Konceptförslag för anonym registerbaserad E-krona med offline-funktion

Vi har granskat *Riksbankens e-kronaprojekt Rapport 1* och vill poängtera att det går att uppfylla offline-funktion samt anonyma betalningar även för en registerbaserad e-krona vilket inte framgår från Tabell 1, sida 19.

I valet mellan ett distribuerat eller registerbaserat system bör beaktas exakt vilket problem som ska lösas samt för och nackdelar med respektive lösning. Vår slutsats är att fördelarna med ett distribuerat system, t.ex. det som Bitcoin bygger på, kommer väl till pass där en naturlig central nod saknas men inte nödvändigtvis tillför fördelar för E-kronan.

Då Riksbankens har fler uppdrag än att verka för att betalningarna kan ske säkert och effektivt kommer Riksbanken även i framtiden vara en naturlig central nod i det svenska betalsystemet. Detta är en egenskap som ett tekniskt system kan dra stora fördelar av och det är mot denna bakgrund vi baserat vårt förslag på en registerbaserad lösning vilket vi redogör för nedan.

Konceptet bygger på digitalt signerade e-checkar som kan användas både offline och online. Den som betalar utfärdar och signerar en e-check till en viss betalningsmottagare. När betalaren eller betalningsmottagaren går online (vilket kan vara omedelbart) skickas e-checken till Riksbanken för signering och validering att betalaren har täckning för e-checken. Konceptet tillåter, om det är önskvärt, anonyma betalningar genom att tillåta konton utan identifierade kontoinnehavare.

Terminologi

- E-konto: Digitalt konto fört av Riksbanken som enbart innehåller kontots balans.
- E-balans: E-kontots balans, signerad av Riksbanken, för att kontoinnehavaren ska kunna bevisa att denne hade en viss balans vid en viss tidpunkt.
- E-check: En av betalaren signerad betalningsinstruktion med information om från vilket e-konto, till vilket e-konto en viss summa e-kronor ska överföras.
- E-giro: Digital adress som refererar till ett e-konto. E-giroadresser allokeras av Riksbanken, hanteras av E-notarier och innehas av identifierade kontoinnehavare.
- E-notarie: Av Riksbanken utsedda betrodda aktörer som har till uppgift att göra ID-kontroll av kontoinnehavaren varpå ett E-certifikat utfärdas för E-girot.
- E-certifikat: En av E-notarie signerad uppgift om vem som är innehavare av ett visst E-giro.
- E-utdrag: Digitalt kontoutdrag för ett E-konto. Sparas enbart hos kontoinnehavare och om så önskas hos externa parter för backup och möjliga tilläggstjänster.

Transaktionsförfarande

Betalaren slår upp betalningsmottagarens e-giro mot ett centralt register för att få reda på vilket e-konto som för tillfället är kopplat till e-girot. För fall då det centrala systemet är otillgängligt kan betalaren även fråga betalningsmottagaren själv om vilket e-konto betalningen önskas till.

Om betalaren är offline frågar betalarens enhet betalningsmottagarens enhet om offline-betalning accepteras. Exempelvis kan vissa betalningsmottagare välja att acceptera enbart online-betalningar och andra enbart offline-betalningar från identifierade e-giron medan vissa till och med kanske är beredda på att acceptera offline-betalningar även från oidentifierade e-konton. Riskaptiten hos betalningsmottagare är utanför detta förslag och lösningar därtill lämpas bäst för marknaden att hantera.

Att man kan ha en e-giroadress istället för enbart ett e-konto är för att man ska kunna byta e-konto och samtidigt låta betalare som har e-giroadressen sparad kunna fortsätta att göra betalningar till samma adress.

Betalaren signerar med sin nyckel en e-check för en transaktion från ett av sina e-konton till betalningsmottagarens e-konto. Om betalaren är online så skickas e-checken direkt till Riksbanken som kontrollerar att tillräcklig e-balans finns på betalarens e-konto, minskar e-balansen med transaktionsbeloppet samt signerar e-checken.

Betalaren och betalningsmottagarens konton med dess balanser är utspridda på olika serverkluster-noder hos Riksbanken. Betalarens riksnod är den som signerar e-checken och ansvarar för betalarens balans. Efter att e-checken är signerad skickar betalarens riksnod e-checken till betalningsmottagarens riksnod. Först när betalningsmottagarens riksnod har mottagit e-checken och verifierat att signaturen av e-checken inte redan har behandlats (genom att göra en uppslagning mot en lokal lista över alla signaturer av e-checkar som har mottagits av betalningsmottagarens riksnod) ökas betalningsmottagarens balans med transaktionsbeloppet. Detta är bara ett exempel på hur systemet kan designas, konceptet som sådant är teknikneutralt.

Oavsett om betalaren är online eller offline så krypteras nu e-checken, inklusive de signaturer den erhållit, och skickas direkt till betalningsmottagarens enhet utan mellanhänder, vilket exempelvis kan ske genom scanning av QR-koder, WiFi, Bluetooth, Internet, eller andra överföringsmekanismer. Värt att notera är att dessa nätverk kan vara okrypterade då själva e-checken krypteras så att den enbart kan läsas av betalningsmottagaren.

E-checken visas för betalningsmottagaren på dess enhet med information om betalarens identitet ifall betalaren valt att visa denna för betalningsmottagaren samt i de fall betalningen skett online, att Riksbanken dragit pengarna från betalarens e-konto och allokerat pengarna för att betalningsmottagaren ska kunna lösa in dessa till sitt e-konto.

Om betalningen skett offline så kommer både betalaren och betalningsmottagaren att skicka e-checken till Riksbanken så fort de kommer online eller vid driftsavbrott så snart avbrottet upphört.

Åtaganden

	Riksbanken	Marknaden
Registerföring av e-balanser	X	
Registerföring av e-giroadresser	X	

Kontrasignering av e-checkar	X	
Utfärdande av e-certifikat	X	X
ID-kontroll och hantering av e-giron		X
Utveckling och drift av terminaler och mjukvara för betalare och betalningsmottagare		X

Säkerhetsmodell och krypteringslösning

Tre krypton med olika ursprung används i kombination så att säkerheten inte äventyras även om säkerhetsbrister skulle upptäckas i upp till två av kryptona. För att kunna kryptera och avkryptera krävs tillgång till samtliga tre nycklar. På användares enheter används samtliga tre kryptonycklar, vilket ger skydd mot enskilda brister i krypton.

Hur anonyma behöver betalningar vara?

Slutligen vill vi poängtera att begreppet anonymitet gällande e-kronan bör sättas i relation till hur anonyma andra betalsätt är, där kontanter ofta är riktmärket för anonyma betalningar. Med dagens teknik skulle det för banker och handlare inte vara några tekniska problem att spåra sedlars serienummer, vem som hämtar ut dem i en bankomat och hur de senare används. Det är således enbart en regelefterlevnad bland inblandade parter som gör kontanter anonyma. Anonymiteten i förslaget ovan bygger på att Riksbanken följer reglerna och enbart sparar e-balanser och inte själva transaktionshistoriken för enskilda e-konton. Som jämförelse kan nämnas att för DLT-baserade kryptovalutor är transaktionshistoriken publik vilket leder till en möjlighet för vem som helst att analysera enskilda konsumenters betalningsmönster.

Finansiell inkludering

För att nå full finansiell inkludering tillåts anonymt skapande av e-konton på valfri enhet och plattform. Därför bör hela systemet vara open source för att även öka samarbetet och vidareutveckling av systemet hos andra riksbanker.

Joel Jakobsson, medgrundare Trustly
Lukas Gratte, medgrundare Trustly
Victor Jacobsson, medgrundare Klarna
Christian Ander, grundare btcx
Marcus Boström, entreprenör