E-kronarapport

e-kronapiloten etapp 2

April 2022

1 Innehållsförteckning

Sammanfattning

I februari 2021 inleddes den andra etappen av e-kronapiloten. Syftet med arbetet var att fortsätta att utveckla och testa den tekniska lösningen som e-kronapiloten bygger på och även att utreda hur ett juridiskt regelverk runt e-kronan skulle kunna se ut. Etapp 2 har varit lärorik och givit Riksbanken djupare kunskaper inför det fortsatta arbetet med en potentiell e-krona. Denna rapport sammanfattar arbetet under etappen samt de slutsatser och lärdomar som Riksbanken dragit.

Integration av deltagare

Fokus för arbetet har varit att testa hur det nätverk för distribution och användning av e-kronor (nedan kallat e-kronanätverket) som etablerades i en testmiljö under etapp 1 skulle kunna integreras med potentiella distributörer och med befintlig betalinfrastruktur. [1] Arbetet som har utförts tillsammans med Handelsbanken och Tietoevry som deltagare i e-kronanätverket, har inneburit att vi testat lösningen där e-kronor utgivna av Riksbanken distribueras till slutanvändare via deltagarna. Slutanvändarna har sedan kunnat hålla och använda e-kronor i transaktioner i ett e-kronanätverk som existerar parallellt men integrerat med deltagarnas interna system och betalinfrastruktur. Arbetet har också visat hur den DLT- och tokenbaserade lösningen baserat på Cordaplattformen möjliggör ett parallellt e-kronanätverk som tydligt skiljer på de privat utgivna pengarna (kontotillgodohavanden) och e-kronan som skulle vara utgiven och garanterad av staten. [2]

Alias för adressering

Etapp 2 har också utrett och implementerat ett mer användarvänligt sätt att adressera transaktioner i e-kronanätverket. Genom en aliastjänst kan varje plånboks tekniska adress kopplas till ett mer användarvänligt alias. Aliastjänsten är centraliserad och slutanvändarna kan anropa den via sin deltagare. Den centraliserade lösningen är ett effektivt sätt att skapa, lagra och använda alias inom nätverket, men den centraliserade modellen väcker en del frågor om hur den fungerar tillsammans med idén om en distribuerad modell som avser att minimera beroendet av centraliserade delar. En viktig fråga om man väljer en centraliserad lösning blir också var ansvaret för aliastjänsten skulle ligga. Det är troligt att ansvaret skulle kunna falla på Riksbanken som ägare av e-kronanätverket, vars innebörd för i så fall skulle behöva utredas närmre.

[1] För mer information om den testade lösningen och det arbete som gjordes under etapp 1 se: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-kronapiloten-etapp-1.pdf

[2] DLT (för *Distributed Ledger Technology)* och tokens har ingen entydig definition. DLT innebär i pilotens lösning att transaktionerna inte registerförs i en central databas utan i noderna hos de deltagare som är direkt inblandade i transaktionen. Tokens i pilotens lösning kan beskrivas som unikt identifierbara digitala värdeenheter med egenskapen att kunna representera e-kronor. I e-kronapiloten används s.k. *fungible tokens* som kan delas och slås ihop till nya tokens som representerar en mindre eller större summa e-kronor.

Andra lösningar för enkla adresseringar, som exempelvis QR-koder, blir allt vanligare och skulle kunna vara intressanta även för en e-krona. Dessa har dock inte utretts tekniskt i piloten.

Plånboksmodeller och möjligheter till offline-betalningar

Arbetet i etapp 2 har också visat hur den tokenbaserade lösningen kan användas på olika sätt för att lagra e-kronor. Detta gör det möjligt att designa olika plånbokstyper för olika syften. Den ena typen innebär att tokens lagras hos deltagaren i nätverket. Designen ger en e-krona som för slutanvändarna liknar hur digitala pengar på konto fungerar, även fast den bakomliggande tekniken skiljer sig mot kontobaserade system. Det gör det möjligt att erbjuda samma typ av tjänster och användarupplevelser som vi är vana vid idag, exempelvis flera betalinstrument som är kopplade till samma pengar och andra betaltjänster som t.ex. autogiro. Den andra plånbokstypen bygger på att slutanvändarna lagrar e-kronor i en lokal plånbok på sin mobil. Detta gör att man kan genomföra transaktioner offline. Sådana transaktioner skulle dock inte vara avvecklade vilket innebär vissa risker. Det har också visat sig att det inte alltid går att få tillbaka lokalt lagrade e-kronor om man förlorar sin plånbok. Därför bör lokalt lagrade e-kronor betraktas som kontanter och bara hållas som en mer begränsad summa för just tillfällen av offline. Och även om det skulle gå att minimera riskerna tekniskt så finns det andra risker med transaktioner offline, som exempelvis penningtvätt och brottslig verksamhet, som innebär att begränsningar kan behövas.

Integrering med POS-terminal

Etapp 2 har också testat att integrera e-kronanätverket mot en POS-terminal (Point Of Sale) som förekommer på marknaden idag. Det har visat sig att det går att installera e-kronaspecifik mjukvara på en terminal så att det går att göra betalningar med e-kronor inom e-kronanätverket, samtidigt som terminalen kan hantera betalningar på de stora kortnätverken. De stora frågorna här är inte nödvändigtvis tekniska utan handlar också om vilka policymål och regelverk som ska gälla för en e-krona, exempelvis hur fristående och parallell en e-krona bör vara till övrig betalinfrastruktur. Att integrera e-kronan på den befintliga terminalmarknaden är en komplex fråga som ofta involverar anpassningar till regelverk och de privata aktörernas terminaler. Utvecklingen på betalmarknaden, såväl i Sverige som internationellt, visar att appbaserade betalningar och nya typer av mobilbaserade terminaler blir allt vanligare. Det blir viktigt att följa den fortsatta utvecklingen och se till att en e-krona och dess regelverk är flexibelt för att kunna fungera vid sådana betalningar.

Prestandatester

Ett viktigt fokusområde för etapp 2 har också varit att fortsätta testa den tekniska lösningens prestanda. Ett grundläggande krav för e-kronan är att den ska kunna användas för omedelbara transaktioner i stor skala och att det ska kunna ske året om och dygnet runt. I arbetet har vi jämfört med de transaktionsvolymer som Swish och ett kortnätverk har under de mest belastade tiderna på året. Att den testade lösningen är

token- och DLT-baserad gör att den har vissa egenskaper som kan innebära utmaningar för just prestandan. För att testa lösningen och förstå var problem kan uppstå har vi designat scenarier för att se var eventuella flaskhalsar kan skapas. Testerna har visat att i de enklare scenarierna så står sig lösningen väl mot Swish och ett kortnätverks transaktionsvolymer. När transaktionerna blir mer komplexa med fler tokens och längre historiska transaktionskedjor försämras prestandan. Förslag på tekniska åtgärder som kan lösa dessa problem har diskuterats, men de är än så länge otestade och vidare arbete skulle krävas för att testa och utvärdera effekten av dessa åtgärder för prestandan och lösningen som helhet.

Legala frågor

Arbetet inom det legala området har huvudsakligen fokuserat på två ämnen: dels hur information delas i ett DLT-nätverk och hur lagstiftningen skulle appliceras på sådan informationsdelning när det kommer till finansiell sekretess och dataskydd, dels på frågan om vilket tillgångsslag e-kronan skulle kunna tillhöra.

Den legala analysen visar att det inte är klarlagt hur den informationsdelning som DLT/blockkedjeteknik är uppbyggd kring förhåller sig till dagens lagstiftning inom finansiell sekretess och dataskydd. Troligtvis är de uppgifter som följer med en transaktion i transaktionshistoriken att anse som personuppgifter och uppgifter som omfattas av finansiell sekretess. Det kan komma att behövas lagändringar och/eller informationssäkerhetsåtgärder om den lösning som har testats i piloten ska uppfylla gällande rätt.

E-kronan i piloten kan enligt den legala analysen vara att se som en elektronisk form av tillgångsslaget kontanter. Den blir då ett nytt alternativ och komplement till den fysiska formen av kontanter som finns idag – sedlar och mynt.

Slutsatser

Sammanfattningsvis så har etapp 2 fokuserats på att fortsätta testa den tekniska lösningen och att gräva djupare i de mer komplicerade frågorna kring en potentiell e-krona. Arbetet har visat hur ett parallellt nätverk med e-kronor, likt den testade lösningen, skulle kunna integreras med deltagares interna system och möjliggöra distribution och transaktioner med e-kronor. Det har också visat hur den tokenbaserade lösningen kan designa plånböcker som för slutanvändaren påminner om ett vanligt konto, men också plånböcker vars e-kronor i vissa avseenden får mer kontantlika egenskaper. Genom att testa att integrera e-kronanätverket med POS-terminal har det praktiskt visats hur e-kronanätverket skulle kunna använda befintlig hårdvara som används på marknaden idag för att hantera kortnätverkens betalningar. Arbetet har också tydliggjort vikten av regelverk och samverkansmodeller med betalmarknadens aktörer om en e-krona ska etableras i handeln. Etapp 2 har också tydliggjort att den testade Cordaplattformen inte är specifikt designad för en så kallad retail-CBDC som e-kronan skulle vara (plattformen är i grunden designad för andra typer av finansiella transaktioner). Det har bland annat blivit tydligt under arbetet med prestandatesterna

där scenarion som en e-krona måste kunna hantera kan innebära problem i den nuvarande versionen av Cordaplattformen. Det gäller även delandet av data inom nätverket, vilket är en grundidé med DLT-tekniken, men som väcker frågor om plattformen kan uppfylla kraven i de legala regelverken. De tekniska anpassningarna som behövs för att komma till rätta med dessa potentiella problem, som exempelvis automatiserad inlösen av e-kronor med långa transaktionskedjor, är otestade och väcker samtidigt andra frågor. De utmaningar som plattformen har betyder inte att den här typen av lösning behöver vara olämplig för en potentiell e-krona. Men det krävs att de svagheter som identifierats kan hanteras i framtida versioner och i designen av ett e-kronanätverk.

En e-krona kommer, oavsett utformning och teknik, att innebära att allmänheten får tillgång till en ny form av pengar som ges ut av Riksbanken. De olika frågorna som rör en e-krona är ofta komplexa, vissa från ett rent tekniskt perspektiv, en del från ett policyperspektiv och andra när det gäller hur ansvar och roller ska fungera i en distributionsmodell för e-kronan. Lägg därtill de juridiska frågorna som måste redas ut för en ny form av pengar. Under etapp 2 har många av dessa frågor behandlats och för pilotens syfte att öka Riksbankens kunskap så har arbetet varit värdefullt. Det ger en bra grund för Riksbankens fortsatta arbete med att formulera utformningen av och kraven på en eventuell utgivningsbar e-krona.

Riksbanken vill rikta ett speciellt tack till Handelsbanken och Tietoevry som genom att delta i etapp 2 av e-kronapiloten har bidragit till att öka Riksbankens kunskaper.[3]

[3] Handelsbanken är en av de större bankerna i Sverige och Tietoevry är en stor IT-leverantör av bl.a. IT-system för banktjänster.

1 Bakgrund – kontanter används alltmer sällan

Sedlar och mynt används alltmer sällan i Sverige. Det beror bland annat på den tekniska utvecklingen som gett oss olika typer av moderna digitala betaltjänster. Riksbanken ser dock potentiella problem med att de pengar som är utgivna av Riksbanken och tillgängliga för allmänheten är på väg att försvinna. Riksbanken har därför sedan 2017 utrett möjligheten att ta fram ett digitalt alternativ av centralbanksutgivna pengar, en så kallad e-krona.

I februari 2020 inledde Riksbanken ett mer praktiskt arbete med e-kronan genom ett tekniskt pilotarbete tillsammans med Accenture där en möjlig lösning för en e-krona har testats. Under den första etappen av e-kronapiloten skapades ett e-kronanätverk på en plattform som baseras på *Distributed Ledger Technology* (DLT) och där e-kronan representeras av tokens. I februari 2021 gick arbetet in i den andra etappen med fortsatt utredning och testande av den tekniska lösningens möjligheter att leva upp till de potentiella kraven på en utgivningsbar e-krona.

Det finns ännu inget beslut om att lansera en e-krona och inte heller om vilken teknik som då skulle användas eller om hur det juridiska regelverket skulle se ut. Syftet med piloten är att Riksbanken genom praktiskt arbete ska lära sig mer om hur en e-krona skulle kunna fungera. Arbetet ska ses som ett sätt för Riksbanken att få en bättre bas för jämförelser med andra möjliga lösningar och som ett sätt att utreda såväl tekniska som juridiska detaljer. Den lösning som utvecklats inom piloten är således inte avsedd för produktion.

2 Tekniskt arbete etapp 2

En e-krona kommer att behöva vara kompatibel med befintliga aktörer och betalinfrastruktur på marknaden för att den ska kunna distribueras ut till allmänheten och användas i transaktioner. Det tekniska arbetet under etapp 2 har därför fokuserat på att testa hur dessa integrationer skulle fungera och hur e-kronan skulle kunna användas som betalmedel i olika situationer. Vi har också testat om den tekniska lösningen skulle kunna användas till omedelbara massbetalningar. Arbetet har visat att den tekniska lösningen kan integreras med befintlig infrastruktur och även att den är flexibel för att designa lösningar för olika betaltjänster och situationer. Att lösningen än så länge är oanvänd i produktion för en retail-CBDC har dock tydliggjort en del av dess utmaningar vad gäller prestanda.

2.1 Framgångsrik integration av deltagare

Ett fokusområde för etapp 2 av e-kronapiloten har varit att testa hur det utvecklade e-kronanätverket skulle kunna integreras med potentiella deltagares interna system. Detta är en grundläggande förutsättning för den modell som lösningen baseras på där Riksbanken skapar e-kronorna och där distributionen till allmänheten sker via godkända deltagare i e-kronanätverket. Handelsbanken och Tietoevry har i rollerna som bank och leverantör av finansiella IT-system deltagit i etapp 2 av e-kronapiloten där de har drivit en nod i e-kronanätverket och integrerat den med sina befintliga konto- och betalsystem. Därmed har det varit möjligt att se hur en potentiell deltagare i ett e-kronanätverk skulle kunna beställa e-kronor från Riksbanken och erbjuda sina kunder möjlighet att växla till sig e-kronor mot kontotillgodohavanden i kontosystemet. Integrationsarbetet har visat att den testade lösningen går att använda för att skapa ett parallellt nätverk där e-kronor utgivna och garanterade av Riksbanken existerar. Vi har också testat att göra transaktioner mellan deltagarna och slutkunder inom e-kronanätverket och även ut ur e-kronanätverket.

Distributionsmodellen liknar dagens modell för kontanter

Den tekniska lösning som testas i e-kronapiloten bygger på en så kallad two-tier-modell där e-kronorna, likt modellen med de fysiska kontanterna, distribueras från Riksbanken till allmänheten via godkända deltagare i ett e-kronanätverk. Deltagarna kan vara exempelvis banker eller andra betaltjänstleverantörer. E-kronanätverket är baserat på företaget R3:s Cordaplattform som är baserad på DLT, och e-kronorna i nätverket representeras av tokens som går att spåra tillbaka till Riksbanken som utgivare. Deltagarna i nätverket driver noder och kan beställa e-kronor från Riksbanken mot debitering av deras reserver i Riksbankens avvecklingssystem, RIX. Därefter kan deltagarna lagra e-kronorna i sina digitala valv. Deltagarna erbjuder sina kunder som slutanvändare möjligheten att öppna digitala e-kronaplånböcker som kan kopplas till

betalinstrument, exempelvis mobilappar eller kort.[4] E-kronaplånböckerna kopplas också till kundernas konton i deltagarens interna system där kunderna har sina kontotillgodohavanden.[5] Detta gör att slutanvändarna kan växla till sig e-kronor från deltagarens valv och betala för dem med sina kontotillgodohavanden hos deltagaren. Och det motsatta om kunderna vill växla *in* e-kronor mot kontotillgodohavanden. Slutanvändarna kan sedan genomföra transaktioner med e-kronorna via sin anslutna deltagares noder i nätverket. Viktigt i denna distributionsmodell är att slutanvändarna ansluter till e-kronan via redan etablerade kundrelationer med deltagaren som distribuerar e-kronan. Man utgår alltså ifrån att slutanvändarna redan är kunder hos banken eller betaltjänstleverantören, har kontotillgodohavanden där och är kända som kunder (KYC). Riksbanken som utgivare av e-kronan ansvarar alltså inte för vare sig anslutningen av kunder eller för processerna runt detta.

Integration med fokus på växling och transaktioner

Lösningen bygger alltså på att deltagarens nod i e-kronanätverket integreras med deltagarens interna kund-, konto- och betalsystem. Då kan en ansluten kund öppna en plånbok och koppla den till ett konto och växla mellan kontotillgodohavanden och e-kronor. Integrationen med andra interna system hos deltagarna, som exempelvis bokföringssystem och AML-system, är också nödvändigt vid en produktionslösning men detta har inte testas under etapp 2. Handelsbanken och Tietoevry har som deltagare i piloten drivit varsin nod i e-kronanätverket och detta har kopplats samman med deltagarens interna banksystem genom ett integrationslager (mer beskrivet nedan).

[4] I e-kronapiloten har en mobilapp utvecklats på telefoner med Android OS, och även kort har testats som betalinstrument under arbetet.

[5] Under etapp 1 testades också möjligheten att ha s.k. anonyma plånböcker som inte kräver identifiering eller koppling mot ett angivet konto hos en deltagare. Denna typ av plånbok skulle förmodligen ha begränsningar när det gäller tillåtna summor och möjligheter att ta emot transaktioner och skulle exempelvis kunna köpas hos godkända återförsäljare.

FAKTA – Integration via en *e-kronamotor*

Corda, som är den DLT-plattform som e-kronanätverket är byggt på, är i sin grunddesign inte specifikt avsedd för så kallade *retail-CBDC* vilket e-kronan skulle vara. Plattformen har ett bredare, mer generellt, användningsområde för överföringar av digitala tillgångar i form av tokens inom ett distribuerat nätverk. För att använda plattformen för en e-krona behövs ett integrationslager, i piloten kallat e-kronamotorn. E-kronamotorn kan beskrivas som ett affärs- och integrationslager som gör att e-kronanätverket kan kopplas ihop med en deltagares interna system och strukturera informationen från DLT-nätverket på ett sätt som användarna förstår.

För att ge ett exempel: Som nämnts så representeras e-kronan i denna tekniska lösning av enskilda tokens vars värde i e-kronor kan variera.[6] För en slutanvändare kan e-kronor bestå av en mängd olika tokens med olika värden, på samma sätt som man kan äga en mängd olika fysiska kontanter och mynt. Men för en slutanvändare är de enskilda tokens som bygger upp ens totala ägande av e-kronor ointressant. Det som är av intresse är hur mycket e-kronor man har. E-kronamotorn möjliggör integration med deltagarnas interna system och förenklar och sammanställer information från Cordaplattformen. Exempelvis summerar den varje slutanvändares saldo, möjliggör visandet av transaktionshistoriken, hanterar alias och andra nödvändiga tjänster som gör att Cordaplattformen kan användas för en e-kronas syften.

I detta skede av piloten har fokus i integrationen främst legat på konto- och betalsystemet för att testa de grundläggande funktionerna. Integrationsarbetet med deltagarna har resulterat i att Handelsbanken och Tietoevry har kunnat

- begära utgivning av e-kronor från Riksbanken, mot debitering av reserver i en simulering av RIX, och lagra dessa i sina e-kronavalv
- öppna e-kronaplånböcker åt sina kunder och koppla plånböckerna till betalinstrument och betalkonton med kontotillgodohavanden
- låta kunderna växla till sig e-kronor mot kontotillgodohavanden
- låta kunderna utföra transaktioner med e-kronor till andra e-kronaplånböcker inom nätverket
- låta kunderna utföra transaktioner med e-kronor till betalkonton hos deltagaren (vilket innebär en växling hos deltagaren som tar emot e-kronorna och krediterar det kommersiella betalkontot)
- låta kunderna växla in e-kronor mot kontotillgodohavanden
- begära inlösen av e-kronor hos Riksbanken mot kreditering av reserver i en simulering av RIX.

[6] Den tekniska lösningen är baserad på asymmetrisk kryptografi där varje token med e-kronor också är kopplad till ett nyckelpar. En publik nyckel som är öppen och visar vem som är ägare av token. En privat nyckel som är knuten till ägaren av e-kronorna som därmed kan utföra transaktioner med tokens med den matchande publika nyckeln. Denna koppling av publik nyckel och e-kronaplånbok som i sin tur är kopplad till en specifik kund görs också i e-kronamotorn. Detta ligger alltså hos deltagaren och är inget som märks hos slutanvändarna.

Deltagarna har under piloten valt olika sätt att implementera och genomföra tester av dessa flöden. Handelsbanken utvecklade under piloten egna webbaserade testgränssnitt enbart för pilotens syfte. Dels för att kunna styra bankens egna beställningar och inlösen av e-kronor från Riksbanken, dels för att kunna simulera hur deras kunder skulle kunna göra växlingar och transaktioner.

Tietoevry byggde för piloten ett webbgränssnitt för att demonstrera hur ett banksystem skulle kunna beställa och lösa in e-kronor och föra bok över sin e-kronabehållning. De utvecklade också ett verktyg som automatiskt kunde begära utgivning eller inlösen hos Riksbanken så fort behållningen i valvet var under eller över vissa satta gränser. För att simulera slutkundernas växlingar och transaktioner använde Tietoevry dels den app som tagits fram under etapp 1 av e-kronapiloten, dels ett egenutvecklat webbgränssnitt. [7]

Handelsbankens och Tietoevrys egna implementeringar och tester har demonstrerat hur deltagare skulle kunna driva noder i e-kronanätverket med kopplade integrationslager och utveckla egna gränssnitt och administrativa verktyg där de kan implementera egna affärsregler anpassade efter deras egen verksamhet och deras kunder. Deltagarnas anslutning till Riksbankens e-kronanätverk implementerades också på olika sätt. För ena deltagaren valde vi att flytta in e-kronanoden i deras egen interna IT-miljö. I det andra fallet valde vi att låta e-kronanoden ligga i den miljö som Riksbanken satt upp för e-kronanätverket. Diagram 1 illustrerar hur e-kronanätverket sattes upp. Tietoevrys och Riksbankens noder implementerades i samma för piloten uppsatta IT-miljö, medan Handelsbankens nod låg i deras egen IT-miljö. Men alla parter kunde kommunicera och utföra transaktioner i ett gemensamt e-kronanätverk.[8]

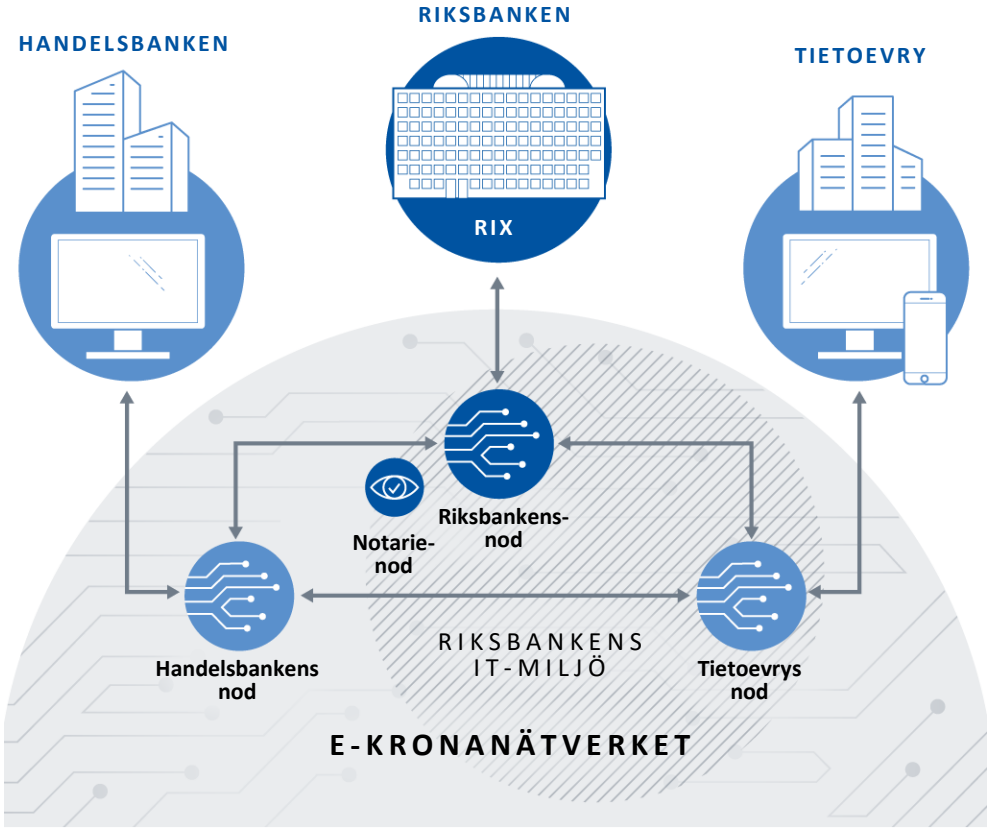
En lärdom med denna design är att två deltagare kan integrera sig mot systemet i olika miljöer och när de senare sammanförs till en och samma miljö krävs inga ytterligare tester för att de ska kunna samverka.

[7] Under https://www.riksbank.se/sv/press-och-publicerat/konferenser/2021/2021-11-29/ finns demonstrationsfilmer från Handelsbankens och Tietoevrys implementeringar och egenutvecklade gränssnitt från etapp 2.

[8] Kommunikationen mellan Riksbanken och deltagarna i nätverket har i piloten gått över internet genom VPN. För ett produktionsmässigt nätverk skulle det ställas högre säkerhetskrav på kommunikationsvägarna men för pilotens syfte har det fungerat väl.

Diagram 1. Så har deltagarna integrerats i e-kronanätverket

Bilden illustrerar hur deltagarnas e-kronanod i nätverket är integrerad mot deras interna kontosystem och betalsystem. Handelsbanken har implementerat sin e-kronanod helt i sin egen IT-miljö medan Tietoevrys e-kronanod finns i Riksbankens IT-miljö.



Lärdomar från integrationsaktiviteten

Arbetet med att integrera externa aktörer som deltagare har konkretiserat konceptet med ett e-kronasystem och ett nätverk där digitala centralbankspengar cirkulerar. E-kronorna i detta nätverk är utgivna och garanterade av Riksbanken fast de distribueras till allmänheten via deltagare i nätverket. Att e-kronorna representeras av unikt identifierbara tokens i ett eget nätverk gör att de tydligt går att skilja från övriga digitala pengar i form av kontotillgodohavanden som allmänheten har tillgång till idag. Arbetet har också visat hur ett parallellt nätverk som är integrerat med existerande konto- och betalinfrastruktur kan fungera. Att nätverket fungerar parallellt kan göra betalmarknaden mer robust och integrationen med existerande konto- och betalinfrastrukturer möjliggör direkta växlingar och överföringar mellan kontotillgodohavanden och e-kronor. Nätverket är alltså beroende av att angränsande konto- och betalsystem fungerar för att det ska gå att fylla på likviditet i plånböckerna, men är parallellt på så sätt att transaktioner *inom* e-kronanätverket inte är strikt beroende av de angränsande systemen. Arbetet med deltagarna har också visat att det för aktörer som Handelsbanken och Tietoevry inte behöver vara någon större teknisk utmaning att integrera ett e-kronanätverk, likt det testade i piloten, med interna banksystem så länge man följer branschpraxis. Detta har även betonats av deltagarna själva som är vana vid att jobba med integration av olika system. Det som testades i piloten var dock

endast en del av de integrationer och säkerhetskrav som skulle krävas för produktion. De regelverk som skulle gälla för en e-krona skulle förstås också avgöra hur en integration med deltagarna skulle behöva fungera. Sådana policyfrågor har dock inte varit i fokus under detta skede av piloten.

2.2 Alias för adressering

Den svenska betalmarknaden ligger idag i framkant vad gäller användarvänliga omedelbara digitala betalningar. Det är också en förklaring till att de fysiska kontanterna används alltmer sällan. Att det går att adressera transaktioner på ett användarvänligt sätt är därför en förutsättning om en e-krona ska kunna bli etablerad och använd. DLT-plattformen som e-kronanätverket baseras på har ingen inbyggd lösning för detta så ett fokusområde för etapp 2 av e-kronapiloten var att utreda hur detta skulle kunna fungera i ett distribuerat nätverk och implementera en teknisk lösning för det.

Som nämnts ovan så är inte cordaplattformen som pilotens tekniska lösning baseras på designad specifikt för en e-kronas syften. I plattformen finns exempelvis endast en teknisk adressering till plånböckerna vars ID består av en lång komplicerad alfanumerisk sträng.[9] Därför behövs en lösning som kopplar plånböckernas ID till något som är enklare att adressera. Betalappen Swish har exempelvis löst detta så att man kan adressera ett bankkonto via ett mobilnummer, vilket är betydligt enklare än att använda det bakomliggande kontonumret. Den lösning som vi valde att testa i piloten blev en fristående central komponent i nätverket som gör att slutanvändare kan skapa och lagra egna alias för sina plånböcker vilket gör det enklare att adressera transaktioner.

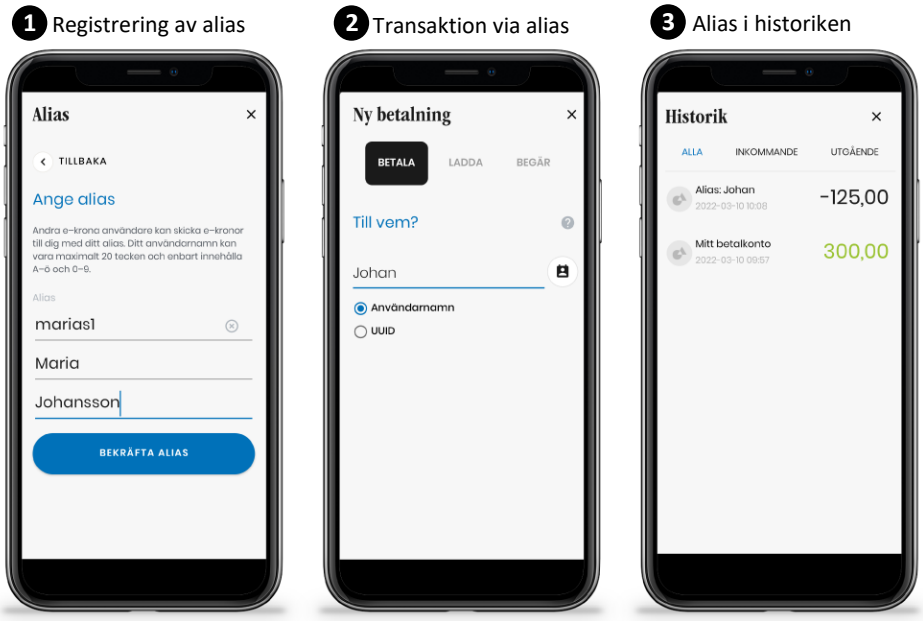
Implementerad aliastjänst

Den möjlighet att skapa ett alias som implementerades under etapp 2 gör att slutanvändaren kan knyta sin plånbok och dess ID till ett alias via gränssnittet i den mobilapp som utvecklats för piloten. Vi har där utgått från man ska kunna använda vilket namn som helst som alias. Detta för att en användare skulle kunna ha flera e-kronaplånböcker. Om det skulle vara det bästa i produktion har inte varit fokus under arbetet. För att denna aliastjänst ska kunna fungera tillsammans med andra adresseringslösningar så kan det också finnas skäl att följa vissa standarder. Tekniskt så finns det dock inte något som hindrar att man skulle införa större begränsningar för hur ett alias skulle kunna se ut. Men för pilotens syfte med de tester som har genomförts så har en friare namnsättning varit att föredra. Diagram 2 visar exempel från det implementerade gränssnittet i pilotens e-kronaapp.

[9] Den alfanumeriska strängen är ett ca 30 tecken långt ID (i Corda UUID för *Universally Unique Identifiers*) bestående av bokstäver och siffror.

Diagram 2. Gränssnitt vid användning av alias

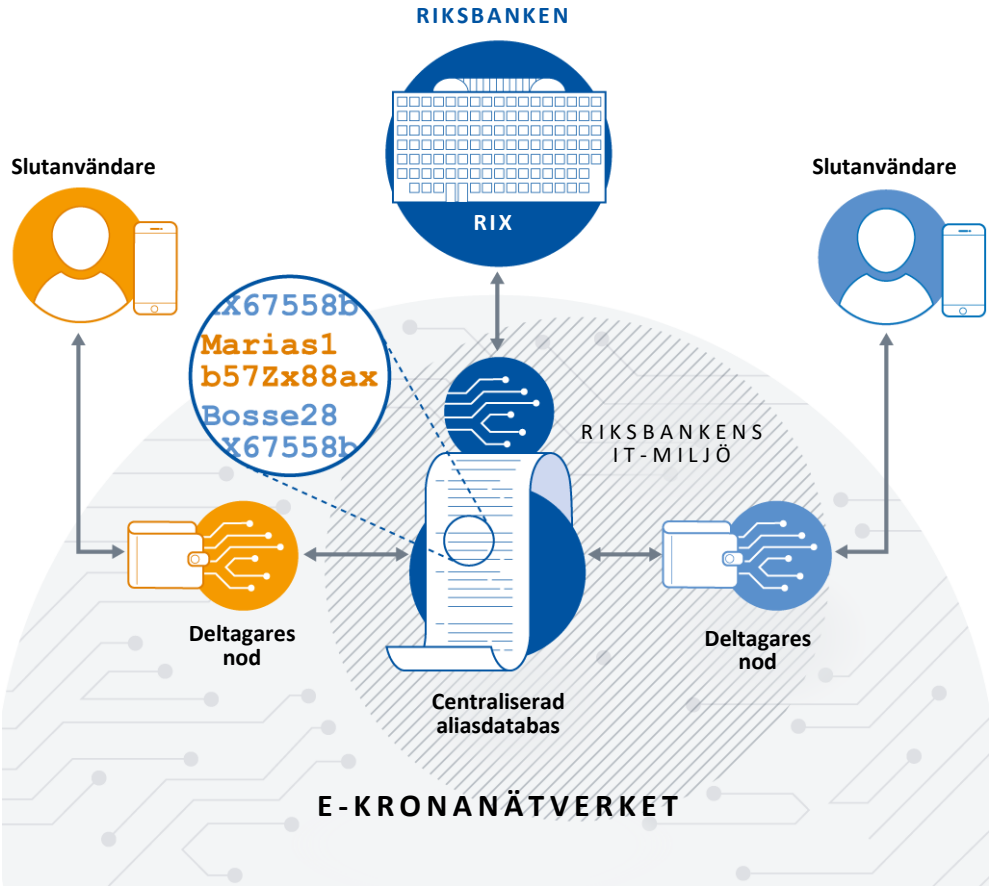
Exempelbilder från den pilotutvecklade testappen över hur den implementerade alias-tjänsten fungerar vid registrering av alias, och användandet av alias i transaktioner.



Det viktigaste under etapp 2 var dock inte att undersöka hur det skulle se ut grafiskt i den app som utvecklats enbart i testsyfte för piloten eller att avgöra vilka begränsningar som skulle gälla vid val av alias. Det mer intressanta var att förstå hur en DLT-plattform, som i grunden inte är designad för den typ av adressering som en e-krona behöver, kan bygga en aliastjänst på ett effektivt sätt. Aliastjänsten som tagits fram i piloten är designad som en frikopplad central komponent i nätverket som deltagarnas e-kronanoder kan kommunicera med. När en slutanvändare anger ett alias så sker det via hens deltagares e-kronamotor som anropar den för nätverket centrala aliastjänsten som lagrar angivet alias tillsammans med kopplat plånboks-ID. Och när en betalning ska göras till den plånboken så kan alias användas som adressering. Tekniskt innebär det att den betalande deltagaren anropar aliastjänsten för att med hjälp av alias hitta det kopplade plånboks-ID som plattformen använder för att skicka betalningen. Ett alias blir alltså ett sätt att genom en central komponent hämta det bakomliggande plånboks-ID:t. Att aliastjänsten är löst kopplad till övriga delar i e-kronanätverket gör att aliastjänsten kan förändras eller bytas ut om nätverket skulle anslutas till andra etablerade adresseringsstandarder. Detta utan att påverka övriga funktioner i e-kronamotorn. Bild 3 visar en förenklad illustration av hur aliastjänsten fungerar.

Diagram 3. Så har aliastjänsten implementerats i e-kronanätverket

Aliastjänsten är en central komponent i nätverket som deltagarnas noder kan anropa vid betalningar med hjälp av alias. Slutanvändarens alias är kopplat till den tekniska adresseringen som finns i nätverket



Lärdomar och reflektioner från arbetet med alias

En viktig fråga för vidare utredning är vad det innebär för konceptet med ett distribuerat nätverk om det introduceras fler centraliserade komponenter som aliastjänsten. En möjlig nackdel med en centraliserad aliastjänst är att nätverket därigenom blir beroende av en centralt lagrad tjänst för att använda alias.

Denna svaghet kan man råda bot på genom att tillåta andra sätt att adressera inom nätverket. I etapp 2 kunde man genom den framtagna testappen även använda det mer komplicerade plånboks-ID:t för adressering om alias saknades eller om det förekom störningar i tjänsten. Det är också tekniskt möjligt att designa en mer decentraliserad lösning för en aliastjänst, vilket har diskuterats under pilotens arbete. Men en sådan blir betydligt mer komplex och innebär andra typer av beroenden av kommunikation mellan deltagare vid exempelvis uppdateringar av en slutanvändares alias. En annan viktig fråga om man använder en centraliserad aliastjänst är vem som har ansvaret för att utveckla och förvalta data. Det är troligt att ansvaret skulle kunna falla på Riksbanken som ägare av e-kronanätverket, även om det var outsourcat till en aktör som låg utanför Riksbankens IT-miljöer. Det skulle kunna innebära att Riksbanken

får ansvar för användaruppgifterna i e-kronanätverket vilket Riksbanken genom att använda denna modell vill undvika för att bibehålla sin nuvarande roll på betalmarknaden och inte behöva hantera uppgifter om slutkunder.

QR-koder är ett annat beprövat och enkelt sätt adressera som blir alltmer vanligt i handeln och som även är väldigt vanligt i vissa länder, exempelvis Kina. En sådan lösning skulle kunna vara intressant som ett alternativ till en aliastjänst eftersom det är absolut nödvändigt att betalningar med en e-krona kan adresseras på ett användarvänligt sätt. Informationen om vem som är kopplad till en viss QR-kod lär dock behövas precis som med ett alias. Innan man kan bygga en adresseringstjänst, via exempelvis alias, på en teknisk lösning som inte har ett inbyggt stöd för det från början måste alltså en del frågor besvaras. Både tekniska frågor om hur det görs mest användarvänligt och frågor om var informationen skulle ligga och vem som har yttersta ansvaret för den.

2.3 Plånboksmodeller och möjligheter till offline-betalningar

Ett viktigt område för e-kronapiloten är att utreda hur en potentiell e-krona skulle kunna erbjuda möjligheter att utföra betalningar offline, det vill säga utan kommunikationsförbindelser till ett e-kronanätverk. I och med att kontanterna blir alltmer marginaliserade så ökar risken att betalmarknaden, och därmed Sveriges ekonomi, blir alltmer sårbar för störningar eller problem med existerande digitala betalmedel. Möjligheten att kunna betala offline är därför av stort intresse för en potentiell e-krona och detta är något som även lyfts fram i den allmänna CBDC-debatten.

Arbetet i etapp 2 har visat att det går att lagra e-kronorna lokalt på en mobiltelefon. På så sätt blir offlinetransaktioner möjliga, men eftersom lösningen är baserad på ett e-kronanätverk som är online så innebär tranaktioner offline risker som skulle behöva hanteras. För att en e-krona ska bli etablerad och använd så är det också viktigt att den i normala fall med uppkoppling kan användas likt de betaltjänster vi är vana vid. Våra tester har visat att e-kronor som lagras i nätverket kan användas för betaltjänster på samma sätt som vi är vana vid idag med våra digitala kontotillgodohavanden.

Olika plånboksmodeller innebär olika möjligheter

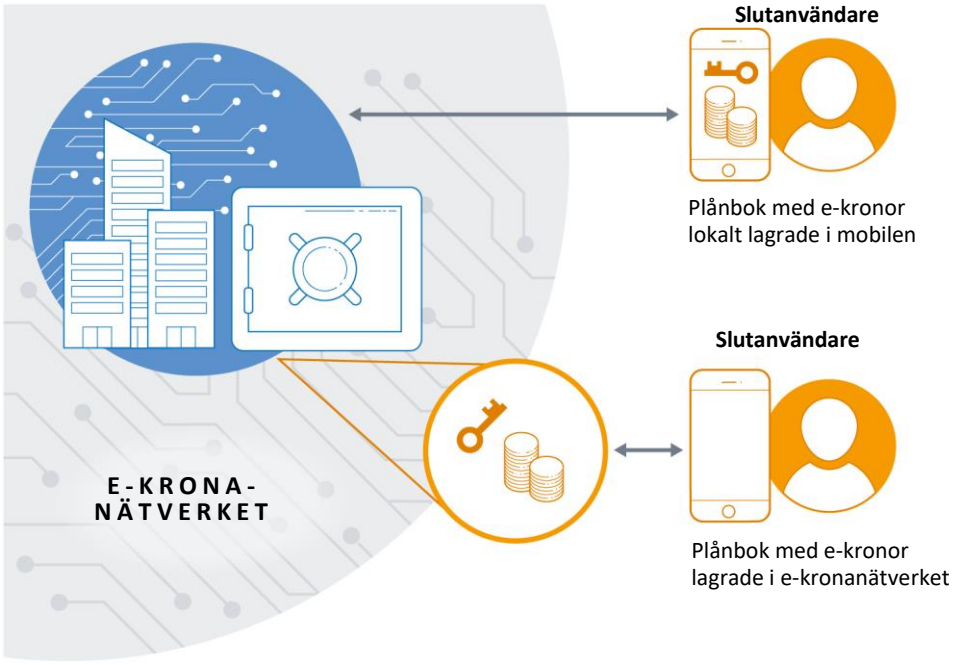
I rapporten för den första etappen av e-kronapiloten diskuterades den tekniska lösningens teoretiska möjligheter att lagra tokens och privata nycklar på olika sätt. Dessa så kallade plånboksmodeller erbjuder olika möjligheter och begränsningar när det gäller betalningar. Den plånboksmodell där tokens och nycklar lagras i nätverket i deltagarens nod innebär att samma typ av tjänster kan erbjudas som i dagens banksystem med digitala kontotillgodohavanden. När tokens med e-kronor och nycklar ligger hos slutanvändarens deltagare kan flera betalinstrument anslutas till e-kronorna. Man kan exempelvis ansluta ett eller flera betalkort och en mobilapp som alla är kopplade till samma e-kronor. Det skulle fungera på samma sätt som idag när vi kommer åt våra pengar via betalkort och appar. Denna möjlighet har testats under etapp 2. I och med att e-kronorna ligger i nätverket så innebär inte heller ett borttappat eller trasigt betalinstrument att pengarna är förlorade. Designen skapar en e-krona som för slutan-

vändaren uppfattas och har samma möjliga funktioner som de digitala kontotillgodohavanden som vi är vana vid idag. Även fast den underliggande tekniken skiljer sig mot traditionella kontobaserade lösningar.

Plånboksmodellen med lagring av tokens och nycklar lokalt i betalinstrumentet, i piloten kallad *lokal plånbok*, är den mer kontantlika designen där slutanvändaren håller både tokens med e-kronor och en nyckel lokalt i e-kronaappen. Denna typ av plånbok innebär att endast slutanvändaren har makt över e-kronorna och modellen erbjuder även möjligheter att initiera betalningar offline utan tillgång till nätverket.

Diagram 4. Plånboksmodeller

Bilden illustrerar olika design av plånboksmodeller som implementerats under etapp 2. Den ena modellen lagrar e-kronor och nycklar online i nätverket hos deltagaren och den andra lagrar lokalt i mobilen.



Testad offlinefunktion

Offlinefunktionen är tänkt att innebära att tokens med e-kronor, nycklar till tokens och möjligheten att validera transaktioner flyttas från deltagarens nod i e-kronanätverket till slutanvändarens mobilapp. Som beskrevs närmre i rapporten från etapp 1 så bygger tekniken i e-kronanätverket på UTXO (*Unspent Transaction Output)* där varje transaktion består av en eller flera insatta tokens och resulterar i en ny token till mottagaren (och eventuellt en token med växel tillbaka till betalaren).[10] Genom att

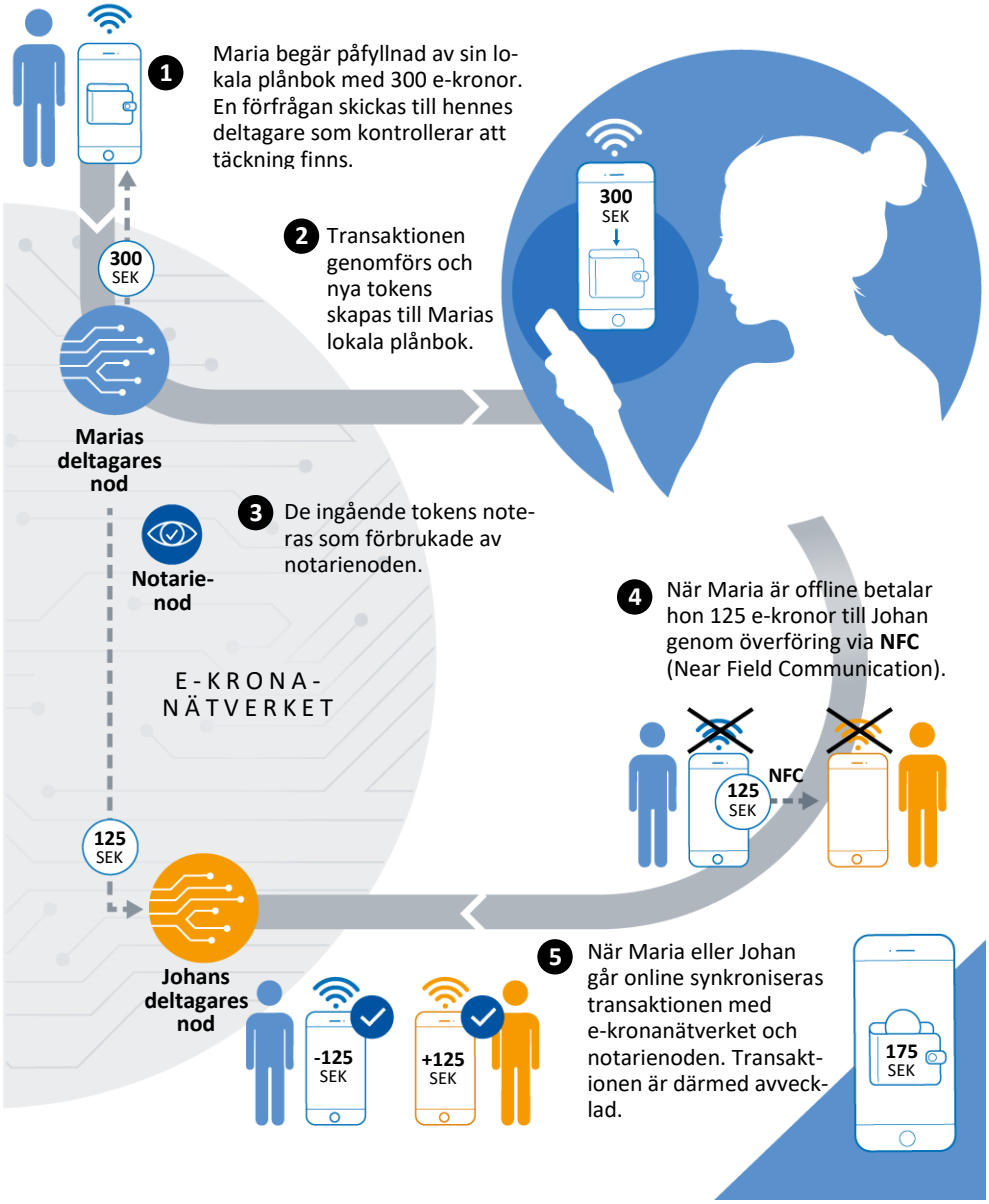
[10] UTXO står för *Unspent transaction Output* vilket i Corda innebär att en token kan vara antingen konsumerad eller inte konsumerad. När en transaktion genomförs så används tokens som inte är konsumerade som ingående tokens och blir därmed förbrukade. Från transaktionen skapas utgående tokens som kan användas i framtida transaktioner.

man lyfter ut den information och funktion som i onlineläget utförs av noderna i nätverket till den lokala mobilappen så kan slutanvändarnas egna mobilappar skapa transaktioner med e-kronor med de lokalt lagrade tokens och via exempelvis NFC (Near Field Communication) föra över dem till en mottagare. Mottagarens mobilapp kontrollerar e-kronornas äkthet och att de har sitt ursprung hos Riksbanken. Mobilappen behöver alltså som betalare kunna skapa en transaktion med insatta tokens enligt Cordas UTXO-modell och som mottagare kunna validera den transaktionskedja som kommer med en transaktion.

Rapporten från etapp 1 förklarade också den så kallade notarienodens funktion, att slutgiltigt reglera transaktioner i e-kronanätverket. Notarienoden kontrollerar att en token som ingår i en transaktion inte har använts tidigare vilket gör den förbrukad. Den funktionen, som är avsedd för att motverka dubbelspendering, kan inte lyftas ut till offlineläge. Detta innebär att transaktioner som utförs i offlineläge inte kan anses vara avvecklade förrän betalaren eller betalningsmottagaren går online och synkar transaktionen med nätverket med kontroll av notarienoden. Diagram 5 visar en illustration av hur e-kronor kan lagras lokalt, användas i offlineläge och sedan synkroniseras online.

Diagram 5. Transaktion offline

Illustration över hur en offlinetransaktion fungerar.



Lärdomar och reflektioner om offlinefunktionens möjligheter och risker

Testerna av offlinefunktionen har visat att det är tekniskt möjligt att lagra tokens och nyckeln lokalt i en mobilapp och med hjälp av NFC föra över e-kronor till en mottagare med uppdaterade saldon för båda. Transaktionerna kan sedan synkas med nätverket och avvecklas när någon går online igen. Det går också att hantera transaktioner i flera steg offline med flera avsändare och mottagare i ett flöde av transaktioner. Dock finns praktiska begränsningar av hur många offlinetransaktioner i följd som kan hanteras av mobilerna och det finns även risker att ta hänsyn till vars konsekvenser och spridning kan bli större ju fler offlinetransaktioner i följd som tolereras.

Transaktionerna kräver som nämnts en synkronisering med nätverket och notarienoden för att de tokens som ingår i en offlinebetalning ska kunna kontrolleras och betalningen därmed avvecklas. Och om det inte går att skydda data om de tokens som lagras i den lokala mobilen så finns det risk att en slutanvändare kan komma åt informationen i mobilen och kopiera tokens och använda dem flera gånger i offlineläge. Ett sådant bedrägeri är inte enkelt att genomföra och det går att minimera riskerna, men det går inte att helt bortse från dem. Men även fysiska sedlar är inte helt riskfria då det finns risk för förfalskningar.

Vid betalningar offline kan man alltså inte helt säkert veta om en token med e-kronor är manipulerad eller har använts tidigare, det så kallade dubbelspenderingsproblemet. Detta problem existerar så länge man använder oskyddad hårdvara, något som en mobiltelefon i detta fall är.[11] En viktig insikt är också att en lösning likt den som testats i e-kronapiloten, vars säkerhet bygger på att nätverket upptäcker och stoppar eventuella försök till manipulation, blottas för risker om man tillåter att transaktioner sker utanför nätverkets övervakning, vilket ju är själva definitionen av offlinetransaktioner. Fysiska kontanter kontrolleras naturligtvis inte mot något nätverk när de används i en transaktion, men de kontrolleras i stället fysiskt av mottagaren, vilket inte är möjligt vid digitala betalningar. Digitala offlinebetalningar behöver kompletteras med ett regelverk som begränsar och hanterar riskerna. [12] Offlinetransaktioner gör det också möjligt att, i alla fall tillfälligt, göra transaktioner utan insyn vilket skapar risker för till exempel penningtvätt och andra brottsliga transaktioner. Därför lär en offlinefunktion behöva begränsas också med hänsyn till just de riskerna, trots att tekniken kan tillåta mer.

Exempel på några frågeställningar kopplade till offline och dess risker:

- Hur mycket pengar ska vara tillåtet att hålla i offlineläge?
- Hur stora transaktioner ska accepteras?
- Ska det vara olika regler för olika e-kronaanvändare (exempelvis konsumenter och handlare)?
- Hur många stegvisa offlinetransaktioner i följd kan tillåtas innan det behövs en synkronisering online med nätverket?
- Hur länge ska en användare tillåtas vara offline?
- Hur ska riskerna fördelas vid betalningar offline?

Det skulle också vara en teknisk utmaning att tillämpa regelverken på ett säkert sätt eftersom eventuella begränsningar, likt tokens, måste finnas i den lokala mobilen för

[11] Det görs mycket utveckling på hårdvara som är designad för att lagra data som ska vara mycket svåra att komma åt och manipulera, s.k. *tamper resistant devices*. Exempelvis speciella kort, dosor eller säkra områden på mobiltelefonens hårdvara. För att offlineanvändning ska fungera på en mobiltelefon krävs dock att en e-kronaapp får tillgång till det säkra området på hårdvaran vilket kräver samarbete med tillverkaren av hårdvaran.

[12] Det finns idag exempel på kortutgivare som tillåter sina kunder att göra transaktioner offline och där de medföljande riskerna med transaktionerna bärs och hanteras av kortutgivaren.

att fungera i offlineläge. Och då behöver de, likt tokens, kunna skyddas från manipulation.

Som bilden visar så har implementeringen i piloten gjorts så att den lokala plånboken med de lokalt lagrade e-kronorna endast är avsedd för offlinetransaktioner till andra lokala plånböcker. Det finns dock inga tekniska hinder för att använda en lokal plånbok med lokalt lagrade tokens även i onlineläge om så skulle önskas. Detta är en medveten avgränsning som vi gjort i piloten och det tål att fundera på om det kan finnas ett värde i att tydligt skilja pengar som är lagrade lokalt och tillgängliga för offlinetransaktioner från de som är lagrade i nätverket.

En orsak till att denna åtskillnad skulle behövas är också att de lokalt lagrade pengarna går förlorade om ägaren tappar sin lokala plånbok, eller om den går sönder. I och med att plånboken kan användas till transaktioner offline så är den per definition, under vissa perioder, utan synkronisering mot nätverket. Om det ska vara möjligt att få tillbaka lokalt lagrade pengar när betalinstrumentet är borttappat eller trasigt så kan det uppstå svårlösta situationer där det inte med säkerhet går att veta hur mycket e-kronor som fanns i det under offlineläget. Förslag på lösningar för att minimera sådana problem finns, men de skulle kunna bli praktiskt svåra att följa upp. En förlorad plånbok med offlinefunktion lär därför behöva betraktas på samma sätt som förlorade kontanter. Detta ser vi idag som ett problem som befintlig teknik inte har kunnat lösa.

2.4 Integrering med POS-terminal

Ett grundläggande mål med en eventuell e-krona är givetvis att den ska vara ett fungerande och gångbart betalmedel i den dagliga handeln, likt dagens betal- och kreditkort och i de flesta fall kontanterna. En betalning med de idag tillgängliga centralbankspengarna, de fysiska kontanterna, kräver endast en betalare och en mottagare för att betalningen ska kunna initieras och avvecklas. Idag genomförs dock majoriteten av betalningar i den fysiska handeln via POS-terminaler (Point Of Sale) enligt kortnätverkens och terminalernas regelverk. En digital betalning med någon form av kort involverar ett flertal olika kommersiella aktörer (kortnätverk, kortutgivare, terminalleverantörer etcetera) som alla behövs för att möjliggöra betalningen. Om Riksbanken ska etablera en e-krona på en digital betalmarknad i handeln måste Riksbanken förhålla sig till de etablerade kommersiella aktörerna och de redan existerande regelverken och protokollen.

En e-krona skulle kunna ha en väldigt oberoende och självständig position vilket skulle ställa högre krav på Riksbanken att designa och förvalta specifik e-kronautrustning i form av kort, terminaler och regelverk. Med helt egen mjukvara, hårdvara och protokoll skulle e-kronan kunna erbjuda en helt fristående betallösning vilket skulle göra betalmarknaden mer robust. Alternativet vore att integrera den med de andra aktörernas hårdvara och standarder. Detta skulle innebära att Riksbanken får mindre direkt ansvar men också blir mer beroende av kommersiella aktörer och deras infrastruktur, standarder och affärsmodeller.

Det finns idag standarder för säkerhet och verifiering av chip i kort och mjukvara i betalterminaler där den vanligaste vid namn EMV används av de stora kortnätverken.[13] Dessa terminaler är ofta fullt kompatibla med kassa- och bokföringssystemen hos butikerna i handeln och har hög säkerhet om de skulle bli utsatta för försök till manipulering av hård- eller mjukvara.

Piloten har i etapp 2 undersökt vilka olika alternativ som finns om man vill etablera en e-krona på en existerande POS-marknad och testat en teknisk integrering med en leverantör vars POS-terminaler finns ute på den svenska betalmarknaden. Målet var att tekniskt testa hur en e-krona i ett separat nätverk skulle kunna användas på terminaler som finns idag och som behandlar betalningar på de stora kortnätverken med deras protokoll.

Testad POS-integrering

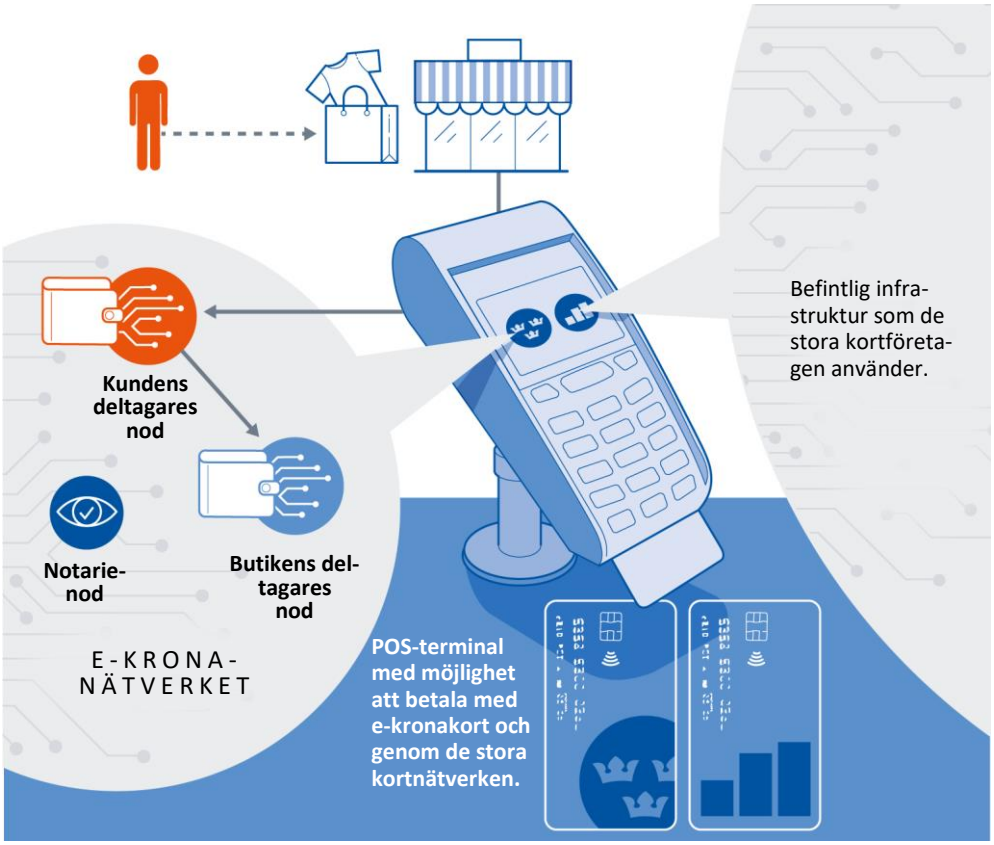
Under etapp 2 testades en POS-integrering som innebär att särskild mjukvara för e-kronan installeras i terminalen så att terminalen kan stödja e-kronabetalningar i e-kronanätverket. Dessa betalningar hanteras separat från de traditionella kortbetalningar som kan göras i samma terminal. Riksbanken ansvarar då på egen hand för mjukvaran, certifieringen av terminalleverantörerna och säkerhetslösningen för terminalerna. Upplägget kräver att Riksbanken når ut till terminalleverantörerna, tecknar avtal med dem och certifierar dem. Dessutom måste Riksbanken ansvara förs utveckla och förvalta den mjukvara och säkerhetslösning som är nödvändig för att e-kronan ska kunna användas i terminalerna.

När e-kronan integreras i en terminal kan leverantörerna ha olika regler och principer för hur man får kommunicera ut från terminalen. Den terminal vi testat tillåter kommunikation direkt från terminalen till e-kronasystemet. Andra leverantörer kan ha helt andra regelverk för hur kommunikationen ska gå via deras hårdvara, vilket kan göra e-kronan beroende av dessa aktörers IT-infrastruktur.

[13] https://www.emvco.com/

Diagram 6. Betalning i POS-terminal

Illustration över hur e-kronaspecifik mjukvara har implementerats i en POS-terminal som möjliggör betalningar med e-krona och andra kortnätverk i samma terminal. Slutanvändaren initierar köp med e-krona mot butikens terminal som kommunicerar direkt med e-kronanätverket. Betalningen genomförs genom deras deltagares noder i nätverket.



Lärdomar och reflektioner från POS-aktiviteten

Om en e-krona skulle lanseras så skulle det innebära att Riksbanken ger ut ett betalmedel på en betalmarknad där det finns befintliga aktörer och etablerade standarder för hur betalningar går till och hur deras säkerhet garanteras. Det är en tydlig skillnad mot dagens kontanter som i större utsträckning kan användas mer självständigt. För att e-kronabetalningar ska bli accepterade i handeln så är det en stor fördel om de kan integreras så smidigt och billigt som möjligt för handeln. Att anpassa e-kronan efter de standarder som redan används av de stora nätverken på kortmarknaden skulle kunna underlätta en etablering och minska Riksbankens arbete med att sätta upp egen mjukvara, regelverk, rutiner och förvaltning. Å andra sidan så är det inte en liten uppgift att fullt integrera en e-krona inom dessa kortnätverk och en parallell lösning kan också ha sina fördelar i och med att den kan göra betalmarknaden mer robust. Swish är ett exempel på en självständig betallösning som börjar etableras allt mer som ett betalmedel i handeln och som inte går över kortnätverkens regelverk. POS-aktiviteten i etapp 2 var konceptuellt liknande, dock som enbart teknisk aktivitet utan ett etablerat regelverk.

Testandet i e-kronapiloten har visat att det går att integrera e-kronanätverket genom att implementera e-kronaspecifik mjukvara och flöden på en etablerad terminal som

också hanterar de stora kortnätverken, vilket innebär att en handlare med terminalen kan ta emot betalningar med e-kronor och betalningar via de stora kortnätverken på samma terminal.

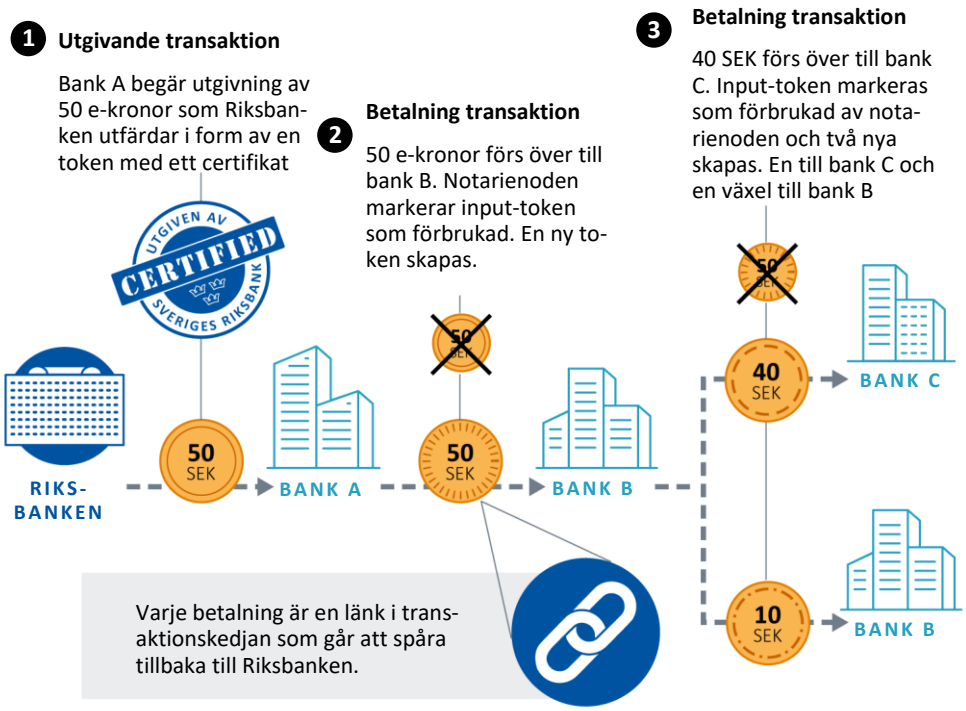
Vad som kan fungera som betalterminaler förändras också just nu där utvecklingen går mot att det även ska gå att använda vanliga mobiler som säkra terminaler. Detta kan skapa ökade möjligheter och flexibilitet för hur e-kronanätverkets betalningar kan integreras mot handeln. Genom att undvika kortnätverkens standarder undviker man en del komplexa frågor och får större frihet, som exempelvis Swish har visat. Om man vänder blicken mot omvärlden så ser man också att de stora initiativen på betalmarknaden, inom såväl CBDC som andra initiativ, fokuserar på de mobilbaserade betalningarna. Oavsett vilka betalinstrument som skulle kunna användas för en e-krona krävs regelverk och samverkan med handelns aktörer för att etablera e-kronan som betalmedel. För det kommande arbetet med e-kronan blir det viktigt att fortsätta utreda hur samverkansmodeller med marknadens aktörer skulle kunna se ut och även arbeta för att göra e-kronan flexibel för att följa den utveckling som sker på betalmarknaden.

2.5 Prestandatester

Ett av de viktigaste kraven på en potentiell e-krona är att den ska kunna användas till digitala transaktioner i realtid. I e-kronapiloten baseras e-kronan och dess nätverk på en teknik som ännu inte använts i produktion för de syften, transaktionsmängder och mönster som en e-krona skulle innebära. Ett viktigt fokusområde under etapp 2 var att fortsätta testa prestandan och att undersöka specifika egenskaper i lösningen som kan ha effekt på dess möjligheter att genomföra transaktioner i realtid. E-kronan i den tekniska lösning som vi testar är utformad som en så kallad token som representerar ett visst värde i e-kronor utgivna av Riksbanken. Varje transaktion med e-kronor består av en eller flera tokens (input) med e-kronor från betalaren som resulterar i en output-token till mottagaren med en eventuell output-token med växel tillbaka till betalaren. De tokens som används som input i en transaktion markeras som konsumerade och e-kronorna går vidare till mottagaren i form av en ny output-token som går att spåra tillbaka till de input-tokens där e-kronorna tidigare fanns. På så sätt skapar varje transaktion en länk till transaktionskedjor inom e-kronanätverket med spårbarhet till Riksbanken som utgivare som garanterar e-kronans äkthet. Detta sker hos deltagarna i nätverket och är inte synbart på något sätt hos slutanvändarna som är ovetande om hur många tokens som deras summa e-krona består av och dessa tokens transaktionskedjor.

Diagram 7. Transaktionskedja

Bilden ger en förenklad illustration över hur transaktionskedjor skapas i den tekniska lösningen där varje token har en spårbarhet till Riksbanken som utgivare av e-kronan.



Anm. De enskilda tokens i bilden har olika mönster för att illustrera hur de är unika och deras spårbarhet i en historisk transaktionskedja

Deltagarna i nätverket kontrollerar att e-kronorna är äkta och kan spåras till Riksbanken och notarienoden kontrollerar att en token inte använts tidigare. Att e-kronan i denna lösning är utformad som unikt identifierbara tokens som alla går att spåra till Riksbanken innebär att den på vissa sätt liknar de fysiska kontanterna. En sådan likhet är att endast Riksbanken kan skapa e-kronorna och de blir på så sätt enkla att särskilja från andra digitala pengar. Men de tillhörande transaktionskedjorna innebär att transaktionerna blir mer komplexa än i mer beprövade kontosystem. Det kan minska lösningens möjligheter att uppnå samma prestanda som de traditionella lösningarna.

För att ge ett enkelt exempel: En transaktion på 100 kronor i den testade lösningen kan bestå av en token med en väldigt kort historisk transaktionskedja vilket innebär en liten mängd information att validera och verifiera. Men den kan också bestå av en mängd olika tokens med olika långa historiska transaktionskedjor vilket innebär en större mängd information att validera och verifiera. Traditionella kontobaserade system som inte baseras på unikt identifierbara pengar har inte samma typ av information i ett saldo och därmed inte heller lika stor variation i hur mycket information som följer med en transaktion.

Under etapp 1 gjordes en första utvärdering av prestanda där man bland annat testade om det med 100 000 användare var möjligt att under 10 minuter genomföra i snitt 100 blandade transaktioner per sekund. Det visade sig möjligt men då var också

transaktionerna enkla och saknade en större mängd tokens med komplext sammansatta transaktionskedjor. Under etapp 2 har därför mer avancerade och utmanande tester utförts. De har designats för att vara lite mer ”stökiga” och verklighetstrogna i exempelvis sammansättningen av tokens, vilket kan påverka prestandan. Det övergripande målet har varit att undersöka om lösningen skulle kunna klara av transaktionsvolymer motsvarande Swishs och de större kortnätverkens volymer vid toppbelastning och kunna hålla genomsnittstiden för en transaktion kring en sekund. Testerna har utförts i en avgränsad testmiljö, begränsad till e-kronanoderna utan kopplingar till slutanvändarnas betalinstrument och till aliastjänsten.

Syftet med testerna var att undersöka vilka egenskaper i den tekniska lösningen och vilka scenarier som skulle kunna orsaka problem vid omedelbara transaktioner. Prestandatesterna undersökte bland annat följande:

- Vilken mängd transaktioner per sekund kan det enklaste scenariot klara? Det enkla scenariot innebär att transaktionerna består av få tokens utan långa transaktionskedjor.
- Hur påverkar längden på transaktionskedjan hastigheten i en transaktion?
- Vilken effekt har antalet tokens på nätverket och på transaktionshastigheten (frågan blir oftast aktuell vid större insättningar/växlingar)?
- Hur påverkar olika typer av transaktioner (utgivning från Riksbanken, uttag och insättningar från kunder, transaktioner inom nätverket och inlösen hos Riksbanken) nätverkets förmåga att leverera omedelbara transaktioner?

Lärdomar och reflektioner från prestandaarbetet

Testerna visar att i de enklaste scenarierna så kan den implementerade lösningen i den avgränsade testmiljön leverera transaktioner per sekund väl i nivå med Swish och kortnätverkens toppbelastning. Dock är dessa scenarier inte troliga i ett system som har varit igång under en tid. Då kommer systemet att bestå av många tokens uppdelade på små och stora värden med tillhörande transaktionskedjor, vilket innebär mer information att validera i transaktionerna. När testerna blir mer komplexa vad gäller exempelvis längden på transaktionskedjorna och antalet tokens i transaktionerna så blir det svårare att uppnå en viss prestanda. Det är framför allt när kedjorna blir väldigt långa och i testfall när mängden tokens ökar avsevärt som det blir problem med prestandan. Det gäller såväl transaktioner inom systemet som när e-kronor ska lösas in hos Riksbanken igen. När en plånbok har många tokens så tar det också längre tid att välja vilka tokens som ska ingå i en transaktion. Dessutom märktes det att det tar lång tid att summera ett saldo som ska visas i exempelvis appen när en plånbok har tusentals enskilda tokens. [14]

För en genomsnittlig privatperson med en e-kronaplånbok är sannolikheten låg att plånboken skulle innehålla så många tokens som i dessa exempel.[15] Men för en nä-

[14] Den version av Cordaplattformen som e-kronapiloten bygger på har också en skarp gräns som innebär att en transaktion som mest får bestå av 10 000 tokens.

[15] Under prestandaarbetet har även storskaliga simuleringar gjorts för att utreda hur tokens och tillhörande transaktionskedjor skulle kunna utvecklas hos systemets användare.

ringsidkare som ska kunna ta emot e-kronabetalningar i den dagliga handeln så kommer mängden tokens att snabbt kunna växa sig stor. Dessa utmaningar visar också på den fundamentala skillnad som finns mellan den testade tokenlösningen, byggd på en UTXO-modell, och en traditionell kontomodell. I en sådan kontomodell är det, lite förenklat, bara saldot som räknas upp och ner och en datapost för en transaktion som adderas, medan man i tokenmodellen måste verifiera, spara, uppdatera och spåra en varierande mängd dataobjekt.

Att designa tester med mer verklighetstrogna scenarier är svårt, inte minst med tanke på att det ännu är oklart exakt hur en e-krona skulle designas och vilken roll den skulle spela på den svenska betalmarknaden. De största utmaningarna med prestandan uppstår när betalkedjorna skapar en fragmentering av tokens som ökar mängden tokens i nätverket och betalningarna. Exakt hur denna fragmentering skulle se ut är svårt att veta på förhand. Prestandatesternas syfte var just att förstå i vilka situationer som lösningen med tokens och transaktionskedjor kan skapa problem med prestandan. Testerna har gett oss en bra uppfattning om detta och under arbetet har vi också från ett teoretiskt perspektiv diskuterat hur sådana problem skulle kunna undvikas.

De föreslagna lösningarna går ut på att designa en mer intelligent hantering av plånböckerna och deras tokens. För en handlare som tagit emot en mängd betalningar med tokens kan en regelbunden sammanslagning av dessa till en större token eller regelbunden insättning förhindra att prestandan får problem. För en deltagare som ofta tar emot förfrågningar om uttag av e-kronor från slutanvändare så kan det i stället vara mer optimalt att ha en större variation av tokens med olika mängd e-kronor. Genom automatiska inlösen och utbyten av äldre tokens med långa transaktionskedjor minskar man också mängden information att hantera i transaktionerna vilket skulle kunna gynna prestandan. De förslagna åtgärderna skulle behöva utredas mer för att säkerställa att de inte påverkar användarnas möjligheter att använda sina e-kronor. Det skulle även behövas vidare utredning för att förstå vilka övriga konsekvenser åtgärderna skulle kunna få för den tekniska lösningen och konceptuella modellen.

En viktig sak att komma ihåg är att en e-kronalösning likt den i piloten består av flera olika komponenter som alla påverkar lösningens prestanda. En stor del av arbetet för att förbättra prestandan har under etapp 2 ägnats åt att optimera e-kronamotorn och hanteringen av databaser. Prestandaarbete är också en kontinuerlig process som alla möjliga tekniska lösningar skulle behöva arbeta med för att garantera skalbarhet i systemet när mängden transaktioner ökar. Det tål också att understryka att arbetet i pilotens etapp 2 har byggt på version 4 av Corda och den plattformen förbättras ständigt, inte minst när det gäller just prestanda och skalbarhet.[16] För pilotens del har arbetet varit givande och hjälpt oss att identifiera vilka potentiella utmaningar lösningar av denna sort kan ha. Vissa lärdomar är förmodligen mer specifika för just den här lösningen och dess implementering. Andra lärdomar är mer generella och kan användas i det fortsatta arbetet med att jämföra olika potentiella lösningar.

[16] Corda 5 som är på väg att lanseras ska innehålla förbättringar bl.a. inom prestanda och skalbarhet.

3 Legalt arbete etapp 2

Den juridiska analysen har utgått från den tekniska lösningen i e-kronapiloten samt den juridiska analys som gjordes i etapp 1. Analysen i projektet visar att de uppgifter som följer med i transaktionskedjan sannolikt kan anses vara uppgifter som omfattas av finansiell sekretess och personuppgifter som omfattas av dataskyddsreglerna. Vidare har vi i etapp 2 fortsatt analysen kring vilket tillgångsslag e-kronan kan vara och kommit fram till att den skulle kunna betraktas som en elektronisk form av tillgångsslaget kontanter och ses som ett nytt alternativ och komplement till den fysiska form av kontanter som finns idag – sedlar och mynt.

3.1 E-kronan, finansiell sekretess och personuppgiftsskydd

Den typ av DLT/blockkedjeteknik som används i e-kronapilotens tekniska lösning innebär att man kontrollerar att tokens är äkta via den transaktionshistorik som följer med till mottagarens betaltjänstleverantör. Detta innebär att mer information delas mellan deltagarna i systemet än i traditionella betalningssystem. Under etapp 1 uppmärksammade projektet att det måste utredas hur denna informationsdelning förhåller sig till finansiell sekretess (används framöver som begrepp för både banksekretess och sekretess enligt betaltjänstlagen) och till dataskydd för personuppgifter.

Det är deltagarna i e-kronanätverket som är skyldiga att följa den finansiella sekretessen. Denna innebär att deltagarna inte får röja uppgifter om kunder för obehöriga. Vad gäller dataskyddsreglerna blir det fråga om huruvida behandlingen i nätverket uppfyller de krav som lagstiftningen ställer. Dessa rör bland annat ändamålet med uppgiftsbehandlingen och olika rättigheter för slutanvändarna, som rätten att få uppgifter raderade.

Det är oklart hur gällande rätt kring finansiell sekretess och dataskydd för personuppgifter förhåller sig till DLT/blockkedjeteknik. Detta är ett område där det är rimligt att tolka lagstiftningen med försiktighet med tanke på de rättigheter och intressen dessa regelverk är till för att skydda. Analysen i projektet visar att de uppgifter som följer med i transaktionskedjan sannolikt kan anses vara uppgifter som omfattas av finansiell sekretess och personuppgifter som omfattas av dataskyddsreglerna.

Som den tekniska lösningen som testats i piloten ser ut idag kan det inte uteslutas att uppgifter i nätverket behandlas på ett sätt som strider mot lagstiftningen om finansiell sekretess och dataskyddslagstiftningen. Det kan därför komma att behövas lagändringar och/eller informationssäkerhetsåtgärder om denna lösning ska uppfylla gällande rätt. Det kan också bli aktuellt med samråd med både den svenska och den europeiska dataskyddsmyndigheten för att få klarhet i hur en lösning baserad på DLT/blockkedjeteknik förhåller sig till dataskyddsreglerna.

3.2 E-kronan - en elektronisk kontant

Under etapp 1 jämförde vi e-kronan som betalningsmedel med de betalningsmedel som vi har idag. Så som e-kronan har utformats i piloten ansåg vi i den legala analysen att e-kronan uppvisade flest rättsliga likheter med kontanter. Under etapp 2 har den legala analysen av lösningen fördjupats och ett förslag på utformning av legala principer för e-kronan har arbetats fram, se Appendix.

En grundläggande fråga har då varit att analysera vad fysiska kontanter har för legal status idag för att sedan gå in på e-kronan i pilotlösningen. Projektet har gjort denna fortsatta analys med hjälp av en juridisk expert inom betalningar. Slutsatserna av den analysen är att fysiska kontanter historiskt sett har utgjort en fordran och att innehavaren har haft rätt till en viss mängd metall i utbyte mot det värde som kontanten representerade. Fysiska kontanter kan däremot idag inte längre anses representera en fordran i juridisk mening utan är i stället något eget, ett betalningsmedel med fristående värde (*sui generis*), som representerar ekonomisk makt/köpkraft. Det visas av att fysiska kontanter inte är räntebärande och inte kan preskriberas. Det finns idag inte heller något direkt krav som innehavaren av en sedel eller mynt kan ställa mot Riksbanken på utgivande av t.ex. en särskild metall. Det är istället ett förhållande som kan sägas bygga på ett förtroende för staten som garant av kontanternas värde.

Liksom fysiska kontanter representerar e-kronan i pilotens lösning ekonomisk makt/köpkraft. Enligt analysen kan den betraktas som en elektronisk form av tillgångsslaget kontanter och ses som ett nytt alternativ och komplement till den fysiska form av kontanter som finns idag – sedlar och mynt. I pilotens lösning är det tänkt att e-kronan ska vara skyddad om en deltagare går i konkurs, eftersom den tillhör slutanvändaren. Deltagarna ser till att slutanvändarna kan genomföra transaktioner i e-kronan och växla mellan e-kronor och andra typer av pengar. Däremot ska e-kronan inte ingå i deltagarens tillgångar när slutanvändaren väl betalt för den. Om pilotens lösning skulle bli verklighet innebär detta att ny lagstiftning skulle behöva komma på plats som ser till att e-kronan får det skydd och den rättsliga ställning som beskrivs här.

Att ha fysiska kontanter i sin besittning innebär vissa rättsliga konsekvenser. När det kommer till e-kronan som en elektronisk kontant skulle innehavet i stället kunna knytas till registreringen i den elektroniska plånboken. Plånboken är det instrument där e-kronorna förvaras, en sorts informationskonto (det kan även vara aktuellt med andra betalningsinstrument). Detta innebär bland annat att det inte får någon direkt rättslig betydelse var nycklarna till den elektroniska plånboken är placerade, något vi funderade över under etapp 1. Valet av teknik skulle alltså inte i någon direkt utsträckning påverka den legala utformningen, utan denna blir teknikneutral.

I och med att e-kronan i pilotlösningen skulle kunna anses tillhöra tillgångsslaget kontanter följer att de regler som är kopplade till fordringar inte är tillämpliga. Detta innebär att e-kronan i så fall inte kan uppbära ränta eller preskriberas enligt den lagstiftning som gäller för fordringar.

Om det finns anledning att begränsa storleken på innehaven av e-krona, alternativt ge incitament till att hålla e-kronor, skulle sådana styrmedel kunna införas i form av antingen beloppsbegränsningar eller avgifter/kompensation knutna till den elektroniska plånboken.

4 Fortsatta arbetet med e-kronan

Projektet går nu in i etapp 3. Arbetet har gett Riksbanken värdefull information om den testade lösningens möjligheter och utmaningar. Det har också varit en bra grund för att utreda generella tekniska och policyorienterade frågor och även vilket legalt ramverk en e-krona skulle kunna gå under. Etapp 3 kommer att fortsätta testa specifika delar av den tekniska lösningen men även rikta fokus på att förbereda målbilden för och kraven på den utgivningsbara e-kronan.

4.1 Den tekniska lösningens möjligheter att erbjuda programmerbara pengar och betalningar

DLT- och tokenbaserade lösningar sägs ofta ha en fördel jämfört med mer traditionella lösningar om man vill gynna innovationer inom betalningar. Begrepp som *programmerbara pengar, smarta pengar* och *smarta betalningar* sägs ofta vara framtiden för betalningar och detta används som ett argument för den nya tekniken. Begreppens innebörd kan variera men de syftar till möjligheten att genom programmering skapa nya effektiva sätt att utföra betalningar och pengar för speciella ändamål. E-kronapiloten har än så länge inte tittat specifikt på om, och i så fall varför, just DLT- och tokenbaserade lösningar skulle kunna gynna innovationer inom betalningar. Men det tekniska arbetet under etapp 3 kommer att fokusera på just det området. Vi vill testa och undersöka hur sådana lösningar kan användas för att skapa nya betaltjänster och varför de i så fall skulle vara effektivare än mer traditionella tekniker. Vi vill också undersöka om det skulle vara möjligt för marknadens aktörer att skapa innovationer utan att e-kronans grundläggande egenskaper riskeras och utan att Riksbanken som utgivare av e-kronan behöver vara direkt delaktig. Vi vill få en djupare förståelse för hur mycket substans det finns i de ofta förekommande argumenten för den nya tekniken och om de är relevanta för en potentiell e-krona.

4.2 Samverkansmodell för en e-krona

Som vi tidigare nämnt så skulle en e-krona enligt den testade modellen kräva ett samarbete mellan Riksbanken och aktörer på marknaden. Distributionsmodellen med deltagarna och POS-aktiviteten är två områden som testats tekniskt under etapp 2. Ett sådant samarbete med flera olika typer av aktörer kräver också någon form av samverkansmodell som definierar de olika parternas roller och ansvar. Om e-kronan ska

vara beroende av privata aktörer så behöver den ha en plats i deras verksamheter och affärsmodeller. Ämnesområdet omfattar också frågor om Riksbankens organisation för drift och förvaltning av en infrastruktur där Riksbanken samverkar med marknadsaktörer. Under etapp 3 kommer frågorna kring samverkansmodellen att utredas mer ingående.

4.3 Legala frågor

Det finns flera frågor att utreda vidare inom det juridiska arbetet. En viktig sådan är att ta ställning till om e-kronasystemet ska ses som ett avvecklingssystem, en annan att avgöra när en betalning är slutgiltigt genomförd. Detta måste klarläggas för att inte systemrisker ska uppstå. I piloten är utgångspunkten att avvecklingen av betalningen ska ske omedelbart och att e-kronorna inte ska ingå i deltagarens/intermediärens konkurs; frågan är därför vilka systemrisker som faktiskt kan uppstå i systemet. Om det ska betraktas som ett avvecklingssystem får det betydelse för vilka som kan delta i e-kronanätverket.

En fråga som identifierats och analyserats redan under etapp 1, och som det finns skäl att analysera vidare, är hur operativa risker och en deltagares eventuella fallissemang ska hanteras. Det blir i det sammanhanget intressant att diskutera vem som ska äga informationen i systemet och vilken samverkansmodell som en lösning kan bygga på.

Inom ramen för det legala arbetet kommer projektet också att fortsatt utreda och analysera den legala utformningen av en e-krona.

4.4 Utformning av och krav på den utgivningsbara e-kronan

Under året kommer Riksbanken också att fokusera mer på hur en eventuell utgivningsbar e-krona skulle se ut och fungera. Vi kommer därför att avsätta mycket tid och resurser till att ta fram sådana förslag. Alla tester, analyser och utredningar som hittills genomförts kommer att ligga till grund för det arbetet. En del av arbetet kommer att innebära att vi jämför den tekniska lösning som har testats med andra möjliga lösningar för en lanserad e-krona. Under våren kommer därför en så kallad *Request For Information (RFI)* att gå ut där aktörer på marknaden får beskriva hur deras föreslagna lösning skulle kunna fungera för en e-krona. Projektet kommer därutöver att ta in synpunkter från olika parter på betalmarknaden och från allmänheten.

APPENDIX – Förslag legal utforming e-kronan

E-kronan – en dematerialisering av fysiska kontanter

Nedan ges förslag på en legal utformning av e-kronan som baseras på en dematerialisering av fysiska kontanter:

Ett betalningsmedel utgivet av Riksbanken

- Fysiska kontanter och digitala kontanter – ”e-kronor” - ska samexistera och komplettera varandra.
- E-kronan ska utgöra ett lagligt betalningsmedel och vara en officiell representation av den svenska valutan (krona) på samma sätt som fysiska kontanter.
- Riksbanken ska ha rätt att ge ut betalningsmedlet kontanter i fysisk och i digital form. E-kronan innebär en dematerialisering av fysiska kontanter.
- Endast Riksbanken ska kunna ge ut och lösa in e-kronor. Det är viktigt att det är centralbanken (staten) som är ensam huvudman och att e-kronan inte sammanblandas med privata alternativ.
- Riksbanken har till uppgift att vårda e-kronornas funktionalitet och värde.
- Utgiven mängd e-kronor ska tas upp som en skuldpost i Riksbankens balansräkning på samma sätt som fysiska kontanter. E-kronor ska ha samma värde och rättsliga status som fysiska kontanter dvs. vara den digitala versionen/representationen av valutan (krona) .

Funktionaliteten för e-kronan

- Riksbanken ska tillhandahålla det betalningssystem som ska möjliggöra transaktioner i e-kronor. E-kronor kunna användas av allmänhet, företag (finansiella och icke-finansiella) och myndigheter som slutanvändare av betalningsmedlet.
- E-kronor ska vara föremål för erforderliga penningtvättskontroller.
- Riksbanken ska ha ensamrätt på att ge ut e-kronor.
- Det är huvudsakligen intermediärer som ska ansluta slutanvändare, distribuera e-kronor till slutanvändare samt möjliggöra transaktioner mellan slutanvändare.
- När slutanvändaren erlagt betalning för e-kronorna förvaras de i en elektronisk plånbok (ett digitalt förvaringsutrymme) eller annat anvisat betalningsinstrument t.ex. betalkort.
- Den elektroniska plånboken och andra anvisade betalningsinstrument tillhandahålls huvudsakligen till slutanvändarna av intermediärer. E-kronor ska vara

slutanvändarens egendom efter det att den placerats i slutanvändarens elektroniska plånbok.

- E-kronor får inte ingå i intermediärens tillgångsmassa efter det att den placerats i slutanvändarens elektroniska plånbok (eller annat anvisat betalningsinstrument) och ska vara skyddad vid intermediärens konkurs.
- E-kronor ska av slutanvändaren kunna användas till betalning och andra överföringar. Betalningar ska kunna genomföras omedelbart.
- En slutanvändare ska kunna köpa samt lösa in e-kronor mot andra typer av betalningsmedel hos intermediären.

Robust och tillgänglig i såväl normalläge som fredstida krissituationer och höjd beredskap

- För att e-kronan ska vara robust och effektiv, i såväl normalläge som i fredstida krissituationer och höjd beredskap, ska Riksbanken ges laglig rätt att styra och kontrollera distribution, tillgänglighet och funktionalitet av e-kronor. Detta bör ske genom att Riksbanken får befogenhet att äga infrastruktur, att ställa krav på intermediärer, slutanvändare och andra aktörer samt att bestämma vilka funktioner en elektronisk plånbok ska ha. För att uppnå detta bör Riksbanken ges rätt att fatta beslut, utfärda föreskrifter samt teckna avtal i frågor som rör e-kronan. Motsvarande befogenheter har Riksbanken vad gäller fysiska kontanter idag.

Reglering

- En reglering av e-kronan kan sannolikt göras utan en ändring av grundlagen men det kan vara lämpligt att göra grundlagen teknikneutral (idag är utgivningsmonopolet kopplat till sedlar och mynt) och att förtydliga att det endast är Riksbanken som får ge ut en e-krona. Därutöver krävs vissa ändringar i 4 kap. i den nya riksbankslagen (Prop. 2021/22:41) som reglerar Riksbankens mandat i fråga om kontanter och andra betalningsmedel samt kontanternas ställning som lagligt betalningsmedel. Sedan skulle det behövas en kortfattad och koncentrerad lag som tar sikte på de civilrättsliga förutsättningarna för och verkningarna av dispositioner med e-kronor (jfr särskilt 6 kap. lag (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument). Denna lag kan endera vara fristående eller föras in som ett särskilt kapitel i den nya riksbankslagen.

- Riksbanken ska kunna utfärda regelverk för tekniska eller monetära begränsningar på de elektroniska plånböckerna och/eller ta ut avgift eller ge kompensation på dessa om Riksbanken anser att detta är ändamålsenligt.

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

PRODUKTION SVERIGES RIKSBANK)
ISSN ISSN. (online)