

Regelverk för säker datadelning inom EHDS, NDI

Niklas Dahlbäck, Johan Eltes

2026-10-01



**Denna presentation innehåller delvis tidiga
hypoteser och ska anses vara arbetsmaterial
som underlag för diskussion**

Agenda

- Syfte
- Översikt av ramverket
- Verksamhetsnivån – Behörig tillgång
- Applikationsnivån – Tjänsteleverans
- Teknisk nivå – Säkerhetslösning
- Diskussion – att tänka på inför remiss

Inledning



Syftet med mötet

- Presentera förslag på regelverk för säker datadelning inom EHDS, NDI
- Får era reflektioner på om regelverket är ändamålsenligt och proportionerligt
- Få råd inför remissrundan



Kort om NDI och EHDS

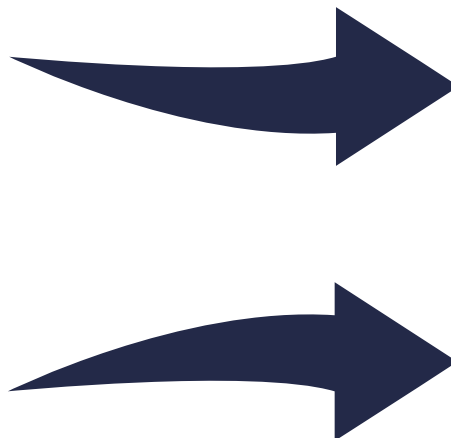
Drivkrafter nationellt och internationellt

Nationellt

Regeringens mål är att hälsodata ska finnas tillgängliga i hela vårdkedjan, oavsett var patienten får vård.

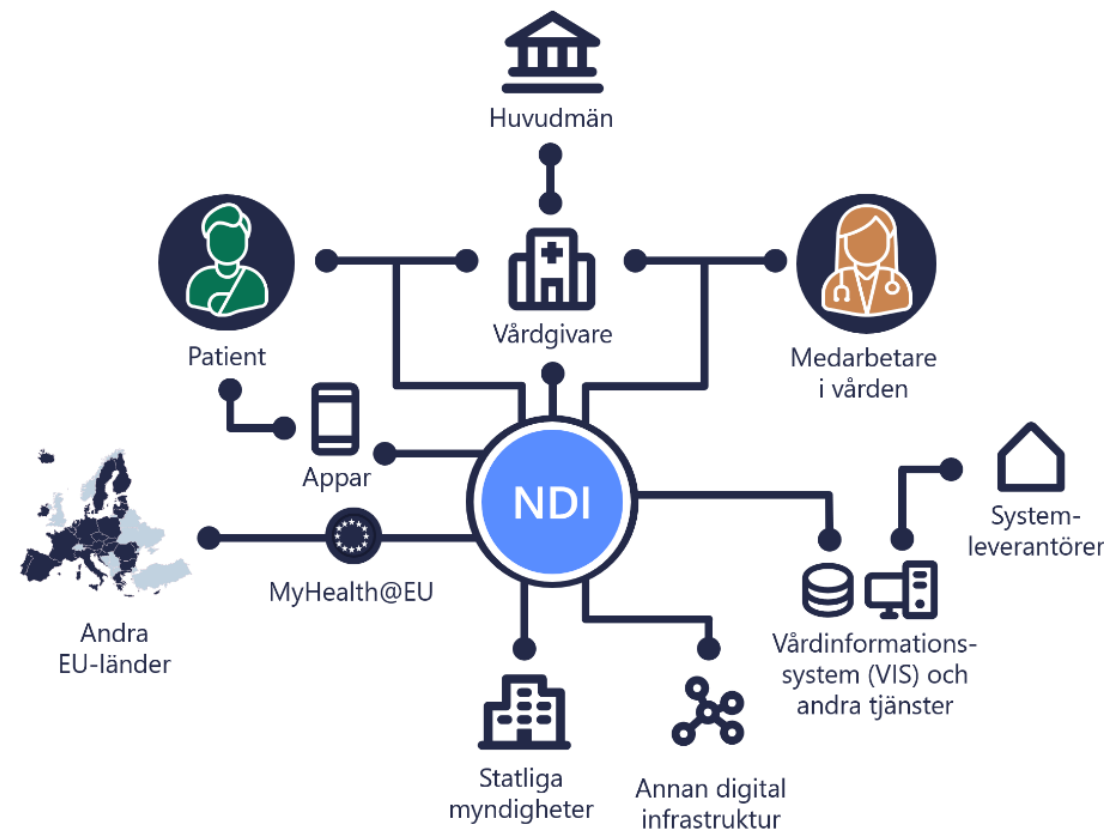
Internationellt

EU:s förordning om det europeiska hälsodataområdet (EHDS) kräver att medlemsstaterna säkerställer delning av hälsodata.



Det europeiska hälsodataområdet (EHDS) och en nationell digital infrastruktur

- För att möta kraven i förordningen behöver Sverige en säker och fungerande nationell digital infrastruktur som gör det möjligt att dela hälsodata mellan olika system och aktörer inom vården.
- Målet är att data ska vara öppna och tillgängliga för alla som har rätt att ta del av data.
- För det behövs flera tekniska lösningar och funktioner, exempelvis för att möjliggöra identifiering av var hälsodata finns och hur det kan hämtas.
- Det kräver också kontroll av behörighet, åtkomst och spårbarhet och att hälsodata lagras i standardiserade format.



An abstract graphic consisting of a network of interconnected nodes and lines, resembling a molecular structure or a complex web. The nodes are represented by small circles, and the lines are thin, light blue. The overall shape is irregular and spans the width of the slide.

Översikt av regelverket

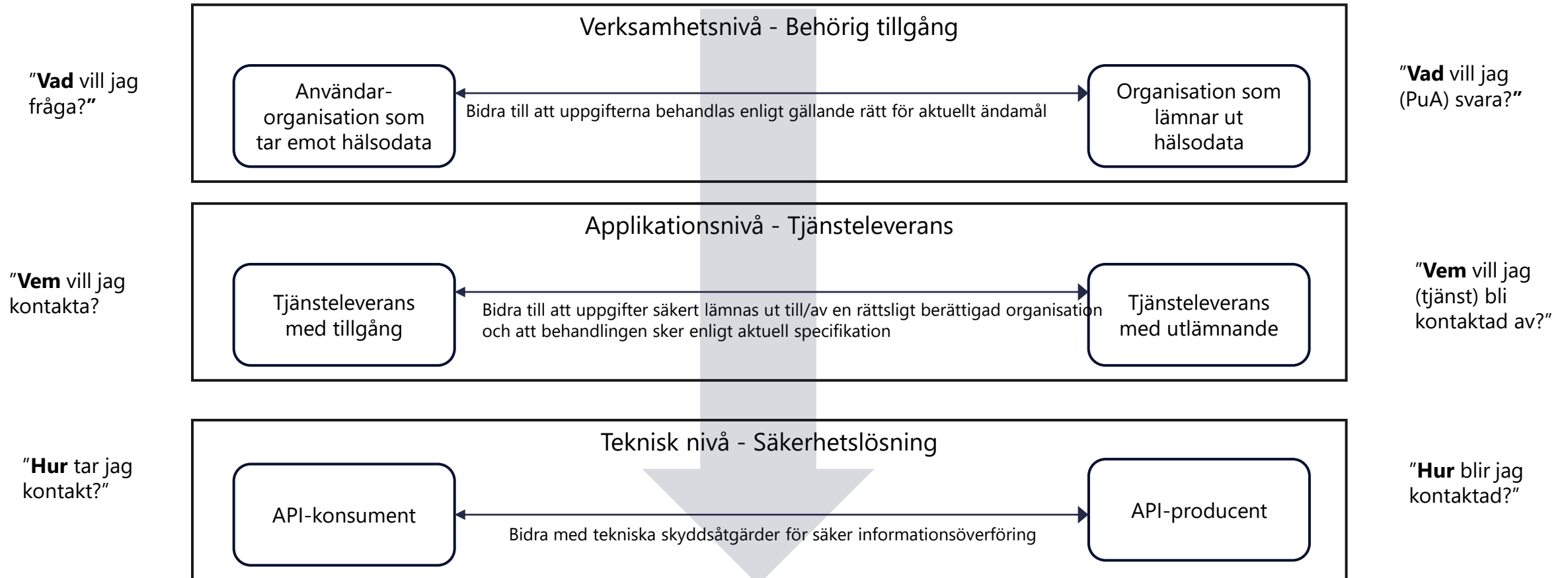
Nya omständigheter som kan öka risken för obehörig tillgång

- Utan vårdavtal med regioner eller kommuner ökar risken för obehörig tillgång
 - Ingen risk att förlora ett avtal, ingen styrning och stöd via medlemskap i HSA-federationen, kanske inte ens är verklig vårdgivare
 - Undantag: Tandvården har infört tillståndsplikt
- I bolag med mycket få anställda minskar eller uteblir effekten av åtkomstkontroll och behörighetstilldelning
- Att vårdgivare i utlandet får teknisk tillgång till svenska hälsodata med personuppgifter kan leda till ökad opt-out med risk för försämrad patientsäkerhet som följd
- Effekten av tillsynsverksamhet minskar när antalet vårdgivare med möjlighet till tillgång ökar utan kraftig resursförstärkning hos tillsynsverksamheten

Det ska kännas tryggt att lämna ut hälsodata med personuppgifter för direktåtkomst



Regelverkets uppbyggnad

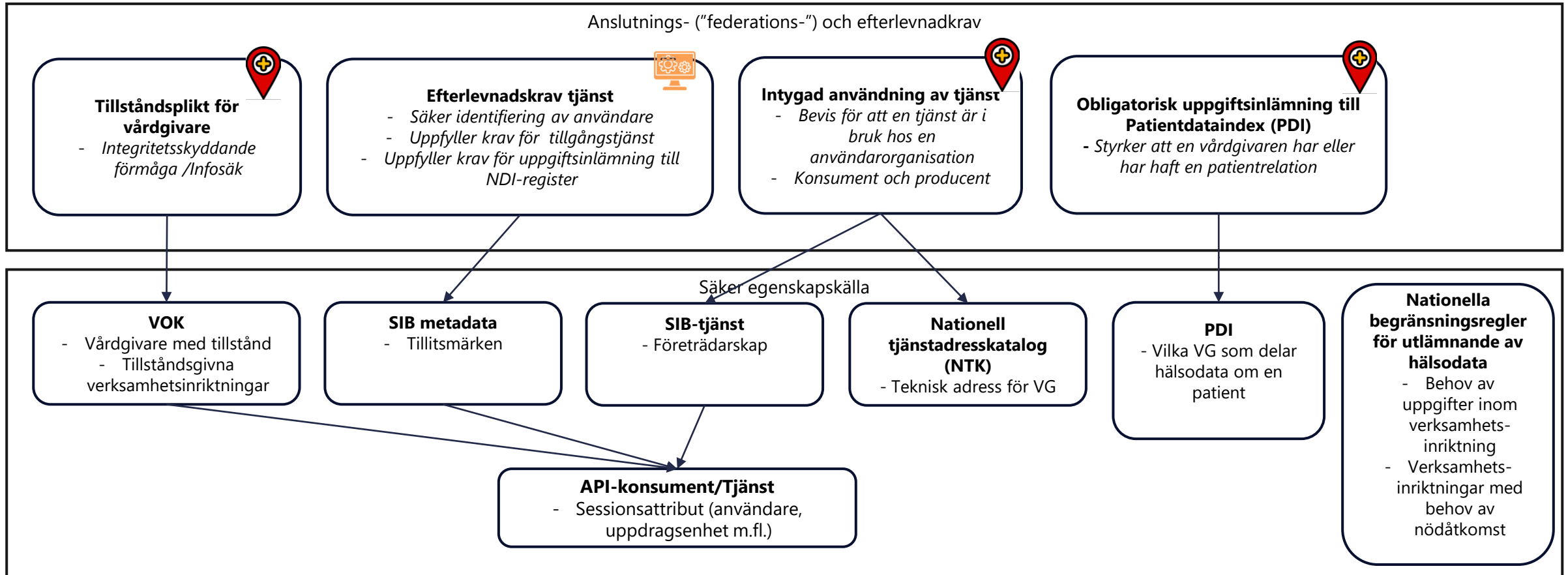


E-hälsomyndigheten har som mål att tillämpa ramverket för all interoperabilitet inom sitt ansvar

Regelverkets innehåll

Primära parter	Sekundära parter	Nivå	Exempel på åtgärder
- Personuppgiftsansvariga organisationer - E-hälsomyndigheten - Vårdgivare (inkl apotek) - Myndigheter med föreskriftsrätt - Ev. E-hälsomyndigheten - Ev. Socialstyrelsen	- Patienten - genom EHDS-rättigheter till loggåtkomst, spär och opt-out - Statliga utredningar relaterade till SVOD, NDI, PDL, NLL m.fl	Verksamhetsnivå - Behörig tillgång Användarorganisation som tar emot hälsodata Bidra till att uppgifterna behandlas enligt gällande rätt för aktuellt ändamål Organisation som lämnar ut hälsodata	- Tillståndsplikt för vårdgivare - Lagstadgad tillsyn - Nationella behörighetsregelverk - Patientens åtkomst till loggar - Tillgänglig patient
- Tjänsteleverantörer (tillhandahållare av systemkomponenter i drift) - SaaS-leverantörer i biträdesroll - Integrationsbiträden - Regioner och kommuner som tjänsteleverantörer till sig själva och i biträdesroll till upphandlade vårdgivare	- Tillverkare av systemkomponenter - Användarorganisationer - Vårdgivare och apoteksaktörer - Förvaltare av svenska api-specifikationer - EHM - Interoprådet - Svenska HL7/IHE	Applikationsnivå - Tjänsteleverans Tjänsteleverans med tillgång Bidra till att uppgifter säkert lämnas ut till/av en rättsligt berättigad organisation och att behandlingen sker enligt aktuell specifikation Tjänsteleverans med utlämnande	- Funktionsgodkännanden och produktmärkning - Tillitsmärkning - Medlemsskap i Ena SIB - Ena företräderskap - Åtkomstpolicy - Attributkrav
- Interoperabla systemkomponenter i drift - API-klienter - API-servrar (ändpunkter) - Auktorisationstjänster - Metadatatjänster	- Fysisk infrastruktur - Nät - Servrar	Teknisk nivå - Säkerhetslösning API-konsument Bidra med tekniska skyddsåtgärder för säker informationsöverföring API-producent	Förmåga att begränsa åtkomst utgående från policyer

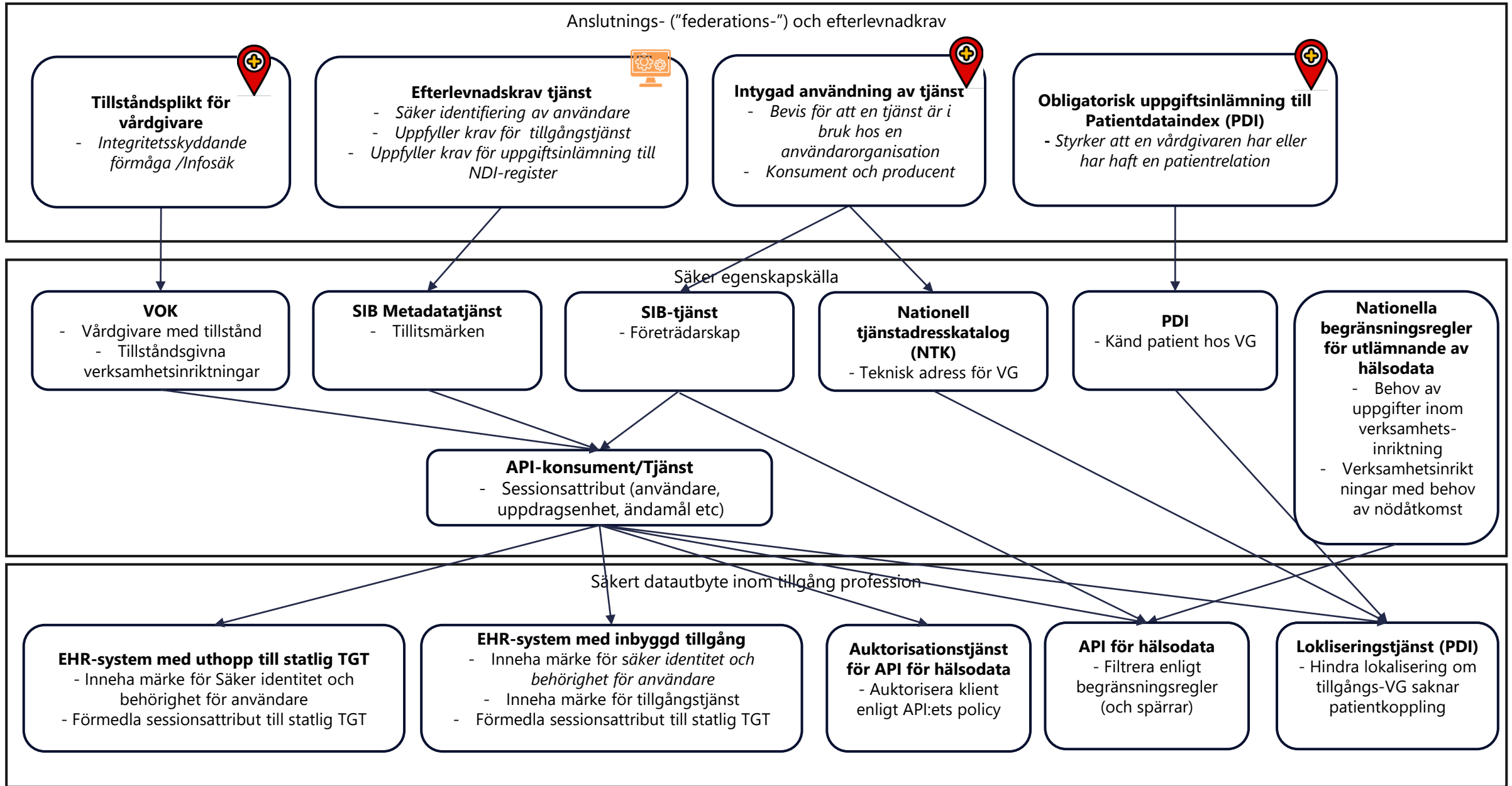
Tillitskedja för säkert datautbyte



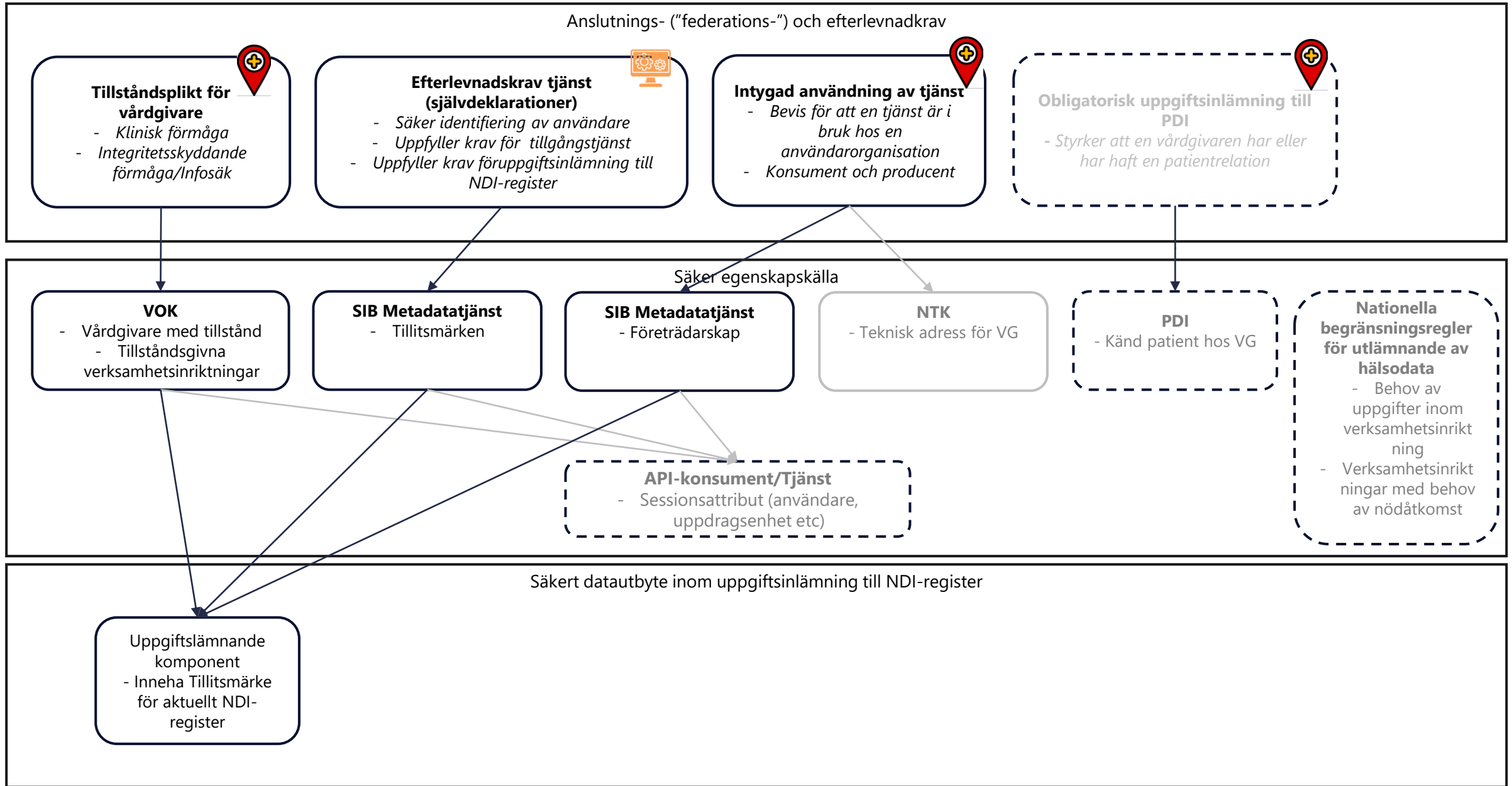
Förutsätter säker provisionering från ansvariga myndigheter

- Provisionering av uppgifter om utfärdade tillstånd inom tillståndsplikten från ansvarig myndighet till EHM/VOK
- Säker källa för nationella begränsningsregler (Socialstyrelsen? Kodverksserver?)

Tillitskedja för säkert datautbyte – Direktåtkomst profession



Tillitskedja för säkert datautbyte – Uppgiftsinlämning till NDI-register





Verksamhetsnivån – Behörig tillgång

Åtgärder för att minska risken att användare hos vårdgivare får obehörig tillgång vid direktåtkomst

Verksamhetsnivån – Behörig tillgång

- Vad är menar vi med obehörig tillgång?
- Åtgärder med proportionalitetsbedömning
- Detaljer om åtgärder (om vi hinner)

Exempel på obehörig tillgång

- *Fel organisation*: att organisationen vars medarbetare får tillgång inte är en vårdgivare och därmed saknar rättsligt stöd för tillgång
- *Fel patient*: att en medarbetare (användare) hos en tillgångsvårdgivare får tillgång till hälsodata från andra vårdgivare trots att patientrelation saknas
- *Fel uppgifter*: att en medarbetare får tillgång till hälsodata med personuppgifter om sin patient, men som inte är nödvändiga för den vård som ges

Åtgärder med proportionalitetsanalys (utdrag)

Åtgärder	Värdering/proportionalitet Kvot Effekt/ snittkonsekvens	Reaktiv /Proaktiv åtgärd	Verkan absolut/ uppföljning	Konsekvens för statliga myndigheter	Konsekvens vårdgivare 1-4	Konsekvens för tillverkare 1-4	Negativa konsekvenser patientsäkerhet 1-4	Effekt på obehörig tillgång 1-4	Kommentar
Patienten som granskare	3/1,0 = 3,0	R	Uppföljning	3	-	-	1	3	kan förstärkas genom notifiering som uppmärksammar nödåtkomst till spärrade uppgifter
Införa tillståndsplikt för vårdgivare	(4/1,6 = 2,5) 4,0 eftersom åtgärden är en förutsättning för regelverkets effekter.	P	Absolut/teknisk	3	1	-	-	4	- Flera andra åtgärder beror av att detta görs. Det återspeglas i värderingen. - Bör också omfatta krav på ledningssystem för informationssäkerhet och rutiner för tilldelning av behörigheter
Ökad tillsyn av vårdgivare hos IMY	2/1,4 = 1,4	R	Uppföljning	4	1	-	-	2	Inom ramen för IMYs befintliga uppdrag
Begränsning av möjligheten av nödåtkomst till spärrade uppgifter baserat på verksamhetsinriktning (absolut teknisk begränsning)	3/1,2 = 2,5	P	Absolut/teknisk	2	1	1	1	3	
Avtalsstyrning	-	P	Deklaration +	-	-	-	-	-	Effekten avser

Riskbegränsande åtgärder för svenska vårdgivares brister i begränsning av vårdpersonalens tillgång

Åtgärd	Förutsätter	Implementerar lösning	Påverkas av åtgärden	Koncept	Minskar risk för fel...
Generell begränsning av vad som lämnas ut till vem	Föreskrift	VIS hos Utlämnande part (frivilligt?)	Vårdgivares användare av tillgångstjänster	Sambandet mellan behov och uppgifters ursprung uttrycks genom verksamhetsinriktning	...uppgifter
Generell begränsning av tillgång till spärrade uppgifter	Föreskrift	VIS hos Utlämnande part (obligatoriskt)	Vårdgivares användare av tillgångstjänster	Verksamhetsinriktning definierar behovet av att åberopa nödsituation vid tillgång	...uppgifter
Förstärk patienten påverkan vid tillgång till uppgifter om tillgång	Funktion i statlig tillgångstjänst och nationella rutiner	EHM, vårdgivare	Vårdgivare som patienten befarar haft obehörig tillgång	Funktion i tillgångstjänst för patient som underlättar att identifiera, rapportera och följa upp uppgifter om tillgång	...patient ...uppgifter
Ökade resurser för tillsyn	Resurser	Tillsynsmyndighet	Vårdgivare	Större resurser	...patient ...uppgifter
Myndighet får ansvar för åtkomstkontroll hos små vårdgivare (?)	Rättsligt stöd	Bef. eller ny myndighet	Vårdgivare	Är detta möjligt pga behovet av sekretessbrytande bestämmelser?	...patient ...uppgifter
Tillgång begränsas till vårdgivarens patienter	Rättsligt stöd	EHM. Funktion i lösning för register över vårdgivares patienter (PDI)	Vårdgivares användare av tillgångstjänster	PDI begränsar vårdgivarens möjligheten till lokalisering av patienters hälsodata till de patienter vårdgivaren rapporterat till PDI	...patient

Riskbegränsande åtgärder för utländska vårdgivares brister i begränsning av vårdpersonalens tillgång

Åtgärd	Förutsätter	Implementerar lösning	Påverkas av åtgärden	Koncept	Minskar risk för fel...
Bevis för patientrelation vid tillgång från utlandet	Reglering? Uppdrag?	EHM (NCP och app för att patienten ska kunna generera ett tillfälligt bevis på patientrelation)	Utländska vårdgivares tillgång, svenska patienter i utlandet (måste generera kod som bevis)	Sverige går på Österrikes och Portugals lösning: att patienten måste generera en kod som vårdpersonalen matar in vid tillgång till svenska hälsodata via NCP. NCP verifierar.	...patient
Möjlighet att spärra uppgifter för tillgång från utländska vårdgivare	Föreskrift/ Reglering kring spärrar		Vårdgivares VIS alternativt EHM NCP om funktionen kan isoleras dit	Koncept från bankvärldens "regionöppning/stängning"	...patient ...uppgifter

Riskbegränsande åtgärder för brister i integritetsskydd och behörighetstilldelning hos svenska vårdgivare med tillgång

Åtgärd	Förutsätter	Implementerar lösning	Påverkas av åtgärden	Koncept	Minskar risk för fel...
Införa tillståndsplikt för vårdgivare	Statligt verksamhet	VIS hos Utlämnande part (frivilligt). VOK hos EHM	Vårdgivare	Tillståndsplikt omfattar informationssäkerhetsarbete och där tillståndet är begränsat utifrån kodverk för verksamhetsinriktning	...vårdgivare ...patient ...uppgifter
Obligatorisk mall för behovs- och riskanalys	Rättsligt stöd	Ej teknisk lösning	Vårdgivare som ska ansluta till NDI	En obligatorisk mall skapar grund för rationell och effektiv följsamhet av föreskrifter och lagar inom området-	...patient ...uppgifter
Självdeklaration avseende följsamhet till gällande rätt (inkl föreskrift 2016:40) för anslutning till NDI	Rättsligt stöd och tillämpning inom anslutning till NDI.	Ej teknisk lösning	Vårdgivare som patienten befarar haft obehörig tillgång	Att det ska motsvara kraven för tillståndsplikt, i väntan på att sådan införs.	(...vårdgivare) ...patient ...uppgifter

Vilka krav påför åtgärderna svenska vårdgivare?

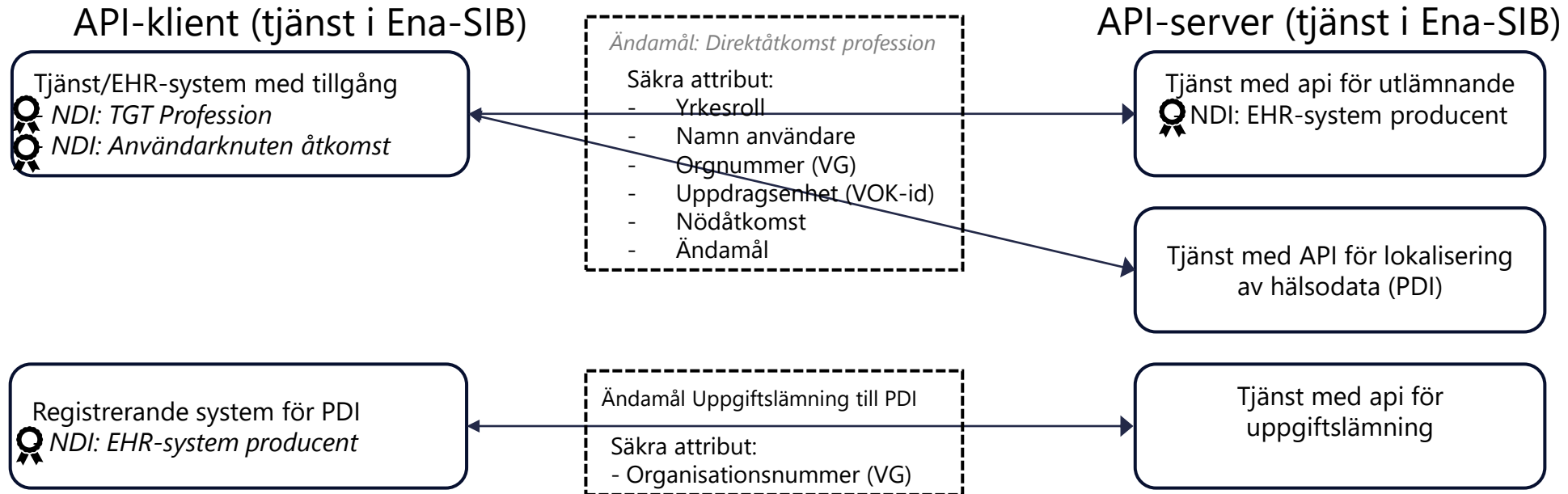
- Erhålla och upprätthålla tillstånd att verka som vårdgivare
- Delta i de rutiner/processer E-hälsomyndigheten inrättar för hantering av det patienten rapporter genom statlig TGT vid upplevd obehörig tillgång
- Använda EHR-system som i producentroll kan...
 - ...filtrera hälsodata på verksamhetsinriktning hos enheten där den dokumenterades (inriktning kan ju ändras över tid...)
 - ...avgöra om spärrade uppgifter ska lämnas ut, baserat på verksamhetsinriktningar för den vårdenhet som står bakom begäran om direktåtkomst
- Använda EHR-system som i konsument kan...
 - (inga - verksamhetsnivåns åtgärder är transparent för tillgångsfunktioner i EHR-system)

An abstract graphic consisting of a network of nodes (dots) connected by thin lines, forming a complex, web-like structure. The nodes are distributed across the entire page, with a higher density in the upper right and lower right areas. One node, located in the upper right quadrant, is highlighted in blue.

Applikationsnivån – Tjänsteleverans

Mönster, märken och ändamål - exempel

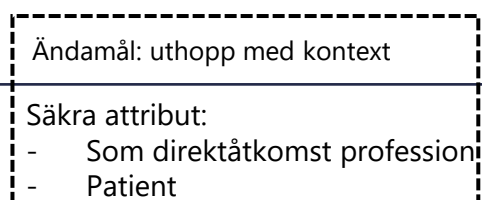
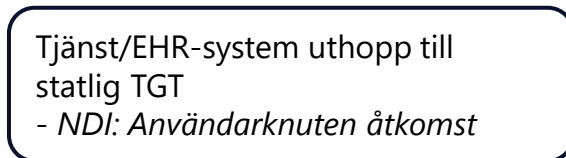
Mönster: Auktorisation genom systemets identitet



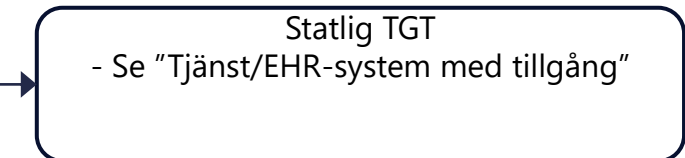
Mönster: Auktorisation genom användarens identitet (uthopp med SMART EHR-launch)

TIDIG HYPOTES
under analys

Session med öppen journal



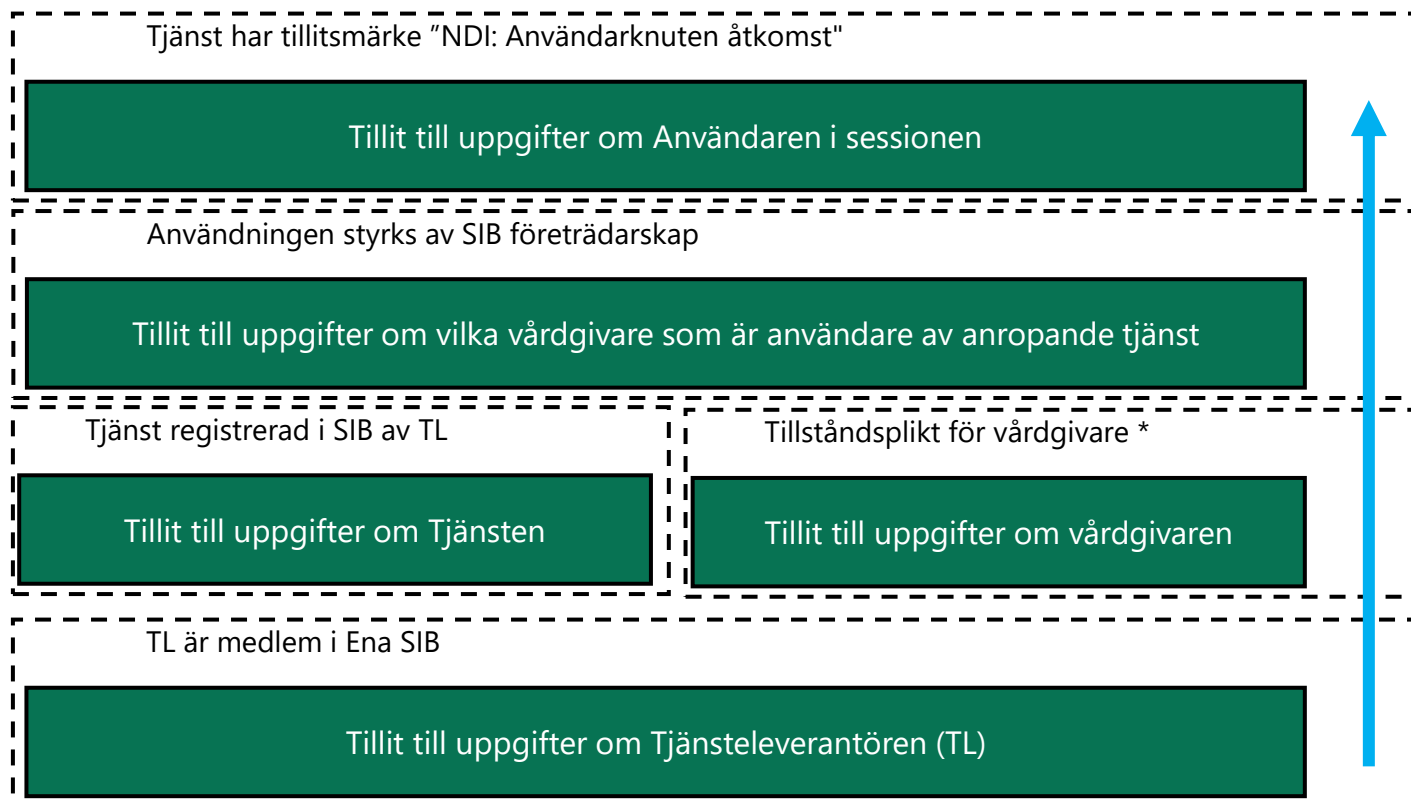
SMART-app inom session



Tillitsstegen

**Säker datadelning
inom NDI, EHDS**

Steg för tillit till de attribut som API-klient kan förmedla till API-server vid begäran om auktorisation



API-servern behöver också kunna verifiera att API-konsumenten uppfyller krav som är specifika för det API som anropas. Det sker genom ändamålsspecifika tillitsmärken.

Ett enskilt API kan betjäna flera ändamål. Därför är ändamålet i sig också ett attribut som API-klienten förmedlar vid begäran om auktorisation.

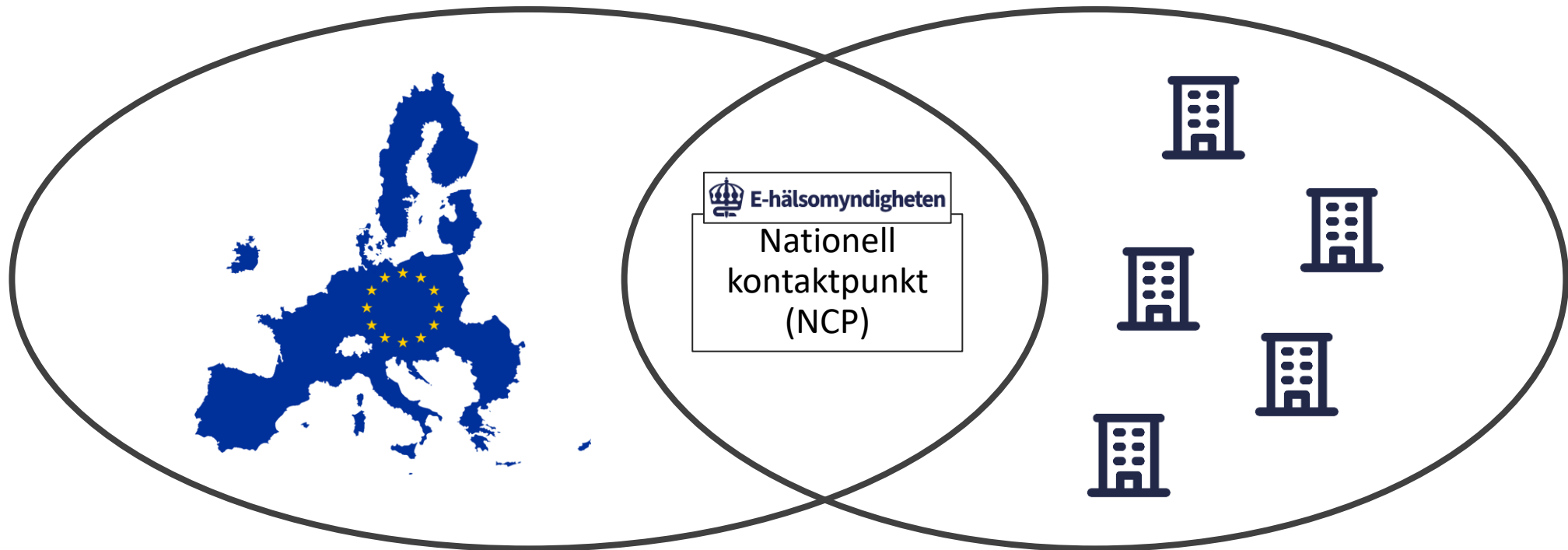
API-servern verifierar att API-klienten (tjänsten) har de tillitsmärken som krävs för det ändamål som anges i auktorisationsbegäran.

** För uppgiftsinlämning till EHMs register inför 2029-03 (från och med 2027-07) är tillståndsplikten inte nödvändig, eftersom integritetsriskerna främst uppstår i samband med tillgång*

Hur fungerar tillit för gränsöverskridande datadelning inom EHDS?

Circle of trust – tillit mellan
medlemsstater genom gemensamma
regler och kontroller

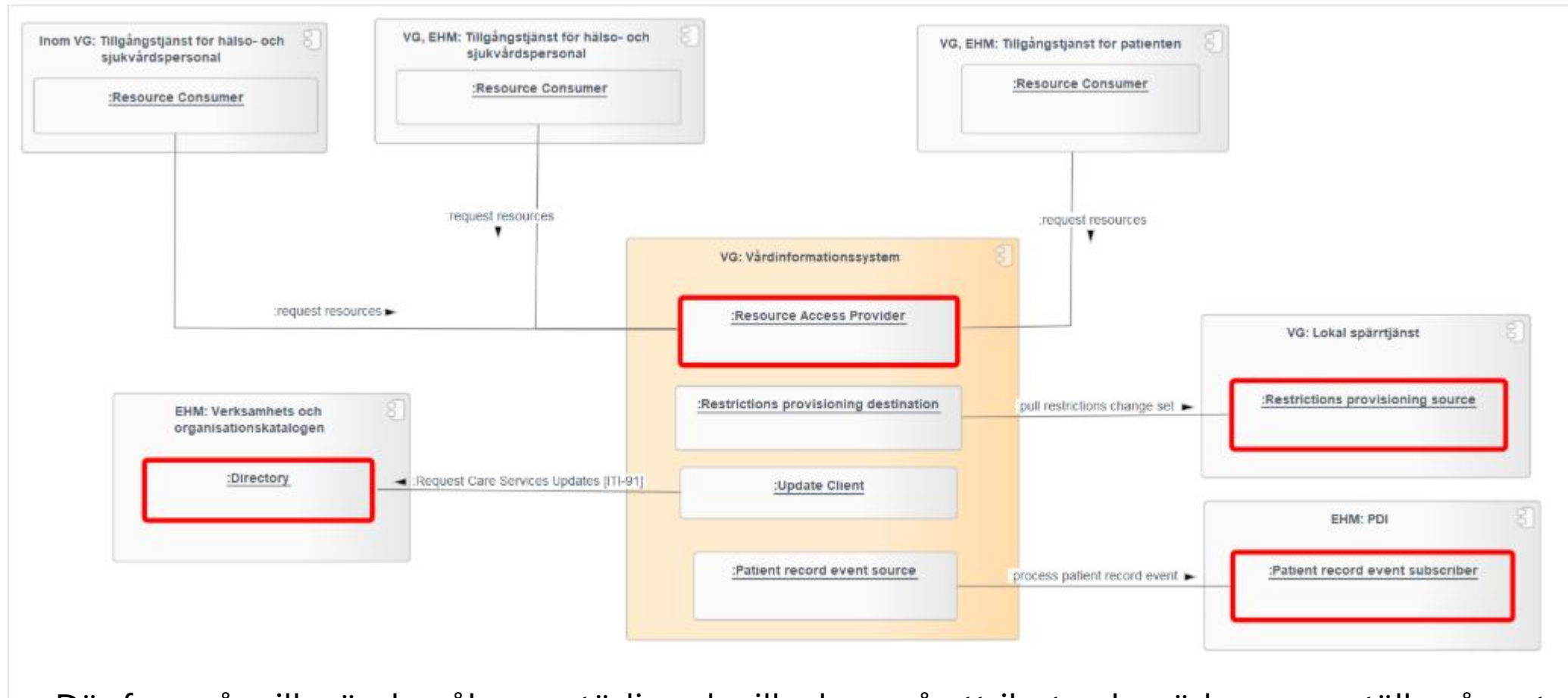
Regelverk för säker datadelning inom
EHDS, NDI med Samordnad identitet och
behörighet



An abstract graphic consisting of a network of nodes (dots) connected by thin lines, forming a complex, web-like structure. The nodes are distributed across the slide, with a higher density on the right side. One node is highlighted in blue.

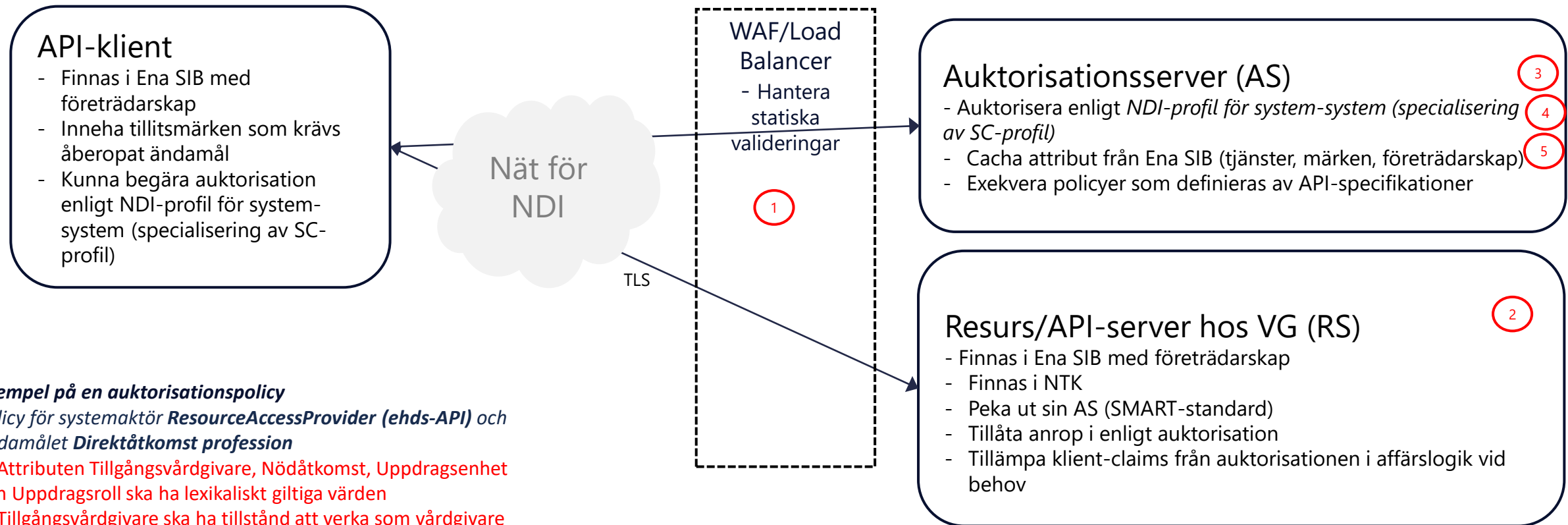
Teknisk nivå – Säkerhetslösning

API-specifikationer beskriver vilken policy för auktorisation som gäller för API:et



Där framgår vilka ändamål som stöds och vilka krav på attribut och märken som ställs på systemaktörerna

Krav på vårdgivarens infrastruktur



Exempel på en auktorisationspolicy

Policy för systemaktör **ResourceAccessProvider (ehds-API)** och ändamålet **Direktåtkomst profession**

1. Attributen Tillgångsvårdgivare, Nödåtkomst, Uppdragsenhet och Uppdragsroll ska ha lexikaliskt giltiga värden
2. Tillgångsvårdgivare ska ha tillstånd att verka som vårdgivare
3. Anropande tjänst ska finnas i SIB metadatatjänst
4. Anropande tjänst ska ha tillitsmärken NDI:TGT-Profession och NDI:Användarknuten åtkomst
5. Det finns metadata i SIB Företrädarskap som styrker att tjänsten (den som auktoriseras) får företräda tillgångsvårdgivaren

An abstract graphic consisting of a network of interconnected nodes and lines, resembling a molecular structure or a complex web. The nodes are represented by small circles, and the lines are thin, light blue. The overall shape is irregular and spans the width of the slide.

Diskussion – att tänka på inför remiss

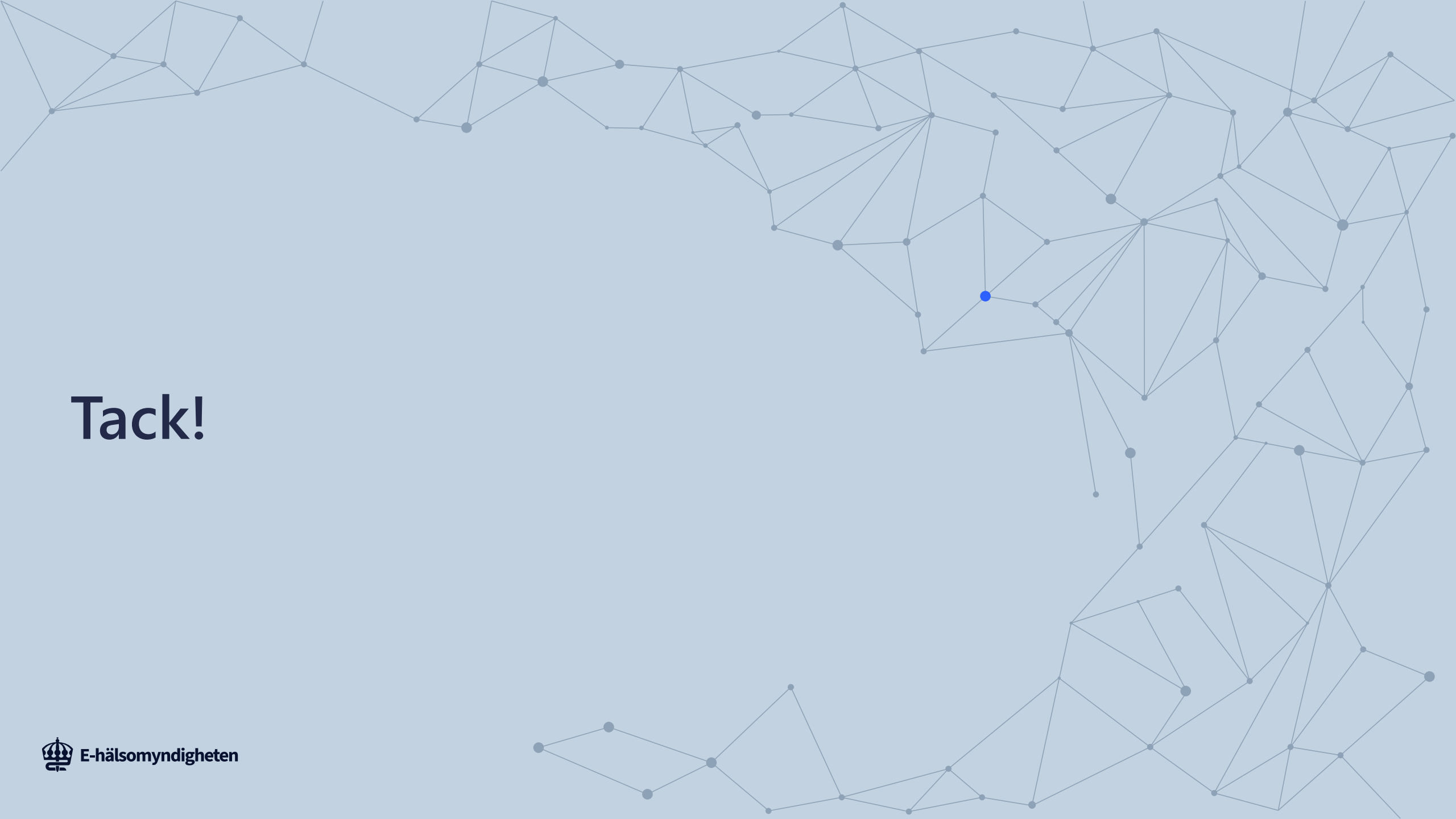
Återkoppling

- Presentera förslag på regelverk för säker datadelning inom EHDS, NDI
- Får era reflektioner på om regelverket är ändamålsenligt och proportionerligt
- Få råd inför remissrundan



E-hälsomyndigheten





Tack!



E-hälsomyndigheten