YTTRANDE
2020-10-14 Dnr I2020/01315

Infrastrukturdepartementet
Malmtorgsgatan 3, 111 51 Stockholm
i.registrator@regeringskansliet.se

Betänkandet SOU 2020:25, Utredningen om ett nationellt biljettsystem för all kollektivtrafik i hela Sverige

Introduktion

Fidesmo är ett teknikföretag som arbetar med integration av säkra chip-baserade applikationer. Vi är idag integrerade till ett flertal EMV baserade system, som Mastercard, det belgiska nationella betalsystemet Bancontact och Visa. Vi arbetar också med andra typer av chipapplikationer, bland annat för kollektivtrafik med den svenska BoB-standarden och den tyska standarden VdV e-Ticket. För passersystem stöder vi HID/Assa Abloys proprietära lösning SEOS.

En chipapplikation är mjukvaran som finns inuti olika typer av enheter, till exempel kort, i en nyckelring eller i en klocka. Chipapplikationen läses kontaktlöst av en läsare, normalt en terminal som finns till exempel vid en ingång till buss eller tunnelbana.

Fidesmo besitter unika kompetenser för kontaktlösa system för betal- (EMV), passersystem och kollektivtrafik. Vi vet hur man bygger säkra, skalbara och kostnadseffektiva system. Vi arbetar idag med några av världens största företag inom området.

Vi kommer i detta yttrande huvudsakligen inrikta våra synpunkter på utredningens förslag kring chip-baserade applikationer där vi anser oss ha en mycket god och unik kunskap om deras fördelar och nackdelar samt de kostnader och ledtider som krävs för att utveckla och designa nya system där chip-baserade applikationer ingår.

Övergripande intryck

I utredningen talar man på ett flertal ställen om att bärare av chip-baserade applikationer kan ges ut av 3:e part, och i utredningens förslag (Alternativ 5, sid 290) pratas om IDF-baserat system i samarbete mellan landets alla RKM. I grunden tycker vi att detta är mycket bra förslag som ger möjligheter till att innovativt, dynamiskt och kostnadseffektivt expandera det nationella biljettsystemet med nya utgivare av identifikatorer, biljettyper och biljettsamarbeten.

Historiskt har det funnits en tanke inom kollektivtrafiken att chip-applikationer finns på kort, och kort ges ut av *kollektivtrafikföretag*. Har man inte ett kort som är utgivet av kollektivtrafikföretaget är man hänvisad till en annan biljettyp baserad på t.ex. optiska koder. Detta är inte rimligt! Skall man ha en öppen, dynamisk lösning där en bärare inte är hårt kopplat till kort, måste det etableras en struktur där man kan använda sig av bärare, oberoende av om det är kort, mobiltelefoner eller andra typer av prylar som taggar, donglar eller klockor, som är utgivna och kontrollerade av 3:e part. Detta är något vi uppfattar som mycket bra, och vi ser stora möjligheter med en sådan struktur.

Vi tycker också att det är bra att utredningen föreslår att kollektivtrafikmyndiheter åläggs en skyldighet att erbjuda sitt produktsortiment för 3:e parts försäljning. Vi tror att detta är ngt som skapar möjligheter för samhället i stort men där individuella kollektivtrafikmyndigheter kan ha svårt att finna resurser att prioritera denna typ av innovationsfrämjande åtgärder.

Det vi dock ser med stor oro kring är hur utredningen tar sig an de tekniska detaljerna kring den omtalade chip-baserade applikationen. Eller om man så vill, standarden för det identifikator-baserade systemet (IDF-baserade systemet). Där bortser man ifrån vad som finns på plats idag, redan implementerat, i produktion och fungerande, och vill ersätta detta med en lösning som inte är definierad, inte säkerställd vad det gäller licenskostnader och utan tydliga tekniska fördelar. Däremot finns en rad nackdelar. Vi kommer i det följande diskutera utredningens föreslagna lösning för IDF-baserade system i förhållande till den existerande lösningen baserad på Samtrafikens BoB-projekt, även kallad MTS7.

Teknisk mognadsgrad på lösning

I utredningen diskuteras fem olika lösningsförslag. Som tidigare nämnts, förordar utredningen ett IDF-baserat system i samarbete mellan landets alla RKM:er. Detta är i mångt och mycket så som BoB är uppbyggt idag, men med den skillnaden att det inom BoB-infrastrukturen inte finns några centrala databaser innehållande alla identifikatorer. Den databasen finns istället hos respektive utgivare av identifierare. Samtrafiken har idag endast en databas över deltagarna i BoB systemet och vissa data kring dessa, tex URL:er och publika nycklar. BoB är alltså uppbyggt med en distribuerad modell, medan det som beskrivs i utredningen är en centraliserad sådan. I ett stycke på sidan 298 i betänkandet nämns kortfattat vissa förutsättningar för distribuerad modell med indelning av sifferföljder (6 och 13 siffror), men hur man tänkt sig denna modell att fungera eller varifrån dessa sifferföljder kommer är inte tydligt och finns inte heller

definierat i det material som vi har fått utlämnat efter begäran till utredningen. Vad har detta för betydelse? Stor ska det visa sig. Speciellt i fallet med ett IDF-baserat system. Det är nämligen så att i ett IDF-baserat system så sker mycket riktigt kopplingen i biljettsystemet till en identifikator, men denna identifikator är kryptografiskt bunden till prylen genom att det också finns en kryptografisk nyckel där. Om denna kryptografiska nyckel inte fanns i chippet, skulle det vara lika enkelt att skapa falska biljetter som i det gamla SMS-baserade biljett systemen. Den enda som kan ansvara för säkerheten av sin identifikator är utgivaren av den, och därmed är också utgivaren av identifikatorn den ende som kan ansvara för databasen av *sina* utgivna identifikatorer.

Något som i samband med detta blir viktigt är då hur den kryptografiska nyckelhanteringen fungerar - dvs vilken part som har hand om vilka nycklar, vilken typ av nycklar de är, hur de hanteras samt hur nycklarna kopplas ihop med olika typer av identifierare, både mänskligt- och maskinellt läsbara.

I BoB-systemet är detta väl genomtänkt, alltifrån de definierade noderna ända ned till vilka identifierare och kryptografiska nycklar som ligger på kortet till hur de olika protokollen interagerar. Att göra om detta till ett centraliserat system kräver arbete, samt tar bort stora delar av den flexibilitet som BoB-arkitekturen medger till *inget* värde. Ett exempel på inflexibilitet som detta skapar är bland annat att Strætó, Islands största kollektivtrafikoperatör, nu inför ett biljettsystem baserat på BoB standarden. Skall de nu ge ut identifierare som hanteras av det svenska IDF-databasen bara för att man skall kunna använda deras kort i svensk kollektivtrafik?

Liknande problem uppstår när man sedan föreslår att själva identifieraren skall baseras på EMV standard istället för MTS7. Detta är ett förslag till förändring där man inte redovisar några skäl för förändringen, och där man visar väldigt lite förståelse för vad man föreslår och implikationer av dessa. Vi kommer i efterföljande stycken diskutera affärsmässiga och legala implikationer av ett val av EMV-teknik istället för MTS7, och här enbart fokusera på den tekniska mognadsgraden.

Fidesmo har i ett flertal projekt med Mastercard, Visa och Bancontact arbetat med olika typer av EMV-applikationer. Det har gjort att vi har en stor insikt i hur dessa system fungerar, och det är tydligt att EMV inte är en standard, utan ett ramverk som man kan bygga nya standarder ovanpå. Även om t.ex. Mastercard och Visa båda använder sig av EMV, har de båda flera olika standarder och implementationer som inte är kompatibla med varandra. I Mastercards fall finns t.ex. två standarder på kortsidan, MChip Advance och MChip Mobile, som båda laddas med olika typer av data och nycklar, och i dessa standarder finns det sedan en uppsjö av olika versioner, som sedan slutligen stöds av olika kortprodukter (tex International Debit, International Credit, Maestro etc). Sedan finns återigen motsvarande komplexitet på läsarsidan (dvs validatorn i ett kollektivtrafik-scenario), där olika "kernels" kan kommunicera med olika standarder på kortsidan, givet att kortapplikationerna har fått rätt data och nycklar. För att ta ett exempel, så använder vi (Fidesmo) i fallet Bancontact en MChip Advance kort-applikation som får Bancontact-specifik data och nycklar för att kunna kommunicera med två olika

Bancontact-kernels på läsarsidan. Utöver detta finns ett flertal proprietära lösningar framtagna av olika korttillverkare som t.ex. Pure från Thales.

Det vi vill belysa i stycket ovan är att det inte är så enkelt som att säga att "vi använder EMV". Man måste också specificera vad man menar med EMV, vilken standard inom EMV, vilken data som används och till vad, hur nyckelhanteringen fungerar och hur denna specifika data underhålls. Detta kommer man *inte* undan bara för att man väljer EMV utan man måste definiera sitt eget system ovanpå EMV. Det finns ingen färdig lösning som man bara kan använda utan att göra och underhålla specifikationer. Nu är det så att detta arbete är redan gjort i BoB samarbetet i och med MTS7, och man kommer alltså att spendera tid och pengar på att definiera något man redan har tillgängligt, med all den osäkerhet som är förknippad med tekniskt specifikations- och implementationsarbete.

Licensiering av teknik

Då utredningen föreslår att det nationella IDF-baserade biljettsystemet baseras på EMV specifikationerna, måste man enligt tidigare diskussion välja *vilken* EMV specifikation man skall basera sin lösning på, och sedan göra ytterligare specificeringar ovanpå detta för att till slut hamna i en ny standard som underhålls av Trafikverket. Här väljer utredningen att föreslå EMV Kernel 5 utan någon ytterligare motivering, och utan att reflektera i vad detta innebär i form av inlåsning, licenskostnader, och möjlighet för mindre parter att delta i utvecklingen av systemet.

EMV Kernel 5 ägs av JCB (Japan Credit Bureau). Här skriver utredningen på sid 349: "Den standard för identifikatorer som utredningen förslår är EMV kernel 5. För att kunna dra nytta av systemet behöver företaget vara beredd att använda den standarden i sin viseringsutrustning. Det innebär inga licenskostnader för kollektivtrafikföretaget." Vad utredningen bygger detta tvärsäkra uttalande på är svårt att utläsa i utredningen, men Fidesmo har begärt ut kompletterande tekniska underlag från utredningen. Där framgår att som underlag för detta påstående finns en beslutsmatris från SL, där de har utvärderat tre olika EMV-alternativ för nästa version av sitt SL Access-kort (dock har inte MTS7 utvärderats!). De utvärderade alternativen är Idemias proprietära variant av EMV kallad Wise, Thales proprietära version Pure, samt Idemias Wise licensierad till en organisation som kallas White Label Alliance (WLA). Valet faller i denna utvärdering på WLA, då de övriga två ger inlåsning till respektive kortleverantör. Ett starkt vägande skäl tycks också vara att SL med detta val kan behålla sin nuvarande kortleverantör utan att göra en ny upphandling.

Vad är då WLA, hur blir man medlem och vad får man för det? Först och främst så finns ingen öppen information om WLA på Internet mer än en pressrelease från 3:e juni 2019. Det gör det svårt att överhuvudtaget diskutera vad som ingår eller inte ingår i medlemskap, vad medlemskap kostar, vilka som behöver vara medlemmar, etc. Vad vi förstår är dock att medlemskap krävs för att få tillgång till standarden (vi vet dock inte hur man blir medlem då ingen information finns om detta), samt att det är medlemskap i WLA som ger licens till EMV Kernel 5 och rätt att ge ut WLA baserade kort. Vi förstår också det som att det krävs en WLA-certifierad chipapplikation (som i dagsläget enbart erbjuds av Idemia vad vi vet). På

kortsidan finns alltså ingen fallback till EMV Kernel 5. De siffror som finns i utredningen på sid 355 om medlemsskap (att endast en part behöver betala ca 50 000 kr) har vi inte kunnat finna belägg för, utan vi har hört betydligt större summor som betydligt fler parter behöver betala. Men det viktiga här är att fakta inte finns på bordet, och att man därför inte har kunnat redovisa vilket underlag man fattar beslut om. Detta visar i sin tur på de enorma osäkerhetsmoment som föreligger med detta förslag.

Om man jämför med MTS7, så är det en helt annorlunda legal kontext. Specifikationen är fullt öppet tillgänglig, vem som helst kan ladda hem den och implementera den utan kostnad. Komplexiteten är också lägre, då det är en specifikation framtagen för det användningsområde som det ämnas användas inom, och inte som EMV som först och främst löser ett komplext problem inom betalningar mellan många parter. Fidesmo har t.ex. också en MTS7-implementation för ett flertal chip från många olika tillverkare.

Vi tror att det kan ta lång tid att lösa vilka som behöver vara medlemmar i WLA för använda sig av specifikationen, att kostnaden för medlemskap i WLA kan vara begränsande för många innovativa företag samt att certifieringskraven på chip kommer att skapa begränsningar i vilka chip som kommer att gå att använda. Sammantaget medför detta att öppenheten minskar och att alla parter, stora som små aktörer, har svårt att delta i utvecklingen av systemet.

Potentiella fördelar med EMV?

Slutligen har i kompletterande tekniskt material som begärts ut från utredningen framförts att ett IDF-baserat system med EMV som grund är lättare att kombinera i viseringsutrustningen om samma viseringsutrustning också skall kunna användas för *tap-and-go* system. Detta är bevisligen möjligt även med en BoB-lösning, då tex Skånetrafiken har implementationer av kombinerade EMV och MTS7 i sin viseringsutrustning.

Det är t.o.m. så, att det i vissa fall skulle kunna var en fördel att inte ha en identifikator implementerad baserat på EMV, då EMV kernels är hårt integrerade i viseringsutrustningen. Till exempel i de fall man har ett kort, klocka eller tagg där det finns både en identifikator samt ett betalkort (Mastercard eller Visa). Då vill man att läsaren först skall läsa identifikatorn för att se om det finns en biljett, och sedan i steg två eventuellt ta betalt via kortet om det saknas biljett. Då skulle t.ex. beloppet som dras också kunna vara bestämt av identifikatorn, genom att den indikerar rabatterat pris eller att en resa är delvis betald.

Vi anser alltså att vi inte har kunnat identifiera några fördelar med EMV men däremot flera fördelar med att basera ett IDF-system på befintliga MTS7.

Legala krav på val av teknik

Slutligen bör ett val av teknik, som innefattar en inlåsning till ett externt ekosystem befattat med kostnader, göras på tekniska meriter och kräver långt mer djupgående utredningar, särskilt om

man avviker från den standard som redan är framtagen. Specifikt så bör man öppet utvärdera vilken EMV standard man i så fall väljer att basera sitt framtida IDF-baserade system på, då de affärsmässiga, legala och tekniska implikationerna kan bli stora för hela ekosystemet.

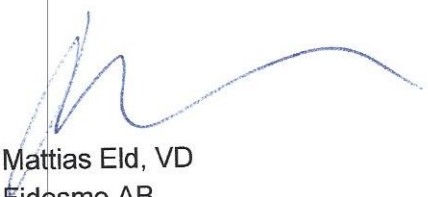
Ställningstagande

Fidesmo avstyrker att det remitterade förslaget läggs till grund för ett genomförande. Vi anser att det teknikval som gjorts i utredning inte baseras på underbyggda fakta, utan endast på en maggropskänsla kring att det borde fungera. Trots att Fidesmo riktat frågor till utredningen och deras konsulter efter teknisk information så har endast knapphändig information gått att få ut. Det finns inget i det tekniska bakgrundsmaterialet som ger något stöd för att det kommer fungerar som antaget.

Vi anser att den jämförelse som gjorts av olika standarder inte är en rättvis jämförelse, utan bör göras om. När kostnader jämförs måste alla kostnader jämföras, hela lösningens livscykelkostnader måste jämföras. Det är elementärt.

Vi anser att utredningens tekniska ben är alldeles för svagt för att kunna användas som bas för de tekniska och affärsmässiga val som har gjorts.

Vi anser att tills annan fakta finns på bordet ska Samtrafikens BoB-standard användas som den gemensamma standarden för kollektivtrafik i Sverige. BoB har den öppenhet och flexibilitet som en modern standard behöver. BoB används redan idag av 7 regionala trafikföretag i Sverige samt inom kort även på Island.



Mattias Eld, VD
Fidesmo AB