Generisk referensmodell

Robust & Säker IoT



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

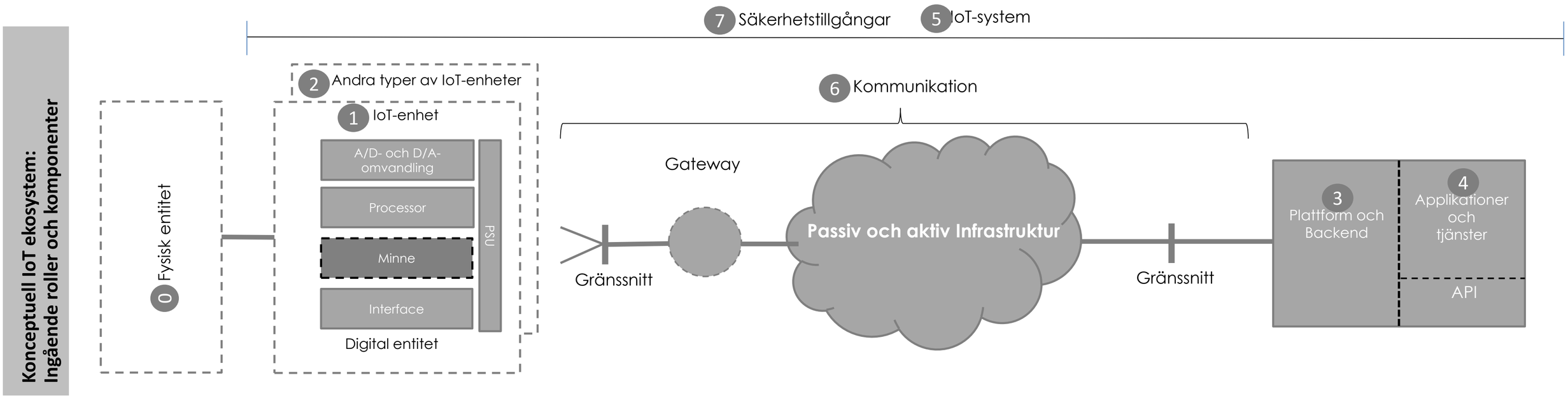
TLP:WHITE

Sju roller inom IoT-systemet

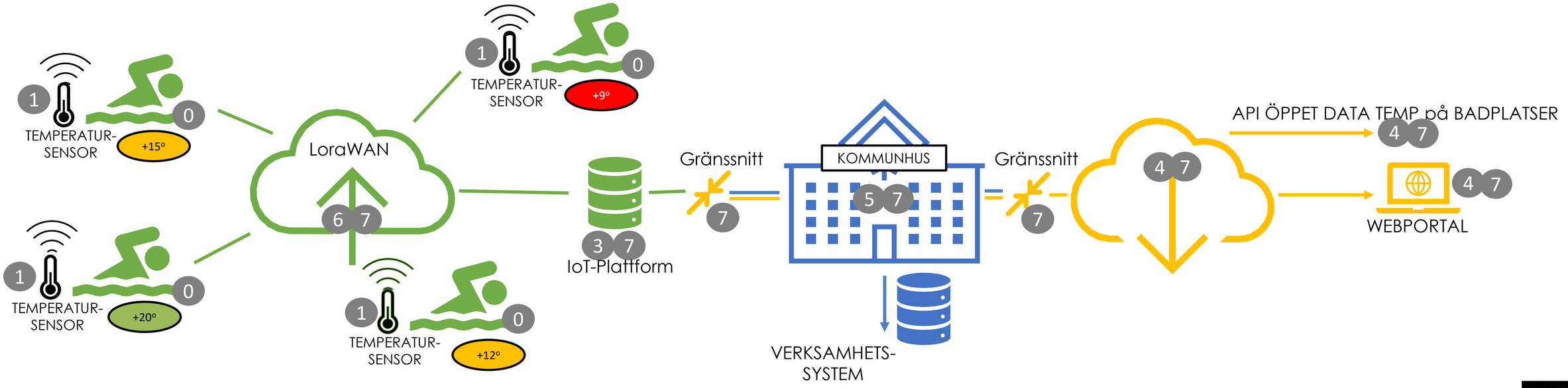
Robust & Säker IoT

	Roller	Beskrivning
1	R1	**R1 – Roller för IoT enheter**
	R1.1	*Utvecklar och tillverkar IoT-enheter*
	R1.2	*Levererar IoT enheter*
2	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*
3	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*
4	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*
5	R5	**R5 – Roller för IoT- system**
	R5.1	*1. Utvecklar (t.ex. design, arkitektur, integration, konfiguration) . Levererar IoT-system*
	R5.2	*2. Systemägare*
6	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*
7	R7	**R7 – Roller för Säkerhetstillgångar**
	R7.1	*Utvecklar och tillverkar säkerhetstillgångar*
	R7.2	*Levererar säkerhetstillgångar*

TLP:WHITE

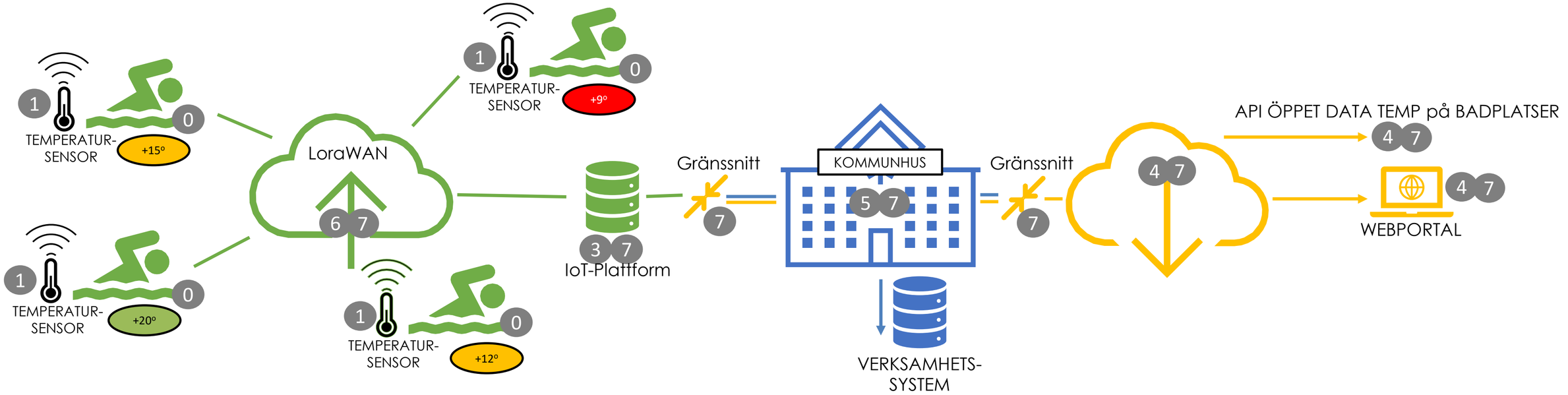


Realiserad IoT: **BADTJÄNST 1**



TLP:WHITE

Realiserad IoT: **BADTJÄNST 1**



Kommunen köper mätning av badtempereratur som tjänst av stadsnätet/LoraWAN-operatör

Kommunen är systemägare men innehar inget eget IoT-system.

Visualisering av data sker via portal som leverantör ombesörjer men integreras med kommunens hemsida och internetaccess.

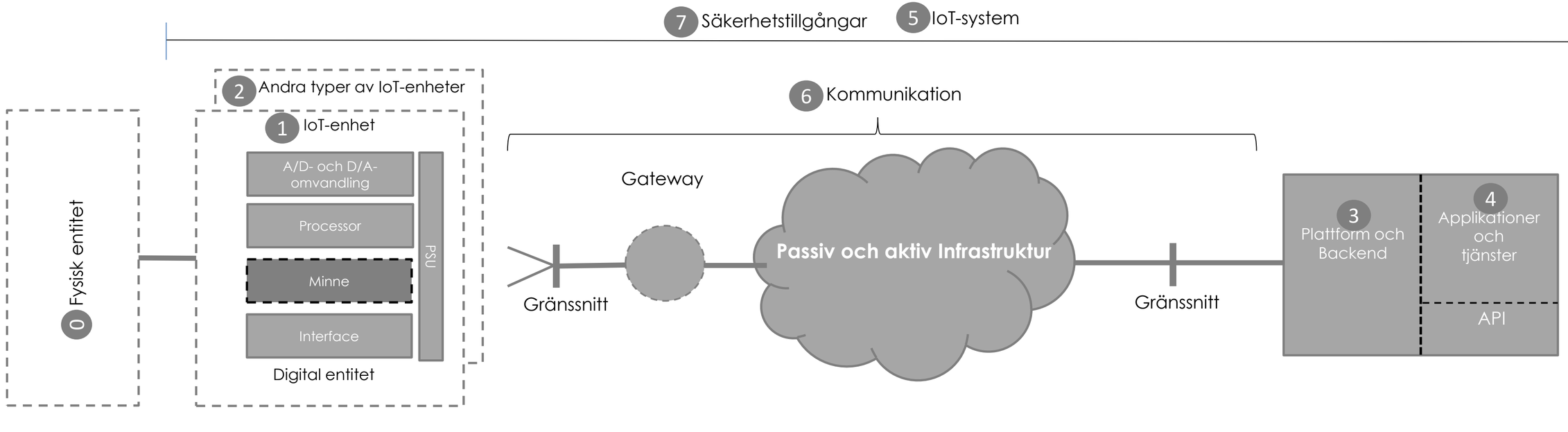
Leverantören levererar data via portal samt som öppet data via API. Allt kanaliseras via kommens ordinarie internet och gränssnitt.

Färger på illustrationer representerar var i purdue-arkitekturen som de tillhör.

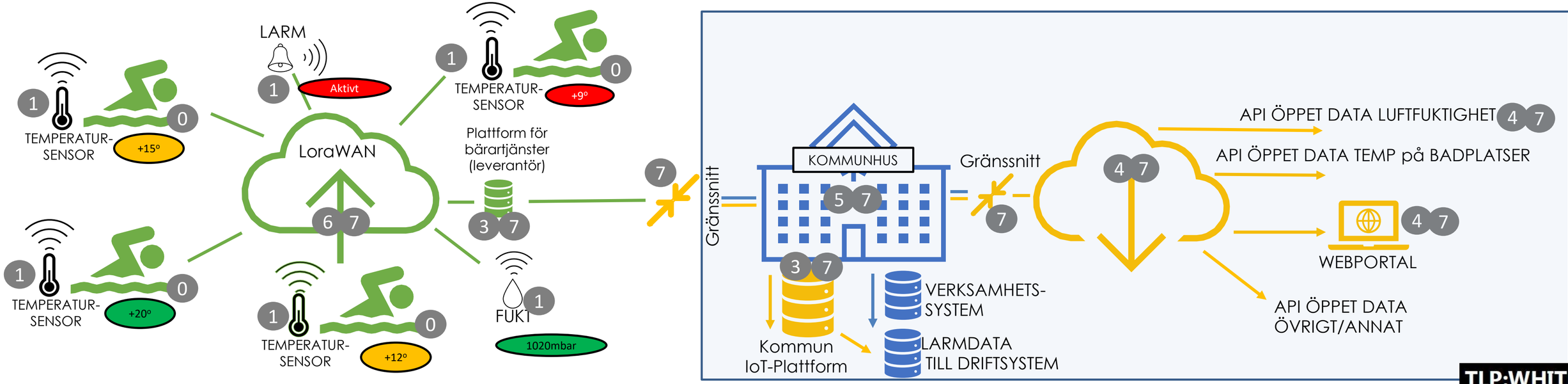
De gråa cirklarna med nummer beskriver vilken roll som illustrationen representerar

TLP:WHITE

Konceptuell IoT ekosystem: Ingående roller och komponenter

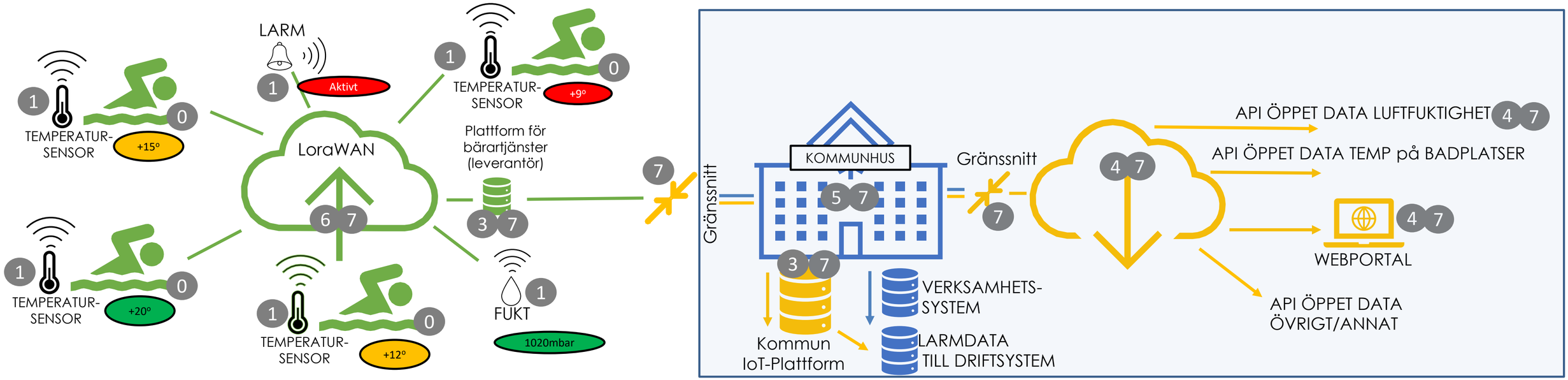


Realiserad IoT: **Transport av mätvärden**



TLP:WHITE

Realiserad IoT: **Transport av mätvärden**



Kommunen köper själv in sensorer och kan aktivera via leverantören av transports IoT-system

Kommunen är systemägare innehar ett eget IoT-system.

Kommunen köper transport av data och hanterar data i eget IoT-system.

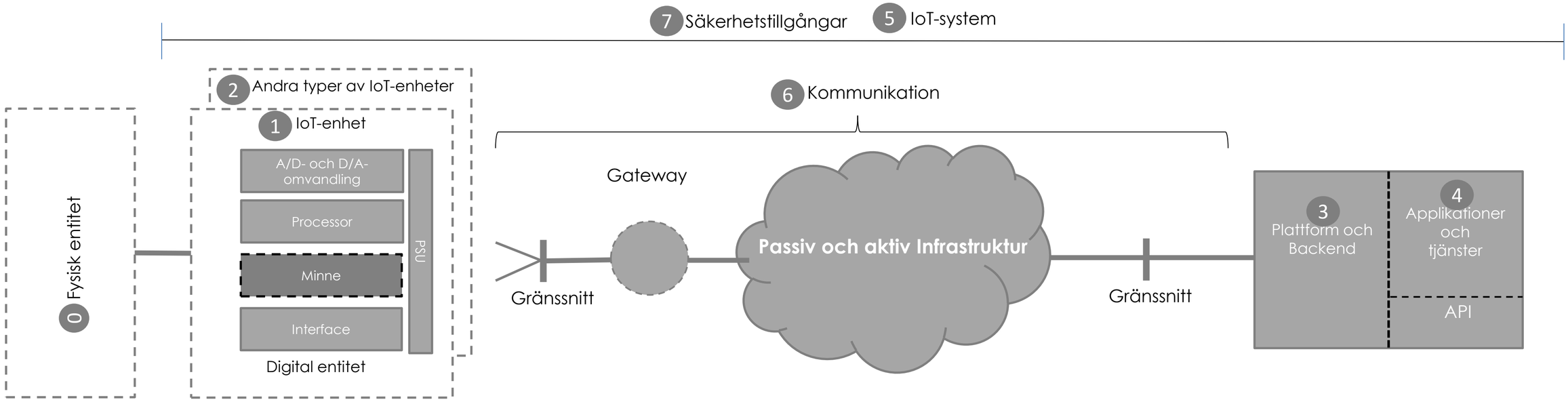
Bearbetning och visualisering via portaler och API sker i kommunens försorg.

Färger på illustrationer representerar var i purdue-arkitekturen som de tillhör.

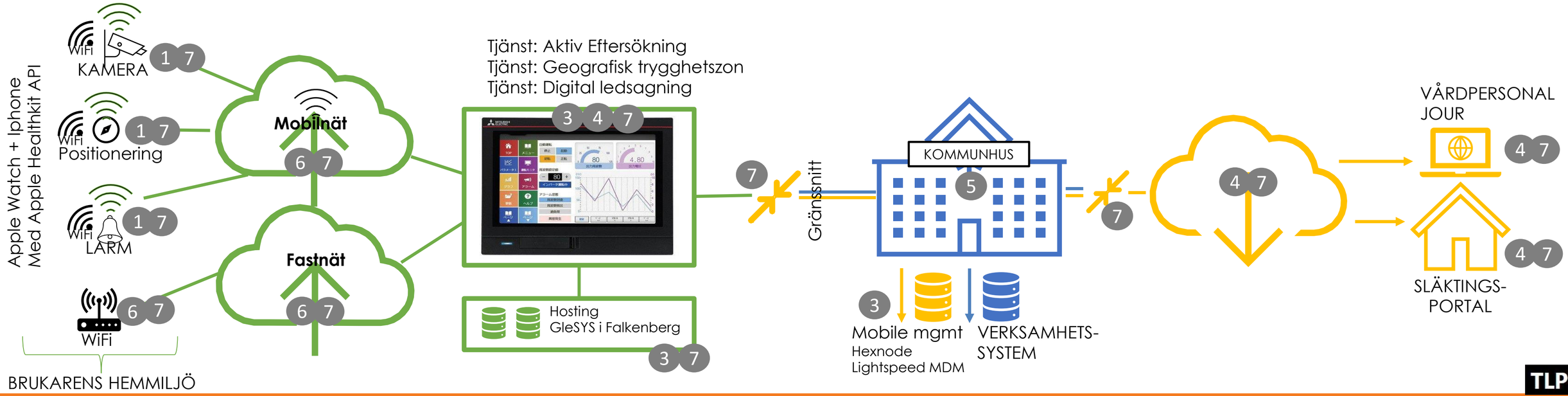
De gråa cirklarna med nummer beskriver vilken roll som illustrationen representerar

TLP:WHITE

Konceptuell IoT ekosystem: Ingående roller och komponenter

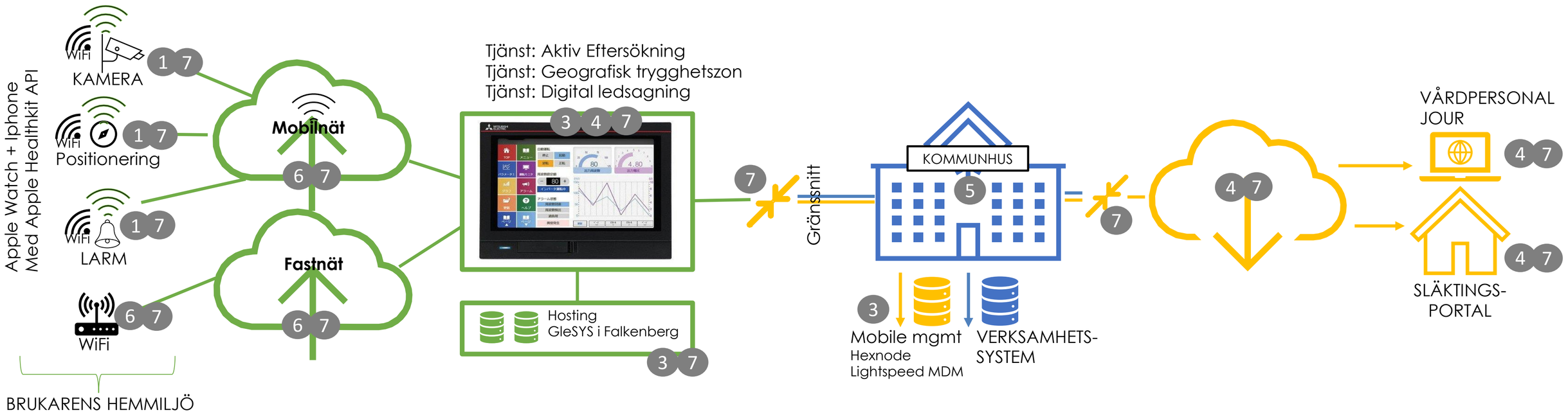


Realiserad IoT: **Stödvård i hemmet**



TLP:WHITE

Realiserad IoT: **Stödvård i hemmet**



Kommunen köper färdiga tjänster och sensorer är vanliga konsumentbaserade wearables.

Kommunen styr rättigheter till wearables, data och användare med inköpt program.

”Brukaren” övervakas och larm går till släktingar samt vård-personal där släktingar är prio. 1.

Kommunen är systemägare över tjänstekonceptet och innehar inget eget IoT-system.

Färger på illustrationer representerar var i purdue-arkitekturen som de tillhör.

De gråa cirklarna med nummer beskriver vilken roll som illustrationen representerar

TLP:WHITE

Tack så mycket för att du lyssnat. Frågor?

Jimmy Persson
Utveckling- och Säkerhetschef
Jimmy.persson@ssnf.org
08-214 640

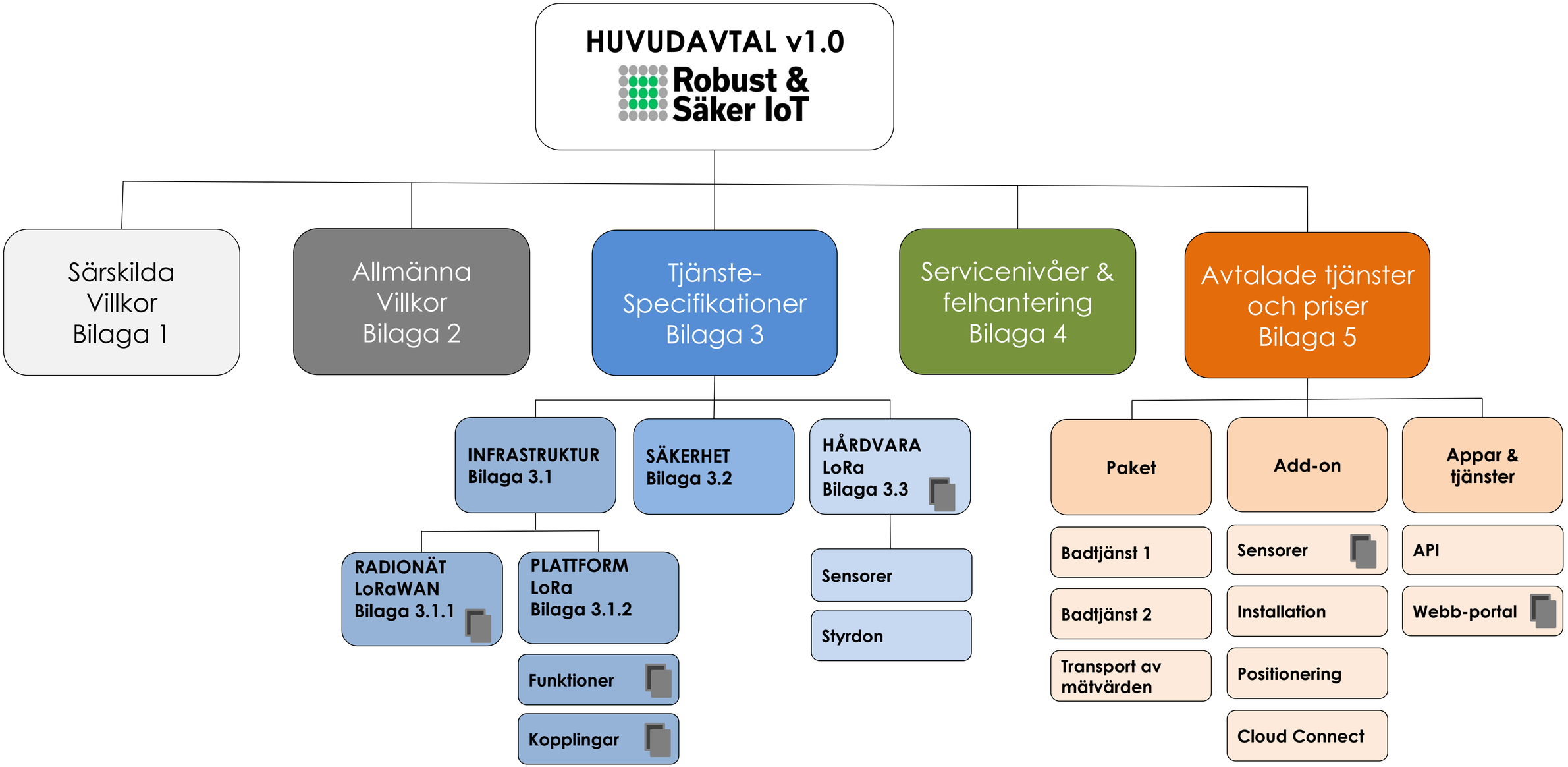
TLP:WHITE

Viktiga avtalsaspekter

Avtal Robust & säker IoT version 1.0

2021-03-10

Robert Wälikangas
Branschjurist
Robert.walikangas@ssnf.org
08-214 420


HUVUDAVTAL v1.0
Robust & Säker IoT
Särskilda Villkor Bilaga 1
Allmänna Villkor Bilaga 2
Tjänste-Specifikationer Bilaga 3
Servicenivåer & felhantering Bilaga 4
Avtalade tjänster och priser Bilaga 5
INFRASTRUKTUR Bilaga 3.1
SÄKERHET Bilaga 3.2
HÅRDVARA LoRa Bilaga 3.3
RADIONÄT LoRaWAN Bilaga 3.1.1
PLATTFORM LoRa Bilaga 3.1.2
Funktioner
Kopplingar
Sensorer
Styrdon
Paket
Add-on
Appar & tjänster
Badtjänst 1
Badtjänst 2
Transport av mätvärden
Sensorer
Installation
Positionering
Cloud Connect
API
Webb-portal

HUVUDAVTAL v1.0

Robust & Säker IoT

Innehåll

Allmänna Villkor Bilaga 2

Robust & Säker IoT

Innehåll

HUVUDAVTAL v1.0

Robust & Säker IoT

De till avtalet tillhörande Allmänna villkoren i bilaga 2 har tagits fram av Stadsnätsföreningen och kan över tid behöva ändras till följd av ändringar i lagstiftning eller myndighetsföreskrifter, vilka publiceras på Stadsnätsföreningens hemsida. För att dessa ändrade allmänna villkor ska bli gällande och tillämpas mellan parterna ska detta särskilt överenskommas genom att det anges i Särskilda villkor bilaga 1 att "*Allmänna villkor daterade xx xx xx, gäller mellan parterna för ingångna och framtida avtal*" eller motsvarande skrivning.

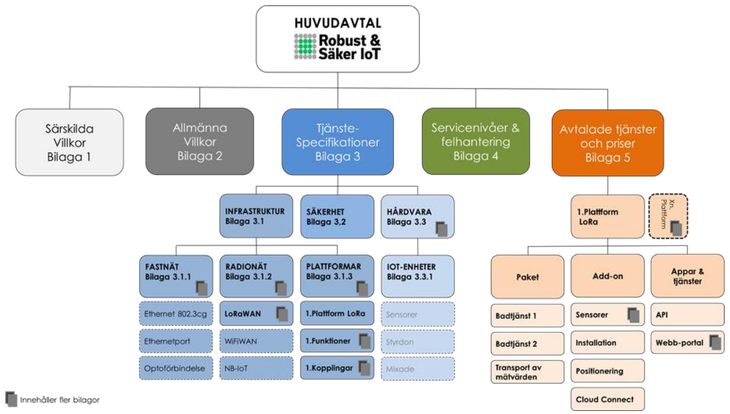
Allmänna Villkor Bilaga 2

Särskilda Villkor Bilaga 1

HUVUDAVTAL v1.0

Robust & Säker IoT

Om parterna själva initierar att göra ändringar i någon av bilagorna så anges ändringen i Särskilda villkor bilaga 1 med angivande av datum från vilken dag ändringen eller den nya bilagan ska gälla ifrån.



Särskilda Villkor Bilaga 1

Allmänna
Villkor
Bilaga 2

Robust &
Säker IoT

4.3 Ansvarsfördelning

Parternas ansvarsfördelning utöver Säkerhetsarbetet i 4.2 sker i tillämpliga delar beroende på avtalad IoT tjänst i bilaga 5, vilka anges nedan i 4.3.1 – 4.3.5 om inte annat skriftligen överenskommits.

Allmänna
Villkor
Bilaga 2

Robust &
Säker IoT

4.4 Personuppgiftsbehandling

Köparen är personuppgiftsansvarig för de eventuella personuppgifter som behandlas i någon del av den avtalade IoT tjänsten. Köparen ansvarar att lagstiftning, såsom dataskyddsförordningen, efterlevs till följd av personuppgiftsbehandlingen. Om inte annat särskilt avtalats mellan parterna ska Köparen således lämna de registrerade erforderlig information och tillse att behandlingen av personuppgifterna vid var tid har laglig grund, exempelvis genom ett uttryckligt samtycke från de registrerade. I de fall IoT-tjänstens tillhandahållande innebär att Säljaren ska behandla personuppgifter för Köparens räkning ska ett erforderligt personuppgiftsbiträdesavtal upprättas. Säljaren har i ett sådant fall rätt till utökad ersättning för att följa tekniska och organisatoriska åtgärder samt Köparens övriga instruktioner till följd av personuppgiftsbiträdesavtalet.

Frågor och reflektioner