## Notat

Til
Transportministeriet

**Rejsekort A/S**

3. Februar 2010

Kopi til

Journal: D13193

**Redegørelse fra Rejsekort A/S**
Under overskriften ” Elektroniske rejsekort er endnu en offentlig IT – skandale ”, bragte TV Avisen den 27. januar 2010 en række påstande, som hermed kommenteres.

I indslaget i TV Avisen fremgik det, at man ved hjælp af en kortlæser og programmer fra internettet nu kan hacke kortet og læse alt, hvad der står på kortet. Dette er ikke nyt, men har været kendt siden de første rapporter om hacking i Holland kom i efteråret 2007.

Det bør dog bemærkes, at der på selve rejsekortet findes forholdsvis få oplysninger, og at de oplysninger, som DR kunne ”hacke” sig til, i øvrigt kan fås i en Rejsekortautomat eller ved henvendelse på et betjent salgssted. Hacking synes dermed at være en ganske besværlig metode til at skaffe sig de oplysninger fra rejsekortet, som DR redegjorde for i indslaget. Det skal endvidere bemærkes, at der på kortet alene fremgår billetoplysninger og kortets saldo. Personlige oplysninger, navn, cpr eller kontooplysninger, lagres ikke på kortet.

I indslaget fremgik endvidere, at man også nemt kan ændre indholdet på kortet”, samt ”på den måde kan man fylde op med penge uden at betale en kr for det. Hertil bemærkes, at ændring af indholdet, herunder øgning af kortets saldo, er beskyttet af flere særlige mekanismer. Det er endnu ikke vist, at nogen har kunnet ændre på kortet eller øge kortets saldo korrekt.

Det skal endvidere bemærkes, at den saldo der står på kortet, alene er en repræsentation af kundens tilgodehavende af de forudbetalte penge (saldo), der er registreret i det bagvedliggende Back-office system. En ændring af kortets data/saldo vil medføre at kortet spærres inden for 24 timer, idet der i Back-office dagligt foretages en gennemgang og verifikation af kortsaldi og ændringer heri. I værste fald vil der kunne rejses i et meget kort tidsrum, indtil spærringen er distribueret til alt udstyr. Der udbetales alene penge tilbage til kunder på basis af oplysninger i back-office, ikke på bag-

grund af oplysninger på kortet.

En hacker vil således ikke kunne skaffe sig rede penge – men i værste fald alene et begrænset antal gratisrejser - ved en hackning som beskrevet i DR's indslag. Den økonomiske risiko herved bæres af Rejsekort A/S. For den enkelte kunde er der ingen risiko, hvis man mister kortet, kan kunden spærre det, og kunden vil ikke komme til at hæfte for misbrug, der måtte følge af andres hacking.

I indslaget blev nævnt, at Holland allerede i 2007 besluttede, at kortene var for usikre. Direktør for Rejsekort i Holland Jeroen Kock siger "*We have prepared to go to the next level with new cards and cardreaders*". I Holland, der var det første land, hvor problemet med hacking af kort til den kollektive trafik blev aktualiseret, har man vedtaget en plan for, hvorledes sikkerheden i det Hollandske system kan højnes i løbet af de kommende 5 år ved en successiv udskiftning af kort. Den hollandske beslutning om at øge sikkerhedsniveauet skyldes en række forhold, og ikke alene den potentielle risiko for hacking, som DR har beskrevet.

I indslaget udtaler Professor Bart Jacobs, at *"samme kode gør et svagt system endnu svagere. I Holland har hver kort sin kode, der skal du bryde hvert kort. I Danmark har du brudt alle, når koden er brudt."*
Sikkerhedssystemerne i Holland og Danmark er dog ikke ens. Sikkerhedsniveauet i det danske system er på niveau med, eller højere, end de fleste andre tilsvarende systemer i verden.

I indslaget påpeges det, at det man er bange for er, at der laves et program, der på computer eller mobiltelefon automatisk kan tanke penge på.. Bart Jacobs udtaler i den forbindelse: *" If this happens in really, really large scale the system brakes down".*

Det er endnu ikke vist, at nogen har kunnet ændre på kortet eller øge kortets saldo korrekt. En ændring af kortets data/saldo vil medføre, at kortet spærres. Systemet er dimensioneret til at kunne håndtere store mængder af spærringer.

Til indslagets spørgsmål om, hvorfor systemet ikke udskiftes nu, må fremhæves, at den aktuelle debat er baseret på én "hackers" demonstration af sine evner. Der er international enighed om, at der ikke er tegn på noget faktisk misbrug af de over 200 mio kort, der allerede er i omløb.

Der er blandt trafikselskaber verden over stor enighed om, at den økonomiske risiko er minimal.  Beslutningerne i andre lande om at højne sikkerheden tager udgangspunkt i imagemæssige eller andre argumenter, og sådanne tiltag indføres successivt, i takt med en naturlig udskiftning af kort,

og over en længere årrække.

I Rejsekort følges situationen internationalt og Rejsekort A/S deltager i flere fælles fora, hvor sikkerhedsforhold bliver behandlet. Afgørende elementer ved valg af kort er forsyningssikkerheden, dvs. at kortet produceres af flere leverandører og anvendes i store kvantiteter på verdensplan, således at vi kan være sikre på at kunne få kortet leveret i de næste mange år, og til konkurrencedygtige priser.

Det kort, som Rejsekort benytter, er det så kaldte MiFare Classic. Dette kort er valgt, især da det er det af trafikselskaber verden over foretrukne kort. Kortet produceres i store mængder af flere leverandører, og der er udstedt over 200 mio. Det faktum at vi har valgt det mest foretrukne kort (det er en hyldevare), gør naturligvis, at dette også er hackernes foretrukne.

Der er ikke på nuværende tidspunkt et åbenlyst alternativ til det nu anvendte kort (MiFare Classic), men der pågår internationalt overvejelser om, hvad der bliver den generelle afløser.

Det er den aktuelle vurdering fra eksperter på området, at uanset situationen, så er Mifare Classic meget bedre beskyttet mod snyd end de nuværende papirbaserede kort og billetter.

Afslutningsvis skal der gøres særlig opmærksom på, at fremstilling af falske kort og misbrug af kort vil medføre en politianmeldelse og deraf følgende alvorlige konsekvenser, der langt overgår de afgifter, der opkræves ved rejser uden gyldigt kort eller billet.