Kultura Bezpieczeństwa
Nauka – Praktyka – Refleksje
Nr 24, 2016 (135–150)
DOI 10.24356/KB/24/5

ANALIZA KONCEPCJI mDOKUMENTÓW

ANALYSIS OF THE mDOCUMENTS CONCEPT

REMIGIUSZ LEWANDOWSKI
Uniwersytet Mikołaja Kopernika w Toruniu

Abstract

The goal of the paper is to present an analysis related to an introduction of citizen identity verification mechanism based on the mobile phone. The analysis refers to the model published by the Ministry of Digitalization in *The Description of an IT Project's Design Brief* "mDocuments in the Public Administration in Poland – Phase 1". The model is based on personal data stored and processed by central registers.

The article is based on the analyses of *The Description of an IT Project's Design Brief,* the literature concerning the issue as well as publicly available data referring to the level of Poland's digitalization.

The analysis shows 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 (resulting from lack of biometric tools), 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.

The article leads to the conclusion that one should consider possible ways of increasing the identification security in the prospective work on the idea

of mDocuments. These ways include identification based on biometric tools and SMS encryption.

Keywords: identity verification, GSM, security

Abstrakt

Celem artykułu jest przedstawienie analizy zagrożeń związanych z wdrożeniem mechanizmu weryfikacji tożsamości obywatela poprzez wykorzystanie telefonu komórkowego. Analiza ta dotyczy modelu opublikowanego przez Ministerstwo Cyfryzacji *Opisu założeń projektu informatycznego* pn. „mDokumenty w Administracji Publicznej w Polsce – Faza 1", opartego o dane identyfikacyjne przechowywane i przetwarzane w ramach rejestrów centralnych.

Artykuł oparto o analizę *Opisu założeń projektu informatycznego* oraz analizę literatury przedmiotu i publicznie dostępnych danych dotyczących stopnia informatyzacji Polski.

Analiza wskazuje, 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 wynikająca m.in. z niezastosowania 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.

Artykuł prowadzi do wniosku, że w dalszych pracach nad koncepcją mDokumentów rozważone powinny zostać możliwości zwiększenia bezpieczeństwa identyfikacyjnego poprzez wprowadzenie identyfikacji opartej o narzędzia biometryczne oraz poprzez wprowadzenie szyfrowania SMS.

Słowa kluczowe: weryfikacja tożsamości, GSM, bezpieczeństwo

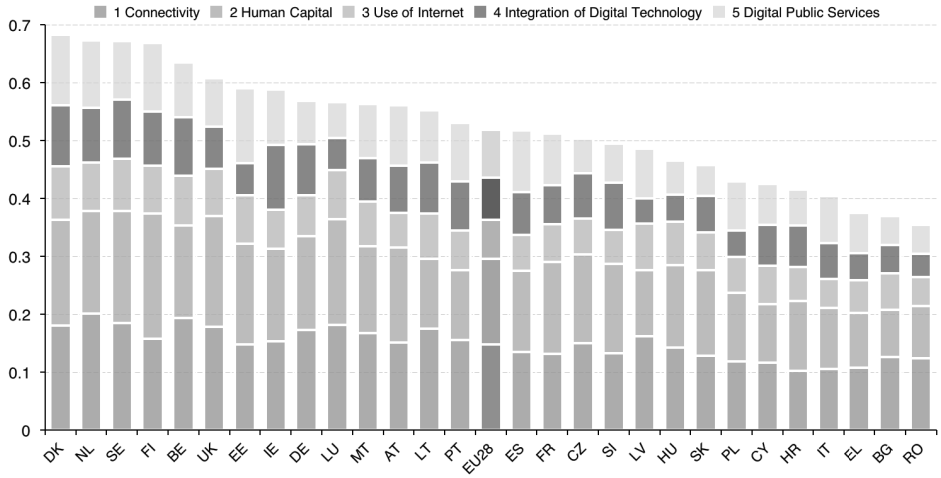
Wstęp

W listopadzie 2016 r. opublikowany został przez Ministerstwo Cyfryzacji *Opis założeń projektu informatycznego* pn. „mDokumenty w Administracji Publicznej w Polsce – Faza 1"[1]. Opracowanie to stanowi kolejną inicjaty-

[1] http://krmc.mc.gov.pl/download/50/14516/OpiszalozenprojektuinformatycznegomDokumenty-faza1-wersjakoncowa.docx (dostęp: 14.11.2016)

wę Ministerstwa Cyfryzacji w zakresie upowszechniania rozwiązań cyfrowych i eliminacji tzw. wykluczenia cyfrowego. Zaprezentowana koncepcja mDokumentów dołącza zatem do sztandarowych projektów w ramach programu Paperless/Cashless, a także m.in. wdrożonej usługi potwierdzania profilu zaufanego poprzez bankowość elektroniczną i przedstawionej koncepcji elektronicznego dowodu osobistego. W ten sposób resort cyfryzacji wprost odnosi się do często podnoszonego w literaturze przedmiotu oraz w mediach zagadnienia niskiego stopnia informatyzacji państwa. Należy zauważyć, 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 nadrabiania przez nią zaległości jest niższe w porównaniu z wynikiem DESI między 2014 a 2015 r."[2] Szczegóły indeksu za 2016 r. przedstawia ryc. 1.

Ryc. 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.

[2] *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).

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)"[3]. 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.

Projekt „mDokumenty w Administracji Publicznej w Polsce – Faza 1" doprowadzić ma do „urzeczywistnienia wizji elektronicznej prezentacji tożsamości i dokumentów obywatela" poprzez „wykorzystanie e-usług polskiej e-administracji pozwalających na wyświetlanie danych dokumentów w postaci elektronicznej z Systemu Rejestrów Państwowych lub innych wiarygodnych baz i systemów"[4]. Innymi słowy chodzi o możliwość potwierdzenia tożsamości obywatela oraz jego uprawnień (wynikających np. z prawa jazdy) poprzez telefon komórkowy. Zagadnienie to jest na tyle istotne dla bezpieczeństwa państwa i bezpieczeństwa obywateli, że wymaga wnikliwej analizy i otwartej dyskusji na temat mocnych i słabych stron prezentowanego rozwiązania, a także ryzyka z nim związanego. Niniejszy artykuł oparto o analizę wskazanego *Opisu założeń projektu informatycznego* oraz analizę literatury przedmiotu i publicznie dostępnych danych dotyczących stopnia informatyzacji Polski.

1. Zasadnicze założenia projektu

Idea funkcjonowania mDokumentu została zaprezentowana na ryc. 1.

[3] Ibidem.

[4] *Opis założeń projektu informatycznego* pn. „mDokumenty w Administracji Publicznej w Polsce – Faza 1", s. 4.

Ryc. 1. Proces weryfikacji tożsamości obywatela przy zastosowaniu mDokumentu.

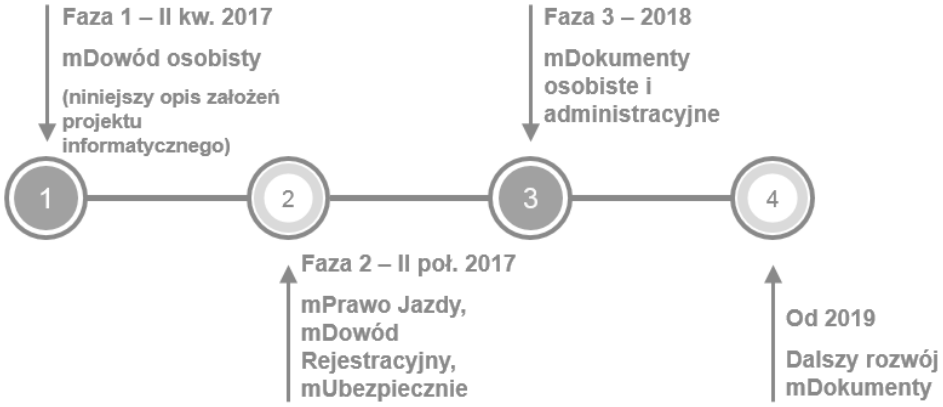
Źródło: *Opis założeń projektu informatycznego* pn. „mDokumenty w Administracji Publicznej w Polsce – Faza 1", s. 7.

Zgodnie ze schematem przedstawionym na ryc. 1 weryfikacja tożsamości obywatela przy zastosowaniu mDokumentu rozpoczyna się od przekazania urzędnikowi lub funkcjonariuszowi Policji (bądź innych służb) numeru PESEL lub numeru telefonu komórkowego przez obywatela, którego tożsamość ma zostać sprawdzona (czynność nr 1). W przypadku podania numeru telefonicznego wymaga to uprzedniego zarejestrowania numeru przez obywatela w odpowiednich rejestrach państwowych. Czynność ta, poprzedzająca cały proces weryfikacji tożsamości, nie została jednak ujęta na schemacie. Kolejnym krokiem jest wprowadzenie wspomnianego numeru telefonicznego lub PESEL do odpowiedniej Aplikacji Dostępowej przez funkcjonariusza państwowego weryfikującego tożsamość (czynność nr 2). Podkreślić należy, że w przypadku weryfikacji tożsamości poza urzędem (np. na ulicy lub podczas kontroli drogowej) konieczne będzie wyposażenie funkcjonariuszy w odpowiednie urządzenia mobilne z dostępem do transferu danych (tablety lub smartfony). Kolejnym etapem

procesu jest weryfikacja numeru przez system informatyczny i przesłanie obywatelowi jednorazowego kodu w formie SMS na telefon obywatela (czynność nr 3). Oparcie projektu o mechanizm kodu w formie SMS umożliwia wykorzystanie do tego celu każdego rodzaju modelu telefonu komórkowego, a nie tylko smartfonów. Przesłany kod obywatel powinien przekazać funkcjonariuszowi (czynność nr 4), który następnie wpisuje go do Aplikacji Dostępowej celem otrzymania dostępu do danych identyfikacyjnych obywatela przechowywanych w Systemie Rejestrów Państwowych (czynność nr 5). Na podstawie wprowadzonego i zweryfikowanego przez system kodu System Rejestrów Państwowych powinien udostępnić na Aplikacji Dostępowej funkcjonariusza dane identyfikacyjne obywatela, w tym jego zdjęcie (czynność nr 6). Zgodnie z przedstawionym w *Opisie założeń projektu informatycznego* weryfikacja tożsamości powinna nastąpić poprzez porównanie zdjęcia wyświetlonego na Aplikacji Dostępowej z rzeczywistym wizerunkiem obywatela (czynność nr 7).

Projekt mDokumentów obejmuje niesprecyzowany katalog dokumentów, których okazywanie przez obywatela miałoby przyjąć formę przedstawioną na ryc. 1. Autorzy *Opisu założeń projektu informatycznego* wskazali, że katalog ten objąć ma dane zawarte w dowodzie osobistym, prawie jazdy, dowodzie rejestracyjnym, ubezpieczeniu OC/AC oraz innych dokumentów (np. akt małżeństwa, akt urodzenia i in.). Projekt udostępniania danych z poszczególnych dokumentów poprzez zaprezentowany wyżej mechanizm został podzielony na 4 etapy, co przedstawiono na ryc. 2.

Ryc. 2. Etapy projektu mDokumentów



Źródło: *Opis założeń projektu informatycznego* pn. „mDokumenty w Administracji Publicznej w Polsce – Faza 1", s. 8.

2. Analiza wybranych zagadnień problematycznych

2.1. Uwagi wstępne

Pozytywnie należy ocenić konstrukcję *Opisu założeń projektu informatycznego* pn. „mDokumenty w Administracji Publicznej w Polsce – Faza 1". W strukturze dokumentu ujęto bowiem wszystkie niezbędne elementy koncepcji, wiążąc je w spójną całość. Przedstawiono zatem przesłanki projektu, w tym identyfikację problemu i potrzeb, alternatywne warianty biznesowe projektu, jego cele i efekty, a także harmonogram, kosztorys i przegląd ryzyk. W dokumencie przedstawiono także analizę kompetencji Ministerstwa Cyfryzacji do realizacji przedmiotowego projektu, metodologię prowadzenia projektu, analizę techniczną oraz analizę bezpieczeństwa. Ujęcie tych wszystkich elementów w *Opisie założeń projektu informatycznego* należy ocenić pozytywnie. Niemniej jednak zasadniczą kwestią jest nie tylko ocena struktury dokumentu, ale również ocena jakości poszczególnych elementów składowych analizowanego dokumentu.

2.2. Przesłanki wdrożenia mDokumentów

Analizę treści projektu należy rozpocząć od przesłanek, które legły u jego podstaw. Za przesłanki te przyjmuje się trzy zagadnienia, zdefiniowane w dokumencie jako „problemy", tj.[5]:

- „konieczność kompletowania, przechowywania i noszenia dokumentów w postaci papierowej/plastikowej przez obywatela w sytuacji, gdy nie istnieje odpowiednia e-usługa. (…) Samo noszenie dużej ilości dokumentów w portfelu może przy tym obywatelowi utrudniać codzienne życie.";
- „konieczność ręcznego przepisywania danych z dokumentów papierowych/plastikowych do formularzy urzędowych lub służb mundurowych (…), co wydłuża czas obsługi obywatela.";
- „przekazywanie wszelkich dokumentów, w tym zaświadczających o ubezpieczeniu pojazdu, innym kierowcom w rodzinie (…). Wielu kierowców zapomina przekazać dokumenty lub wręcz ich przekazanie nie jest możliwe."

Powyższych przesłanek nie można uznać za wystarczające do podjęcia decyzji o implementacji omawianego projektu. Traktowanie tradycyjnych dokumentów noszonych w portfelu jako znaczącego utrudnienia

[5] Ibidem, s. 11–12.

„codziennego życia" Polaków, czy też przesłanka katorżniczej czynności przekazywania dowodu rejestracyjnego z OC/AC innej osobie korzystającej z tego samego pojazdu nie przekonują o konieczności i zasadności wprowadzenia mDokumentów. Ponadto, jeśli nawet uznać wszystkie trzy przesłanki jako wyczerpującą argumentację za wprowadzeniem mDokumentów, to nie można ich traktować a priori jako „problemy". Tymczasem niezweryfikowane hipotezy zostały potraktowane właśnie jako tezy, tj. problemy, których rozwiązanie wymaga wprowadzenia mDokumentów. To rażący błąd metodologiczny. W pierwszej kolejności należałoby bowiem zbadać, czy faktycznie obywatele traktują noszenie dowodu osobistego i prawa jazdy w portfelu jako „znaczną ilość" dokumentów i czy faktycznie stanowi to dla nich „utrudnienie życia codziennego". Analogicznie, przeprowadzenia dowodu wymaga a priori przyjęta hipoteza, że obsługa obywatela przy zastosowaniu tradycyjnych dokumentów zabiera statystycznie istotnie więcej czasu aniżeli obsługa przy pomocy mDokumentów. Na marginesie należy zaznaczyć, że powierzchowna analiza wszystkich siedmiu czynności wymaganych przy weryfikacji tożsamości za pomocą mDokumentu skłania raczej do wniosku nie o skróceniu czasu obsługi obywatela, ale wręcz przeciwnie – o jego wydłużeniu. Wreszcie weryfikacji wymaga trzecia przesłanka związana z uciążliwością przekazywania dowodu rejestracyjnego i OC/AC pomiędzy kierowcami korzystającymi z tego samego pojazdu. Bez weryfikacji tych trzech przesłanek nie można ich uznać za poważne argumenty na rzecz wprowadzenia mDokumentów. Zresztą nawet pozytywna weryfikacja tych hipotez nie stanowić będzie wystarczającej podstawy do podjęcia decyzji o wprowadzeniu mDokumentów, albowiem nawet jeśli prawdziwe, to jednak są to argumenty zbyt słabe w odniesieniu do skali zagrożeń, które niosą za sobą mDokumenty i do skali środków publicznych koniecznych do realizacji omawianego przedsięwzięcia. Przesłanki i potrzeby nie zostały więc wystarczająco precyzyjnie oraz prawidłowo zidentyfikowane.

2.3. Poprawność i wiarygodność weryfikacji tożsamości

Kolejną słabością koncepcji mDokumentów jest oparcie procesu weryfikacji tożsamości o wizualne porównanie zdjęcia obywatela z jego rzeczywistym wizerunkiem podczas procesu 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 w 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 okresy krótsze ważności dokumentu, np. 5-letnie). Weryfikacja oparta wyłącznie o subiektywny zmysł 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. Tymczasem mDokumenty mają w swej koncepcji opierać się właśnie o subiektywny zmysł widzenia i subiektywne porównanie zdjęcia danej osoby z jej rzeczywistym wizerunkiem.

Zastosowanie omawianej metody weryfikacji tożsamości w mDokumentów stanowi zatem krok wstecz, bowiem nawet niedoskonała *Koncepcja wdrożenia polskiego dowodu osobistego z warstwą elektroniczną* zakłada wydawanie nowych dowodów osobistych z danymi biometrycznymi i wykorzystanie właśnie tych danych w procesie weryfikacji tożsamości. Biometria to wiedza o rozpoznawaniu żywych osób w oparciu o pomiary 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)[6]. Współcześnie biometria stanowi stałe, a zarazem kluczowe ogniwo łańcucha wartości dokumentów identyfikacyjnych.

W literaturze przedmiotu wskazuje się na warunki konieczne, które towarzyszyć muszą skutecznemu uwierzytelnianiu biometrycznemu, takie jak optymalne warunki dokonania pomiaru biometrycznego, aktualizacja pomiaru biometrycznego, optymalny poziom tolerancji.[7] 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.

Trudno zrozumieć odrzucenie biometrii jako narzędzia weryfikacji tożsamości w mDokumentach. Prawidłowość i pewność weryfikacji tożsamości są podstawowym atrybutem bezpieczeństwa identyfikacyj-

[6] B. Hołyst, J. Pomykała, *Biometria w systemach uwierzytelniania*, Biuletyn WAT, vol. LX, nr 4, 2011, s. 418–419.

[7] 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.

nego.[8] W przypadku omawianej koncepcji mDokumentów te czynniki bezpieczeństwa identyfikacyjnego nie są zachowane, a zastosowane narzędzie weryfikacji tożsamości (subiektywne porównanie zdjęcia z osobą się legitymującą) nie przystaje do współczesnych zagrożeń i dostępnych technologii, a w szczególności narzędzi opartych o biometrię.

2.4. Definicje

W dokumencie zdefiniowano szereg pojęć, które są stosowane w tekście. Sam fakt ujęcia w dokumencie definicji wybranych pojęć należy ocenić pozytywnie. Niemniej jednak same definicje są niedoskonałe i wymagają doprecyzowania.

W *Opisie założeń projektu informatycznego* mDokumenty definiuje się jako „zbiór danych dotyczących osoby lub rzeczy udostępnianych z rejestrów państwowych na wniosek Strony Weryfikującej. Zbiór danych z zakresie (winno chyba być: „w zakresie", przyp.: RL) każdego dokumentu mobilnego będzie podlegać modyfikacjom na podstawie odrębnych przepisów analogicznie, do modyfikacji dotyczących tradycyjnych wersji tych dokumentów"[9]. W definicji tej użyto nigdzie indziej nie zdefiniowanego pojęcia „dokumentu mobilnego". Czy autorzy traktują pojęcia „mDokumentu" i „dokumentu mobilnego" synonimicznie, czy też są to pojęcia różnoznaczne? *Opis założeń projektu informatycznego* tego nie rozstrzyga. Przytoczona definicja nie precyzuje także, jak szeroki jest zakres danych udostępnianych w ramach mDokumentu. Czy jest on tożsamy z zakresem danych umieszczonych w jego „analogowym" odpowiedniku, czy też jest on szerszy lub węższy? Tego definicja również nie precyzuje.

Jeszcze większe wątpliwości budzi definicja mDowodu Osobistego jako „zbioru danych powiązanych z identyfikatorem obywatela stanowiących podstawę do określenia cech jego dokumentu tożsamości (np. numer dowodu, data wydania, organ wydający, data ważności)"[10]. Ta definicja z kolei posługuje się pojęciem „identyfikatora obywatela", które nie zostało nigdzie indziej sprecyzowane. Czym zatem jest mDowód Osobisty? Czy

---

[8] 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.

[9] *Opis*…, op. cit., s. 9.

[10] Ibidem, s. 9.

stanowi zbiór danych pozwalających na zidentyfikowanie numeru „analogowego" dowodu osobistego? Czy jest zbiór wybranych danych z dowodu osobistego? Wątpliwości interpretacyjnych jest wiele.

Podobnych wątpliwości jest więcej i dotyczą one praktycznie wszystkich pojęć zdefiniowanych w *Opisie założeń projektu informatycznego.*

2.5. Zakres funkcjonowania mDokumentów

Dokumenty identyfikacyjne są powszechnie używane w obrocie gospodarczym i prawnym w relacjach:
– obywatel – administracja publiczna, w tym służby mundurowe,
– obywatel – obywatel,
– obywatel – podmioty gospodarcze.

Z tego powodu dąży się do tego, aby dokumenty te mogły być łatwo weryfikowane nie tylko przez specjalistów czy funkcjonariuszy służb mundurowych pod względem autentyczności oraz pod względem zgodności tożsamości osoby legitymującej się danym dowodem z tożsamością osoby, której dany dokument dotyczy. Dokumenty są bowiem czynnikiem zapewniającym ład wewnętrzny w państwie i administrowanie państwem[11]. Tymczasem koncepcja mDokumentu, przynajmniej w odniesieniu do zaprezentowanej fazy projektu, ogranicza się do możliwości jego wykorzystania wyłącznie w relacjach obywatel – administracja publiczna, w tym służby mundurowe. Oznacza to, że omawiana koncepcja bardziej może służyć aparatowi państwowemu aniżeli obywatelowi. To błędne założenie, albowiem e-usługi państwa powinny być w pierwszej kolejności nakierowane na potrzeby obywateli i podmiotów gospodarczych, a nie urzędników. mDokument nie znajdzie zatem zastosowania w bankowości przy zakładaniu rachunku, zaciąganiu kredytu czy wypłacie gotówki w oddziale. mDokumentem nie będzie się można posługiwać, chcąc zweryfikować tożsamość osoby, z którą podpisywana jest umowa. Wreszcie mDokument nie przyda się w sytuacji kolizji drogowej, kiedy jego uczestnicy bez udziału Policji chcą wzajemnie spisać swoje dane. Czy w takiej zatem formie jest mDokumenty będą spełniać swoje służebne wobec obywateli funkcje?

Inną słabością koncepcji jest uzależnienie od przebywania w zasięgu sieci GSM. W Polsce cały czas do czynienia mamy z istnieniem stref nie

[11] R. Lewandowski, *Dylematy metodologicznej triady: bezpieczeństwo, gospodarka, władza państwowa*, [w:] W. Kitler, T. Kośmider, *Metodologiczne i dydaktyczne aspekty bezpieczeństwa narodowego*, Difin, Warszawa 2015, s. 264.

pokrytych zasięgiem GSM. W takiej sytuacji system mDokumentu jest całkowicie bezużyteczny. Podobnie bezużyteczny mDokument staje się w sytuacji wyładowania baterii telefonu komórkowego. To poważne mankamenty osłabiające funkcjonalność mDokumentu.

2.6. Ryzyko kradzieży tożsamości

Zagadnienie kradzieży tożsamości jako jednego z najważniejszych ryzyk towarzyszących implementacji rozwiązań opartych o ideę „dokumentu w telefonie" lub „dokumentu w Internecie". mDokument wydaje się doskonałym narzędziem z punktu widzenia hakerów zainteresowanych przejęciem cudzej tożsamości w różnych celach, w szczególności terrorystycznych lub związanych z przestępczością gospodarczą. Potwierdza to *Raport 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 dokonywania płatności w Internecie, np. bitcoin, pozostając poza jakąkolwiek kontrolą instytucji finansowych"[12].

Raport 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 tożsamości obywateli i ich bezpieczeństwa identyfikacyjnego – po rozszczelnieniu systemu dostępu do danych

[12] *Raport o stanie bezpieczeństwa w Polsce w 2014 r.*, http://isp.policja.pl/isp/aktualnosci/7789,Raport-o-stanie-bezpieczenstwa-w-Polsce-w-2014-r.html (dostęp: 20.11.2016).

identyfikacyjnych obywateli. Innym zagrożeniem związanym z mDokumentem jest wskazane w samym *Opisie założeń projektu informatycznego* ryzyko wykorzystania cudzego aparatu telefonicznego i wykorzystania go w celu podszycia się pod inną osobę (kradzieży tożsamości) w ramach funkcjonalności mDokumentu. Numer telefoniczny, na który wysyłany ma być SMS, związany jest nierozerwalnie z kartą SIM, a nie z obywatelem będącym posiadaczem karty. W sytuacji braku implementacji rozwiązań biometrycznych w mDokumencie ryzyko skuteczności takiej kradzieży tożsamości można uznać za wysokie. Ponadto, *Opis założeń projektu informatycznego* wskazuje niekontrolowany dostęp do usługi mDokumenty oraz zrealizowanie zbyt trywialnego rozwiązania (szczególnie ze zdjęciem) i łatwego do złamania oraz hakowania jako duże ryzyka wpływające na realizację projektu. 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”[13]. Koncepcja mDokumentu musi zatem odpowiadać na powyższe zagrożenia.

Skalę potencjalnych zagrożeń pozwala dostrzec analiza wybranych przypadków znaczących cyberataków. Dobrym przykładem w tym zakresie jest włamanie do profesjonalnego systemu do generowania, przechowywania i dystrybucji certyfikatów elektronicznych. Holenderskie centrum certyfikacji elektronicznej DigiNotar, wystawiające cyfrowe certyfikaty kwalifikowane i certyfikaty SSL dla potrzeb zabezpieczenia komunikacji z witrynami internetowymi, było przedmiotem co najmniej kilku włamań, w efekcie których hakerzy wystawili 531 fałszywych certyfikatów, zarówno dla serwisów komercyjnych (np. Google oraz Facebook), jak i rządowych agencji zajmujących się bezpieczeństwem[14]. W literaturze przedmiotu podkreśla się także podatność publicznych bramek SMS jako systemów używanych w szczególności przy przestępstwach związanych z włamaniami do kont bankowych poprzez wykorzystanie mechanizmu autoryzacji transakcji przez SMS[15]. Przejęcie treści SMS możliwe jest także poza bramkami publicznymi SMS. Jak wskazuje praktyka tego rodza-

[13] B. Hołyst, J. Pomykała, *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, s. 131.

[14] T. Goliński, *Dokumenty biometryczne a cyberprzestępczość*, „Człowiek i Dokumenty”, nr 38/2015, s, 39.

[15] B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor, K. Butler, *Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gates*, IEEE Symposium on Secu-

ju zdarzenia mogą mieć miejsce poprzez atak hakerski na Centrum SMS (SMS Center)[16], tj. centrum zarządzające wiadomościami SMS i pośredniczące pomiędzy abonentami przy przesyłaniu wiadomości SMS. Z tego względu w przypadku konieczności ochrony treści SMS szczególnego znaczenia nabierają dostępne możliwości ich szyfrowania.

2.7. Koszty

Całkowity koszt projektu trzech etapów szacowany jest na 4,4 mln zł brutto, a przewidywany roczny koszt utrzymania trwałości projektu na 0,9 mln zł brutto rocznie. Założeniom tym towarzyszy zastrzeżenie, że ryzyko niedoszacowania kosztów projektu jest duże. W przedmiotowych kosztach nie ujęto jednak znaczących nakładów koniecznych na infrastrukturę towarzyszącą całemu projektowi, tj. wyposażenie funkcjonariuszy w urządzenia mobilne do weryfikacji tożsamości za pomocą mDokumentów (tablety lub smartfony) oraz koszty utrzymania tej infrastruktury i koszty łączności. Ocena skutków finansowych omawianego przedsięwzięcia powinna być zatem oparta o łączne koszty z niego wynikające.

Podsumowanie

Przedstawiony *Opis założeń projektu informatycznego* pn. „mDokumenty w Administracji Publicznej w Polsce – Faza 1" wymaga poprawy. 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 materiale wątpliwości. W szczególności rozważone powinny zostać możliwości zwiększenia bezpieczeństwa identyfikacyjnego poprzez wprowadzenie identyfikacji opartej o narzędzia biometryczne oraz poprzez wprowadzenie szyfrowania SMS. Ważne jest, aby obiektywnej i ważnej potrzeby bezpieczeństwa identyfikacyjnego nie przesłoniła pogoń za mylnie rozumianą innowacją czy też po prostu modą. Zaprezentowana na obecnym etapie koncepcja mDokumentów zdaje się jednak przeczyć temu postulatowi. Zakłada ona, jako jeden z podstawowych celów projektu, „wykonanie całego procesu wyświetlania danych dowodu osobistego, od wywołania usługi poprzez autoryzację za pomocą kodu

rity and Privacy, 2016, s. 339, https://www.cise.ufl.edu/~traynor/papers/reaves-sp16.pdf (dostęp: 27.11.2016).

[16] M. Khan, *SMS Security in Mobile Devices: A Survey*, "International Journal of Advanced Networking and Applications", 5 (2)/2013, s. 1873–1874.

sms, po wyświetlenie danych na uprawnionym urządzeniu urzędnika". Korzyść z tego celu określono zaś jako „realizację procesu w sposób cyfrowy, bez korzystania z papierowych dokumentów". W tak sformułowanym celu i wynikających z niego korzyści uderza brak wartości dodanej z punktu widzenia obywatela i zaspokojenia jego obiektywnych potrzeb.

W świetle przedstawionych założeń wydaje się jednak, że pochodząca sprzed kilku lat wizja „systemów identyfikacyjnych funkcjonujących bez udziału zewnętrznych nośników informacji, które dotychczas zawierały dane niezbędne do weryfikacji tożsamości"[17], świata „bez dokumentów, gdyż informacje w określonym zakresie dotyczące danej osoby będą dostępne innym systemom"[18] i człowieka jako podstawowego zbioru informacji o jego tożsamości (na podstawie unikatowych cech fizjologicznych) ma szansę na realizację. Przedstawiony jednak *Opis założeń projektu informatycznego* wymaga znaczących korekt, aby faktycznie przybliżyć się do tak zarysowanej wizji.

Bibliografia

1. Goliński T., *Dokumenty biometryczne a cyberprzestępczość*, „Człowiek i Dokumenty", nr 38/2015.
2. Hołyst B., Pomykała J., *Biometria w systemach uwierzytelniania*, Biuletyn WAT, vol. LX, nr 4, 2011.
3. 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.
4. Khan M., *SMS Security in Mobile Devices: A Survey*, "International Journal of Advanced Networking and Applications", 5 (2)/2013.
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. Lewandowski R., *Dylematy metodologicznej triady: bezpieczeństwo, gospodarka, władza państwowa*, [w:] W. Kitler, T. Kośmider, *Metodologiczne i dydaktyczne aspekty bezpieczeństwa narodowego*, Difin, Warszawa 2015.
7. Lewandowski R., *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych i banknotów*, [w:] M. Goc, T. Tomaszewski, R. Lewan-

[17] D. Poślad, *Przyszłość dokumentów identyfikacyjnych*, „Człowiek i Dokumenty", nr 28/2013, s. 38.

[18] Ibidem.

dowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Volumina, Warszawa 2016.
8. Poślad D., *Przyszłość dokumentów identyfikacyjnych*, „Człowiek i Dokumenty", nr 28/2013.
9. *Raport o stanie bezpieczeństwa w Polsce w 2014 r.*, http://isp.policja.pl/isp/aktualnosci/7789,Raport-o-stanie-bezpieczenstwa-w-Polsce-w-2014-r.html (dostęp: 20.11.2016).
10. Reaves B., Scaife N., Tian D., Blue L., Traynor P., Butler K., *Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gates*, IEEE Symposium on Security and Privacy, 2016, https://www.cise.ufl.edu/~traynor/papers/reaves-sp16.pdf (dostęp: 27.11.2016).
11. M. Tomaszewska, *Technologia biometryczna w Polsce* [w:] B. Hołyst (red.), *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, PWN, Warszawa 2014.

Remigiusz Lewandowski (urodzony w Toruniu w 1977 r.) – ekspert zajmujący się bezpieczeństwem identyfikacyjnym oraz cyberbezpieczeństwem. W swojej karierze zawodowej związany m.in. z Polską Wytwórnią Papierów Wartościowych S.A, a także z wieloma spółkami kapitałowymi działającymi w branży IT i e-payments, gdzie zajmował stanowiska zarządcze. Równocześnie współpracuje z Wydziałem Bezpieczeństwa Narodowego Akademii Sztuki Wojennej w Warszawie oraz Wydziałem Nauk Ekonomicznych i Zarządzania UMK w Toruniu, na którym w 2011 r. uzyskał stopień doktora nauk ekonomicznych. Jest członkiem Rady Przemysłowo-Programowej Wydziału Elektroniki Wojskowej Akademii Technicznej w Warszawie. Zainteresowania badawcze dra R. Lewandowskiego obejmują bezpieczeństwo narodowe, zarządzanie strategiczne, zarządzanie finansami oraz zagadnienia corporate governance. Jest autorem kilkudziesięciu artykułów naukowych oraz rozdziałów w monografiach poświęconych wyżej wskazanym zagadnieniom.

Dr R. Lewandowski jest absolwentem Aarhus School of Business w Danii (obecnie Uniwersytet w Aarhus) na kierunku Master of Science in Finance and International Business oraz Wydziału Nauk Ekonomicznych i Zarządzania UMK w Toruniu, a także studiów specjalnych w zakresie prawa europejskiego na Wydziale Prawa i Administracji oraz Centrum Studiów Europejskich UMK. Uczestniczył w stażach i stypendiach naukowych na uczelniach zagranicznych w Finlandii (Uniwersytet Wschodniej Finlandii, Uniwersytet Techniczny Północnej Karelii) oraz Australii (RMIT University). Absolwent programu Executive MBA prowadzonego przez Uniwersytet Warszawski w kooperacji z University of Illinois.