Myndigheten för samhällsskydd och beredskap

FOI

FORSKNING/STUDIE

Framtida nationell användning av Galileo/PRS

Faktaruta

Titel:
Framtida nationell användning av Galileo/PRS

År:
2018

Utförare:
Totalförsvarets forskningsinstitut (FOI)

Författare:
Mikael Alexandersson, Fredrik Marsten Eklöf och Björn Gabrielsson

Sammanfattning:
Galileo är ett europeiskt satellitnavigeringssystem som idag har en initial operativ förmåga och planeras vid slutet av 2020 vara fullt operativt. Galileo erbjuder flera så kallade PNT-tjänster (Positionering, Navigering och Tid) anpassade för olika typer av användargrupper. Tjänsten ”Public Regulated Service” (PRS) är anpassad för myndighetsanvändning och primärt inom området civil säkerhet och beredskap, t.ex. blåljusmyndigheterna, samt försvar. PRS-tjänsten erbjuder en robust och säker källa för PNT och har hög robusthet mot störning samt är skyddad mot vilseledning genom kryptering.

Den här rapporten beskriver egenskaper hos PRS och fördelar med att använda tjänsten för viktiga samhällsfunktioner. Rapporten ger även en kort genomgång av potentiella användargrupper och en beskrivning av den myndighetsfunktion som hanterar PRS-tjänsten.

MSB:s kontaktpersoner:
Kristoffer Hultgren, 010-240 41 05

Omslagsfoto: Alecom AB

Publikationsnummer MSB1290 - oktober 2018
ISBN 978-91-7383-883-2

MSB har beställt och finansierat genomförandet av denna forskningsrapport.
Författarna är ensamma ansvariga för rapportens innehåll.

Innehållsförteckning

Sammanfattning

Galileo är ett europeiskt satellitnavigeringssystem som idag har en initial operativ förmåga och beräknas vara fullt operativt 2020-2021. Galileo erbjuder flera så kallade PNT-tjänster (Positionering, Navigering och Tid) anpassade för olika typer av användargrupper. Tjänsten ”Public Regulated Service” (PRS) är anpassad för myndighetsanvändning och primärt inom området civil säkerhet och beredskap, t.ex. blåljusmyndigheterna, samt försvar. PRS-tjänsten erbjuder en robust och säker källa för PNT och har hög robusthet mot störning samt är skyddad mot vilseledning genom kryptering.

Galileo byggs upp av EU (projektägare) som genom ”European Space Agency” (ESA) utvecklar rymd- och kontrollsegmenten samt myndigheten ”European GNSS Agency” (GSA) som utvecklar användarsegmentet. Europeiska kommissionen och medlemsstaterna styr Galileo på en övergripande nivå.

Medlemsstaterna bestämmer hur PRS-tjänsten ska nyttjas nationellt baserat på av EU fastställda regler som benämns ”*Common Minimum Standards” (CMS)*. Enligt CMS ska en myndighetsfunktion, ”Competent PRS Authority” (CPA), upprättas nationellt för att hantera PRS-tjänsten. Utan en CPA kan inte medlemsstaten ha access till och nyttja PRS-tjänsten. Idag hanterar UD/NSA funktionen CPA i Sverige.

Användningen av PNT-tjänster inom blåljusmyndigheterna och andra aktörer inom området civil säkerhet och beredskap är omfattande och bedömningen är att det finns ett beroende av PNT-tjänster för att kunna genomföra verksamhet på ett effektivt sätt. Idag används framförallt civil (okrypterad) GPS/GNSS som inte är anpassad för att vara robust och säker mot externa hot som störning och vilseledning. PRS-tjänsten erbjuder robust funktionalitet och är utvecklad för dessa tillämpningar.

Hur PRS-tjänsten ska användas nationellt är inte utrett och fastställt. Det finns intresse från blåljusmyndigheterna att använda PRS-tjänsten. Omfattningen på PRS-användningen kommer att påverka utformningen av CPA-funktionen.

1. Ordlista

AIS	Automatic Identification System
CDMA	Code Division Multiple Access
FDMA	Frequency Division Multiple Access
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning Satellite System
GSA	European GNSS Agency
IOV	In-Orbit Validation
MEO	Medium Earth Orbit
OTAR	Over The Air Rekeying
PNT	Position, Navigation and Timing
STRIKE3	Standardisation of GNSS Threat Reporting and Receiver Testing Through International Knowledge Exchange, Experimentation and Exploitation
Öppen/Civil GNSS	Okrypterade tjänster, tex Galileo Open Service (OS) eller GPS C/A
Säker/skyddad GNSS	GNSS-tjänst som är krypterad för att säkerställa a) enbart auktoriserade användare har tillgång till tjänsten. b) skydda mot vilseledning, då en motståndare inte kan generera en trovärdig signal för att vilseleda/lura en mottagare att ge falska utdata. Exempel på skyddade GNSS-tjänster är Galileo PRS och PPS (Militär) GPS.

2. Bakgrund

Syftet med rapporten är att beskriva egenskaper hos PRS och fördelar med att använda tjänsten för viktiga samhällsfunktioner. Rapporten ger även en kort genomgång av potentiella användargrupper och en beskrivning av CPA-funktionen. En del av innehållet bygger på tidigare material som redan har avrapporterats till MSB [1].

Med ett satellitnavigeringssystem (GNSS – Global Navigation Satellite System) kan en mottagare bestämma sin position och tid globalt med hög noggrannhet och tillgänglighet. Systemen har flera fördelar jämfört med traditionella navigerings- och tidssystem. Användningen av GNSS är idag mycket omfattande för ett stort antal kommersiella (t.ex. UAV:er, fordonssystem, mobiltelefoner) och professionella (t.ex. ledningssystem, larmsystem, övervakningssystem) tillämpningar. En allt viktigare tillämpning är synkronisering och tidhållning i olika typer av system. Användningen av PNT-tjänster inom blåljusmyndigheterna och andra aktörer inom området civil säkerhet och beredskap är omfattande och bedömningen är att det finns ett beroende av PNT-tjänster för att kunna genomföra verksamhet på ett effektivt sätt. Idag används framförallt civil GPS/GNSS som inte är anpassad för att vara robust och säker mot externa hot som störning och vilseledning. Det finns en hotbild mot GNSS eftersom störsändare finns öppet tillgängliga via internet till en låg kostnad.

Möjligheten att vilseleda civila GNSS-mottagare har ökat genom utvecklingen av mjukvaruradio och tillgång till fri källkod för generering av GNSS-signaler.

Det Europeiska satellitnavigeringssystemet Galileo är under uppbyggnad sedan ett flertal år tillbaka och idag har systemet en initial operativ förmåga samt används för ett flertal kommersiella tillämpningar. En av grundtankarna med Galileo är att få ett satellitbaserat navigeringssystem som är under europeisk kontroll. ”European GNSS Agency” (GSA), lokaliserad i Prag, ansvarar bland annat för utvecklingen av Galileos PNT-tjänster och användarsegmentet.

Som en del av Galileo-systemet finns en tjänst avsedd för myndighetsbruk benämnd PRS (”Public Regulated Service”). Varje medlemsland som vill använda PRS skall ha funktioner inom landet för att hantera tillgång och användning av tjänsten. Dessa funktioner samlas i en myndighetsfunktion kallad ”Competent PRS Authority” (CPA), som är kontaktytan mellan Sverige och ansvariga myndigheter inom EU. Sverige behöver ta fram en plan för utvärdering av PRS-tjänsten och hur tilltänkta användare kan dra nytta av de fördelar PRS har jämfört med övriga PNT-tjänster för att säkerställa och maximera nyttan Sverige får av investeringen i Galileo och PRS. Ett av huvudsyftena med Galileo PRS-tjänsten är att erbjuda en robust och säker tjänst för positionering och tidgivning, primärt inom området civil säkerhet och beredskap, t.ex. blåljusmyndigheterna, och försvar. Sverige finansierar utbyggnaden av Galileo inom EU och ESA-budgeterna.

3. Hotbild

Det finns en tydlig hotbild på användarsidan av GNSS som kan delas upp i två delar:

- **Störning:** Syftet är att förhindra en eller flera GNSS-mottagare att bestämma dess position och tid. Följden blir att tjänsten blockeras helt för användaren eller att noggrannheten degraderas.
- **Vilseledning:** Syftet är att få en eller flera GNSS-mottagare att erhålla en felaktig position och/eller tid, på så sätt kan mottagaren och användaren luras, se Figur 2.

Kriminella använder idag störsändare för ett flertal syften, exempelvis för att slå ut spårsändare (GNSS-baserade) och radiobaserade larmsystem.

Hot mot själva Galileo-infrastrukturen med satelliter och mark/kontrollsystem har inte beaktats i denna studie men bedöms generellt kräva resurser från stater att genomföra och infrastrukturen är utformad för att vara robust mot sådana attacker.

3.1 Störning

Störning innebär att GNSS-signalerna hos en mottagare blockeras genom sändning av en radiosignal som orsakar en högre mottagen effekt (överröstar) än den som sänds ut av satelliterna. Den mottagna signalnivån i mottagaren från GNSS-signalerna är mycket låg på grund av det stora avståndet till satelliterna. Detta innebär att störsändare även med låg utsänd effekt kan blockera signalerna och på så sätt störa ut mottagare. Störsändare kan realiseras med enkel hårdvara och finns tillgängliga att köpa via internet, se exempel i Figur 1, och till en kostnad från 25 USD [11] - [14]. Högre uteffekt (störeffekt) medför att en GNSS-mottagare kan blockeras på ett större avstånd och kostnaden för störsändaren ökar.

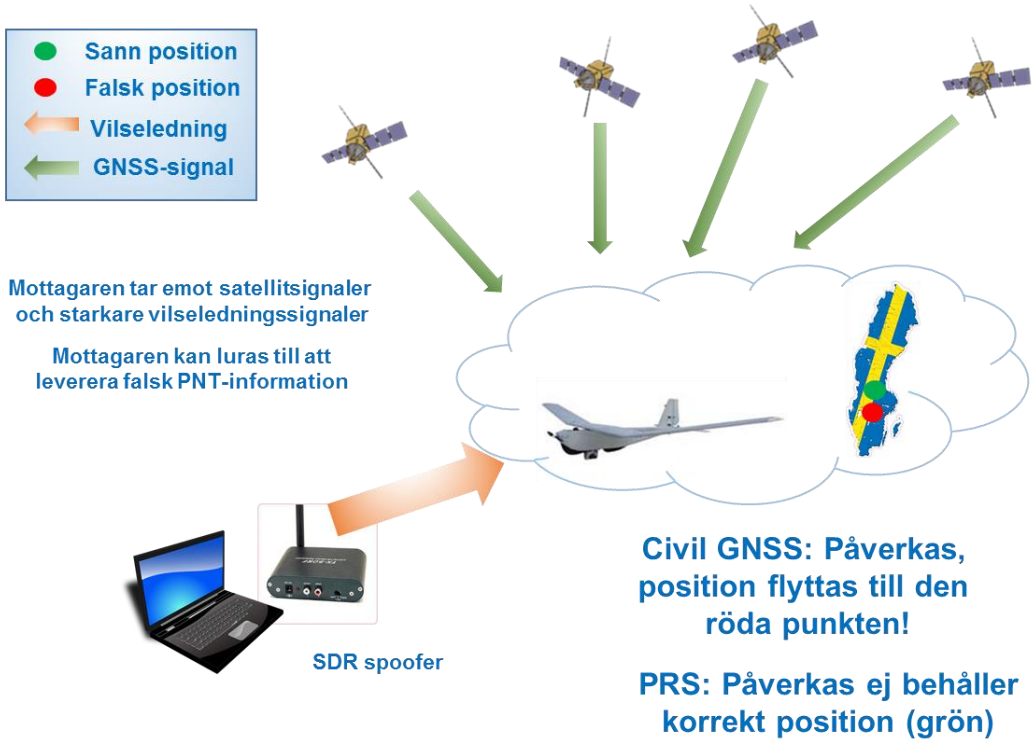
Figur 1, Exempel på störsändare tillgängliga via internet.

Störsändare som kan köpas via internet, finns tillgängliga med låg till medelhög uteffekt. Det finns ett flertal bekräftade fall där störsändare har använts både nationellt och internationellt [15] – [20]. Ett nyligen

uppmärksammat fall är den person som dömdes för att ha kartlagt journalister. Personen dömdes för grovt vapenbrott och innehav av störsändare [25]. På YouTube finns ett flertal exempel på hur företag eller privatpersoner marknadsför störsändare och hur de kan användas i olika syften [21] – [24]. Genom det EU-finansierade Horizon 2020 projektet STRIKE3 har en kartläggning av förekomsten av GPS-störsändare som använder det civila frekvensbandet L1 påbörjats [2]. En tre månaders mätkampanj under projektets inledande period har påvisat ett stort antal incidenter [3].

3.2 Vilseledning

Tidigare ansågs hotbilden för vilseledning av GNSS mot det civila samhället vara låg, men idag har detta reviderats på grund av den snabba teknikutvecklingen. Enkel och billig mjukvarubaserad radiohårdvara (SDR – ”Software Defined Radio”) kan användas för att realisera ett vilseledningssystem. Utförlig och beskrivande information finns tillgängligt på internet [26] – [30].



Figur 2, Illustration av vilseledning.

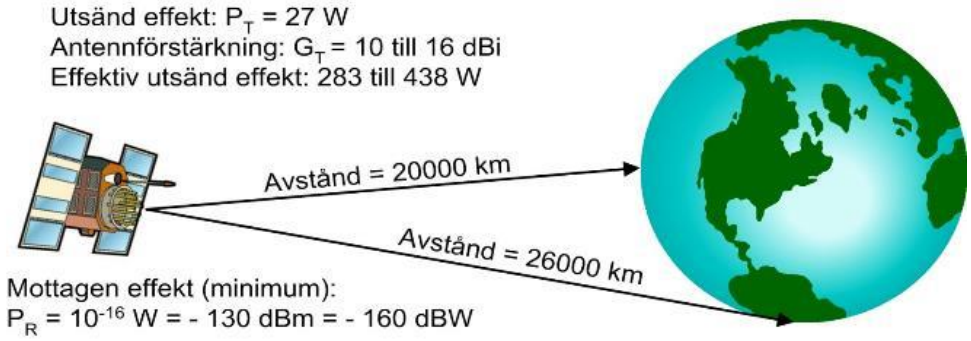
Ryssland och andra länder bedöms idag ha en hög förmåga att störa GNSS med telekrigssystem. Militärt har ett flertal incidenter med GPS-/GNSS-störning förekommit. Ett antal incidenter som har skett i närtid kan på olika sätt knytas till Ryssland, exempelvis under kriget i Ukraina [4] och i Nordnorge i samband med övningen Zapad17 [5]. Vid ryska svartahavskusten rapporterade ett flertal fartyg felaktiga positioner (motsvarande positioner på land) vilket indikerar vilseledning. Detta har dokumenterats både på de enskilda fartygen och med hjälp av AIS-systemet [6] och [7].

4. Beskrivning av GNSS

Med ett satellitnavigeringssystem kan en mottagare bestämma sin position i tre dimensioner och tid oberoende av var på jorden den befinner sig (global täckning). Antalet samtidiga användare av systemet är obegränsat då en mottagare enbart lyssnar på satellitsignalerna. Det finns idag fyra globala satellitnavigeringssystem: GPS (USA), GLONASS (Ryssland), Galileo (EU) och BDS (Kina). Idag är GPS och GLONASS fullt operativa, Galileo har en initial operativ förmåga och BDS är under uppbyggnad. GPS är ett amerikanskt militärt system där den civila och kommersiella användningen garanteras av ett presidentdirektiv från 2010 [31].

Systemen är uppbyggda enligt samma grundprincip och består av tre segment: användarsegment (mottagare), rymdsegment (satelliter) och ett kontrollsegment. För ytterligare information om GNSS se appendix 1 och referenser [32] – [37]. Mottagaren bestämmer sin position baserat på mätningar av avståndet till minst 4 satelliter som är försedda med ett noggrant system av klockor (vanligen tre till fyra atomur). Genom triangulering kan positionen på jordytan bestämmas med hög noggrannhet och eftersom avståndet mäts i tid så är GNSS också en källa till noggrann tid.

En utmaning med att använda ett satellitbaserat navigeringssystem är avståndet till satelliterna som medför att GNSS-signalen kommer att dämpas markant innan den når mottagaren. Den mottagna signaleffekten på jordytan är mycket låg, och ligger under det normala bakgrundsbruset, Figur 3.



Figur 3, Illustration av mottagen signaleffekt för GNSS.

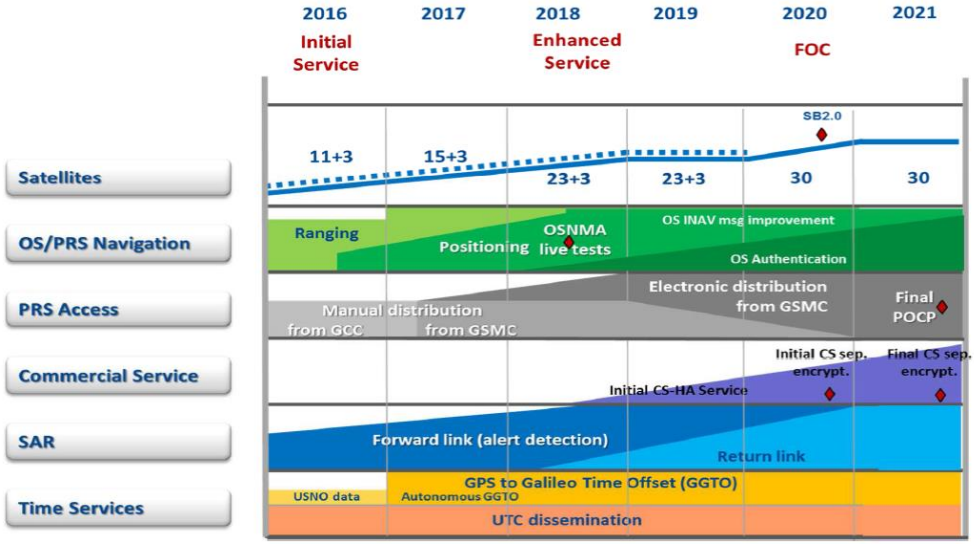
5. Beskrivning av Galileo

Galileo är ett europeiskt system som utvecklats av EU och ESA sedan början av 2000-talet, där Europeiska kommissionen är projektägare, ESA upphandlar rymd- och kontrollsegment och GSA utvecklar användarsegmentet. Galileo står under kontroll av EU:s medlemsstater och Europeiska kommissionen. Galileo är EU:s största infrastrukturprojekt med omfattning på ca 90 miljarder SEK. Galileo brukar benämnas som ett civilt projekt under civil kontroll.

Den första satelliten sköts upp i augusti 2005 och den senaste i juli 2018. Från den 15 december 2016 erbjuder Galileo-systemet en initial förmåga som benämns ”Initial Service” (IS), baserad på befintlig infrastruktur med avseende på operativa satelliter och kontrollsegmentet. Systemet består för närvarande av 17 operativa satelliter och ytterligare 5 satelliter som ska driftsättas. En av de fyra första Galileosatelliterna (IOV-generationen) har havererat och två satelliter befinner sig i en felaktig bana på grund av en misslyckad uppskjutning och den framtida användningen av dessa är ännu oklar.

När de sex satelliterna tas i drift planeras nästa fas som benämns ”Enhanced Service” (ES). En full konstellation för Galileo (eng. ”Full Operational Capability”, FOC), kommer att bestå av 30 satelliter och beräknas vara i drift ca år 2020-2021. För att kunna realisera detta har ytterligare 8 Galileosatelliter upphandlats av ESA. För ytterligare beskrivning av Galileo se referenser [38] – [41].

Tidplan över införandet av Galileos funktionalitet återfinns i Figur 4. Under perioderna IS och ES kommer funktioner för att hantera och använda PRS att byggas upp. Under IS är hantering och distribution av kryptonycklarna manuell för att stegvis införa en elektronisk distribution som skall vara klar till senast FOC.



Figur 4, Tidplan för Galileos driftsättning.

Enligt tidplanen i Figur 4 så skulle ES, där samtliga uppskjutna Galileosatelliter är operativa, införas under Q2-Q3 2018. Detta är försenat och förväntas till Q4 2018 eller Q1 2019.

Marksegmentet för Galileosystemet består av följande funktioner:

- Två kontrollcentraler (”Ground Control Center”, GCC) som ansvarar för driften är lokaliserade till Oberpfaffenhofen i Tyskland och Fucino i Italien.
- Sex övervakningsstationer (”Telemetry, Tracking and Control”, TT&C) som bland annat övervakar satelliternas positioner och status. Esrange är en av dessa stationer.
- Fem sändarstationer (”Mission Uplink Stations”, ULS) som skickar information till satelliterna.
- Ett globalt nätverk av 16 sensorstationer (”Galileo Sensor Stations”, GSS) som samlar in mätningar på Galileo-satelliterna och skickar informationen till GCC i realtid.
- Ett servicecentrum (”European GNSS Service Center”, GSC) som är kontaktytan mellan Galileo-systemet och användare av Galileo-tjänsterna OS (Open Service) och CS (Commersial Service, för närvarande kallad HAS).

Marksegmentets delar är framförallt placerade inom Europa eller på områden som kontrolleras av ett EU-medlemsland. Sensorstationerna är placerade globalt för att erhålla en kontinuerlig övervakning av Galileo-satelliterna, Figur 5.

Figur 5, Bild på placering av kontrollsegmentet för Galileo.

5.1 Strategiska mål för Galileo

De strategiska målen för Galileo är att:

- Stärka Europas självständighet avseende tillgång och användning av rymden i en säker och trygg omgivning.
- Erbjuda ett europeiskt navigeringssystem under civil kontroll.
- Maximera nyttan av rymden för samhälle och EU:s ekonomi.
- Utveckla en global och konkurrenskraftig europeisk rymdsektor.

- Stärka Europas roll som global aktör och främja internationellt samarbete.

5.2 Tjänster i Galileo

Galileo erbjuder totalt fyra tjänster där de två OS och PRS kommer att tillhandahållas under IS- och ES-faserna medan HAS (f.d. CS) och SAR förväntas först till FOC. Galileo-systemet använder CDMA-teknik och sänder på tre frekvenser, se Tabell 1.

Tabell 1, Översikt över Galileo.

Benämning	Frekvens [MHz]	Signal	Användning	Egenskaper
E1	1575,42	OS	Civil	Öppen
		PRS	Myndighet	Krypterad
E6	1278,75	HAS	Kommersiell	Licensierad
		PRS	Myndighet	Krypterad
E5a/E5b	1191,795	OS	Civil	Öppen
		HAS	Kommersiell	Licensierad

5.2.1 Open Service (OS)

OS är en öppen tjänst motsvarande den tjänst som har funnit sedan 1990-talet i amerikanska GPS-systemets L1 C/A-signal. Signalen är inte krypterad och är tänkt för massmarknadsmottagare för civil användning.

5.2.2 High Accuracy Service (HAS)

HAS är en tjänst som ska komplettera OS och erbjuda en utökad tjänst med avseende på tillgänglighet och noggrannhet. HAS signal kan vara krypterad för att reglera tillgång till tjänsten. Tidigare benämndes tjänsten för ”Commercial Service” (CS). Tjänsten är idag inte fullt definierad.

5.2.3 Search And Rescue (SAR)

SAR är en tjänst för att hitta personer i nöd, och arbetar tillsammans med COSPAS-SARSAT-systemet [8] för att detektera nödsändningar på 406 MHz-bandet och vidarebefordra dem från satelliterna på L6/E6-bandet till markstationer.

6. Public Regulated Service (PRS)

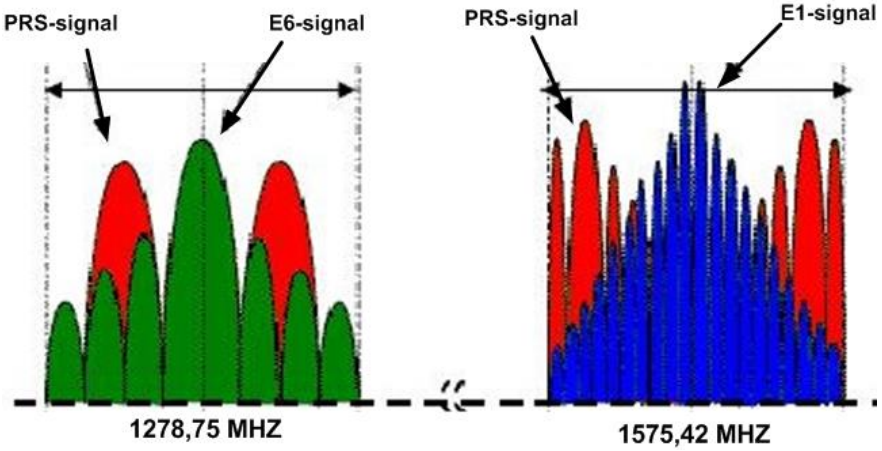
Galileo PRS är en PNT-tjänst avsedd för ackrediterade användare som har behov av hög robusthet mot störning och vilseledning, samt hög tillgänglighet. Detta realiseras genom funktioner i systemet och egenskaper för PRS-signalen samt funktioner i mottagarna.

PRS är en tjänst där vissa delar av driften sköts separat från övrig drift av Galileo, för att säkerställa att PRS fungerar även i händelse av vissa fel på övriga system.

PRS-signalen är krypterad för att förhindra vilseledning, där krypteringen medför att det krävs mottagare med en säkerhetsmodul laddad med giltiga kryptonycklar för att kunna avkoda signalen.

PRS kan jämföras med RAKEL som är ett robust kommunikationssystem för blåljusmyndigheterna. På samma sätt som RAKEL ger robust kommunikation är PRS designad för att tillhandahålla en robust och autentiserad PNT-tjänst.

Signalen sänds samtidigt både på E1- och E6-bandet för ökad robusthet och precision, se Figur 6. PRS-tjänsten beräknas vara i full drift 2020-2021.



Figur 6, Frekvensspektrum för Galileo PRS, rött spektrum är PRS-signalen.

Tjänsten har följande fördelar jämfört med civil GNSS:

- Robustare mot störning
- Minskad risk för tids- och positionsfel
- Ger varning till användaren vid störning
- Europeiskt system
- Dess frekvensspektrum är skiljt från civil GNSS, vilket ger möjlighet att störa civil användning av GNSS, utan att påverka PRS
- PRS-signalerna sänds på två frekvensband

- Krypterad, skyddad mot vilseledning
- Bättre prestanda (tillgänglighet, noggrannhet, robusthet).

Eftersom en PRS-mottagare är försedd med kryptofunktioner, så kan följande punkter anses vara fördyrande och försvåra hantering av PRS-mottagare jämfört med mottagare utan kryptofunktion:

- Högre inköpskostnad eftersom mottagaren innehåller kryptofunktioner
- Kostnader för användning av PRS-mottagare är högre beroende på krav på hantering av krypto, utbildning och underhållskostnader.

PRS-mottagaren innehåller också nya tekniklösningar, som exempelvis nya modulationsformer, som innebär att nya chipset måste tas fram och provas ut, eftersom äldre teknologi inte är användbar fullt ut.

6.1 Beskrivning av CPA

Användningen av PRS ska utformas och ske enligt ”Common Minimum Standards” (CMS). Enligt CMS ska en så kallad ”Competent PRS Authority” *(*CPA*)* upprättas nationellt. Genom CPA ska medlemsstaterna utforma och styra den nationella användningen. Tillverkning av PRS-mottagare med säkerhetsmodul ska övervakas av CPA och ske enligt CMS.

Utformningen och implementeringen av CPA-funktionen är ett nationellt ansvar och beslut. Idag ansvarar UD för CPA-funktionen i Sverige, men den slutliga utformningen och organiseringen är inte utredd och fastställd.

CPA skall ansvara för den nationella PRS-användningen, PRS-användarna och deras organisation i användargrupper samt vara kontaktorganisation med GSA och ”Galileo Security Monitoring Centre” (GSMC). En distributionskedja för hantering av kryptonycklar skall upprättas för att säkerställa korrekt distribution från att de nationella nycklarna erhålls från GSA till att de nyttjas av de nationella användarna. En nationell styrande policy för användningen av PRS ska tas fram inom varje land.

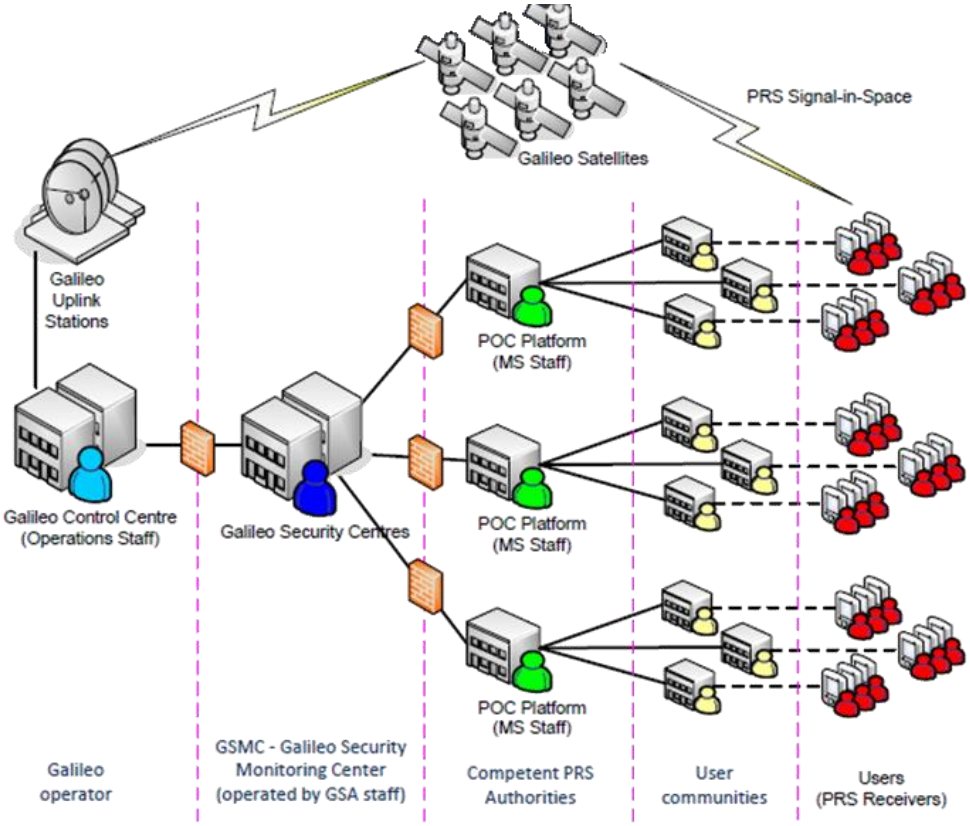
Nedan redovisas några av de krav och funktioner som CPA skall följa och inneha, se även Figur 7.

- CPA ger tillgång till PRS-signalen för godkända PRS-användare och säkerställer att endast godkända PRS-mottagare används i enlighet med the ”Common Minimum Standards”
- CPA organiserar PRS-användare i PRS användargrupper; varje PRS användargrupp har tillgång till förmåga i enlighet med tilldelade rättigheter
- En PRS-användare skall kunna användare mottagaren när följande villkor är uppfyllda:
    - Mottagaren har blivit registrerad i systemet av CPA
    - Mottagaren har laddats med parametrar i enlighet med de rättigheter som gäller för den användargrupp som mottagaren är placerad i. Mottagaren har laddats med

nödvändiga kryptonycklar som ger tillgång till avsedd tjänst

- All PRS funktionalitet är tillgänglig
- Infrastrukturen för PRS är i drift
- Myndigheter/CPA kan prova PRS procedurer
- Användare har tillgång till PRS utrustning
- Användare kan prova PRS funktionen

För uppgiften att fungera som nationellt ansvarigt organ för PRS krävs goda kontakter med de tilltänkta nationella användarorganisationerna. Dessutom krävs god kunskap om organisationernas behov och krav på en robust positioneringstjänst eller säker tidsbestämning. PRS-tjänsten bör integreras i befintliga systemlösningar eller på annat sätt användas av organisationer som arbetar med samhällets skydd och säkerhet.



Figur 7, schematisk bild över hur PRS är tänkt att implementeras.

GSMC är en del av Galileos PRS infrastruktur, och har följande huvudsakliga funktioner:

- **Galileo Security Monitoring:** GSMC övervakar och reagerar på säkerhetshot, säkerhetsvarningar och driftsstatus på system komponenterna.
- **Hantera åtkomst till PRS på systemnivå:** GSMC ser till att känslig information avseende användningen av ”Public Regulated Service” (PRS) hanteras lämpligt och skyddat, och inte exponerat för ”Galileo Operating Centre”. GSMC fungerar som ett gränssnitt mellan länder/myndigheter (genom ”Computerised Point of Contract Platforms” eller POCPs) för att

begära kryptografiska nycklar, och med Galileo huvudkomponenter för satellit relaterade meddelanden.

- **Implementation av gemensamma handlingsinstruktioner:** Högsta beslutande organ är Europeiska Rådet, som om enhälligt, kan ge instruktioner till GSA och det företag som har driftskontraktet att justera driften av systemet, exempelvis stänga ner en eller flera tjänster. Detta är tänkt för undantagsfall där säkerhetshot eller internationell kris mot EU eller en medlemsstat har kopplingar till systemet. Det skulle också kunna vara vid ett direkt hot mot driften av Galileo-systemet självt.
- **Tillhandahålla expertis och analys avseende PRS och Galileo.**

Idag finns två GSMC där den primära är lokaliserad i Saint Germain en Laye, nära Paris och är en del av GSA. Anläggningen i Frankrike är operativ sedan 2014. Den sekundära GSMC var lokaliserad i Swanwick, Storbritannien, men har under våren 2018 flyttats till Spanien på grund av Storbritanniens kommande utträde ur EU. Denna GSMC är under uppbyggnad och är tänkt som en aktiv reservanläggning med möjlighet till omedelbar drift om primäranläggningen inte fungerar eller är möjlig att använda.

6.2 Nationell PRS-organisation

Ett flertal funktioner för en CPA-myndighetsfunktion med tillhörande frågeställningar har identifierats:

- GSA ska tillförsäkra att ett interferensövervakningssystem (”interference monitoring system”) sätts upp och ska koordinera arbetet med respektive medlemsland. Idag saknas information om vad detta innebär för respektive medlemsland. Om avsikten är att kunna detektera och därefter lokalisera interferenser och störsändare, krävs ett genomtänkt koncept och metodik för att kunna arbeta effektivt. PTS, FOI och FM har viss förmåga och resurser som kan nyttjas för detta, men har inte operativ beredskap eller rutiner för att hantera ett interferensövervakningssystem. Att omhänderta en störsändare är en polisiär uppgift och kan därför inte göras av ovannämnda myndigheter. Beroende på ambitionsnivå kan det vara en omfattande och kostsam uppgift att bygga upp ett system för interferensövervakning.
- Upprätta nationella användargrupper enligt givna riktlinjer och sköta tillsyn av att de uppfyller ställda säkerhetskrav. CPA-organisationen skall enligt GSA använda olika rutiner för normalförhållanden och krissituationer. Respektive användarorganisation (t ex en myndighet) skall delta i arbetet med att definiera hur dess PRS-användare ska organiseras i användargrupper.
- En databas ska upprätthållas och kontinuerligt hållas uppdaterad för de nationella användargrupperna. En förteckning över samtliga PRS-mottagare skall upprätthållas (”accounting system”).
- Upprätta nyckelhanteringsfunktion. För hanteringen av kryptonycklar är det naturliga att utnyttja befintliga rutiner och

organisationer som används inom myndigheter som idag använder kryptoutrustningar.

- Identifiera “essential users” vars nyttjande skall upprätthållas även i en krissituation. Troligen innebär detta att om PRS-användare inte kan erhålla nya kryptonycklar genom OTAR, exempelvis på grund av störning, utan är hänvisade till att nyttja manuell distribution av nycklarna så kommer dessa ”essential users” att prioriteras.
- Infrastrukturen för Galileo skall skyddas. Påverkan av säkerheten för PRS om en PRS-mottagare går förlorad skall utvärderas. Detta behövs för att snabbt kunna bestämma hur situationen ska hanteras och vilka åtgärder som behöver vidtas. Effekten av förlust av en PRS-mottagare kommer att bero på scenariot (detta kommer att ingå i “National PRS Security Policy”).
- CPA-organisationen har tillsynsansvar för utveckling, tillverkning och försäljning av PRS-mottagare och applikationer inom sitt land.

Nationellt behöver teknisk kompetens om PRS-tjänsten och PRS-mottagare byggas upp för att stötta användare och CPA-funktionen. För att tilltänkta användare ska kunna nyttja PRS-tjänsten på ett fullgott sätt är det av stor vikt att denna kompetens finns nationellt. För att kunna vara med och kravställa den fortsätta utvecklingen av PRS mot GSA och Europeiska kommissionen är det viktigt att kompetens finns inom Sverige. Utvecklingen av Galileo PRS genomförs inom ett flertal arbetsgrupper där medlemsstaterna deltar. Det är av största vikt att Sverige finns representerad i dessa grupper och att nödvändigt arbete kan genomföras.

Ett samarbetsråd bestående av representanter för de tilltänkta PRS-användarna bör inrättas för att kontinuerligt kunna informera och i dialog utforma den nationella användningen av PRS-tjänsten.

Vid eventuell nationell tillverkning av PRS-mottagare och/eller applikationer har CPA-organisationen tillsynsansvar. Nationell tillverkning av PRS-mottagare i Sverige bedöms idag som mindre sannolikt, men ett flertal företag kan komma att använda och integrera PRS i produkter och system.

6.3 Riktlinjer för användningen av PRS

Användning av PRS beskrivs och styrs av Europaparlamentets och Rådets beslut nr 1104/2011/EU [9] och CMS, i detta ingår exempelvis;

- PRS-användargruppers organisation.
- Fastställande och förvaltning av tillträdesrättigheter för PRS-användare och användargrupper bland PRS-deltagarna.
- Distribution av PRS-nycklar och därtill relaterad säkerhetsskyddsklassificerad information mellan GSMC och de behöriga PRS-myndigheterna och användargrupperna.
- Säkerhetsförvaltning, inbegripet säkerhetsincidenter, och riskbedömning för PRS-mottagare och därtill relaterad säkerhetsskyddsklassificerad teknik och information.

- Rapportering om upptäckt av potentiellt skadlig elektromagnetisk interferens som kan påverka PRS.
- Operativa koncept och förfaranden för PRS-mottagare.

För länder som vill utveckla eller tillverka PRS-mottagare eller säkerhetsmoduler tillkommer;

- Ackreditering av PRS-användarsegment.
- Säkerhet avseende PRS-mottagare och PRS-teknik under forsknings-, utvecklings- och tillverkningsfaserna.
- Integrering av PRS-mottagare och PRS-teknik.
- Skyddsprofil för PRS-mottagare, säkerhetsmoduler och material med användning av PRS-teknik.

6.4 Kostnader

Galileo-systemet bekostas genom EU-kommissionens budget. Där bidrar Sverige via avgiften för medlemskap i EU. En betydande del av kostnaden för Galileo beror på PRS-tjänstens krav på säkerhet och skydd.

Att uppskatta kostnad och omfattning för CPA-organisationens verksamhet är i dagsläget svårt. Om befintliga strukturer kan användas, exempelvis för nyckelhantering och beredskap, borde omfattningen vara relativt begränsad. Omfattningen för CPA-organisationens verksamhet uppskattas, med dessa antaganden, till 4 – 6 personår. De befintliga organisationer som får ett utökat ansvar kommer troligen kräva mer resurser än så.

Om det krävs beredskap dygnet runt kommer omfattningen på CPA-organisationen att öka markant.

Om tillverkning av PRS-mottagare eller applikationer kommer att ske nationellt kommer omfattningen för CPA-organisationen att behöva ökas på grund av tillsynsansvaret.

6.5 PRS-mottagare

För att en mottagare ska kunna använda den krypterade PRS-signalen krävs en säkerhetsmodul som hanterar dekrypteringen och funktionerna för själva PRS-tjänsten. Tjänsten ska kunna användas för olika tillämpningar och det kommer krävas utveckling av flera typer av PRS-mottagare. En nyckelteknik är själva säkerhetsmodulen.

Med en PRS-mottagare tillkommer krav på hur den ska hanteras och förvaras. För att en mottagare ska kunna hanteras på ett enkelt sätt även när den är laddad med kryptonycklar måste kryptomodulen skydda informationen även om den utsätts för extern påverkan.

Det pågår utveckling av PRS-mottagare som finansieras av EU men också nationellt finansierad utveckling.

EU har utvecklat PRS-mottagare som benämns ”pre-operational” under programmet P3RS-2 [42]. Syftet är att utveckla teknik för kryptomoduler och mottagare som kan användas för demonstrationer under realistiska scenarion och förutsättningar. Denna typ av demonstrationer benämns av EU som ”Joint Test Activity” (JTA) eller ”pilot projects”.

EU finansierar utvecklingen av PRS-mottagare inom flera parallellt pågående program [43]:

- FRAME (”Framing the definition and development of new PRS use cases based on innovative technologies”): Utveckling av grundläggande teknik och delar för PRS-mottagare. Programmet genomförs i flera steg och i kontrakt med europeisk industri.
- DISPATCH (”Development of Server based PRS TeCHnologies to support future applications”): Utveckling av PRS-mottagare som inte har en egen kryptomodul. Se beskrivning nedan.
- PRISMA (”Development of low end operational PRS Receivers including Security Modules”): Utveckling av PRS-mottagare för mängdtillämpningar med krav på låg kostnad.

En traditionellt utformad mottagare genomför samtliga steg internt för att kunna bestämma en position. För en mottagare som använder krypterade signaler innebär det att nycklar och algoritmer måste skyddas så att dessa inte läcker ur mottagaren. Detta ”kassaskåp” kring hemligheterna i en PRS-mottagare är tänkt att implementeras i en säkerhetsmodul. Denna måste dels skydda hemlig kryptoinformation, samtidigt som den skall vara enkel att hantera för slutanvändarna. Utveckling av säkerhetsmoduler är kostsamt, samtidigt som de i sina första generationer troligtvis inte kommer vara lika små och effektsnåla som en kretslösning för de okrypterade civila signalerna. Serverbaserade PRS-mottagare försöker hantera säkerhetsutmaningar genom att terminalen inte behandlar hemlig information. Funktionen är istället flyttade till en säker serverplats. Ett exempel på en sådan uppdelning är att terminalen samplar en begränsad mängd RF-data som skickas till servern där signalen behandlas i en säker miljö, varpå resultatet kan skickas tillbaka till terminalen. Detta är en tekniklösning som undersöks och är mycket intressant för att få ner kostnader och komplexitet för PRS-mottagare för vissa tillämpningar.

7. Användare av PRS i Sverige

Nedan följer en genomgång av några potentiella användare av PRS. Dock bör en grundligare studie genomföras där användare och deras behov kartläggs, se exempelvis rapporten ”Satellite-derived Time and Position: A Study of Critical Dependencies” skriven av ”Government Office for Science” i Storbritannien [10].

7.1 Blåljusmyndigheter

Flertalet av blåljusmyndigheterna, t.ex. polisen, använder positionering av egen personal och enheter för att effektivt kunna leda insatser och öka deras säkerhet vid larm. Att positionsinformationen som distribueras i polisens och andra blåsljusmyndigheters ledningssystem är korrekt och tillförlitligt är av stor vikt.

7.2 Nytt gemensamt och säkert kommunikationssystem

Rakel är idag det huvudsakliga sambandsmedlet för samverkan mellan aktörer inom allmän ordning, säkerhet, hälsa och försvar. Systemet leverera främst talkommunikation men har begränsad kapacitet för mobil dataöverföring. Det pågår därför ett arbete för en ny kommunikationslösning som skall komplettera och på sikt helt ersätta Rakel.

Det befintliga RAKEL-systemet använder för närvarande GPS som positioneringstjänst. Då den nya lösningen måste uppfylla höga krav på offentlig kontroll, informationssäkerhet, robusthet, skydd och tillgänglighet bör en integration av Galileo PRS undersökas och en pilotstudie för att utvärdera prestanda och ökad förmåga tillsammans med robusthetsvinst bör övervägas.

7.3 Kriminalvården

Kriminalvården använder idag civil GPS/GNSS för ett flertal tillämpningar, t.ex. vid persontransporter mellan anstalter och domstolar.

7.4 Kritisk infrastruktur

Korrekt och spårbar tid är idag en kritisk del av infrastrukturen i Sverige. För att kunna öka tillgången till robust tid och frekvens kan Galileo PRS vara en komponent. Nedan följer exempel på viktiga aktörer och funktioner inom området för tid och takt:

- Post- och telestyrelsen (PTS) och Research Institute of Sweden (RICE, fd SP) som ansvarar för tid i Sverige
- Ägare av infrastruktur för Internet och telekommunikation
- Elkraftproduktion
- Börshandel och andra finansiella transaktioner
- Kommunala transporter

7.5 Försvarsmakten

Försvarsmakten använder idag militär GPS, och får på så sätt en ökad robusthet, men kan på sikt vara intresserade av PRS-tjänsten som komplement. Mottagare som kan kombinera Galileo PRS och militär GPS är en intressant tekniklösning som diskuteras inom NATO.

7.6 Flygtrafikledning

Civil flygtrafikledning använder både position och tid för daglig drift av sin verksamhet. Diskussion om PRS-tjänsten bör initieras med berörda aktörer.

7.7 Antal PRS-användare

En bedömning av antalet möjliga PRS-användare är idag svår att göra baserad på tillgänglig information. Under 2006-2007 genomfördes en initial studie på antal PRS-användare, [1]. Studien identifierade redan då ett relativt stort antal användare och användargrupper men förutsättningarna och användningsområdena har sedan dess ökat och ändrats markant.

En ny studie på antalet möjliga PRS-användare är lämpligt att genomföra då detta kommer att påverka utformningen av CPA-funktionen.

8. Slutsats och kommentarer

Galileo är det europeiska satellitnavigeringssystemet som byggs upp av EU och kommer erbjuda flera PNT-tjänster som är anpassade för olika användargrupper. Systemet har idag en initial operativ förmåga och förväntas vara fullt operativt efter 2020. Kommersiellt används Galileo som ett komplement till andra GNSS som GPS och GLONASS. Galileo står under kontroll av Europeiska kommissionen och EU:s medlemsstater.

Tjänsten PRS är anpassad för myndighetsanvändning och området civil säkerhet och beredskap, t.ex. blåljusmyndigheterna, samt försvar. Tjänsten erbjuder en robust och säker källa för PNT som har hög robusthet mot störning och är skyddad mot vilseledning genom kryptering. En motsvarande tjänst som kan nyttjas för civil säkerhet och beredskap finns inte tillgänglig genom andra GNSS. Försvarsmakten använder militär GPS som har motsvarande robusta egenskaper som PRS, men militär GPS är inte tillgänglig för civila användare.

Galileo PRS-tjänsten kommer vara fullt operativ efter 2020. För nationell användningen krävs en fullt implementerad och operativ CPA-funktion.

Det pågår utveckling av PRS-mottagare inom EU-finansierade program och direkt av några medlemsstater. Det förväntas finnas ett antal typer av PRS-mottagare tillgängliga efter 2020, som är anpassade för olika användningsområden.

De tilltänkta användargrupperna behöver informeras och den möjliga omfattningen inventeras. I första hand inriktas detta mot blåljusmyndigheterna och därefter mot övriga möjliga användningsområden. Tilltänkta användargrupper behöver påbörja aktiviteter för att förbereda en eventuellt framtida användning.

Omfattningen på CPA-arbetet behöver ökas stegvis för att stötta och utveckla användningen av PRS och för att hantera själva PRS-tjänsten och dess funktioner. Inom EU genomförs arbete med att utveckla PRS-tjänsten inom ett flertal arbetsgrupper och bemanning av dessa från svenskt håll måste vara kontinuerlig.

Teknisk kompetens kring PRS-tjänsten behöver byggas upp nationellt för att kunna stötta tilltänkta användargrupper och CPA-funktionen.

Försvarssektorn och därmed svenska Försvarsmakten är en tilltänkt användare av PRS. Deras eventuella och möjliga användning av PRS ingår inte i denna studie och rapport. Försvarsmakten följer utvecklingen av PRS.

9. Referenser

1. F. Marsten Eklöf, FOI dia. nr: 07-507, 2007.
2. ”STRIKE3 - Monitor, Detect, Characterise, Standardize, Mitigate and Protect,” 2017. [Online]. Available: http://www.gnss-strike3.eu/. [Använd 2018].
3. P. Eliardsson, M. Alexandersson, M. Pattinson, S. Hill, Å. Waern, Y. Ying och D. Fryganiotis, 2017. [Online]. Available: http://www.aic-aachen.org/strike3/downloads/STRIKE3%20och%20Detetektiossystemet_RNN_2017-10-18.pdf. [Använd 2018-03-05].
4. S. Linder och M. Alexandersson, ”Användning av störsändning i konflikten i Ukraina - en sammanställning från öppna källor,” FOI MEMO 5625, 2016.
5. J. Rantakokko, ”En beskrivning av två fall av störning och vilseledning som genomförts mot GPS under 2017,” FOI MEMO 6260, 2017.
6. M. Jones, ”GPSWorld: Spoofing in the Black Sea: What really happened?,” http://gpsworld.com/spoofing-in-the-black-sea-what-really-happened, [Använd 2018-09-27].
7. G. Hayes, ”Marine Electronics Journal: Manipulating AIS – Spoofing the system is possible, but there are safeguards.,” https://www.marineelectronicsjournal.com/content/newsm/news.asp?show=VIEW&a=119, [Använd 2018-09-27].
8. ”The International Cospas-Sarsat Programme,” https://cospas-sarsat.int/en/, [Använd 2018-09-27].
9. ”EUROPAPARLAMENTETS OCH RÅDETS BESLUT nr 1104/2011/EU,” http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32011D1104&from=EN, [Använd 2018-09-27].
10. ”UK Government Office for Science, Satellite-derived Time and Position: A Study of Critical Dependencies,”, https://www.gov.uk/government/publications/satellite-derived-time-and-position-blackett-review, [Använd 2018-09-27].
11. http://www.cell-jammers.com/gps-jammers/, [Använd 2018-09-27].
12. http://www.alljammer.com/, [Använd 2018-09-27].
13. http://www.thesignaljammer.com/categories/GPS-Jammers/, [Använd 2018-09-27].
14. http://www.jammerfromchina.com/categories/GPS_Jammers/, [Använd 2018-09-27].
15. http://www.hallandsposten.se/nyheter/halmstad/två-av-tre-fälls-i-hälerihärvan, [Använd 2018-09-27].
16. http://www.dn.se/nyheter/sverige/tjuvarnas-nya-metod-gor-dyra-larm-vardelosa/, [Använd 2018-09-27].
17. http://www.expressen.se/gt/sa-latt-lansar-ligorna-din-bil-svart-att-bevisa/, [Använd 2018-09-27].
18. https://www.elsakerhetsverket.se/globalassets/publikationer/aktuellt/2018/rapport-projekt-storsandare.pdf, [Använd 2018-09-27].

19. http://www.expressen.se/kvallsposten/sa-slar-tjuvarna-ut-ditt-larm-pa-bara-sekunder/, [Använd 2018-09-27].
20. http://www.expressen.se/dinapengar/polisens-nya-larm-om-storsandare-mot-bilar/, [Använd 2018-09-27].
21. https://www.youtube.com/watch?v=JCHcq2Fzsh8, [Använd 2018-09-27].
22. https://www.youtube.com/watch?v=-6hI5aTV2O8, [Använd 2018-09-27].
23. https://www.youtube.com/watch?v=Sj6KS6zoiJQ, [Använd 2018-09-27].
24. http://www.youtube.com/watch?v=uHm8eXyPaNU, [Använd 2018-09-27].
25. https://www.dn.se/nyheter/sverige/nazist-ska-ha-kartlagt-journalister-dom-i-dag/, [Använd 2018-09-27].
26. https://github.com/osqzss/gps-sdr-sim, [Använd 2018-09-27].
27. https://www.rtl-sdr.com/using-a-hackrf-to-spoof-gps-navigation-in-cars-and-divert-drivers/, [Använd 2018-09-27].
28. https://www.rtl-sdr.com/spoofing-gps-locations-with-low-cost-tx-sdrs/, [Använd 2018-09-27].
29. https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf, [Använd 2018-09-27].
30. https://www.crazydanishhacker.com/gps-spoofing-bladerf-software-defined-radio-series-23/, [Använd 2018-09-27].
31. https://www.gps.gov/policy/docs/2010/, [Använd 2018-09-27].
32. https://www.u-blox.com/sites/default/files/products/documents/GPS-Compendium_Book_%28GPS-X-02007%29.pdf, [Använd 2018-09-27].
33. https://www.novatel.com/an-introduction-to-gnss/, [Använd 2018-09-27].
34. http://www.gage.upc.edu/tutorials, [Använd 2018-09-27].
35. https://gnss-sdr.org/docs/tutorials/, [Använd 2018-09-27].
36. https://www.gps.gov/systems/gnss/, [Använd 2018-09-27].
37. https://en.wikipedia.org/wiki/Satellite_navigation, [Använd 2018-09-27].
38. https://en.wikipedia.org/wiki/Galileo_(satellite_navigation), [Använd 2018-09-27].
39. https://www.gsa.europa.eu/european-gnss/galileo/galileo-european-global-satellite-based-navigation-system, [Använd 2018-09-27].
40. http://galileognss.eu/, [Använd 2018-09-27].
41. https://www.esa.int/Our_Activities/Navigation, [Använd 2018-09-27].
42. https://www.gsa.europa.eu/%E2%80%9Cp3rs-2%E2%80%9D-procurement-galileo-prs-pre-operational-receivers, [Använd 2018-09-27].
43. GSA PRS USER SEGMENT ROCUREMENTS ACTIVITIES, Galileo Services Meeting, Prague, 25 November 2015, Marco Detratti, PRS Officer GSA Security Department

Appendix 1. Övriga GNSS

Detta appendix ger en kort teknisk beskrivning av övriga GNSS.

A.1 GPS

GPS är ett amerikanskt system, utvecklat under 1970-talet och driftsatt i maj 1994. Systemet består för närvarande av 32 satelliter (30 i drift) som sänder samtidigt på två eller tre frekvenser beroende på generation av satelliten, Tabell A1.

GPS-systemet använder CDMA-teknik, som innebär att alla satelliter sänder på samma frekvenser samtidigt, men att en spridningskod per satellit används för att avkoda innehållet.

Tabell A1, Översikt över GPS.

Benämning	Frekvens [MHz]	Signal	Användning	Egenskaper
L1	1575.42	C/A	civil och militär	öppen
		P(Y)	militär	krypterad
		L1C	civil	öppen
		M-kod	militär	krypterad
L2	1227.60	L2C	civil,	öppen
		P(Y)	militär	krypterad
		M-kod	militär	krypterad
L5	1176.45	L5	civil, flyg	öppen

P(Y)-koden är en krypterad signal som används av militära GPS-mottagare. Sverige är i dag ackrediterad användare av P(Y)-kod för militärt bruk. M-kod är en ny krypterad signal som på sikt kommer att ersätta P(Y)-koden för militärt bruk. L5-signalen är primärt tänkt för flygsäkerhetstillämpningar, men mottagare som utnyttjar L5 utvecklas även för masskonsumentmarknaden, och kommer troligen att vara ett viktigt komplement till en civil mottagare för att öka robusthet och noggrannhet.

A.2 GLONASS

GLONASS är ett ryskt system, utvecklat under 1980-talet och driftsatt under 1995. Systemet består för närvarande av 25 (22 i drift) satelliter som sänder samtidigt på tre frekvenser, se Tabell A2. GLONASS använder FDMA-teknik, som innebär att varje satellit sänder en signal på en egen frekvens och totalt finns det 14 frekvenser per signal i systemet.

GLONASS använder L1/G1-signalen för civil användning och L1/G1+L2/G2 för militär användning. L3 är en nyutvecklad signal för civil användning som bygger på CDMA-teknik, såsom övriga GNSS-system.

GLONASS-HS signalen är inte krypterad, och CDMA-sekvensen är inte officiellt publicerad, men har gjorts tillgänglig via akademisk forskning

och används av vissa kommersiella mottagare. Ryssland förbehåller sig rätten att vid behov ändra frekvensen.

Tabell A2, Översikt över GLONASS.

Benämning	Frekvens [MHz]	Signal	Användning	Egenskaper
L1/G1	1602	SP	Civil	Öppen
		HS	militär	Ej beskriven
L2/G2	1246	SP	Civil	Öppen
		HS	militär	Ej beskriven
L3	1201	L3	Civil	Öppen

A.3 BeiDou (fd COMPASS)

Kinesiskt system, utvecklat under 2000-talet och driftsatt i december 2012. Systemet består för närvarande av 27 satelliter (18 i drift) som sänder samtidigt på tre frekvenser, se Tabell A3. BeiDou-systemet använder CDMA-teknik.

Tabell A3, Översikt över BeiDou.

Benämning	Frekvens [MHz]	Signal	Användning	Egenskaper
B1	1561,098/1589,742	B1 GSO, B2 N-GSO	Civil, militär	Öppen + Licensierad (krypterad)
B2	1207,14	B2 GSO, B2 N-GSO	Civil, militär	Öppen + Licensierad (krypterad)
B3	1268,52	B3 GSO, B3 N-GSO	Civil	

A.4 NavIC (fd IRNSS)

Regionalt indiskt system, utvecklat under 2010-talet, den första satelliten sköts upp i september 2010 och den sjunde och sista satelliten april 2016. Systemet består av sju satelliter som sänder samtidigt på två frekvenser, se Tabell A4. NavIC-systemet använder CDMA-teknik.

Tabell A4, Översikt över NavIC.

Benämning	Frekvens [MHz]	Signal	Användning	Egenskaper
L5	1176,45	SPS, PS(RS)	Civil, militär	Öppen + Krypterad
S	2492,028	SPS, PS(RS)	Civil, militär	Öppen + Krypterad

A.5 QZSS

Regionalt japanskt system, utvecklat under 2010-talet, den första satelliten sköts upp i september 2010 och den fjärde satelliten oktober 2017. Systemet beräknas vara i drift 2018. Systemet består av fyra satelliter som sänder på fyra frekvenser samtidigt, se Tabell A5. QZSS-systemet använder CDMA-teknik.

Tabell A5, Översikt över QZSS

Benämning	Frekvens [MHz]	Signal	Användning	Egenskaper
L1	1575.42	C/A, L1C, SAIF	Civil	Öppen
L2	1227.60	L2C	Civil, militär	Öppen + Krypterad
L5	1176.45	L5I, L5Q	Civil	Öppen
E6	1278,75	LEX	Militär?	Krypterad?
S	2 GHz band	Safety	Räddning	

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1290 - oktober 20118 ISBN 978-91-7383-883-2