ANALIZA ZAGROŻEŃ ZWIĄZANYCH Z WERYFIKACJĄ TOŻSAMOŚCI OBYWATELA POPRCZEZ TELEFON KOMÓRKOWY

Remigiusz LEWANDOWSKI

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU

Streszczenie. Artykuł przedstawia analizę zagrożeń związanych z wdrożeniem mechanizmu weryfikacji tożsamości obywatela poprzez wykorzystanie telefonu komórkowego. Analiza ta dotyczy dwóch możliwych modeli: opartego o dane identyfikacyjne przechowywane i przetwarzane w telefonie oraz bazującego na danych identyfikacyjnych przechowywanych i przetwarzanych w ramach rejestrów centralnych. Analiza prowadzi do wniosku, że wykorzystanie telefonu komórkowego jako narzędzia identyfikacji obywatela budzi wątpliwości i obarczone jest poważnymi mankamentami. Najważniejsze z nich to: niewystarczająca pewność co do poprawności weryfikacji tożsamości (w przypadku braku zastosowania narzędzi biometrycznych), wysokie ryzyko kradzieży tożsamości poprzez phishing lub poprzez kradzież aparatu telefonicznego, uzależnienie procesu weryfikacji tożsamości od żywotności baterii w telefonie oraz od przebywania w zasięgu działania sieci GSM.

Słowa kluczowe: weryfikacja tożsamości, GSM, bezpieczeństwo.

Wstęp

W literaturze przedmiotu oraz w mediach bardzo często podnosi się zagadnienie niskiego stopnia informatyzacji państwa w naszym kraju. Podkreślenia wymaga fakt, że zgodnie z indeksem DESI Komisji Europejskiej z 2016 r. (the Digital Economy and Society Index) Polska pozostaje na 22. miejscu wśród państw członkowskich Unii Europejskiej pod względem zaawansowania w budowie gospodarki cyfrowej i społeczeństwa cyfrowego. Autorzy raportu poświęconego DESI 2016 zwracają uwagę, że „Polska spada do grupy państw pozostających w tyle, gdyż tempo nadrobienia przez nią zaległości jest niższe w porównaniu z wynikiem DESI między 2014 a 2015 r.”¹. Szczegóły indeksu za 2016 r. przedstawia rys. 1.

¹ Indeks gospodarki cyfrowej i społeczeństwa cyfrowego na 2016 r. Profil krajowy Polska, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=14161 [dostęp: 20.11.2016].

Rys. 1. Indeks DESI 2016

Źródło: <https://ec.europa.eu/digital-single-market/desi> [dostęp: 20.11.2016]

Oznaczenia: 1. Connectivity – jakość sieci połączeń; 2. Human Capital – kapitał ludzki; 3. Use of Internet – korzystanie z Internetu; 4. Integration of Digital Technology – integracja technologii cyfrowej; 5. Digital Public Services – cyfrowe usługi publiczne

Spośród badanych w ramach indeksu obszarów – w relacji do średniej UE – dość nisko ocenione zostały przez unijnych ekspertów: kapitał ludzki (w odniesieniu do umiejętności korzystania z IT i Internetu), integracja technologii cyfrowych oraz dostęp do łączności internetowej. Co ciekawe, obszar cyfrowych usług publicznych kształtuje się na poziomie zbliżonym do średniej UE, niemniej jednak eksperci zwracają uwagę, że „aktywne wykorzystanie e-administracji utrzymuje się na stosunkowo niskim poziomie i zaledwie 22% użytkowników Internetu składa formularze elektroniczne (21. miejsce w UE)”². Ta konstatacja pozostaje zgodna z – jak się wydaje – powszechnym odczuciem w tym zakresie, tj. z niezadowoleniem z wąskiego katalogu dostępnych elektronicznie usług publicznych oraz z narzędzi służących do dostępu do nich.

Z tych względów niezwykle cieszą aktywność, dynamika i determinacja Ministerstwa Cyfryzacji zmierzające do poprawy zobrazowanego powyżej stanu rzeczy. Zaprezentowany przez minister cyfryzacji, Annę Streżyńską, i przekazany do konsultacji społecznych Program zintegrowanej informatyzacji państwa³ wraz ze Strategią informatyzacji państwa – Planem działań Ministra Cyfryzacji⁴ stanowią w dużym stopniu odpowiedź na zdiagnozowane m.in. przez Komisję Europejską i odczuwalne dość boleśnie przez Polaków słabe strony i deficyty informatyzacji państwa.

² Ibidem.

³ <https://mc.gov.pl/konsultacje/program-zintegrowanej-informatyzacji-panstwa/program-zintegrowanej-informatyzacji-panstwa> [dostęp: 20.11.2016].

⁴ <https://mc.gov.pl/konsultacje/program-zintegrowanej-informatyzacji-panstwa/zalacznik-1-strategia-informatyzacji-panstwa-plan-dzialan-ministra-cyfryzacji> [dostęp: 20.11.2016].

Entuzjazm towarzyszący wskazanym wyżej działaniom nie powinien jednak przesłonić niedoskonałości niektórych z proponowanych rozwiązań, a w szczególności nie powinien ograniczyć zdrowego rozsądku, jakiego oczekuje się przy realizacji każdej inicjatywy publicznej. W ramach niniejszego artykułu skupiono się na jednym zagadnieniu: koncepcji wykorzystania telefonów komórkowych i towarzyszących im systemów teleinformatycznych do identyfikacji tożsamości obywatela jako alternatywy względem klasycznych dokumentów publicznych, a w szczególności dowodu osobistego.

1. Dokumenty publiczne

We współczesnym świecie nikt nie neguje potrzeby wykorzystania rozwiązań informatycznych w sferze dokumentów publicznych, w tym także w sferze związanej z zarządzaniem tożsamością. Zasadniczym pytaniem jest jednak, czy rozwiązania informatyczne powinny pełnić funkcję subsydiarną w odniesieniu do dokumentów publicznych i zarządzania tożsamością, czy też powinny (docelowo) zastąpić dokumenty „analogowe”. Nie jest to zagadnienie ani błahe, ani czysto teoretyczne, albowiem takie pytania stawiane są w aktualnej debacie publicznej, która towarzyszy zapowiadanym przez Ministerstwo Cyfryzacji działaniom.

Przed podjęciem próby udzielenia odpowiedzi na powyższe pytania należy jednak doprecyzować zakres rozważań podjętych w niniejszym artykule. Obejmuje on:

- 1) dokumenty publiczne i ich potencjalną transformację w dokument cyfrowy, a w szczególności mobilny, tj. dostępny poprzez telefon komórkowy;
- 2) narzędzia dostępu do elektronicznych usług publicznych, a w szczególności potencjalne wykorzystanie dokumentów publicznych jako tego rodzaju narzędzia.

W ramach niniejszego artykułu dokument publiczny definiuję jako odpowiednio zabezpieczony dokument urzędowy, wytwarzany według określonego wzoru w seriach lub w znacznej liczbie, gotowy w całości lub jako blankiet wymagający indywidualizacji bądź personalizacji, a służący do identyfikacji osób, rzeczy lub potwierdzający stan prawny albo prawa osób posługujących się takim dokumentem. Dokumentami publicznymi w szczególności są:

- 1) dowód osobisty;
- 2) paszport;
- 3) dokumenty ubezpieczenia zdrowotnego;
- 4) dokumenty tożsamości cudzoziemca: polski dokument tożsamości cudzoziemca, tymczasowe zaświadczenie tożsamości cudzoziemca;
- 5) dokumenty podróży dla cudzoziemców: dokument podróży dla cudzoziemca zgodny z konwencją genewską, polski dokument podróży dla cudzoziemca, tymczasowy polski dokument podróży dla cudzoziemca, naklejka wizowa, zezwolenie na przekraczanie granicy w ramach małego ruchu granicznego;

- 6) dokumenty dotyczące pobytu: karta pobytu, dokument potwierdzający prawo stałego pobytu, zgoda na pobyt tolerowany, karta pobytu członka rodziny obywatela UE, karta stałego pobytu członka rodziny obywatela UE, oświadczenia o zamiarze powierzenia pracy cudzoziemcowi;
- 7) dokumenty komunikacyjne: prawo jazdy, dowód rejestracyjny, karta pojazdu;
- 8) odpisy aktów stanu cywilnego i zaświadczenia USC;
- 9) wypisy aktów notarialnych;
- 10) znaki akcyzy;
- 11) legitymacje funkcjonariusza Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Służby Kontrwywiadu Wojskowego, Straży Granicznej;
- 12) legitymacje funkcjonariuszy i pracowników innych organów administracji centralnej;
- 13) świadectwa i dyplomy ukończenia szkół;
- 14) sądowe tytuły wykonawcze;
- 15) wyroki sądowe oraz zaświadczenia o niekaralności;
- 16) książeczki wojskowe;
- 17) dokumenty związane z posiadaniem broni palnej;
- 18) inne druki, w tym zaświadczenia, licencje, patenty, świadectwa kwalifikacji, dokumenty poświadczające określony stan prawny itp., mające znaczenie dla bezpieczeństwa państwa, bezpieczeństwa obrotu prawnego i gospodarczego.

2. Tożsamość obywatela i dokument publiczny a bezpieczeństwo państwa

Spośród szeregu różnego rodzaju dokumentów publicznych za najważniejsze należy uznać dokumenty potwierdzające tożsamość oraz określone uprawnienia⁵. Z dokumentami tymi wiąże się pojęcie bezpieczeństwa identyfikacyjnego, rozumiane jako stan niezakłóconego bezpieczeństwa państwa w obszarze obejmującym:

- 1) prawidłową weryfikację deklarowanej tożsamości osób,
- 2) weryfikację prawidłowości przyporządkowania danej osoby i jej tożsamości do określonych uprawnień wynikających z dokumentu, jakim się ona posługuje,
- 3) obrót prawny i gospodarczy związany z użyciem dokumentów potwierdzających tożsamość lub określone uprawnienia,
- 4) ochronę obywateli przed kradzieżą tożsamości⁶.

⁵ R. Lewandowski, *O potrzebie regulacji sfery dokumentów publicznych*, „Człowiek i Dokumenty”, nr 42/2016, s. 53-58.

⁶ Idem, *Evaluation of legal and technical solutions with respect to new types of documents in the health care system – KUZ, KSM and KSA*, „Journal of Health Policy, Insurance and Management – Polityka Zdrowotna”, No. XVI/VI/2015, s. 77.

W tym kontekście należy uznać, że bezpieczeństwo identyfikacyjne i dotyczące go dokumenty publiczne są związane z bezpieczeństwem państwa. Związek ten obejmuje w szczególności dwie kategorie bezpieczeństwa państwa:

- 1) bezpieczeństwo ekonomiczne,
- 2) bezpieczeństwo publiczne.

Wymiar bezpieczeństwa ekonomicznego państwa wynika bezpośrednio z faktu, że stabilność systemu płatniczego związana z pewnością i wiarygodnością realizowanego obrotu gospodarczego i prawnego jest zależna od prawidłowości i pewności identyfikacji stron tego obrotu⁷. A zatem warunkiem koniecznym zachowania bezpieczeństwa państwa w omawianej dziedzinie jest zapewnienie wiarygodności dokumentów publicznych, które są narzędziem identyfikacji i weryfikacji stron rzeczonoego obrotu. Zarządzanie wiarygodnością dokumentów sprowadza się do ich optymalnego zabezpieczenia przed fałszerstwami przy równoczesnym zachowaniu wysokiej użyteczności publicznej. Termin „optymalny” oznacza w omawianym przypadku osiągnięcie punktu równowagi pomiędzy poziomem zastosowanych zabezpieczeń a ich kosztami, tzn. dobór takich zabezpieczeń, które minimalizują koszty społeczne związane z potencjalnymi fałszerstwami dokumentów⁸. Wspomniana wyżej „użyteczność publiczna” wiąże się z wykorzystaniem dokumentu nie tylko na potrzeby państwa, lecz także na potrzeby samego obywatela i relacji obywatel–obywatel oraz obywatel–podmioty gospodarcze. Ważne jest zatem możliwie szerokie spektrum zastosowania dokumentu przez obywatela, wygoda użytkowania dokumentu, a także jego (multi)funkcjonalność.

Zależności pomiędzy wiarygodnością dokumentów a bezpieczeństwem państwa przedstawiono na rys. 2.

Koszty społeczne wynikające z fałszerstw czy kradzieży tożsamości są znaczące. Dotyczą one zarówno przestępczości gospodarczej, jak i terrorystycznej i dotyczą nie tylko podmioty bezpośrednio poszkodowane (podmioty gospodarcze, osoby fizyczne, Skarb Państwa), lecz także wpływają na dobrobyt wszystkich obywateli w wyniku uszczuplenia wpływów finansowych Skarbu Państwa, ryzyka zachwiania stabilności systemu płatniczego i ryzyka naruszenia bezpieczeństwa publicznego. W skrajnych przypadkach naruszenie bezpieczeństwa identyfikacyjnego może powodować zachwianie systemu gospodarczego państwa i godzić w jego podstawowe interesy ekonomiczne⁹. W polskim systemie prawnym przestępstwo fałszowania pieniędzy postrzegane jest jako większe zagrożenie niż fałszowanie dokumentów, gdyż jest zagrożone wyższymi karami. Jednakże w praktyce przestępcy często

⁷ R. Lewandowski, T. Goliński, *Zarządzanie wiarygodnością dokumentów a bezpieczeństwo ekonomiczne*, [w:] K. Raczkowski (red.), *Zarządzanie w systemie gospodarczym. Szanse i zagrożenia*, Wolters Kluwer, Warszawa 2015, s. 118-119.

⁸ Ibidem, s. 118.

⁹ R. Lewandowski, *Rola narodowego wytwórcy banknotów, dokumentów i towarzyszących im systemów IT w systemie bezpieczeństwa obrotu gospodarczego i prawnego*, [w:] K. Raczkowski (red.), *Bezpieczeństwo ekonomiczne obrotu gospodarczego*, Wolters Kluwer, Warszawa 2014, s. 255; J. Grzemski, A. Krześ, *Analiza pojęcia „przestępstwa godzące w podstawy ekonomiczne państwa” w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, „Przegląd Bezpieczeństwa Wewnętrznego” nr 2/2010, s. 150.

mogą przy mniejszym ryzyku zyskać więcej i przysporzyć więcej strat, fałszując dokumenty¹⁰. Najczęściej ujawnianymi kategoriami przestępstw związanych z fałszowaniem dokumentów lub wykorzystaniem cudzej tożsamości są wyłudzenia kredytów, wyłudzenie dotacji lub towarów, nielegalna migracja, handel ludźmi oraz kradzież samochodów.

Rys. 2. Czynniki kształtujące bezpieczeństwo państwa w zakresie wiarygodności identyfikacji

Źródło: R. Lewandowski, *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych i banknotów*, [w:] M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Volumina, Warszawa 2016, s. 289

Z dokumentami, a w szczególności dokumentami identyfikacyjnymi, wiąże się zagadnienie bezpieczeństwa danych osobowych. Dane te powinny podlegać zaawansowanej ochronie, ponieważ dotyczą one wszystkich obywateli, którym dany rodzaj dokumentu wydano. Dane osobowe obejmują również dane biometryczne obywateli. Bezpieczeństwo danych osobowych narażone jest na wiele zagrożeń, takich jak udostępnienie ich osobom nieupoważnionym, przetwarzanie ich z naruszeniem przepisów prawa, zmiana, utrata, uszkodzenie czy zniszczenie danych osobowych¹¹.

Fałszowanie dokumentów i kradzież tożsamości towarzyszy również działalności agenturalnej i terrorystycznej, czy też szerzej – działalności wymierzonej w bezpieczeństwo publiczne. Ten wymiar związków pomiędzy bezpieczeństwem identyfikacyjnym a bezpieczeństwem państwa ma – jak się wydaje – znaczenie

¹⁰ R. Lewandowski, T. Goliński, op. cit., s. 126.

¹¹ R. Lewandowski, *Rola (...)*, op. cit., s. 251.

większe od wcześniej omówionego bezpieczeństwa ekonomicznego. Skradziona tożsamość lub sfalszowany dokument stanowią bowiem zwykle niezbędny atrybut terrorysty. Specjalista do spraw terroryzmu – K. Izak, w odniesieniu do zamachu na World Trade Center 11 września 2001 r. precyzyjnie nakreślił rolę dokumentów w ataku: „amerykańska komisja powołana po atakach z 11 września 2001 r. stwierdziła w swoim raporcie, że dla terrorystów dokumenty podróży są tak samo ważne jak uzbrojenie. W sierpniu 2002 r. na lotnisku Johna Kennedy’ego aresztowano Mohammada al-Atrissa, obywatela USA pochodzenia egipskiego, który sprzedał fałszywe dokumenty tożsamości dwóm zamachowcom z 11 września 2001 r.: Chalidowi Almidharowi i Abdulowi Azizowi Alomarowi. Al-Atriss miał stać na czele grupy przestępczej zajmującej się produkcją i sprzedażą fałszywych amerykańskich dokumentów tożsamości. Podczas przeszukania jego mieszkania znaleziono 75 fałszywych dokumentów. Fałszywym paszportem posługiwał się również Sulejman Abu Ghajs, zięć Osamy bin Ladena, zatrzymany w styczniu 2013 r. w hotelu w Ankarze. Do Turcji przyleciał z Iranu. Ankarą odmówiła jego wydania Amerykanom, obawiając się odwetowych zamachów Al-Kaidy, i wydała go z kraju. Abu Ghajs udał się do Jordanii. Od pobytu w Turcji śledzony był przez agentów CIA, którzy w Jordanii dokonali jego zatrzymania. Został przewieziony do USA, gdzie w marcu stanął przed sądem oskarżony o udział w spisku, którego celem było zabijanie Amerykanów”¹².

W odniesieniu do Polski skalę zagrożenia przestępstwami przeciwko wiarygodności dokumentów przedstawiają rys. 3 i 4. Na rys. 3 zaprezentowano liczbę wszczętych postępowań oraz stwierdzonych przestępstw z art. 270 k.k., tj. w zakresie podrabiania i przerabiania dokumentów, przygotowania do tych przestępstw oraz wypełniania podpisanego blankietu niezgodnie z wolą podpisującego.

Rys. 3. Liczba wszczętych postępowań oraz stwierdzonych przestępstw z art. 270 k.k.

Źródło: <http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-15> [dostęp: 28.12.2016]

¹² K. Izak, *Fałszywe dokumenty w rękach terrorystów*, „Człowiek i Dokumenty”, nr 32/2014, s. 10-11.

Z rys. 3 wynika, że w ostatnich latach liczba wszczętych postępowań z art. 270 k.k. kształtuje się na poziomie ok. 30 tys. rocznie, zaś liczba wszczętych postępowań wynosi ponad 20 tys. rocznie. Wykres wskazuje, że w długim okresie mamy do czynienia raczej z tendencją malejącą wskazanej kategorii przestępstw, przy czym podkreślić należy, że przytaczane dane nie obejmują jeszcze 2015 i 2016 r.

Na rys. 4 przedstawiono z kolei liczbę przestępstw z art. 275 k.k., tj. w zakresie posługiwania się dokumentem stwierdzającym tożsamość innej osoby albo jej prawa majątkowe, kradzieży lub przywłaszczenia takiego dokumentu, a także jego bezprawnego przewożenia, przenoszenia lub przesyłania za granicę.

Niewątpliwie należy uznać zatem, że zarówno w odniesieniu do przestępstw gospodarczych, jak i przestępstw wymierzonych przeciwko porządkowi prawnemu, publicznemu i ładowi wewnętrznemu „dokument jest głównym i najważniejszym narzędziem działania przestępczego”¹³.

Rys. 4. Liczba przestępstw z art. 275 k.k.

Źródło: <http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-15> [dostęp: 28.12.2016]

Z wykresu wynika, że od kilku lat liczba przestępstw z art. 275 k.k., zarówno stwierdzonych, jak i wszczętych, utrzymuje się na podobnym poziomie kilkunastu tysięcy rocznie, a w ujęciu długookresowym zarysowuje się tendencja spadkowa. Niemniej jednak w 2014 r. zauważalny jest wzrost o ok. 10%.

3. Weryfikacja tożsamości poprzez telefon komórkowy

Czy zatem warto podjąć prace nad transformacją dokumentów publicznych w dokumenty cyfrowe dostępne poprzez telefon komórkowy? Przed udzieleniem odpowiedzi nasuwa się kolejne pytanie: czym miałyby być owe „dokumenty cyfrowe”?

¹³ H. Kolečki, *Dokumenty publiczne – narzędzie przestępstwa czy ochrony przed nim?*, „Człowiek i Dokumenty”, nr 8/2008, s. 25.

Tu otwiera się olbrzymie pole do dywagacji i projekcji, które jednak zawężono do luźnej koncepcji zaprezentowanej przez Annę Streżyńską, minister cyfryzacji, w tygodniku „Wprost”¹⁴:

„– Smartfon zastąpi dowód osobisty?

- To mój cel! Za cztery lata, wychodząc z tego ministerstwa, chcę mieć na telefonie wszystko, co tylko da się zakodować na takim urządzeniu elektronicznym: dowód osobisty, kartę płatniczą, biblioteczną, dowód rejestracyjny, prawo jazdy... I akt odwołania”.

Rozpatrywać można dwa zasadnicze podejścia do wykorzystania telefonów komórkowych przy weryfikacji tożsamości obywatela:

- 1) podejście zakładające przechowywanie i przetwarzanie danych identyfikacyjnych obywatela przez niego samego przy wykorzystaniu telefonu komórkowego;
- 2) podejście zakładające przechowywanie i przetwarzanie danych identyfikacyjnych obywatela przez serwer kontrolowany przez administrację publiczną (np. w ramach Systemu Rejestrów Państwowych).

Pierwsze podejście mogłoby np. zakładać umieszczenie odpowiednich danych identyfikacyjnych (np. imię, nazwisko, data i miejsce urodzenia, zdjęcie, dane biometryczne itd.), kluczy kryptograficznych i kwalifikowanego podpisu elektronicznego na karcie SIM operatora GSM lub na kryptograficznej karcie mSD. Alternatywnie zastosowanie mogłaby znaleźć odpowiednia aplikacja umieszczana na telefonie i prezentująca wybrane dane identyfikacyjne obywatela, które można by następnie przekazać (przy wykorzystaniu technologii, np. Bluetooth lub NFC) stronie weryfikującej.

Drugie podejście z kolei zakłada wykorzystanie telefonu komórkowego i indywidualnego numeru telefonicznego jako narzędzia pośredniczącego w autoryzacji dostępu do danych identyfikacyjnych. Przykładowo, na żądanie strony weryfikującej, na numer telefoniczny obywatela mógłby być kierowany jednorazowy kod (w formie SMS/TAN), który udostępniony z kolei stronie weryfikującej mógłby umożliwić autoryzację pobrania z centralnych serwerów państwowych (np. w ramach Systemu Rejestrów Państwowych) odpowiednich danych identyfikacyjnych obywatela.

Bez względu jednak na wybór docelowego rozwiązania, weryfikacja tożsamości lub uprawnień obywatela (np. w zakresie uprawnienia do kierowania pojazdem) albo szczególnych uprawnień (np. wynikających ze statusu funkcjonariusza Policji i służb specjalnych) poprzez telefon komórkowy budzi poważne wątpliwości. Należy zwrócić bowiem uwagę, że forma dokumentu publicznego (w tym sposób jego zabezpieczenia) powinna zapewniać:

- 1) szybką i jednoznaczną weryfikację tego, czy dokument jest prawdziwy,
- 2) szybką i jednoznaczną weryfikację tego, czy dane osobowe i wizerunek zapisane w dokumencie odpowiadają tożsamości osoby legitymującej się danym dokumentem,

¹⁴ C. Bielakowski, A. Grabek, *Dowód, karta płatnicza i prawo jazdy na telefonie? Streżyńska: To mój cel*, „Wprost”, <https://www.wprost.pl/tylko-u-nas/535894/Dowod-karta-platnicza-i-prawo-jazdy-na-telefonie-Strezyńska-To-moj-cel.html> [dostęp: 20.11.2016].

- 3) ochronę przed przerabianiem i podrabianiem dokumentu,
- 4) ochronę tożsamości obywateli przed kradzieżą,
- 5) możliwość weryfikacji, o której mowa w pkt 1 i 2, w odniesieniu do wybranych dokumentów (np. prawa jazdy) również przez funkcjonariuszy służb zagranicznych.

Dokument w telefonie komórkowym nie wypełnia tych warunków koniecznych. W odróżnieniu od dokumentu w formie materialnej, dokument w telefonie jest możliwy do okazania jedynie tak długo, na ile pozwala bateria w telefonie oraz na ile łączność internetowa udostępnia komunikację z rejestrami państwowymi. A zatem tego rodzaju „dokument” posiadałby cechę nietrwałości i nieciągłości działania, co negatywnie weryfikuje dwa pierwsze warunki konieczne, wskazane powyżej. W sytuacji wymagającej kontroli tożsamości lub uprawnień taka weryfikacja mogłaby się okazać niemożliwa do przeprowadzenia (ponieważ np. bateria się rozładowała lub brakuje zasięgu sieci GSM).

Druga słabość omawianych rozwiązań to podatność na ataki hakerów. Na całym świecie tego rodzaju ataki trwają praktycznie bez przerwy. Dotyczą one także naszego państwa. Choćby ostatnio – odnotowany w lipcu br. atak na serwery Netii, w efekcie którego ujawniono dane personalne klientów i historie przeprowadzanych przez nich transakcji¹⁵ czy też atak z sierpnia br. na serwery międzynarodowej korporacji IT, Opera Software AS¹⁶, w wyniku którego najprawdopodobniej doszło do wycieku danych i haseł 1,7 mln klientów Opera Sync. Działalność sprofesjonalizowanych międzynarodowych grup hakerskich to bardzo poważne zagrożenie dla bezpieczeństwa państwa. Dokument tożsamości w formie aplikacji telefonicznej wydaje się doskonałym narzędziem z punktu widzenia hakerów zainteresowanych przejęciem cudzej tożsamości w różnych celach, w szczególności terrorystycznych lub związanych z przestępczością gospodarczą. Jak wskazano w *Raporcie o stanie bezpieczeństwa w Polsce w 2014 roku*: „Cyberprzestrzeń pozostaje obszarem działania zarówno indywidualnych przestępców, jak i zorganizowanych grup przestępczych oraz środowisk ekstremistycznych i organizacji terrorystycznych. Upowszechnienie dostępu do Internetu, w kontekście globalnego charakteru cyberprzestrzeni, przy jednocześnie stosunkowo dużej możliwości zachowania anonimowości i popełniania przestępstw na terenie jednego państwa z obszaru innego, sprzyja występowaniu różnego rodzaju zagrożeń, zarówno dotyczących bezpieczeństwa systemów informatycznych, jak i o charakterze stricte przestępczym (przestępczość o charakterze ekonomicznym, kryminalnym i narkotykowym). Istotne jest również, że cyberzagrożenia mają charakter elastyczny i bezpośrednio zależny od kierunków rozwoju nowoczesnych technologii. Sprawcy przestępstw coraz częściej wykorzystują dedykowane oprogramowanie umożliwiające kamuflowanie miejsca, z którego działają, korzystają z sieci anonimizujących, m.in. TOR, czy wirtualnych systemów

¹⁵ D. Kosiński, *Netia zaatakowana! Dane klientów zostały wykradzione i ujawnione*, <http://www.spidersweb.pl/2016/07/netia-atak-2016.html> [dostęp: 20.11.2016].

¹⁶ <http://www.spidersweb.pl/2016/08/opera-sync-atak.html> [dostęp: 20.11.2016].

dokonywania płatności w Internecie, np. bitcoin, pozostając poza jakąkolwiek kontrolą instytucji finansowych”¹⁷.

Analizując poziom bezpieczeństwa w mobilnych kanałach komunikacji (telefon komórkowy, tablet itd.), należy zauważyć, że w przeważającej większości instytucji państwowych oraz przedsiębiorstw komunikacja mobilna nie jest zabezpieczona w ogóle lub we właściwy sposób. Poza stosunkowo rzadko stosowanymi ze względu na koszty specjalnymi aparatami telefonicznymi umożliwiającymi szyfrowanie rozmów¹⁸ oraz Sieci Łączności Rządowej CATEL brakuje na rynku polskim kompleksowego narzędzia pozwalającego na zapewnienie (np. poprzez szyfrowanie) poufności informacji przekazywanej w ramach SMS, komunikatorów, połączeń głosowych i poczty elektronicznej. Na rynku dostępne są jedynie rozwiązania, które punktowo wypełniają powyższe potrzeby, tj. zapewniają szyfrowanie jedynie komunikacji głosowej i/lub SMS, ale nie gwarantują poufności i kontroli nad wymianą poczty elektronicznej na urządzeniach mobilnych. Tymczasem we współczesnym świecie w działalności gospodarczej oraz w zarządzaniu państwem informacja stanowi strategiczne aktywo. Strategiczny wymiar informacji dotyczy m.in. jej poufności, w tym nadzoru nad jej przepływem. Z tego powodu fundamentalne stają się kwestie związane z bezpieczeństwem teleinformatycznym, a w jego zakresie rozwiązania zapewniające poufność informacji i kontrolę nad jej przepływem. W tym kontekście szczególnie istotne jest zapewnienie przedmiotowego bezpieczeństwa w najpowszechniej stosowanych kanałach przepływu informacji, tj. właśnie w komunikacji mobilnej.

Raport o stanie bezpieczeństwa w Polsce w 2014 roku jako jedną z podstawowych kategorii przestępstw popełnianych w cyberprzestrzeni wskazuje phishing, polegający na pozyskiwaniu za pośrednictwem Internetu danych wrażliwych, takich jak hasła, loginy itd., a także kampanie cyberszpiegowskie wymierzone w poszczególne państwa. To realne zagrożenie dla dokumentów identyfikacyjnych i dokumentów potwierdzających określone uprawnienia – po umieszczeniu ich w cyberprzestrzeni. Zagrożenie to jest szczególnie widoczne w dobie globalnego terroryzmu. Z tego względu mDokumenty wymagają wysokiej jakości rozwiązań chroniących je przed atakami hakerów oraz wysokiej jakości narzędzi kryptograficznych zapewniających bezpieczną transmisję danych.

B. Hołyst i J. Pomykała dodatkowo zwracają uwagę, że „cyberprzestępca, który pragnie uzyskać poufne informacje, ma do dyspozycji olbrzymi arsenał metod, aby osiągnąć swój cel”¹⁹. W tym kontekście trudno jest znaleźć uzasadnienie dla konceptu tworzenia „wirtualnych” dokumentów publicznych, zwłaszcza że dokumenty

¹⁷ <https://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html> [dostęp: 20.11.2016].

¹⁸ Np. z zastosowaniem uznanych standardów protokołów szyfrujących RSA, AES, SHA256; autoryzacją połączenia poprzez wymianę kluczy uwierzytelniających itd.

¹⁹ B. Hołyst, J. Pomykała, *Bezpieczeństwo informacji w świetle kryptografii, kanałów ukrytych i steganografii*, [w:] B. Hołyst, J. Pomykała, P. Potęjko (red.), *Nowe techniki badań kryminalistycznych a bezpieczeństwo informacji*, PWN, Warszawa 2014, s. 131.

fizyczne dobrze spełniają swoje funkcje i zapewniają bezpieczeństwo identyfikacyjne. Co więcej, współczesne technologie polegające na współistnieniu warstwy fizycznej dokumentu z warstwą elektroniczną (mikroprocesorem wraz z odpowiednimi danymi, np. biometrycznymi, kwalifikowanym podpisem elektronicznym itd.) znacząco podnoszą bezpieczeństwo.

4. Poprawność i wiarygodność weryfikacji tożsamości

Podstawową funkcją „klasycznego” dowodu osobistego jest umożliwienie weryfikacji tożsamości osoby, której dowód został wydany i która legitymuje się tym dowodem. Obecnie weryfikacja tożsamości następuje przede wszystkim dzięki subiektywnemu porównaniu fotografii widniejącej na dowodzie osobistym z twarzą posiadacza i stwierdzeniu wystarczającej zgodności cech. Nie jest to weryfikacja łatwa, nawet dla wyspecjalizowanych służb, zwłaszcza w kontekście 10-letniego terminu ważności dowodu osobistego (stąd też w niektórych państwach stosuje się krótsze okresy ważności dokumentu, np. 5-letnie). Weryfikacja bazująca wyłącznie na subiektywnym zmyśle widzenia nie jest doskonała i siłą rzeczy nie może dawać wymaganej pewności. Stąd we współczesnych dokumentach stosuje się rozwiązania pozwalające na powiązanie z większą trafnością dokumentu z osobą, dla której został on wydany. Z tego powodu opracowana przez Ministerstwo Cyfryzacji *Koncepcja wdrożenia polskiego dowodu osobistego z warstwą elektroniczną*²⁰ zakładać powinna wydawanie nowych dowodów osobistych z danymi biometrycznymi i wykorzystanie właśnie tych danych w procesie weryfikacji tożsamości.

Ewentualne pominięcie narzędzi biometrycznych w koncepcji wykorzystania telefonów komórkowych do weryfikacji tożsamości obywatela i oparcie weryfikacji o subiektywny zmysł widzenia i subiektywne porównanie zdjęcia danej osoby z jej rzeczywistym wizerunkiem stanowiłoby zatem krok wstecz w stosunku do dostępnych technologii. Biometria to wiedza o rozpoznawaniu żywych osób, bazując na pomiarach cech biologicznych (anatomicznych i fizjologicznych), zarówno pasywnych (jak np. wzór tęczówki oka, odcisk palców, twarz, wzory siatkówki oka, geometria dłoni, układ naczyń krwionośnych), jak i aktywnych (np. dynamika pisma ręcznego, głos, ruch warg, chód)²¹. Współcześnie biometria stanowi stałe, a zarazem kluczowe ogniwo łańcucha wartości dokumentów identyfikacyjnych. Jest jedną z najbardziej niezawodnych metod uwierzytelniania i weryfikacji tożsamości człowieka (lub identyfikacji osoby), choć jej skuteczność nie jest bezwarunkowa. W literaturze przedmiotu wskazuje się na warunki konieczne, które towarzyszyć muszą skutecznemu uwierzytelnianiu biometrycznemu, takie jak optymalne warunki dokonania pomiaru biometrycznego, aktualizacja pomiaru biometrycznego,

²⁰ <https://mc.gov.pl/aktualnosci/koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna-zapraszamy-do> [dostęp: 20.11.2016].

²¹ B. Hołyst, J. Pomykała, *Biometria w systemach uwierzytelniania*, „Biuletyn WAT”, vol. LX, nr 4, 2011, s. 418-419.

optymalny poziom tolerancji²². Skuteczność biometrii znacząco można podnieść poprzez wprowadzenie pomiaru nie jednej, lecz co najmniej dwóch cech biometrycznych. W ten sposób jeszcze mocniej powiązać można daną osobę z dokumentem, którym się ona posługuje. Prawidłowość i pewność weryfikacji tożsamości są podstawowym atrybutem bezpieczeństwa identyfikacyjnego²³. Pominięcie weryfikacji biometrycznej w koncepcji wykorzystania telefonów komórkowych do weryfikacji tożsamości obywatela oznaczać będzie zachwianie wskazanych wyżej czynników bezpieczeństwa identyfikacyjnego.

5. Narzędzia dostępu do e-usług

Koncepcja wykorzystania telefonów komórkowych do weryfikacji tożsamości obywatela powinna być ukierunkowana na ułatwienie obywatelowi załatwiania codziennych spraw wymagających potwierdzenia tożsamości, a równocześnie zachowanie optymalnego poziomu bezpieczeństwa identyfikacyjnego. W tym kontekście ważna pozostaje kwestia narzędzi używanych do korzystania z e-usług publicznych. Wydaje się, że podstawową przyczyną znikomego funkcjonowania w praktyce e-usług w Polsce są słabe narzędzia dostępu. Obecnie korzystać można z dwóch podstawowych narzędzi: kwalifikowanego podpisu elektronicznego (narzędzie płatne o marginalnym zastosowaniu w odniesieniu do korzystania z e-usług) oraz profilu zaufanego, o którym minister cyfryzacji Anna Streżyńska mówi, że jest to „rzecz, która na tyle jest odstraszaająca dla klientów, że zaledwie 300 tys. osób w Polsce korzysta z profilu zaufanego jako środka komunikacji i potwierdzania swojej woli w kontaktach z administracją. Można powiedzieć, że są to pasjonaci, ponieważ profil zaufany jest powiązany bezpośrednio z serwisem ePUAP, który został zbudowany za ponad 150 mln zł i niestety jest wysoce awaryjnym produktem”²⁴.

Instrumenty dostępu do e-usług publicznych muszą gwarantować prawidłową weryfikację tożsamości osoby pragnącej skorzystać z tego rodzaju usług. A zatem narzędzie to zapewnia odpowiednie uwierzytelnienie dające dostęp do e-usług. Obecnie Ministerstwo Cyfryzacji rozważa jako tzw. dostawców tożsamości: narodowego dostawcę tożsamości, banki, operatorów telekomunikacyjnych i operatorów pocztowych²⁵. Ryzykowne wydaje się powierzenie wskazanej wyżej roli tak szerokiemu gronu podmiotów. Raz jeszcze podkreślenia wymaga relatywna

²² Ibidem, s. 420-421; M. Tomaszewska, *Technologia biometryczna w Polsce*, [w:] B. Hołyst (red.), *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, PWN, Warszawa 2014, s. 721.

²³ R. Lewandowski, *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych i banknotów*, [w:] M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Volumina, Warszawa 2016, s. 287-288.

²⁴ <http://www.rdc.pl/informacje/anna-strezyńska-w-polsce-zaledwie-300-tys-osob-korzysta-z-profilu-zaufanego-jako-srodka-komunikacji-posluchaj/> [dostęp: 17.01.2017].

²⁵ Załącznik nr 2 do SIP: opis docelowego modelu eID. *Krajowy Schemat Identyfikacji Elektronicznej (eID) w Polsce z uwzględnieniem budowy państwowego brokera eID i wykorzystaniem usług zaufania*, https://mc.gov.pl/files/zalacznik_nr_2_do_sip.pdf [dostęp: 20.11.2016].

słabość funkcjonujących obecnie komercyjnych systemów teleinformatycznych. Przestępczość internetowa, a szczególnie phishing, w tym kontekście generuje realne ryzyko naruszające bezpieczeństwo identyfikacyjne obywateli²⁶. Warto podkreślić, że w związku z planami emisji dowodu elektronicznego wyposażonego w mikroprocesor, to właśnie ten rodzaj dokumentu powinien być naturalnym instrumentem uwierzytelniającym obywatela online. Alternatywne pomysły, np. wykorzystanie bankowości elektronicznej, obarczone są szeregiem bardzo poważnych słabości (np. phishing, brak certyfikacji, luki w systemach, przypadki włamań do systemów e-bankowości, przypadki infiltracji prywatnych podmiotów przez zagraniczne służby specjalne, ryzyko wynikające z braku nadzoru kapitałowego państwa itp.), a praktyka stosowana przez kraje najbardziej zaawansowane w informatyzacji państwa to potwierdza. Szczególnie dobry jest tu przykład Estonii, gdzie ok. 70% logowań do Portalu e-Uslug Państwowych wykonuje się poprzez elektroniczny dowód osobisty²⁷, który stanowi powszechny instrument identyfikacji każdego obywatela. Jedynie ok. 30% logowań odbywa się poprzez mobilne ID (Mobiil ID), które wymaga jednak dodatkowej umowy z operatorem telefonii komórkowej i wymiany karty SIM.

Podsumowanie

Idea ograniczania wykluczenia cyfrowego Polaków, ułatwiania prowadzenia działalności gospodarczej oraz życia społecznego poprzez wprowadzanie różnego rodzaju rozwiązań informatycznych nie budzi żadnych wątpliwości. Ważne jest jednak, aby przy analizie nowych rozwiązań kompleksowo podchodzić z jednej strony do generowanych przez nie korzyści, a z drugiej zaś do ryzyka, jakie one tworzą. Wykorzystanie telefonu komórkowego jako narzędzia identyfikacji obywatela budzi wątpliwości i obarczone jest poważnymi mankamentami. Najważniejsze z nich to: niewystarczająca pewność co do poprawności weryfikacji tożsamości (w przypadku braku zastosowania narzędzi biometrycznych), wysokie ryzyko kradzieży tożsamości poprzez phishing lub kradzież aparatu telefonicznego, uzależnienie procesu weryfikacji tożsamości od żywotności baterii w telefonie oraz od przebywania w zasięgu działania sieci GSM.

Zdiagnozowane w artykule słabości koncepcji mDokumentów mają zasadnicze znaczenie z punktu widzenia bezpieczeństwa państwa. mDokumenty, jako cyfrowy odpowiednik dokumentów publicznych, odgrywają bowiem tożsame funkcje w systemie bezpieczeństwa państwa. Zatem niewystarczająco dobrze zabezpieczone mDokumenty powodują potencjalne obniżenie wiarygodności, pewności i bezpieczeństwa tożsamości obywateli (oraz identyfikacji rzeczy lub stanu prawnego) oraz potencjalnie naruszają stabilność systemu płatniczego związanego z pewnością

²⁶ R. Lewandowski, *O potrzebie regulacji sfery dokumentów publicznych*, „Człowiek i Dokumenty”, nr 42/2016, s. 53-58.

²⁷ Dane za estońską fundacją e-Governance Academy.

i wiarygodnością realizowanych transakcji w obrocie prawnym i gospodarczym. Interes bezpieczeństwa państwa wymaga więc wyeliminowania dostrzeżonych mankamentów w koncepcji mDokumentów.

Ponadto, ewentualnemu projektowi wdrożeniowemu w zakresie wykorzystania telefonu komórkowego jako narzędzia identyfikacji obywatela musi towarzyszyć obiektywnie stwierdzona znacząca korzyść społeczna, której – w ramach niniejszej analizy – nie stwierdzono. Zasadność i warunki cyfrowego dostępu do wybranych dokumentów identyfikacyjnych oraz potwierdzających określone uprawnienia czy też określony stan prawny powinny być rozpatrywane przy uwzględnieniu przedstawionych w niniejszym artykule wątpliwości. Obiektywna i istotna potrzeba bezpieczeństwa identyfikacyjnego nie może zostać przesłonięta przez pogoń za mylnie rozumianą innowacją czy też po prostu modą.

Przeprowadzona analiza mDokumentów skłania do wniosku, że przedmiotowy projekt można udoskonalić przede wszystkim poprzez:

- 1) wprowadzenie weryfikacji tożsamości opartej na biometrii: tylko poprzez biometrię można uzyskać wymaganą pewność co do tożsamości danej osoby; w mDokumentach zastosowanie może znaleźć zarówno rozwiązanie lokalne (dane biometryczne w telefonie posiadacza), jak i rozwiązanie centralne (rządowa baza danych biometrycznych);
- 2) transmisję danych zabezpieczoną kryptograficznie: jakkolwiek transmisja danych związanych z weryfikacją tożsamości w ramach mDokumentów (np. SMS, TAN itd.) powinna być zabezpieczona kryptograficznie;
- 3) wprowadzenie funkcjonalności mDokumentów w relacji obywatel – obywatel oraz obywatel – firma: społeczna użyteczność mDokumentów zostanie zrealizowana, jeśli mDokumenty będą funkcjonować nie tylko na potrzeby Policji lub urzędników, ale również na potrzeby samych obywateli; mDokumenty zatem powinny dawać możliwość potwierdzenia tożsamości nie tylko przed funkcjonariuszami czy urzędnikami, lecz także przed bankami, firmami i innymi obywatelami w celu realizacji wygodnego dla społeczeństwa oraz bezpiecznego obrotu prawnego i gospodarczego.

BIBLIOGRAFIA

- [1] BIELAKOWSKI C., GRABEK A., *Dowód, karta płatnicza i prawo jazdy na telefonie? Streżyńska: To mój cel*, <https://www.wprost.pl/tylko-u-nas/535894/Dowod-karta-pлатnicza-i-prawo-jazdy-na-telefonie-Strezyńska-To-moj-cel.html> [dostęp: 20.11.2016].
- [2] GRZEMSKI J., KRZEŚ A., *Analiza pojęcia „przestępstwa godzące w podstawy ekonomiczne państwa” w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, „Przegląd Bezpieczeństwa Wewnętrznego”, nr 2/2010.
- [3] HOŁYST B., POMYKAŁA J., *Biometria w systemach uwierzytelniania*, „Biuletyn WAT”, vol. LX, nr 4, 2011.

- [4] HOŁYST B., POMYKAŁA J., *Bezpieczeństwo informacji w świetle kryptografii, kanałów ukrytych i steganografii*, [w:] B. Hołyst, J. Pomykała, P. Potejko (red.), *Nowe techniki badań kryminalistycznych a bezpieczeństwo informacji*, PWN, Warszawa 2014.
- [5] *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego na 2016 r. Profil krajowy Polska*, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=14161 [dostęp: 20.11.2016].
- [6] IZAK K., *Falszywe dokumenty w rękach terrorystów*, „Człowiek i Dokumenty”, nr 32/2014.
- [7] KOŁECKI H., *Dokumenty publiczne – narzędzie przestępstwa czy ochrony przed nim?*, „Człowiek i Dokumenty”, nr 8/2008.
- [8] KOSIŃSKI D., *Netia zaatakowana! Dane klientów zostały wykradzione i ujawnione*, <http://www.spidersweb.pl/2016/07/netia-atak-2016.html> [dostęp: 20.11.2016].
- [9] LEWANDOWSKI R., *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych i banknotów*, [w:] M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Volumina, Warszawa 2016.
- [10] LEWANDOWSKI R., *Evaluation of legal and technical solutions with respect to new types of documents in the health care system – KUZ, KSM and KSA*, „Journal of Health Policy, Insurance and Management – Polityka Zdrowotna”, no. XVI/VI/2015.
- [11] LEWANDOWSKI R., *O potrzebie regulacji sfery dokumentów publicznych*, „Człowiek i Dokumenty”, nr 42/2016.
- [12] LEWANDOWSKI R., *Rola narodowego wytwórcy banknotów, dokumentów i towarzyszących im systemów IT w systemie bezpieczeństwa obrotu gospodarczego i prawnego*, [w:] K. Raczkowski (red.), *Bezpieczeństwo ekonomiczne obrotu gospodarczego*, Wolters Kluwer, Warszawa 2014.
- [13] LEWANDOWSKI R., GOLIŃSKI T., *Zarządzanie wiarygodnością dokumentów a bezpieczeństwo ekonomiczne*, [w:] K. Raczkowski (red.), *Zarządzanie w systemie gospodarczym. Szanse i zagrożenia*, Wolters Kluwer, Warszawa 2015.
- [14] *Raport o stanie bezpieczeństwa w Polsce w 2014 roku*, <https://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html> [dostęp: 20.11.2016].
- [15] TOMASZEWSKA M., *Technologia biometryczna w Polsce*, [w:] B. Hołyst (red.), *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, PWN, Warszawa 2014.
- [16] Załącznik nr 2 do SIP: opis docelowego modelu eID. *Krajowy Schemat Identyfikacji Elektronicznej (eID) w Polsce z uwzględnieniem budowy państwowego brokera eID i wykorzystaniem usług zaufania*, https://mc.gov.pl/files/zalacznik_nr_2_do_sip.pdf [dostęp: 20.11.2016].
- [17] <http://www.spidersweb.pl/2016/08/opera-sync-atak.html> [dostęp: 20.11.2016].
- [18] <https://mc.gov.pl/konsultacje/program-zintegrowanej-informatyzacji-panstwa/program-zintegrowanej-informatyzacji-panstwa> [dostęp: 20.11.2016].
- [19] <https://mc.gov.pl/konsultacje/program-zintegrowanej-informatyzacji-panstwa/zalacznik-1-strategia-informatyzacji-panstwa-plan-dzialan-ministra-cyfryzacji> [dostęp: 20.11.2016].
- [20] <http://www.rdc.pl/informacje/anna-strezynska-w-polsce-zaledwie-300-tys-osob-korzysta-z-profilu-zaufanego-jako-srodka-komunikacji-posluchaj/> [dostęp: 20.11.2016].
- [21] <http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-15> [dostęp: 28.12.2016].

THE ANALYSIS OF THREATS RELATED TO CITIZEN IDENTITY VERIFICATION WITH USE OF THE MOBILE PHONE

Abstract. The paper presents an analysis related to the introduction of the citizen identity verification mechanisms based on the mobile phone operation. The analysis refers to two possible models: one based on personal data stored and processed on the phone, and the other based on personal data stored and processed by central registers. The analysis leads to the conclusion that using a mobile phone as an instrument of citizen identification is questionable and it has various drawbacks. The most important of them refer to insufficient confidence related to the correctness of a verified identity (in case of no biometric tools used), high risk of identity theft by phishing or phone theft, dependence of the identity verification process on the battery lifespan, as well as GSM coverage.

Keywords: identity verification, GSM, security.