S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 143–162 ROK 2017

ISSN 2543–7321

Mariusz Terebecki

Akademia Pomorska
Słupsk
mariusz.terebecki@apsl.edu.pl

Marcin Olkiewicz

Politechnika Koszalińska
Koszalin
marcin.olkiewicz@tu.koszalin.pl

JAKOŚĆ ZABEZPIECZEŃ INFORMACJI DETERMINANTĄ ROZWOJU BANKOWOŚCI INTERNETOWEJ

QUALITY OF INFORMATION SECURITY FOR DETERMINANTS DEVELOPMENT OF INTERNET BANKING

***Zarys treści*:** W warunkach szybko zmieniającego się otoczenia banki poszukują nowych sposobów na uzyskanie przewagi konkurencyjnej na rynku. Znaczącą determinantą kreującą zmiany jest jakość, a w szczególności jakość bezpieczeństwa informacji. To właśnie między innymi ona zmusza banki do ponoszenia nakładów na dostosowanie systemów informatycznych do oczekiwań międzynarodowych i światowych rynków finansowych oraz interesariuszy. Współczesny, wymagający interesariusz coraz częściej domaga się usług o wysokim standardzie, często dostarczanych za pomocą nowych technologii. Dlatego banki podejmują strategiczne działania mające na celu dostosowanie swoich produktów, usług do wymagań i oczekiwań interesariuszy a jednocześnie, poprzez wdrażane innowacje, generowanie nowych potrzeb. Należy jednak pamiętać, że wszystkie działania bankowe muszą gwarantować interesariuszom banku bezpieczeństwo informacji. Celem pracy jest ukazanie, jakie aspekty zabezpieczeń, które pośrednio wpływają na jakość oferowanej usługi bankowej, są kluczowe w bankowości elektronicznej. W publikacji zostaną przeanalizowane certyfikaty i zabezpieczenia, które są wykorzystywane w chwili kontaktu klienta z badanym bankiem poprzez platformę internetową. Do celów badawczych wykorzystano raporty PRNews.pl o stanie bankowości w Polsce w IV kwartale 2016 r.

***Słowa kluczowe*:** zabezpieczenia, jakość, bankowość internetowa, bank
***Key words*:** security, quality, online banking, bank

Wprowadzenie

Jakość obsługi klienta jest jednym z ważniejszych elementów kreowania przewagi konkurencyjnej przedsiębiorstwa. Widoczne jest to również w bankowości, a szczególnie w bankowości elektronicznej. Bankowość elektroniczna, jako innowacyjność procesu świadczenia usług, w obecnych czasach stała się standardem w bankowości, tworząc wartość dodaną dla poszczególnych banków oraz ich klientów. Brak bezpośredniego kontaktu z pracownikami banku sprawia, że istotna jest jakość oferowanej elektronicznie usługi, która w odpowiedni sposób musi przekazywać, przetwarzać i generować informacje, poprzez odpowiednie zabezpieczenia gwarantujące i kreujące odpowiednią relację banku z klientem.

Należy zatem uznać, że jakość oferowanych produktów, asortyment oraz dostępność stały się determinantami rozwoju banków w Polsce. Dowodzą tego ostatnie trzy raporty opublikowane przez PRNews.pl pod koniec marca 2017 r., które podsumowują IV kwartał 2016 r. w obszarach: liczby klientów w bankach[1], rynku kont osobistych[2] oraz bankowości internetowej[3]. Przedstawione dane wyraźnie wskazują, iż liczba klientów z dostępem do bankowości elektronicznej sukcesywnie wzrasta i wynosi około 31 mln[4]. Widoczny trend wynikać może z odpowiedniego sposobu zarządzania bankami, w ramach odpowiednich systemów zarządzania, poprzez podejmowane i realizowane strategiczne działania ukierunkowane na jakość[5]. Odpowiednie i odpowiedzialne zarządzanie jakością, w ramach ciągłego doskonalenia, jest wynikiem rosnących oczekiwań i wymagań klientów, a także zagrożeń rynkowych widocznych w szczególności w sieci bankowości internetowej. Zaspokajanie potrzeb oraz zwiększanie satysfakcji interesariuszy sektora bankowego wymaga wysokiej skuteczności banku m.in. z zakresu marketingu – oferowania nowych produktów, a także teleinformatyki – gwarantowania bezpiecznego sposobu dostarczania i zakupu usługi.

Celowe zatem staje się sprawdzenie wdrożonych przez poszczególne banki zabezpieczeń dostępu do usług z rodziny e-bankingu. Ponadto przyjęta[6] przez banki

---

[1] Raport PRNews.pl: Liczba klientów w bankach – IV kw. 2016, http://prnews.pl/wiadomosci/raport-prnewspl-liczba-klientow-w-bankach-iv-kw-2016-6554091.html (dostęp: 31.03.2017).

[2] Raport PRNews.pl: Rynek kont osobistych – IV kw. 2016, http://prnews.pl/raporty/raport-prnewspl-rynek-kont-osobistych-iv-kw-2016-6553975.html (dostęp: 31.03.2017).

[3] Raport PRNews.pl: Rynek bankowości internetowej – IV kw. 2016, http://prnews.pl/wiadomosc/raport-prnewspl-rynek-bankowosci-internetowej-iv-kw-2016-6554056.html (dostęp: 31.03.2017).

[4] Wartość ta nie może być bezpośrednio zestawiona z liczbą ludności w Polsce, wynika to z prostego faktu – istnieje na pewno spora grupa klientów, którzy są klientami równocześnie kilku banków.

[5] M. Olkiewicz, *Zarządzanie jakością w sektorze bankowym w dobie wejścia do Unii Europejskiej*, [w:] *Rynki finansowe w przestrzeni elektronicznej*, red. B. Świecka, Szczecin 2004.

[6] W dniu 8 stycznia 2013 r. Komisja Nadzoru Finansowego jednogłośnie przyjęła Rekomendację D dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach. KNF przewidywała, że zalecenia zostaną wprowadzone nie później niż do dnia 31 grudnia 2014 r.

Rekomendacja D[7], dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, zobowiązuje je m.in. do systematycznego wykonywania analizy ryzyka teleinformatycznego. Zatem świadczone usługi powinny być na najwyższym poziomie, zgodnym z obowiązującą wiedzą informatyczną z dziedziny bezpieczeństwa oraz winny być odporne na znane rodzaje ataków wymierzone we wdrożone zabezpieczenia.

Rekomendacja D

Banki, uważane za instytucje zaufania publicznego, szczególną uwagę zwracają na jakość usługi bankowej, a przede wszystkim bezpieczeństwo finansowe[8] odbiorcy informacji. Poczucie bezpieczeństwa odczuwane przez interesariuszy banku wpływa pośrednio między innymi na wymianę informacji o bankach i ich produktach dostosowanych do jakości życia społeczeństwa (fora internetowe, portale społecznościowe itd.) a także na kreowanie wizerunku oraz marki.

Mając na uwadze fakt, że na ocenę końcową jakości usługi determinujący wpływ ma efekt końcowy procesu świadczenia, należy w działaniach strategicznych ochrony informacji banku zwrócić szczególną uwagę na zagrożenia dla bezpieczeństwa informacji wynikające między innymi z: dostępności, poufności, integralności, rozliczalności informacji oraz niezgodności z przepisami. Analiza ryzyk występujących w scenariuszach zagrożeń powoduje konieczność eliminacji lub minimalizacji zagrożeń lub ich efektów przez zabezpieczenie się w ramach Rekomendacji D.

Rekomendacja D zawiera 22 wytyczne szczegółowe, obejmujące cztery „obszary ryzyk" środowiska teleinformatycznego[9]:

- strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa,
- rozwój środowiska IT,
- utrzymanie i eksploatacja IT,
- zarządzanie bezpieczeństwem IT.

Rekomendacja wprowadza zdefiniowane pojęcie dotyczące bezpieczeństwa informacji jako zachowanie poufności, integralności i dostępności informacji; w ramach bezpieczeństwa informacji mogą być uwzględniane również inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (na podstawie ISO/IEC 27000:2009)[10].

Z punktu widzenia niniejszego artykułu bardzo ważna jest Szczegółowa Rekomendacja nr 16 ww. dokumentu, której brzmienie jest następujące: „Bank świadczący usługi z wykorzystaniem elektronicznych kanałów dostępu powinien posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsa-

[7] https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf (dostęp: 22.02.2017).
[8] S. Wojciechowska-Filipek, *Zarządzanie jakością informacji w organizacjach zhierarchizowanych*, Warszawa 2015, s. 11.
[9] https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf (dostęp: 22.02.2017).
[10] Tamże, s. 6.

mości i bezpieczeństwo danych oraz środków klientów, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów”[11].

Należy również podkreślić, że w punkcie 16.4. wskazano, iż „dodatkowo, bank powinien zapewnić, że: sesje połączeniowe bankowości elektronicznej są szyfrowane oraz prowadzone są dodatkowe mechanizmy, które w możliwie największym stopniu uodparniają te sesje na manipulacje”[12].

Warto w tym momencie zaznaczyć, że w procesie odpowiedniego zarządzania jakością podejmowane są działania proinnowacyjne[13], które pozwolą interesariuszom korzystać z multikanałowości banków. Oznacza to, iż obecnie interesariusze banku korzystają z przeróżnych systemów operacyjnych, które w różnym stopniu obsługują standardy dotyczące używanych protokołów internetowych mających za zadanie zabezpieczyć kanał komunikacji elektronicznej pomiędzy klientem a serwerem. Jednocześnie wykorzystują różne urządzenia końcowe – nie są to tylko komputery PC lub laptopy, ale także tablety, smartfony, iPady, czyli urządzenia mobilne.

Identyfikacja polskiego sektora bankowego

Sektor bankowy w Polsce jest jednym z najbardziej rozwijających się obszarów gospodarki. Wysoka jakość usług oferowanych przez banki wynikać może z realizowanych odpowiedzialnych strategii ukierunkowanych na wzrost efektywności i konkurencyjności. Zarządzanie jakością w bankach pozwoliło stworzyć standaryzację usług, które w znaczący sposób oddziaływały na optymalizację kosztów, a także zmianę kreowania podejścia do interesariuszy i generowania innowacyjnych produktów. Natomiast odpowiednie zarządzanie finansami banku ukierunkowane było na proces podejmowania decyzji finansowych i inwestycyjnych (pozyskiwania źródeł finansowania działalności operacyjnej od interesariuszy), ich zagospodarowania tak, aby realizować cel strategiczny, jakim jest wzrost wartości banku przy określonym regulacjami nadzorczymi poziomie ryzyka[14]. Należy jednak pamiętać, że wszystkie podejmowane działania ukierunkowane są na kształtowanie odpowiednich relacji i interakcji w ujęciu interesariusze – bank.

Obszerną analizę obszarów rozwoju bankowości przedstawiają Raporty PR-News.pl, w których poddana została ocenie działalność 19 banków działających na terenie Polski. Ze względu na tematykę publikacji, zwrócono szczególną uwagę w raportach na: liczbę klientów ogółem[15], liczbę klientów indywidualnych[16], liczbę

[11] Tamże, s. 48–49.
[12] Tamże, s. 49.
[13] M. Olkiewicz, *Knowledge management as a determinant of innovation in enterprises*, [w:] *Proceedings of the 9th International Management Conference. Management and Innovation For Competitive Advantage*, Bucharest 2015, s. 399–409.
[14] M. Capiga, *Zarządzanie bankami*, Warszawa 2010, s. 63.
[15] Każdy bank do struktury swoich klientów wlicza nie tylko osoby fizyczne, dla banku klientem są: korporacje, spółki, firmy, szkoły, gminy, miasta, stowarzyszenia, fundacje itp.
[16] Niektóre banki do klientów indywidualnych zaliczają także małe firmy, np. jednoosobowe działalności gospodarcze.

Tabela 1

Podsumowanie IV kwartału 2016 r. w polskim sektorze bankowym

Table 1

Summary of IV quarter 2016 in the Polish banking sector

Bank	[1]	[2]	[3]	[4]	[5]	[6]
PKO BP i Inteligo	9 199 000	8 756 000	8 805 000	3 579 000	6 850 000	52,25%
Bank Pekao SA	5 232 748	4 939 652	3 176 917	1 708 571	3 773 443	45,28%
mBank i Orange Finanse	4 476 000	4 455 000	3 960 712	1 982 578	3 542 509	55,97%
BZ WBK	4 400 000	4 000 000	2 875 360	1 770 338	3 120 000	56,74%
ING Bank Śląski	4 318 400	4 270 000	3 172 806	1 836 129	2 689 000	68,28%
Alior Bank	3 505 685	3 318 429	1 771 434	734 391	1 944 299	37,77%
Bank BGŻ BNP Paribas i BGŻOptima	2 600 000	2 400 000	928 825	451 072	763 006	59,12%
Credit Agricole Bank Polska	2 100 000*	1 000 000	761 715	382 092	970 610	39,37%
Bank Millennium	2 088 000	2 026 000	1 798 731	b.d.	1 898 888	b.d.
Getin Noble Bank	2 000 000*	1 900 000*	b.d.	321 200	971 300	33,07%
Eurobank	1 453 208	1 453 208	446 866	197 060	1 453 208	13,56%
Bank Pocztowy	1 324 801	1 142 918	510 867	161 912	831 235	19,48%
Raiffeisen Polbank	763 300	680 500	680 450	232 070	630 950	36,78%
Citi Handlowy	687 000	680 800	669 930	322 000	267 000	120,60%[17]
T-Mobile Usługi Bankowe	608 768	608 768	608 768	b.d.	534 171	b.d.
Deutsche Bank	396 200	356 000	296 639**	186 824***	250 000	74,73%
Plus Bank	290 129	280 536	122 980	54 640	197 903	27,61%
BOŚ	255 000*	250 000*	133 100**	b.d.	263 900****	b.d.
Santander Consumer Bank	b.d.	2 017 151	b.d.	b.d.	b.d.	b.d.
RAZEM:	**45 698 239**	**44 534 962**	**30 721 100**	**13 919 877**	**30 951 422**	

Legenda:
[1] Liczba klientów ogółem
[2] Liczba klientów indywidualnych
[3] Liczba klientów indywidualnych mających podpisaną umowę umożliwiającą korzystanie z bankowości internetowej (nie tylko ROR)
[4] Liczba klientów indywidualnych, którzy przynajmniej raz w miesiącu logują się do ROR za pomocą bankowości internetowej
[5] Liczba ROR (klienci indywidualni – jedynie konta złotowe, bez rachunków oszczędnościowych)
[6] Procentowy udział klientów aktywnych w stosunku do liczby ROR-ów
* Bank nie podał danych na koniec 2016. Przyjęto szacunki
** Deutsche Bank i BOŚ nie podały danych za IV kw. 2016 r. Przyjęto dane z III kw. 2016 r.[18]
*** Deutsche Bank nie podał danych za IV kw. 2016 r. Przyjęto dane z III kw. 2016 r.
**** BOŚ wyniki za IV kw. 206 r. poda dopiero 31.III.2016 r. Podane są dane za III kw. 2016 r.

Źródło: Opracowanie własne na podstawie PRNews.pl

[17] Niektóre banki umożliwiają aktywowanie dostępu do bankowości internetowej bez zakładania rachunku.

[18] Raport PRNews.pl: Rynek bankowości internetowej – III kw. 2016, http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-internetowej-iii-kw-2016-6553450.html (dostęp: 31.03.2017).

klientów indywidualnych mających podpisaną umowę umożliwiającą korzystanie z bankowości internetowej[19], liczbę „klientów aktywnych"[20] oraz liczbę prowadzonych przez banki ROR-ów. Mimo że nie wszystkie banki podały pełne informacje, to jednak nie zdecydowano się usunąć żadnej pozycji, gdyż uniemożliwiałoby to późniejsze porównanie otrzymanych wyników.

Wszystkie banki posiadają w swoich portfelach ogółem około 46 mln umów. Istotny dla prowadzonych rozważań jest fakt, iż aż około 30 mln z nich, to umowy umożliwiające korzystanie z bankowości elektronicznej. Również z 30 mln rachunków typu ROR około 14 mln ma aktywnych użytkowników bankowości elektronicznej. W celu lepszej prezentacji jakościowej i ilościowej wskazanych parametrów sporządzono tabelę 1.

Analiza danych w tabeli 1 pozwoliła na zidentyfikowanie, w każdej kategorii, pierwszej piątki wiodących banków oraz wyliczenie procentowego udziału aktywnych klientów w stosunku do liczby ROR-ów[21]. Głównymi parametrami i wielkościami charakteryzującymi wielką piątkę są[22]:

- liczba klientów ogółem – 60,45% (ok. 28 mln klientów);
- liczba klientów indywidualnych – 59,33% (ok. 26 mln klientów);
- liczba klientów indywidualnych mających podpisaną umowę umożliwiającą korzystanie z bankowości internetowej (nie tylko ROR) – 71,58% (ok. 22 mln klientów);
- liczba klientów indywidualnych, którzy przynajmniej raz w miesiącu logują się do ROR za pomocą bankowości internetowej – 78,14% (ok. 11 mln klientów);
- liczba ROR – 64,54% (ok. 20 mln rachunków typu ROR[23]);
- średni procentowy udział klientów aktywnych w stosunku do liczby ROR-ów – 55,70% (średnia wszystkich banków 49,37%).

Warto podkreślić, iż udział „wielkiej piątki", w każdym przedstawionym aspekcie przekracza 50% ogólnego portfela. Zatem zarządzanie bezpieczeństwem informacji ma istotne znaczenie dla rozwoju usług on-line.

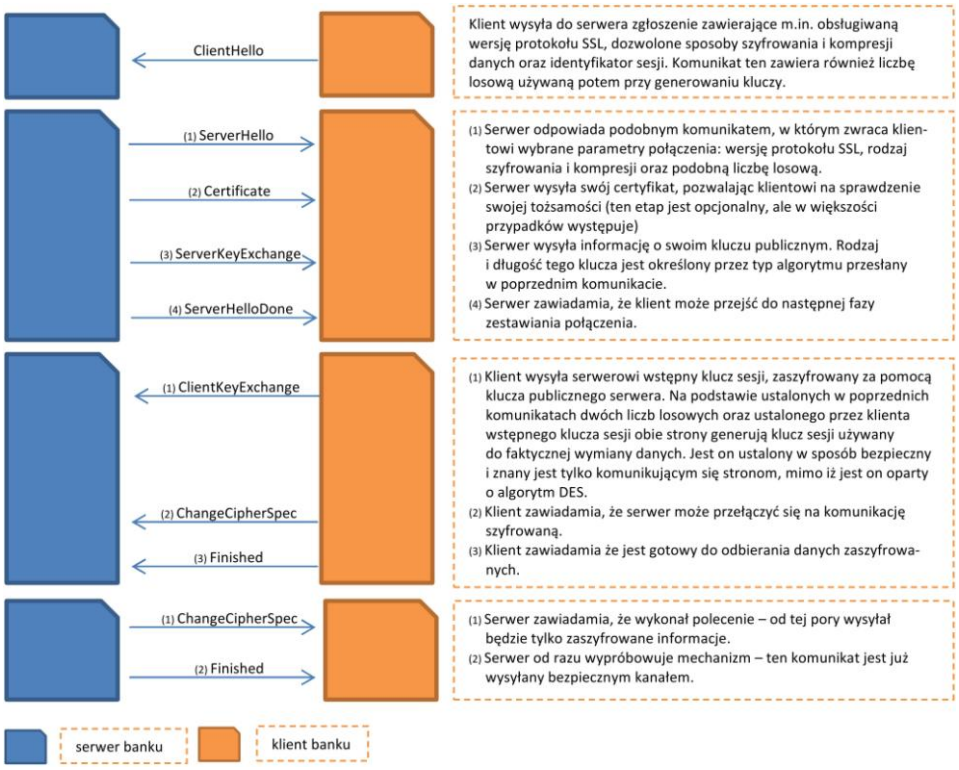
Kanał informatyczny jako uwierzytelnienie relacji serwer – klient

Podczas korzystania z usług e-bankingu musi zajść zdarzenie polegające na tym, że dwie strony (serwer i klient), które zamierzają się skomunikować ze sobą, są zobowiązane przeprowadzić „pewne" ustalenia dotyczące kanału komunikacyjnego. Podczas tego procesu dochodzi do wymiany określonych komunikatów (nazwanych standardem komunikacyjnym), w których między innymi określana jest wersja pro-

[19] Liczba umów nie dotyczy tylko i wyłącznie rachunków ROR.
[20] ROR – rachunek oszczędnościowo-rozliczeniowy.
[21] Niektóre banki umożliwiają aktywowanie dostępu do bankowości internetowej bez zakładania rachunku.
[22] Wielka piątka: PKO BP i Inteligo, Bank Pekao SA, mBank i Orange Finanse, BZ WBK, ING Bank Śląski.
[23] Klienci indywidualni – jedynie konta złotowe, bez rachunków oszczędnościowych.

tokołu[24], sposobu szyfrowania i kompresji danych. Wysyłane są również certyfikaty bezpieczeństwa, które umożliwiają sprawdzenie tożsamości jednej ze stron lub obydwóch stron.

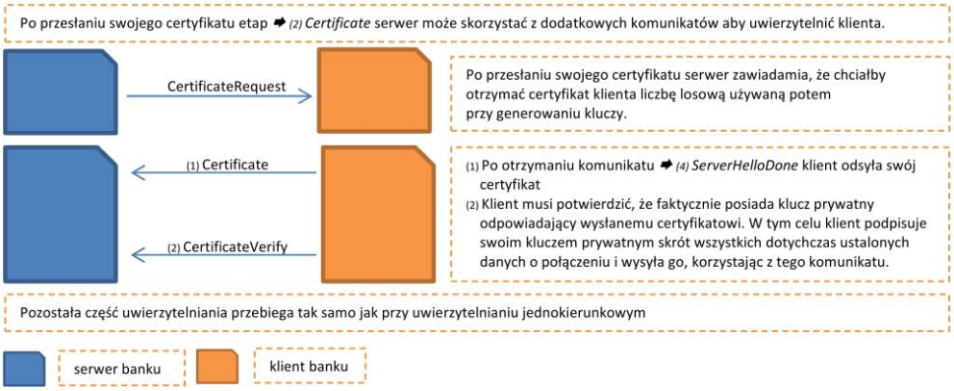
Celem przybliżenia mechanizmu działania procesu komunikacji przedstawiono na rysunku 1 schematy uwierzytelniania jednokierunkowego (uwierzytelnienie serwera) pomiędzy serwerem a klientem i na rysunku 2 uwierzytelniania dwukierunkowego (uwierzytelnienie klienta).



Rys. 1. Uwierzytelnienie jednokierunkowe – uwierzytelnienie serwera
Fig. 1. One-way authentication – server authentication

Źródło: Opracowanie własne, na podstawie https://pl.wikipedia.org/wiki/Transport_Layer_Security.

[24] Protokół SSL (ang. *Secure Socket Layer*) – protokół służący do bezpiecznej transmisji zaszyfrowanego strumienia danych i jego rozwinięcie, czyli protokół TLS (ang. *Transport Layer Security*) – protokół zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy klienta; opiera się na szyfrowaniu asymetrycznym oraz certyfikatach X.509; więcej informacji: https://pl.wikipedia.org/wiki/Transport_Layer_Security.



Rys. 2. Uwierzytelnienie dwukierunkowe – uwierzytelnienie klienta
Fig. 2. Two-way authentication - client authentication

Źródło: Opracowanie własne, na podstawie https://pl.wikipedia.org/wiki/Transport_Layer_Security.

Jak można zauważyć analizując powyższe schematy, proces uzgadniania odpowiednich poziomów bezpieczeństwa jest procesem długotrwałym oraz dodatkowo wymaga skomplikowanych obliczeń. Aby podczas przerwania kanału komunikacyjnego lub w przypadkach krótkich połączeń nie dochodziło do sytuacji ponownego zestawiania odpowiednich parametrów komunikacyjnych, istnieje możliwość kontynuowania wcześniej rozpoczętej sesji (klient musi wysłać odpowiedni komunikat ⬅ *ClientHello* zawierający parametr SessionId).

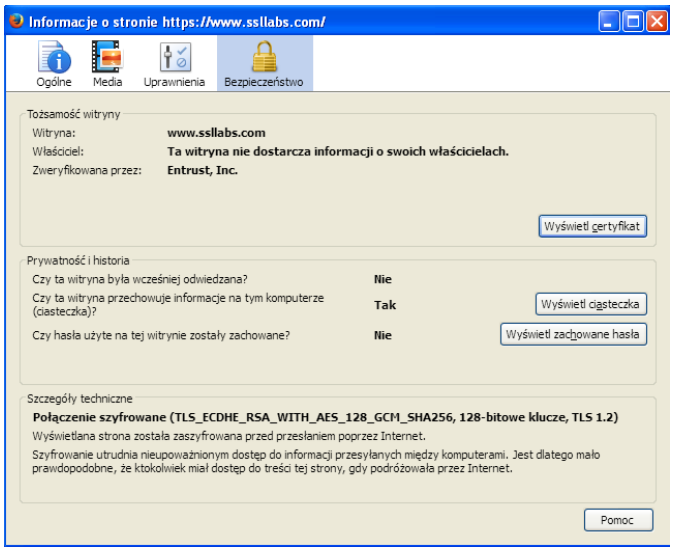
Oczywiście długość pamiętania poprzedniej sesji jest nadzorowana przez serwer i w przypadku jej minięcia klient mimo wysłania identyfikatora równego parametrowi SessionId nie będzie mógł jej kontynuować ze względu na jej przeterminowanie (wygaśnięcie).

Warto zaznaczyć, że gdyby nawet pominąć skomplikowanie ustalenia parametrów kanału komunikacyjnego na drodze klient – serwer, to i tak nie można zapomnieć o tym, iż obecne bezpieczeństwo kanału komunikacyjnego, bez względu na rodzaj użytego szyfrowania, opiera się na krytycznym parametrze określającym siłę szyfrowania, czyli długości klucza. Im dłuższy klucz, tym trudniej go złamać, a przez to odszyfrować transmisję.

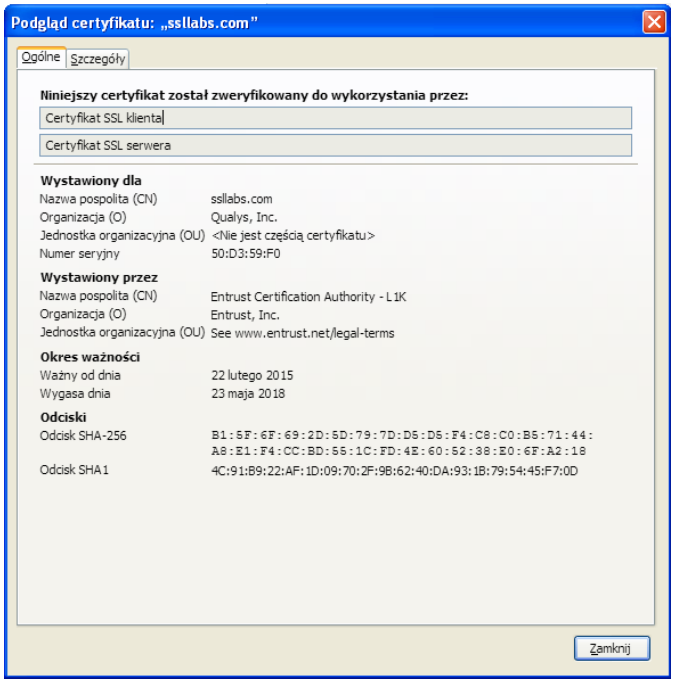
Określenie długości klucza jest wymogiem każdego banku, gdyż to właśnie on gwarantuje swemu klientowi bezpieczeństwo, gdyż przejęcie kanału komunikacyjnego i jego odszyfrowanie pozwala stronie trzeciej na dowolną modyfikację przesyłanych wiadomości przez ten kanał i np. dokonanie zmiany parametrów przelewu.

Analiza bezpieczeństwa użytej metody szyfrowania – przegląd zabezpieczeń

Klienci bankowi edukowani są, iż powinni zwracać uwagę na fakt występowania „zielonej kłódki" na pasku przeglądarki, gdyż taki stan świadczy o zabezpieczonym połączeniu. Dodatkowo wszystkie połączenia z usługami e-bankingu powinny być



Rys. 3. Informacje bezpieczeństwa dla witryny
Fig. 3. Security information for your site
Źródło: Opracowanie własne.



Rys. 4. Podgląd informacji dotyczących certyfikatu
Fig. 4. View information about the certificate
Źródło: Opracowanie własne.

poprzedzone przez adres internetowy zaczynający się od https://[25]. Cóż zatem kryje się za zieloną kłódką i protokołem https? Za pomocą zwykłego sprawdzenia bezpieczeństwa danej witryny użytkownik może się przekonać o tożsamości witryny oraz zobaczyć dla kogo i przez kogo został wystawiony certyfikat bezpieczeństwa. Przykładowa informacja, jaka jest dostępna dla użytkownika z poziomu każdej przeglądarki internetowej, przedstawiona została rysunkach 3 i 4. Rysunki przedstawiają informację na temat strony www firmy Qualys i jej produktu SSL Labs.

Warto zastanowić się, czy takie informacje wystarczają, aby stwierdzić, że dana witryna jest bezpieczna? W większości wypadków można odpowiedzieć twierdząco. Ale czy można zweryfikować tę jakość poprzez niezależne źródło? Oczywiście, że tak, gdyż w erze powszechnego dostępu do informacji i niezależnych usług nie stanowi to większego problemu.

Na potrzeby publikacji wszystkie testy[26] zostały oparte na raportach generowanych przez specjalne ogólnodostępne narzędzie[27] SSL Server Test[28]. Jednocześnie, aby ograniczyć ilość informacji przedstawionych w danym raporcie postanowiono, że pokazane zostanie tylko podsumowanie dla wielkiej piątki oraz odnośniki do raportów dla pozostałych banków.

PKO BP i INTELIGO

A. iPKO (https://www.pkobp.pl/)[29]

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów[30]: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania[31] dla TLS 1.2[32]:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,

[25] HTTPS (ang. *Hypertext Transfer Protocol Secure*), to szyfrowana wersja protokołu HTTP w relacji serwer – klient/klient – serwer, szyfrowanie to zapobiega to przechwytywaniu i zmienianiu przesyłanych danych.

[26] Zabezpieczenia oceniane są za pomocą liter: A+, A, B, C, D, E, F; gdzie A+ ocena najwyższa, zaś F ocena najniższa.

[27] Narzędzie te jest dostępne na stronach https://www.ssllabs.com/ (dostęp: 31.03.2017).

[28] Metodologia wykorzystywana podczas rankingu serwisów https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide (dostęp: 31.03.2017).

[29] https://www.ssllabs.com/ssltest/analyze.html?d=www.ipko.pl (dostęp: 31.03.2017).

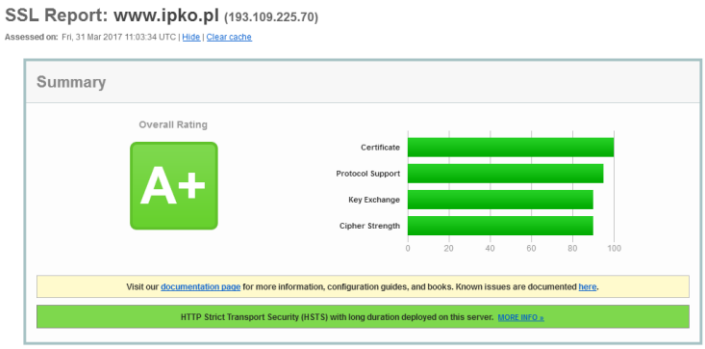
[30] Kwestia istotna ze względu na używanie danego systemu i agenta (przeglądarki internetowej, dedykowanego oprogramowania) w realizowaniu połączenia serwer – klient – nie każdy agent potrafi nawiązać połączenia, wykorzystując najlepszy/najbezpieczniejszy protokół.

[31] Tylko dla najwyższego protokołu, reszta informacji dla innych protokołów dostępna w pełnym raporcie.

[32] Algorytmy opisane zostały w dokumencie referencyjnym RFC5289, https://www.ietf.org/rfc/rfc5289.txt (dostęp: 31.03.2017).

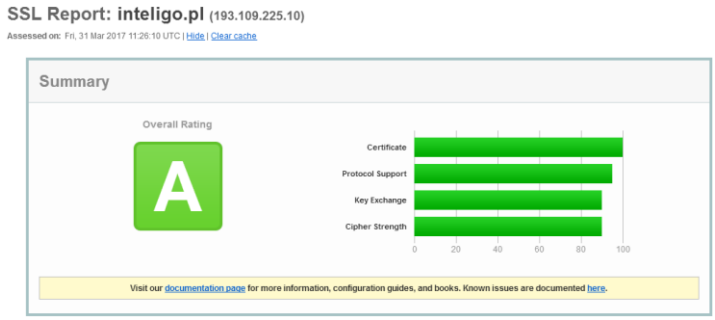
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_3DES_EDE_CBC_SHA.

- Nieudana symulacja połączenia: IE 6 / XP.



Rys. 5. Podsumowanie raportu dla ipko
Fig. 5. Summary report for ipko
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

B. Inteligo (https://inteligo.pl/secure)[33]



Rys. 6. Podsumowanie raportu dla Inteligo
Fig. 6. Summary report for Inteligo
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.*com*

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,

[33] https://www.ssllabs.com/ssltest/analyze.html?d=inteligo.pl (dostęp: 31.03.2017).

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_3DES_EDE_CBC_SHA.

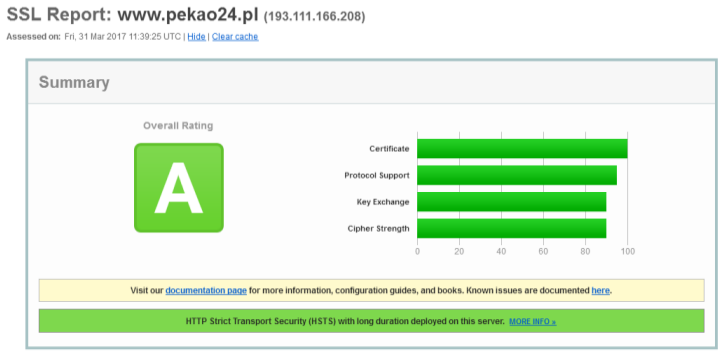
- Nieudana symulacja połączenia: IE 6 / XP.

BANK PEKAO SA

C. Pekao24 (https://www.pekao24.pl/)[34]

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  TLS_RSA_WITH_AES_256_GCM_SHA384,
  TLS_RSA_WITH_AES_256_GCM_SHA384,
  TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_RSA_WITH_AES_128_CBC_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA,
  TLS_RSA_WITH_AES_128_CBC_SHA,
  TLS_RSA_WITH_3DES_EDE_CBC_SHA.
- Nieudana symulacja połączenia: IE 6 / XP.

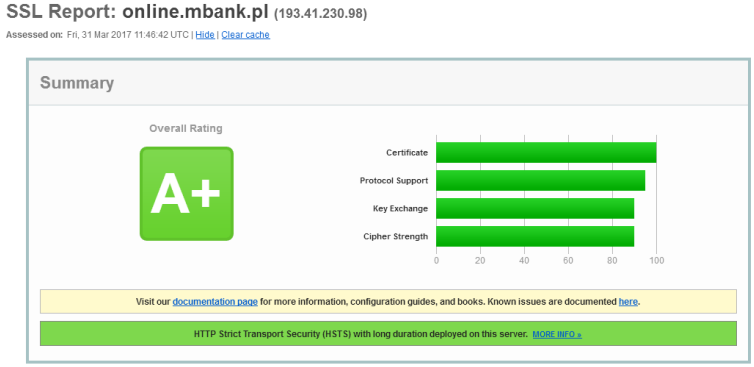


Rys. 7. Podsumowanie raportu dla Pekao24
Fig. 7. Summary report for Pekao24
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

[34] https://www.ssllabs.com/ssltest/analyze.html?d=www.pekao24.pl (dostęp: 31.03.2017).

MBANK i ORANGE FINANSE

D. mbank (https://online.mbank.pl/)[35]



Rys. 8. Podsumowanie raportu dla mbank
Fig. 8. Summary report for mbank
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  TLS_RSA_WITH_AES_256_GCM_SHA384,
  TLS_RSA_WITH_AES_128_GCM_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_RSA_WITH_AES_128_CBC_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA,
  TLS_RSA_WITH_AES_128_CBC_SHA.
- Nieudana symulacja połączenia: IE 6 / XP, IE 8 / XP.

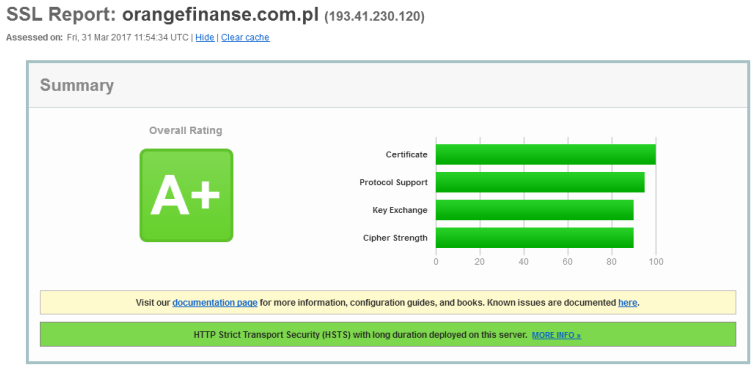
E. Orange Finanse (https://orangefinanse.com.pl/)[36]

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)

[35] https://www.ssllabs.com/ssltest/analyze.html?d=online.mbank.pl (dostęp: 31.03.20107).
[36] https://www.ssllabs.com/ssltest/analyze.html?d=orangefinanse.com.pl (dostęp: 31.03.2017).

- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  TLS_RSA_WITH_AES_256_GCM_SHA384,
  TLS_RSA_WITH_AES_128_GCM_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_RSA_WITH_AES_128_CBC_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA,
  TLS_RSA_WITH_AES_128_CBC_SHA.
- Nieudana symulacja połączenia: IE 6 / XP, IE 8 / XP.



Rys. 9. Podsumowanie raportu dla Orange Finanse
Fig. 9. Summary report for Orange Finance
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

BZ WBK

F. BZWBK24 (https://www.centrum24.pl/)[37]

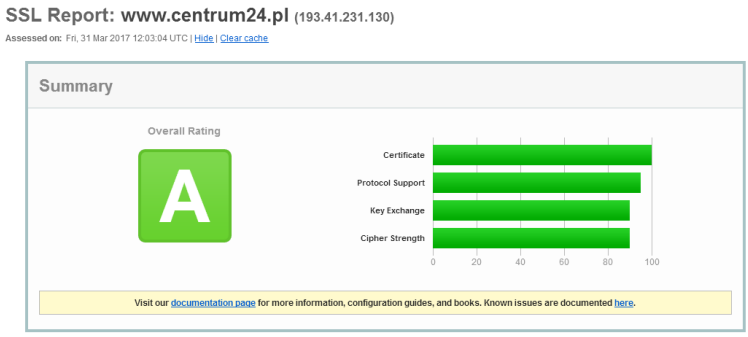
Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,

[37] https://www.ssllabs.com/ssltest/analyze.html?d=www.centrum24.pl (dostęp: 31.03.2017).

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA.

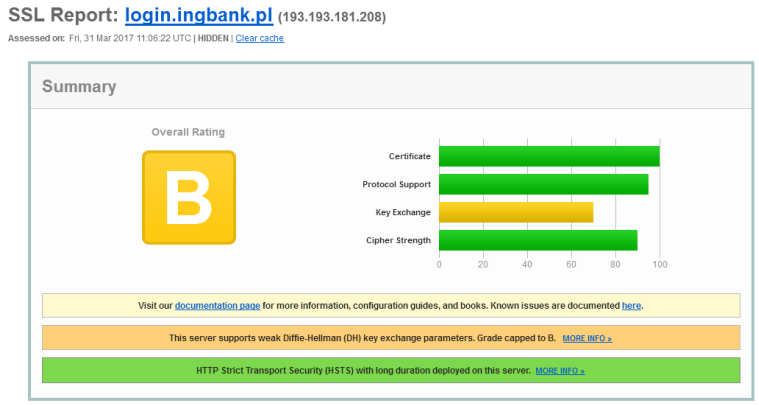
- Nieudana symulacja połączenia: IE 6 / XP, IE 8 / XP, Java 6u45.



Rys. 10. Podsumowanie raportu dla BZWBK24
Fig. 10. Summary report for BZWBK24
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

ING BANK ŚLĄSKI

G. Moje ING (https://login.ingbank.pl/)[38]



Rys. 11. Podsumowanie raportu dla Moje ING
Fig. 11. Summary report for My ING
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)

[38] https://www.ssllabs.com/ssltest/analyze.html?d=login.ingbank.pl&s=193.193.181.208 (dostęp: 31.03.2017).

- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA.
- Nieudana symulacja połączenia: IE 6 / XP.

POZOSTAŁE BANKI

Analiza pozostałych banków pozwoliła zidentyfikować i ocenić na:

- Alior Bank (https://aliorbank.pl/hades/)[39] – ocena ogólna[40] A;
- Bank BGŻ BNP Paribas i BGŻOptima (https://login.bgzbnpparibas.pl/)[41] – ocena ogólna A;
- Credit Agricole Bank Polska (https://e-bank.credit-agricole.pl/)[42] – ocena ogólna C;
- Bank Millennium (https://www.bankmillennium.pl/)[43] – ocena ogólna A+;
- Getin Noble Bank (https://secure.getinbank.pl)[44] – ocena ogólna A+;
- Eurobank (https://online.eurobank.pl/)[45] – ocena ogólna A+ z perspektywą obniżenia oceny do poziomu C;
- Bank Pocztowy (https://www.pocztowy24.pl/)[46] – ocena ogólna A;
- Raiffeisen Polbank (https://moj.raiffeisenpolbank.com/)[47] – ocena ogólna A[48];
- Citi Handlowy (https://www.online.citibank.pl/)[49] – ocena ogólna A;
- T-Mobile Usługi Bankowe (https://online.t-mobilebankowe.pl/)[50] – ocena ogólna A;
- Deutsche Bank (https://dbeasynet.deutschebank.pl/)[51] – ocena ogólna A;
- Plus Bank (https://plusbank24.pl/)[52] – ocena ogólna A;

[39] https://www.ssllabs.com/ssltest/analyze.html?d=aliorbank.pl (dostęp: 31.03.2017).
[40] poziomu zabezpieczeń.
[41] https://www.ssllabs.com/ssltest/analyze.html?d=login.bgzbnpparibas.pl (dostęp: 31.03.2017).
[42] https://www.ssllabs.com/ssltest/analyze.html?d=e-bank.credit-agricole.pl (dostęp: 31.03.2017).
[43] https://www.ssllabs.com/ssltest/analyze.html?d=www.bankmillennium.pl (dostęp: 31.03.2017).
[44] https://www.ssllabs.com/ssltest/analyze.html?d=secure.getinbank.pl (dostęp: 31.03.2017).
[45] https://www.ssllabs.com/ssltest/analyze.html?d=online.eurobank.pl (dostęp: 31.03.2017).
[46] https://www.ssllabs.com/ssltest/analyze.html?d=www.pocztowy24.pl (dostęp: 31.03.2017).
[47] https://www.ssllabs.com/ssltest/analyze.html?d=moj.raiffeisenpolbank.com (dostęp: 31.03.2017).
[48] Bank w raporcie ma wskazanie dotyczące zmiany funkcji skrótu do certyfikatu z SHA1 do SHA2. Na początku roku 2017 firma Google udostępniła dokumenty, z których jasno wynika, iż możliwe są udane, efektywne i praktyczne ataki na funkcję skrótu SHA1.
[49] https://www.ssllabs.com/ssltest/analyze.html?d=www.online.citibank.pl (dostęp: 31.03.2017).
[50] https://www.ssllabs.com/ssltest/analyze.html?d=online.t-mobilebankowe.pl (dostęp: 31.03.2017).
[51] https://www.ssllabs.com/ssltest/analyze.html?d=dbeasynet.deutschebank.pl (dostęp: 31.03.2017).
[52] https://www.ssllabs.com/ssltest/analyze.html?d=plusbank24.pl (dostęp: 31.03.2017).

- BOŚ (https://bosbank24.pl/)[53] – ocena ogólna A[54];
- Santander Consumer Bank (https://online.santanderconsumer.pl/)[55] – ocena ogólna A+ z perspektywą obniżenia oceny do poziomu C.

Podsumowanie

Zmieniające się otoczenie oraz niepewność i związane z nią ryzyko wymusza na organizacjach podejmowanie strategicznych działań. Banki poszukują metod, narzędzi, które zwiększając efektowność działania zminimalizują ryzyka i ich skutki. Jednym z obszarów ciągłego zarządzania jest jakość bezpieczeństwa informacji. Przeprowadzając analizę raportów stwierdzono, że wszystkie banki korzystają z silnego szyfrowania opartego na kluczu o długości 2048 bitów[56]. Szyfrowanie to oparte jest o szyfrowanie asymetryczne RSA. Wykazano również, że banki wspierają bezpieczne protokoły z rodziny TLS, jednocześnie wykluczając przestarzałe już protokoły SSL. Ważne jest, że wspierane protokoły posiadają wszystkie zalecane algorytmy szyfrowania. Należy również dodać, iż serwery poprawnie odrzucają przestarzałych agentów (m.in.: IE 6, IE 8 pracujących na systemie Microsoft XP; środowisko Java 6u45) oraz wspierają systemy mobilne.

Z przeprowadzonej analizy banków funkcjonujących w kraju wynika, że najgorzej z wielkiej piątki wypadła bankowość elektroniczna oferowana przez ING Bank Śląski – ocena B. Obniżenie oceny wynikło z faktu wspierania przez serwer bankowy słabego protokołu Diffiego-Hellmana[57]. Wśród pozostałych banków najgorzej zostały ocenione:

- Credit Agricole Bank Polska – ocena C, obniżenie oceny nastąpiło ze względu na fakt używania szyfru strumieniowego RC4[58] oraz za niewspieranie technologii utajnienia przekazywania[59].
- Eurobank i Santander Consumer Bank – spowodowane jest to zmianami w sys-

[53] https://www.ssllabs.com/ssltest/analyze.html?d=bosbank24.pl (dostęp: 31.03.2017).
[54] Bank w raporcie ma wskazanie dotyczące zmiany funkcji skrótu do certyfikatu z SHA1 do SHA2.
[55] https://www.ssllabs.com/ssltest/analyze.html?d=online.santanderconsumer.pl (dostęp: 31.03.2017).
[56] Dla kluczy asymetrycznych długością sugerowaną jest obecnie 2048 bitów.
[57] Protokół uzgadniania kluczy szyfrujących.
[58] RC4 należy do szyfrów strumieniowych. Używany jest w protokołach, takich jak SSL oraz WEP. Szyfr ten nie jest odporny na kryptoanalizę liniową i kryptoanalizę różnicową. Obecnie jest uznawany za niedostatecznie bezpieczny. Szyfr ten nie jest zalecany do używania w nowych systemach.
[59] Utajnienie przekazywania (ang. *Forward Secrecy* – FS) jest własnością zabezpieczonych protokołów komunikacyjnych; powoduje ono zabezpieczenie w sytuacji, gdy zostaje złamany tzw. klucz długoterminowy. Złamanie jednak tego klucza nie rodzi dalszych konsekwencji, czyli nie powoduje skompromitowania kluczy użytych w poprzednich sesjach. Jeżeli FS jest wykorzystywany, szyfrowane komunikacje oraz sesje utworzone w przeszłości nie mogą zostać odzyskane i odszyfrowane w przypadku kompromitacji haseł lub kluczy długoterminowych w późniejszymi okresie.

temie klasyfikacji[60] oraz wspieraniem szyfrowania, które nie jest już uznawane za bezpieczne[61].

Należy zauważyć, że Getin Noble Bank jest najbardziej wymagający, jeżeli chodzi o dopuszczone systemy operacyjne.

Reasumując, zielona kłódka i zaufany certyfikat wcale nie oznaczają bezpiecznego kanału informacyjnego. Zbadany też został tylko jeden aspekt bezpieczeństwa – obsługa protokołów szyfrujących po stronie serwera. Każdy kanał zaś ma dwie strony, co za tym idzie ta druga strona (klient) może mieć szereg innych mankamentów, które mogą obniżyć ogólne standardy bezpieczeństwa.

Bibliografia

Capiga M., *Zarządzanie bankami*, Warszawa 2010.

Olkiewicz M., *Knowledge management as a determinant of innovation in enterprises*, [w:] *Proceedings of the 9th International Management Conference. Management and Innovation For Competitive Advantage*, Bucharest 2015.

Olkiewicz M., *Zarządzanie jakością w sektorze bankowym w dobie wejścia do Unii Europejskiej*, [w:] *Rynki finansowe w przestrzeni elektronicznej*, red. B. Świecka, Szczecin 2004.

Wojciechowska-Filipek S., *Zarządzanie jakością informacji w organizacjach zhierarchizowanych*, Warszawa 2015.

http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-internetowej-iii-kw-2016-6553450.html (dostęp: 31.03.2017).

http://prnews.pl/raporty/raport-prnewspl-rynek-kont-osobistych-iv-kw-2016-6553975.html (dostęp: 31.03.2017).

http://prnews.pl/wiadomosc/raport-prnewspl-rynek-bankowosci-internetowej-iv-kw-2016-6554056.html (dostęp: 31.03.2017).

http://prnews.pl/wiadomosci/raport-prnewspl-liczba-klientow-w-bankach-iv-kw-2016-6554091.html (dostęp: 31.03.2017).

https://blog.qualys.com/ssllabs/2017/01/18/ssl-labs-grading-changes-january-2017 (dostęp: 31.03.2017).

https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide (dostęp: 31.03.2017).

https://www.ietf.org/rfc/rfc5289.txt (dostęp: 31.03.2017).

https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf (dostęp: 22.02.2017).

https://www.ssllabs.com/ (dostęp: 31.03.2017).

https://www.ssllabs.com/ssltest/analyze.html?d=aliorbank.pl (dostęp: 31.03.2017).

https://www.ssllabs.com/ssltest/analyze.html?d=bosbank24.pl (dostęp: 31.03.2017).

https://www.ssllabs.com/ssltest/analyze.html?d=dbeasynet.deutschebank.pl (dostęp: 31.03.2017).

[60] https://blog.qualys.com/ssllabs/2017/01/18/ssl-labs-grading-changes-january-2017 (dostęp: 31.03.2017).

[61] Kara za użycie szyfrowania 3DES w połączeniu z protokołem TLS 1.1 lub nowszym.

https://www.ssllabs.com/ssltest/analyze.html?d=e-bank.credit-agricole.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=inteligo.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=login.bgzbnpparibas.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=login.ingbank.pl&s=193.193.181.208 (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=moj.raiffeisenpolbank.com (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=online.eurobank.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=online.mbank.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=online.santanderconsumer.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=online.t-mobilebankowe.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=orangefinanse.com.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=plusbank24.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=secure.getinbank.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.bankmillennium.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.centrum24.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.ipko.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.online.citibank.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.pekao24.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.pocztowy24.pl (dostęp: 31.03.2017).

Summary

Internet banking is becoming an important part of life in the information society. Risk management in services related to broadly understood e-banking is becoming an extremely important issue, and even a factor determining the existence of a bank in cyberspace. This process must be continually monitored and rapidly modified as new threats are detected. The issue of implementing server-side procedures and their implementation in security is another important issue as well.

With the current development of internet technologies and the dangers of using them, special attention is paid to security - the "green padlock" in the browser does not give 100% certainty in the area of information security. It only tells you that the certificate is secure and has been signed by a trusted authentication center. The "green padlock" also has its security levels that affect the quality of the service provided, since the certificate, friendly application and nice layout of the site will not guarantee the security of the communication channel.