Principbibliotek - Målarkitektur för Identitet och Åtkomst

Målarkitektur för identitet & åtkomst

Ansvarig arkitekt: Rickard Stormhammar
Version: 1
Datum: 2025-03-27

VÄSTRA GÖTALANDSREGIONEN

Principer

Under arkitekturarbetet har följande principer från referensmaterialen sammanfattats i ett bibliotek.
(Hög relevans för målarkitekturen)

	🏛 Principbibliotek 🏛 - Målarkitektur för identitet och åtkomst
1	**Standardisering** - Prioritera gemensamma arbetssätt (EA2) - Minimera antalet verksamhetsapplikationer (EA8) - Återanvänd före köp före utveckling (EA9) - Teknisk interoperabilitet genom standardisering (EA10) - Masterdata ska alltid hämtas och underhållas i av VGR utpekade källor (MD3) - Masterdata ska vara applikationsoberoende (MD8) - Nationell funktionell skalbarhet (TB2) - Lös koppling & interoperabilitet (TB3) - Separera e-tjänster och IT-infrastruktur med standardiserade gränssnitt (IÅ1) - Anslut e-tjänster via biljettbaserad teknik (IÅ3) - Federerade identitetsdata utgör basen för e-tjänsternas behörighetsprofil (IÅ4) - Plattformsneutral infrastruktur för identitet och åtkomst (IÅ5) - Begränsa omfattning av innehåll i lokala kopior (GK2) - Standardiserade gränssnitt (ES1) - Linjera med Referensarkitektur IAM (ES5) - Plattformsneutralitet (ES6)
2	**Tillgänglighet** - Information ska vara tillgänglig (EA5) - Masterdata ska vara lättillgängligt (MD10) - Öppna upp (DS3) - Skapa transparens till den interna hanteringen (DS4) - Se till att information och data kan överföras (DS6) - Sätt användaren i centrum (DS7) - Gör digitala tjänster tillgängliga och inkluderande (DS8) - Hitta rätt balans för den personliga integriteten (DS10) - Använd ett språk som användarna förstår (DS11) - Gör administrationen enkel (DS12) - Lokalt driven e-tjänsteförsörjning (TB5) - Inloggning till e-tjänster sker via gemensam tjänst för e-legitimering (IÅ2) - Stöd för flera alternativa bärare för e-id vid flerfaktorautentisering (IÅ8) - E-legitimering för underskrift (ES2) - ”Det du ser är vad du undertecknar” - WYSIWYS3 (ES4)
3	**Samverkan** - Flera aktörer - en region (EA1) - Samverka som förstahandsval (DS1) - Återanvänd från andra (DS5) - Systematisk och Samlad Ansats (NS1) - Kunskap och Kompetensutveckling (NS5) - Internationellt Samarbete (NS6) - Samverkan i federation (TB4) - Tillit till andra organisationer skapas via öppna tillitsramverk (IÅ6)
4	**Datakvalitet** - Prioritera digitalisering (EA3) - Information är en strategisk tillgång (EA4) - Information utgår från gemensamma begrepp och standarder (EA6)

	- Masterdata ska förvaltas och styras som en förutsättning för digitalisering (MD1) - Finns av VGR fastställda masterdata ska den användas (MD2) - Masterdata ska vara spårbar och ha en unik identifierare som nyckel (MD4) - Masterdata ska vara unika (MD5) - Masterdataändringar ska vara sanktionerade och kopplade till en beslutsprocess (MD6) - All masterdata ska ha en ägare (MD7) - Masterdata ska vara aktuell och hållas uppdaterad (MD9) - Ha helhetssyn på informationshantering (DS13) - Information om förändrade katalogposter (GK1) - Historiska katalogposter (GK3)
5	**Säkerhet** - Informationssäkerhet baseras på informationens värde (EA7) - Arbeta aktivt med juridiken (DS2) - Gör det säkert (DS9) - Säkerhet i Nätverk, Produkter och System (NS2) - Förebygga och Hantera Cyberattacker (NS3) - Bekämpa IT-relaterad Brottslighet (NS4) - Principen om behovsbaserad åtkomst (need-to-know) (ISO1) - Principen om behovsbaserad användning (need-to-use) (ISO2) - Informationssäkerhet (TB1) - Flerfaktorautentisering samt säker utgivningsprocess möjliggör stark autentisering (IA7) - Tillåt autentisering i separat säkerhetskanal (IA9) - Håll biometriska data nära användaren (IA10) - Uppgiftsminimering (ES3) - Säkerställ bevarande av dokument och signatur (ES7) - Riskbaserad åtkomstkontroll (NIS1) - Stark autentisering och åtkomstskydd (NIS2) - Identitetshantering (IAM) (NIS3) - Åtkomstloggning och spårbarhet (NIS4) - Säkerhet i fjärråtkomst och externa gränssnitt (NIS5) - Segmentering och isolering av känsliga system (NIS6)

#	Princip	Relevans	Tema	Referens
EA1	**Flera aktörer - en region** Samverkan sker inom regionen och med externa parter för att skapa kvalitet och effektivitet inom berörda verksamheter. Gränserna mellan olika aktörer ska utifrån invånarnas och organisationers perspektiv suddas ut. Genom samverkan ökar förutsättningarna att de tjänster som erbjuds uppfattas som meningsfulla.		**Samverkan**	EA-principer [1]
EA2	**Prioritera gemensamma arbetssätt** Regionala och gemensamma arbetssätt ska prioriteras för en enhetlig och effektiv verksamhet.		**Standardisering**	EA-principer [1]
EA3	**Prioritera digitalisering** Digitalisera regionens utbud för att möta samhällets och invånarnas förväntan på digitala tjänster. Digitaliseringen är också en nödvändig del i utvecklingen och effektiviseringen av regionens verksamhet för att kunna möte ett ökande vårdbehov. (ökande behov av tjänster från regionens verksamheter).		**Datakvalitet**	EA-principer [1]
EA4	**Information är en strategisk tillgång** Den information som Västra Götalandsregionen hanterar ska behandlas och vårdas som en strategisk, taktisk och operativ tillgång.		**Datakvalitet**	EA-principer [1]
EA5	**Information ska vara tillgänglig** Verksamheten, invånare och externa aktörer har tillgång till		**Tillgänglighet**	EA-principer [1]

	den information de behöver för att utföra sina uppgifter. Information delas mellan olika verksamhetsfunktioner, organisatoriska enheter och ska tillgängliggöras för externa parter i så stor omfattning som möjligt, med beaktande av sekretess- och integritetsaspekter			
EA6	**Information utgår från gemensamma begrepp och standarder** Regionens information skall så långt som möjligt bygga på en gemensam utveckling av informationsstrukturer och terminologier, vilka ska utgå från regionala beslut.		**Datakvalitet**	EA-principer [1]
EA7	**Informationssäkerhet baseras på informationens värde** Värdet på informationen ligger till grund för vilket skydd, nivå av tillgänglighet och behov av riktighet som krävs för hantering av informationen.		**Säkerhet**	EA-principer [1]
EA8	**Minimera antalet verksamhetsapplikationer** Eftersträva att hålla nere antalet verksamhetsapplikationer samt konsolidera där det är möjligt. Ambitionen är att det för varje verksamhetsfunktion endast ska finnas en verksamhetsapplikation dvs. minimera förekomster av flera verksamhetsapplikationer som utför samma sak samt flera driftsatta versioner av samma verksamhetsapplikation. Ett komplext applikationslandskap med många applikationer är både kostnadsdrivande och påverkar ledtider vid förändringar.		**Standardisering**	EA-principer [1]
EA9	**Återanvänd före köp före utveckling** Applikationer, infrastruktur- och systemkomponenter ska i första hand återanvändas, i andra hand inköpas om det behövs och i sista hand byggas och utvecklas endast om det finns unika behov eller krav som inte kan uppfyllas på annat sätt.		**Standardisering**	EA-principer [1]
EA10	**Teknisk interoperabilitet genom standardisering** Mjukvara och hårdvara ska följa regionalt beslutade standarder för att på ett säkert sätt kunna utbyta information med den kvalitet som parterna i ett informationsutbyte kommit överens om för att uppnå teknisk interoperabilitet.		**Standardisering**	EA-principer [1]
MD1	**Masterdata ska förvaltas och styras som en förutsättning för digitalisering** Masterdata är en tillgång för organisationen och en förutsättning för korrekt beslutsfattande. Precis som andra resurser och tillgångar så som personal, utrustning, fastigheter etc. så ska den vårdas och tillvaratas på ett strukturerat sätt.		**Datakvalitet**	Masterdata-principer [2]
MD2	**Finns av VGR fastställda masterdata ska den användas** Genom att använda fastställd masterdata säkerställs att information som används i verksamheten håller hög kvalitet genom att den t.ex. är fullständig, aktuell och följer uppsatta regler.		**Datakvalitet**	Masterdata-principer [2]
MD3	**Masterdata ska alltid hämtas och underhållas i av VGR utpekade källor** En användare ska aldrig behöva vara i tvivel om vilken informationskälla som är korrekt. Principen ska säkerställa att existerande masterdata används, oavsett om de finns i regionens egna IT-system eller hämtas från andra nationella eller internationella källor.		**Standardisering**	Masterdata-principer [2]
MD4	**Masterdata ska vara spårbar och ha en unik identifierare som nyckel** Denna princip innebär att det ska vara möjligt att spåra ändringar i masterdata och vem som ansvarade för ändringen. Spårbarhet innebär även att det skall vara möjligt att säkerställa att masterdata hålls oförändrad genom systemmiljön. Genom att masterdata har en unik identifierare som används som		**Datakvalitet**	Masterdata-principer [2]

	nyckel överallt säkerställs en enhetlig och enkel åtkomst av masterdata.			
MD5	**Masterdata ska vara unika** Masterdata måste vara identifierbara och unika. Att masterdata är unik innebär att samma information bara skall förekomma en gång. Om samma eller en delmängd av samma information lagras i två masterdataattribut kan det resultera i inkonsistens och ökade kostnader för förvaltning. All masterdata måste därför ha en tydlig beskrivning över vilken informationsmängd den innehåller.		**Datakvalitet**	Masterdata-principer [2]
MD6	**Masterdataändringar ska vara sanktionerade och kopplade till en beslutsprocess** Ändringar av masterdata ska vara styrda av kvalitetssäkrade beslut och godkända enligt beslutade processer och rutiner.		**Datakvalitet**	Masterdata-principer [2]
MD7	**All masterdata ska ha en ägare** All masterdata måste ha en ägare vilket innebär att masterdata måste indelas logiskt på ett sätt så att ägarskap kan fördelas.		**Datakvalitet**	Masterdata-principer [2]
MD8	**Masterdata ska vara applikationsoberoende** Masterdata ska definieras utifrån verksamhetens behov, (inte efter nuvarande applikationers datainnehåll). Denna princip ska säkerställa att informationsinnehållet är baserat på verkliga verksamhetsbehov och att det finns ett livscykelperspektiv på masterdata. Applikationer kommer och går, masterdatabehovet består. Det ska vara möjligt att byta applikation utan att byta informationsstruktur.		**Standardisering**	Masterdata-principer [2]
MD9	**Masterdata ska vara aktuell och hållas uppdaterad** Denna princip ska säkerställa att den masterdata som används inom VGR är aktuell. Med aktuell avses att informationen är korrekt och kvalitetssäkrad. För att den skall vara det krävs att informationen alltid hålls uppdaterad. Masterdata är basen för många system, aktualitet och snabb publicering av ändrad information är därför viktigt.		**Datakvalitet**	Masterdata-principer [2]
MD10	**Masterdata ska vara lättillgängligt** Masterdata måste vara lättillgängligt för de användare och applikationer som ska använda data. Med lätt avses att det skall finnas tydliga rutiner och hantering för hur projekt och användare får tillgång till masterdata.		**Tillgänglighet**	Masterdata-principer [2]
DS1	**Samverka som förstahandsval** Den offentliga sektorn behöver stärka sin förmåga att se och agera utifrån ett helhetsperspektiv och skapa större samlad samhällsnytta. Offentliga organisationer behöver säkerställa att man, enskilt och i samverkan med andra, gör rätt saker och på rätt sätt.		**Samverkan**	Grundläggande principer för digital samverkan [3]
DS2	**Arbeta aktivt med juridiken** De juridiska förutsättningarna för digital samverkan varierar mellan olika organisationer. Utöver det gemensamma författningsstödet har enskilda offentliga organisationer specifika författningar att förhålla sig till.		**Säkerhet**	Grundläggande principer för digital samverkan [3]
DS3	**Öppna upp** Data är en gemensam resurs som ska kunna återanvändas för andra syften än vad de först var tänkta för. Offentliga organisationer samlar in och tar fram enorma mängder data. Dessa data är en gemensam resurs som offentliga organisationer ska öppna upp och tillgängliggöra för andra att använda.		**Tillgänglighet**	Grundläggande principer för digital samverkan [3]
DS4	**Skapa transparens till den interna hanteringen** Privatpersoner och företag ska kunna förstå offentliga organisationers processer och hantering av ärenden som man är berörd av samt hur den egna informationen hanteras och delas med andra organisationer. Det innebär att det för privatpersoner		**Tillgänglighet**	Grundläggande principer för digital samverkan [3]

	och företag måste vara tydligt vilka organisationer som gör vad, samt i vilken ordning som frågor hanteras i olika organisationer.			
DS5	**Återanvänd från andra** Offentliga organisationer ska dra nytta av andra organisationers erfarenheter och ta tillvara befintliga lösningar och produkter. Återanvändning av IT-lösningar (till exempel programvarukomponenter, gränssnitt för tillämpningsprogram, standarder), information och data bidrar till en förbättrad kvalitet i offentliga tjänster och kan spara både tid och pengar. Återanvändning och delning kan effektivt stödjas genom samarbetsplattformar.		**Samverkan**	Grundläggande principer för digital samverkan [3]
DS6	**Se till att information och data kan överföras** Tillgång till och effektivt utbyte av information är en grundförutsättning för framgångsrik digitalisering. För att öka rörligheten av information och data behöver data enkelt kunna överföras och återanvändas mellan aktörer och tekniska system. Offentliga organisationer ska se till att deras information och datas tillgänglighet och återanvändning inte är beroende av någon speciell teknik eller produkt, till exempel ett proprietärt format.		**Tillgänglighet**	Grundläggande principer för digital samverkan [3]
DS7	**Sätt användaren i centrum** För att offentlig sektor ska kunna möta framtidens utmaningar behövs nya sätt att tänka och en djupare förståelse för vad som skapar värde för de offentliga organisationer, privatpersoner eller företag som behöver ha tillgång till och dra nytta av dessa tjänster. Offentliga organisationer ska stödja användardriven innovation. Det innebär att användarnas olika behov och krav ska vara vägledande för vilka tjänster som utvecklas samt för hur tjänsterna utformas och utvecklas. Därutöver ska privatpersoner och företag ges möjlighet att delta i utformningen av nya tjänster, bidra till förbättringen av tjänsterna och återkoppla om befintliga offentliga tjänsters kvalitet.		**Tillgänglighet**	Grundläggande principer för digital samverkan [3]
DS8	**Gör digitala tjänster tillgängliga och inkluderande** Inkludering och tillgänglighet behöver hanteras i hela utvecklingsprocessen för offentliga tjänster. Detta gäller utformning, informationsinnehåll och tillhandahållande av tjänster. Offentliga organisationer ska följa allmänt vedertagna specifikationer för digital tillgänglighet på nationell och internationell nivå. För att alla ska ha jämlika möjligheter – och dra största möjliga nytta av den nya tekniken vid användning av offentliga tjänster – ska alla användare av offentliga tjänster vara inkluderade genom god tillgänglighet. Personer med funktionsnedsättning och andra grupper med särskilda behov kan då använda offentliga tjänster med jämförbar servicenivå som andra privatpersoner.		**Tillgänglighet**	Grundläggande principer för digital samverkan [3]
DS9	**Gör det säkert** I sina kontakter med offentliga organisationer måste privatpersoner och företag kunna lita på att verksamheten och informationsbehandlingen sker i en säker och pålitlig miljö och i enlighet med gällande bestämmelser. Detta gäller allt från forskningsresultat och fotografier till fastighetsförteckningar och storleken på en utbetalning. Informationen kan ibland till och med vara livsviktig såsom informationen i patientjournaler eller styrsystemen i ett vattenreningsverk. Är den informationen förlorad eller felaktig kan det få katastrofala följder.		**Säkerhet**	Grundläggande principer för digital samverkan [3]
DS10	**Hitta rätt balans för den personliga integriteten** Offentliga organisationer behöver hitta rätt avvägning mellan den personliga integriteten för privatpersoner och andra aspekter (till exempel skyddade personuppgifter, allmänhetens rätt till information och effektivitet i verksamheten) som säkerställer att privatpersoners privatliv skyddas på ett ändamålsenligt sätt och att information som tillhandahålls av		**Tillgänglighet**	Grundläggande principer för digital samverkan [3]

	privatpersoner och företag behandlas förtroligt, är äkta och fullständig. I utvecklingen av offentliga tjänster behöver privatpersoner och företag i utökad grad få möjlighet att själv avgöra vem som tar del av uppgifter som rör den enskilde eller företaget.			
DS11	**Använd ett språk som användarna förstår** Offentliga organisationer måste beakta flerspråkighet vid utformningen av tjänster. De offentliga tjänsterna kan användas inom Sverige men även av användare från andra länder – inte minst andra medlemsstater i EU. Medborgarna i EU har ofta svårt att få tillträde till och använda digitala offentliga tjänster om de inte är tillgängliga på ett språk som personerna behärskar.		**Tillgänglighet**	Grundläggande principer för digital samverkan [3]
DS12	**Gör administrationen enkel** Offentliga organisationer behöver ta tillvara digitaliseringens möjligheter och rationalisera och förenkla sina administrativa processer. Detta är nödvändigt utifrån ett externt användarperspektiv, ett internt medarbetarperspektiv samt av samhällsekonomiska skäl.		**Tillgänglighet**	Grundläggande principer för digital samverkan [3]
DS13	**Ha helhetssyn på informationshantering** Data är en gemensam resurs. För att ta tillvara digitaliseringens möjligheter behövs en helhetssyn på informationshantering och en ökad proaktivitet. Det innebär att offentliga organisationer, redan från det att data skapas, behöver ha en beredskap för hur man ska hantera, bevara och tillgängliggöra data.		**Datakvalitet**	Grundläggande principer för digital samverkan [3]
NS1	**Systematisk och Samlad Ansats** Utveckla en nationell modell för informationssäkerhetsarbete och förbättra samverkan och informationsdelning mellan olika aktörer.		**Samverkan**	Nationell strategi för samhällets informations- och cybersäkerhet [4]
NS2	**Säkerhet i Nätverk, Produkter och System** Öka säkerheten i elektroniska kommunikationsnät och industriella informations- och styrsystem samt implementera säkra kryptosystem.		**Säkerhet**	Nationell strategi för samhällets informations- och cybersäkerhet [4]
NS3	**Förebygga och Hantera Cyberattacker** Förbättra förmågan att upptäcka och hantera cyberattacker och IT-incidenter samt utveckla ett robust cyberförsvar.		**Säkerhet**	Nationell strategi för samhällets informations- och cybersäkerhet [4]
NS4	**Bekämpa IT-relaterad Brottslighet** Stärka de brottsbekämpande myndigheternas förmåga att bekämpa IT-relaterade brott och utveckla förebyggande åtgärder.		**Säkerhet**	Nationell strategi för samhällets informations- och cybersäkerhet [4]
NS5	**Kunskap och Kompetensutveckling** Öka kunskapen om informationssäkerhet i samhället och främja forskning och utveckling inom informations- och cybersäkerhet.		**Samverkan**	Nationell strategi för samhällets informations- och cybersäkerhet [4]
NS6	**Internationellt Samarbete** Stärka internationella samarbeten för att hantera cybersäkerhetsutmaningar och främja ett globalt, öppet och säkert internet.		**Samverkan**	Nationell strategi för samhällets informations- och cybersäkerhet [4]
ISO1	**Principen om behovsbaserad åtkomst (need-to-know)** En entitet beviljas endast åtkomst till den information som den behöver för att utföra sina uppgifter (olika uppgifter eller roller innebär olika behov av information och därmed olika åtkomstprofiler),		**Säkerhet**	SS-EN ISO/IEC 27002:2022 [14]
ISO2	**Principen om behovsbaserad användning (need-to-use)** En entitet beviljas endast åtkomst till IT-infrastruktur om ett uppenbart behov föreligger.		**Säkerhet**	SS-EN ISO/IEC 27002:2022 [14]
TB1	**Informationssäkerhet** Tillgänglighet, sekretess, riktighet och spårbarhet ska säkerställas vid all samverkan.		**Säkerhet**	T-boken [15]
TB2	**Nationell funktionell skalbarhet** Skalbarhet från lokalt till nationellt och vice versa. Lösningarna		**Standardisering**	T-boken [15]

	behöver kunna appliceras såväl på det lokala planet som det nationella. Arkitekturen ska inte begränsa dess användning i detta avseende.			
TB3	**Lös koppling & interoperabilitet** Innebär bl.a. att en komponent i en lösning kan bytas ut oberoende av andra. Uppnås genom en tjänstebaserad arkitektur med kommunikation genom gemensamma, standardiserade gränsytor mellan komponenter. Interoperabla, internationellt beprövade och för leverantörer tillgängliga (öppna) standarder tillämpas för meddelandeutbyte mellan system.		**Standardisering**	T-boken [15]
TB4	**Samverkan i federation** Samverkan över organisationsgränser sker genom federation, såsom exempelvis via identitetsfederation. Federation bygger på gemensamma överenskomna regelverk, t.ex. kring krav på autentisering av användare i IT-system, tekniska regelverk osv.		**Samverkan**	T-boken [15]
TB5	**Lokalt driven e-tjänsteförsörjning** E-tjänsteförsörjning i vård och omsorg är i grunden driven från lokala behov. Regelverk för arkitektur stödjer att lokalt etablerade e-tjänster gradvis kan bredda sin bas av användare över vårdgivargränser och så småningom berika det nationella e-tjänsteutbudet. För invånaren erbjuder varje e-tjänstekanal en sammanhållen användarupplevelse (”virtuell portal”) oavsett vilken part som tekniskt och utvecklingsmässigt står bakom en enskild e-tjänst.		**Tillgänglighet**	T-boken [15]
IÅ1	**Separera e-tjänster och IT-infrastruktur med standardiserade gränssnitt** Ger en lös och standardiserad koppling mellan e-tjänsterna och de generella funktionerna för identitet och åtkomst. Produktanpassningar blir applicerbara på en global marknad, och bättre förutsättningar för att marknadens produkter kommer anslutningsklara från början. Skapar även grundförutsättningar för en samlad administrationspunkt, federativa lösningar och återanvändning av investeringar i säkerhetsteknik. Minskar inlåsningseffekterna mot viss hårdvara och mjukvara.		**Standardisering**	Referensarkitektur för identitet och åtkomst [16]
IÅ2	**Inloggning till e-tjänster sker via gemensam tjänst för e-legitimering** Underlättar att skapa en samordnad användarinloggning med hög igenkänningsfaktor och hög tillit. Ökar flexibiliteten och möjliggör att lägga till nya inloggningsmetoder och ny autentiseringsteknik utan att påverka anslutna e-tjänster.		**Tillgänglighet**	Referensarkitektur för identitet och åtkomst [16]
IÅ3	**Anslut e-tjänster via biljettbaserad teknik** Gränssnittet mot e-tjänsten blir stabilare över tid då det inte påverkas av nya användarkrav på inloggningsfunktionen eller den senaste autentiseringstekniken, vilket ger ökad förvaltningsbarhet och minskade kostnader för IT-säkerhetslösningar. E-tjänsten kan i första hand fokusera på den verksamhetsfunktion den ska leverera.		**Standardisering**	Referensarkitektur för identitet och åtkomst [16]
IÅ4	**Federerade identitetsdata utgör basen för e-tjänsternas behörighetsprofil** En gemensam bas för identitet och behörighet skapar förutsättning för god skalbarhet och minskad administrativ börda i verksamheterna. Identitets- och behörighetsadministration kan konsolideras till en funktion där en användare samlat kan ges grundläggande rättigheter att arbeta med de IT-system och den information som hens arbete eller individuella behov kräver. Även borttag av rättigheterna (t.ex. när medarbetare slutar anställning) underlättas.		**Standardisering**	Referensarkitektur för identitet och åtkomst [16]
IÅ5	**Plattformsneutral infrastruktur för identitet och åtkomst** IT-infrastruktur för identitet och åtkomst (såsom inloggningsfunktionalitet) behöver kunna nyttjas för alla de olika typer av e-tjänster och enheter som ingår i verksamhetens IT-stöd: webb, tunna och feta klienter, mobila plattformar osv.		**Standardisering**	Referensarkitektur för identitet och åtkomst [16]

	Alternativet är att bygga, förvalta och administrera parallell IT-infrastruktur, vilket är resurs- och kostnadsdrivande.			
IÅ6	**Tillit till andra organisationer skapas via öppna tillitsramverk** Genom öppna beskrivna tillitsramverk som kan delas av de parter som behöver kommunicera, kan man undvika att behöva skapa många bilaterala överenskommelser, som även riskerar att divergera och skapa suboptimerade lösningar.		**Samverkan**	Referensarkitektur för identitet och åtkomst [16]
IÅ7	**Flerfaktorautentisering samt säker utgivningsprocess möjliggör för stark autentisering** Gemensam syn på vad som är tillräckligt för stark autentisering är en viktig förutsättning för samverkan mellan organisationerna. Genom kopplingen till tillitsramverk blir olika autentiseringslösningar jämförbara med varandra.		**Säkerhet**	Referensarkitektur för identitet och åtkomst [16]
IÅ8	**Stöd för flera alternativa bärare för e-id vid flerfaktorautentisering** Ger en flexibilitet som bättre kan stödja olika verksamhetsbehov och teknikskiften, och därmed minskar trösklarna för att införa säkra autentiseringslösningar i verksamheterna. Med anpassade lösningar för e-id och e-legitimering, ökar möjligheterna att i verksamheten implementera säkra lösningar för åtkomst till IT-stödet.		**Tillgänglighet**	Referensarkitektur för identitet och åtkomst [16]
IÅ9	**Tillåt autentisering i separat säkerhetskanal** Autentisering i separat kanal medför minskat beroende till vilken hårdvara som kan användas som kanal för informationssystemet, t.ex. en läsplatta, en digital whiteboard i korridoren, en kapslad tryckskärm i en operationsavdelning osv. Alternativet, att alltid endast använda samma kanal för både information och autentisering, leder till starka tekniska krav och begränsningar på den utrustning som kan användas i IT-stödet.		**Säkerhet**	Referensarkitektur för identitet och åtkomst [16]
IÅ10	**Håll biometriska data nära användaren** Biometriska data är integritetskänslig information. Det kan finnas fall då biometriska data har ett värde att hanteras och lagras i ett centralt register, men detta bör alltså undvikas främst pga. integritetsskäl. Biometri rekommenderas inte i enfaktorslösningar, eftersom det inte går att återkalla (”revokera)” en persons biometriska data.		**Säkerhet**	Referensarkitektur för identitet och åtkomst [16]
GK1	**Information om förändrade katalogposter** Arkitekturen ska möjliggöra delgivande av information om förändrade poster, så att lokala kopior kan hållas uppdaterade utan att hela källan behöver kopieras.		**Datakvalitet**	Referensarkitektur för grunddata och katalog [17]
GK2	**Begränsa omfattning av innehåll i lokala kopior** Arkitekturen ska möjliggöra att lokala kopior består av minsta möjliga antal poster, snarare än en fullständig kopia av hela katalogen**.**		**Standardisering**	Referensarkitektur för grunddata och katalog [17]
GK3	**Historiska katalogposter** Arkitekturen ska omfatta såväl aktuell information som historisk information, så att information kan delges om hur en katalogpost såg ut vid en viss specifik tidpunkt.		**Datakvalitet**	Referensarkitektur för grunddata och katalog [17]
ES1	**Standardiserade gränssnitt** E-tjänsterna respektive IT-infrastrukturen för elektroniska underskrifter och stämplar separeras genom standardiserade gränssnitt.		**Standardisering**	Referensarkitektur för elektronisk underskrift och stämpel [18]
ES2	**E-legitimering för underskrift** Lösningar för e-underskrift bör möjliggöra att använda s.k. e-legitimering för underskrift, vilket innebär att den elektroniska identitetshandlingen som används för att identifiera och autentisera användaren i e-tjänsten, även används vid e-underskriften.		**Tillgänglighet**	Referensarkitektur för elektronisk underskrift och stämpel [18]
ES3	**Uppgiftsminimering** Lösningar för elektronisk underskrift och stämpel bör möjliggöra att minimera de uppgifter som behöver lämnas ut till tredje part. Det bör vara möjligt att behålla skyddet för känslig information, även vid användande av extern, och		**Säkerhet**	Referensarkitektur för elektronisk underskrift och stämpel [18]

	eventuellt delad, underskriftstjänst. T.ex. bör dokument som undertecknas eller valideras inte behöva lämnas ut till externa tjänster.			
ES4	**”Det du ser är vad du undertecknar” - WYSIWYS3** Lösningar för elektroniska underskrifter ska utformas så att det semantiska innehållet i det dokument som undertecknas, vilket undertecknaren ges möjlighet att granska, alltid bevaras genom den elektroniska underskriften.		**Tillgänglighet**	Referensarkitektur för elektronisk underskrift och stämpel [18]
ES5	**Linjera med Referensarkitektur IAM** Utformning av lösningar för elektroniska underskrifter och stämplar ska linjera med Referensarkitektur för Identitets- och åtkomst [IAM-RA]. För tillämpliga delar innebär det bl.a. att tjänsterna ska kunna samverka, och att de styrande principer för området identitet och åtkomst även gäller inom detta område.		**Standardisering**	Referensarkitektur för elektronisk underskrift och stämpel [18]
ES6	**Plattformsneutralitet** IT-infrastruktur för elektroniska underskrifter och stämplar byggs i grunden plattformsneutral. Eventuella plattformsspecifika delar läggs till som anpassningar ovanpå grundstrukturen.		**Standardisering**	Referensarkitektur för elektronisk underskrift och stämpel [18]
ES7	**Säkerställ bevarande av dokument och signatur** Utformning av lösningar och val av format för elektroniska underskrifter och stämplar ska säkerställa att krav kring bevarande av digitalt signerade dokument (handlingar) kan uppfyllas. Principen omfattar bevarande av det signerade dokumentet, signaturen självt samt förmågan att i efterhand validera signaturen.		**Säkerhet**	Referensarkitektur för elektronisk underskrift och stämpel [18]
NIS1	**Riskbaserad åtkomstkontroll** Åtkomst till nätverk och informationssystem ska begränsas till auktoriserade användare och processer. Användare ska bara ha tillgång till det de behöver för sitt arbete – varken mer eller mindre (principen om *least privilege*). Roller och behörigheter ska kartläggas och begränsas så långt det är möjligt. Åtkomsträttigheter ska granskas **regelbundet** och justeras vid rollförändringar eller avslut. Automatiserad behörighetsstyrning (IGA) rekommenderas för att minska manuella fel och öka spårbarhet.		**Säkerhet**	NIS2 [19]
NIS2	**Stark autentisering och åtkomstskydd** Flerfaktorautentisering eller lösningar för kontinuerlig autentisering ska införas där det är lämpligt. MFA (Multi-Factor Authentication) är ett **krav i alla känsliga system**, särskilt för fjärråtkomst och administrativa konton. MFA ska implementeras där data eller tjänster är känsliga, system är exponerade eller där åtkomst sker över organisationsgränser. Kontinuerlig autentisering (t.ex. genom sessionsövervakning, platsbaserad åtkomst) är rekommenderat för vissa miljöer.		**Säkerhet**	NIS2 [19]
NIS3	**Identitetshantering (IAM)** Organisationer ska införa riktlinjer och rutiner för identitets- och åtkomsthantering. Tydlig struktur för skapa–ändra–avsluta-processen för användarkonton. Roll- och behörighetsmodeller ska definieras och kopplas till verksamhetens struktur. Identiteter ska vara unika, spårbara och kopplade till en ansvarig ägare. Det ska vara tydligt vilka personer eller system som har åtkomst till vad – och varför.		**Säkerhet**	NIS2 [19]
NIS4	**Åtkomstloggning och spårbarhet** Säkerställ förmåga att övervaka och logga åtkomst till kritiska system och data. Alla känsliga åtkomster ska loggas, inklusive inloggningar, förändringar i behörigheter och åtkomst till kritisk information. Loggar ska vara omanipulerbara, bevarade enligt regelverk och tillgängliga vid incidentutredning. Logghantering är även grundläggande för incidentdetektion och rapportering.		**Säkerhet**	NIS2 [19]
NIS5	**Säkerhet i fjärråtkomst och externa gränssnitt** Fjärråtkomst ska vara säker och lämpligt begränsad. Fjärråtkomst till system ska ske genom krypterade anslutningar, stark autentisering och segmentering (användaren		**Säkerhet**	NIS2 [19]

	kommer bara åt det nödvändiga). Externa leverantörer (t.ex. driftpartners) måste omfattas av samma krav som interna användare.			
NIS6	**Segmentering och isolering av känsliga system** Inför lämpliga riktlinjer för segmentering av nätverk och informationssystem. Känsliga system (t.ex. patientjournaler, identitetstjänster) ska separeras logiskt och tekniskt från andra delar av nätverket. Privilegierade användarkonton ska endast användas i särskilda, säkra miljöer. “Break glass”-access (akut åtkomst) ska vara tydligt reglerad och spårbar.		**Säkerhet**	NIS2 [19]