Olika användningsområden som riskfaktor: Bank-ID för Swish och buss

– En dunderblunder som snart rättas till?

Claes Martinson, Göteborgs universitet

1

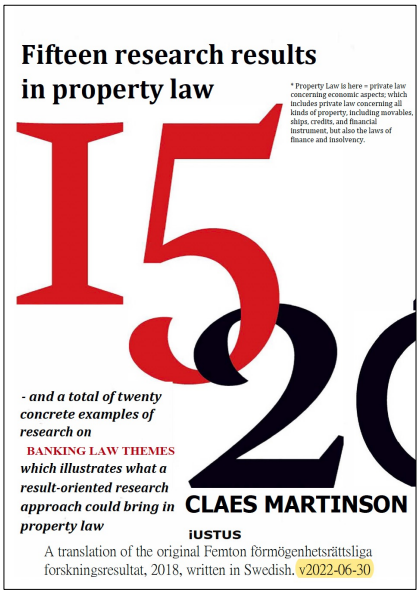
Tidigare projekt kring obehöriga korttransaktioner

Redovisat i boken

Femton förmögenhetsrättsliga forskningsresultat, 2018.

Resultat: ARN:s hantering föreföll avvika från lagstiftarens intentioner, såsom de uttryckts över tid.

En tydlig parallell till den hantering vi sett av fallen av obehöriga transaktioner.



2

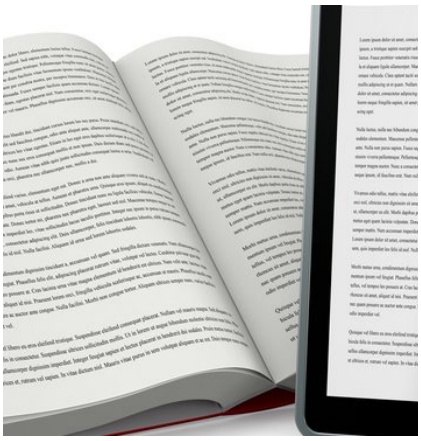
En annan angränsande studie – rättsföljderna av obehörig användning av e-legitimation

Särskilt om rättsföljderna av vissa av fallen, där "pengarna flyttas vidare".

Återställa kontot vs bättre rätt till "pengarna"

Relationell modell vs objektsmodell

Realism vs fiktion



3

Olika användningsområden som riskfaktor

- BankID har i dag fått så stort genomslag att det i många fall inte går att köpa ens en bussbiljett utan att använda sitt BankID och detsamma gäller vid små transaktioner som genomförs med hjälp av Swish.
- Men hur bra är det egentligen ur säkerhetssynpunkt att man som resenär förväntas stå på busshållplatser eller på bussar/spårvagnar och slå in sin kod i BankID:et inför ögonen på andra, och vad värre är, inför övervakningskameror och mobilkameror?
- Kan förväntningen om användning av BankID för småsaker i det offentliga rummet bidra till att konsumenter underskattar de risker som finns om ens BankID skulle komma på avvägar?
- Och är det verkligen nödvändigt att använda högsta grad av säkerhet även för små belopp?

4

Projektet – en förstudie

Kunskapsintresse: rättsligt relevant kunskap om användande av bank-id för transaktioner i offentliga miljöer.

Forskningsfråga: Vilka rättsliga faktorer kan bli styrande i sådan mån att ett system som bank-id blir använt för transaktioner i offentliga miljöer?

Metoder (så här långt):

i) identifiera normativa rutiner avseende hantering av samhällsrisk i sammanhanget betalningstransaktioner

ii) identifiera relevanta rättskällor; dvs författningstexten och förarbeten etc

iii) undersöka hur några personer som arbetar med att sälja tjänster respektive bygger system resonerar.

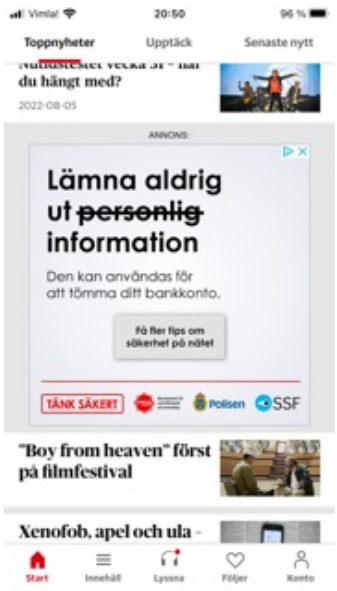
Resultat (så här långt): Inget resultat, men tesen att den handlingslogik som regleringen genererar är en annan än intentionerna med författningen, dvs med den rättsliga logiken.

5

i) normativa rutiner avseende hantering av samhällsrisk i sammanhanget betalningstransaktioner

Hur brukar man resonera kring användar-id och lösenord?

Svar: Använd inte samma användar-id och lösenord för olika verksamheter eftersom det ökar riskerna!



6

Förändringen

Den typiske användaren använde Bank-ID i lugn och ro, ensam i en avskild inomhusmiljö. Möjligheten för någon annan att snappa upp koden var därmed mycket liten. Därmed påverkades också möjligheterna att komma åt digitala banktjänster.

Numera även offentliga miljöer, såsom lokaltrafikföretag och betaltjänsten Swish. Dessa används i helt andra miljöer än i lugn och ro, i ensamhet i ett rum. Andra människor runt omkring, det finns övervakningskameror och det finns mobilkameror.

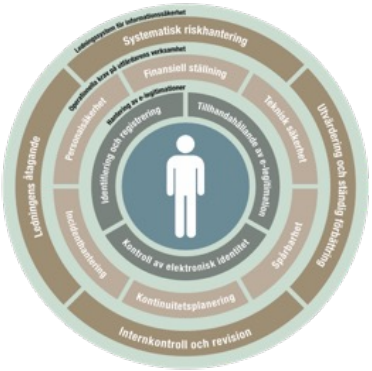
Att snappa upp koden som en användare slår in är i dessa miljöer definitivt möjligt.

Att hugga av någons finger för att komma åt bank-id är också möjligt.

7

Vägledning och krav från myndighet

Tillitsramverket för Svensk e-legitimation: Tillitsnivåer



Möjliga konsekvenser vid felaktig identifiering

Riskområde	Tillitsnivå 1	Tillitsnivå 2	Tillitsnivå 3	Tillitsnivå 4
Olägenhet, oro eller ryktesskada	Begränsad	Måttlig	Betydande	Allvarlig
Finansiell skada eller skadeståndsansvar	Begränsad	Måttlig	Betydande	Allvarlig
Röjande av känsliga uppgifter till obehöriga	*Ska inte användas*	Måttlig	Betydande	Allvarlig
Brottsyttringar	*Ska inte användas*	Begränsad	Betydande	Allvarlig
Skada på verksamhet och allmänintresse	*Ska inte användas*	Begränsad	Måttlig	Allvarlig
Personsäkerhet	*Ska inte användas*	*Ska inte användas*	Måttlig	Betydande

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

8

ii) identifiera relevanta rättskällor

eIDAS-förordningen;

dvs EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

I artikel 8 stadgas att det skall finnas olika tillitsnivåer i system för elektronisk identifiering

Syftet är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, osv.

9

forts … ii) identifiera relevanta rättskällor

Betaltjänstlagen 2010:751

1 kap 7 § Denna lag gäller inte betalningstransaktioner som ...

8. genomförs via en leverantör av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster vilken fungerar som mellanhand, om betalningstransaktionerna faktureras på leverantörens faktura och

a) avser inköp av digitalt innehåll och röstbaserade tjänster, eller

b) genomförs från eller via elektronisk utrustning för välgörenhetsändamål eller för inköp av biljetter.

En förutsättning för undantag enligt första stycket 8 är att värdet på de enskilda betalningstransaktionerna inte överstiger ett belopp motsvarande 50 euro och betalningstransaktionernas sammanlagda värde för en abonnent inte överstiger ett belopp motsvarande 300 euro per månad.

10

forts … ii) identifiera relevanta rättskällor

SOU 2016:53 s 15, 187-189

”undantag från betaltjänstlagens tillämpningsområde ska göras för bl.a. betalningstransaktioner som genomförs med hjälp av mobiltelefoner eller annan teknisk utrustning, t.ex. vid köp av en SMS-biljett för en resa.”

Prop. 2017/18:77 s 135-136

”I de fall där t.ex. en systemoperatör bara agerar som mellanhand i en betalningstransaktion, som vid köp av en sms-biljett för en resa, aktualiseras undantaget …”

11

forts … ii) identifiera relevanta rättskällor

Marianne Rødvei Aagaard, JT 22-23 s 77-78

”Dessutom kan det diskuteras om det verkligen är nödvändigt (och ur säkerhetssynpunkt acceptabelt) att **beställning av nya betalningsinstrument** kan göras så snabbt och enkelt som idag. Det som ur praktisk synvinkel är mycket lyckat, nämligen att ett och samma verktyg med stor lätthet kan användas för olika ändamål och i olika sammanhang, blir i detta sammanhang en omständighet som kan skapa osäkerhet kring regleringens tillämpning.”

12

iii) undersöka hur några personer som arbetar med att sälja tjänster respektive bygger system resonerar

Kundtjänstpersonal och överordnade vid ett regionägt lokaltrafikföretag

Svarade med totalt oförstående – svaren gick ut på att ”det står i lagen”

Systemvetarpersonal vid samma region
+ Programmerare

Svarade med att riskerna är tillräckligt låga, eftersom det krävs att de obehöriga kommer åt själva telefonen,
(eller har utvecklat ett mycket sofistikerat system för att simulera telefonen).

13

Är projektet/förstudien relevant?

Vad kan eventuell fortsatt forskning generera för kunskap?

Resultat (så här långt): Inget resultat, men tesen att den handlingslogik som regleringen genererar är en annan än intentionerna med författningen, dvs med den rättsliga logiken.

Tänkbara orsaker

a) de tekniska aspekterna blir i hög grad blir normerande,

b) vilken kritik som de ansvariga föredrar att värja sig mot.

14