E-kronarapport

# E-kronapiloten etapp 4

Mars 2024

S V E R I G E S  R I K S B A N K

# Innehållsförteckning

# Ordlista

**Betalningsinstrument:** En elektronisk enhet som slutanvändaren använder för att betala med, till exempel kort eller mobiltelefon.

**Betalterminal:** Hårdvarulösning där butiken tar emot betalningar från betalinstrument. Point of Sale-terminal (PoS) på engelska.

**CBDC:** Engelsk förkortning för Central Bank Digital Currency. En digital form av centralbankspengar.

**Corda:** DLT-plattform som e-kronapilotens testnätverk är byggt på.

**Corda-nod:** Håller och hanterar plånböcker.

**DLT:** Distributed Ledger Technology - distribuerad lagring av information, exempelvis från en transaktion. Informationen är spridd bland deltagare i ett nätverk i stället för lagrad på en central plats. Medlemmar i nätverket kan vanligtvis läsa och, beroende på behörighet, lägga till information.

**E-krona:** Svensk CBDC tillgänglig för allmänheten.

**E-kronanod:** Del av DLT-plattformen som är utlagd på och drivs av respektive intermediär.

**E-kronamotor:** Nod där intermediärer kan bygga egen affärslogik.

**E-kronanätverk:** Nätverk bestående av Riksbanken och godkända deltagare, så kallade intermediärer, där e-kronor distribueras och används i transaktioner. Nätverket är byggt på en DLT-plattform vid namn Corda.

**Intermediär:** Samlingsnamn för olika former av aktörer som är anslutna till E-kronaplattformen. Juridisk person som har rätt att agera ombud och/eller tillhandhålla tjänster för e-krona.

**NFC:** Engelsk förkortning för Near Field Communication. Teknik som möjliggör trådlös kommunikation mellan enheter som till exempel betalkort och betalterminaler.

**Notarie-nod:** Kontrollerar så att dubbelspendering inte sker.

**Offline:** När kommunikation mellan betalningsinstrument och e-kronanätverk inte är tillgänglig.

**Offlineplånbok:** Finns på betalinstrumentet, exempelvis ett betalkort.

**Onlineplånbok:** Finns i intermediärens nod.

**Plånbok:** Förvaringsutrymme för e-kronainnehav

**Skuggplånbok:** Finns i intermediärens nod och är en spegling av användarens offlineplånbok. Skuggplånboken är förbindelsen mellan offline- och online-plånböckerna.

**Token:** Inom e-kronapiloten en unik identifierbar digital värdeenhet som kan bära värdet av kronor.

**Synkronisering:** En åtgärd för att stämma av data lagrade på betalkortet mot uppgifter lagrade hos intermediären.

# 1 Sammanfattning

I den fjärde etappen har fokus varit att testa och utvärdera om det går att utforma en säker, saldobaserad offlinelösning utifrån förutsättningarna i e-kronapilotens testmiljö. I lösningen reserveras e-kronor för offlineanvändning i en så kallad skuggplånbok i online-systemet. Betalningsinstrumentet i form av ett kort registrerar skuggplånbokens saldo och efterföljande offline-transaktioner. De faktiska e-kronorna som är utgivna av Riksbanken lämnar aldrig online-systemet och byter ägare först då betalningsinstrumenten synkroniseras. Lösningen skiljer sig alltså från den offline-lösning som testades i etapp 2 vilken var token-baserad och innebar att kopior av e-kronorna flyttades till betalningsinstrumentet.

Tre olika användningsfall testades; laddning och återföring av e-kronor till betalningsinstrumentet, offlinebetalning från kort till betalterminal (PoS) samt offlinebetalning mellan två kort. Dessutom testades att införa begränsningar i saldo och antal transaktioner på betalningsinstrumentet. Eftersom korten inte kan kommunicera själva krävs mobiltelefoner och appar som länk. Lösningen utgick från att dessa mobiltelefoner inte kunde anses säkra vilket ställde stora krav på kortens och e-kronasystemets möjlighet att säkra transaktionernas integritet.

Laddning av e-kronor till kortet görs av användaren med hjälp av en mobiltelefonapp ansluten till online-systemet. Laddning av e-kronor på kortet kräver förtroende för intermediärens system och processer då saldot som registreras inte är tekniskt spårbart till de av Riksbanken utgivna e-kronorna.

Betalning till butik gjordes via en mobiltelefon som agerade PoS-terminal. Eftersom åtkomst till terminalens säkra hårdvara saknades implementerades vissa egna säkerhetsfunktioner för att skydda de lagrade transaktionerna.

Betalning mellan användare kräver, med utgångspunkten att mobiltelefonerna är osäkra komponenter, många steg för att kunna betraktas som säkra vilket går ut över användarvänligheten. Detta är en direkt konsekvens av att korten kräver en läsare i form av en mobiltelefon för att kunna kommunicera. Möjligheten att minska antalet steg bedöms som små i denna design.

Betalningar som har gjorts offline behöver synkroniseras för att saldot i offlineplånboken ska motsvara de e-kronor som är reserverade i skuggplånboken i onlinesystemet. Beroende på i vilken ordning användare synkroniserar, kan problem uppstå då likviditet saknas i vissa skuggplånböcker.

Många lärdomar har gjorts under projektet där den viktigaste är att en säker och funktionell offlinelösning kräver mycket utvecklingsarbete både av teknik, regelverk och processer. Slutsatsen är ändå att det med rätt avgränsningar och regelverk skulle kunna vara möjligt att utveckla en säker och användbar offlinelösning.

# 2 E-kronapiloten

Riksbanken har sedan 2017 undersökt möjligheten att ge ut digitala centralbankspengar avsedda för allmänheten, så kallade e-kronor. Sedan 2020 har Riksbanken drivit en e-kronapilot.[1] Arbetet i e-kronapiloten har varit inriktat på att testa olika tekniska lösningar och att parallellt undersöka olika legala aspekter. Syftet har varit att Riksbanken genom praktiskt arbete ska lära sig mer om hur en e-krona skulle kunna fungera. Denna rapport beskriver kortfattat arbetet och slutsatserna från pilotens fjärde och sista etapp där fokus har varit att integrera säkra offlinebetalningar i e-kronans pilotmiljö. Det finns idag inget beslut om att ge ut e-kronor och inte heller om vilken teknik som i så fall skulle användas.

Riksbankens arbete kring e-kronan har efter den fjärde etappen av piloten gått in i en ny fas. Den tekniska piloten avslutades i oktober 2023 och arbetet med att analysera vilka krav som måste ställas på en e-krona och konsekvenserna av att ge ut en sådan samt kommunicera Riksbankens syn på hur en e-krona bör utformas fortsätter. Parallellt med detta följer Riksbanken den internationella utvecklingen. Digitaliseringen kommer att fortsätta både i Sverige och i omvärlden, vilket kommer att kräva nya betalningslösningar. En e-krona kan komma att bli ett viktigt komplement på betalningsmarknaden.

Det e-krona-arbete som denna och tidigare rapporter fokuserat på är det som brukar benämnas som en *retail CBDC*, det vill säga digitala centralbankspengar tillgängliga för allmänheten. Under e-kronapilotens föregående etapper har vi i en testmiljö byggt upp ett e-kronanätverk där e-kronorna distribueras till slutanvändare via av Riksbanken godkända deltagare i nätverket. Vi har därefter vidare testat bland annat hur ett e-kronanätverk skulle kunna integreras med deltagarnas interna system: hur en offlinelösning skulle kunna fungera, hur e-kronan skulle kunna fungera i befintliga betalterminaler och vilken prestanda den testade lösningen har.

Vi har även undersökt hur Riksbanken skulle kunna samverka med aktörer på marknaden när e-kronor ska distribueras till allmänheten. Vidare har vi testat möjligheterna att främja innovation på betalmarknaden, till exempel smartare och effektivare sätt att betala. Pilotens testmiljö har även använts för internationellt samarbete som projektet Icebreaker där vi undersökt om en e-krona kan möjliggöra effektivare och säkrare betalningar mellan länder och CBDC-nätverk.

[1] E-kronapilotens rapporter finns att läsa på hemsidan, https://www.riksbank.se/sv/betalningar--kontanter/e-krona/

I den fjärde etappen har pilotens arbete varit avgränsat till att undersöka:

- Om det går att utforma en saldobaserad offlinelösning utifrån förutsättningarna i e-kronapilotens testmiljö och analysera hur säker den kan bli.
- Säkerheten i en offlinelösning baserad på ett för e-kronan specifikt betalkort och en betalterminal för butik.
- Möjligheten att använda den befintliga EMV-standarden[2] som är global standard för debet- och kreditkort.

[2] EMV är den standard som togs fram av Europay, Mastercard och Visa. Standarden hanteras idag av EMVco som består av American Express, Discover, JCB, Mastercard, UnionPay och Visa.

# 3 Säkra offlinebetalningar

Den saldobaserade lösning som utvecklats i den fjärde etappen av e-kronapiloten visar att offlinebetalningar går att genomföra men att det finns utmaningar med säkerheten när det gäller exempelvis person till person-betalningar. Det kan också uppstå problem med likvida medel när flera betalningar görs efter varandra utan att synkroniseras. Med begränsningar i antalet transaktioner eller ett maxbelopp kan riskerna minskas men det återstår att finna en lösning som gör att dessa kan ändras utan att man behöver distribuera ut nya kort.

## 3.1 Mål och förutsättningar

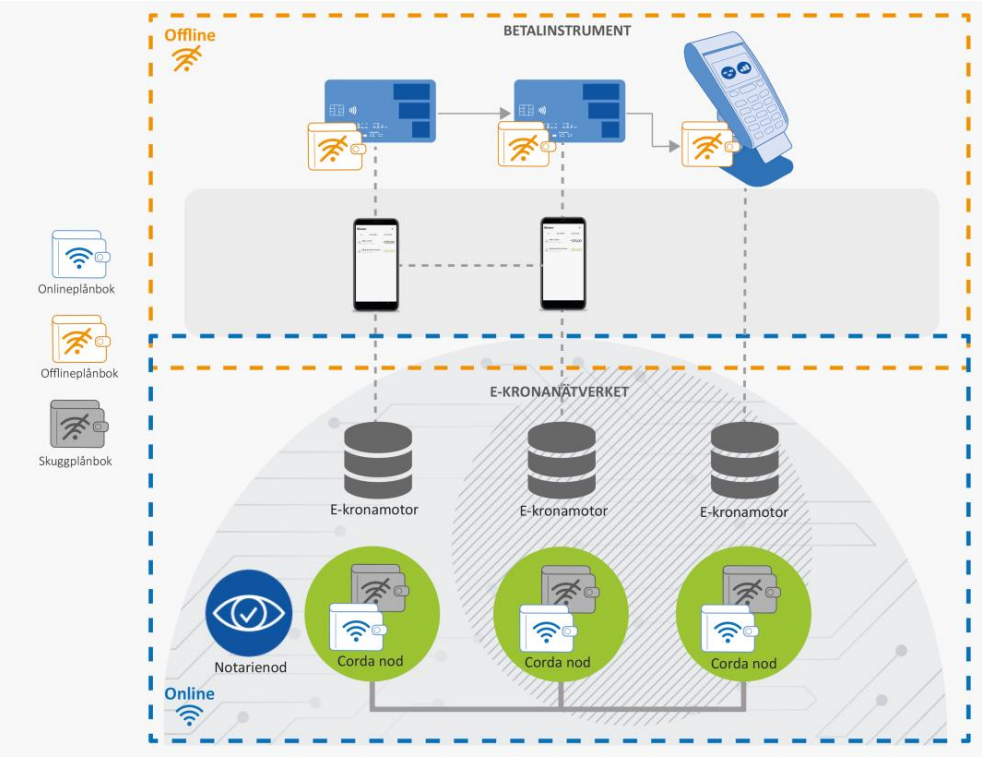
Riksbankens mål med etapp fyra har varit att utforma en säker offlinelösning med e-kronapilotens förutsättningar och sedan testa och utvärdera denna. Vi har alltså utnyttjat den pilotmiljö för e-krona och betalinstrument som tidigare utvecklats. Dessutom undersöktes om det var teoretiskt möjligt att nyttja EMV-standarden som används globalt för debet- och kreditkort eftersom den är beprövad och fungerar väl.

E-kronapiloten har utvecklats på en DLT-baserad systemlösning byggd på plattformen Corda. Riksbanken och intermediärerna ingår i ett isolerat testnätverk med egna noder. För att e-kronan ska fungera offline behövs ett betalinstrument som inte är beroende av kontinuerlig kommunikation med e-krona-systemet. I den här etappen har betalkort och mobilappar vidareutvecklats för att detta skulle vara möjligt. På betalkortet har det implementerats en så kallad *Store value-lösning* där saldo för offline-användning sparas.

Vi har också undersökt om det skulle vara möjligt att erbjuda offlinebetalningar där man endast använder mobiltelefon. Detta var dock inte möjligt då vår bedömning är att det inte gick att uppnå tillräcklig säkerhet. Vi valde därför att basera offlinelösningen enbart på kort.

## 3.2 Övergripande design

I denna etapp valde vi att återanvända den tidigare utvecklade pilotmiljön för e-krona med oförändrade roller för Riksbanken och intermediärerna.




*Figur 1. Övergripande design*

Även här ansvarar Riksbanken för en notarienod där e-kronatransaktioner verifieras och avvecklas. Intermediärerna förser användare och handlare med e-kronaplånböcker, betalningsinstrument och betalterminaler. Användarna ska kunna genomföra transaktioner med andra användare och betala hos handlare även när e-kronanätverket inte är tillgängligt, det vill säga offline.

Med dessa grundförutsättningar utformade vi en offlinelösning baserad på betalkort och undersökte hur säker den var. De kort som användes var samma kort som använts under tidigare etapper av piloten.[3]

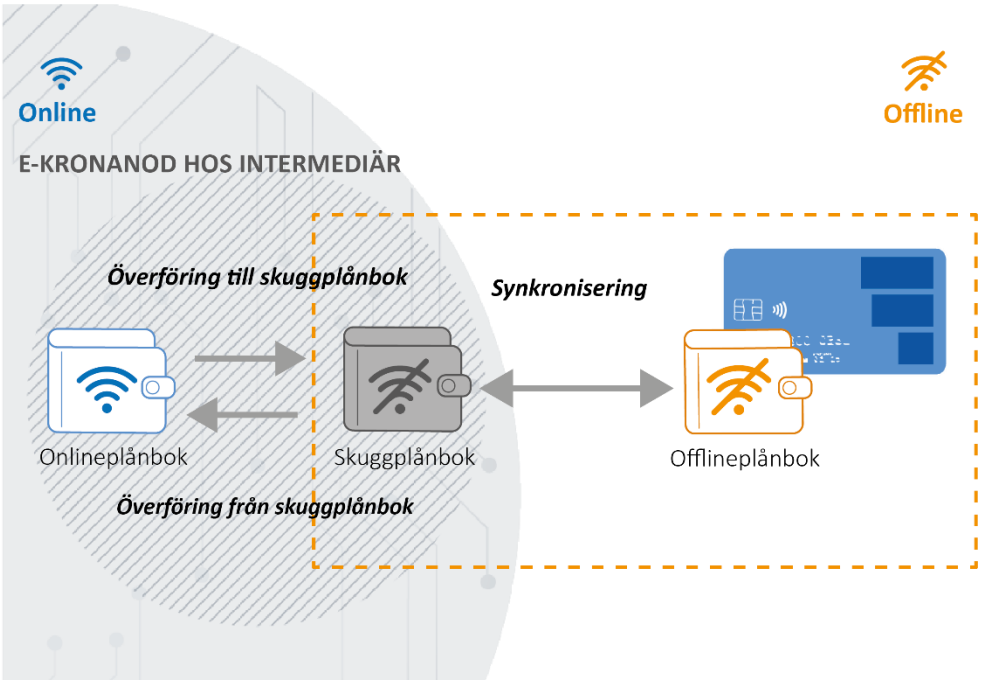
Skillnaden jämfört med den tidigare offlinelösningen är att under etapp två baserades lösningen på tokens med transaktionskedjor som lagrades på en Android mobiltelefon. I etapp fyra så lagras istället endast saldo och offlinetransaktioner på slutanvändarens betalkort eller i handlarens betalterminal. Betalningsinstrumentet som sparar saldo och offlinetransaktioner kallar vi för offlineplånbok. I båda lösningarna, etapp två och etapp fyra, behöver varje användare en extra plånbokstyp för att hantera off-

[3] "Dual-interface" med "NXP P71 Secure Element chip" och operativsystemet "JavaCard JCOP4".

linebetalningar. I etapp fyra kallar vi denna plånbok skuggplånbok, se Figur 2. Det innebär att varje användare har två plånböcker i intermediärens Corda-nod, skuggplånboken och den vanliga onlineplånboken.

Skuggplånböckerna används för att hantera användarnas offlinetransaktioner. Till exempel:

- När användaren vill fylla på eller tömma sina reserverade e-kronor för offlinetransaktioner.
- När offlineplånböckerna ska synkronisera alla offlinetransaktioner.




*Figur 2. Varje användare har en egen onlineplånbok, skuggplånbok och offlineplånbok.*

## Säkerhetsdesign

Lösningen bygger på hantering av saldo och transaktioner på ett kort, så kallad Stored Value Card. Certifikat och olika räknare är införda för att öka säkerheten. Syftet har varit att se hur en säker lösning för offlinebetalningar kan se ut.

Designen och lösningen förlitar sig på att intermediärernas system (e-kronamotorer) och kort har ett starkt skydd och att administratörerna hanterar systemen korrekt. Designen utgår också från att PoS-terminaler och mobiltelefoner som används för offlinebetalningar är osäkra och även kan vara hackade. För att betalningsinstrumenten, det vill säga korten, ska lita på instruktioner från intermediärerna och för att intermediärerna ska lita på meddelanden från betalningsinstrumenten används digitala certifikat. Certifikaten var i detta fall självsignerade men för att uppnå hög säkerhet i en produktionssatt lösning behövs en betrodd och verifierad PKI, *Public Key Infrastructure*, eller motsvarande som utgivning, signering och kryptering kan knytas till.

Förutom digitala certifikat använder betalningsinstrument och e-kronamotorer flera olika räknare för att säkerställa att offlinebetalningarna är synkroniserade och att instruktionerna till och från kortet inte redan har hanterats. Här finns också skydd mot återuppspelningsattacker ”*replay attack*”, där samma e-kronor används flera gånger. Varje transaktion har även ett unikt nummer som sparas i intermediärernas e-kronamotorer.

## 3.3 Limiter och begränsningar

I en offlinelösning kan det vara nödvändigt att införa begränsningar för hur många och hur stora betalningar som kan accepteras offline. Skälen kan vara att minska risker och försvåra penningtvätt och bedrägerier. Om man inför begränsningar så behöver slutanvändarna gå online oftare för att synkronisera offlineplånbokens transaktioner, vilket också bidrar till att intermediärerna lättare kan se vilka kunder som har pengar offline och hur mycket. När synkroniseringen är gjord nollställs kortets räknare och nya offlinetransaktioner kan göras.

I syfte att utvärdera hur begränsingar för offlineanvändning av e-kronor kan implementeras införde vi följande regler:

- Betalkort kan genomföra maximalt fem transaktioner offline.
- Saldot på ett kort får aldrig överstiga 3 000 kronor.
- En betalterminal kan ta emot maximalt tolv transaktioner offline.
- Summan av mottagna pengar på en betalterminal får aldrig överstiga 20 000 kronor.
- Pengar som har tagits emot av betalterminaler i offlineläge kan inte användas för nya offlinebetalningar.

Begränsningarna är implementerade direkt i programkoden på kortet och inte som separata konfigurationer. Detta gjorde det enkelt att införa begränsningarna men nackdelen är att det i stället kan vara svårt att vid behov ändra dem efterhand.

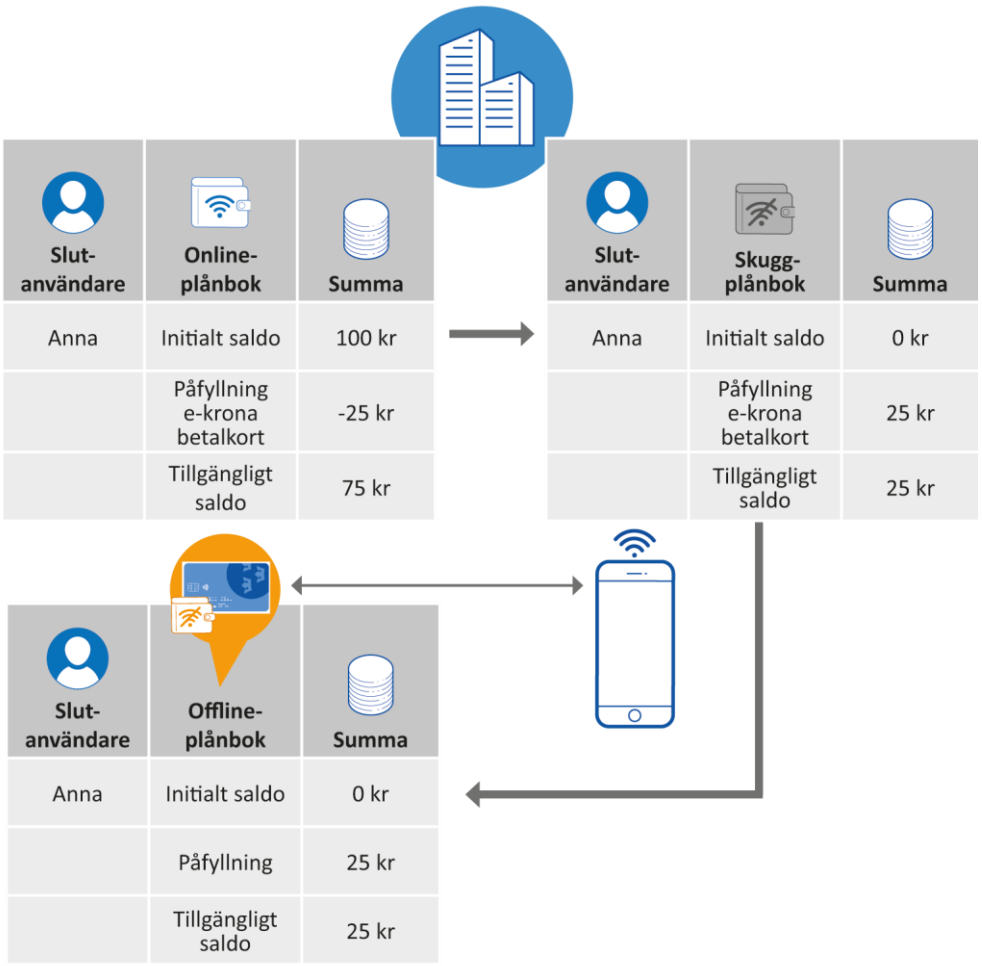
**Lärdomar om limiter och begränsningar**

Det är fullt möjligt att införa begränsningar på betalkort. Med säkerhetsfunktioner på korten, exempelvis *write once,* kan man sätta och göra begränsningarna permanenta. Nackdelen är då att man behöver distribuera nya kort om man vill ändra begränsningarna.

Det kan också bli en pedagogisk utmaning att förklara för slutanvändare hur limiter och begränsningar fungerar i praktiken och hur de i vissa fall kan stoppa en betalning. Till exempel kan en betalare ha utrymme kvar för att genomföra en betalning offline, samtidigt som betalterminalen ligger nära sin limit för att kunna ta emot betalningen. Då skulle betalningen inte kunna genomföras trots att betalaren har möjlighet.

## 3.4 Överföringar mellan onlineplånbok och betalningsinstrument för offline

När användare får sitt kort för offlinebetalningar så finns det inga pengar på kortet. För att kunna använda kortet offline behöver användaren fylla på kortet med pengar från onlineplånboken.



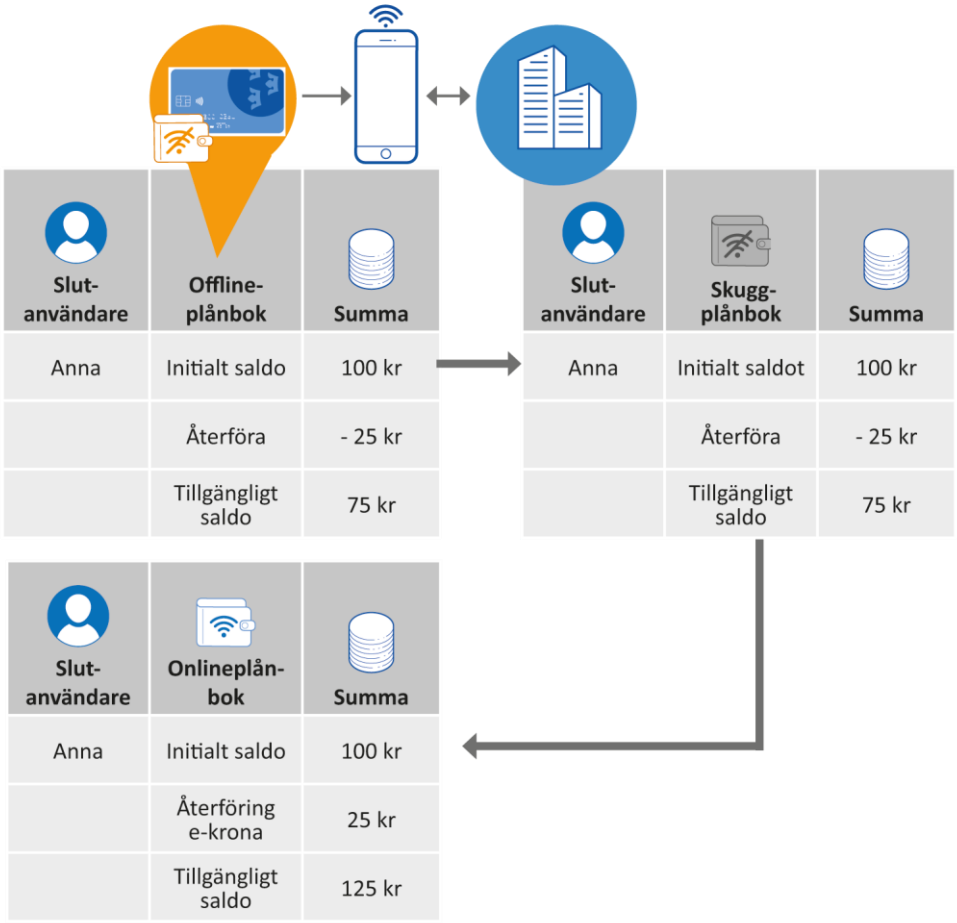

*Figur 3. Användare laddar sitt kort för offlinebetalningar*

Påfyllningen av betalkortet går till så här:

1. Användaren öppnar sin e-kronaapp i mobiltelefonen och skriver in beloppet som ska överföras.
2. Användaren skriver in e-kronaappens PIN-kod och för kortet till mobiltelefonens NFC-läsare.
3. Mobiltelefonen skapar en digitalt signerad förfrågan som skickas till intermediärens e-kronanod.
4. Intermediären verifierar den digitala signaturen och för över beloppet från användarens onlineplånbok till användarens skuggplånbok.

5. Intermediären läser av det uppdaterade saldot på användarens skuggplånbok, signerar saldovärdet och sänder det signerade saldovärdet till användarens e-kronaapp.
6. Användaren håller kvar kortet mot mobiltelefonens NFC-läsare och användarens e-kronaapp sänder över det uppdaterade saldovärdet till kortet.
7. Kortet ändrar sitt saldo till det uppdaterade saldovärdet.

Användaren kan även tömma kortet på valfritt belopp, se Figur 4. Innan kortet kan tömmas så behöver alla offlinetransaktioner vara synkroniserade.




*Figur 4. Användare minskar sitt belopp för offlinebetalningar*

Så här gör den slutanvändaren som vill minska sitt innehav av pengar som kan användas offline:

1. Användaren öppnar sin e-kronaapp i mobiltelefonen och skriver in beloppet som ska återföras.
2. Användaren skriver in kortets pin-kod i e-kronaappen och för kortet till mobiltelefonens NFC-läsare.
3. Kortet verifierar PIN och sänder över en engångskod till e-kronaappen.
4. E-kronaappen sänder förfrågan till intermediären om att återföra innehav. Intermediären verifierar att beloppet finns på användarens skuggplånbok.

5. Intermediären räknar ut vad det kommande saldot på skuggplånboken kommer att bli efter minskningen och skickar detta saldovärde digitalt signerat tillbaka till e-kronaappen.
6. Användaren håller kvar kortet mot mobiltelefonens NFC-läsare och e-kronaappen sänder över det signerade saldovärdet till kortet.
7. Kortet verifierar signaturen och uppdaterar saldot på kortet.
8. Kortet sänder tillbaka en bekräftelse till e-kronaappen, digitalt signerad av kortet, att saldot är uppdaterat.
9. E-kronaappen sänder denna information vidare till intermediären.
10. Intermediären verifierar kortets signatur och för över beloppet från användarens skuggplånbok till onlineplånboken.

**Lärdomar om överföringar mellan onlineplånbok och betalinstrument för offline**

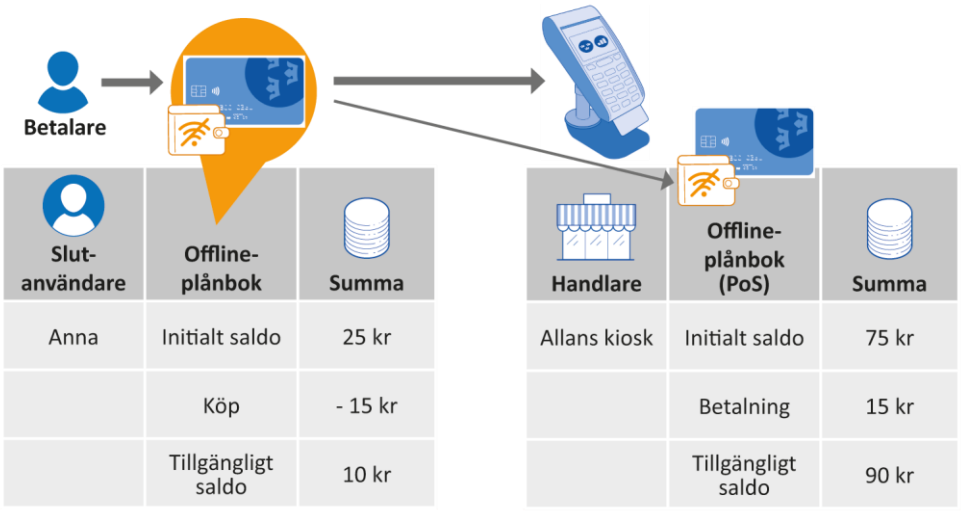
Intermediärerna har en skuggplånbok för varje användare för att kunna skilja ut vilka e-kronor som är tillgängliga för transaktioner offline från de som kan användas online. Det är viktigt för intermediärerna att ha information om mängden e-kronor i samtliga offlineplånböcker, dels för att hantera risker men också i det fall som begränsningar eller avgifter har införts för e-kronainnehav. Varje intermediär kan räkna ut hur många e-kronor som deras kunder har avsatt för offline. Det är dock viktigt att poängtera att de transaktioner som sker offline mellan användare hos olika intermediärer förblir okända tills samtliga utestående offlinetransaktioner har registrerats online.

En svårighet som behöver hanteras är skuggplånböckernas integritet. Saldot på offlineplånboken, det vill säga betalinstrumentet för offline, sätts av intermediärens system. Det behöver därför finnas en kontrollfunktion som säkerställer att det saldo som intermediären registrerar på offlineplånboken avspeglar saldot på skuggplånboken. I annat fall skulle intermediären kunna skapa pengar som inte finns i onlinesystemet.

## 3.5 Offlinebetalningar till butik

Vi har också testat och utvärderat hur en användare med offlineplånbok kan göra offlinebetalningar hos handlare. Vi använde en lösning för detta som byggde vidare på den betalterminal, så kallad *Point of Sale*, som användes i etapp två. Som PoS-terminal användes en Android-lösning som gjorde det möjligt att använda en vanlig Android-telefon som Point of Sale. PoS-terminalen behöver kunna spara offlinetransaktioner på ett säkert sätt. Riksbanken hade dock inte möjlighet att använda mobiltelefonens säkra del för lagring och exekvering, *Trusted Execution Environment*, utan behövde utveckla en egen lösning som kan skydda betalningar från insyn.

Datakommunikationen mellan betalkort och PoS-terminal använde *Near Field Communication* (NFC).




*Figur 5. Användare gör en offlinebetalning i butik*

Följande steg utförs när en användare gör en offlinebetalning till betalterminalen hos en handlare:

1. Handlaren startar betalningen genom att skapa en betalningsförfrågan, *Request to Pay*.
2. PoS-terminalen visar belopp och uppmanar kunden till kontaktlös betalning med PIN-kod.
3. Kunden matar in betalkortets PIN-kod och för betalkortet till PoS-terminalen.
4. Kortet verifierar PIN-koden, drar av beloppet från kortets saldo och skapar en digitalt signerad offline-transaktion som innehåller betalare, betalningsmottagare och belopp.
5. Förutom att kortet sparar den digitalt signerade offlinetransaktionen så sänds den även till PoS-terminalen.
6. PoS-terminalen verifierar signaturen och sparar den digitalt signerade offline-transaktionen.
7. PoS-terminalen visar en bekräftelse på att transaktionen är mottagen och registrerad.

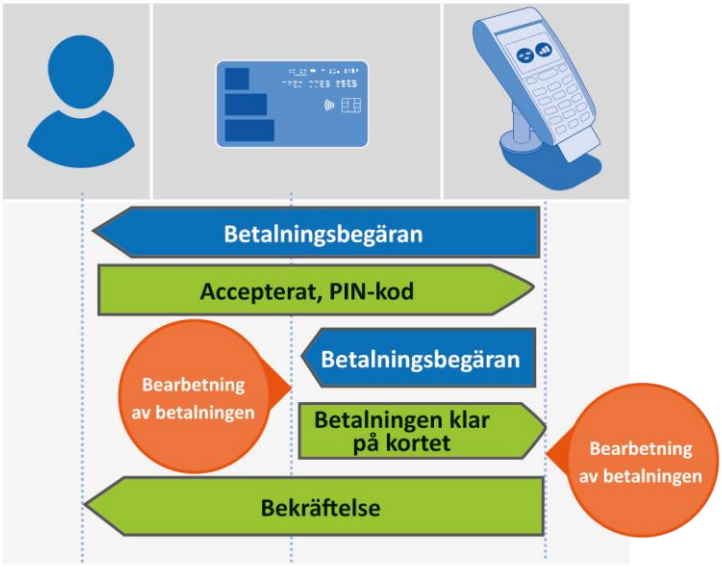
Offlinetransaktionerna som sparas i PoS-terminalen kan inte manipuleras utan att det upptäcks vid kontroll i och med att de är digitalt signerade. Utan offline-plånböckernas privata nycklar kan de inte ändras. Det är även viktigt att hindra utomstående från att se de sparade offlinetransaktionerna. PoS-terminalen, som är en Android-app, skapar en egen krypteringsnyckel och offlinetransaktionerna krypteras innan de sparas. Hantering av nyckel och kryptering i PoS-terminalen tillhandahålls av Androids egen KeyStore-funktion.

### Lärdomar om offlinebetalningar till butik

Vi kan konstatera att det med en PoS-terminal går att ta emot betalningar offline med de limiter vi har använt under etapp fyra. PoS-terminalen kan spara betalningsinform-

ation krypterat, utan att vi har tillgång till mobiltelefonens säkra del för lagring och exekvering, *Trusted Execution Environment*. Vi har dock inte helt verifierat vilken nivå av säkerhet som behövs för att transaktionen inte ska kunna manipuleras.

En viktig observation är att betalningen sker i två separata steg. I det första steget registreras offlinetransaktionen på betalarens kort. I det andra steget tar betalterminalen emot offlinetransaktionen och först då är transaktionen slutförd.




*Figur 6. Betalning från användare till PoS-terminal*

Det kan dock uppstå fel mellan de två stegen, som till exempel att kortet har utfört transaktionen och uppdaterat saldot men att PoS-terminalen inte tar emot någon transaktion eller av annan anledning inte behandlar den. Resultatet blir då att pengar har dragits från slutanvändarens kort, men eftersom att handlaren inte kan se det kommer kunden inte att få sina varor. Det är en problematisk situation; kunden har ”förlorat” pengar. Om kunden skulle synkronisera sina lagrade offlinebetalningar på kortet skulle handlaren få pengar insatta på sin skuggplånbok men kunden har inte fått något för pengarna.

En lösning som minskar risken för en sådan situation implementerades därför. En funktion infördes som gör att den sista offlinetransaktionen på ett kort vid behov kan skickas på nytt. Ingen ny transaktion registreras på kortet och saldot ändras inte heller men betalningsmottagaren får informationen att betalningen är genomförd.

Det är viktigt att varje transaktion initieras av mottagaren för att överföringar inte ska kunna ske om inte mottagaren har begärt det. Designen är också sådan att all kommunikation mellan kortet och PoS-terminalen kan ske i en följd utan att kortet behöver ”blippas” flera gånger till skillnad fram lösningen i etapp två.

Däremot signerar PoS-terminalen inte betalningsförfrågningar, något som skulle kunna öka säkerheten. Om betalningsmottagaren har signerat en betalningsförfrågan

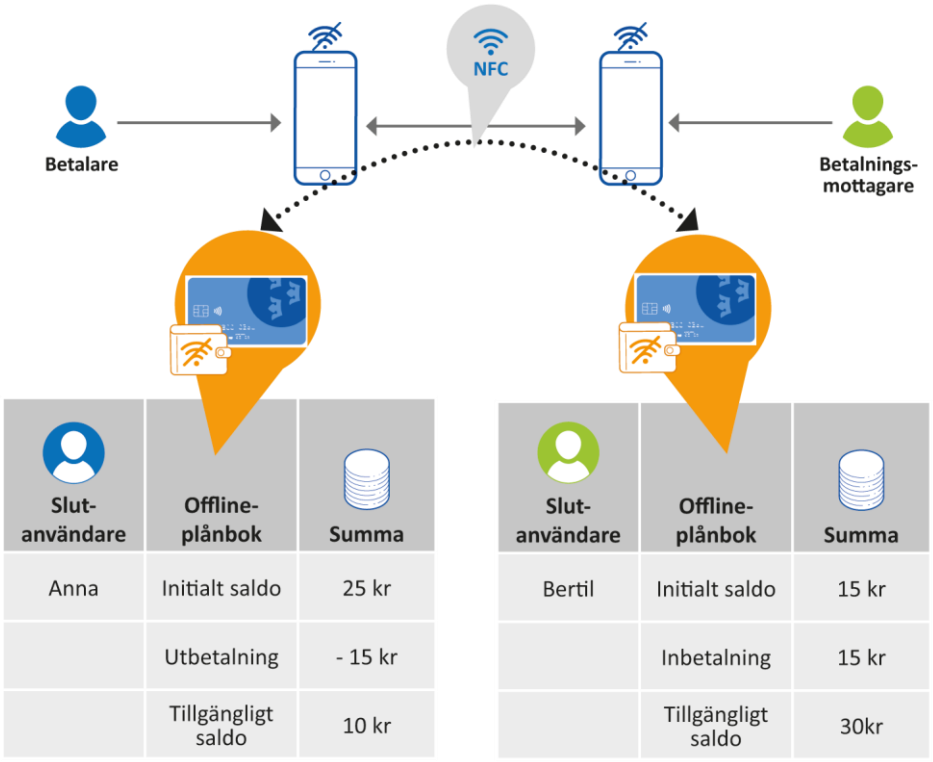
kan kortet verifiera betalningsmottagaren och transaktionen som sparas på kortet är då signerad av båda parter. Det säkerställer för betalaren att betalningsmottagaren är den som den utger sig för att vara.

Under etapp fyra använde vi räknare i kortet för att hålla reda på utförda transaktioner och synkroniseringar. Vi valde medvetet att implementera räknare som säkerhetsfunktion för att förhindra manipulation av lagrade betalningar och för att stoppa möjligheten att återupprepa betalningar för att skapa pengar men minsta fel i dessa räknare gör att offlinetransaktioner och synkroniseringar inte utförs. En viktig obesvarad fråga är också hur befintliga PoS-terminaler behöver anpassas eller bytas ut för att kunna ta emot offlinebetalningar med e-kronor.

## 3.6 Offlinetransaktioner mellan användare

När en användare vill göra en offlinetransaktion till en annan användare behövs en design som är användarvänlig utan att brista i säkerhet. För säker lagring och programexekvering av offlinetransaktioner har vi använt ett betalkort. För att användaren ska kunna hantera sitt kort finns en mobilapp. Den design som valdes liknar kortbetalningar i butik.

Målet var att värde, på ett mycket säkert sätt, ska föras över från betalarens offlineplånbok till betalningsmottagarens. Utgångspunkten för designen var att betalare och betalningsmottagare inte litar på den andres mobiltelefon. Interaktionen och transaktionen skulle ske genom kontaktlös överföring.




*Figur 7. Offline-transaktion mellan två användare*

Så här går en offline-transaktion mellan två användare till:

1. Betalningsmottagaren väljer ett belopp i sin e-kronaapp och för sitt kort till sin mobiltelefon. Kortet läser av beloppet och skapar en digitalt signerad betalningsförfrågan som skickas tillbaka till betalningsmottagarens mobiltelefon.
2. Betalningsmottagaren och betalaren för ihop sina mobiltelefoner och den signerade betalningsförfrågan skickas över till betalarens mobiltelefon.
3. Betalaren ser betalningsförfrågan och godkänner den genom att mata in kortets PIN-kod för att sedan föra sitt kort till sin mobiltelefon. Mobiltelefonen skickar över PIN och betalningsförfrågan som är signerad av betalningsmottagaren till kortet. Kortet verifierar PIN, minskar sitt saldo med beloppet i betalningsförfrågan och signerar i sin tur betalningsförfrågan och skickar tillbaka den till mobiltelefonen.
4. Betalare och betalningsmottagare för återigen ihop sina mobiltelefoner och betalningsförfrågan som nu är signerad av båda korten förs över till betalningsmottagaren.
5. Betalningsmottagaren accepterar betalningen genom att mata in PIN-koden till sitt kort för att sedan föra sitt kort till sin mobiltelefon. Mobiltelefonen skickar över PIN och betalningsförfrågan till kortet. Kortet verifierar PIN och signaturer för att därefter öka sitt saldo med beloppet i betalningsförfrågan. Flödet avslutas med att kortet återrapporterar till betalningsmottagarens mobiltelefon att transaktionen lyckades.

**Lärdomar om offlinetransaktioner mellan användare**

Den säkra designen innebär att både betalare och betalningsmottagare måste gå igenom många olika steg och detta minskar användarvänligheten. Både betalningsmottagare och betalare behöver dessutom digitalt visa att de äger sina offlineplånböcker via sina respektive signeringar.

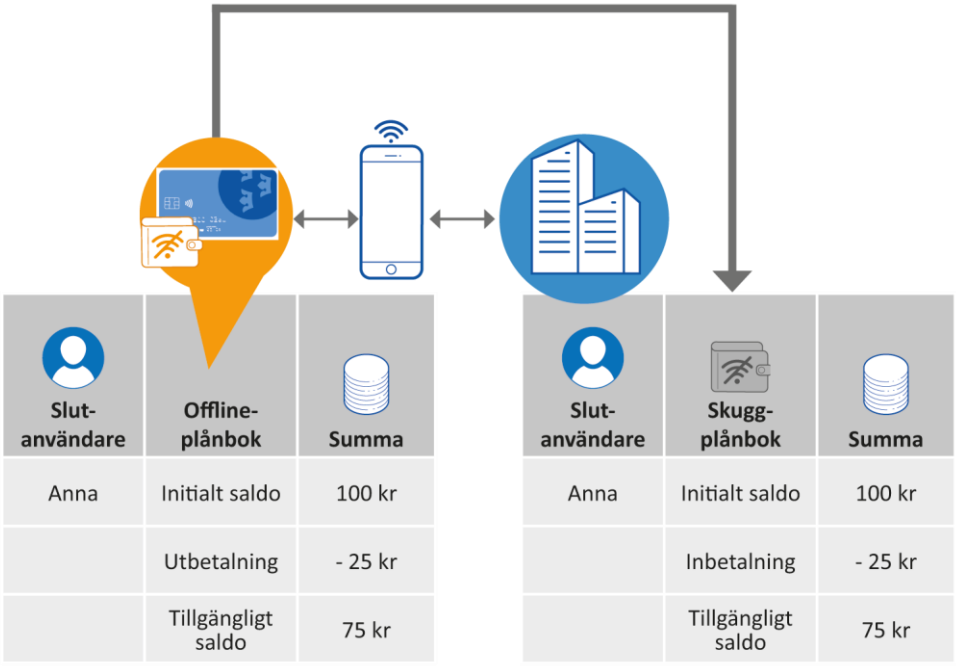
Det måste också vara möjligt att hantera offlinetransaktioner i de fall där betalningsmottagare väljer att avbryta och inte tar emot en offlinetransaktion som betalningsmottagaren har påbörjat. I den här lösningen har vi valt att inkludera olika räknare i programvaran på betalkortet som håller reda på transaktionerna. Varje påbörjad transaktion räknas för att förhindra att samma betalning registreras två gånger. Men eftersom vi har satt en begränsning om fem offlinetransaktioner så skulle flera utestående betalningar helt enkelt stoppa ytterligare offlinebetalningar.

## 3.7 Synkronisering av sparade offlinetransaktioner

Om PoS-terminalen eller kortet har sparade offlinebetalningar så behöver de synkroniseras. Tanken med synkroniseringen är

- att kunna nollställa räknare och tillåta nya offlinetransaktioner
- att kunna läsa av aktuellt saldo på kortet
- att kunna registrera och avveckla offlinetransaktioner
- att kunna identifiera avvikelser som till exempel dubbelspendering eller skapande av pengar.

Flödena för kort och PoS är mycket lika men på några punkter skiljer de sig åt.




*Figur 8. Registrering av utestående offlinetransaktioner (synkronisering)*

Synkronisering av offlinetransaktioner behöver utföras i flera steg. En modell är att låta synkroniseringen starta automatiskt varje gång som användaren läser av kortets saldo när mobiltelefonen är online. Men för att det skulle bli enkelt att testa lösningen valde vi i stället en design där slutanvändaren själv initierar en synkronisering:

1. Slutanvändaren väljer i sin e-kronaapp att hantera sitt kort och matar in kortets PIN-kod för att sedan föra sitt kort till mobiltelefonen.
2. PIN-koden förs över till kortet som verifierar den. Om kortet har sparade offlinetransaktioner så skickas de till mobiltelefonen. För PoS-terminalen kan appen läsa transaktionerna direkt från databasen.
3. Mobiltelefonen skickar transaktionerna vidare till intermediären.
4. Intermediären verifierar transaktionerna. Intermediären utför varje transaktion som den inte tidigare har haft kännedom om genom att flytta e-kronor från betalarens skuggplånbok till betalningsmottagarens skuggplånbok.

5. Intermediären läser av det uppdaterade saldot på användarens skuggplånbok, signerar saldovärdet och sänder det till användarens e-kronaapp.
6. Användaren håller kvar kortet mot mobiltelefonens NFC-läsare och användarens e-kronaapp sänder över det uppdaterade saldovärdet till kortet.
7. Kortet ändrar sitt saldo till det uppdaterade saldovärdet och nollställer räknaren för offlinetransaktioner samt raderar sparade offlinetransaktioner.

**Avveckling av offlinebetalningar**

Betalningar mellan betalare och betalningsmottagare i offlinelösningen är inte slutligt avvecklade förrän de synkroniserats mot skuggplånböckerna i onlinesystemet. Alla offline-transaktioner finns alltid registrerade i båda betalningsinstrumenten. Detta innebär att avveckling sker när det första betalningsinstrumentet synkroniserar. När det andra betalningsinstrumentet synkroniserar sker en kontroll först om den aktuella transaktionen redan har avvecklats. Om så är fallet görs ingen ytterligare åtgärd. Detta för att en betalning inte ska utföras dubbelt när både betalare och betalningsmottagare synkroniserar sina offlinebetalningar.

När betalare och betalningsmottagare finns hos samma intermediär så kan överföringen göras direkt mellan de två skuggplånböckerna oavsett vem som synkroniserar först. Om betalare och betalningsmottagare finns hos olika intermediärer så behöver i vissa fall en begäran om betalning skickas mellan intermediärerna enligt följande:

Om det är PoS-terminalen som synkroniseras så behöver intermediären göra en förfrågan om betalning från betalarens skuggplånbok till handlarens skuggplånbok. Om det är en transaktion med ett kort kontrolleras om offlinebetalningen som ska synkroniseras är från eller till kortet. Om den är till kortet så fungerar det på samma sätt som för PoS-terminalen och om betalningen är från kortet utför intermediären en vanlig överföring från kortets skuggplånbok till mottagarens skuggplånbok.

Förfrågan om betalning sker genom att betalningsmottagarens intermediär skickar överföringsförfrågan till betalarens intermediär som utan verifikation skickar över det förfrågade beloppet. Hela flödet är mycket förenklat i e-kronapiloten och för att det ska fungera i verkligheten behöver de olika intermediärernas e-krona-motorer kunna skicka meddelanden till varandra.

När alla offlinebetalningar är synkroniserade skickar intermediären tillbaka ett signerat återställningsmeddelande så att kortet eller PoS-terminalen vet att transaktionerna har blivit synkroniserade och att eventuella begränsningar kan återställas.

**Lärdomar om synkronisering av lagrade offlinetransaktioner**

Att genomföra synkronisering innebär att

- läsa av sparade offlinetransaktioner och uppdatera e-kronanätverkets skuggplånböcker
- återställa kortets transaktionsräknare så att det kan genomföras nya offlinetransaktioner

- uppdatera kortets saldo så att det avspeglar skuggplånbokens uppdaterade saldo.

Det kan uppstå kommunikationsfel på flera ställen eftersom synkroniseringen är helt beroende av att en mobiltelefon förmedlar information mellan kort och intermediär. Detta kan innebära att uppdateringen sker på ett ställe men inte på ett annat, till exempel att skuggplånboken uppdateras men inte betalkortet.

Under designarbetet diskuterades möjligheten att införa återkoppling från offlineplånboken till intermediären för att säkerställa att uppdateringen är utförd. Detta skulle dock inte hjälpa i fall kommunikationen bryts i det sista steget för då behöver intermediären hantera denna situation i stället.

Andra problem som kan uppstå vid synkroniseringen är följande:

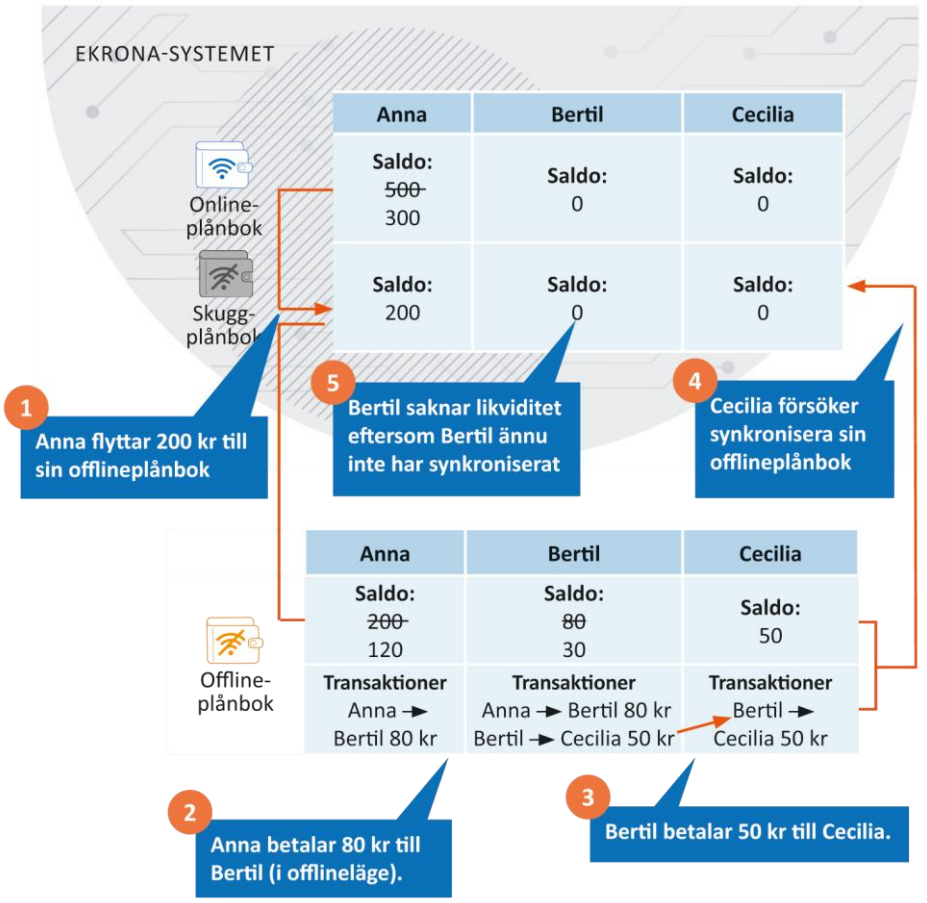
- Kortet blir inte synkroniserat och därmed nollställs inte transaktionsräknaren så att nya offlinetransaktioner blir möjliga.
- De räknare som finns på kortet och motsvarande räknare hos intermediären skiljer sig på ett sätt som inte är förväntat. Därmed blir kortet obrukbart.
- En offlinetransaktion på kortet avvisas av intermediären.

Vissa av problemen borde kunna lösas genom att man synkroniserar kortet igen eller genom att man fyller på kortet med mer pengar. Då skulle saldot och räknaren uppdateras.

**Likviditetsproblem vid synkronisering**

Under analys och design av lösningen upptäckte vi att det kan uppstå en situation där det saknas likviditet i en betalares skuggplånbok.

Situationen uppstår när flera användare i följd gör transaktioner och ingen går online.




*Figur 9. Likviditetsproblem vid synkronisering*

Exempel: Anna för över 200 kronor till sin offlineplånbok (1) och har därmed ett saldo om 200 kronor även på skuggplånboken. I offlineläge betalar Anna 80 kronor till Bertil (2) som sedan i sin tur betalar 50 kronor till Cecilia (3). Nu har Anna 120 kronor i sin offlineplånbok medan Bertil har 30 kronor och Cecilia har 50 kronor. Annas skuggplånbok innehåller fortfarande 200 kronor medan Bertils och Cecilias är tomma eftersom ingen synkronisering har gjorts ännu. Om Cecilia går online för att synkronisera (4) uppstår problem då de 50 kronor som Cecilia har fått från Bertil inte kan flyttas från Bertils skuggplånbok (5) eftersom saldot där är 0. Om Anna eller Bertil har synkroniserat före Cecilia så kommer det däremot att finnas likviditet för transaktionen.

Riksbanken har undersökt hur man skulle kunna lösa detta problem. En möjlighet är att centralbanken tillhandahåller en likviditetspool för betalningarna, en annan att införa begränsningar för hur pengar får användas offline, exempelvis att pengar mottagna i offlineläge inte kan användas för offlinebetalningar innan betalningsinstrumentet är synkroniserat. Riksbanken har dock inte gjort några djupare analyser av dessa möjliga lösningar och kan därför inte säga vad som är genomförbart.

## 3.8 Lärdomar om säkerhetsdesign

Under etappens gång har ett antal insikter dykt upp som skulle behöva undersökas och hanteras vidare. Nedan följer ett urval:

- Instruktioner och betalningar till kort är inte unikt adresserade vilket blir ett säkerhetsproblem. På grund av detta kan till exempel laddning av korten återuppspelas i en så kallas replay attack.
- En offlinebetalning skulle kunna utföras dubbelt om betalaren och betalningsmottagaren synkroniserade exakt samtidigt. Vid denna så kallade *race condition* söker båda intermediärerna i sina databaser efter transaktionsnumret samtidigt och båda utför överföringen eftersom ingen av dem hittar transaktionen.
- Instruktioner till korten signeras inte av intermediären vilket är en teoretisk svaghet. Exempelvis skulle någon annan part kunna programmera ett kort att utföra andra instruktioner.
- En betalningsmottagare bör kunna välja att inte ta emot en betalning. På grund av designen är detta inte möjligt. Om betalaren har påbörjat betalningen så är den redan registrerad på betalarens kort och kommer därför att genomföras när betalaren synkroniserar denna betalning.
- De limiter som implementerades på betalkorten, som maximalt saldo och antal offlinebetalningar, är hårdkodade och går inte att ändra utan att distribuera ut nya kort.
- PoS-terminalens privata nyckel för offlinebetalningar har brister i skyddet. PoS-appen kunde manipuleras och därigenom förmås att signera valfria meddelanden. Denna brist skulle kunna utnyttjas för olika typer av bedrägliga betalningar.
- Det finns olika räknare på offline-korten och matchande räknare hos intermediärerna. Det är en enkel och effektiv lösning för att behålla integriteten i lösningen. Dock kan de olika räknarna komma i osynk, till exempel om något kort inte registrerar ett meddelande. Man vet då inte om felen i räknarna har uppstått på grund av angreppsförsök eller tekniska buggar. Det är en utmaning att kunna hantera olika typer av fel utan att riskera systemets integritet eller användarens pengar.

**SVERIGES RIKSBANK**
Tel 08 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUKTION SVERIGES RIKSBANK)
ISSN ISSN. (online)