

Jak przekonać, że pl.ID będzie bezpieczne?

<http://ipsec.pl/kryptografia/jak-przekonac-ze-plid-bedzie-bezpieczne.html>

Za niedawnymi problemami z bezpieczeństwem niemieckich elektronicznych kart identyfikacyjnych nieuchronnie muszą pojawić się analogiczne wątpliwości odnośnie pl.ID.

Computer Chaos Club [ja href="http://www.theregister.co.uk/2010/09/03/german_id_card_hack/" > zademonstrował jak niemieckich kart można osiągnąć dane biometryczne oraz kod PIN. Ekstrapolowanie tych \[ahref = "" > pl.ID nie jest uzasadnione bopolskie karty nie będą ani bezstykowe ani nie będą zawierać danych biometrycznych.\]\(http://www.theregister.co.uk/2010/09/03/german_id_card_hack/\)](http://www.theregister.co.uk/2010/09/03/german_id_card_hack/)

Informacje [ja href="http://cpi.mswia.gov.pl/portal/cpi/38/195/plID.html" > i na stronach CPI \[i/a\]\(http://cpi.mswia.gov.pl/portal/cpi/38/195/plID.html\) są co najwyżej szczątkowe. Jedyne informacje na temat bezpieczeństwa kart są sformułowane ogólnikowo i nie poparte żadnymi argumentami: {"obywatel nie będzie mógł odczytać danych zapisanych w warstwie elektronicznej", {"dowód osobisty będzie zabezpieczony zarówno w warstwie graficznej, jak i w części elektronicznej"} \(\[ja href="http://cpi.mswia.gov.pl/portal/cpi/346/1249/Ochrona_danych.html" > Ochrona danych \\). Zabawnym przykładem urzędniczej mowy konspiracyjnej jest sekcja \\[ahref = "http://cpi.mswia.gov.pl/portal/cpi/346/1262/Technologia.html" > Technologia , w której autorka w swojej wypowiedzi \\\("Jakie parametry techniczne będzie posiadał elektroniczny dowód osobisty"\\\) sama\\]\\(http://cpi.mswia.gov.pl/portal/cpi/346/1262/Technologia.html\\)\]\(http://cpi.mswia.gov.pl/portal/cpi/346/1249/Ochrona_danych.html\)](http://cpi.mswia.gov.pl/portal/cpi/38/195/plID.html)

Wiemy, że w polskiej administracji publicznej nie ma tradycji traktowania obywatela jako [ja href="http://pl.wikipedia.org/wiki/Interesariusz" > i interesariusza \[i/a\]\(http://pl.wikipedia.org/wiki/Interesariusz\) projektów robionych deklaracyjnie dla niego. Gdyby jednak CPI chciało wyjść na przeciw oczekiwaniom społeczeństwa informacyjnego i zapewnić sobie miękki lądowanie w razie odkrycia błędów w przyszłości to warto by podjęło następujące działania:](http://pl.wikipedia.org/wiki/Interesariusz)

- {"Sporządzenie jakościowej analizy ryzyka systemu pl.ID. Umożliwi zademonstrowanie, że CPI zidentyfikowało ryzyka, na które narażony jest system i odpowiednio się przed nimi zabezpieczyło, zaś urzędnicy i obywatele będą świadomi przed czym system chroni, a przed czym nie. W szczególności umożliwi to uniknięcie w przyszłości żenujących sporów w rodzaju kłótni o różne znaczenia "bezpiecznego urządzenia" ([ja href="http://ipsec.pl/podpis-elektroniczny/klotnia-o-dziury-w-e-podpisie-g-data-vs-certum.html" > i G DATA vs Certum \[i/a\]\(http://ipsec.pl/podpis-elektroniczny/klotnia-o-dziury-w-e-podpisie-g-data-vs-certum.html\)\). i {"Zamówienie niezależnej oceny bezpieczeństwa architektury projektu. Pozwoli to zademonstrować, że architektura nie jest oparta o widzimisie studenta ostatniego roku AGH zatrudnionego przez wiodącą polską spółkę informatyczną na stanowisku {senior security architect.](http://ipsec.pl/podpis-elektroniczny/klotnia-o-dziury-w-e-podpisie-g-data-vs-certum.html)
- {"Zamówienie niezależnego testu penetracyjnego systemu. Pozwoli to zademonstrować, że CPI uniknęło popełnienia błędów implementacyjnych np. w wyniku nieroztropnego zawierzenia producentowi jednej z technologii. Na dłuższą metę pozwoli to również uniknąć żenujących tłumaczeń, że "z prawnego punktu widzenia wszystko jest w porządku" i konieczności dołożenia do budżetu zakończonemu już projektowi kolejnego miliona na załatwienie dziur przez tego samego producenta ([ja href="http://blog.securitystandard.pl/news/355052.html" > i ZTM \[i/a\]\(http://blog.securitystandard.pl/news/355052.html\)\).](http://blog.securitystandard.pl/news/355052.html)

Oczywiście mam świadomość, że np. testy penetracyjne są często prowadzone tak czy inaczej. Niestety przykład [ja href="http://ipsec.pl/podpis-elektroniczny/2008/odpowiedz-mswia-na-zapytanie-w-sprawie-e-puap.html" > i uruchomienia ePUAP sprzed dwóch lat \[i/a\]\(http://ipsec.pl/podpis-elektroniczny/2008/odpowiedz-mswia-na-zapytanie-w-sprawie-e-puap.html\) pokazuje, że marnowany jest cały ich potencjał jako narzędzia dającego projektantom podstawę do twierdzenia "tak, dochowaliśmy najwyższej staranności". Wyduszona z zamawiającego odpowiedź "testy zostaną przeprowadzone", anonimowy wykonawca testu, nieopublikowane wyniki \(executive summary\) i ogólna atmosfera ściemniania nie budują zaufania do produktu jak i administracji jako takiej.](http://ipsec.pl/podpis-elektroniczny/2008/odpowiedz-mswia-na-zapytanie-w-sprawie-e-puap.html)

Tymczasem administracja publiczna, jako dysponent środków publicznych, powinien dokładać [ja href="http://ipsec.pl/administracja-publiczna/2010/czy-w-projektach-publicznych-mozna-kierowac-sie-zasadami-ekonomii.html" > i szczególnych starań \[i/a\]\(http://ipsec.pl/administracja-publiczna/2010/czy-w-projektach-publicznych-mozna-kierowac-sie-zasadami-ekonomii.html\), by przekonać obywatela, że jednak warto na to państwo płacić podatki.](http://ipsec.pl/administracja-publiczna/2010/czy-w-projektach-publicznych-mozna-kierowac-sie-zasadami-ekonomii.html)