

Pericolele pașapoartelor electronice:

1) citirea datelor cu caracter personal (nume, prenume, CNP, naționalitate, vârstă, etc.)

Aceste date pot fi folosite pentru deschiderea unor conturi bancare. Pot fi folosite, de asemenea, pentru achiziționarea de proprietăți, derularea de licitații electronice, înființarea unor societăți comerciale fantomă. Toate acestea în scopul desfășurării unor activități ce implică spălarea de bani, excrocherie, crimă organizată, terorism și altele asemenea. Dat fiind că datele folosite sunt ale dumneavoastră, deci date reale, pe de-o parte tranzacțiile vor decurge ușor, falsul fiind greu de descoperit, iar pe de altă parte nu veți putea dovedi că altcineva a făcut aceste lucruri decât extrem de greu și de încet (în unele cazuri, deja întâlnite în S.U.A. la furturile de identitate, victima va fi în pușcărie înainte să-și poată dovedi nevinovăția și va avea nevoie de ani de zile pentru a ieși – cu o viață distrusă).

2) citirea datelor cu caracter biometric (amprenta digitală, amprenta facială, amprenta retinei)

Pot fi folosite pentru clonarea amprentelor digitale și amprentelor de retină (lentile de contact personalizate). Pot fi folosite pentru a avea ulterior acces la anumite informații securizate ale persoanei respective sau la locul de muncă al acesteia (multe calculatoare și instituții folosesc genul acesta de control al accesului). Pot fi folosite pentru plantarea de probe false la locul unei infracțiuni, în special a amprentelor, care sunt cel mai ușor de clonate (pe suport de latex). Pot fi folosite pentru confecționarea de măști personalizate sau trucare de înregistrări de imagini – adăugându-se amprenta dumneavoastră facială la locul comiterii unei infracțiuni.

3) clonarea cip-urilor, modificare datelor și atașarea lor la un alt pașaport

Clonarea înseamnă citirea datelor de pe un cip urmată de scrierea lor, în aceeași formă, pe alt cip și atașarea acestui nou cip la un alt pașaport. Nu trebuie (neapărat) să fie modificate datele de pe cip-ul original (deși se poate face asta, iar adevăratul posesor al datelor poate fi transformat în „infractor”). Modificările pot fi făcute pe cip-ul "clonă", care urmează să fie atașat la pașaportul fizic falsificat în prealabil (sau pur și simplu cumpărat de la firma producătoare – legal sau nu – cu un cip fără date). Se înțelege că în felul acesta falsul este aproape imposibil de detectat, pașaportul fiind declarat 100% valid de către cititorul RFID, singura speranță rămânând, ca și până acum, în ochiul vigilent al vameșului. Dacă datele sunt clonate pe un pașaport original cumpărat pe sub mână – lucru ușor de făcut în orice țară în care există corupție – atunci falsul nu poate fi descoperit decât cu totul excepțional. Victima nu va avea nicio șansă să se justifice în libertate, odată ce infracțiunile au fost comise de purtătorul unui asemenea pașaport. Va intra în închisoare și va trebui să adune dovezile nevinovăției sale de acolo. Viața socială îi va fi distrusă, cariera de asemenea. Problema cea mai gravă este că aceste falsuri vor putea fi făcute cu datele reale ale unei persoane. Până acum măcar falsurile se făceau cu date personale la rândul lor false, care puteau fi mai ușor detectate.

4) urmărirea individului purtător de act electronic cu cip

Cip-ul pașaportului se identifică printr-un număr unic ce ține de țara din care provine. Chiar dacă datele personale de pe pașaport nu pot fi accesate decât de la distanțe relativ mici, cip-ul poate fi scanat după acest ID unic de la distanțe extrem de mari. Oficial, cip-ul poate fi accesat în bune condiții de la distanța de minimum 10 cm. Asta înseamnă ca el are o "dimensiune" radio sferică, având un diametru minim de 20 de cm. Cel mai mic obiect care poate fi oficial interceptat fizic de un satelit civil aflat pe o orbită joasă este de 30 cm. Un satelit militar depășește cu mult această performanță. Deci, posesorul unui pașaport cu un anumit ID poate fi identificat și urmărit prin satelit.

Persoanele purtătoare de pașaport cu un anumit ID național pot astfel deveni extrem de ușor ținta unor atentate teroriste punctuale. Pot fi realizate, de pildă, atacuri teroriste cu bombă sau arme chimice plasate în anumite containere, în aeroporturi, și care să nu se declanșeze decât în momentul în care pe lângă locația respectivă trece un purtător (sau un grup de purtători) de pașaport electronic dintr-o anumită țară. De asemenea, rețelele de spionaj pot beneficia din plin de aceste neajunsuri în activitățile lor curente.

5) sustragerea datelor personale și biometrice din bazele de date Schengen

Oficial, datele din noile pașapoarte biometrice urmează să fie centralizate într-o bază de date unică la nivel european, cu terminale în toate statele membre Schengen. Auditul de securitate pentru această bază

nu a fost făcut niciodată public. Atâta vreme cât servere cu lungă tradiție (NASA, Pentagon, etc.) cad victime periodic atacurilor informatice de tot felul, nu avem niciun motiv să credem că baza SIS II, atât de atrăgătoare pentru crima organizată și pentru alte activități infracționale, va reprezenta o excepție. Odată ajunse pe mâinile rețelelor de crimă organizată, eșantioanele de date biometrice vor putea fi folosite în modurile arătate mai sus pentru a crea un adevărat haos infracțional și social. Recuperarea acestor date va fi practic imposibilă, ele putând fi transmise în câteva clipe în orice colț al lumii. Oamenii ale căror date biometrice au fost furate nu vor mai putea niciodată să aibă o viață liniștită. Dacă privim datele biometrice ca pe o *cheie* a identității personale, să nu uităm că această cheie *nu poate fi schimbată*. Dacă datele biometrice au fost furate, nu pot fi înlocuite în niciun fel și mereu vor apare noi și noi incidente, accidente, contravenții și infracțiuni pentru care omul ale cărui date au fost furate va trebui să se justifice. Perspectiva este limpede și îngrozitoare: milioane de vieți distruse de introducerea actelor electronice!

Permisele de conducere cu cip propuse pentru România conțin și următoarele pericole suplimentare față de pașapoartele electronice:

1) citirea datelor cu caracter personal într-un mod extrem de facil

Spre deosebire de cip-urile RFID din pașapoarte, cele din permisele de conducere nu posedă niciun fel de sistem de criptare a datelor. Ele pot fi accesate de orice cititor compatibil cu frecvența dispozitivului. Orice infractor își poate procura un astfel de cititor la un preț de cca 200 euro. Adăugându-i o antenă performantă – de asemenea ușor de procurat la un preț modic – poate începe să scaneze datele celor care circulă pe stradă, dacă au asupra lor carnetul de conducere. Orice șofer este potențială victimă.

2) citirea datelor cu caracter personal folosind dispozitive compatibile GSM

Spre deosebire de cip-urile RFID din pașapoarte, cele din permisele de conducere funcționează la o frecvență înaltă (900 MHz) compatibilă cu cea GSM (GSM-900). Deci, anumite telefoane mobile pot fi modificate și folosite ca scannere improvizate (dar eficiente) pentru astfel de cip-uri. Distanța de citire este și ea, se înțelege, mult mai mare (anumite teste avansează distanțe extrem de mari, de ordinul sutelor de metri).

Inutil să spunem ce mană cerească reprezintă aceste lucruri pentru rețelele de crimă organizată și/sau spionaj. Presupunând ca un om nu poartă tot timpul pașaportul la el (decât atunci când călătorește), permisul de conducere îl poartă aproape sigur mai tot timpul la el.

Toate problemele prezente la pașapoarte se echivalează și în cazul permiselor, cu mențiunea ca acestea sunt MULT mai ușor de urmărit și accesat decât pașapoartele.

LUCIAN CORNIANU,
Președinte ACESDS,
Inginer fizician,
Inginer de sistem